# OnCommand Insight Dokumentation

## OnCommand Insight

NetApp
October 24, 2024

This PDF was generated from https://docs.netapp.com/de-de/oncommand-insight/index.html on October 24, 2024. Always check docs.netapp.com for the latest.

# Inhalt


OnCommand Insight Dokumentation . . . 1
Versionshinweise . . . 2
  Versionshinweise . . . 2
Was ist OnCommand Insight? . . . 3
  Übersicht über OnCommand Insight . . . 3
  Insight Architektur . . . 3
  Nutzung von Insight durch Administratoren, Manager und Planer . . . 5
Installation für Linux . . . 7
  Installationsvoraussetzungen . . . 7
  Installationsanleitung für Insight . . . 14
  Aktualisieren Von Insight . . . 28
  OnCommand Insight wird deinstalliert . . . 36
Installation für Microsoft Windows . . . 39
  Installationsvoraussetzungen . . . 39
  Installationsanleitung für Insight . . . 48
  OnCommand Insight wird aktualisiert . . . 64
  Deinstallieren der Software . . . 90
Konfiguration und Administration . . . 93
  Insight einrichten . . . 93
  Insight Sicherheit . . . 189
  Unterstützung für Smart Card- und Zertifikatanmeldung . . . 215
  Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung . . . 224
  Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher) . . . 226
  Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher) . . . 228
  SSL-Zertifikate werden importiert . . . 230
  Die Hierarchie Ihrer Geschäftseinheiten . . . 233
  Anmerkungen definieren . . . 236
  Elemente werden abgefragt . . . 252
  Insight – Datenquellmanagement . . . 259
  Geräteauflösung . . . 365
  Transparenz Aufrechterhalten . . . 385
  Monitoring Ihrer Umgebung und . . . 410
  OCI Data Collector: Support Matrix . . . 441
Data Warehouse-Administration . . . 759
  Willkommen im OnCommand Insight Data Warehouse . . . 759
  Erste Schritte mit Data Warehouse . . . 765
  Administrative Aufgaben, die Sie mit Data Warehouse durchführen können . . . 787
Berichterstellung . . . 815
  Willkommen beim OnCommand Insight Reporting . . . 815
  Berichterstellung leicht gemacht . . . 819
  Verwalten von Berichten . . . 828
  Erstellen benutzerdefinierter Ad-hoc-Berichte . . . 831

Datenmodell für die Berichterstellung . . . 833
Häufig gestellte Fragen . . . 841
Allgemeine Fragen . . . 841
OnCommand Insight-Lizenzierung . . . 843
Konfiguration und unterstützte Geräte . . . 844
Skalierbarkeit und Benutzerfreundlichkeit . . . 846
Fehlerbehebung bei der Performance . . . 847
Management Ihrer Umgebung . . . 848
Integration von Insight in andere Tools . . . 849
Data ONTAP Storage-IOPS . . . 850
Anleitungen . . . 852
Erste Schritte mit Insight . . . 852
Erstellen benutzerdefinierter Dashboards . . . 867
Erstellung von Performance-Richtlinien . . . 904
Fehlerbehebung für Fibre Channel BB Credit 0-Fehler . . . 908
Analyse der Infrastruktur . . . 914
Einführung zur Risikominimierung beim Thin Provisioning . . . 919
Erfassen von Host- und VM-Dateisystemauslastungs-Daten . . . 926
Konfigurieren des Systems zur Erstellung von Chargeback-Daten . . . 930
Berichte zur I/O-Dichte beschreiben nur interne Daten-Volumes . . . 937
Erfassung von Integrationsdaten . . . 939
Analyse eines Applikations-Performance-Problems . . . 948
Erfassen und Reporting von AWS-Abrechnungsdaten . . . 956
OCI Data Collector: Support Matrix . . . 965
HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage . . . 965
Amazon AWS EC2 . . . 977
Brocade Fibre Channel Switches . . . 980
Brocade Network Advisor HTTP . . . 988
Cisco MDS und Nexus Fabric Switches . . . 991
EMC Celerra (SSH) . . . 997
EMC CLARiiON (NaviCLI) . . . 1004
EMC Data Domain (SSH) . . . 1015
EMC ECS . . . 1023
Dell EMC Isilon/PowerScale (CLI) . . . 1028
EMC PowerStore REST . . . 1042
EMC RecoverPoint (HTTP) . . . 1048
EMC Symmetrix CLI . . . 1052
Dell Unisphere-REST . . . 1064
EMC VNX (SSH) . . . 1072
EMC VNXe und Unity Unisphere (CLI) . . . 1083
EMC VPLEX . . . 1094
EMC XtremIO (HTTP) . . . 1101
NetApp E-Series . . . 1112
HDS HCP (HTTPS) . . . 1122
HiCommand Device Manager . . . 1127

HDS HNAS (CLI) . . . 1136
HPE Nimble/Alletra 6000 Storage . . . 1145
Huawei OceanStor (REST/HTTPS) . . . 1153
IBM SVC (CLI) . . . 1159
Infiniat Infinibox (HTTP) . . . 1170
Microsoft Hyper-V . . . 1177
NetApp 7-Modus . . . 1182
NetApp Clustered Data ONTAP 8.1 und höher . . . 1199
NetApp SolidFire 8.1 oder höher . . . 1223
NetApp StorageGRID (HTTPS) . . . 1234
Nutanix Storage (REST) . . . 1243
Oracle ZFS (HTTPS) . . . 1254
Pure Storage FlashArray (HTTP) . . . 1264
VMware vSphere (Web Services) . . . 1275
Rechtliche Hinweise . . . 1282
Urheberrecht . . . 1282
Marken . . . 1282
Patente . . . 1282
Datenschutzrichtlinie . . . 1282
Hinweis . . . 1282

# OnCommand Insight Dokumentation

# Versionshinweise

## Versionshinweise

Versionshinweise zu OnCommand Insight sind außerhalb des Dokumentationszentrums erhältlich. Sie werden aufgefordert, sich mit Ihren Anmeldedaten für die NetApp Support Site anzumelden.

"Versionshinweise .PDF" (Wird in einem neuen Fenster geöffnet)

# Was ist OnCommand Insight?

## Übersicht über OnCommand Insight

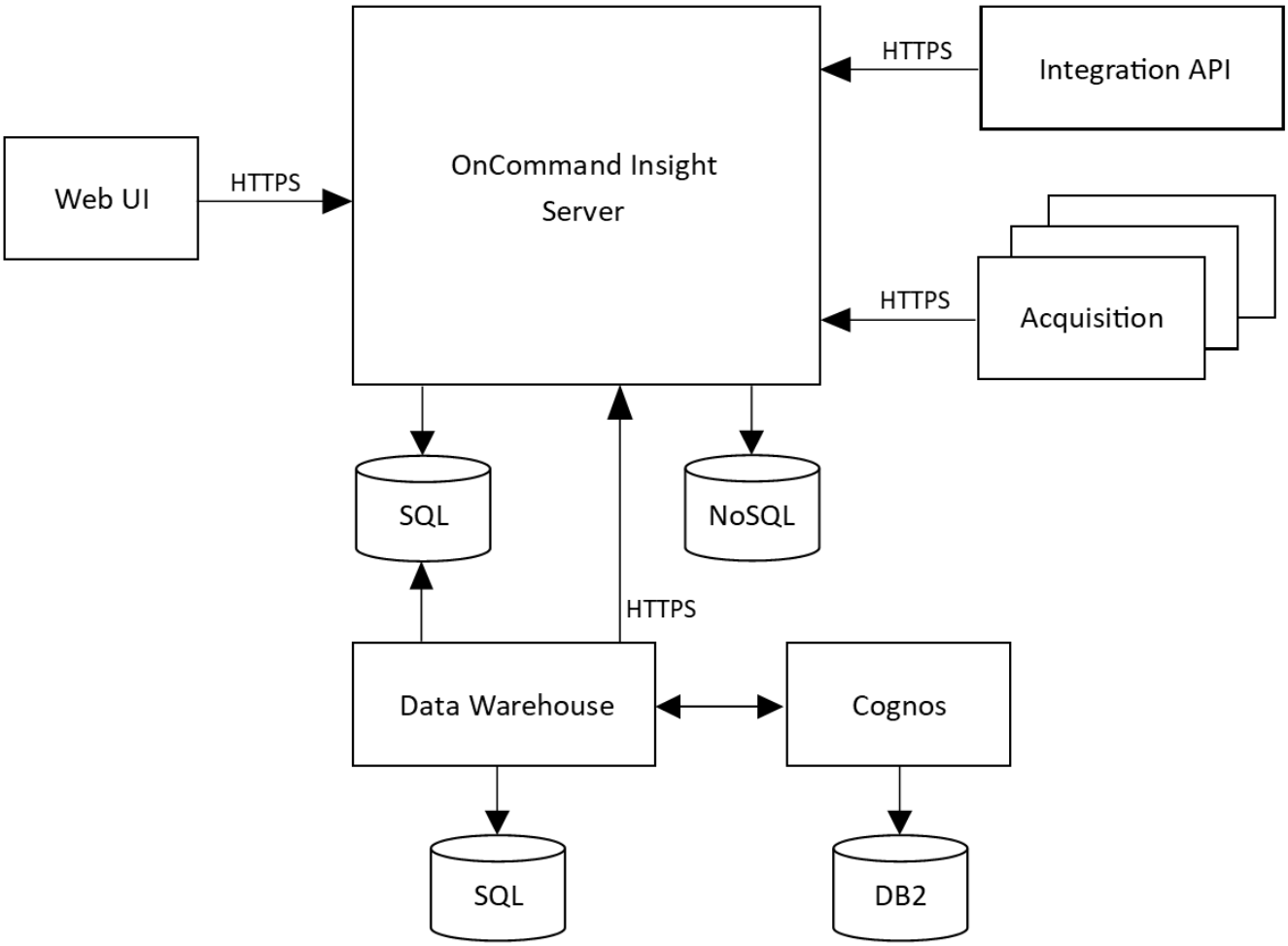
Mit OnCommand Insight vereinfachen Sie das Betriebsmanagement komplexer Private und Hybrid Clouds sowie virtueller IT-Umgebungen. Insight ist eine Einzellösung, die bereichsübergreifendes, anbieterübergreifendes Ressourcenmanagement und Analyse für Netzwerke, Storage und Server in physischen und virtuellen Umgebungen ermöglicht.

Insight hilft Ihnen, Ihre aktuelle Infrastruktur zu optimieren und Abläufe an Ihre Geschäftsanforderungen anzupassen. So können sie einfacher feststellen, wann welche Anschaffungen erforderlich sind. Es verringert zudem die Risiken während komplexer Technologiemigrationen, wie z. B. beim Wechsel in eine Hybrid Cloud, da die Lösung erkennt, welche Workloads für eine Migration in die Cloud in Frage kommen. Mit Insight lässt sich die IT-Infrastruktur als umfassender Service managen, indem die Ressourcen in die gesamte IT-Servicekette des Unternehmens integriert werden.

## Insight Architektur

Eine typische Installation von OnCommand Insight umfasst Datenerfassung und Data Warehousing mit Berichten, die über eine webbasierte Benutzeroberfläche leicht zugänglich sind. Für sicherere Umgebungen kann die Erfassung über eine Fernbedienungseinheit erfolgen.

Das folgende Diagramm zeigt die wichtigsten Komponenten der Architektur von Insight:




- **OnCommand Insight-Server**

  Der OnCommand Insight-Server enthält die wichtigsten Daten-Repositorys und Analysekomponenten. Der Server baut kontinuierlich eine End-to-End-Topologie der Umgebung auf, analysiert die Umgebung und generiert Warnmeldungen, wenn ein Vorfall oder eine Verletzung erkannt wird.

- **Akquisition**

  Die Insight Collection Engine basiert auf einer oder mehreren Erfassungseinheiten. Jeder Insight-Server enthält eine lokale Erfassungseinheit und kann Remote-Erfassungseinheiten unterstützen. Jede Einheit ist ein Dienst, der im Netzwerk ausgeführt wird und über Module, die als *Datenquellen* bezeichnet werden, Daten von Geräten im Rechenzentrum erfasst. Die von den Erfassungseinheiten erfassten Informationen werden dann zur Analyse an den Server gesendet.

  Die Sammel-Engine ist so konzipiert, dass sie sehr modular und leicht gepatcht werden kann.

- **Integrations-API**

  Eine API ermöglicht die Erfassung von Daten von externen Agenten. Integrationsdaten können über Abfragen und Widgets in der Web-Benutzeroberfläche angezeigt werden. Dashboards können „native“ Insight-Daten und Integrationsdaten enthalten. Sie können Filter, Rollups und Gruppierungen auf die Daten in diesen Dashboards anwenden.

- **Web UI**

Über die webbasierte HTML5-Benutzeroberfläche für Insight können Sie Datenquellen und Ihre Überwachungsumgebung einrichten, einschließlich Richtlinien, Schwellenwerte und Warnmeldungen. Anschließend nutzen Sie das UIAsset Dashboard und die Asset-Seiten im Internet, um potenzielle Probleme zu identifizieren und zu untersuchen. Sie können benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen, von denen jede große Flexibilität bei der Anzeige, Analyse und Dokumentation Ihrer Daten bietet.

- **Data Warehouse**

  Das OnCommand Insight Data Warehouse ist ein zentralisiertes Repository, das Daten von mehreren Insight Servern speichert und Daten zu einem gemeinsamen, mehrdimensionalen Datenmodell für Abfrage und Analyse transformiert.

  Das OnCommand Insight Data Warehouse ermöglicht den Zugriff auf eine offene Datenbank mit mehreren Datentabellen, mit denen Sie benutzerdefinierte Kapazitäts- und Performance-Berichte generieren können, beispielsweise Chargeback-Berichte, Trendberichte mit Archivdaten, Verbrauchsanalysen und Prognoseberichte.

  Das Data Warehouse konsolidiert und bereitet die Daten für die Berichterstellung für eine oder mehrere Installationen von Insight vor. Zu den Daten gehören Verlaufsdaten, Trends, Inventar, Chargeback, Showback und Datenpräsentationen, die eine langfristige Planung der Datacenter-Infrastruktur unterstützen.

- **Cognos**

  Cognos ist die Reporting Engine für Insight, ein IBM Business Intelligence Tool, mit dem Sie vordefinierte Berichte anzeigen oder benutzerdefinierte Berichte erstellen können. In den Insight Berichten werden Berichte aus den Data Warehouse-Daten generiert.

# Nutzung von Insight durch Administratoren, Manager und Planer

## OnCommand Insight liefert Informationen, die für Storage-Administratoren, Manager und Storage-Architekten für die Fehlerbehebung und Analyse entscheidend sind.

Erfahrene Storage-Administratoren nutzen OnCommand Insight zusammen mit ihren Netzwerk-Storage-Kenntnissen, um folgende typische Aufgaben durchzuführen:

- Management der SAN- und NAS-Umgebung
- Arbeiten Sie mit SAN-Technikern zusammen, um Netzwerkprobleme zu bearbeiten.
- Evaluierung, Test und Integration neuer Storage-Technologien in die Umgebung
- Behebung von Performance-Problemen, Alarmen, Richtlinienverstößen und Schwachstellen

Manager und Netzwerkplaner führen mit OnCommand Insight folgende Aufgaben aus:

- Kapazitätsplanung
- Entwicklung von Projektbudgets und -Zeitplänen
- Evaluieren und überarbeiten Sie Projektpläne, um sich ändernden Projektanforderungen gerecht zu werden.
- Verwaltung von Projektplanung und -Ausgaben

- Kauf von Hardware und Software
- Bereitstellen von Geschäftsberichten für Kapazitätsmanagement, Chargeback-Abrechnung, richtige Dimensionierung und Service Level Agreements

# Installation für Linux

## Installationsvoraussetzungen

Bevor Sie OnCommand Insight installieren, müssen Sie die aktuelle Softwareversion herunterladen, die entsprechende Lizenz erwerben und Ihre Umgebung einrichten.

Stellen Sie vor der Installation von OnCommand Insight sicher, dass folgende Informationen zur Verfügung stehen:

- OnCommand Insight-Softwaredateien im heruntergeladenen Installationspaket für die aktuelle Version
- Eine Lizenz zum Betrieb der heruntergeladenen OnCommand Insight-Version
- Minimale Hardware- und Softwareumgebung

  Das aktuelle Produkt verbraucht möglicherweise zusätzliche Hardwareressourcen (aufgrund der erweiterten OnCommand Insight-Produktfunktionen), die bei früheren Versionen des OnCommand Insight Produkts nicht in Anspruch genommen wurden.

- Ein Bereitstellungsplan, der die Hardware- und Netzwerkkonfigurationen für den OnCommand Insight-Server, das Data Warehouse und die Berichterstellung sowie die Remote-Erfassungseinheiten umfasst.

### Planen der Implementierung

Um eine erfolgreiche Bereitstellung zu gewährleisten, müssen Sie bestimmte Systemelemente berücksichtigen, bevor Sie OnCommand Insight installieren.

#### Über diese Aufgabe

Zur Planung Ihrer Insight Implementierung gehören die folgenden Systemelemente:

- Insight Architektur
- Ihre zu überwachenden Netzwerkkomponenten
- Voraussetzungen für die Insight Installation und Serveranforderungen
- Webbrowser-Anforderungen für Insight

#### Informationen zur Unterstützung der Datenquelle

Im Rahmen Ihrer Konfigurationsplanung sollten Sie sicherstellen, dass die Geräte in Ihrer Umgebung von Insight überwacht werden können. Dazu können Sie die Data Source Support Matrix für Details zu Betriebssystemen, spezifischen Geräten und Protokollen überprüfen. Einige Datenquellen sind möglicherweise nicht auf allen Betriebssystemen verfügbar.

##### Speicherort der aktuellsten Version der Data Source Support Matrix

Die Support-Matrix für die Datenquelle von OnCommand Insight wird mit jeder Service Pack-Version aktualisiert. Die aktuellste Version des Dokuments finden Sie unter "NetApp Support Website". .

### Geräteerkennung und Planung der Datenquelle

## Im Rahmen Ihrer Bereitstellungsplanung sollten Sie Informationen zu den Geräten in Ihrer Umgebung sammeln.

Sie benötigen die folgende Software, Konnektivität und Informationen zu jedem Gerät in Ihrer Umgebung:

- IP-Adresse oder Hostname, der vom OCI-Server aufgelöst werden kann
- Anmeldename und Passwort
- Art des Zugriffs auf das Gerät, z. B. Controller und Management Station

> Der schreibgeschützte Zugriff ist für die meisten Geräte ausreichend, für einige Geräte sind jedoch Administratorberechtigungen erforderlich.

- Port-Konnektivität mit dem Gerät, je nach den Anforderungen an den Port der Datenquelle
- Für Switches, SNMP-schreibgeschützte Community-Zeichenfolge (Benutzer-ID oder Passwort für den Zugriff auf die Switches)
- Software von Drittanbietern, die auf dem Gerät benötigt wird, z. B. Solutions Enabler.
- Weitere Informationen zu den Berechtigungen und Anforderungen der Datenquelle finden Sie in der Hilfe zur Webbenutzeroberfläche oder im *OnCommand Insight Konfigurations- und Administrationshandbuch*.

### Von OnCommand Insight generierter Netzwerkverkehr

## Der von OnCommand Insight erzeugte Netzwerkdatenverkehr, die Menge der verarbeiteten Daten, die das Netzwerk durchlaufen, und die von OnCommand Insight auf Geräten aufbereitete Last unterscheiden sich durch viele Faktoren.

Der Datenverkehr, die Daten und die Last unterscheiden sich je nach Umgebung anhand der folgenden Faktoren:

- Rohdaten
- Konfiguration von Geräten
- Implementierungstopologie von OnCommand Insight
- Verschiedene Abfrageintervalle für die Bestandsaufnahme und Performance-Datenquellen, die reduziert werden können, um langsame Geräte zu erkennen oder die Bandbreite zu erhalten

Es können große Unterschiede bei den Rohdaten, die OnCommand Insight sammelt, gegeben sein.

Das folgende Beispiel zeigt, wie die Konfigurationsdaten variieren können und wie Datenverkehr, Daten und Last von vielen Konfigurationsfaktoren beeinflusst werden. Beispielsweise könnten Sie zwei Arrays mit jeweils 1,000 Festplatten verwenden:

- Array 1: Hat 1,000 SATA-Festplatten alle 1 TB Größe. Alle 1,000 Festplatten befinden sich in einem Speicherpool, und es gibt 1,000 LUNs, die alle denselben 32 Nodes in einem ESX Cluster bereitgestellt (zugeordnet und maskiert) werden.
- Array 2: Verfügt über 400 2-TB-Datenfestplatten, 560 600-GB-FC-Festplatten und 40 SSDs. Es gibt 3 Speicherpools, aber 320 der FC-Festplatten werden in herkömmlichen RAID-Gruppen verwendet. Die auf die RAID-Gruppen geschnitzten LUNs verwenden einen traditionellen Maskierungstyp (symmaskdb), während die Thin Provisioning, Pool-basierten LUNs einen neueren Maskierungstyp (symmaskdb)

verwenden. Es sind 600 LUNs auf 150 verschiedenen Hosts präsentiert. Es gibt 200 BCVs (Full Block Replikatvolumes von 200 der 600 LUNs). Es gibt auch 200 R2-Volumes, Remote-Replikatvolumes von Volumes, die auf einem Array an einem anderen Standort vorhanden sind.

Diese Arrays haben jeweils 1,000 Festplatten und 1,000 logische Volumes. Möglicherweise sind sie physisch mit der Menge an Rack-Platz identisch, die sie im Datacenter verbrauchen. Vielleicht wird sogar dieselbe Firmware ausgeführt, aber das zweite Array ist in seiner Konfiguration viel komplexer als das erste Array.

## Deinstallieren von MariaDB

Sie müssen MariaDB auf den Insight- oder Data Warehouse-Servern deinstallieren, bevor Sie OnCommand Insight oder das Data Warehouse installieren. Andernfalls können Sie mit der Installation nicht fortfahren. MySQL ist nicht kompatibel mit MariaDB. Wenn Sie eine Installation auf einem der Server versuchen, ohne MariaDB zu entfernen, wird die Installation mit einer Fehlermeldung beendet, die Sie auffordert, MariaDB zu deinstallieren.

### Bevor Sie beginnen

Sie müssen über Sudo-Berechtigungen verfügen.

### Schritte

1. Melden Sie sich beim Insight Server an.
2. Eine Liste der MariaDB-Komponenten abrufen:

   ```
   rpm -qa | grep mariadb
   ```

3. Geben Sie für jede auf dem Server installierte MariaDB-Komponente Folgendes ein:

   ```
   yum remove component_name
   ```

## Anforderungen für Insight Server

Es wird ein dedizierter Server empfohlen. Installieren Sie Insight nicht auf einem Server, auf dem andere Anwendungen installiert sind. Sowohl physische als auch virtuelle Server werden unterstützt, sofern die Produktanforderungen erfüllt sind.

Sie müssen über sudo-Berechtigungen verfügen, um die OnCommand Insight-Serversoftware zu installieren.

Für einige Insight Komponenten sind möglicherweise während der Installation abhängige Pakete erforderlich. Vergewissern Sie sich, dass vor der Installation von Insight auf das YUM-Repository zugegriffen werden kann.

Die Dimensionierung für OnCommand Insight weist mehrere Abhängigkeiten auf, wie z. B. Art und Größe der Datenquelle, Anzahl der Assets in Ihrer Umgebung, Abfrageintervalle und mehr. Die folgenden Beispiele zur Größenbestimmung sind nur Richtlinien und stellen einige der Umgebungen dar, in denen Insight getestet wurde. Wenn sich diese oder andere Faktoren in der Umgebung ändern, können sich die Dimensionierungsanforderungen für Insight ändern. Diese Richtlinien enthalten Speicherplatz für Performance-Archivdaten von bis zu 90 Tagen.

Vor der Installation oder dem Upgrade der Insight sollten Sie sich an Ihren Sales Engineer wenden, um eine

detaillierte Anleitung zur Größenbemessung zu erhalten.

**Beispiele:**

| Umgebungsfaktoren: | Getesteter Festplattenspeicher, CPUs und Speicher: |
|---|---|
| 80 Storage-Volume4.000<br><br>4,000 VMs<br><br>4,000 Switch-Ports | 250 GB Festplattenspeicherplatz 8 Kerne<br><br>32 GB RAM |
| 160 Storage-Volume40.000<br><br>8,000 VMs<br><br>8,000 Switch-Ports | 1 TB Festplattenspeicherplatz, 12 Kerne<br><br>48 GB RAM |

**Voraussetzungen:**

| Komponente | Erforderlich |
|---|---|
| Betriebssystem | Ein Computer, auf dem eine lizenzierte Version einer der folgenden Versionen ausgeführt wird, auf dem keine andere Software auf Anwendungsebene ausgeführt wird:<br><br>• Red Hat Enterprise Linux 7.9, 8.10, 9.4<br>• CentOS 8 Stream, CentOS 9 Stream<br>• Oracle Enterprise Linux 7.9, 8.10, 9.4<br><br>Eine lizenzierte Version stellt sicher, dass Abhängigkeiten, die von der Installation benötigt werden, automatisch vom Betriebssystem behoben werden.<br><br>Sie müssen MariaDB deinstallieren, bevor Sie Insight installieren.<br><br>Durch die Deinstallation von MariaDB wird auch der Postfix Mail Transport Agent entfernt.<br><br>Es wird ein dedizierter Server empfohlen. |
| Virtuelle Maschine (VM) | Diese Komponente kann in einer virtuellen Umgebung ausgeführt werden, sofern die CPU- und Arbeitsspeicherressourcen für Ihre Instanz reserviert sind. |

| | |
|---|---|
| Arbeitsspeicher und CPU | 24 BIS 256 GB RAM<br><br>8 - 32 Kerne |
| Verfügbarer Festplattenspeicher | 100 GB - 3 TB installiere Festplattenspeicher<br><br>50 GB - 1 TB Performance Archiv Speicherplatz<br><br>Die folgenden Partitionsausfälle werden für eine Beispiel-500-GB-Umgebung empfohlen:<br><br>• /Opt Verzeichnis — 50 GB<br>• /Var/log Directory — 100 GB<br>• Verzeichnis /var/lib — 350 GB<br><br>Es ist eine Best Practice zu montieren `/opt` Und `/var` Auf separaten Datenträgern aus dem Root-Dateisystem (`/`).<br><br>Für den Insight-Installationsbereich werden SSD-Festplatten empfohlen. |
| Netzwerk | Ethernet-Verbindung und -Ports:<br><br>• Ethernet-Verbindung mit 100 Mbit/s oder 1 Gbit/s mit dedizierter (statischer) IP-Adresse und IP-Konnektivität zu allen Komponenten im SAN, einschließlich FC-Geräten und Remote-Akquisitionseinheiten.<br>• Die Portanforderungen für den OnCommand Insight-Serverprozess sind 80, 443, 1090 bis 1100, 3873, 8083, 4444 bis 4446, 5445, 5455, 4712 bis 4714, 5500, Und 5501.<br>• Die Port-Anforderungen für den Akquisitionsprozess sind 12123 und 5679.<br>• Die Portanforderung für MySQL ist 3306.<br>• Die Portanforderungen für Elasticsearch lauten 9200 und 9310<br><br>Die Ports 443 und 3306 erfordern externen Zugriff über jede vorhandene Firewall. |

| | |
|---|---|
| Berechtigungen | Sudo-Berechtigungen sind auf dem OnCommand Insight-Server erforderlich.<br><br>Wenn einer der folgenden Ordner symbolische Links sind, stellen Sie sicher, dass die Zielverzeichnisse über '755'-Berechtigungen verfügen.<br><br>• /Opt/netapp<br>• /Var/lib/netapp<br>• /Var/log/netapp |
| Remote-Konnektivität | Internetverbindung für den WebEx-Zugriff oder eine Remote-Desktop-Verbindung, um den Support bei der Installation und nach der Installation zu erleichtern. |
| Zugänglichkeit | HTTPS-Zugriff ist erforderlich. |
| HTTP- oder HTTPS-Server | Apache HTTP-Server oder andere HTTPS-Server sollten nicht mit denselben Ports (443) konkurrieren wie der OnCommand Insight-Server und sollten nicht automatisch gestartet werden. Wenn sie auf Port 443 hören müssen, müssen Sie den OnCommand Insight-Server so konfigurieren, dass andere Ports verwendet werden. |

## Serveranforderungen für Data Warehouse

Der Data Warehouse-Server muss auf einem Computer ausgeführt werden, der mit den bestehenden Hardware- und Softwareanforderungen kompatibel ist. Sie müssen sicherstellen, dass der Apache-Webserver oder die Berichterstellungssoftware nicht bereits auf diesem Computer installiert ist.

Die Größenbestimmung für OnCommand Insight umfasst mehrere Abhängigkeiten, wie z. B. Anzahl der Assets in Ihrer Umgebung, Menge der gespeicherten Archivdaten und vieles mehr. Die folgenden Beispiele zur Größenanpassung eines Data Warehouses sind nur Richtlinien und stellen einige der Umgebungen dar, in denen Insight getestet wurde. Wenn sich diese oder andere Faktoren in der Umgebung ändern, können sich die Dimensionierungsanforderungen für Insight ändern.

Vor der Installation oder dem Upgrade der Insight sollten Sie sich an Ihren Sales Engineer wenden, um eine detaillierte Anleitung zur Größenbemessung zu erhalten.

**Beispiele:**

| Umgebungsfaktoren: | Getesteter Festplattenspeicher, CPUs und Speicher: |
|---|---|
| 18 Storage-Arrays3.400 VMs<br><br>4,500 Switch-Ports | 200-GB-Festplatte, 8 Kerne<br><br>32 GB RAM |

| | |
|---|---|
| 110 Storage-Arrays11'500 VMs<br><br>14,500 Switch-Ports | 300-GB-Festplatte, 8 Kerne<br><br>48 GB RAM |

**Voraussetzungen:**

| Komponente | Erforderlich |
|---|---|
| Betriebssystem | Ein Computer, auf dem eine lizenzierte Version einer der folgenden Versionen ausgeführt wird, auf dem keine andere Software auf Anwendungsebene ausgeführt wird:<br>• Red Hat Enterprise Linux 7.9, 8.10, 9.4<br>• CentOS 8 Stream, CentOS 9 Stream<br>• Oracle Enterprise Linux 7.9, 8.10, 9.4 |
| Virtuelle Maschine (VM) | Diese Komponente kann in einer virtuellen Umgebung ausgeführt werden, sofern die CPU- und Arbeitsspeicherressourcen für Ihre Instanz reserviert sind. |
| CPU | 8 bis 40 CPU-Kerne |
| Speicher | 32 GB - 2 TB RAM |
| Verfügbarer Festplattenspeicher | 200 GB - 512 GB freier Festplattenspeicher im sollten mindestens 50 GB freier Festplattenspeicher vorhanden sein `/var/lib` Partition und 25 GB freier Festplattenspeicher im `/opt` Und `/var/log` Partitionen: |
| Netzwerk | • Ethernet-Verbindung mit 100 Mbit/s oder 1 Gbit/s.<br>• Statische IP-Adresse<br>• Für den OnCommand Insight DWH-Serverprozess, Ports 80, 443, 1098, 1099, 3873, 8083 und 4444 bis 4446<br>• Für MySQL, Port 3306 |

## Anforderungen an den Remote Acquisition Unit-Server

Sie müssen eine Remote Acquisition Unit (rau) installieren, um Informationen von SAN-Geräten zu erhalten, die sich hinter einer Firewall, an einem Remote-Standort, in einem privaten Netzwerk oder in verschiedenen Netzwerksegmenten befinden. Bevor Sie die rau installieren, sollten Sie sicherstellen, dass Ihre Umgebung den Anforderungen an das rau-Betriebssystem, die CPU, den Arbeitsspeicher und den Festplattenspeicher

entspricht.

| Komponente | Anforderungen |
| --- | --- |
| Betriebssystem | Ein Computer, auf dem eine lizenzierte Version einer der folgenden Versionen ausgeführt wird, auf dem keine andere Software auf Anwendungsebene ausgeführt wird:<br>• Red Hat Enterprise Linux 7.9, 8.10, 9.4<br>• CentOS 8 Stream, CentOS 9 Stream<br>• Oracle Enterprise Linux 7.9, 8.10, 9.4<br>Es wird ein dedizierter Server empfohlen. |
| CPU | 4 CPU-Kerne |
| Speicher | 16 GB RAM |
| Verfügbarer Festplattenspeicher | 40 GB |
| Netzwerk | 100 Mbit/s /1 Gbit/s Ethernet-Verbindung, statische IP-Adresse, IP-Verbindung zu allen FC-Geräten und ein erforderlicher Port zum OnCommand Insight-Server (80 oder 443). |
| Berechtigungen | Sudo-Berechtigungen auf dem rau-Server |

### Von OnCommand Insight unterstützte Browser

Die browserbasierte OnCommand Insightweb-Benutzeroberfläche kann auf mehreren verschiedenen Browsern betrieben werden.

Insight unterstützt neuere Versionen von nicht-Beta-Versionen der folgenden Browser:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Eine vollständige Liste aller für OnCommand Insight qualifizierten Browser-Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

# Installationsanleitung für Insight

Für die Installation müssen mehrere OnCommand Insight Komponenten, Insight Server und Data Warehouse installiert werden.

Die Installation umfasst die folgenden Hauptaufgaben:

- Herunterladen des OnCommand Insight-Installationsprogramms
- OnCommand Insight-Server wird installiert
- Installieren von Lizenzen
- Optional Installation von DWH und Reporting (muss auf einer separaten Maschine oder virtuellen Maschine installiert sein. Für die Berichterstellung ist Microsoft Windows erforderlich.)
- Optional können Sie eine Remote Acquisition Unit (rau) installieren, die Informationen von den Geräteressourcen erfasst, die sich hinter einer Firewall befinden, sich an einem Remote-Standort befinden oder sich in einem privaten Netzwerk befinden

Nach der Installation müssen Sie Insight konfigurieren, um Informationen über Ihre Umgebung zu erfassen. Die erforderlichen Aufgaben werden im *OnCommand Insight Konfigurations- und Administrationshandbuch* beschrieben.

## Herunterladen des OnCommand Insight-Installationsprogramms

Sie können das OnCommand Insight Installationsprogramm von der NetApp Support-Website herunterladen.

### Bevor Sie beginnen

Sie müssen sich auf der NetApp Support Site unter anmelden "mysupport.netapp.com".

Darüber hinaus müssen Sie über ein Entzip-Dienstprogramm verfügen, mit dem Sie die Installation öffnen können `.ZIP` Dateien:

### Schritte

1. Melden Sie sich bei dem Server an, auf dem Sie OnCommand Insight installieren möchten.
2. Laden Sie die Installationsdatei von der NetApp Support-Website herunter.

## Installieren des OnCommand Insight-Servers

Der OnCommand Insight-Server wird über die Befehlszeile installiert.

### Bevor Sie beginnen

Sie müssen alle Installationsvoraussetzungen erfüllt haben.

### Schritte

1. Melden Sie sich beim Insight-Server mit einem Konto mit sudo-Berechtigungen an.
2. Navigieren Sie zu dem Verzeichnis auf dem Server, in dem sich die Installationsdateien befinden, und geben Sie den folgenden Befehl ein:

   ```
   unzip oci-<version>-linux-x86_64.zip
   ```

   Überprüfen Sie die Versionsnummer der Installationsdatei. Die Versionsnummer kann sich von der im Befehl angezeigten Versionsnummer unterscheiden.

3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh` :

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
```

4. Führen Sie das Installationsskript aus:

   ```
   sudo ./oci-<version>-linux-x86_64/oci-install.sh
   ```

   Bei der Installation von Insight Server unter CentOS 9 Stream, Red hat Enterprise Linux 9.4 oder Oracle Linux 9.4 müssen Sie zuerst in das Verzeichnis wechseln, das die Installer-Datei enthält, und dann den Befehl install mit der Befehlszeilenoption "--install-mysql-dependencies" ausführen:

   ```
   cd /tmp/oci-7.3.16.1.297-linux-x86_64
   sudo ./oci-install.sh --install-mysql-dependencies
   ```

5. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie und befolgen Sie die Anweisungen.
6. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Senden von Nutzungsinformationen an NetApp aktivieren. Eingabe `Y` An dieser Eingabeaufforderung.

**Ergebnisse**

Nachdem Sie alle Eingabeaufforderungen beantwortet haben, beginnt die Installation und sollte je nach installierter Anwendung ca. 10 Minuten dauern.

1. Wenn Sie eine Remote Acquisition Unit (rau) installieren, müssen Sie das SecurityAdmin-Tool ausführen, um ein Passwort für den Benutzer *Acquisition* zu erstellen. Sie benötigen dieses Passwort, wenn Sie die rau installieren.

   Hinweis: Wenn Sie dieses Passwort erstellt haben, müssen Sie den Server und die rau wie unten angegeben synchronisieren.

**Server mit DWH und rau synchronisieren**

Nach der Installation der Remote-Erfassungseinheit und/oder des Data Warehouse müssen Sie die rau/DWH mit dem OnCommand Insight-Server synchronisieren. Führen Sie die folgenden Schritte aus:

"Server und rau synchronisieren (Windows)"

"Server und DWH synchronisieren (Windows)"

"Server und rau synchronisieren (Linux)"

"Server und DWH synchronisieren (Linux)"

## OnCommand Insight Data Warehouse wird installiert

Die Installation ist in sich geschlossen und beinhaltet die Elemente, die für den Betrieb und Betrieb des OnCommand Insight Data Warehouse (DWH) erforderlich sind.

### Bevor Sie beginnen

Sie müssen alle Installationsvoraussetzungen erfüllt haben.

### Über diese Aufgabe

Data Warehouse verfügt über Cognos-Berichtsfunktionen. Wenn Sie Insight auf einem Linux-Server installieren, können Sie diese Funktionen jedoch nur verwenden, wenn Sie das Data Warehouse auf einem Windows-Server installieren. Informationen zur Installation des Data Warehouse unter Windows und Cognos-Berichtsfunktionen finden Sie im *OnCommand Insight-Installationshandbuch für Microsoft Windows*.

### Schritte

1. Melden Sie sich beim Data Warehouse-Server mit einem Konto mit sudo-Berechtigungen an.
2. Navigieren Sie zu dem Verzeichnis auf dem Server, in dem sich die Installationsdateien befinden, und geben Sie den folgenden Befehl ein:

   `unzip oci-dwh-<version>-linux-x86_64.zip`

   Überprüfen Sie die Versionsnummer der Installationsdatei. Die Versionsnummer kann sich von der im Befehl angezeigten Versionsnummer unterscheiden.

3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh` Bevor Sie mit der Installation beginnen:

   `sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help`

4. Führen Sie das Installationsskript aus:

   `sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh`

   Wenn Sie Insight Server oder Data Warehouse auf CentOS 9 Stream, Red hat Enterprise Linux 9.4 oder Oracle Linux 9.4 installieren, müssen Sie zuerst in das Verzeichnis wechseln, das die Installer-Datei enthält, und dann den Befehl install mit der Befehlszeilenoption "--install-mysql-dependencies" ausführen:

   ```
   cd /tmp/oci-7.3.16.1.297-linux-x86_64
   sudo ./oci-install.sh --install-mysql-dependencies
   ```

5. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie und befolgen Sie die Anweisungen.

### Ergebnisse

Nachdem Sie alle Eingabeaufforderungen beantwortet haben, beginnt die Installation und sollte je nach installierter Anwendung ca. 10 Minuten dauern.

### Server und DWH synchronisieren

Nach der Installation des Data Warehouse müssen Sie das Data Warehouse mit dem OnCommand Insight Server synchronisieren. Führen Sie hierzu folgende Schritte aus:

1. Starten Sie auf dem OnCommand Insight-Serversystem das Tool **SecurityAdmin** im interaktiven Modus

```
 securityadmin -i
. Ändern Sie das Passwort für die Benutzer _inventar_ und _dwh_internal_
in Passwörter Ihrer Wahl. *Beachten Sie diese Passwörter*, da Sie sie
unten benötigen.
. Starten Sie den DWH-Dienst neu
. Starten Sie bei *each Connector* das Tool *SecurityAdmin* im
interaktiven Modus. Sie benötigen die Passwörter, die Sie in Schritt 2
oben angegeben haben.
```

```
 securityadmin -i
. Ändern Sie die Passwörter für die Benutzer _inventar_ und
_dwh_internal_ in die in Schritt 2 verwendeten Passwörter.
. Starten Sie die Dienste auf den Connectors neu.
. Fügen Sie die Connectors zu DWH hinzu, indem Sie die Passwörter für
_Inventory_ und _dwh_Internal_ Benutzer aus Schritt 2 verwenden
```

## Installieren einer Remote-Erfassungseinheit

Sie können eine oder mehrere Remote-Erfassungseinheiten (Raus) in Ihrer OnCommand Insight-Umgebung installieren. Erfassungseinheiten laufen im Netzwerk, das (über Module namens Data *sources*) zugreift und Daten von verschiedenen Geräten im Rechenzentrum sammelt.

#### Bevor Sie beginnen

Sie müssen alle Installationsvoraussetzungen erfüllt haben.

Mindestens ein Port muss offen und zwischen dem rau-Server und dem OnCommand Insight-Server verfügbar sein, um Änderungsinformationen an den Server weiterzuleiten. Wenn Sie sich darüber nicht sicher sind, validieren Sie ihn, indem Sie einen Webbrowser auf dem rau-Computer öffnen und ihn zum OnCommand Insight-Server leiten:

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

Der Erfassungsport ist standardmäßig auf 443 eingestellt, aber er hat sich möglicherweise während der Serverinstallation geändert. Wenn die Verbindung erfolgreich war, wird eine OnCommand Insight-Antwortseite angezeigt, die einen offenen und verfügbaren Port zwischen der rau und dem OnCommand Insight-Server anzeigt.

In Umgebungen, in denen Network Address Translation oder Port Address Translation (NAT/PAT: I.e, beliebige Übersetzung von IP-Adressen) verwendet wird, unterstützt Insight nur das Einfügen einer RAU zwischen NAT und dem Gerät.

- Unterstützt: OnCommand Insight -> NAT -> rau -> Gerät
- Nicht unterstützt: OnCommand Insight -> rau -> NAT -> Gerät

**Schritte**

1. Melden Sie sich beim rau-Server mit einem Konto mit sudo-Berechtigungen an.
2. Navigieren Sie zu dem Verzeichnis auf dem Server, in dem sich die Installationsdateien befinden, und geben Sie den folgenden Befehl ein:

   ```
   unzip oci-rau-<version>-linux-x86_64.zip
   ```

3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh`:

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
   ```

4. Führen Sie das Installationsskript aus:

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
   ```

5. Lesen Sie die Lizenzvereinbarung, akzeptieren Sie sie, und befolgen Sie dann die Anweisungen.

   Nachdem Sie alle Eingabeaufforderungen beantwortet haben, beginnt die Installation und sollte je nach installierter Anwendung ca. 10 Minuten dauern.

Wenn Ihre Daten zu erfassen beginnen, sind Sie alle eingestellt; Sie müssen den Server und die rau wie unten angegeben synchronisieren.

**Server und rau synchronisieren**

Wenn die Datenerfassung nach der Installation der Remote-Erfassungseinheit nicht beginnt, synchronisieren Sie die rau mit dem OnCommand Insight-Server. Führen Sie hierzu folgende Schritte aus:

1. Starten Sie auf dem OnCommand Insight-Serversystem das Tool **SecurityAdmin** im interaktiven Modus

   ```
    securityadmin -i
   . Ändern Sie das Passwort für den Benutzer _Acquisition_ für den Insight
   Server in ein Passwort Ihrer Wahl. *Bitte beachten Sie dieses Passwort*
   wie Sie es unten benötigen.
   . Starten Sie den Server/LAU neu.
   . Starten Sie auf dem rau-System (Remote Acquisition Unit) das Tool
   *SecurityAdmin* im interaktiven Modus. Sie benötigen das Passwort, das
   Sie in Schritt 2 oben angegeben haben.
   ```

   ```
    securityadmin -i
   . Ändern Sie das Passwort für den Benutzer _Acquisition_ auf das in
   Schritt 2 verwendete Passwort.
   . Starten Sie den RAU neu.
   ```

#### Überprüfen der Installation der Fernbedienungseinheit

Um die ordnungsgemäße Installation der Remote Acquisition Unit zu überprüfen, können Sie den Status der Remote Acquisition Units anzeigen, die mit Ihrem Server verbunden sind.

##### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Acquisition Units**.
3. Überprüfen Sie, ob die neue Fernaufnahmungseinheit korrekt registriert wurde und den Status „Verbunden“ aufweist.

   Wenn der Status nicht verbunden ist, versuchen Sie, den Dienst neu zu starten. Melden Sie sich beim System der Remote-Erfassungseinheit an, und führen Sie den folgenden Befehl aus:

   ```
   oci-service.sh restart acquisition
   ```

   Wenn die Verbindung weiterhin nicht hergestellt werden kann, wenden Sie sich an den technischen Support.

## Überprüfen der Installation

Nach Abschluss der Installation befindet sich das Installationsverzeichnis in `/opt/netapp/oci`. Sie können Insight in einem unterstützten Browser öffnen, um die Installation zu überprüfen. Möglicherweise sollten Sie auch die Insight-Protokolldateien überprüfen.

Wenn Sie Insight zum ersten Mal öffnen, wird die Seite zur Lizenzeinrichtung geöffnet. Nachdem Sie die Lizenzinformationen eingegeben haben, müssen Sie die Datenquellen einrichten. Informationen zum Eingeben von Datenquellen-Definitionen und zum Einrichten von Insight-Benutzern und -Benachrichtigungen finden Sie im *OnCommand Insight-Konfigurations- und Administrationshandbuch*.

Bei Problemen mit der Installation wenden Sie sich an den technischen Support, und geben Sie die gewünschten Informationen an.

#### Überprüfung der Installation neuer Insight Komponenten

Nach der Installation sollten Sie überprüfen, ob die neuen Komponenten auf Ihrem Server vorhanden sind.

##### Schritte

1. Um eine Liste der Dienste anzuzeigen, die derzeit auf dem Server ausgeführt werden, bei dem Sie angemeldet sind, geben Sie Folgendes ein:

   ```
   sudo oci-service.sh status all
   ```

2. Je nach Server, bei dem Sie angemeldet sind, überprüfen Sie die folgenden Insight-Dienste in der Liste

und stellen Sie sicher, dass sie den Status „`running`“ haben.

- Insight-Server: wildfly, Akquisition, mysql, elasticsearch
- Data Warehouse Server: wildfly, mysql
- Remote-Akquisitionsserver: Akquisition

#### Ergebnisse

Wenn diese Komponenten nicht aufgeführt sind, wenden Sie sich an den technischen Support.

### Insight-Protokolle

Insight bietet zahlreiche Protokolldateien, die Sie bei der Recherche und Fehlerbehebung unterstützen. Die verfügbaren Protokolle werden im Protokollverzeichnis aufgeführt. Sie können ein Protokollüberwachungstool wie BareTail verwenden, um alle Protokolle gleichzeitig anzuzeigen.

Die Protokolldateien befinden sich im `/var/log/netapp/oci/wildfly/` Verzeichnis. Die Erfassungsprotokolle befinden sich im `/var/log/netapp/oci/acq` Verzeichnis. Die Datendateien befinden sich in `/var/lib/netapp/oci`.

### Zugriff auf die Web-UI

Nach der Installation von OnCommand Insight müssen Sie Ihre Lizenzen installieren und dann Insight einrichten, um Ihre Umgebung zu überwachen. Dazu rufen Sie die Web-UI von Insight über einen Webbrowser auf.

#### Schritte

1. Führen Sie einen der folgenden Schritte aus:

   - Open Insight auf dem Insight-Server:

     `https://fqdn`

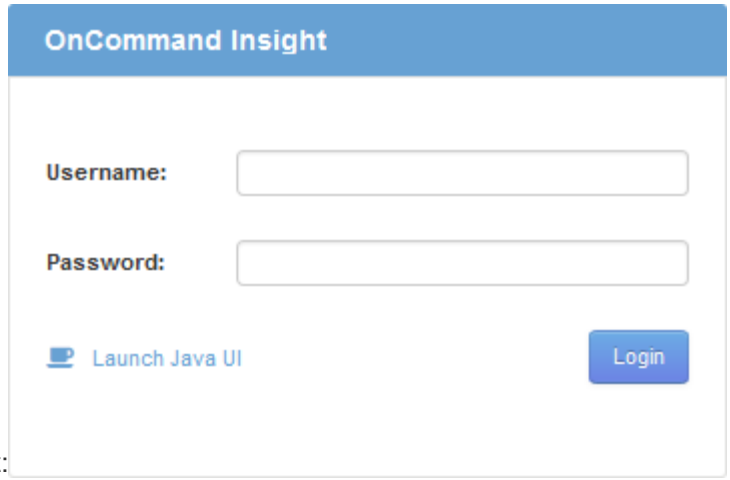
   - Insight von jedem beliebigen anderen Speicherort aus öffnen:

     `https://fqdn:port`

     Die Portnummer ist entweder 443 oder ein anderer Port, der bei der Installation des Insight-Servers konfiguriert wurde. Die Portnummer ist standardmäßig 443, wenn Sie sie nicht in der URL angeben.

   Das Dialogfeld OnCommand Insight wird

angezeigt:




2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.

   Wenn die Lizenzen installiert wurden, wird die Seite zur Einrichtung der Datenquelle angezeigt.

   Eine Insight Browser-Sitzung, die 30 Minuten lang inaktiv war, wurde überschritten, und Sie werden automatisch vom System abgemeldet. Für zusätzliche Sicherheit empfiehlt es sich, den Browser nach der Abmeldung von Insight zu schließen.

### Installieren Ihrer Insight Lizenzen

Wenn Sie die Lizenzdatei mit den Insight Lizenzschlüsseln von NetApp erhalten haben, können Sie mithilfe der Setup-Funktionen alle Ihre Lizenzen gleichzeitig installieren.

#### Über diese Aufgabe

Die Insight Lizenzschlüssel werden in einem gespeichert `.txt` Oder `.lcn` Datei:

#### Schritte

1. Öffnen Sie die Lizenzdatei in einem Texteditor und kopieren Sie den Text.
2. Öffnen Sie Insight in Ihrem Browser.
3. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
4. Klicken Sie Auf **Setup**.
5. Klicken Sie auf die Registerkarte **Lizenzen**.
6. Klicken Sie Auf **Lizenz Aktualisieren**.
7. Kopieren Sie den Text des Lizenzschlüssels in das Textfeld **Lizenz**.
8. Wählen Sie den Vorgang **Update (am häufigsten)** aus.
9. Klicken Sie Auf **Speichern**.
10. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Kontrollkästchen aktivieren, um das Senden von Nutzungsinformationen an NetApp im Abschnitt **Nutzungsdaten senden** zu aktivieren. Proxy muss ordnungsgemäß konfiguriert und für Ihre Umgebung aktiviert sein.

#### Nachdem Sie fertig sind

Nach der Installation der Lizenzen können Sie die folgenden Konfigurationsaufgaben ausführen:

- Datenquellen konfigurieren.
- Erstellen Sie OnCommand Insight-Benutzerkonten.

#### OnCommand Insight-Lizenzen

## OnCommand Insight arbeitet mit Lizenzen, die bestimmte Funktionen auf dem Insight Server ermöglichen.

- **Entdecken**

  Discover ist die grundlegende Insight-Lizenz, die die Inventarisierung unterstützt. Sie müssen über eine Discover-Lizenz verfügen, um OnCommand Insight verwenden zu können, und die Discover-Lizenz muss mit mindestens einer der Lizenzen Assure, Perform oder Plan gekoppelt werden.

- * Versichern*

  Eine Assure Lizenz bietet Support für Assurance-Funktionalität, einschließlich globaler und SAN-Pfadrichtlinien und Management von Verstößen. Mit einer Assure-Lizenz können Sie auch Schwachstellen anzeigen und managen.

- **Ausführen**

  Eine Lizenz ausführen unterstützt die Leistungsüberwachung auf Bestandsseiten, Dashboard-Widgets, Abfragen usw. sowie die Verwaltung von Performance-Richtlinien und -Verstößen.

- **Plan**

  Eine Planlizenz unterstützt Planungsfunktionen, einschließlich Ressourcenverwendung und -Zuweisung.

- **Host Utilization Pack**

  Eine Host-Nutzungslizenz unterstützt die Auslastung des Dateisystems auf Hosts und virtuellen Maschinen.

- **Authoring Melden**

  Eine Lizenz zur Erstellung von Berichten unterstützt zusätzliche Autoren für die Berichterstellung. Diese Lizenz erfordert die Planlizenz.

OnCommand Insight Module sind für einen Jahreszeitraum oder unbefristet lizenziert:

- Nach Terabyte überwachter Kapazität für Discover, Assure, Plan, Perform Module
- Nach Anzahl der Hosts für das Host Utilization Pack
- Nach Anzahl der zusätzlichen für die Berichterstellung erforderlichen Cognos Pro-Autoren

Lizenzschlüssel sind ein Satz eindeutiger Zeichenfolgen, die für jeden Kunden generiert werden. Sie können die Lizenzschlüssel von Ihrem OnCommand Insight-Vertreter beziehen.

Ihre installierten Lizenzen steuern die folgenden Optionen, die in der Software verfügbar sind:

- **Entdecken**

  Inventarisierung und Bestandsverwaltung (Foundation)

  Überwachen von Änderungen und Verwalten von Bestandsrichtlinien

- * Versichern*

  Anzeige und Management von Richtlinien und Verstößen für SAN-Pfade

  Anzeigen und Verwalten von Schwachstellen

  Anzeigen und Managen von Aufgaben und Migrationen

- **Plan**

  Anfragen anzeigen und verwalten

  Anzeigen und Verwalten ausstehender Aufgaben

  Anzeige und Verwaltung von Reservierungsverletzungen

  Anzeige und Verwaltung von Verstößen gegen die Portbilanz

- **Ausführen**

  Überwachen Sie Leistungsdaten, einschließlich Daten in Dashboard-Widgets, Bestandsseiten und Abfragen

  Anzeige und Management von Performance-Richtlinien und -Verstößen

Die folgenden Tabellen enthalten Details zu den Funktionen, die mit und ohne die Lizenz „Perform“ für Administratorbenutzer und Benutzer ohne Administratorrechte verfügbar sind.

| Funktion (Admin) | Mit Perform Lizenz | Ohne Lizenz ausführen |
|---|---|---|
| Applikation | Ja. | Keine Leistungsdaten oder Diagramme |
| Virtual Machine | Ja. | Keine Leistungsdaten oder Diagramme |
| Hypervisor | Ja. | Keine Leistungsdaten oder Diagramme |
| Host | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenspeicher | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| VMDK | Ja. | Keine Leistungsdaten oder Diagramme |
| Internes Volumen | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenmenge | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Pool | Ja. | Keine Leistungsdaten oder Diagramme |
| Festplatte | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Node | Ja. | Keine Leistungsdaten oder Diagramme |
| Fabric | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch-Port | Ja. | Keine Leistungsdaten oder Diagramme; „`Port Errors`“ zeigt „`N/A`“ an |
| Speicherport | Ja. | Ja. |
| NPV-Port | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| NPV-Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| Qtrees | Ja. | Keine Leistungsdaten oder Diagramme |
| Kontingente | Ja. | Keine Leistungsdaten oder Diagramme |
| Pfad | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| Zone | Ja. | Keine Leistungsdaten oder Diagramme |
| Zonenmitglied | Ja. | Keine Leistungsdaten oder Diagramme |
| Generisches Gerät | Ja. | Keine Leistungsdaten oder Diagramme |
| Tape | Ja. | Keine Leistungsdaten oder Diagramme |
| Maskierung | Ja. | Keine Leistungsdaten oder Diagramme |
| ISCSI-Sitzungen | Ja. | Keine Leistungsdaten oder Diagramme |
| ICSI-Netzwerkportale | Ja. | Keine Leistungsdaten oder Diagramme |
| Suche | Ja. | Ja. |
| Admin | Ja. | Ja. |
| Dashboard | Ja. | Ja. |
| Widgets | Ja. | Teilweise verfügbar (nur Asset-, Abfrage- und Admin-Widgets sind verfügbar) |
| Dashboard zu Verstößen | Ja. | Verborgen |
| Ressourcen-Dashboard | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Management von Performance-Richtlinien | Ja. | Verborgen |
| Verwalten von Anmerkungen | Ja. | Ja. |
| Verwalten von Anmerkungsregeln | Ja. | Ja. |
| Management von Applikationen | Ja. | Ja. |

| | | |
|---|---|---|
| Abfragen | Ja. | Ja. |
| Verwalten von Geschäftseinheiten | Ja. | Ja. |

| Merkmal | User - mit Perform-Lizenz | Guest - mit Perform-Lizenz | User - ohne Lizenz ausführen | Guest - ohne Lizenz durchführen |
|---|---|---|---|---|
| Ressourcen-Dashboard | Ja. | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Benutzerdefiniertes Dashboard | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) |
| Management von Performance-Richtlinien | Ja. | Verborgen | Verborgen | Verborgen |
| Verwalten von Anmerkungen | Ja. | Verborgen | Ja. | Verborgen |
| Management von Applikationen | Ja. | Verborgen | Ja. | Verborgen |
| Verwalten von Geschäftseinheiten | Ja. | Verborgen | Ja. | Verborgen |
| Abfragen | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) |

## Fehlerbehebung bei Installationen

OnCommand Insight-Installationen werden in der Regel über die Installationsassistenten verwaltet. Es kann jedoch zu Problemen bei Upgrades oder Konflikten aufgrund von Computerumgebungen kommen.

Sie sollten außerdem sicher sein, dass Sie alle erforderlichen OnCommand Insight-Lizenzen für die Installation der Software installieren.

#### Fehlende Lizenzen

Für verschiedene OnCommand Insight-Funktionen sind unterschiedliche Lizenzen erforderlich. Die in OnCommand Insight angezeigten Informationen werden von Ihren

installierten Lizenzen gesteuert. Informationen über die Funktionen, die von den einzelnen Lizenzen gesteuert werden, finden Sie im Abschnitt OnCommand Insight-Lizenzen.

Informationen über die Funktionen, die von den einzelnen Lizenzen gesteuert werden, finden Sie im Abschnitt OnCommand Insight-Lizenzen.

#### Einreichung einer technischen Online-Support-Anfrage

Wenn Sie als registrierter Support-Kunde Probleme mit der Installation von Insight haben, können Sie eine technische Online-Support-Anfrage stellen.

##### Bevor Sie beginnen

Sie müssen sich unter Verwendung Ihrer Unternehmens-E-Mail-Adresse als Support-Kunde registrieren, um Online-Support-Services zu erhalten. Die Registrierung erfolgt über die Support Site .

##### Über diese Aufgabe

Um den Kunden-Support bei der Lösung des Installationsproblem zu unterstützen, sollten Sie so viele Informationen wie möglich sammeln, einschließlich der folgenden Punkte:

- Insight Seriennummer
- Beschreibung des Problems
- Alle Insight-Protokolldateien
- Bildschirmaufnahme aller Fehlermeldungen

##### Schritte

1. Erstellen Sie ein `.zip` Datei der Informationen, die Sie gesammelt haben, um ein Fehlerbehebungspaket zu erstellen.
2. Melden Sie sich auf der Support-Website unter an "mysupport.netapp.com" Und wählen Sie **Technische Unterstützung**.
3. Klicken Sie auf **Fall öffnen**.
4. Befolgen Sie die Anweisungen zu Ihrem Datenpaket.

##### Nachdem Sie fertig sind

Sie können **Fallstatus prüfen** auf der Seite Technische Unterstützung verwenden, um Ihrer Anfrage zu folgen.

# Aktualisieren Von Insight

Wenn eine neue Version von OnCommand Insight verfügbar ist, sollten Sie ein Upgrade durchführen, um von neuen Funktionen und Fehlerbehebungen zu profitieren. Sie müssen den Insight-Server und das Data Warehouse (DWH) separat aktualisieren.

Sie sollten keine automatischen oder manuellen Backups in den Insight-Installationsverzeichnissen speichern, da der gesamte Installationsordner während des Upgrade-Vorgangs überschrieben wird. Wenn Sie Sicherungsdateien in einem dieser Verzeichnisse gespeichert haben, müssen Sie Ihre Backups an einen anderen Speicherort verschieben, bevor Sie einen Upgrade- oder Deinstallationsvorgang durchführen.

Neuere Versionen von Insight verfügen über mehr Speicherplatz, Arbeitsspeicher und CPU-Anforderungen. Lesen Sie vor dem Upgrade auf die neueste Version von Insight die Installationsanforderungen. Es wird dringend empfohlen, sich vor der Installation oder dem Upgrade von Insight an Ihren Sales Engineer zu wenden, um eine detaillierte Anleitung zur Größenbestimmung zu erhalten.

Es empfiehlt sich, vor dem Upgrade der Insight-Software ein Sicherheits-Backup und ein Datenbank-Backup durchzuführen.

## Aktualisieren von Insight auf Version 7.3.12 oder höher - Linux

Vor dem Upgrade von OnCommand Insight 7.3.10 auf 7.3.11 Version 7.3.12 oder höher müssen Sie das OCI Datenmigrationstool ausführen.

### Hintergrund

OnCommand Insight Version 7.3.12 und höher verwenden zugrunde liegende Software, die möglicherweise mit früheren Versionen nicht kompatibel ist. Insight Version 7.3.12 und höher enthalten ein **Data Migration Tool** zur Unterstützung beim Upgrade.

OnCommand Insight Versionen 7.3.9 und früher werden nicht mehr unterstützt. Wenn Sie eine dieser Versionen ausführen, müssen Sie vor dem Upgrade auf 7.3.12 oder höher auf Insight Version 7.3.10 oder höher (7.3.11 wird dringend empfohlen) aktualisieren.

### Welche Funktionen Bietet Das Datenmigrationstool?

Das Migrationstool führt zunächst eine Kompatibilitätsprüfung durch und folgt dann einem von drei verschiedenen Upgrade-Pfaden. Der ausgewählte Pfad basiert auf der Datenkompatibilität Ihrer aktuellen Version.

Vor dem Upgrade müssen Sie das Data Migration Tool ausführen und die empfohlenen Schritte ausführen.

### Bevor Sie beginnen

- Es wird dringend empfohlen, das OnCommand Insight-System vor dem Ausführen des Datenmigrationstools zu sichern.
- Der Elasticsearch-Service auf dem Server muss betriebsbereit sein.
- Das Data Migration Tool *must* muss für die Datenbank und alle Performance-Archive ausgeführt werden, bevor Sie Insight aktualisieren.

### Ausführen des Data Migration Tools

1. Laden Sie die aktuelle Version des Data Migration Tools (z. B. *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) sowie die entsprechende Insight Installer-Datei auf Ihren Insight Server herunter. Entpacken Sie die ZIP-Datei in einen Arbeitsordner. Downloads finden Sie auf der "NetApp Support Website".

2. Öffnen Sie ein Befehlsfenster, und navigieren Sie zu Ihrem Arbeitsordner.
   - Bash Shell wird empfohlen.
3. Führen Sie das Datenmigrationstool über den folgenden Befehl aus:
   - `*sudo ./SANScreenDataMigrationTool.sh*`
4. Befolgen Sie bei Bedarf die Anweisungen. Im Folgenden ein Beispiel.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

Das Data Migration Tool überprüft, ob veraltete Indizes auf Ihrem System vorhanden sind, und meldet, ob sie gefunden wurden. Wenn keine vorhanden sind, wird das Werkzeug beendet.

Einige Indizes können migriert werden, während der SANscreen-Serverdienst ausgeführt wird. Andere können nur migriert werden, wenn der Server angehalten wird. Wenn keine Indizes vorhanden sind, die migriert werden können, wird das Tool beendet. Befolgen Sie andernfalls die Anweisungen, wie Sie dazu aufgefordert werden.

Wenn das Data Migration Tool abgeschlossen ist, wird es erneut auf veraltete Indizes überprüft. Wenn alle Indizes migriert wurden, informiert Sie das Tool darüber, dass ein Upgrade auf OnCommand Insight 7.3.12 unterstützt wird. Sie können jetzt mit dem Upgrade der Insight fortfahren.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking for obsolete (version 5) indexes...
Found 76 obsolete OCI indexes. Of these,
76 indexes may be migrated with OCI server running

SANscreen Server service is running

Proceed with online migration of 76 indexes (y or [n])? y
If you supply performance archive location, entries for any dates with
migrated
indexes will be replaced. Each orginal entry will be renamed and you may
delete
it after migration is completed.
When prompted enter the archive location including the site-name
directory.

Enter the location of the performance archive or blank if none:
Performance archive entries will not be updated

Running the migration application with options -u http://localhost:9200
--online -sa -

Preparing to migrate oci-timeseries-disk-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-internalvolume-2021-03-22: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-port-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
...
Preparing to migrate oci-timeseries-disk-2021-03-27: copied; backup;
delete old; restore new; cleanup; done.
Execution time 0:08:17
Checking for obsolete (version 5) indexes...

No obsolete indexes found. Upgrade and Inline Upgrade to 7.3.12+ are
supported
```

Wenn Sie aufgefordert wurden, den SANscreen-Dienst zu beenden, starten Sie ihn vor dem Upgrade von Insight neu.

#### Validierungsfehler

Falls die Indexvalidierung fehlschlägt, informiert Sie das Migrationstool vor dem Beenden über das Problem.

**OnCommand Insight ist nicht vorhanden:**

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

**Ungültige Insight-Version:**

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

**Elasticsearch-Dienst läuft nicht:**

```
./SanscreenDataMigrationTool.sh
NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

#### Befehlszeilenoptionen

Das Datenmigrationstool enthält einige optionale Parameter, die sich auf den Betrieb auswirken.

| Option (Linux) | Funktion |
| --- | --- |
| -S --stumm | Alle Eingabeaufforderungen unterdrücken |
| -A --Archiv | Wenn angegeben, werden vorhandene Archiveinträge für alle Daten ersetzt, deren Index(e) migriert werden. Der Pfad sollte auf das Verzeichnis verweisen, das die ZIP-Dateien für den Archiveintrag enthält.<br><br>Ein Argument von '-' kann angegeben werden, um anzuzeigen, dass kein Performance-Archiv aktualisiert werden muss.<br><br>Wenn dieses Argument vorhanden ist, wird die Eingabeaufforderung für den Archivspeicherort unterdrückt. |
| -C --Check | Falls vorhanden, wird das Skript sofort nach der Meldung der Indexzahlen beendet. |
| -D --dryrun | Falls vorhanden, meldet die ausführbare Migrationsdatei die Aktionen, die ausgeführt werden würden (zum Migrieren von Daten und Aktualisieren von Archiveinträgen), führt die Vorgänge jedoch nicht aus. |
| -P --Port | Falls vorhanden, verwenden Sie den angegebenen Wert als REST-Port von Elasticsearch. Falls nicht vorhanden, erhalten Sie den Wert aus der Installation, falls möglich; andernfalls verwenden Sie den Standardwert 9200.<br><br>Bei einigen Linux OnCommand Insight-Installationen wird der Elasticsearch-REST-Port möglicherweise nicht auf dem Standard-Port 9200 ausgeführt. Verwenden Sie in diesem Fall die Option --Port, um den Wert zu liefern |
| -H --help | Nutzungsinformationen anzeigen |

**Fehlerbehebung**

Wenn Archiveinträge aktualisiert wurden, müssen Sie _sicherstellen, dass die Eigentumsrechte und Berechtigungen für die aktualisierten Archive korrekt sind. Sie sollten **ocisys ocisys 644** sein. Wenn dies nicht der Fall ist, navigieren Sie zum Ordner Performance Archive, und führen Sie die folgenden Befehle aus:

```
chown ocisys *
chgrp ocisys *
chmod 644 *
```

## Upgrade der Insight Server Software

Sie können nach der Anmeldung beim Server nach OnCommand Insight-Serveraktualisierungen suchen.

> Es wird dringend empfohlen, den Vault und die Datenbank vor dem Upgrade von OnCommand Insight zu sichern.
>
> Weitere Informationen zum Tresor finden "Sicherheitstool"Sie in den Anweisungen.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf das Symbol **Hilfe**.
2. Wählen Sie **nach Updates suchen**.
3. Klicken Sie auf **OK**, wenn die `Version is up to date` Meldung wird angezeigt.
4. Wenn eine neuere Version erkannt wird, klicken Sie im Meldungsfeld auf den Link **hier herunterladen**.
5. Klicken Sie auf der Seite **Download** auf **Download**. Notieren Sie sich den Speicherort des Download-Verzeichnisses.

   Sie können die neuere Version auch von der NetApp Support-Website herunterladen.
6. Melden Sie sich beim Insight-Server mit einem Konto mit sudo-Berechtigungen an.
7. Navigieren Sie zum Download-Verzeichnis, und geben Sie den folgenden Befehl ein:

   `unzip oci-<version>-linux-x86_64.zip`

   Stellen Sie sicher, dass Sie die korrekte Versionsnummer der Installationsdatei haben.
8. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh`:

   `sudo ./oci-<version>-linux-x86_64/oci-install.sh --help`
9. Führen Sie das Installationsskript aus:

   `sudo ./oci-<version>-linux-x86_64/oci-install.sh`
10. Akzeptieren Sie die Lizenzvereinbarung, und befolgen Sie die Anweisungen.

## Aktualisieren der Data Warehouse-Software

Nach dem Upgrade der Insight Server Software müssen Sie die Data Warehouse Software aktualisieren.

### Über diese Aufgabe

Es wird dringend empfohlen, den Tresor und die Datenbank vor der Aktualisierung der DWH zu sichern.

Weitere Informationen zum Tresor finden "Sicherheitstool"Sie in den Anweisungen.

### Schritte

1. Melden Sie sich beim Data Warehouse (DWH)-Server mit einem Konto mit sudo-Berechtigungen an.
2. Laden Sie die Insight DWH Software von der NetApp Support-Website herunter.
3. Navigieren Sie zum Download-Verzeichnis, und geben Sie den folgenden Befehl ein:

   ```
   unzip oci-dwh-<version>-linux-x86_64.zip
   ```

   Stellen Sie sicher, dass Sie die korrekte Versionsnummer der Installationsdatei haben.

4. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh` :

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
   ```

5. Führen Sie das Installationsskript aus:

   ```
   sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
   ```

6. Akzeptieren Sie die Lizenzvereinbarung, und befolgen Sie die Anweisungen.

## Aktualisierung der Remote Acquisition Unit-Software

Nach dem Upgrade der Insight Server-Software müssen Sie die Software für die Remote-Erfassung aktualisieren.

Es wird dringend empfohlen, den Tresor und die Datenbank vor der Aktualisierung der DWH zu sichern.

Weitere Informationen zum Tresor finden "Sicherheitstool"Sie in den Anweisungen.

### Schritte

1. Melden Sie sich beim RAU-Server (Remote Acquisition Unit) mit einem Konto mit sudo-Berechtigungen an.
2. Laden Sie die Insight rau Software von der NetApp Support-Website herunter.
3. Navigieren Sie zum Download-Verzeichnis, und geben Sie den folgenden Befehl ein:

   ```
   unzip oci-rau-<version>-linux-x86_64.zip
   ```

   Stellen Sie sicher, dass Sie die korrekte Versionsnummer der Installationsdatei haben.

4. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-install.sh` :

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
   ```

5. Führen Sie das Installationsskript aus:

   ```
   sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
   ```

6. Akzeptieren Sie die Lizenzvereinbarung, und befolgen Sie die Anweisungen.

### Migration von Windows auf Linux

Um Insight unter Linux zu verwenden, wenn Sie über eine vorhandene Windows-Installation verfügen, müssen Sie eine Migration durchführen. Sie müssen dieses Verfahren sowohl für die Insight Server- als auch für die Data Warehouse-Komponenten durchführen.

#### Schritte

1. Sichern Sie Ihre aktuelle Insight-Installation auf Ihrem Server.

   Informationen zum Backup der OCI-Datenbank finden Sie im *OnCommand Insight Konfigurations- und Administrationshandbuch*.

2. Installieren Sie Insight für Linux.
3. Stellen Sie die Datenbank für Ihre vorherige Version wieder her.

   Informationen zum Wiederherstellen der OCI-Datenbank finden Sie im *OnCommand Insight Konfigurations- und Administrationshandbuch*.

4. Deinstallieren Sie Ihre vorherige Version von Insight für Windows.

# OnCommand Insight wird deinstalliert

Sie können die OnCommand Insight-Komponenten bei Bedarf deinstallieren. Sie müssen die OnCommand Insight-Komponenten separat deinstallieren.

> **Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern.
>
> Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

Jede Komponente wird separat deinstalliert.

### Deinstallieren des OnCommand Insight-Servers

Sie können den OnCommand Insight-Server bei Bedarf deinstallieren.

> **Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern.
>
> Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

### Bevor Sie beginnen

Best Practice: Sichern Sie vor der Deinstallation von Insight die OnCommand Insight-Datenbank.

### Schritte

1. Melden Sie sich beim OnCommand Insight-Server mit einem Konto mit sudo-Berechtigungen an.
2. Stellen Sie sicher, dass alle OnCommand Insight-Fenster geschlossen sind.
3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `oci-uninstall.sh` Indem Sie den folgenden Befehl eingeben:

   ```
   sudo /usr/bin/oci-uninstall.sh --help
   ```

   Bei einer normalen Deinstallation werden weder die Insight-Lizenz noch tägliche Backups entfernt. Um die gesamte Installation zu entfernen, verwenden Sie die `--purge` Optioon mit dem`oci-install.sh` Befehl.

4. Geben Sie den folgenden Befehl ein:

   ```
   sudo /usr/bin/oci-uninstall.sh
   ```

## Data Warehouse Wird Deinstalliert

Sie können Data Warehouse bei Bedarf deinstallieren.

> **Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern.
>
> Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

### Bevor Sie beginnen

Sichern Sie die aktuelle Version der Datenbank des OnCommand Insight Data Warehouse (DWH).

### Über diese Aufgabe

Durch das Deinstallieren des OnCommand Insight Data Warehouse werden alle zuvor gesammelten Daten endgültig gelöscht.

### Schritte

1. Melden Sie sich beim Data Warehouse-Server mit einem Konto mit sudo-Berechtigungen an.
2. Stellen Sie sicher, dass alle OnCommand Insight-Fenster geschlossen sind.
3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `uninstall.sh` Indem Sie den folgenden Befehl eingeben: `sudo /usr/bin/oci-uninstall.sh --help`
4. Geben Sie den folgenden Befehl ein: `sudo /usr/bin/oci-uninstall.sh`

## Deinstallieren einer Remote-Akquisitionseinheit

Sie können eine Remote-Erfassungseinheit deinstallieren, wenn Sie sie nicht mehr benötigen.

**Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

**Schritte**

1. Melden Sie sich beim Remote Acquisition Unit-Server mit einem Konto mit sudo-Berechtigungen an.
2. Stellen Sie sicher, dass alle OnCommand Insight-Fenster geschlossen sind.
3. Sie können Syntax, Befehlsargumente und Parameterverwendung für anzeigen `uninstall.sh` Indem Sie den folgenden Befehl eingeben: `sudo /usr/bin/oci-uninstall.sh --help`
4. Geben Sie den folgenden Befehl ein: `sudo /usr/bin/oci-uninstall.sh`

   Das Deinstallationsskript wird ausgeführt. Befolgen Sie alle Anweisungen.

# Installation für Microsoft Windows

## Installationsvoraussetzungen

Bevor Sie OnCommand Insight installieren, müssen Sie die aktuelle Softwareversion herunterladen, die entsprechende Lizenz erwerben und Ihre Umgebung einrichten.

Stellen Sie vor der Installation von OnCommand Insight sicher, dass folgende Informationen zur Verfügung stehen:

- OnCommand Insight-Softwaredateien im heruntergeladenen Installationspaket für die aktuelle Version
- Eine Lizenz zum Betrieb der heruntergeladenen OnCommand Insight-Version
- Minimale Hardware- und Softwareumgebung

  Das aktuelle Produkt verbraucht möglicherweise zusätzliche Hardwareressourcen (aufgrund der erweiterten OnCommand Insight-Produktfunktionen), die bei früheren Versionen des OnCommand Insight Produkts nicht in Anspruch genommen wurden.

- Ein Bereitstellungsplan, der die Hardware- und Netzwerkkonfigurationen für den OnCommand Insight-Server, das Data Warehouse und die Berichterstellung sowie die Remote-Erfassungseinheiten umfasst.
- Virenscan-Software deaktiviert

  Während der Installation von OnCommand Insight müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Komponente Insight verwendeten Pfade (Installations-, Backup- und Archivierpfade) vom Virenscan ausgeschlossen werden, zusätzlich zum Ausschluss des gesamten `sanscreen` Verzeichnis aus dem Scan.

  Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen.

Wenn Sie eine vollständige Installation als Upgrade oder als Migration auf neue Hardware durchführen und Ihr vorhandenes System eine nicht standardmäßige Sicherheitskonfiguration enthält, müssen Sie die Sicherheitskonfiguration sichern, bevor Sie die Installation durchführen. Nach Abschluss der Installation müssen Sie die Sicherheitskonfiguration wiederherstellen, bevor Sie den Server (der die lokale Erfassungseinheit enthält) oder die Data Warehouse-Datenbank wiederherstellen.Sie müssen die Sicherheitskonfiguration auf allen Insight-Servern wiederherstellen, bevor Sie die DWH-Datenbank wiederherstellen.

Bei einem in-Place-Upgrade (nur für Insight Server verfügbar) wird die Sicherheitskonfiguration ordnungsgemäß ausgeführt und Sie müssen sie nicht wiederherstellen.

Sie verwenden das `securityadmin` Tool zum Erstellen einer Sicherungskopie der Konfiguration und zum Wiederherstellen der gespeicherten Konfiguration. Weitere Informationen erhalten Sie, wenn Sie nach suchen `securityadmin` Im OnCommand Insight Dokumentationszentrum: http://docs.netapp.com/oci-73/index.jsp

### Planen der Implementierung

Um eine erfolgreiche Bereitstellung zu gewährleisten, müssen Sie bestimmte Systemelemente berücksichtigen, bevor Sie OnCommand Insight installieren.

### Über diese Aufgabe

Zur Planung Ihrer Insight Implementierung gehören die folgenden Systemelemente:

- Insight Architektur
- Ihre zu überwachenden Netzwerkkomponenten
- Voraussetzungen für die Insight Installation und Serveranforderungen
- Webbrowser-Anforderungen für Insight

### Informationen zur Unterstützung der Datenquelle

Im Rahmen Ihrer Konfigurationsplanung sollten Sie sicherstellen, dass die Geräte in Ihrer Umgebung von Insight überwacht werden können. Dazu können Sie die Data Source Support Matrix für Details zu Betriebssystemen, spezifischen Geräten und Protokollen überprüfen. Einige Datenquellen sind möglicherweise nicht auf allen Betriebssystemen verfügbar.

#### Speicherort der aktuellsten Version der Data Source Support Matrix

Die Support-Matrix für die Datenquelle von OnCommand Insight wird mit jeder Service Pack-Version aktualisiert. Die aktuellste Version des Dokuments finden Sie unter "NetApp Support Website". .

### Geräteerkennung und Planung der Datenquelle

Im Rahmen Ihrer Bereitstellungsplanung sollten Sie Informationen zu den Geräten in Ihrer Umgebung sammeln.

Sie benötigen die folgende Software, Konnektivität und Informationen zu jedem Gerät in Ihrer Umgebung:

- IP-Adresse oder Hostname, der vom OCI-Server aufgelöst werden kann
- Anmeldename und Passwort
- Art des Zugriffs auf das Gerät, z. B. Controller und Management Station

> Der schreibgeschützte Zugriff ist für die meisten Geräte ausreichend, für einige Geräte sind jedoch Administratorberechtigungen erforderlich.

- Port-Konnektivität mit dem Gerät, je nach den Anforderungen an den Port der Datenquelle
- Für Switches, SNMP-schreibgeschützte Community-Zeichenfolge (Benutzer-ID oder Passwort für den Zugriff auf die Switches)
- Software von Drittanbietern, die auf dem Gerät benötigt wird, z. B. Solutions Enabler.
- Weitere Informationen zu den Berechtigungen und Anforderungen der Datenquelle finden Sie in der Hilfe zur Webbenutzeroberfläche oder im *OnCommand Insight Konfigurations- und Administrationshandbuch*.

### Von OnCommand Insight generierter Netzwerkverkehr

Der von OnCommand Insight erzeugte Netzwerkdatenverkehr, die Menge der verarbeiteten Daten, die das Netzwerk durchlaufen, und die von OnCommand Insight auf Geräten aufbereitete Last unterscheiden sich durch viele Faktoren.

Der Datenverkehr, die Daten und die Last unterscheiden sich je nach Umgebung anhand der folgenden Faktoren:

- Rohdaten
- Konfiguration von Geräten
- Implementierungstopologie von OnCommand Insight
- Verschiedene Abfrageintervalle für die Bestandsaufnahme und Performance-Datenquellen, die reduziert werden können, um langsame Geräte zu erkennen oder die Bandbreite zu erhalten

Es können große Unterschiede bei den Rohdaten, die OnCommand Insight sammelt, gegeben sein.

Das folgende Beispiel zeigt, wie die Konfigurationsdaten variieren können und wie Datenverkehr, Daten und Last von vielen Konfigurationsfaktoren beeinflusst werden. Beispielsweise könnten Sie zwei Arrays mit jeweils 1,000 Festplatten verwenden:

- Array 1: Hat 1,000 SATA-Festplatten alle 1 TB Größe. Alle 1,000 Festplatten befinden sich in einem Speicherpool, und es gibt 1,000 LUNs, die alle denselben 32 Nodes in einem ESX Cluster bereitgestellt (zugeordnet und maskiert) werden.
- Array 2: Verfügt über 400 2-TB-Datenfestplatten, 560 600-GB-FC-Festplatten und 40 SSDs. Es gibt 3 Speicherpools, aber 320 der FC-Festplatten werden in herkömmlichen RAID-Gruppen verwendet. Die auf die RAID-Gruppen geschnitzten LUNs verwenden einen traditionellen Maskierungstyp (symmaskdb), während die Thin Provisioning, Pool-basierten LUNs einen neueren Maskierungstyp (symmaskdb) verwenden. Es sind 600 LUNs auf 150 verschiedenen Hosts präsentiert. Es gibt 200 BCVs (Full Block Replikatvolumes von 200 der 600 LUNs). Es gibt auch 200 R2-Volumes, Remote-Replikatvolumes von Volumes, die auf einem Array an einem anderen Standort vorhanden sind.

Diese Arrays haben jeweils 1,000 Festplatten und 1,000 logische Volumes. Möglicherweise sind sie physisch mit der Menge an Rack-Platz identisch, die sie im Datacenter verbrauchen. Vielleicht wird sogar dieselbe Firmware ausgeführt, aber das zweite Array ist in seiner Konfiguration viel komplexer als das erste Array.

## Deaktivierung der Virenscan-Software

Wenn Antivirensoftware auf Ihrem System aktiv ist, schlägt die OnCommand Insight-Installation fehl. Sie können dieses Problem verhindern, indem Sie die Virenscan-Software vor der Installation deaktivieren.

Um einen Installationsfehler aufgrund einer aktiven Virenscanner-Software zu verhindern, müssen Sie während der Installation jeder OnCommand Insight-Komponente alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Komponente Insight verwendeten Pfade (Installations-, Backup- und Archivierpfade) vom Virenscan ausgeschlossen werden.

Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen.

## Anforderungen für Insight Server

Es wird ein dedizierter Server empfohlen. Installieren Sie Insight nicht auf einem Server, auf dem andere Anwendungen installiert sind. Sowohl physische als auch virtuelle Server werden unterstützt, sofern die Produktanforderungen erfüllt sind.

Sie müssen über lokale Administratorberechtigungen verfügen, um die OnCommand Insight-Serversoftware

installieren zu können.

Die Dimensionierung für OnCommand Insight weist mehrere Abhängigkeiten auf, wie z. B. Art und Größe der Datenquelle, Anzahl der Assets in Ihrer Umgebung, Abfrageintervalle und mehr. Die folgenden Beispiele zur Größenbestimmung sind nur Richtlinien und stellen einige der Umgebungen dar, in denen Insight getestet wurde. Wenn sich diese oder andere Faktoren in der Umgebung ändern, können sich die Dimensionierungsanforderungen für Insight ändern. Diese Richtlinien enthalten Speicherplatz für Performance-Archivdaten von bis zu 90 Tagen.

Vor der Installation oder dem Upgrade der Insight sollten Sie sich an Ihren Sales Engineer wenden, um eine detaillierte Anleitung zur Größenbemessung zu erhalten.

**Beispiele:**

| Umgebungsfaktoren: | Getesteter Festplattenspeicher, CPUs und Speicher: |
|---|---|
| 80 Storage-Volume4.000<br><br>4,000 VMs<br><br>4,000 Switch-Ports | 250 GB Festplattenspeicherplatz 8 Kerne<br><br>32 GB RAM |
| 160 Storage-Volume40.000<br><br>8,000 VMs<br><br>8,000 Switch-Ports | 1 TB Festplattenspeicherplatz, 12 Kerne<br><br>48 GB RAM |

**Voraussetzungen:**

| Komponente | Erforderlich |
|---|---|
| Betriebssystem | Ein Computer, auf dem 64-Bit Microsoft Windows Server 2016, 2019 oder 2022 mit dem neuesten Service Pack ausgeführt wird. Windows .NET Framework Version 3.5 muss vor der Installation von OnCommand Insight installiert werden.<br><br>Das mit Windows Server 2012 eingeführte ausfallsichere Dateisystem (ReFS) ist nicht mit OnCommand Insight kompatibel. Die Windows-Installation von OnCommand Insight wird nur auf dem NTFS-Dateisystem unterstützt.<br><br>Es wird ein dedizierter Server empfohlen. |
| Virtuelle Maschine (VM) | Diese Komponente kann in einer virtuellen Umgebung ausgeführt werden, sofern die CPU- und Arbeitsspeicherressourcen für Ihre Instanz reserviert sind. |

| | |
|---|---|
| Arbeitsspeicher und CPU | 24 BIS 256 GB RAM<br><br>8 - 32 Kerne<br><br>Es wird dringend empfohlen, die Größe der Auslagerungsdatei auf „`Windows Managed`“ zu setzen. Kleine Paging-Dateien fester Größe können die erfolgreiche Speicherung von Insight-Leistungsdaten beeinträchtigen. |
| Verfügbarer Festplattenspeicher | 100 GB - 3 TB installiere Festplattenspeicher<br><br>50 GB - 1 TB Performance Archiv Speicherplatz<br><br>Für den Insight-Installationsbereich werden SSD-Festplatten empfohlen. |
| Netzwerk | Ethernet-Verbindung und -Ports:<br><br>• Ethernet-Verbindung mit 100 Mbit/s oder 1 Gbit/s mit dedizierter (statischer) IP-Adresse und IP-Konnektivität zu allen Komponenten im SAN, einschließlich FC-Geräten und Remote-Akquisitionseinheiten.<br>• Die Portanforderungen für den OnCommand Insight-Serverprozess sind 80, 443, 1090 bis 1100, 3873, 8083, 4444 bis 4446, 5445, 5455, 4712 bis 4714, 5500, Und 5501.<br>• Die Port-Anforderungen für den Akquisitionsprozess sind 12123 und 5679.<br>• Die Portanforderung für MySQL ist 3306.<br>• Die Portanforderungen für Elasticsearch lauten 9200 und 9310<br>• Die Anforderungen für dynamische Ports auf Win2008/2012 sind 49152 bis 65535<br><br>Die Ports 443 und 3306 erfordern externen Zugriff über jede vorhandene Firewall. |
| Berechtigungen | Lokale Administratorberechtigungen sind auf dem OnCommand Insight-Server erforderlich.<br><br>Wenn einer der folgenden Ordner symbolische Links sind, stellen Sie sicher, dass die Zielverzeichnisse über '755'-Berechtigungen verfügen.<br><br>• /Opt/netapp<br>• /Var/lib/netapp<br>• /Var/log/netapp |

| | |
|---|---|
| Remote-Konnektivität | Internetverbindung für den WebEx-Zugriff oder eine Remote-Desktop-Verbindung, um den Support bei der Installation und nach der Installation zu erleichtern. |
| Zugänglichkeit | HTTPS-Zugriff ist erforderlich. |
| Virenscan | Während der Installation dieser OnCommand Insight-Komponente müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Komponente Insight verwendeten Pfade (Installations-, Backup- und Archivierpfade) vom Virenscan ausgeschlossen werden.<br><br>Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen. |
| HTTP- oder HTTPS-Server | Microsoft Internetinformationsdienste (IIS) oder andere HTTPS-Server sollten nicht mit denselben Ports (443) konkurrieren wie der OnCommand Insight-Server und nicht automatisch starten. Wenn sie auf Port 443 hören müssen, müssen Sie den OnCommand Insight-Server so konfigurieren, dass andere Ports verwendet werden. |

## Serveranforderungen für Data Warehouse und Reporting

Sie müssen das Data Warehouse und den Reporting-Server auf einem Computer ausführen, der mit den bestehenden Hardware- und Softwareanforderungen kompatibel ist, und sicherstellen, dass der Apache-Webserver oder die Berichterstellungssoftware nicht bereits auf diesem Computer installiert ist.

Die Größenbestimmung für OnCommand Insight umfasst mehrere Abhängigkeiten, wie z. B. Anzahl der Assets in Ihrer Umgebung, Menge der gespeicherten Archivdaten und vieles mehr. Die folgenden Beispiele zur Größenanpassung eines Data Warehouses sind nur Richtlinien und stellen einige der Umgebungen dar, in denen Insight getestet wurde. Wenn sich diese oder andere Faktoren in der Umgebung ändern, können sich die Dimensionierungsanforderungen für Insight ändern.

Vor der Installation oder dem Upgrade der Insight sollten Sie sich an Ihren Sales Engineer wenden, um eine detaillierte Anleitung zur Größenbemessung zu erhalten.

**Beispiele:**

| Umgebungsfaktoren: | Getesteter Festplattenspeicher, CPUs und Speicher: |
|---|---|
| 18 Storage-Arrays3.400 VMs<br><br>4,500 Switch-Ports | 200-GB-Festplatte, 8 Kerne<br><br>32 GB RAM |

| | |
|---|---|
| 110 Storage-Arrays11'500 VMs<br><br>14,500 Switch-Ports | 300-GB-Festplatte, 8 Kerne<br><br>48 GB RAM |

**Voraussetzungen:**

| Komponente | Erforderlich |
|---|---|
| Betriebssystem | Ein Computer, auf dem 64-Bit Microsoft Windows Server 2016, 2019 oder 2022 mit dem neuesten Service Pack ausgeführt wird. Windows .NET Framework Version 3.5 muss vor der Installation von OnCommand Insight installiert werden. |
| Virtuelle Maschine (VM) | Diese Komponente kann in einer virtuellen Umgebung ausgeführt werden, sofern die CPU- und Arbeitsspeicherressourcen für Ihre Instanz reserviert sind. |
| CPU | 8 bis 40 CPU-Kerne |
| Speicher | 32 GB - 2 TB RAM Best Practice: Es wird dringend empfohlen, die Auslagerungsdateigröße auf „`Windows Managed`“ zu setzen. Kleine Paging-Dateien fester Größe können die erfolgreiche Speicherung von Insight-Leistungsdaten beeinträchtigen. |

| | |
|---|---|
| Verfügbarer Festplattenspeicher | 200 GB - 2 TB FestplattenspeicherDie Installation erfordert mindestens 20 GB frei auf dem Laufwerk C:.<br><br>Unter Windows erfordert Insight Data Warehouse mit Reporting, dass die Unterstützung für die Erstellung von 8dot3-Namen auf dem Installationslaufwerk vor der Installation aktiviert ist. Für das Laufwerk C: Ist dies normalerweise standardmäßig aktiviert. Sie können überprüfen, ob die Erstellung von 8dot3-Namen auf dem Zielinstallationslaufwerk aktiviert ist, indem Sie den folgenden Befehl ausführen (Ersetzen Sie D: Mit dem Zielinstallationslaufwerk):<br><br>Fsutil 8dot3Namensabfrage D:<br><br>Um die Erstellung von 8dot3-Namen zu aktivieren, führen Sie den folgenden Befehl aus (ersetzen Sie D: Mit Zielinstallationslaufwerk):<br><br>Fsutil 8dot3namensset D: 0 |
| Netzwerk | • Ethernet-Verbindung mit 100 Mbit/s oder 1 Gbit/s.<br>• Statische IP-Adresse<br>• Port 50000 muss verfügbar sein, bevor Data Warehouse mit Reporting unter Windows installiert werden kann<br>• Für den OnCommand Insight DWH-Serverprozess, Ports 80, 443, 1098, 1099, 3873, 8083 und 4444 bis 4446<br>• Für die Reporting Engine, Ports 1527, 9362, 9300 und 9399<br>• Für MySQL, Port 3306<br>• Stellen Sie sicher, dass DNS ordnungsgemäß funktioniert, indem Sie einen durchführen `nslookup` Gegen den Host |
| Virenscan | Während der Installation dieser OnCommand Insight-Komponente müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Komponente Insight verwendeten Pfade (Installations-, Backup- und Archivierpfade) und alle Installationspfade der DWH-Komponenten (SANscreen-, DB2- und Backup-Pfade) vom Virenscan ausgeschlossen werden. |

| | |
|---|---|
| Visual Studio | Visual Studio 2019 "Weiterverteilbare Dateien" Muss vor der Installation von Data Warehouse mit Reporting unter Windows installiert werden. |

### Anforderungen an den Remote Acquisition Unit-Server

Sie müssen eine Remote Acquisition Unit (rau) installieren, um Informationen von SAN-Geräten zu erhalten, die sich hinter einer Firewall, an einem Remote-Standort, in einem privaten Netzwerk oder in verschiedenen Netzwerksegmenten befinden. Bevor Sie die rau installieren, sollten Sie sicherstellen, dass Ihre Umgebung den Anforderungen an das rau-Betriebssystem, die CPU, den Arbeitsspeicher und den Festplattenspeicher entspricht.

| Komponente | Anforderungen |
|---|---|
| Betriebssystem | Ein Computer, auf dem 64-Bit Microsoft Windows Server 2016, 2019 oder 2022 mit dem neuesten Service Pack ausgeführt wird. Windows .NET Framework Version 3.5 muss vor der Installation von OnCommand Insight installiert werden. |
| CPU | 4 CPU-Kerne |
| Speicher | 16 GB RAM |
| Verfügbarer Festplattenspeicher | 40 GB |
| Netzwerk | 100 Mbit/s /1 Gbit/s Ethernet-Verbindung, statische IP-Adresse, IP-Verbindung zu allen FC-Geräten und ein erforderlicher Port zum OnCommand Insight-Server (80 oder 443). |
| Berechtigungen | Lokale Administratorberechtigungen auf dem rau-Server |
| Virenscan | Während der Installation dieser OnCommand Insight-Komponente müssen Sie alle Virenscanner vollständig deaktivieren. Nach der Installation müssen die von der Insight-Komponente verwendeten Pfade vom Virenscan ausgeschlossen werden. Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen. |

### Von OnCommand Insight unterstützte Browser

Die browserbasierte OnCommand Insightweb-Benutzeroberfläche kann auf mehreren

verschiedenen Browsern betrieben werden.

Insight unterstützt neuere Versionen von nicht-Beta-Versionen der folgenden Browser:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Eine vollständige Liste aller für OnCommand Insight qualifizierten Browser-Versionen finden Sie im "NetApp Interoperabilitäts-Matrix-Tool".

# Installationsanleitung für Insight

Bei der Installation müssen Sie mehrere OnCommand Insight Komponenten installieren, darunter Insight Server sowie Data Warehouse und Reporting.
Die Installation umfasst die folgenden Hauptaufgaben:

- Herunterladen des OnCommand Insight-Installationsprogramms
- OnCommand Insight-Server wird installiert
- Installieren von Lizenzen
- Optional Installation von DWH und Reporting (muss auf einer separaten Maschine oder virtuellen Maschine installiert sein)
- Optional können Sie eine Remote Acquisition Unit (rau) installieren, die Informationen von den Geräteressourcen erfasst, die sich hinter einer Firewall befinden, sich an einem Remote-Standort befinden oder sich in einem privaten Netzwerk befinden
- Aktualisieren der OnCommand Insight-Berichte für Upgrades.

Nach der Installation müssen Sie Insight konfigurieren, um Informationen über Ihre Umgebung zu erfassen. Die erforderlichen Aufgaben werden im *OnCommand Insight Konfigurations- und Administrationshandbuch* beschrieben.

## Herunterladen des OnCommand Insight-Installationsprogramms

Sie können das OnCommand Insight Installationsprogramm von der NetApp Support-Website herunterladen.

### Bevor Sie beginnen

Sie müssen sich auf der NetApp Support Site unter anmelden "mysupport.netapp.com".

### Schritte

1. Melden Sie sich bei dem Server an, auf dem Sie OnCommand Insight installieren möchten.
2. Laden Sie die Installationsdatei von der NetApp Support-Website herunter.

## Installieren des OnCommand Insight-Servers

Sie können den OnCommand Insight-Server ganz einfach mithilfe des OnCommand

## Insight-Einrichtungsassistenten installieren.

### Bevor Sie beginnen

Sie müssen alle Installationsvoraussetzungen erfüllt haben.

> Wenn Sie OnCommand Insight aktualisieren, müssen Sie den Tresor vor der Deinstallation oder Aktualisierung Ihrer aktuellen Version sichern.

### Schritte

1. Melden Sie sich beim Insight-Server mit einem Konto mit Administratorrechten an.
2. Öffnen Sie Windows Explorer, und navigieren Sie zu dem Verzeichnis, in dem sich die Installationsdateien befinden.
3. Doppelklicken Sie auf `.MSI` Heruntergeladene Datei.
4. Klicken Sie auf **Weiter**, um fortzufahren.
5. Lesen Sie die Lizenzvereinbarung, aktivieren Sie das Kontrollkästchen **Ich akzeptiere die Bedingungen im Lizenzvertrag**, und klicken Sie dann auf **Weiter**.
6. Geben Sie den Kundennamen und den Standortnamen in das Fenster **Customer Information** ein und klicken Sie auf **Next**.

   **Best Practice:** Verwenden Sie den Kundennamen als Präfix für die Website: Zum Beispiel NetApp.

7. Geben Sie ein Administratorkennwort ein. Bestätigen Sie das Passwort.
8. Gehen Sie im Fenster **Customer Information: Konfigurieren Sie NetApp ASUP** folgendermaßen vor:

   a. Wählen Sie eine der folgenden Optionen aus, um die Datenbank mit den Daten auszuwählen, die Sie auf ASUP hochladen möchten:

      - **Kein Datenbank-Backup**: Ein Backup wird nicht an ASUP gesendet.
      - **Sicherung ohne Leistungsdaten**: Ein Backup wird erstellt und an ASUP gesendet, enthält aber keine Leistungsdaten.
      - **Backup mit Leistungsdaten**: Ein Backup wird erstellt, das Leistungsdaten enthält, aber dies könnte eine riesige erzeugen `*.gz` Datei:

   > ASUP wird über HTTPS-Protokoll geliefert.

   +

   a. Wählen Sie unter **Logs** aus, ob keine Protokolle, Basisprotokolle oder erweiterte Protokolle, die eine Datenquellaufzeichnung enthalten, verwendet werden sollen.
   b. Klicken Sie Auf **Weiter**.

9. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Kontrollkästchen aktivieren, um das Senden von Nutzungsinformationen an NetApp im Abschnitt **Nutzungsdaten senden** zu aktivieren.
10. Klicken Sie Auf **Weiter**
11. Wählen Sie im Fenster **Server konfigurieren** die entsprechenden Konfigurationsparameter aus oder legen Sie sie fest, um den OnCommand Insight-Server zu konfigurieren:

| Option | Beschreibung |
| --- | --- |
| Portal-Port (HTTP) | Ports, die vom OnCommand Insight-Server zur Unterstützung von Benutzerwebservices verwendet werden, einschließlich eines Portals zur Durchführung von Verwaltungsaufgaben. Verwenden Sie den Standardwert (80). Wenn der Standardport verwendet wird, ändern Sie ihn jedoch in einen anderen Port. |
| Portal-Port (HTTPS) | Port, der von Remote-Akquisitionseinheiten verwendet wird, um SAN-Änderungsinformationen über einen sicheren Kanal an den OnCommand Insight-Server zu senden. Verwenden Sie den Standardwert (443). Wenn der Standardport verwendet wird, ändern Sie ihn jedoch in einen anderen Port. Sie geben diese gleiche Portnummer bei der Konfiguration von raus an. |
| Interner Datenbank-Port (SQL) | Port, der intern vom PC verwendet wird, auf dem der OnCommand Insight-Server ausgeführt wird, um als Zugriffspunkt für die Datenbank zu dienen. Verwenden Sie den Standardwert (3306). Wenn der Standardport verwendet wird, ändern Sie ihn jedoch in einen anderen Port. |

12. Klicken Sie Auf **Weiter**.
13. Klicken Sie auf **Installieren**, um fortzufahren.

    Die Installation sollte je nach installierter Anwendung ca. 20 Minuten dauern.

14. Klicken Sie Auf **Fertig Stellen**.
15. Wenn Sie eine Remote Acquisition Unit (rau) installieren, müssen Sie das SecurityAdmin-Tool ausführen, um ein Passwort für den Benutzer *Acquisition* zu erstellen. Sie benötigen dieses Passwort, wenn Sie die rau installieren.

    Hinweis: Wenn Sie dieses Passwort erstellt haben, müssen Sie den Server und die rau wie unten angegeben synchronisieren.

### Server mit DWH und rau synchronisieren

Nach der Installation der Remote-Erfassungseinheit und/oder des Data Warehouse müssen Sie die rau/DWH mit dem OnCommand Insight-Server synchronisieren. Führen Sie die folgenden Schritte aus:

"Server und rau synchronisieren (Windows)"

"Server und DWH synchronisieren (Windows)"

"Server und rau synchronisieren (Linux)"

"Server und DWH synchronisieren (Linux)"

## Installieren von OnCommand Insight Data Warehouse und Reporting

Die Installation ist in sich abgeschlossen und beinhaltet die Elemente, die zum Ausführen und Betrieb des OnCommand Insight Data Warehouse (DWH) und der Reporting-Dienstprogramme erforderlich sind.

### Bevor Sie beginnen

Beachten Sie Folgendes, bevor Sie die Installation oder Aktualisierung durchführen.

- Wenn Sie ein Upgrade durchführen, erstellen Sie ein Backup von DWH.
- Sie müssen über lokale *Administrator*Berechtigungen verfügen, um OnCommand Insight Data Warehouse mit Berichterstellung zu installieren.
- Stellen Sie sicher, dass der Windows Modules Installer-Dienst aktiviert ist (entweder automatisch oder manuell).
- Bei der Installation auf einem Laufwerk ohne C: Müssen kurze Dateinamen aktiviert sein. Wenn es nicht aktiviert ist, wird es vom Installationsprogramm aktiviert.
- Für die DB2-Komponente kann der DB2-Benutzer entweder *Domain* user oder *local* user sein.
  - Wenn der DB2-Benutzer ein *Domain*-Benutzer ist, müssen Sie über Folgendes verfügen:
    - DB2-Benutzer muss bereits erstellt worden sein, und Sie müssen den Benutzernamen und das Kennwort kennen
    - Als Benutzer, der DWH mit Reporting installiert, müssen Sie in der Lage sein, den DB2-Benutzer abzufragen. Sie können dies mit dem folgenden Befehl überprüfen:
      - `net user <db2 user name> /domain`
  - Wenn DB2-Benutzer ein *local*-Benutzer ist, müssen Sie über Folgendes verfügen:
    - Benutzername und Passwort für den Benutzer, der als DB2-Benutzer ausgeführt wird. Wenn dieser Benutzer nicht existiert, wird er von der Installation erstellt.
  - [HINWEIS]

Der DB2-Benutzername sowie der Windows-Anmeldename haben folgende Einschränkungen: * Gültige Zeichen sind: 'A' bis 'Z'; 'A' bis 'z'; '0' bis '9'; '@'; *''; '!'; '('; ')'; '{'; '}'; '-'; und '.'. * Bei Verwendung der Sonderzeichen '!'; ' '('; ')'; '{'; '}'; '-'; und '.' Sie müssen für den Benutzernamen alle Großbuchstaben verwenden. * Das erste Zeichen in der Zeichenfolge muss ein alphabetisches Zeichen, @, # oder € sein; es kann keine Zahl sein oder die Buchstabensequenzen _SYS*, *DBM* oder *IBM* * Es darf 128 Byte lang sein. * Es kann nicht BENUTZER sein, ADMINISTRATOREN, GÄSTE, ÖFFENTLICH, LOKAL oder ein SQL-reserviertes Wort.

- Der DB2-Benutzer kann nicht mit dem Benutzer identisch sein, der die Installation durchführt.

### Schritte

1. Melden Sie sich beim Data Warehouse-Server mit einem Konto mit Administratorrechten an.
2. Laden Sie die ZIP-Datei „Data Warehouse with Reporting“ herunter, und extrahieren Sie die Dateien in einen Installationsordner.

3. Navigieren Sie zum Ordner *<download location>\oci_dwh_Installer* und führen Sie das Skript *install_oci_dwh.bat* aus.

   Bei OnCommand Insight 7.3.10 und höher müssen Sie das Skript für die ordnungsgemäße Installation von DWH/Reporting ausführen. Führen Sie die ausführbare .MSI-Installationsdatei nicht aus.

4. Geben Sie die DB2-Domäne ein, oder drücken Sie die Eingabetaste für die lokale Domäne.
5. Geben Sie den DB2-Benutzernamen ein. Einschränkungen für Benutzernamen siehe oben.
6. Geben Sie das Kennwort für den DB2-Benutzer ein. Geben Sie das Passwort erneut ein, wenn Sie dazu aufgefordert werden.
7. Geben Sie den Installationspfad für die DB2-Komponente ein, oder drücken Sie die Eingabetaste, um die Standardeinstellung zu übernehmen.
8. Die von Ihnen eingegebenen Informationen werden angezeigt. Überprüfen Sie alle Einstellungen sorgfältig. Drücken Sie die Eingabetaste, um die Installation zu starten.
9. Wenn Sie dazu aufgefordert werden, lassen Sie Windows mit der DB2-Installation fortfahren.
10. Nach der DB2-Installation wird der DWH-Installationsassistent ausgeführt. Befolgen Sie die Anweisungen, um DWH mit Reporting zu installieren.

    Data Warehouse mit Reporting Installation kann bis zu einer Stunde dauern.

### Server und DWH synchronisieren

Nach der Installation des Data Warehouse müssen Sie das Data Warehouse mit dem OnCommand Insight Server synchronisieren. Führen Sie hierzu folgende Schritte aus:

1. Starten Sie auf dem OnCommand Insight-Serversystem das Tool **SecurityAdmin** im interaktiven Modus

```
 securityadmin -i
. Ändern Sie das Passwort für die Benutzer _inventar_ und _dwh_internal_
in Passwörter Ihrer Wahl. *Beachten Sie diese Passwörter*, da Sie sie
unten benötigen.
. Starten Sie den DWH-Dienst neu.
. Starten Sie bei *each Connector* das Tool *SecurityAdmin* im
interaktiven Modus. Sie benötigen die Passwörter, die Sie in Schritt 2
oben angegeben haben.
```

```
 securityadmin -i
. Ändern Sie die Passwörter für die Benutzer _inventar_ und
_dwh_internal_ in die in Schritt 2 verwendeten Passwörter.
. Starten Sie die Dienste auf den Connectors neu.
. Fügen Sie die Connectors zu DWH hinzu, indem Sie die Passwörter für
_Inventory_ und _dwh_Internal_ Benutzer aus Schritt 2 verwenden
```

### Suche nach IBM Cognos-Dokumentation

Grundlegende Informationen zum Starten und Stoppen der Berichtsportal-Software finden Sie in der Dokumentation von IBM Cognos, die mit dem Produkt installiert ist. Sie können mit einem Webbrowser Informationen zu allen IBM Cognos-Berichtsprodukten wie Query Studio, Report Studio, Business Insight oder Business Insight Advanced auf der IBM-Website in den Informationszentren für diese Softwareprodukte suchen.

#### Schritte

1. Navigieren Sie zu diesem Verzeichnis, um die mit OnCommand Insight installierte IBM Cognos-Dokumentation zu finden.

   ```
   <install_dir\>\cognos\c10_64\webcontent\documentation\help_docs.html
   ```

2. Sie können auch Themen anzeigen, die einzelne IBM Cognos-Fenster beschreiben, die im OnCommand Insight-Berichtsportal verwendet werden. Klicken Sie in der Symbolleiste des Fensters auf das Symbol **?**.

### Überprüfen der Installation von Data Warehouse und Reporting

Nach einer erfolgreichen OnCommand Insight-Data-Warehouse-Installation sollten Sie sicherstellen, dass alle DWH- und Berichtsdienste in Ihren Microsoft Windows-Diensten verfügbar sind.

#### Schritte

1. Wählen Sie im Windows-Startmenü die Option MENU:Systemsteuerung [System und Sicherheit > Verwaltung > Dienste].
2. Stellen Sie sicher, dass die folgenden Einträge in der Liste der Dienste angezeigt werden:

| Name / Bundesland | Beschreibung |
|---|---|
| **SANscreen-Server / läuft** | Der OnCommand Insight DWH-Server |
| **MySQL / Running** | Die OnCommand Insight SQL-Datenbank |
| **IBM Cognos/Running** | IBM Cognos Content Database |
| **DB2- DB2COPY1 - DB2-0 / LÄUFT** | Management von DB2-Datenbanken |
| **DB2 Governor (DB2COPY1) / wird nicht ausgeführt** | Sammelt Statistiken für Anwendungen, die mit DB2-Datenbanken verbunden sind. |
| **DB2-Lizenzserver (DB2COPY1)/nicht ausgeführt** | Überwacht die Einhaltung von DB2-Lizenzen. |
| **DB2 Management Service (DB2COPY1) / läuft** | Verwaltet DB2-Registrierungseinträge auf Kompatibilität mit früheren DB2-Kopierversionen. |

| | |
|---|---|
| **DB2 Remote Command Server (DB2COPY1) / läuft** | Unterstützt Remote-Ausführung von DB2-Befehlen. |
| **IBM Secure Shell Server für Windows / nicht aktiv** | IBM Secure Shell Server für Windows |

## Installieren einer Remote Acquisition Unit (rau)

Installieren Sie einen oder mehrere RAUS in Ihrer OnCommand Insight-Umgebung.

### Bevor Sie beginnen

Sie müssen alle Installationsvoraussetzungen erfüllt haben.

Mindestens ein Port muss geöffnet und zwischen dem rau-Server und dem OnCommand Insight-Server verfügbar sein, um Änderungsinformationen an den Server weiterzuleiten. Wenn Sie sich darüber nicht sicher sind, validieren Sie ihn, indem Sie einen Webbrowser auf dem rau-Computer öffnen und ihn zum OnCommand Insight-Server leiten:

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

Der Erfassungsport ist standardmäßig auf 443 eingestellt, wurde jedoch möglicherweise während der Serverinstallation geändert. Wenn die Verbindung erfolgreich war, wird eine OnCommand Insight-Antwortseite angezeigt, die einen offenen und verfügbaren Port zwischen der rau und dem OnCommand Insight-Server anzeigt.

### Schritte

1. Melden Sie sich beim rau-Server mit einem Konto mit Administratorrechten an.
2. Öffnen Sie Windows Explorer, und navigieren Sie zu dem Verzeichnis, in dem sich die rau-Installationsdatei befindet.
3. Doppelklicken `.MSI` Datei, um die Installation zu starten.
4. Klicken Sie auf **Weiter**, um mit dem Fenster fortzufahren, in dem die Lizenzvereinbarung angezeigt wird. Lesen Sie diese und akzeptieren Sie die Bedingungen der Lizenzvereinbarung und klicken Sie auf **Weiter**.
5. Wählen Sie diese Option, um die rau auf einer lokalen Festplatte oder die gesamte Funktion auf einer lokalen Festplatte zu installieren. (Sie können den Link Festplattennutzung überprüfen, um sicherzustellen, dass Sie über genügend Speicherplatz verfügen – 116 MB sind erforderlich.) Klicken Sie Auf **Weiter**.
6. Legen Sie im Fenster Konfigurieren die für Ihren Standort spezifischen Parameter fest:
   - **OnCommand Insight Servername oder -Adresse** - Hostname oder IP-Adresse, um den OnCommand Insight-Server zu identifizieren. Die rau verwendet diesen Namen/diese IP, um eine Kommunikationsverbindung mit dem Server zu öffnen. Wenn Sie einen Hostnamen angeben, stellen Sie sicher, dass dieser über DNS aufgelöst werden kann.
   - **Name der Akquisitionseinheit** - eindeutiger Name, der die rau identifiziert.
   - **OnCommand Insight Secured Remote Acquisition Port (HTTPS)** - Port, der von Remote Acquisition Units verwendet wird, um Umgebungsänderungsinformationen an den OnCommand Insight-Server zu senden. Diese Einstellung sollte mit dem bei der Installation des OnCommand

Insight-Servers eingegebenen Wert übereinstimmen und auf allen raus gleich sein.

- Geben Sie das Benutzerpasswort *Acquisition* ein.

7. Überprüfen Sie Ihre Auswahl. Klicken Sie auf **Zurück**, um zurückzugehen und Änderungen vorzunehmen. Klicken Sie Auf **Weiter**.
8. Klicken Sie auf **Installieren**, um die Installation zu starten.

   Warten Sie, bis die Installation abgeschlossen ist. Dies dauert etwa 5 bis 10 Minuten.

### Nachdem Sie fertig sind

Nach Abschluss der Installation wird ein letztes Fenster angezeigt. Klicken Sie auf das Feld **Remote Acquisition Service starten**, um die rau zu starten, und klicken Sie auf **Finish**, um diesen Vorgang zu beenden.

Wenn Ihre Daten zu erfassen beginnen, sind Sie alle eingestellt; Sie müssen den Server und die rau wie unten angegeben synchronisieren.

### Server und rau synchronisieren

Wenn die Datenerfassung nach der Installation der Remote-Erfassungseinheit nicht beginnt, synchronisieren Sie die rau mit dem OnCommand Insight-Server. Führen Sie hierzu folgende Schritte aus:

1. Starten Sie auf dem OnCommand Insight-Serversystem das Tool **SecurityAdmin** im interaktiven Modus

```
 securityadmin -i
. Ändern Sie das Passwort für den Benutzer _Acquisition_ für den Insight
Server in ein Passwort Ihrer Wahl. *Bitte beachten Sie dieses Passwort*
wie Sie es unten benötigen.
. Starten Sie den Server/LAU neu.
. Starten Sie auf dem rau-System (Remote Acquisition Unit) das Tool
*SecurityAdmin* im interaktiven Modus. Sie benötigen das Passwort, das
Sie in Schritt 2 oben angegeben haben.
```

```
 securityadmin -i
. Ändern Sie das Passwort für den Benutzer _Acquisition_ auf das in
Schritt 2 verwendete Passwort.
. Starten Sie den RAU neu.
```

### Überprüfen des Dienstes der Fernbedienungseinheit

Nach erfolgreicher Installation einer Remote Acquisition Unit (rau) sollte der OnCommand Insight rau-Service in der Microsoft Windows-Serviceumgebung verfügbar sein.

**Schritte**

1. Um zu überprüfen, ob die rau zu den Windows-Diensten hinzugefügt wurde, öffnen Sie das Windows-Startmenü und wählen Sie **Systemsteuerung** > **Verwaltung** > **Dienste**.
2. Suchen Sie in der Liste **OnCommand Insight Acq – OnCommand Insight's Remote Acquisition Unit (rau)**.

### Überprüfen der Installation der Fernbedienungseinheit

Um die ordnungsgemäße Installation der Remote Acquisition Unit zu überprüfen, können Sie den Status der Remote Acquisition Units anzeigen, die mit Ihrem Server verbunden sind.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Acquisition Units**.
3. Überprüfen Sie, ob die neue Fernaufnahmungseinheit korrekt registriert wurde und den Status „Verbunden“ aufweist.

   Ist dies nicht der Fall, wenden Sie sich an den technischen Support.

## Überprüfen der Installation

Sie können Insight in einem unterstützten Browser öffnen, um die Installation zu überprüfen. Möglicherweise sollten Sie auch die Insight-Protokolldateien überprüfen.

Wenn Sie Insight zum ersten Mal öffnen, wird die Seite zur Lizenzeinrichtung geöffnet. Nachdem Sie die Lizenzinformationen eingegeben haben, müssen Sie die Datenquellen einrichten. Informationen zum Eingeben von Datenquellen-Definitionen und zum Einrichten von Insight-Benutzern und -Benachrichtigungen finden Sie im *OnCommand Insight-Konfigurations- und Administrationshandbuch*.

Bei Problemen mit der Installation wenden Sie sich an den technischen Support, und geben Sie die gewünschten Informationen an.

### Überprüfung der neuen Insight-Dienste

Nach einer erfolgreichen Installation sollten Sie überprüfen, ob die Dienste für die Insight-Komponenten auf Ihrem Server ausgeführt werden.

**Schritte**

1. So zeigen Sie eine Liste der derzeit ausgeführten Dienste an:
   a. Klicken Sie auf die Schaltfläche **Start**.
   b. Klicken Sie Auf **Ausführen**.
   c. Geben Sie Folgendes ein:

      ```
      cmd
      ```

   d. Drücken Sie Die Eingabetaste.

e. Geben Sie im Fenster **Eingabeaufforderung** Folgendes ein:

```
net start
```

2. Prüfen Sie in der Liste auf die folgenden Insight-Services:
   - **SANscreen-Server**
   - **SANscreen Acq** (der Akquisitionsprozess)
   - **MySQL** (Insight SQL-Datenbank)
   - **Elasticsearch** (Data Store for Insight Data) Falls diese Dienste nicht in der Liste angezeigt werden, wenden Sie sich an den technischen Support.

#### Insight-Protokolle

Insight bietet zahlreiche Protokolldateien, die Sie bei der Recherche und Fehlerbehebung unterstützen. Die verfügbaren Protokolle werden im Protokollverzeichnis aufgeführt. Sie können ein Protokollüberwachungstool wie BareTail verwenden, um alle Protokolle gleichzeitig anzuzeigen.

Die Protokolldateien befinden sich im `<install directory>\SANscreen\wildfly\standalone\log` Verzeichnis. Die Erfassungsprotokolle befinden sich im `<install directory>\SANscreen\Acq\Log` Verzeichnis.

#### Zugriff auf die Web-UI

Nach der Installation von OnCommand Insight müssen Sie Ihre Lizenzen installieren und dann Insight einrichten, um Ihre Umgebung zu überwachen. Dazu rufen Sie die Web-UI von Insight über einen Webbrowser auf.

##### Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Open Insight auf dem Insight-Server:

     ```
     https://fqdn
     ```

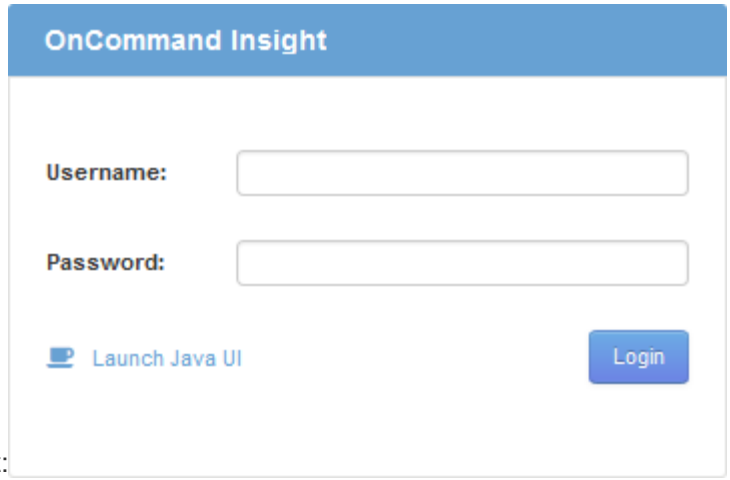
   - Insight von jedem beliebigen anderen Speicherort aus öffnen:

     ```
     https://fqdn:port
     ```

     Die Portnummer ist entweder 443 oder ein anderer Port, der bei der Installation des Insight-Servers konfiguriert wurde. Die Portnummer ist standardmäßig 443, wenn Sie sie nicht in der URL angeben.

   Das Dialogfeld OnCommand Insight wird

angezeigt:




2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.

   Wenn die Lizenzen installiert wurden, wird die Seite zur Einrichtung der Datenquelle angezeigt.

   Eine Insight Browser-Sitzung, die 30 Minuten lang inaktiv war, wurde überschritten, und Sie werden automatisch vom System abgemeldet. Für zusätzliche Sicherheit empfiehlt es sich, den Browser nach der Abmeldung von Insight zu schließen.

### Installieren Ihrer Insight Lizenzen

Wenn Sie die Lizenzdatei mit den Insight Lizenzschlüsseln von NetApp erhalten haben, können Sie mithilfe der Setup-Funktionen alle Ihre Lizenzen gleichzeitig installieren.

#### Über diese Aufgabe

Die Insight Lizenzschlüssel werden in einem gespeichert `.txt` Oder `.lcn` Datei:

#### Schritte

1. Öffnen Sie die Lizenzdatei in einem Texteditor und kopieren Sie den Text.
2. Öffnen Sie Insight in Ihrem Browser.
3. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
4. Klicken Sie Auf **Setup**.
5. Klicken Sie auf die Registerkarte **Lizenzen**.
6. Klicken Sie Auf **Lizenz Aktualisieren**.
7. Kopieren Sie den Text des Lizenzschlüssels in das Textfeld **Lizenz**.
8. Wählen Sie den Vorgang **Update (am häufigsten)** aus.
9. Klicken Sie Auf **Speichern**.
10. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Kontrollkästchen aktivieren, um das Senden von Nutzungsinformationen an NetApp im Abschnitt **Nutzungsdaten senden** zu aktivieren. Proxy muss ordnungsgemäß konfiguriert und für Ihre Umgebung aktiviert sein.

#### Nachdem Sie fertig sind

Nach der Installation der Lizenzen können Sie die folgenden Konfigurationsaufgaben ausführen:

- Datenquellen konfigurieren.
- Erstellen Sie OnCommand Insight-Benutzerkonten.

#### OnCommand Insight-Lizenzen

## OnCommand Insight arbeitet mit Lizenzen, die bestimmte Funktionen auf dem Insight Server ermöglichen.

- **Entdecken**

  Discover ist die grundlegende Insight-Lizenz, die die Inventarisierung unterstützt. Sie müssen über eine Discover-Lizenz verfügen, um OnCommand Insight verwenden zu können, und die Discover-Lizenz muss mit mindestens einer der Lizenzen Assure, Perform oder Plan gekoppelt werden.

- * Versichern*

  Eine Assure Lizenz bietet Support für Assurance-Funktionalität, einschließlich globaler und SAN-Pfadrichtlinien und Management von Verstößen. Mit einer Assure-Lizenz können Sie auch Schwachstellen anzeigen und managen.

- **Ausführen**

  Eine Lizenz ausführen unterstützt die Leistungsüberwachung auf Bestandsseiten, Dashboard-Widgets, Abfragen usw. sowie die Verwaltung von Performance-Richtlinien und -Verstößen.

- **Plan**

  Eine Planlizenz unterstützt Planungsfunktionen, einschließlich Ressourcenverwendung und -Zuweisung.

- **Host Utilization Pack**

  Eine Host-Nutzungslizenz unterstützt die Auslastung des Dateisystems auf Hosts und virtuellen Maschinen.

- **Authoring Melden**

  Eine Lizenz zur Erstellung von Berichten unterstützt zusätzliche Autoren für die Berichterstellung. Diese Lizenz erfordert die Planlizenz.

OnCommand Insight Module sind für einen Jahreszeitraum oder unbefristet lizenziert:

- Nach Terabyte überwachter Kapazität für Discover, Assure, Plan, Perform Module
- Nach Anzahl der Hosts für das Host Utilization Pack
- Nach Anzahl der zusätzlichen für die Berichterstellung erforderlichen Cognos Pro-Autoren

Lizenzschlüssel sind ein Satz eindeutiger Zeichenfolgen, die für jeden Kunden generiert werden. Sie können die Lizenzschlüssel von Ihrem OnCommand Insight-Vertreter beziehen.

Ihre installierten Lizenzen steuern die folgenden Optionen, die in der Software verfügbar sind:

- **Entdecken**

  Inventarisierung und Bestandsverwaltung (Foundation)

  Überwachen von Änderungen und Verwalten von Bestandsrichtlinien

- * Versichern*

  Anzeige und Management von Richtlinien und Verstößen für SAN-Pfade

  Anzeigen und Verwalten von Schwachstellen

  Anzeigen und Managen von Aufgaben und Migrationen

- **Plan**

  Anfragen anzeigen und verwalten

  Anzeigen und Verwalten ausstehender Aufgaben

  Anzeige und Verwaltung von Reservierungsverletzungen

  Anzeige und Verwaltung von Verstößen gegen die Portbilanz

- **Ausführen**

  Überwachen Sie Leistungsdaten, einschließlich Daten in Dashboard-Widgets, Bestandsseiten und Abfragen

  Anzeige und Management von Performance-Richtlinien und -Verstößen

Die folgenden Tabellen enthalten Details zu den Funktionen, die mit und ohne die Lizenz „Perform“ für Administratorbenutzer und Benutzer ohne Administratorrechte verfügbar sind.

| Funktion (Admin) | Mit Perform Lizenz | Ohne Lizenz ausführen |
|---|---|---|
| Applikation | Ja. | Keine Leistungsdaten oder Diagramme |
| Virtual Machine | Ja. | Keine Leistungsdaten oder Diagramme |
| Hypervisor | Ja. | Keine Leistungsdaten oder Diagramme |
| Host | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenspeicher | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| VMDK | Ja. | Keine Leistungsdaten oder Diagramme |
| Internes Volumen | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenmenge | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Pool | Ja. | Keine Leistungsdaten oder Diagramme |
| Festplatte | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Node | Ja. | Keine Leistungsdaten oder Diagramme |
| Fabric | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch-Port | Ja. | Keine Leistungsdaten oder Diagramme; „`Port Errors`“ zeigt „`N/A`“ an |
| Speicherport | Ja. | Ja. |
| NPV-Port | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| NPV-Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| Qtrees | Ja. | Keine Leistungsdaten oder Diagramme |
| Kontingente | Ja. | Keine Leistungsdaten oder Diagramme |
| Pfad | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| Zone | Ja. | Keine Leistungsdaten oder Diagramme |
| Zonenmitglied | Ja. | Keine Leistungsdaten oder Diagramme |
| Generisches Gerät | Ja. | Keine Leistungsdaten oder Diagramme |
| Tape | Ja. | Keine Leistungsdaten oder Diagramme |
| Maskierung | Ja. | Keine Leistungsdaten oder Diagramme |
| ISCSI-Sitzungen | Ja. | Keine Leistungsdaten oder Diagramme |
| ICSI-Netzwerkportale | Ja. | Keine Leistungsdaten oder Diagramme |
| Suche | Ja. | Ja. |
| Admin | Ja. | Ja. |
| Dashboard | Ja. | Ja. |
| Widgets | Ja. | Teilweise verfügbar (nur Asset-, Abfrage- und Admin-Widgets sind verfügbar) |
| Dashboard zu Verstößen | Ja. | Verborgen |
| Ressourcen-Dashboard | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Management von Performance-Richtlinien | Ja. | Verborgen |
| Verwalten von Anmerkungen | Ja. | Ja. |
| Verwalten von Anmerkungsregeln | Ja. | Ja. |
| Management von Applikationen | Ja. | Ja. |

| | | |
|---|---|---|
| Abfragen | Ja. | Ja. |
| Verwalten von Geschäftseinheiten | Ja. | Ja. |

| Merkmal | User - mit Perform-Lizenz | Guest - mit Perform-Lizenz | User - ohne Lizenz ausführen | Guest - ohne Lizenz durchführen |
|---|---|---|---|---|
| Ressourcen-Dashboard | Ja. | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Benutzerdefiniertes Dashboard | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) |
| Management von Performance-Richtlinien | Ja. | Verborgen | Verborgen | Verborgen |
| Verwalten von Anmerkungen | Ja. | Verborgen | Ja. | Verborgen |
| Management von Applikationen | Ja. | Verborgen | Ja. | Verborgen |
| Verwalten von Geschäftseinheiten | Ja. | Verborgen | Ja. | Verborgen |
| Abfragen | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) |

## Fehlerbehebung bei Installationen

OnCommand Insight-Installationen werden in der Regel über die Installationsassistenten verwaltet. Es kann jedoch zu Problemen bei Upgrades oder Konflikten aufgrund von Computerumgebungen kommen.

Sie sollten außerdem sicher sein, dass Sie alle erforderlichen OnCommand Insight-Lizenzen für die Installation der Software installieren.

#### Fehlende Lizenzen

Für verschiedene OnCommand Insight-Funktionen sind unterschiedliche Lizenzen erforderlich. Die in OnCommand Insight angezeigten Informationen werden von Ihren

installierten Lizenzen gesteuert. Informationen über die Funktionen, die von den einzelnen Lizenzen gesteuert werden, finden Sie im Abschnitt OnCommand Insight-Lizenzen.

Informationen über die Funktionen, die von den einzelnen Lizenzen gesteuert werden, finden Sie im Abschnitt OnCommand Insight-Lizenzen.

#### Einreichung einer technischen Online-Support-Anfrage

Wenn Sie als registrierter Support-Kunde Probleme mit der Installation von Insight haben, können Sie eine technische Online-Support-Anfrage stellen.

##### Bevor Sie beginnen

Sie müssen sich unter Verwendung Ihrer Unternehmens-E-Mail-Adresse als Support-Kunde registrieren, um Online-Support-Services zu erhalten. Die Registrierung erfolgt über die Support Site .

##### Über diese Aufgabe

Um den Kunden-Support bei der Lösung des Installationsproblem zu unterstützen, sollten Sie so viele Informationen wie möglich sammeln, einschließlich der folgenden Punkte:

- Insight Seriennummer
- Beschreibung des Problems
- Alle Insight-Protokolldateien
- Bildschirmaufnahme aller Fehlermeldungen

##### Schritte

1. Erstellen Sie ein `.zip` Datei der Informationen, die Sie gesammelt haben, um ein Fehlerbehebungspaket zu erstellen.
2. Melden Sie sich auf der Support-Website unter an "mysupport.netapp.com" Und wählen Sie **Technische Unterstützung**.
3. Klicken Sie auf **Fall öffnen**.
4. Befolgen Sie die Anweisungen zu Ihrem Datenpaket.

##### Nachdem Sie fertig sind

Sie können **Fallstatus prüfen** auf der Seite Technische Unterstützung verwenden, um Ihrer Anfrage zu folgen.

# OnCommand Insight wird aktualisiert

Normalerweise muss ein Upgrade auf allen Insight Servern (Insight Server, Data Warehouse Server, Remote Acquisition Unit) durchgeführt werden. Die Upgrade-Anforderungen für eine neue Version von OnCommand Insight sollten immer in den Versionshinweisen nachschlagen.

Sofern nicht anders angegeben, gelten die Anforderungen und Verfahren für das Upgrade von Insight 7.x auf die aktuelle Version von Insight. Wenn Sie ein Upgrade von einer Version vor 7.0 durchführen, wenden Sie sich an Ihren Kundenbetreuer.

## Aktualisieren von Insight auf Version 7.3.12 oder höher - Windows

Vor dem Upgrade von OnCommand Insight 7.3.10 auf 7.3.11 Version 7.3.12 oder höher müssen Sie das OCI Datenmigrationstool ausführen.

### Hintergrund

OnCommand Insight Version 7.3.12 und höher verwenden zugrunde liegende Software, die möglicherweise mit früheren Versionen nicht kompatibel ist. Insight Version 7.3.12 und höher enthalten ein **Data Migration Tool** zur Unterstützung beim Upgrade.

OnCommand Insight Versionen 7.3.9 und früher werden nicht mehr unterstützt. Wenn Sie eine dieser Versionen ausführen, müssen Sie vor dem Upgrade auf 7.3.12 oder höher auf Insight Version 7.3.10 oder höher (7.3.11 wird dringend empfohlen) aktualisieren.

### Welche Funktionen Bietet Das Datenmigrationstool?

Das Migrationstool führt zunächst eine Kompatibilitätsprüfung durch und folgt dann einem von drei verschiedenen Upgrade-Pfaden. Der ausgewählte Pfad basiert auf der Datenkompatibilität Ihrer aktuellen Version.

Vor dem Upgrade müssen Sie das Data Migration Tool ausführen und die empfohlenen Schritte ausführen.

### Bevor Sie beginnen

- Es wird dringend empfohlen, das OnCommand Insight-System vor dem Ausführen des Datenmigrationstools zu sichern.
- Der Elasticsearch-Service auf dem Server muss betriebsbereit sein.
- Das Data Migration Tool *must* muss für die Datenbank und alle Performance-Archive ausgeführt werden, bevor Sie Insight aktualisieren.

### Ausführen des Data Migration Tools

1. Laden Sie die aktuelle Version des Data Migration Tools (z. B. *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) sowie die entsprechende Insight Installer-Datei auf Ihren Insight Server herunter. Entpacken Sie die ZIP-Datei in einen Arbeitsordner. Downloads finden Sie auf der "NetApp Support Website".
2. Öffnen Sie ein Befehlsfenster, und navigieren Sie zu Ihrem Arbeitsordner.
   - Öffnen Sie PowerShell als Administrator.
3. Führen Sie das Datenmigrationstool über den folgenden Befehl aus:
   - `.\*SANScreenDataMigrationTool.ps1*`
4. Befolgen Sie bei Bedarf die Anweisungen. Im Folgenden ein Beispiel.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
       the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

Das Data Migration Tool überprüft, ob veraltete Indizes auf Ihrem System vorhanden sind, und meldet, ob sie gefunden wurden. Wenn keine vorhanden sind, wird das Werkzeug beendet.

Einige Indizes können migriert werden, während der SANscreen-Serverdienst ausgeführt wird. Andere können nur migriert werden, wenn der Server angehalten wird. Wenn keine Indizes vorhanden sind, die migriert werden können, wird das Tool beendet. Befolgen Sie andernfalls die Anweisungen, wie Sie dazu aufgefordert werden.

Wenn das Data Migration Tool abgeschlossen ist, wird es erneut auf veraltete Indizes überprüft. Wenn alle Indizes migriert wurden, informiert Sie das Tool darüber, dass ein Upgrade auf OnCommand Insight 7.3.12 unterstützt wird. Sie können jetzt mit dem Upgrade der Insight fortfahren.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-127

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory:  D:\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 5 obsolete indexes. Of these,
     5 indexes need to be migrated with OCI server stopped

Verifying migration component is present...
SANscreen Server service is Stopped

Proceed with offline migration of 5 indexes (y or [n])?: y
Preparing to perform migration...
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;
backup; delete old; restore new; cleanup; done.
Execution time 0:00:15

Checking for obsolete (version 5) indexes...
No obsolete indexes found.  Upgrade to 7.3.12+ is supported.

C:\Users\root\Desktop\SANScreenDataMigrationTool-x64-7.3.12-127>
```

Wenn Sie aufgefordert wurden, den SANscreen-Dienst zu beenden, starten Sie ihn vor dem Upgrade von Insight neu.

**Validierungsfehler**

Falls die Indexvalidierung fehlschlägt, informiert Sie das Migrationstool vor dem Beenden über das Problem.

**OnCommand Insight ist nicht vorhanden:**

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

**Ungültige Insight-Version:**

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

**Elasticsearch-Dienst läuft nicht:**

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory:  C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

**Befehlszeilenoptionen**

Das Datenmigrationstool enthält einige optionale Parameter, die sich auf den Betrieb auswirken.

| Option (Windows) | Funktion |
|---|---|

| | |
|---|---|
| -S | Alle Eingabeaufforderungen unterdrücken |
| -Perf_Archive | Wenn angegeben, werden vorhandene Archiveinträge für alle Daten ersetzt, deren Index(e) migriert werden. Der Pfad sollte auf das Verzeichnis verweisen, das die ZIP-Dateien für den Archiveintrag enthält.<br><br>Ein Argument von '-' kann angegeben werden, um anzuzeigen, dass kein Performance-Archiv aktualisiert werden muss.<br><br>Wenn dieses Argument vorhanden ist, wird die Eingabeaufforderung für den Archivspeicherort unterdrückt. |
| -Check | Falls vorhanden, wird das Skript sofort nach der Meldung der Indexzahlen beendet. |
| -Dryrun | Falls vorhanden, meldet die ausführbare Migrationsdatei die Aktionen, die ausgeführt werden würden (zum Migrieren von Daten und Aktualisieren von Archiveinträgen), führt die Vorgänge jedoch nicht aus. |

## Überblick über den OnCommand Insight Upgrade-Prozess

Bevor Sie mit dem Upgrade von Insight beginnen, sollten Sie sich unbedingt über den Upgrade-Prozess informieren. Der Upgrade-Prozess ist für die meisten Versionen von Insight gleich.

**Sie müssen den Tresor** sichern, bevor Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

Der Upgrade-Prozess für Insight umfasst die folgenden grundlegenden Aufgaben:

- Herunterladen der Installationspakete
- Sichern der Data Warehouse-Datenbank

  Um die Möglichkeit falscher Berichte zu vermeiden, müssen Sie die Data Warehouse-Datenbank sichern, bevor Sie die Insight-Datenbank sichern.

- Sichern der Insight-Datenbank

  Die Insight Datenbank wird automatisch gesichert, wenn Sie das Upgrade durchführen. Es empfiehlt sich, vor dem Upgrade ein Backup der Datenbank zu erstellen und das Backup an einem anderen Ort als auf dem Insight Server abzulegen. Während des Upgrade-Prozesses erfasst Insight keine neuen Daten. Um die Menge der nicht erfassten Daten zu minimieren, müssen Sie das Datenbank-Backup innerhalb von ein oder zwei Stunden Ihrer geplanten Upgrade-Zeit starten.

- Sichern Sie die Sicherheitskonfiguration für Data Warehouse und Remote Acquisition Unit, wenn die Konfiguration von der Standardkonfiguration geändert wurde.

  Die nicht standardmäßige Sicherheitskonfiguration muss nach Abschluss des Upgrades auf dem Data Warehouse und dem rau-Server wiederhergestellt werden, bevor die Data Warehouse-Datenbank auf dem System wiederhergestellt wird.

- Erstellen von Backups benutzerdefinierter Data Warehouse-Berichte

  Wenn Sie die Data Warehouse-Datenbank sichern, werden benutzerdefinierte Berichte eingeschlossen. Die Sicherungsdatei wird auf dem Data Warehouse-Server erstellt. Es wird empfohlen, die benutzerdefinierten Berichte an einem anderen Speicherort als dem Data Warehouse-Server zu sichern.

- Deinstallieren des Data Warehouse und der Remote Acquisition Unit-Software, falls zutreffend

  Der Insight-Server verfügt über ein in-Place-Upgrade. Sie müssen die Software nicht deinstallieren. Mit dem in-Place-Upgrade wird die Datenbank gesichert, die Software deinstalliert, die neue Version installiert und die Datenbank dann wiederhergestellt.

- Aktualisieren der Software auf dem Insight-Server, dem Data Warehouse und den Remote Acquisition Units

  Alle zuvor angewendeten Lizenzen verbleiben in der Registrierung; Sie müssen diese Lizenzen nicht erneut anwenden.

- Ausführen der Aufgaben nach dem Upgrade

### OnCommand Insight Upgrade-Checkliste

Sie können die bereitgestellten Checklisten verwenden, um Ihren Fortschritt bei der Vorbereitung des Upgrades zu erfassen. Diese Aufgaben sollen dazu beitragen, das Risiko von Upgrade-Fehlern zu mindern und den Recovery- und Wiederherstellungsaufwand zu beschleunigen.

#### Checkliste zur Vorbereitung des Upgrades (erforderlich)

**Sie müssen den Tresor** sichern, bevor Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

| Zustand | Abgeschlossen? |
| --- | --- |
| Stellen Sie sicher, dass Sie auf allen Insight-Servern über lokale Windows-Administratorberechtigungen verfügen, die für die Durchführung des Upgrade-Prozesses erforderlich sind. | |
| Wenn sich Ihre Insight-, Data Warehouse- oder Remote Acquisition Unit-Server auf 32-Bit-Plattformen befinden, müssen Sie Ihre Server auf 64-Bit-Plattformen aktualisieren. Ab Insight 7.x sind Upgrades nur für 64-Bit-Plattformen verfügbar. | |

| | |
|---|---|
| Stellen Sie sicher, dass Sie über die erforderlichen Berechtigungen verfügen, um die Antivirensoftware auf allen Servern in Ihrer Umgebung zu ändern oder zu deaktivieren. Um einen Aktualisierungsfehler aufgrund einer aktiven Virenscan-Software zu verhindern, müssen Sie das Insight-Installationsverzeichnis ausschließen (`disk drive:\install directory\sanscreen` Vom Zugriff auf Virenschutzprüfungen während des Upgrades. Nachdem Sie alle Komponenten aktualisiert haben, können Sie die Antivirensoftware sicher wieder aktivieren. Stellen Sie jedoch sicher, dass Sie den Scan so konfigurieren, dass er im Insight-Installationsverzeichnis weiterhin alle Komponenten ausschließt.<br><br>Außerdem müssen Sie den IBM/DB2-Ordner (z. B. *C:\Program Files\IBM\DB2*) nach der Installation von der Virenprüfung ausschließen. | |

**Checkliste zur Vorbereitung des Upgrades (Best Practice)**

| Zustand | Abgeschlossen? |
|---|---|
| Planen Sie ein Upgrade ein, und berücksichtigen Sie dabei, dass die meisten Upgrades mindestens 4 bis 8 Stunden dauern. Größere Unternehmen benötigen länger. Die Upgrade-Zeiten hängen von den verfügbaren Ressourcen (Architektur, CPU und Arbeitsspeicher), der Größe der Datenbanken und der Anzahl der in Ihrer Umgebung überwachten Objekte ab. | |
| Wenden Sie sich bezüglich Ihrer Upgrade-Pläne an Ihren Ansprechpartner, informieren Sie sich über die installierte Insight Version und welche Version Sie aktualisieren möchten. | |
| Stellen Sie sicher, dass Ihre aktuellen Ressourcen, die den Insight, Data Warehouse und Remote Acquisition Units zugewiesen sind, weiterhin die empfohlenen Spezifikationen erfüllen. Weitere Informationen finden Sie in den Richtlinien zur Dimensionierung für alle Server.Alternativ können Sie sich an Ihren Ansprechpartner wenden, um die Richtlinien zur Dimensionierung zu besprechen. | |

| | |
|---|---|
| Stellen Sie sicher, dass genügend Speicherplatz für die Sicherung und Wiederherstellung der Datenbank vorhanden ist. Die Backup- und Restore-Prozesse benötigen etwa das Fünffache des Speicherplatzes, der von der Backup-Datei auf den Insight- und Data Warehouse-Servern belegt wird. Ein 50-GB-Backup benötigt beispielsweise 250 bis 300 GB freien Festplattenspeicher. | |
| Stellen Sie sicher, dass Sie Zugriff auf Firefox® oder den Chrome™ Browser haben, wenn Sie die Insight- und Data Warehouse-Datenbanken sichern. Internet Explorer wird nicht empfohlen, da beim Hochladen und Herunterladen von Dateien größer als 4 GB Probleme auftreten. | |
| Löschen Sie die `.tmp` Dateien auf dem Insight-Server, die Sie an folgendem Speicherort finden: `<install directory>\SANscreen\wildfly\standalone\tmp`. | |
| Doppelte Datenquellen und stillgelegte Datenquellen werden vom Insight Client entfernt. Das Entfernen stillgelegten oder doppelter Datenquellen verringert die für die Durchführung des Upgrades benötigte Zeit und verringert die Möglichkeit einer Datenbeschädigung. | |
| Wenn Sie einen der mit Insight ausgelieferten Standardberichte geändert haben, sollten Sie die Berichte unter einem anderen Namen speichern und anschließend im Ordner „Kundenberichte“ speichern, damit Sie Ihren geänderten Bericht nicht verlieren, wenn Sie das System aktualisieren oder wiederherstellen. | |
| Wenn Sie benutzerdefinierte oder geänderte Data Warehouse-Berichte von Ihnen oder Professional Services erstellt haben, erstellen Sie ein Backup dieser Berichte, indem Sie sie in XML exportieren und dann in den Ordner Kundenberichte verschieben. Stellen Sie sicher, dass sich das Backup nicht auf dem Data Warehouse-Server befindet. Wenn Sie Ihre Berichte nicht in die empfohlenen Ordner verschieben, werden diese Berichte möglicherweise nicht durch den Upgrade-Prozess gesichert. Bei früheren Versionen von Insight kann das Suchen von Berichten in den entsprechenden Ordnern zum Verlust benutzerdefinierter und geänderter Berichte führen. | |

| | |
|---|---|
| Notieren Sie alle Einstellungen im IBM Cognos-Konfigurationsdienstprogramm, da diese nicht im Data Warehouse-Backup enthalten sind. Sie müssen diese Einstellungen nach dem Upgrade neu konfigurieren. Das Dienstprogramm befindet sich im `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Verzeichnis auf dem Data Warehouse-Server, und Sie führen es mit aus `cogconfigw` Command.Alternativ können Sie eine vollständige Sicherung von Cognos durchführen und anschließend alle Einstellungen importieren. Weitere Informationen finden Sie in der Dokumentation zu IBM Cognos. | |

**Checkliste zur Vorbereitung des Upgrades (falls zutreffend)**

| Zustand | Abgeschlossen? |
|---|---|
| Wenn Sie die selbstsignierten Zertifikate, die die Insight-Installation aufgrund von Sicherheitswarnungen im Browser erstellt hat, durch von Ihrer internen Zertifizierungsstelle signierte Zertifikate ersetzt haben, sichern Sie die Keystore-Datei an folgendem Speicherort: `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` Und stellen Sie sie nach dem Upgrade wieder her. Dadurch werden die selbstsignierten Zertifikate ersetzt, die Insight mit Ihren signierten Zertifikaten erstellt. | |
| Wenn eine Ihrer Datenquellen für Ihre Umgebung geändert wurde und Sie sich nicht sicher sind, ob diese Änderungen in der Insight-Version verfügbar sind, auf die Sie aktualisieren, erstellen Sie eine Kopie des folgenden Verzeichnisses, das Ihnen bei Problemen mit der Wiederherstellung hilft: `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`. | |
| Sichern Sie alle benutzerdefinierten Datenbanktabellen und -Ansichten mithilfe des `mysqldump` Befehlszeilen-Tool.das Wiederherstellen benutzerdefinierter Datenbanktabellen erfordert privilegierten Zugriff auf die Datenbank. Wenden Sie sich an den technischen Support, um Hilfe beim Wiederherstellen dieser Tabellen zu erhalten. | |

| | |
|---|---|
| In ist sichergestellt, dass keine benutzerdefinierten Integrationsskripte, Komponenten von Drittanbietern, die für Insight-Datenquellen, Backups oder andere erforderliche Daten erforderlich sind `disk drive:\install directory\sanscreen` Verzeichnis, da der Inhalt dieses Verzeichnisses durch den Upgrade-Prozess gelöscht wird.Stellen Sie sicher, dass Sie diese Dinge aus dem verschieben `\sanscreen` An einen anderen Speicherort. Wenn Ihre Umgebung beispielsweise benutzerdefinierte Integrationsskripte enthält, stellen Sie sicher, dass Sie die folgende Datei in ein anderes Verzeichnis als das kopieren `\sanscreen` Verzeichnis:<br><br>`\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`. | |

## Herunterladen der OnCommand Insight-Installationspakete

Sie sollten die Installationspakete für Insight, Data Warehouse und die Remote Acquisition Unit (falls zutreffend) vor dem Tag herunterladen, an dem Sie das Upgrade durchführen möchten. Download-Zeiten für die Pakete (`.msi` Dateien) variieren je nach verfügbarer Bandbreite.

### Über diese Aufgabe

Sie können die Installationspakete über die WebUI von Insight oder über den entsprechenden Link zu OnCommand Insight von herunterladen http://support.netapp.com/NOW/cgi-bin/software.

Gehen Sie wie folgt vor, um das Installationspaket vom Insight-Server herunterzuladen:

### Schritte

1. Öffnen Sie die Web-UI von Insight, indem Sie einen Webbrowser öffnen und einen der folgenden eingeben:
   - Auf dem Insight-Server: `https://localhost`
   - Von jedem Ort: `https://IP Address:port or fqdn:port`

     Die Portnummer lautet entweder 443 oder der Port, der bei der Installation des Insight-Servers konfiguriert wurde. Die Portnummer ist standardmäßig 443, wenn Sie die Portnummer nicht in der URL angeben.
2. Melden Sie sich bei Insight an.
3. Klicken Sie auf das Hilfesymbol und wählen Sie **nach Updates suchen**.
4. Wenn eine neuere Version erkannt wird, befolgen Sie die Anweisungen im Meldungsfeld.

   Sie werden zur Seite InsightDescription für die neuere Version weitergeleitet.

5. Klicken Sie auf der Seite **Beschreibung** auf **Weiter**.
6. Wenn die Endbenutzer-Lizenzvereinbarung (EULA) angezeigt wird, klicken Sie auf **Accept**.
7. Klicken Sie für jede Komponente (Insight Server, Data Warehouse, Remote Acquisition Unit) auf den Link für das Installationspaket und klicken Sie auf **Speichern unter**, um das Installationspaket zu speichern.

   Bevor Sie ein Upgrade durchführen, sollten Sie sicherstellen, dass Sie die Installationspakete für Data Warehouse und Remote Acquisition Unit auf Festplatten kopieren, die auf ihren jeweiligen Servern lokal sind.

8. Klicken Sie auf **CHECKSUM**, und notieren Sie sich die numerischen Werte, die mit jedem Installationspaket verknüpft sind.
9. Überprüfen Sie, ob die Installationspakete vollständig und fehlerfrei sind, nachdem Sie sie heruntergeladen haben.

   Unvollständige Dateiübertragungen können Probleme mit dem Upgrade-Prozess verursachen.

   Um MD5-Hash-Werte für die Installationspakete zu generieren, können Sie ein Drittanbieter-Dienstprogramm wie Microsoft verwenden"Dateiüberprüfung der Integrität" Utility:

## Sichern der Datenbanken

Bevor Sie ein Upgrade durchführen, sollten Sie sowohl die Data Warehouse- als auch die OnCommand Insight-Datenbanken sichern. Für die Aktualisierung ist ein Backup der Data Warehouse-Datenbank erforderlich, damit Sie die Datenbank später im Upgrade wiederherstellen können. Mit dem in-Place-Upgrade für Insight wird die Datenbank gesichert. Vor dem Upgrade sollten Sie jedoch als Best Practice eine Sicherung der Datenbank durchführen.

> **Sie müssen den Tresor** sichern, bevor Sie OnCommand Insight aktualisieren.
>
> Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

Um falsche Berichte zu vermeiden, sollten Sie die Data Warehouse-Datenbank vor dem Backup der Insight-Datenbank sichern. Wenn Sie über eine Testumgebung verfügen, sollten Sie außerdem sicherstellen, dass Sie das Backup wiederherstellen können, bevor Sie mit dem Upgrade fortfahren.

### Sichern der Data Warehouse-Datenbank

Sie können die Data Warehouse-Datenbank, die auch ein Cognos-Backup enthält, in einer Datei sichern und später mithilfe des Data Warehouse-Portals wiederherstellen. Mit einem solchen Backup können Sie auf einen anderen Data Warehouse-Server migrieren oder auf eine neue Data Warehouse-Version aktualisieren.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Wählen Sie im Navigationsfenster links **Backup/Restore** aus.
3. Klicken Sie auf **Backup** und wählen Sie Ihre Backup-Konfiguration aus:

a. Alle Datamarts außer Performance Datamart
b. Alle Datamarts

   Dieser Vorgang kann 30 Minuten oder länger dauern.

+ Data Warehouse erstellt eine Sicherungsdatei und zeigt ihren Namen an.

4. Klicken Sie mit der rechten Maustaste auf die Sicherungsdatei, und speichern Sie sie an einem gewünschten Speicherort.

   Sie möchten den Dateinamen möglicherweise nicht ändern. Sie sollten die Datei jedoch außerhalb des Installationspfads des Data Warehouse speichern.

   Die Data Warehouse Backup-Datei enthält MySQL der DWH-Instanz; benutzerdefinierte Schemas (MySQL DBs) und Tabellen; LDAP-Konfiguration; die Datenquellen, die Cognos mit der MySQL-Datenbank verbinden (nicht die Datenquellen, die den Insight-Server mit Geräten verbinden, um Daten zu erfassen); Importieren und Exportieren von Aufgaben, die Berichte importiert oder exportiert haben; Reporting von Sicherheitsrollen, Gruppen und Namespaces; Benutzerkonten; Alle geänderten Reporting Portal-Berichte sowie alle benutzerdefinierten Berichte, unabhängig davon, wo sie gespeichert sind, selbst im Verzeichnis „Meine Ordner“. Cognos-Systemkonfigurationsparameter wie SMTP-Servereinstellungen und Cognos-Einstellungen für benutzerdefinierten Speicher werden nicht gesichert.

   Die Standardschemas, in denen benutzerdefinierte Tabellen gesichert werden, umfassen Folgendes:

| |
|---|
| dwh_Capacity |
| dwh_Capacity_Staging |
| dwh_Bemaßungen |
| dwh_fs_util |
| dwh_Inventory |
| dwh_Inventory_Staging |
| dwh_Inventory_transient |
| dwh_Management |
| dwh_Performance |
| dwh_Performance_Staging |
| dwh_Ports |
| dwh_Reports |

| |
|---|
| dwh_sa_Staging |

Schemas, bei denen benutzerdefinierte Tabellen vom Backup ausgeschlossen werden, umfassen Folgendes:

| |
|---|
| Information_Schema |
| Akquisition |
| Cloud_Modell |
| Host_Data |
| innodb |
| Inventar |
| Inventory_private |
| Inventory_Time |
| Protokolle |
| Vereinfachtes |
| mysql |
| nas |
| Performance |
| Performance_Schema |
| Performance_Views |
| SANscreen |
| Schrubben |
| Servicesicherheit |
| Test |

| |
|---|
| Tmp |
| workbench |
| |
| |
| |

Bei manuell initiierten Backups wird ein angezeigt `.zip` Datei wird erstellt, die folgende Dateien enthält:

- Ein tägliches Backup `.zip` Datei, die Cognos-Berichtsdefinitionen enthält
- Ein meldet Backup `.zip` Datei, die alle Berichte in Cognos enthält, einschließlich der Berichte im Verzeichnis eigene Ordner
- Eine Data Warehouse-Datenbank-Sicherungsdatei Zusätzlich zu manuellen Backups, die Sie jederzeit durchführen können, erstellt Cognos täglich ein Backup (automatisch jeden Tag in einer Datei mit dem Namen generiert) `DailyBackup.zip`), das die Berichtsdefinitionen enthält. Die tägliche Sicherung umfasst die wichtigsten Ordner und Pakete, die mit dem Produkt geliefert werden. Das Verzeichnis „Meine Ordner“ und alle Verzeichnisse, die Sie außerhalb der obersten Produktordner erstellen, sind nicht im Cognos-Backup enthalten.

> Aufgrund der Art und Weise, wie Insight die Dateien in benennt `.zip` Datei, zeigen einige Entpackprogramme, dass die Datei leer ist, wenn sie geöffnet wird. So lange wie die `.zip` Die Datei hat eine Größe größer als 0 und endet nicht mit einem `.bad` Erweiterung, die `.zip` Datei ist gültig. Sie können die Datei mit einem anderen Entpackprogramm wie 7-Zip oder WinZip® öffnen.

#### Sichern der OnCommand Insight-Datenbank

Sichern Sie die Insight-Datenbank, um sicherzustellen, dass Sie ein Backup vor kurzem haben, falls nach dem Upgrade ein Problem auftritt. Während der Backup- und Wiederherstellungsphase werden keine Performance-Daten erfasst, daher sollte das Backup so nah wie möglich an der Upgrade-Zeit erfolgen.

##### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Klicken Sie Auf **Admin** > **Fehlerbehebung**.
3. Klicken Sie auf der Seite **Fehlerbehebung** auf **Backup**.

   Die Dauer für die Sicherung der Datenbank kann je nach verfügbaren Ressourcen (Architektur, CPU und Arbeitsspeicher), der Größe der Datenbank und der Anzahl der in Ihrer Umgebung überwachten Objekte variieren.

   Wenn die Sicherung abgeschlossen ist, werden Sie gefragt, ob Sie die Datei herunterladen möchten.

4. Laden Sie die Sicherungsdatei herunter.

## Sichern der Sicherheitskonfiguration

Wenn Ihre Insight-Komponenten eine nicht standardmäßige Sicherheitskonfiguration verwenden, müssen Sie die Sicherheitskonfiguration sichern und die Konfiguration

anschließend auf allen Komponenten wiederherstellen, nachdem die neue Software installiert wurde. Die Sicherheitskonfiguration muss wiederhergestellt werden, bevor das Data Warehouse-Datenbankbackup wiederhergestellt wird.

#### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zum Erstellen einer Sicherungskopie der Konfiguration und zum Wiederherstellen der gespeicherten Konfiguration. Weitere Informationen erhalten Sie, wenn Sie nach suchen `securityadmin` Im OnCommand Insight Dokumentationszentrum: http://docs.netapp.com/oci-73/index.jsp

## Erstellen von benutzerdefinierten Data Warehouse-Berichten

Wenn Sie benutzerdefinierte Berichte erstellt haben und nicht über den verfügen `.xml` Quelldateien für sie, dann sollten Sie diese Berichte vor dem Upgrade sichern. Sie sollten sie dann auf einen anderen Server als den Data Warehouse-Server kopieren.

#### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://fqdn/dwh`.
2. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Reporting Portal zu öffnen und sich anzumelden.
3. Wählen Sie **Datei** > **Öffnen**.
4. Wählen Sie den Ordner aus, in dem sich der Bericht befindet, wählen Sie den Bericht aus, und klicken Sie dann auf **Öffnen**.
5. Wählen Sie **Extras** > **Bericht in Zwischenablage kopieren**.
6. Öffnen Sie einen Texteditor, fügen Sie den Inhalt des Berichts ein, und speichern Sie die Datei unter `report_name.txt`, Wo `report _name` Ist der Name des Berichts.
7. Speichern Sie die Berichte auf einem anderen Server als dem Data Warehouse-Server.

## Durchführen des Software-Upgrades

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie alle Insight-Komponenten auf eine neue Version aktualisieren, indem Sie das entsprechende Installationspaket auf jedem Server herunterladen und ausführen.

#### Aktualisieren Von Insight

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, melden Sie sich beim Insight Server an und führen das Installationspaket aus, um das Upgrade abzuschließen. Beim Upgrade wird die vorhandene Software deinstalliert, die neue Software installiert und der Server anschließend neu gestartet.

#### Bevor Sie beginnen

Das Insight-Installationspaket muss sich auf dem Server befinden.

**Sie müssen den Tresor** sichern, bevor Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

#### Schritte

1. Melden Sie sich beim Insight-Server mit einem Konto an, das über lokale Windows-Administratorberechtigungen verfügt.
2. Suchen Sie das Insight Installationspaket (`SANscreenServer-x64-version_number-build_number.msi`) Verwenden Sie Windows Explorer und doppelklicken Sie darauf.

   Der OnCommand InsightSetup-Assistent wird angezeigt.
3. Bewegen Sie das Fortschrittsfenster von der Mitte des Bildschirms weg und weg vom **Setup**-Wizard -Fenster, so dass alle generierten Fehler nicht aus der Ansicht ausgeblendet werden.
4. Befolgen Sie die Anweisungen des Setup-Assistenten.

   Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

#### Nachdem Sie fertig sind

Um zu überprüfen, ob das Upgrade erfolgreich war oder Fehler generiert wurden, überprüfen Sie das Upgrade-Protokoll am folgenden Speicherort: `<install directory>\SANscreen\wildfly\standalone\log`.

### Data Warehouse Wird Aktualisiert

## Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie sich beim Data Warehouse-Server anmelden und das Installationspaket ausführen, um das Upgrade abzuschließen.

#### Über diese Aufgabe

Inline-Upgrade wird vom Data Warehouse (DWH) nicht unterstützt. Führen Sie die folgenden Schritte aus, um auf die neue Version der DWH-Software zu aktualisieren.

**Sie müssen den Tresor** sichern, bevor Sie das DWH-Upgrade durchführen.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

#### Schritte

Beim Aktualisieren des Data Warehouse müssen Sie die folgenden Aktionen ausführen:

1. Stellen Sie nach der Installation von DWH 7.3.16 den Tresor und die Datenbank in der folgenden Reihenfolge wieder her:
   a. Vault
   b. Datenbank
2. Melden Sie sich beim DWH-Server mit einem Konto an, das über lokale Windows-Administratorberechtigungen verfügt.

3. Sichern Sie die DWH-DB und Berichte über die DWH-Portalschnittstelle.
4. Sichern Sie den Vault. Siehe "Sicherheitsadministration"Dokumentation.
5. Deinstallieren Sie die DWH-Software vom Server.
6. Starten Sie den Server neu, um Komponenten aus dem Speicher zu entfernen.
7. Installieren Sie die neue Version von DWH auf dem Server.

   Die Installation dauert etwa 2 Stunden. Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

8. Stellen Sie den Tresor auf dem DWH-Server wieder her.
9. Stellen Sie die DWH-Datenbank auf dem Server wieder her.

#### Nachdem Sie fertig sind

Nach dem Upgrade müssen Sie die Data Warehouse-Datenbank wiederherstellen, die so lange oder länger dauern kann wie das Upgrade.

> Während eines OnCommand Insight-Upgrades ist es nicht ungewöhnlich, dass ein Kunde zu einem anderen Insight-Server wechselt. Wenn Sie Ihren Insight-Server geändert haben, zeigen die vorhandenen Konnektoren nach der Wiederherstellung der Data Warehouse-Datenbank auf die vorherige Server-IP-Adresse oder den Hostnamen. Es empfiehlt sich, den Konnektor zu löschen und einen neuen zu erstellen, um mögliche Fehler zu vermeiden.

#### Beibehalten von benutzerdefinierten Cognos-Einstellungen während einer Data Warehouse-Aktualisierung

Benutzerdefinierte Cognos-Einstellungen, z. B. nicht standardmäßige SMTP-E-Mail-Einstellungen, werden nicht automatisch als Teil eines Data Warehouse-Upgrades gesichert. Sie müssen die benutzerdefinierten Einstellungen nach einem Upgrade manuell dokumentieren und wiederherstellen.

Bevor Sie das Data Warehouse aktualisieren, erstellen Sie eine Checkliste mit allen benutzerdefinierten Cognos-Einstellungen, die Sie beibehalten möchten, und überprüfen Sie die Liste vor dem Upgrade des Systems. Nach Abschluss der Aktualisierung können Sie die Werte manuell wiederherstellen, um sie auf die Einstellungen in der ursprünglichen Konfiguration zurückzusetzen.

### Aktualisierung der Server der Remote-Akquisitionseinheit

Nachdem Sie alle erforderlichen Aufgaben abgeschlossen haben, können Sie sich beim Server der Remote-Erfassungseinheit anmelden und das Installationspaket ausführen, um das Upgrade abzuschließen. Sie müssen diese Aufgabe auf allen Remote-Akquisitionsservern in Ihrer Umgebung ausführen.

#### Bevor Sie beginnen

- Sie müssen ein Upgrade von OnCommand Insight durchgeführt haben.
- Das OnCommand Insight-Installationspaket muss sich auf dem Server befinden.

Sie müssen den Vault vor dem Upgrade sichern.

Weitere Informationen zum Tresor finden "Sicherheitstool"Sie in den Anweisungen.

**Schritte**

1. Melden Sie sich beim Server der Remote-Erfassungseinheit mit einem Konto an, das über lokale Windows-Administratorberechtigungen verfügt.
2. Sichern Sie den Vault.
3. Suchen Sie das Insight Installationspaket (`RAU-x64-version_number-build_number.msi`) Verwenden Sie Windows Explorer und doppelklicken Sie darauf.

   Der OnCommand Insight-Einrichtungsassistent wird angezeigt.
4. Verschieben Sie das Fenster mit dem Installationsassistenten vom Zentrum des Bildschirms weg und entfernen Sie es aus dem Fenster mit dem Installationsassistenten, sodass generierte Fehler nicht aus der Ansicht ausgeblendet werden.
5. Befolgen Sie die Anweisungen des Setup-Assistenten.

   Es empfiehlt sich, alle Standardeinstellungen ausgewählt zu lassen.

**Nachdem Sie fertig sind**

- Um zu überprüfen, ob das Upgrade erfolgreich war oder Fehler generiert wurden, überprüfen Sie das Upgrade-Protokoll am folgenden Speicherort: `<install directory>\SANscreen\bin\log`.
- Verwenden Sie die `securityadmin` Tool zum Wiederherstellen der gespeicherten Sicherheit

  Konfiguration. Weitere Informationen finden Sie im OnCommand Insight nach securityadmin

  Dokumentationscenter: http://docs.netapp.com/oci-73/index.jsp
- Löschen Sie den Cache und den Verlauf Ihres Browsers, um sicherzustellen, dass Sie die neuesten Daten vom Server empfangen.

## Aufgaben nach dem Upgrade werden ausgeführt

Nachdem Sie ein Upgrade auf die neueste Version von Insight durchgeführt haben, müssen Sie weitere Aufgaben ausführen.

### Installieren von Patches für Datenquellen

Falls zutreffend, sollten Sie die neuesten Patches installieren, die für Ihre Datenquellen verfügbar sind, um die neuesten Funktionen und Verbesserungen nutzen zu können. Nach dem Hochladen eines Datenquellpatches können Sie ihn auf allen Datenquellen desselben Typs installieren.

**Bevor Sie beginnen**

Sie müssen sich an den technischen Support wenden und den erhalten haben `.zip` Datei, die die neuesten Datenquellpatches enthält, indem sie ihnen die Version bereitstellt, von der Sie ein Upgrade durchführen

möchten, und die Version, auf die Sie aktualisieren möchten.

#### Schritte

1. Platzieren Sie die Patch-Datei auf dem Insight-Server.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Patches**.
4. Wählen Sie über die Schaltfläche Aktionen die Option **Patch anwenden** aus.
5. Klicken Sie im Dialogfeld **Data source Patch anwenden** auf **Browse**, um die hochgeladene Patch-Datei zu finden.
6. Überprüfen Sie die Typen **Patch-Name**, **Beschreibung** und **betroffene Datenquellen**.
7. Wenn der ausgewählte Patch korrekt ist, klicken Sie auf **Patch anwenden**.

   Alle Datenquellen des gleichen Typs werden mit diesem Patch aktualisiert. Insight zwingt den Neustart der Erfassung automatisch, sobald eine Datenquelle hinzugefügt wird. Die Erkennung umfasst die Erkennung von Änderungen in der Netzwerktopologie, einschließlich des Hinzufügens oder Löschens von Knoten oder Schnittstellen.

8. Um den Ermittlungsvorgang manuell zu erzwingen, klicken Sie auf **Datenquellen** und klicken Sie neben der Datenquelle auf **erneut abrufen**, um die Datenerhebung sofort zu erzwingen.

   Wenn sich die Datenquelle bereits in einem Erfassungsprozess befindet, ignoriert Insight die Abfrage erneut.

### Ersetzen eines Zertifikats nach dem Upgrade von OnCommand Insight

Das Öffnen der OnCommand Insight-Web-Benutzeroberfläche nach einem Upgrade führt zu einer Zertifizierungswarnung. Die Warnmeldung wird angezeigt, weil nach dem Upgrade kein gültiges selbstsigniertes Zertifikat verfügbar ist. Um zu verhindern, dass die Warnmeldung in Zukunft angezeigt wird, können Sie ein gültiges selbstsigniertes Zertifikat installieren, um das ursprüngliche Zertifikat zu ersetzen.

#### Bevor Sie beginnen

Ihr System muss die minimale Verschlüsselungsbit-Ebene (1024 Bit) erfüllen.

#### Über diese Aufgabe

Die Zertifizierungswarnung hat keinen Einfluss auf die Benutzerfreundlichkeit des Systems. An der Eingabeaufforderung können Sie angeben, dass Sie das Risiko verstanden haben, und dann mit Insight fortfahren.

#### Schritte

1. Listen Sie den Inhalt des Keystore auf: `C:\Program Files\SANscreen\java64\bin>keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Weitere Informationen zum Einstellen oder Ändern des Kennworts für den Keystore finden "Sicherheitsadministration"Sie in der Dokumentation.

Es sollte mindestens ein Zertifikat im Schlüsselspeicher vorhanden sein, `ssl certificate`.

2. Löschen Sie die `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Einen neuen Schlüssel generieren: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Wenn Sie nach vor- und Nachnamen gefragt werden, geben Sie den vollständig qualifizierten Domänennamen (FQDN) ein, den Sie verwenden möchten.
   b. Geben Sie die folgenden Informationen zu Ihrer Organisation und Organisationsstruktur an:
      - Land: Zweistellige ISO-Abkürzung für Ihr Land (z. B. USA)
      - Bundesland oder Provinz: Name des Bundesstaates oder der Provinz, in dem sich der Hauptsitz Ihres Unternehmens befindet (z. B. Massachusetts)
      - Ort: Name der Stadt, in der sich der Hauptsitz Ihrer Organisation befindet (z. B. Waltham)
      - Name des Unternehmens: Name des Unternehmens, dem der Domain-Name gehört (z. B. NetApp)
      - Name der Organisationseinheit: Name der Abteilung oder Gruppe, die das Zertifikat verwenden soll (z. B. Support)
      - Domänenname/ Allgemeiner Name: Der FQDN, der für DNS-Suchen Ihres Servers verwendet wird (z. B. www.example.com). Das System antwortet mit Informationen wie den folgenden: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Eingabe `Yes` Wenn der allgemeine Name (CN) gleich dem FQDN ist.
   d. Wenn Sie zur Eingabe des Schlüsselpassworts aufgefordert werden, geben Sie das Kennwort ein, oder drücken Sie die Eingabetaste, um das vorhandene Schlüsselspeicher-Passwort zu verwenden.
4. Erstellen Sie eine Zertifikatanforderungsdatei: `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   Der `c:\localhost.csr` Die Datei ist die neu generierte Zertifikatanforderungsdatei.
5. Senden Sie die `c:\localhost.csr` Bei der Zertifizierungsstelle zur Genehmigung einreichen.

   Nachdem die Zertifikatanforderungsdatei genehmigt wurde, möchten Sie das Zertifikat in zurücksenden `.der` Formatieren. Die Datei wird möglicherweise als zurückgegeben `.der` Datei: Das Standarddateiformat ist `.cer` Für Microsoft CA-Services.
6. Importieren Sie das genehmigte Zertifikat: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Passwort für den Keystore ein.

      Vom System wird die folgende Meldung angezeigt: `Certificate reply was installed in keystore`
7. Starten Sie den SANscreen-Serverdienst neu.

#### Ergebnisse

Der Webbrowser meldet keine Zertifikatwarnungen mehr.

### Cognos-Speicher wird erhöht

Bevor Sie die Data Warehouse-Datenbank wiederherstellen, sollten Sie die Java-Zuweisung für Cognos von 768 MB auf 2048 MB erhöhen, um die Zeit für die Berichterstellung zu verkürzen.

#### Schritte

1. Öffnen Sie ein Eingabeaufforderungsfenster als Administrator auf dem Data Warehouse-Server.
2. Navigieren Sie zum `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Verzeichnis.
3. Geben Sie den folgenden Befehl ein: `cogconfigw`

   Das Fenster IBM Cognos Configuration wird angezeigt.

   > Die Verknüpfung IBM Cognos Configuration verweist auf `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Wenn Insight im Verzeichnis Programme (Leerzeichen zwischen) installiert ist, das als Standard anstelle von ProgramFiles (kein Leerzeichen) dient, wird der installiert `.bat` Die Datei funktioniert nicht. Klicken Sie in diesem Fall mit der rechten Maustaste auf die Anwendungsverknüpfung, und ändern Sie sie `cognosconfigw.bat` Bis `cognosconfig.exe` Um die Verknüpfung zu korrigieren.

4. Erweitern Sie im linken Navigationsbereich **Environment**, erweitern Sie **IBM Cognos Services** und klicken Sie dann auf **IBM Cognos**.
5. Wählen Sie **Maximum Memory for Tomcat in MB** und ändern Sie 768 MB auf 2048 MB.
6. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf (Speichern).

   Es wird eine Informationsmeldung angezeigt, die Sie über die Aufgaben informiert, die Cognos ausführt.

7. Klicken Sie Auf **Schließen**.
8. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf (Stopp).
9. Klicken Sie in der Symbolleiste IBM Cognos Configuration auf (Start).

### Wiederherstellen der Data Warehouse-Datenbank

Wenn Sie die Data Warehouse-Datenbank sichern, erstellt Data Warehouse einen `.zip` Datei, die Sie später zur Wiederherstellung derselben Datenbank verwenden können.

#### Über diese Aufgabe

Wenn Sie die Data Warehouse-Datenbank wiederherstellen, können Sie auch Benutzerkontoinformationen aus dem Backup wiederherstellen. Benutzerverwaltungstabellen werden von der Data Warehouse-Berichtsengine in einer reinen Data Warehouse-Installation verwendet.

**Schritte**

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster links auf **Backup/Restore**.
3. Klicken Sie im Abschnitt **Datenbank und Berichte wiederherstellen** auf **Durchsuchen**, und suchen Sie den `.zip` Datei, die das Data Warehouse-Backup enthält.
4. Es ist eine Best Practice, beide der folgenden Optionen ausgewählt zu lassen:
   - **Datenbank wiederherstellen**

     Enthält Data Warehouse-Einstellungen, Data Marts, Verbindungen und Benutzerkontoinformationen.
   - **Berichte wiederherstellen**

     Umfasst benutzerdefinierte Berichte, vordefinierte Berichte, Änderungen an vordefinierten Berichten, die Sie vorgenommen haben, und Berichtseinstellungen, die Sie in der Berichtsverbindung vorgenommen haben.
5. Klicken Sie Auf **Wiederherstellen**.

   Navigieren Sie nicht vom Wiederherstellungsstatus weg. Wenn Sie dies tun, wird der Wiederherstellungsstatus nicht mehr angezeigt und Sie erhalten keine Anzeige mehr, wenn der Wiederherstellungsvorgang abgeschlossen ist.
6. Um den Upgrade-Prozess zu überprüfen, lesen Sie die `dwh_upgrade.log` Datei, die sich am folgenden Speicherort befindet: `<install directory>\SANscreen\wildfly\standalone\log`.

   Nachdem der Wiederherstellungsvorgang abgeschlossen ist, erscheint eine Meldung direkt unter der Schaltfläche **Wiederherstellen**. Wenn die Wiederherstellung erfolgreich war, wird die Meldung erfolgreich angezeigt. Wenn der Wiederherstellungsvorgang fehlschlägt, zeigt die Meldung die spezifische Ausnahme an, die aufgetreten ist, um den Fehler zu verursachen. Wenden Sie sich in diesem Fall an den technischen Support und stellen Sie diese bereit `dwh_upgrade.log` Datei: Wenn eine Ausnahme auftritt und der Wiederherstellungsvorgang fehlschlägt, wird die ursprüngliche Datenbank automatisch zurückgesetzt.

   Wenn der Wiederherstellungsvorgang mit der Meldung „`Failed upgrading cognos content Store`“ fehlschlägt, stellen Sie die Data Warehouse-Datenbank ohne ihre Berichte wieder her (nur Datenbank) und verwenden Sie Ihre XML-Berichtsbackups zum Importieren Ihrer Berichte.

### Benutzerdefinierte Data Warehouse-Berichte werden wiederhergestellt

Falls zutreffend, können Sie alle benutzerdefinierten Berichte, die Sie vor dem Upgrade gesichert haben, manuell wiederherstellen. Sie müssen dies jedoch nur tun, wenn Sie Berichte verlieren, wenn diese beschädigt wurden.

**Schritte**

1. Öffnen Sie Ihren Bericht mit einem Texteditor, und wählen Sie den Inhalt aus, und kopieren Sie ihn.
2. Melden Sie sich beim Reporting-Portal unter an `https://fqdn/reporting`.
3. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Insight Reporting-Portal zu öffnen.

4. Wählen Sie im Menü Start die Option **Report Studio**.
5. Wählen Sie ein beliebiges Paket aus.

   Report Studio wird angezeigt.

6. Klicken Sie auf **Create New**.
7. Wählen Sie **Liste**.
8. Wählen Sie im Menü Extras die Option **Bericht aus Zwischenablage öffnen**.

   Das Dialogfeld **Bericht aus Zwischenablage öffnen** wird angezeigt.

9. Wählen Sie im Menü Datei die Option **Speichern unter** und speichern Sie den Bericht im Ordner Benutzerdefinierte Berichte.
10. Öffnen Sie den Bericht, um zu überprüfen, ob er importiert wurde.

    Wiederholen Sie diese Aufgabe für jeden Bericht.

> Beim Laden eines Berichts wird möglicherweise ein „`Expression Parsing error`“ angezeigt. Das bedeutet, dass die Abfrage einen Verweis auf mindestens ein Objekt enthält, das nicht vorhanden ist, was bedeutet, dass im Fenster Quelle kein Paket ausgewählt ist, um den Bericht zu validieren. Klicken Sie in diesem Fall mit der rechten Maustaste auf eine Data-Mart-Dimension im Fenster Quelle, und wählen Sie Berichtspaket, Wählen Sie dann das dem Bericht zugeordnete Paket aus (z. B. das Bestandspaket, wenn es sich um einen Bestandsbericht handelt, oder eines der Leistungspakete, wenn es sich um einen Leistungsbericht handelt), damit Report Studio es validieren und speichern kann.

#### Überprüfung, ob das Data Warehouse historische Daten enthält

Nachdem Sie Ihre benutzerdefinierten Berichte wiederhergestellt haben, sollten Sie überprüfen, ob Data Warehouse historische Daten sammelt, indem Sie Ihre benutzerdefinierten Berichte anzeigen.

##### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://fqdn/dwh`.
2. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Insight Reporting-Portal zu öffnen und sich anzumelden.
3. Öffnen Sie den Ordner, der Ihre benutzerdefinierten Berichte enthält (z. B. Benutzerdefinierte Berichte).
4. Klicken Sie Auf Um die Ausgabeformatoptionen für diesen Bericht zu öffnen.
5. Wählen Sie die gewünschten Optionen aus und klicken Sie auf **Ausführen**, um sicherzustellen, dass sie mit Speicher-, Rechen- und Switch-historischen Daten gefüllt sind.

#### Wiederherstellung des Performance-Archivs

Bei Systemen, die eine Performance-Archivierung durchführen, werden im Upgrade-Prozess nur Archivdaten von sieben Tagen wiederhergestellt. Sie können die verbleibenden Archivdaten wiederherstellen, nachdem das Upgrade konkurriert wurde.

#### Über diese Aufgabe

Führen Sie die folgenden Schritte aus, um das Performance-Archiv wiederherzustellen.

#### Schritte

1. Klicken Sie in der Symbolleiste auf **Admin** > **Fehlerbehebung**
2. Klicken Sie im Abschnitt Wiederherstellen unter **Load Performance Archive** auf **Load**.

   Das Laden des Archivs erfolgt im Hintergrund. Das vollständige Archiv kann sehr lange geladen werden, da die archivierten Performance-Daten der einzelnen Tage in Insight eingetragen sind. Der Status des Archivladens wird im Archiv-Bereich dieser Seite angezeigt.

### Prüfen der Anschlüsse

Nach dem Upgrade möchten Sie die Konnektoren testen, um sicherzustellen, dass eine Verbindung zwischen dem OnCommand Insight Data Warehouse und dem OnCommand Insight-Server besteht.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.
3. Wählen Sie den ersten Anschluss aus.

   Die Seite Connector bearbeiten wird angezeigt.

4. Klicken Sie Auf **Test**.
5. Wenn der Test erfolgreich ist, klicken Sie auf **Schließen**; wenn er fehlschlägt, geben Sie den Namen des Insight-Servers in das Feld **Name** und seine IP-Adresse in das Feld **Host** ein und klicken Sie auf **Test**.
6. Wenn eine erfolgreiche Verbindung zwischen dem Data Warehouse und dem Insight-Server besteht, klicken Sie auf **Speichern**.

   Wenn dies nicht gelingt, überprüfen Sie die Verbindungskonfiguration und stellen Sie sicher, dass der Insight-Server keine Probleme hat.

7. Klicken Sie Auf **Test**.

   Data Warehouse testet die Verbindung.

### Überprüfen der Planung für Extrahieren, Transformieren und Laden

Nach dem Upgrade sollten Sie sicherstellen, dass der ETL-Prozess (Extrahieren, Transformieren und Laden) Daten aus den OnCommand Insight-Datenbanken abruft, die Daten transformiert und in den Data Marts speichert.

#### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://fqdn/dwh`.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan**.

3. Klicken Sie auf **Zeitplan bearbeiten**.
4. Wählen Sie **Täglich** oder **wöchentlich** aus der Liste **Typ** aus.

   Es wird empfohlen, die Ausführung von ETL einmal pro Tag zu planen.

5. Vergewissern Sie sich, dass die ausgewählte Zeit die Zeit ist, zu der der Job ausgeführt werden soll.

   Dadurch wird sichergestellt, dass der Build-Job automatisch ausgeführt wird.

6. Klicken Sie Auf **Speichern**.

#### Festplattenmodelle werden aktualisiert

Nach der Aktualisierung sollten Sie über aktualisierte Festplattenmodelle verfügen. Wenn Insight jedoch aus irgendeinem Grund neue Laufwerksmodelle nicht erkennen konnte, können Sie sie manuell aktualisieren.

##### Bevor Sie beginnen

Sie müssen den technischen Support von erhalten haben `.zip` Datei, die die neuesten Patches für die Datenquelle enthält.

##### Schritte

1. Stoppen Sie den SANscreen Acq-Dienst.
2. Navigieren Sie zum folgenden Verzeichnis: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Verschieben Sie den aktuellen `diskmodels.jar` An einem anderen Speicherort ablegen.
4. Kopieren Sie das neue `diskmodels.jar` In die Datei `datasources.war` Verzeichnis.
5. Starten Sie den SANscreen Acq-Dienst.

#### Überprüfung der Ausführung von Business Intelligence-Tools

Falls zutreffend, sollten Sie überprüfen, ob Ihre Business Intelligence-Tools ausgeführt werden und Daten nach dem Upgrade abrufen.

Stellen Sie sicher, dass Business Intelligence-Tools wie BMC Atrium und ServiceNow ausgeführt werden und Daten abrufen können. Dazu gehören der BMC-Anschluss und Lösungen, die REST nutzen.

## Fehlerbehebung bei einem Upgrade

Wenn nach einem OnCommand Insight-Upgrade Probleme auftreten, können Sie die Fehlerbehebungsinformationen zu einigen möglichen Problemen prüfen.

#### Cognos kann nicht über das Windows-Startmenü gestartet werden

Die Existenz eines Raumes vor `\SANscreen\cognos` Im Pfadnamen liegt ein Problem vor. Weitere Informationen finden Sie in der NetApp Customer Success Community unter: https://forums.netapp.com/thread/62721.

#### Fehlermeldung „Keine gültige win32-Anwendung“

Dies ist ein Problem mit Microsoft Windows. Um dieses Problem zu beheben, müssen Sie Anführungszeichen um den Bildpfad in der Registrierung setzen. Weitere Informationen finden Sie in der folgenden Dokumentation: https://support.microsoft.com/en-us/kb/812486/en-us.

#### Anmerkungen sind nicht vorhanden

Wenn ein Data Warehouse-ETL-Job Anmerkungen von einer Insight-Instanz abfragt, erhält er manchmal eine leere Antwort (ein 0-Ergebnis) als Fehler. Dieser Fehler führt zu Anmerkungen für bestimmte Objekte, die zwischen dem Status „Present“ und „Not Present“ im Data Warehouse hin und her verschoben werden. Weitere Informationen finden Sie im Folgenden: https://forums.netapp.com/docs/DOC-44167

#### Unterschiede bei den in Berichten angezeigten Werten

Vor 7.0 waren Berichte ganzzahlig. Sie sind jetzt dezimal-basiert; daher können Sie nach dem Upgrade feststellen, dass die Anzeige der Werte erhöht oder verringert wird.

#### Daten werden nicht in Berichten angezeigt

In 7.0 wurden mehrere Modellnamen geändert (z. B. wurde Symmetrix in Symmetrix VMAX geändert). Wenn ein Bericht daher einen Filter für „Symmetrix“ enthält, werden beim Ausführen des Berichts keine Daten angezeigt. Um den Bericht zu ändern, müssen Sie den Bericht mit dem Abfrage-Explorer in Report Studio öffnen, nach dem Modellnamen suchen, ihn durch den neuen Modellnamen ersetzen und den Bericht speichern.

# Deinstallieren der Software

Sie müssen die alten Versionen von Data Warehouse und Remote Acquisition deinstallieren, um die neuen Versionen zu installieren. Sie sollten dies tun, bevor Sie versuchen, eine dieser Komponenten zu aktualisieren. Die Software auf dem Insight-Server wird während des in-Place-Upgrades deinstalliert.

**Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern. **Sie müssen den Tresor** sichern, wenn Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

## Deinstallieren des OnCommand Insight-Servers

Sie können den OnCommand Insight-Server bei Bedarf deinstallieren.

**Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

#### Bevor Sie beginnen

Best Practice: Sichern Sie vor der Deinstallation von Insight die OnCommand Insight-Datenbank.

**Schritte**

1. Melden Sie sich beim OnCommand Insight-Server mit einem Konto mit Administratorrechten an.
2. Stellen Sie sicher, dass alle Insight-Fenster auf dem Server geschlossen sind.
3. Öffnen Sie die Funktion **Programm deinstallieren** auf dem Bedienfeld und wählen Sie die OnCommand Insight-Anwendung zum Entfernen aus.
4. Klicken Sie auf **Deinstallieren** und folgen Sie den Anweisungen.

## Deinstallieren der Data Warehouse-Software

Sie müssen die Data Warehouse-Software deinstallieren, bevor Sie ein Upgrade durchführen können.

**Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern. **Sie müssen den Tresor** sichern, wenn Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

**Bevor Sie beginnen**

Wenn Sie Änderungen an Berichten vorgenommen haben, die Sie behalten möchten, ist es wichtig, dass Sie vor der Deinstallation von Data Warehouse ein Backup erstellen. Durch die Deinstallation von Data Warehouse werden alle zuvor erfassten Daten endgültig gelöscht und alle Berichte, einschließlich neu erstellter oder bearbeiteter Berichte, entfernt.

**Schritte**

1. Melden Sie sich beim Data Warehouse-Server an.
2. Stellen Sie sicher, dass alle Insight-Fenster auf dem Server geschlossen sind.
3. So deinstallieren Sie die Software über die Systemsteuerung:
   a. Öffnen Sie **Programm deinstallieren** aus dem Bedienfeld und wählen Sie die OnCommand Insight-Anwendung zum Entfernen. Klicken Sie auf **Deinstallieren** und folgen Sie den Anweisungen.
   b. Wählen Sie die IBM DB2-Anwendung zum Entfernen aus. Klicken Sie auf **Deinstallieren** und folgen Sie den Anweisungen.
   c. Löschen Sie den DB2-Installationsordner (z. B. *C:\Program Files\IBM\DB2*), um die DB2-Datenbank vollständig zu entfernen.
4. So deinstallieren Sie das Programm mithilfe des angegebenen Skripts:
   a. Navigieren Sie zum Ordner *<download location>\oci_dwh_uninstall* und führen Sie das Skript *uninstall_oci_dwh.bat* aus.
5. Starten Sie den Server neu.

## Deinstallieren der Software der Remote-Erfassungseinheit

Sie müssen die vorhandene Version der Remote-Erfassungseinheit-Software deinstallieren, bevor Sie auf eine neue Version aktualisieren können. Sie sollten diese Aufgabe auf allen Remote-Erfassungseinheiten-Servern in Ihrer Umgebung durchführen.

**Es wird dringend empfohlen, den Tresor** vor der Deinstallation von OnCommand Insight zu sichern. **Sie müssen den Tresor** sichern, wenn Sie OnCommand Insight aktualisieren.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

**Schritte**

1. Melden Sie sich beim Server der Remote-Erfassungseinheit an.
2. Stellen Sie sicher, dass alle OnCommand Insight-Fenster auf dem Server geschlossen sind.
3. Öffnen Sie die Funktion **Programm deinstallieren** auf dem Bedienfeld und wählen Sie das Programm der OnCommand Insight-Fernbedienungseinheit aus, um es zu entfernen.
4. Klicken Sie auf **Deinstallieren** und folgen Sie den Anweisungen.

# Konfiguration und Administration

## Insight einrichten

Für die Einrichtung von Insight müssen Sie Insight Lizenzen aktivieren, Datenquellen einrichten, Benutzer und Benachrichtigungen definieren, Backups aktivieren und alle erforderlichen erweiterten Konfigurationsschritte durchführen.

Nach der Installation des OnCommand Insight-Systems müssen Sie die folgenden Setup-Aufgaben durchführen:

- Installieren Sie Ihre Insight Lizenzen.
- Richten Sie Ihre Datenquellen in Insight ein.
- Richten Sie Benutzerkonten ein.
- Konfigurieren Sie Ihre E-Mail-Adresse.
- Definieren Sie bei Bedarf Ihre SNMP-, E-Mail- oder Syslog-Benachrichtigungen.
- Aktivieren Sie automatische wöchentliche Backups Ihrer Insight-Datenbank.
- Führen Sie alle erforderlichen erweiterten Konfigurationsschritte durch, einschließlich der Definition von Annotationen und Schwellenwerten.

### Zugriff auf die Web-UI

Nach der Installation von OnCommand Insight müssen Sie Ihre Lizenzen installieren und dann Insight einrichten, um Ihre Umgebung zu überwachen. Dazu rufen Sie die Web-UI von Insight über einen Webbrowser auf.

#### Schritte

1. Führen Sie einen der folgenden Schritte aus:
   - Open Insight auf dem Insight-Server:

     `https://fqdn`

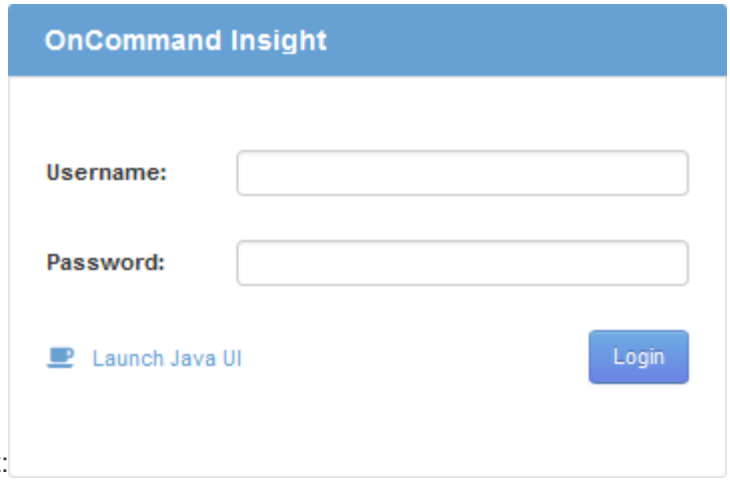
   - Insight von jedem beliebigen anderen Speicherort aus öffnen:

     `https://fqdn:port`

     Die Portnummer ist entweder 443 oder ein anderer Port, der bei der Installation des Insight-Servers konfiguriert wurde. Die Portnummer ist standardmäßig 443, wenn Sie sie nicht in der URL angeben.

   Das Dialogfeld OnCommand Insight wird

angezeigt:




2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.

   Wenn die Lizenzen installiert wurden, wird die Seite zur Einrichtung der Datenquelle angezeigt.

   Eine Insight Browser-Sitzung, die 30 Minuten lang inaktiv war, wurde überschritten, und Sie werden automatisch vom System abgemeldet. Für zusätzliche Sicherheit empfiehlt es sich, den Browser nach der Abmeldung von Insight zu schließen.

## Installieren Ihrer Insight Lizenzen

Wenn Sie die Lizenzdatei mit den Insight Lizenzschlüsseln von NetApp erhalten haben, können Sie mithilfe der Setup-Funktionen alle Ihre Lizenzen gleichzeitig installieren.

### Über diese Aufgabe

Die Insight Lizenzschlüssel werden in einem gespeichert `.txt` Oder `.lcn` Datei:

### Schritte

1. Öffnen Sie die Lizenzdatei in einem Texteditor und kopieren Sie den Text.
2. Öffnen Sie Insight in Ihrem Browser.
3. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
4. Klicken Sie Auf **Setup**.
5. Klicken Sie auf die Registerkarte **Lizenzen**.
6. Klicken Sie Auf **Lizenz Aktualisieren**.
7. Kopieren Sie den Text des Lizenzschlüssels in das Textfeld **Lizenz**.
8. Wählen Sie den Vorgang **Update (am häufigsten)** aus.
9. Klicken Sie Auf **Speichern**.
10. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Kontrollkästchen aktivieren, um das Senden von Nutzungsinformationen an NetApp im Abschnitt **Nutzungsdaten senden** zu aktivieren. Proxy muss ordnungsgemäß konfiguriert und für Ihre Umgebung aktiviert sein.

**Nachdem Sie fertig sind**

Nach der Installation der Lizenzen können Sie die folgenden Konfigurationsaufgaben ausführen:

- Datenquellen konfigurieren.
- Erstellen Sie OnCommand Insight-Benutzerkonten.

**OnCommand Insight-Lizenzen**

OnCommand Insight arbeitet mit Lizenzen, die bestimmte Funktionen auf dem Insight Server ermöglichen.

- **Entdecken**

  Discover ist die grundlegende Insight-Lizenz, die die Inventarisierung unterstützt. Sie müssen über eine Discover-Lizenz verfügen, um OnCommand Insight verwenden zu können, und die Discover-Lizenz muss mit mindestens einer der Lizenzen Assure, Perform oder Plan gekoppelt werden.

- * Versichern*

  Eine Assure Lizenz bietet Support für Assurance-Funktionalität, einschließlich globaler und SAN-Pfadrichtlinien und Management von Verstößen. Mit einer Assure-Lizenz können Sie auch Schwachstellen anzeigen und managen.

- **Ausführen**

  Eine Lizenz ausführen unterstützt die Leistungsüberwachung auf Bestandsseiten, Dashboard-Widgets, Abfragen usw. sowie die Verwaltung von Performance-Richtlinien und -Verstößen.

- **Plan**

  Eine Planlizenz unterstützt Planungsfunktionen, einschließlich Ressourcenverwendung und -Zuweisung.

- **Host Utilization Pack**

  Eine Host-Nutzungslizenz unterstützt die Auslastung des Dateisystems auf Hosts und virtuellen Maschinen.

- **Authoring Melden**

  Eine Lizenz zur Erstellung von Berichten unterstützt zusätzliche Autoren für die Berichterstellung. Diese Lizenz erfordert die Planlizenz.

OnCommand Insight Module sind für einen Jahreszeitraum oder unbefristet lizenziert:

- Nach Terabyte überwachter Kapazität für Discover, Assure, Plan, Perform Module
- Nach Anzahl der Hosts für das Host Utilization Pack
- Nach Anzahl der zusätzlichen für die Berichterstellung erforderlichen Cognos Pro-Autoren

Lizenzschlüssel sind ein Satz eindeutiger Zeichenfolgen, die für jeden Kunden generiert werden. Sie können die Lizenzschlüssel von Ihrem OnCommand Insight-Vertreter beziehen.

Ihre installierten Lizenzen steuern die folgenden Optionen, die in der Software verfügbar sind:

- **Entdecken**

  Inventarisierung und Bestandsverwaltung (Foundation)

  Überwachen von Änderungen und Verwalten von Bestandsrichtlinien

- * Versichern*

  Anzeige und Management von Richtlinien und Verstößen für SAN-Pfade

  Anzeigen und Verwalten von Schwachstellen

  Anzeigen und Managen von Aufgaben und Migrationen

- **Plan**

  Anfragen anzeigen und verwalten

  Anzeigen und Verwalten ausstehender Aufgaben

  Anzeige und Verwaltung von Reservierungsverletzungen

  Anzeige und Verwaltung von Verstößen gegen die Portbilanz

- **Ausführen**

  Überwachen Sie Leistungsdaten, einschließlich Daten in Dashboard-Widgets, Bestandsseiten und Abfragen

  Anzeige und Management von Performance-Richtlinien und -Verstößen

Die folgenden Tabellen enthalten Details zu den Funktionen, die mit und ohne die Lizenz „Perform“ für Administratorbenutzer und Benutzer ohne Administratorrechte verfügbar sind.

| Funktion (Admin) | Mit Perform Lizenz | Ohne Lizenz ausführen |
|---|---|---|
| Applikation | Ja. | Keine Leistungsdaten oder Diagramme |
| Virtual Machine | Ja. | Keine Leistungsdaten oder Diagramme |
| Hypervisor | Ja. | Keine Leistungsdaten oder Diagramme |
| Host | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenspeicher | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| VMDK | Ja. | Keine Leistungsdaten oder Diagramme |
| Internes Volumen | Ja. | Keine Leistungsdaten oder Diagramme |
| Datenmenge | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Pool | Ja. | Keine Leistungsdaten oder Diagramme |
| Festplatte | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage | Ja. | Keine Leistungsdaten oder Diagramme |
| Storage-Node | Ja. | Keine Leistungsdaten oder Diagramme |
| Fabric | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch-Port | Ja. | Keine Leistungsdaten oder Diagramme; „`Port Errors`“ zeigt „`N/A`“ an |
| Speicherport | Ja. | Ja. |
| NPV-Port | Ja. | Keine Leistungsdaten oder Diagramme |
| Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| NPV-Switch | Ja. | Keine Leistungsdaten oder Diagramme |
| Qtrees | Ja. | Keine Leistungsdaten oder Diagramme |
| Kontingente | Ja. | Keine Leistungsdaten oder Diagramme |
| Pfad | Ja. | Keine Leistungsdaten oder Diagramme |

| | | |
|---|---|---|
| Zone | Ja. | Keine Leistungsdaten oder Diagramme |
| Zonenmitglied | Ja. | Keine Leistungsdaten oder Diagramme |
| Generisches Gerät | Ja. | Keine Leistungsdaten oder Diagramme |
| Tape | Ja. | Keine Leistungsdaten oder Diagramme |
| Maskierung | Ja. | Keine Leistungsdaten oder Diagramme |
| ISCSI-Sitzungen | Ja. | Keine Leistungsdaten oder Diagramme |
| ICSI-Netzwerkportale | Ja. | Keine Leistungsdaten oder Diagramme |
| Suche | Ja. | Ja. |
| Admin | Ja. | Ja. |
| Dashboard | Ja. | Ja. |
| Widgets | Ja. | Teilweise verfügbar (nur Asset-, Abfrage- und Admin-Widgets sind verfügbar) |
| Dashboard zu Verstößen | Ja. | Verborgen |
| Ressourcen-Dashboard | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Management von Performance-Richtlinien | Ja. | Verborgen |
| Verwalten von Anmerkungen | Ja. | Ja. |
| Verwalten von Anmerkungsregeln | Ja. | Ja. |
| Management von Applikationen | Ja. | Ja. |

| | | |
|---|---|---|
| Abfragen | Ja. | Ja. |
| Verwalten von Geschäftseinheiten | Ja. | Ja. |

| Merkmal | User - mit Perform-Lizenz | Guest - mit Perform-Lizenz | User - ohne Lizenz ausführen | Guest - ohne Lizenz durchführen |
|---|---|---|---|---|
| Ressourcen-Dashboard | Ja. | Ja. | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) | Teilweise verfügbar (Storage-IOPS und VM-IOPS-Widgets sind ausgeblendet) |
| Benutzerdefiniertes Dashboard | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) | Nur Ansicht (keine Optionen zum Erstellen, Bearbeiten oder Speichern) |
| Management von Performance-Richtlinien | Ja. | Verborgen | Verborgen | Verborgen |
| Verwalten von Anmerkungen | Ja. | Verborgen | Ja. | Verborgen |
| Management von Applikationen | Ja. | Verborgen | Ja. | Verborgen |
| Verwalten von Geschäftseinheiten | Ja. | Verborgen | Ja. | Verborgen |
| Abfragen | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) | Ja. | Nur anzeigen und bearbeiten (keine Speicheroption) |

## Einrichten und Verwalten von Benutzerkonten

Benutzerkonten, Benutzerauthentifizierung und Benutzerautorisierung können auf zwei Arten definiert und verwaltet werden: Im Microsoft Active Directory-Server (Version 2 oder 3) LDAP-Server (Lightweight Directory Access Protocol) oder in einer internen OnCommand Insight-Benutzerdatenbank. Die Verwendung eines anderen Benutzerkontos für jede Person ermöglicht die Kontrolle der Zugriffsrechte, individuellen Einstellungen und Verantwortlichkeiten. Verwenden Sie ein Konto, das über Administratorrechte für diesen Vorgang verfügt.

### Bevor Sie beginnen

Sie müssen die folgenden Aufgaben ausgeführt haben:

- Installieren Sie Ihre OnCommand Insight Lizenzen.
- Weisen Sie jedem Benutzer einen eindeutigen Benutzernamen zu.
- Legen Sie fest, welche Passwörter verwendet werden sollen.
- Weisen Sie die richtigen Benutzerrollen zu.

Wenn Sie ein LDAP-Zertifikat importieren und *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Bewährte Sicherheitsmethoden legen fest, dass Administratoren das Host-Betriebssystem so konfigurieren, dass die interaktive Anmeldung von nicht-Administrator-/Standardbenutzern verhindert wird.

### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Setup**.
4. Wählen Sie die Registerkarte **Users**aus.
5. Um einen neuen Benutzer zu erstellen, klicken Sie auf die Schaltfläche **Aktionen** und wählen **Benutzer hinzufügen**.

   Sie geben die Adresse **Name**, **Passwort**, **E-Mail** ein und wählen eine der Benutzer **Rollen** als Administrator, Benutzer oder Gast aus.

6. Um die Informationen eines Benutzers zu ändern, wählen Sie den Benutzer aus der Liste aus und klicken Sie rechts neben der Benutzerbeschreibung auf das Symbol **Benutzerkonto bearbeiten**.
7. Um einen Benutzer aus dem OnCommand Insight-System zu entfernen, wählen Sie den Benutzer aus der Liste aus und klicken Sie rechts neben der Benutzerbeschreibung auf **Benutzerkonto löschen**.

### Ergebnisse

Wenn sich ein Benutzer bei OnCommand Insight anmeldet, versucht der Server zunächst, sich über LDAP zu authentifizieren, wenn LDAP aktiviert ist. Wenn OnCommand Insight den Benutzer auf dem LDAP-Server nicht finden kann, wird in der lokalen Insight-Datenbank gesucht.

### Insight-Benutzerrollen

Jedem Benutzerkonto wird eine der drei möglichen Berechtigungsstufen zugewiesen.

- Gäste können sich bei Insight anmelden und die verschiedenen Seiten ansehen.
- Benutzer erlaubt alle Berechtigungen auf Gastebene sowie den Zugriff auf Insight Vorgänge, z. B. die Definition von Richtlinien und die Identifizierung generischer Geräte. Der Benutzerkontotyp erlaubt es Ihnen nicht, Datenquellenvorgänge durchzuführen oder andere Benutzerkonten als Ihr eigenes hinzuzufügen oder zu bearbeiten.

- Der Administrator ermöglicht Ihnen, alle Vorgänge auszuführen, einschließlich des Hinzufügens neuer Benutzer und der Verwaltung von Datenquellen.

**Best Practice:** Schränken Sie die Anzahl der Benutzer mit Administratorberechtigungen ein, indem Sie die meisten Konten für Benutzer oder Gäste erstellen.

#### Konfigurieren von Insight für LDAP(s)

## OnCommand Insight muss mit LDAP-Einstellungen (Lightweight Directory Access Protocol) konfiguriert werden, da diese in Ihrer LDAP-Domäne des Unternehmens konfiguriert sind.

Bevor Sie Insight für die Verwendung mit LDAP oder Secure LDAP (LDAPS) konfigurieren, notieren Sie sich die Active Directory-Konfiguration in Ihrer Unternehmensumgebung. Insight-Einstellungen müssen mit denen in der LDAP-Domänenkonfiguration Ihres Unternehmens übereinstimmen. Lesen Sie die folgenden Konzepte, bevor Sie Insight für die Verwendung mit LDAP konfigurieren, und wenden Sie sich an Ihren LDAP-Domänenadministrator, um die richtigen Attribute für Ihre Umgebung zu ermitteln.

Für alle Secure Active Directory (d. h. LDAPS)-Benutzer müssen Sie den AD-Servernamen genau so verwenden, wie er im Zertifikat definiert ist. Sie können die IP-Adresse nicht für die sichere AD-Anmeldung verwenden.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert "Sicherheitsadministration"haben, starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

OnCommand Insight unterstützt LDAP und LDAPS über Microsoft Active Directory Server oder Azure AD. Zusätzliche LDAP-Implementierungen funktionieren möglicherweise, wurden aber nicht für Insight qualifiziert. Die Verfahren in diesen Handbüchern gehen davon aus, dass Sie Microsoft Active Directory Version 2 oder 3 LDAP (Lightweight Directory Access Protocol) verwenden.

#### User Principal Name Attribut:

Das Attribut LDAP User Principal Name (userPrincipalName) wird von Insight als Attribut username verwendet. Der Hauptname des Benutzers ist in einer Active Directory (AD)-Gesamtstruktur garantiert global eindeutig, aber in vielen großen Unternehmen ist der Hauptname eines Benutzers möglicherweise nicht sofort ersichtlich oder bekannt. Ihr Unternehmen kann für den primären Benutzernamen eine Alternative zum Attribut User Principal Name verwenden.

Im Folgenden finden Sie einige alternative Werte für das Attributfeld User Principal Name:

- **SAMAccountName**

  Dieses Benutzerattribut ist der alte Benutzername vor Windows 2000 NT - das ist es, was die meisten Benutzer gewohnt sind, sich auf ihrem persönlichen Windows-Rechner anzumelden. Dies ist nicht garantiert weltweit einzigartig in einer AD-Gesamtstruktur.

  SAMAccountName berücksichtigt Groß- und Kleinschreibung für das Attribut User Principal Name.

- **Mail**

In AD-Umgebungen mit MS Exchange ist dieses Attribut die primäre E-Mail-Adresse für den Endbenutzer. Dies sollte global einzigartig in einer AD-Gesamtstruktur sein (und auch für Endbenutzer bekannt), im Gegensatz zu ihrem userPrincipalName-Attribut. Das Mail-Attribut ist in den meisten nicht-MS Exchange-Umgebungen nicht vorhanden.

- **Empfehlung**

  Eine LDAP-Weiterleitung ist die Art und Weise eines Domänencontrollers, einer Client-Anwendung zu zeigen, dass sie keine Kopie eines angeforderten Objekts hat (genauer gesagt: Dass es nicht den Abschnitt des Verzeichnisbaums enthält, in dem das Objekt sein würde, wenn es tatsächlich existiert) und dem Client einen Speicherort gibt, der das Objekt wahrscheinlicher enthält. Der Client wiederum verwendet die Weiterleitung als Grundlage für eine DNS-Suche nach einem Domänencontroller. Im Idealfall verweisen Verweise immer auf einen Domänencontroller, der das Objekt tatsächlich enthält. Es ist jedoch möglich, dass der verwies Domänencontroller eine weitere Empfehlung generiert, obwohl es in der Regel nicht lange dauert, zu erkennen, dass das Objekt nicht existiert und den Client zu informieren.

SAMAccountName wird im Allgemeinen dem Hauptnamen des Benutzers vorgezogen. SAMAccountName ist in der Domain eindeutig (obwohl er in der Domänenstruktur nicht eindeutig ist), aber es ist die String-Domain, die Benutzer normalerweise für die Anmeldung verwenden (z. B.,*netapp\username*).der Distinguished Name ist der eindeutige Name in der Gesamtstruktur, ist aber in der Regel von den Benutzern nicht bekannt.

Auf dem Windows-Systemteil derselben Domäne können Sie immer eine Eingabeaufforderung öffnen und SET eingeben, um den richtigen Domänennamen zu finden (USERDOMAIN=). Der OCI-Anmeldename lautet dann `USERDOMAIN\sAMAccountName`.

Verwenden Sie für den Domainnamen **mydomain.x.y.z.com** `DC=x,DC=y,DC=z,DC=com` Geben Sie in Insight im Feld Domain ein.

**Ports**:

Der Standardport für LDAP ist 389, und der Standardport für LDAPS ist 636

Typische URL für LDAPS: `ldaps://<ldap_server_host_name>:636`

Protokolle befinden sich bei:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

Standardmäßig erwartet Insight die in den folgenden Feldern angegebenen Werte. Wenn sich diese Änderungen in Ihrer Active Directory-Umgebung ändern, müssen Sie sie in der Insight LDAP-Konfiguration ändern.

| Rollenattribut |
| --- |
| Mitgliedschafts |
| Mail-Attribut |
| E-Mail |

| |
|---|
| Attribut Distinguished Name |
| Name wird unterschieden |
| Empfehlung |
| Folgen |

**Gruppen:**

Um Benutzer mit unterschiedlichen Zugriffsrollen auf den OnCommand Insight- und DWH-Servern zu authentifizieren, müssen Sie Gruppen in Active Directory erstellen und diese Gruppennamen auf OnCommand Insight- und DWH-Servern eingeben. Die folgenden Gruppennamen sind nur Beispiele. Die Namen, die Sie für LDAP in Insight konfigurieren, müssen mit denen übereinstimmen, die für Ihre Active Directory-Umgebung eingerichtet wurden.

| Insight Group | Beispiel |
|---|---|
| Insight Server Administratorgruppe | insight.server.admins |
| Insight Administratoren | Insight.Administratoren |
| Insight Benutzergruppe | insight.users |
| Insight Gästegruppe | Insight.Gäste |
| Administratorgruppe für Berichte | Insight.Report.Administratoren |
| Gruppe der pro-Autoren berichten | insight.report.proauthors |
| Gruppe „Verfasser von Berichten“ | insight.report.business.authors |
| Gruppe der meldesstattenen Verbraucher | Insight.Report.Business.Consumers |
| Gruppe der Reporting-Empfänger | Insight.Report.Empfänger |

#### Konfigurieren von Benutzerdefinitionen mithilfe von LDAP

## Um OnCommand Insight (OCI) für die Benutzerauthentifizierung und -Autorisierung von einem LDAP-Server zu konfigurieren, müssen Sie auf dem LDAP-Server als OnCommand Insight-Serveradministrator definiert sein.

### Bevor Sie beginnen

Sie müssen die Benutzer- und Gruppenattribute kennen, die für Insight in Ihrer LDAP-Domäne konfiguriert wurden.

Für alle Secure Active Directory (d. h. LDAPS)-Benutzer müssen Sie den AD-Servernamen genau so verwenden, wie er im Zertifikat definiert ist. Sie können die IP-Adresse nicht für die sichere AD-Anmeldung verwenden.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert "Sicherheitsadministration"haben, starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

### Über diese Aufgabe

OnCommand Insight unterstützt LDAP und LDAPS über Microsoft Active Directory Server. Zusätzliche LDAP-Implementierungen funktionieren möglicherweise, wurden aber nicht für Insight qualifiziert. Bei diesem Verfahren wird davon ausgegangen, dass Sie Microsoft Active Directory Version 2 oder 3 LDAP (Lightweight Directory Access Protocol) verwenden.

LDAP-Benutzer werden zusammen mit den lokal definierten Benutzern in der Liste **Admin** > **Setup** › **Users** angezeigt.

### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Setup**.
3. Klicken Sie auf die Registerkarte **Users**.
4. Blättern Sie zum Abschnitt LDAP.
5. Klicken Sie auf **LDAP aktivieren**, um die LDAP-Benutzerauthentifizierung und -Autorisierung zu ermöglichen.
6. Füllen Sie die Felder aus:

   ◦ `LDAP servers`: Insight akzeptiert eine kommagetrennte Liste von LDAP-URLs. Insight versucht, eine Verbindung zu den bereitgestellten URLs herzustellen, ohne das LDAP-Protokoll zu überprüfen.

   Um die LDAP-Zertifikate zu importieren, klicken Sie auf **Zertifikate** und importieren oder suchen Sie die Zertifikatdateien automatisch.

   Die IP-Adresse oder der DNS-Name, der zur Identifizierung des LDAP-Servers verwendet wird, wird in der Regel in diesem Format eingegeben:

   ```
   ldap://<ldap-server-address>:port
   ```

   Oder, wenn Sie den Standardport verwenden:

   ```
   ldap://<ldap-server-address>
   ```

   +
   Stellen Sie bei der Eingabe mehrerer LDAP-Server in dieses Feld sicher, dass bei jedem Eintrag die richtige Portnummer verwendet wird.

- `User name`: Geben Sie die Anmeldeinformationen für einen Benutzer ein, der für Anfragen zur Verzeichnissuche auf den LDAP-Servern autorisiert ist.
- `Password`: Geben Sie das Passwort für den oben genannten Benutzer ein. Um dieses Passwort auf dem LDAP-Server zu bestätigen, klicken Sie auf **Validieren**.

7. Wenn Sie diesen LDAP-Benutzer genauer definieren möchten, klicken Sie auf **Mehr anzeigen** und füllen Sie die Felder für die aufgelisteten Attribute aus.

   Diese Einstellungen müssen mit den in Ihrer LDAP-Domäne konfigurierten Attributen übereinstimmen. Wenden Sie sich an Ihren Active Directory-Administrator, wenn Sie sich nicht sicher sind, welche Werte für diese Felder eingegeben werden müssen.

   - **Admins-Gruppe**

     LDAP-Gruppe für Benutzer mit Insight Administrator-Berechtigungen. Standard ist `insight.admins`.

   - **Benutzergruppe**

     LDAP-Gruppe für Benutzer mit Insight-Benutzerberechtigungen. Standard ist `insight.users`.

   - **Gästegruppe**

     LDAP-Gruppe für Benutzer mit Insight Gastberechtigungen. Standard ist `insight.guests`.

   - **Server Admins-Gruppe**

     LDAP-Gruppe für Benutzer mit Insight Server Administrator-Berechtigungen. Standard ist `insight.server.admins`.

   - **Timeout**

     Dauer der Wartezeit auf eine Antwort vom LDAP-Server vor der Zeitüberschreitung in Millisekunden. Der Standardwert ist 2,000, was in allen Fällen angemessen ist und nicht geändert werden sollte.

   - **Domäne**

     LDAP-Knoten, auf dem OnCommand Insight nach dem LDAP-Benutzer suchen soll. Dies ist in der Regel die Domäne der obersten Ebene für das Unternehmen. Beispiel:

     ```
     DC=<enterprise>,DC=com
     ```

   - **Attribut des Hauptnamens des Benutzers**

     Attribut, das jeden Benutzer im LDAP-Server identifiziert. Standard ist `userPrincipalName`, Die weltweit einzigartig ist. OnCommand Insight versucht, den Inhalt dieses Attributs mit dem oben angegebenen Benutzernamen abzugleichen.

   - **Rollenattribut**

     LDAP-Attribut, das die Passung des Benutzers innerhalb der angegebenen Gruppe identifiziert. Standard ist `memberOf`.

   - **Mail-Attribut**

LDAP-Attribut, das die E-Mail-Adresse des Benutzers identifiziert. Standard ist `mail`. Dies ist nützlich, wenn Sie Berichte von OnCommand Insight abonnieren möchten. Insight erfasst die E-Mail-Adresse des Benutzers bei der ersten Anmeldung und sucht danach nicht mehr.

Wenn sich die E-Mail-Adresse des Benutzers auf dem LDAP-Server ändert, müssen Sie sie in Insight aktualisieren.

- **Distinguished Name Attribut**

  LDAP-Attribut, das den Distinguished Name des Benutzers identifiziert. Der Standardwert ist `distinguishedName`.

8. Klicken Sie Auf **Speichern**.

### Benutzerpasswörter werden geändert

Ein Benutzer mit Administratorrechten kann das Kennwort für jedes auf dem lokalen Server definierte OnCommand Insight-Benutzerkonto ändern.

#### Bevor Sie beginnen

Die folgenden Punkte müssen abgeschlossen sein:

- Benachrichtigungen an alle Personen, die sich bei dem Benutzerkonto anmelden, das Sie ändern möchten.
- Neues Passwort, das nach dieser Änderung verwendet werden soll.

#### Über diese Aufgabe

Bei Verwendung dieser Methode können Sie das Kennwort für einen Benutzer, der über LDAP validiert wird, nicht ändern.

#### Schritte

1. Melden Sie sich mit Administratorrechten an.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Setup**.
4. Klicken Sie auf die Registerkarte **Users**.
5. Suchen Sie die Zeile, in der das Benutzerkonto angezeigt wird, das Sie ändern möchten.
6. Rechts neben den Benutzerinformationen klicken Sie auf **Benutzerkonto bearbeiten**.
7. Geben Sie das neue **Passwort** ein und geben Sie es dann erneut in das Bestätigungsfeld ein.
8. Klicken Sie Auf **Speichern**.

### Bearbeiten einer Benutzerdefinition

Ein Benutzer mit Administratorrechten kann ein Benutzerkonto bearbeiten, um die E-Mail-Adresse oder Rollen für OnCommand Insight- oder DWH- und Berichtsfunktionen zu ändern.

#### Bevor Sie beginnen

Legen Sie den Typ des Benutzerkontos fest (OnCommand Insight, DWH oder eine Kombination), das geändert werden muss.

#### Über diese Aufgabe

Für LDAP-Benutzer können Sie die E-Mail-Adresse nur mit dieser Methode ändern.

#### Schritte

1. Melden Sie sich mit Administratorrechten an.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Setup**.
4. Klicken Sie auf die Registerkarte **Users**.
5. Suchen Sie die Zeile, in der das Benutzerkonto angezeigt wird, das Sie ändern möchten.
6. Klicken Sie rechts neben den Benutzerinformationen auf das Symbol **Benutzerkonto bearbeiten**.
7. Nehmen Sie die erforderlichen Änderungen vor.
8. Klicken Sie Auf **Speichern**.

#### Löschen eines Benutzerkontos

Jeder Benutzer mit Administratorrechten kann ein Benutzerkonto löschen, wenn es nicht mehr verwendet wird (für eine lokale Benutzerdefinition), oder um OnCommand Insight zu zwingen, die Benutzerinformationen bei der nächsten Anmeldung des Benutzers (für einen LDAP-Benutzer) neu zu ermitteln.

#### Schritte

1. Melden Sie sich mit Administratorrechten bei OnCommand Insight an.
2. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
3. Klicken Sie Auf **Setup**.
4. Klicken Sie auf die Registerkarte **Users**.
5. Suchen Sie die Zeile, in der das Benutzerkonto angezeigt wird, das Sie löschen möchten.
6. Rechts neben den Benutzerinformationen klicken Sie auf das Symbol **Benutzerkonto löschen** „**x**“.
7. Klicken Sie Auf **Speichern**.

## Festlegen einer Warnmeldung für die Anmeldung

Mit OnCommand Insight können Administratoren eine benutzerdefinierte Textmeldung festlegen, die bei der Anmeldung des Benutzers angezeigt wird.

#### Schritte

1. So legen Sie die Meldung auf dem OnCommand Insight-Server fest:
   a. Navigieren Sie zu dem Menü:Admin[Fehlerbehebung > Erweiterte Fehlerbehebung > Erweiterte Einstellungen].

b. Geben Sie Ihre Login-Nachricht in den Textbereich ein.
c. Klicken Sie auf das Kontrollkästchen **Client zeigt Anmelde-Warnmeldung an**.
d. Klicken Sie Auf **Speichern**.

   Die Meldung wird bei der Anmeldung für alle Benutzer angezeigt.

2. So legen Sie die Meldung im Data Warehouse (DWH) und Reporting (Cognos) fest:
   a. Navigieren Sie zu **System Information** und klicken Sie auf die Registerkarte **Login Warning**.
   b. Geben Sie Ihre Login-Nachricht in den Textbereich ein.
   c. Klicken Sie Auf **Speichern**.

      Die Meldung wird bei der DWH- und Cognos Reporting-Anmeldung für alle Benutzer angezeigt.

## Sicherheitstool

OnCommand Insight bietet Funktionen, mit denen Insight Umgebungen sicherer betrieben werden können. Diese Funktionen umfassen Verschlüsselung, Passwort-Hashing und die Möglichkeit, interne Benutzerpasswörter und Schlüsselpaare zu ändern, die Kennwörter verschlüsseln und entschlüsseln. Sie können diese Funktionen auf allen Servern in der Insight-Umgebung mit dem **SecurityAdmin Tool** verwalten.

### Was ist das SecurityAdmin-Tool?

Das Sicherheits-Admin-Tool unterstützt Änderungen am Inhalt der Vaults sowie koordinierte Änderungen an der OnCommand Insight-Installation.

Die primären Verwendungszwecke für das SecurityAdmin-Tool sind **Backup** und **Restore** der Sicherheitskonfiguration (d.h. Tresor) und Passwörter. Sie können beispielsweise den Tresor auf einer lokalen Erfassungseinheit sichern und auf einer Remote-Erfassungseinheit wiederherstellen, um die Passwortkoordination in Ihrer gesamten Umgebung sicherzustellen. Oder wenn Sie mehrere OnCommand Insight-Server in Ihrer Umgebung haben, möchten Sie möglicherweise ein Backup des Server-Tresors erstellen und diese auf anderen Servern wiederherstellen, um die Passwörter unverändert zu halten. Dies sind nur zwei Beispiele für die Art und Weise, wie SecurityAdmin verwendet werden kann, um die Kohäsion in Ihren Umgebungen zu gewährleisten.

Es wird dringend empfohlen, den Vault * zu sichern, wenn Sie eine OnCommand Insight-Datenbank sichern. Andernfalls kann der Zugriff verloren gehen.

Das Tool bietet sowohl **Interactive** als auch **command line** Modi.

Viele Operationen des SecurityAdmin Tools ändern den Inhalt des Tresors und nehmen auch Änderungen an der Installation vor, um sicherzustellen, dass der Tresor und die Installation synchron bleiben.

Beispiel:

- Wenn Sie ein Insight-Benutzerpasswort ändern, wird der Benutzereintrag in der Tabelle SANscreen.Users mit dem neuen Hash aktualisiert.
- Wenn Sie das Passwort eines MySQL-Benutzers ändern, wird die entsprechende SQL-Anweisung ausgeführt, um das Kennwort des Benutzers in der MySQL-Instanz zu aktualisieren.

In einigen Situationen werden mehrere Änderungen an der Installation vorgenommen:

- Wenn Sie den dwh MySQL-Benutzer ändern, werden neben der Aktualisierung des Passworts in der MySQL-Datenbank auch mehrere Registrierungseinträge für ODBC aktualisiert.

In den folgenden Abschnitten wird der Begriff "koordinierte Änderungen" verwendet, um diese Änderungen zu beschreiben.

**Ausführungsmodi**

- Normaler/Standardbetrieb – der SANscreen-Serverdienst muss ausgeführt werden

  Für den Standardausführungsmodus erfordert das SecurityAdmin-Tool, dass der **SANscreen-Serverdienst** ausgeführt wird. Der Server wird für die Authentifizierung verwendet, und viele koordinierte Änderungen an der Installation werden durch Aufrufen des Servers vorgenommen.

- Direkter Betrieb – der SANscreen-Serverdienst wird möglicherweise ausgeführt oder angehalten.

  Bei Ausführung auf einem OCI-Server oder einer DWH-Installation kann das Tool auch im „direkten“ Modus ausgeführt werden. In diesem Modus werden Authentifizierung und koordinierte Änderungen über die Datenbank durchgeführt. Der Serverdienst wird nicht verwendet.

  Der Betrieb ist mit dem normalen Modus identisch, mit den folgenden Ausnahmen:

- Die Authentifizierung wird nur für Benutzer unterstützt, die keine Domäne haben. (Benutzer, deren Passwort und Rollen sich in der Datenbank befinden, nicht LDAP).
- Der Vorgang „Schlüssel ersetzen“ wird nicht unterstützt.
- Der Schritt zur erneuten Verschlüsselung der Vault-Wiederherstellung wird übersprungen.
- Wiederherstellungsmodus das Tool kann auch dann ausgeführt werden, wenn der Zugriff auf den Server und die Datenbank nicht möglich ist (z. B. weil das Root-Passwort im Tresor falsch ist).

  Bei Ausführung in diesem Modus ist keine Authentifizierung möglich und daher kann kein Vorgang mit koordinierter Änderung der Installation durchgeführt werden.

  Der Wiederherstellungsmodus kann verwendet werden, um:

- Bestimmen Sie, welche Vault-Einträge falsch sind (mit dem Verifizierungs-Vorgang).
- Ersetzen Sie das falsche Root-Passwort durch den richtigen Wert. (Das Passwort wird dadurch nicht geändert. Der Benutzer muss das aktuelle Passwort eingeben.)

> Wenn das Root-Passwort im Tresor falsch ist und das Passwort nicht bekannt ist und es keine Sicherung des Tresors mit dem korrekten Root-Passwort gibt, kann die Installation nicht mit dem SecurityAdmin-Tool wiederhergestellt werden. Die einzige Möglichkeit, die Installation wiederherzustellen, ist das Zurücksetzen des Passworts der MySQL-Instanz nach dem unter dokumentierten Verfahren https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Verwenden Sie nach dem Zurücksetzen den Vorgang Correct-stored-password, um das neue Passwort in den Tresor einzugeben.

**Befehle**

#### Unbeschränkte Befehle

Unbeschränkte Befehle nehmen alle koordinierten Änderungen an der Installation vor (außer Vertrauensstellungen). Unbeschränkte Befehle können ohne Benutzerauthentifizierung ausgeführt werden.

| Befehl | Beschreibung |
|---|---|
| Backup-Vault | Erstellen Sie eine ZIP-Datei mit dem Tresor. Der relative Pfad zu den Vault-Dateien stimmt mit dem Pfad der Vaults relativ zum Installationsroot überein.<br>• wildfly/Standalone/Configuration/Vault/*<br>• acq/conf/Vault/*<br>Beachten Sie, dass es dringend empfohlen wird, den Tresor zu sichern, wenn Sie eine OnCommand Insight-Datenbank sichern. |
| Nach Standardschlüsseln suchen | Überprüfen Sie, ob die Schlüssel des Tresors mit denen des Standard-Tresors übereinstimmen, der in Instanzen vor 7.3.16 verwendet wird. |
| Korrekt gespeichertes Passwort | Ersetzen Sie ein (falsches) Kennwort, das im Tresor gespeichert ist, durch das korrekte Kennwort, das dem Benutzer bekannt ist.<br>Dies kann verwendet werden, wenn der Tresor und die Installation nicht konsistent sind. **Beachten Sie, dass es das eigentliche Passwort in der Installation nicht ändert.** |
| | Change-Trust-Store-password Ändern Sie das für einen Trust-Store verwendete Passwort und speichern Sie das neue Passwort im Tresor. Das aktuelle Kennwort des Vertrauenshauses muss „bekannt“ sein. |
| Verify-keystore | Prüfen Sie, ob die Werte im Tresor korrekt sind:<br>• Stimmt der Hash des Passworts für OCI-Benutzer mit dem Wert in der Datenbank überein<br>• Für MySQL-Benutzer kann eine Datenbankverbindung hergestellt werden<br>• Für Schlüsselspeicher kann der Schlüsselspeicher geladen und seine Schlüssel (falls vorhanden) gelesen werden |
| Listentasten | Einträge im Tresor auflisten (ohne Anzeige des gespeicherten Wertes) |

#### Eingeschränkte Befehle

Für alle nicht verborgenen Befehle, die koordinierte Änderungen an der Installation vornehmen, ist eine Authentifizierung erforderlich:

| Befehl | Beschreibung |
|---|---|

| | |
|---|---|
| Restore-Vault-Backup | Ersetzt den aktuellen Tresor durch den Tresor, der in der angegebenen Vault-Sicherungsdatei enthalten ist.<br><br>Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Kennwörtern im wiederhergestellten Tresor entspricht:<br><br>• Aktualisieren Sie die Benutzerpasswörter für die OCI-Kommunikation<br>• Aktualisieren Sie die MySQL-Benutzerpasswörter, einschließlich Root<br>• Wenn das Schlüsselspeicher-Passwort „bekannt“ ist, aktualisieren Sie den Schlüsselspeicher mit den Kennwörtern aus dem wiederhergestellten Tresor.<br><br>Bei der Ausführung im normalen Modus werden auch alle verschlüsselten Werte von der Instanz gelesen, mit dem Verschlüsselungsdienst des aktuellen Tresors entschlüsselt, mit dem Verschlüsselungsdienst des wiederhergestellten Tresors erneut verschlüsselt und der neu verschlüsselte Wert gespeichert. |
| Sync-with-Vault | Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Benutzerpasswörtern im wiederhergestellten Tresor entspricht:<br><br>• Aktualisiert die Benutzerpasswörter für die OCI-Kommunikation<br>• Aktualisiert die MySQL-Benutzerpasswörter, einschließlich Root |
| Passwort ändern | Ändert das Passwort im Tresor und führt die koordinierten Aktionen durch. |
| Schlüssel ersetzen | Erstellen Sie einen neuen leeren Tresor (der andere Schlüssel als der vorhandene Tresor hat). Kopieren Sie dann die Einträge aus dem aktuellen Tresor in den neuen Tresor. Liest dann jeden verschlüsselten Wert aus der Instanz, entschlüsselt ihn mit dem Verschlüsselungsdienst des aktuellen Tresors, verschlüsselt ihn mit dem Verschlüsselungsdienst des wiederhergestellten Tresors und speichert den neu verschlüsselten Wert. |

### Koordinierte Maßnahmen

#### Server Vault

| | |
|---|---|
| _Intern | Passwort-Hash für Benutzer in Datenbank aktualisieren |
| Akquisition | Passwort-Hash für Benutzer in Datenbank aktualisieren<br><br>Wenn der Akquisitionssault vorhanden ist, aktualisieren Sie auch den Eintrag im Akquisitions-Vault |
| dwh_intern | Passwort-Hash für Benutzer in Datenbank aktualisieren |

| | |
|---|---|
| cognos_admin | Passwort-Hash für Benutzer in Datenbank aktualisieren<br><br>Wenn DWH und Windows, aktualisieren Sie SANscreen/cognos/Analytics/Configuration/SANscreenAP.properties, um die Eigenschaft cognos.admin auf das Passwort zu setzen. |
| Stamm | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| Inventar | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| dwh | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren<br><br>Wenn DWH und Windows, aktualisieren Sie die Windows-Registrierung, um die folgenden ODBC-bezogenen Einträge auf das neue Passwort zu setzen:<br><br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud_Cost\PWD |
| Whuser | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| Hosts | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |

| | |
|---|---|
| Keystore_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.keystore |
| Trustore_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.trustore |
| Key_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/sso.jks |
| cognos_Archive | Keine |

**Akquisitions-Vault**

| | |
|---|---|
| Akquisition | Keine |
| Trustore_password | Schreiben Sie den Keystore mit dem neuen Passwort (falls vorhanden) neu - acq/conf/cert/Client.keystore |

### Ausführen des Security Admin Tools - Befehlszeile

Die Syntax zum Ausführen des SA-Tools im Befehlszeilenmodus lautet:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Hinweise:

- Die Option „-i“ ist möglicherweise nicht in der Befehlszeile vorhanden (da hier der interaktive Modus ausgewählt wird).
- Für die Optionen „-s“ und „-au“:
  - „-s“ ist auf einer rau nicht zulässig
  - „-au“ ist auf DWH nicht zulässig

- Wenn keines vorhanden ist, dann
  - Der Server-Vault wird auf Server, DWH und Dual ausgewählt
  - Der Aufnahmevault wird auf der rau ausgewählt
- Die Optionen -lu und -lp werden für die Benutzerauthentifizierung verwendet.
  - Wenn <user> angegeben ist und <password> nicht angegeben ist, wird der Benutzer zur Eingabe des Passworts aufgefordert.
  - Wenn <user> nicht bereitgestellt wird und eine Authentifizierung erforderlich ist, wird der Benutzer aufgefordert, sowohl <user> als auch <password> einzugeben.

**Befehle:**

| Befehl | Zu Verwenden |
|---|---|
| Korrekt gespeichertes Passwort | `securityadmin [-s` |
| -au] [-db] -pt <key> [<value>]<br><br>`where`<br><br>-pt specifies the command ("put")<br><key> is the key<br><value> is the value. If not present, user will be prompted for value<br><br> | Backup-Vault |
| `securityadmin [-s` | -au] [-db] -b [<backup-dir>]<br><br>where<br><br>-b specified command<br><backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used<br>The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip<br><br> |
| Backup-Vault | `securityadmin [-s` |

| | |
|---|---|
| -au] [-db] -ub <backup-file><br><br>where<br><br>-ub specified command ("upgrade-backup")<br><backup-file> The location to write the backup file<br><br>``` | Listentasten |
| ```<br>securityadmin [-s<br>``` | -au] [-db] -l<br><br>where<br><br>-l specified command<br><br>``` |
| Prüfschlüssel | ```<br>securityadmin [-s<br>``` |
| -au] [-db] -ck<br><br>where<br><br>-ck specified command<br><br>exit code:<br>1 error<br>2 default key(s)<br>3 unique keys<br><br>``` | Verify-keystore (Server) |
| ```<br>securityadmin [-s] [-db] -v<br><br>where<br><br>-v specified command<br>``` | Upgrade |

| | |
|---|---|
| `securityadmin [-s` | -au] [-db] [-lu <user>] [-lp <password>] -u<br><br>where<br><br>-u specified command<br><br>For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault.<br>For acquisition vault, if -lu is not present, then no authentication will be attempted<br><br>`` |
| Schlüssel ersetzen | `securityadmin [-s` |
| -au] [-db] [-lu <user>] [-lp <password>] -rk<br><br>where<br><br>-rk specified command<br><br>`` | Restore-Vault-Backup |
| `securityadmin [-s` | -au] [-db] [-lu <user>] [-lp <password>] -r <backup-file><br><br>where<br><br>-r specified command<br><backup-file> the backup file location<br><br>`` |
| Change-Password (Server) | `securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`<br><br>`where`<br><br>`-up specified command ("update-password")`<br>`-un <user> entry ("user") name to update`<br>`-p <password> new password. If <password not supplied, user will be prompted.`<br>`-sh for mySQL user, use strong hash` |

| | |
|---|---|
| Change-Passwort für Akquisitionsbenutzer (Akquisition) | `securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`<br><br>`where`<br><br>`-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.` |
| Change-password für Truststore-_password (Akquisition) | `securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`<br><br>`where`<br><br>`-utp specified command ("update-truststore-password") -p <password> new password. If <password not supplied, user will be prompted.` |
| Synchronisieren mit Tresor (Server) | `securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`<br><br>`where`<br><br>`-sv specified command` |

### Ausführen des Security Admin Tools – Interaktiver Modus

#### Interaktiv – Hauptmenü

Um das SA-Tool im interaktiven Modus auszuführen, geben Sie den folgenden Befehl ein:

```
 securityadmin -i
Bei einer Server- oder Doppelinstallation fordert SecurityAdmin den
Benutzer auf, entweder den Server oder die lokale Erfassungseinheit
auszuwählen.
```

Knoten der Server- und Erfassungseinheit erkannt! Wählen Sie den Knoten aus, dessen Sicherheit neu konfiguriert werden muss:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

Auf DWH wird automatisch „Server“ ausgewählt. Auf einer externen AU wird automatisch „Acquisition Unit“ ausgewählt.

#### Interactive - Server: Wiederherstellung des Root-Passworts

Im Server-Modus überprüft das SecurityAdmin-Tool zunächst, ob das gespeicherte Root-Passwort korrekt ist. Wenn dies nicht der Fall ist, zeigt das Tool den Bildschirm zur Wiederherstellung des Root-Passworts an.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

#### Interactive - Server: Korrektes Passwort

Mit der Aktion „Passwort korrigieren“ wird das im Tresor gespeicherte Passwort so geändert, dass es mit dem für die Installation erforderlichen Kennwort übereinstimmt. Dieser Befehl ist nützlich in Situationen, in denen eine Änderung an der Installation durch etwas anderes als das securityadmin-Tool vorgenommen wurde. Beispiele:

- Das Passwort für einen SQL-Benutzer wurde durch direkten Zugriff auf MySQL geändert.
- Ein Keystore wird ersetzt oder das Passwort eines Keystore wird mit keytool geändert.
- Eine OCI Datenbank wurde wiederhergestellt, und diese Datenbank enthält unterschiedliche Passwörter für die internen Benutzer

„Passwort korrigieren“ fordert den Benutzer zuerst auf, das Kennwort auszuwählen, um den richtigen Wert zu speichern.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Nach Auswahl des zu korrigenden Eintrags wird der Benutzer gefragt, wie er den Wert angeben möchte.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers
zurück.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers zurück.

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers angezeigt.

#### Interactive - Server: Überprüfen Sie Den Inhalt Des Tresores

Überprüfen Sie, ob Vault Contents Schlüssel enthält, die mit dem StandardVault übereinstimmen, der mit früheren OCI-Versionen verteilt ist, und überprüft, ob jeder Wert im Vault mit der Installation übereinstimmt.

Die möglichen Ergebnisse für jeden Schlüssel sind:

| | |
|---|---|
| OK | Der Vault-Wert ist korrekt |

| | |
|---|---|
| Nicht Aktiviert | Der Wert kann nicht mit der Installation verglichen werden |
| SCHLECHT | Der Wert stimmt nicht mit der Installation überein |
| Fehlt | Ein erwarteter Eintrag fehlt. |

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

#### Interaktiv – Server: Sicherung

Beim Backup wird das Verzeichnis angezeigt, in dem die ZIP-Sicherungsdatei gespeichert werden soll. Das Verzeichnis muss bereits vorhanden sein, und der Dateiname lautet ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

#### Interactive - Server: Anmeldung

Die Anmeldeaktion wird verwendet, um einen Benutzer zu authentifizieren und Zugriff auf Vorgänge zu erhalten, die die Installation ändern. Der Benutzer muss über Admin-Privileges verfügen. Bei der Ausführung mit dem Server kann jeder Admin-Benutzer verwendet werden; bei der Ausführung im direkten Modus muss der Benutzer ein lokaler Benutzer und kein LDAP-Benutzer sein.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

Oder

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Wenn das Passwort korrekt ist und der Benutzer ein Admin-Benutzer ist, wird das Menü eingeschränkt angezeigt.

Wenn das Passwort falsch ist, wird Folgendes angezeigt:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Wenn der Benutzer kein Administrator ist, wird Folgendes angezeigt:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

#### Interactive - Server: Eingeschränktes Menü

Sobald sich der Benutzer angemeldet hat, zeigt das Tool das eingeschränkte Menü an.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

#### Interactive - Server: Passwort Ändern

Mit der Aktion „Passwort ändern“ können Sie ein Installationspasswort in einen neuen Wert ändern.

„Kennwort ändern“ fordert den Benutzer zuerst auf, das zu ändernde Kennwort auszuwählen.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Wenn der Benutzer ein MySQL-Benutzer ist, wird der Benutzer nach der Auswahl des zu korrigenden Eintrags gefragt, ob er das Passwort stark hashing

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Anschließend wird der Benutzer zur Eingabe des neuen Passworts aufgefordert.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Wenn ein nicht leeres Passwort eingegeben wird, wird der Benutzer aufgefordert, das Passwort zu bestätigen.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Wenn die Änderung nicht erfolgreich war, wird der Fehler oder die Ausnahme angezeigt.

#### Interaktiv – Server: Wiederherstellen

#### Interactive - Server: Ändern Sie Die Verschlüsselungsschlüssel

Die Aktion Verschlüsselungsschlüssel ändern ersetzt den Verschlüsselungsschlüssel, der zum Verschlüsseln der Vault-Einträge verwendet wird, und ersetzt den Verschlüsselungsschlüssel, der für den Verschlüsselungsdienst des Tresors verwendet wird. Da der Schlüssel des Verschlüsselungsdienstes geändert wird, werden verschlüsselte Werte in der Datenbank erneut verschlüsselt; sie werden gelesen, mit dem aktuellen Schlüssel entschlüsselt, mit dem neuen Schlüssel verschlüsselt und in der Datenbank gespeichert.

Diese Aktion wird im direkten Modus nicht unterstützt, da der Server für einige Datenbankinhalte die erneute Verschlüsselung bereitstellt.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

#### Interactive - Server: Installation Beheben

Mit der Aktion Installation beheben wird die Installation aktualisiert. Alle Installationspasswörter, die über das securityadmin-Tool außer root geändert werden können, werden auf die Passwörter im Tresor gesetzt.

- Die Passwörter interner OCI-Benutzer werden aktualisiert.
- Die Passwörter von MySQL-Benutzern, mit Ausnahme von root, werden aktualisiert.
- Die Passwörter der Schlüsselspeicher werden aktualisiert.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

Die Aktion wird bei der ersten nicht erfolgreichen Aktualisierung angehalten und zeigt den Fehler oder die Ausnahme an.

#### Sicherheitsmanagement auf dem Insight-Server

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Insight-Server verwalten. Die Sicherheitsverwaltung umfasst das Ändern von Kennwörtern, das Generieren neuer Schlüssel, das Speichern und Wiederherstellen von von von von Ihnen erstellten Sicherheitskonfigurationen oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

##### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

#### Verwaltung der Sicherheit auf der lokalen Erfassungseinheit

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen für den lokalen Akquisitionsbenutzer (LAU) verwalten. Die Sicherheitsverwaltung umfasst das Verwalten von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen von Sicherheitskonfigurationen, die Sie erstellen oder auf die Standardeinstellungen wiederherstellen.

##### Bevor Sie beginnen

Dieser muss unbedingt vorhanden sein `admin` Berechtigungen zum Ausführen von Sicherheitskonfigurationsaufgaben.

##### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

#### Verwaltung der Sicherheit auf einer rau

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf raus verwalten. Möglicherweise müssen Sie eine Vault-Konfiguration sichern oder wiederherstellen, Verschlüsselungsschlüssel ändern oder Kennwörter für die Erfassungseinheiten aktualisieren.

##### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Ein Szenario für die Aktualisierung der Sicherheitskonfiguration für die LAU/rau ist die Aktualisierung des Benutzerpassworts für die Erfassung, wenn das Kennwort für diesen Benutzer auf dem Server geändert wurde. Die LAU und alle raus verwenden das gleiche Passwort wie das des Benutzer „Acquisition“ des Servers, um mit dem Server zu kommunizieren.

Der Benutzer „Acquisition“ ist nur auf dem Insight-Server vorhanden. Die rau oder LAU melden sich als dieser Benutzer an, wenn sie eine Verbindung zum Server herstellen.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

#### Verwaltung der Sicherheit im Data Warehouse

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Data Warehouse-Server verwalten. Die Sicherheitsverwaltung umfasst die Aktualisierung interner Passwörter für interne Benutzer auf dem DWH-Server, das Erstellen von Backups der Sicherheitskonfiguration oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

##### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

#### Ändern der internen OnCommand Insight-Benutzerpasswörter

In Sicherheitsrichtlinien müssen Sie möglicherweise die Passwörter in Ihrer OnCommand Insight-Umgebung ändern. Einige der Passwörter auf einem Server sind auf einem anderen Server in der Umgebung vorhanden, sodass Sie das Passwort auf beiden Servern ändern müssen. Wenn Sie beispielsweise das Benutzerpasswort „`inventar`“ auf dem Insight Server ändern, müssen Sie das Benutzerpasswort „`inventar`“ auf dem für diesen Insight Server konfigurierten Data Warehouse Server Connector zuordnen.

**Bevor Sie beginnen**

Sie sollten die Abhängigkeiten der Benutzerkonten verstehen, bevor Sie Passwörter ändern. Wenn Passwörter nicht auf allen erforderlichen Servern aktualisiert werden, kommt es zu Kommunikationsfehlern zwischen den Insight-Komponenten.

**Über diese Aufgabe**

In der folgenden Tabelle sind die internen Benutzerpasswörter für den Insight Server aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Passwort übereinstimmen müssen.

| Passwörter Für Insight Server | Erforderliche Änderungen |
|---|---|
| _Intern | |
| Akquisition | LAU, RAU |
| dwh_intern | Data Warehouse |
| Hosts | |
| Inventar | Data Warehouse |
| Stamm | |

In der folgenden Tabelle sind die internen Benutzerkennwörter für das Data Warehouse und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Kennwort übereinstimmen müssen.

| Data Warehouse-Passwörter | Erforderliche Änderungen |
|---|---|
| cognos_admin | |
| dwh | |
| dwh_Internal (geändert mit der Server Connector-Konfigurationsoberfläche) | Insight Server |
| Whuser | |
| Hosts | |
| Inventarisierung (geändert mit der Server Connector-Konfigurationsoberfläche) | Insight Server |
| Stamm | |

### Ändern von Kennwörtern in der DWH Server Connection Configuration UI

In der folgenden Tabelle ist das Benutzerpasswort für DIE LAU aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern, die mit dem neuen Passwort übereinstimmen müssen.

| LAU-Passwörter | Erforderliche Änderungen |
|---|---|
| Akquisition | Insight Server, rau |

#### Ändern der Passwörter „inventar“ und „dwh_internal“ mithilfe der Benutzeroberfläche für die Serververbindungskonfiguration

Wenn Sie die Passwörter „`inventar`“ oder „`dwh_internal`“ so ändern müssen, dass sie mit denen auf dem Insight-Server übereinstimmen, verwenden Sie die Data Warehouse-Benutzeroberfläche.

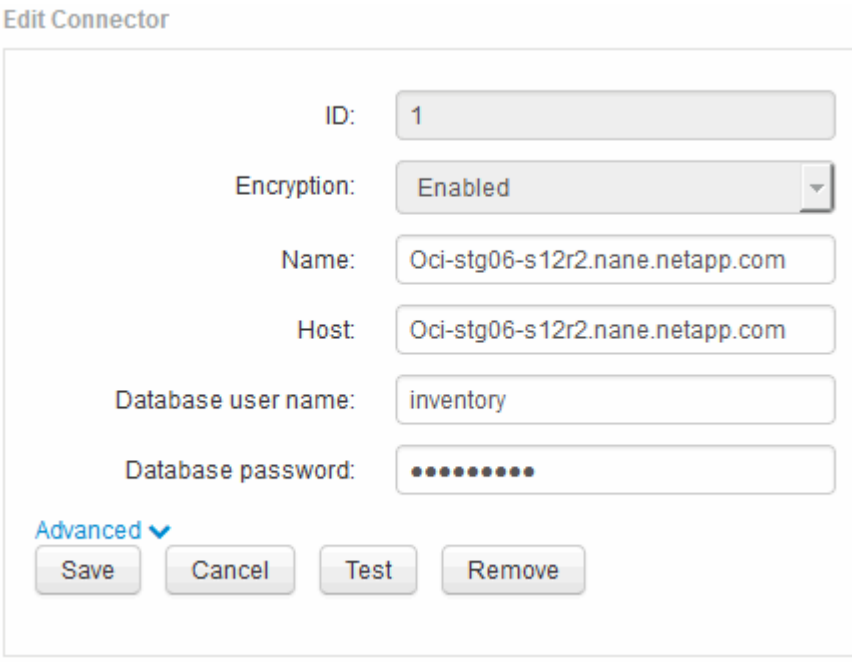
### Bevor Sie beginnen

Sie müssen als Administrator angemeldet sein, um diese Aufgabe ausführen zu können.

### Schritte

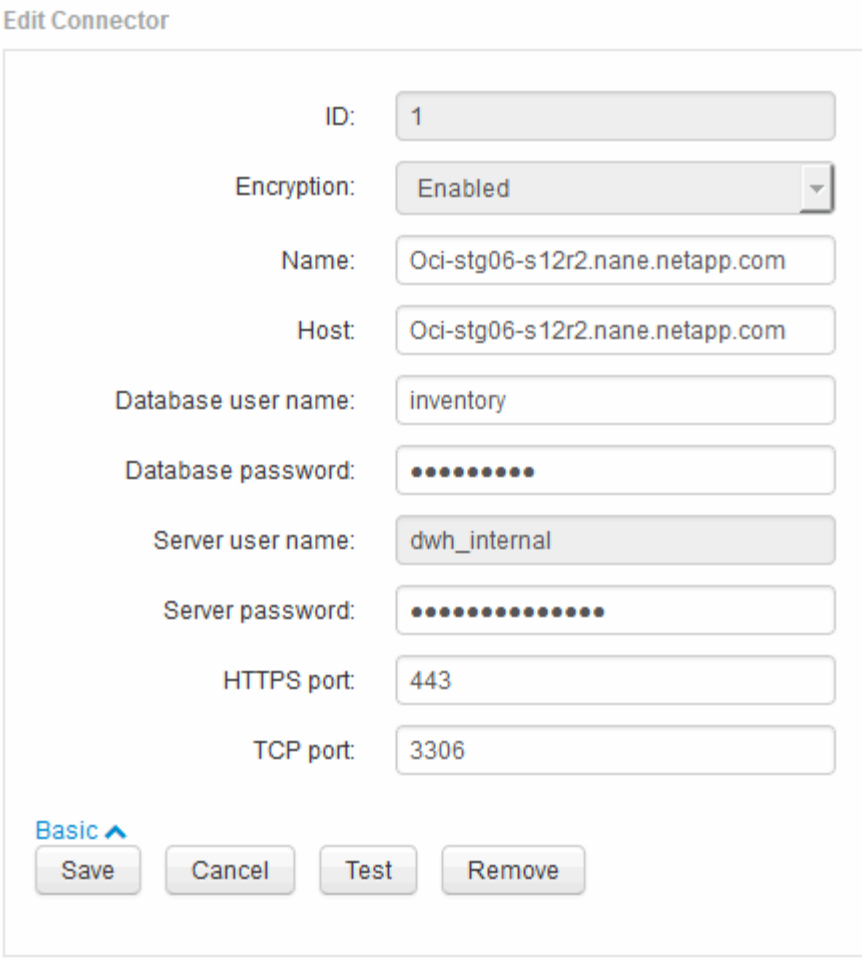
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   Der Bildschirm **Connector bearbeiten** wird angezeigt.




3. Geben Sie ein neues „`Inventory`“-Passwort für das Feld **Datenbankkennwort** ein.
4. Klicken Sie Auf **Speichern**
5. Um das Passwort „`dwh_internal`“ zu ändern, klicken Sie auf **Erweitert.**

   Der Bildschirm Edit Connector Advanced wird angezeigt.




6. Geben Sie das neue Passwort in das Feld **Server-Passwort** ein:
7. Klicken Sie auf Speichern.

#### Ändern des dwh-Kennworts mit dem ODBC-Verwaltungstool

Wenn Sie das Passwort für den dwh-Benutzer auf dem Insight-Server ändern, muss das Passwort auch auf dem Data Warehouse-Server geändert werden. Sie verwenden das ODBC-Datenquellenadministrator-Tool, um das Kennwort im Data Warehouse zu ändern.

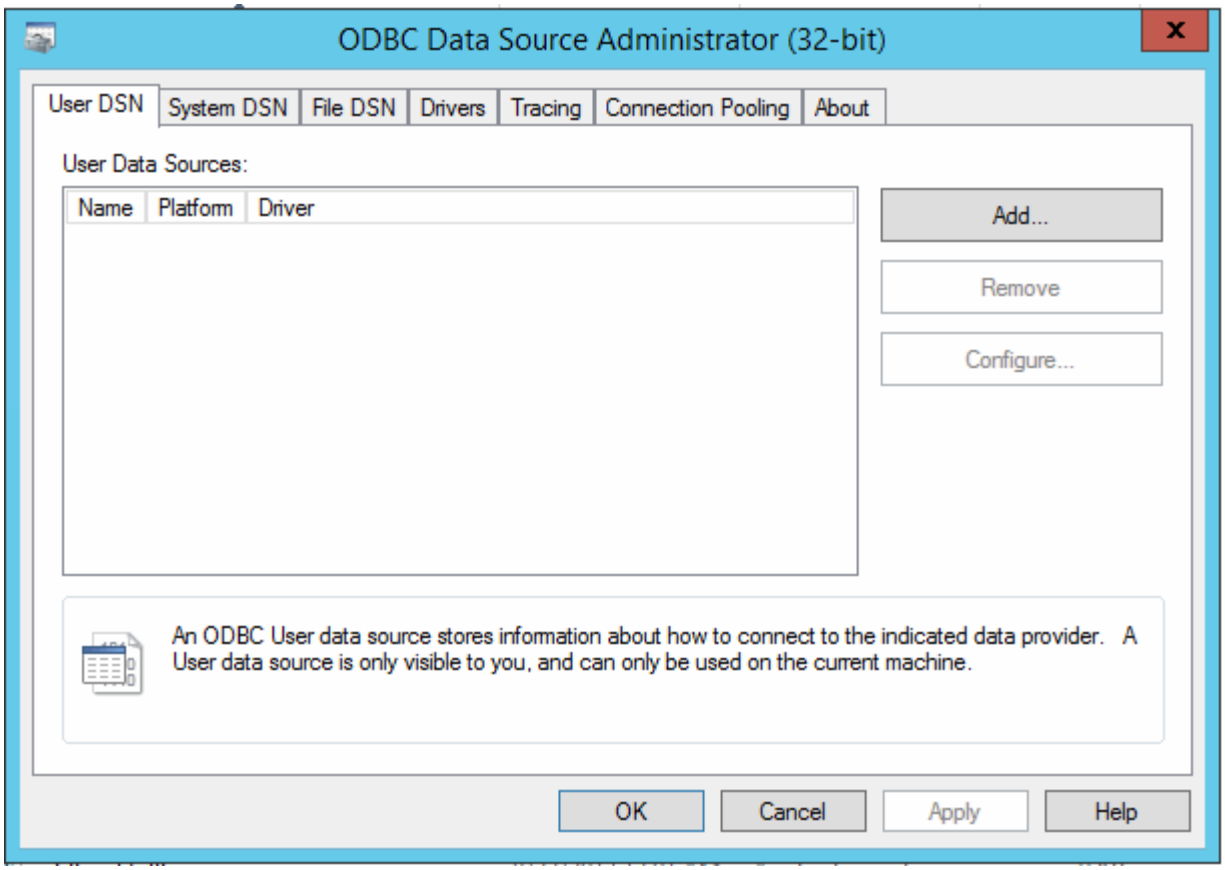
#### Bevor Sie beginnen

Sie müssen eine Remote-Anmeldung beim Data Warehouse-Server mit einem Konto mit Administratorrechten durchführen.

#### Schritte

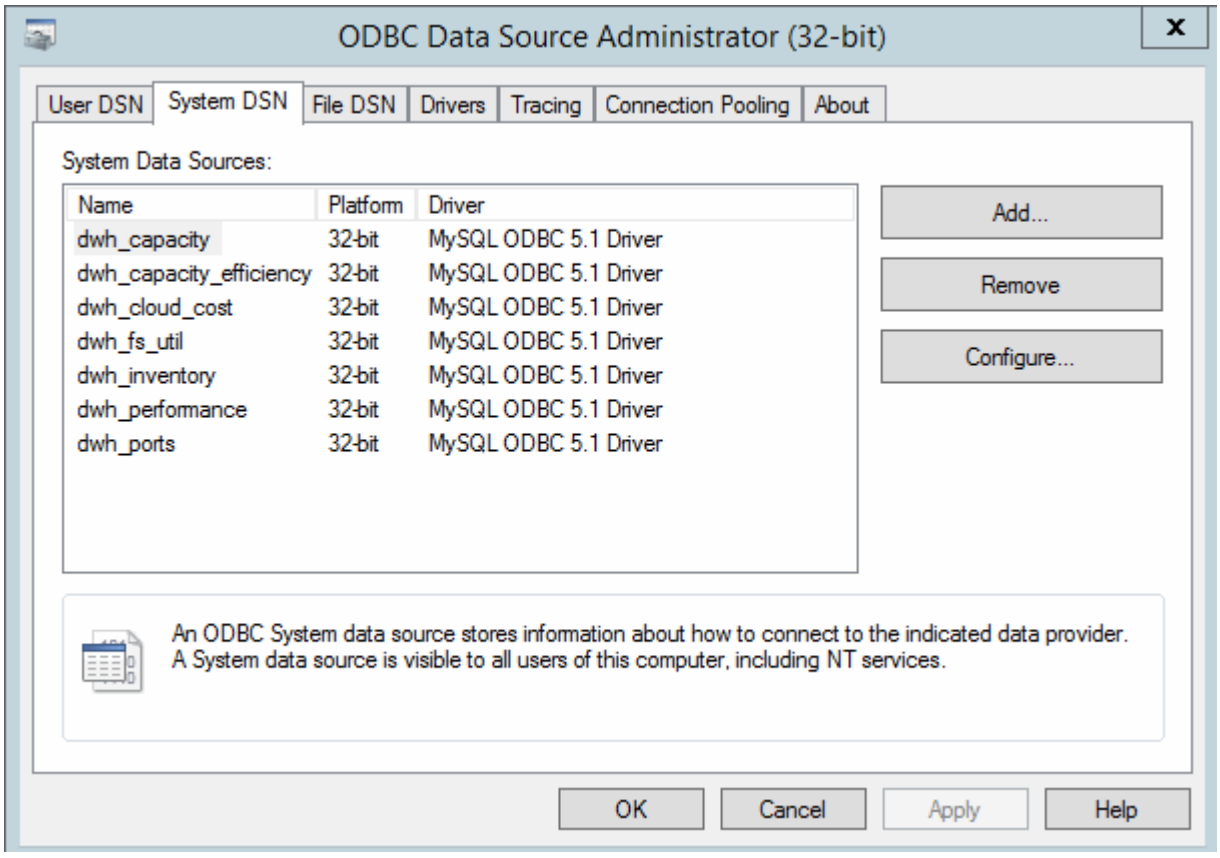
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

   Das System zeigt den ODBC-Bildschirm „Data Source Administrator“ an.



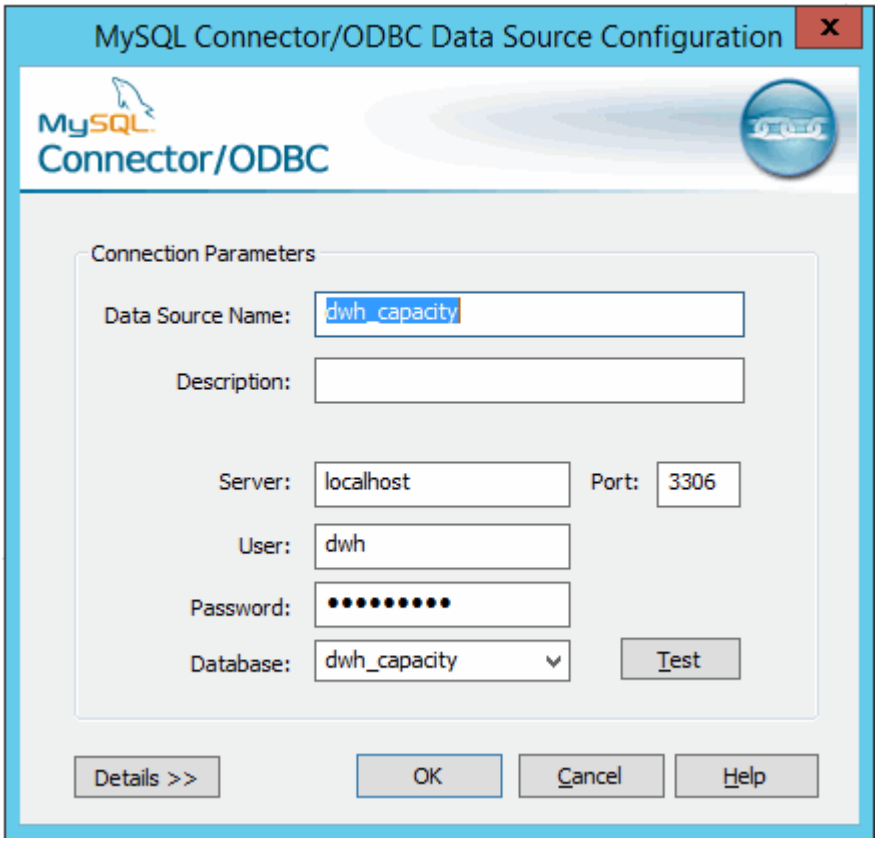

3. Klicken Sie auf **System DSN**

   Die Systemdatenquellen werden angezeigt.



4. Wählen Sie eine OnCommand Insight-Datenquelle aus der Liste aus.
5. Klicken Sie Auf **Konfigurieren**

   Der Bildschirm „Konfiguration der Datenquelle“ wird angezeigt.




6. Geben Sie das neue Passwort in das Feld **Passwort** ein.

## Unterstützung für Smart Card- und Zertifikatanmeldung

OnCommand Insight unterstützt die Verwendung von Smart Cards (CAC) und Zertifikaten zur Authentifizierung von Benutzern, die sich bei den Insight-Servern anmelden. Sie müssen das System konfigurieren, um diese Funktionen zu aktivieren.

Nach der Konfiguration des Systems zur Unterstützung von CAC und Zertifikaten führt das Navigieren zu einer neuen Sitzung von OnCommand Insight im Browser zu einem systemeigenen Dialogfeld, in dem dem der Benutzer eine Liste mit persönlichen Zertifikaten zur Auswahl hat. Diese Zertifikate werden basierend auf den persönlichen Zertifikaten gefiltert, die von CAS ausgestellt wurden, denen der OnCommand Insight-Server vertraut ist. Meistens gibt es eine einzige Wahl. Standardmäßig überspringt Internet Explorer dieses Dialogfeld, wenn nur eine Option vorhanden ist.

Für CAC-Benutzer enthalten Smartcards mehrere Zertifikate, von denen nur eines mit der vertrauenswürdigen Zertifizierungsstelle übereinstimmen kann. Das CAC-Zertifikat für `identification` Sollte verwendet werden.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

### Konfigurieren von Hosts für die Smart Card- und Zertifikatanmeldung

Sie müssen Änderungen an der OnCommand Insight-Hostkonfiguration vornehmen, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

#### Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die ID eines Benutzers enthält.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

#### Schritte

1. Verwenden Sie die `regedit` Dienstprogramm zum Ändern von Registrierungswerten in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Ändern Sie die Option JVM_ `DclientAuth=false` Bis `DclientAuth=true.`

2. Backup der Keystore-Datei: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Öffnen Sie eine Eingabeaufforderung mit der Angabe `Run as administrator`
4. Löschen Sie das selbstgenerierte Zertifikat: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Neues Zertifikat generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Zertifikatsignierungsanforderung (CSR) generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Nachdem die CSR in Schritt 6 zurückgegeben wurde, importieren Sie das Zertifikat, exportieren Sie das Zertifikat im Base-64-Format und legen Sie es in ein `"C:\temp" named servername.cer`.
8. Extrahieren Sie das Zertifikat aus dem Schlüsselspeicher:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extrahieren Sie einen privaten Schlüssel aus der p12-Datei: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Führen Sie das in Schritt 7 exportierte Base-64-Zertifikat mit dem privaten Schlüssel zusammen: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importieren Sie das zusammengeführte Zertifikat in den Schlüsselspeicher: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importieren Sie das Stammzertifikat: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importieren Sie das Stammzertifikat in den Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Zwischenzertifikat importieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file`

```
"C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"
```

Wiederholen Sie diesen Schritt für alle Zwischenzertifikate.

15. Geben Sie die Domäne in LDAP an, die diesem Beispiel entspricht.
16. Starten Sie den Server neu.

### Konfigurieren eines Clients zur Unterstützung der Smart Card- und Zertifikatanmeldung

Client-Rechner erfordern Middleware und Änderungen an Browsern, um die Verwendung von Smart Cards und die Zertifikatanmeldung zu ermöglichen. Kunden, die bereits Smart Cards verwenden, sollten keine zusätzlichen Änderungen an ihren Client-Computern benötigen.

#### Bevor Sie beginnen

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

#### Über diese Aufgabe

Die folgenden allgemeinen Anforderungen an die Client-Konfiguration:

- Installieren von Smart Card Middleware, z. B. ActivClient (siehe
- Ändern des IE-Browsers (siehe
- Ändern des Firefox-Browsers (siehe

### Aktivieren von CAC auf einem Linux-Server

Einige Änderungen sind erforderlich, um CAC auf einem Linux OnCommand Insight-Server zu aktivieren.

Die Stammzertifizierungsstelle muss in den Truststore importiert werden.

#### Schritte

1. Navigieren Sie zu `/opt/netapp/oci/conf/`
2. Bearbeiten `wildfly.properties` Und ändern Sie den Wert von `CLIENT_AUTH_ENABLED` Zu „wahr“

3. Importieren Sie das „`root Certificate`“, das unter vorhanden ist `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Starten Sie den Server neu

#### Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung

## Sie müssen die OnCommand Insight-Data-Warehouse-Konfiguration ändern, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

##### Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die Regierungs-ID-Nummer eines Benutzers enthält.

  Der auf staatlich ausgestellten CACs gespeicherte allgemeine Name (CN) wird normalerweise im folgenden Format gespeichert: `first.last.ID`. Für einige LDAP-Felder, z. B. `sAMAccountName`Dieses Format ist zu lang. Für diese Felder extrahiert OnCommand Insight nur die ID-Nummer aus dem CNS.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

##### Schritte

1. Verwenden Sie regedit, um Registrierungswerte in zu ändern `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Ändern Sie die Option JVM_ `-DclientAuth=false` Bis `-DclientAuth=true`.

   Ändern Sie für Linux die `clientAuth` Parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Zertifizierungsstellen (CAS) zum Data Warehouse trustore hinzufügen:

a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\wildfly\standalone\configuration`.

b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + in der Dokumentation finden Sie "Sicherheitsadministration"weitere Informationen zum Festlegen oder Ändern des Passworts für Server_trustore.

   Das erste Wort in jeder Zeile gibt den CA-Alias an.

c. Geben Sie bei Bedarf eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei: Um die CAS des Kunden mit vertrauenswürdigen Data Warehouse-CAS aufzunehmen, gehen Sie zu `..\SANscreen\wildfly\standalone\configuration` Und verwenden Sie die `keytool` Importbefehl: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   My_alias ist normalerweise ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.

3. Auf dem OnCommand Insight-Server wird die angezeigt `wildfly/standalone/configuration/standalone-full.xml` Die Datei muss durch Aktualisierung von verify-Client auf „ANGEFORDERT“ in geändert werden `/subsystem=undertow/server=default-server/https-listener=default-https`Um CAC zu aktivieren. Melden Sie sich beim Insight-Server an, und führen Sie den entsprechenden Befehl aus:

| BETRIEBSSYSTEM | Skript |
| --- | --- |
| Windows | <install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat |
| Linux | /Opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh |

   Warten Sie nach der Ausführung des Skripts, bis der Neustart des wildfly-Servers abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren.

4. Starten Sie den OnCommand Insight-Server neu.

### Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher)

Sie müssen die Konfiguration des OnCommand Insight Data Warehouse ändern, um Smart Card- (CAC) und Zertifikatanmeldungen für den Cognos-Server zu unterstützen.

#### Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

**Schritte**

1. Fügen Sie dem Cognos trustore Zertifizierungsstellen (CAS) hinzu.
   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `..\..\ ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      Das erste Wort in jeder Zeile gibt den CA-Alias an.
   c. Wenn keine geeigneten Dateien vorhanden sind, geben Sie eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei:
   d. Wenn Sie Zertifizierungsstellen des Kunden mit vertrauenswürdigen Zertifizierungsstellen von OnCommand Insight einbeziehen möchten, besuchen Sie `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Verwenden Sie die `keytool` Dienstprogramm zum Importieren des `.pem` Datei: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Ist in der Regel ein Alias, der die CA in der Operation leicht identifizieren würde`keytool -list`.
   f. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat* ein.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Gehen Sie wie folgt vor, um den CAC-Modus zu aktivieren:
   a. Konfigurieren Sie die CAC-Abmeldeseite mit den folgenden Schritten:
      - Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
      - (Nur für 7.3.10 und 7.3.11) Klicken Sie auf Verwalten -> Konfiguration -> System -> Sicherheit
      - (Nur für 7.3.10 und 7.3.11) Geben Sie cacLogout.html gegen Abmeldung ein Umleiten Sie die URL -> Anwenden

- Browser schließen.

b. Ausführen `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

3. Gehen Sie wie folgt vor, um den CAC-Modus zu deaktivieren:

a. Ausführen `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

c. (Nur für 7.3.10 und 7.3.11) Unconfigure CAC Logout page, mit den folgenden Schritten:

- Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
- Klicken Sie Auf Verwalten -> Konfiguration -> System -> Sicherheit
- Geben Sie cacLogout.html für die URL zur Umleitung von Abmeldung ein -> Anwenden
- Browser schließen.

#### Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher)

Sie können SSL-Zertifikate hinzufügen, um eine erweiterte Authentifizierung und Verschlüsselung für Ihre Data Warehouse- und Cognos-Umgebung zu ermöglichen.

##### Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

##### Über diese Aufgabe

Sie müssen über Administratorrechte verfügen, um dieses Verfahren durchführen zu können.

##### Schritte

1. Beenden Sie Cognos mit dem IBM Cognos Configuration Tool. Schließen Sie Cognos.
2. Erstellen Sie Backups des `..\SANScreen\cognos\analytics\configuration` Und `..\SANScreen\cognos\analytics\temp\cam\freshness` Ordner.

3. Erstellen Sie eine Zertifikatsverschlüsselungsanforderung von Cognos. Führen Sie in einem Admin-CMD-Fenster Folgendes aus:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Anmerkung: Hier sollen -H und -i subjectAltNames wie dns und ipaddress hinzufügen.
   c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Geben Sie den Inhalt von encryptRequest.csr ein, und erstellen Sie das Zertifikat mithilfe des CA-Signing-Portals.
6. Laden Sie die Kettenzertifikate unter Einbeziehung des Stammzertifikats im PKCS7-Format herunter

   Dadurch wird die Datei fqdn.p7b heruntergeladen
7. Holen Sie sich ein Zertifikat im .p7b-Format von Ihrer CA. Verwenden Sie einen Namen, der ihn als Zertifikat für den Cognos-Webserver kennzeichnet.
8. ThirdPartyCertificateTool.bat kann die gesamte Kette nicht importieren, so dass mehrere Schritte erforderlich sind, um alle Zertifikate zu exportieren. Teilen Sie die Kette auf, indem Sie sie einzeln wie folgt exportieren:
   a. Öffnen Sie das .p7b-Zertifikat unter „`Crypto Shell Extensions`“.
   b. Navigieren Sie im linken Fensterbereich zu „`Zertifikate`“.
   c. Klicken Sie mit der rechten Maustaste auf Stammzertifizierungsstelle > Alle Aufgaben > Exportieren.
   d. Wählen Sie Base64-Ausgabe.
   e. Geben Sie einen Dateinamen ein, der ihn als Stammzertifikat identifiziert.
   f. Wiederholen Sie die Schritte 8a bis 8e, um alle Zertifikate separat in .cer-Dateien zu exportieren.
   g. Benennen Sie die Dateien intermediateX.cer und cognos.cer.
9. Ignorieren Sie diesen Schritt, wenn Sie nur ein CA-Zertifikat haben, andernfalls fügen Sie root.cer und intermediateX.cer in eine Datei zusammen.
   a. Öffnen Sie root.cer mit Notepad und kopieren Sie den Inhalt.
   b. Öffnen Sie intermediate.cer mit Notepad und fügen Sie den Inhalt von 9a an (intermediate first und root next).
   c. Speichern Sie die Datei unter Chain.cer.
10. Importieren Sie die Zertifikate in den Cognos-Keystore mithilfe der Admin-CMD-Eingabeaufforderung:
    a. cd „`Program Files\sanscreen\cognos\Analytics\bin`“
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\Chain.cer
11. Öffnen Sie die IBM Cognos-Konfiguration.
    a. Wählen Sie Lokale Konfiguration-→ Sicherheit -→ Kryptographie -→ Cognos
    b. „`Drittanbieter-CA verwenden?`“ ändern Nach wahr.

c. Speichern Sie die Konfiguration.

d. Cognos Neu Starten

12. Exportieren Sie das neueste Cognos-Zertifikat in cognos.crt mithilfe der Admin CMD-Eingabeaufforderung:

    a. cd „`C:\Program Files\SANscreen“

    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\Analytics\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias -Verschlüsselung

    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.

13. Sichern Sie den DWH-Server trustore unter`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Importieren Sie „`c:\temp\cognos.crt`“ in DWH trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.

    a. cd „`C:\Program Files\SANscreen“

    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\Standalone\Configuration\Server.trustore -storepass <password> -alias cognos3rdca

    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.

15. Starten Sie den SANscreen-Dienst neu.

16. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

17. Die folgenden Schritte sollten auch dann durchgeführt werden, wenn nur das “ssl-Zertifikat” geändert wird und die Standard-Cognos-Zertifikate unverändert bleiben. Andernfalls kann Cognos sich über das neue SANscreen-Zertifikat beschweren oder keine DWH-Sicherung erstellen.

    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass <password> -alias “ssl certificate”`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    Diese Schritte werden normalerweise im Rahmen des in beschriebenen Cognos-Zertifikatimportprozesses ausgeführt "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

## SSL-Zertifikate werden importiert

Sie können SSL-Zertifikate hinzufügen, um die erweiterte Authentifizierung und Verschlüsselung zu aktivieren und so die Sicherheit Ihrer OnCommand Insight-Umgebung zu erhöhen.

### Bevor Sie beginnen

Sie müssen sicherstellen, dass Ihr System die erforderliche Mindestbitebene (1024 Bit) erfüllt.

### Über diese Aufgabe

Es wird dringend empfohlen, den Tresor vor dem Upgrade zu sichern.

Weitere Informationen zum Tresor- und Passwortmanagement finden "Sicherheitstool"Sie in den Anweisungen.

### Schritte

1. Erstellen Sie eine Kopie der ursprünglichen Keystore-Datei: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Listen Sie den Inhalt des Keystore auf: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Das System zeigt den Inhalt des Keystore an. Es sollte mindestens ein Zertifikat im Schlüsselspeicher vorhanden sein, `"ssl certificate"`.

3. Löschen Sie die `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Einen neuen Schlüssel generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Wenn Sie nach vor- und Nachnamen gefragt werden, geben Sie den vollständig qualifizierten Domänennamen (FQDN) ein, den Sie verwenden möchten.
   b. Geben Sie die folgenden Informationen zu Ihrer Organisation und Organisationsstruktur an:
      - Land: Zweistellige ISO-Abkürzung für Ihr Land (z. B. USA)
      - Bundesland oder Provinz: Name des Bundesstaates oder der Provinz, in dem sich der Hauptsitz Ihres Unternehmens befindet (z. B. Massachusetts)
      - Ort: Name der Stadt, in der sich der Hauptsitz Ihrer Organisation befindet (z. B. Waltham)
      - Name des Unternehmens: Name des Unternehmens, dem der Domain-Name gehört (z. B. NetApp)
      - Name der Organisationseinheit: Name der Abteilung oder Gruppe, die das Zertifikat verwenden soll (z. B. Support)
      - Domänenname/ Allgemeiner Name: Der FQDN, der für DNS-Suchen Ihres Servers verwendet wird (z. B. www.example.com). Das System antwortet mit Informationen wie den folgenden: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Eingabe `Yes` Wenn der allgemeine Name (CN) gleich dem FQDN ist.
   d. Wenn Sie zur Eingabe des Schlüsselpassworts aufgefordert werden, geben Sie das Kennwort ein, oder drücken Sie die Eingabetaste, um das vorhandene Schlüsselspeicher-Passwort zu verwenden.
5. Erstellen Sie eine Zertifikatanforderungsdatei: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file`

`c:\localhost.csr`

Der `c:\localhost.csr` Die Datei ist die neu generierte Zertifikatanforderungsdatei.

6. Senden Sie die `c:\localhost.csr` Bei der Zertifizierungsstelle zur Genehmigung einreichen.

   Nachdem die Zertifikatanforderungsdatei genehmigt wurde, möchten Sie das Zertifikat in zurücksenden `.der` Formatieren. Die Datei wird möglicherweise als zurückgegeben `.der` Datei: Das Standarddateiformat ist `.cer` Für Microsoft CA-Services.

   Die CAS der meisten Unternehmen verwenden ein Vertrauensstellungsmodell, einschließlich einer Stammzertifizierungsstelle, die häufig offline ist. Es hat die Zertifikate für nur wenige untergeordnete CAS, bekannt als intermediate CAS, unterzeichnet.

   Sie müssen den öffentlichen Schlüssel (Zertifikate) für die gesamte Vertrauenskette erhalten – das Zertifikat für die Zertifizierungsstelle, die das Zertifikat für den OnCommand Insight-Server signiert hat, und alle Zertifikate zwischen dieser Zertifizierungsstelle bis hin zur Unternehmensstammzertifizierungsstelle.

   Wenn Sie in einigen Unternehmen eine Signaturanfrage einreichen, erhalten Sie möglicherweise eine der folgenden Informationen:

   - Eine PKCS12-Datei, die Ihr signiertes Zertifikat und alle öffentlichen Zertifikate in der Vertrauenskette enthält
   - A `.zip` Datei, die einzelne Dateien (einschließlich Ihres signierten Zertifikats) und alle öffentlichen Zertifikate in der Vertrauenskette enthält
   - Nur Ihr signiertes Zertifikat

     Sie müssen die öffentlichen Zertifikate erhalten.

7. Importieren Sie das genehmigte Zertifikat für Server.keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für den Keystore ein.

      Die folgende Meldung wird angezeigt: `Certificate reply was installed in keystore`

8. Importieren Sie das genehmigte Zertifikat für den Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. Geben Sie bei Aufforderung das trustore-Passwort ein.

      Die folgende Meldung wird angezeigt: `Certificate reply was installed in trustore`

9. Bearbeiten Sie das `SANscreen\wildfly\standalone\configuration\standalone-full.xml` Datei:

   Ersetzen Sie die folgende Alias-Zeichenfolge: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Beispiel:

   ```
   <keystore path="server.keystore" relative-to="jboss.server.config.dir"
   ```

```
keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
02.muccbc.hq.netapp.com" key-
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. Starten Sie den SANscreen-Serverdienst neu.

    Sobald Insight ausgeführt wird, können Sie auf das Vorhängeschloss-Symbol klicken, um die auf dem System installierten Zertifikate anzuzeigen.

    Wenn ein Zertifikat mit Informationen „ausgestellt an“ angezeigt wird, die mit den Informationen „ausgestellt von“ übereinstimmen, ist weiterhin ein selbstsigniertes Zertifikat installiert. Selbstsignierte Insight Zertifikate, die vom Insight Installer generiert werden, laufen 100 Jahre ab.

    NetApp kann nicht garantieren, dass dieses Verfahren Warnungen zu digitalen Zertifikaten entfernt. NetApp kann nicht steuern, wie Ihre Endbenutzer-Workstations konfiguriert sind. Betrachten Sie die folgenden Szenarien:

    - Microsoft Internet Explorer und Google Chrome verwenden beide Microsoft-native Zertifikatfunktionalität auf Windows.

      Das bedeutet, dass wenn Ihre Active Directory-Administratoren die CA-Zertifikate Ihres Unternehmens in die Zertifikattrustores des Endbenutzers übertragen, die Benutzer dieser Browser die Zertifikatwarnungen verschwinden sehen, wenn die selbstsignierten OnCommand Insight-Zertifikate durch die Zertifikate ersetzt wurden, die von der internen CA-Infrastruktur signiert wurden.

    - Java und Mozilla Firefox haben ihre eigenen Zertifikatsspeicher.

      Wenn Ihre Systemadministratoren das Einspielen der CA-Zertifikate in die vertrauenswürdigen Zertifikatsspeicher dieser Anwendungen nicht automatisieren, kann die Verwendung des Firefox-Browsers weiterhin Zertifikatwarnungen aufgrund eines nicht vertrauenswürdigen Zertifikats generieren, selbst wenn das selbstsignierte Zertifikat ersetzt wurde. Eine zusätzliche Anforderung ist, die Zertifikatskette Ihres Unternehmens in den trustore zu installieren.

## Einrichtung wöchentlicher Backups für Ihre Insight-Datenbank

Möglicherweise möchten Sie zur Sicherung Ihrer Daten automatische wöchentliche Backups für Ihre Insight-Datenbank einrichten. Diese automatischen Backups überschreiben die Dateien im angegebenen Sicherungsverzeichnis.

### Über diese Aufgabe

**Best Practice**: Wenn Sie das wöchentliche Backup der OCI-Datenbank einrichten, müssen Sie die Backups auf einem anderen Server als Insight speichern, falls der Server ausfällt. Speichern Sie keine manuellen Backups im wöchentlichen Backup-Verzeichnis, da jedes wöchentliche Backup die Dateien im Verzeichnis überschreibt.

Die Sicherungsdatei enthält Folgendes:

- Bestandsdaten
- Leistungsdaten von bis zu 7 Tagen

### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** > **Setup**.
2. Klicken Sie auf die Registerkarte **Backup & Archive**.
3. Wählen Sie im Abschnitt wöchentliches Backup **wöchentliches Backup aktivieren** aus.
4. Geben Sie den Pfad zum **Backup-Speicherort** ein. Dies kann auf dem lokalen Insight-Server oder auf einem Remote-Server erfolgen, auf den über den Insight-Server zugegriffen werden kann.

> Die Backup-Speicherort-Einstellung ist im Backup selbst enthalten. Wenn Sie das Backup auf einem anderen System wiederherstellen, beachten Sie, dass der Speicherort des Backup-Ordners auf dem neuen System möglicherweise ungültig ist. Überprüfen Sie nach dem Wiederherstellen einer Sicherung die Einstellungen des Sicherungsstandorts.

5. Wählen Sie die Option **Cleanup**, um entweder die letzten zwei oder die letzten fünf Backups beizubehalten.
6. Klicken Sie Auf **Speichern**.

### Ergebnisse

Sie können auch unter **Admin** > **Troubleshooting** ein On-Demand-Backup erstellen.

### Im Backup enthaltene Funktionen

Wöchentliche und On-Demand-Backups können zur Fehlerbehebung oder Migration verwendet werden.

Das wöchentliche oder On-Demand Backup beinhaltet Folgendes:

- Bestandsdaten
- Performance-Daten (wenn für die Aufnahme in das Backup ausgewählt)
- Datenquellen und Einstellungen der Datenquelle
- Integrationspakete
- Fernbedienungseinheiten
- ASUP/Proxy-Einstellungen
- Einstellungen für den Speicherort der Sicherung
- Einstellungen für den Archivspeicherort
- Benachrichtigungseinstellungen
- Benutzer
- Performance-Richtlinien
- Geschäftseinheiten und Applikationen
- Regeln und Einstellungen für die Geräteauflösung
- Dashboards und Widgets
- Dashboards und Widgets für die Asset-Seite
- Abfragen

- Anmerkungen und Anmerkungsregeln

Die wöchentliche Sicherung beinhaltet nicht:

- Einstellungen des Sicherheitstools/Vault-Informationen (gesichert über separaten CLI-Prozess)
- Protokolle (können bei Bedarf in einer ZIP-Datei gespeichert werden)
- Performance-Daten (wenn nicht für die Aufnahme in das Backup ausgewählt)
- Lizenzen Zu Haben

Wenn Sie Performance-Daten in das Backup aufnehmen möchten, werden die Daten der letzten sieben Tage gesichert. Die übrigen Daten befinden sich im Archiv, wenn diese Funktion aktiviert ist.

## Archivierung von Performance-Daten

Mit OnCommand Insight 7.3 können Performance-Daten täglich archiviert werden. Dies ergänzt Konfigurations- und Performance-Daten-Backups.

OnCommand Insight speichert bis zu 90 Tage Daten zu Performance- und Verstößen. Beim Erstellen einer Sicherung dieser Daten werden jedoch nur die neuesten Informationen in das Backup aufgenommen. Durch die Archivierung können Sie die übrigen Performance-Daten speichern und nach Bedarf laden.

Sobald der Archivspeicherort konfiguriert und die Archivierung aktiviert ist, archiviert Insight einmal am Tag die Leistungsdaten des Vortages für alle Objekte im Archivspeicherort. Das Archiv eines jeden Tages wird im Archivordner in einer separaten Datei aufbewahrt. Die Archivierung findet im Hintergrund statt und wird fortgesetzt, solange Insight ausgeführt wird.

Die Archive der letzten 90 Tage werden aufbewahrt. Archivdateien, die älter als 90 Tage sind, werden gelöscht, wenn neuere Archive erstellt werden.

#### Performance-Archivierung

Führen Sie die folgenden Schritte aus, um die Archivierung von Performance-Daten zu aktivieren.

##### Schritte

1. Klicken Sie in der Symbolleiste auf **Admin** > **Setup**.
2. Wählen Sie die Registerkarte **Backup & Archive** aus.
3. Im Abschnitt Leistungsarchiv sicherstellen, dass**enable Performance Archive** geprüft wird.
4. Geben Sie einen gültigen Archivspeicherort an.

   Sie können keinen Ordner im Insight-Installationsordner angeben.

   Best Practice: Geben Sie nicht denselben Ordner für das Archiv an wie den Speicherort für das Insight-Backup.

5. Klicken Sie Auf **Speichern**.

   Der Archivierungsprozess wird im Hintergrund verarbeitet und beeinträchtigt nicht andere Insight-Aktivitäten.

#### Performance-Archiv wird geladen

Führen Sie zum Laden des Performance-Datenarchivs die folgenden Schritte aus.

##### Bevor Sie beginnen

Vor dem Laden des Performance-Datenarchivs müssen Sie eine gültige wöchentliche oder manuelle Sicherung wiederherstellen.

##### Schritte

1. Klicken Sie in der Symbolleiste auf **Admin** > **Fehlerbehebung**.
2. Klicken Sie im Abschnitt Wiederherstellen unter **Load Performance Archive** auf **Load**.

> Das Laden des Archivs erfolgt im Hintergrund. Das vollständige Archiv kann sehr lange geladen werden, da die archivierten Performance-Daten der einzelnen Tage in Insight eingetragen sind. Der Status des Archivladens wird im Archiv-Bereich dieser Seite angezeigt.

## Konfigurieren Ihrer E-Mail-Adresse

Sie müssen OnCommand Insight für den Zugriff auf Ihr E-Mail-System konfigurieren, damit dieOnCommand Insight Server Ihre E-Mail-Adresse verwenden kann, um Berichte, die Sie abonnieren, bereitzustellen und Support-Informationen zur Fehlerbehebung an den technischen Support von NetApp zu übermitteln.

#### Voraussetzungen für die E-Mail-Konfiguration

Bevor Sie OnCommand Insight für den Zugriff auf Ihr E-Mail-System konfigurieren können, müssen Sie den Hostnamen oder die IP-Adresse ermitteln, um den E-Mail-Server (SMTP oder Exchange) zu identifizieren und ein E-Mail-Konto für OnCommand Insight-Berichte zuzuweisen.

Bitten Sie Ihren E-Mail-Administrator, ein E-Mail-Konto für OnCommand Insight zu erstellen. Sie benötigen folgende Informationen:

- Der Hostname oder die IP-Adresse zur Identifizierung des von Ihrer Organisation verwendeten E-Mail-Servers (SMTP oder Exchange). Diese Informationen finden Sie in der Anwendung, mit der Sie Ihre E-Mail lesen. In Microsoft Outlook können Sie beispielsweise den Namen des Servers finden, indem Sie Ihre Kontokonfiguration anzeigen: Tools - E-Mail-Konten - vorhandenes E-Mail-Konto anzeigen oder ändern.
- Name des E-Mail-Kontos, über das OnCommand Insight regelmäßig Berichte versendet. Das Konto muss eine gültige E-Mail-Adresse in Ihrem Unternehmen sein. (Die meisten E-Mail-Systeme senden keine Nachrichten, es sei denn, sie werden von einem gültigen Benutzer gesendet.) Wenn der E-Mail-Server einen Benutzernamen und ein Kennwort zum Senden von E-Mails benötigt, erhalten Sie diese Informationen von Ihrem Systemadministrator.

#### Konfigurieren Ihrer E-Mail-Adresse für Insight

Wenn Ihre Benutzer Insight-Berichte in ihren E-Mail-Konten erhalten möchten, müssen Sie Ihren E-Mail-Server konfigurieren, um diese Funktion zu aktivieren.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Notifications**.
2. Scrollen Sie nach unten zum Abschnitt **E-Mail** der Seite.
3. Geben Sie im Feld **Server** den Namen Ihres SMTP-Servers in Ihrer Organisation ein, der entweder über einen Hostnamen oder eine IP-Adresse (*nnn.nnn.nnn.nnn* Format) identifiziert wird.

   Wenn Sie einen Hostnamen angeben, stellen Sie sicher, dass der Name über DNS aufgelöst werden kann.
4. Geben Sie im Feld **Benutzername** Ihren Benutzernamen ein.
5. Geben Sie im Feld **Passwort** das Passwort für den Zugriff auf den E-Mail-Server ein, das nur erforderlich ist, wenn Ihr SMTP-Server passwortgeschützt ist. Dies ist dasselbe Passwort, das Sie für die Anmeldung bei der Anwendung verwenden, mit der Sie Ihre E-Mail lesen können. Wenn ein Kennwort erforderlich ist, müssen Sie es zur Überprüfung erneut eingeben.
6. Geben Sie im Feld **Absender-E-Mail** das E-Mail-Konto des Absenders ein, das bei allen OnCommand Insight-Berichten als Absender identifiziert wird.

   Dieses Konto muss ein gültiges E-Mail-Konto in Ihrem Unternehmen sein.
7. Geben Sie in das Feld **Email Signature** den Text ein, den Sie in jede gesendete E-Mail einfügen möchten.
8. Klicken Sie im Feld Empfänger auf ✚Geben Sie eine E-Mail-Adresse ein, und klicken Sie auf **OK**.

   Um eine E-Mail-Adresse zu bearbeiten, wählen Sie die Adresse aus, und klicken Sie auf . Um eine E-Mail-Adresse zu löschen, wählen Sie die Adresse aus, und klicken Sie auf ✖.
9. Um eine Test-E-Mail an die angegebenen Empfänger zu senden, klicken Sie auf ✔.
10. Klicken Sie Auf **Speichern**.

## Konfigurieren von SNMP-Benachrichtigungen

OnCommand Insight unterstützt SNMP-Benachrichtigungen bei Änderungen an der Konfiguration und an globalen Pfadrichtlinien sowie bei Verstößen. SNMP-Benachrichtigungen werden beispielsweise gesendet, wenn die Schwellenwerte für die Datenquelle überschritten werden.

**Bevor Sie beginnen**

Folgendes muss abgeschlossen sein:

- Identifizieren der IP-Adresse des Servers, der Traps für jeden Ereignistyp konsolidiert.

  Sie müssen sich eventuell mit Ihrem Systemadministrator in Verbindung setzen, um diese Informationen zu erhalten.
- Identifizieren der Portnummer, über die der designierte Rechner SNMP-Traps für jeden Ereignistyp erhält.

  Der Standardport für SNMP-Traps ist 162.
- Kompilieren der MIB an Ihrem Standort.

  Die proprietäre MIB kommt mit der Installationssoftware zur Unterstützung von OnCommand Insight-Traps. Die NetApp MIB ist mit allen Standard-SNMP-Management-Software kompatibel und ist auf dem Insight

Server in `<install dir>\SANscreen\MIBS\sanscreen.mib`.

**Schritte**

1. Klicken Sie auf **Admin** und wählen Sie **Benachrichtigungen**.
2. Scrollen Sie nach unten zum Abschnitt **SNMP** der Seite.
3. Klicken Sie auf **actions** und wählen Sie **Trap-Quelle hinzufügen**.
4. Geben Sie im Dialogfeld **SNMP-Trap-Empfänger hinzufügen** folgende Werte ein:
   - **IP**

     Die IP-Adresse, an die OnCommand Insight SNMP-Trap-Meldungen sendet.
   - **Port**

     Die Portnummer, an die OnCommand Insight SNMP-Trap-Meldungen sendet.
   - **Community String**

     Verwenden Sie „`public`“ für SNMP-Trap-Nachrichten.
5. Klicken Sie Auf **Speichern**.

## Aktivieren der Syslog-Funktion

Sie können einen Speicherort für das Protokoll der OnCommand Insight Verstöße, Performance-Alarme und Audit-Meldungen ermitteln und den Protokollierungsprozess aktivieren.

**Bevor Sie beginnen**

- Sie müssen über die IP-Adresse des Servers verfügen, auf dem das Systemprotokoll gespeichert werden soll.
- Sie müssen die Einrichtungsebene kennen, die dem Programmtyp entspricht, der die Meldung protokolliert, z. B. LOCAL1 oder BENUTZER.

**Über diese Aufgabe**

Das Syslog enthält die folgenden Informationstypen:

- Meldungen zu Verstößen
- Performance-Warnmeldungen
- Optional: Audit-Protokollmeldungen

Die folgenden Einheiten werden im Syslog verwendet:

- Auslastungsmetriken: Prozentsatz
- Verkehrsmetriken: MB
- Datenverkehrsrate: MB/s

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Notifications**.
2. Scrollen Sie nach unten zum Abschnitt **Syslog** der Seite.
3. Aktivieren Sie das Kontrollkästchen **enable syslog**.
4. Aktivieren Sie bei Bedarf das Kontrollkästchen **Audit senden**. Neue Überwachungsprotokollmeldungen werden zusätzlich zur Anzeige auf der Seite „Audit“ an syslog gesendet. Beachten Sie, dass bereits vorhandene Audit-Log-Meldungen nicht an syslog gesendet werden, sondern nur neu generierte Protokollmeldungen werden gesendet.
5. Geben Sie im Feld **Server** die IP-Adresse des Protokollservers ein.

   Sie können einen benutzerdefinierten Port angeben, indem Sie ihn nach einem Doppelpunkt am Ende der Server-IP anhängen (z. B. Server:Port). Wenn der Port nicht angegeben ist, wird der Standard-Syslog-Port von 514 verwendet.

6. Wählen Sie im Feld **Anlage** die Einrichtungsebene aus, die dem Programmtyp entspricht, der die Nachricht protokolliert.
7. Klicken Sie Auf **Speichern**.

#### Insight Syslog-Inhalte

Sie können ein Syslog auf einem Server aktivieren, um Insight-Verstöße und Performance-Warnmeldungen zu sammeln, die Nutzungs- und Verkehrsdaten enthalten.

##### Nachrichtentypen

Im Insight syslog werden drei Meldungsarten aufgelistet:

- VERSTÖSSE GEGEN SAN-Pfade
- Allgemeine Verstöße
- Performance-Warnmeldungen

##### Daten bereitgestellt

Zu den Beschreibungen der Verstöße zählen die beteiligten Elemente, die Uhrzeit des Ereignisses sowie der relative Schweregrad oder die Priorität des Verstoßes.

Zu den Performance-Warnmeldungen gehören folgende Daten:

- Auslastungswerte
- Verkehrstypen
- Verkehrsrate in MB gemessen

## Konfiguration der Performance und Sicherstellung von Benachrichtigungen über Verstöße

OnCommand Insight unterstützt Benachrichtigungen bei Performance-Verstößen und stellt diese sicher. Standardmäßig sendet Insight keine Benachrichtigungen für diese Verstöße. Sie müssen Insight so konfigurieren, dass E-Mails gesendet, Syslog-

Meldungen an den Syslog-Server gesendet oder SNMP-Benachrichtigungen gesendet werden, wenn eine Verletzung auftritt.

#### Bevor Sie beginnen

Sie müssen E-Mail-, Syslog- und SNMP-Sendemethoden für Verstöße konfiguriert haben.

#### Schritte

1. Klicken Sie Auf **Admin** > **Benachrichtigungen**.
2. Klicken Sie Auf **Events**.
3. Klicken Sie im Abschnitt **Performance Violations Events** oder **Assure Violations Events** auf die Liste für die gewünschte Benachrichtigungsmethode (**Email**, **Syslog** oder **SNMP**) und wählen Sie den Schweregrad (**Warnung und höher** oder **kritisch**) für die Verletzung aus.
4. Klicken Sie Auf **Speichern**.

## Konfigurieren von Ereignisbenachrichtigungen auf Systemebene

OnCommand Insight unterstützt Benachrichtigungen bei Ereignissen auf Systemebene, z. B. bei Ausfällen von Erfassungseinheiten oder Datenquellfehlern. Um Benachrichtigungen zu erhalten, müssen Sie Insight so konfigurieren, dass E-Mails gesendet werden, wenn eines oder mehrere dieser Ereignisse auftreten.

#### Bevor Sie beginnen

Sie müssen E-Mail-Empfänger für den Empfang von Benachrichtigungen in **Admin** > **Benachrichtigungen** > **Sendemethoden** konfiguriert haben.

#### Schritte

1. Klicken Sie Auf **Admin** > **Benachrichtigungen**.
2. Klicken Sie Auf **Events**.
3. Wählen Sie im Abschnitt **System Alert Events** E-Mail den Schweregrad (**Warnung und höher** oder **kritisch**) für die Benachrichtigung aus, oder wählen Sie **nicht senden**, wenn Sie keine Benachrichtigungen über Ereignisse auf Systemebene erhalten möchten.
4. Klicken Sie Auf **Speichern**.
5. Klicken Sie auf **Admin** > **System Alerts**, um die Warnungen selbst zu konfigurieren.
6. Um eine neue Warnung hinzuzufügen, klicken Sie auf **+Hinzufügen** und geben Sie der Warnung einen eindeutigen **Namen**. Sie können auch auf das rechte Symbol klicken, um einen bestehenden Alarm zu bearbeiten.
7. Wählen Sie den **Ereignistyp** aus, auf den Sie eine Warnung ausgeben möchten, z. B. *Acquisition Unit Failure*.
8. Wählen Sie ein **Snooze**-Intervall, um Benachrichtigungen bei doppelten Ereignissen des ausgewählten Typs für das ausgewählte Zeitintervall zu unterdrücken. Wenn Sie „*Never*“ auswählen, erhalten Sie einmal pro Minute wiederholte Benachrichtigungen, bis das Ereignis nicht mehr stattfindet.
9. Wählen Sie einen **Schweregrad** (Warnung oder kritisch) für die Ereignisbenachrichtigung.
10. Standardmäßig werden E-Mail-Benachrichtigungen an die globale E-Mail-Empfängerliste gesendet, oder

Sie können auf den bereitgestellten Link klicken, um die globale Liste zu überschreiben und Benachrichtigungen an bestimmte Empfänger zu senden.

11. Klicken Sie auf Speichern, um die Warnmeldung hinzuzufügen.

## Konfigurieren der ASUP Verarbeitung

Alle NetApp Produkte sind mit automatisierten Funktionen ausgestattet, die den bestmöglichen Support für Kunden bieten. Der automatische Support (ASUP) sendet periodisch vordefinierte und spezifische Informationen an den Kunden-Support. Sie haben die Kontrolle über die Informationen, die an NetApp weitergeleitet werden und wie oft sie gesendet werden.

### Bevor Sie beginnen

Sie müssen OnCommand Insight so konfigurieren, dass Daten weitergeleitet werden, bevor Daten gesendet werden.

### Über diese Aufgabe

ASUP Daten werden über das HTTPS-Protokoll weitergeleitet.

### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Setup**.
3. Klicken Sie auf die Registerkarte **ASUP & Proxy**.
4. Wählen Sie im Abschnitt **ASUP ASUP aktivieren** aus, um die ASUP-Funktion zu aktivieren.
5. Wenn Sie Ihre Unternehmensinformationen ändern möchten, aktualisieren Sie die folgenden Felder:
   - **Firmenname**
   - **Standortname**
   - **Was zu senden ist**: Protokolle, Konfigurationsdaten, Leistungsdaten
6. Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass die angegebene Verbindung funktioniert.
7. Klicken Sie Auf **Speichern**.
8. Wählen Sie im Abschnitt **Proxy** aus, ob Sie **Proxy** aktivieren möchten, und geben Sie Ihre Proxy **Host**-, **Port**- und **user**-Informationen an.
9. Klicken Sie auf **Verbindung testen**, um sicherzustellen, dass der von Ihnen angegebene Proxy funktioniert.
10. Klicken Sie Auf **Speichern**.

### Inhalt des AutoSupport-Pakets (ASUP)

Das AutoSupport-Paket enthält die Datenbanksicherung sowie erweiterte Informationen.

Das AutoSupport-Paket umfasst Folgendes:

- Bestandsdaten

- Performance-Daten (wenn für die Aufnahme in ASUP ausgewählt)
- Datenquellen und Einstellungen der Datenquelle
- Integrationspakete
- Fernbedienungseinheiten
- ASUP/Proxy-Einstellungen
- Einstellungen für den Speicherort der Sicherung
- Einstellungen für den Archivspeicherort
- Benachrichtigungseinstellungen
- Benutzer
- Performance-Richtlinien
- Geschäftseinheiten und Applikationen
- Regeln und Einstellungen für die Geräteauflösung
- Dashboards und Widgets
- Dashboards und Widgets für die Asset-Seite
- Abfragen
- Anmerkungen und Anmerkungsregeln
- Protokolle
- Lizenzen Zu Haben
- Erfassungs-/Datenquellstatus
- MySQL-Status
- Systeminformationen

Das AutoSupport-Paket umfasst Folgendes nicht:

- Einstellungen des Sicherheitstools/Vault-Informationen (gesichert über separaten CLI-Prozess)
- Performance-Daten (wenn nicht für die Aufnahme in ASUP ausgewählt)

> Wenn Sie sich dafür entscheiden, Performance-Daten in ASUP zu integrieren, werden auch die Daten der letzten sieben Tage berücksichtigt. Die übrigen Daten befinden sich im Archiv, wenn diese Funktion aktiviert ist. Archivdaten sind nicht in ASUP enthalten.

## Definieren von Anwendungen

Wenn Sie Daten zu bestimmten Applikationen verfolgen möchten, die in Ihrer Umgebung ausgeführt werden, müssen Sie diese Applikationen definieren.

### Bevor Sie beginnen

Wenn Sie die Applikation einer Geschäftseinheit zuordnen möchten, müssen Sie die Geschäftseinheit bereits erstellt haben.

### Über diese Aufgabe

Applikationen können folgenden Assets zugewiesen werden: Hosts, virtuelle Maschinen, Volumes, interne Volumes, qtrees, Freigaben und Hypervisoren:

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anwendungen**.

   Nachdem Sie eine Applikation definiert haben, werden auf der Seite Anwendungen der Name der Applikation, ihre Priorität und gegebenenfalls die mit der Applikation verknüpfte Geschäftseinheit angezeigt.

3. Klicken Sie Auf **Hinzufügen**.

   Das Dialogfeld Anwendung hinzufügen wird angezeigt.

4. Geben Sie einen eindeutigen Namen für die Anwendung in das Feld **Name** ein.
5. Klicken Sie auf **Priorität** und wählen Sie die Priorität (kritisch, hoch, mittel oder niedrig) für die Anwendung in Ihrer Umgebung aus.
6. Wenn Sie diese Anwendung mit einer Business Entity verwenden möchten, klicken Sie auf **Business Entity** und wählen Sie die Entity aus der Liste aus.
7. **Optional**: Wenn Sie keine Volume-Freigabe verwenden, klicken Sie auf das Kontrollkästchen **Volume-Freigabe validieren** deaktivieren.

   Dies erfordert die Assure-Lizenz. Legen Sie diese Einstellung fest, wenn Sie sicherstellen möchten, dass jeder Host Zugriff auf dieselben Volumes in einem Cluster hat. Beispielsweise müssen Hosts in Hochverfügbarkeits-Clustern oft für Failover auf dieselben Volumes maskiert werden, allerdings müssen Hosts in verwandten Applikationen in der Regel nicht auf dieselben physischen Volumes zugreifen. Außerdem müssen Sie gemäß den Richtlinien möglicherweise aus Sicherheitsgründen nicht in Verbindung stehende Anwendungen nicht auf dieselben physischen Volumes zugreifen können.

8. Klicken Sie Auf **Speichern**.

   Die Anwendung wird auf der Seite Anwendungen angezeigt. Wenn Sie auf den Namen der Anwendung klicken, zeigt Insight die Seite der Anlage für die Anwendung an.

### Nachdem Sie fertig sind

Nachdem Sie eine Anwendung definiert haben, können Sie eine Anlagenseite für Host, virtuelle Maschine, Volume, internes Volume oder Hypervisor aufrufen, um eine Anwendung einem Asset zuzuweisen.

### Zuweisen von Anwendungen zu Assets

Nachdem Sie Applikationen mit oder ohne Geschäftseinheiten definiert haben, können Sie die Applikationen mit Assets verknüpfen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie das Asset (Host, virtuelle Maschine, Volume oder internes Volume), auf das Sie die

Anwendung anwenden möchten, indem Sie einen der folgenden Schritte ausführen:

- Klicken Sie auf **Dashboard**, wählen Sie **Assets Dashboard** aus und klicken Sie auf das Asset.
- Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Namen des Assets ein, und wählen Sie dann das Asset aus der Liste aus.

3. Positionieren Sie im Abschnitt **Benutzerdaten** der Asset-Seite den Cursor über den Namen der Applikation, die dem Asset derzeit zugewiesen ist (wenn keine Anwendung zugewiesen ist, wird stattdessen **Keine** angezeigt), und klicken Sie dann auf (Anwendung bearbeiten).

   Die Liste der verfügbaren Anwendungen für die ausgewählte Anlage wird angezeigt. Den Anwendungen, die derzeit mit dem Asset verknüpft sind, wird ein Häkchen vorangestellt.

4. Sie können in das Suchfeld eingeben, um die Anwendungsnamen zu filtern, oder Sie können in der Liste nach unten blättern.
5. Wählen Sie die Anwendungen aus, die Sie dem Asset zuordnen möchten.

   Sie können dem Host, der virtuellen Maschine und dem internen Volume mehrere Anwendungen zuweisen. Sie können dem Volume jedoch nur eine Anwendung zuweisen.

6. Klicken Sie Auf So weisen Sie der Anlage die ausgewählte Applikation oder die ausgewählten Anwendungen zu.

   Die Applikationsnamen werden im Abschnitt Benutzerdaten angezeigt. Wenn die Applikation mit einer Geschäftseinheit verknüpft ist, wird auch der Name der Geschäftseinheit in diesem Abschnitt angezeigt.

### Bearbeiten von Anwendungen

## Sie können die Priorität einer Anwendung, die mit einer Anwendung verknüpfte Geschäftseinheit oder den Status der Volume-Freigabe ändern.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anwendungen**.
3. Bewegen Sie den Cursor über die Anwendung, die Sie bearbeiten möchten, und klicken Sie auf .

   Das Dialogfeld Anwendung bearbeiten wird angezeigt.

4. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Priority** und wählen Sie eine andere Priorität.

     Sie können den Namen der Anwendung nicht ändern.

   - Klicken Sie auf **Business Entity** und wählen Sie eine andere Business Entity aus, der die Applikation zugeordnet werden soll, oder wählen Sie **None** aus, um die Verknüpfung der Applikation mit der Business Entity zu entfernen.
   - Klicken Sie auf, um die Option zu löschen oder wählen Sie **Volume-Freigabe validieren**.

     Diese Option ist nur verfügbar, wenn Sie über die Lizenz „Assure“ verfügen.

5. Klicken Sie Auf **Speichern**.

#### Löschen von Anwendungen

Eine Applikation kann gelöscht werden, wenn sie in Ihrer Umgebung keinen Bedarf mehr erfüllt.

##### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anwendungen**.
3. Setzen Sie den Cursor auf die Anwendung, die Sie löschen möchten, und klicken Sie auf .

   Es wird ein Bestätigungsdialogfeld angezeigt, in dem Sie gefragt werden, ob Sie die Anwendung löschen möchten.

4. Klicken Sie auf **OK**.

## Die Hierarchie Ihrer Geschäftseinheiten

Sie können Geschäftseinheiten definieren, um Ihre Umgebungsdaten granular zu verfolgen und darüber Berichte zu erstellen.

In OnCommand Insight enthält die Hierarchie der Geschäftseinheiten die folgenden Ebenen:

- **Mandant** wird primär von Service-Providern genutzt, um Ressourcen einem Kunden zuzuordnen, zum Beispiel NetApp.
- **Line of Business (Lob)** ist ein Geschäftsbereich oder eine Produktlinie innerhalb eines Unternehmens, z. B. Data Storage.
- **Business Unit** repräsentiert eine traditionelle Business Unit wie Legal oder Marketing.
- **Projekt** wird häufig verwendet, um ein bestimmtes Projekt innerhalb einer Geschäftseinheit zu identifizieren, für die Sie Kapazitätszuweisungen wünschen. Beispielsweise kann „Patente“ ein Projektname für die Rechtsabteilung und „Verkaufsveranstaltungen“ ein Projektname für die Geschäftseinheit Marketing sein. Beachten Sie, dass die Namen der Ebenen Leerzeichen enthalten können.

Sie müssen nicht alle Ebenen für das Design Ihrer Unternehmenshierarchie verwenden.

#### Entwerfen der Hierarchie Ihrer Geschäftseinheiten

Sie müssen die Elemente Ihrer Unternehmensstruktur verstehen und wissen, was in den Geschäftseinheiten vertreten werden muss, da diese eine feste Struktur in Ihrer OnCommand Insight-Datenbank werden. Sie können die folgenden Informationen verwenden, um Ihre Geschäftseinheiten einzurichten. Denken Sie daran, dass Sie nicht alle Hierarchieebenen verwenden müssen, um Daten in diesen Kategorien zu erfassen.

##### Schritte

1. Prüfen Sie jede Ebene der Hierarchie der Geschäftseinheiten, um festzustellen, ob diese Ebene in die Hierarchie Ihrer Unternehmenseinheit für Ihr Unternehmen aufgenommen werden soll:

- **Tenant** Level ist erforderlich, wenn Ihr Unternehmen ein ISP ist und Sie die Nutzung von Ressourcen durch Kunden verfolgen möchten.
- **Line of Business (Lob)** wird in der Hierarchie benötigt, wenn die Daten für verschiedene Produktlinien nachverfolgt werden müssen.
- **Business Unit** ist erforderlich, wenn Sie Daten für verschiedene Abteilungen verfolgen müssen. Diese Hierarchieebene ist oft wertvoll, wenn es darum geht, eine Ressource zu trennen, die von einer Abteilung genutzt wird, die von anderen Abteilungen nicht genutzt wird.
- **Projekt**-Ebene kann für spezialisierte Arbeiten innerhalb einer Abteilung verwendet werden. Diese Daten können nützlich sein, um die Technologieanforderungen eines separaten Projekts im Vergleich zu anderen Projekten in einem Unternehmen oder einer Abteilung zu lokalisieren, zu definieren und zu überwachen.

2. Erstellen Sie ein Diagramm, in dem jede Geschäftseinheit mit den Namen aller Ebenen innerhalb der Einheit angezeigt wird.
3. Überprüfen Sie die Namen in der Hierarchie, um sicherzustellen, dass sie in OnCommand Insight-Ansichten und -Berichten selbsterklärend sind.
4. Identifizieren Sie alle Applikationen, die den einzelnen Unternehmenseinheiten zugeordnet sind.

### Erstellen von Geschäftseinheiten

Nachdem Sie die Hierarchie der Geschäftseinheiten für Ihr Unternehmen entworfen haben, können Sie Anwendungen einrichten und die Geschäftseinheiten den Anwendungen zuordnen. Dieser Prozess erstellt die Struktur der Geschäftseinheiten in Ihrer OnCommand Insight-Datenbank.

#### Über diese Aufgabe

Das Zuordnen von Anwendungen zu Geschäftseinheiten ist optional; es handelt sich jedoch um eine Best Practice.

#### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Business Entities**.

   Die Seite Business Entities wird angezeigt.

3. Klicken Sie Auf + Add Um mit dem Erstellen einer neuen Einheit zu beginnen.

   Das Dialogfeld **Business Entity hinzufügen** wird angezeigt.

4. Für jede Entitätsebene (Mandant, Geschäftsbereich, Geschäftsbereich und Projekt) können Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie auf die Liste der Entitätsebene, und wählen Sie einen Wert aus.
   - Geben Sie einen neuen Wert ein, und drücken Sie die Eingabetaste.
   - Lassen Sie den Wert auf Entitätsebene als N/A stehen, wenn Sie die Entitätsebene für die Geschäftseinheit nicht verwenden möchten.
5. Klicken Sie Auf **Speichern**.

### Zuordnen von Geschäftseinheiten zu Assets

Sie können einer Ressource eine Geschäftseinheit zuweisen (Host, Port, Speicher, Switch, virtuelle Maschine, Qtree, Share, Volume oder internes Volume) ohne Zuordnung der Geschäftseinheit zu einer Applikation, doch werden Geschäftseinheiten automatisch einer Ressource zugewiesen, wenn diese Ressource einer Applikation zugeordnet ist, die zu einer Geschäftseinheit gehört.

#### Bevor Sie beginnen

Sie müssen bereits eine Geschäftseinheit erstellt haben.

#### Über diese Aufgabe

Sie können Geschäftseinheiten zwar direkt Assets zuweisen, es wird jedoch empfohlen, Applikationen Assets zuzuweisen und dann Geschäftseinheiten Assets zuzuweisen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie das Asset, auf das Sie die Geschäftseinheit anwenden möchten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Asset Dashboard auf das Asset.
   - Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Namen des Assets ein, und wählen Sie dann das Asset aus der Liste aus.
3. Positionieren Sie im Abschnitt **Benutzerdaten** der Asset-Seite Ihren Cursor auf **Keine** neben **Business Entities** und klicken Sie dann auf .

   Die Liste der verfügbaren Geschäftseinheiten wird angezeigt.
4. Geben Sie in das Feld **Suchen** ein, um die Liste nach einer bestimmten Entität zu filtern, oder scrollen Sie in der Liste nach unten; wählen Sie eine Business Entity aus der Liste aus.

   Wenn die ausgewählte Geschäftseinheit mit einer Applikation verknüpft ist, wird der Anwendungsname angezeigt. In diesem Fall wird neben dem Namen der Geschäftseinheit das Wort „`derived`“ angezeigt. Wenn Sie die Einheit nur für das Asset und nicht für die zugehörige Anwendung verwalten möchten, können Sie die Zuweisung der Anwendung manuell überschreiben.
5. Um eine Anwendung zu überschreiben, die von einer Geschäftseinheit abgeleitet wurde, setzen Sie den Cursor auf den Anwendungsnamen, und klicken Sie auf Wählen Sie eine andere Geschäftseinheit aus, und wählen Sie eine andere Anwendung aus der Liste aus.

### Zuordnen von Geschäftseinheiten zu oder Entfernen von Geschäftseinheiten aus mehreren Assets

Sie können Business Entities mehreren Assets zuweisen oder diese entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell zuweisen oder entfernen zu müssen.

#### Bevor Sie beginnen

Sie müssen bereits die Geschäftseinheiten erstellt haben, die Sie zu den gewünschten Assets hinzufügen möchten.

**Schritte**

1. Erstellen Sie eine neue Abfrage, oder öffnen Sie eine vorhandene Abfrage.
2. Filtern Sie bei Bedarf nach den Assets, denen Sie Business Entities hinzufügen möchten.
3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den ausgewählten Assets eine Geschäftseinheit hinzuzufügen, klicken Sie auf

. Wenn dem ausgewählten Asset-Typ Business Entities zugewiesen werden können, wird die Menüauswahl **Add Business Entity** angezeigt. Wählen Sie diese Option aus.
5. Wählen Sie die gewünschte Geschäftseinheit aus der Liste aus und klicken Sie auf **Speichern**.

   Jede neue Business Entity, die Sie zuweisen, überschreibt alle Business Entities, die bereits dem Asset zugewiesen wurden. Durch das Zuweisen von Anwendungen zu Assets werden auch die Business Entities überschrieben, die auf die gleiche Weise zugewiesen wurden. Das Zuweisen von Geschäftseinheiten als Anlage kann auch alle Anwendungen überschreiben, die dieser Anlage zugewiesen sind.

6. Um eine Geschäftseinheit zu entfernen, die den Assets zugewiesen ist, klicken Sie auf

Und wählen Sie **Business Entity entfernen**.
7. Wählen Sie die gewünschte Geschäftseinheit aus der Liste aus und klicken Sie auf **Löschen**.

## Anmerkungen definieren

Wenn Sie OnCommand Insight zur Nachverfolgung von Daten gemäß Ihren Unternehmensanforderungen anpassen, können Sie beliebige spezialisierte Annotationen definieren, die erforderlich sind, um einen vollständigen Überblick über Ihre Daten zu erhalten, wie z. B. Ende der Nutzungsdauer von Assets, Datacenter, Gebäudestandort, Storage-Ebene oder Volume. Und internem Service-Level für Volumes.

**Schritte**

1. Geben Sie die Terminologie an, der die Umgebungsdaten zugeordnet werden müssen.
2. Geben Sie die Unternehmensterminologie an, mit der Umgebungsdaten verknüpft werden müssen, die nicht bereits mit den Geschäftseinheiten verfolgt wird.
3. Geben Sie alle standardmäßigen Anmerkungstypen an, die Sie verwenden können.
4. Ermitteln Sie, welche benutzerdefinierten Anmerkungen Sie erstellen müssen.

### Verwendung von Annotationen zum Monitoring Ihrer Umgebung

Wenn Sie OnCommand Insight so anpassen, dass Daten für Ihre Unternehmensanforderungen nachverfolgt werden, können Sie spezielle Hinweise, die so genannten *Annotationen*, definieren und diese Ihren Ressourcen zuweisen. Beispielsweise können Assets mit Informationen wie Asset-Lebensende, Datacenter, Gebäudestandort, Storage-Klassen oder Service-Leveln für Volumes versehen werden.

Durch die Verwendung von Annotationen zum Monitoring Ihrer Umgebung werden die folgenden grundlegenden Aufgaben aufgeführt:

- Erstellen oder Bearbeiten von Definitionen für alle Anmerkungstypen.
- Anzeigen von Asset-Seiten und Verknüpfen jeder Anlage mit einer oder mehreren Anmerkungen.

  Wenn z. B. ein Asset geleast wird und der Mietvertrag innerhalb von zwei Monaten abläuft, können Sie eine End-of-Life-Anmerkung auf das Asset anwenden. Dadurch wird verhindert, dass andere diese Ressource über einen längeren Zeitraum nutzen können.

- Erstellen von Regeln, um Anmerkungen automatisch auf mehrere Assets desselben Typs anzuwenden.
- Verwenden des Importdienstprogramms für Anmerkungen zum Importieren von Anmerkungen.
- Filtern Sie Assets nach ihren Anmerkungen.
- Gruppieren von Daten in Berichten auf der Grundlage von Anmerkungen und Erstellen dieser Berichte.

  Weitere Informationen zu Berichten finden Sie im *OnCommand Insight Reporting Guide*.

#### Verwalten von Anmerkungstypen

OnCommand Insight bietet einige standardmäßige Annotationstypen an, z. B. Lebenszyklus von Assets (Geburtstag oder Ende der Nutzungsdauer), Gebäude- oder Datacenter-Standort und -Ebene, die Sie an die Anzeige in Ihren Berichten anpassen können. Sie können Werte für Standard-Anmerkungstypen definieren oder eigene benutzerdefinierte Anmerkungstypen erstellen. Sie können diese Werte später bearbeiten.

#### Standard-Anmerkungstypen

OnCommand Insight bietet einige standardmäßige Anmerkungstypen. Mit diesen Annotationen können Daten gefiltert oder gruppiert und die Datenberichterstattung gefiltert werden.

Sie können Assets mit Standardanmerkungstypen verknüpfen, z. B.:

- Lebenszyklus von Anlagen, z. B. Geburtstag, Sonnenuntergang oder Ende des Lebenszyklus
- Positionsinformationen zu einem Gerät wie z. B. Rechenzentren, Gebäude oder Etage
- Klassifizierung von Assets, z. B. nach Qualität (Tiers), nach angeschlossenen Geräten (Switch-Ebene) oder nach Service-Level
- Status, z. B. „heiß“ (hohe Auslastung)

In der folgenden Tabelle sind die Standardbeschriftungstypen aufgeführt. Sie können diese Beschriftungsnamen ganz nach Ihren Bedürfnissen bearbeiten.

| Anmerkungstypen | Beschreibung | Typ |
|---|---|---|
| Alias | Benutzerfreundlicher Name für eine Ressource. | Text |
| Geburtstag | Datum, an dem das Gerät online gestellt wurde oder wird. | Datum |

| | | |
|---|---|---|
| Gebäude | Physischer Standort von Host-, Storage-, Switch- und Bandressourcen. | Liste |
| Stadt | Standort der Gemeinde von Host-, Storage-, Switch- und Tape-Ressourcen | Liste |
| Rechnerressourcengruppe | Gruppenzuweisung, die von der Datenquelle „Host“ und „VM-Dateisysteme“ verwendet wird. | Liste |
| Kontinent | Geografischer Standort von Host-, Storage-, Switch- und Tape-Ressourcen | Liste |
| Land | Nationaler Standort von Host-, Storage-, Switch- und Bandressourcen. | Liste |
| Rechenzentrum | Physischer Standort der Ressource und steht für Hosts, Speicher-Arrays, Switches und Bänder zur Verfügung. | Liste |
| Direkt Verbunden | Gibt an (Ja oder Nein), ob eine Speicherressource direkt mit Hosts verbunden ist. | Boolesch |
| Ende des Supports | Datum, an dem ein Gerät offline genommen wird, z. B. wenn der Lease abgelaufen ist oder die Hardware außer Betrieb genommen wird. | Datum |
| Fabric-Alias | Benutzerfreundlicher Name für eine Fabric. | Text |
| Boden | Standort eines Geräts auf einem Stockwerk eines Gebäudes. Kann für Hosts, Speicher-Arrays, Switches und Bänder eingerichtet werden. | Liste |
| Heiß | Geräte, die bereits regelmäßig oder an der Kapazitätsgrenze stark genutzt werden. | Boolesch |

| | | |
|---|---|---|
| Hinweis | Kommentare, die einer Ressource zugeordnet werden sollen. | Text |
| Rack | Rack, in dem sich die Ressource befindet. | Text |
| Zimmer | Raum in einem Gebäude oder einem anderen Standort mit Host-, Speicher-, Switch- und Bandressourcen. | Liste |
| San | Logische Partition des Netzwerks. Verfügbar auf Hosts, Speicher-Arrays, Bändern, Switches und Anwendungen. | Liste |
| Service-Level | Eine Reihe unterstützter Service-Level, die Sie Ressourcen zuweisen können. Zeigt eine Liste mit bestellten Optionen für interne Volumes, qtree und Volumes an. Bearbeiten Sie Service Levels, um Performance-Richtlinien für unterschiedliche Level festzulegen. | Liste |
| Bundesland/Kanton | Bundesland oder Provinz, in der sich die Ressource befindet. | Liste |
| Sonnenuntergang | Schwellenwert, nach dem keine neuen Zuordnungen an das Gerät vorgenommen werden können. Nützlich für geplante Migrationen und andere ausstehende Netzwerkänderungen. | Datum |
| Switch-Ebene | Enthält vordefinierte Optionen zum Einrichten von Kategorien für Switches. Normalerweise bleiben diese Bezeichnungen für die gesamte Lebensdauer des Geräts erhalten, obwohl Sie sie bei Bedarf bearbeiten können. Nur für Switches verfügbar. | Liste |

| | | |
|---|---|---|
| Ebene | Sie können darüber hinaus verwendet werden, um in Ihrer Umgebung verschiedene Service Levels zu definieren. Tiers können den Typ des Levels definieren, z. B. die erforderliche Geschwindigkeit (z. B. Gold oder Silber). Diese Funktion ist nur für interne Volumes, qtrees, Storage Arrays, Storage-Pools und Volumes verfügbar. | Liste |
| Schweregrad Der Verletzung | Rangfolge (z. B. Major) eines Verstoßes (z. B. fehlende Host-Ports oder fehlende Redundanz) in einer Hierarchie von höchster bis niedrigster Bedeutung. | Liste |

Alias, Rechenzentrum, Hot, Service-Level, Sonnenuntergang, Switch Level, Service Level, Tier und Verletzung Severity sind Anmerkungen auf Systemebene, die Sie nicht löschen oder umbenennen können. Sie können nur die ihnen zugewiesenen Werte ändern.

**Wie Anmerkungen zugewiesen werden**

Mithilfe von Anmerkungsregeln können Sie Anmerkungen manuell oder automatisch zuweisen. OnCommand Insight weist auch automatisch einige Anmerkungen zum Erwerb von Vermögenswerten und nach Vererbung zu. Alle Anmerkungen, die Sie einem Asset zuweisen, werden im Abschnitt „Benutzerdaten“ der Seite „Anlage“ angezeigt.

Anmerkungen werden auf folgende Weise zugewiesen:

- Sie können einer Anlage eine Anmerkung manuell zuweisen.

  Wenn eine Anmerkung direkt einer Anlage zugewiesen wird, wird die Anmerkung als normaler Text auf einer Anlagenseite angezeigt. Anmerkungen, die manuell zugewiesen werden, haben immer Vorrang vor Annotationen, die durch Annotationsregeln geerbt oder zugewiesen werden.

- Sie können eine Anmerkungsregel erstellen, um Anlagen desselben Typs automatisch Anmerkungen zuzuweisen.

  Wenn die Anmerkung nach Regel zugewiesen ist, zeigt Insight den Regelnamen neben dem Namen der Anmerkung auf einer Anlagenseite an.

- Insight ordnet Ihrem Storage-Tier automatisch ein Tier-Modell zu und beschleunigt so die Zuweisung von Storage-Annotationen zu Ihren Ressourcen bei der Beschaffung von Assets.

  Bestimmte Speicherressourcen werden automatisch einem vordefinierten Tier zugeordnet (Tier 1 und Tier 2). Beispielsweise basiert die Symmetrix-Speicherebene auf der Symmetrix- und VMAX-Produktreihe und ist Tier 1 zugeordnet. Sie können die Standardwerte an Ihre Ebenenanforderungen anpassen. Wenn die Anmerkung von Insight zugewiesen wird (z. B. „Tier“), wird „`systemdefiniert`“ angezeigt, wenn Sie den Cursor über den Namen der Anmerkung auf einer Anlagenseite positionieren.

- Einige Ressourcen (untergeordnete Elemente einer Anlage) können die vordefinierte Tier-Annotation aus ihrer Anlage (übergeordnete Anlage) ableiten.

  Wenn Sie beispielsweise einem Storage eine Annotation zuweisen, wird die Tier-Annotation von allen Speicherpools, internen Volumes, Volumes, qtrees und Shares abgeleitet, die zum Storage gehören. Wenn auf ein internes Volume des Storage eine andere Annotation angewendet wird, wird diese Annotation anschließend von allen Volumes, qtrees und Shares abgeleitet. „`abgeleitete`“ wird neben dem Namen der Anmerkung auf einer Anlagenseite angezeigt.

#### Zuordnen von Kosten zu Anmerkungen

Bevor Sie kostenbezogene Berichte erstellen, sollten Sie Anmerkungen auf Systemebene Service Level, Switch-Level und Tiering zuordnen, die Kostenverrechnung für die Storage-Benutzer auf Basis der tatsächlichen Nutzung von Produktions- und replizierter Kapazität ermöglichen. Beispielsweise können Sie für die Stufe „Tier“ möglicherweise Werte für die Stufe „Gold“ und „Silber“ festlegen und der Stufe „Gold“ höhere Kosten zuweisen als der Stufe „Silber“.

#### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf Verwalten und wählen Sie **Anmerkungen**.

   Die Seite Anmerkung wird angezeigt.

3. Bewegen Sie den Mauszeiger über die Beschriftung Service Level, Switch Level oder Tier, und klicken Sie auf .

   Das Dialogfeld Anmerkung bearbeiten wird angezeigt.

4. Geben Sie die Werte für alle vorhandenen Ebenen in das Feld **Kosten** ein.

   Die Tier- und Service-Level-Anmerkungen weisen die Werte für Auto-Tier bzw. Objekt-Storage auf, die Sie nicht entfernen können.

5. Klicken Sie Auf + Add Um weitere Ebenen hinzuzufügen.
6. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

##### Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. OnCommand Insight bietet zwar eine Reihe von Standardanmerkungen, aber Sie können feststellen, dass Sie Daten auf andere Weise anzeigen möchten. Die Daten in benutzerdefinierten Annotationen ergänzen die bereits erfassten Gerätedaten wie Switch-Hersteller, Anzahl Ports und Leistungsstatistiken. Die mit Annotationen hinzugefügten Daten werden von Insight nicht erkannt.

**Schritte**

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Auf der Seite Anmerkungen wird die Liste der Anmerkungen angezeigt.

3. Klicken Sie Auf

.

   Das Dialogfeld **Anmerkung hinzufügen** wird angezeigt.

4. Geben Sie einen Namen und eine Beschreibung in die Felder **Name** und **Beschreibung** ein.

   Sie können in diese Felder bis zu 255 Zeichen eingeben.

   Beschriftungsnamen, die mit einem Punkt beginnen oder enden. Werden nicht unterstützt.

5. Klicken Sie auf **Typ** und wählen Sie dann eine der folgenden Optionen aus, die den in dieser Anmerkung zulässigen Datentyp darstellt:

   - Boolesch

     Dadurch wird eine Dropdown-Liste mit den Optionen „Ja“ und „Nein“ erstellt Die Anmerkung „`Direct Attached`“ ist z. B. Boolesch.

   - Datum

     Dadurch wird ein Feld erstellt, das ein Datum enthält. Wenn es sich bei der Anmerkung um ein Datum handelt, wählen Sie diese Option aus.

   - Liste

     Dadurch können folgende Elemente erstellt werden:

     - Eine feste Dropdown-Liste

       Wenn andere diesem Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste keine weiteren Werte hinzufügen.

     - Eine Liste mit flexiblen Dropdown-Menüs

       Wenn Sie beim Erstellen dieser Liste die Option **Neue Werte hinzufügen** auswählen, wenn andere diesen Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste weitere Werte hinzufügen.

   - Nummer

     Dadurch wird ein Feld erstellt, in dem der Benutzer, der die Anmerkung zuweist, eine Zahl eingeben kann. Wenn der Anmerkungstyp beispielsweise „`Boden`“ lautet, kann der Benutzer den Wertetyp „`Zahl`“ auswählen und die Etagennummer eingeben.

   - Text

     Dadurch wird ein Feld erstellt, das Freiformtext ermöglicht. Sie können beispielsweise „`Sprache`“ als Anmerkungstyp eingeben, „`Text`“ als Wertetyp auswählen und eine Sprache als Wert eingeben.

Nachdem Sie den Typ festgelegt und Ihre Änderungen gespeichert haben, können Sie den Typ der Anmerkung nicht ändern. Wenn Sie den Typ ändern müssen, müssen Sie die Anmerkung löschen und eine neue erstellen.

6. Wenn Sie **Liste**als Anmerkungstyp auswählen, gehen Sie wie folgt vor:
   a. Wählen Sie **Neue Werte hinzufügen auf der Fly** aus, wenn Sie der Anmerkung weitere Werte hinzufügen möchten, wenn Sie auf einer Asset-Seite, die eine flexible Liste erstellt.

      Angenommen, Sie befinden sich auf einer Asset-Seite und das Asset hat die City-Anmerkung mit den Werten Detroit, Tampa und Boston. Wenn Sie die Option **Neue Werte hinzufügen auf der Fly** ausgewählt haben, können Sie City wie San Francisco und Chicago direkt auf der Asset-Seite zusätzliche Werte hinzufügen, anstatt zur Seite Anmerkungen zu gehen, um sie hinzuzufügen. Wenn Sie diese Option nicht wählen, können Sie beim Anwenden der Anmerkung keine neuen Anmerkungswerte hinzufügen; dadurch wird eine feste Liste erstellt.

   b. Geben Sie einen Wert und einen Namen in die Felder **Wert** und **Beschreibung** ein.
   c. Klicken Sie Auf

Um weitere Werte hinzuzufügen.
   d. Klicken Sie Auf Um einen Wert zu entfernen.
7. Klicken Sie Auf **Speichern**.

Ihre Anmerkungen werden in der Liste auf der Seite Anmerkungen angezeigt.

#### Verwandte Informationen

"Importieren und Exportieren von Benutzerdaten"

### Manuelles Zuweisen von Anmerkungen zu Assets

Durch das Zuweisen von Annotationen zu Assets können Sie Assets auf eine für Ihr Unternehmen relevante Weise sortieren, gruppieren und protokollieren. Obwohl Sie Anlagen eines bestimmten Typs automatisch Anmerkungen zuweisen können, können Sie mithilfe von Anmerkungsregeln Anmerkungen zu einer einzelnen Anlage über die zugehörige Anlagenseite zuweisen.

#### Bevor Sie beginnen

Sie müssen die Anmerkung erstellt haben, die Sie zuweisen möchten.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie die Anlage, auf die Sie die Anmerkung anwenden möchten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Asset Dashboard auf das Asset.
   - Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Typ oder den Namen des Assets ein, und wählen Sie dann das Asset aus der angezeigten Liste aus.

     Die Seite Anlage wird angezeigt.

3. Klicken Sie im Abschnitt **Benutzerdaten** der Seite Asset auf + Add.

   Das Dialogfeld Anmerkung hinzufügen wird angezeigt.

4. Klicken Sie auf **Anmerkung** und wählen Sie eine Anmerkung aus der Liste aus.
5. Klicken Sie auf **Wert**, und führen Sie je nach Art der ausgewählten Anmerkung einen der folgenden Schritte aus:
   - Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   - Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
6. Klicken Sie Auf **Speichern**.
7. Wenn Sie den Wert der Anmerkung ändern möchten, nachdem Sie sie zugewiesen haben, klicken Sie auf Und wählen Sie einen anderen Wert aus.

   Wenn die Anmerkung vom Listentyp ist, für den die Option **Werte dynamisch bei Anmerkungszuweisung hinzufügen** ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

### Anmerkungen ändern

Sie können den Namen, die Beschreibung oder die Werte für eine Anmerkung ändern oder eine Anmerkung löschen, die Sie nicht mehr verwenden möchten.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Die Seite Anmerkungen wird angezeigt.

3. Bewegen Sie den Cursor über die Anmerkung, die Sie bearbeiten möchten, und klicken Sie auf .

   Das Dialogfeld * Anmerkung bearbeiten* wird angezeigt.

4. Sie können die folgenden Änderungen an einer Anmerkung vornehmen:

   a. Ändern Sie den Namen, die Beschreibung oder beides.

      Beachten Sie jedoch, dass Sie für den Namen und die Beschreibung maximal 255 Zeichen eingeben können und Sie den Typ einer Anmerkung nicht ändern können. Bei Anmerkungen auf Systemebene können Sie den Namen oder die Beschreibung nicht ändern. Sie können jedoch Werte hinzufügen oder entfernen, wenn es sich um einen Listentyp handelt.

      Wenn eine benutzerdefinierte Anmerkung im Data Warehouse veröffentlicht wird und Sie sie umbenennen, gehen die historischen Daten verloren.

   a. Um einer Anmerkung des Listentyps einen weiteren Wert hinzuzufügen, klicken Sie auf + Add.
   b. Um einen Wert aus einer Anmerkung des Listentyps zu entfernen, klicken Sie auf .

      Sie können einen Anmerkungswert nicht löschen, wenn dieser Wert einer Anmerkung zugeordnet ist, die in einer Anmerkungsregel, einer Abfrage oder einer Leistungsrichtlinie enthalten ist.

5. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

#### Nachdem Sie fertig sind

Wenn Sie Anmerkungen im Data Warehouse verwenden möchten, müssen Sie eine Aktualisierung der Anmerkungen im Data Warehouse erzwingen. Weitere Informationen finden Sie im *OnCommand Insight Data Warehouse Administration Guide*.

#### Anmerkungen werden gelöscht

Sie können eine Anmerkung löschen, die Sie nicht mehr verwenden möchten. Eine Annotation auf Systemebene oder eine Annotation, die in einer Annotationsregel, einer Abfrage oder einer Performance-Richtlinie verwendet wird, kann nicht gelöscht werden.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Die Seite Anmerkungen wird angezeigt.

3. Setzen Sie den Cursor auf die Anmerkung, die Sie löschen möchten, und klicken Sie auf 🗑.

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf **OK**.

##### Zuordnen von Anmerkungen zu Anlagen mithilfe von Anmerkungsregeln

Um Assets anhand von Kriterien, die Sie definieren, automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerkungsregeln. OnCommand Insight weist den Assets anhand dieser Regeln die Annotationen zu. Insight bietet außerdem zwei standardmäßige Anmerkungsregeln, die Sie an Ihre Anforderungen anpassen oder entfernen können, wenn Sie sie nicht verwenden möchten.

#### Standardmäßige Regeln für Storage-Annotationen

Um die Zuweisung von Storage-Annotationen zu Ihren Ressourcen zu beschleunigen, bietet OnCommand Insight 21 standardmäßige Annotationsregeln, die eine Tier-Stufe mit einem Storage-Tier-Modell verknüpfen. Alle Storage-Ressourcen werden bei Erwerb der Assets in Ihrer Umgebung automatisch einem Tier zugeordnet.

Die Standardbeschriftungsregeln wenden eine Ebenenbeschriftung wie folgt an:

- Tier 1, Quality Tier für Storage

  Die Beschriftung der Stufe 1 wird auf die folgenden Anbieter und deren angegebene Produktfamilien angewendet: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 oder FAS6200) und Violin (Speicher).

- Tier 2, Quality Tier für Storage

Die Tier 2-Annotation wird für die folgenden Anbieter und deren Familien angewendet: HP (3PAR StoreServ oder EVA), EMC (CLARiiON), HDS (AMS oder D800), IBM (XIV) und NetApp (FAS3000, FAS3100 und FAS3200).

Sie können die Standardeinstellungen dieser Regeln entsprechend Ihren Ebenenanforderungen bearbeiten oder entfernen, wenn Sie sie nicht benötigen.

### Anmerkungsregeln werden erstellt

Alternativ zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Wenn Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

### Bevor Sie beginnen

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

### Über diese Aufgabe

Sie können zwar die Anmerkungstypen bearbeiten, während Sie die Regeln erstellen, aber Sie sollten die Typen bereits im Voraus definiert haben.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Klicken Sie Auf + Add.

   Das Dialogfeld Regel hinzufügen wird angezeigt.

4. Gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Dieser Name wird auf der Seite Anmerkungsregeln angezeigt.

   b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die OnCommand Insight verwenden soll, um die Anmerkung auf Anlagen anzuwenden.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Beschriftung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise als Anmerkung Geburtstag auswählen, geben Sie ein Datum für den Wert an.

5. Klicken Sie Auf **Speichern**.
6. Klicken Sie auf **Alle Regeln**, wenn Sie alle Regeln sofort ausführen möchten; andernfalls werden die Regeln in einem regelmäßigen geplanten Intervall ausgeführt.

### Festlegen der Priorität der Anmerkungsregel

Standardmäßig bewertet OnCommand Insight Annotationsregeln sequenziell. Sie können jedoch die Reihenfolge konfigurieren, in der OnCommand Insight Annotationsregeln auswertet, wenn Sie möchten, dass Insight Regeln in einer bestimmten Reihenfolge auswertet.

#### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Bewegen Sie den Cursor über eine Anmerkungsregel.

   Die Rangfolge-Pfeile erscheinen rechts von der Regel.

4. Um eine Regel in der Liste nach oben oder unten zu verschieben, klicken Sie auf den Aufwärtspfeil oder den Abwärtspfeil.

   Standardmäßig werden neue Regeln nacheinander zur Liste der Regeln hinzugefügt. Wenn Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

### Anmerkungsregeln ändern

Sie können eine Anmerkungsregel ändern, um den Namen der Regel, ihre Anmerkung, den Wert der Anmerkung oder die mit der Regel verknüpfte Abfrage zu ändern.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Suchen Sie die Regel, die Sie ändern möchten:
   - Auf der Seite Anmerkungsregeln können Sie die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben.
   - Klicken Sie auf eine Seitenzahl, um die Anmerkungsregeln nach Seite zu durchsuchen, wenn mehr Regeln als auf eine Seite passen.
4. Führen Sie einen der folgenden Schritte aus, um das Dialogfeld **Regel bearbeiten** anzuzeigen:
   - Wenn Sie sich auf der Seite Anmerkungsregeln befinden, setzen Sie den Cursor auf die Anmerkungsregel, und klicken Sie auf .
   - Wenn Sie sich auf einer Bestandsseite befinden, setzen Sie den Cursor auf die Anmerkung, die der Regel zugeordnet ist, setzen Sie den Cursor auf den Namen der Regel, wenn sie angezeigt wird, und klicken Sie dann auf den Namen der Regel.
5. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Speichern**.

#### Anmerkungsregeln werden gelöscht

Sie können eine Anmerkungsregel löschen, wenn die Regel nicht mehr erforderlich ist, um die Objekte im Netzwerk zu überwachen.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten**, und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.
3. Suchen Sie die zu löschende Regel:
   - Auf der Seite Anmerkungsregeln können Sie die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben.
   - Klicken Sie auf eine Seitenzahl, um die Anmerkungsregeln nach Seite zu durchsuchen, wenn mehr Regeln als auf eine einzelne Seite passen.
4. Zeigen Sie mit dem Cursor auf die Regel, die Sie löschen möchten, und klicken Sie dann auf 🗑.

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Regel löschen möchten.
5. Klicken Sie auf **OK**.

#### Importieren von Anmerkungswerten

Wenn Sie Anmerkungen zu SAN-Objekten (wie Storage, Hosts und Virtual Machines) in einer CSV-Datei beibehalten, können Sie diese Informationen in OnCommand Insight importieren. Sie können Applikationen, Geschäftseinheiten oder Annotationen wie Tiering und Building importieren.

**Über diese Aufgabe**

Es gelten die folgenden Regeln:

- Wenn ein Anmerkungswert leer ist, wird diese Anmerkung vom Objekt entfernt.
- Wenn Sie Volumes oder interne Volumes mit Anmerkungen versehen, ist der Objektname eine Kombination aus Storage-Namen und Volume-Namen. Verwenden Sie dabei den Bindestrich und das Pfeiltrennzeichen (->):

  ```
  <storage_name>-><volume_name>
  ```

- Wenn Speicher, Switches oder Ports mit Anmerkungen versehen werden, wird die Spalte Anwendung ignoriert.
- Die Spalten Tenant, Line_of_Business, Business_Unit und Project bilden eine Geschäftseinheit.

  Alle Werte können leer bleiben. Wenn eine Applikation bereits mit einer anderen Business Entity als den Eingabewerten verknüpft ist, wird die Applikation der neuen Business Entity zugewiesen.

Die folgenden Objekttypen und Schlüssel werden im Importdienstprogramm unterstützt:

| Typ | Taste |
| --- | --- |
| Host | `id-><id>` Oder `<Name>` Oder `<IP>` |
| VM | `id-><id>` Oder `<Name>` |
| Storage-Pool | `id-><id>` Oder `<Storage_name>-><Storage_Pool_name>` |
| Internes Volumen | `id-><id>` Oder `<Storage_name>-><Internal_volume_name>` |
| Datenmenge | `id-><id>` Oder `<Storage_name>-><Volume_name>` |
| Storage | `id-><id>` Oder `<Name>` Oder `<IP>` |
| Switch | `id-><id>` Oder `<Name>` Oder `<IP>` |
| Port | `id-><id>` Oder `<WWN>` |
| Share | `id-><id>` Oder `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol><Qtree>` Ist optional, wenn es einen Standard-qtree gibt. |
| Qtree | `id-><id>` Oder `<Storage Name>-><Internal Volume Name>-><Qtree Name>` |

Die CSV-Datei sollte das folgende Format verwenden:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

**Schritte**

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Admin** und wählen Sie **Troubleshooting**.

   Die Seite Fehlerbehebung wird angezeigt.
3. Klicken Sie im Abschnitt **andere Aufgaben** der Seite auf den Link **OnCommand Insight-Portal**.
4. Klicken Sie auf **Insight Connect API**.
5. Melden Sie sich beim Portal an.
6. Klicken Sie Auf **Annotation Import Utility**.
7. Speichern Sie die `.zip` Datei, entpacken und lesen `readme.txt` Datei für weitere Informationen und Beispiele.
8. Platzieren Sie die CSV-Datei in demselben Ordner wie die `.zip` Datei:
9. Geben Sie im Befehlszeilenfenster Folgendes ein:

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   Die Option -l, die die zusätzliche Protokollierung ermöglicht, und die Option -c, die die Groß-/Kleinschreibung aktiviert, sind standardmäßig auf false gesetzt. Daher müssen Sie diese nur angeben, wenn Sie die Funktionen verwenden möchten.

   Zwischen den Optionen und ihren Werten gibt es keine Leerzeichen.

Die folgenden Schlüsselwörter sind reserviert und verhindern, dass Benutzer sie als Anmerkungsnamen angeben: - Application - Application_Priority - Tenant - Line_of_Business - Business_Unit - Projektfehler werden generiert, wenn Sie versuchen, einen Anmerkungstyp mit einem der reservierten Schlüsselwörter zu importieren. Wenn Sie mit diesen Stichwörtern Beschriftungsnamen erstellt haben, müssen Sie diese ändern, damit das Importdienstprogramm ordnungsgemäß funktioniert.

Das Dienstprogramm Annotation Import erfordert Java 8 oder Java 11. Stellen Sie sicher, dass eine dieser Komponenten vor dem Ausführen des Importdienstprogramms installiert ist. Es wird empfohlen, die neueste OpenJDK 11 zu verwenden.

#### Zuweisen von Anmerkungen zu mehreren Anlagen mithilfe einer Abfrage

Durch das Zuweisen einer Anmerkung zu einer Gruppe von Assets können Sie diese zugehörigen Assets leichter identifizieren oder in Abfragen oder Dashboards verwenden.

**Bevor Sie beginnen**

Anmerkungen, die Sie Anlagen zuweisen möchten, müssen zuvor erstellt worden sein.

**Über diese Aufgabe**

Sie können das Zuweisen einer Anmerkung zu mehreren Anlagen vereinfachen, indem Sie eine Abfrage verwenden. Wenn Sie beispielsweise allen Arrays an einem bestimmten Standort im Datacenter eine benutzerdefinierte Adressenanmerkung zuweisen möchten,

**Schritte**

1. Erstellen Sie eine neue Abfrage, um die Assets zu identifizieren, denen Sie eine Anmerkung zuweisen möchten. Klicken Sie Auf **Abfragen** > **+Neue Abfrage**.
2. Wählen Sie in der Dropdown-Liste **Suchen nach… Speicher**. Sie können Filter festlegen, um die Liste der angezeigten Speicher weiter einzugrenzen.
3. Wählen Sie in der angezeigten Liste der Speicher einen oder mehrere Speicher aus, indem Sie auf das Kontrollkästchen neben dem Speichernamen klicken. Sie können auch alle angezeigten Speicher auswählen, indem Sie oben in der Liste auf das Hauptfeld klicken.
4. Wenn Sie alle gewünschten Speicher ausgewählt haben, klicken Sie auf **actions** > **Anmerkung bearbeiten**.

   Das Dialogfeld Anmerkung hinzufügen wird angezeigt.

5. Wählen Sie die **Anmerkung** und **Wert** aus, die Sie den Speichern zuweisen möchten, und klicken Sie auf **Speichern**.

   Wenn Sie die Spalte für diese Anmerkung anzeigen, wird sie auf allen ausgewählten Speichern angezeigt.

6. Sie können die Anmerkung jetzt verwenden, um nach Speichern in einem Widget oder einer Abfrage zu filtern. In einem Widget können Sie Folgendes tun:

   a. Erstellen Sie ein Dashboard oder öffnen Sie ein vorhandenes. Fügen Sie eine **Variable** hinzu und wählen Sie die Anmerkung aus, die Sie auf den obigen Speichern festgelegt haben. Die Variable wird dem Dashboard hinzugefügt.

b. Klicken Sie in dem neu hinzugefügten Variablenfeld auf **any** und geben Sie den entsprechenden Wert ein, nach dem gefiltert werden soll. Klicken Sie auf das Häkchen, um den Variablenwert zu speichern.

c. Widget hinzufügen. Klicken Sie in der Abfrage des Widgets auf die Schaltfläche**Filter by+**und wählen Sie die entsprechende Anmerkung aus der Liste aus.

d. Klicken Sie auf **any** und wählen Sie die oben hinzugefügte Anmerkungsvariable aus. Die von Ihnen erstellten Variablen beginnen mit „``“ und werden in der Dropdown-Liste angezeigt.

e. Stellen Sie alle anderen Filter oder Felder, die Sie wünschen, dann klicken Sie **Speichern**, wenn das Widget nach Ihren Wünschen angepasst ist.

Im Widget auf dem Dashboard werden nur die Daten für die Speicher angezeigt, denen Sie die Anmerkung zugewiesen haben.

## Elemente werden abgefragt

Abfragen ermöglichen Ihnen die Überwachung und Fehlerbehebung im Netzwerk, indem Sie die Assets in Ihrer Umgebung auf granularer Ebene durchsuchen, die auf vom Benutzer ausgewählten Kriterien (Annotationen und Performance-Metriken) basieren. Außerdem ist für Anmerkungsregeln, die Anlagen automatisch Anmerkungen zuweisen, eine Abfrage erforderlich.

#### In Abfragen und Dashboards verwendete Assets

### Insight-Abfragen und Dashboard-Widgets können mit einer Vielzahl von Asset-Typen verwendet werden

Die folgenden Asset-Typen können in Abfragen, Dashboard-Widgets und benutzerdefinierten Asset-Seiten verwendet werden. Die für Filter, Ausdrücke und Anzeigen verfügbaren Felder und Zähler variieren je nach Asset-Typen. Nicht alle Assets können in allen Widgets verwendet werden.

- Applikation
- Datenspeicher
- Festplatte
- Fabric
- Generisches Gerät
- Host
- Internes Volumen
- ISCSI-Sitzung
- ISCSI-Netzwerkportal
- Pfad
- Port
- Qtree
- Kontingente
- Share
- Storage

- Storage-Node
- Storage-Pool
- Switch
- Tape
- VMDK
- Virtual Machine
- Datenmenge
- Zone
- Zonenmitglied

### Erstellen einer Abfrage

Sie können eine Abfrage erstellen, um die Assets in Ihrer Umgebung auf granularer Ebene zu durchsuchen. Mithilfe von Abfragen können Sie Daten aufteilen, indem Sie Filter hinzufügen und die Ergebnisse sortieren, um Bestands- und Leistungsdaten in einer Ansicht anzuzeigen.

#### Über diese Aufgabe

Sie können beispielsweise eine Abfrage für Volumes erstellen, einen Filter hinzufügen, um bestimmte Speicher zu finden, die dem ausgewählten Volume zugeordnet sind, einen Filter hinzufügen, um eine bestimmte Anmerkung, wie z. B. Schicht 1, für die ausgewählten Speicher zu finden, Und schließlich fügen Sie einen weiteren Filter hinzu, um alle Speicher mit IOPS - Lesen (IO/s) größer als 25 zu finden. Wenn die Ergebnisse angezeigt werden, können Sie die mit der Abfrage verknüpften Datenspalten in aufsteigender oder absteigender Reihenfolge sortieren.

Wenn eine neue Datenquelle hinzugefügt wird, die Assets erfasst oder Anmerkungen oder Anwendungszuweisungen vorgenommen werden, können Sie nach der Indizierung der Abfragen, die in einem regelmäßig geplanten Intervall stattfinden, nach diesen Assets, Anmerkungen oder Anwendungen suchen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **+ Neue Abfrage**.
3. Klicken Sie auf **Select Resource Type** und wählen Sie einen Asset-Typ aus.

   Wenn eine Ressource für eine Abfrage ausgewählt wird, werden automatisch eine Reihe von Standardspalten angezeigt. Sie können diese Spalten jederzeit entfernen oder neue hinzufügen.

4. Geben Sie in das Textfeld **Name** den Namen des Assets ein oder geben Sie einen Textteil ein, um durch die Anlagennamen zu filtern.

   Sie können die folgenden Elemente allein oder kombiniert verwenden, um Ihre Suche in einem beliebigen Textfeld auf der Seite Neue Abfrage zu verfeinern:

   - Mit einem Sternchen können Sie nach allem suchen. Beispiel: `vol*rhel` Zeigt alle Ressourcen an, die mit „`vol`“ beginnen und mit „`RHEL`“ enden.
   - Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Beispiel: `BOS-`

`PRD??-S12` Zeigt BOS-PRD12-S12, BOS-PRD13-S12 usw. an.

- Mit dem Operator ODER können Sie mehrere Einheiten angeben. Beispiel: `FAS2240 OR CX600 OR FAS3270` Findet mehrere Storage-Modelle
- Der NICHT-Operator ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen. Beispiel: `NOT EMC*` Findet alles, was nicht mit „`EMC`“ beginnt. Verwenden Sie können `NOT *` So zeigen Sie Felder an, die keinen Wert enthalten.

5. Klicken Sie Auf Um die Assets anzuzeigen.
6. Um ein Kriterium hinzuzufügen, klicken Sie auf

Und führen Sie eine der folgenden Aktionen aus:
   - Geben Sie ein, um nach bestimmten Kriterien zu suchen, und wählen Sie es aus.
   - Blättern Sie in der Liste nach unten, und wählen Sie ein Kriterium aus.
   - Geben Sie einen Wertebereich ein, wenn Sie eine Performance-Metrik wie IOPS - Lesen (IO/s) auswählen. Von Insight bereitgestellte Standardanmerkungen werden durch angezeigt; Es ist möglich, Anmerkungen mit doppelten Namen zu haben.

   In den Listenaktualisierungen wird der Liste Abfrageergebnisse eine Spalte für die Kriterien und die Ergebnisse der Abfrage hinzugefügt.
7. Optional können Sie auf klicken Um eine Anmerkung oder Performance-Metrik aus den Abfrageergebnissen zu entfernen.

   Wenn Ihre Abfrage beispielsweise die maximale Latenz und den maximalen Durchsatz für Datastores anzeigt und Sie nur die maximale Latenz in der Liste der Abfrageergebnisse anzeigen möchten, klicken Sie auf diese Schaltfläche und deaktivieren Sie das Kontrollkästchen **Throughput - max**. Die Spalte Throughput - Max (MB/s) wird aus der Liste der Abfrageergebnisse entfernt.

   Abhängig von der Anzahl der Spalten, die in der Abfrageergebnistabelle angezeigt werden, können Sie möglicherweise keine weiteren hinzugefügten Spalten anzeigen. Sie können eine oder mehrere Spalten entfernen, bis die gewünschten Spalten angezeigt werden.
8. Klicken Sie auf **Speichern**, geben Sie einen Namen für die Abfrage ein und klicken Sie erneut auf **Speichern**.

   Wenn Sie über ein Konto mit einer Administratorrolle verfügen, können Sie benutzerdefinierte Dashboards erstellen. Ein benutzerdefiniertes Dashboard kann alle Widgets aus der Widget-Bibliothek enthalten, von denen mehrere Sie Abfrageergebnisse in einem benutzerdefinierten Dashboard darstellen können. Weitere Informationen zu benutzerdefinierten Dashboards finden Sie im *OnCommand Insight Handbuch zum Einstieg*.

### Verwandte Informationen

"Importieren und Exportieren von Benutzerdaten"

### Anzeigen von Abfragen

Sie können Ihre Abfragen anzeigen, um Ihre Assets zu überwachen und zu ändern, wie Ihre Abfragen die Daten zu Ihren Assets anzeigen.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.
3. Sie können die Anzeige von Abfragen mit einer der folgenden Methoden ändern:
   - Sie können Text in das Feld **Filter** eingeben, um nach bestimmten Abfragen zu suchen.
   - Sie können die Sortierreihenfolge der Spalten in der Tabelle der Abfragen durch Klicken auf den Pfeil in der Spaltenüberschrift auf aufsteigender (Aufwärtspfeil) oder absteigender (Abwärtspfeil) ändern.
   - Wenn Sie die Größe einer Spalte ändern möchten, bewegen Sie den Mauszeiger über die Spaltenüberschrift, bis ein blauer Balken angezeigt wird. Legen Sie die Maus über die Leiste, und ziehen Sie sie nach rechts oder links.
   - Um eine Spalte zu verschieben, klicken Sie auf die Spaltenüberschrift und ziehen Sie sie nach rechts oder links.
   - Beachten Sie beim Durchblättern der Abfrageergebnisse, dass sich die Ergebnisse ändern können, wenn Insight Ihre Datenquellen automatisch abfragt. Dies kann dazu führen, dass einige Elemente fehlen oder einige Elemente in der Reihenfolge erscheinen, je nachdem, wie sie sortiert sind.

### Abfrageergebnisse werden in eine CSV-Datei exportiert

Sie können die Ergebnisse einer Abfrage in eine CSV-Datei exportieren, um die Daten in eine andere Anwendung zu importieren.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

3. Klicken Sie auf eine Abfrage.
4. Klicken Sie Auf So exportieren Sie Abfrageergebnisse in ein `.CSV` Datei:
5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Öffnen mit** und dann auf **OK**, um die Datei mit Microsoft Excel zu öffnen und die Datei an einem bestimmten Speicherort zu speichern.
   - Klicken Sie auf **Datei speichern** und dann auf **OK**, um die Datei im Ordner Downloads zu speichern. Nur die Attribute für die angezeigten Spalten werden exportiert. Einige angezeigte Spalten, insbesondere solche, die Teil komplexer verschachtelter Beziehungen sind, werden nicht exportiert.

     Wenn ein Komma in einem Anlagennamen angezeigt wird, schließt der Export den Namen in Anführungszeichen ein, wobei der Name des Assets und das entsprechende .csv-Format erhalten bleiben.

     + beim Exportieren von Abfrageergebnissen ist zu beachten, dass **alle** Zeilen in der Ergebnistabelle exportiert werden, nicht nur die auf dem Bildschirm ausgewählten oder angezeigten Zeilen, maximal 10,000 Zeilen.

Wenn Sie eine exportierte CSV-Datei mit Excel öffnen, wenn Sie einen Objektnamen oder ein anderes Feld im Format NN:NN haben (zwei Ziffern gefolgt von einem Doppelpunkt gefolgt von zwei weiteren Ziffern), interpretiert Excel diesen Namen manchmal als Zeitformat, statt Textformat. Dies kann dazu führen, dass in Excel falsche Werte in diesen Spalten angezeigt werden. Ein Objekt mit dem Namen „81:45“ wird beispielsweise in Excel als „81:45:00“ angezeigt. Um dies zu umgehen, importieren Sie die .CSV-Datei in Excel anhand der folgenden Schritte:

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

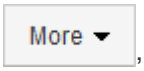
#### Ändern von Abfragen

Sie können die Kriterien ändern, die einer Abfrage zugeordnet sind, wenn Sie die Suchkriterien für die abfragenden Assets ändern möchten.

##### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

3. Klicken Sie auf den Abfragenamen.
4. Um ein Kriterium aus der Abfrage zu entfernen, klicken Sie auf .
5. Um der Abfrage ein Kriterium hinzuzufügen, klicken Sie auf 

, Und wählen Sie ein Kriterium aus der Liste aus.
6. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um die Abfrage mit dem ursprünglich verwendeten Namen zu speichern.
   - Klicken Sie auf **Speichern unter**, um die Abfrage mit einem anderen Namen zu speichern.
   - Klicken Sie auf **Umbenennen**, um den Abfragenamen zu ändern, den Sie ursprünglich verwendet haben.
   - Klicken Sie auf **revert**, um den Namen der Abfrage auf den Namen zurück zu ändern, den Sie ursprünglich verwendet hatten.

### Abfragen werden gelöscht

Sie können Abfragen löschen, wenn sie keine nützlichen Informationen über Ihre Assets mehr sammeln. Eine Abfrage kann nicht gelöscht werden, wenn sie in einer Anmerkungsregel verwendet wird.

#### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

3. Setzen Sie den Cursor auf die Abfrage, die Sie löschen möchten, und klicken Sie auf .

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Abfrage löschen möchten.

4. Klicken Sie auf **OK**.

### Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen aus Assets

Sie können mehrere Anwendungen zu Assets zuweisen oder sie aus diesen Anwendungen entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell zuweisen oder entfernen zu müssen.

#### Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets findet, die Sie bearbeiten möchten.

#### Schritte

1. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets findet.

   Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den ausgewählten Assets eine Anwendung hinzuzufügen, klicken Sie auf Actions, Und wählen Sie **Anwendung bearbeiten**.
   a. Klicken Sie auf **Anwendung** und wählen Sie eine oder mehrere Anwendungen aus.

      Sie können mehrere Anwendungen für Hosts, interne Volumes und virtuelle Maschinen auswählen. Sie können jedoch nur eine Anwendung für ein Volume auswählen.

   b. Klicken Sie Auf **Speichern**.

5. Klicken Sie auf, um eine der Assets zugewiesene Anwendung zu entfernen Actions Und wählen Sie **Anwendung entfernen**.

   a. Wählen Sie die Anwendung oder die Anwendungen aus, die Sie entfernen möchten.

   b. Klicken Sie Auf **Löschen**.

   Neue Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem anderen Asset abgeleitet wurden. Beispielsweise übernehmen Volumes Applikationen von Hosts, und wenn neuen Applikationen einem Volume zugewiesen werden, hat die neue Applikation Vorrang vor der abgeleiteten Applikation.

### Bearbeiten oder Entfernen mehrerer Anmerkungen aus Anlagen

Sie können mehrere Anmerkungen für Anlagen bearbeiten oder mehrere Anmerkungen aus Anlagen entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell bearbeiten oder entfernen zu müssen.

#### Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets sucht, die Sie bearbeiten möchten.

#### Schritte

1. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets sucht.

   Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf ☐ Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den Assets eine Anmerkung hinzuzufügen oder den Wert einer Anmerkung zu bearbeiten, die den Assets zugewiesen ist, klicken Sie auf Actions, Und wählen Sie **Anmerkung bearbeiten**.

   a. Klicken Sie auf **Anmerkung** und wählen Sie eine Anmerkung aus, für die Sie den Wert ändern möchten, oder wählen Sie eine neue Anmerkung aus, um sie allen Anlagen zuzuweisen.

   b. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

   c. Klicken Sie Auf **Speichern**.

5. Um eine den Assets zugewiesene Anmerkung zu entfernen, klicken Sie auf Actions, Und wählen Sie **Anmerkung entfernen**.

   a. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie aus den Assets entfernen möchten.

   b. Klicken Sie Auf **Löschen**.

#### Tabellenwerte werden kopiert

Sie können Werte in Tabellen kopieren, um sie in Suchfeldern oder anderen Anwendungen zu verwenden.

##### Über diese Aufgabe

Es gibt zwei Methoden, mit denen Sie Werte aus Tabellen oder Abfrageergebnissen kopieren können.

##### Schritte

1. Methode 1: Markieren Sie den gewünschten Text mit der Maus, kopieren Sie ihn und fügen Sie ihn in Suchfelder oder andere Anwendungen ein.
2. Methode 2: Bewegen Sie bei Einzelwertfeldern, deren Länge die Breite der Tabellenspalte überschreitet, die durch Ellipsen (…) gekennzeichnet sind, den Mauszeiger über das Feld und klicken Sie auf das Clipboard-Symbol. Der Wert wird zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopiert.

   Beachten Sie, dass nur Werte, die Verknüpfungen zu Assets darstellen, kopiert werden können. Beachten Sie auch, dass nur Felder, die einzelne Werte enthalten (d. h. nicht-Listen), das Kopiersymbol haben.

## Management von Performance-Richtlinien

Mit OnCommand Insight lassen sich Performance-Richtlinien erstellen, um im Netzwerk verschiedene Schwellenwerte zu überwachen und bei Überschreitung dieser Schwellenwerte Alarme auszugeben. Mithilfe von Performance-Richtlinien können Sie einen Schwellenverletzungen sofort erkennen, die Auswirkungen identifizieren und die Auswirkungen und die Ursache des Problems auf eine Weise analysieren, die eine schnelle und effektive Korrektur ermöglicht.

Mithilfe einer Performance-Richtlinie können Sie für alle Objekte (Datenspeicher, Festplatte, Hypervisor, internes Volume, Port, Storage, Storage-Node, Storage-Pool, VMDK, Virtual Machine, Und Volume) mit gemeldeten Performance-Zählern (z. B. gesamte IOPS). Wenn ein Schwellenwert verletzt wird, erkennt Insight ihn auf der zugehörigen Asset-Seite und meldet ihn. Dazu wird ein roter durchgehender Kreis angezeigt, gegebenenfalls per E-Mail-Benachrichtigung und im Dashboard für Verstöße oder einem benutzerdefinierten Dashboard, das Verstöße meldet.

Insight bietet einige Standard-Performance-Richtlinien, die Sie für die folgenden Objekte ändern oder löschen können, falls sie sich nicht auf Ihre Umgebung anwenden lassen:

- Hypervisor

  Es gibt Richtlinien für ESX-Swapping und ESX-Auslastung.

- Internes Volume und Volume

  Für jede Ressource gibt es zwei Latenzrichtlinien, eine mit Anmerkungen für Tier 1 und die andere mit Anmerkungen für Tier 2.

- Port

  Es gibt eine Richtlinie für BB-Kredit Null.

- Storage-Node

  Es gibt eine Richtlinie für die Node-Auslastung.

- Virtual Machine

  Es gibt VM-Swapping und Richtlinien für ESX-CPU und -Speicher.

- Datenmenge

  Es gibt Verzögerungen je Ebene und falsch ausgerichtete Volume-Richtlinien.

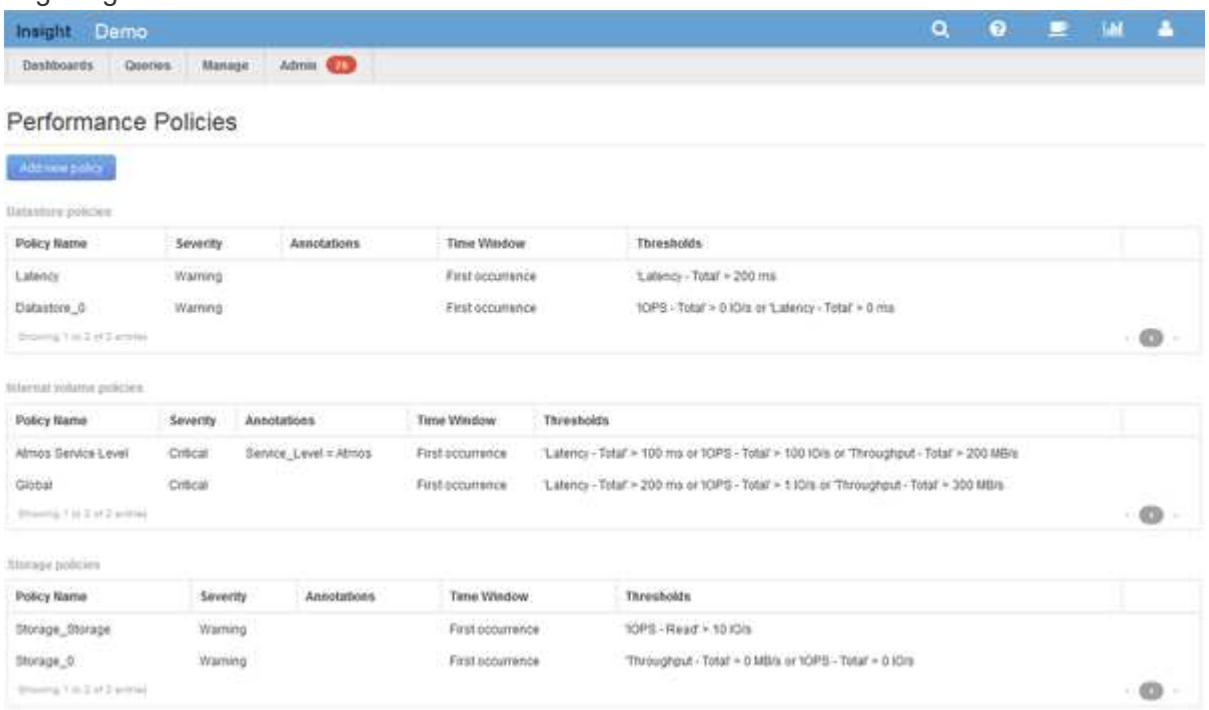
### Erstellung von Performance-Richtlinien

Sie erstellen Performance-Richtlinien, um Schwellenwerte festzulegen, die Warnmeldungen auslösen, um Sie über Probleme im Zusammenhang mit den Ressourcen in Ihrem Netzwerk zu informieren. Sie können beispielsweise eine Performance-Richtlinie erstellen, um Sie zu benachrichtigen, wenn die Gesamtauslastung für Storage-Pools über 60 % liegt.

#### Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser.
2. Wählen Sie **Verwalten** > **Leistungsrichtlinien** Aus.

   Die Seite Leistungsrichtlinien wird angezeigt.




   Richtlinien werden nach Objekten organisiert und in der Reihenfolge bewertet, in der sie in der Liste für das Objekt angezeigt werden.

3. Klicken Sie auf **Neue Richtlinie hinzufügen**.

Das Dialogfeld Richtlinie hinzufügen wird angezeigt.

4. Geben Sie im Feld **Richtlinienname** einen Namen für die Richtlinie ein.

   Sie müssen einen Namen verwenden, der sich von allen anderen Richtliniennamen für das Objekt unterscheidet. Sie können beispielsweise nicht zwei Richtlinien mit dem Namen „`Latency`“ für ein internes Volume verwenden. Sie können jedoch eine „`Latency`“-Richtlinie für ein internes Volume und eine weitere „`Latency`“-Richtlinie für ein anderes Volume haben. Es empfiehlt sich, immer einen eindeutigen Namen für eine Richtlinie zu verwenden, unabhängig vom Objekttyp.

5. Wählen Sie in der Liste **auf Objekte des Typs anwenden** den Objekttyp aus, für den die Richtlinie gilt.
6. Wählen Sie in der Liste **with annotation** ggf. einen Anmerkungstyp aus und geben Sie einen Wert für die Anmerkung in das Feld **Wert** ein, um die Richtlinie nur auf Objekte anzuwenden, die diesen speziellen Anmerkungssatz haben.
7. Wenn Sie **Port** als Objekttyp ausgewählt haben, wählen Sie aus der Liste **Connected To** aus, mit welchem Port verbunden ist.
8. Wählen Sie in der Liste **Übernehmen nach einem Fenster von** aus, wann eine Warnung ausgelöst wird, um eine Schwellenverletzung anzuzeigen.

   Die Option „Erstes Auftreten“ löst eine Warnung aus, wenn ein Schwellenwert bei der ersten Datenprobe überschritten wird. Alle anderen Optionen lösen eine Warnung aus, wenn der Schwellenwert einmal überschritten wird und mindestens die angegebene Zeit lang kontinuierlich überschritten wird.

9. Wählen Sie aus der Liste **with severity** den Schweregrad für die Verletzung aus.
10. Standardmäßig werden E-Mail-Benachrichtigungen zu Richtlinienverstößen an die Empfänger in der globalen E-Mail-Liste gesendet. Sie können diese Einstellungen überschreiben, sodass Benachrichtigungen für eine bestimmte Richtlinie an bestimmte Empfänger gesendet werden.
    - Klicken Sie auf den Link, um die Empfängerliste zu öffnen, und klicken Sie dann auf die Schaltfläche **+**, um Empfänger hinzuzufügen. Verstöße gegen diese Richtlinie werden an alle Empfänger in der Liste gesendet.
11. Klicken Sie auf den Link **any** im Abschnitt **Create alert if eines der folgenden sind wahr**, um zu steuern, wie Alarme ausgelöst werden:
    - **Beliebig**

      Dies ist die Standardeinstellung, die Warnungen erstellt, wenn einer der Schwellenwerte für eine Richtlinie überschritten wird.

    - * Alle*

      Durch diese Einstellung wird eine Meldung erstellt, wenn alle Schwellenwerte für eine Richtlinie überschritten werden. Wenn Sie **all** auswählen, wird der erste Schwellenwert, den Sie für eine Performance Policy erstellen, als primäre Regel bezeichnet. Sie müssen sicherstellen, dass der primäre Regelschwellenwert der Verstoß ist, den Sie für die Performance Policy am meisten befürchten.

12. Wählen Sie im Abschnitt **Warnung erstellen, wenn** einen Leistungszähler und einen Operator aus, und geben Sie dann einen Wert ein, um einen Schwellenwert zu erstellen.
13. Klicken Sie auf **Schwellenwert hinzufügen**, um weitere Schwellenwerte hinzuzufügen.
14. Um einen Schwellenwert zu entfernen, klicken Sie auf das Papierkorb-Symbol.
15. Aktivieren Sie das Kontrollkästchen **Verarbeitung weiterer Richtlinien beenden, wenn Warnung**

**generiert wird**, wenn die Policy die Verarbeitung beenden soll, wenn eine Warnung auftritt.

Wenn Sie beispielsweise vier Richtlinien für Datastores haben und die zweite Richtlinie so konfiguriert ist, dass sie die Verarbeitung bei Auftreten einer Meldung stoppt, werden die dritte und vierte Richtlinie nicht verarbeitet, während ein Verstoß gegen die zweite Richtlinie aktiv ist.

16. Klicken Sie Auf **Speichern**.

Die Seite Performance Policies wird angezeigt, und die Performance Policy wird in der Liste der Policies für den Objekttyp angezeigt.

#### Bewertung der Performance-Richtlinien Vorrang

Auf der Seite Performance Policies werden Richtlinien nach Objekttyp gruppiert. Insight bewertet die Richtlinien in der Reihenfolge, in der sie in der Liste der Performance-Richtlinien des Objekts aufgeführt werden. Sie können die Reihenfolge ändern, in der Insight Richtlinien auswertet, um die für Sie wichtigsten Informationen in Ihrem Netzwerk anzuzeigen.

Insight bewertet alle Richtlinien, die sequenziell für ein Objekt gelten, wenn Muster der Performance-Daten für das entsprechende Objekt in das System aufgenommen werden. Abhängig von Annotationen gelten jedoch nicht alle Richtlinien für eine Objektgruppe. Angenommen, das interne Volume verfügt über die folgenden Richtlinien:

- Richtlinie 1 (Standardrichtlinie von Insight)
- Richtlinie 2 (mit einer Annotation von „`Service Level = Silver`“ mit der Option **Verarbeitung weiterer Richtlinien beenden, wenn Warnung generiert wird**
- Richtlinie 3 (mit einer Annotation von „`Service Level = Gold`“)
- Richtlinie 4

Für eine interne Volume-Ebene mit einer Gold-Annotation bewertet Insight Richtlinie 1, ignoriert Richtlinie 2 und evaluiert anschließend Richtlinie 3 und Richtlinie 4. Für eine Stufe ohne Anmerkungen bewertet Insight nach der Reihenfolge der Richtlinien. Daher bewertet Insight nur Richtlinie 1 und Richtlinie 4. Für eine interne Volume-Ebene mit einer Silver-Annotation bewertet Insight die Richtlinien 1 und 2. Wird jedoch eine Meldung bei der Überschreitung des Richtlinienschwellenwerts ausgelöst und für das in der Richtlinie festgelegte Zeitfenster kontinuierlich überschritten, wird Insight die anderen Richtlinien in der Liste nicht mehr bewerten, während die aktuellen Zähler für das Objekt ausgewertet werden. Wenn Insight die nächsten Performance-Samples für das Objekt erfasst, beginnt es erneut, die Performance-Richtlinien für das Objekt nach Filter und anschließend nach Reihenfolge zu bewerten.

##### Ändern der Priorität einer Performance Policy

Standardmäßig bewertet Insight die Richtlinien eines Objekts sequenziell. Sie können die Reihenfolge konfigurieren, in der Insight die Performance-Richtlinien evaluiert. Wenn Sie beispielsweise eine Richtlinie konfiguriert haben, die die Verarbeitung bei einem Verstoß für Gold-Tier-Speicher beendet, können Sie diese Richtlinie an erster Stelle in der Liste platzieren und vermeiden, dass weitere allgemeine Verstöße für dieselbe Speicherressource auftreten.

**Schritte**

1. Öffnen Sie Insight in Ihrem Browser.
2. Wählen Sie im Menü **Verwalten** die Option **Leistungsrichtlinien** aus.

   Die Seite Leistungsrichtlinien wird angezeigt.

3. Bewegen Sie den Mauszeiger über einen Richtliniennamen in der Liste der Performance-Richtlinien eines Objekttyps.

   Die Rangfolge-Pfeile erscheinen rechts von der Richtlinie.

4. Um eine Richtlinie in der Liste nach oben zu verschieben, klicken Sie auf den Aufwärtspfeil. Um eine Richtlinie in der Liste nach unten zu verschieben, klicken Sie auf den Abwärtspfeil.

   Standardmäßig werden neue Richtlinien nacheinander zur Liste der Richtlinien eines Objekts hinzugefügt.

### Bearbeiten von Leistungsrichtlinien

Sie können vorhandene und standardmäßige Performance-Richtlinien bearbeiten, um zu ändern, wie Insight die für Sie in Ihrem Netzwerk geltenden Bedingungen überwacht. Sie können beispielsweise den Schwellenwert einer Richtlinie ändern.

#### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Wählen Sie im Menü **Verwalten** die Option **Leistungsrichtlinien** aus.

   Die Seite Leistungsrichtlinien wird angezeigt.

3. Bewegen Sie den Mauszeiger über einen Richtliniennamen in der Liste der Leistungsrichtlinien eines Objekts.
4. Klicken Sie Auf .

   Das Dialogfeld Richtlinie bearbeiten wird angezeigt.

5. Nehmen Sie die erforderlichen Änderungen vor.

   Wenn Sie eine andere Option als den Richtliniennamen ändern, löscht Insight alle vorhandenen Verstöße für diese Richtlinie.

6. Klicken Sie Auf **Speichern.**

### Löschen von Performance-Richtlinien

Sie können eine Performance-Richtlinie löschen, wenn Sie der Ansicht sind, dass sie nicht mehr für die Überwachung der Objekte in Ihrem Netzwerk gilt.

#### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Wählen Sie im Menü **Verwalten** die Option **Leistungsrichtlinien** aus.

Die Seite Leistungsrichtlinien wird angezeigt.

3. Bewegen Sie den Mauszeiger über den Namen einer Richtlinie in der Liste der Leistungsrichtlinien eines Objekts.
4. Klicken Sie Auf ✖.

   Es wird eine Meldung angezeigt, in der Sie gefragt werden, ob Sie die Richtlinie löschen möchten.

5. Klicken Sie auf **OK**.

## Importieren und Exportieren von Benutzerdaten

Mit den Import- und Exportfunktionen können Sie Anmerkungen, Anmerkungsregeln, Abfragen, Performance-Richtlinien und benutzerdefinierte Dashboards in eine Datei exportieren. Diese Datei kann dann in verschiedene OnCommand Insight-Server importiert werden.

Die Export- und Importfunktionen werden nur zwischen Servern unterstützt, auf denen dieselbe Version von OnCommand Insight ausgeführt wird.

Um Benutzerdaten zu exportieren oder zu importieren, klicken Sie auf **Admin** und wählen **Setup**, und wählen Sie dann die Registerkarte **Benutzerdaten importieren/exportieren**.

Während des Importvorgangs werden je nach importierten Objekten und Objekttypen Daten hinzugefügt, zusammengeführt oder ersetzt.

- Anmerkungstypen
  - Fügt eine Anmerkung hinzu, wenn im Zielsystem keine Anmerkung mit demselben Namen vorhanden ist.
  - Fügt eine Anmerkung zusammen, wenn der Anmerkungstyp eine Liste ist, und eine Anmerkung mit dem gleichen Namen existiert im Zielsystem.
  - Ersetzt eine Anmerkung, wenn der Anmerkungstyp eine andere als eine Liste ist und eine Anmerkung mit dem gleichen Namen im Zielsystem vorhanden ist.

  ⓘ Wenn im Zielsystem eine Anmerkung mit demselben Namen, jedoch mit einem anderen Typ vorhanden ist, schlägt der Import fehl. Wenn Objekte von der fehlgeschlagenen Annotation abhängen, können diese Objekte falsche oder unerwünschte Informationen anzeigen. Nach Abschluss des Importvorgangs müssen alle Anmerkungsabhängigkeiten geprüft werden.

- Anmerkungsregeln
  - Fügt eine Anmerkungsregel hinzu, wenn im Zielsystem keine Anmerkungsregel mit demselben Namen vorhanden ist.
  - Ersetzt eine Anmerkungsregel, wenn im Zielsystem eine Anmerkungsregel mit demselben Namen vorhanden ist.

  ⓘ Anmerkungsregeln hängen von Abfragen und Anmerkungen ab. Nach Abschluss des Importvorgangs müssen alle Anmerkungsregeln auf ihre Genauigkeit überprüft werden.

- Richtlinien

- Fügt eine Richtlinie hinzu, wenn im Zielsystem keine Richtlinie mit demselben Namen vorhanden ist.
- Ersetzt eine Richtlinie, wenn im Zielsystem eine Richtlinie mit demselben Namen vorhanden ist.

> Richtlinien können nach Abschluss des Importvorgangs außer Betrieb sein. Sie müssen die Richtlinienreihenfolge nach dem Import überprüfen. Richtlinien, die von Anmerkungen abhängen, können fehlschlagen, wenn die Anmerkungen falsch sind. Nach dem Import müssen alle Anmerkungsabhängigkeiten überprüft werden.
>
> +

- Abfragen
  - Fügt eine Abfrage hinzu, wenn im Zielsystem keine Abfrage mit demselben Namen vorhanden ist.
  - Ersetzt eine Abfrage, wenn im Zielsystem eine Abfrage mit demselben Namen vorhanden ist, auch wenn der Ressourcentyp der Abfrage unterschiedlich ist.

> Wenn der Ressourcentyp einer Abfrage anders ist, können nach dem Import alle Dashboard-Widgets, die diese Abfrage verwenden, unerwünschte oder falsche Ergebnisse anzeigen. Sie müssen nach dem Import alle abfragebasierten Widgets auf ihre Genauigkeit überprüfen. Abfragen, die von Anmerkungen abhängig sind, können fehlschlagen, wenn die Anmerkungen falsch sind. Nach dem Import müssen alle Anmerkungsabhängigkeiten überprüft werden.
>
> +

- Dashboards
  - Fügt ein Dashboard hinzu, wenn im Zielsystem kein Dashboard mit demselben Namen vorhanden ist.
  - Ersetzt ein Dashboard, wenn im Zielsystem ein Dashboard mit demselben Namen vorhanden ist, auch wenn der Ressourcentyp der Abfrage unterschiedlich ist.

> Sie müssen nach dem Import alle abfragebasierten Widgets in Dashboards auf ihre Genauigkeit überprüfen. Wenn der Quellserver über mehrere Dashboards mit demselben Namen verfügt, werden alle exportiert. Allerdings wird nur der erste auf den Zielserver importiert. Um Fehler beim Import zu vermeiden, sollten Sie sicherstellen, dass Ihre Dashboards vor dem Exportieren eindeutige Namen haben.
>
> +

# Insight Sicherheit

OnCommand Insight bietet Funktionen, mit denen Insight Umgebungen sicherer betrieben werden können. Diese Funktionen umfassen Verschlüsselung, Passwort-Hashing und die Möglichkeit, interne Benutzerpasswörter und Schlüsselpaare zu ändern, die Kennwörter verschlüsseln und entschlüsseln. Sie können diese Funktionen auf allen Servern in der Insight-Umgebung mit dem SecurityAdmin-Tool verwalten.

## Was ist das SecurityAdmin-Tool?

Das Sicherheits-Admin-Tool unterstützt Änderungen am Inhalt der Vaults sowie koordinierte Änderungen an der OnCommand Insight-Installation.

Die primären Verwendungszwecke für das SecurityAdmin-Tool sind **Backup** und **Restore** der Sicherheitskonfiguration (d.h. Tresor) und Passwörter. Sie können beispielsweise den Tresor auf einer lokalen Erfassungseinheit sichern und auf einer Remote-Erfassungseinheit wiederherstellen, um die Passwortkoordination in Ihrer gesamten Umgebung sicherzustellen. Oder wenn Sie mehrere OnCommand Insight-Server in Ihrer Umgebung haben, möchten Sie möglicherweise ein Backup des Server-Tresors erstellen und diese auf anderen Servern wiederherstellen, um die Passwörter unverändert zu halten. Dies sind nur zwei Beispiele für die Art und Weise, wie SecurityAdmin verwendet werden kann, um die Kohäsion in Ihren Umgebungen zu gewährleisten.

Es wird dringend empfohlen, den Vault * zu sichern, wenn Sie eine OnCommand Insight-Datenbank sichern. Andernfalls kann der Zugriff verloren gehen.

Das Tool bietet sowohl **Interactive** als auch **command line** Modi.

Viele Operationen des SecurityAdmin Tools ändern den Inhalt des Tresors und nehmen auch Änderungen an der Installation vor, um sicherzustellen, dass der Tresor und die Installation synchron bleiben.

Beispiel:

- Wenn Sie ein Insight-Benutzerpasswort ändern, wird der Benutzereintrag in der Tabelle SANscreen.Users mit dem neuen Hash aktualisiert.
- Wenn Sie das Passwort eines MySQL-Benutzers ändern, wird die entsprechende SQL-Anweisung ausgeführt, um das Kennwort des Benutzers in der MySQL-Instanz zu aktualisieren.

In einigen Situationen werden mehrere Änderungen an der Installation vorgenommen:

- Wenn Sie den dwh MySQL-Benutzer ändern, werden neben der Aktualisierung des Passworts in der MySQL-Datenbank auch mehrere Registrierungseinträge für ODBC aktualisiert.

In den folgenden Abschnitten wird der Begriff "koordinierte Änderungen" verwendet, um diese Änderungen zu beschreiben.

## Ausführungsmodi

- Normaler/Standardbetrieb – der SANscreen-Serverdienst muss ausgeführt werden

  Für den Standardausführungsmodus erfordert das SecurityAdmin-Tool, dass der **SANscreen-Serverdienst** ausgeführt wird. Der Server wird für die Authentifizierung verwendet, und viele koordinierte Änderungen an der Installation werden durch Aufrufen des Servers vorgenommen.

- Direkter Betrieb – der SANscreen-Serverdienst wird möglicherweise ausgeführt oder angehalten.

  Bei Ausführung auf einem OCI-Server oder einer DWH-Installation kann das Tool auch im „direkten“ Modus ausgeführt werden. In diesem Modus werden Authentifizierung und koordinierte Änderungen über die Datenbank durchgeführt. Der Serverdienst wird nicht verwendet.

  Der Betrieb ist mit dem normalen Modus identisch, mit den folgenden Ausnahmen:

- Die Authentifizierung wird nur für Benutzer unterstützt, die keine Domäne haben. (Benutzer, deren Passwort und Rollen sich in der Datenbank befinden, nicht LDAP).
- Der Vorgang „Schlüssel ersetzen“ wird nicht unterstützt.
- Der Schritt zur erneuten Verschlüsselung der Vault-Wiederherstellung wird übersprungen.

- Wiederherstellungsmodus das Tool kann auch dann ausgeführt werden, wenn der Zugriff auf den Server und die Datenbank nicht möglich ist (z. B. weil das Root-Passwort im Tresor falsch ist).

  Bei Ausführung in diesem Modus ist keine Authentifizierung möglich und daher kann kein Vorgang mit koordinierter Änderung der Installation durchgeführt werden.

  Der Wiederherstellungsmodus kann verwendet werden, um:

- Bestimmen Sie, welche Vault-Einträge falsch sind (mit dem Verifizierungs-Vorgang).
- Ersetzen Sie das falsche Root-Passwort durch den richtigen Wert. (Das Passwort wird dadurch nicht geändert. Der Benutzer muss das aktuelle Passwort eingeben.)

> Wenn das Root-Passwort im Tresor falsch ist und das Passwort nicht bekannt ist und es keine Sicherung des Tresors mit dem korrekten Root-Passwort gibt, kann die Installation nicht mit dem SecurityAdmin-Tool wiederhergestellt werden. Die einzige Möglichkeit, die Installation wiederherzustellen, ist das Zurücksetzen des Passworts der MySQL-Instanz nach dem unter dokumentierten Verfahren https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Verwenden Sie nach dem Zurücksetzen den Vorgang Correct-stored-password, um das neue Passwort in den Tresor einzugeben.

## Befehle

### Unbeschränkte Befehle

Unbeschränkte Befehle nehmen alle koordinierten Änderungen an der Installation vor (außer Vertrauensstellungen). Unbeschränkte Befehle können ohne Benutzerauthentifizierung ausgeführt werden.

| Befehl | Beschreibung |
|---|---|
| Backup-Vault | Erstellen Sie eine ZIP-Datei mit dem Tresor. Der relative Pfad zu den Vault-Dateien stimmt mit dem Pfad der Vaults relativ zum Installationsroot überein.<br>• wildfly/Standalone/Configuration/Vault/*<br>• acq/conf/Vault/* |
| Nach Standardschlüsseln suchen | Überprüfen Sie, ob die Schlüssel des Tresors mit denen des Standard-Tresors übereinstimmen, der in Instanzen vor 7.3.16 verwendet wird. |
| Korrekt gespeichertes Passwort | Ersetzen Sie ein (falsches) Kennwort, das im Tresor gespeichert ist, durch das korrekte Kennwort, das dem Benutzer bekannt ist.<br>Dies kann verwendet werden, wenn der Tresor und die Installation nicht konsistent sind. **Beachten Sie, dass es das eigentliche Passwort in der Installation nicht ändert.** |
| Change-Trust-Store-password | Ändern Sie das für einen Vertrauensspeicher verwendete Passwort, und speichern Sie das neue Kennwort im Tresor. Das aktuelle Kennwort des Vertrauenshauses muss „bekannt“ sein. |

| | |
|---|---|
| Verify-keystore | Prüfen Sie, ob die Werte im Tresor korrekt sind:<br>• Stimmt der Hash des Passworts für OCI-Benutzer mit dem Wert in der Datenbank überein<br>• Für MySQL-Benutzer kann eine Datenbankverbindung hergestellt werden<br>• Für Schlüsselspeicher kann der Schlüsselspeicher geladen und seine Schlüssel (falls vorhanden) gelesen werden |
| Listentasten | Einträge im Tresor auflisten (ohne Anzeige des gespeicherten Wertes) |

**Eingeschränkte Befehle**

Für alle nicht verborgenen Befehle, die koordinierte Änderungen an der Installation vornehmen, ist eine Authentifizierung erforderlich:

| Befehl | Beschreibung |
|---|---|
| Restore-Vault-Backup | Ersetzt den aktuellen Tresor durch den Tresor, der in der angegebenen Vault-Sicherungsdatei enthalten ist.<br>Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Kennwörtern im wiederhergestellten Tresor entspricht:<br>• Aktualisieren Sie die Benutzerpasswörter für die OCI-Kommunikation<br>• Aktualisieren Sie die MySQL-Benutzerpasswörter, einschließlich Root<br>• Wenn das Schlüsselspeicher-Passwort „bekannt“ ist, aktualisieren Sie den Schlüsselspeicher mit den Kennwörtern aus dem wiederhergestellten Tresor.<br>Bei der Ausführung im normalen Modus werden auch alle verschlüsselten Werte von der Instanz gelesen, mit dem Verschlüsselungsdienst des aktuellen Tresors entschlüsselt, mit dem Verschlüsselungsdienst des wiederhergestellten Tresors erneut verschlüsselt und der neu verschlüsselte Wert gespeichert. |
| Sync-with-Vault | Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Benutzerpasswörtern im wiederhergestellten Tresor entspricht:<br>• Aktualisiert die Benutzerpasswörter für die OCI-Kommunikation<br>• Aktualisiert die MySQL-Benutzerpasswörter, einschließlich Root |
| Passwort ändern | Ändert das Passwort im Tresor und führt die koordinierten Aktionen durch. |
| Schlüssel ersetzen | Erstellen Sie einen neuen leeren Tresor (der andere Schlüssel als der vorhandene Tresor hat). Kopieren Sie dann die Einträge aus dem aktuellen Tresor in den neuen Tresor. Liest dann jeden verschlüsselten Wert aus der Instanz, entschlüsselt ihn mit dem Verschlüsselungsdienst des aktuellen Tresors, verschlüsselt ihn mit dem Verschlüsselungsdienst des wiederhergestellten Tresors und speichert den neu verschlüsselten Wert. |

### Ausgeblendete Befehle

Das SA-Tool bietet die folgenden Befehle, die keine Authentifizierung erfordern, aber koordinierte Änderungen an der Installation vornehmen.

| | |
|---|---|
| Aktualisierung der Listenschlüssel (Server) | Wenn sich der Benutzer nicht authentifiziert hat, authentifizieren Sie sich mit dem _internen Konto und Passwort im aktuellen Tresor. Ersetzen Sie dann den aktuellen Tresor durch den Tresor in der Sicherungsdatei, und führen Sie die koordinierten Aktionen durch. |
| Upgrade (Anschaffung) | Ersetzen Sie den aktuellen Tresor durch den Tresor in der Sicherungsdatei, und führen Sie die koordinierten Aktionen durch. |

## Koordinierte Maßnahmen

### Server Vault

| | |
|---|---|
| _Intern | Passwort-Hash für Benutzer in Datenbank aktualisieren |
| Akquisition | Passwort-Hash für Benutzer in Datenbank aktualisieren<br><br>Wenn der Akquisitionssault vorhanden ist, aktualisieren Sie auch den Eintrag im Akquisitions-Vault |
| dwh_intern | Passwort-Hash für Benutzer in Datenbank aktualisieren |
| cognos_admin | Passwort-Hash für Benutzer in Datenbank aktualisieren<br><br>Wenn DWH und Windows, aktualisieren Sie SANscreen/cognos/Analytics/Configuration/SANscreenAP.properties, um die Eigenschaft cognos.admin auf das Passwort zu setzen. |
| Stamm | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| Inventar | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |

| | |
|---|---|
| dwh | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren<br><br>Wenn DWH und Windows, aktualisieren Sie die Windows-Registrierung, um die folgenden ODBC-bezogenen Einträge auf das neue Passwort zu setzen:<br><br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD<br>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Cloud_Cost\PWD |
| Whuser | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| Hosts | Führen Sie SQL aus, um das Benutzerpasswort in der MySQL-Instanz zu aktualisieren |
| Keystore_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.keystore |
| Trustore_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/Server.trustore |
| Key_password | Schreiben Sie den Keystore mit dem neuen Passwort neu - wildfly/Standalone/Configuration/sso.jks |
| cognos_Archive | Keine |

**Akquisitions-Vault**

| | |
|---|---|
| Akquisition | Keine |
| Trustore_password | Schreiben Sie den Keystore mit dem neuen Passwort (falls vorhanden) neu - acq/conf/cert/Client.keystore |

## Ausführen des Security Admin Tools - Befehlszeile

Die Syntax zum Ausführen des SA-Tools im Befehlszeilenmodus lautet:

```
securityadmin [-s | -au] [-db] [-lu <user> [-lp <password>]] <additional-
options>

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

-lu <user>              user for authentication
-lp <password>          password for authentication
<addition-options>      specifies command and command arguments as
described below
```

Hinweise:

- Die Option „-i“ ist möglicherweise nicht in der Befehlszeile vorhanden (da hier der interaktive Modus ausgewählt wird).
- Für die Optionen „-s“ und „-au“:
  - „-s“ ist auf einer rau nicht zulässig
  - „-au“ ist auf DWH nicht zulässig
  - Wenn keines vorhanden ist, dann
    - Der Server-Vault wird auf Server, DWH und Dual ausgewählt
    - Der Aufnahmevault wird auf der rau ausgewählt
- Die Optionen -lu und -lp werden für die Benutzerauthentifizierung verwendet.
  - Wenn <user> angegeben ist und <password> nicht angegeben ist, wird der Benutzer zur Eingabe des Passworts aufgefordert.
  - Wenn <user> nicht bereitgestellt wird und eine Authentifizierung erforderlich ist, wird der Benutzer aufgefordert, sowohl <user> als auch <password> einzugeben.

**Befehle:**

| Befehl | Zu Verwenden |
| --- | --- |
| Korrekt gespeichertes Passwort | `securityadmin [-s` |
| -au] [-db] -pt <key> [<value>]<br><br>`where`<br><br>-pt specifies the command ("put")<br><key> is the key<br><value> is the value. If not present, user will be prompted for value<br><br> | Backup-Vault |
| `securityadmin [-s` | -au] [-db] -b [<backup-dir>]<br><br>where<br><br>-b specified command<br><backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used<br>The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip |
| Backup-Vault | `securityadmin [-s` |

| | |
|---|---|
| -au] [-db] -ub <backup-file><br><br>where<br><br>-ub specified command ("upgrade-backup")<br><backup-file> The location to write the backup file<br><br>``` | Listentasten |
| ```<br>securityadmin [-s<br>``` | -au] [-db] -l<br><br>where<br><br>-l specified command<br><br>``` |
| Prüfschlüssel | ```<br>securityadmin [-s<br>``` |
| -au] [-db] -ck<br><br>where<br><br>-ck specified command<br><br>exit code:<br>1 error<br>2 default key(s)<br>3 unique keys<br><br>``` | Verify-keystore (Server) |
| ```<br>securityadmin [-s] [-db] -v<br><br>where<br><br>-v specified command<br>``` | Upgrade |

| | |
|---|---|
| `securityadmin [-s` | -au] [-db] [-lu <user>] [-lp <password>] -u<br><br>where<br><br>-u specified command<br><br>For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault.<br>For acquisition vault, if -lu is not present, then no authentication will be attempted<br><br>`` |
| Schlüssel ersetzen | `securityadmin [-s` |
| -au] [-db] [-lu <user>] [-lp <password>] -rk<br><br>where<br><br>-rk specified command<br><br>`` | Restore-Vault-Backup |
| `securityadmin [-s` | -au] [-db] [-lu <user>] [-lp <password>] -r <backup-file><br><br>where<br><br>-r specified command<br><backup-file> the backup file location<br><br>`` |
| Change-Password (Server) | `securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`<br><br>`where`<br><br>`-up specified command ("update-password")`<br>`-un <user> entry ("user") name to update`<br>`-p <password> new password. If <password not supplied, user will be prompted.`<br>`-sh for mySQL user, use strong hash` |

| | |
|---|---|
| Change-Passwort für Akquisitionsbenutzer (Akquisition) | `securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`<br><br>`where`<br><br>`-up specified command ("update-password") -p <password> new password. If <password not supplied, user will be prompted.` |
| Change-password für Truststore-_password (Akquisition) | `securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`<br><br>`where`<br><br>`-utp specified command ("update-truststore-password") -p <password> new password. If <password not supplied, user will be prompted.` |
| Synchronisieren mit Tresor (Server) | `securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`<br><br>`where`<br><br>`-sv specified command` |

## Ausführen des Security Admin Tools – Interaktiver Modus

### Interaktiv – Hauptmenü

Um das SA-Tool im interaktiven Modus auszuführen, geben Sie den folgenden Befehl ein:

```
 securityadmin -i
Bei einer Server- oder Doppelinstallation fordert SecurityAdmin den
Benutzer auf, entweder den Server oder die lokale Erfassungseinheit
auszuwählen.
```

Knoten der Server- und Erfassungseinheit erkannt! Wählen Sie den Knoten aus, dessen Sicherheit neu konfiguriert werden muss:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

Auf DWH wird automatisch „Server“ ausgewählt. Auf einer externen AU wird automatisch „Acquisition Unit“ ausgewählt.

**Interactive - Server: Wiederherstellung des Root-Passworts**

Im Server-Modus überprüft das SecurityAdmin-Tool zunächst, ob das gespeicherte Root-Passwort korrekt ist. Wenn dies nicht der Fall ist, zeigt das Tool den Bildschirm zur Wiederherstellung des Root-Passworts an.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Drücken Sie ENTER, um zum Wiederherstellungsmenü zurückzukehren.
```

**Interactive - Server: Korrektes Passwort**

Mit der Aktion „Passwort korrigieren“ wird das im Tresor gespeicherte Passwort so geändert, dass es mit dem für die Installation erforderlichen Kennwort übereinstimmt. Dieser Befehl ist nützlich in Situationen, in denen eine Änderung an der Installation durch etwas anderes als das securityadmin-Tool vorgenommen wurde. Beispiele:

- Das Passwort für einen SQL-Benutzer wurde durch direkten Zugriff auf MySQL geändert.
- Ein Keystore wird ersetzt oder das Passwort eines Keystore wird mit keytool geändert.
- Eine OCI Datenbank wurde wiederhergestellt, und diese Datenbank enthält unterschiedliche Passwörter für die internen Benutzer

„Passwort korrigieren“ fordert den Benutzer zuerst auf, das Kennwort auszuwählen, um den richtigen Wert zu speichern.

```
Replace incorrect stored password with correct password.  (Does not change
the required password)
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Nach Auswahl des zu korrigenden Eintrags wird der Benutzer gefragt, wie er den Wert angeben möchte.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Wenn Option 1 ausgewählt ist, wird der Benutzer aufgefordert, das richtige Passwort einzugeben.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Wenn das richtige Passwort eingegeben wird, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers
zurück.
```

Wenn das falsche Passwort eingegeben wird, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER kehren Sie zum uneingeschränkten Menü des Servers zurück.

Wenn Option 2 ausgewählt ist, wird der Benutzer aufgefordert, den Namen einer Sicherungsdatei anzugeben, aus der das korrekte Kennwort gelesen werden soll:

```
 Enter Backup File Location:
Wenn das Passwort aus dem Backup korrekt ist, wird Folgendes angezeigt.
```

```
 Password verified.  Vault updated
Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers
angezeigt.
```

Wenn das Passwort im Backup nicht korrekt ist, wird Folgendes angezeigt

```
Password verification failed - {additional information}
Vault entry not updated.
```

Durch Drücken von ENTER wird das Menü ohne Einschränkung des Servers angezeigt.

**Interactive - Server: Überprüfen Sie Den Inhalt Des Tresores**

Überprüfen Sie, ob Vault Contents Schlüssel enthält, die mit dem StandardVault übereinstimmen, der mit früheren OCI-Versionen verteilt ist, und überprüft, ob jeder Wert im Vault mit der Installation übereinstimmt.

Die möglichen Ergebnisse für jeden Schlüssel sind:

| | |
|---|---|
| OK | Der Vault-Wert ist korrekt |

| | |
|---|---|
| Nicht Aktiviert | Der Wert kann nicht mit der Installation verglichen werden |
| SCHLECHT | Der Wert stimmt nicht mit der Installation überein |
| Fehlt | Ein erwarteter Eintrag fehlt. |

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

**Interaktiv – Server: Sicherung**

Beim Backup wird das Verzeichnis angezeigt, in dem die ZIP-Sicherungsdatei gespeichert werden soll. Das Verzeichnis muss bereits vorhanden sein, und der Dateiname lautet ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

**Interactive - Server: Anmeldung**

Die Anmeldeaktion wird verwendet, um einen Benutzer zu authentifizieren und Zugriff auf Vorgänge zu erhalten, die die Installation ändern. Der Benutzer muss über Admin-Privileges verfügen. Bei der Ausführung mit dem Server kann jeder Admin-Benutzer verwendet werden; bei der Ausführung im direkten Modus muss der Benutzer ein lokaler Benutzer und kein LDAP-Benutzer sein.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

Oder

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Wenn das Passwort korrekt ist und der Benutzer ein Admin-Benutzer ist, wird das Menü eingeschränkt angezeigt.

Wenn das Passwort falsch ist, wird Folgendes angezeigt:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Wenn der Benutzer kein Administrator ist, wird Folgendes angezeigt:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

**Interactive - Server: Eingeschränktes Menü**

Sobald sich der Benutzer angemeldet hat, zeigt das Tool das eingeschränkte Menü an.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

**Interactive - Server: Passwort Ändern**

Mit der Aktion „Passwort ändern“ können Sie ein Installationspasswort in einen neuen Wert ändern.

„Kennwort ändern“ fordert den Benutzer zuerst auf, das zu ändernde Kennwort auszuwählen.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Wenn der Benutzer ein MySQL-Benutzer ist, wird der Benutzer nach der Auswahl des zu korrigenden Eintrags gefragt, ob er das Passwort stark hashing

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Anschließend wird der Benutzer zur Eingabe des neuen Passworts aufgefordert.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Wenn ein nicht leeres Passwort eingegeben wird, wird der Benutzer aufgefordert, das Passwort zu bestätigen.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Wenn die Änderung nicht erfolgreich war, wird der Fehler oder die Ausnahme angezeigt.

**Interaktiv – Server: Wiederherstellen**

**Interactive - Server: Ändern Sie Die Verschlüsselungsschlüssel**

Die Aktion Verschlüsselungsschlüssel ändern ersetzt den Verschlüsselungsschlüssel, der zum Verschlüsseln der Vault-Einträge verwendet wird, und ersetzt den Verschlüsselungsschlüssel, der für den Verschlüsselungsdienst des Tresors verwendet wird. Da der Schlüssel des Verschlüsselungsdienstes geändert wird, werden verschlüsselte Werte in der Datenbank erneut verschlüsselt; sie werden gelesen, mit dem aktuellen Schlüssel entschlüsselt, mit dem neuen Schlüssel verschlüsselt und in der Datenbank gespeichert.

Diese Aktion wird im direkten Modus nicht unterstützt, da der Server für einige Datenbankinhalte die erneute Verschlüsselung bereitstellt.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

**Interactive - Server: Installation Beheben**

Mit der Aktion Installation beheben wird die Installation aktualisiert. Alle Installationspasswörter, die über das securityadmin-Tool außer root geändert werden können, werden auf die Passwörter im Tresor gesetzt.

- Die Passwörter interner OCI-Benutzer werden aktualisiert.
- Die Passwörter von MySQL-Benutzern, mit Ausnahme von root, werden aktualisiert.
- Die Passwörter der Schlüsselspeicher werden aktualisiert.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

Die Aktion wird bei der ersten nicht erfolgreichen Aktualisierung angehalten und zeigt den Fehler oder die Ausnahme an.

## Sicherheitsmanagement auf dem Insight-Server

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Insight-Server verwalten. Die Sicherheitsverwaltung umfasst das Ändern von Kennwörtern, das Generieren neuer Schlüssel, das Speichern und Wiederherstellen von von von von Ihnen erstellten Sicherheitskonfigurationen oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

## Verwaltung der Sicherheit auf der lokalen Erfassungseinheit

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen für den lokalen Akquisitionsbenutzer (LAU) verwalten. Die Sicherheitsverwaltung umfasst das Verwalten von Schlüsseln und Passwörtern, das Speichern und Wiederherstellen von Sicherheitskonfigurationen, die Sie erstellen oder auf die Standardeinstellungen wiederherstellen.

### Bevor Sie beginnen

Dieser muss unbedingt vorhanden sein `admin` Berechtigungen zum Ausführen von Sicherheitskonfigurationsaufgaben.

### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

## Verwaltung der Sicherheit auf einer rau

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf raus verwalten. Möglicherweise müssen Sie eine Vault-Konfiguration sichern oder wiederherstellen, Verschlüsselungsschlüssel ändern oder Kennwörter für die Erfassungseinheiten aktualisieren.

### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Ein Szenario für die Aktualisierung der Sicherheitskonfiguration für die LAU/rau ist die Aktualisierung des Benutzerpassworts für die Erfassung, wenn das Kennwort für diesen Benutzer auf dem Server geändert wurde. Die LAU und alle raus verwenden das gleiche Passwort wie das des Benutzer „Acquisition“ des Servers, um mit dem Server zu kommunizieren.

Der Benutzer „Acquisition“ ist nur auf dem Insight-Server vorhanden. Die rau oder LAU melden sich als dieser Benutzer an, wenn sie eine Verbindung zum Server herstellen.

Weitere Informationen finden Sie in den "Sicherheitstool" Anweisungen.

## Verwaltung der Sicherheit im Data Warehouse

Der `securityadmin` Mit dem Tool können Sie Sicherheitsoptionen auf dem Data Warehouse-Server verwalten. Die Sicherheitsverwaltung umfasst die Aktualisierung interner Passwörter für interne Benutzer auf dem DWH-Server, das Erstellen von Backups der Sicherheitskonfiguration oder das Wiederherstellen von Konfigurationen auf die Standardeinstellungen.

### Über diese Aufgabe

Sie verwenden das `securityadmin` Tool zur Verwaltung der Sicherheit:

- Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux `/bin/oci-securityadmin.sh`

Weitere Informationen finden Sie in der "Sicherheitsadministration" Dokumentation.

## Ändern der internen OnCommand Insight-Benutzerpasswörter

In Sicherheitsrichtlinien müssen Sie möglicherweise die Passwörter in Ihrer OnCommand Insight-Umgebung ändern. Einige der Passwörter auf einem Server sind auf einem anderen Server in der Umgebung vorhanden, sodass Sie das Passwort auf beiden Servern ändern müssen. Wenn Sie beispielsweise das Benutzerpasswort „`inventar`“ auf dem Insight Server ändern, müssen Sie das Benutzerpasswort „`inventar`“ auf dem für diesen Insight Server konfigurierten Data Warehouse Server Connector zuordnen.

### Bevor Sie beginnen

Sie sollten die Abhängigkeiten der Benutzerkonten verstehen, bevor Sie Passwörter ändern. Wenn Passwörter nicht auf allen erforderlichen Servern aktualisiert werden, kommt es zu Kommunikationsfehlern zwischen den Insight-Komponenten.

### Über diese Aufgabe

In der folgenden Tabelle sind die internen Benutzerpasswörter für den Insight Server aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Passwort übereinstimmen müssen.

| Passwörter Für Insight Server | Erforderliche Änderungen |
|---|---|
| _Intern | |
| Akquisition | LAU, RAU |
| dwh_intern | Data Warehouse |
| Hosts | |
| Inventar | Data Warehouse |
| Stamm | |

In der folgenden Tabelle sind die internen Benutzerkennwörter für das Data Warehouse und die Insight-Komponenten mit abhängigen Kennwörtern aufgeführt, die mit dem neuen Kennwort übereinstimmen müssen.

| Data Warehouse-Passwörter | Erforderliche Änderungen |
|---|---|
| cognos_admin | |
| dwh | |
| dwh_Internal (geändert mit der Server Connector-Konfigurationsoberfläche) | Insight Server |
| Whuser | |
| Hosts | |
| Inventarisierung (geändert mit der Server Connector-Konfigurationsoberfläche) | Insight Server |
| Stamm | |

### Ändern von Kennwörtern in der DWH Server Connection Configuration UI

In der folgenden Tabelle ist das Benutzerpasswort für DIE LAU aufgeführt und die Insight-Komponenten mit abhängigen Kennwörtern, die mit dem neuen Passwort übereinstimmen müssen.

| LAU-Passwörter | Erforderliche Änderungen |
|---|---|
| Akquisition | Insight Server, rau |

### Ändern der Passwörter „inventar“ und „dwh_internal“ mithilfe der Benutzeroberfläche für die Serververbindungskonfiguration

Wenn Sie die Passwörter „`inventar`“ oder „`dwh_internal`“ so ändern müssen, dass sie mit denen auf dem Insight-Server übereinstimmen, verwenden Sie die Data Warehouse-Benutzeroberfläche.

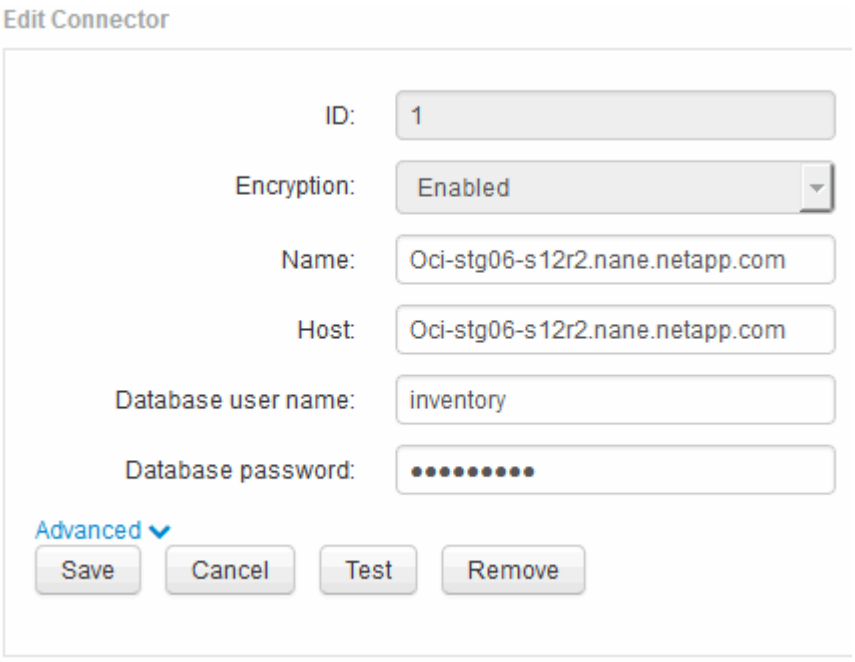
#### Bevor Sie beginnen

Sie müssen als Administrator angemeldet sein, um diese Aufgabe ausführen zu können.

#### Schritte

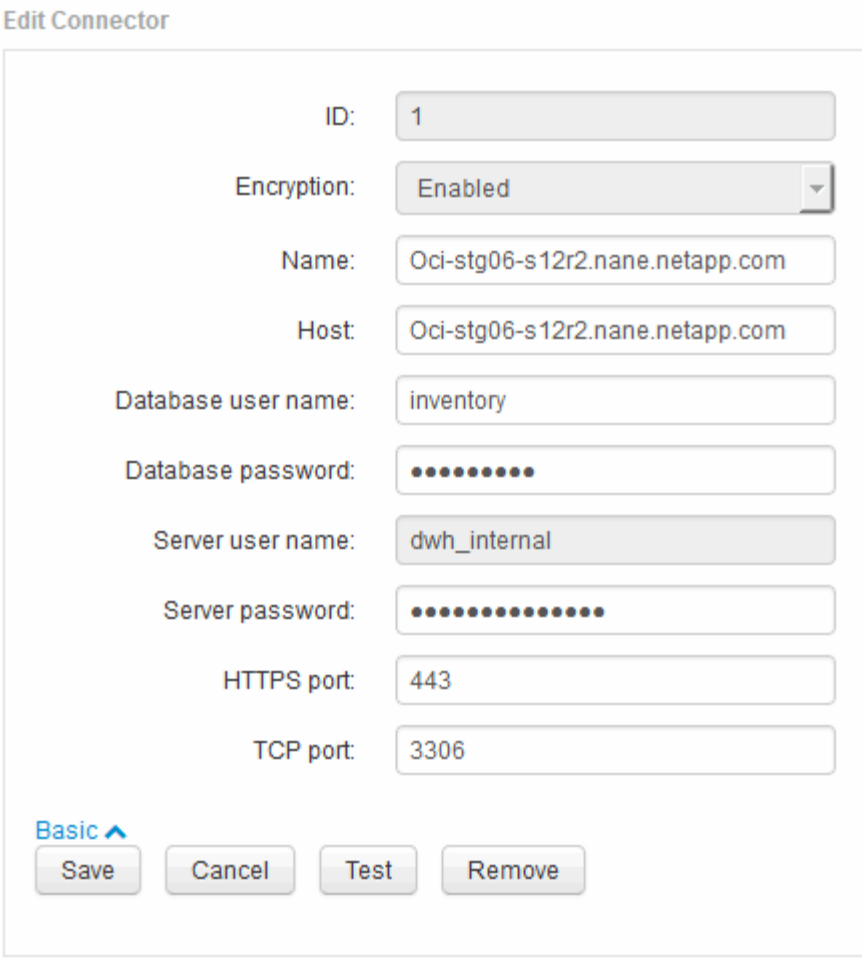
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   Der Bildschirm **Connector bearbeiten** wird angezeigt.




3. Geben Sie ein neues „`Inventory`“-Passwort für das Feld **Datenbankkennwort** ein.
4. Klicken Sie Auf **Speichern**
5. Um das Passwort „`dwh_internal`“ zu ändern, klicken Sie auf **Erweitert.**

   Der Bildschirm Edit Connector Advanced wird angezeigt.




6. Geben Sie das neue Passwort in das Feld **Server-Passwort** ein:
7. Klicken Sie auf Speichern.

### Ändern des dwh-Kennworts mit dem ODBC-Verwaltungstool

Wenn Sie das Passwort für den dwh-Benutzer auf dem Insight-Server ändern, muss das Passwort auch auf dem Data Warehouse-Server geändert werden. Sie verwenden das ODBC-Datenquellenadministrator-Tool, um das Kennwort im Data Warehouse zu ändern.

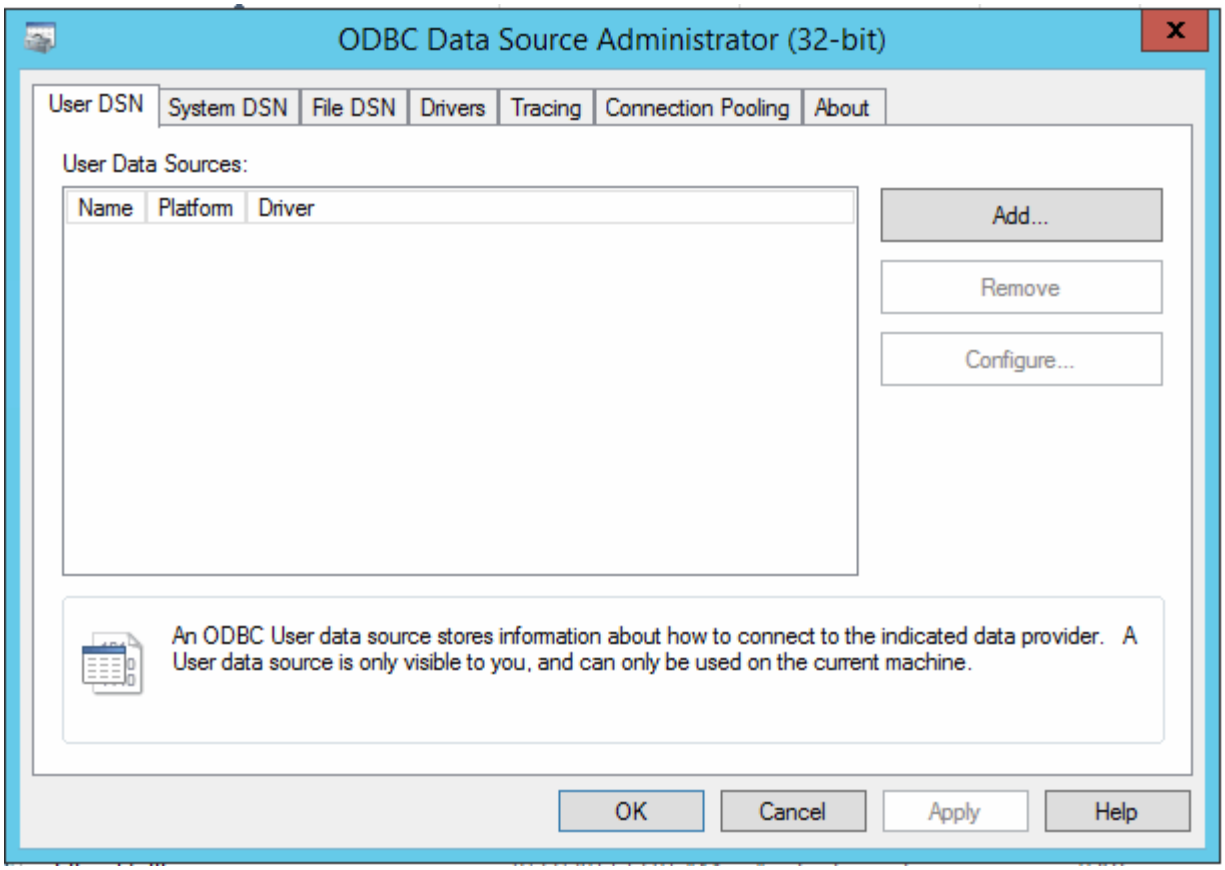
#### Bevor Sie beginnen

Sie müssen eine Remote-Anmeldung beim Data Warehouse-Server mit einem Konto mit Administratorrechten durchführen.

#### Schritte

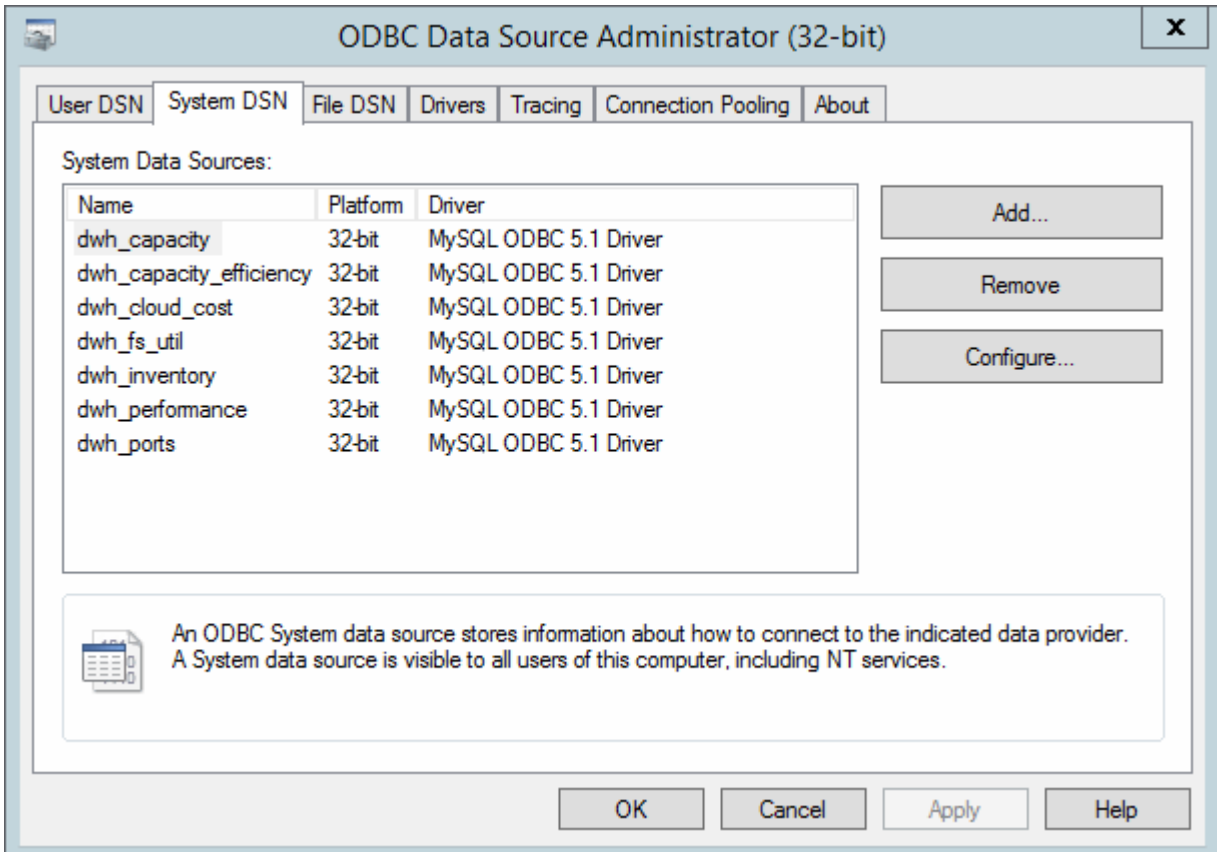
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

   Das System zeigt den ODBC-Bildschirm „Data Source Administrator“ an.



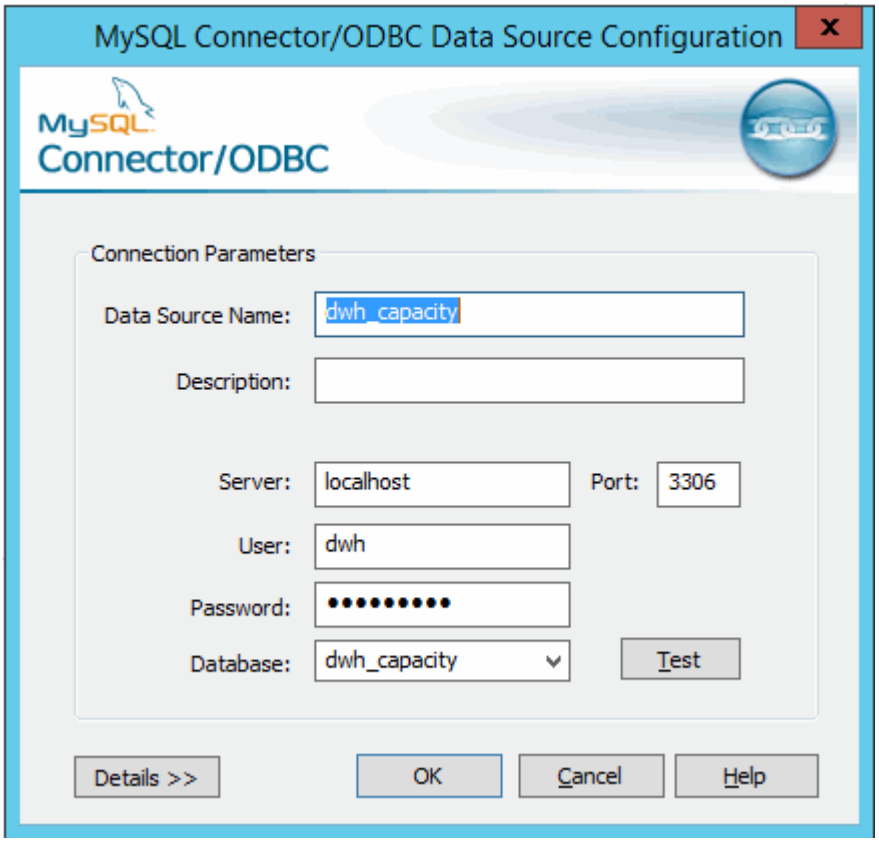

3. Klicken Sie auf **System DSN**

   Die Systemdatenquellen werden angezeigt.



4. Wählen Sie eine OnCommand Insight-Datenquelle aus der Liste aus.
5. Klicken Sie Auf **Konfigurieren**

   Der Bildschirm „Konfiguration der Datenquelle“ wird angezeigt.




6. Geben Sie das neue Passwort in das Feld **Passwort** ein.

# Unterstützung für Smart Card- und Zertifikatanmeldung

OnCommand Insight unterstützt die Verwendung von Smart Cards (CAC) und Zertifikaten zur Authentifizierung von Benutzern, die sich bei den Insight-Servern anmelden. Sie müssen das System konfigurieren, um diese Funktionen zu aktivieren.

Nach der Konfiguration des Systems zur Unterstützung von CAC und Zertifikaten führt das Navigieren zu einer neuen Sitzung von OnCommand Insight im Browser zu einem systemeigenen Dialogfeld, in dem dem der Benutzer eine Liste mit persönlichen Zertifikaten zur Auswahl hat. Diese Zertifikate werden basierend auf den persönlichen Zertifikaten gefiltert, die von CAS ausgestellt wurden, denen der OnCommand Insight-Server vertraut ist. Meistens gibt es eine einzige Wahl. Standardmäßig überspringt Internet Explorer dieses Dialogfeld, wenn nur eine Option vorhanden ist.

Für CAC-Benutzer enthalten Smartcards mehrere Zertifikate, von denen nur eines mit der vertrauenswürdigen Zertifizierungsstelle übereinstimmen kann. Das CAC-Zertifikat für `identification` Sollte verwendet werden.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

## Konfigurieren von Hosts für die Smart Card- und Zertifikatanmeldung

Sie müssen Änderungen an der OnCommand Insight-Hostkonfiguration vornehmen, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

### Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die ID eines Benutzers enthält.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

### Schritte

1. Verwenden Sie die `regedit` Dienstprogramm zum Ändern von Registrierungswerten in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Ändern Sie die Option JVM_ `DclientAuth=false` Bis `DclientAuth=true.`

2. Backup der Keystore-Datei: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Öffnen Sie eine Eingabeaufforderung mit der Angabe `Run as administrator`
4. Löschen Sie das selbstgenerierte Zertifikat: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Neues Zertifikat generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"`
6. Zertifikatsignierungsanforderung (CSR) generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"`
7. Nachdem die CSR in Schritt 6 zurückgegeben wurde, importieren Sie das Zertifikat, exportieren Sie das Zertifikat im Base-64-Format und legen Sie es in ein `"C:\temp" named servername.cer.`
8. Extrahieren Sie das Zertifikat aus dem Schlüsselspeicher:`C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12`
9. Extrahieren Sie einen privaten Schlüssel aus der p12-Datei: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Führen Sie das in Schritt 7 exportierte Base-64-Zertifikat mit dem privaten Schlüssel zusammen: `openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"`
11. Importieren Sie das zusammengeführte Zertifikat in den Schlüsselspeicher: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"`
12. Importieren Sie das Stammzertifikat: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"`
13. Importieren Sie das Stammzertifikat in den Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"`
14. Zwischenzertifikat importieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file`

```
"C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"
```

Wiederholen Sie diesen Schritt für alle Zwischenzertifikate.

15. Geben Sie die Domäne in LDAP an, die diesem Beispiel entspricht.
16. Starten Sie den Server neu.

## Konfigurieren eines Clients zur Unterstützung der Smart Card- und Zertifikatanmeldung

Client-Rechner erfordern Middleware und Änderungen an Browsern, um die Verwendung von Smart Cards und die Zertifikatanmeldung zu ermöglichen. Kunden, die bereits Smart Cards verwenden, sollten keine zusätzlichen Änderungen an ihren Client-Computern benötigen.

### Bevor Sie beginnen

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

### Über diese Aufgabe

Die folgenden allgemeinen Anforderungen an die Client-Konfiguration:

- Installieren von Smart Card Middleware, z. B. ActivClient (siehe
- Ändern des IE-Browsers (siehe
- Ändern des Firefox-Browsers (siehe

## Aktivieren von CAC auf einem Linux-Server

Einige Änderungen sind erforderlich, um CAC auf einem Linux OnCommand Insight-Server zu aktivieren.

Die Stammzertifizierungsstelle muss in den Truststore importiert werden.

**Schritte**

1. Navigieren Sie zu `/opt/netapp/oci/conf/`
2. Bearbeiten `wildfly.properties` Und ändern Sie den Wert von `CLIENT_AUTH_ENABLED` Zu „wahr“
3. Importieren Sie das „`root Certificate`“, das unter vorhanden ist `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Starten Sie den Server neu

## Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung

Sie müssen die OnCommand Insight-Data-Warehouse-Konfiguration ändern, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

**Bevor Sie beginnen**

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die Regierungs-ID-Nummer eines Benutzers enthält.

  Der auf staatlich ausgestellten CACs gespeicherte allgemeine Name (CN) wird normalerweise im folgenden Format gespeichert: `first.last.ID`. Für einige LDAP-Felder, z. B. `sAMAccountName`Dieses Format ist zu lang. Für diese Felder extrahiert OnCommand Insight nur die ID-Nummer aus dem CNS.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

**Schritte**

1. Verwenden Sie regedit, um Registrierungswerte in zu ändern `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

a. Ändern Sie die Option JVM_ `-DclientAuth=false` Bis `-DclientAuth=true`.

Ändern Sie für Linux die `clientAuth` Parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Zertifizierungsstellen (CAS) zum Data Warehouse trustore hinzufügen:
   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\wildfly\standalone\configuration`.
   b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + in der Dokumentation finden Sie "Sicherheitsadministration"weitere Informationen zum Festlegen oder Ändern des Passworts für Server_trustore.

      Das erste Wort in jeder Zeile gibt den CA-Alias an.

   c. Geben Sie bei Bedarf eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei: Um die CAS des Kunden mit vertrauenswürdigen Data Warehouse-CAS aufzunehmen, gehen Sie zu `..\SANscreen\wildfly\standalone\configuration` Und verwenden Sie die `keytool` Importbefehl: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      My_alias ist normalerweise ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.

3. Auf dem OnCommand Insight-Server wird die angezeigt `wildfly/standalone/configuration/standalone-full.xml` Die Datei muss durch Aktualisierung von verify-Client auf „ANGEFORDERT“ in geändert werden `/subsystem=undertow/server=default-server/https-listener=default-https`Um CAC zu aktivieren. Melden Sie sich beim Insight-Server an, und führen Sie den entsprechenden Befehl aus:

| BETRIEBSSYSTEM | Skript |
| --- | --- |
| Windows | <install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat |
| Linux | /Opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh |

   Warten Sie nach der Ausführung des Skripts, bis der Neustart des wildfly-Servers abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren.

4. Starten Sie den OnCommand Insight-Server neu.

## Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher)

Sie müssen die Konfiguration des OnCommand Insight Data Warehouse ändern, um Smart Card- (CAC) und Zertifikatanmeldungen für den Cognos-Server zu unterstützen.

### Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

### Schritte

1. Fügen Sie dem Cognos trustore Zertifizierungsstellen (CAS) hinzu.
   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `..\..\ ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      Das erste Wort in jeder Zeile gibt den CA-Alias an.
   c. Wenn keine geeigneten Dateien vorhanden sind, geben Sie eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei:
   d. Wenn Sie Zertifizierungsstellen des Kunden mit vertrauenswürdigen Zertifizierungsstellen von OnCommand Insight einbeziehen möchten, besuchen Sie `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Verwenden Sie die `keytool` Dienstprogramm zum Importieren des `.pem` Datei: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Ist in der Regel ein Alias, der die CA in der Operation leicht identifizieren würde`keytool -list`.
   f. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat* ein.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Gehen Sie wie folgt vor, um den CAC-Modus zu aktivieren:
   a. Konfigurieren Sie die CAC-Abmeldeseite mit den folgenden Schritten:
      - Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)

- (Nur für 7.3.10 und 7.3.11) Klicken Sie auf Verwalten -> Konfiguration -> System -> Sicherheit
- (Nur für 7.3.10 und 7.3.11) Geben Sie cacLogout.html gegen Abmeldung ein Umleiten Sie die URL -> Anwenden
- Browser schließen.

b. Ausführen `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

3. Gehen Sie wie folgt vor, um den CAC-Modus zu deaktivieren:

a. Ausführen `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

c. (Nur für 7.3.10 und 7.3.11) Unconfigure CAC Logout page, mit den folgenden Schritten:

- Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
- Klicken Sie Auf Verwalten -> Konfiguration -> System -> Sicherheit
- Geben Sie cacLogout.html für die URL zur Umleitung von Abmeldung ein -> Anwenden
- Browser schließen.

## Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher)

Sie können SSL-Zertifikate hinzufügen, um eine erweiterte Authentifizierung und Verschlüsselung für Ihre Data Warehouse- und Cognos-Umgebung zu ermöglichen.

### Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

### Über diese Aufgabe

Sie müssen über Administratorrechte verfügen, um dieses Verfahren durchführen zu können.

**Schritte**

1. Beenden Sie Cognos mit dem IBM Cognos Configuration Tool. Schließen Sie Cognos.
2. Erstellen Sie Backups des `..\SANScreen\cognos\analytics\configuration` Und `..\SANScreen\cognos\analytics\temp\cam\freshness` Ordner.
3. Erstellen Sie eine Zertifikatsverschlüsselungsanforderung von Cognos. Führen Sie in einem Admin-CMD-Fenster Folgendes aus:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Anmerkung: Hier sollen -H und -i subjectAltNames wie dns und ipaddress hinzufügen.
   c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Geben Sie den Inhalt von encryptRequest.csr ein, und erstellen Sie das Zertifikat mithilfe des CA-Signing-Portals.
6. Laden Sie die Kettenzertifikate unter Einbeziehung des Stammzertifikats im PKCS7-Format herunter

   Dadurch wird die Datei fqdn.p7b heruntergeladen
7. Holen Sie sich ein Zertifikat im .p7b-Format von Ihrer CA. Verwenden Sie einen Namen, der ihn als Zertifikat für den Cognos-Webserver kennzeichnet.
8. ThirdPartyCertificateTool.bat kann die gesamte Kette nicht importieren, so dass mehrere Schritte erforderlich sind, um alle Zertifikate zu exportieren. Teilen Sie die Kette auf, indem Sie sie einzeln wie folgt exportieren:
   a. Öffnen Sie das .p7b-Zertifikat unter „`Crypto Shell Extensions`“.
   b. Navigieren Sie im linken Fensterbereich zu „`Zertifikate`“.
   c. Klicken Sie mit der rechten Maustaste auf Stammzertifizierungsstelle > Alle Aufgaben > Exportieren.
   d. Wählen Sie Base64-Ausgabe.
   e. Geben Sie einen Dateinamen ein, der ihn als Stammzertifikat identifiziert.
   f. Wiederholen Sie die Schritte 8a bis 8e, um alle Zertifikate separat in .cer-Dateien zu exportieren.
   g. Benennen Sie die Dateien intermediateX.cer und cognos.cer.
9. Ignorieren Sie diesen Schritt, wenn Sie nur ein CA-Zertifikat haben, andernfalls fügen Sie root.cer und intermediateX.cer in eine Datei zusammen.
   a. Öffnen Sie root.cer mit Notepad und kopieren Sie den Inhalt.
   b. Öffnen Sie intermediate.cer mit Notepad und fügen Sie den Inhalt von 9a an (intermediate first und root next).
   c. Speichern Sie die Datei unter Chain.cer.
10. Importieren Sie die Zertifikate in den Cognos-Keystore mithilfe der Admin-CMD-Eingabeaufforderung:
    a. cd „`Program Files\sanscreen\cognos\Analytics\bin`“
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer

d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\Chain.cer

11. Öffnen Sie die IBM Cognos-Konfiguration.
    a. Wählen Sie Lokale Konfiguration-→ Sicherheit -→ Kryptographie -→ Cognos
    b. „`Drittanbieter-CA verwenden?`“ ändern Nach wahr.
    c. Speichern Sie die Konfiguration.
    d. Cognos Neu Starten
12. Exportieren Sie das neueste Cognos-Zertifikat in cognos.crt mithilfe der Admin CMD-Eingabeaufforderung:
    a. cd „`C:\Program Files\SANscreen“
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\Analytics\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias -Verschlüsselung
    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.
13. Sichern Sie den DWH-Server trustore unter`..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importieren Sie „`c:\temp\cognos.crt`“ in DWH trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.
    a. cd „`C:\Program Files\SANscreen“
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\Standalone\Configuration\Server.trustore -storepass <password> -alias cognos3rdca
    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.
15. Starten Sie den SANscreen-Dienst neu.
16. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.
17. Die folgenden Schritte sollten auch dann durchgeführt werden, wenn nur das “ssl-Zertifikat” geändert wird und die Standard-Cognos-Zertifikate unverändert bleiben. Andernfalls kann Cognos sich über das neue SANscreen-Zertifikat beschweren oder keine DWH-Sicherung erstellen.
    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`
    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass <password> -alias “ssl certificate”`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    Diese Schritte werden normalerweise im Rahmen des in beschriebenen Cognos-Zertifikatimportprozesses ausgeführt "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

# Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung

Sie müssen die OnCommand Insight-Data-Warehouse-Konfiguration ändern, um Smart Card- (CAC) und Zertifikatanmeldungen zu unterstützen.

## Bevor Sie beginnen

- LDAP muss auf dem System aktiviert sein.
- Das LDAP `User principal account name` Das Attribut muss mit dem LDAP-Feld übereinstimmen, das die Regierungs-ID-Nummer eines Benutzers enthält.

  Der auf staatlich ausgestellten CACs gespeicherte allgemeine Name (CN) wird normalerweise im folgenden Format gespeichert: `first.last.ID`. Für einige LDAP-Felder, z. B. `sAMAccountName`Dieses Format ist zu lang. Für diese Felder extrahiert OnCommand Insight nur die ID-Nummer aus dem CNS.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert haben"Sicherheitsadministration", starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

## Schritte

1. Verwenden Sie regedit, um Registrierungswerte in zu ändern `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Ändern Sie die Option JVM_ `-DclientAuth=false` Bis `-DclientAuth=true`.

   Ändern Sie für Linux die `clientAuth` Parameter in `/opt/netapp/oci/scripts/wildfly.server`

2. Zertifizierungsstellen (CAS) zum Data Warehouse trustore hinzufügen:

   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\wildfly\standalone\configuration`.

   b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + in der Dokumentation finden Sie "Sicherheitsadministration"weitere Informationen zum Festlegen oder Ändern des Passworts für Server_trustore.

   Das erste Wort in jeder Zeile gibt den CA-Alias an.

c. Geben Sie bei Bedarf eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei: Um die CAS des Kunden mit vertrauenswürdigen Data Warehouse-CAS aufzunehmen, gehen Sie zu `..\SANscreen\wildfly\standalone\configuration` Und verwenden Sie die `keytool` Importbefehl: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   My_alias ist normalerweise ein Alias, der die CA in der leicht identifizieren würde`keytool -list` Betrieb.

3. Auf dem OnCommand Insight-Server wird die angezeigt `wildfly/standalone/configuration/standalone-full.xml` Die Datei muss durch Aktualisierung von verify-Client auf „ANGEFORDERT“ in geändert werden `/subsystem=undertow/server=default-server/https-listener=default-https`Um CAC zu aktivieren. Melden Sie sich beim Insight-Server an, und führen Sie den entsprechenden Befehl aus:

| BETRIEBSSYSTEM | Skript |
| --- | --- |
| Windows | <install dir>\SANscreen\wildfly\bin\enableCACforRemoteEJB.bat |
| Linux | /Opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh |

   Warten Sie nach der Ausführung des Skripts, bis der Neustart des wildfly-Servers abgeschlossen ist, bevor Sie mit dem nächsten Schritt fortfahren.

4. Starten Sie den OnCommand Insight-Server neu.

# Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher)

Sie müssen die Konfiguration des OnCommand Insight Data Warehouse ändern, um Smart Card- (CAC) und Zertifikatanmeldungen für den Cognos-Server zu unterstützen.

## Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

## Schritte

1. Fügen Sie dem Cognos trustore Zertifizierungsstellen (CAS) hinzu.
   a. Wechseln Sie in einem Befehlsfenster zu `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Verwenden Sie das `keytool` Dienstprogramm, um die vertrauenswürdigen CAS aufzulisten: `..\..\ ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      Das erste Wort in jeder Zeile gibt den CA-Alias an.

   c. Wenn keine geeigneten Dateien vorhanden sind, geben Sie eine Zertifizierungsstellenzertifikatsdatei an, in der Regel eine `.pem` Datei:
   d. Wenn Sie Zertifizierungsstellen des Kunden mit vertrauenswürdigen Zertifizierungsstellen von OnCommand Insight einbeziehen möchten, besuchen Sie `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Verwenden Sie die `keytool` Dienstprogramm zum Importieren des `.pem` Datei: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` Ist in der Regel ein Alias, der die CA in der Operation leicht identifizieren würde`keytool -list`.

   f. Wenn Sie zur Eingabe eines Kennworts aufgefordert werden, geben Sie das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat* ein.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Gehen Sie wie folgt vor, um den CAC-Modus zu aktivieren:
   a. Konfigurieren Sie die CAC-Abmeldeseite mit den folgenden Schritten:
      - Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
      - (Nur für 7.3.10 und 7.3.11) Klicken Sie auf Verwalten -> Konfiguration -> System -> Sicherheit
      - (Nur für 7.3.10 und 7.3.11) Geben Sie cacLogout.html gegen Abmeldung ein Umleiten Sie die URL -> Anwenden

- Browser schließen.

b. Ausführen `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

3. Gehen Sie wie folgt vor, um den CAC-Modus zu deaktivieren:

a. Ausführen `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

b. Starten Sie den IBM Cognos-Dienst. Warten Sie, bis der Cognos-Dienst gestartet wird.

c. (Nur für 7.3.10 und 7.3.11) Unconfigure CAC Logout page, mit den folgenden Schritten:

- Anmeldung beim Cognos-Portal (Benutzer muss Teil der Gruppe „Systemadministratoren“ sein, d. h. cognos_admin)
- Klicken Sie Auf Verwalten -> Konfiguration -> System -> Sicherheit
- Geben Sie cacLogout.html für die URL zur Umleitung von Abmeldung ein -> Anwenden
- Browser schließen.

# Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher)

Sie können SSL-Zertifikate hinzufügen, um eine erweiterte Authentifizierung und Verschlüsselung für Ihre Data Warehouse- und Cognos-Umgebung zu ermöglichen.

## Bevor Sie beginnen

Dieses Verfahren gilt für Systeme mit OnCommand Insight 7.3.10 und höher.

Die aktuellsten CAC- und Zertifikatanweisungen finden Sie in den folgenden Knowledgebase-Artikeln (Support-Anmeldung erforderlich):

- "So konfigurieren Sie die Common Access Card (CAC)-Authentifizierung für OnCommand Insight"
- "Konfigurieren der Authentifizierung für allgemeine Zugriffskarten (Common Access Card, CAC) für OnCommand Insight Data Warehouse"
- "Erstellen und Importieren eines signierten Zertifikats einer Zertifizierungsstelle (CA) in OnComand Insight und OnCommand Insight Data Warehouse 7.3.x"
- "So erstellen Sie ein selbstsigniertes Zertifikat in OnCommand Insight 7.3.X, das auf einem Windows-Host installiert ist"
- "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

## Über diese Aufgabe

Sie müssen über Administratorrechte verfügen, um dieses Verfahren durchführen zu können.

## Schritte

1. Beenden Sie Cognos mit dem IBM Cognos Configuration Tool. Schließen Sie Cognos.

2. Erstellen Sie Backups des `..\SANScreen\cognos\analytics\configuration` Und `..\SANScreen\cognos\analytics\temp\cam\freshness` Ordner.
3. Erstellen Sie eine Zertifikatsverschlüsselungsanforderung von Cognos. Führen Sie in einem Admin-CMD-Fenster Folgendes aus:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Anmerkung: Hier sollen -H und -i subjectAltNames wie dns und ipaddress hinzufügen.
   c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Geben Sie den Inhalt von encryptRequest.csr ein, und erstellen Sie das Zertifikat mithilfe des CA-Signing-Portals.
6. Laden Sie die Kettenzertifikate unter Einbeziehung des Stammzertifikats im PKCS7-Format herunter

   Dadurch wird die Datei fqdn.p7b heruntergeladen
7. Holen Sie sich ein Zertifikat im .p7b-Format von Ihrer CA. Verwenden Sie einen Namen, der ihn als Zertifikat für den Cognos-Webserver kennzeichnet.
8. ThirdPartyCertificateTool.bat kann die gesamte Kette nicht importieren, so dass mehrere Schritte erforderlich sind, um alle Zertifikate zu exportieren. Teilen Sie die Kette auf, indem Sie sie einzeln wie folgt exportieren:
   a. Öffnen Sie das .p7b-Zertifikat unter „`Crypto Shell Extensions`“.
   b. Navigieren Sie im linken Fensterbereich zu „`Zertifikate`“.
   c. Klicken Sie mit der rechten Maustaste auf Stammzertifizierungsstelle > Alle Aufgaben > Exportieren.
   d. Wählen Sie Base64-Ausgabe.
   e. Geben Sie einen Dateinamen ein, der ihn als Stammzertifikat identifiziert.
   f. Wiederholen Sie die Schritte 8a bis 8e, um alle Zertifikate separat in .cer-Dateien zu exportieren.
   g. Benennen Sie die Dateien intermediateX.cer und cognos.cer.
9. Ignorieren Sie diesen Schritt, wenn Sie nur ein CA-Zertifikat haben, andernfalls fügen Sie root.cer und intermediateX.cer in eine Datei zusammen.
   a. Öffnen Sie root.cer mit Notepad und kopieren Sie den Inhalt.
   b. Öffnen Sie intermediate.cer mit Notepad und fügen Sie den Inhalt von 9a an (intermediate first und root next).
   c. Speichern Sie die Datei unter Chain.cer.
10. Importieren Sie die Zertifikate in den Cognos-Keystore mithilfe der Admin-CMD-Eingabeaufforderung:
    a. cd „`Program Files\sanscreen\cognos\Analytics\bin`“
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\root.cer
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c:\temp\intermediate.cer
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\Chain.cer
11. Öffnen Sie die IBM Cognos-Konfiguration.

a. Wählen Sie Lokale Konfiguration-→ Sicherheit -→ Kryptographie -→ Cognos

b. „`Drittanbieter-CA verwenden?`“ ändern Nach wahr.

c. Speichern Sie die Konfiguration.

d. Cognos Neu Starten

12. Exportieren Sie das neueste Cognos-Zertifikat in cognos.crt mithilfe der Admin CMD-Eingabeaufforderung:

    a. cd „`C:\Program Files\SANscreen“

    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\Analytics\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias -Verschlüsselung

    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.

13. Sichern Sie den DWH-Server trustore unter`..\SANscreen\wildfly\standalone\configuration\server.trustore`

14. Importieren Sie „`c:\temp\cognos.crt`“ in DWH trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.

    a. cd „`C:\Program Files\SANscreen“

    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\Standalone\Configuration\Server.trustore -storepass <password> -alias cognos3rdca

    c. Verwenden Sie für <password> das Kennwort aus der Datei */SANscreen/bin/cognos_info.dat*.

15. Starten Sie den SANscreen-Dienst neu.

16. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

17. Die folgenden Schritte sollten auch dann durchgeführt werden, wenn nur das “ssl-Zertifikat” geändert wird und die Standard-Cognos-Zertifikate unverändert bleiben. Andernfalls kann Cognos sich über das neue SANscreen-Zertifikat beschweren oder keine DWH-Sicherung erstellen.

    a. `cd “%SANSCREEN_HOME%cognos\analytics\bin\”`

    b. `“%SANSCREEN_HOME%java64\bin\keytool.exe” -exportcert -file “c:\temp\sanscreen.cer” -keystore “%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore” -storepass <password> -alias “ssl certificate”`

    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r “c:\temp\sanscreen.cer”`

    Diese Schritte werden normalerweise im Rahmen des in beschriebenen Cognos-Zertifikatimportprozesses ausgeführt "Importieren eines von Cognos signierten Zertifikats einer Zertifizierungsstelle (CA) in OnCommand DataWarehouse 7.3.3 und höher"

# SSL-Zertifikate werden importiert

Sie können SSL-Zertifikate hinzufügen, um die erweiterte Authentifizierung und Verschlüsselung zu aktivieren und so die Sicherheit Ihrer OnCommand Insight-Umgebung zu erhöhen.

## Bevor Sie beginnen

Sie müssen sicherstellen, dass Ihr System die erforderliche Mindestbitebene (1024 Bit) erfüllt.

## Über diese Aufgabe

Es wird dringend empfohlen, den Tresor vor dem Upgrade zu sichern.

Weitere Informationen zum Tresor- und Passwortmanagement finden "Sicherheitstool"Sie in den Anweisungen.

## Schritte

1. Erstellen Sie eine Kopie der ursprünglichen Keystore-Datei: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Listen Sie den Inhalt des Keystore auf: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Das System zeigt den Inhalt des Keystore an. Es sollte mindestens ein Zertifikat im Schlüsselspeicher vorhanden sein, `"ssl certificate"`.
3. Löschen Sie die `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Einen neuen Schlüssel generieren: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Wenn Sie nach vor- und Nachnamen gefragt werden, geben Sie den vollständig qualifizierten Domänennamen (FQDN) ein, den Sie verwenden möchten.
   b. Geben Sie die folgenden Informationen zu Ihrer Organisation und Organisationsstruktur an:
      - Land: Zweistellige ISO-Abkürzung für Ihr Land (z. B. USA)
      - Bundesland oder Provinz: Name des Bundesstaates oder der Provinz, in dem sich der Hauptsitz Ihres Unternehmens befindet (z. B. Massachusetts)
      - Ort: Name der Stadt, in der sich der Hauptsitz Ihrer Organisation befindet (z. B. Waltham)
      - Name des Unternehmens: Name des Unternehmens, dem der Domain-Name gehört (z. B. NetApp)
      - Name der Organisationseinheit: Name der Abteilung oder Gruppe, die das Zertifikat verwenden soll (z. B. Support)
      - Domänenname/ Allgemeiner Name: Der FQDN, der für DNS-Suchen Ihres Servers verwendet wird (z. B. www.example.com). Das System antwortet mit Informationen wie den folgenden: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Eingabe `Yes` Wenn der allgemeine Name (CN) gleich dem FQDN ist.
   d. Wenn Sie zur Eingabe des Schlüsselpassworts aufgefordert werden, geben Sie das Kennwort ein, oder drücken Sie die Eingabetaste, um das vorhandene Schlüsselspeicher-Passwort zu verwenden.

5. Erstellen Sie eine Zertifikatanforderungsdatei: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

   Der `c:\localhost.csr` Die Datei ist die neu generierte Zertifikatanforderungsdatei.

6. Senden Sie die `c:\localhost.csr` Bei der Zertifizierungsstelle zur Genehmigung einreichen.

   Nachdem die Zertifikatanforderungsdatei genehmigt wurde, möchten Sie das Zertifikat in zurücksenden `.der` Formatieren. Die Datei wird möglicherweise als zurückgegeben `.der` Datei: Das Standarddateiformat ist `.cer` Für Microsoft CA-Services.

   Die CAS der meisten Unternehmen verwenden ein Vertrauensstellungsmodell, einschließlich einer Stammzertifizierungsstelle, die häufig offline ist. Es hat die Zertifikate für nur wenige untergeordnete CAS, bekannt als intermediate CAS, unterzeichnet.

   Sie müssen den öffentlichen Schlüssel (Zertifikate) für die gesamte Vertrauenskette erhalten – das Zertifikat für die Zertifizierungsstelle, die das Zertifikat für den OnCommand Insight-Server signiert hat, und alle Zertifikate zwischen dieser Zertifizierungsstelle bis hin zur Unternehmensstammzertifizierungsstelle.

   Wenn Sie in einigen Unternehmen eine Signaturanfrage einreichen, erhalten Sie möglicherweise eine der folgenden Informationen:

   - Eine PKCS12-Datei, die Ihr signiertes Zertifikat und alle öffentlichen Zertifikate in der Vertrauenskette enthält
   - A `.zip` Datei, die einzelne Dateien (einschließlich Ihres signierten Zertifikats) und alle öffentlichen Zertifikate in der Vertrauenskette enthält
   - Nur Ihr signiertes Zertifikat

     Sie müssen die öffentlichen Zertifikate erhalten.

7. Importieren Sie das genehmigte Zertifikat für Server.keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   a. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für den Keystore ein.

      Die folgende Meldung wird angezeigt: `Certificate reply was installed in keystore`

8. Importieren Sie das genehmigte Zertifikat für den Server.trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"`

   a. Geben Sie bei Aufforderung das trustore-Passwort ein.

      Die folgende Meldung wird angezeigt: `Certificate reply was installed in trustore`

9. Bearbeiten Sie das `SANscreen\wildfly\standalone\configuration\standalone-full.xml` Datei:

Ersetzen Sie die folgende Alias-Zeichenfolge: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Beispiel:

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"
keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
02.muccbc.hq.netapp.com" key-
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. Starten Sie den SANscreen-Serverdienst neu.

    Sobald Insight ausgeführt wird, können Sie auf das Vorhängeschloss-Symbol klicken, um die auf dem System installierten Zertifikate anzuzeigen.

    Wenn ein Zertifikat mit Informationen „ausgestellt an“ angezeigt wird, die mit den Informationen „ausgestellt von“ übereinstimmen, ist weiterhin ein selbstsigniertes Zertifikat installiert. Selbstsignierte Insight Zertifikate, die vom Insight Installer generiert werden, laufen 100 Jahre ab.

    NetApp kann nicht garantieren, dass dieses Verfahren Warnungen zu digitalen Zertifikaten entfernt. NetApp kann nicht steuern, wie Ihre Endbenutzer-Workstations konfiguriert sind. Betrachten Sie die folgenden Szenarien:

    - Microsoft Internet Explorer und Google Chrome verwenden beide Microsoft-native Zertifikatfunktionalität auf Windows.

      Das bedeutet, dass wenn Ihre Active Directory-Administratoren die CA-Zertifikate Ihres Unternehmens in die Zertifikattrustores des Endbenutzers übertragen, die Benutzer dieser Browser die Zertifikatwarnungen verschwinden sehen, wenn die selbstsignierten OnCommand Insight-Zertifikate durch die Zertifikate ersetzt wurden, die von der internen CA-Infrastruktur signiert wurden.

    - Java und Mozilla Firefox haben ihre eigenen Zertifikatsspeicher.

      Wenn Ihre Systemadministratoren das Einspielen der CA-Zertifikate in die vertrauenswürdigen Zertifikatsspeicher dieser Anwendungen nicht automatisieren, kann die Verwendung des Firefox-Browsers weiterhin Zertifikatwarnungen aufgrund eines nicht vertrauenswürdigen Zertifikats generieren, selbst wenn das selbstsignierte Zertifikat ersetzt wurde. Eine zusätzliche Anforderung ist, die Zertifikatskette Ihres Unternehmens in den trustore zu installieren.

# Die Hierarchie Ihrer Geschäftseinheiten

## Sie können Geschäftseinheiten definieren, um Ihre Umgebungsdaten granular zu verfolgen und darüber Berichte zu erstellen.

In OnCommand Insight enthält die Hierarchie der Geschäftseinheiten die folgenden Ebenen:

- **Mandant** wird primär von Service-Providern genutzt, um Ressourcen einem Kunden zuzuordnen, zum Beispiel NetApp.
- **Line of Business (Lob)** ist ein Geschäftsbereich oder eine Produktlinie innerhalb eines Unternehmens, z. B. Data Storage.
- **Business Unit** repräsentiert eine traditionelle Business Unit wie Legal oder Marketing.
- **Projekt** wird häufig verwendet, um ein bestimmtes Projekt innerhalb einer Geschäftseinheit zu identifizieren, für die Sie Kapazitätszuweisungen wünschen. Beispielsweise kann „Patente“ ein Projektname für die Rechtsabteilung und „Verkaufsveranstaltungen“ ein Projektname für die

Geschäftseinheit Marketing sein. Beachten Sie, dass die Namen der Ebenen Leerzeichen enthalten können.

Sie müssen nicht alle Ebenen für das Design Ihrer Unternehmenshierarchie verwenden.

## Entwerfen der Hierarchie Ihrer Geschäftseinheiten

Sie müssen die Elemente Ihrer Unternehmensstruktur verstehen und wissen, was in den Geschäftseinheiten vertreten werden muss, da diese eine feste Struktur in Ihrer OnCommand Insight-Datenbank werden. Sie können die folgenden Informationen verwenden, um Ihre Geschäftseinheiten einzurichten. Denken Sie daran, dass Sie nicht alle Hierarchieebenen verwenden müssen, um Daten in diesen Kategorien zu erfassen.

### Schritte

1. Prüfen Sie jede Ebene der Hierarchie der Geschäftseinheiten, um festzustellen, ob diese Ebene in die Hierarchie Ihrer Unternehmenseinheit für Ihr Unternehmen aufgenommen werden soll:
   - **Tenant** Level ist erforderlich, wenn Ihr Unternehmen ein ISP ist und Sie die Nutzung von Ressourcen durch Kunden verfolgen möchten.
   - **Line of Business (Lob)** wird in der Hierarchie benötigt, wenn die Daten für verschiedene Produktlinien nachverfolgt werden müssen.
   - **Business Unit** ist erforderlich, wenn Sie Daten für verschiedene Abteilungen verfolgen müssen. Diese Hierarchieebene ist oft wertvoll, wenn es darum geht, eine Ressource zu trennen, die von einer Abteilung genutzt wird, die von anderen Abteilungen nicht genutzt wird.
   - **Projekt**-Ebene kann für spezialisierte Arbeiten innerhalb einer Abteilung verwendet werden. Diese Daten können nützlich sein, um die Technologieanforderungen eines separaten Projekts im Vergleich zu anderen Projekten in einem Unternehmen oder einer Abteilung zu lokalisieren, zu definieren und zu überwachen.
2. Erstellen Sie ein Diagramm, in dem jede Geschäftseinheit mit den Namen aller Ebenen innerhalb der Einheit angezeigt wird.
3. Überprüfen Sie die Namen in der Hierarchie, um sicherzustellen, dass sie in OnCommand Insight-Ansichten und -Berichten selbsterklärend sind.
4. Identifizieren Sie alle Applikationen, die den einzelnen Unternehmenseinheiten zugeordnet sind.

## Erstellen von Geschäftseinheiten

Nachdem Sie die Hierarchie der Geschäftseinheiten für Ihr Unternehmen entworfen haben, können Sie Anwendungen einrichten und die Geschäftseinheiten den Anwendungen zuordnen. Dieser Prozess erstellt die Struktur der Geschäftseinheiten in Ihrer OnCommand Insight-Datenbank.

### Über diese Aufgabe

Das Zuordnen von Anwendungen zu Geschäftseinheiten ist optional; es handelt sich jedoch um eine Best Practice.

### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Business Entities**.

   Die Seite Business Entities wird angezeigt.
3. Klicken Sie Auf

Um mit dem Erstellen einer neuen Einheit zu beginnen.

   Das Dialogfeld **Business Entity hinzufügen** wird angezeigt.
4. Für jede Entitätsebene (Mandant, Geschäftsbereich, Geschäftsbereich und Projekt) können Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie auf die Liste der Entitätsebene, und wählen Sie einen Wert aus.
   - Geben Sie einen neuen Wert ein, und drücken Sie die Eingabetaste.
   - Lassen Sie den Wert auf Entitätsebene als N/A stehen, wenn Sie die Entitätsebene für die Geschäftseinheit nicht verwenden möchten.
5. Klicken Sie Auf **Speichern**.

## Zuordnen von Geschäftseinheiten zu Assets

Sie können einer Ressource eine Geschäftseinheit zuweisen (Host, Port, Speicher, Switch, virtuelle Maschine, Qtree, Share, Volume oder internes Volume) ohne Zuordnung der Geschäftseinheit zu einer Applikation, doch werden Geschäftseinheiten automatisch einer Ressource zugewiesen, wenn diese Ressource einer Applikation zugeordnet ist, die zu einer Geschäftseinheit gehört.

### Bevor Sie beginnen

Sie müssen bereits eine Geschäftseinheit erstellt haben.

### Über diese Aufgabe

Sie können Geschäftseinheiten zwar direkt Assets zuweisen, es wird jedoch empfohlen, Applikationen Assets zuzuweisen und dann Geschäftseinheiten Assets zuzuweisen.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie das Asset, auf das Sie die Geschäftseinheit anwenden möchten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Asset Dashboard auf das Asset.
   - Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Namen des Assets ein, und wählen Sie dann das Asset aus der Liste aus.
3. Positionieren Sie im Abschnitt **Benutzerdaten** der Asset-Seite Ihren Cursor auf **Keine** neben **Business Entities** und klicken Sie dann auf .

   Die Liste der verfügbaren Geschäftseinheiten wird angezeigt.

4. Geben Sie in das Feld **Suchen** ein, um die Liste nach einer bestimmten Entität zu filtern, oder scrollen Sie in der Liste nach unten; wählen Sie eine Business Entity aus der Liste aus.

   Wenn die ausgewählte Geschäftseinheit mit einer Applikation verknüpft ist, wird der Anwendungsname angezeigt. In diesem Fall wird neben dem Namen der Geschäftseinheit das Wort „`derived`“ angezeigt. Wenn Sie die Einheit nur für das Asset und nicht für die zugehörige Anwendung verwalten möchten, können Sie die Zuweisung der Anwendung manuell überschreiben.

5. Um eine Anwendung zu überschreiben, die von einer Geschäftseinheit abgeleitet wurde, setzen Sie den Cursor auf den Anwendungsnamen, und klicken Sie auf Wählen Sie eine andere Geschäftseinheit aus, und wählen Sie eine andere Anwendung aus der Liste aus.

### Zuordnen von Geschäftseinheiten zu oder Entfernen von Geschäftseinheiten aus mehreren Assets

Sie können Business Entities mehreren Assets zuweisen oder diese entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell zuweisen oder entfernen zu müssen.

#### Bevor Sie beginnen

Sie müssen bereits die Geschäftseinheiten erstellt haben, die Sie zu den gewünschten Assets hinzufügen möchten.

#### Schritte

1. Erstellen Sie eine neue Abfrage, oder öffnen Sie eine vorhandene Abfrage.
2. Filtern Sie bei Bedarf nach den Assets, denen Sie Business Entities hinzufügen möchten.
3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den ausgewählten Assets eine Geschäftseinheit hinzuzufügen, klicken Sie auf Actions. Wenn dem ausgewählten Asset-Typ Business Entities zugewiesen werden können, wird die Menüauswahl **Add Business Entity** angezeigt. Wählen Sie diese Option aus.
5. Wählen Sie die gewünschte Geschäftseinheit aus der Liste aus und klicken Sie auf **Speichern**.

   Jede neue Business Entity, die Sie zuweisen, überschreibt alle Business Entities, die bereits dem Asset zugewiesen wurden. Durch das Zuweisen von Anwendungen zu Assets werden auch die Business Entities überschrieben, die auf die gleiche Weise zugewiesen wurden. Das Zuweisen von Geschäftseinheiten als Anlage kann auch alle Anwendungen überschreiben, die dieser Anlage zugewiesen sind.

6. Um eine Geschäftseinheit zu entfernen, die den Assets zugewiesen ist, klicken Sie auf Actions Und wählen Sie **Business Entity entfernen**.
7. Wählen Sie die gewünschte Geschäftseinheit aus der Liste aus und klicken Sie auf **Löschen**.

# Anmerkungen definieren

Wenn Sie OnCommand Insight zur Nachverfolgung von Daten gemäß Ihren Unternehmensanforderungen anpassen, können Sie beliebige spezialisierte

Annotationen definieren, die erforderlich sind, um einen vollständigen Überblick über Ihre Daten zu erhalten, wie z. B. Ende der Nutzungsdauer von Assets, Datacenter, Gebäudestandort, Storage-Ebene oder Volume. Und internem Service-Level für Volumes.

### Schritte

1. Geben Sie die Terminologie an, der die Umgebungsdaten zugeordnet werden müssen.
2. Geben Sie die Unternehmensterminologie an, mit der Umgebungsdaten verknüpft werden müssen, die nicht bereits mit den Geschäftseinheiten verfolgt wird.
3. Geben Sie alle standardmäßigen Anmerkungstypen an, die Sie verwenden können.
4. Ermitteln Sie, welche benutzerdefinierten Anmerkungen Sie erstellen müssen.

## Verwendung von Annotationen zum Monitoring Ihrer Umgebung

Wenn Sie OnCommand Insight so anpassen, dass Daten für Ihre Unternehmensanforderungen nachverfolgt werden, können Sie spezielle Hinweise, die so genannten *Annotationen*, definieren und diese Ihren Ressourcen zuweisen. Beispielsweise können Assets mit Informationen wie Asset-Lebensende, Datacenter, Gebäudestandort, Storage-Klassen oder Service-Leveln für Volumes versehen werden.

Durch die Verwendung von Annotationen zum Monitoring Ihrer Umgebung werden die folgenden grundlegenden Aufgaben aufgeführt:

- Erstellen oder Bearbeiten von Definitionen für alle Anmerkungstypen.
- Anzeigen von Asset-Seiten und Verknüpfen jeder Anlage mit einer oder mehreren Anmerkungen.

  Wenn z. B. ein Asset geleast wird und der Mietvertrag innerhalb von zwei Monaten abläuft, können Sie eine End-of-Life-Anmerkung auf das Asset anwenden. Dadurch wird verhindert, dass andere diese Ressource über einen längeren Zeitraum nutzen können.

- Erstellen von Regeln, um Anmerkungen automatisch auf mehrere Assets desselben Typs anzuwenden.
- Verwenden des Importdienstprogramms für Anmerkungen zum Importieren von Anmerkungen.
- Filtern Sie Assets nach ihren Anmerkungen.
- Gruppieren von Daten in Berichten auf der Grundlage von Anmerkungen und Erstellen dieser Berichte.

  Weitere Informationen zu Berichten finden Sie im *OnCommand Insight Reporting Guide*.

#### Verwalten von Anmerkungstypen

OnCommand Insight bietet einige standardmäßige Annotationstypen an, z. B. Lebenszyklus von Assets (Geburtstag oder Ende der Nutzungsdauer), Gebäude- oder Datacenter-Standort und -Ebene, die Sie an die Anzeige in Ihren Berichten anpassen können. Sie können Werte für Standard-Anmerkungstypen definieren oder eigene benutzerdefinierte Anmerkungstypen erstellen. Sie können diese Werte später bearbeiten.

**Standard-Anmerkungstypen**

## OnCommand Insight bietet einige standardmäßige Anmerkungstypen. Mit diesen Annotationen können Daten gefiltert oder gruppiert und die Datenberichterstattung gefiltert werden.

Sie können Assets mit Standardanmerkungstypen verknüpfen, z. B.:

- Lebenszyklus von Anlagen, z. B. Geburtstag, Sonnenuntergang oder Ende des Lebenszyklus
- Positionsinformationen zu einem Gerät wie z. B. Rechenzentren, Gebäude oder Etage
- Klassifizierung von Assets, z. B. nach Qualität (Tiers), nach angeschlossenen Geräten (Switch-Ebene) oder nach Service-Level
- Status, z. B. „heiß“ (hohe Auslastung)

In der folgenden Tabelle sind die Standardbeschriftungstypen aufgeführt. Sie können diese Beschriftungsnamen ganz nach Ihren Bedürfnissen bearbeiten.

| Anmerkungstypen | Beschreibung | Typ |
|---|---|---|
| Alias | Benutzerfreundlicher Name für eine Ressource. | Text |
| Geburtstag | Datum, an dem das Gerät online gestellt wurde oder wird. | Datum |
| Gebäude | Physischer Standort von Host-, Storage-, Switch- und Bandressourcen. | Liste |
| Stadt | Standort der Gemeinde von Host-, Storage-, Switch- und Tape-Ressourcen | Liste |
| Rechnerressourcengruppe | Gruppenzuweisung, die von der Datenquelle „Host“ und „VM-Dateisysteme“ verwendet wird. | Liste |
| Kontinent | Geografischer Standort von Host-, Storage-, Switch- und Tape-Ressourcen | Liste |
| Land | Nationaler Standort von Host-, Storage-, Switch- und Bandressourcen. | Liste |
| Rechenzentrum | Physischer Standort der Ressource und steht für Hosts, Speicher-Arrays, Switches und Bänder zur Verfügung. | Liste |

| | | |
|---|---|---|
| Direkt Verbunden | Gibt an (Ja oder Nein), ob eine Speicherressource direkt mit Hosts verbunden ist. | Boolesch |
| Ende des Supports | Datum, an dem ein Gerät offline genommen wird, z. B. wenn der Lease abgelaufen ist oder die Hardware außer Betrieb genommen wird. | Datum |
| Fabric-Alias | Benutzerfreundlicher Name für eine Fabric. | Text |
| Boden | Standort eines Geräts auf einem Stockwerk eines Gebäudes. Kann für Hosts, Speicher-Arrays, Switches und Bänder eingerichtet werden. | Liste |
| Heiß | Geräte, die bereits regelmäßig oder an der Kapazitätsgrenze stark genutzt werden. | Boolesch |
| Hinweis | Kommentare, die einer Ressource zugeordnet werden sollen. | Text |
| Rack | Rack, in dem sich die Ressource befindet. | Text |
| Zimmer | Raum in einem Gebäude oder einem anderen Standort mit Host-, Speicher-, Switch- und Bandressourcen. | Liste |
| San | Logische Partition des Netzwerks. Verfügbar auf Hosts, Speicher-Arrays, Bändern, Switches und Anwendungen. | Liste |
| Service-Level | Eine Reihe unterstützter Service-Level, die Sie Ressourcen zuweisen können. Zeigt eine Liste mit bestellten Optionen für interne Volumes, qtree und Volumes an. Bearbeiten Sie Service Levels, um Performance-Richtlinien für unterschiedliche Level festzulegen. | Liste |

| | | |
|---|---|---|
| Bundesland/Kanton | Bundesland oder Provinz, in der sich die Ressource befindet. | Liste |
| Sonnenuntergang | Schwellenwert, nach dem keine neuen Zuordnungen an das Gerät vorgenommen werden können. Nützlich für geplante Migrationen und andere ausstehende Netzwerkänderungen. | Datum |
| Switch-Ebene | Enthält vordefinierte Optionen zum Einrichten von Kategorien für Switches. Normalerweise bleiben diese Bezeichnungen für die gesamte Lebensdauer des Geräts erhalten, obwohl Sie sie bei Bedarf bearbeiten können. Nur für Switches verfügbar. | Liste |
| Ebene | Sie können darüber hinaus verwendet werden, um in Ihrer Umgebung verschiedene Service Levels zu definieren. Tiers können den Typ des Levels definieren, z. B. die erforderliche Geschwindigkeit (z. B. Gold oder Silber). Diese Funktion ist nur für interne Volumes, qtrees, Storage Arrays, Storage-Pools und Volumes verfügbar. | Liste |
| Schweregrad Der Verletzung | Rangfolge (z. B. Major) eines Verstoßes (z. B. fehlende Host-Ports oder fehlende Redundanz) in einer Hierarchie von höchster bis niedrigster Bedeutung. | Liste |

Alias, Rechenzentrum, Hot, Service-Level, Sonnenuntergang, Switch Level, Service Level, Tier und Verletzung Severity sind Anmerkungen auf Systemebene, die Sie nicht löschen oder umbenennen können. Sie können nur die ihnen zugewiesenen Werte ändern.

#### Wie Anmerkungen zugewiesen werden

Mithilfe von Anmerkungsregeln können Sie Anmerkungen manuell oder automatisch zuweisen. OnCommand Insight weist auch automatisch einige Anmerkungen zum Erwerb von Vermögenswerten und nach Vererbung zu. Alle Anmerkungen, die Sie einem Asset zuweisen, werden im Abschnitt „Benutzerdaten“ der Seite „Anlage“ angezeigt.

Anmerkungen werden auf folgende Weise zugewiesen:

- Sie können einer Anlage eine Anmerkung manuell zuweisen.

  Wenn eine Anmerkung direkt einer Anlage zugewiesen wird, wird die Anmerkung als normaler Text auf einer Anlagenseite angezeigt. Anmerkungen, die manuell zugewiesen werden, haben immer Vorrang vor Annotationen, die durch Annotationsregeln geerbt oder zugewiesen werden.

- Sie können eine Anmerkungsregel erstellen, um Anlagen desselben Typs automatisch Anmerkungen zuzuweisen.

  Wenn die Anmerkung nach Regel zugewiesen ist, zeigt Insight den Regelnamen neben dem Namen der Anmerkung auf einer Anlagenseite an.

- Insight ordnet Ihrem Storage-Tier automatisch ein Tier-Modell zu und beschleunigt so die Zuweisung von Storage-Annotationen zu Ihren Ressourcen bei der Beschaffung von Assets.

  Bestimmte Speicherressourcen werden automatisch einem vordefinierten Tier zugeordnet (Tier 1 und Tier 2). Beispielsweise basiert die Symmetrix-Speicherebene auf der Symmetrix- und VMAX-Produktreihe und ist Tier 1 zugeordnet. Sie können die Standardwerte an Ihre Ebenenanforderungen anpassen. Wenn die Anmerkung von Insight zugewiesen wird (z. B. „Tier“), wird „`systemdefiniert`“ angezeigt, wenn Sie den Cursor über den Namen der Anmerkung auf einer Anlagenseite positionieren.

- Einige Ressourcen (untergeordnete Elemente einer Anlage) können die vordefinierte Tier-Annotation aus ihrer Anlage (übergeordnete Anlage) ableiten.

  Wenn Sie beispielsweise einem Storage eine Annotation zuweisen, wird die Tier-Annotation von allen Speicherpools, internen Volumes, Volumes, qtrees und Shares abgeleitet, die zum Storage gehören. Wenn auf ein internes Volume des Storage eine andere Annotation angewendet wird, wird diese Annotation anschließend von allen Volumes, qtrees und Shares abgeleitet. „`abgeleitete`“ wird neben dem Namen der Anmerkung auf einer Anlagenseite angezeigt.

#### Zuordnen von Kosten zu Anmerkungen

Bevor Sie kostenbezogene Berichte erstellen, sollten Sie Anmerkungen auf Systemebene Service Level, Switch-Level und Tiering zuordnen, die Kostenverrechnung für die Storage-Benutzer auf Basis der tatsächlichen Nutzung von Produktions- und replizierter Kapazität ermöglichen. Beispielsweise können Sie für die Stufe „Tier“ möglicherweise Werte für die Stufe „Gold“ und „Silber“ festlegen und der Stufe „Gold“ höhere Kosten zuweisen als der Stufe „Silber“.

**Schritte**

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf Verwalten und wählen Sie **Anmerkungen**.

   Die Seite Anmerkung wird angezeigt.

3. Bewegen Sie den Mauszeiger über die Beschriftung Service Level, Switch Level oder Tier, und klicken Sie auf .

   Das Dialogfeld Anmerkung bearbeiten wird angezeigt.

4. Geben Sie die Werte für alle vorhandenen Ebenen in das Feld **Kosten** ein.

Die Tier- und Service-Level-Anmerkungen weisen die Werte für Auto-Tier bzw. Objekt-Storage auf, die Sie nicht entfernen können.

5. Klicken Sie Auf

Um weitere Ebenen hinzuzufügen.
6. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

#### Erstellen benutzerdefinierter Anmerkungen

Mithilfe von Annotationen können Sie benutzerdefinierte geschäftsspezifische Daten hinzufügen, die auf die Anforderungen Ihres Unternehmens an Assets abgestimmt sind. OnCommand Insight bietet zwar eine Reihe von Standardanmerkungen, aber Sie können feststellen, dass Sie Daten auf andere Weise anzeigen möchten. Die Daten in benutzerdefinierten Annotationen ergänzen die bereits erfassten Gerätedaten wie Switch-Hersteller, Anzahl Ports und Leistungsstatistiken. Die mit Annotationen hinzugefügten Daten werden von Insight nicht erkannt.

##### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Auf der Seite Anmerkungen wird die Liste der Anmerkungen angezeigt.
3. Klicken Sie Auf

.

   Das Dialogfeld **Anmerkung hinzufügen** wird angezeigt.
4. Geben Sie einen Namen und eine Beschreibung in die Felder **Name** und **Beschreibung** ein.

   Sie können in diese Felder bis zu 255 Zeichen eingeben.

   Beschriftungsnamen, die mit einem Punkt beginnen oder enden. Werden nicht unterstützt.
5. Klicken Sie auf **Typ** und wählen Sie dann eine der folgenden Optionen aus, die den in dieser Anmerkung zulässigen Datentyp darstellt:
   - Boolesch

     Dadurch wird eine Dropdown-Liste mit den Optionen „Ja“ und „Nein“ erstellt Die Anmerkung „`Direct Attached`“ ist z. B. Boolesch.
   - Datum

     Dadurch wird ein Feld erstellt, das ein Datum enthält. Wenn es sich bei der Anmerkung um ein Datum handelt, wählen Sie diese Option aus.
   - Liste

     Dadurch können folgende Elemente erstellt werden:
     - Eine feste Dropdown-Liste

Wenn andere diesem Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste keine weiteren Werte hinzufügen.

- Eine Liste mit flexiblen Dropdown-Menüs

  Wenn Sie beim Erstellen dieser Liste die Option **Neue Werte hinzufügen** auswählen, wenn andere diesen Anmerkungstyp auf einem Gerät zuweisen, können sie der Liste weitere Werte hinzufügen.

◦ Nummer

Dadurch wird ein Feld erstellt, in dem der Benutzer, der die Anmerkung zuweist, eine Zahl eingeben kann. Wenn der Anmerkungstyp beispielsweise „`Boden`“ lautet, kann der Benutzer den Wertetyp „`Zahl`“ auswählen und die Etagennummer eingeben.

◦ Text

Dadurch wird ein Feld erstellt, das Freiformtext ermöglicht. Sie können beispielsweise „`Sprache`“ als Anmerkungstyp eingeben, „`Text`“ als Wertetyp auswählen und eine Sprache als Wert eingeben.

Nachdem Sie den Typ festgelegt und Ihre Änderungen gespeichert haben, können Sie den Typ der Anmerkung nicht ändern. Wenn Sie den Typ ändern müssen, müssen Sie die Anmerkung löschen und eine neue erstellen.

6. Wenn Sie **Liste**als Anmerkungstyp auswählen, gehen Sie wie folgt vor:
   a. Wählen Sie **Neue Werte hinzufügen auf der Fly** aus, wenn Sie der Anmerkung weitere Werte hinzufügen möchten, wenn Sie auf einer Asset-Seite, die eine flexible Liste erstellt.

      Angenommen, Sie befinden sich auf einer Asset-Seite und das Asset hat die City-Anmerkung mit den Werten Detroit, Tampa und Boston. Wenn Sie die Option **Neue Werte hinzufügen auf der Fly** ausgewählt haben, können Sie City wie San Francisco und Chicago direkt auf der Asset-Seite zusätzliche Werte hinzufügen, anstatt zur Seite Anmerkungen zu gehen, um sie hinzuzufügen. Wenn Sie diese Option nicht wählen, können Sie beim Anwenden der Anmerkung keine neuen Anmerkungswerte hinzufügen; dadurch wird eine feste Liste erstellt.

   b. Geben Sie einen Wert und einen Namen in die Felder **Wert** und **Beschreibung** ein.
   c. Klicken Sie Auf

Um weitere Werte hinzuzufügen.
   d. Klicken Sie Auf Um einen Wert zu entfernen.
7. Klicken Sie Auf **Speichern**.

Ihre Anmerkungen werden in der Liste auf der Seite Anmerkungen angezeigt.

### Verwandte Informationen

"Importieren und Exportieren von Benutzerdaten"

#### Manuelles Zuweisen von Anmerkungen zu Assets

Durch das Zuweisen von Annotationen zu Assets können Sie Assets auf eine für Ihr Unternehmen relevante Weise sortieren, gruppieren und protokollieren. Obwohl Sie Anlagen eines bestimmten Typs automatisch Anmerkungen zuweisen können, können

Sie mithilfe von Anmerkungsregeln Anmerkungen zu einer einzelnen Anlage über die zugehörige Anlagenseite zuweisen.

### Bevor Sie beginnen

Sie müssen die Anmerkung erstellt haben, die Sie zuweisen möchten.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie die Anlage, auf die Sie die Anmerkung anwenden möchten, indem Sie einen der folgenden Schritte ausführen:
   - Klicken Sie im Asset Dashboard auf das Asset.
   - Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Typ oder den Namen des Assets ein, und wählen Sie dann das Asset aus der angezeigten Liste aus.

     Die Seite Anlage wird angezeigt.
3. Klicken Sie im Abschnitt **Benutzerdaten** der Seite Asset auf + Add.

   Das Dialogfeld Anmerkung hinzufügen wird angezeigt.
4. Klicken Sie auf **Anmerkung** und wählen Sie eine Anmerkung aus der Liste aus.
5. Klicken Sie auf **Wert**, und führen Sie je nach Art der ausgewählten Anmerkung einen der folgenden Schritte aus:
   - Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   - Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
6. Klicken Sie Auf **Speichern**.
7. Wenn Sie den Wert der Anmerkung ändern möchten, nachdem Sie sie zugewiesen haben, klicken Sie auf Und wählen Sie einen anderen Wert aus.

   Wenn die Anmerkung vom Listentyp ist, für den die Option **Werte dynamisch bei Anmerkungszuweisung hinzufügen** ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

#### Anmerkungen ändern

Sie können den Namen, die Beschreibung oder die Werte für eine Anmerkung ändern oder eine Anmerkung löschen, die Sie nicht mehr verwenden möchten.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Die Seite Anmerkungen wird angezeigt.
3. Bewegen Sie den Cursor über die Anmerkung, die Sie bearbeiten möchten, und klicken Sie auf .

   Das Dialogfeld * Anmerkung bearbeiten* wird angezeigt.

4. Sie können die folgenden Änderungen an einer Anmerkung vornehmen:

   a. Ändern Sie den Namen, die Beschreibung oder beides.

      Beachten Sie jedoch, dass Sie für den Namen und die Beschreibung maximal 255 Zeichen eingeben können und Sie den Typ einer Anmerkung nicht ändern können. Bei Anmerkungen auf Systemebene können Sie den Namen oder die Beschreibung nicht ändern. Sie können jedoch Werte hinzufügen oder entfernen, wenn es sich um einen Listentyp handelt.

      Wenn eine benutzerdefinierte Anmerkung im Data Warehouse veröffentlicht wird und Sie sie umbenennen, gehen die historischen Daten verloren.

   a. Um einer Anmerkung des Listentyps einen weiteren Wert hinzuzufügen, klicken Sie auf + Add.
   b. Um einen Wert aus einer Anmerkung des Listentyps zu entfernen, klicken Sie auf .

      Sie können einen Anmerkungswert nicht löschen, wenn dieser Wert einer Anmerkung zugeordnet ist, die in einer Anmerkungsregel, einer Abfrage oder einer Leistungsrichtlinie enthalten ist.

5. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

### Nachdem Sie fertig sind

Wenn Sie Anmerkungen im Data Warehouse verwenden möchten, müssen Sie eine Aktualisierung der Anmerkungen im Data Warehouse erzwingen. Weitere Informationen finden Sie im *OnCommand Insight Data Warehouse Administration Guide*.

#### Anmerkungen werden gelöscht

Sie können eine Anmerkung löschen, die Sie nicht mehr verwenden möchten. Eine Annotation auf Systemebene oder eine Annotation, die in einer Annotationsregel, einer Abfrage oder einer Performance-Richtlinie verwendet wird, kann nicht gelöscht werden.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungen**.

   Die Seite Anmerkungen wird angezeigt.

3. Setzen Sie den Cursor auf die Anmerkung, die Sie löschen möchten, und klicken Sie auf .

   Ein Bestätigungsdialogfeld wird angezeigt.

4. Klicken Sie auf **OK**.

### Zuordnen von Anmerkungen zu Anlagen mithilfe von Anmerkungsregeln

Um Assets anhand von Kriterien, die Sie definieren, automatisch Anmerkungen zuzuweisen, konfigurieren Sie Anmerkungsregeln. OnCommand Insight weist den Assets anhand dieser Regeln die Annotationen zu. Insight bietet außerdem zwei standardmäßige Anmerkungsregeln, die Sie an Ihre Anforderungen anpassen oder entfernen können, wenn Sie sie nicht verwenden möchten.

#### Standardmäßige Regeln für Storage-Annotationen

Um die Zuweisung von Storage-Annotationen zu Ihren Ressourcen zu beschleunigen, bietet OnCommand Insight 21 standardmäßige Annotationsregeln, die eine Tier-Stufe mit einem Storage-Tier-Modell verknüpfen. Alle Storage-Ressourcen werden bei Erwerb der Assets in Ihrer Umgebung automatisch einem Tier zugeordnet.

Die Standardbeschriftungsregeln wenden eine Ebenenbeschriftung wie folgt an:

- Tier 1, Quality Tier für Storage

  Die Beschriftung der Stufe 1 wird auf die folgenden Anbieter und deren angegebene Produktfamilien angewendet: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 oder FAS6200) und Violin (Speicher).

- Tier 2, Quality Tier für Storage

  Die Tier 2-Annotation wird für die folgenden Anbieter und deren Familien angewendet: HP (3PAR StoreServ oder EVA), EMC (CLARiiON), HDS (AMS oder D800), IBM (XIV) und NetApp (FAS3000, FAS3100 und FAS3200).

Sie können die Standardeinstellungen dieser Regeln entsprechend Ihren Ebenenanforderungen bearbeiten oder entfernen, wenn Sie sie nicht benötigen.

#### Anmerkungsregeln werden erstellt

Alternativ zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Wenn Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

**Bevor Sie beginnen**

Sie müssen eine Abfrage für die Anmerkungsregel erstellt haben.

**Über diese Aufgabe**

Sie können zwar die Anmerkungstypen bearbeiten, während Sie die Regeln erstellen, aber Sie sollten die Typen bereits im Voraus definiert haben.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Klicken Sie Auf

.

   Das Dialogfeld Regel hinzufügen wird angezeigt.

4. Gehen Sie wie folgt vor:
   a. Geben Sie im Feld **Name** einen eindeutigen Namen ein, der die Regel beschreibt.

      Dieser Name wird auf der Seite Anmerkungsregeln angezeigt.

   b. Klicken Sie auf **Abfrage** und wählen Sie die Abfrage aus, die OnCommand Insight verwenden soll, um die Anmerkung auf Anlagen anzuwenden.
   c. Klicken Sie auf **Anmerkung** und wählen Sie die Beschriftung aus, die Sie anwenden möchten.
   d. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

      Wenn Sie beispielsweise als Anmerkung Geburtstag auswählen, geben Sie ein Datum für den Wert an.
5. Klicken Sie Auf **Speichern**.
6. Klicken Sie auf **Alle Regeln**, wenn Sie alle Regeln sofort ausführen möchten; andernfalls werden die Regeln in einem regelmäßigen geplanten Intervall ausgeführt.

#### Festlegen der Priorität der Anmerkungsregel

Standardmäßig bewertet OnCommand Insight Annotationsregeln sequenziell. Sie können jedoch die Reihenfolge konfigurieren, in der OnCommand Insight Annotationsregeln auswertet, wenn Sie möchten, dass Insight Regeln in einer bestimmten Reihenfolge auswertet.

**Schritte**

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.
3. Bewegen Sie den Cursor über eine Anmerkungsregel.

   Die Rangfolge-Pfeile erscheinen rechts von der Regel.
4. Um eine Regel in der Liste nach oben oder unten zu verschieben, klicken Sie auf den Aufwärtspfeil oder den Abwärtspfeil.

   Standardmäßig werden neue Regeln nacheinander zur Liste der Regeln hinzugefügt. Wenn Insight die Anmerkungsregeln auswertet, haben Annotationen, die manuell auf den Seiten einzelner Assets festgelegt wurden, Vorrang vor regelbasierten Annotationen.

#### Anmerkungsregeln ändern

Sie können eine Anmerkungsregel ändern, um den Namen der Regel, ihre Anmerkung, den Wert der Anmerkung oder die mit der Regel verknüpfte Abfrage zu ändern.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten** und wählen Sie **Anmerkungsregeln**.

Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Suchen Sie die Regel, die Sie ändern möchten:
   - Auf der Seite Anmerkungsregeln können Sie die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben.
   - Klicken Sie auf eine Seitenzahl, um die Anmerkungsregeln nach Seite zu durchsuchen, wenn mehr Regeln als auf eine Seite passen.
4. Führen Sie einen der folgenden Schritte aus, um das Dialogfeld **Regel bearbeiten** anzuzeigen:
   - Wenn Sie sich auf der Seite Anmerkungsregeln befinden, setzen Sie den Cursor auf die Anmerkungsregel, und klicken Sie auf .
   - Wenn Sie sich auf einer Bestandsseite befinden, setzen Sie den Cursor auf die Anmerkung, die der Regel zugeordnet ist, setzen Sie den Cursor auf den Namen der Regel, wenn sie angezeigt wird, und klicken Sie dann auf den Namen der Regel.
5. Nehmen Sie die erforderlichen Änderungen vor und klicken Sie auf **Speichern**.

#### Anmerkungsregeln werden gelöscht

Sie können eine Anmerkungsregel löschen, wenn die Regel nicht mehr erforderlich ist, um die Objekte im Netzwerk zu überwachen.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Verwalten**, und wählen Sie **Anmerkungsregeln**.

   Auf der Seite Anmerkungsregeln wird die Liste der vorhandenen Anmerkungsregeln angezeigt.

3. Suchen Sie die zu löschende Regel:
   - Auf der Seite Anmerkungsregeln können Sie die Anmerkungsregeln filtern, indem Sie einen Wert in das Filterfeld eingeben.
   - Klicken Sie auf eine Seitenzahl, um die Anmerkungsregeln nach Seite zu durchsuchen, wenn mehr Regeln als auf eine einzelne Seite passen.
4. Zeigen Sie mit dem Cursor auf die Regel, die Sie löschen möchten, und klicken Sie dann auf .

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Regel löschen möchten.

5. Klicken Sie auf **OK**.

#### Importieren von Anmerkungswerten

Wenn Sie Anmerkungen zu SAN-Objekten (wie Storage, Hosts und Virtual Machines) in einer CSV-Datei beibehalten, können Sie diese Informationen in OnCommand Insight importieren. Sie können Applikationen, Geschäftseinheiten oder Annotationen wie Tiering und Building importieren.

##### Über diese Aufgabe

Es gelten die folgenden Regeln:

- Wenn ein Anmerkungswert leer ist, wird diese Anmerkung vom Objekt entfernt.
- Wenn Sie Volumes oder interne Volumes mit Anmerkungen versehen, ist der Objektname eine Kombination aus Storage-Namen und Volume-Namen. Verwenden Sie dabei den Bindestrich und das Pfeiltrennzeichen (->):

  ```
  <storage_name>-><volume_name>
  ```

- Wenn Speicher, Switches oder Ports mit Anmerkungen versehen werden, wird die Spalte Anwendung ignoriert.
- Die Spalten Tenant, Line_of_Business, Business_Unit und Project bilden eine Geschäftseinheit.

  Alle Werte können leer bleiben. Wenn eine Applikation bereits mit einer anderen Business Entity als den Eingabewerten verknüpft ist, wird die Applikation der neuen Business Entity zugewiesen.

Die folgenden Objekttypen und Schlüssel werden im Importdienstprogramm unterstützt:

| Typ | Taste |
|---|---|
| Host | `id-><id>` Oder `<Name>` Oder `<IP>` |
| VM | `id-><id>` Oder `<Name>` |
| Storage-Pool | `id-><id>` Oder `<Storage_name>-><Storage_Pool_name>` |
| Internes Volumen | `id-><id>` Oder `<Storage_name>-><Internal_volume_name>` |
| Datenmenge | `id-><id>` Oder `<Storage_name>-><Volume_name>` |
| Storage | `id-><id>` Oder `<Name>` Oder `<IP>` |
| Switch | `id-><id>` Oder `<Name>` Oder `<IP>` |
| Port | `id-><id>` Oder `<WWN>` |
| Share | `id-><id>` Oder `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol>` `<Qtree>` Ist optional, wenn es einen Standard-qtree gibt. |
| Qtree | `id-><id>` Oder `<Storage Name>-><Internal Volume Name>-><Qtree Name>` |

Die CSV-Datei sollte das folgende Format verwenden:

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

**Schritte**

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Admin** und wählen Sie **Troubleshooting**.

   Die Seite Fehlerbehebung wird angezeigt.
3. Klicken Sie im Abschnitt **andere Aufgaben** der Seite auf den Link **OnCommand Insight-Portal**.
4. Klicken Sie auf **Insight Connect API**.
5. Melden Sie sich beim Portal an.
6. Klicken Sie Auf **Annotation Import Utility**.
7. Speichern Sie die `.zip` Datei, entpacken und lesen `readme.txt` Datei für weitere Informationen und Beispiele.
8. Platzieren Sie die CSV-Datei in demselben Ordner wie die `.zip` Datei:
9. Geben Sie im Befehlszeilenfenster Folgendes ein:

   ```
   java -jar rest-import-utility.jar [-uusername] [-ppassword]
   [-aserver name or IP address] [-bbatch size] [-ccase
   sensitive:true/false]
   [-lextra logging:true/false] csv filename
   ```

   Die Option -l, die die zusätzliche Protokollierung ermöglicht, und die Option -c, die die Groß-/Kleinschreibung aktiviert, sind standardmäßig auf false gesetzt. Daher müssen Sie diese nur angeben, wenn Sie die Funktionen verwenden möchten.

   Zwischen den Optionen und ihren Werten gibt es keine Leerzeichen.

Die folgenden Schlüsselwörter sind reserviert und verhindern, dass Benutzer sie als Anmerkungsnamen angeben: - Application - Application_Priority - Tenant - Line_of_Business - Business_Unit - Projektfehler werden generiert, wenn Sie versuchen, einen Anmerkungstyp mit einem der reservierten Schlüsselwörter zu importieren. Wenn Sie mit diesen Stichwörtern Beschriftungsnamen erstellt haben, müssen Sie diese ändern, damit das Importdienstprogramm ordnungsgemäß funktioniert.

Das Dienstprogramm Annotation Import erfordert Java 8 oder Java 11. Stellen Sie sicher, dass eine dieser Komponenten vor dem Ausführen des Importdienstprogramms installiert ist. Es wird empfohlen, die neueste OpenJDK 11 zu verwenden.

### Zuweisen von Anmerkungen zu mehreren Anlagen mithilfe einer Abfrage

Durch das Zuweisen einer Anmerkung zu einer Gruppe von Assets können Sie diese zugehörigen Assets leichter identifizieren oder in Abfragen oder Dashboards verwenden.

#### Bevor Sie beginnen

Anmerkungen, die Sie Anlagen zuweisen möchten, müssen zuvor erstellt worden sein.

#### Über diese Aufgabe

Sie können das Zuweisen einer Anmerkung zu mehreren Anlagen vereinfachen, indem Sie eine Abfrage verwenden. Wenn Sie beispielsweise allen Arrays an einem bestimmten Standort im Datacenter eine benutzerdefinierte Adressenanmerkung zuweisen möchten,

#### Schritte

1. Erstellen Sie eine neue Abfrage, um die Assets zu identifizieren, denen Sie eine Anmerkung zuweisen möchten. Klicken Sie Auf **Abfragen** > **+Neue Abfrage**.
2. Wählen Sie in der Dropdown-Liste **Suchen nach… Speicher**. Sie können Filter festlegen, um die Liste der angezeigten Speicher weiter einzugrenzen.
3. Wählen Sie in der angezeigten Liste der Speicher einen oder mehrere Speicher aus, indem Sie auf das Kontrollkästchen neben dem Speichernamen klicken. Sie können auch alle angezeigten Speicher auswählen, indem Sie oben in der Liste auf das Hauptfeld klicken.
4. Wenn Sie alle gewünschten Speicher ausgewählt haben, klicken Sie auf **actions** > **Anmerkung bearbeiten**.

   Das Dialogfeld Anmerkung hinzufügen wird angezeigt.

5. Wählen Sie die **Anmerkung** und **Wert** aus, die Sie den Speichern zuweisen möchten, und klicken Sie auf **Speichern**.

   Wenn Sie die Spalte für diese Anmerkung anzeigen, wird sie auf allen ausgewählten Speichern angezeigt.

6. Sie können die Anmerkung jetzt verwenden, um nach Speichern in einem Widget oder einer Abfrage zu filtern. In einem Widget können Sie Folgendes tun:

   a. Erstellen Sie ein Dashboard oder öffnen Sie ein vorhandenes. Fügen Sie eine **Variable** hinzu und wählen Sie die Anmerkung aus, die Sie auf den obigen Speichern festgelegt haben. Die Variable wird dem Dashboard hinzugefügt.

b. Klicken Sie in dem neu hinzugefügten Variablenfeld auf **any** und geben Sie den entsprechenden Wert ein, nach dem gefiltert werden soll. Klicken Sie auf das Häkchen, um den Variablenwert zu speichern.

c. Widget hinzufügen. Klicken Sie in der Abfrage des Widgets auf die Schaltfläche**Filter by+**und wählen Sie die entsprechende Anmerkung aus der Liste aus.

d. Klicken Sie auf **any** und wählen Sie die oben hinzugefügte Anmerkungsvariable aus. Die von Ihnen erstellten Variablen beginnen mit „``“ und werden in der Dropdown-Liste angezeigt.

e. Stellen Sie alle anderen Filter oder Felder, die Sie wünschen, dann klicken Sie **Speichern**, wenn das Widget nach Ihren Wünschen angepasst ist.

Im Widget auf dem Dashboard werden nur die Daten für die Speicher angezeigt, denen Sie die Anmerkung zugewiesen haben.

# Elemente werden abgefragt

Abfragen ermöglichen Ihnen die Überwachung und Fehlerbehebung im Netzwerk, indem Sie die Assets in Ihrer Umgebung auf granularer Ebene durchsuchen, die auf vom Benutzer ausgewählten Kriterien (Annotationen und Performance-Metriken) basieren. Außerdem ist für Anmerkungsregeln, die Anlagen automatisch Anmerkungen zuweisen, eine Abfrage erforderlich.

## In Abfragen und Dashboards verwendete Assets

### Insight-Abfragen und Dashboard-Widgets können mit einer Vielzahl von Asset-Typen verwendet werden

Die folgenden Asset-Typen können in Abfragen, Dashboard-Widgets und benutzerdefinierten Asset-Seiten verwendet werden. Die für Filter, Ausdrücke und Anzeigen verfügbaren Felder und Zähler variieren je nach Asset-Typen. Nicht alle Assets können in allen Widgets verwendet werden.

- Applikation
- Datenspeicher
- Festplatte
- Fabric
- Generisches Gerät
- Host
- Internes Volumen
- ISCSI-Sitzung
- ISCSI-Netzwerkportal
- Pfad
- Port
- Qtree
- Kontingente
- Share
- Storage

- Storage-Node
- Storage-Pool
- Switch
- Tape
- VMDK
- Virtual Machine
- Datenmenge
- Zone
- Zonenmitglied

## Erstellen einer Abfrage

Sie können eine Abfrage erstellen, um die Assets in Ihrer Umgebung auf granularer Ebene zu durchsuchen. Mithilfe von Abfragen können Sie Daten aufteilen, indem Sie Filter hinzufügen und die Ergebnisse sortieren, um Bestands- und Leistungsdaten in einer Ansicht anzuzeigen.

### Über diese Aufgabe

Sie können beispielsweise eine Abfrage für Volumes erstellen, einen Filter hinzufügen, um bestimmte Speicher zu finden, die dem ausgewählten Volume zugeordnet sind, einen Filter hinzufügen, um eine bestimmte Anmerkung, wie z. B. Schicht 1, für die ausgewählten Speicher zu finden, Und schließlich fügen Sie einen weiteren Filter hinzu, um alle Speicher mit IOPS - Lesen (IO/s) größer als 25 zu finden. Wenn die Ergebnisse angezeigt werden, können Sie die mit der Abfrage verknüpften Datenspalten in aufsteigender oder absteigender Reihenfolge sortieren.

Wenn eine neue Datenquelle hinzugefügt wird, die Assets erfasst oder Anmerkungen oder Anwendungszuweisungen vorgenommen werden, können Sie nach der Indizierung der Abfragen, die in einem regelmäßig geplanten Intervall stattfinden, nach diesen Assets, Anmerkungen oder Anwendungen suchen.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **+ Neue Abfrage**.
3. Klicken Sie auf **Select Resource Type** und wählen Sie einen Asset-Typ aus.

   Wenn eine Ressource für eine Abfrage ausgewählt wird, werden automatisch eine Reihe von Standardspalten angezeigt. Sie können diese Spalten jederzeit entfernen oder neue hinzufügen.

4. Geben Sie in das Textfeld **Name** den Namen des Assets ein oder geben Sie einen Textteil ein, um durch die Anlagennamen zu filtern.

   Sie können die folgenden Elemente allein oder kombiniert verwenden, um Ihre Suche in einem beliebigen Textfeld auf der Seite Neue Abfrage zu verfeinern:

   - Mit einem Sternchen können Sie nach allem suchen. Beispiel: `vol*rhel` Zeigt alle Ressourcen an, die mit „`vol`“ beginnen und mit „`RHEL`“ enden.
   - Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Beispiel: `BOS-`

`PRD??-S12` Zeigt BOS-PRD12-S12, BOS-PRD13-S12 usw. an.

- Mit dem Operator ODER können Sie mehrere Einheiten angeben. Beispiel: `FAS2240 OR CX600 OR FAS3270` Findet mehrere Storage-Modelle
- Der NICHT-Operator ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen. Beispiel: `NOT EMC*` Findet alles, was nicht mit „EMC“ beginnt. Verwenden Sie können `NOT *` So zeigen Sie Felder an, die keinen Wert enthalten.

5. Klicken Sie Auf Um die Assets anzuzeigen.
6. Um ein Kriterium hinzuzufügen, klicken Sie auf

Und führen Sie eine der folgenden Aktionen aus:
   - Geben Sie ein, um nach bestimmten Kriterien zu suchen, und wählen Sie es aus.
   - Blättern Sie in der Liste nach unten, und wählen Sie ein Kriterium aus.
   - Geben Sie einen Wertebereich ein, wenn Sie eine Performance-Metrik wie IOPS - Lesen (IO/s) auswählen. Von Insight bereitgestellte Standardanmerkungen werden durch angezeigt; Es ist möglich, Anmerkungen mit doppelten Namen zu haben.

   In den Listenaktualisierungen wird der Liste Abfrageergebnisse eine Spalte für die Kriterien und die Ergebnisse der Abfrage hinzugefügt.
7. Optional können Sie auf klicken Um eine Anmerkung oder Performance-Metrik aus den Abfrageergebnissen zu entfernen.

   Wenn Ihre Abfrage beispielsweise die maximale Latenz und den maximalen Durchsatz für Datastores anzeigt und Sie nur die maximale Latenz in der Liste der Abfrageergebnisse anzeigen möchten, klicken Sie auf diese Schaltfläche und deaktivieren Sie das Kontrollkästchen **Throughput - max**. Die Spalte Throughput - Max (MB/s) wird aus der Liste der Abfrageergebnisse entfernt.

   Abhängig von der Anzahl der Spalten, die in der Abfrageergebnistabelle angezeigt werden, können Sie möglicherweise keine weiteren hinzugefügten Spalten anzeigen. Sie können eine oder mehrere Spalten entfernen, bis die gewünschten Spalten angezeigt werden.
8. Klicken Sie auf **Speichern**, geben Sie einen Namen für die Abfrage ein und klicken Sie erneut auf **Speichern**.

   Wenn Sie über ein Konto mit einer Administratorrolle verfügen, können Sie benutzerdefinierte Dashboards erstellen. Ein benutzerdefiniertes Dashboard kann alle Widgets aus der Widget-Bibliothek enthalten, von denen mehrere Sie Abfrageergebnisse in einem benutzerdefinierten Dashboard darstellen können. Weitere Informationen zu benutzerdefinierten Dashboards finden Sie im *OnCommand Insight Handbuch zum Einstieg*.

**Verwandte Informationen**

"Importieren und Exportieren von Benutzerdaten"

## Anzeigen von Abfragen

Sie können Ihre Abfragen anzeigen, um Ihre Assets zu überwachen und zu ändern, wie Ihre Abfragen die Daten zu Ihren Assets anzeigen.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.
3. Sie können die Anzeige von Abfragen mit einer der folgenden Methoden ändern:
   - Sie können Text in das Feld **Filter** eingeben, um nach bestimmten Abfragen zu suchen.
   - Sie können die Sortierreihenfolge der Spalten in der Tabelle der Abfragen durch Klicken auf den Pfeil in der Spaltenüberschrift auf aufsteigender (Aufwärtspfeil) oder absteigender (Abwärtspfeil) ändern.
   - Wenn Sie die Größe einer Spalte ändern möchten, bewegen Sie den Mauszeiger über die Spaltenüberschrift, bis ein blauer Balken angezeigt wird. Legen Sie die Maus über die Leiste, und ziehen Sie sie nach rechts oder links.
   - Um eine Spalte zu verschieben, klicken Sie auf die Spaltenüberschrift und ziehen Sie sie nach rechts oder links.
   - Beachten Sie beim Durchblättern der Abfrageergebnisse, dass sich die Ergebnisse ändern können, wenn Insight Ihre Datenquellen automatisch abfragt. Dies kann dazu führen, dass einige Elemente fehlen oder einige Elemente in der Reihenfolge erscheinen, je nachdem, wie sie sortiert sind.

## Abfrageergebnisse werden in eine CSV-Datei exportiert

Sie können die Ergebnisse einer Abfrage in eine CSV-Datei exportieren, um die Daten in eine andere Anwendung zu importieren.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.
3. Klicken Sie auf eine Abfrage.
4. Klicken Sie Auf So exportieren Sie Abfrageergebnisse in ein `.CSV` Datei:
5. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Öffnen mit** und dann auf **OK**, um die Datei mit Microsoft Excel zu öffnen und die Datei an einem bestimmten Speicherort zu speichern.
   - Klicken Sie auf **Datei speichern** und dann auf **OK**, um die Datei im Ordner Downloads zu speichern. Nur die Attribute für die angezeigten Spalten werden exportiert. Einige angezeigte Spalten, insbesondere solche, die Teil komplexer verschachtelter Beziehungen sind, werden nicht exportiert.

     Wenn ein Komma in einem Anlagennamen angezeigt wird, schließt der Export den Namen in Anführungszeichen ein, wobei der Name des Assets und das entsprechende .csv-Format erhalten bleiben.

     + beim Exportieren von Abfrageergebnissen ist zu beachten, dass **alle** Zeilen in der Ergebnistabelle exportiert werden, nicht nur die auf dem Bildschirm ausgewählten oder angezeigten Zeilen, maximal 10,000 Zeilen.

Wenn Sie eine exportierte CSV-Datei mit Excel öffnen, wenn Sie einen Objektnamen oder ein anderes Feld im Format NN:NN haben (zwei Ziffern gefolgt von einem Doppelpunkt gefolgt von zwei weiteren Ziffern), interpretiert Excel diesen Namen manchmal als Zeitformat, statt Textformat. Dies kann dazu führen, dass in Excel falsche Werte in diesen Spalten angezeigt werden. Ein Objekt mit dem Namen „81:45“ wird beispielsweise in Excel als „81:45:00“ angezeigt. Um dies zu umgehen, importieren Sie die .CSV-Datei in Excel anhand der folgenden Schritte:

+

```
-   Open a new sheet in Excel.
-   On the "Data" tab, choose "From Text".
-   Locate the desired .CSV file and click "Import".
-   In the Import wizard, choose "Delimited" and click Next.
-   Choose "Comma" for the delimiter and click Next.
-   Select the desired columns and choose "Text" for the column data
format.
-   Click Finish.
Your objects should show in Excel in the proper format.
```

+

## Ändern von Abfragen

Sie können die Kriterien ändern, die einer Abfrage zugeordnet sind, wenn Sie die Suchkriterien für die abfragenden Assets ändern möchten.

### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.
3. Klicken Sie auf den Abfragenamen.
4. Um ein Kriterium aus der Abfrage zu entfernen, klicken Sie auf .
5. Um der Abfrage ein Kriterium hinzuzufügen, klicken Sie auf

, Und wählen Sie ein Kriterium aus der Liste aus.
6. Führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Speichern**, um die Abfrage mit dem ursprünglich verwendeten Namen zu speichern.
   - Klicken Sie auf **Speichern unter**, um die Abfrage mit einem anderen Namen zu speichern.
   - Klicken Sie auf **Umbenennen**, um den Abfragenamen zu ändern, den Sie ursprünglich verwendet haben.
   - Klicken Sie auf **revert**, um den Namen der Abfrage auf den Namen zurück zu ändern, den Sie ursprünglich verwendet hatten.

## Abfragen werden gelöscht

Sie können Abfragen löschen, wenn sie keine nützlichen Informationen über Ihre Assets mehr sammeln. Eine Abfrage kann nicht gelöscht werden, wenn sie in einer Anmerkungsregel verwendet wird.

### Schritte

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

3. Setzen Sie den Cursor auf die Abfrage, die Sie löschen möchten, und klicken Sie auf .

   Es wird eine Bestätigungsmeldung angezeigt, in der Sie gefragt werden, ob Sie die Abfrage löschen möchten.

4. Klicken Sie auf **OK**.

## Zuweisen mehrerer Anwendungen zu oder Entfernen mehrerer Anwendungen aus Assets

Sie können mehrere Anwendungen zu Assets zuweisen oder sie aus diesen Anwendungen entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell zuweisen oder entfernen zu müssen.

### Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets findet, die Sie bearbeiten möchten.

### Schritte

1. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets findet.

   Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den ausgewählten Assets eine Anwendung hinzuzufügen, klicken Sie auf Actions, Und wählen Sie **Anwendung bearbeiten**.
   a. Klicken Sie auf **Anwendung** und wählen Sie eine oder mehrere Anwendungen aus.

      Sie können mehrere Anwendungen für Hosts, interne Volumes und virtuelle Maschinen auswählen. Sie können jedoch nur eine Anwendung für ein Volume auswählen.

b. Klicken Sie Auf **Speichern**.

5. Klicken Sie auf, um eine der Assets zugewiesene Anwendung zu entfernen Actions Und wählen Sie **Anwendung entfernen**.

   a. Wählen Sie die Anwendung oder die Anwendungen aus, die Sie entfernen möchten.

   b. Klicken Sie Auf **Löschen**.

   Neue Anwendungen, die Sie zuweisen, überschreiben alle Anwendungen auf dem Asset, die von einem anderen Asset abgeleitet wurden. Beispielsweise übernehmen Volumes Applikationen von Hosts, und wenn neuen Applikationen einem Volume zugewiesen werden, hat die neue Applikation Vorrang vor der abgeleiteten Applikation.

## Bearbeiten oder Entfernen mehrerer Anmerkungen aus Anlagen

Sie können mehrere Anmerkungen für Anlagen bearbeiten oder mehrere Anmerkungen aus Anlagen entfernen, indem Sie eine Abfrage verwenden, anstatt sie manuell bearbeiten oder entfernen zu müssen.

### Bevor Sie beginnen

Sie müssen bereits eine Abfrage erstellt haben, die alle Assets sucht, die Sie bearbeiten möchten.

### Schritte

1. Klicken Sie auf **Abfragen** und wählen Sie **Alle Anfragen anzeigen**.

   Die Seite Abfragen wird angezeigt.

2. Klicken Sie auf den Namen der Abfrage, die die Assets sucht.

   Die Liste der mit der Abfrage verknüpften Assets wird angezeigt.

3. Wählen Sie die gewünschten Assets in der Liste aus, oder klicken Sie auf ☐ Um **Alle** auszuwählen.

   Die Schaltfläche **actions** wird angezeigt.

4. Um den Assets eine Anmerkung hinzuzufügen oder den Wert einer Anmerkung zu bearbeiten, die den Assets zugewiesen ist, klicken Sie auf Actions, Und wählen Sie **Anmerkung bearbeiten**.

   a. Klicken Sie auf **Anmerkung** und wählen Sie eine Anmerkung aus, für die Sie den Wert ändern möchten, oder wählen Sie eine neue Anmerkung aus, um sie allen Anlagen zuzuweisen.

   b. Klicken Sie auf **Wert** und wählen Sie einen Wert für die Anmerkung aus.

   c. Klicken Sie Auf **Speichern**.

5. Um eine den Assets zugewiesene Anmerkung zu entfernen, klicken Sie auf Actions, Und wählen Sie **Anmerkung entfernen**.

   a. Klicken Sie auf **Anmerkung** und wählen Sie die Anmerkung aus, die Sie aus den Assets entfernen möchten.

   b. Klicken Sie Auf **Löschen**.

### Tabellenwerte werden kopiert

Sie können Werte in Tabellen kopieren, um sie in Suchfeldern oder anderen Anwendungen zu verwenden.

#### Über diese Aufgabe

Es gibt zwei Methoden, mit denen Sie Werte aus Tabellen oder Abfrageergebnissen kopieren können.

#### Schritte

1. Methode 1: Markieren Sie den gewünschten Text mit der Maus, kopieren Sie ihn und fügen Sie ihn in Suchfelder oder andere Anwendungen ein.
2. Methode 2: Bewegen Sie bei Einzelwertfeldern, deren Länge die Breite der Tabellenspalte überschreitet, die durch Ellipsen (…) gekennzeichnet sind, den Mauszeiger über das Feld und klicken Sie auf das Clipboard-Symbol. Der Wert wird zur Verwendung in Suchfeldern oder anderen Anwendungen in die Zwischenablage kopiert.

   Beachten Sie, dass nur Werte, die Verknüpfungen zu Assets darstellen, kopiert werden können. Beachten Sie auch, dass nur Felder, die einzelne Werte enthalten (d. h. nicht-Listen), das Kopiersymbol haben.

# Insight – Datenquellmanagement

Datenquellen sind die kritischsten Komponenten zur Aufrechterhaltung einer OnCommand Insight Umgebung. Da sie die primäre Informationsquelle für Insight sind, müssen die Datenquellen unbedingt im laufenden Zustand gehalten werden.

Sie können die Datenquellen in Ihrem Netzwerk überwachen, indem Sie eine Datenquelle auswählen, um die Ereignisse im Zusammenhang mit ihrem Status zu überprüfen, und alle Änderungen, die möglicherweise Probleme verursacht haben, notieren.

Zusätzlich zur Untersuchung einer individuellen Datenquelle können Sie folgende Operationen durchführen:

- Klonen einer Datenquelle, um viele ähnliche Datenquellen in Insight zu erstellen
- Informationen zur Datenquelle bearbeiten
- Anmeldedaten ändern
- Kontrolle der Abfrage
- Löschen Sie die Datenquelle
- Installieren von Patches für Datenquellen
- Installieren Sie eine neue Datenquelle aus einem Patch
- Erstellen eines Fehlerberichts für den NetApp Customer Support

### Richten Sie Ihre Datenquellen in Insight ein

Datenquellen sind die kritischsten Komponenten bei der Wartung einer Insight Umgebung. Datenquellen erkennen Netzwerkinformationen, die zur Analyse und Validierung verwendet werden. Die Datenquellen müssen in Insight so konfiguriert

werden, dass sie innerhalb des Netzwerks überwacht werden können.

Für jede Datenquelle hängen die spezifischen Anforderungen zur Definition dieser Datenquelle vom Anbieter und Modell der entsprechenden Geräte ab. Bevor Sie die Datenquellen hinzufügen, benötigen Sie Netzwerkadressen, Kontoinformationen und Passwörter für alle Geräte und möglicherweise folgende zusätzliche Details:

- Schalter
- Gerätemanagement-Stationen
- Storage-Systeme mit IP-Konnektivität
- Speicherverwaltungsstationen
- Hostserver, auf denen die Managementsoftware für Speichergeräte ausgeführt wird, die keine IP-Verbindung haben

Weitere Informationen zu den Definitionen Ihrer Datenquellen finden Sie in den Informationen zu „Vendor-Specific Data source reference“ in diesem Abschnitt.

### Informationen zur Unterstützung der Datenquelle

Im Rahmen Ihrer Konfigurationsplanung sollten Sie sicherstellen, dass die Geräte in Ihrer Umgebung von Insight überwacht werden können. Dazu können Sie die Data Source Support Matrix für Details zu Betriebssystemen, spezifischen Geräten und Protokollen überprüfen. Einige Datenquellen sind möglicherweise nicht auf allen Betriebssystemen verfügbar.

#### Speicherort der aktuellsten Version der Data Source Support Matrix

Die Support-Matrix für die Datenquelle von OnCommand Insight wird mit jeder Service Pack-Version aktualisiert. Die aktuellste Version des Dokuments finden Sie unter "NetApp Support Website". .

### Hinzufügen von Datenquellen

Über das Dialogfeld Datenquelle hinzufügen können Sie Datenquellen schnell hinzufügen.

#### Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser, und melden Sie sich als Benutzer mit Administratorrechten an.
2. Wählen Sie **Admin** und wählen Sie **Datenquellen**.
3. Klicken Sie auf die Schaltfläche **+Add**.

   Der Assistent Datenquelle hinzufügen wird geöffnet.

4. Geben Sie im Abschnitt **Einstellungen** folgende Informationen ein:

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| Name | Geben Sie einen eindeutigen Netzwerknamen für diese Datenquelle ein. HINWEIS: Nur Buchstaben, Zahlen und der Unterstrich (_) sind im Datenquellennamen zulässig. |
| Anbieter | Wählen Sie den Anbieter der Datenquelle aus der Dropdown-Liste aus. |
| Modell | Wählen Sie das Modell der Datenquelle aus der Dropdown-Liste aus. |
| Laufort | Wählen Sie „Lokal“, oder wählen Sie eine Remote-Erfassungseinheit aus, wenn RAUs in Ihrer Umgebung konfiguriert sind. |
| Was zu sammeln ist | Für die meisten Datenquellen sind diese Optionen „Bestandsaufnahme“ und „Leistung“. Die Option „Inventar“ ist standardmäßig immer ausgewählt und kann nicht deaktiviert werden. Beachten Sie, dass einige Datenquellen unterschiedliche Optionen haben können. Die von Ihnen ausgewählten Erfassungsoptionen ändern die verfügbaren Felder in den Abschnitten Konfiguration und Erweiterte Konfiguration. |

5. Klicken Sie auf den Link **Konfiguration** und geben Sie die grundlegenden Setup-Informationen ein, die für die Datenquelle mit Ihrem ausgewählten Datenerfassungstyp erforderlich sind.
6. Wenn diese Art von Datenquelle normalerweise detailliertere Informationen benötigt, um sie in Ihrem Netzwerk einzurichten, klicken Sie auf den Link **Erweiterte Konfiguration**, um zusätzliche Informationen einzugeben.
7. Weitere Informationen zur Konfiguration oder zur erweiterten Konfiguration, die für Ihre spezifische Datenquelle erforderlich oder verfügbar sind, finden Sie unter "Herstellerspezifische Datenquelle".
8. Klicken Sie auf den Link **Test**, um sicherzustellen, dass die Datenquelle ordnungsgemäß konfiguriert ist.
9. Klicken Sie Auf **Speichern**.

#### Importieren von Datenquellen aus einer Tabelle

Sie können mehrere Datenquellen aus einer Tabelle in OnCommand Insight importieren. Dies könnte hilfreich sein, wenn Sie Ihre Ermittlungsgeräte bereits in einer Tabelle verwalten. Dieser Prozess fügt neue Datenquellen hinzu, kann jedoch nicht zur Aktualisierung vorhandener Datenquellen verwendet werden.

**Über diese Aufgabe**

OnCommand Insight enthält eine Tabelle zur Erstellung von Datenquellen. Diese Tabelle hat die folgenden Attribute:

- Die Tabelle kann mit Microsoft Excel 2003 oder höher verwendet werden.

- Jede Registerkarte enthält einen Datenquelltyp, z. B. Brocade SSH/CLI.
- Jede Zeile stellt eine Instanz einer neuen Datenquelle dar, die erstellt werden soll.

Die Tabelle enthält ein Makro, das eine neue Datenquelle in OnCommand Insight erstellt.

**Schritte**

1. Suchen Sie die Tabelle im `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
2. Geben Sie in der Tabelle die Informationen zur Datenquelle in die Zellen mit Farbe ein.
3. Leere Zeilen löschen.
4. Führen Sie in der Tabelle die aus `CreateDataSources` Makro, um die Datenquellen zu erstellen.
5. Wenn Sie zur Eingabe der Anmeldeinformationen aufgefordert werden, geben Sie den Benutzernamen und das Kennwort für die OnCommand Insight-Serveradministration ein.

   Die Ergebnisse werden im Erfassungsprotokoll protokolliert.

6. Eine Eingabeaufforderung fragt, ob auf dem Computer, auf dem das Makro ausgeführt wird, OnCommand Insight installiert ist.

   Wählen Sie eine der folgenden Optionen:

   - Nein: Wählen Sie „Nein“, wenn eine Batch-Datei erstellt wird, die auf dem OnCommand Insight-Rechner ausgeführt werden muss. Führen Sie diese Batch-Datei aus dem Installationsverzeichnis aus.
   - Ja: Wählen Sie „Ja“, wenn OnCommand Insight bereits installiert ist und keine weiteren Schritte erforderlich sind, um die Datenquellinformationen zu generieren.
7. Um das Hinzufügen der Datenquellen zu überprüfen, öffnen Sie Insight in Ihrem Browser.
8. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
9. Überprüfen Sie die Liste Datenquellen, die Sie importiert haben.

#### Hinzufügen einer neuen Datenquelle nach Patch

Neue Datenquellen werden als Patch-Dateien freigegeben, die mit dem Patch-Prozess auf das System geladen werden können. Dadurch sind neue Datenquellen zwischen geplanten Versionen von OnCommand Insight verfügbar.

**Bevor Sie beginnen**

Sie müssen die Patch-Datei hochgeladen haben, die Sie installieren möchten.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Wählen Sie **Patches**.
3. Wählen Sie **Actions** > **Service Pack oder Patch installieren**.
4. Klicken Sie im Dialogfeld **Service Pack oder Patch installieren** auf **Durchsuchen**, um die hochgeladene Patch-Datei zu suchen und auszuwählen.

5. Klicken Sie im Dialogfeld **Patch Summary** auf **Weiter**.
6. Überprüfen Sie die **Read Me**-Informationen, und klicken Sie auf **Next**, um fortzufahren.
7. Klicken Sie im Dialogfeld **Installieren** auf **Fertig stellen**.

### Klonen einer Datenquelle

Mit der Clone Facility können Sie schnell eine Datenquelle hinzufügen, die dieselben Anmeldedaten und Attribute wie eine andere Datenquelle enthält. Klonen ermöglicht Ihnen die einfache Konfiguration mehrerer Instanzen desselben Gerätetyps.

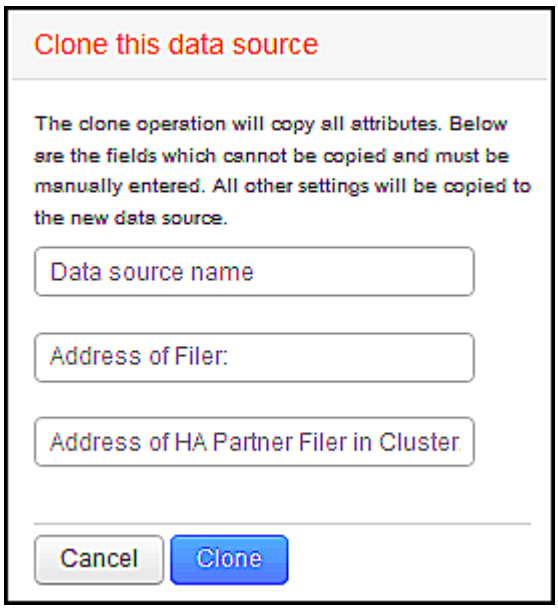
#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.

   Die Liste Datenquellen wird geöffnet.

2. Markieren Sie die Datenquelle mit den Setup-Informationen, die Sie für Ihre neue Datenquelle verwenden möchten.
3. Klicken Sie rechts neben der markierten Datenquelle auf das Symbol **Clone**.

   Im Dialogfeld „Diese Datenquelle klonen“ werden die Informationen aufgeführt, die Sie für die ausgewählte Datenquelle angeben müssen, wie in diesem Beispiel für eine NetApp Datenquelle dargestellt:




4. Geben Sie die erforderlichen Informationen in die Felder ein. Diese Angaben können nicht aus der vorhandenen Datenquelle kopiert werden.
5. Klicken Sie Auf **Clone**.

#### Ergebnisse

Beim Klonvorgang werden alle anderen Attribute und Einstellungen kopiert, um die neue Datenquelle zu erstellen.

#### Testen der Datenquellkonfiguration

Wenn Sie eine Datenquelle hinzufügen, können Sie die Richtigkeit der Konfiguration für die Kommunikation mit dem Gerät überprüfen, bevor Sie diese Datenquelle speichern oder aktualisieren.

Wenn Sie im Datenquellassistenten auf die Schaltfläche **Test** klicken, wird die Kommunikation mit dem angegebenen Gerät überprüft. Der Test liefert eines der folgenden Ergebnisse:

- BESTANDEN: Die Datenquelle ist korrekt konfiguriert.
- WARNUNG: Die Tests waren unvollständig, wahrscheinlich aufgrund einer Zeitüberschreitung bei der Verarbeitung oder nicht laufender Akquisition.
- FEHLGESCHLAGEN: Die Datenquelle kann nicht wie konfiguriert mit dem angegebenen Gerät kommunizieren. Überprüfen Sie die Konfigurationseinstellungen und führen Sie einen erneuten Test durch.

## Herstellerspezifische Datenquelle

Die Konfigurationsdetails variieren je nach Hersteller und Modell der hinzuzufügenden Datenquelle.

Wenn die Datenquelle eines Anbieters erweiterte Insight-Konfigurationsanweisungen, z. B. spezielle Anforderungen und bestimmte Befehle, erfordert, finden Sie diese Informationen in diesem Abschnitt.

#### 3PAR InServ Datenquelle

OnCommand Insight verwendet die Datenquelle „3PAR InServ“ (Firmware 2.2.2+, SSH), um den Bestand für HP 3PAR StoreServ-Speicher-Arrays zu ermitteln.

##### Terminologie

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der Datenquelle „3PAR InServ“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Physisches Laufwerk | Festplatte |
| Storage-System | Storage |
| Controller-Node | Storage-Node |
| Gemeinsame Bereitstellungsgruppe | Storage-Pool |
| Virtual Volume | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- IP-Adresse oder FQDN des InServ-Clusters
- Für die Bestandsaufnahme, schreibgeschützter Benutzername und Kennwort an den InServ-Server.
- Für die Leistung, Lese-Schreib-Benutzername und Passwort an den InServ-Server.
- Port-Anforderungen: 22 (Inventory Collection), 5988 oder 5989 (Performance Collection) [Hinweis: 3PAR Performance wird für InServ OS 3.x+ unterstützt]
- Bestätigen Sie zur Performance-Erfassung, dass SMI-S aktiviert ist, indem Sie sich über SSH beim 3PAR-Array anmelden.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Cluster-IP | IP-Adresse oder vollständig qualifizierter Domänenname des InServ-Clusters |
| Benutzername | Benutzername für den InServ-Server |
| Passwort | Kennwort für den InServ-Server |
| SMI-S-HOST-IP | IP-Adresse des SMI-S Provider-Hosts |
| SMI-S-Benutzername | Benutzername für den SMI-S Provider Host |
| SMI-S-Passwort | Passwort, das für den SMI-S Provider-Host verwendet wird |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Geräte Ausschließen | Kommagetrennte Liste der auszuschließenden Geräte-IPs |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 60 Sekunden) |
| Anzahl der SSH-Wiederholungen | Anzahl der SSH-Wiederholungsversuche |
| SSH-Banner-Wartezeit (Sek.) | SSH Banner Wait Timeout (Standard: 20 Sekunden) |
| SMI-S-Port | Vom SMI-S Provider-Host verwendeter Port |
| Protokoll | Protokoll für die Verbindung mit dem SMI-S-Provider |

| | |
|---|---|
| SMI-S Namespace | SMI-S Namespace |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Anzahl der erneuten SMI-S-Verbindungsversuche | Anzahl der Wiederholungsversuche für SMI-S-Verbindungen |

**Amazon AWS EC2 Datenquelle**

OnCommand Insight verwendet diese Datenquelle, um Inventar und Performance für Amazon AWS EC2 zu erkennen.

**Voraussetzungen:**

Um Daten von Amazon EC2 Geräten zu erfassen, müssen Sie folgende Informationen haben:

- Sie müssen über die ID des IAM-Zugriffsschlüssels verfügen
- Sie müssen über den geheimen Zugriffsschlüssel für Ihr Amazon EC2 Cloud-Konto verfügen
- Sie müssen über die Berechtigung „Listenorganisation“ verfügen
- Port 433 HTTPS
- EC2-Instanzen können als Virtual Machine oder (weniger natürlich) als Host gemeldet werden. EBS Volumes können sowohl von der VM als virtualisierte Festplatte genutzt werden als auch als Datenspeicher, die die Kapazität der virtuellen Festplatte bereitstellen.

Zugriffsschlüssel bestehen aus einer Zugriffsschlüssel-ID (z. B. AKIAIOSFODN7EXAMPLE) und einem geheimen Zugriffsschlüssel (z. B. wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Sie verwenden Zugriffsschlüssel, um programmatische Anfragen zu signieren, die Sie an EC@ stellen, wenn Sie die Amanzon EC2-SDKs, REST- oder Abfrage-API-Operationen verwenden. Diese Schlüssel werden mit Ihrem Vertrag von Amazon zur Verfügung gestellt.

**So konfigurieren Sie diese Datenquelle**

Zum Konfigurieren der Amazon AWS EC2 Datenquelle benötigen Sie die AWS IAM Access Key ID und den Secret Access Key für Ihr AWS Konto.

Füllen Sie die Datenquellenfelder gemäß den folgenden Tabellen aus:

**Konfiguration:**

| Feld | Beschreibung |
|---|---|
| AWS Region | Wählen Sie die Region AWS |
| IAM-Rolle | Nur zur Verwendung bei Übernahme auf einer AU in AWS. Im Folgenden finden Sie weitere Informationen zu IAM-Rollen. |

| | |
|---|---|
| AWS IAM Access Key-ID | Geben Sie die AWS IAM-Zugriffsschlüssel-ID ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden. |
| AWS IAM Secret Access Key | Geben Sie den AWS IAM-Schlüssel für den geheimen Zugriff ein. Erforderlich, wenn Sie die IAM-Rolle nicht verwenden. |
| Ich verstehe, dass AWS mir API-Anfragen in Rechnung stellt | Überprüfen Sie dies, um zu überprüfen, ob AWS Ihnen bei API-Anfragen, die durch Insight Polling gestellt werden, Rechnungen stellt |

**Erweiterte Konfiguration:**

| Feld | Beschreibung |
|---|---|
| Zusätzliche Regionen Einschließen | Geben Sie zusätzliche Bereiche an, die in die Abfrage einbezogen werden sollen. |
| Accountübergreifende Rolle | Rolle für den Zugriff auf Ressourcen in unterschiedlichen AWS Konten. |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| HTTP-Verbindung und Socket-Timeout (s) | HTTP-Verbindungs-Timeout (Standard: 300 Sekunden) |
| AWS-Tags einschließen | Aktivieren Sie diese Option, um die Unterstützung für AWS-Tags in Insight Annotationen zu aktivieren |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abfragen (Standard: 1800 Sekunden) |

**Zuordnen von AWS Tags zu Insight Annotationen**

Die AWS EC2 Datenquelle enthält eine Option, mit der Sie Insight Annotationen mit auf AWS konfigurierten Tags füllen können. Die Annotationen müssen genau wie die AWS Tags benannt werden. Insight wird immer Anmerkungen vom gleichen Namen in Textart einfügen und einen „besten Versuch“ machen, Anmerkungen anderer Typen (Zahl, Boolesch usw.) zu füllen. Wenn Ihre Anmerkung einen anderen Typ hat und die Datenquelle sie nicht ausfüllen kann, muss die Anmerkung möglicherweise entfernt und als Textart neu erstellt werden.

Bei AWS muss die Groß-/Kleinschreibung nicht beachtet werden. Bei Insight muss die Groß-/Kleinschreibung nicht beachtet werden. Wenn Sie also in Insight eine Annotation mit dem Namen „`OWNER`“ und Tags mit den Namen „`OWNER`“, „`owner`“ und „`owner`“ erstellen, werden alle AWS-Variationen von „`owner`“ der Annotation „`OWNER`“ von Insight zugeordnet.

Verwandte Informationen:

"Verwalten von Zugriffsschlüsseln für IAM-Benutzer"

#### Zusätzliche Regionen Einschließen

Im Abschnitt AWS Data Collector **Erweiterte Konfiguration** können Sie das Feld * zusätzliche Regionen* so einstellen, dass zusätzliche durch Komma oder Semikolon getrennte Bereiche einbezogen werden. Standardmäßig ist dieses Feld auf ***US-.**** gesetzt, das auf allen US AWS Regionen sammelt. Um in *all* Regionen zu sammeln, setzen Sie dieses Feld auf ***.**.

Ist das Feld **zusätzliche Regionen** leer, sammelt der Datensammler die im Feld **AWS Region** angegebenen Werte, wie im Abschnitt **Konfiguration** angegeben.

#### Sammeln von AWS Child Accounts

Insight unterstützt die Erfassung von untergeordneten Konten für AWS innerhalb eines einzigen AWS-Datensammlers. Die Konfiguration dieser Sammlung erfolgt in der AWS-Umgebung:

- Sie müssen jedes untergeordnete Konto so konfigurieren, dass es über eine AWS-Rolle verfügt, die es der primären Konto-ID ermöglicht, über das untergeordnete Konto auf EC2-Details zuzugreifen.
- Für jedes untergeordnete Konto muss der Rollenname als dieselbe Zeichenfolge konfiguriert sein
- Geben Sie diese Zeichenfolge für den Rollennamen im Abschnitt Insight AWS Data Collector **Advanced Configuration** im Feld **Cross Account role** ein.

Best Practice: Es wird dringend empfohlen, die AWS vordefinierte AmazonEC2ReadOnly Access Policy dem ECS-Hauptkonto zuzuweisen. Außerdem sollte dem in der Datenquelle konfigurierten Benutzer mindestens die vordefinierte *AWSOrganisationenReadOnlyAccess*Policy zugewiesen sein, um AWS abzufragen.

Im Folgenden finden Sie Informationen zur Konfiguration Ihrer Umgebung, damit Insight von untergeordneten AWS-Konten erfasst werden kann:

"Tutorial: Delegieren des Zugriffs über AWS Konten mithilfe von IAM-Rollen"

"AWS Setup: Zugriff auf einen IAM-Benutzer in einem anderen AWS-Konto bereitstellen, das Sie besitzen"

"Erstellen einer Rolle zum Delegieren von Berechtigungen an einen IAM-Benutzer"

#### IAM-Rollen

Wenn Sie *IAM Role* Security verwenden, müssen Sie sicherstellen, dass die von Ihnen erstellte oder angegebene Rolle über die entsprechenden Berechtigungen verfügt, die für den Zugriff auf Ihre Ressourcen erforderlich sind.

Wenn Sie beispielsweise eine IAM-Rolle mit dem Namen *InstanceEc2ReadOnly* erstellen, müssen Sie die Richtlinie einrichten, um allen EC2-Ressourcen für diese IAM-Rolle schreibgeschützten Zugriff auf EC2-Listen zu gewähren. Außerdem müssen Sie STS (Security Token Service)-Zugriff gewähren, damit diese Rolle Rollenübergreifende Konten übernehmen kann.

Nachdem Sie eine IAM-Rolle erstellt haben, können Sie sie beim Erstellen einer neuen EC2-Instanz oder einer vorhandenen EC2-Instanz anhängen.

Nachdem Sie die IAM-Rolle *InstanceEc2ReadOnly* an eine EC2-Instanz angehängt haben, können Sie die temporären Anmeldedaten über die Metadaten der Instanz per IAM-Rollennamen abrufen und verwenden, um von jeder auf dieser EC2-Instanz ausgeführten Anwendung auf AWS-Ressourcen zuzugreifen.

Die IAM-Rolle kann nur verwendet werden, wenn die Acquisition Unit in einer AWS-Instanz ausgeführt wird.

### Datenquelle von Brocade Enterprise Fabric Connectivity Manager

OnCommand Insight verwendet die Datenquelle „Brocade Enterprise Fabric Connectivity Manager“ (EFCM) zur Bestandsaufnahme von Brocade EFCM-Switches. Insight unterstützt EFCM Versionen 9.5, 9.6 und 9.7.

#### Anforderungen

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht verfügbar.

- Netzwerkadresse oder vollqualifizierter Domänenname für den EFCM-Server
- EFCM-Version muss 9.5, 9.6 oder 9.7 sein
- IP-Adresse des EFCM-Servers
- Schreibgeschützter Benutzername und Kennwort für den EFCM-Server
- Validierter Zugriff auf den Connectrix-Switch über Telnet vom Insight-Server unter Verwendung des schreibgeschützten Benutzernamens und des Kennworts über Port 51512

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| EFC-Server | IP-Adresse oder vollqualifizierter Domänenname des EFC-Servers |
| Benutzername | Benutzername für den Switch |
| Passwort | Passwort für den Switch |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 15 Minuten) |
| Fabric-Name | Fabric-Name, der von der EFCM-Datenquelle gemeldet werden soll. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden. |
| Kommunikations-Port | Port, der für die Kommunikation mit dem Switch verwendet wird |

| | |
|---|---|
| Trapping Aktivieren | Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren. |
| Mindestzeit zwischen Traps (s) | Mindestzeit zwischen den von Traps ausgelösten Erfassungsversuchen (Standard: 15 Sekunden) |
| Inaktive Zoneets | Kommagetrennte Liste inaktiver Zonesets, auf denen die Erfassung durchgeführt werden soll, sowie die Erfassung für die aktiven Zonensätze |
| Zu verwendende NIC | Geben Sie an, welche Netzwerkschnittstelle auf der RAU verwendet werden soll, wenn Sie über SAN-Geräte berichten |
| Geräte Ausschließen | Kommagetrennte Liste von Einheitennamen, die ein- oder ausgeschlossen werden sollen |
| Verwenden Sie den Spitznamen des EFCM-Switches als Namen des Insight-Switches | Wählen Sie diese Option, um den Spitznamen des EFCM-Switches als Namen des Insight-Switches zu verwenden |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

**Datenquelle des Brocade FC Switch**

OnCommand Insight verwendet die Brocade FC Switch (SSH)-Datenquelle zur Erkennung des Inventars für Brocade- oder umbenannte Switch-Geräte, auf denen FOS-Firmware (Factsored Operating System) 4.2 und höher ausgeführt wird. Geräte werden sowohl im FC-Switch- als auch im Access Gateway-Modus unterstützt.

**Terminologie**

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der Datenquelle „Brocade FC Switch“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Switch | Switch |
| Port | Port |
| Virtual Fabric, Physische Fabric | Fabric |
| Zone | Zone |

| | |
|---|---|
| Logischer Switch | Logischer Switch |
| LSAN-Zone zu erreichen | IVR-Zone |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- Die Acquisition Unit (lokal oder Remote) initiiert Verbindungen zu TCP-Port 22 auf Brocade-Switches, um Bestandsdaten zu sammeln. Die AU wird auch Verbindungen zu UDP Port 161 für die Sammlung von Leistungsdaten initiieren.
- Für alle Switches in der Fabric muss eine IP-Konnektivität vorhanden sein. Wenn Sie das Kontrollkästchen Alle Switches in der Fabric ermitteln aktivieren, identifiziert OCI alle Switches in der Fabric. Zur Erkennung ist jedoch eine IP-Verbindung zu diesen zusätzlichen Switches erforderlich.
- Weltweit ist dasselbe Konto über alle Switches in der Fabric erforderlich. Sie können PuTTY (Open Source Terminal Emulator) verwenden, um den Zugriff zu bestätigen.
- Wenn die Lizenz „Ausführen“ installiert ist, müssen die Ports 161 und 162 für alle Switches in der Fabric offen sein, um die SNMP-Performance-Abfrage durchführen zu können.
- SNMP Read-Only Community String

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Switch-IP | IP-Adresse oder vollqualifizierter Domain-Name des Switches |
| Benutzername | Benutzername für den Switch |
| Passwort | Passwort für den Switch |
| SNMP-Version | SNMP-Version |
| SNMP-Community-Zeichenfolge | SNMP read-only Community String verwendet, um auf den Switch zugreifen |
| SNMP-Benutzername | Benutzername des SNMP-Versionsprotokolls (gilt nur für SNMP v3) |
| SNMP-Kennwort | SNMP-Versionsprotokoll-Kennwort (gilt nur für SNMP v3) |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| Fabric-Name | Fabric-Name, der von der Datenquelle gemeldet werden soll. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden. |
| Geräte Ausschließen | Kommagetrennte Liste der Geräte-IDs, die von der Abfrage ausgeschlossen werden sollen |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 15 Minuten) |
| Zeitüberschreitung (Sek.) | Verbindungs-Timeout (Standard: 30 Sekunden) |
| Zeitüberschreitung bei der Bannerwartezeit (Sek.) | SSH Banner Wait Timeout (Standard: 5 Sekunden) |
| Admin-Domänen Aktiv | Wählen Sie, wenn Sie Admin-Domains verwenden |
| MPR-Daten abrufen | Auswählen, um Routingdaten von Ihrem Multiprotocol-Router (MPR) zu erfassen |
| Trapping Aktivieren | Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren. |
| Mindestzeit zwischen Traps (s) | Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden) |
| Erkennung aller Switches in der Fabric | Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen |
| Entscheiden Sie sich für HBA vs Zonenaliase | Wählen Sie, ob HBA- oder Zonenaliasen bevorzugt werden sollen |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| SNMP-Auth-Protokoll | SNMP-Authentifizierungsprotokoll (nur SNMP v3) |
| SNMP-Datenschutzprotokoll | SNMP-Datenschutzprotokoll (nur SNMP v3) |
| SNMP-Datenschutzkennwort | SNMP-Datenschutzkennwort (nur SNMP v3) |
| SNMP wird erneut verwendet | Anzahl der SNMP-Wiederholungsversuche |
| SNMP-Timeout (ms) | SNMP-Timeout (Standard 5000 ms) |

### Datenquelle von Brocade Sphereon/Intrepid Switch

OnCommand Insight verwendet die Brocade Sphereon/Intrepid Switch (SNMP) Datenquelle zur Bestandsaufnahme von Brocade Sphereon oder Intrepid Switches.

#### Anforderungen

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht verfügbar.

- Für alle Switches in der Fabric muss eine IP-Konnektivität vorhanden sein. Wenn Sie das Kontrollkästchen Alle Switches in der Fabric ermitteln aktivieren, identifiziert OCI alle Switches in der Fabric. Zur Erkennung ist jedoch eine IP-Verbindung zu diesen zusätzlichen Switches erforderlich.
- Schreibgeschützte Community-Zeichenfolge bei Verwendung von SNMP V1 oder SNMP V2
- HTTP-Zugriff auf den Switch, um Zoning-Informationen zu erhalten.
- Greifen Sie auf die Validierung zu, indem Sie den ausführen `snmpwalk` Dienstprogramm zum Schalter (siehe `<install_path\>\bin\)`.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Sphereon Switch | IP-Adresse oder vollqualifizierter Domain-Name des Switches |
| SNMP-Version | SNMP-Version |
| SNMP-Community | SNMP read-only Community String verwendet, um auf den Switch zugreifen |
| Benutzername | SMI-S-Benutzername für den Switch (nur SNMP v3) |
| Passwort | SMI-S-Kennwort für den Switch (nur SNMP v3) |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 15 Minuten) |
| SNMP-Auth-Protokoll | SNMP-Authentifizierungsprotokoll (nur SNMPv3) |
| SNMP-Datenschutzprotokoll | SNMP-Datenschutzprotokoll (nur SNMPv3) |
| SNMP-Datenschutzkennwort | SNMP-Datenschutzkennwort |
| SNMP-Anzahl der Wiederholungen | Anzahl der SNMP-Wiederholungsversuche |

| | |
|---|---|
| SNMP-Timeout (ms) | SNMP-Timeout (Standard 5000 ms) |
| Fabric-Name | Fabric-Name, der von der Datenquelle gemeldet werden soll. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden. |
| Trapping Aktivieren | Wählen Sie diese Option aus, um die Erfassung beim Empfang eines SNMP-Trap vom Gerät zu aktivieren. Wenn Sie Trapping aktivieren auswählen, müssen Sie auch SNMP aktivieren. |
| Mindestzeit zwischen Ttraps (Sekunden) | Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

**Cisco FC Switch Firmware (SNMP) Datenquelle**

OnCommand Insight verwendet die Datenquelle „Cisco FC Switch Firmware 2.0+“ (SNMP) zur Bestandsaufnahme von Cisco MDS Fibre Channel Switches sowie einer Vielzahl von Cisco Nexus FCoE Switches, auf denen der FC-Service aktiviert ist. Darüber hinaus können Sie mit dieser Datenquelle viele Modelle von Cisco-Geräten im NPV-Modus entdecken.

**Terminologie**

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der Datenquelle „Cisco FC Switch“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Switch | Switch |
| Port | Port |
| VSAN | Fabric |
| Zone | Zone |
| Logischer Switch | Logischer Switch |
| Name Server-Eintrag | Name Server-Eintrag |
| Inter-VSAN Routing-Zone (IVR | IVR-Zone |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- Eine IP-Adresse eines Switches in der Fabric oder den einzelnen Switches
- Chassis-Erkennung für die Fabric-Erkennung
- Bei Verwendung von SNMP V2, nur lesbare Community-String
- Port 161 wird für den Zugriff auf das Gerät verwendet
- Zugriffsvalidierung mit `snmpwalk` Dienstprogramm zum Schalter (siehe `<install_path\>\bin\`)

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Cisco Switch IP | IP-Adresse oder vollqualifizierter Domain-Name des Switches |
| SNMP-Version | Für die Leistungserfassung ist SNMP Version v2 oder höher erforderlich |
| SNMP-Community-Zeichenfolge | SNMP Read-Only-Community-String zum Zugriff auf den Switch (gilt nicht für SNMP v3) |
| Benutzername | Benutzername für den Switch (nur SNMP v3) |
| Passwort | Passwort für den Switch (nur SNMPv3) |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| SNMP-Auth-Protokoll | SNMP-Authentifizierungsprotokoll (nur SNMPv3) |
| SNMP-Datenschutzprotokoll | SNMP-Datenschutzprotokoll (nur SNMPv3) |
| SNMP-Datenschutzkennwort | SNMP-Datenschutzkennwort |
| SNMP wird erneut verwendet | Anzahl der SNMP-Wiederholungsversuche |
| SNMP-Timeout (ms) | SNMP-Timeout (Standard 5000 ms) |

| | |
|---|---|
| Trapping Aktivieren | Wählen Sie, um das Überfüllen zu aktivieren. Wenn Sie Trapping aktivieren, müssen Sie auch SNMP-Benachrichtigungen aktivieren. |
| Mindestzeit zwischen Traps (s) | Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden) |
| Alle Fabric Switches Erkennen | Wählen Sie diese Option, um alle Switches in der Fabric zu erkennen |
| Geräte Ausschließen | Kommagetrennte Liste der Geräte-IP-Adressen, die von der Abfrage ausgeschlossen werden sollen |
| Geräte Einschließen | Kommagetrennte Liste der Geräte-IPs, die in Abfrage aufgenommen werden sollen |
| Überprüfen Sie Den Gerätetyp | Wählen Sie diese Option aus, um nur die Geräte zu akzeptieren, die sich explizit als Cisco-Geräte bewerben |

| | |
|---|---|
| Primärer Alias-Typ | Geben Sie eine erste Präferenz für die Auflösung des Alias an. Wählen Sie eine der folgenden Optionen:<br>• **Geräte-Alias**<br>Dies ist ein benutzerfreundlicher Name für einen Port-WWN (PWWN), der bei Bedarf in allen Konfigurationsbefehlen verwendet werden kann. Alle Switches der Produktfamilie Cisco MDS 9000 unterstützen Distributed Device Alias Services (Geräte-Aliase).<br>• **Keine**<br>Melden Sie keinen Alias<br>• **Port-Beschreibung**<br>Eine Beschreibung zur Identifizierung des Ports in einer Liste von Ports<br>• **Zone Alias (alle)**<br>Ein benutzerfreundlicher Name für einen Port, der nur für die Zonenkonfiguration verwendet werden kann<br>• **Zone Alias (nur aktiv)**<br>Ein benutzerfreundlicher Name für einen Port, der nur für die aktive Konfiguration verwendet werden kann. Dies ist die Standardeinstellung. |
| Sekundärer Alias-Typ | Geben Sie eine zweite Vorliebe für die Auflösung des Alias an |
| Tertiärer Alias-Typ | Geben Sie eine dritte Präferenz für die Auflösung des Alias an |
| Aktivieren Sie die Unterstützung für den SANTAP-Proxy-Modus | Wählen Sie aus, ob Ihr Cisco Switch SANTAP im Proxy-Modus verwendet. Wenn Sie EMC RecoverPoint verwenden, verwenden Sie wahrscheinlich SANTAP. |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### EMC Celerra Datenquelle

Die Celerra (SSH)-Datenquelle erfasst Bestandsdaten vom Celerra-Speicher. Für die Konfiguration erfordert diese Datenquelle die IP-Adresse der Speicherprozessoren und

einen *Read-Only* Benutzernamen und ein Passwort.

**Terminologie**

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC Celerra-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Celerra Network Server | Storage |
| Celerra Meta Volume/Celerra Storage Pool | Storage-Pool |
| File-System | Internes Volumen |
| Data Mover | Controller |
| Dateisystem, das auf einem Data Mover gemountet ist | Dateifreigabe |
| CIFS- und NFS-Exporte | Share |
| Festplatten-Volume | Back-End LUN |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- Die IP-Adresse des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- SSH-Port 22

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Adresse der Celerra | IP-Adresse oder vollständig qualifizierter Domänenname des Celerra-Geräts |
| Benutzername | Name, der für die Anmeldung beim Celerra-Gerät verwendet wird |
| Passwort | Passwort für die Anmeldung beim Celerra-Gerät |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (Minuten) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 600 Sekunden) |
| Anzahl Wiederholungen | Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme |
| SSH-Banner-Wartezeit (Sek.) | SSH Banner Wait Timeout (Standard: 20 Sekunden) |

### EMC CLARiiON (NaviCLI)-Datenquelle

Stellen Sie vor der Konfiguration dieser Datenquelle sicher, dass die EMC Navisphere CLI auf dem Zielgerät und auf dem Insight-Server installiert ist. Die Navisphere CLI-Version muss mit der Firmware-Version auf dem Controller übereinstimmen. Für die Erfassung von Performancedaten muss die Statistikprotokollierung aktiviert sein.

#### Navisphere Command Line Interface-Syntax

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC CLARiiON-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte | Festplatte |
| Storage | Storage |
| Storage Processor | Storage-Node |
| Thin Pool, RAID-Gruppe | Storage-Pool |
| LUN | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- Eine IP-Adresse für jeden CLARiiON-Speicherprozessor
- Navisphere-Benutzername und -Kennwort für die CLARiiON-Arrays, schreibgeschützt
- Navicli muss auf dem Insight Server/rau installiert sein
- Zugriffsvalidierung: Führen Sie NaviCLI vom Insight-Server zu jedem Array mit dem oben genannten Benutzernamen und Passwort aus.
- Die navicli-Version sollte mit dem neuesten FLARE-Code auf Ihrem Array übereinstimmen
- Für die Performance muss die Statistikprotokollierung aktiviert sein.
- Port-Anforderungen: 80, 443

**Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| CLARiiON-Speicher | IP-Adresse oder vollständig qualifizierter Domänenname des CLARiiON-Speichers |
| Benutzername | Name, der für die Anmeldung beim CLARiiON-Speichergerät verwendet wird. |
| Passwort | Kennwort für die Anmeldung beim CLARiiON-Speichergerät. |
| CLI Pfad zu Pfad navicli.exe oder Pfad NaviSECCLI.exe | Vollständiger Pfad zum `navicli.exe` ODER `naviseccli.exe` Ausführbar |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Secure Client verwenden (naviseccli) | Auswählen, um sicheren Client zu verwenden (navseccli) |
| Umfang | Der Umfang des sicheren Clients. Die Standardeinstellung ist Global. |
| CLARiiON-CLI-Port | Für CLARiiON CLI verwendeter Port |
| Zeitlimit für externen Prozess für Bestandsaufnahme (Sek.) | Externes Prozess-Timeout (Standard: 1800 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

| | |
|---|---|
| Performance Externes Prozesszeitlimit (s) | Externes Prozess-Timeout (Standard: 1800 Sekunden) |

### EMC Data Domain Datenquelle

Diese Datenquelle erfasst Speicher- und Konfigurationsinformationen von EMC Data Domain Deduplizierungssystemen. Um die Datenquelle hinzuzufügen, müssen Sie spezifische Konfigurationsanweisungen und -Befehle verwenden und die Anforderungen an die Datenquelle sowie Empfehlungen zur Verwendung kennen.

#### Terminologie

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der EMC Data Domain-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte | Festplatte |
| Array Erledigen | Storage |
| Port | Port |
| Dateiys | Internes Volumen |
| Mtree | Qtree |
| Kontingente | Kontingente |
| NFS- und CIFS-Freigabe | Dateifreigabe |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- IP-Adresse des Data Domain-Geräts
- Schreibgeschützter Benutzername und Kennwort für den Data Domain-Speicher
- SSH-Port 22

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| IP-Adresse | Die IP-Adresse oder der vollqualifizierte Domänenname des Data Domain-Speicherarrays |

| | |
|---|---|
| Benutzername | Der Benutzername für das Data Domain-Speicherarray |
| Passwort | Das Kennwort für das Data Domain-Speicherarray |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 180 Sekunden) |
| SSH-Port | SSH-Service-Port |

### EMC ECC StorageScope Datenquelle

Das EMC ECC StorageScope-Gerät verfügt über drei Arten von Datenquellen: 5.x, 6.0 und 6.1.

**Konfiguration**

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht mehr verfügbar.

| Feld | Beschreibung |
|---|---|
| ECC-Server | IP-Adresse oder vollständig qualifizierter Domänenname des ECC-Servers |
| Benutzername | Benutzername für den ECC-Server |
| Passwort | Passwort des ECC-Servers |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| ECC-Port | Für den ECC-Server verwendeter Port |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 30 Minuten) |
| Protokoll zur Verbindung mit Datenbank | Protokoll für die Verbindung mit der Datenbank |

| | |
|---|---|
| Dateisysteminformationen Abfragen | Wählen Sie diese Option aus, um Details für WWN-Aliase und Dateisysteme abzurufen. |

### Dell EMC ECS-Datenquelle

Dieser Datensammler erfasst Bestands- und Performancedaten von EMC ECS Speichersystemen. Für die Konfiguration benötigt der Data Collector eine IP-Adresse des ECS-Servers und ein Administrator-Level-Domänenkonto.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC ECS-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Cluser | Storage |
| Mandant | Storage-Pool |
| Eimer | Internes Volumen |
| Festplatte | Festplatte |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Eine IP-Adresse der ECS Management Console
- Domain-Konto auf Administratorebene für das ECS-System
- Port 443 (HTTPS): Erfordert eine ausgehende Verbindung zum TCP-Port 443 des ECS-Systems.
- Für die Leistung können Sie den schreibgeschützten Benutzernamen und das Kennwort für den ssh/scp-Zugriff verwenden.
- Für die Leistung ist Port 22 erforderlich.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| ECS Host | IP-Adressen oder vollständig qualifizierte Domänennamen des ECS-Systems |
| ECS-Host-Port | Port, der für die Kommunikation mit ECS Host verwendet wird |

| | |
|---|---|
| ECS Anbieter-ID | Anbieter-ID für ECS |
| Passwort | Passwort wird für ECS verwendet |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (Minuten) | Intervall zwischen Bestandsabstimmungen Der Standardwert ist 360 Minuten. |

### EMC Isilon Datenquelle

Die Isilon SSH-Datenquelle erfasst Inventar und Performance aus EMC Isilon Scale-out-NAS-Speicher.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC Isilon-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Laufwerk | Festplatte |
| Cluster | Storage |
| Knoten | Storage-Node |
| File-System | Internes Volumen |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Administratorberechtigungen für den Isilon-Speicher
- Validierter Zugriff durch `telnet` Zu Port 22

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| IP-Adresse | Die IP-Adresse oder der vollständig qualifizierte Domänenname des Isilon-Clusters |

| | |
|---|---|
| Benutzername | Der Benutzername für das Isilon-Cluster |
| Passwort | Das Passwort für den Isilon-Cluster |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Zeitüberschreitung für SSH-Prozess | SSH-Prozess-Timeout (Standard: 60 Sekunden) |
| SSH-Port | SSH-Service-Port |

**Ausführen von CLI-Befehlen**

Ab OnCommand Insight Version 7.3.11 und Service Pack 9 enthält die Datenquelle von EMC Isilon eine Erweiterung, die dazu führt, dass Insight mehr CLI-Befehle ausführt. Wenn Sie einen nicht-Root-Benutzer in Ihrer Datenquelle verwenden, haben Sie wahrscheinlich eine „sudoers“-Datei konfiguriert, um diesem Benutzerkonto die Möglichkeit zu geben, bestimmte CLI-Befehle über SSH auszuführen.

Damit Insight die Funktion „Access Zones“ von EMC verstehen kann, führt Insight nun zusätzlich die folgenden neuen CLI-Befehle aus:

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insight analysiert die Ausgabe dieser Befehle und führt mehrere Instanzen vorhandener Befehle aus, um die logische Konfiguration von Objekten wie qtrees, Quotas und NAS-Freigaben/-Exporten zu erhalten, die sich in nicht standardmäßigen Access Zones befinden. Insight meldet diese Objekte nun als Ergebnis dieser Verbesserung für nicht standardmäßige Zugriffszonen. Da Insight diese Daten durch Ausführen vorhandener Befehle (mit unterschiedlichen Optionen) erhält, ist keine Änderung der sudoers-Datei erforderlich, damit diese funktionieren; nur mit der Einführung der neuen Befehle oben ist die Änderung erforderlich.

Aktualisieren Sie Ihre sudoers-Datei, damit Ihr Insight-Servicekonto diese Befehle ausführen kann, bevor Sie ein Upgrade auf diese Insight-Version durchführen. Wenn Sie dies nicht tun, kann es zu einem Ausfall Ihrer Isilon-Datenquellen kommen.

**Statistik „Dateisystem“**

Ab OnCommand Insight 7.3.12 führt der EMC Isilon Data Collector Statistiken zum „Dateisystem“ für das Node-Objekt für EMC Isilon ein. Die von OnCommand Insight gemeldeten bestehenden Node-Statistiken basieren auf „Festplatten“ – d. h. für IOPS und Durchsatz eines Storage-Nodes, welche Vorgänge machen die Festplatten in diesem Node aggregiert? Bei Workloads, bei denen Lesezugriffe im Speicher zwischengespeichert und/oder Komprimierung verwendet werden, kann der Filesystem-Workload erheblich höher sein als die tatsächlichen Treffer auf den Festplatten – ein Datensatz, der 5:1 komprimiert, könnte daher

einen „Filesystem-Lesedurchsatz“ Wert haben den 5-fachen des Storage-Node-Lesedurchsatzes. Bei Letzterem werden die Lesevorgänge von der Festplatte gemessen. Diese werden um das 5-Fache erweitert, wenn der Node die Daten entkomprimiert, um die Leseanforderung des Kunden zu bedienen.

### Dell EMC PowerStore Datenquelle

Der Dell EMC PowerStore-Datensammler sammelt Bestandsinformationen aus dem Dell EMC PowerStore-Speicher. Zur Konfiguration benötigt der Datensammler die IP-Adresse der Speicherprozessoren sowie einen schreibgeschützten Benutzernamen und ein Kennwort.

#### Terminologie

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der EMC Data Domain-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Host | Host |
| Host_Volume_Zuordnung | Host_Volume_Zuordnung |
| Hardware (es hat Laufwerke unter „extra_Details“-Objekt): Laufwerke | Festplatte |
| Appliance | Storage Pool |
| Cluster | Storage Array Durchführt |
| Knoten | StorageNode |
| fc_Port | Port |
| Datenmenge | Datenmenge |
| InternalVolume | File_System |
| Dateiys | Internes Volumen |
| Mtree | Qtree |
| Kontingente | Kontingente |
| NFS- und CIFS-Freigabe | Dateifreigabe |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort

#### Erläuterung der übergeordneten Seriennummer

Traditionell ist Insight in der Lage, die Seriennummer des Storage-Arrays oder die Seriennummern der einzelnen Storage-Nodes zu melden. Einige Storage-Array-Architekturen lassen sich diesem jedoch nicht ordnungsgemäß anpassen. Ein PowerStore Cluster kann aus 1-4 Appliances bestehen, und jede Appliance verfügt über 2 Nodes. Wenn die Appliance selbst über eine Seriennummer verfügt, ist diese Seriennummer weder die Seriennummer für das Cluster noch für die Nodes.

Das Attribut „Parent Serial Number“ auf dem Speicher-Node-Objekt wird für Dell/EMC PowerStore-Arrays entsprechend aufgefüllt, wenn sich die einzelnen Nodes in einer Zwischenanwendung/einem Gehäuse befinden, die nur Teil eines größeren Clusters ist.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| PowerStore Gateway(s) | IP-Adressen oder vollqualifizierte Domain-Namen des PowerStore-Speichers |
| Benutzername | Benutzername für PowerStore |
| Passwort | Passwort, das für PowerStore verwendet wird |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| HTTPS-Port | Der Standardwert ist 443 |
| Abfrageintervall für Bestand (Minuten) | Intervall zwischen Bestandsabstimmungen Der Standardwert ist 60 Minuten. |

Die PowerStore Performance-Sammlung von OnCommand Insight nutzt die 5-Minuten-Detailgenauigkeit der Quelldaten von PowerStore. Daher fragt Insight diese Daten alle fünf Minuten ab, und dies ist nicht konfigurierbar.

### EMC RecoverPoint-Datenquelle

Die EMC RecoverPoint-Datenquelle erfasst Bestandsdaten aus EMC RecoverPoint-Speicher. Für die Konfiguration benötigt die Datenquelle die IP-Adresse der Speicherprozessoren und einen *Read-Only* Benutzernamen und ein Passwort.

Die EMC RecoverPoint-Datenquelle erfasst die Replikationsbeziehungen zwischen Volumes, die RecoverPoint über andere Speicher-Arrays hinweg koordiniert. OnCommand Insight zeigt ein Speicher-Array für jeden RecoverPoint-Cluster an und sammelt Bestandsdaten für Knoten und Speicherports auf diesem Cluster. Es werden keine Storage-Pool- oder Volume-Daten erfasst.

#### Anforderungen

- IP-Adresse oder vollqualifizierter Domain-Name des Speicherprozessors
- Schreibgeschützter Benutzername und Kennwort
- REST-API-Zugriff über Port 443
- SSH-Zugriff über PuTTY

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Adresse von RecoverPoint | IP-Adresse oder vollqualifizierter Domain-Name des RecoverPoint-Clusters |
| Benutzername | Benutzername für das RecoverPoint-Cluster |
| Passwort | Kennwort für den RecoverPoint-Cluster |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| TCP-Port | TCP-Port für die Verbindung mit dem RecoverPoint-Cluster |
| Abfrageintervall für Bestand (Minuten) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Ausgeschlossene Cluster | Kommagetrennte Liste von Cluster-IDs oder Namen, die beim Abfragen ausgeschlossen werden sollen |

### EMC Solutions Enabler mit SMI-S Performance-Datenquelle

OnCommand Insight erkennt Symmetrix-Speicher-Arrays mithilfe von Solutions Enabler `symcli` Befehle in Verbindung mit einem vorhandenen Solutions Enabler-Server in Ihrer Umgebung. Der vorhandene Solutions Enabler-Server verfügt über eine Verbindung zum Symmetrix-Speicher-Array durch Zugriff auf Gatekeeper-Volumes. Für den Zugriff auf dieses Gerät sind Administratorberechtigungen erforderlich.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der Datenquelle „EMC Solutions Enabler“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende

Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte | Festplatte |
| Festplattengruppe | Festplattengruppe |
| Storage Array Durchführt | Storage |
| Direktor | Storage-Node |
| Geräte-Pool, Storage-Ressourcen-Pool (SRP) | Storage-Pool |
| Gerät, TDEV | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

Bevor Sie diese Datenquelle konfigurieren, sollten Sie sicherstellen, dass der OnCommand Insight-Server über eine TCP-Verbindung zu Port 2707 auf dem vorhandenen Solutions Enabler-Server verfügt. OnCommand Insight ermittelt alle Symmetrix-Arrays, die „`Local`“ für diesen Server sind, wie in der Ausgabe von „`symcfg list`“ dieses Servers dargestellt.

- Die EMC Solutions Enabler (CLI) mit SMI-S Provider-Anwendung muss installiert sein und die Version muss mit der auf dem Solutions Enabler Server ausgeführten Version übereinstimmen oder älter sein.
- Eine ordnungsgemäß konfiguriert `{installdir}\EMC\SYMAPI\config\netcnfg` Datei ist erforderlich. Diese Datei definiert Dienstnamen für Solutions Enabler-Server sowie die Zugriffsmethode (SECURE / NOSECURE /ANY).
- Wenn Sie eine Lese-/Schreiblatenz auf Speicherknotenebene benötigen, muss der SMI-S-Provider mit einer laufenden Instanz der UNISPHERE for VMAX-Anwendung kommunizieren.
- Administratorberechtigungen auf dem Solutions Enabler (SE)-Server
- Schreibgeschützter Benutzername und Kennwort für die SE-Software
- Anforderungen für Solutions Enabler Server 6.5X:
  - SMI-S Provider 3.3.1 für SMIS-S V1.2 installiert
  - Führen Sie nach der Installation aus `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- DIE UNISPHERE for VMAX-Anwendung muss ausgeführt werden und Statistiken für die Symmetrix VMAX-Speicher-Arrays sammeln, die von der SMI-S Provider-Installation gemanagt werden
- Zugriffsvalidierung: Überprüfen Sie, ob der SMI-S-Provider ausgeführt wird: `telnet <se_server\> 5988`

**Konfiguration**

Wenn die SMI-S-Benutzerauthentifizierung nicht aktiviert ist, werden die Standardwerte in der OnCommand Insight-Datenquelle ignoriert.

Wenn Symauth auf Symmetrix-Arrays aktiviert ist, kann OnCommand Insight diese möglicherweise nicht erkennen. Die OnCommand Insight-Erfassung wird als SYSTEMBENUTZER auf dem Server der OnCommand Insight/Remote-Erfassungseinheit ausgeführt, der mit dem Solutions Enabler-Server kommuniziert. Wenn hostname\SYSTEM keine symauth-Berechtigungen hat, kann OnCommand Insight das Array nicht ermitteln.

Die Datenquelle EMC Solutions Enabler Symmetrix CLI umfasst Unterstützung für die Gerätekonfiguration für Thin Provisioning und Symmetrix Remote Data Facility (SRDF).

Definitionen werden für Fibre-Channel- und Switch-Performance-Pakete bereitgestellt.

| Feld | Beschreibung |
|---|---|
| Name Des Service | Dienstname wie in der netcnfg-Datei angegeben |
| Vollständiger Pfad zur CLI | Vollständiger Pfad zur Symmetrix-CLI |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die Array-Liste unten bei der Datenerfassung ein- oder ausgeschlossen werden soll |
| Inventory Exclude Devices | Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen |

| | |
|---|---|
| Verbindungs-Caching | Verbindungszwischenspeicherung wählen:<br>• LOKAL bedeutet, dass der OnCommand Insight Acquisition-Service auf dem Solutions Enabler-Server ausgeführt wird, der über Fibre-Channel-Konnektivität zu den Symmetrix-Arrays verfügt, die Sie ermitteln möchten, und Zugriff auf Gatekeeper-Volumes hat. Dies ist möglicherweise in einigen Konfigurationen der Remote Acquisition Unit (rau) zu sehen.<br>• REMOTE_CACHED ist die Standardeinstellung und sollte in den meisten Fällen verwendet werden. Hierbei werden die NETCNFG-Dateieinstellungen verwendet, um eine Verbindung über IP mit dem Solutions Enabler-Server herzustellen. Dieser muss über eine Fibre-Channel-Verbindung zu den Symmetrix-Arrays verfügen, die Sie ermitteln möchten, und hat Zugriff auf Gatekeeper-Volumes.<br>• Falls DIE REMOTE_CACHED-Optionen CLI-Befehle fehlschlagen lassen, verwenden Sie die REMOTE-Option. Denken Sie daran, dass es den Erfassungsprozess verlangsamen wird (möglicherweise auf Stunden oder sogar Tage in extremen Fällen). Die NETCNFG-Dateieinstellungen werden weiterhin für eine IP-Verbindung zum Solutions Enabler-Server verwendet, der über Fibre Channel-Verbindungen zu den erkannten Symmetrix-Arrays verfügt.<br>Diese Einstellung ändert das OnCommand Insight-Verhalten in Bezug auf die Arrays, die in der Ausgabe „symcfg list“ als REMOTE aufgeführt werden, nicht. OnCommand Insight sammelt nur Daten auf Geräten, die mit diesem Befehl als LOKAL angezeigt werden. |
| CLI-Zeitüberschreitung (Sek.) | CLI-Prozess-Timeout (Standard: 7200 Sekunden) |
| SMI-S-HOST-IP | IP-Adresse des SMI-S Provider-Hosts |
| SMI-S-Port | Vom SMI-S Provider-Host verwendeter Port |
| Protokoll | Protokoll für die Verbindung mit dem SMI-S-Provider |
| SMI-S Namespace | Für die Verwendung durch den SMI-S-Provider konfigurierte Interoperabilität |

| | |
|---|---|
| SMI-S-Benutzername | Benutzername für den SMI-S Provider Host |
| SMI-S-Passwort | Benutzername für den SMI-S Provider Host |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 1000 Sekunden) |
| Typ Des Leistungsfilters | Geben Sie an, ob die unten aufgeführte Array-Liste beim Erfassen von Performancedaten einbezogen oder ausgeschlossen werden soll |
| Geräteliste Für Leistungsfilter | Kommagetrennte Liste der Geräte-IDs, die einbezogen oder ausgeschlossen werden sollen |
| RPO-Abfrageintervall (s) | Intervall zwischen RPO-Abfragen (Standard: 300 Sekunden) |

**EMC VNX-Datenquelle**

Für die Konfiguration erfordert die Datenquelle EMC VNX (SSH) die IP-Adresse der Control Station sowie einen Benutzernamen und ein Kennwort *Read-Only*.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| VNX-IP | IP-Adresse oder vollqualifizierter Domänenname der VNX Control Station |
| VNX-Benutzername | Benutzername für die VNX Control Station |
| VNX-Kennwort | Kennwort für die VNX Control Station |

**Anforderungen**

- Eine IP-Adresse der Control Station
- Nur-Lese-Benutzername und Kennwort.
- Zugriffsvalidierung: Überprüfen Sie den SSH-Zugriff über PuTTY.

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |

| | |
|---|---|
| VNX SSH-Zeitüberschreitung beim Prozess (Sek.) | VNX SSH-Prozess-Timeout (Standard: 600 Sekunden) |
| Wiederholversuche Für Celerra-Befehle | Anzahl der Wiederholversuche für Celerra-Befehle |
| CLARiiON External Process Timeout for Inventory (Sek.) | CLARiiON-Timeout für externen Prozess für Bestandsaufnahme (Standard: 1800 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| CLARiiON External Process Timeout for Performance (Sek.) | CLARiiON-Timeout für externe Prozesse für Performance (Standard: 1800 Sekunden) |

**EMC VNXe -Datenquelle**

## Die EMC VNXe Datenquelle bietet Bestandsunterstützung für EMC VNXe- und Unity Unified Storage-Arrays.

Diese Datenquelle ist CLI-basiert und erfordert, dass Sie Unisphere for VNXe CLI (uemcli.exe) auf der Erfassungseinheit installieren, auf der sich die VNXe-Datenquelle befindet. uemcli.exe verwendet HTTPS als Transportprotokoll, daher muss die Erfassungseinheit in der Lage sein, HTTPS-Verbindungen zu den VNXe/Unity-Arrays zu initiieren. Sie müssen mindestens einen schreibgeschützten Benutzer zur Verwendung durch die Datenquelle haben.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC VNXe -Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte | Festplatte |
| Storage Array Durchführt | Storage |
| Prozessor | Storage-Node |
| Storage-Pool | Storage-Pool |
| Allgemeine iSCSI-Block-Informationen, VMware VMFS | Datenmenge |
| Freigegebener Ordner | Internes Volumen |
| CIFS-Freigabe, NFS-Freigabe, Freigabe vom VMware-NFS-Datastore | Share |

| | |
|---|---|
| Remote-Replikationssystem | Synchronisierung |
| ISCSI-Node | ISCSI-Ziel-Node |
| ISCSI-Initiator | ISCSI-Target-Initiator |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieser Datenquelle:

- Der VNXe-Datensammler ist CLI-basiert. Sie müssen Unisphere for VNXe CLI (uemcli.exe) auf der Erfassungseinheit installieren, in der sich Ihr VNXe-Datensammler befindet.
- uemcli.exe verwendet HTTPS als Transportprotokoll, sodass die Erfassungseinheit in der Lage sein muss, HTTPS-Verbindungen zur VNXe zu initiieren.
- Sie müssen mindestens einen schreibgeschützten Benutzer zur Verwendung durch die Datenquelle haben.
- IP-Adresse des Managing Solutions Enabler Servers.
- HTTPS am Port 443 ist erforderlich
- Der EMC VNXe Data Collector bietet NAS- und iSCSI-Unterstützung für die Bestandsaufnahme. Fibre-Channel-Volumes werden erkannt, Insight jedoch keine Berichte über FC-Mapping, -Maskierung oder Speicherports.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| VNXe-Speicher | IP-Adresse oder vollqualifizierter Domänenname des VNXe -Geräts |
| Benutzername | Benutzername für das VNXe-Gerät |
| Passwort | Kennwort für das VNXe -Gerät |
| Vollständiger Pfad zur ausführbaren Datei uemcli | Vollständiger Pfad zum `uemcli.exe` Ausführbar |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| VNXe-CLI-Port | Port, der für die VNXe-CLI verwendet wird |

| | |
|---|---|
| Zeitlimit für externen Prozess für Bestandsaufnahme (Sek.) | Externes Prozess-Timeout (Standard: 1800 Sekunden) |

### EMC VPLEX-Datenquelle

Für die Konfiguration erfordert diese Datenquelle eine IP-Adresse des VPLEX-Servers und ein Domänenkonto auf Administratorebene.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der EMC VPLEX-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Cluster | Storage |
| Motor | Storage-Node |
| Gerät, System Erweitern | Back-End Storage-Pool |
| Virtual Volume | Datenmenge |
| Front-End-Port, Back-End-Port | Port |
| Verteiltes Gerät | Storage-Synchronisierung |
| Übersicht Storage | Volume Map, Volume Mask |
| Storage Volume | Back-End LUN |
| ITLS | Back-End-Pfad |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Eine IP-Adresse des VPLEX-Servers
- Domänenkonto auf Administratorebene für den VPLEX-Server
- Port 443 (HTTPS): Erfordert eine ausgehende Verbindung zum TCP-Port 443 auf der VPLEX-Managementstation.
- Für die Leistung können Sie den schreibgeschützten Benutzernamen und das Kennwort für den ssh/scp-Zugriff verwenden.
- Für die Leistung ist Port 22 erforderlich.

- Überprüfen Sie den Zugriff mit `telnet` Zu Port 443. Für einen anderen Port als den Standardport, mit jedem Browser verwenden

**Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| IP-Adresse der VPLEX Management Console | IP-Adresse oder vollqualifizierter Domänenname der VPLEX Management Console |
| Benutzername | Benutzername für VPLEX-CLI |
| Passwort | Passwort, das für die VPLEX-CLI verwendet wird |
| Remote-IP-Adresse der Performance der VPLEX-Managementkonsole | Performance Remote IP-Adresse der VPLEX Management Console |
| Performance Remote User Name | Performance Remote-Benutzername der VPLEX Management Console |
| Kennwort Für Das Remote-Netzwerk Der Performance | Remote-Kennwort für die Performance der VPLEX Management Console |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Kommunikations-Port | Für VPLEX-CLI verwendeter Port |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungs-Timeout (Sek.) | Verbindungs-Timeout (Standard: 60 Sekunden) |
| Anzahl Wiederholungen | Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abfragen (Standard: 600 Sekunden) |
| Performance SSH-Prozess Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 600 Sekunden) |
| SSH-Banner-Wartezeit (Sek.) | SSH Banner Wait Timeout (Standard: 20 Sekunden) |
| Anzahl Wiederholungen | Anzahl der Wiederholversuche für die Performance |

### EMC XtremIO Datenquelle

Um die Datenquelle EMC XtremIO (HTTP) zu konfigurieren, müssen Sie über die Hostadresse des XtremIO Management Server (XMS) und ein Konto mit Administratorrechten verfügen.

#### Terminologie

OnCommand Insight bezieht die folgenden Inventarinformationen aus der Datenquelle „EMC XtremIO“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte (SSD) | Festplatte |
| Cluster | Storage |
| Controller | Storage-Node |
| Datenmenge | Datenmenge |
| LUN-Zuordnung | Volume-Zuordnung |
| Initiator, Ziel | Volume-Maske |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Eine IP-Adresse jedes XtremIO Management Servers
- Ein Konto mit Administratorrechten
- Zugriff auf Port 443 (HTTPS)

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| XMS-Host | IP-Adresse oder vollqualifizierter Domain-Name des XtremIO Management Servers |
| Benutzername | Benutzername für den XtremIO Management Server |
| Passwort | Passwort für den XtremIO Management Server |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| TCP-Port | TCP-Port zur Verbindung mit dem XtremIO Management Server (Standard 443 ) |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Verbindungs-Timeout (Sek.) | Verbindungs-Timeout (Standard: 60 Sekunden) |
| Abfrageintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

### Fujitsu ETERNUS Datenquelle

Die Fujitsu ETERNUS Datenquelle benötigt die IP-Adresse des Speichers. Sie darf nicht durch Komma getrennt werden.

#### Terminologie

OnCommand Insight erwirbt die folgenden Bestandsinformationen aus der Fujitsu ETERNUS Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| --- | --- |
| Festplatte | Festplatte |
| Storage | Storage |
| Thin Pool, Flexibler Tier-Pool<br><br>Raid-Gruppe | Storage-Pool |
| Standard-Volume, Snap Data Volume (SDV),<br><br>Snap Data Pool Volume (SDPV),<br><br>Thin Provisioning-Volume (TPV) | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Eine IP-Adresse des ETERNUS-Speichers, die nicht durch Komma getrennt werden kann
- Benutzername und Passwort der SSH-Administration

- Port 22
- Stellen Sie sicher, dass der Seitenlauf deaktiviert ist. (Clienv-show-more-scroll deaktivieren)

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| IP-Adresse des ETERNUS-Speichers | IP-Adresse des ETERNUS-Speichers |
| Benutzername | Benutzername für ETERNUS-Speicher |
| Passwort | Passwort für den Sternus |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 600 Sekunden) |

### Hitachi Content Platform (HCP) Datenquelle

Dieser Datensammler unterstützt die Hitachi Content Platform (HCP) mithilfe der HCP Management API.

**Terminologie**

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der HCP-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| HCP-Cluster | Storage |
| Mandant | Storage-Pool |
| Namespace | Internes Volumen |
| Knoten | Knoten |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Inventaranforderungen

- IP-Adresse des HCP-Servers
- Schreibgeschützter Benutzername und Kennwort für die HCP-Software und die Peer-Rechte

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| HCP-Host | IP-Adresse oder vollqualifizierter Domänenname des HCP-Hosts |
| HCP-Anschluss | Der Standardwert ist 9090 |
| HCP-Benutzer-ID | Benutzername für den HCP-Host |
| HCP-Kennwort | Kennwort für den HCP-Host |
| HCP-Authentifizierungstyp | Wählen Sie HCP_LOCAL oder ACTIVE_DIRECTORY |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abfragen (Standard: 900 Sekunden) |

### Datenquelle von HDS HiCommand Device Manager

Die Datenquellen HDS HiCommand und HiCommand Lite unterstützen den HiCommand Device Manager-Server. OnCommand Insight kommuniziert über die standardmäßige HiCommand-API mit dem HiCommand-Geräte-Manager-Server.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsdaten aus den HDS HiCommand- und HiCommand Lite-Datenquellen. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| PDEV | Festplatte |
| Journalpool | Festplattengruppe |

| | |
|---|---|
| Storage Array Durchführt | Storage |
| Port Controller | Storage-Node |
| Array-Gruppe, DP-Pool | Storage-Pool |
| Logische Einheit, LDEV | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Inventaranforderungen

- IP-Adresse des HiCommand Device Manager-Servers
- Schreibgeschützter Benutzername und Kennwort für die HiCommand Device Manager-Software und Peer-Berechtigungen
- Port-Anforderungen: 2001 (http) oder 2443 (https)
- Zugriff validieren:
  - Melden Sie sich bei der HiCommand Device Manager-Software mit dem Benutzernamen und Kennwort des Kollegen an.
  - Überprüfen Sie den Zugriff auf die HiCommand Device Manager-API: `telnet <HiCommand Device_Manager_server_ip\> 2001`

#### Performance-Anforderungen Erfüllt

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.
  - Das Export-Tool (`Export.exe`) Muss auf den OnCommand Insight-Server kopiert werden.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- HDS AMS-Leistung
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm des Speichernavigators Modular 2 (SNM2) muss auf dem OnCommand Insight-Server installiert sein.
  - Sie müssen alle AMS-, WMS- und SMS-Speicher-Arrays registrieren, deren Leistung von OnCommand Insight erworben werden muss, indem Sie den folgenden Befehl verwenden:
  - Sie müssen sicherstellen, dass alle Arrays, die Sie registriert haben, in der Ausgabe dieses Befehls aufgeführt sind: `auunitref.exe`.

#### Konfiguration

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| HiCommand Server | IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers |
| Benutzername | Benutzername für den HiCommand Device Manager-Server. |
| Passwort | Passwort, das für den HiCommand Device Manager-Server verwendet wird. |
| GERÄTE – VSP G1000 (R800), VSP (R700), HUS VM (HM700) UND USP-SPEICHER | Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Storage benötigt:<br>• IP-Adresse des Arrays: IP-Adresse des Speichers<br>• Benutzername: Benutzername für den Speicher<br>• Passwort: Passwort für den Speicher<br>• Ordner mit Export Utility JAR-Dateien: Der Ordner, der das Export-Dienstprogramm enthält `.jar` Dateien |
| SNM2Geräte - WMS/SMS/AMS-Speicher | Geräteliste für WMS/SMS/AMS-Speicher. Jeder Storage benötigt:<br>• IP-Adresse des Arrays: IP-Adresse des Speichers<br>• Speicher Navigator CLI-Pfad: SNM2 CLI-Pfad<br>• Kontoauthentifizierung gültig: Wählen Sie die Option zur Auswahl einer gültigen Kontokertifizierung aus<br>• Benutzername: Benutzername für den Speicher<br>• Passwort: Passwort für den Speicher |
| Wählen Sie Tuning Manager für Leistung | Wählen Sie Tuning Manager, um die Leistung anzuzeigen und andere Leistungsoptionen außer Kraft zu setzen |
| Tuning Manager Host | IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers |
| Tuning-Manager-Port | Port, der für Tuning Manager verwendet wird |
| Benutzername Für Tuning Manager | Benutzername für Tuning Manager |
| Kennwort Für Tuning-Manager | Passwort für Tuning Manager |

Bei HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| HiCommand Server-Port | Port, der für den HiCommand Device Manager verwendet wird |
| HTTPS aktiviert | Wählen Sie diese Option aus, um HTTPS zu aktivieren |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die Array-Liste unten bei der Datenerfassung ein- oder ausgeschlossen werden soll |
| Schließen Sie Geräte aus oder schließen Sie sie ein | Kommagetrennte Liste der Geräte-IDs oder Array-Namen, die einbezogen oder ausgeschlossen werden sollen |
| Abfrage-Host-Manager | Wählen Sie diese Option aus, um den Hostmanager abzufragen |
| HTTP-Timeout (Sek.) | HTTP-Verbindungs-Timeout (Standard: 60 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Ausfuhrzeitlimit in Sekunden | Timeout des Exportdienstprogramms (Standard: 300 Sekunden) |

#### Datensammler Hitachi Ops Center

Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Bestands- und Performancedaten mehrerer Speichergeräte zuzugreifen. Eine Bestandsaufnahme und Kapazitätserkennung muss in Ihrer Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Zur Performance-Erfassung muss zusätzlich „Analyzer“ implementiert sein.

### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Laufzeit der OnCommand Insight |
| --- | --- |
| Storage-Systeme | Storage |

| Anbieter-/Modelllaufzeit | Laufzeit der OnCommand Insight |
|---|---|
| Datenmenge | Datenmenge |
| Paritätsgruppen | Speicherpool (RAID), Festplattengruppen |
| Festplatte | Festplatte |
| Storage-Pool | Speicherpool (Thin, SNAP) |
| Externe Paritätsgruppen | Speicherpool (Backend), Festplattengruppen |
| Port | Storage-Node → Controller-Node →-Port |
| Host-Gruppen | Volume-Zuordnung und -Maskierung |
| Volume-Paare | Storage-Synchronisierung |

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

### Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse oder Hostname des Ops Center-Servers, der die „Common Services“-Komponente hostet
- Root/sysadmin Benutzerkonto und Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center Komponenten gehostet werden. HDS hat KEINE REST-API-Unterstützung für LDAP/SSO-Benutzer bis Ops Center 10.8+ implementiert

### Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- Das HDS Ops Center „Analyzer“-Modul muss installiert sein
- Speicher-Arrays müssen das Ops Center „Analyzer“-Modul speisen

### Konfiguration

| Feld | Beschreibung |
|---|---|
| Hitachi Ops Center-IP-Adresse | IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, der die Komponente „Allgemeine Dienste“ hostet |
| Benutzername | Benutzername für den Ops-Center-Server. |
| Passwort | Passwort, das für den Ops-Center-Server verwendet wird. |

### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Verbindungstyp | HTTPS (Port 443) ist der Standard |

| | |
|---|---|
| TCP-Port überschreiben | Geben Sie den zu verwendenden Port an, wenn nicht der Standardport |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40. |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll. |
| Geräteliste filtern | Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300. |

#### HDS-Speicher

## Begriffe, die auf Objekte oder Referenzen angewendet werden, die auf den Landing Pages für HDS-Storage-Assets zu finden sind.

### HDS-Speicherterminologie

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name — kommt direkt vom HDS HiCommand Device Manager-Attribut „`Name`“ über den XML-API-Aufruf von GetStorageArray
- Modell – wird direkt vom HDS HiCommand Device Manager-Attribut „`arrayType`“ über den XML-API-Aufruf von GetStorageArray geliefert
- Anbieter — HDS
- Familie - kommt direkt vom HDS HiCommand Device Manager ‘arrayFamily’ Attribut über den GetStorageArray XML API-Aufruf
- IP – hierbei handelt es sich um die Management-IP-Adresse des Arrays, keine vollständige Liste aller IP-Adressen auf dem Array
- RAW Capacity – ein base2-Wert, der die Summe der Gesamtkapazität aller Festplatten in diesem System darstellt, unabhängig von der Festplattenrolle.

#### HDS-Speicherpool

## Begriffe, die auf Objekte oder Referenzen angewendet werden, die Sie auf den Landing Pages für HDS-Speicherpools finden können.

### HDS-Speicherpool-Terminologie

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf HDS Storage Pool Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Typ: Der Wert hier ist einer von:
  - RESERVIERT — wenn dieser Pool für andere Zwecke als Datenvolumes, d. h. Journaling, Snapshots, reserviert ist

- Thin Provisioning — wenn dies ein HDP-Pool ist
- RAID-Gruppe — Sie werden diese wahrscheinlich aus einigen Gründen nicht sehen:

  OCI verfolgt eine starke Haltung, um zu vermeiden, dass bei allen Kosten eine doppelte Kapazität gezählt wird. Auf HDS muss man normalerweise RAID-Gruppen von Festplatten erstellen, Pool-Volumes auf diesen RAID-Gruppen erstellen und Pools (oft HDP, könnte aber besonderer Zweck sein) aus diesen Pool Volumes erstellen. Wenn OCI sowohl die zugrunde liegenden RAID-Gruppen wie auch die Pools meldet, würde die Summe ihrer Rohkapazität die Summe der Festplatten deutlich übersteigen.

Stattdessen verringert der HDS HiCommand-Datensammler von OCI die Größe von RAID-Gruppen willkürlich anhand der Kapazität von Pool Volumes. Dies kann dazu führen, dass OCI keine Berichte über die RAID-Gruppe erstellt. Darüber hinaus werden alle resultierenden RAID-Gruppen so gekennzeichnet, dass sie in der OCI WebUI nicht sichtbar sind, aber in das OCI Data Warehouse (DWH) fließen. Der Zweck dieser Entscheidungen ist es, UI-Unordnung für Dinge zu vermeiden, die den meisten Benutzern egal sind — Wenn Ihr HDS-Array RAID-Gruppen mit 50 MB frei hat, können Sie diesen freien Speicherplatz wahrscheinlich nicht für ein sinnvolles Ergebnis verwenden.

- Node – k. A., da HDS Pools nicht an einen bestimmten Node gebunden sind
- Redundanz: Der RAID-Level des Pools. Möglicherweise mehrere Werte für einen HDP-Pool, die aus mehreren RAID-Typen bestehen
- Kapazität % - der Prozentsatz, der für die Datenverwendung des Pools verwendet wird, wobei die verwendete GB und die gesamte logische GB-Größe des Pools verwendet werden
- Überbelegte Kapazität – ein abgeleiteter Wert, der „`die logische Kapazität dieses Pools wird durch diesen Prozentsatz überzeichnet, da die Summe der logischen Volumes die logische Kapazität des Pools um diesen Prozentsatz übersteigt`“
- Snapshot - zeigt die Kapazität an, die für die Snapshot-Nutzung in diesem Pool reserviert ist

#### HDS-Speicher-Node

## Begriffe, die auf Objekte oder Referenzen angewendet werden, die auf den Landing Pages für HDS-Storage-Node-Assets zu finden sind.

### HDS-Speicher-Node-Terminologie

Die folgenden Begriffe beziehen sich auf Objekte oder Referenzen, die auf den HDS Storage Node Asset Landing Pages zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Name: Der Name des Front-End-Directors (FED) oder des Channel-Adapters auf monolithischen Arrays oder der Name des Controllers auf einem modularen Array. Ein bestimmtes HDS-Array verfügt über zwei oder mehr Storage-Nodes
- Volumes – die Volume-Tabelle zeigt jedes Volume an, das einem beliebigen Port dieses Speicherknoten zugeordnet ist

### Datensammler Hitachi Ops Center

## Dieser Datensammler verwendet die integrierte Anwendungssuite von Hitachi Ops Center, um auf Bestands- und Performancedaten mehrerer Speichergeräte zuzugreifen. Eine Bestandsaufnahme und Kapazitätserkennung muss in Ihrer Ops Center-Installation sowohl die Komponenten „Common Services“ als auch „Administrator“ enthalten. Zur

# Performance-Erfassung muss zusätzlich „Analyzer“ implementiert sein.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus diesem Datensammler. Für jeden erfassten Asset-Typ wird die am häufigsten für dieses Dokument verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Laufzeit der OnCommand Insight |
|---|---|
| Storage-Systeme | Storage |
| Datenmenge | Datenmenge |
| Paritätsgruppen | Speicherpool (RAID), Festplattengruppen |
| Festplatte | Festplatte |
| Storage-Pool | Speicherpool (Thin, SNAP) |
| Externe Paritätsgruppen | Speicherpool (Backend), Festplattengruppen |
| Port | Storage-Node → Controller-Node →-Port |
| Host-Gruppen | Volume-Zuordnung und -Maskierung |
| Volume-Paare | Storage-Synchronisierung |

Hinweis: Es handelt sich hierbei nur um allgemeine Terminologiezuordnungen. Diese stellen für diesen Datensammler möglicherweise nicht alle Fälle dar.

#### Inventaranforderungen

Zur Erfassung von Bestandsdaten müssen Sie Folgendes haben:

- IP-Adresse oder Hostname des Ops Center-Servers, der die „Common Services“-Komponente hostet
- Root/sysadmin Benutzerkonto und Passwort, die auf allen Servern vorhanden sind, auf denen Ops Center Komponenten gehostet werden. HDS hat KEINE REST-API-Unterstützung für LDAP/SSO-Benutzer bis Ops Center 10.8+ implementiert

#### Performance-Anforderungen erfüllt

Zur Erfassung von Leistungsdaten müssen die folgenden Anforderungen erfüllt sein:

- Das HDS Ops Center „Analyzer“-Modul muss installiert sein
- Speicher-Arrays müssen das Ops Center „Analyzer“-Modul speisen

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Hitachi Ops Center-IP-Adresse | IP-Adresse oder vollqualifizierter Domänenname des Ops Center-Servers, der die Komponente „Allgemeine Dienste“ hostet |
| Benutzername | Benutzername für den Ops-Center-Server. |

| Feld | Beschreibung |
| --- | --- |
| Passwort | Passwort, das für den Ops-Center-Server verwendet wird. |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Verbindungstyp | HTTPS (Port 443) ist der Standard |
| TCP-Port überschreiben | Geben Sie den zu verwendenden Port an, wenn nicht der Standardport |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen Der Standardwert ist 40. |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die unten aufgeführte Array-Liste beim Sammeln von Daten aufgenommen oder ausgeschlossen werden soll. |
| Geräteliste filtern | Kommagetrennte Liste der einzuschließenden oder auszuschließenden Geräteseriennummer |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen Der Standardwert ist 300. |

### HDS NAS (HNAS)-Datenquelle

Die HDS NAS (HNAS)-Datenquelle ist eine Bestands- und Konfigurationsdatenquelle, die die Erkennung von HDS-NAS-Clustern unterstützt. Insight unterstützt die Erkennung von NFS- und CIFS-Freigaben, Filesystemen (interne Insight Volumes) und Zeitspannen (Insight Storage Pools).

Diese Datenquelle basiert auf SSH. Daher muss die Erfassungseinheit, die sie hostet, SSH-Sitzungen zu TCP 22 auf dem HNAS selbst oder der Systems Management Unit (SMU) initiieren können, mit der das Cluster verbunden ist.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der HNAS-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| --- | --- |
| Ebene | Festplattengruppe |
| Cluster | Storage |
| Knoten | Storage-Node |
| Span | Storage-Pool |

| | |
|---|---|
| File-System | Internes Volumen |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieser Datenquelle:

- IP-Adresse des Geräts
- Port 22, SSH-Protokoll
- Benutzername und Passwort - Berechtigungsebene: Supervisor
- HINWEIS: Dieser Datensammler basiert auf SSH. Daher muss die AU, die sie hostet, SSH-Sitzungen zu TCP 22 auf dem HNAS selbst oder der Systems Management Unit (SMU) initiieren können, mit der das Cluster verbunden ist.

Dieser Datensammler basiert auf SSH, sodass die AU, die sie hostet, SSH-Sitzungen zu TCP 22 auf dem HNAS selbst oder der Systems Management Unit (SMU) initiieren kann, mit der das Cluster verbunden ist.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| HNAS-Host | IP-Adresse oder vollqualifizierter Domain-Name des HNAS Management Host |
| Benutzername | Benutzername für HNAS CLI |
| Passwort | Passwort, das für HNAS-CLI verwendet wird |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 30 Minuten) |
| SSH-Banner-Wartezeit (Sek.) | SSH Banner Wait Timeout (Standard: 15 Sekunden) |
| SSH-Befehlstaste Timeout (Sek.) | SSH-Befehlszeitlimit (Standard: 30 Sekunden) |

### HP CommandView AE-Datenquelle

Die Datenquellen HP CommandView Advanced Edition (AE) und CommandView AE CLI/SMI (AE Lite) unterstützen die Bestandsaufnahme und Leistung über einen CommandView (auch HiCommand genannt) Device Manager-Server.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsdaten aus den Datenquellen HP CommandView AE und AE Lite. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| PDEV | Festplatte |
| Journalpool | Festplattengruppe |
| Storage Array Durchführt | Storage |
| Port Controller | Storage-Node |
| Array-Gruppe, DP-Pool | Storage-Pool |
| Logische Einheit, LDEV | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Inventaranforderungen

- IP-Adresse des HiCommand Device Manager-Servers
- Schreibgeschützter Benutzername und Kennwort für die CommandView AE-Software und Peer-Berechtigungen
- Für die CommandView AE Lite-Version des Gerätemanagers ist nur die CLI lizenziert
- Port-Anforderung: 2001

#### Performance-Anforderungen Erfüllt

- HDS USP, USP V und VSP Performance
  - Performance Monitor muss lizenziert sein.
  - Überwachungsschalter muss aktiviert sein.
  - Das Export-Tool (`Export.exe`) Muss auf den OnCommand Insight-Server kopiert werden.
  - Die Version des Exportwerkzeugs muss mit der Microcode-Version des Ziel-Arrays übereinstimmen.
- HDS AMS-Leistung
  - Performance Monitor muss lizenziert sein.
  - Das CLI-Dienstprogramm des Speichernavigators Modular 2 (SNM2) muss auf dem OnCommand Insight-Server installiert sein.
  - Sie müssen alle AMS-, WMS- und SMS-Speicher-Arrays registrieren, deren Leistung von OnCommand Insight erworben werden muss, indem Sie den folgenden Befehl verwenden:
  - Sie müssen sicherstellen, dass alle Arrays, die Sie registriert haben, in der Ausgabe dieses Befehls

aufgeführt sind: `auunitref.exe`.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| HiCommand Server | IP-Adresse oder vollqualifizierter Domänenname des HiCommand Device Manager-Servers |
| Benutzername | Benutzername für den HiCommand Device Manager-Server. |
| Passwort | Passwort, das für den HiCommand Device Manager-Server verwendet wird. |
| Geräte – USP, USP V, VSP/R600-Speicher | Geräteliste für VSP G1000 (R800), VSP (R700), HUS VM (HM700) und USP-Speicher. Jeder Storage benötigt:<br>• IP-Adresse des Arrays: IP-Adresse des Speichers<br>• Benutzername: Benutzername für den Speicher<br>• Passwort: Passwort für den Speicher<br>• Ordner mit Export Utility JAR-Dateien: Der Ordner, der das Export-Dienstprogramm enthält `.jar` Dateien |
| SNM2Geräte - WMS/SMS/AMS-Speicher | Geräteliste für WMS/SMS/AMS-Speicher. Jeder Storage benötigt:<br>• IP-Adresse des Arrays: IP-Adresse des Speichers<br>• Speicher Navigator CLI-Pfad: SNM2 CLI-Pfad<br>• Kontoauthentifizierung gültig: Wählen Sie die Option zur Auswahl einer gültigen Kontokertifizierung aus<br>• Benutzername: Benutzername für den Speicher<br>• Passwort: Passwort für den Speicher |
| Wählen Sie Tuning Manager für Leistung | Wählen Sie Tuning Manager, um die Leistung anzuzeigen und andere Leistungsoptionen außer Kraft zu setzen |
| Tuning Manager Host | IP-Adresse oder vollqualifizierter Domain-Name des Tuning Managers |
| Tuning-Manager-Port | Port, der für Tuning Manager verwendet wird |
| Benutzername Für Tuning Manager | Benutzername für Tuning Manager |

| | |
|---|---|
| Kennwort Für Tuning-Manager | Passwort für Tuning Manager |

Bei HDS USP, USP V und VSP kann jede Festplatte zu mehr als einer Array-Gruppe gehören.

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| HiCommand Server-Port | Port, der für den HiCommand Device Manager verwendet wird |
| HTTPS aktiviert | Wählen Sie diese Option aus, um HTTPS zu aktivieren |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die Array-Liste unten bei der Datenerfassung ein- oder ausgeschlossen werden soll |
| Schließen Sie Geräte aus oder schließen Sie sie ein | Kommagetrennte Liste der Geräte-IDs oder Array-Namen, die einbezogen oder ausgeschlossen werden sollen |
| Abfrage-Host-Manager | Wählen Sie diese Option aus, um den Hostmanager abzufragen |
| HTTP-Timeout (Sek.) | HTTP-Verbindungs-Timeout (Standard: 60 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Ausfuhrzeitlimit in Sekunden | Timeout des Exportdienstprogramms (Standard: 300 Sekunden) |

### HP EVA Storage-Datenquelle

Für die Konfiguration benötigt die EVA Storage (SSSU) Datenquelle die IP-Adresse des Command View (CV)-Servers und einen *Read-only* Benutzernamen und ein Passwort für die CV-Software. Der Benutzer muss in der CV-Software definiert sein.

#### Terminologie

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der HP EVA-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| --- | --- |
| Festplatte | Festplatte |
| Festplattengruppe | Festplattengruppe (nicht modelliert) |
| Speicherzelle | Storage |
| Virtuelles Laufwerk | Storage-Pool |
| Virtuelles Laufwerk | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Inventaranforderungen

- IP-Adresse des CV-Servers
- Schreibgeschützter Benutzername und Kennwort für die CV-Software. Der Benutzer muss in der CV-Software definiert sein.
- Software von Drittanbietern, die auf dem OnCommand Insight-Server/rau installiert ist: `sssu.exe`. Der `sssu.exe` Version sollte der CV-Version entsprechen.
- Zugriffsvalidierung: Ausführen `sssu.exe` Befehle mit Benutzername und Passwort.

#### Performance-Anforderungen Erfüllt

Die HP StorageWorks Command View EVA-Softwaresuite muss auf dem OnCommand Insight-Server installiert sein. Alternativ können Sie eine Remote Acquisition Unit (rau) auf dem EVA-Server installieren:

1. Installieren Sie die HP StorageWorks Command View EVA Softwaresuite auf dem OnCommand Insight-Server oder installieren Sie eine Remote-Akquisitionseinheit auf dem Command View EVA-Server.
2. Suchen Sie das `evaperf.exe` Befehl. Beispiel: `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Führen Sie die folgenden Schritte mithilfe der IP des Command View-Servers aus:
   a. Führen Sie diesen Befehl aus, wobei 860 der Standardport ist `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. Geben Sie das Passwort für den Command View-Server an der Eingabeaufforderung ein.

      Dies sollte eine Eingabeaufforderung und nichts anderes zurückgeben.
4. Überprüfen Sie das Setup, indem Sie ausführen `evaperf.exe ls`.

   Es sollte eine Liste der vom Command View-Server verwalteten Arrays oder Controller angezeigt werden. Jede Zeile zeigt einen Controller in einem EVA-Array.

**Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| CommandView-Server | IP-Adresse oder vollständig qualifizierter Domänenname des EVA Storage Manager |
| Benutzername | Benutzername für den Command View-Manager. Der Name muss in der Command View definiert werden. |
| Passwort | Für den Command View-Manager verwendetes Passwort. |
| Name Des Performance-Benutzers | Für die Performance der Benutzername für den Command View Manager. Der Name muss in der Command View definiert werden. |
| Leistungspasswort | Für die Performance das für den Command View-Manager verwendete Passwort. |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| CLI-Startseite | Vollständiger Pfadname des CLI Home-Verzeichnisses, wo `sssu.exe` Befindet sich |
| Inventory Exclude Devices | Kommagetrennte Liste der einzuschließen |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Performance CLI-Startseite | Für Array-Performance: Vollständiger Pfadname des CLI-Home-Verzeichnisses, in dem sich sssu.exe befindet. Um den Zugriff zu validieren, führen Sie aus `sssu.exe` |
| Zeitüberschreitung des Befehls (s) | `evaperf` Timeout für Befehlstaste (standardmäßig 600 Sekunden) |
| Die Leistung Schließt Geräte Aus | Kommagetrennte Liste der Gerätenamen, die von der Erfassung von Leistungsdaten ausgeschlossen werden sollen |

### HPE Nimble Datenquelle

# Der HPE Nimble-Datensammler unterstützt Bestands- und Performance-Daten für HPE Nimble-Storage-Arrays.

#### Terminologie

OnCommand Insight erfasst die folgenden Inventarinformationen aus der HPE Nimble Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Array Erledigen | Storage |
| Festplatte | Festplatte |
| Pool | Storage-Pool |
| Datenmenge | Datenmenge |
| Initiator | Storage-Host-Alias |
| Controller | Storage-Node |
| Fibre Channel-Schnittstelle | Controller |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Das Array muss installiert und konfiguriert sein und über den Client über seinen vollständig qualifizierten Domänennamen (FQDN) oder die Array-Management-IP-Adresse erreichbar sein.
- Auf dem Array muss NimbleOS 2.3.x oder höher ausgeführt werden.
- Sie müssen einen gültigen Benutzernamen und ein gültiges Kennwort für das Array haben.
- Port 5392 muss auf dem Array geöffnet sein.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Array-Management-IP-Adresse | Vollständig qualifizierter Domain-Name (FQDN) oder Array-Management-IP-Adresse. |
| Benutzername | Benutzername für das Nimble-Array |

| | |
|---|---|
| Passwort | Passwort für das Nimble-Array |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Port | Der von Nimble REST API verwendete Port. Der Standardwert ist 5392. |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |

Hinweis: Das Standard-Performance-Abfrageintervall beträgt 300 Sekunden und kann nicht geändert werden. Dies ist das einzige von Nimble unterstützte Intervall.

### Datenquelle von Huawei OceanStor

OnCommand Insight verwendet die Datenquelle Huawei OceanStor (REST/HTTPS), um Bestände für Huawei OceanStor-Speicher zu ermitteln.

#### Terminologie

OnCommand Insight erwirbt die folgenden Bestands- und Leistungsinformationen vom Huawei OceanStor. Für jeden von OnCommand Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieses Datensammlers die folgende Terminologie:

| | |
|---|---|
| Anbieter-/Modelllaufzeit | Laufzeit der OnCommand Insight |
| Storage-Pool | Storage-Pool |
| File-System | Internes Volumen |
| Controller | Storage-Node |
| FC-Port (zugeordnet) | Volume-Zuordnung |
| Host FC Initiator (zugeordnet) | Volume-Maske |
| NFS/CIFS-Freigabe | Share |
| Share | ISCSI-Ziel-Node |
| ISCSI-Link-Initiator | ISCSI-Initiator-Node |
| Festplatte | Festplatte |

| | |
|---|---|
| LUN | Datenmenge |

#### Anforderungen

Die folgenden Anforderungen gelten für die Konfiguration und Verwendung dieses Datensammlers:

- Geräte-IP
- Anmeldeinformationen für den Zugriff auf OceanStor Geräte-Manager
- Port 8088 muss verfügbar sein

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| OceanStor Host-IP-Adresse | IP-Adresse oder vollqualifizierter Domain-Name des OceanStor Device Managers |
| Benutzername | Name, der zur Anmeldung beim OceanStor Device Manager verwendet wird |
| Passwort | Passwort zur Anmeldung beim OceanStor Device Manager |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| TCP-Port | TCP-Port zur Verbindung mit OceanStor Device Manager (Standard 8088 ) |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Verbindungs-Timeout (s) | Verbindungs-Timeout (Standard: 60 Sekunden) |

### IBM Cleversafe Datenquelle

Diese Datenquelle sammelt Bestands- und Leistungsdaten für IBM Cleversafe.

#### Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- Manager-IP-Adresse oder Hostname
- Ein Benutzername und ein Passwort für dasselbe
- Port 9440

#### Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Cleversafe Manager Hostname oder IP-Adresse | Host-IP-Adresse des CleverSafe-Geräts |
| Benutzername | Name für die Anmeldung bei Cleversafe |
| Passwort | Passwort für die Anmeldung bei Cleversafe |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Der Standardwert ist 60 Minuten |
| HTTP-Verbindungs-Timeout) | Der Standardwert ist 60 Sekunden |

### IBM DS-Datenquelle

Die IBM DS (CLI)-Datenquelle unterstützt nur DS6xxx- und DS8xxx-Geräte. DS3xxx, DS4xxx und DS5xxx Geräte werden von der NetApp E-Series Datenquelle unterstützt. Unterstützte Modelle und Firmware-Versionen finden Sie in der Insight Datenquellen-Support-Matrix.

#### Terminologie

OnCommand Insight bezieht die folgenden Bestandsinformationen aus der IBM DS-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| --- | --- |
| Festplattenmodul | Festplatte |
| Storage-Bild | Storage |
| Extent-Pool | Storage-Pool |
| Festes Block-Volume | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- IP-Adresse jedes DS-Arrays
- Der Name der Speicheranzeige ist optional und nur kosmetisch

- Schreibgeschützter Benutzername und Kennwort auf jedem DS-Array
- Software von Drittanbietern, die auf dem Insight Server installiert ist: IBM dscli
- Zugriffsvalidierung: Ausführen `dscli` Befehle, die den Benutzernamen und das Passwort verwenden
- Port-Anforderungen: 80, 443 und 1750

**Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| DS-Speicher | IP-Adresse oder vollständig qualifizierter Domänenname des DS-Speicherhosts |
| Benutzername | Der für die DS-CLI verwendete Name |
| Passwort | Für die DS-CLI verwendetes Passwort |
| Ausführbarer Pfad dscli.exe | Vollständiger Pfad zum `dscli.exe`Utility: |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Anzeigename Für Speicher | Name des IBM DS-Speicherarrays |
| Inventory Exclude Devices | Kommagetrennte Liste von Geräteseriennummer, die von der Bestandserfassung ausgeschlossen werden sollen |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Typ Des Leistungsfilters | Enthalten: Daten, die nur von Geräten in der Liste erfasst werden. Ausschließen: Es werden keine Daten von diesen Geräten erfasst |
| Geräteliste Für Leistungsfilter | Kommagetrennte Liste der Geräte-IDs, die die Leistungssammlung einschließen oder ausschließen sollen |

**IBM PowerVM-Datenquelle**

Die IBM PowerVM (SSH)-Datenquelle sammelt Informationen über virtuelle Partitionen, die auf IBM POWER Hardware-Instanzen ausgeführt werden, die von einer Hardware Management Console (HMC) verwaltet werden. Für die Konfiguration erfordert diese

# Datenquelle die Anmeldung beim HMC über SSH mit dem Benutzernamen und die Berechtigung auf Ansichtebene für HMC-Konfigurationen.

**Terminologie**

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der IBM PowerVM-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Hdisk | Virtuelles Laufwerk |
| Managed System | Host |
| LPAR, VIO Server | Virtual Machine |
| Volume-Gruppe | Datastore |
| Physisches Volume | LUN |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- IP-Adresse der Hardware Management Console (HMC)
- Benutzername und Passwort, die über SSH Zugriff auf HMC bieten
- Port-Anforderung SSH-22
- Zeigen Sie Berechtigungen auf allen Verwaltungssystemen und Sicherheitsdomänen logischer Partitionen an

  Der Benutzer muss darüber hinaus über die Berechtigung View für HMC-Konfigurationen und die Möglichkeit verfügen, VPD-Informationen für die Sicherheitsgruppierung der HMC-Konsole zu sammeln. Der Benutzer muss außerdem den Zugriff auf den virtuellen IO-Server-Befehl unter der Sicherheitsgruppierung der logischen Partition zulassen. Es ist eine bewährte Vorgehensweise, von einer Rolle eines Bedieners zu beginnen und dann alle Rollen zu entfernen. Schreibgeschützte Benutzer auf dem HMC haben keine Berechtigungen zum Ausführen von Proxed-Befehlen auf AIX-Hosts.

- Die Best Practice von IBM besteht darin, dass die Geräte von zwei oder mehr HMCs überwacht werden. Beachten Sie, dass dies dazu führen kann, dass OnCommand Insight doppelte Geräte meldet. Daher wird dringend empfohlen, redundante Geräte zur Liste „Geräte ausschließen“ in der erweiterten Konfiguration für diesen Datensammler hinzuzufügen.

**Konfiguration**

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| Hardware Management Console (HMC)-Adresse | IP-Adresse oder vollqualifizierter Domänenname der PowerVM Hardware Management Console |
| HMC-Benutzer | Benutzername für die Hardware Management Console |
| Passwort | Kennwort, das für die Hardware-Verwaltungskonsole verwendet wird |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| SSH-Port | Port, der für SSH zu PowerVM verwendet wird |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 600 Sekunden) |
| Anzahl Wiederholungen | Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme |
| Geräte Ausschließen | Kommagetrennte Liste von Geräte-IDs oder zu schließenden Anzeigenamen |

### IBM SVC-Datenquelle

Die IBM SVC-Datenquelle erfasst Bestands- und Leistungsdaten mithilfe von SSH und unterstützt eine Vielzahl von Geräten, auf denen das SVC-Betriebssystem ausgeführt wird. Die Liste der unterstützten Geräte umfasst Modelle wie SVC, v7000, v5000 und v3700. Unterstützte Modelle und Firmware-Versionen finden Sie in der Insight Datenquellen-Supportmatrix.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der IBM SVC-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| | |
|---|---|
| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| Laufwerk | Festplatte |
| Cluster | Storage |
| Knoten | Storage-Node |

| | |
|---|---|
| Mdisk-Gruppe | Storage-Pool |
| Vdisk | Datenmenge |
| Mdisk | Back-End LUN |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Inventaranforderungen**

- IP-Adresse jedes SVC-Clusters
- Port 22 verfügbar
- Öffentliches und privates Schlüsselpaar, das Sie entweder mitInsight generieren oder ein bereits auf Ihrem SVC verwendeter Schlüsselcode wiederverwenden

  Wenn Sie eine vorhandene Tasteneingabe erneut verwenden, müssen Sie sie vom Putty-Format in das OpenSSH-Format konvertieren.
- Auf dem SVC-Cluster installierter öffentlicher Schlüssel
- Der private Schlüssel muss in der Datenquelle identifiziert werden
- Zugriffsvalidierung: Offen `ssh` Sitzung mit dem privaten Schlüssel zum SVC-Cluster

Es muss keine Software von Drittanbietern installiert werden.

**Performance-Anforderungen Erfüllt**

- SVC-Konsole, die für jeden SVC-Cluster obligatorisch und für das Foundation-Paket für die SVC-Erkennung erforderlich ist
- Administratorzugriffsebene ist nur für das Kopieren von Performance-Datendateien von Cluster Nodes auf den Konfigurations-Node erforderlich.

  Da diese Zugriffsebene für das SVC Foundation Discovery-Paket nicht erforderlich ist, kann der SVC Foundation-Benutzer möglicherweise nicht erfolgreich arbeiten.
- Port 22 erforderlich
- Für diesen Benutzer muss ein privater und öffentlicher SSH-Schlüssel generiert und der private Schlüssel gespeichert werden, damit er über die Erfassungseinheit zugänglich ist. Wenn der SVC Foundation-Benutzer über die entsprechenden Berechtigungen verfügt, funktionieren derselbe Benutzer und derselbe Schlüssel. Derselbe SSH-Schlüssel kann für Bestands- und Leistungsdaten verwendet werden.
- Aktivieren Sie die Datenerfassung, indem Sie über SSH eine Verbindung zum SVC-Cluster herstellen und Folgendes ausführen: `svctask startstats -interval 1`

  Alternativ können Sie die Datenerfassung über die Benutzeroberfläche des SVC-Managements aktivieren.

#### Erläuterung der übergeordneten Seriennummer

Traditionell ist Insight in der Lage, die Seriennummer des Storage-Arrays oder die Seriennummern der einzelnen Storage-Nodes zu melden. Einige Storage-Array-Architekturen lassen sich diesem jedoch nicht ordnungsgemäß anpassen. Ein SVC-Cluster kann aus 1-4 Appliances bestehen, und jede Appliance verfügt über 2 Nodes. Wenn die Appliance selbst über eine Seriennummer verfügt, ist diese Seriennummer weder die Seriennummer für das Cluster noch für die Nodes.

Das Attribut „Parent Serial Number“ auf dem Speicher-Node-Objekt wird für IBM SVC-Arrays entsprechend aufgefüllt, wenn die einzelnen Knoten in einer Zwischenanwendung/einem Gehäuse sitzen, die nur Teil eines größeren Clusters ist.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Cluster-s-IP | IP-Adresse des vollständig qualifizierten Domänennamens für den SVC-Speicher |
| Wählen Sie „Kennwort“ oder „OpenSSH-Schlüsseldatei“, um den Anmeldeinformationstyp anzugeben | Der Anmeldetyp, der für die Verbindung mit dem Gerät über SSH verwendet wird |
| Benutzername Des Inventurbenutzers | Benutzername für die SVC-CLI |
| Inventurpasswort | Passwort für die SVC-CLI |
| Vollständiger Pfad zum privaten Bestandsschlüssel | Vollständiger Pfad zur Datei mit dem privaten Inventory-Schlüssel |
| Name Des Performance-Benutzers | Benutzername für die SVC-CLI für die Performance-Erfassung |
| Leistungspasswort | Kennwort für die SVC-CLI für die Performance-Erfassung |
| Vollständiger Pfad zum privaten Leistungsschlüssel | Vollständiger Pfad zur Datei mit dem privaten Leistungsschlüssel |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Geräte Ausschließen | Kommagetrennte Liste der Geräte-IDs, die von der Bestandserfassung ausgeschlossen werden sollen |

| | |
|---|---|
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 200 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Die Leistung Schließt Geräte Aus | Kommagetrennte Liste der Geräte-IDs, die von der Performance-Erfassung ausgeschlossen werden sollen |
| Performance SSH-Prozess Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 200 Sekunden) |
| Um dumpte Statistikdateien zu bereinigen | Wählen Sie diese Option, um die gespeicherten Statistikdateien zu bereinigen |

### Datenquelle von IBM Tivoli Monitoring

Diese Datenquelle wird ausschließlich zur Auslastung des Dateisystems verwendet. Sie kommuniziert direkt mit der Tivoli Monitoring Database, auch bekannt als Tivoli Monitoring Data Warehouse. Oracle- und DB2-Datenbanken werden unterstützt.

#### Oracle-Fehlermeldung

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht mehr verfügbar.

Wenn die angegebene SID zu der Fehlermeldung „ORA-12154“ beim Verbindungsversuch führt, überprüfen Sie die Konfiguration des Oracle DB-Netzwerkdienstes. Wenn die Zugriffskonfiguration einen vollständig qualifizierten Hostnamen angibt (z. B. „NAMES.DEFAULT_DOMAIN“), versuchen Sie, den vollständig qualifizierten Dienstnamen in das Feld SID einzufügen. Ein einfaches Beispiel wäre, dass die Verbindung zu SID `testdb` Ist fehlerhaft, und Ihre Oracle-Konfiguration gibt eine Domäne von an`company.com`. Der folgende String kann anstelle der Basis-SID verwendet werden, um eine Verbindung herzustellen: `testdb.company.com`.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Tivoli Monitoring Datenbank-IP | IP-Adresse oder vollständig qualifizierter Domänenname des Tivoli Monitoring-Servers |
| Benutzername | Benutzername für den Tivoli Monitoring-Server |
| Passwort | Kennwort für den Tivoli Monitoring-Server |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| Port Der Tivoli-Überwachungsdatenbank | Port, der für die Tivoli-Überwachungsdatenbank verwendet wird |
| Oracle SID oder DB2 Database Name | Oracle Listener-Dienst-ID oder DB2-Datenbankname |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Zu verwendenden Datenbanktreiber | Wählen Sie den zu verwendenden Datenbanktreiber aus |
| Protokoll für die Verbindung mit der Datenbank | Protokoll für die Verbindung mit der Datenbank |
| Datenbankschema | Geben Sie Das Datenbankschema Ein |

#### IBM TotalStorage DS4000 Datenquelle

Diese Datenquelle erfasst Bestands- und Leistungsinformationen. Es gibt zwei mögliche Konfigurationen (Firmware 6.x und 7.x+), und beide haben die gleichen Werte. Die API sammelt die Volume-Datenstatistiken.

##### Konfiguration

| Feld | Beschreibung |
|---|---|
| Kommagetrennte Liste der Array-SANtricity-Controller-IPs | IP-Adressen oder vollständig qualifizierte Domänennamen von Controllern, durch Kommas getrennt |

##### Anforderungen

- Die IP-Adresse jedes DS5- oder FAStT-Arrays
- Zugriffsvalidierung: Pingen Sie die IP-Adresse beider Controller auf jedem Array.

##### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 30 Minuten) |
| Leistungsintervall (bis zu 3600 Sekunden) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### IBM XIV-Datenquelle

Die IBM XIV (CLI)-Datenquelle wird über die XIV-Befehlszeilenschnittstelle inventarisiert.

# Die XIV-Leistung wird durch SMI-S-Aufrufe an das XIV-Array erreicht, das einen SMI-S-Provider auf Port 5989 ausführt.

#### Terminologie

OnCommand Insight erwirbt die folgenden Inventarinformationen aus der IBM XIV-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Festplatte | Festplatte |
| Storage-System | Storage |
| Storage-Pool | Storage-Pool |
| Datenmenge | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Port-Anforderung: TCP-Port 7778
- IP-Adresse der XIV-Verwaltungsschnittstelle
- Schreibgeschützter Benutzername und Kennwort
- Die XIV CLI muss auf dem Insight Server oder der rau installiert sein
- Zugriffsvalidierung: Melden Sie sich über den Insight Server bei der XIV-Benutzeroberfläche mit Benutzername und Passwort an.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| IP-Adresse | IP-Adresse oder vollständig qualifizierter Domänenname für den XIV-Speicher |
| Benutzername | Benutzername für den XIV Storage |
| Passwort | Passwort für den XIV-Speicher |
| Vollständiger Pfad zum XIV CLI-Verzeichnis | Vollständiger Pfad zum XIV CLI-Verzeichnis |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 40 Minuten) |
| Zeitüberschreitung bei CLI-Prozess (ms) | CLI-Prozess-Timeout (Standard: 7200000 ms) |
| SMI-S-HOST-IP | IP-Adresse des SMI-S Provider-Hosts |
| SMI-S-Port | Vom SMI-S Provider-Host verwendeter Port |
| SMI-S-Protokoll | Protokoll für die Verbindung mit dem SMI-S-Provider |
| SMI-S Namespace | SMI-S Namespace |
| Benutzername | Benutzername für den SMI-S Provider Host |
| Passwort | Kennwort für den SMI-S Provider-Host |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |
| Anzahl der erneuten SMI-S-Verbindungsversuche | Anzahl der Wiederholungsversuche für SMI-S-Verbindungen |

**Infinidat Infinibox Datenquelle**

Die Infinidat Infinidat Infinibox (HTTP) Datenquelle wird verwendet, um Informationen aus dem Infinidat Infinibox Speicher zu sammeln. Sie müssen Zugriff auf den Infinibox Management Node haben.

**Terminologie**

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der Infinibox-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Laufwerk | Festplatte |
| Infinibox | Storage |
| Knoten | Storage-Node |
| Pool | Storage-Pool |
| Datenmenge | Datenmenge |

| | |
|---|---|
| FC-Port | Port |
| Dateisystem | Internes Volumen |
| Dateisystem | Dateifreigabe |
| Dateisystem-Exporte | Share |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| InfiniBox Host | IP-Adresse oder vollqualifizierter Domainname des InfiniBox Management Node |
| Benutzername | Benutzername für InfiniBox Management Node |
| Passwort | Passwort für den InfiniBox Management-Knoten |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| TCP-Port | TCP-Port zur Verbindung mit Infinibox Server (Standard 443 ) |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Zeitüberschreitung Der Verbindung | Verbindungs-Timeout (Standard: 60 Sekunden) |

### Microsoft Azure Compute-Datenquelle

OnCommand Insights verwendet den Azure Computing-Datensammler, um Inventar- und Performance-Daten aus Azure Computing-Instanzen zu erfassen.

**Anforderungen**

Sie benötigen die folgenden Informationen, um diesen Datensammler zu konfigurieren:

- Port-Anforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Azure Service Principal Application (Client) ID (Benutzerkonto)

- Azure Service Principal Authentication Key (Benutzerkennwort)

Sie müssen ein Azure-Konto für die Insight Discovery einrichten. Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure-Instanz bei Insight zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten:https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

#### Konfiguration

Geben Sie Daten in die Datenquellenfelder gemäß der folgenden Tabelle ein:

| Feld | Beschreibung |
|---|---|
| Azure Service Principal Application (Client)-ID (Reader-Rolle erforderlich) | Anmelde-ID bei Azure. Erfordert Zugriff auf die Leserrolle. |
| Azure-Mandanten-ID | Microsoft Mandanten-ID |
| Authentifizierungsschlüssel Des Azure Service Principal | Anmeldeauthentifizierungsschlüssel |
| Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt | Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt. |

#### Erweiterte Konfiguration

Geben Sie Daten in die Datenquellenfelder gemäß der folgenden Tabelle ein:

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Der Standardwert ist 60 |
| Wählen Sie „exclude“ oder „include“, um VMs nach Tags zu filtern | Geben Sie an, ob VM’s by Tags beim Sammeln von Daten einbezogen oder ausgeschlossen werden sollen. Wenn ‘include’ ausgewählt ist, darf das Feld Tag Key nicht leer sein. |
| Markieren Sie Schlüssel und Werte, nach denen VMs gefiltert werden sollen | Klicken Sie auf **+ Filter Tag**, um die VMs (und die zugehörigen Festplatten) auszuwählen, die durch Filtern nach Schlüsseln und Werten, die Schlüssel und Werte von Tags auf der VM entsprechen, einzuschließen bzw. auszuschließen. Tag-Schlüssel erforderlich, Tag-Wert ist optional. Wenn der Tag-Wert leer ist, wird die VM solange gefiltert, wie sie dem Tag-Schlüssel entspricht. |
| Leistungsintervall (Sek. | Der Standardwert ist 300 |

### Azure NetApp Files Datenquelle

Diese Datenquelle erfasst Inventar- und Performance-Daten für Azure NetApp Files (ANF).

#### Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- Port-Anforderung: 443 HTTPS
- Azure Management Rest-IP (management.azure.com)
- Azure Service Principal Application (Client) ID (Benutzerkonto)
- Azure Service Principal Authentifizierungsschlüssel (Benutzerpasswort)
- Sie müssen ein Azure Konto für die Cloud Insights-Erkennung einrichten.

  Sobald das Konto ordnungsgemäß konfiguriert ist und Sie die Applikation in Azure registrieren, verfügen Sie über die erforderlichen Zugangsdaten, um die Azure Instanz mit Cloud Insights zu ermitteln. Über den folgenden Link wird beschrieben, wie Sie das Konto für die Ermittlung einrichten:

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Azure Service Principal Application (Client) ID | Anmelde-ID bei Azure |
| Azure Mandanten-ID | Azure Mandanten-ID |
| Authentifizierungsschlüssel Des Azure Service Principal | Anmeldeauthentifizierungsschlüssel |
| Ich verstehe, dass Microsoft mir API-Anforderungen in Rechnung stellt | Überprüfen Sie dies, um zu überprüfen, ob Microsoft Ihnen die durch eine Insight-Umfrage gestellten API-Anforderungen abrechnungen aufstellt. |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Der Standardwert ist 60 Minuten |

### Microsoft Hyper-V Datenquelle

Für die Konfiguration erfordert die Microsoft Hyper-V-Datenquelle die IP-Adresse oder den auflösbaren DNS-Namen für den physischen Host (Hypervisor). Diese Datenquelle verwendet PowerShell (zuvor WMI verwendet).

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus der Hyper-V-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Virtuelle Festplatte | Virtuelles Laufwerk |
| Host | Host |
| Virtual Machine | Virtual Machine |
| Cluster Shared Volumes (CSV), Partition Volume | Datastore |
| Internet SCSI-Gerät, Multi Path SCSI LUN | LUN |
| Fibre Channel-Port | Port |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Für die Hyper-V muss Port 5985 geöffnet sein, damit Daten erfasst und Remote-Zugriff/-Management erfolgen können.
- IP-Adresse des Knoten der Clustering-Gruppe
- Lokaler Administrator-Benutzer und Passwort auf dem Hypervisor
- Benutzerkonto auf Administratorebene
- Port-Anforderungen: Port 135 und dynamische TCP-Ports zugewiesen 1024-65535 für Windows 2003 und älter und 49152-65535 für Windows 2008.
- Die DNS-Auflösung muss erfolgreich sein, auch wenn der Datensammler nur auf eine IP-Adresse verweist.
- Für jeden Hyper-V Hypervisor muss „`Resource Metering`“ für jede VM auf jedem Host aktiviert sein. Dadurch kann jeder Hypervisor auf jedem Gast mehr Daten für Cloud Insights zur Verfügung stellen. Wenn diese Einstellung nicht festgelegt ist, werden für jeden Gast weniger Performance-Metriken erfasst. Weitere Informationen zur Ressourcenmessung finden Sie in der microsoft-Dokumentation:

  "Hyper-V Übersicht zur Ressourcenmessung"

  "Aktivieren-VMressourcenMetering"

#### Konfiguration

| Feld | Beschreibung |
|---|---|

| | |
|---|---|
| IP-Adresse des physischen Hosts | Die IP-Adresse oder der vollqualifizierte Domänenname für den physischen Host (Hypervisor). |
| Benutzername | Der Administrator-Benutzername wird vom Hypervisor verwendet |
| Passwort | Kennwort für den Hypervisor |
| NT-Domäne | Der von den Nodes im Cluster verwendete DNS-Name |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungs-Timeout (ms) | Verbindungs-Timeout (Standard: 60000 ms) |

### Datenquelle von NetApp Clustered Data ONTAP

Diese Datenquelle sollte für Storage-Systeme mit Clustered Data ONTAP verwendet werden. Sie erfordert ein Administratorkonto, das für schreibgeschützte API-Aufrufe verwendet wird.

#### Terminologie

OnCommand Insight erfasst die folgenden Inventarinformationen aus der Datenquelle von Clustered Data ONTAP. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| | |
|---|---|
| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| Festplatte | Festplatte |
| Raid-Gruppe | Festplattengruppe |
| Cluster | Storage |
| Knoten | Storage-Node |
| Aggregat | Storage-Pool |
| LUN | Datenmenge |

| | |
|---|---|
| Datenmenge | Internes Volumen |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Administratorkonto wird für schreibgeschützte API-Aufrufe verwendet
- Ziel-IP ist die LIF zum Cluster-Management
- Benutzername (mit schreibgeschütztem Rollenname zur ontapi-Applikation auf dem Standard-Vserver) und Passwort zur Anmeldung beim NetApp Cluster
- Port-Anforderungen: 80 oder 443
- Lizenzanforderungen: FCP-Lizenz und zugeordnete/maskierte Volumes, die für die Erkennung erforderlich sind

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| NetApp Management IP | IP-Adresse oder vollqualifizierter Domain-Name des NetApp Clusters |
| Benutzername | Benutzername für das NetApp Cluster |
| Passwort | Passwort für den NetApp Cluster |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### Clustered Data ONTAP Storage

## Bedingungen für Objekte oder Referenzen, die auf den Landing-Pages für NetApp Clustered Data ONTAP Storage-Assets möglicherweise zu finden sind.

### Clustered Data ONTAP – Storage-Terminologie

Die folgenden Begriffe gelten für Objekte oder Verweise, die auf den Landing Pages für NetApp Clustered Data ONTAP Storage-Ressourcen möglicherweise zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Model – Eine durch Kommas getrennte Liste der eindeutigen, diskreten Node-Modellnamen in diesem Cluster. Wenn alle Nodes in den Clustern denselben Modelltyp aufweisen, wird nur ein Modellname angezeigt.
- Vendor – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer — die Seriennummer des Arrays. Bei Storage-Systemen mit Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern „`Storage-Nodes`“.
- IP – im Allgemeinen sind die IP(s) oder Hostnamen (s) wie in der Datenquelle konfiguriert.
- Microcode-Version — Firmware.
- RAW Capacity — Basis 2 Summe aller physischen Festplatten im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der mit dem Host konfrontiert Workloads, sowohl bei Lese- als auch bei Schreibvorgängen. Idealerweise bezieht OCI diesen Wert direkt, ist aber oft nicht der Fall. Statt dieses Arrays anzubieten, führt OCI im Allgemeinen eine IOPS-gewichtete Berechnung aus den Statistiken der einzelnen internen Volumes` durch.
- Durchsatz – aggregiert von internen Volumes.
- Verwaltung – dieser kann einen Hyperlink für die Managementoberfläche des Geräts enthalten. Programmgesteuert von der Insight-Datenquelle als Teil der Bestandsberichterstattung erstellt.

#### Storage-Pool von Clustered Data ONTAP

## Bedingungen für Objekte oder Referenzen, die auf den Landing Pages für NetApp Clustered Data ONTAP Storage-Pool-Ressourcen möglicherweise zu finden sind.

### Clustered Data ONTAP – Terminologie für Storage-Pools

Die folgenden Begriffe gelten für Objekte oder Verweise, die auf den Landing Pages für NetApp Clustered Data ONTAP Storage-Pools möglicherweise zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ — ein beschreibender Wert aus einer Liste einer aufgezählten Liste von Möglichkeiten. Am häufigsten ist „`Aggregate`“ oder „`RAID-Gruppe`“`“.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicher-Node gehören, wird dessen Name hier als Hyperlink zur eigenen Landing Page angezeigt.
- Verwendet Flash Pool — Ja/Nein-Wert — werden in diesem SATA/SAS-basierten Pool SSDs zur Cache-Beschleunigung verwendet?
- Redundanz – RAID-Level oder Schutzschema. RAID_DP ist Dual-Parity, RAID_TP ist die dreifache Parität.
- Kapazität – die Werte hier sind die genutzte logische Kapazität, die nutzbare Kapazität und die logische Gesamtkapazität sowie der verwendete Prozentsatz.
- Überbelegte Kapazität – Wenn Sie mithilfe von Effizienztechnologien eine Gesamtmenge an Volume- oder internen Volume-Kapazitäten zugewiesen haben, die größer als die logische Kapazität des Speicherpools ist, dann ist der prozentuale Wert hier größer als 0 %.
- Snapshot – verwendete Snapshot-Kapazitäten und insgesamt, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität für Segmente reserviert, Bereiche ausschließlich für Snapshots. ONTAP in MetroCluster-Konfigurationen werden dies wahrscheinlich zeigen, während andere ONTAP-Konfigurationen weniger sind.

- Auslastung — ein Prozentwert, der den höchsten Prozentsatz der Festplattenauslastung anzeigt, der zur Kapazität dieses Speicherpools beiträgt. Die Festplattenauslastung steht nicht unbedingt in engem Zusammenhang mit der Array-Performance – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. hoch sein, wenn auf dem Host keine Workloads ausgeführt werden. Außerdem kann die Festplattenauslastung bei vielen`-Replikationsimplementierungen nicht als internes Volume oder Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität für diesen Speicherpool beisteuern.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die die Kapazität dieses Speicherpools beisteuern.

#### Storage-Node von Clustered Data ONTAP

## Bedingungen für Objekte oder Referenzen, die auf den Storage-Node-Ressourcen-Landing-Pages von NetApp Clustered Data ONTAP zu finden sind.

### Clustered Data ONTAP – Terminologie für Storage-Nodes

Die folgenden Begriffe gelten für Objekte oder Verweise, die auf den Landing Pages für NetApp Clustered Data ONTAP Storage-Pool-Ressourcen möglicherweise zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Storage – zu welchem Speicher-Array dieser Node gehört. Obligatorisch.
- HA Partner — auf Plattformen, bei denen ein Knoten auf einen und nur einen anderen Knoten umfunktioniert, wird er hier im Allgemeinen angezeigt.
- Status – Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Model – Modellname des Knotens.
- Version — Versionsname des Geräts.
- Seriennummer — die Seriennummer des Node.
- Speicher — Basis-2-Speicher, falls verfügbar.
- Auslastung: Bei ONTAP handelt es sich um einen Controller-Stress-Index eines proprietären Algorithmus. Bei jeder Performance-Umfrage wird anhand einer Zahl zwischen 0 und 100 % angegeben, die der höhere Wert bei WAFL-Festplattenkonflikten oder der durchschnittlichen CPU-Auslastung ist. Wenn Sie kontinuierliche Werte von > 50 % beobachten, ist das Anhaltspunkt dafür, dass die Größe nicht ausreichend ist – möglicherweise ist ein Controller/Node nicht groß genug oder nicht genug rotierende Festplatten, um den Schreib-Workload abzufangen.
- IOPS – direkt von ONTAP-ZAPI-Aufrufen auf dem Node-Objekt abgeleitet.
- Latenz – direkt von ONTAP-ZAPI-Aufrufen des Node-Objekts abgeleitet.
- Durchsatz — direkt von ONTAP-ZAPI-Aufrufen des Node-Objekts abgeleitet.
- Prozessoren – CPU-Anzahl.

### NetApp Clustered Data ONTAP für Unified Manager Datenquelle

## Diese Datenquelle erfasst ONTAP 8.1.x-Daten von der Unified Manager (um) 6.0+-Datenbank. Mithilfe dieser Datenquelle erkennt Insight alle in um konfigurierten und mit Daten befüllten Cluster. Zur Steigerung der Effizienz ruft Insight im Cluster selbst keine Zapis auf. Die Leistung wird in dieser Datenquelle nicht unterstützt.

#### Konfiguration

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht mehr verfügbar.

| Feld | Beschreibung |
|---|---|
| Unified Manager-IP | IP-Adresse oder vollständig qualifizierter Domain-Name von Unified Manager |
| Benutzername | Benutzername für Unified Manager |
| Passwort | Kennwort für den Unified Manager |
| Port | Port für die Kommunikation mit Unified Manager (Standard 3306) |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Intervall für Bestandsabfrage (min) | Intervall zwischen Bestandsabstimmungen (Standard: 15 Minuten) |
| Cluster Ausschließen | Kommagetrennte Liste der auszuschließenden Cluster-IPs |

### NetApp Data ONTAP Datenquelle in 7-Mode

Bei Storage-Systemen mit der Data ONTAP Software 7-Mode sollten Sie die ONTAPI Datenquelle verwenden, die zum Abrufen von Kapazitätsnummern die CLI verwendet.

#### Terminologie

OnCommand Insight erfasst die folgenden Inventarinformationen aus der NetApp Data ONTAP 7-Mode Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| | |
|---|---|
| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| Festplatte | Festplatte |
| Raid-Gruppe | Festplattengruppe |
| Filer | Storage |
| Filer | Storage-Node |

| | |
|---|---|
| Aggregat | Storage-Pool |
| LUN | Datenmenge |
| Datenmenge | Internes Volumen |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- IP-Adresse des FAS Storage Controllers und des Partners
- Port 443
- Benutzername und Passwort für den Controller und den Partner
- Ein benutzerdefinierter Benutzername und Passwort für den Admin-Level für den Controller und den Partner-Controller mit den folgenden Rollenfunktionen für 7-Mode:
  - „api-*“: Nutzen Sie diese, um OnCommand Insight die Ausführung aller NetApp Storage-API-Befehle zu ermöglichen.
  - „login-http-admin“: Hiermit kann OnCommand Insight über HTTP eine Verbindung mit dem NetApp Storage herstellen.
  - „Security-API-vfiler“: Nutzen Sie dies, um OnCommand Insight zu ermöglichen, NetApp Storage API Befehle auszuführen, um vFiler Einheitsinformationen abzurufen.
  - „cli-Optionen“: Hier können Sie Storage-Systemoptionen lesen.
  - „cli-lun“: Greifen Sie auf diese Befehle zum Verwalten von LUNs zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
  - „cli-df“: Verwenden Sie dies, um freien Speicherplatz anzuzeigen.
  - „cli-ifconfig“: Verwenden Sie diese, um Schnittstellen und IP-Adressen anzuzeigen.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Adresse des Filer | IP-Adresse oder vollqualifizierter Domänenname für den NetApp Filer |
| Benutzername | Benutzername für den NetApp Filer |
| Passwort | Passwort für den NetApp Filer |
| Adresse des HA Partner Filer im Cluster | IP-Adresse oder vollqualifizierter Domänenname für den HA-Partner Filer |
| Benutzername des HA Partner Filer in Cluster | Benutzername für den NetApp HA Partner Filer |

| | |
|---|---|
| Passwort des HA Partner Filer in Cluster | Passwort für den NetApp HA-Partner Filer |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungstyp | Wählen Sie den Verbindungstyp |
| Verbindungsport | Für NetApp API verwendeter Port |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

**Storage-Systemverbindung**

Als Alternative zur Verwendung des standardmäßigen administrativen Benutzers für diese Datenquelle können Sie einen Benutzer mit administrativen Rechten direkt auf den NetApp Storage-Systemen konfigurieren, damit diese Datenquelle Daten von NetApp Storage-Systemen erfassen kann.

Für die Verbindung zu NetApp Storage-Systemen muss der Benutzer, der beim Erwerb der Haupt-pfiler angegeben ist (auf dem das Speichersystem vorhanden ist), die folgenden Bedingungen erfüllen:

- Der Benutzer muss auf vfiler0 (root Filer/pfiler) sein.

  Storage-Systeme werden beim Erwerb der Haupt-Filer erworben.

- Mit den folgenden Befehlen werden die Fähigkeiten der Benutzerrolle definiert:
  - „api-*“: Nutzen Sie diese, um OnCommand Insight die Ausführung aller NetApp Storage-API-Befehle zu ermöglichen. Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.
  - „login-http-admin“: Hiermit kann OnCommand Insight über HTTP eine Verbindung mit dem NetApp Storage herstellen. Dieser Befehl ist erforderlich, um das ZAPI zu verwenden.
  - „Security-API-vfiler“: Nutzen Sie dies, um OnCommand Insight zu ermöglichen, NetApp Storage API Befehle auszuführen, um vFiler Einheitsinformationen abzurufen.
  - „cli-Opes“: Zum Befehl „Opes“, der für Partner-IP und aktivierte Lizenzen verwendet wird.
  - „ cli-lun“: Greifen Sie zum Verwalten von LUNs auf diesen Befehl zu. Zeigt den Status (LUN-Pfad, Größe, Online/Offline-Zustand und Shared-Zustand) der angegebenen LUN oder Klasse von LUNs an.
  - „cli-df“: Für „df -s“, „df -r“, „df -A -r“ und für die Anzeige des freien Speicherplatzes
  - „cli-ifconfig“: Für „ifconfig -a“ Befehl und verwendet für das Abrufen von Filer IP Adresse.
  - "cli-rdfile": Für den Befehl "rdfile /etc/netgroup" und für das Abrufen von Netzgruppen verwendet.
  - „cli-Datum“: Für den Befehl „Datum“ und mit dem vollständigen Datum für das Abrufen von Snapshot Kopien.
  - „cli-Snap“: Für den Befehl „Snap list“ und zum Abrufen von Snapshot Kopien verwendet.

Wenn cli-Datum oder cli-Snap Berechtigungen nicht bereitgestellt werden, kann die Erfassung abgeschlossen

werden. Snapshot Kopien werden jedoch nicht gemeldet.

Um eine 7-Mode Datenquelle erfolgreich zu erhalten und keine Warnungen auf dem Speichersystem zu generieren, sollten Sie eine der folgenden Befehlstrings verwenden, um Ihre Benutzerrollen zu definieren. Der zweite hier aufgeführte String ist eine optimierte Version des ersten:

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

#### NetApp E-Series Datenquelle

Die NetApp E-Series Datenquelle erfasst Informationen zum Bestand und zur Performance. Es gibt zwei mögliche Konfigurationen (Firmware 6.x und Firmware 7.x+), und beide haben die gleichen Werte.

##### Terminologie

OnCommand Insight erfasst die folgenden Inventarinformationen aus der NetApp E-Series Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Laufwerk | Festplatte |
| Volume-Gruppe | Festplattengruppe |
| Storage Array Durchführt | Storage |
| Controller | Storage-Node |
| Volume-Gruppe | Storage-Pool |
| Datenmenge | Datenmenge |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

##### Anforderungen

- Die IP-Adresse jedes Controllers im Array
- Port-Anforderung 2463

##### Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Kommagetrennte Liste der Array-SANtricity-Controller-IPs | IP-Adressen und/oder vollqualifizierte Domain-Namen für die Array Controller |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 30 Minuten) |
| Leistungsintervall (bis zu 3600 Sekunden) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### E-Series Storage

## Begriffe, die auf Objekte oder Referenzen angewendet werden, die auf Landing-Pages für Storage-Assets der NetApp E-Series möglicherweise zu finden sind.

### E-Series Storage-Terminologie

Die folgenden Begriffe gelten für Objekte oder Referenzen, die Sie auf den Landing Pages für Storage-Assets der NetApp E-Series finden können. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Model – Modellname des Geräts.
- Vendor – derselbe Anbietername, den Sie sehen würden, wenn Sie eine neue Datenquelle konfigurieren würden.
- Seriennummer — die Seriennummer des Arrays. Bei Storage-Systemen mit Cluster-Architektur wie NetApp Clustered Data ONTAP ist diese Seriennummer möglicherweise weniger nützlich als die einzelnen Seriennummern „`Storage-Nodes`“.
- IP – im Allgemeinen sind die IP(s) oder Hostnamen (s) wie in der Datenquelle konfiguriert.
- Microcode-Version — Firmware.
- RAW Capacity — Basis 2 Summe aller physischen Festplatten im System, unabhängig von ihrer Rolle.
- Latenz – eine Darstellung der mit dem Host konfrontiert Workloads, sowohl bei Lese- als auch bei Schreibvorgängen. Insight berechnet einen IOPS-gewichteten Durchschnitt aus den Volumes im Storage.
- Durchsatz – der gesamte für den Host bestimmte Durchsatz des Arrays. Insight summiert den Durchsatz der Volumes`, um diesen Wert abzuleiten.
- Verwaltung – dieser kann einen Hyperlink für die Managementoberfläche des Geräts enthalten. Programmgesteuert von der Insight-Datenquelle als Teil der Bestandsberichterstattung erstellt.

#### E-Series Storage-Pool

## Bedingungen für Objekte oder Referenzen, die auf den Landing Pages für Storage-Pools der NetApp E-Series möglicherweise zu finden sind.

### E-Series Storage Pool-Terminologie

Die folgenden Begriffe gelten für Objekte oder Verweise, die auf Landing Pages für Storage-Pools der NetApp E-Series möglicherweise zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Speicher – auf welchem Speicher-Array dieser Pool lebt. Obligatorisch.
- Typ — ein beschreibender Wert aus einer Liste einer aufgezählten Liste von Möglichkeiten. Am häufigsten ist „`Thin Provisioning`“ oder „`RAID Group`“.
- Node – Wenn die Architektur dieses Speicherarrays so ist, dass Pools zu einem bestimmten Speicher-Node gehören, wird dessen Name hier als Hyperlink zur eigenen Landing Page angezeigt.
- Verwendet Flash Pool — Ja/Nein-Wert.
- Redundanz – RAID-Level oder Schutzschema. E-Series Bericht „`RAID 7`“ für DDP-Pools
- Kapazität – die Werte hier sind die genutzte logische Kapazität, die nutzbare Kapazität und die logische Gesamtkapazität sowie der verwendete Prozentsatz. Zu diesen beiden Werten gehört die Kapazität „`konservierung`“ der E-Series, sodass sowohl die Zahlen als auch der prozentuale Anteil höher sind, als die Benutzeroberfläche der E-Series zeigen mag.
- Überbelegte Kapazität – Wenn Sie mithilfe von Effizienztechnologien eine Gesamtmenge von Volume-Kapazitäten zugewiesen haben, die größer ist als die logische Kapazität des Speicherpools, dann ist der prozentuale Wert hier größer als 0 %.
- Snapshot – verwendete Snapshot-Kapazitäten und insgesamt, wenn Ihre Speicherpoolarchitektur einen Teil ihrer Kapazität für Segmente reserviert, Bereiche ausschließlich für Snapshots.
- Auslastung – ein Prozentwert, der den höchsten Prozentsatz aller Festplatten anzeigt, die zur Kapazität dieses Speicherpools beitragen. Die Festplattenauslastung steht nicht unbedingt in engem Zusammenhang mit der Array-Performance – die Auslastung kann aufgrund von Festplattenwiederherstellungen, Deduplizierungsaktivitäten usw. hoch sein, wenn auf dem Host keine Workloads ausgeführt werden. Außerdem kann die Festplattenauslastung durch viele`-Replikationsimplementierungen nicht als Volume-Workload angezeigt werden.
- IOPS – die Summe der IOPS aller Festplatten, die Kapazität für diesen Speicherpool beisteuern.
- Durchsatz – der Gesamtdurchsatz aller Festplatten, die die Kapazität dieses Speicherpools beisteuern.

#### E-Series Storage-Node

## Begriffe, die auf Objekte oder Referenzen angewendet werden, die auf Landing-Pages für Storage-Nodes der NetApp E-Series möglicherweise zu finden sind.

### E-Series Storage-Node-Terminologie

Die folgenden Begriffe gelten für Objekte oder Verweise, die auf Landing Pages für Storage-Pools der NetApp E-Series möglicherweise zu finden sind. Viele dieser Bedingungen gelten auch für andere Datensammler.

- Storage – zu welchem Speicher-Array dieser Node gehört. Obligatorisch.
- HA Partner — auf Plattformen, bei denen ein Knoten auf einen und nur einen anderen Knoten umfunktioniert, wird er hier im Allgemeinen angezeigt.
- Status – Systemzustand des Node. Nur verfügbar, wenn das Array ordnungsgemäß genug ist, um von einer Datenquelle inventarisiert zu werden.
- Model – Modellname des Knotens.
- Version — Versionsname des Geräts.

- Seriennummer — die Seriennummer des Node.
- Speicher — Basis-2-Speicher, falls verfügbar.
- Auslastung – die Auslastung ist derzeit für die NetApp E-Series nicht verfügbar.
- IOPS – berechnet durch Zusammenfassung aller IOPS für Volumes, die ausschließlich zu diesem Knoten gehören.
- Latenz – eine Zahl, die die typische Host-Latenz oder Reaktionszeit auf diesem Controller darstellt. Insights berechnet einen gewichteten IOPS-Durchschnitt aus Volumes, die ausschließlich zu diesem Node gehören.
- Throughput: Eine Zahl, die den Host-gesteuerten Durchsatz auf diesem Controller darstellt. Berechnet durch Zusammenfassung des gesamten Durchsatzes für Volumes, die ausschließlich zu diesem Knoten gehören.
- Prozessoren – CPU-Anzahl.

#### NetApp Host und VM File Systems Datenquelle

Mithilfe der NetApp Host- und VM-Dateisystemquelle können Sie Details zum Filesystem und Storage-Ressourcenzuordnungen für alle Microsoft Windows Host- und VM-Dateisysteme (Virtual Machine) und für alle unterstützten Linux VMs (nur virtuell zugeordnete VMs) abrufen. Vorhanden im Insight-Server, die mit der konfigurierten Compute Resource Group (CRG) beschriftet werden.

##### Allgemeine Anforderungen

- Diese Funktion muss separat erworben werden.

  Wenden Sie sich an Ihren Insight-Ansprechpartner, um Unterstützung zu erhalten.

- Überprüfen Sie bitte die Supportmatrix von Insight, um sich zu vergewissern, dass Ihr Host oder das Betriebssystem Ihrer Virtual Machine unterstützt wird.

  Um zu überprüfen, ob Verknüpfungen zwischen Dateisystemen und Speicherressourcen erstellt werden, prüfen Sie, ob der betreffende Speicher- oder Virtualisierungsanbietertyp und die Version die erforderlichen Identifikationsdaten für das Volume oder die virtuellen Laufwerke melden.

##### Anforderungen Für Microsoft Windows

- Diese Datenquelle verwendet WMI-Datenstrukturen (Window Management Instrumentation), um Daten abzurufen.

  Dieser Service muss betriebsbereit sein und Remote verfügbar sein. Insbesondere muss Port 135 zugänglich sein und geöffnet werden, wenn hinter einer Firewall.

- Windows-Domänenbenutzer müssen über die entsprechenden Berechtigungen verfügen, um auf WMI-Strukturen zuzugreifen.
- Administratorberechtigungen sind erforderlich.
- Dynamische TCP-Ports, die 1024-65535 für Windows 2003 und älter zugewiesen sind
- Ports 49152—65535 für Windows 2008

Wenn Sie versuchen, eine Firewall zwischen Insight, einer AU und dieser Datenquelle zu verwenden, sollten Sie Ihr Microsoft Team konsultieren, um die Ports zu identifizieren, von denen sie glauben, dass sie erforderlich sind.

**Linux-Anforderungen**

- Diese Datenquelle verwendet eine SSH-Verbindung (Secure Shell) zur Ausführung von Befehlen auf Linux VMs.

  Der SSH-Service muss betriebsbereit sein und Remote verfügbar sein. Insbesondere muss Port 22 zugänglich sein und geöffnet werden, wenn hinter einer Firewall.

- SSH-Benutzer müssen über sudo-Berechtigungen verfügen, um schreibgeschützte Befehle auf Linux-VMs auszuführen.

  Sie müssen dasselbe Passwort verwenden, um sich bei SSH anzumelden und jede Sudo-Kennwortherausforderung zu beantworten.

**Nutzungsempfehlungen**

- Sie sollten eine Gruppe von Hosts und virtuellen Maschinen mit gemeinsamen Betriebssystemanmeldeinformationen mit derselben Anmerkung zu Compute Resource Group versehen.

  Jede Gruppe verfügt über eine Instanz dieser Datenquelle, die Dateisystemdetails von diesen Hosts und virtuellen Maschinen ermittelt.

- Wenn Sie eine Instanz dieser Datenquelle haben, für die die Erfolgsrate niedrig ist (z. B. ermittelt OnCommand Insight Dateisystemdetails für nur 50 von 1000 Hosts und virtuelle Maschinen in einer Gruppe), Sie sollten die Hosts und virtuellen Maschinen, für die die Erkennung erfolgreich war, in eine separate Compute Resource Group verschieben.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| Benutzername | Betriebssystembenutzer mit den entsprechenden Rechten zum Abrufen von Dateisystemdaten für Windows-Betriebssystembenutzer muss das Domänenpräfix enthalten. |
| Passwort | Passwort für den Betriebssystembenutzer |
| Rechnerressourcengruppe | Der Anmerkungswert, der zum Markieren von Host- und virtuellen Maschinen für die Datenquelle verwendet wird, erkennt Dateisysteme.Ein leerer Wert gibt an, dass die Datenquelle Dateisysteme für alle Hosts und virtuellen Maschinen erkennt, die derzeit nicht mit einer Compute Resource Group beschriftet sind. |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 360 Minuten) |

### NetApp SolidFire Datenquelle

Die NetApp SolidFire Datenquelle unterstützt sowohl iSCSI- als auch Fibre Channel SolidFire-Konfigurationen für Bestandsaufnahme- und Performance-Erfassung.

Die SolidFire Datenquelle verwendet die SolidFire REST API. Die Erfassungseinheit, in der sich die Datenquelle befindet, muss HTTPS-Verbindungen zu TCP-Port 443 an der SolidFire-Cluster-Management-IP-Adresse initiieren können. Die Datenquelle benötigt Zugangsdaten, die REST API-Abfragen auf dem SolidFire-Cluster ermöglichen.

#### Terminologie

OnCommand Insight bezieht die folgenden Inventarinformationen aus der NetApp SolidFire Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| --- | --- |
| Laufwerk | Festplatte |
| Cluster | Storage |
| Knoten | Storage-Node |
| Datenmenge | Datenmenge |
| Fibre Channel-Port | Port |
| Volume Access Group, LUN-Zuweisung | Volume-Zuordnung |
| ISCSI-Sitzung | Volume-Maske |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- Management Virtual IP-Adresse
- Port 443

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| Management Virtual IP-Adresse (MVIP) | Management-virtuelle IP-Adresse des SolidFire-Clusters |
| Benutzername | Name, der zur Anmeldung im SolidFire Cluster verwendet wird |
| Passwort | Passwort, das zur Anmeldung beim SolidFire Cluster verwendet wird |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| TCP-Port | TCP-Port zur Verbindung mit dem SolidFire-Server (Standard 443 ) |
| Verbindungs-Timeout (s) | Verbindungs-Timeout (Standard: 60 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### Fehlerbehebung

Wenn SolidFire einen Fehler meldet, wird er in OnCommand Insight wie folgt angezeigt:

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

Wo?

- Die ←Methode> ist eine HTTP-Methode, z. B. GET oder PUT.
- Der <parameterString> ist eine kommagetrennte Liste von Parametern, die im REST-Aufruf enthalten waren.
- Die Meldung <message> ist das Gerät, das als Fehlermeldung zurückgegeben wurde.

### NetApp StorageGRID Datenquelle

Diese Datenquelle erfasst Inventar- und Performance-Daten für StorageGRID.

#### Anforderungen

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- StorageGRID-Host-IP-Adresse
- Ein Benutzername und ein Passwort für einen Benutzer, dem die Rollen Metric Query und Tenant Access zugewiesen sind
- Port 443

#### Konfiguration

| Feld | Beschreibung |
| --- | --- |
| StorageGRID-Host-IP-Adresse (MVIP) | Host-IP-Adresse des StorageGRID |
| Benutzername | Name, der für die Anmeldung bei der StorageGRID verwendet wird |
| Passwort | Passwort für die Anmeldung beim StorageGRID |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abfragen (Standard: 900 Sekunden) |

### OpenStack Datenquelle

Die OpenStack Datenquelle (REST API / KVM) erfasst Informationen zu OpenStack Hardware-Instanzen. Diese Datenquelle erfasst Inventardaten für alle OpenStack Instanzen sowie optional VM Performance-Daten.

#### Anforderungen

Folgende Anforderungen gelten für die Konfiguration der OpenStack Datenquelle.

- IP-Adresse des OpenStack Controllers
- Es werden Anmeldeinformationen für die OpenStack Admin-Rolle und sudo-Zugriff auf den Linux KVM-Hypervisor empfohlen.

> Wenn Sie kein Administratorkonto oder Administratorrechte verwenden, können Sie dennoch Daten aus der Datenquelle abrufen. Sie müssen die Richtlinienkonfigurationsdatei ändern (z. B. etc/Nova/Policy.json), damit Benutzer mit nicht-Admin-Rolle die API aufrufen können:

- „os_Compute_API:os-Availability-Zone:Detail“: „“
- „os_Compute_API:os-Hypervisoren“: „“
- os_Compute_API:Server:Detail:get_all_Tenants“: „“

- Für die Performance-Erfassung muss das OpenStack Ceilometer Modul installiert und konfiguriert sein. Die Konfiguration des Ceilometers erfolgt durch Bearbeiten des `nova.conf` Datei für jeden Hypervisor und starten Sie dann den Nova Compute Service auf jedem Hypervisor neu. Die Optionsnamen ändern sich für verschiedene OpenStack Versionen:
  - Icehouse
  - Juno
  - Kilo
  - Freiheit
  - Mitaka
  - Newton
  - Kata
- Für CPU-Statistiken muss "Compute_Monitors=ComputeDriverCPUMonitor" in /etc/Nova/Nova.conf auf Compute-Knoten aktiviert sein.
- Port-Anforderungen:
  - 5000 für http und 13000 für https, für den Keystone Service
  - 22 für KVM SSH
  - 8774 für Nova Compute Service
  - 8776 für Cinder Block Service
  - 8777 für den Ceilometer Performance Service
  - 9292 für Glance Image Service

Der Port bindet an den spezifischen Dienst, und der Dienst kann auf dem Controller oder einem anderen Host in größeren Umgebungen ausgeführt werden.

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| OpenStack-Controller-IP-Adresse | IP-Adresse oder vollqualifizierter Domain-Name des OpenStack Controllers |
| OpenStack Administrator | Benutzername für einen OpenStack Admin |
| OpenStack Passwort | Passwort, das für den OpenStack Admin verwendet wird |
| OpenStack Administrator-Mandant | OpenStack Administrator-Mandant |
| KVM-Sudo-Benutzer | KVM sudo Benutzername |

| | |
|---|---|
| Wählen Sie „Kennwort“ oder „OpenSSH-Schlüsseldatei“, um den Anmeldeinformationstyp anzugeben | Der Anmeldetyp, der für die Verbindung mit dem Gerät über SSH verwendet wird |
| Vollständiger Pfad zum privaten Bestandsschlüssel | Vollständiger Pfad zum privaten Bestandsschlüssel |
| KVM-Sudo-Kennwort | KVM-Sudo-Kennwort |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Aktivieren der Erkennung des Hypervisor-Inventars über SSH | Aktivieren Sie diese Option, um die Erkennung des Hypervisor-Inventars über SSH zu aktivieren |
| OpenStack Admin-URL-Port | OpenStack Admin-URL-Port |
| Verwenden Sie HTTPS | Überprüfen Sie, ob sicheres HTTP verwendet wird |
| HTTP-Verbindungszeitlimit (Sek.) | Timeout für HTTP-Verbindung (Standard: 300 Sekunden) |
| SSH-Port | Port, der für SSH verwendet wird |
| SSH-Prozess-Wartezeit (Sek.) | SSH-Prozess-Timeout (Standard: 30 Sekunden) |
| SSH-Prozess wird erneut ausgeführt | Anzahl der Versuche für einen erneuten Versuch in der Bestandsaufnahme |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |

### Oracle ZFS-Datenquelle

Die Oracle ZFS-Datenquelle unterstützt die Bestands- und Performanceerfassung.

#### Terminologie

OnCommand Insight erfasst die folgenden Bestandsinformationen aus dieser Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| | |
|---|---|
| Anbieter-/Modelllaufzeit | Insight Laufzeit |
| Festplatte (SDD) | Festplatte |
| Cluster | Storage |

| | |
|---|---|
| Controller | Storage-Node |
| LUN | Datenmenge |
| LUN-Zuordnung | Volume-Zuordnung |
| Initiator, Ziel | Volumenmaske |
| Share | Internes Volumen |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

Für die Konfiguration dieser Datenquelle gelten folgende Anforderungen:

- Host-Namen für den ZFS-Controller-1 und den ZFS-Controller-2
- Benutzername und Anmeldeinformationen des Administrators
- Port-Anforderung: 215 HTTP/HTTPS

**Konfiguration**

| | |
|---|---|
| ZFS Controller-1-Hostname | Host Name für Storage Controller 1 |
| ZFS Controller-2-Hostname | Host-Name für Storage Controller 2 |
| Benutzername | Benutzername für das Benutzerkonto des Speichersystemadministrators |
| Passwort | Kennwort für das Administratorbenutzerkonto |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| TCP-Port | TCP-Port zur Verbindung mit ZFS (Standard 215 ) |
| Verbindungstyp | HTTP oder HTTPS |
| Abfrageintervall für den Bestand | Intervall für Bestandsabfrage (Standard: 60 Minuten) |
| Zeitüberschreitung Der Verbindung | Der Standardwert ist 60 Sekunden |

| | |
|---|---|
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

#### Fehlerbehebung

Einige Dinge zu versuchen, wenn Sie Probleme mit diesem Datensammler stoßen:

| Problem: | Versuchen Sie Das: |
|---|---|
| „Ungültige Anmeldeinformationen“ | ZFS-Benutzerkonto und -Passwort validieren |
| „Konfigurationsfehler“ mit der Fehlermeldung „`REST-Service ist deaktiviert`“ | Vergewissern Sie sich, dass DER REST-Dienst auf diesem Gerät aktiviert ist. |
| „Konfigurationsfehler “ mit der Fehlermeldung „`Benutzer nicht autorisiert für Befehl`“ | Wahrscheinlich aufgrund bestimmter Rollen (z. B. 'Advanced_Analytics') sind für den konfigurierten Benutzer <userName> nicht enthalten.Mögliche Lösung:<br>• Korrigieren Sie den Bereich Analytics (Statistik) für den Benutzer €{user} mit der nur-Lese-Rolle:- Setzen Sie auf dem Bildschirm Configuration → Users die Maus über die Rolle und doppelklicken Sie, um die Bearbeitung zu ermöglichen<br>• Wählen Sie im Dropdown-Menü „Bereich“ die Option „Analyse“ aus. Eine Liste der möglichen Eigenschaften wird angezeigt.<br>• Klicken Sie auf das oberste Kontrollkästchen und es werden alle drei Eigenschaften ausgewählt.- Klicken Sie auf die Schaltfläche Hinzufügen auf der rechten Seite.<br>• Klicken Sie oben rechts im Popup-Fenster auf die Schaltfläche Übernehmen. Das Popup-Fenster wird geschlossen. |

### Pure Storage FlashArray Datenquelle

Die Datenquelle „Pure Storage FlashArray (HTTP)“ wird verwendet, um Informationen vom Pure Storage Flash Array zu erfassen. Insight unterstützt sowohl die Bestandsaufnahme als auch die Performance-Sammlung.

#### Terminologie

OnCommand Insight erfasst die folgenden Inventarinformationen aus der Datenquelle „Pure Storage FlashArray“. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|

| | |
|---|---|
| Laufwerk (SSD) | Festplatte |
| Array Erledigen | Storage |
| Controller | Storage-Node |
| Datenmenge | Datenmenge |
| Port | Port |
| LUN-Zuordnung (Host, Host-Gruppe, Ziel-Port) | Volume Map, Volume Mask |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

**Anforderungen**

- IP-Adresse des Storage-Systems
- Benutzername und Kennwort für das Administratorkonto des Pure Storage-Systems.
- Port-Anforderung: HTTP/HTTPS 80/443

**Konfiguration**

| Feld | Beschreibung |
|---|---|
| FlashArray Host | IIP-Adresse oder vollständig qualifizierter Domänenname des FlashArray Management Server |
| Benutzername | Benutzername für den FlashArray Management Server |
| Passwort | Passwort für den FlashArray Management Server |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
|---|---|
| Verbindungstyp | Management Server |
| TCP-Port | TCP-Port zur Verbindung mit FlashArray Server (Standard 443 ) |
| Verbindungs-Timeout (s) | Verbindungs-Timeout (Standard: 60 Sekunden) |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 60 Minuten) |

| | |
|---|---|
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (Standard: 300 Sekunden) |

#### Datenquelle von QLogic FC Switch

Für die Konfiguration erfordert die QLogic FC Switch (SNMP) Datenquelle die Netzwerkadresse für das FC Switch-Gerät, die als IP-Adresse angegeben ist, und eine SNMP *Read-Only* Community-Zeichenfolge, die für den Zugriff auf das Gerät verwendet wird.

##### Konfiguration

| Feld | Beschreibung |
|---|---|
| SANsurfer-Switch | IP-Adresse oder vollständig qualifizierter Domänenname für den SANsurfer-Switch |
| SNMP-Version | SNMP-Version |
| SNMP-Community | SNMP-Community-Zeichenfolge |
| Benutzername | Benutzername für den SANsurfer Switch |
| Passwort | Passwort für den SANsurfer-Switch |

##### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 15 Minuten) |
| SNMP-Auth-Protokoll | SNMP-Authentifizierungsprotokoll (nur SNMPv3) |
| SNMP wird erneut verwendet | Anzahl der SNMP-Wiederholungsversuche |
| SNMP-Timeout (ms) | SNMP-Timeout (Standard 5000 ms) |
| Trapping Aktivieren | Wählen Sie diese Option, um das Überfüllen zu aktivieren |
| Mindestzeit zwischen Traps (s) | Mindestzeit zwischen durch Traps ausgelösten Erfassungsversuchen (Standard: 10 Sekunden) |

| | |
|---|---|
| Fabric-Name | Fabric-Name, der von der Datenquelle gemeldet werden soll. Lassen Sie das Feld leer, um den Fabric-Namen als WWN zu melden. |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

### Red hat (RHEV) Datenquelle

Die Red hat Enterprise Virtualization (REST)-Datenquelle sammelt Informationen über RHEV-Instanzen über HTTPS.

#### Anforderungen

- IP-Adresse des RHEV-Servers über Port 443 über REST-API
- Nur-Lese-Benutzername und Kennwort
- RHEV Version 3.0+

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| RHEV-Server-IP-Adresse | IP-Adresse oder vollständig qualifizierter Domänenname des RHEV-Servers |
| Benutzername | Benutzername für den RHEV-Server |
| Passwort | Für den RHEV-Server verwendetes Passwort |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| HTTPS-Kommunikationsschnittstelle | Port, der für die HTTPS-Kommunikation mit RHEV verwendet wird |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungs-Timeout (Sek.) | Verbindungs-Timeout (Standard: 60 Sekunden) |

### Datenquelle von Violin Flash Memory Array

Die Datenquelle des Flash Memory Array (HTTP) von Violin 6000-Series erfasst Netzwerkinformationen für die Analyse und Validierung von Flash-Speicher-Arrays der Violin 6000-Series.

#### Terminologie

Dieser Datensammler ist ab OnCommand Insight 7.3.11 nicht mehr verfügbar.

OnCommand Insight erfasst die folgenden Inventarinformationen aus der Datenquelle des Flash-Speicher-Arrays der Violin 6000-Serie. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Violin Intelligent Memory Module (VIMM) | Festplatte |
| Container | Storage |
| Speicher-Gateway | Storage-Node |
| LUN | Datenmenge |
| Initiator, Initiatorgruppe, Ziel | Volume Map, Volume Mask |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- Sie benötigen einen schreibgeschützten Benutzernamen und ein Kennwort für den Speicher.
- Validieren Sie den Zugriff über einen Webbrowser unter Verwendung der Storage-IP-Adresse.

#### Konfiguration

| Feld | Beschreibung |
|---|---|
| IP-Adresse oder FQDN des Hauptgateways des Violin Memory Array | IP-Adresse oder vollständig qualifizierter Domänenname des Haupt-Gateways des Violin Memory Array |
| Benutzername | Benutzername für das Haupt-Gateway des Violin Memory Array |
| Passwort | Passwort für das Haupt-Gateway des Violin Memory Array |

#### Erweiterte Konfiguration

| Feld | Beschreibung |
|---|---|
| Kommunikations-Port | Port für die Kommunikation mit Violin Array |

| | |
|---|---|
| HTTPS aktiviert | Wählen Sie aus, um HTTPS zu verwenden |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungs-Timeout (Sek.) | Verbindungs-Timeout (Standard: 60 Sekunden) |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

**VMware vSphere Datenquelle**

## Die Datenquelle „VMware vSphere (Web Services)“ sammelt ESX-Host-Informationen und erfordert Berechtigungen für alle Objekte im Virtual Center.

#### Terminologie

OnCommand Insight bezieht die folgenden Inventarinformationen aus der VMware vSphere-Datenquelle. Für jeden von Insight erworbenen Asset-Typ wird die für dieses Asset am häufigsten verwendete Terminologie angezeigt. Beachten Sie bei der Anzeige oder Fehlerbehebung dieser Datenquelle die folgende Terminologie:

| Anbieter-/Modelllaufzeit | Insight Laufzeit |
|---|---|
| Virtuelles Laufwerk | Festplatte |
| Host | Host |
| Virtual Machine | Virtual Machine |
| Datastore | Datastore |
| LUN | LUN |
| Fibre Channel-Port | Port |

Es handelt sich dabei nur um gängige Terminologiezuordnungen, die für diese Datenquelle möglicherweise nicht alle Fälle darstellen.

#### Anforderungen

- IP-Adresse des Virtual Center-Servers
- Schreibgeschützter Benutzername und Kennwort in Virtual Center
- Schreibgeschützte Berechtigungen für alle Objekte im Virtual Center.
- SDK-Zugriff auf dem Virtual Center-Server
- Port-Anforderungen: http-80 HTTPS-443

- Überprüfen Sie den Zugriff, indem Sie sich mit Ihrem Benutzernamen und Kennwort beim Virtual Center Client anmelden und überprüfen, ob das SDK aktiviert ist, indem Sie eingeben `telnet <vc_ip\> 443`.

**Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Virtual Center-Adresse | Netzwerkadresse für den Virtual Center- oder vSphere-Server, angegeben als IP *(nnn.nnn.nnn.nnn* Format)-Adresse oder als Hostname, der über DNS aufgelöst werden kann. |
| Benutzername | Benutzername für den VMware-Server. |
| Passwort | Kennwort für den VMware-Server. |

**Erweiterte Konfiguration**

| Feld | Beschreibung |
| --- | --- |
| Abfrageintervall für Bestand (min) | Intervall zwischen Bestandsabstimmungen (Standard: 20 Minuten) |
| Verbindungs-Timeout (ms) | Verbindungs-Timeout (Standard: 60000 ms) |
| Filtern von VMs nach | Wählen Sie aus, wie VMs gefiltert werden sollen |
| Wählen Sie „Ausschließen“ oder „Einschließen“, um eine Liste anzugeben | Geben Sie an, ob die VM-Liste unten bei der Datenerfassung ein- oder ausgeschlossen werden soll |
| Liste der zu filternden VMs (durch Komma getrennt oder durch Semikolon getrennt, wenn im Wert Komma verwendet wird) | Kommagetrennte oder durch Semikolon getrennte Liste von VMs, die ein- oder vom Abruf ausgeschlossen werden sollen |
| Anzahl der Wiederholungen für Anfragen an vCenter | Anzahl der erneuten Versuche der vCenter-Anforderung |
| Kommunikations-Port | Für VMware-Server verwendeter Port |
| Leistungsintervall (Sek.) | Intervall zwischen Performance-Abstimmungen (standardmäßig 300 Sekunden) |

## Die Anmeldedaten der Datenquelle werden geändert

Wenn mehrere Datenquellen desselben Typs einen Benutzernamen und ein Kennwort gemeinsam nutzen, können Sie das Kennwort für alle Geräte in der Gruppe gleichzeitig ändern.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.

   Die Liste **Datenquellen** wird geöffnet.

2. Klicken Sie auf die Schaltfläche **actions** und wählen Sie die Option **Change credentials**.
3. Wählen Sie im Dialogfeld Credentials Management eine der Datenquellgruppen aus der Liste aus.

   Das Symbol Bearbeiten, ein Stift auf einem Blatt Papier, wird rechts aktiviert.

4. Klicken Sie Auf **Bearbeiten**.
5. Geben Sie das neue Passwort ein und bestätigen Sie es.

## Änderungen, die zu Datenerfassungsproblemen führen

Wenn bei OnCommand Insight Probleme mit der Datenerfassung auftreten, sind Änderungen in Ihrer Umgebung wahrscheinlich die Ursache. Als allgemeine Wartungsregel sollten Sie alle Änderungen in Ihrer Umgebung auch in Insight berücksichtigen.

Mithilfe dieser Checkliste können Sie Änderungen an Ihrem Netzwerk identifizieren, die möglicherweise Probleme verursachen:

- Haben Sie Passwörter geändert? Wurden diese Passwörter in Insight geändert?
- Haben Sie ein Gerät aus Ihrem Netzwerk entfernt? Sie müssen das Gerät auch aus OnCommand Insight entfernen, um zu verhindern, dass es erneut erkannt und wieder eingeführt wird.
- Haben Sie die Infrastruktursoftware (wie HP CommandView EVA oder EMC Solutions Enabler) aktualisiert?

  Stellen Sie sicher, dass die entsprechenden Versionen der Client-Tools auf der Erfassungseinheit installiert sind. Wenn die Datenquelle weiterhin Fehler macht, müssen Sie sich an den technischen Support wenden, um Unterstützung und möglicherweise einen Patch für die Datenquelle anzufordern.

- Verwenden alle Ihre OnCommand Insight-Akquisitionseinheiten die gleiche OnCommand Insight-Version? Wenn die Remote-Erfassungseinheiten und die lokale Erfassungseinheit verschiedene OnCommand Insight-Versionen ausführen, installieren Sie dieselbe Version auf allen Geräten, um das Problem mit der Datenerfassung zu beheben.

  Wenn Sie eine neue Version von OnCommand Insight auf allen Akquisitionseinheiten installieren müssen, gehen Sie zur Support-Website und laden Sie die korrekte Version herunter.

- Haben Sie Domain-Namen geändert oder eine neue Domain hinzugefügt? Sie müssen die Methoden für die Geräteauflösung (früher automatische Auflösung) aktualisieren.

## Eine Datenquelle im Detail untersuchen

Wenn Sie feststellen, dass eine Datenquelle fehlgeschlagen oder verlangsamt ist, sollten Sie eine detaillierte Zusammenfassung der Informationen für diese Datenquelle prüfen, um die Ursache des Problems zu ermitteln. Datenquellen mit Bedingungen, die Ihre Aufmerksamkeit erfordern, sind mit einem durchgehenden roten Kreis gekennzeichnet.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.

   Die Liste **Datenquellen** wird geöffnet. Alle aufgelisteten Datenquellen mit potenziellen Problemen sind mit einem durchgehenden roten Kreis gekennzeichnet. Die schwerwiegendsten Probleme stehen ganz oben auf der Liste.

2. Wählen Sie die Datenquelle aus, die Bedenken auslöst.
3. Klicken Sie auf den Link Name der Datenquelle.
4. Überprüfen Sie auf der Seite Datenquellenzusammenfassung die Informationen in einem der folgenden Abschnitte:
   - **Zeitachse des Events**

     Listet Ereignisse auf, die mit dem aktuellen Status in der Liste Datenquellen verknüpft sind. Ereignisse in dieser Zusammenfassung werden pro Gerät angezeigt. Fehler werden rot angezeigt. Sie können Ihren Mauszeiger auf Zeitachsenelemente positionieren, um zusätzliche Informationen anzuzeigen.

   - **Von dieser Datenquelle gemeldete Geräte**

     Listet die Gerätetypen, ihre IP-Adressen und Links zu detaillierteren Informationen für jedes Gerät auf.

   - **Änderungen, die von dieser Datenquelle gemeldet werden (letzte 3 Wochen)**

     Listet alle Geräte auf, die hinzugefügt oder entfernt wurden oder an der Konfiguration geändert wurden.

5. Nach der Untersuchung der Datenquellinformationen sollten Sie eine dieser Vorgänge mithilfe der Schaltflächen oben auf der Seite ausführen:
   - **Bearbeiten** die Beschreibung der Datenquelle, um das Problem zu beheben.
   - **Erneut abfragen** zwingt die Umfrage, um zu erkennen, ob das Problem andauernd oder intermittierend war.
   - *Datenquellenabfrage für 3, 7 oder 30 Tage verschieben, um Ihnen Zeit zu geben, das Problem zu untersuchen und die Warnmeldungen zu stoppen.
   - **Installieren Sie einen Patch** auf der Datenquelle, um das Problem zu beheben.
   - Bereiten Sie einen **Fehlerbericht** für den technischen Support vor.
   - **Löschen** der Datenquelle aus Ihrer Insight Monitoring-Umgebung.

## Suche nach einer fehlerhaften Datenquelle

Wenn eine Datenquelle die Meldung **"Inventory failed !"** oder **"Performance failed !"** und eine hohe oder mittlere Auswirkung hat, müssen Sie dieses Problem mithilfe der Datenquellenzusammenfassung mit ihren verknüpften Informationen untersuchen.

**Schritte**

1. Klicken Sie auf den verknüpften **Name** der Datenquelle, um die Übersichtsseite zu öffnen.
2. Lesen Sie auf der Übersichtsseite im Bereich **Kommentare** alle Notizen, die von einem anderen Techniker hinterlassen wurden, der möglicherweise auch diesen Fehler untersucht.
3. Notieren Sie alle Leistungsmeldungen.
4. Wenn ein Patch auf diese Datenquelle angewendet wird, klicken Sie auf den Link, um die Seite **Patch** zu überprüfen, um zu sehen, ob dies das Problem verursacht hat.
5. Bewegen Sie den Mauszeiger über die Segmente des Diagramms **Event Timeline**, um zusätzliche Informationen anzuzeigen.
6. Wählen Sie eine Fehlermeldung für ein Gerät aus, die unter der Ereigniszeitleiste angezeigt wird, und klicken Sie auf das Symbol **Fehlerdetails**, das rechts neben der Meldung angezeigt wird.

   Die Fehlerdetails enthalten den Text der Fehlermeldung, die wahrscheinlichsten Ursachen, die verwendeten Informationen und Vorschläge, was versucht werden kann, das Problem zu beheben.

7. Im Bereich Geräte, die von dieser Datenquelle gemeldet werden, können Sie die Liste so filtern, dass nur Geräte von Interesse angezeigt werden, und Sie können auf den verknüpften **Name** eines Geräts klicken, um die *Asset-Seite* für dieses Gerät anzuzeigen.
8. Um zu den zuvor angezeigten Seiten zurückzukehren, verwenden Sie eine der folgenden Methoden:
   - Klicken Sie auf den Zurück-Pfeil des Browsers.
   - Klicken Sie mit der rechten Maustaste auf den Zurück-Pfeil, um eine Liste der Seiten anzuzeigen und die gewünschte Seite auszuwählen.
9. Um detaillierte Informationen zu anderen Ressourcen anzuzeigen, klicken Sie auf andere verknüpfte Namen.
10. Wenn Sie zur Datenquellübersicht zurückkehren, überprüfen Sie im Bereich **changes** unten auf der Seite, ob die letzten Änderungen das Problem verursacht haben.

## Steuerung der Datenquellabfrage

Nachdem Sie eine Änderung an einer Datenquelle vorgenommen haben, möchten Sie möglicherweise, dass diese sofort abgefragt wird, um Ihre Änderungen zu überprüfen, oder Sie möchten die Datenerfassung in einer Datenquelle für einen, drei oder fünf Tage verschieben, während Sie an einem Problem arbeiten.

**Schritte**

1. Klicken Sie auf **Admin** und navigieren Sie zur Ansicht der Datenquellliste
2. Wählen Sie die Datenquelle aus, für die Sie die Abfrage steuern möchten.
3. Klicken Sie auf den Link Name der Datenquelle.
4. Überprüfen Sie auf der Seite Datenquellenzusammenfassung die Informationen, und klicken Sie auf eine der folgenden beiden Abfrageoptionen:
   - **Noch einmal** um die Datenquelle zu zwingen, Daten sofort zu sammeln.
   - **Verschieben** und wählen Sie die Länge der Wahlverzögerung von 3, 7 oder 30 Tagen.

**Nachdem Sie fertig sind**

Wenn Sie die Datenerfassung auf eine Datenquelle verschoben haben und die Sammlung neu starten möchten, klicken Sie auf der Übersichtsseite auf **Fortsetzen**.

## Bearbeiten von Datenquellinformationen

Sie können die Setup-Informationen der Datenquelle schnell bearbeiten.

**Schritte**

1. Klicken Sie auf **Admin** und navigieren Sie zur Ansicht der Datenquellliste
2. Suchen Sie die Datenquelle, die Sie bearbeiten möchten.
3. Verwenden Sie eine dieser Methoden, um die Änderungen zu beginnen:
   - Klicken Sie rechts neben der ausgewählten Datenquelle auf **Datenquelle bearbeiten**.
   - Klicken Sie auf den verknüpften Namen der ausgewählten Datenquelle und dann auf **Bearbeiten**. Beide Methoden öffnen das Dialogfeld Datenquelle bearbeiten.
4. Nehmen Sie die gewünschten Änderungen vor und klicken Sie auf **Speichern**.

## Bearbeiten von Informationen für mehrere Datenquellen

Sie können die meisten Informationen für mehrere Datenquellen desselben Anbieters und Modells gleichzeitig bearbeiten. Wenn diese Datenquellen beispielsweise einen Benutzernamen und ein Passwort gemeinsam nutzen, können Sie das Passwort an einem Ort ändern und damit das Passwort für alle ausgewählten Datenquellen aktualisieren.

**Über diese Aufgabe**

Optionen, die Sie für die ausgewählten Datenquellen nicht bearbeiten können, werden abgeblendet angezeigt oder im Dialogfeld Datenquelle bearbeiten nicht angezeigt. Wenn eine Option einen Wert von **gemischt** anzeigt, zeigt sie außerdem an, dass der Wert für die Option zwischen den ausgewählten Datenquellen variiert. Beispiel: Wenn die Option **Timeout (sec)** für zwei ausgewählte Datenquellen **Mixed** ist, könnte eine Datenquelle einen Timeout-Wert von 60 haben und die andere einen Wert von 90 haben; Wenn Sie diesen Wert auf 120 ändern und die Änderungen an den Datenquellen speichern, wird die Timeout-Einstellung für beide Datenquellen zu 120.

**Schritte**

1. Klicken Sie auf **Admin** und navigieren Sie zur Ansicht der Datenquellliste
2. Wählen Sie die Datenquellen aus, die Sie ändern möchten. Die ausgewählten Datenquellen müssen demselben Anbieter, Modell und derselben Erfassungseinheit angehören.
3. Klicken Sie auf die Schaltfläche **actions** und wählen Sie die Option **Edit**.
4. Ändern Sie im Editierdialog die **Einstellungen** nach Bedarf.
5. Klicken Sie auf den Link **Konfiguration**, um eine der grundlegenden Optionen für die Datenquellen zu ändern.
6. Klicken Sie auf den Link **Erweiterte Konfiguration**, um eine der erweiterten Optionen für die Datenquellen zu ändern.

7. Klicken Sie Auf **Speichern**.

## Zuordnen von Datenquelltags zu Beschriftungen

Wenn eine Datenquelle für die Abfrage von Tag-Daten konfiguriert ist, setzt Insight automatisch Anmerkungswerte für eine vorhandene Insight-Anmerkung mit demselben Namen wie ein Tag.

Wenn die Insight-Anmerkung vorhanden ist, bevor die Tags in der Datenquelle aktiviert werden, werden die Datenquellkennungsdaten automatisch der Insight-Anmerkung hinzugefügt.

Wenn Sie eine Anmerkung erstellen, nachdem das Tag aktiviert wurde, wird die Anmerkung beim ersten Abruf der Datenquelle nicht automatisch aktualisiert. Es gibt eine Verzögerung in der Zeit, die benötigt wird, um die Insight-Anmerkung zu ersetzen oder zu füllen. Um die Verzögerung zu vermeiden, können Sie die Aktualisierung der Beschriftung erzwingen, indem Sie die Datenquelle verschieben und dann wieder aufnehmen.

## Löschen einer Datenquelle

Wenn Sie eine Datenquelle aus Ihrer Umgebung entfernt haben, müssen Sie sie auch aus der OnCommand Insight Monitoring-Umgebung löschen.

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.

   Die Liste Datenquellen wird geöffnet.

2. Wählen Sie die Datenquelle aus, die Sie löschen möchten.
3. Klicken Sie auf den Namen der verknüpften Datenquelle.
4. Überprüfen Sie die Informationen für die ausgewählte Datenquelle auf der Übersichtsseite, um sicherzustellen, dass sie die zu löschende Datenquelle ist.
5. Klicken Sie Auf **Löschen**.
6. Klicken Sie auf **OK**, um den Vorgang zu bestätigen.

## Was sind Datenquellpatches

Durch Patches für Datenquellen werden Probleme mit vorhandenen Patches behoben und neue Datenquelltypen (Anbieter und Modelle) können problemlos hinzugefügt werden. Sie können für jeden Datenquelltyp im Netzwerk Patches für Datenquellen hochladen. Sie können den Patching-Prozess auch installieren, testen und verwalten. Allerdings kann jeweils nur ein Patch für einen Datenquellentyp aktiv sein.

Für jeden Patch können Sie folgende Aufgaben ausführen:

- Überprüfen Sie den vorher- und Nachher-Vergleich jeder Datenquelle, die den Patch empfängt.
- Schreiben Sie Kommentare, um Entscheidungen zu erklären oder die Forschung zusammenzufassen.
- Nehmen Sie Änderungen an einer Datenquelle vor, die nicht gut auf den Patch reagiert.

- Genehmigen Sie den Patch, der an Ihren Insight-Server übertragen werden soll.
- Führen Sie ein Rollback für einen Patch durch, der nicht wie vorgesehen funktioniert.
- Ersetzen Sie einen fehlerhaften Patch durch einen anderen.

### Anwenden eines Datenquellpatches

Datenquellen-Patches sind regelmäßig verfügbar und ermöglichen es Ihnen, Probleme mit einer vorhandenen Datenquelle zu beheben, eine Datenquelle für einen neuen Anbieter hinzuzufügen oder ein neues Modell für einen Anbieter hinzuzufügen.

#### Bevor Sie beginnen

Sie müssen die erworben haben `.zip` Datei, die die neueste Datenquelle enthält `.patch` Dateien vom technischen Support.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.
3. Wählen Sie über die Schaltfläche Aktionen die Option **Patch anwenden** aus.
4. Klicken Sie im Dialogfeld **Data source Patch anwenden** auf **Browse**, um den zu suchen `.patch` Datei:
5. Überprüfen Sie die Datenquelltypen **Patch-Name**, **Beschreibung** und **betroffene Datenquelltypen**.
6. Wenn der ausgewählte Patch korrekt ist, klicken Sie auf **Patch anwenden**.

   Wenn Sie einen Patch anwenden, der Probleme mit einer Datenquelle behebt, werden alle Datenquellen desselben Typs mit dem Patch aktualisiert und Sie müssen den Patch genehmigen. Patches, die keine konfigurierten Datenquellen betreffen, werden automatisch genehmigt.

#### Nachdem Sie fertig sind

Wenn Sie einen Patch anwenden, der eine Datenquelle für einen neuen Anbieter oder ein neues Modell hinzufügt, müssen Sie die Datenquelle hinzufügen, nachdem Sie den Patch angewendet haben.

### Installation eines Patches auf einer Datenquelle

Nach dem Hochladen eines Datenquellpatches können Sie ihn auf allen Datenquellen desselben Typs installieren.

#### Bevor Sie beginnen

Sie müssen eine Patch-Datei hochgeladen haben, die Sie auf einer Datenquelle installieren möchten.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.
3. Wählen Sie über die Schaltfläche Aktionen die Option **Patch anwenden** aus.
4. Klicken Sie im Dialogfeld **Data source Patch anwenden** auf **Browse**, um die hochgeladene Patch-Datei

zu finden.

5. Überprüfen Sie die Typen **Patch-Name**, **Beschreibung** und **betroffene Datenquellen**.
6. Wenn der ausgewählte Patch korrekt ist, klicken Sie auf **Patch anwenden**.

   Alle Datenquellen des gleichen Typs werden mit diesem Patch aktualisiert.

### Verwalten von Patches

Sie können den aktuellen Status aller Datenquellpatches überprüfen, die auf Ihr Netzwerk angewendet werden. Wenn Sie eine Aktion für einen Patch ausführen möchten, können Sie in der Tabelle Patches, die derzeit unter Review steht, auf den verknüpften Namen klicken.

#### Bevor Sie beginnen

Sie müssen bereits hochgeladen haben und mindestens einen Patch installieren.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.

   Wenn keine Patches installiert werden, ist die Tabelle der derzeit zu prüfenden Patches leer.

3. Prüfen Sie in **Patches, die aktuell überprüft werden**, den Status der aktuell angewendeten Datenquellpatches.
4. Um die Details zu einem bestimmten Patch zu untersuchen, klicken Sie auf den verknüpften Namen des Patches.
5. Für den ausgewählten Patch können Sie auf eine der folgenden Optionen klicken, um die nächste Aktion für den Patch durchzuführen:
   - **Approve Patch** überträgt den Patch an die Datenquellen.
   - **Rollback** entfernt den Patch.
   - **Replace Patch** ermöglicht es Ihnen, einen anderen Patch für diese Datenquellen auszuwählen.

### Festlegen eines Datenquellpatches

Anhand der Informationen in der Patch-Zusammenfassung können Sie entscheiden, ob der Patch erwartungsgemäß funktioniert, und dann den Patch an Ihr Netzwerk übertragen.

#### Bevor Sie beginnen

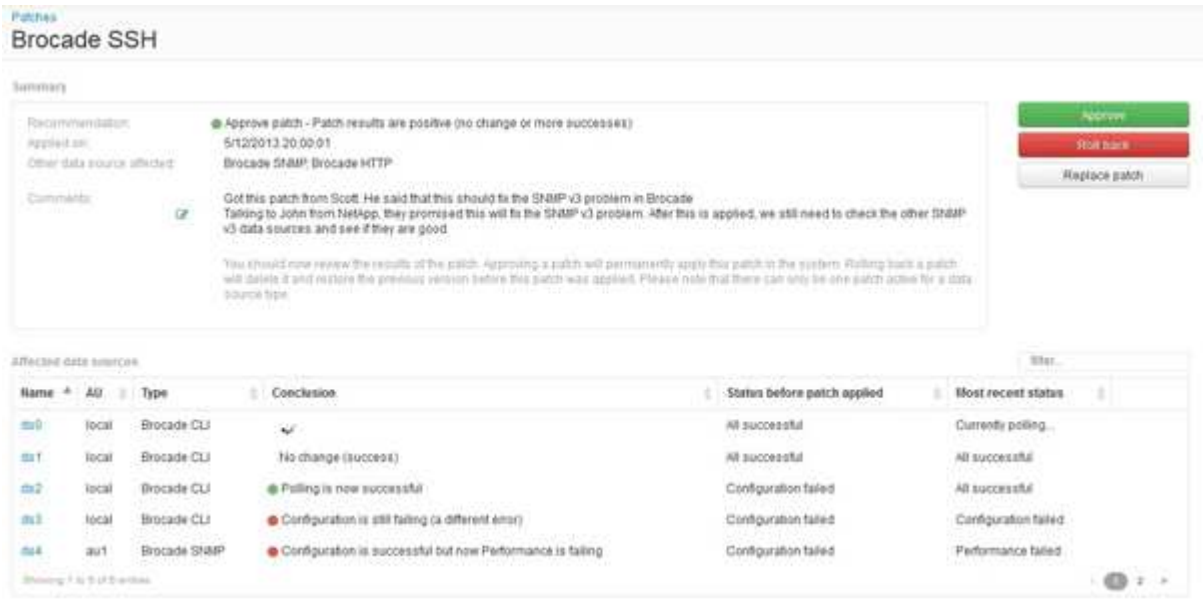
Sie haben einen Patch installiert und müssen entscheiden, ob der Patch erfolgreich ist und genehmigt werden sollte.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.

Wenn keine Patches installiert werden, sind die derzeit zu prüfenden Patches leer.

3. Prüfen Sie in **Patches, die aktuell überprüft werden**, den Status der aktuell angewendeten Datenquellpatches.
4. Um die Details zu einem bestimmten Patch zu untersuchen, klicken Sie auf den verknüpften Namen des Patches.
5. Überprüfen Sie in der Zusammenfassung der Patches, die in diesem Beispiel gezeigt wird, die **Empfehlung** und **Kommentare**, um den Fortschritt des Patches zu bewerten.




6. Überprüfen Sie die Tabelle **betroffene Datenquellen**, um den Status jeder betroffenen Datenquelle vor und nach dem Patch anzuzeigen.

   Wenn Sie Bedenken haben, dass ein Problem mit einer der Datenquellen besteht, die gepatcht werden, klicken Sie in der Tabelle betroffene Datenquellen auf den verknüpften Namen.

7. Wenn Sie schließen, dass der Patch auf diesen Datentyp angewendet werden soll, klicken Sie auf **Approve**.

   Die Datenquellen werden geändert, und der Patch wird aus Patches entfernt, die derzeit geprüft werden.

### Rollback eines Datenquellpatches

Wenn ein Datenquellpatch nicht so funktioniert, wie Sie es erwartet haben, können Sie es erneut ausführen. Durch ein Rollback eines Patches wird dieser gelöscht und die vorherige Version wird wie vor der Anwendung dieses Patches wiederhergestellt.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.
3. Klicken Sie unter **Patches, die aktuell überprüft werden** auf den verknüpften Namen des Patches, der anscheinend nicht erfolgreich ist.
4. Prüfen Sie auf der Seite Patches für die Datenquelle diese Informationen:

- **Zusammenfassung** beschreibt, wann der Patch angewendet wurde, die betroffenen Datenquellen und Kommentare über den Patch von Ihnen oder anderen Mitgliedern Ihres Teams.
- **Betroffene Datenquellen** listet alle zu patchenden Datenquellen auf und enthält einen Vergleich des vor- und Nachpatchstatus.

5. Um die Details für eine Datenquelle anzuzeigen, die den Patch nicht erfolgreich verarbeitet, klicken Sie auf den verknüpften **Name**.
   a. Überprüfen Sie die Zusammenfassung.
   b. Überprüfen Sie die **Event Timeline**, um alle Konfigurations- oder Leistungsdaten zu sehen, die diese Datenquelle beeinflussen könnten.
6. Wenn Sie feststellen, dass der Patch nicht erfolgreich sein wird, klicken Sie auf den Zurück-Pfeil des Browsers, um zur Übersichtsseite der Patches zurückzukehren.
7. Klicken Sie auf **Rollback**, um diesen Patch zu entfernen.

   Wenn Sie von einem anderen Patch wissen, der mit größerer Wahrscheinlichkeit erfolgreich sein wird, klicken Sie auf **Replace Patch** und laden Sie den neuen Patch hoch.

# Geräteauflösung

Sie müssen alle Geräte ermitteln, die Sie mit OnCommand Insight überwachen möchten. Eine Bestandsaufnahme ist erforderlich, um die Performance und Bestandsaufnahme in Ihrer Umgebung exakt zu verfolgen. In der Regel werden die meisten Geräte in Ihrer Umgebung durch automatische Geräteauflösung erkannt.

Wenn Sie ein Upgrade durchführen und inaktive Regeln für die automatische Auflösung im System haben, von dem Sie aktualisieren, werden diese Regeln während des Upgrades gelöscht. Um inaktive Regeln für die automatische Auflösung beizubehalten, aktivieren Sie die Regeln (aktivieren Sie das Kontrollkästchen), bevor das Upgrade durchgeführt wird.

Nach der Installation und Konfiguration von Datenquellen werden Geräte in Ihrer Umgebung, einschließlich Switches, Storage-Arrays und Hypervisoren und VMs, identifiziert. Dies erkennt jedoch normalerweise nicht 100 % der Geräte in Ihrer Umgebung.

Nachdem Geräte vom Typ der Datenquelle konfiguriert wurden, empfiehlt es sich, Regeln zur Geräteauflösung zu nutzen, um die verbleibenden unbekannten Geräte in Ihrer Umgebung zu identifizieren. Die Geräteauflösung kann Ihnen dabei helfen, unbekannte Geräte als die folgenden Gerätetypen zu lösen:

- Physische Hosts
- Storage Arrays
- Bänder
- Switches

Geräte, die nach der Geräteauflösung als „`unbekannt`“ verbleiben, gelten als generische Geräte, die Sie auch in Abfragen und Dashboards anzeigen können.

Die wiederum erstellten Regeln identifizieren automatisch neue Geräte mit ähnlichen Attributen, wie sie Ihrer Umgebung hinzugefügt werden. In einigen Fällen ermöglicht die Geräteauflösung auch die manuelle Identifizierung unter Umgehung der Regeln für die Geräteauflösung für nicht erkannte Geräte in Insight.

Eine unvollständige Identifizierung von Geräten kann zu folgenden Problemen führen:

- Unvollständige Pfade
- Nicht identifizierte Multipath-Verbindungen
- Applikationen können nicht gruppieren
- Ungenaue Topologieansichten
- Ungenaue Daten im Data Warehouse und Berichterstellung

Die Funktion Geräteauflösung (**Verwalten** > **Geräteauflösung**) umfasst die folgenden Registerkarten, die jeweils eine Rolle bei der Planung und Anzeige der Ergebnisse der Geräteauflösung spielen:

- „`FC identify`“ enthält eine Liste von WWNs und Portinformationen von Fibre-Channel-Geräten, die nicht durch automatische Geräteauflösung aufgelöst wurden. Auf der Registerkarte wird außerdem der Prozentsatz der erkannten Geräte angegeben.
- „`IP identify`“ enthält eine Liste von Geräten, die auf CIFS-Freigaben und NFS-Freigaben zugreifen, die nicht durch die automatische Geräteauflösung identifiziert wurden. Auf der Registerkarte wird außerdem der Prozentsatz der erkannten Geräte angegeben.
- „`Regeln für die automatische Auflösung`“ enthält die Liste der Regeln, die bei der Ausführung der Fibre-Channel-Geräteauflösung ausgeführt werden. Dies sind Regeln, die Sie erstellen, um nicht identifizierte Fibre Channel-Geräte zu lösen.
- „`Einstellungen`“ bietet Konfigurationsoptionen, mit denen Sie die Geräteauflösung an Ihre Umgebung anpassen.

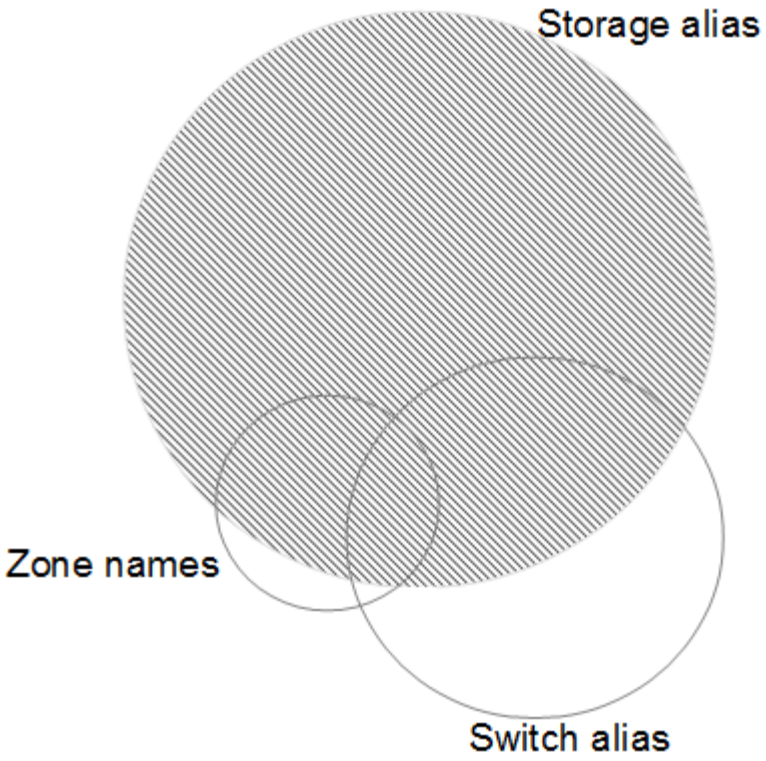
## Bevor Sie beginnen

Sie müssen wissen, wie Ihre Umgebung konfiguriert ist, bevor Sie die Regeln für die Identifizierung von Geräten definieren. Je mehr Sie über Ihre Umgebung wissen, desto einfacher ist es, Geräte zu identifizieren.

Sie müssen die folgenden Fragen beantworten, um genaue Regeln zu erstellen:

- Gibt es in Ihrer Umgebung Namensstandards für Zonen oder Hosts, und wie viel Prozent dieser Standards sind korrekt?
- Verwendet Ihre Umgebung einen Switch-Alias oder Storage-Alias und stimmt mit dem Host-Namen überein?
- Verwendet Ihre Umgebung ein SRM-Tool, und können Sie es verwenden, um Hostnamen zu identifizieren? Welche Abdeckung bietet SRM?
- Wie oft ändern sich Benennungsschemata in Ihrer Umgebung?
- Gab es Übernahmen oder Fusionen, bei denen verschiedene Benennungsschemata eingeführt wurden?

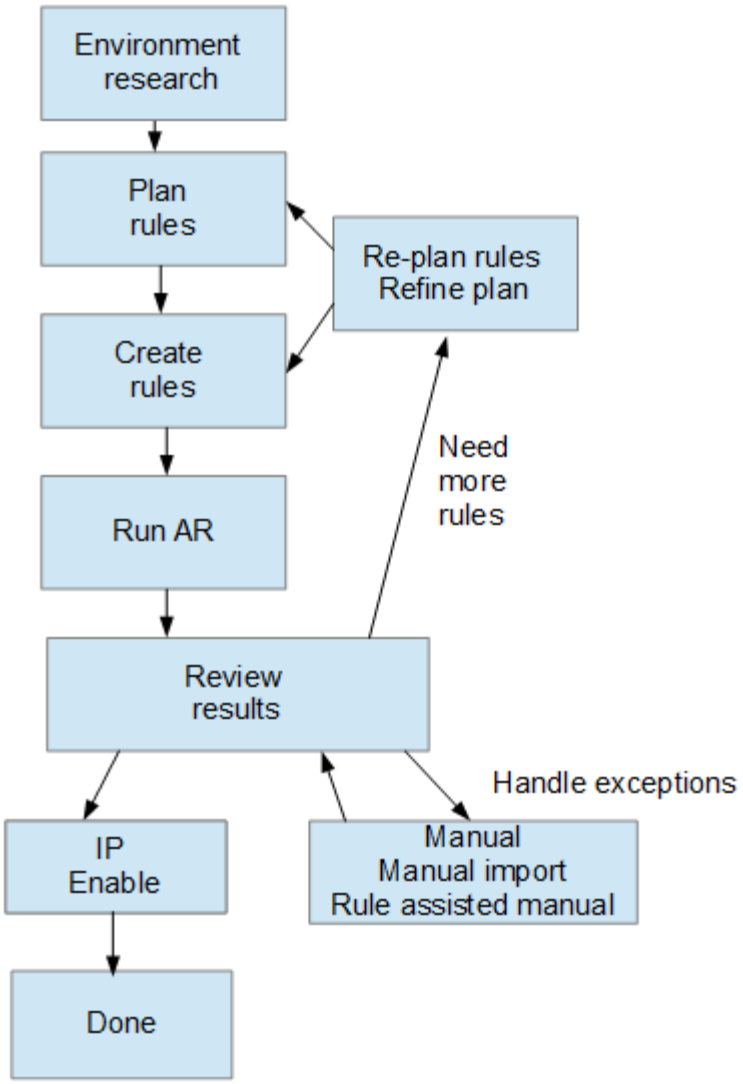
Nach der Analyse Ihrer Umgebung sollten Sie in der Lage sein, zu identifizieren, welche Benennungsstandards existieren, die Sie mit der Zuverlässigkeit rechnen können. Die gesammelten Informationen können grafisch in einer Abbildung dargestellt werden, die der folgenden ähnelt:




In diesem Beispiel wird die größte Anzahl von Geräten zuverlässig durch Speicheraliasen dargestellt. Regeln, die Hosts mit Speicheraliasen identifizieren, sollten zuerst geschrieben werden, Regeln mit Switch-Aliasen sollten als Nächstes geschrieben werden, und die letzten erstellten Regeln sollten Zonenaliasen verwenden. Aufgrund der Überlappung der Verwendung von Zonen-Aliasen und Switch-Aliasen können einige Speicher-Alias-Regeln zusätzliche Geräte identifizieren, so dass weniger Regeln für Zonen-Aliase und Switch-Aliase erforderlich sind.

**Schritte zum Definieren von Geräten in Ihrer Umgebung**

In der Regel würden Sie ähnliche Workflows wie die folgenden verwenden, um Geräte in Ihrer Umgebung zu identifizieren. Die Identifizierung ist ein iterativer Prozess und erfordert möglicherweise mehrere Schritte bei der Planung und Verfeinerung von Regeln.




Wenn Sie in Ihrer Umgebung nicht identifizierte Geräte (auch bekannt als „`unknown`“ oder generische Geräte) haben und anschließend eine Datenquelle konfigurieren, die diese Geräte beim Abfragen identifiziert, werden diese nicht mehr als generische Geräte angezeigt oder gezählt.

## Planen von Regeln für die Geräteauflösung für Ihre Umgebung

Die Verwendung von Regeln zur Identifizierung von Geräten in Ihrer Umgebung ist in der Regel ein iterativer Prozess, der eine gründliche Analyse Ihrer Umgebung und die Erstellung mehrerer Regeln erfordert, um so viele Geräte wie möglich zu identifizieren. Im besten Fall sollten Sie sich das Ziel setzen, 100 % der Geräte in Ihrer Umgebung zu ermitteln.

Die effizienteste Reihenfolge für Regeln besteht darin, die restriktivsten Regeln an die erste Stelle zu setzen, was dazu führt, dass die meisten Einträge nicht mit Mustern übereinstimmen, wobei der Prozess zu weniger restriktiven Regeln führt. Dadurch kann Insight mehr Muster auf jeden Eintrag anwenden, wodurch die Möglichkeit des Musterabgleichs und der positiven Hostidentifikation erhöht wird.

Wenn Sie Regeln erstellen, sollten Sie Regeln erstellen, die die größte Anzahl nicht identifizierter Geräte adressieren, die möglich sind. Beispielsweise ist das Erstellen von Regeln, die einem Muster der Deckung

ähnlich wie die folgenden folgen, viel effizienter als das Erstellen von 30 Regeln mit niedrigeren Prozentsätzen der Deckung:

| Regel | Prozentsatz der Abdeckung |
|---|---|
| Regel 1 | 60 % erreicht |
| Regel 2 | 25 % erzielt |
| Regel 3 | 8 % erreicht |
| Regel 4 | 4 % erreicht |
| Regel 5 | 1 % |

## Erstellen von Regeln für die Geräteauflösung

Sie erstellen Regeln für die Geräteauflösung, um Hosts, Speicher und Bänder zu identifizieren, die derzeit von OnCommand Insight nicht automatisch erkannt werden. Die Regeln, die Sie erstellen, identifizieren Geräte, die sich derzeit in Ihrer Umgebung befinden, und identifizieren ähnliche Geräte, die Ihrer Umgebung hinzugefügt werden.

### Über diese Aufgabe

Wenn Sie Regeln erstellen, müssen Sie zunächst die Informationsquelle identifizieren, auf die die Regel angewendet wird, die Methode, mit der Informationen extrahiert werden sollen, und ob DNS-Suche auf die Ergebnisse der Regel angewendet wird.

| |
|---|
| Quelle, mit der das Gerät identifiziert wird |
| • SRM-Aliase für Hosts<br>• Speicheralias, der einen eingebetteten Host- oder Bandnamen enthält<br>• Switch-Alias, der einen eingebetteten Host- oder Bandnamen enthält<br>• Zonennamen, die einen eingebetteten Hostnamen enthalten |
| Methode, die zum Extrahieren des Gerätenamens aus der Quelle verwendet wird |
| • Wie ist (extrahieren Sie einen Namen aus einem SRM)<br>• Trennzeichen<br>• Reguläre Ausdrücke |
| DNS-Suche |
| Gibt an, ob Sie DNS zur Überprüfung des Hostnamens verwenden. |

Sie erstellen Regeln auf der Registerkarte Regeln für die automatische Auflösung. Die folgenden Schritte beschreiben den Prozess zur Regelerstellung.

**Schritte**

1. Klicken Sie auf **Verwalten** > **Geräteauflösung**
2. Klicken Sie auf der Registerkarte **Automatische Auflösungsregeln** auf **+Hinzufügen**

   Der Bildschirm Neue Regel wird angezeigt.

   Der Bildschirm Neue Regel enthält ein **?**-Symbol, das Hilfe und Beispiele zum Erstellen regulärer Ausdrücke enthält.

3. Wählen Sie in der Liste **Typ** das Gerät aus, das Sie identifizieren möchten.

   Sie können Host oder Band auswählen.

4. Wählen Sie in der Liste **Quelle** die Quelle aus, mit der Sie den Host identifizieren möchten.

   Je nach gewählter Quelle zeigt Insight die folgende Antwort an:

   - In Zonen sind die Zonen und WWN aufgeführt, die von Insight identifiziert werden müssen.
   - SRM listet die nicht identifizierten Aliase auf, die von Insight identifiziert werden müssen
   - Im Storage-Alias werden Storage-Aliase und WWN aufgeführt, die von Insight identifiziert werden müssen
   - Switch-Alias listet die Switch-Aliase auf, die von Insight identifiziert werden müssen

5. Wählen Sie in der Liste **Methode** die Methode aus, die Sie verwenden möchten, um den Host zu identifizieren.

| Quelle | Methode |
|---|---|
| SRM | „as is“, „Trennzeichen“, „reguläre Ausdrücke“ |
| Storage-Alias | „Trennzeichen“ oder „reguläre Ausdrücke“ |
| Alias wechseln | „Trennzeichen“ oder „reguläre Ausdrücke“ |
| Zonen | „Trennzeichen“ oder „reguläre Ausdrücke“ |

   - Regeln, die „Trennzeichen“ verwenden, erfordern die Trennzeichen und die Mindestlänge des Hostnamens.

     Die Mindestlänge des Hostnamens ist die Anzahl der Zeichen, die Insight zur Identifizierung eines Hosts verwenden sollte. Insight führt DNS-Suchvorgänge nur für Hostnamen aus, die so lang oder länger sind.

     Bei Regeln, die Trennzeichen verwenden, wird die Eingabeszeichenfolge durch das Trennzeichen getokenisiert, und eine Liste von Hostnamenkandidaten wird durch das Erstellen mehrerer

Kombinationen des benachbarten Tokens erstellt. Die Liste wird dann sortiert, die größte bis die kleinste. Beispiel: Für vipsnq03_hba3_emc3_12ep0 würde die Liste Folgendes ergeben:

- Vipsnq03_hba3_emc3_12ep0
- Vipsnq03_hba3_emc3
- Hba3 emc3_12ep0
- Vipsnq03_hba3
- Emc3_12ep0
- Hba3_emc3
- Vipsnq03
- 12ep0
- Emc3
- Hba3

◦ Regeln, die „`regulärer Ausdruck`“ verwenden, erfordern einen regulären Ausdruck, das Format und die Sensitivitätsauswahl für Fälle.

6. Klicken Sie Auf

Um alle Regeln auszuführen, oder klicken Sie auf den Abwärtspfeil in der Schaltfläche, um die erstellte Regel (und alle anderen Regeln, die seit der letzten vollständigen Ausführung von AR erstellt wurden) auszuführen.

**Ergebnisse**

Die Ergebnisse der Regelausführung werden auf der Registerkarte FC Identify angezeigt.

#### Starten einer automatischen Aktualisierung der Geräteauflösung

Ein Update zur Geräteauflösung setzt manuelle Änderungen fest, die seit der letzten vollständigen automatischen Gerätelaufauflösung hinzugefügt wurden. Das Ausführen eines Updates kann verwendet werden, um nur die neuen manuellen Einträge für die Konfiguration der Geräteauflösung zu übergeben und auszuführen. Es wird keine vollständige Gerätelaufauflösung durchgeführt.

##### Schritte

1. Melden Sie sich bei der Web-UI von Insight an.
2. Klicken Sie Auf **Verwalten** > **Geräteauflösung**
3. Klicken Sie im Bildschirm **Geräteauflösung** auf den Abwärtspfeil in der Schaltfläche **AR ausführen**.
4. Klicken Sie auf **Aktualisieren**, um die Aktualisierung zu starten.

#### Regelgestützte manuelle Identifizierung

Diese Funktion wird für spezielle Fälle verwendet, in denen Sie eine bestimmte Regel oder eine Liste von Regeln (mit oder ohne eine einmalige Neuanordnung) ausführen möchten, um unbekannte Hosts, Speicher und Bandgeräte oder Gruppen von ihnen zu lösen.

**Bevor Sie beginnen**

Sie verfügen über eine Reihe von Geräten, die nicht identifiziert wurden, und Sie haben auch mehrere Regeln, die andere Geräte erfolgreich identifiziert haben.

**Über diese Aufgabe**

Wenn Ihre Quelle nur einen Teil eines Host- oder Gerätenamens enthält, verwenden Sie eine Regel für reguläre Ausdrücke, und formatieren Sie sie, um den fehlenden Text hinzuzufügen.

**Schritte**

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** > **Geräteauflösung**
3. Klicken Sie auf die Registerkarte **FC identifiere**.

   Das System zeigt die identifizierten und nicht identifizierten Geräte an.

4. Wählen Sie mehrere nicht identifizierte Geräte aus.
5. Klicken Sie auf **identifiere** > **set Host Resolution** oder **> set Tape Resolution**

   Das System zeigt den Identify-Bildschirm an, der eine Liste aller Regeln enthält, die Geräte erfolgreich identifiziert haben.

6. Ändern Sie die Reihenfolge der Regeln in eine Bestellung, die Ihren Anforderungen entspricht.

   Die Reihenfolge der Regeln wird im Identify-Bildschirm geändert, aber nicht global geändert.

7. Wählen Sie die Methode aus, die Ihren Anforderungen entspricht.

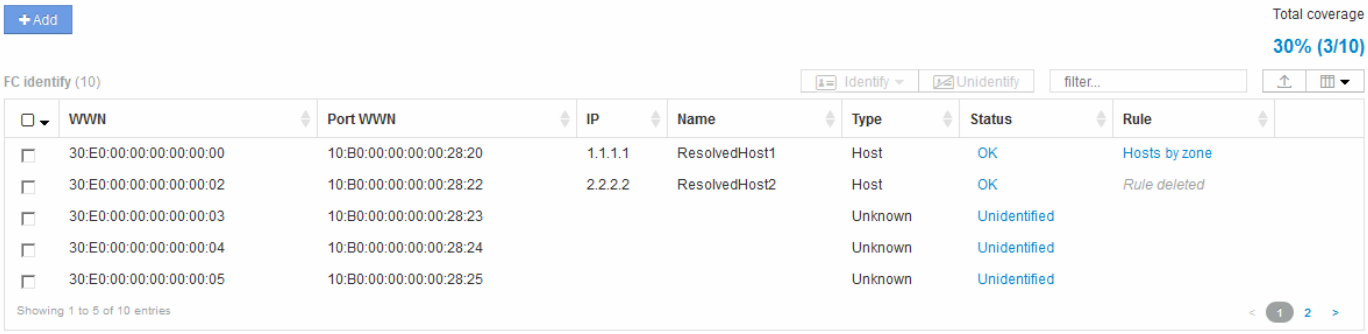
   OnCommand Insight führt den Host-Auflösungsprozess in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit den Methoden oben.

   Wenn geltende Regeln gefunden werden, werden in der Spalte Regeln Regelnamen angezeigt und als Handbuch identifiziert.

## Fibre Channel-Geräteauflösung

Auf dem Bildschirm FC-Identifizierung werden WWN und WWPN von Fibre-Channel-Geräten angezeigt, deren Hosts nicht durch die automatische Geräteauflösung identifiziert wurden. Auf dem Bildschirm werden auch alle Geräte angezeigt, die durch manuelle Geräteauflösung gelöst wurden.

Geräte, die durch manuelle Auflösung aufgelöst wurden, enthalten den Status „`OK`“ und identifizieren die Regel, mit der das Gerät identifiziert wird. Fehlende Geräte haben den Status „`nicht identifiziert`“. Die Gesamtabdeckung für die Identifizierung von Geräten ist auf dieser Seite aufgeführt.




Sie führen Massenaktionen durch, indem Sie auf der linken Seite des FC-Identifizieren-Bildschirms mehrere Geräte auswählen. Aktionen können auf einem einzelnen Gerät durchgeführt werden, indem Sie den Mauszeiger über ein Gerät bewegen und die Schaltflächen Identifizieren oder Identifizieren ganz rechts in der Liste auswählen.

Der Link Gesamtabdeckung zeigt eine Liste der „Anzahl der identifizierten Geräte/Anzahl der verfügbaren Geräte“ für Ihre Konfiguration an:

- SRM-Alias
- Storage-Alias
- Alias wechseln
- Zonen
- Benutzerdefiniert

### Manuelles Hinzufügen eines Fibre-Channel-Geräts

Sie können ein Fibre-Channel-Gerät manuell zu OnCommand Insight hinzufügen, indem Sie die manuelle Add-Funktion verwenden, die auf der Registerkarte Geräteauflösung FC-Identifizierung verfügbar ist. Dieser Prozess kann für die Voridentifizierung eines Geräts verwendet werden, das in Zukunft entdeckt werden soll.

#### Bevor Sie beginnen

Zum erfolgreichen Hinzufügen einer Geräteidentifikation zum System müssen Sie die WWN- oder IP-Adresse und den Gerätenamen kennen.

#### Über diese Aufgabe

Sie können einen Host, Speicher, Band oder ein unbekanntes Fibre Channel-Gerät manuell hinzufügen.

#### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an
2. Klicken Sie auf **Verwalten** > **Geräteauflösung**
3. Klicken Sie auf die Registerkarte **FC identifiere**.
4. Klicken Sie auf die Schaltfläche Hinzufügen.

   Das Dialogfeld Gerät hinzufügen wird angezeigt

5. Geben Sie die WWN- oder IP-Adresse, den Gerätenamen ein, und wählen Sie den Gerätetyp aus.

#### Ergebnisse

Das von Ihnen eingegebene Gerät wird der Liste der Geräte auf der Registerkarte FC-Identifizierung hinzugefügt. Die „`Regel`“ wird als manuell gekennzeichnet.

### Importieren der Fibre-Channel-Geräteidentifikation aus einer CSV-Datei

Sie können die Fibre-Channel-Geräteidentifikation manuell in die OnCommand Insight-Geräteauflösungsfunktion importieren, indem Sie eine Liste von Geräten in einer CSV-Datei verwenden.

#### Bevor Sie beginnen

Sie müssen über eine korrekt formatierte CSV-Datei verfügen, um Gerätekennungen direkt in die Funktion Geräteauflösung importieren zu können. Die CSV-Datei für Fibre-Channel-Geräte erfordert die folgenden Informationen:

| |
|---|
| WWN |
| IP |
| Name |
| Typ |

> Als Best Practice wird empfohlen, zunächst die FC-Identifizieren-Informationen in eine CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in FC Identify zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten in der richtigen Reihenfolge vorhanden sind.

So importieren Sie FC-Identifizieren-Informationen:

#### Schritte

1. Melden Sie sich bei der Web-UI von Insight an.
2. Klicken Sie Auf **Verwalten** > **Geräteauflösung**
3. Wählen Sie die Registerkarte **FC identifiere** aus.
4. Klicken Sie auf **identifier** > **identifier from file**
   .
   a. Navigieren Sie zu dem Ordner mit den CSV-Dateien für den Import, und wählen Sie die gewünschte Datei aus.

   Die von Ihnen eingegebenen Geräte werden der Liste der Geräte auf der Registerkarte FC-Identifizierung hinzugefügt. Die „`Regel`“ wird als „`manuell`“ gekennzeichnet.

### Exportieren von Fibre-Channel-Gerätekennungen in eine CSV-Datei

Sie können vorhandene Fibre-Channel-Gerätekennungen aus der OnCommand Insight-

Geräteauflösungsfunktion in eine CSV-Datei exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Insight importieren können, wo sie dann zur Identifizierung von Geräten verwendet wird, die denen ähneln, die ursprünglich mit der exportierten Identifizierung übereinstimmen.

**Über diese Aufgabe**

Dieses Szenario kann verwendet werden, wenn Geräte ähnliche Attribute haben, die einfach in der CSV-Datei bearbeitet und dann wieder in das System importiert werden können.

Wenn Sie eine Fibre-Channel-Gerätekennung in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

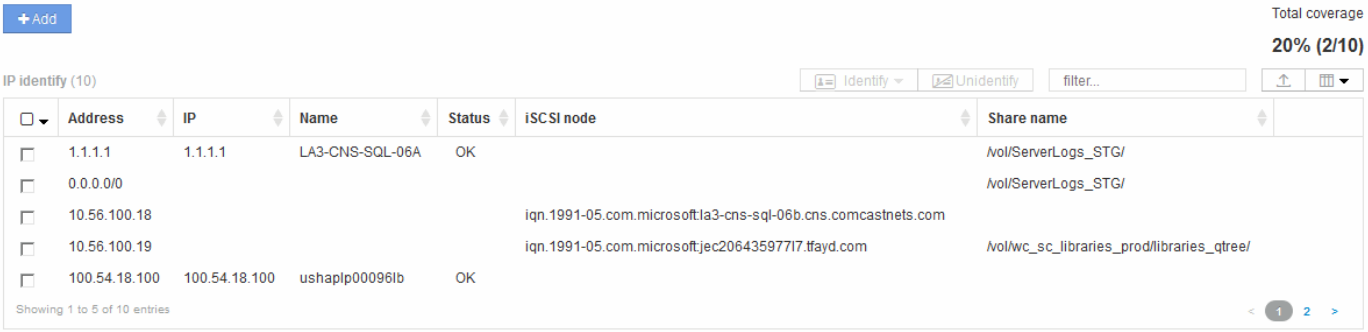
| |
|---|
| WWN |
| IP |
| Name |
| Typ |

**Schritte**

1. Melden Sie sich bei der Web-UI von Insight an.
2. Klicken Sie Auf **Verwalten** > **Geräteauflösung**
3. Wählen Sie die Registerkarte **FC identifiere** aus.
4. Wählen Sie das Fibre-Channel-Gerät oder die Geräte aus, deren Kennung Sie exportieren möchten.
5. Klicken Sie auf den Export Symbol.
6. Wählen Sie aus, ob Sie die CSV-Datei öffnen oder die Datei speichern möchten.

## IP-Geräteauflösung

Auf dem Bildschirm IP-Identifizierung werden alle iSCSI- und CIFS- oder NFS-Freigaben angezeigt, die durch die automatische Geräteauflösung oder durch manuelle Geräteauflösung identifiziert wurden. Auch nicht identifizierte Geräte werden angezeigt. Der Bildschirm enthält die IP-Adresse, den Namen, den Status, den iSCSI-Knoten und den Freigabenamen für Geräte. Der Prozentsatz der erfolgreich identifizierten Geräte wird ebenfalls angezeigt.




### Manuelles Hinzufügen von IP-Geräten

Sie können ein IP-Gerät manuell zu OnCommand Insight hinzufügen, indem Sie die manuelle Zusatzfunktion verwenden, die im IP-Identifizieren-Bildschirm verfügbar ist.

#### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an.
2. Klicken Sie auf **Verwalten** > **Geräteauflösung**
3. Klicken Sie auf die Registerkarte **IP identiffy**.
4. Klicken Sie auf die Schaltfläche Hinzufügen.

   Das Dialogfeld Gerät hinzufügen wird angezeigt

5. Geben Sie die Adresse, die IP-Adresse und einen eindeutigen Gerätenamen ein.

#### Ergebnisse

Das von Ihnen eingegebene Gerät wird der Liste der Geräte auf der Registerkarte IP-Identifizierung hinzugefügt.

### Importieren der IP-Geräteidentifikation aus einer CSV-Datei

Sie können IP-Gerätekennungen manuell in die Funktion Geräteauflösung importieren, indem Sie eine Liste der Gerätekennungen in einer CSV-Datei verwenden.

#### Bevor Sie beginnen

Sie müssen eine korrekt formatierte CSV-Datei haben, um Gerätekennungen importieren zu können. Für die CSV-Datei für IP-Geräte sind folgende Informationen erforderlich:

| |
|---|
| Adresse |
| IP |
| Name |

Als Best Practice empfiehlt es sich, zunächst die IP-Ident-Informationen in eine CSV-Datei zu exportieren, die gewünschten Änderungen in dieser Datei vorzunehmen und die Datei dann wieder in die IP-Identifizierung zu importieren. Dadurch wird sichergestellt, dass die erwarteten Spalten in der richtigen Reihenfolge vorhanden sind.

So importieren Sie IP-Identifizieren-Informationen:

#### Schritte

1. Melden Sie sich bei der Web-UI von Insight an.
2. Klicken Sie Auf **Verwalten** > **Geräteauflösung**
3. Wählen Sie die Registerkarte **IP identiffy**.
4. Klicken Sie auf **identifier** > **identifier from file**
   .
   a. Navigieren Sie zu dem Ordner mit den CSV-Dateien für den Import, und wählen Sie die gewünschte Datei aus.

   Die von Ihnen eingegebenen Geräte werden der Liste der Geräte auf der Registerkarte IP-Identifizierung hinzugefügt.

### Exportieren der IP-Geräteidentifikation in eine CSV-Datei

Sie können vorhandene IP-Gerätekennungen über die Funktion „Geräteauflösung“ aus Insight exportieren. Möglicherweise möchten Sie eine Gerätekennung exportieren, damit Sie sie ändern und dann wieder in Insight importieren können, damit sie zur Identifizierung von Geräten verwendet werden kann, die denen der exportierten Identifikation ähneln.

#### Über diese Aufgabe

Wenn Sie eine IP-Geräteidentifikation in eine CSV-Datei exportieren, enthält die Datei die folgenden Informationen in der angezeigten Reihenfolge:

| |
|---|
| Adresse |
| IP |
| Name |

#### Schritte

1. Melden Sie sich bei der Web-UI von Insight an.
2. Klicken Sie Auf **Verwalten** > **Geräteauflösung**
3. Wählen Sie die Registerkarte **IP identiffy**.
4. Wählen Sie das IP-Gerät oder die Geräte aus, deren Kennung Sie exportieren möchten.
5. Klicken Sie auf den Export Symbol.

6. Wählen Sie aus, ob Sie die CSV-Datei öffnen oder die Datei speichern möchten.

## Einstellungen auf der Registerkarte Einstellungen

Auf der Registerkarte „Voreinstellungen für die Geräteauflösung“ können Sie einen Zeitplan für die automatische Auflösung erstellen, Speicher- und Bandanbieter angeben, die die Identifizierung einschließen oder ausschließen sollen, und DNS-Suchoptionen festlegen.

### Zeitplan für die automatische Auflösung

Ein Zeitplan für die automatische Auflösung kann festlegen, wann die automatische Gerätelaufauflösung ausgeführt wird:

| Option | Beschreibung |
|---|---|
| Alle | Verwenden Sie diese Option, um die automatische Geräteauflösung in Intervallen von Tagen, Stunden oder Minuten durchzuführen. |
| Jeden Tag | Verwenden Sie diese Option, um die automatische Geräteauflösung täglich zu einem bestimmten Zeitpunkt auszuführen. |
| Manuell | Verwenden Sie diese Option, um nur die automatische Geräteauflösung manuell auszuführen. |
| Bei jeder Umgebungsänderung | Verwenden Sie diese Option, um bei jeder Änderung der Umgebung eine automatische Geräteauflösung auszuführen. |

Wenn Sie manuell angeben, wird die automatische Geräteauflösung nachts deaktiviert.

### DNS-Verarbeitungsoptionen

Mit den DNS-Verarbeitungsoptionen können Sie die folgenden Funktionen auswählen:

- Wenn die Verarbeitung der DNS-Suchtresultat aktiviert ist, können Sie eine Liste von DNS-Namen hinzufügen, die an aufgelöste Geräte angehängt werden sollen.
- Sie können „`Automatische Auflösung von IPs:`“ auswählen, um die automatische Hostauflösung für iSCSI-Initiatoren und Hosts zu aktivieren, die auf NFS-Freigaben über DNS Lookup zugreifen. Wenn dies nicht angegeben wird, wird nur FC-basierte Auflösung ausgeführt.
- Sie können Unterstriche in Hostnamen zulassen und anstelle des Standard-Port-Alias in Results einen Alias „Connected to“ verwenden.

### Einschließlich oder mit Ausnahme bestimmter Storage- und Tape-Anbieter

Zur automatischen Lösung können Sie bestimmte Speicher- und Bandanbieter ein- oder ausschließen. Möglicherweise möchten Sie bestimmte Anbieter ausschließen, wenn Sie beispielsweise wissen, dass ein bestimmter Host zu einem veralteten Host wird und von Ihrer neuen Umgebung ausgeschlossen werden sollte.

Sie können auch Anbieter, die Sie zuvor ausgeschlossen haben, erneut hinzufügen, möchten aber nicht mehr ausgeschlossen werden.

Die Regeln für die Geräteauflösung für Bänder gelten nur für WWNs, wobei der Hersteller für diesen WWN in den Voreinstellungen des Herstellers auf **nur als Band enthalten** gesetzt ist.

## Beispiele für reguläre Ausdrücke

Wenn Sie den Ansatz für reguläre Ausdrücke als Namensstrategie für Quellen ausgewählt haben, können Sie die Beispiele für reguläre Ausdrücke als Leitfaden für Ihre eigenen Ausdrücke verwenden, die in den automatischen Auflösungsmethoden von OnCommand Insight verwendet werden.

#### Formatieren von regulären Ausdrücken

Wenn Sie reguläre Ausdrücke für die automatische Auflösung von OnCommand Insight erstellen, können Sie das Ausgabeformat konfigurieren, indem Sie Werte in ein Feld mit dem Namen eingeben `FORMAT`.

Die Standardeinstellung ist `\1`, Das bedeutet, dass ein Zonenname, der dem regulären Ausdruck entspricht, durch den Inhalt der ersten Variablen ersetzt wird, die durch den regulären Ausdruck erzeugt wird. In einem regelmäßigen Ausdruck werden variable Werte durch parteiliche Aussagen erzeugt. Wenn mehrere parenthetische Aussagen auftreten, werden die Variablen numerisch von links nach rechts referenziert. Die Variablen können in beliebiger Reihenfolge im Ausgabeformat verwendet werden. Konstanter Text kann auch in die Ausgabe eingefügt werden, indem er dem hinzugefügt wird `FORMAT` Feld.

Möglicherweise haben Sie beispielsweise die folgenden Zonennamen für diese Zonenbenennung:

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_Filer_FC1
- S14_Tampa_hostname2_Switch_FC4
- S3991_Boston_Hostname3_windows2K_FC0
- S44_Raleigh_Hostnamen 4_solaris_FC1

Möglicherweise soll die Ausgabe im folgenden Format vorliegen:

```
        [hostname]-[data center]-[device type]
```

Dazu müssen Sie die Felder Hostname, Rechenzentrum und Gerätetyp in Variablen erfassen und in der Ausgabe verwenden. Der folgende reguläre Ausdruck würde dies tun:

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

Da es drei Klammern gibt, die Variablen `\1`, `\2` Und `\3` Würde ausgefüllt werden.

Sie können dann das folgende Format verwenden, um die Ausgabe in Ihrem bevorzugten Format zu

empfangen:

```
\2-\1-\3
```

Ihr Output wäre wie folgt:

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

Die Bindestriche zwischen den Variablen liefern ein Beispiel für konstanten Text, der in die formatierte Ausgabe eingefügt wird.

**Beispiel 1 mit Zonennamen**

In diesem Beispiel verwenden Sie den regulären Ausdruck, um einen Hostnamen aus dem Zonennamen zu extrahieren. Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

Der reguläre Ausdruck, mit dem Sie den Hostnamen erfassen können, lautet:

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

Das Ergebnis ist eine Übereinstimmung aller Zonen, die mit S beginnen, gefolgt von einer beliebigen Kombination von Ziffern, gefolgt von einem Unterstrich, dem alphanumerischen Hostnamen (myComputer1Name), einem Unterstrich oder Bindestrich, den Großbuchstaben HBA und einer einzelnen Ziffer (0-9). Der Hostname allein ist in der Variablen **\1** gespeichert.

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- „S“ steht für den Zonennamen und beginnt den Ausdruck. Dies entspricht nur einem „S“ am Anfang des Zonennamens.
- Die Zeichen [0-9] in Klammern geben an, dass das folgende „S“ eine Ziffer zwischen 0 und 9, einschließlich sein muss.
- Das +-Zeichen gibt an, dass das Auftreten der Informationen in den vorhergehenden Klammern 1 oder mehr Mal bestehen muss.
- Der _ (Unterstrich) bedeutet, dass den Ziffern nach S sofort nur ein Unterstrich im Zonennamen folgen muss. In diesem Beispiel verwendet die Namenskonvention für die Zone den Unterstrich, um den Zonennamen vom Hostnamen zu trennen.
- Nach dem erforderlichen Unterstrich geben die Klammern an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.

- Die in Klammern getierten Zeichen [A-ZA-Z0-9] geben an, dass es sich bei den Zeichen um alle Buchstaben (unabhängig von Groß- und Kleinschreibung) und Zahlen handelt.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die Klammern [_-] (Unterstrich und Strich) geben an, dass dem alphanumerischen Muster ein Unterstrich oder ein Strich folgen muss.
- Die Buchstaben HBA im regulären Ausdruck geben an, dass diese genaue Reihenfolge der Zeichen im Zonennamen erfolgen muss.
- Der letzte Satz mit Klammern [0-9] entspricht einer einstelligen Ziffer von 0 bis 9, inklusive.

**Beispiel 2**

überspringen Sie in diesem Beispiel den ersten Unterstrich "*", dann passen Sie E und alles danach bis zum zweiten "*", und überspringen Sie danach alles.

**Zone:** `Z_E2FHDBS01_E1NETAPP`

**Hostname:** `E2FHDBS01`

**RegExp:** `.?(E.?).*?`

**Beispiel 3**

Die Klammern "( )" um den letzten Abschnitt im regulären Ausdruck (unten) geben an, welcher Teil der Hostname ist. Wenn VSAN3 der Hostname sein soll, lautet dies: _([A-ZA-Z0-9]).*

**Zone:** `A_VSAN3_SR48KENT_A_CX2578_SPA0`

**Hostname:** `SR48KENT`

**RegExp:** `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

**Beispiel 4 zeigt ein komplizierteren Benennungsmuster**

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- MyComputerName123-HBA1_Symm1_FA3
- MyComputerName123-HBA2_Symm1_FA5
- MyComputerName123-HBA3_Symm1_FA7

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
([a-zA-Z0-9]*)_.*
```

Der `\1` Variable würde nur enthalten `myComputerName123` Nach Auswertung durch diesen Ausdruck.

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.

- Die Klammern [A-ZA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig vom Fall) oder jede Ziffer übereinstimmen wird.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Das Zeichen _ (Unterstrich) im regulären Ausdruck bedeutet, dass der Zonenname unmittelbar nach dem alphanumerischen String, der mit den vorangegangenen Klammern übereinstimmt, einen Unterstrich aufweisen muss.
- Der . (Periode) entspricht einem beliebigen Zeichen (ein Platzhalter).
- Das Sternchen * (Sternchen) zeigt an, dass der Platzhalter für den vorherigen Zeitraum 0 oder mehr Mal auftreten kann.

  Mit anderen Worten, die Kombination .* zeigt jedes Zeichen an, jede beliebige Anzahl von Zeiten.

**Beispiel 5 zeigt Zonennamen ohne Muster an**

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- MyComputerName_HBA1_Symm1_FA1
- MyComputerName123_HBA1_Symm1_FA1

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
(.*?)_.*
```

Die Variable \1 enthält *MyComputerName* (im Beispiel für den ersten Zonennamen) oder *myComputerName123* (im Beispiel für den zweiten Zonennamen). Dieser reguläre Ausdruck würde somit alles vor dem ersten Unterstrich entsprechen.

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die ? Charakter macht den Match nicht-gierig. Dies zwingt es, beim ersten Unterstrich nicht beim letzten zu stimmen.
- Die Zeichen _.* entsprechen dem ersten gefundenen Unterstrich und allen Zeichen, die ihm folgen.

**Beispiel 6 zeigt Computernamen mit einem Muster an**

Sie können einen regulären Ausdruck erstellen, wenn Sie etwas Ähnliches wie die folgenden Zonennamen haben:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

Der reguläre Ausdruck, mit dem Sie diese erfassen können, wäre:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Da die Namenskonvention für die Zone mehr ein Muster hat, könnten wir den obigen Ausdruck verwenden, der allen Instanzen eines Hostnamen (MyComputerName im Beispiel) entspricht, der entweder mit Einer A, einem B oder einem T endet und diesen Hostnamen in die \1-Variable setzt.

Der reguläre Ausdruck kann in seine Komponenten unterteilt werden:

- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.
- Die ? Charakter macht den Match nicht-gierig. Dies zwingt es, beim ersten Unterstrich nicht beim letzten zu stimmen.
- Das Unterstrich-Zeichen entspricht dem ersten Unterstrich im Zonennamen.
- Die erste Kombination von .*?_ entspricht somit den Zeichen *Storage1_* im Beispiel des ersten Zonennamens.
- Die zweite *.*?-Kombination verhält sich wie die erste, entspricht aber _Switch1_* im Beispiel für den ersten Zonennamen.
- Die Klammern geben an, dass das in enthaltene Muster in der Variablen \1 gespeichert wird.
- Die Klammern [A-ZA-Z0-9] bedeuten, dass jeder Buchstabe (unabhängig vom Fall) oder jede Ziffer übereinstimmen wird.
- Das * (Sternchen) nach den Klammern zeigt an, dass die Klammern 0 oder mehr Mal auftreten.
- Die Klammern im regulären Ausdruck [ABT] entsprechen einem einzelnen Zeichen im Zonennamen, das A, B oder T. sein muss
- Der _ (Unterstrich) nach den Klammern zeigt an, dass der [ABT]-Zeichenabgleiche einen Unterstrich nachgehen muss.
- Das .* (Periodensternzeichen) stimmt mit einem beliebigen Zeichen überein, beliebig oft.

Das Ergebnis würde daher dazu führen, dass die Variable \1 alle alphanumerischen Zeichenfolgen enthält, die:

- Zuvor waren einige alphanumerische Zeichen und zwei Unterstriche
- Gefolgt von einem Unterstrich (und dann einer beliebigen Anzahl alphanumerischer Zeichen)
- Hatte vor dem dritten Unterstrich einen letzten Charakter von A, B oder T.

**Beispiel 7**

**Zone:** `myComputerName123_HBA1_Symm1_FA1`

**Hostname:** `myComputerName123`

**RegExp:** `([a-zA-Z0-9]+)_.*`

**Beispiel 8**

Dieses Beispiel findet alles vor dem ersten _.

**Zone:** `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

**Hostname:** `MyComputerName`

**RegExp:** `(.?)_.`

**Beispiel 9**

Dieses Beispiel findet alles nach dem 1. _ Und bis zum zweiten _.

**Zone:** `Z_MyComputerName_StorageName`

**Hostname:** `MyComputerName`

**RegExp:** `.?(.?).*?`

**Beispiel 10**

Dieses Beispiel extrahiert „MyComputerName123“ aus den Zonenbeispielen.

**Zone:** `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

**Hostname:** `MyComputerName123`

**RegExp:** `.?.?([a-zA-Z0-9]+)[ABT]_.`

**Beispiel 11**

**Zone:** `Storage1_Switch1_MyComputerName123A_A1_FC1`

**Hostname:** `MyComputerName123A`

**RegExp:** `.?.?([a-zA-z0-9]+).*?`

**Beispiel 12**

Das ^ (circumflex oder caret) **inside Square brackets** negiert den Ausdruck, zum Beispiel [^FF] bedeutet alles außer Groß- oder Kleinbuchstaben F, und [^a-z] bedeutet alles außer Kleinbuchstaben a bis z, und im obigen Fall alles außer _. Die Formatanweisung fügt den Namen des Ausgabehosts in „-“ hinzu.

**Zone:** `mhs_apps44_d_A_10a0_0429`

**Hostname:** `mhs-apps44-d`

**RegExp:** `([^_])_([AB]).*`+Format in OnCommand Insight:

`([^_])_().*`Format in OnCommand Insight:

**Beispiel 13**

In diesem Beispiel wird der Speicher-Alias durch "\" getrennt und der Ausdruck muss mit "\\" definieren, dass tatsächlich "\" in der Zeichenfolge verwendet wird und dass diese nicht Teil des Ausdrucks selbst sind.

**Speicheralias:** `\Hosts\E2DOC01C1\E2DOC01N1`

**Hostname:** `E2DOC01N1`

**RegExp:** `\\.?\\.?\\(.*?)`

**Beispiel 14**

Dieses Beispiel extrahiert „PD-RV-W-AD-2“ aus den Zonenbeispielen.

**Zone:** `PD_D-PD-RV-W-AD-2_01`

**Hostname:** `PD-RV-W-AD-2`

**RegExp:** `[^-]-(.-\d+).+`

**Beispiel 15**

Die Formateinstellung in diesem Fall fügt dem Hostnamen die „US-BV-“ hinzu.

**Zone:** `SRV_USBVM11_F1`

**Hostname:** `US-BV-M11`

**RegExp:** `SRV_USBV([A-Za-z0-9]+)_F[12]`

**Format:** `US-BV-\1`

# Transparenz Aufrechterhalten

Unabhängig davon, ob Sie für Insight neu sind und ein neues System einrichten möchten oder Ihr System bereits seit einiger Zeit in Betrieb ist, müssen Sie Maßnahmen ergreifen, um den reibungslosen Betrieb von Insight und Ihrem Netzwerk aufrechtzuerhalten. Das wichtigste Wartungskonzept ist, dass Änderungen in Ihrem Netzwerk in der Regel in Insight berücksichtigt werden müssen.

Dies sind die häufigsten Wartungsaufgaben:

- Verwalten von Insight-Backups
- Abgelaufene Insight-Lizenzen werden aktualisiert
- Koordination von Patches für Datenquellen
- Aktualisieren der Insight-Version auf allen Erfassungseinheiten
- Löschen von entfernten Datenquellen aus Insight

## Managen Von Insight

OnCommand Insight überwacht Ihre Umgebung und ermöglicht Ihnen die Untersuchung potenzieller Probleme, bevor eine Krise gemeldet wird. Das Asset Dashboard bietet zusammenfassende Kreisdiagramme, Heatmaps für IOPS und ein interaktives Diagramm der 10 am häufigsten verwendeten Speicherpools.

**Schritte**

1. Öffnen Sie das Insight**Assets Dashboard**, und bewegen Sie den Cursor über die Kreisdiagramme, um die Vermögensverteilung in diesen drei Diagrammen zu untersuchen:
   - Die Kapazität nach Anbieter gibt die gesamte Storage-Bruttokapazität für die einzelnen Anbieter an.
   - Die Kapazität nach Tier gibt die nutzbare Gesamtkapazität für die einzelnen Storage-Tiers an.
   - Das Kreisdiagramm Switch Ports zeigt die Hersteller der Ports und den Prozentsatz der verwendeten Ports.
2. Unter **Fakten über Ihre Umgebung** finden Sie Informationen über die genutzte Kapazität Ihrer Umgebung, die Effizienz der Kapazität, die verbrauchten FC-Ressourcen und Statistiken über virtuelle Infrastrukturen.
3. Bewegen Sie den Cursor über eine Speicherpoolleiste im Diagramm **Top 10 Used Pools**, um die genutzte und ungenutzte Kapazität des Speicherpools anzuzeigen.
4. Klicken Sie in der Heatmap **Storage IOP** auf einen beliebigen Anlagennamen, der im Großtext angezeigt wird (was darauf hinweist, dass das Asset Probleme aufweist), um eine Seite anzuzeigen, die den aktuellen Status dieses Assets zusammenfasst.
5. Klicken Sie in der unteren rechten Ecke des **Assets Dashboard** auf einen beliebigen Asset-Namen, der im Großtext angezeigt wird (was darauf hinweist, dass das Asset Probleme hat), um eine Seite anzuzeigen, die den aktuellen Status des Assets zusammenfasst.
6. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
7. Beachten Sie alle Bereiche mit durchgehenden roten Kreisen.

   In der Benutzeroberfläche von OnCommand Insightweb sind potenzielle Probleme mit einem durchgehenden roten Kreis markiert.

8. Klicken Sie auf **Datenquellen**, um eine Liste aller überwachten Datenquellen zu prüfen.

   Untersuchen Sie eine Datenquelle mit einer Spalte **Status**, die eine Nachricht mit einem durchgehenden roten Kreis und mit einem **Impact** als hoch oder Mittel aufgelistet enthält. Diese befinden sich oben auf dem Tisch. Die Probleme mit diesen Datenquellen wirken sich auf einen Großteil Ihres Netzwerks aus, den Sie beheben müssen.

9. Klicken Sie auf **Acquisition Units**, um den Status für jede IP-Adresse zu notieren, die Insight ausführt, und ggf. eine Acquisition Unit neu zu starten
10. Klicken Sie auf **Health**, um die Überwachung der Insight-Server auf hoher Ebene anzuzeigen.

## Monitoring des OnCommand Insight Systemzustands

Sie sollten regelmäßig den aktuellen Status Ihrer Insight Systemkomponenten überprüfen, indem Sie auf der Systemzustandsseite nachsehen, auf der der Status jeder Komponente angezeigt wird und Sie beim Auftreten eines Problems benachrichtigt werden.

**Schritte**

1. Melden Sie sich bei der Insight Web-Benutzeroberfläche an.
2. Klicken Sie auf **Admin** und wählen Sie **Health**.

   Die Seite Systemzustand wird angezeigt.

3. Sehen Sie sich die Zusammenfassung des aktuellen Status der Komponenten an und achten Sie besonders auf jeden Aufmerksamkeitsstatus in der Spalte **Details**, der durch einen roten Kreis vorangestellt ist, der auf ein Problem hinweist, das Sie sofort beachten müssen.

   Auf der Seite Systemzustand werden basierend auf der Systemkonfiguration Informationen zu den folgenden Insight Komponenten angezeigt:

| Komponente | Test | Details | Anzeigen |
|---|---|---|---|
| Akquisition | Verarbeitung von Bestandsdaten | Status der lokalen Erfassungseinheit | „`OK`“, wenn die Anzahl der gleichzeitig abfragenden Datenquellen weniger als 75 % des maximalen Ausführungspools beträgt (Standardwert ist 30). „`Akquisition ist besetzt`“, wenn die Auslastung mehr als 75 % beträgt, empfiehlt, das Abfrageintervall zu erhöhen oder weitere Remote-Akquisitionseinheiten hinzuzufügen. |
| DWH | Backup | Status der geplanten Datensicherung im Data Warehouse | „`OK`“ und die letzte erfolgreiche DWH-Sicherungszeit, wenn die DWH-geplante Sicherung aktiviert ist. Andernfalls werden Informationen über gefundene Fehler angezeigt. |
| DWH | ETL | Status der Data Warehouse ETL | „`OK`“ und die letzte erfolgreiche DWH-Build-Zeit, wenn keine Fehler aufgetreten sind. Andernfalls werden Informationen über gefundene Fehler angezeigt. |

| | | | |
|---|---|---|---|
| Server | ASUP | Status von ASUP | „ASUP enabled“ und, falls verfügbar, die letzte erfolgreiche PhoneHome-Zeit. „ASUP failed“, wenn phonehome aktiviert ist, aber ein Problem aufgetreten ist.<br><br>+ „Ungültiger Sicherungsort“, wenn das Sicherungsverzeichnis ungültig ist.<br><br>+ zeigt die letzte erfolgreiche Telefonhomezeit sowie die Zeit des letzten fehlgeschlagenen Versuchs an, falls verfügbar.<br><br>+ „ASUP disabled“, wenn Phoneho deaktiviert ist. |
| Server | Automatische Auflösung | Status der automatischen Geräteauflösung | „OK“, wenn keine Fehler vorliegen. „Automatische Auflösung ist blockiert“, wenn Identifikationsfehler den Fortschritt der Auflösung verhindern.<br><br>+ „niedrige Erfolgsrate“, wenn weniger als 75 % der generischen Geräte identifiziert werden konnten. |

| | | | |
|---|---|---|---|
| Server | Elasticsearch | Status des Datenspeichers bei elastischen Suchvorgängen | „OK“, wenn keine Fehler vorliegen. „Service nicht verfügbar“, wenn keine Verbindung zum elastischen Suchdienst hergestellt werden kann.<br><br>+ „Cluster Mode detected“, wenn mehr als ein Knoten erkannt wird.<br><br>+ „hohe Speicherauslastung“, wenn der genutzte Heap-Speicherplatz mehr als 85 % beträgt.<br><br>+ "Status: ROT" zeigt einen Fehler an, der von der elastischen Suche gemeldet wird. Zeigt Informationen über den Fehler an und empfiehlt, sich an den Kundendienst zu wenden. |
| Server | CPU | Insight CPU-Auslastung | „OK“, wenn die CPU-Last weniger als 65 % beträgt. „die CPU-Auslastung des Systems ist hoch. Reduzieren Sie Ihre CPU-Auslastung.“ Wenn die CPU-Last größer als 65 % ist. |
| Server | Festplattenspeicher benötigen | Status des Festplattenspeichers | Freier Festplattenspeicher, von Insight belegter Speicherplatz und für Insight reservierter Speicherplatz. „geringer Festplattenspeicher“, wenn die Festplattenauslastung mehr als 80 % beträgt. |

| | | | |
|---|---|---|---|
| Server | EventBus | Status des EventBus | „`EventBus ist leer`“, wenn die EventBus-Warteschlange leer ist, wird andernfalls der Status der EventBus-Warteschlange angezeigt. |
| Server | Verarbeitung von Bestandsdaten | Status der Verarbeitungsfähigkeit von Bestandsdaten des Insight Servers | „`OK`“, wenn der Insight-Server nicht ausgelastet ist. „`Server ist ausgelastet`“, wenn der Server mindestens 75 % der Zeit der letzten Stunde belegt ist. Empfiehlt, keine weiteren Datenquellen hinzuzufügen, und empfiehlt, die Umgebung auf mehrere Server zu verteilen. |
| Server | MySQL | Status der MySQL-Datenbank | „`OK`“, wenn keine Probleme erkannt werden. „`die Datenbank hat Performance-Probleme. Einige Abfragen dauern zu lange, um`" auszuführen, wenn die Anzahl der langsamen Abfragen mehr als 5% beträgt.<br><br>+ "`die Datenbankprotokolldatei wuchs in der letzten Stunde um mehr als <size>. Überprüfen Sie die MySQL-Protokolldatei`“, wenn das Fehlerprotokoll auf mehr als 20 KB anwächst. |
| Server | Performance-Archivierung | Status des Performance-Archivs | „`Performance Archive is enabled`“ oder „`Performance Archive is not enabled`“. |

| | | | |
|---|---|---|---|
| Server | Physischer Speicher | Status des physischen Speichers | „OK“, wenn die Speicherauslastung unter 85 % liegt. „die Speichernutzung ist hoch. Reduzieren Sie den gesamten Speicherbedarf für Systemstabilität“, wenn der Speicherverbrauch über 85 % liegt. |
| Server | Service Pack | Verfügbarkeit des Service Packs | Zeigt an, ob ein Service Pack für Insight verfügbar ist. Wenn ein Service Pack verfügbar ist, werden Anweisungen angezeigt. |
| Server | Verwendungsinformationen | Status des Versands von Nutzungsinformationen | Zeigt an, ob das Senden von Nutzungsinformationen an NetApp aktiviert oder deaktiviert ist. Empfiehlt die Aktivierung, falls deaktiviert. Zeigt die letzte oder letzte erfolgreiche Sendezeit an.<br><br>+ zeigt Informationen zu aufgetretenen Problemen an. |

| | | | |
|---|---|---|---|
| Server | Verletzung | Status offener Verstöße | „OK“, wenn die Anzahl der offenen Verstöße weniger als 75 % des Grenzwerts für Verstöße ist. „maximal zulässige Anzahl offener Verstöße ist <number>“, wenn die Anzahl der offenen Verstöße größer als 75 % des Grenzwerts für Verstöße ist. Empfiehlt, die Konfiguration der Performance-Richtlinien zu überprüfen.<br><br>+ „Verletzungsmanager ist blockiert“, wenn die Anzahl der offenen Verstöße am Grenzwert für Verstöße liegt.<br><br>+ Beachten Sie, dass der Verletzer-Manager keine neuen Verstöße erstellen kann und empfiehlt, die Konfiguration der Leistungsrichtlinien zu überprüfen. |
| Server | Wöchentliches Backup | Status der wöchentlichen Sicherung | „OK“, wenn die wöchentliche Sicherung aktiviert ist, wird andernfalls „die wöchentliche Sicherung ist nicht aktiviert“ angezeigt. |

## Inaktive Geräte werden gelöscht

Das Löschen inaktiver Geräte hilft dabei, Ihre Daten sauberer und übersichtlicher zu machen.

### Über diese Aufgabe

Gehen Sie wie folgt vor, um inaktive Geräte aus Insight zu löschen:

**Schritte**

1. Erstellen Sie eine neue Abfrage oder öffnen Sie eine vorhandene Abfrage.
2. Wählen Sie entweder den Asset-Typ *generic device*, *Host*, *Storage*,*Switch* oder *Tape*.
3. Fügen Sie einen Filter für **is Active** hinzu und setzen Sie den Filter auf **No**.

   In der Ergebnistabelle werden nur nicht aktive Assets angezeigt.

4. Wählen Sie die Geräte aus, die Sie löschen möchten.
5. Klicken Sie auf die Schaltfläche **actions** und wählen Sie **inaktive Geräte löschen**.

   Ihre inaktiven Geräte werden gelöscht und nicht mehr in Insight angezeigt.

## Überwachen von System- und Benutzeraktivitäten

Wenn Sie unerwartete Änderungen suchen möchten, können Sie einen Audit-Trail des OnCommand Insight-Systems und seiner Benutzeraktivitäten anzeigen. Audit-Protokollmeldungen können optional an syslog gesendet werden, zusätzlich zur Anzeige auf der Seite „Audit“.

**Über diese Aufgabe**

Insight generiert Audit-Einträge für alle Benutzeraktivitäten, die sich auf das Storage-Netzwerk oder dessen Management auswirken, darunter:

- Anmelden
- Autorisieren oder Entautorisieren eines Pfads
- Aktualisieren eines autorisierten Pfads
- Festlegen globaler Richtlinien oder Schwellenwerte
- Hinzufügen oder Entfernen einer Datenquelle
- Starten oder Stoppen einer Datenquelle
- Eigenschaften der Datenquelle werden aktualisiert
- Hinzufügen, Bearbeiten oder Löschen einer Aufgabe
- Entfernen einer Anwendungsgruppe
- Identifizieren oder Ändern der Identifikation eines Geräts
- Erstellen Sie einen Benutzer
- Löschen Sie einen Benutzer
- Änderung der Benutzerrolle
- Ändern eines Benutzers (Gast à Admin)
- Abmelden eines Benutzers (entweder erzwungene Abmeldung oder manuelle Abmeldung)
- Löschen einer Erfassungseinheit
- Lizenz Aktualisieren
- Aktivieren der Sicherung

- Deaktivieren Der Sicherung
- Aktivieren von ASUP (die Aktivierung von Proxy auf derselben Seite wird im Revisionsprotokoll gemeldet)
- Deaktivieren von ASUP (Deaktivieren von Proxy auf derselben Seite wird im Auditprotokoll gemeldet)
- Sicherheit – Neuschlüssel, Ändern der Systemkennwörter.
- Entfernen/Hinzufügen von Anmerkungen zu Anlagen
- CAC-Benutzeranmeldung/Abmeldung
- CAC-Benutzersitzungszeitlimit

**Schritte**

1. Öffnen Sie Insight in Ihrem Browser.
2. Klicken Sie auf **Admin** und wählen Sie **Audit**.

   Auf der Seite Audit werden die Audit-Einträge in einer Tabelle angezeigt.

3. Sie können die folgenden Details in der Tabelle anzeigen:

   - **Zeit**

     Datum und Uhrzeit der Änderungen

   - * Benutzer*

     Name des Benutzers, der dem Überwachungseintrag zugeordnet ist

   - * Rolle*

     Die Rolle des Benutzerkontos, d. h. Gast, Benutzer oder Administrator

   - **IP**

     Mit dem Überwachungseintrag verknüpfte IP-Adresse

   - **Aktion**

     Art der Aktivität im Audit-Eintrag

   - **Details**

     Details zum Audit-Eintrag

     Wenn eine Benutzeraktivität vorhanden ist, die sich auf eine Ressource auswirkt, z. B. eine Datenquelle oder eine Anwendung, enthalten die Details einen Link zur Landing Page der Ressource.

     Wenn eine Datenquelle gelöscht wird, enthalten die Details der Benutzeraktivität, die sich auf die Datenquelle beziehen, keinen Link mehr zur Landing Page der Datenquelle.

4. Sie können Überwachungseinträge anzeigen, indem Sie einen bestimmten Zeitraum (1 Stunde, 3 Stunden, 24 Stunden, 3 Tage und 7 Tage) auswählen, Mit Insight, die eine maximale Anzahl von 1000 Verstößen für den ausgewählten Zeitraum anzeigt.

   Sie können auf eine Seitenzahl unter der Tabelle klicken, um Daten nach Seite zu durchsuchen, wenn

mehr Daten als auf eine einzelne Seite passen.

5. Sie ändern die Sortierreihenfolge der Spalten in einer Tabelle entweder aufsteigend (Aufwärtspfeil) oder absteigend (Abwärtspfeil), indem Sie auf den Pfeil in der Spaltenüberschrift klicken. Um zur Standardsortierreihenfolge zurückzukehren, klicken Sie auf eine beliebige andere Spaltenüberschrift.

   Standardmäßig werden die Einträge in absteigender Reihenfolge in der Tabelle angezeigt.

6. Sie können das Feld **Filter** verwenden, um nur die Einträge anzuzeigen, die Sie in der Tabelle haben möchten.

   Um nur die Audit-Einträge durch den Benutzer anzuzeigen `izzyk`Geben Sie ein `izzyk` Im Feld **Filter**.

## Überwachung der Verstöße in Ihrem Netzwerk

Wenn Insight aufgrund der in den Performance-Richtlinien festgelegten Schwellenwerte Verstöße generiert, können Sie diese über das Dashboard für Verstöße anzeigen. Das Dashboard listet alle Verstöße auf, die in Ihrem Netzwerk auftreten, und ermöglicht es Ihnen, Probleme zu lokalisieren und zu beheben.

### Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser.
2. Klicken Sie in der Insight-Symbolleiste auf **Dashboards** und wählen Sie **Dashboard für Verstöße**.

   Das Dashboard „Verstöße“ wird angezeigt.

3. Sie können das Kreisdiagramm **Verstöße nach Richtlinien** auf folgende Weise verwenden:
   - Sie können den Cursor über einen beliebigen Diagrammabschnitt bewegen, um den Prozentsatz der Gesamtverletzungen anzuzeigen, die für eine bestimmte Richtlinie oder Metrik aufgetreten sind.
   - Sie können auf eine Schicht eines Diagramms klicken, um es „`vergrößern`“ zu öffnen. Dadurch können Sie diese Schicht hervorheben und genauer untersuchen, indem Sie sie vom Rest des Diagramms entfernen.
   - Sie können auf klicken Symbol in der oberen rechten Ecke, um das Kreisdiagramm im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren. Ein Kreisdiagramm kann maximal fünf Schichten enthalten. Wenn Sie also sechs Richtlinien haben, die Verstöße erzeugen, kombiniert Insight die fünfte und sechste Schicht in einem „`others`“-Slice. Insight weist der ersten Schicht die meisten Verstöße zu, der zweiten die zweithäufigsten Verstöße usw.
4. Sie können das Diagramm **Historie der Verstöße** auf folgende Weise verwenden:
   - Sie können den Cursor über das Diagramm bewegen, um die Gesamtzahl der zu einem bestimmten Zeitpunkt aufgetretenen Verstöße und die Anzahl der aufgetretenen Verstöße für jede angegebene Metrik anzuzeigen.
   - Sie können auf eine Legende klicken, um die mit der Legende verknüpften Daten aus dem Diagramm zu entfernen.

     Klicken Sie auf die Legende, um die Daten erneut anzuzeigen.

   - Sie können auf klicken Symbol in der oberen rechten Ecke, um die Karte im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren.

5. Sie können die **Tabelle der Verstöße** auf folgende Weise verwenden:
   - Sie können auf klicken Symbol in der oberen rechten Ecke, um die Tabelle im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren.

     Wenn Ihre Fenstergröße zu klein ist, werden in der Tabelle „Verstöße“ nur drei Spalten angezeigt, wenn Sie jedoch auf klicken, Zusätzliche Spalten (bis zu sieben) werden angezeigt.
   - Sie können Verstöße für einen bestimmten Zeitraum anzeigen (**1h**, **3h**, **24h**, **3d**, **7d**, Und **30d**), wobei Insight eine maximale Anzahl von 1000 Verstößen für den ausgewählten Zeitraum anzeigt.
   - Sie können das Feld **Filter** verwenden, um nur die gewünschten Verstöße anzuzeigen.
   - Sie können die Sortierreihenfolge der Spalten in einer Tabelle entweder aufsteigend (Aufwärtspfeil) oder absteigend (Abwärtspfeil) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken. Um zur Standardsortierreihenfolge zurückzukehren, klicken Sie auf eine beliebige andere Spaltenüberschrift.

     Standardmäßig werden die Verstöße in absteigender Reihenfolge in der Tabelle angezeigt.
   - Sie können in der Spalte „ID“ auf eine Verletzung klicken, um die Seite „Anlage“ für die Dauer der Verletzung anzuzeigen.
   - Sie können in der Spalte Beschreibung auf die Ressourcenverknüpfungen (z. B. Speicherpool und Speichervolume) klicken, um die mit diesen Ressourcen verknüpften Asset-Seiten anzuzeigen.
   - Sie können auf den Link Leistungsrichtlinie in der Spalte Richtlinie klicken, um das Dialogfeld Richtlinie bearbeiten anzuzeigen.

     Sie können die Schwellenwerte für eine Richtlinie anpassen, wenn Sie der Ansicht sind, dass sie zu wenige oder zu viele Verstöße verursacht.
   - Sie können auf eine Seitenzahl klicken, um Daten nach Seite zu durchsuchen, wenn mehr Daten als auf eine einzelne Seite passen.
   - Klicken Sie auf Um den Verstoß zu verwerfen.

## Status der Erfassungseinheit

Der Bildschirm „Acquisition Unit“ bietet eine Übersicht über alle Ihre Akquisitionseinheiten, einschließlich des Status und aller vorhandenen Fehler.

Der Status der mit Ihrem Server verbundenen Insight-Erfassungseinheiten wird in der Tabelle **Admin** > **Acquisition Units** angezeigt. In dieser Tabelle werden die folgenden Informationen für jede Erfassungseinheit angezeigt:

- **Name**
- **IP**
- **Status** ist der Betriebszustand der Erfassungseinheit.
- **Letzte Meldung**zeigt das letzte Mal an, wenn eine Datenquelle mit der Erfassungseinheit verbunden wurde.
- **Hinweis** zeigt eine vom Benutzer eingegebene Notiz im Zusammenhang mit der AU an.

Wenn bei einer Erfassungseinheit in der Liste ein Problem auftritt, zeigt das Feld Status einen roten Kreis mit kurzen Informationen zum Problem an. Sie sollten alle Probleme mit den Erfassungseinheiten untersuchen, da diese sich wahrscheinlich auf die Datenerfassung auswirken.

Um eine Erfassungseinheit neu zu starten, bewegen Sie den Mauszeiger über das Gerät und klicken Sie auf die Schaltfläche *Neustarten der Erfassungseinheit*, die angezeigt wird.

Um eine Textnotiz hinzuzufügen, bewegen Sie den Mauszeiger über eine Erfassungseinheit, und klicken Sie auf die Schaltfläche „*Notiz hinzufügen*“, die angezeigt wird. Es wird nur die zuletzt eingegebene Notiz angezeigt.

## Wiederherstellen der Insight-Datenbank

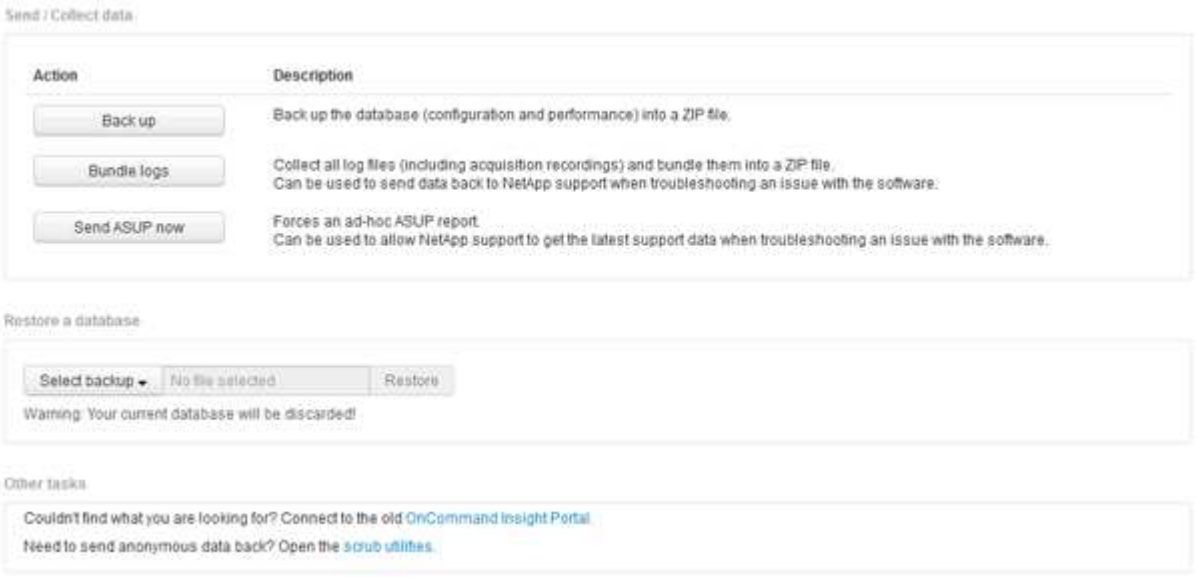
Um Ihre Insight-Datenbank aus einer verifizierten Sicherungsdatei wiederherzustellen, verwenden Sie die Fehlerbehebungsoptionen. Dieser Vorgang ersetzt Ihre aktuellen OnCommand Insight-Daten vollständig.

### Bevor Sie beginnen

**Best Practice:**bevor Sie Ihre OnCommand Insight-Datenbank wiederherstellen, verwenden Sie den manuellen Sicherungsprozess, um eine Kopie der aktuellen Datenbank zu erstellen. Überprüfen Sie die Sicherungsdatei, die Sie wiederherstellen möchten, um sicherzustellen, dass es sich um ein erfolgreiches Backup mit den Dateien handelt, die Sie wiederherstellen möchten.

### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Fehlerbehebung**.




3. Wählen Sie im Abschnitt Datenbank wiederherstellen aus dem Menü **Backup auswählen** die Sicherungsdatei aus, die Sie wiederherstellen möchten.
4. Klicken Sie Auf **Wiederherstellen**.
5. Klicken Sie in der Warnung, dass alle Daten ersetzt werden, auf **OK**

   Der Status der Wiederherstellungsaktivität wird auf der Wiederherstellungsseite angezeigt.

## Abgelaufene Lizenzen werden aktualisiert

Wenn eine oder mehrere Ihrer Insight-Lizenzen abgelaufen sind, können Sie die Lizenzen schnell mit demselben Verfahren aktualisieren, wie Sie die Lizenzen ursprünglich installiert haben.

### Schritte

1. Öffnen Sie in einem Text-Editor, z. B. Editor, die neue Lizenzdatei, die Sie vom NetApp Support erhalten haben, und kopieren Sie den Text des Lizenzschlüssels in die Zwischenablage in Windows.
2. Öffnen Sie OnCommand Insight in Ihrem Browser.
3. Klicken Sie in der Symbolleiste auf **Admin**.
4. Klicken Sie Auf **Setup**.
5. Klicken Sie auf die Registerkarte **Lizenzen**.
6. Klicken Sie Auf **Lizenz Aktualisieren**.
7. Kopieren Sie den Text des Lizenzschlüssels in das Textfeld **Lizenz**.
8. Wählen Sie den Vorgang **Update (am häufigsten)** aus.

   Durch diesen Vorgang werden Ihre neuen Lizenzen allen derzeit aktiven Insight-Lizenzen hinzugefügt.
9. Klicken Sie Auf **Speichern**.
10. Wenn Sie das Insight Consumption Licensing-Modell verwenden, müssen Sie das Kontrollkästchen aktivieren, um das Senden von Nutzungsinformationen an NetApp im Abschnitt „Verwendung“ zu aktivieren. Proxy muss ordnungsgemäß konfiguriert und für Ihre Umgebung aktiviert sein.

### Lizenzen sind nicht mehr kompatibel

Wenn Sie auf der Insight-Lizenzseite die Meldung „nicht konform“ sehen, verwaltet Insight mehr Terabyte als Ihr Unternehmen lizenziert hat.

Die Meldung „nicht konform“ bedeutet, dass Ihr Unternehmen für weniger Terabyte bezahlt hat, als Insight derzeit verwaltet. Der Unterschied zwischen den verwalteten Terabytes und der lizenzierten Anzahl von Terabytes wird neben der Meldung „Nichteinhaltung“ angezeigt.

Der Betrieb Ihres Insight Systems wird dadurch nicht beeinträchtigt, wenden Sie sich jedoch an Ihren NetApp Ansprechpartner, um Ihren Lizenzabdeckung zu erhöhen und die entsprechende Lizenz zu aktualisieren.

### Ersetzen von Lizenzen für ältere Insight-Versionen

Wenn Sie eine neue Insight-Version erworben haben, die nicht abwärtskompatibel mit Ihrer älteren Version des Produkts ist, müssen Sie die älteren Lizenzen durch die neuen Lizenzen ersetzen.

Wenn Sie die neuen Lizenzen installieren, müssen Sie den Vorgang **Replace** auswählen, bevor Sie den Text des Lizenzschlüssels speichern.

## Anwenden eines Service Packs

Es sind regelmäßig Service Packs verfügbar, die Sie anwenden können, um die Vorteile von Fixes und Verbesserungen an OnCommand Insight zu nutzen.

#### Bevor Sie beginnen

- Sie müssen die Service Pack-Datei heruntergeladen haben (z. B. `7.2service_pack_1.patch`) Aus der NOW Site.
- Sie müssen alle Patches genehmigt haben.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Patches**.
3. Wählen Sie über die Schaltfläche Aktionen die Option **Patch anwenden** aus.
4. Klicken Sie im Dialogfeld **Data source Patch anwenden** auf **Browse**, um die Service Pack-Datei zu suchen.
5. Überprüfen Sie **Patch-Name**, **Beschreibung**, **betroffene Datenquellentypen**, die anzeigen, ob Datenquellen betroffen sind, und **Details**, welche die Verbesserungen beschreiben, die das Service Pack enthält.
6. Wenn das ausgewählte Service Pack korrekt ist, klicken Sie auf **Patch anwenden**.

   Service Packs werden automatisch genehmigt, weitere Maßnahmen sind nicht erforderlich.

## Vorbereiten eines speziellen Fehlersuchberichts

Insight sendet automatisch über das von Ihnen nach der Installation der Software festgelegte ASUP System Informationen an den NetApp Kunden-Support. Möglicherweise möchten Sie jedoch einen Fehlerbehebungsbericht erstellen und beim Support-Team einen Fall für ein bestimmtes Problem eröffnen.

In Insight können Sie mit den Tools ein manuelles Insight Backup durchführen, die Protokolle bündeln und diese Informationen an den NetApp Customer Support senden.

#### Manuelles Backup der OnCommand Insight-Datenbank

Wenn Sie wöchentliche Backups für die OnCommand Insight-Datenbank aktiviert haben, erstellen Sie automatisch Kopien, mit denen Sie die Datenbank bei Bedarf wiederherstellen können. Wenn Sie vor der Wiederherstellung ein Backup erstellen oder an den technischen Support von NetApp senden müssen, um Hilfe zu erhalten, können Sie ein Backup erstellen `.zip` Datei manuell erstellen.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Fehlerbehebung**.

3. Klicken Sie im Abschnitt Daten senden/sammeln auf **Backup**.
4. Klicken Sie Auf **Datei Speichern**.
5. Klicken Sie auf **OK**.

#### Bündelung der Protokolle für den Support

Wenn Sie ein Problem mit der Insight Software beheben, können Sie schnell eine ZIP-Datei (im „gz“-Format) der Protokolle und Aufnahmeaufzeichnungen erstellen, die an den NetApp Customer Support gesendet werden sollen.

##### Schritte

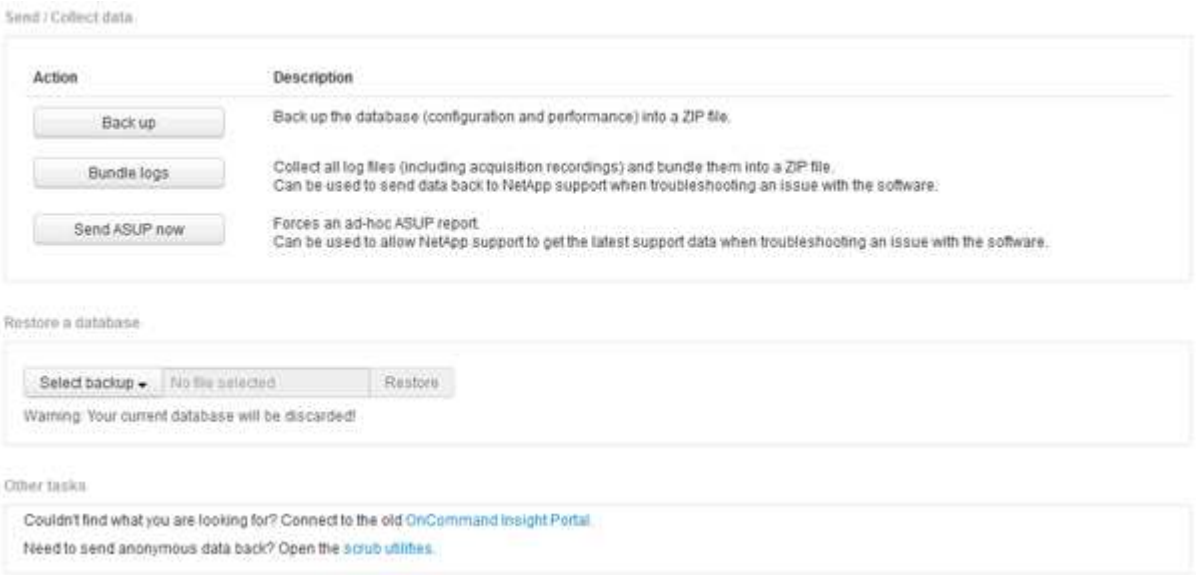
1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt Daten senden/erfassen auf **Paketprotokolle**.
4. Klicken Sie Auf **Datei Speichern**.
5. Klicken Sie auf **OK**.

#### Senden von Informationen an den NetApp Support

Über die automatische Support-Einrichtung (ASUP) von NetApp werden Fehlerbehebungsinformationen direkt an das NetApp Kundensupportteam gesendet. Sie können das Senden eines speziellen Berichts erzwingen.

##### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Setup**.
3. Klicken Sie auf die Registerkarte **Backup/ASUP**.
4. Klicken Sie im Bereich Daten senden/erfassen auf **ASUP jetzt senden**, um Ihre Protokolle, Aufzeichnungen und Backups an den NetApp Support zu senden.



### Bereinigung von Daten für die Übertragung an den Support

Kunden mit sicheren Umgebungen müssen mit dem NetApp Customer Service kommunizieren, um Probleme zu beheben, die entstehen, ohne die Datenbankinformationen zu gefährden. Mit den OnCommand Insight Scrub-Dienstprogrammen können Sie ein umfassendes Wörterbuch von Schlüsselwörtern und Mustern einrichten, sodass Sie sensible Daten „bereinigen“ und gereinigte Dateien an den Kundendienst senden können.

#### Schritte

1. Klicken Sie in der Web-Benutzeroberfläche auf **Admin** und wählen Sie **Troubleshooting**.
2. Klicken Sie unten auf der Seite im Bereich andere Aufgaben auf den Link **Scrub Utilities**.

   Es gibt mehrere Scrub-Abschnitte: Suche im Wörterbuch, Scrub-Daten, Build-Wörterbuch, Benutzerdefinierte Schlüsselwörter und reguläre Ausdrücke.

.

+
.. Geben Sie im Abschnitt**Suche im Wörterbuch** einen Code ein, um den Wert anzuzeigen, den er ersetzt, oder geben Sie einen Wert ein, um den Code zu sehen, der ihn ersetzt. Hinweis: Bevor Sie eine Suche machen können, müssen Sie das Wörterbuch **build** erstellen, um Werte zu identifizieren, die aus den Support-Daten schrubben sollen.

1. Um Ihre eigenen Schlüsselwörter hinzuzufügen, die aus den Support-Daten gescrub werden sollen, klicken Sie im Abschnitt **Benutzerdefinierte Schlüsselwörter** auf MENU:Actions[Benutzerdefiniertes Schlüsselwort hinzufügen]. Geben Sie ein Schlüsselwort ein und klicken Sie auf **Speichern**. Das Schlüsselwort wird dem Wörterbuch hinzugefügt.
2. Erweitern Sie * Muster (regexp)**. Klicken Sie auf *Hinzufügen**, um das Dialogfeld zur Eingabe eines neuen Musters aufzurufen.
3. Um einen regulären Ausdruck zu verwenden, um Wörter oder Sätze zu identifizieren, die zu schrubben sind, geben Sie ein Muster oder Muster im Abschnitt **reguläre Ausdrücke** ein. Klicken Sie auf **Actions › Add Regular Expression**, geben Sie einen Namen für das Muster und den regulären Ausdruck in die Felder ein und klicken Sie auf **Save**. Die Informationen wurden dem Wörterbuch hinzugefügt.

   Muster müssen durch runde Klammern umschlossen werden, um eine Gruppe zu identifizieren, die einen regulären Ausdruck erfasst.

4. Klicken Sie im Abschnitt**build dictionary** auf **build**, um die Zusammenstellung des Wörterbuchs aller Wörter, die als sensibel aus der OnCommand Insight-Datenbank identifiziert wurden, zu initiieren.

   Wenn Sie fertig sind, wird eine Aufforderung angezeigt, die Sie darüber informiert, dass das überarbeitete Wörterbuch verfügbar ist. Die Datenbankbeschreibung enthält eine Zeile, die angibt, wie viele Schlüsselwörter im Wörterbuch enthalten sind. Überprüfen Sie Ihre Suchbegriffe im Wörterbuch auf Genauigkeit. Wenn Sie Probleme finden und das Wörterbuch neu erstellen möchten, klicken Sie im Datenbankblock auf **Zurücksetzen**, um alle aus der OnCommand Insight-Datenbank gesammelten Schlüsselwörter aus dem Wörterbuch zu entfernen. Wie die Aufforderung mitteilt, werden keine anderen Schlüsselwörter gelöscht. Kehren Sie zu den Scrub-Dienstprogrammen zurück, und geben Sie Ihre benutzerdefinierten Schlüsselwörter erneut ein.

5. Nachdem Sie ein Scrub-Wörterbuch erstellt haben, können Sie es verwenden, um eine Protokoll-, XML- oder andere Textdatei zu scrub, um die Daten anonym zu machen.
6. Um eine Log-, XML- oder andere Textdatei zu scrub, navigieren Sie im Abschnitt **Scrub-Daten** nach der Datei und klicken Sie auf **Scrub-Datei**.

## Erweiterte Fehlerbehebung

Um die OnCommand Insight-Konfiguration abzuschließen, müssen Sie die erweiterten Tools zur Fehlerbehebung verwenden. Diese Tools laufen im Browser und werden auf der Seite **Admin** > **Troubleshooting** geöffnet.

Um die erweiterten Tools zur Fehlerbehebung im Browser zu öffnen, klicken Sie unten auf der Seite auf den Link **Erweiterte Fehlerbehebung**.

Mit den erweiterten Fehlerbehebungstools können Sie verschiedene Berichte, Systeminformationen, installierte Pakete und Protokolle anzeigen sowie zahlreiche Aktionen ausführen, wie z. B. den Neustart des Servers oder der Erfassungseinheiten, die Aktualisierung von DWH-Anmerkungen und den Import von Anmerkungen.

Alle verfügbaren Optionen finden Sie auf der Seite Erweiterte Fehlerbehebung.

#### Konfigurieren der Anzahl der Stunden, die dynamische Daten ignorieren sollen

Sie können die Anzahl der Stunden konfigurieren, in denen OnCommand Insight die Aktualisierung dynamischer Daten ignoriert, z. B. die verwendete Kapazität. Wenn die Standardeinstellung von sechs Stunden verwendet wird und keine Konfigurationsänderungen vorgenommen werden, werden die Berichte erst nach der Standardstundenzahl mit dynamischen Daten aktualisiert. Diese Option verbessert die Leistung, da diese Option Aktualisierungen deaktiviert, wenn sich nur die dynamischen Daten ändern.

##### Über diese Aufgabe

Wenn für diese Option ein Wert festgelegt wird, aktualisiert OnCommand Insight dynamische Daten auf der Grundlage der folgenden Regeln:

- Wenn keine Konfigurationsänderungen auftreten, aber Kapazitätsdaten geändert werden, werden die Daten nicht aktualisiert.
- Dynamische Daten (außer Konfigurationsänderungen) werden erst nach dem in dieser Option angegebenen Timeout aktualisiert.
- Bei Konfigurationsänderungen werden Konfigurations- und dynamische Daten aktualisiert.

Dynamische Daten, die von dieser Option betroffen sind, umfassen Folgendes:

- Daten zu Kapazitätsverletzungen
- Dateisysteme zugewiesene Kapazität und genutzte Kapazität
- Hypervisor
  - Genutzte Kapazität Des Virtuellen Laufwerks
  - Genutzte Kapazität Der Virtual Machine

- Internes Volumen
  - Zugewiesener Speicherplatz
  - Genutzte Kapazität Von Daten
  - Einsparungen Durch Deduplizierung
  - Zuletzt Bekannte Zugriffszeit
  - Zeitpunkt Des Letzten Snapshots
  - Andere Genutzte Kapazität
  - Anzahl Snapshots
  - Verwendete Snapshot-Kapazität
  - Insgesamt Genutzte Kapazität
- ISCSI-Session-Initiator-IPs, Ziel-Session-ID und Initiator-Session-ID
- Genutzte Kapazität Von Qtree-Kontingent
- Verwendete Dateien und genutzte Kapazität quota
- Storage-Effizienz-Technologie, Gewinn/Verlust und potenzieller Gewinn/Verlust
- Storage-Pool
  - Genutzte Kapazität Von Daten
  - Einsparungen Durch Deduplizierung
  - Andere Genutzte Kapazität
  - Verwendete Snapshot-Kapazität
  - Insgesamt Genutzte Kapazität
- Datenmenge
  - Einsparungen Durch Deduplizierung
  - Zuletzt Bekannte Zugriffszeit
  - Genutzte Kapazität

**Schritte**

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf die Registerkarte **Erweiterte Einstellungen**, geben Sie im Abschnitt dynamische Attribute der Erfassung die Anzahl der Stunden ein, die OnCommand Insight dynamische Daten für dynamische Attribute der Erfassung ignorieren soll.
4. Klicken Sie Auf **Speichern**.
5. (Optional) um die Erfassungseinheit neu zu starten, klicken Sie auf den Link **Erfassungseinheit neu starten**.

   Bei der Wiederherstellung der lokalen Erfassungseinheit werden alle OnCommand Insight-Datenquellansichten neu geladen. Diese Änderung wird während der nächsten Abfrage übernommen, sodass Sie die Erfassungseinheit nicht neu starten müssen.

### Erstellen von Protokollen für den Kundendienst

Generieren Sie auf Anfrage des Kundensupports einen Server, eine Akquisition oder ein Remote-Protokoll zur Fehlerbehebung.

#### Über diese Aufgabe

Wenn der NetApp Kundensupport Anfragen, verwenden Sie diese Option, um die Protokolle zu generieren.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der nächsten Seite im Menü Erweitert auf den Link **Fehlerbehebung**.
4. Klicken Sie auf die Registerkarte **Logs** und wählen Sie die Protokolldatei zum Herunterladen aus.

   Es wird ein Dialogfeld geöffnet, in dem Sie das Protokoll öffnen oder lokal speichern können.

### Anzeigen von Systeminformationen

Sie können die Microsoft Windows IP-Konfigurationsinformationen über das System anzeigen, auf dem der OnCommand Insight-Server bereitgestellt wird.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Seite Erweiterte Fehlerbehebung auf die Registerkarte **Reports**.
4. Klicken Sie Auf **Systeminformationen**.

   Die Windows-IP-Konfiguration umfasst Informationen wie Hostname, DNS, IP-Adresse, Subnetzmaske, Betriebssysteminformationen, Speicher, Startgerät und Verbindungsname.

### Auflisten der installierten OnCommand Insight-Komponenten

Sie können eine Liste der installierten OnCommand Insight-Komponenten anzeigen, darunter unter anderem Inventar, Kapazität, Abmessungen, Und die Data Warehouse-Ansichten. Der Customer Support fragt Sie möglicherweise nach diesen Informationen, oder Sie möchten vielleicht sehen, welche Softwareversionen installiert wurden und wann sie installiert wurden.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Seite Erweiterte Fehlerbehebung auf die Registerkarte **Reports**.
4. Klicken Sie Auf **Installierte Softwarepakete**.

### Berechnung der Anzahl der Datenbankobjekte

Verwenden Sie die Funktion Skalierung berechnen, um die Anzahl der Objekte in der OnCommand Insight-Datenbank zu ermitteln.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Seite Erweiterte Fehlerbehebung auf die Registerkarte **Reports**.
4. Klicken Sie Auf **Berechnete Skala**.

### OnCommand Insight-Server wird neu gestartet

Wenn Sie den OnCommand Insight-Server neu starten, aktualisieren Sie die Seite, und melden Sie sich erneut beim OnCommand Insight-Portal an.

#### Über diese Aufgabe

Beide Optionen sollten nur auf Anfrage durch den NetApp Kunden-Support genutzt werden. Vor dem Neustart erfolgt keine Bestätigung.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der nächsten Seite im Menü Erweitert auf die Registerkarte **Aktionen**.
4. Klicken Sie Auf **Server Neu Starten**.

### Verschieben von MySQL Daten mit der Option „Migrate“

Sie können das MySQL-Datenverzeichnis in ein anderes Verzeichnis migrieren. Sie können das aktuelle Datenverzeichnis beibehalten. Sie können die Option „Migrieren“ im Menü „Fehlerbehebung“ verwenden oder die Befehlszeile verwenden. Dieses Verfahren beschreibt die Verwendung der Option **Fehlerbehebung** > **MySQL-Daten migrieren**.

#### Über diese Aufgabe

Wenn Sie das aktuelle Datenverzeichnis beibehalten, wird es als Backup beibehalten und umbenannt.

#### Schritte

1. Klicken Sie in der Web-Benutzeroberfläche auf **Admin** und wählen Sie **Troubleshooting**.
2. Klicken Sie Auf **Erweiterte Fehlerbehebung**.
3. Wählen Sie die Registerkarte **actions**
4. Wählen Sie **MySQL-Daten migrieren**.
5. Geben Sie den Pfad ein, auf den Sie die Daten migrieren möchten.

6. Um das vorhandene Datenverzeichnis beizubehalten, aktivieren Sie **bestehendes Datenverzeichnis beibehalten.**
7. Klicken Sie Auf * Migrieren*.

#### MySQL-Daten werden über die Befehlszeile verschoben

Sie können das MySQL-Datenverzeichnis in ein anderes Verzeichnis migrieren. Sie können das aktuelle Datenverzeichnis beibehalten. Sie können die Option „Migrieren“ im Menü „Fehlerbehebung“ verwenden oder alternativ die Befehlszeile verwenden. In diesem Verfahren wird die Verwendung der Befehlszeile beschrieben.

**Über diese Aufgabe**

Wenn Sie das aktuelle Datenverzeichnis beibehalten, wird es als Backup beibehalten und umbenannt.

Sie können das Dienstprogramm MySQL Data migrieren verwenden oder ein verwenden `java -jar mysqldatamigrator.jar` Option im OnCommand Insight-Pfad von `\bin\mysqldatamigrator` Dabei sollten die folgenden Parameter verwendet werden:

- Obligatorische Parameter
  - **-Pfad**

    Der neue Datenpfad, in den der Datenordner kopiert wird.
- Optionale Parameter
  - **-myCnf <my .cnf file>**

    Der Pfad für die .cnf-Datei. Die Standardeinstellung lautet `<install path>\mysql\my.cnf`. Verwenden Sie dieses Flag nur, wenn ein nicht standardmäßiges MySQL verwendet wird.
  - **-doBackup**

    Wenn dieses Flag gesetzt ist, wird der aktuelle Datenordner umbenannt, aber nicht gelöscht.

**Schritte**

1. Greifen Sie hier auf das Befehlszeilen-Tool zu: `<installation path>` \Bin\mysqldatamigrator\mysqldatamigrator.jar``

**Beispielverwendung**

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

#### Erzwingen von Anmerkungsaktualisierungen

Wenn Sie die Anmerkungen geändert haben und sie sofort in Berichten verwenden möchten, verwenden Sie eine der Optionen für Anmerkungen erzwingen.

#### Schritte

1. Klicken Sie in der Web-Benutzeroberfläche auf **Admin** und wählen Sie **Troubleshooting**.
2. Klicken Sie unten auf der Seite auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf die Registerkarte **actions**.
4. Wählen Sie eine der folgenden Optionen aus:
   - **Aktualisierung der DWH-Anmerkungen**, um die Aktualisierung von Anmerkungen im Data Warehouse für Berichte zu erzwingen.
   - **DWH-Anmerkungen aktualisieren (inkl. Gelöscht)**, um eine Aktualisierung von Anmerkungen (einschließlich gelöschter Objekte) im Data Warehouse zu erzwingen, die für Berichte verwendet werden soll.

### Überprüfen des Status der Serverressourcen

Mit dieser Option werden die Informationen des OnCommand Insight-Servers angezeigt, einschließlich Serverspeicher, Festplattenspeicher, Betriebssystem sowie Informationen zur CPU- und OnCommand Insight-Datenbank, einschließlich der InnoDB-Datengröße und des freien Festplattenspeichers, in dem sich die Datenbank befindet.

#### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Admin** und wählen Sie **Fehlerbehebung**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **OnCommand Insight-Portal**.
3. Klicken Sie auf der nächsten Seite im Menü Erweitert auf den Link **Fehlerbehebung**.
4. Klicken Sie Auf **Server Resources Status**.

   **Für fortgeschrittene OnCommand Insight-Benutzer:** der Administrator kann einige SQL-Tests durchführen, um die Reaktionszeit der Datenbank und des Servers über die Schaltfläche am Ende der Informationsübersicht zu überprüfen. Diese Option zeigt eine Warnung an, wenn die Serverressource zu niedrig ist.

### Suchen von Geisterdatenquellen

Wenn Sie ein Gerät entfernt haben, aber die Gerätedaten erhalten bleiben, können Sie alle Geisterdatenquellen suchen, so dass Sie sie entfernen können.

#### Schritte

1. Klicken Sie in der Web-Benutzeroberfläche auf **Admin** und wählen Sie **Troubleshooting**.
2. Klicken Sie unten auf der Seite im Bereich Weitere Aufgaben auf den Link **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Registerkarte **Reports** auf den Link **Ghost Data Sources**.

   OnCommand Insight erstellt eine Liste der Ersteller mit ihren Geräteinformationen.

### Hinzufügen eines fehlenden Festplattenmodells

Wenn die Erfassung aufgrund eines unbekannten Festplattenmodells fehlschlägt, können

## Sie dem das fehlende Laufwerksmodell hinzufügen `new_disk_models.txt` Datei erstellen und die Akquisition erneut ausführen.

#### Über diese Aufgabe

Im Rahmen einer Abfrage eines Speichergeräts durch OnCommand Insight-Erfassung werden die Datenträgermodelle auf dem Speichergerät gelesen. Wenn ein Anbieter seinem Array neue Festplattenmodelle hinzugefügt hat, über die Insight nicht Bescheid weiß, oder wenn die Modellnummer, nach der Insight sucht, nicht mit der vom Storage-Gerät zurückgegebenen übereinstimmt, schlägt die Datenerfassung der Datenquelle mit einem Fehler fehl. Um diese Fehler zu vermeiden, ist es notwendig, die Informationen zum Festplattenmodell, die Insight bekannt ist, zu aktualisieren. Insight verfügt über neue Festplattenmodelle mit Updates, Patches und Wartungs-Releases. Sie können jedoch entscheiden, diese Informationen manuell zu aktualisieren, anstatt auf einen Patch oder eine Aktualisierung zu warten.

Da OnCommand Insight die Festplattenmodelldatei alle fünf Minuten liest, werden alle neu eingegebenen Datenmodellinformationen automatisch aktualisiert. Sie müssen den Server nicht neu starten, damit die Änderungen wirksam werden, aber Sie können den Server und alle Remote-Akquisitionseinheiten (raus) neu starten, damit die Änderungen vor der nächsten Aktualisierung wirksam werden.

Aktualisierungen des Festplattenmodells werden dem hinzugefügt `new_disk_models.txt` Datei befindet sich im`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` Verzeichnis. Informieren Sie sich vor der Aktualisierung des über die erforderlichen Informationen zur Beschreibung Ihres neuen Festplattenmodells `new_disk_models.txt` Datei: Ungenaue Informationen in der Datei führen zu falschen Systemdaten und können zu einer fehlgeschlagenen Erfassung führen.

Befolgen Sie diese Anweisungen, um Insight-Festplattenmodelle manuell zu aktualisieren:

#### Schritte

1. Suchen Sie die richtigen Informationen für Ihr Festplattenmodell.
2. Öffnen Sie mit einem Texteditor die `new_disk_models.txt` Datei:
3. Fügen Sie die erforderlichen Informationen für die neue Datenquelle hinzu.
4. Speichern Sie die Datei im `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` Verzeichnis auf Ihrem Server.
5. Sichern Sie die `new_disk_models.txt` An einem sicheren Speicherort ablegen. Bei jedem nachfolgenden OnCommand Insight-Upgrade wird diese Datei überschrieben. Wenn in der aktualisierten Datei keine Informationen zum Laufwerksmodell vorhanden sind, müssen Sie sie erneut eingeben.

#### Suchen der erforderlichen Informationen für das neue Festplattenmodell

## Um die Informationen zum Festplattenmodell zu finden, geben Sie den Hersteller und die Modellnummer an, und führen Sie eine Internetsuche durch.

### Über diese Aufgabe

Das Auffinden von Datenträgermodellinformationen ist so einfach wie das Ausführen einer Internetsuche. Notieren Sie sich vor der Suche den Herstellernamen und die Laufwerksmodellnummer.

**Schritte**

1. Es wird empfohlen, eine erweiterte Internetsuche für den Hersteller, das Modell und den Dokumenttyp „`PDF`“ zu verwenden, um das Datenblatt und/oder das Installationshandbuch des Anbieters für das Laufwerk zu finden. Diese Datenblätter sind in der Regel die beste Quelle für Informationen über die Hersteller von Festplatten.
2. In den Herstellerspezifikationen werden nicht immer alle erforderlichen Informationen auf der Grundlage der vollständigen Modellnummer bereitgestellt. Es ist oft sinnvoll, nach verschiedenen Teilen der Modellnummer-Zeichenfolge auf der Website des Anbieters zu suchen, um alle Informationen zu finden.
3. Suchen Sie den Namen des Festplattenanbieters, die vollständige Modellnummer, die Festplattengröße und -Geschwindigkeit und den Schnittstellentyp. Um das neue Festplattenmodell in OnCommand Insight zu definieren, können Sie die folgende Tabelle als Leitfaden verwenden, um diese Informationen bei der Suche zu notieren:

| Für dieses Feld: | Diese ist: | Geben Sie Folgendes ein: |
|---|---|---|
| Modellnummer (auch als Schlüssel bezeichnet) | Erforderlich | |
| Anbieter | Erforderlich | |
| Festplattengeschwindigkeit (U/min) | Erforderlich | |
| Größe (in GB) | Erforderlich | |
| Schnittstellentyp (eine auswählen) | Erforderlich | ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, ANDERE |
| Suchzeit in ms | Optional | |
| Maximale Übertragungsrate in MB/s | Optional | |
| Übertragungsrate der Schnittstelle in MB/s | Optional | |
| Link zu Hersteller-/Modellinformationen | Optional, aber empfohlen | |

4. Geben Sie diese Informationen in das ein `new_disk_models.txt` Datei: Siehe "Inhalt der Datei new_disk_models.txt" Für Format, Reihenfolge und Beispiele.

**Inhalt der Datei new_disk_models.txt**

Der `new_disk_models.txt` Die Datei enthält Pflichtfelder und optionale Felder. Die Felder sind durch Kommas getrennt. Verwenden Sie daher keine Kommas *innerhalb* der Felder.

Alle Felder sind mit Ausnahme von Suchzeit, Transferraten und additional_info erforderlich. Falls verfügbar, fügen Sie den Link der Hersteller-/Modell-Website in das Feld additional_info ein.

Geben Sie in einem Texteditor für jedes neue Laufwerksmodell, das Sie hinzufügen möchten, die folgenden durch Kommas getrennten Informationen in dieser Reihenfolge ein:

1. **Schlüssel**: Verwenden Sie die Modellnummer (erforderlich)
2. **Anbieter**: Name (erforderlich)
3. **Modellnummer**: Volle Zahl (normalerweise der gleiche Wert wie in "Schlüssel") (erforderlich)
4. **U/min der Scheibe**: Zum Beispiel 10000 oder 15000 (erforderlich)
5. **Größe**: Kapazität in GB (erforderlich)
6. **Schnittstellentyp**: ATA, SATA, FC, SAS, FATA, SSD, ANDERE (erforderlich)
7. **Suchzeit**: In ms (optional)
8. **Potenzielle Übertragungsrate**: Die mögliche Übertragungsrate in MB/s. Maximale Übertragungsrate der Festplatte selbst. (Optional)
9. **Übertragungsrate der Schnittstelle**: Die Rate zum und vom Host in MB/s (optional).
10. **Zusätzliche Info**: Alle zusätzlichen Informationen, die Sie erfassen möchten. Als Best Practice empfiehlt es sich, den Link zur Anbieterseite einzugeben, auf der die Spezifikationen gefunden werden, um darauf Bezug zu nehmen (optional).

Wenn Sie optionale Felder leer lassen möchten, müssen Sie das Komma eingeben.

Beispiele (jeweils in einer Zeile ohne Leerzeichen):

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

# Monitoring Ihrer Umgebung und

Insight ermöglicht die Vermeidung von Systemproblemen und ermöglicht eine schnelle Behebung potenzieller Probleme.

## Daten der Bestandsseite

Asset-Seiten bieten Daten zur Fehlerbehebung bei der Performance und zeigen zusammenfassende Informationen zu einem Basiselement (z. B. einer virtuellen Maschine oder einem Volume) und den zugehörigen Assets an, die es verwendet (z. B. Speicherpools, Speicherknoten und verbundene Switch-Ports), sowie Links zu zusätzlichen Informationen.

Beginnend mit OnCommand Insight 7.3 haben alle Asset-Seiten eine **Main** Seite und eine **zusätzliche Daten** Seite. Auf der Hauptseite finden Sie eine Zusammenfassung der Anlage und verschiedene Abschnitte für Diagramme, Topologie und andere Informationen. Auf der Seite **zusätzliche Daten** können Sie eine

anpassbare Dashboard-Seite für den aktuellen Asset-Typ konfigurieren.

Ein roter Kreis neben einer Zeile oder Nachricht auf der Hauptregisterkarte der Systembestandsseite zeigt mögliche Probleme mit der überwachten Umgebung an.

#### Typen von Bestandsseiten

Die Asset-Seiten fassen den aktuellen Status eines Assets zusammen und enthalten Links zu zusätzlichen Informationen über das Asset und die zugehörigen Assets.

OnCommand Insight stellt Asset-Seiten für die folgenden Ressourcen bereit:

- Virtual Machine
- Datenmenge
- Internes Volumen
- Physischer Host
- Storage-Pool
- Storage
- Datenspeicher
- Hypervisor
- Applikation
- Storage-Node
- Qtree
- Festplatte
- VMDK
- Port
- Switch
- Fabric
- Objektspeicher (z. B. Atmos, Centera, Amazon S3)
- Zone

Zuordnungs- und Maskierungsinformationen können in Tabellen auf den Bestandsseiten Zone, Volume, VM und Host/Hypervisor angezeigt werden.

Zusammenfassende Informationen sind für Objekt-Storage-Ressourcen verfügbar. Sie können diese Informationen jedoch nur über die Detailseite Datenquellen aufrufen.

#### In Ihrer Umgebung nach bestimmten Assets suchen

Sie können Informationen zu bestimmten Assets über die Suchfunktion finden. Wenn beispielsweise ein Systembenutzer den Speicheradministrator mit einer Beschwerde über einen bestimmten Server kontaktiert, kann der Administrator den Servernamen durchsuchen und eine Bestandsseite anzeigen, die den Status zusammenfasst und zusätzliche verknüpfte Informationen liefert.

#### Schritte

1. Öffnen Sie die Benutzeroberfläche von OnCommand Insight.
2. Klicken Sie in der Symbolleiste auf .

   Das Feld **Assets suchen** wird angezeigt.

3. Geben Sie den Namen eines Assets oder eines Teils des Namens ein.
4. Wählen Sie die gewünschte Ressource aus den Suchergebnissen aus.

   Die Bestandsseite für diese Ressource wird angezeigt.

#### Erweiterte Suchtechniken

Es können mehrere Suchmethoden verwendet werden, um in Ihrer überwachten Umgebung nach Daten oder Objekten zu suchen.

### Wildcard-Suche

Sie können Platzhaltersuche für mehrere Zeichen mit dem * Zeichen durchführen. Zum Beispiel würde *applic*n* die Anwendung zurückgeben.

### Bei der Suche verwendete Ausdrücke

Ein Ausdruck ist eine Gruppe von Wörtern, die von doppelten Anführungszeichen umgeben sind, z. B. „PAW VNX LUN 5“. Sie können doppelte Anführungszeichen verwenden, um nach Dokumenten zu suchen, die Leerzeichen in ihren Namen oder Attributen enthalten.

### Boolesche Operatoren

Mit Booleschen Operatoren können Sie mehrere Begriffe zu einer komplexeren Abfrage kombinieren.

- **ODER**
  - Der OR-Operator ist der Standard-Konjunktion-Operator.

    Wenn zwischen zwei Begriffen kein Boolescher Operator vorhanden ist, wird der OPERATOR ODER verwendet.

  - Der OR-Operator verknüpft zwei Begriffe und findet ein passendes Dokument, wenn einer der Termini in einem Dokument vorhanden ist.

    Beispielsweise sucht „`storage ODER netapp`“ nach Dokumenten, die entweder „`storage`“ oder „`netapp`“ enthalten.

  - Hohe Bewertungen werden an Dokumente vergeben, die den meisten Bedingungen entsprechen.
- **UND**

  Sie können den OPERATOR UND verwenden, um Dokumente zu suchen, in denen beide Suchbegriffe in einem einzigen Dokument vorhanden sind. Beispielsweise sucht „`aurora AND netapp`“ nach Dokumenten, die sowohl „`storage`“ als auch „`netapp`“ enthalten.

  Sie können das Symbol && anstelle des Wortes UND verwenden.

- **NICHT**

  Wenn Sie den NICHT-Operator verwenden, werden alle Dokumente, die den Begriff nachher NICHT enthalten, von den Suchergebnissen ausgeschlossen. Beispiel: „`storage NOT netapp`“ sucht nach Dokumenten, die nur „`storage`“ und nicht „`netapp`“ enthalten.

  Sie können das Symbol verwenden ! Statt des Wortes NICHT.

**Suche nach Präfix und Suffix**

- Sobald Sie eine Suchzeichenfolge eingeben, führt die Suchmaschine eine Präfix- und Suffixsuche durch, um die beste Übereinstimmung zu finden.
- Exakte Übereinstimmungen erhalten eine höhere Bewertung als eine Präfix- oder Suffix-Übereinstimmung. Die Bewertung wird anhand der Entfernung des Suchbegriffs vom tatsächlichen Suchergebnis berechnet. Zum Beispiel haben wir drei Speicher: “aurora”, “aurora1” und “aurora11”. Die Suche nach “aur” gibt alle drei Lager zurück. Das Suchergebnis für “aurora” hat jedoch die höchste Punktzahl, da es den nächstliegenden Abstand zum Suchstring hat.
- Die Suchmaschine sucht auch nach Begriffen in umgekehrter Reihenfolge, wodurch Sie eine Suffix-Suche durchführen können. Wenn Sie beispielsweise „`345`“ in das Suchfeld eingeben, sucht die Suchmaschine nach „`345`“.
- Die Groß-/Kleinschreibung der Suche wird nicht berücksichtigt.

**Suche mit indizierten Begriffen**

Suchvorgänge, die mehr der indizierten Begriffe entsprechen, führen zu höheren Punktzahlen.

Der Suchstring wird in separate Suchbegriffe nach Leerzeichen aufgeteilt. Beispielsweise ist der Suchtext „`storage aurora netapp`“ in drei Schlüsselwörter unterteilt: „`storage`“, „`aurora`“ und „`netapp`“. Die Suche wird unter Verwendung aller drei Begriffe durchgeführt. Die Dokumente, die den meisten dieser Begriffe entsprechen, haben die höchste Punktzahl. Je mehr Informationen Sie zur Verfügung stellen, desto besser sind die Suchergebnisse. Sie können beispielsweise anhand des Namens und des Modus nach einem Speicher suchen.

Die Benutzeroberfläche zeigt die Suchergebnisse für verschiedene Kategorien mit den drei besten Ergebnissen pro Kategorie an. Wenn Sie kein Dokument gefunden haben, das Sie erwartet haben, können Sie mehr Begriffe in die Suchzeichenfolge einfügen, um die Suchergebnisse zu verbessern.

Die folgende Tabelle enthält eine Liste indizierter Begriffe, die der Suchzeichenfolge hinzugefügt werden können.

| Kategorie | Indizierte Begriffe |
| --- | --- |
| Storage | • „`storage`“<br>• Name<br>• Anbieter<br>• Modell |

| | |
|---|---|
| Storage Pool | • „storagepool“<br>• Name<br>• Name des Speichers<br>• IP-Adressen des Speichers<br>• Seriennummer des Speichers<br>• Storage-Anbieter<br>• Storage-Modell<br>• Namen für alle zugeordneten internen Volumes<br>• Namen für alle zugeordneten Festplatten |
| Internes Volumen | • „internalvolume“<br>• Name<br>• Name des Speichers<br>• IP-Adressen des Speichers<br>• Seriennummer des Speichers<br>• Storage-Anbieter<br>• Storage-Modell<br>• Name des Speicherpools<br>• Namen aller zugeordneten Freigaben<br>• Namen aller zugehörigen Applikationen und Geschäftseinheiten |
| Datenmenge | • „Volume“<br>• Name<br>• Etikett<br>• Namen aller internen Volumes<br>• Name des Speicherpools<br>• Name des Speichers<br>• IP-Adressen des Speichers<br>• Seriennummer des Speichers<br>• Storage-Anbieter<br>• Storage-Modell |

| | |
|---|---|
| Storage-Node | • „storagenode“<br>• Name<br>• Name des Speichers<br>• IP-Adressen des Speichers<br>• Seriennummer des Storage<br>• Storage-Anbieter<br>• Storage-Modell |
| Host | • „Host“<br>• Name<br>• IP-Adressen<br>• Namen aller zugehörigen Applikationen und Geschäftseinheiten |
| Datenspeicher | • „Datastore“<br>• Name<br>• IP des virtuellen Zentrums<br>• Namen aller Volumes<br>• Namen aller internen Volumes |
| Virtual Machines | • „virtualmachine“<br>• Name<br>• DNS-Name<br>• IP-Adressen<br>• Name des Hosts<br>• IP-Adressen des Hosts<br>• Namen aller Datastores<br>• Namen aller zugehörigen Applikationen und Geschäftseinheiten |

| | |
|---|---|
| Switches (normal und Kapitalwert) | • „sHexe“<br>• IP-Adresse<br>• wwn<br>• Name<br>• Seriennummer<br>• Modell<br>• Domänen-ID<br>• Name der Fabric<br>• wwn der Fabric |
| Applikation | • „Anwendung“<br>• Name<br>• Mandant<br>• Geschäftsbereich<br>• Geschäftseinheit<br>• Projekt |
| Tape | • „Tape“<br>• IP-Adresse<br>• Name<br>• Seriennummer<br>• Anbieter |
| Port | • „Port“<br>• wwn<br>• Name |
| Fabric | • „Stoff“<br>• wwn<br>• Name |

**Ändern des Zeitbereichs der angezeigten Daten**

Standardmäßig werden auf einer Bestandsseite die letzten 24 Stunden der Daten angezeigt. Sie können jedoch das angezeigte Datensegment ändern, indem Sie eine andere feste Zeit oder einen benutzerdefinierten Zeitraum auswählen, um weniger oder mehr Daten anzuzeigen.

#### Über diese Aufgabe

Sie können das Zeitsegment der angezeigten Daten ändern, indem Sie eine Option verwenden, die sich auf jeder Asset-Seite befindet, unabhängig vom Asset-Typ.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web-Benutzeroberfläche an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.
3. Klicken Sie oben links auf der Seite auf eines der folgenden Zeitsymbole, um das angezeigte Datensegment zu ändern:
   - **3h**

     Zeigt die Daten der letzten drei Stunden an.
   - **24h**

     Zeigt die Daten der letzten 24 Stunden an.
   - * 3d*

     Zeigt die Daten der letzten drei Tage an.
   - **7d**

     Zeigt die Daten der letzten sieben Tage an.
   - **30d**

     Zeigt die Daten der letzten dreißig Tage an.
   - **Benutzerdefiniert**

     Zeigt ein Dialogfeld an, in dem Sie einen benutzerdefinierten Zeitraum auswählen können. Sie können bis zu 31 Tage Daten gleichzeitig anzeigen.
4. Wenn Sie **Custom** gewählt haben, gehen Sie wie folgt vor:
   a. Klicken Sie auf das Datumsfeld, und wählen Sie einen Monat, einen Tag und ein Jahr für das Anfangsdatum aus.
   b. Klicken Sie auf die Liste Zeit, und wählen Sie eine Startzeit aus.
   c. Wiederholen Sie beide Schritte a und b für die Enddaten und die Endzeit.
   d. Klicken Sie Auf .

### Ermitteln des Erfassungsstatus der Datenquelle

Da Datenquellen die primäre Informationsquelle für Insight sind, müssen Sie unbedingt

sicherstellen, dass diese weiterhin ausgeführt werden.

Die Möglichkeit, den Erfassungsstatus der Datenquelle anzuzeigen, steht auf jeder Seite der Anlage für alle Assets zur Verfügung, die direkt erfasst werden. Es kann zu einem der folgenden Erfassungsszenarien kommen, in denen der Status in der oberen rechten Ecke der Bestandsseite angezeigt wird:

- Erfolgreich von Datenquelle erfasst

  Zeigt den Status „Acquired" an `xxxx``", where `xxxx Gibt die letzte Erfassungszeit der Datenquellen des Assets an.

- Es liegt ein Erfassungsfehler vor.

  Zeigt den Status „Acquired" an `xxxx``", where `xxxx Gibt die letzte Erfassungszeit der Datenquelle des Assets mit an ⚠. Wenn Sie auf klicken ⚠, In einem Fenster werden jede Datenquelle für das Asset, der Status der Datenquelle und der Zeitpunkt der letzten Datenerfassung angezeigt. Durch Klicken auf eine Datenquelle wird die Detailseite der Datenquelle angezeigt.

Wenn ein Asset nicht direkt erfasst wird, wird kein Status angezeigt.

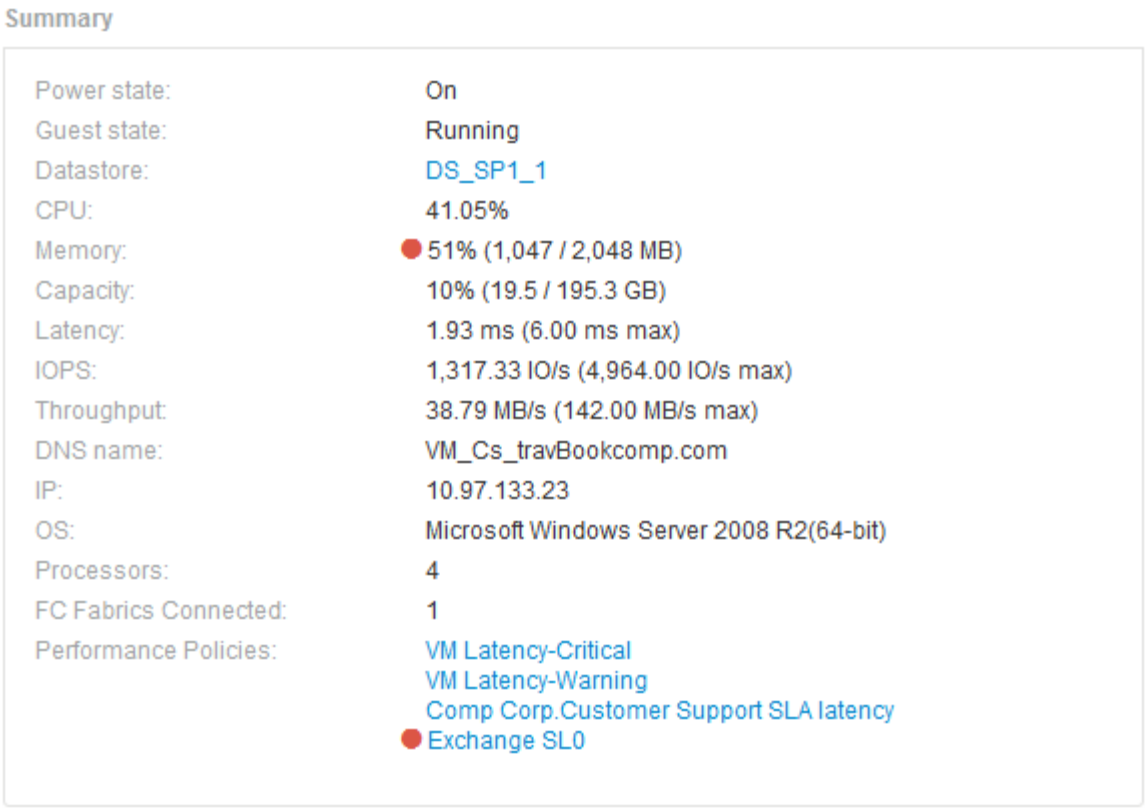
#### Abschnitte der Anlagenseite

Auf einer Anlagenseite werden mehrere Abschnitte mit Informationen angezeigt, die für die Anlage relevant sind. Die angezeigten Abschnitte hängen vom Typ des Assets ab.

##### Zusammenfassung

Der Abschnitt Zusammenfassung auf einer Anlagenseite zeigt eine Zusammenfassung der Informationen über das jeweilige Asset an und zeigt Probleme im Zusammenhang mit dem Asset an, die durch einen roten Kreis gekennzeichnet sind, mit Hyperlinks zu zusätzlichen Informationen über verwandte Assets und zu allen Performance Policies, die dem Asset zugewiesen sind.

Das folgende Beispiel zeigt einige der Informationstypen, die im Abschnitt Zusammenfassung einer Bestandsseite für eine virtuelle Maschine verfügbar sind. Jedes Element mit einem durchgehenden roten Kreis daneben weist auf potenzielle Probleme mit der überwachten Umgebung hin.




### Verwenden des Abschnitts Zusammenfassung

Sie können den Abschnitt Zusammenfassung anzeigen, um allgemeine Informationen über ein Asset anzuzeigen. Insbesondere ist es hilfreich zu prüfen, ob Kennzahlen (wie Arbeitsspeicher, Kapazität und Latenz) oder Performance-Richtlinien Bedenken haben, die OnCommand Insight anzeigt, indem ein roter Kreis neben der Metrik oder der Performance-Richtlinie angezeigt wird.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.

   Die Informationen, die im Abschnitt Zusammenfassung angezeigt werden, hängen von der Art der angezeigten Bestandsseite ab.
3. Sie können auf einen der Asset-Links klicken, um die Asset-Seiten anzuzeigen.

   Wenn Sie beispielsweise einen Storage-Node anzeigen, können Sie auf einen Link klicken, um die Asset-Seite des Storage anzuzeigen, mit dem er verknüpft ist, oder auf klicken, um die Asset-Seite des HA-Partners anzuzeigen.

4. Sie können die Metriken anzeigen, die mit der Ressource verknüpft sind.

   Ein roter Kreis neben einer Metrik zeigt an, dass Sie mögliche Probleme diagnostizieren und lösen müssen.

   Sie können feststellen, dass die Volume-Kapazität bei einigen Storage-Assets größer als 100 % sein kann. Das liegt an Metadaten, die sich auf die Kapazität des Volumes beziehen, die Teil der verbrauchten Kapazitätsdaten sind, die von der Ressource gemeldet wurden.

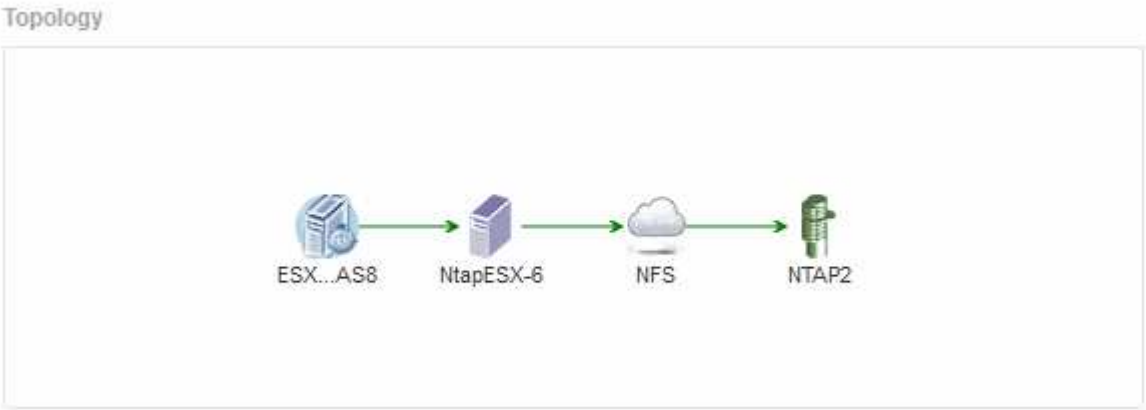
5. Falls zutreffend, können Sie auf einen Link zu einer Leistungsrichtlinie klicken, um die mit der Ressource verbundenen Leistungsrichtlinien oder -Richtlinien anzuzeigen.

   Wenn neben einer Performance Policy ein roter Kreis angezeigt wird, bedeutet dies, dass eine Anlage den definierten Schwellenwert der Performance Policy überschritten hat. Sie sollten die Leistungsrichtlinie überprüfen, um das Problem weiter zu diagnostizieren.

#### Topologie

Im Abschnitt Topologie können Sie sehen, wie eine Basisressource mit ihren zugehörigen Assets verbunden ist, sofern dies für ein Asset relevant ist.

Das folgende Beispiel zeigt, was im Abschnitt Topologie einer Seite mit virtuellen Maschinen angezeigt werden könnte.




Wenn die Topologie für das Asset größer ist, als in den Abschnitt passt, wird stattdessen der Link **Klicken angezeigt, um den Topology**-Hyperlink zu sehen.

#### Verwenden des Abschnitts Topologie

Im Abschnitt „Topologie“ können Sie anzeigen, wie die Assets in Ihrem Netzwerk miteinander verbunden sind, und Informationen zu zugehörigen Assets anzeigen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.

- Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt. Sie finden den Abschnitt Topologie in der oberen rechten Ecke der Seite Anlage.

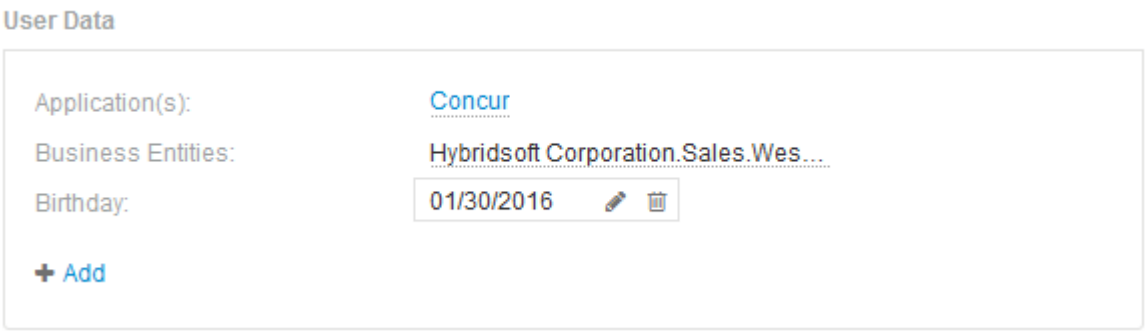
Wenn die Topologie für das Asset größer ist, als in den Abschnitt passt, klicken Sie auf den Link *Klicken, um den Topologie-Hyperlink zu sehen.

3. Um weitere Informationen über die zugehörigen Assets der Basisressource anzuzeigen, setzen Sie den Cursor auf ein zubezogenes Asset in der Topologie und klicken Sie auf dessen Namen, der die zugehörige Asset-Seite anzeigt.

#### Benutzerdaten

Im Abschnitt Benutzerdaten einer Anlagenseite werden benutzerdefinierte Daten wie Anwendungen, Geschäftseinheiten und Anmerkungen angezeigt und können geändert werden.

Das folgende Beispiel zeigt, was im Abschnitt „Benutzerdaten“ einer Asset-Seite einer virtuellen Maschine angezeigt werden kann, wenn der Ressource eine Applikation, eine Geschäftseinheit und eine Annotation zugewiesen werden:




#### Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anwendungen

Sie können Applikationen, die in Ihrer Umgebung ausgeführt werden, bestimmten Ressourcen zuweisen (Host, Virtual Machines, Volumes, interne Volumes und Hypervisoren). Im Abschnitt Benutzerdaten können Sie die einem Asset zugewiesene Anwendung ändern oder einem Asset eine Anwendung oder zusätzliche Anwendungen zuweisen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.
3. Sie haben folgende Möglichkeiten:
   - Klicken Sie auf den Namen der Anwendung, um die Bestandsseite für die Anwendung anzuzeigen.

- Um die zugewiesene Anwendung zu ändern oder eine Anwendung oder weitere Anwendungen zuzuweisen, setzen Sie Ihren Cursor über den Anwendungsnamen, wenn eine Anwendung zugewiesen ist, oder über **Keine**, wenn keine Anwendung zugewiesen ist, klicken Sie auf Geben Sie ein, um nach einer Anwendung zu suchen, oder wählen Sie eine aus der Liste aus, und klicken Sie dann auf .

  Wenn Sie eine Anwendung auswählen, die einer Geschäftseinheit zugeordnet ist, wird die Geschäftseinheit automatisch der Anlage zugewiesen. Wenn Sie in diesem Fall den Cursor über den Namen der Geschäftseinheit setzen, wird das Wort *abgeleitet* angezeigt. Wenn Sie die Einheit nur für das Asset und nicht für die zugehörige Anwendung verwalten möchten, können Sie die Zuweisung der Anwendung manuell überschreiben.

- Um eine Anwendung zu entfernen, klicken Sie auf .

#### Verwenden des Abschnitts Benutzerdaten, um Geschäftseinheiten zuzuweisen oder zu ändern

Sie können Geschäftseinheiten definieren, um Ihre Umgebungsdaten granular zu verfolgen und darüber Berichte zu erstellen. Im Abschnitt „Benutzerdaten“ auf der Seite „Anlage“ können Sie die einem Asset zugewiesene Geschäftseinheit ändern oder eine Geschäftseinheit aus einem Asset entfernen.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.
3. Sie haben folgende Möglichkeiten:
   - Um die zugewiesene Entität zu ändern oder eine Entität zuzuweisen, klicken Sie auf Und wählen Sie eine Einheit aus der Liste aus.
   - Um eine Geschäftseinheit zu entfernen, klicken Sie auf .

> Sie können keine Entität entfernen, die von einer Anwendung abgeleitet wurde, die dem Asset zugewiesen ist.

#### Verwenden des Abschnitts „Benutzerdaten“ zum Zuweisen oder Ändern von Anmerkungen

Wenn Sie OnCommand Insight so anpassen, dass Daten für Ihre Unternehmensanforderungen nachverfolgt werden, können Sie spezielle Hinweise, die so genannten *Annotationen*, definieren und diese Ihren Ressourcen zuweisen. Im Abschnitt „Benutzerdaten“ einer Asset-Seite werden Anmerkungen angezeigt, die einem Asset zugeordnet sind, und Sie können auch die Anmerkungen ändern, die diesem Asset zugewiesen sind.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.
3. Klicken Sie im Abschnitt **Benutzerdaten** der Seite Asset auf + Add.

   Das Dialogfeld Anmerkung hinzufügen wird angezeigt.
4. Klicken Sie auf **Anmerkung** und wählen Sie eine Anmerkung aus der Liste aus.
5. Klicken Sie auf **Wert**, und führen Sie je nach Art der ausgewählten Anmerkung einen der folgenden Schritte aus:
   - Wenn der Anmerkungstyp Liste, Datum oder Boolean ist, wählen Sie einen Wert aus der Liste aus.
   - Wenn es sich bei dem Anmerkungstyp um Text handelt, geben Sie einen Wert ein.
6. Klicken Sie Auf **Speichern**.

   Die Anmerkung wird dem Asset zugewiesen. Sie können Assets später mithilfe einer Abfrage nach Anmerkungen filtern.
7. Wenn Sie den Wert der Anmerkung ändern möchten, nachdem Sie sie zugewiesen haben, klicken Sie auf Und wählen Sie einen anderen Wert aus.

   Wenn die Anmerkung vom Listentyp ist, für den die Option **Werte dynamisch bei Anmerkungszuweisung hinzufügen** ausgewählt ist, können Sie zusätzlich zur Auswahl eines vorhandenen Werts einen neuen Wert eingeben.

#### Expertenansicht

Im Abschnitt „Expertenansicht“ einer Bestandsseite können Sie ein Leistungsbeispiel für die Basisressource anzeigen, das auf einer beliebigen Anzahl anwendbarer Kennzahlen im Kontext eines ausgewählten Zeitraums (3 Stunden, 24 Stunden, 3 Tage, 7 Tage, Oder einen benutzerdefinierten Zeitraum) in der Leistungsübersicht und den damit verbundenen Anlagen enthalten.

Im Folgenden finden Sie ein Beispiel für den Abschnitt „Expertenansicht“ auf einer Seite mit Volume-Assets:

Sie können die Metriken auswählen, die im Performance-Diagramm für den ausgewählten Zeitraum angezeigt werden sollen.

Im Abschnitt „Ressourcen“ werden der Name des Basiswerts und die Farbe für das Basiselement im Leistungsdiagramm angezeigt. Wenn der Abschnitt „Top Correlated“ kein Asset enthält, das Sie im Leistungsdiagramm anzeigen möchten, können Sie das Feld „Assets suchen“ im Abschnitt „zusätzliche Ressourcen“ verwenden, um das Asset zu suchen und es dem Leistungsdiagramm hinzuzufügen. Beim Hinzufügen von Ressourcen werden diese im Abschnitt zusätzliche Ressourcen angezeigt.

Sind auch im Abschnitt Ressourcen aufgeführt, sofern zutreffend, alle Assets, die sich auf das Basivermögen in den folgenden Kategorien beziehen:

- Oben korreliert

  Zeigt die Assets, die eine hohe Korrelation (in Prozent) mit einem oder mehreren Performance-Kennzahlen zur Basisinressource haben.

- Top-Mitwirkende

  Zeigt die Assets an, die (in Prozent) zur Basisinressource beitragen.

- Gierig

  Zeigt die Ressourcen, die Systemressourcen durch gemeinsame Nutzung derselben Ressourcen wie Hosts, Netzwerke und Storage-Ressourcen von der Ressource wegnehmen.

- Beeinträchtigt

  Zeigt die Ressourcen an, die aufgrund dieser Ressource zur Neige gehen, wenn sie sich auf die Systemressourcen aufgestockt haben.

#### Metrische Definitionen der Expertenansicht

Im Abschnitt „Expertenansicht“ einer Asset-Seite werden je nach dem für das Asset ausgewählten Zeitraum mehrere Metriken angezeigt. Jede Metrik wird in einem eigenen Performance-Diagramm angezeigt. Je nachdem, welche Daten angezeigt werden sollen,

können Sie Metriken und zugehörige Assets in den Diagrammen hinzufügen oder entfernen.

| Metrisch | Beschreibung |
| --- | --- |
| BB Credit Null Rx, Tx | Die Anzahl der Empfangs-/Übertragungs-Buffer-zu-Buffer-Gutschriften wurde während des Probenzeitraums auf Null übertragen. Diese Metrik gibt an, wie oft der angeschlossene Port die Übertragung beenden musste, da dieser Port nicht mehr als Credits zur Verfügung stand. |
| BB Kredit Null Dauer Tx | Zeit in Millisekunden, während der der transmit BB-Guthaben während des Abtastintervalls null war. |
| Cache-Trefferrverhältnis (gesamt, Lesen, Schreiben) % | Prozentsatz von Anforderungen, die zu Cache-Treffern führen. Je höher die Anzahl der Treffer im Vergleich zum Volume ist, desto besser ist die Performance. Diese Spalte ist leer für Speicher-Arrays, die keine Cache-Trefferinformationen erfassen. |
| Cache-Auslastung (gesamt) % | Gesamtprozentsatz der Cacheanforderungen, die zu Cache-Treffern führen |
| Discards der Klasse 3 | Anzahl der Rückwürfe für die Datenübertragung in der Fibre Channel-Klasse 3 |
| CPU-Auslastung (gesamt) % | Menge der aktiv genutzten CPU-Ressourcen als Prozentsatz der insgesamt verfügbaren (über alle virtuellen CPUs) |
| CRC-Fehler | Anzahl der Frames mit ungültigen zyklischen Redundanzprüfungen (CRCs), die vom Port während des Probenahmezeitraums erkannt wurden |
| Frame-Rate | Bildrate in Bildern pro Sekunde übertragen (FPS) |
| Bildgröße durchschnittlich (Rx, Tx) | Verhältnis von Datenverkehr zu Bildgröße. Mit dieser Metrik können Sie feststellen, ob es Overhead Frames in der Fabric gibt. |
| Rahmengröße zu lang | Anzahl der zu langen Fibre Channel-Datenübertragungsrahmen |
| Rahmengröße zu kurz | Anzahl der zu kurzen Fibre Channel-Datenübertragungsrahmen |

| | |
|---|---|
| I/O-Dichte (gesamt, Lesen, Schreiben) | Anzahl der IOPS geteilt durch genutzte Kapazität (wie bei der letzten Inventarabfrage der Datenquelle erworben) für das Element Volume, Internal Volume oder Storage. Diese wird anhand der Anzahl der I/O-Vorgänge pro Sekunde pro TB gemessen. |
| IOPS (gesamt, Lesen, Schreiben) | Anzahl der Lese-/Schreib-I/O-Serviceanfragen, die den I/O-Kanal oder einen Teil dieses Kanals pro Zeiteinheit durchlaufen (gemessen in I/O pro Sekunde) |
| IP-Durchsatz (gesamt, Lesen, Schreiben) | Gesamt: Aggregierte Rate, bei der IP-Daten in Megabyte pro Sekunde übertragen und empfangen wurden. Lesen: IP-Durchsatz (Empfangen): Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde empfangen wurden.<br><br>Write: IP Throughput (Transmit): Durchschnittliche Rate, mit der IP-Daten in Megabyte pro Sekunde übertragen wurden. |
| Latenz (Gesamt, Lesen, Schreiben) | Latenz (R&W): Geschwindigkeit, mit der Daten in einem festgelegten Zeitraum gelesen oder auf die Virtual Machines geschrieben werden Der Wert wird in Megabyte pro Sekunde gemessen.<br><br>Latenz: Durchschnittliche Antwortzeit der Virtual Machines in einem Datenspeicher.<br><br>Höchste Latenz: Die höchste Reaktionszeit der Virtual Machines eines Datenspeichers. |
| Verbindungsfehler | Anzahl der Verbindungsfehler, die der Port während des Probenahmezeitraums entdeckt hat. |
| Link Reset Rx, Tx | Anzahl der Rücksetzungen von Empfangs- oder Übertragungsverbindung während des Probenzeitraums. Diese Metrik gibt die Anzahl der vom angeschlossenen Port an diesen Port ausgegebenen Link-Resets an. |
| Speicherauslastung (gesamt) % | Schwellenwert für den vom Host verwendeten Speicher. |

| | |
|---|---|
| Teilweise R/W (gesamt) % | Gesamtzahl der Male, die ein Lese-/Schreibvorgang einen Stripe-Grenzwert auf einem Festplattenmodul in RAID 5, RAID 1/0 oder RAID 0 LUN überschreitet, sind Stripe-Crossings in der Regel nicht von Vorteil, da jeder eine zusätzliche I/O-Operation erfordert Ein geringer Prozentsatz zeigt eine effiziente Stripe-Elementgröße an und gibt Aufschluss über eine nicht ordnungsgemäße Ausrichtung eines Volumes (oder einer NetApp LUN).<br><br>Bei CLARiiON ist dieser Wert die Anzahl der Stripe-Crossings, geteilt durch die Gesamtzahl der IOPS. |
| Port-Fehler | Bericht über Port-Fehler über den Probenzeitraum/den angegebenen Zeitraum. |
| Signalverlust zählen | Anzahl der Signalverlustfehler. Wenn ein Signalverlustfehler auftritt, gibt es keine elektrische Verbindung und es besteht ein physikalisches Problem. |
| Swap-Rate (Gesamtrate, Rate, out-Rate) | Rate, mit welcher der Speicher während des Probenzeitraums in den aktiven Speicher des Laufwerks oder aus dem Datenträger in den aktiven Speicher eingetauscht wird. Dieser Zähler bezieht sich auf virtuelle Maschinen. |
| Synchrone Verlustzahl | Anzahl der Fehler bei Synchronisierungsverlust. Wenn ein Fehler bei der Synchronisierung auftritt, kann die Hardware den Datenverkehr nicht erkennen oder darauf sperren. Das gesamte Gerät verwendet möglicherweise nicht die gleiche Datenrate, oder die optischen oder physischen Verbindungen können von schlechter Qualität sein. Der Port muss nach jedem solchen Fehler erneut synchronisiert werden, was sich auf die Systemleistung auswirkt. Gemessen in KB/Sek. |
| Durchsatz (Gesamt, Lesen, Schreiben) | Geschwindigkeit, mit der Daten übertragen, empfangen oder in einem festen Zeitraum als Reaktion auf I/O-Serviceanfragen (gemessen in MB pro s) gesendet werden. |
| Timeout - Rahmen verwerfen - Tx | Anzahl der durch Timeout verursachten verworfenen Übertragungsrahmen. |
| Traffic-Rate (gesamt, Lesen, Schreiben) | Der während des Probenahmezeitraums übertragenen, empfangenen oder beide empfangenen Datenverkehr in Mebibyte pro Sekunde. |

| | |
|---|---|
| Traffic-Auslastung (gesamt, Lesen, Schreiben) | Verhältnis der empfangenen/übertragenen/gesamten Kapazität zu Empfangs-/Übertragungs-/Gesamtkapazität während des Probenzeitraums. |
| Auslastung (Gesamt, Lesen, Schreiben) % | Prozentsatz der verfügbaren Bandbreite für die Übertragung (Tx) und den Empfang (Rx). |
| Ausstehende Schreibvorgänge (Gesamt) | Anzahl der ausstehenden Schreib-I/O-Serviceanfragen. |

#### Verwenden des Abschnitts „Expertenansicht“

In der Ansicht „Experten“ können Sie Leistungsdiagramme für ein Asset anzeigen, die auf einer beliebigen Anzahl von anwendbaren Metriken während eines ausgewählten Zeitraums basieren, und zugehörige Assets hinzufügen, um Asset- und Performance-Werte über verschiedene Zeiträume zu vergleichen und zu kontrastieren.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt. Standardmäßig werden im Performance-Diagramm zwei Metriken für den Zeitraum angezeigt, der für die Seite Anlage ausgewählt wurde. Beispielsweise zeigt das Performance-Diagramm für einen Storage standardmäßig die Latenz und die IOPS insgesamt an. Im Abschnitt Ressourcen werden der Ressourcenname und der Abschnitt „zusätzliche Ressourcen“ angezeigt, in dem Sie nach Assets suchen können. Je nach Asset können Sie auch Assets in den Abschnitten „Top Correlated“, „Top Contributor“, „Greedy“ und „degradierte Werte“ sehen.
3. Sie können auf **anzuzeigende Metriken auswählen** klicken und eine Metrik auswählen, um ein Leistungsdiagramm für eine Metrik hinzuzufügen.

   Für die ausgewählte Metrik wird ein Leistungsdiagramm hinzugefügt. Das Diagramm zeigt die Daten für den ausgewählten Zeitraum an. Sie können den Zeitraum ändern, indem Sie auf einen anderen Zeitraum in der linken oberen Ecke der Anlagenseite klicken.

   Sie können den Schritt erneut ausführen und auf klicken, um eine Metrik zu löschen. Das Leistungsdiagramm für die Kennzahl wird entfernt.

4. Sie können den Cursor über das Diagramm setzen und die angezeigten Metrikdaten ändern, indem Sie je nach Anlage auf eine der folgenden Optionen klicken:
   - **Lesen** oder **Schreiben**
   - **Tx**oder **Rx Total** ist die Standardeinstellung.
5. Sie können den Cursor über die Datenpunkte im Diagramm ziehen, um zu sehen, wie sich der Wert der Metrik im ausgewählten Zeitraum ändert.

6. Im Abschnitt **Ressourcen** können Sie, falls zutreffend, beliebige zugehörige Assets zu den Leistungsdiagrammen hinzufügen:
   - Sie können in den Abschnitten „Top korrelated“, „Top Contributors“, „Greedy“ oder „Degraded“ eine zugehörige Ressource auswählen, um für jede ausgewählte Metrik Daten aus dieser Ressource zum Leistungsdiagramm hinzuzufügen. Die Vermögenswerte müssen eine Korrelation von mindestens 15 % oder einen Beitrag aufweisen, um angezeigt zu werden.

     Nachdem Sie das Element ausgewählt haben, wird neben dem Element ein Farbblock angezeigt, der die Farbe seiner Datenpunkte im Diagramm kennzeichnet.

   - Für jedes angezeigte Asset können Sie auf den Namen des Assets klicken, um seine Asset-Seite anzuzeigen, oder Sie können auf den Prozentsatz klicken, den das Asset korreliert oder zum BasisAsset beiträgt, um weitere Informationen über die Asset-Beziehung zum BasisAsset anzuzeigen.

     Wenn Sie beispielsweise auf den verknüpften Prozentsatz neben einem Top-korrelierten Asset klicken, wird eine Informationsmeldung angezeigt, die den Typ der Korrelation zwischen der Anlage und der Basisinressource vergleicht.

   - Wenn der Abschnitt „Top Correlated“ kein Asset enthält, das Sie zu Vergleichszwecken in einem Performance-Diagramm anzeigen möchten, können Sie das Feld „Assets suchen“ im Abschnitt „zusätzliche Ressourcen“ verwenden, um nach anderen Assets zu suchen. Nachdem Sie ein Asset ausgewählt haben, wird es im Abschnitt zusätzliche Ressourcen angezeigt. Wenn Sie keine Informationen über das Asset mehr anzeigen möchten, klicken Sie auf .

#### Verwandte Assets

Falls zutreffend, wird auf einer Seite „Anlagen“ ein Abschnitt „Verwandte Anlagen“ angezeigt. Beispielsweise kann eine Seite mit Volume-Assets Informationen zu Assets wie Speicherpools, verbundenen Switch-Ports und Rechenressourcen anzeigen. Jeder Abschnitt enthält eine Tabelle, in der alle zugehörigen Assets in dieser Kategorie aufgelistet sind, mit Links zu den jeweiligen Bestandsseiten und mehreren Leistungsstatistiken, die sich auf das Asset beziehen.

#### Verwenden des Abschnitts „Zugehörige Assets“

Im Abschnitt „Verwandte Assets“ können Sie alle Assets anzeigen, die mit der Basisressource in Verbindung stehen. Jede zugehörige Anlage wird zusammen mit den zugehörigen Statistiken für die Anlage in einer Tabelle angezeigt. Sie können die Asset-Informationen exportieren, die Asset-Statistiken in den Leistungsdiagrammen der Expertenansicht anzeigen oder ein Diagramm anzeigen, in dem nur Statistiken für verwandte Assets angezeigt werden.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt.

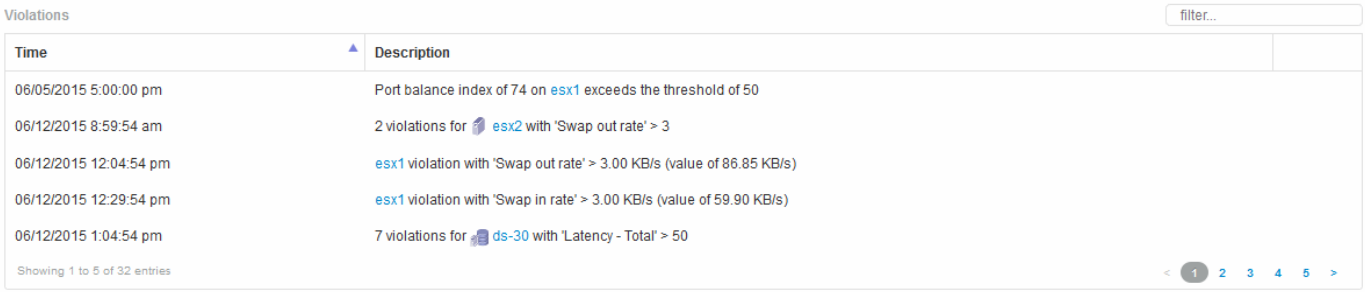
3. So steuern Sie, wie Assets in der Tabelle angezeigt werden:
   - Klicken Sie auf den Namen einer Anlage, um die zugehörige Anlagenseite anzuzeigen.
   - Verwenden Sie das Feld **Filter**, um nur bestimmte Assets anzuzeigen.
   - Klicken Sie auf eine Seitenzahl, um die Assets nach Seite zu durchsuchen, wenn die Tabelle mehr als fünf Elemente enthält.
   - Ändern Sie die Sortierreihenfolge der Spalten in einer Tabelle entweder aufsteigend (Aufwärtspfeil) oder absteigend (Abwärtspfeil), indem Sie auf den Pfeil in der Spaltenüberschrift klicken.
   - Fügen Sie einem Leistungsdiagramm im Abschnitt „Expertenansicht“ eine zugehörige Ressource hinzu, indem Sie den Mauszeiger über die zugehörige Ressource bewegen und auf klicken .
4. So exportieren Sie die in der Tabelle angezeigten Informationen in ein `.CSV` Datei:
   a. Klicken Sie Auf .
   b. Klicken Sie auf **Öffnen mit** und dann auf **OK**, um die Datei mit Microsoft Excel zu öffnen und an einem bestimmten Speicherort zu speichern, oder klicken Sie auf **Datei speichern** und dann auf **OK**, um die Datei in Ihrem Download-Ordner zu speichern.

      Alle Objektattribute für die aktuell zur Anzeige ausgewählten Spalten werden in die Datei exportiert. Nur die Attribute für die angezeigten Spalten werden exportiert. Beachten Sie, dass nur die ersten 10,000 Zeilen der Tabelle exportiert werden.
5. Klicken Sie auf, um die zugehörigen Anlageninformationen in einem Diagramm unter der Tabelle anzuzeigen Und führen Sie einen der folgenden Schritte aus:
   - Klicken Sie auf **Lesen**,**Schreiben** oder **Gesamt**, um die angezeigten metrischen Daten zu ändern. **Total** ist die Standardeinstellung.
   - Klicken Sie Auf Um eine andere Metrik auszuwählen.
   - Klicken Sie Auf Um den Diagrammtyp zu ändern. **Liniendiagramm** ist die Standardeinstellung.
   - Bewegen Sie den Mauszeiger über die Datenpunkte im Diagramm, um zu sehen, wie sich der Wert der Metrik im ausgewählten Zeitraum für jedes zugehörige Asset ändert.
   - Klicken Sie in der Diagrammlegende auf ein zubezogenes Asset, um es dem Diagramm hinzuzufügen oder aus diesem zu entfernen.
   - Klicken Sie in der zugehörigen Anlagentabelle auf eine Seitenzahl, um weitere verwandte Assets im Diagramm anzuzeigen.
   - Klicken Sie Auf Um das Diagramm zu schließen.

#### Verstöße

Sie können den Abschnitt Verstöße auf einer Bestandsseite verwenden, um die Verstöße, falls vorhanden, zu sehen, die in Ihrer Umgebung aufgrund einer Performance-Richtlinie auftreten, die einem Asset zugewiesen wurde. Leistungsrichtlinien überwachen Ihre Netzwerkschwellenwerte und ermöglichen es Ihnen, einen Verstoß gegen einen Schwellenwert sofort zu erkennen, die Auswirkungen zu erkennen und die Auswirkungen und die Ursache des Problems auf eine Weise zu analysieren, die eine schnelle und effektive Korrektur ermöglicht.

Das folgende Beispiel zeigt den Abschnitt „Violations“, der auf einer Asset-Seite für einen Hypervisor angezeigt wird:




### Verwenden des Abschnitts „Verstöße“

Im Abschnitt „Verstöße“ können Sie alle Verstöße anzeigen und verwalten, die aufgrund einer Performance-Richtlinie, die einem Asset zugewiesen wurde, in Ihrem Netzwerk auftreten.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie eine Asset-Seite, indem Sie eine der folgenden Aktionen ausführen:
   - Klicken Sie in der Insight-Symbolleiste auf Geben Sie den Namen des Assets ein, und wählen Sie das Asset aus der Liste aus.
   - Klicken Sie auf **Dashboards**, wählen Sie **Assets Dashboard**, suchen Sie einen Asset-Namen und klicken Sie darauf. Die Seite Anlage wird angezeigt. Der Abschnitt „Verstöße“ zeigt den Zeitpunkt des Verstoßes und eine Beschreibung des Schwellenwerts an, der überschritten wurde, sowie einen Hyperlink zu dem Asset, auf dem der Verstoß aufgetreten ist (z. B. „`2 Verstöße FIR ds-30 mit Latenz - Gesamt > 50`“).
3. Sie können eine der folgenden optionalen Aufgaben ausführen:
   - Verwenden Sie das Feld **Filter**, um nur bestimmte Verstöße anzuzeigen.
   - Klicken Sie auf eine Seitenzahl, um die Verstöße nach Seite zu durchsuchen, wenn die Tabelle mehr als fünf Verstöße enthält.
   - Ändern Sie die Sortierreihenfolge der Spalten in einer Tabelle entweder aufsteigend (Aufwärtspfeil) oder absteigend (Abwärtspfeil), indem Sie auf den Pfeil in der Spaltenüberschrift klicken.
   - Klicken Sie in einer beliebigen Beschreibung auf den Namen des Assets, um dessen Anlagenseite anzuzeigen. Ein roter Kreis zeigt Probleme an, die einer weiteren Untersuchung bedürfen.

     Sie können auf die Leistungsrichtlinie klicken, in der das Dialogfeld „Richtlinie bearbeiten“ angezeigt wird, um die Leistungsrichtlinie zu überprüfen und gegebenenfalls Änderungen an der Richtlinie vorzunehmen.

   - Klicken Sie Auf Um einen Verstoß aus der Liste zu entfernen, wenn Sie feststellen, dass das Problem nicht mehr ein Grund zur Besorgnis ist.

#### Anpassbare Bestandsseite

Zusätzliche Daten können in anpassbaren Widgets auf jeder Bestandsseite angezeigt werden. Wenn Sie die Seite für ein Asset anpassen, wird die Anpassung für alle Assets dieses Typs auf die Seiten angewendet.

Sie können Widgets für die Bestandsseite anpassen, indem Sie die folgenden Aktionen ausführen:

1. Fügen Sie der Seite ein Widget hinzu
2. Erstellen Sie eine Abfrage oder einen Ausdruck für das Widget, um die gewünschten Daten zu zeigen
3. Wählen Sie bei Bedarf einen Filter aus
4. Wählen Sie eine Rollup- oder Gruppierungsmethode aus
5. Speichern Sie das Widget
6. Wiederholen Sie dies für alle gewünschten Widgets
7. Speichern Sie die Bestandsseite

Sie können auch Variablen zur Seite für benutzerdefinierte Elemente hinzufügen, die verwendet werden können, um Ihre angezeigten Daten in Widgets weiter zu verfeinern. Zusätzlich zu regulären Variablen kann jeder Asset-Typ einen Satz von „€Diese“-Variablen verwenden, um schnell Ressourcen zu identifizieren, die direkt mit dem aktuellen Asset in Verbindung stehen, z. B. alle virtuellen Maschinen, die vom selben Hypervisor gehostet werden, der die aktuelle virtuelle Maschine hostet.

Diese benutzerdefinierte Bestandsseite ist sowohl für jeden Benutzer als auch für jeden Asset-Typ eindeutig. Wenn z. B. Benutzer A eine benutzerdefinierte Bestandsseite für eine virtuelle Maschine erstellt, wird diese benutzerdefinierte Seite für jede Seite der virtuellen Maschine für diesen Benutzer angezeigt.

Benutzer können nur benutzerdefinierte Asset-Seiten anzeigen, bearbeiten oder löschen, die sie erstellen.

Benutzerdefinierte Bestandsseiten sind nicht in der Export-/Importfunktion von Insight enthalten.

#### Die Variablen „ USD“ verstehen

Spezielle Variablen auf der anpassbaren Seite „zusätzliche Daten“ eines Assets ermöglichen es Ihnen, auf einfache Weise zusätzliche Informationen anzuzeigen, die direkt mit dem aktuellen Asset in Verbindung stehen.

#### Über diese Aufgabe

Um die Variablen „`` €“ in Widgets auf der anpassbaren Landing Page Ihres Assets zu verwenden, führen Sie die folgenden Schritte aus. Für dieses Beispiel fügen wir ein Tabellen-Widget hinzu.

> „ diese“-Variablen sind nur für die anpassbare Landing Page eines Assets gültig. Für andere Insight Dashboards sind sie nicht verfügbar. Die verfügbaren Variablen „ this“ variieren je nach Asset-Typ.

#### Schritte

1. Navigieren Sie zu einer Anlagenseite für ein Asset Ihrer Wahl. Wählen wir für dieses Beispiel eine Seite mit den Assets der Virtual Machine (VM) aus. Suchen Sie nach einer VM, und klicken Sie auf den Link, um zur Bestandsseite der VM zu gelangen.

   Die Bestandsseite für die VM wird geöffnet.

2. Klicken Sie auf das Dropdown-Menü **Ansicht ändern:** > **zusätzliche Daten der virtuellen Maschine**, um zur anpassbaren Landing Page des Assets zu gelangen.
3. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie **Tabelle Widget**.

   Das Widget „Tabelle“ wird zur Bearbeitung geöffnet. Standardmäßig werden alle Speicher in der Tabelle

angezeigt.

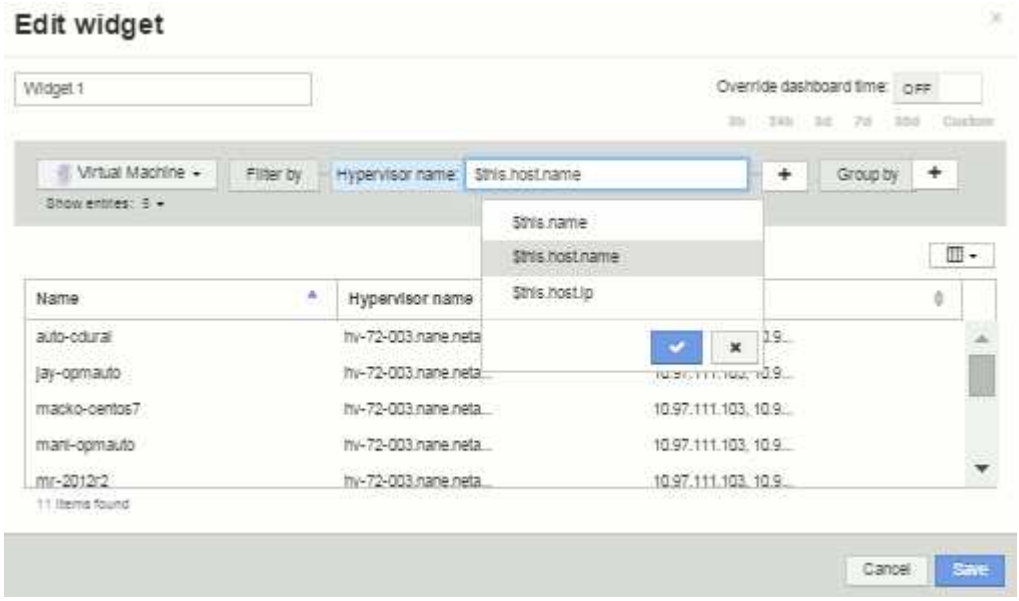
4. Wir wollen alle virtuellen Maschinen anzeigen. Klicken Sie auf die Asset Selector und ändern Sie **Storage** in **Virtual Machine**.

   Alle virtuellen Maschinen werden nun in der Tabelle angezeigt.

5. Klicken Sie auf die Schaltfläche **Spaltenauswahl*** **Und fügen Sie der Tabelle das Feld *Hypervisor Name** hinzu.

   Der Hypervisor-Name wird für jede VM in der Tabelle angezeigt.

6. Es ist uns nur der Hypervisor wichtig, der die aktuelle VM hostet. Klicken Sie auf die Schaltfläche**+**des Felds **Filter by** und wählen Sie **Hypervisor Name** aus.
7. Klicken Sie auf **any** und wählen Sie die Variable * this.host.name* aus. Klicken Sie auf die Schaltfläche, um den Filter zu speichern.




8. Die Tabelle zeigt nun alle VMs, die vom Hypervisor der aktuellen VM gehostet werden. Klicken Sie Auf **Speichern**.

### Ergebnisse

Die Tabelle, die Sie für diese Seite „VM-Anlage“ erstellt haben, wird für alle angezeigten VM-Asset-Seiten angezeigt. Die Verwendung der Variablen * this.host.name €* im Widget bedeutet, dass nur die VMs, die dem Hypervisor der aktuellen Assets gehören, in der Tabelle angezeigt werden.

## Ausgleichen von Netzwerkressourcen

Um Probleme mit dem Ausgleich zu beheben, suchen Sie auf den Bestandsseiten nach Problemen und identifizieren Sie zu wenig ausgelastete Volumen mit hoher Kapazität.

### Schritte

1. Öffnen Sie das Asset Dashboard in Ihrem Browser.

2. In der IOPS-Heatmap der Virtual Machines stellen Sie den Namen einer VM in sehr großem Druck fest, der häufig über Probleme berichtet.
3. Klicken Sie auf den VM-Namen, um die Seite Asset anzuzeigen.
4. Prüfen Sie, ob in der Zusammenfassung Fehlermeldungen angezeigt werden.
5. Prüfen Sie die Performance-Diagramme und insbesondere die am häufigsten korrelierten Ressourcen, um alle Volumes zu finden, die möglicherweise in Konflikt stehen.
6. Fügen Sie dem Leistungsdiagramm Volumes hinzu, um die Aktivitätsmuster zu vergleichen und weitere Bestandsseiten für andere Ressourcen anzuzeigen, die an dem Problem beteiligt sind.
7. Scrollen Sie zum Ende der Asset-Seite, um Listen aller mit der VM verbundenen Ressourcen anzuzeigen. Notieren Sie alle VMDKs, die mit hoher Kapazität laufen. Die Ursache für den Konflikt ist wahrscheinlich.
8. Um das Problem des Ausgleichs zu lösen, identifizieren Sie eine Ressource, die nicht ausgelastet ist, um die Last von einer überlasteten Ressource zu empfangen, oder entfernen Sie eine weniger anspruchsvolle Anwendung von der stark ausgelasteten Ressource.

## Überprüfung der Netzwerkleistung

Sie können die Performance Ihrer Storage-Umgebung untersuchen und unzureichend ausgelastete und überlastete Ressourcen identifizieren und Risiken identifizieren, bevor diese zu Problemen werden.

Mithilfe von Insight können Sie Performance- und Verfügbarkeitsprobleme beheben und verhindern, die durch die erfassten Storage-Daten verursacht werden.

Sie können Insight verwenden, um die folgenden Aufgaben zum Performance-Management durchzuführen:

- Überwachung der Performance in der gesamten Umgebung
- Ermittlung von Ressourcen, die die Leistung anderer Geräte beeinflussen

### Die Bedeutung von Ports

Für den Insight Server und den Data Warehouse (DWH)-Server müssen möglicherweise mehrere TCP-Ports frei sein, um zuverlässig arbeiten zu können. Einige dieser Ports werden nur für Prozesse verwendet, die an den localhost-Adapter gebunden sind (127.0.0.1), aber dennoch benötigt werden, damit die Kerndienste zuverlässig arbeiten können. Die Anzahl der erforderlichen Ports ist eine Überzahl der Ports, die im gesamten Netzwerk verwendet werden.

### Insight Server-Ports

Für Insight Server können Software-Firewalls installiert sein. Die "Löcher", die geöffnet werden müssten, wären wie unten beschrieben.

**Inbound HTTPS 443** - vorausgesetzt, Sie haben die Insight WebUI auf TCP 443 ausgeführt, müssen Sie das als, um alle und alle der folgenden Verbraucher zu ermöglichen offenlegen:

- Insight Benutzer der WebUI
- Remote-Erfassungseinheiten, die eine Verbindung zum Insight-Server herstellen möchten
- OCI DWH-Server mit Verbindungen zu diesem Insight-Server.
- Programmatische Interaktionen mit der Insight REST-API

Unsere allgemeine Empfehlung für alle, die eine Firewall auf Insight Server-Ebene implementieren möchten, ist der HTTPS-Zugriff auf alle IP-Blöcke des Unternehmensnetzwerks.

**Inbound MySQL (TCP 3306)**. Dieser Port muss nur jedem Insight DWH-Server mit einem Konnektor zugänglich sein

Während Insight Dutzende von Datensammlern umfasst, sind sie alle Umfragebasiert – Insight wird dazu führen, dass seine Acquisition Units (aus) ausgehende Kommunikation mit verschiedenen Geräten initiieren. Solange Ihre hostbasierte Firewall „statusorientiert“ ist, sodass sie Rückverkehr über die Firewall zulässt, sollten hostbasierte Firewalls auf dem Insight Server die Datenerfassung nicht beeinträchtigen.

#### Data Warehouse-Ports

Für Insight DWH-Server:

**Inbound HTTPS 443** - vorausgesetzt, Sie haben die Insight WebUI läuft auf TCP 443, müssen Sie das als die folgenden Verbraucher zu ermöglichen:

- Insight administrative Benutzer des DWH Admin-Portals

**Inbound HTTPS (TCP 9300)** - das ist die Cognos Reporting-Schnittstelle. Wenn Benutzer mit der Cognos-Reporting-Schnittstelle interagieren, muss diese Remote angezeigt werden.

Wir können uns Umgebungen vorstellen, in denen das DWH möglicherweise nicht offengelegt werden muss - vielleicht stellen die Verfasser des Berichts einfach RDP-Verbindungen zum DWH-Server her und erstellen und planen dort Berichte, während alle Berichte über SMTP geliefert oder auf ein Remote-Dateisystem geschrieben werden sollen.

**Inbound MySQL (TCP 3306)**. Dieser Port muss nur dann offengelegt werden, wenn Ihr Unternehmen MySQL-basierte Integrationen mit DWH-Daten hat. Extrahieren Sie Daten aus den verschiedenen DWH-Data Marts zur Aufnahme in andere Anwendungen wie CMDBs, Chargeback-Systeme usw.

#### Analyse der langsamen PC-Leistung

Wenn Sie Anrufe von Netzwerkbenutzern erhalten, die sich beschweren, dass ihre Computer langsam laufen, müssen Sie die Hostleistung analysieren und die betroffenen Ressourcen identifizieren.

##### Bevor Sie beginnen

In diesem Beispiel gab der Anrufer den Hostnamen an.

##### Schritte

1. Öffnen Sie Insight in Ihrem Browser.
2. Geben Sie den Hostnamen in das Feld **Assets suchen** ein und klicken Sie in den Suchergebnissen auf den Hostnamen.

   Die *Asset-Seite* für die Ressource wird geöffnet.

3. Prüfen Sie auf der Systemseite für den Host die Leistungsdiagramme in der Mitte der Seite. Neben der üblicherweise vorab ausgewählten Latenz und IOPS können Sie verschiedene Datentypen anzeigen. Aktivieren Sie die Kontrollkästchen für andere Datentypen, wie Durchsatz, Speicher, CPU oder IP-Durchsatz, je nach Gerätetyp.

4. Um eine Beschreibung eines Punktes auf einem Diagramm anzuzeigen, positionieren Sie den Mauszeiger über dem Punkt.
5. Sie können auch den Zeitraum ändern, indem Sie die Auswahl oben auf der Seite auf 3 Stunden bis zu 7 Tagen oder Alle verfügbaren Daten festlegen.
6. Untersuchen Sie die Liste der **Top korrelierten Ressourcen**, um zu sehen, ob es andere Ressourcen mit dem gleichen Aktivitätsmuster wie die Basisressource gibt.

   Die erste Ressource in der Liste ist immer die Basisressource.

   a. Klicken Sie auf einen verknüpften Prozentsatz neben einer korrelierten Ressource, um zu sehen, ob das korrelierte Aktivitätsmuster für IOPS oder CPU für die Basisressource und eine andere Ressource ist.
   b. Aktivieren Sie das Kontrollkästchen für eine korrelierte Ressource, um ihre Daten zu den Leistungsdiagrammen hinzuzufügen.
   c. Klicken Sie auf den verknüpften Namen der korrelierten Ressource, um die Bestandsseite anzuzeigen.
7. Suchen Sie für eine VM, wie in diesem Beispiel, den Speicherpool unter **Top correlated Resources** und klicken Sie auf den Namen des Speicherpools.

#### Analyse korrelierter Ressourcen

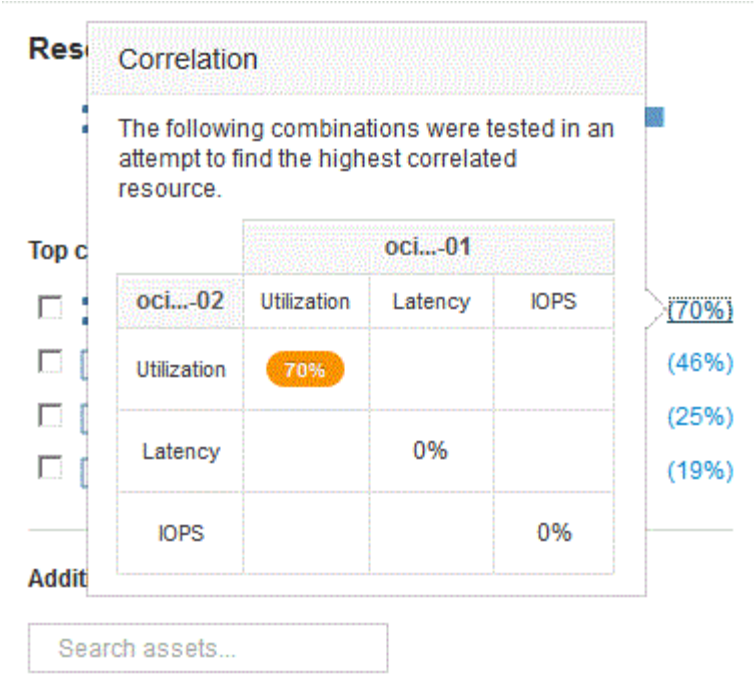
Wenn Sie Leistungsprobleme untersuchen und die *Asset-Seite* für ein Gerät öffnen, sollten Sie die Liste Top Correlated Resources verwenden, um die in den Leistungsdiagrammen angezeigten Daten zu verfeinern. Eine Ressource mit einem hohen Prozentsatz zeigt an, dass die Ressource ähnliche Vorgänge wie die Basisressource hat.

##### Über diese Aufgabe

Sie untersuchen derzeit ein Leistungsproblem und öffnen die Bestandsseite für ein Gerät.

##### Schritte

1. In der Liste **Top Correlated Resources** ist die erste Ressource die Basisressource. Die korrelierten Ressourcen in der Liste werden nach Prozentsatz der korrelierten Aktivität mit dem ersten Gerät sortiert. Klicken Sie auf den verknüpften Prozentsatz der Korrelation, um die Details anzuzeigen. In diesem Beispiel wird der 70-prozentige Korrelation in der Auslastung dargestellt. Sowohl die Basisressource als auch diese korrelierte Ressource haben also eine gleich hohe Auslastung.




2. Um eine korrelierte Ressource zu den Leistungsdiagrammen hinzuzufügen, aktivieren Sie das Kontrollkästchen in der Liste **Top correlated Resources** für die Ressource, die Sie hinzufügen möchten. Standardmäßig enthält jede Ressource die verfügbaren Gesamtdaten, Sie können jedoch im Menü des Kontrollkästchens nur Daten lesen oder nur Daten schreiben auswählen.

   Jede Ressource in den Diagrammen hat eine andere Farbe, sodass Sie die Leistungsmessungen für jede Ressource vergleichen können. Nur der geeignete Datentyp wird für die ausgewählten Messgrößen dargestellt. CPU-Daten enthalten z. B. keine Lese- oder Schreibmetriken, sodass nur die Gesamtdaten verfügbar sind.

3. Klicken Sie auf den verknüpften Namen der korrelierten Ressource, um die Bestandsseite anzuzeigen.
4. Wenn in den Top-korrelierten Ressourcen, die Ihrer Meinung nach bei der Analyse berücksichtigt werden sollten, keine Ressource angezeigt wird, können Sie diese Ressource über das Feld **Search Assets** finden.

## Überwachung der Fibre-Channel-Umgebung

Über die Fibre Channel-Ressourcen-Seiten von OnCommand Insight können Sie die Performance und Bestandsaufnahme der Fabrics in Ihrer Umgebung überwachen und sämtliche Änderungen berücksichtigen, die möglicherweise zu Problemen führen.

### Fibre Channel-Asset-Seiten

Auf den Assetseiten von Insight finden Sie zusammenfassende Informationen über die Ressource, ihre Topologie (das Gerät und ihre Verbindungen), Leistungsdiagramme und Tabellen der zugehörigen Ressourcen. Sie können die Fabric-, Switch- und Port-Asset-Seiten zur Überwachung Ihrer Fibre-Channel-Umgebung verwenden. Besonders hilfreich bei der Fehlerbehebung bei einem Fibre-Channel-Problem ist das Performance-Diagramm für jede Port-Ressource, das den Datenverkehr für den ausgewählten Port mit den wichtigsten Beiträgen anzeigt. Darüber hinaus können Sie in diesem Diagramm auch Kredit-Kennzahlen und Port-Fehler zwischen Puffern anzeigen, sodass Insight für jede Metrik ein separates Performance-Diagramm anzeigt.

### Performance-Richtlinien für Port-Metriken

Insight ermöglicht die Erstellung von Performance-Richtlinien, um Ihr Netzwerk auf verschiedene Schwellenwerte zu überwachen und bei Überschreitung dieser Schwellenwerte Alarme auszugeben. Sie können Performance-Richtlinien für Ports basierend auf verfügbaren Port-Kennzahlen erstellen. Wenn ein Schwellenwert verletzt wird, erkennt Insight diesen und meldet ihn auf der zugehörigen Asset-Seite. Dazu wird ein roter durchlässiger Kreis angezeigt, gegebenenfalls per E-Mail-Benachrichtigung und im Dashboard für Verstöße oder einem benutzerdefinierten Dashboard, das Verstöße meldet.

## Time-to-Live (TTL)- und Downsampling-Daten

Ab OnCommand Insight 7.3 wurde die Datenaufbewahrung oder Time-to-Live (TTL) von 7 auf 90 Tage erhöht. Da dadurch viel mehr Daten für Diagramme und Tabellen verarbeitet werden und das Potenzial für Zehntausende von Datenpunkten besteht, werden die Daten vor der Anzeige heruntergesampelt.

Downsampling bietet eine statistische Näherung Ihrer Daten in Diagrammen, sodass Sie einen effizienten Überblick über die Daten erhalten, ohne jeden Datenpunkt anzeigen zu müssen, während Sie gleichzeitig eine genaue Ansicht Ihrer gesammelten Daten erhalten.

### Warum ist ein Downsampling erforderlich?

Bei Insight 7.3 wird die Live-Zeit (TTL) für Daten auf 90 Tage erhöht. Dies bedeutet eine Erhöhung der Verarbeitungsmenge, die erforderlich ist, um Daten für die Anzeige in Diagrammen und Diagrammen vorzubereiten. Damit Diagramme schnell und effizient angezeigt werden können, werden die Daten so heruntergesampelt, dass die Gesamtform eines Diagramms erhalten bleibt, ohne dass für dieses Diagramm jeder einzelne Datenpunkt verarbeitet werden muss.

Beim Downsampling gehen keine tatsächlichen Daten verloren. Sie können die tatsächlichen Daten für Ihr Diagramm anstelle von abtasteten Daten anzeigen, indem Sie die unten dargestellten Schritte befolgen.

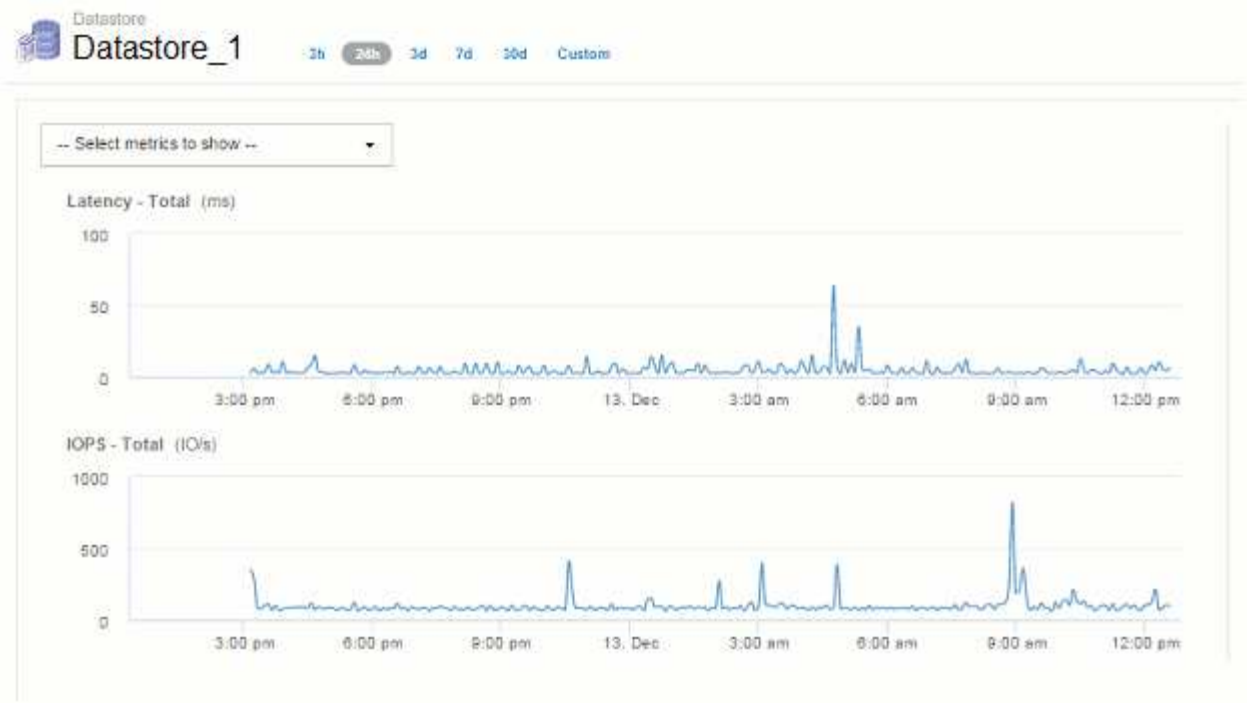
### Funktionsweise von Downsampling

Die Daten werden unter den folgenden Bedingungen heruntererfasst:

- Wenn Ihr ausgewählter Zeitraum Daten von maximal 7 Tagen enthält, erfolgt keine Downsampling-Messung. Diagramme zeigen tatsächliche Daten an.
- Wenn Ihr ausgewählter Zeitraum mehr als 7 Tage Daten enthält, jedoch weniger als 1,000 Datenpunkte, erfolgt keine Downsampling-Messung. Diagramme zeigen tatsächliche Daten an.
- Wenn Ihr ausgewählter Zeitbereich mehr als 7 Tage Daten und mehr als 1,000 Datenpunkte umfasst, werden die Daten nach unten abgetastet. Diagramme zeigen angenähte Daten an.

Die folgenden Beispiele zeigen ein Downsampling in Aktion. Die erste Abbildung zeigt die Latenz- und IOPS-Diagramme auf einer Datastore-Bestandsseite für einen Zeitraum von 24 Stunden, wie durch Auswählen von **24h** auf der Zeitauswahl der Asset-Seite dargestellt. Sie können die gleichen Daten auch sehen, indem Sie **Custom** auswählen und den Zeitbereich auf den gleichen 24-Stunden-Zeitraum einstellen.

Da wir einen Zeitbereich von weniger als 7 Tagen wählen und wir weniger als 1,000 Datenpunkte haben, sind die angezeigten Daten tatsächliche Daten. Es erfolgt keine Downsampling-Messung.




Wenn Sie jedoch Daten anzeigen, indem Sie entweder **30d** auf der Zeitauswahl der Anlagenseite wählen, Wenn Sie einen benutzerdefinierten Zeitraum von mehr als 7 Tagen festlegen (oder wenn Insight mehr als 1,000 Datenproben für den ausgewählten Zeitraum erfasst hat), werden die Daten vor der Anzeige heruntergerechnet. Wenn Sie ein abtasteter Diagramm vergrößern, werden im Display weiterhin die approximierten Daten angezeigt.

Wenn Sie ein Diagramm mit Downsampling vergrößern, handelt es sich bei dem Zoom um einen digitalen Zoom. Die Anzeige zeigt weiterhin die approximierten Daten an.

Sie sehen dies in der folgenden Abbildung, in der der Zeitbereich zuerst auf 30d gesetzt wird, und das Diagramm wird dann vergrößert, um den gleichen 24-Stunden-Zeitraum wie oben anzuzeigen.

Die abtasteten Diagramme zeigen den gleichen 24-Stunden-Zeitraum wie die oben genannten "tatsächlichen" Diagramme, sodass die Linien die gleiche allgemeine Form folgen, so dass Sie schnell interessante Gipfel oder Täler in Ihren Leistungsdaten zu erkennen.

Aufgrund der Angleichung der Daten an die Abtastrate können die Diagrammlinien beim Vergleich von Downsampling vs. Leicht ausgeschaltet werden Aktuelle Daten, um eine bessere Ausrichtung in den Diagrammen zu ermöglichen. Die Differenz ist jedoch minimal und wirkt sich nicht auf die Gesamtgenauigkeit der angezeigten Daten aus.

**Verstöße gegen herunterbeprobierte Diagramme**

Beachten Sie beim Anzeigen von Downsampling-Diagrammen, dass Verstöße nicht angezeigt werden. Um Verstöße zu sehen, können Sie eine von zwei Dingen tun:

- Zeigen Sie die aktuellen Daten für diesen Zeitbereich an, indem Sie in der Zeitauswahl der Anlagenseite „Benutzerdefiniert“ auswählen und einen Zeitbereich von weniger als 7 Tagen eingeben. Bewegen Sie den Mauszeiger über jeden roten Punkt. In der QuickInfo wird der aufgetretene Verstoß angezeigt.
- Notieren Sie den Zeitbereich, und suchen Sie die Verstöße im Dashboard für Verstöße.

## Beschneidung der Bestandshistorie

Ab Version 7.3.2 speichert Insight 90 Tage lang den Verlaufs der Bestandsänderungen (Grundlagen). In früheren Versionen von Insight wurden die gesamten Bestandsänderungsverläufe ab dem Zeitpunkt der Installation gespeichert. Nach einem Upgrade von einer älteren Version von Insight wird der ältere Bestandsverlauf auf 90 Tage reduziert und dann aufbewahrt.

Nach dem Upgrade auf die aktuelle Version von OnCommand Insight wird die Historie auf die letzten 90 Tage zurückgeführt. Insight beschneidet die Geschichte in 30-Tage-Brocken, die einmal am Tag auftreten, beginnend mit dem ältesten, bis 90 Tage Wert der Geschichte bleibt. Dann wird Geschichte täglich geschnitten, um nur 90 Tage’ Wert der Bestandsänderung Geschichte zu halten.

## NAS-Pfad für VMs

OnCommand Insight 7.3 unterstützt NAS-Pfade für virtuelle Maschinen zu Storage Shares. Diese Pfade ähneln NAS-Pfaden für Hosts zu Storage-Freigaben. Wenn die IP-Adresse einer VM auf eine Freigabe zugreifen darf, wird ein NAS-Pfad erstellt.

NAS-Pfade für virtuelle Maschinen werden auf der Landing Page Internal Volumes angezeigt. Diese Seite enthält ein Widget „Storage Resources“, das auf das Gast gemountet ist und die internen Volumes angibt, auf die VMs Zugriff haben.

- NAS-Pfade werden erstellt, wenn virtuelle Maschinen auf die Backend-Freigaben zugreifen. Es gibt keine Bestätigung, ob die virtuellen Maschinen auf die Freigaben zugreifen oder nicht.
- Die Korrelationsberechnung basiert auf Latenzen und IOPS und schließt nicht Fälle ein, in denen VMs NAS-Pfade zum Back-End Storage aufweisen.
- Der Benutzer kann die Freigabe nach Initiator-IP-Adresse abfragen, aber Abfragen nach Pfad werden nicht unterstützt.

In der Tabelle Compute Resources des internen Volumes werden jetzt auch VMs mit NAS-Pfaden angezeigt.

Für jede VM, CPU und jeder Arbeitsspeicher werden Auslastungs- und Performance-Daten bereitgestellt.

**Auswirkungen auf das Data Warehouse**

Folgende Änderungen am Data Warehouse sind nach dem Upgrade auf OnCommand Insight 7.3 enthalten:

- Die Tabelle dwh_Inventory.nas_Logical wird aus dem Inventory Data Mart entfernt und durch eine Ansicht ersetzt.

  Alle Insight 7.2.x-Berichte, die die NFS-Pfadtabelle enthalten, werden beibehalten.

- Die Tabelle dwh_Inventory.nas_cr_Logical wird dem Inventory Data Mart hinzugefügt und enthält Folgendes:
  - Compute-Ressource
  - Internes Volumen
  - Storage
  - NAS-Freigabe

## Kapazität als Zeitreihe

Mit OnCommand Insight 7.3 werden Kapazitätsinformationen als Zeitreihendaten gemeldet und eingetragen.

Bisher wurden aus Datenquellen erfasste Kapazitätsinformationen ausschließlich „Point-in-Time“ (PIT)-Daten verwendet, was bedeutet, dass sie in Diagrammen nicht als Zeitreihendaten verwendet werden konnten. Jetzt können Kapazitätswerte für Assets wie folgt als Zeitreihendaten verwendet werden:

- Grafische Darstellung in Tabellen, Widgets, Expertenansichten und an jedem Ort, an dem Zeitreihendaten angezeigt werden
- Angewendet auf Leistungsschwellenwerte mit Verstößen unter Verwendung vorhandener Semantik
- Wird gegebenenfalls in Ausdrücken mit anderen Leistungsindikatoren verwendet

Beachten Sie, dass bei einem Upgrade von einer früheren Version von Insight frühere PIT-Kapazitätswerte, die in Abfragen oder in Filtern für benutzerdefinierte Dashboards verwendet werden, durch Kapazitätsdaten für Zeitreihen ersetzt werden. Dies kann zu kleinen Änderungen in der Art und Weise führen, wie Kapazitätsdaten gemeldet oder gefiltert werden, wenn sie mit den äquivalenten Daten in früheren Insight-Versionen verglichen werden.

# OCI Data Collector: Support Matrix

Die Data Collector Support Matrix bietet Referenz für Data Collectors, die von OCI unterstützt werden, einschließlich Hersteller- und Modellinformationen.

## HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7440C HPE_3PAR 7450C HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3PAR 7200 HP_3PAR 7200C HP_3PAR 7400 HP_3PAR 7400C HP_3PAR 7450C HP_3PAR 8200 HP_3PAR 8440 | 3.2.2 (MU2) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 (MU2) 3.3.1 (MU5) 4.4.1 Auslösetyp: Standard Support Release |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
| --- | --- | --- | --- | --- | --- |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | Volumenreferenz | Name | Implementiert | SSH | |
| | | Storage-Ip | Implementiert | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Verhältnis | | | |
| | | Server-ID | Implementiert | SMI-S | |
| **Produkt** | **Kategorie** | **Funktion/Attribut lesen** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Gesamtdurchsatz | Implementiert | SMI-S | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SMI-S | |
| | | „Ausstehend“ | Implementiert | SMI-S | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| 3PAR SMI-S | SMI-S | HTTP/HTTPS | 5988/5989 | | Richtig | Richtig | Richtig | Richtig |
| 3PAR-CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

## Amazon AWS EC2

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- 1 2014-10-01

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Disk | VirtualisierungsDisk OID | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Virtual Machine | Implementiert | HTTPS | |
| | Host | Host-Betriebssystem | Implementiert | HTTPS | |
| | | IPS | Implementiert | HTTPS | |
| | | Hersteller | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | OID | Implementiert | HTTPS | |
| | Info | Api-Beschreibung | Implementiert | HTTPS | |
| | | Api-Name | Implementiert | HTTPS | |
| | | Api-Version | Implementiert | HTTPS | |
| | | Name der Datenquelle | Implementiert | HTTPS | Info |
| | | Datum | Implementiert | HTTPS | |
| | | Ersteller-ID | Implementiert | HTTPS | |
| | | Erstellschlüssel | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EC2 API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## Brocade Fibre Channel Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 184.0 Brocade 200E Brocade 300E Brocade 4024 Embedded Brocade 4100 Brocade 4900 Brocade 5000 Brocade 5100 Brocade 6510 Brocade 6520 Embedded Brocade 7800 Brocade 5300 Brocade 5480 Brocade 6505 Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade M5224 Embedded Brocade M6505 Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-8 | v5.3.0a v6.1.0c v6.1.0h v6.2.1b v6.2.1b v6.2.2f v6.2.2f v6.3.2b v6.4.1b v6.4.1b v6.4.2b1 v7.0.2c v7.2.1c v7.2.1c v7.2.1d v8.2 01 857687 01 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
| --- | --- | --- | --- | --- | --- |

| | | | | | |
|---|---|---|---|---|---|
| | | Gigabits | | | |
| | | Unbekannte Konnektivität | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | WWN | Implementiert | SSH | |
| | Switch | Domänen-Id | Implementiert | SSH | |
| | | Firmware-Version | Implementiert | SSH | |
| | | IP | Implementiert | SSH | |
| | | URL managen | Implementiert | SSH | |
| | | Hersteller | Implementiert | SSH | |
| | | Modell | Implementiert | SSH | |
| | | Name | Implementiert | Manuelle Eingabe | |
| | | Seriennummer | Implementiert | SSH | |
| | | Switch-Rolle | Implementiert | SSH | |
| | | Switch-Status | Implementiert | SSH | |
| | | Switch-Status | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | | VSAN aktiviert | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |
| | Zone | Zonenname | Implementiert | SSH | |
| | Zonenmitglied | Typ | Lücke | SSH | |
| | | WWN | Implementiert | SSH | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | SSH | |
| | | Konfigurationsname | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Port-Fehler | Implementiert | SNMP | Port-Fehler Verlust |
| | | Port-Fehler | Implementiert | SNMP | Port-Fehler Synchronisierung |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Port-Fehler: Zeitüberschreitung Bei Der Übertragung Des Discard-Moduls | Implementiert | SNMP | Port-Fehler Zeitüberschreitung Verwerfen |
| | | Gesamtanzahl Der Portfehler | Implementiert | SNMP | Gesamtanzahl an Port-Fehlern |
| | | Server-ID | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Gesamte Traffic Frame Rate | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Durchschnittliche Bildgröße | Implementiert | SNMP | Durchschnittliche Größe des Datenverkehrs |
| | | TX-Rahmen | Implementiert | SNMP | Durchschnittliche Größe des Verkehrsaufkommens |
| | | Rate Des Verkehrsaufkommens | Implementiert | SNMP | |
| | | Gesamte Datenverkehrrate | Implementiert | SNMP | |
| | | Übertragungsrate Des Datenverkehrs | Implementiert | SNMP | |
| | | Auslastung Des Erfressenen Datenverkehrs | Implementiert | SNMP | |
| | | Gesamtauslastung Des Datenverkehrs | Implementiert | SNMP | Gesamte Traffic-Auslastung |
| | | Auslastung Des Datenverkehrs | Implementiert | SNMP | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Brocade SNMP | SNMP | SNMPv1, SNMPv2 UND SNMPv3 | 161 | | Richtig | Richtig | Richtig | Richtig |
| Brocade SSH | SSH | SSH | 22 | | Falsch | Falsch | Richtig | Richtig |
| Konfiguration des Datenquellenassistenten | Manuelle Eingabe | | | | Richtig | Richtig | Richtig | Richtig |

## Brocade Network Advisor HTTP

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- 14.4.5

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | Fabric | Name | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Info | Api-Beschreibung | Implementiert | HTTP/S | |
| | | Api-Name | Implementiert | HTTP/S | |
| | | Api-Version | Implementiert | HTTP/S | |
| | | Name der Datenquelle | Implementiert | HTTP/S | Info |
| | | Datum | Implementiert | HTTP/S | |
| | | Ersteller-ID | Implementiert | HTTP/S | |
| | | Erstellschlüssel | Implementiert | HTTP/S | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTP/S | |
| | | Objekttyp | Implementiert | HTTP/S | |
| | | Quelle | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Zone | Zonenname | Implementiert | HTTP/S | |
| | Zonenmitglied | Typ | Lücke | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | HTTP/S | |
| | | Konfigurationsname | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Port | BB Credit Null Gesamt | Implementiert | HTTP/S | BB Credit Null Gesamt |
| | | BB Credit Zero übertragen | Implementiert | HTTP/S | BB Credit Zero übertragen |
| | | BB Credit Zero MS übertragen | Implementiert | HTTP/S | BB Credit Zero MS übertragen |
| | | Port-Fehler Klasse 3 Verwerfen | Implementiert | HTTP/S | |
| | | Port-Fehler Crc | Implementiert | HTTP/S | Port-Fehler Crc |
| | | Port-Fehler Enc In | Implementiert | HTTP/S | Port-Fehler Enc In |
| | | Port-Fehler Kurzer Rahmen | Implementiert | HTTP/S | Port-Fehler aufgrund des kurzen Rahmens |
| | | Verbindungsfehler Bei Portfehlern | Implementiert | HTTP/S | Verbindungsfehler bei Port-Fehlern |
| | | Signalverlust Bei Port-Fehler | Implementiert | HTTP/S | Port-Fehler signalisieren Verlust |
| | | Port-Fehler Sync-Verlust | Implementiert | HTTP/S | Port-Fehler Synchronisierungsverlust |
| | | Port-Fehler: Zeitüberschreitung Bei Der Übertragung Des Discard-Moduls | Implementiert | HTTP/S | Port-Fehler Zeitüberschreitung Verwerfen |
| | | Gesamtanzahl Der Portfehler | Implementiert | HTTP/S | Gesamtanzahl an Port-Fehlern |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Brocade Network Advisor REST-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

## Cisco MDS und Nexus Fabric Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| C97148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148 DS-C9148 DS-C9559 DS-C9488 DS-C9559 DS-C969148T C9 DS-C9559 DS-C966K9 DS-C9509 DS-C9 8978 2 | 3.2 6.2 7.1 7.3 11 7.3 7 8.1 2 8.4 8.4(2c) 9 4 7.3 7.3 7 7.3 8.3 8.4 8.4 8.4(3a) 23 6.2 33 6.2 7.3 7.3 13 7.3 8 8.3 8.4 8.4(1a) 6.2(6.2)N1(3.13e) 6.2(21)N2(4.04i) 29(17)N2(4.13j) 6.2(6.2)N1(4.21k) 6.2(1) 15(19) N1(6.2) 6.2(1) 13(8g) 6.2(5.2)N1(41a) 6.2(5.2)6.2)5.2(5.2) 5.2) 8(3) 5.2) 3) 5.0) 5.0(5.0) 3) 5.0) 3(5.0) 3) 4.1 8.4 8.4 8.5 9.2 2 9.3 9.3 2 9.3 9.4) |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | SNMP | |
| | | VSAN aktiviert | Implementiert | SNMP | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | WWN | Implementiert | SNMP | |
| | WWN-Alias | Host-Aliase | Implementiert | SNMP | |
| | | Objekttyp | Implementiert | SNMP | |
| | | Quelle | Implementiert | SNMP | |
| | | WWN | Implementiert | SNMP | |
| | Zone | Zonenname | Implementiert | SNMP | |
| | | Zonentyp | Implementiert | SNMP | |
| | Zonenmitglied | Typ | Lücke | SNMP | |
| | | WWN | Implementiert | SNMP | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | SNMP | |
| | | Konfigurationsname | Implementiert | SNMP | |
| | | Standardverhalten Für Zoneneinzug | Implementiert | SNMP | |
| | | Steuerung Zusammenführen | Implementiert | SNMP | |
| | | WWN | Implementiert | SNMP | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Discard-Moduls | | | |
| | | Gesamtanzahl Der Portfehler | Implementiert | SNMP | Gesamtanzahl an Port-Fehlern |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Gesamte Traffic Frame Rate | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Durchschnittliche Bildgröße | Implementiert | SNMP | Durchschnittliche Größe des Datenverkehrs |
| | | TX-Rahmen | Implementiert | SNMP | Durchschnittliche Größe des Verkehrsaufkommens |
| | | Rate Des Verkehrsaufkommens | Implementiert | SNMP | |
| | | Gesamte Datenverkehrrate | Implementiert | SNMP | |
| | | Übertragungsrate Des Datenverkehrs | Implementiert | SNMP | |
| | | Auslastung Des Erfressenen Datenverkehrs | Implementiert | SNMP | |
| | | Gesamtauslastung Des Datenverkehrs | Implementiert | SNMP | Gesamte Traffic-Auslastung |
| | | Auslastung Des Datenverkehrs | Implementiert | SNMP | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Cisco SNMP | SNMP | SNMPv1 (nur Inventar), SNMPv2, SNMPv3 | 161 | | Richtig | Richtig | Richtig | Richtig |

## EMC Celerra (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| NSX VG8 VNX5600 | 5.5.38-1 7.1.76-4 7.1.79-8 8.1.9-184 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | SSH | |

| Produkt | Kategorie | Fähigkeitsattribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Celerra-CLI | SSH | SSH | | | Richtig | Falsch | Richtig | Richtig |

## EMC CLARiiON (NaviCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 6.28 7.32 7.33 | CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000 | 04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | | Speicherpool-Id | Implementiert | CLI | |
| | | Thin Provisioning | Implementiert | CLI | |
| | | Typ | Lücke | CLI | |
| | | UUID | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | Volume-Zuordnung | LUN | Implementiert | CLI | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | CLI | |
| | | Storage-Port | Implementiert | CLI | |
| | | Typ | Lücke | CLI | |
| | Volume-Maske | Initiator | Implementiert | CLI | |
| | | Protokoll-Controller | Implementiert | CLI | |
| | | Storage-Port | Implementiert | CLI | |
| | | Typ | Lücke | CLI | |
| | Volumenmitglied | Kapazität | Implementiert | CLI | Verwendete Kapazität des Snapshot in MB |
| | | Name | Implementiert | CLI | |
| | | Rang | Implementiert | CLI | |
| | | Gesamtbruttokapazität | Implementiert | CLI | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | CLI | Redundanzebene |
| | | Speicherpool-Id | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | WWN-Alias | Host-Aliase | Implementiert | CLI | |
| | | IP | Implementiert | CLI | |
| | | Objekttyp | Implementiert | CLI | |
| | | Quelle | Implementiert | CLI | |
| | | WWN | Implementiert | CLI | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | Storage Pools: Kapazität | Implementiert | CLI | |
|---|---|---|---|---|---|
| | | Taste | Implementiert | CLI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | CLI | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | CLI | |
| | | Bruttokapazität | Implementiert | CLI | |
| | | Gesamtkapazität | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | CLI | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | CLI | |
| | | Taste | Implementiert | CLI | |
| | | Sonstige Gesamtkapazität | Implementiert | CLI | |
| | | Andere Genutzte Kapazität | Implementiert | CLI | |
| | | Server-ID | Implementiert | CLI | |
| | | Reservierte Snapshot-Kapazität | Implementiert | CLI | |
| | | Verwendete Snapshot-Kapazität | Implementiert | CLI | |
| | | Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie | Implementiert | CLI | Als Zeitreihe gemeldet |
| | Datenmenge | Bruttokapazität | Implementiert | CLI | |
| | | Gesamtkapazität | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | CLI | |
| | | Taste | Implementiert | CLI | |
| | | Server-ID | Implementiert | CLI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Navi CLI | CLI | | 6389,2162,2163,443 (HTTPS)/80 (HTTP) | | Richtig | Richtig | Richtig | Falsch |

## EMC Data Domain (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990 | 5.4.6.0-503967 5.5.0.9-471508 5.5.2.1-486308 6.1.0.5-567091 6.2.1.30-663869 6.2.1.50-680189 7.10.1.15-1078832 7.10.1.20-1090468 7.2.0.70-686759 7.6.5.25-1078970.4.0-1017976 7.7.5.11-1046187 7.7.0.40-691389 7.7 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | SSH | Verhältnis zur Konvertierung von nutzbarer |
|---|---|---|---|---|---|
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Speicherpool-Id | Implementiert | SSH | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | SSH | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | SSH | |
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Data Domain CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |

## EMC ECS

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| ECS | 3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | Storage-Node | Name | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Version | Implementiert | HTTPS | Softwareversion |
| | Storage-Pool | In Dwh-Kapazität Einbeziehen | Implementiert | HTTPS | Ein Weg von ACQ zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind |
| | | Name | Implementiert | HTTPS | |
| | | Kapazität der physischen Festplatte (MB) | Implementiert | HTTPS | Wird als Rohkapazität für den Storage-Pool verwendet |
| | | Raid-Gruppe | Implementiert | HTTPS | Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt |
| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | HTTPS | Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | HTTPS | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | HTTPS | |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC ECS REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## Dell EMC Isilon/PowerScale (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| A200 A2000 A300 A3000 F800 H400 H500 H500-4U-Single-128 GB-1 x 1 GE-2 x 10 GE SFP+-30 TB-1638 GB SSD H700 NL400 NL410 Traceback (letzter Anruf zuletzt): X210 X400 Sudo Python | 9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8.0.0.6 v8.0.0.7 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Zugehöriges Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Fehlerhafte Bruttokapazität | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Standardattribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Storage-Node-Daten | IOPS Lesen | Implementiert | SSH | Anzahl der Lese-IOPS im Dateisystem |
| | | IOPS Schreiben | Implementiert | SSH | IOPS Schreiben des Dateisystems |
| | | Lesedurchsatz Des Dateidurchsatzes | Implementiert | SSH | |
| | | Durchsatz des Dateisystems | Implementiert | SSH | Dateisystem-Durchsatz schreiben |
| | | IOPS Lesen | Implementiert | SSH | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | SSH | |
| | | IOPS Schreiben | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Latenz Insgesamt | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | | Durchsatz Beim Lesen | Implementiert | SSH | |
| | | Gesamtdurchsatz | Implementiert | SSH | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SSH | |
| | | Auslastung Insgesamt | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Isilon SSH | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

## EMC PowerStore REST

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| PowerStore 1000T PowerStore 5000T PowerStore 5200T | 2.1.1.1 3.2.1.0 3.5.0.2 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 520 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | | |
| | | Einheitliche | Implementiert | | Handelt es sich um ein Gerät zur |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen? |
|---|---|---|---|---|---|
| | Datenmenge | Kapazität | Implementiert | | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | | |
| | | Name | Implementiert | | |
| | | Gesamtbruttokapazität | Implementiert | | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Speicherpool-Id | Implementiert | | |
| | | Thin Provisioning | Implementiert | | |
| | | Typ | Lücke | | |
| | | UUID | Implementiert | | |
| | | Genutzte Kapazität | Implementiert | | |
| | | QoS: Richtlinie | Implementiert | | |
| | Volume-Zuordnung | LUN | Implementiert | | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Typ | Lücke | | |
| | WWN-Alias | Host-Aliase | Implementiert | | |
| | | Objekttyp | Implementiert | | |
| | | Quelle | Implementiert | | |
| | | WWN | Implementiert | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | IOPS Sonstiges | Implementiert | | |
| | | IOPS Lesen | Implementiert | | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | | |
| | | IOPS Schreiben | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Latenzleseszeit | Implementiert | | |
| | | Latenz Insgesamt | Implementiert | | |
| | | Latenz – Schreiben | Implementiert | | |
| | | Server-ID | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC POWERSTORE REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## EMC RecoverPoint (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| RecoverPoint | 5.1.SP3.P1(g. 69) 5.1.SP4.HF1(h.83)<br>5.1.SP4.P1(h.89) |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen?** |
| | Storage-Node | Speichergröße | Lücke | HTTPS | Gerätespeicher in MB |
| | | Modell | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Prozessoranzahl | Implementiert | HTTPS | Geräte-CPU |
| | | Seriennummer | Implementiert | HTTPS | |
| | | Status | Implementiert | HTTPS | Kostenloser Text, der den Gerätestatus beschreibt |
| | | UUID | Implementiert | HTTPS | |
| | | Version | Implementiert | HTTPS | Softwareversion |
| | Storage-Synchronisierung | Modus | Implementiert | HTTPS | |
| | | Modus Enum | Implementiert | HTTPS | |
| | | Quell-Storage | Implementiert | HTTPS | |
| | | Quell-Volume | Implementiert | HTTPS | |
| | | Status | Implementiert | HTTPS | Kostenloser Text, der den Gerätestatus beschreibt |
| | | Staatsummen | Implementiert | HTTPS | |
| | | Ziel-Storage | Implementiert | HTTPS | |
| | | Ziel-Volume | Implementiert | HTTPS | |
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verändert |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| RecoverPoint-REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## EMC Symmetrix CLI

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| V10.0.0.0 V10.0.0.3 V10.0.1.0 V10.0.1.3 V10.1.0.0 V10.1.0.3 V8.3.0.6 V9.1.0.15 V9.2.0.0 V9.2.3.0 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.6 | PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F | 5876.286.194 6 5978.714.714 (16F40000) Build 115 5978.479.479 34 5978.714.714 61 5978.714.714 (175A0000) Build 372 5978.711.711 85 (175A0000) Build 179 5978.711.711 (175A0000) Build 205 5978.711.711 (175A0000) Build 49 5978.714.714 (175A0000) Build 365 5978.711.711 (175A0000) Build 374 5978.711.711 (175A0000) Build 448 5978.711.711 (175A0000) Build 484 5978.711.711 (1750000) Build 539 5978.711.711 (1750000) Build 239 5978.711.711 A00517500 542 5978.714.714) A0000 5978.714.714) A17500 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |
| | Volumenmitglied | Automatisiertes Tiering | Implementiert | | Gibt an, ob dieser storagepool an Auto-Tiering mit anderen Pools beteiligt ist |
| | | Kapazität | Implementiert | | Verwendete Kapazität des Snapshot in MB |
| | | Zylinder | Implementiert | | |
| | | Name | Implementiert | | |
| | | Rang | Implementiert | | |
| | | Gesamtbruttokapazität | Implementiert | | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | | Redundanzebene |
| | | Speicherpool-Id | Implementiert | | |
| | | UUID | Implementiert | | |
| | WWN-Alias | Host-Aliase | Implementiert | | |
| | | Objekttyp | Implementiert | | |
| | | Quelle | Implementiert | | |
| | | WWN | Implementiert | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | auf allen Festplatten) in MB/s |
| **Produkt** | **Kategorie** | **Funktionsname/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Schreiben | Implementiert | | |
| | | „Ausstehend“ | Implementiert | | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| symcli | CLI | | 2707 | | Richtig | Richtig | Richtig | Richtig |
| Symmetrix SMI-S | SMI-S | HTTP/HTTPS | 5988/5989 | | Richtig | Falsch | Falsch | Richtig |

## Dell Unisphere-REST

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| V10.0.1.3 V10.1.0.1 V10.1.0.5 V10.1.0.6 V9.2.4.7 V9.2.4.9 | PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F | 5978.714.714 5978.714.714 Build 6 5978.714.714 Build 61 5978.714.714 Build 85 6079.225.0 Build 127 6079.225.0 Build 216 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | um ein Gerät zur Storage-Virtualisierung? |
|---|---|---|---|---|---|
| **Produkt** | **Kategorie** | **Funktion/Attribut-Gruppen** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Schreiben | | | |
| | | Server-ID | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktionsattribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Durchsatz lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | „Ausstehend“ | Implementiert | HTTPS | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Dell Unisphere-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## EMC VNX (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| VNX5300 VNX5400 VNX5800 VNX7500 | 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 550 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | SSH | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | SSH | |
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | IP | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | Storage Pools: Kapazität | Implementiert | SSH | |
|---|---|---|---|---|---|
| | | Taste | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | SSH | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | SSH | |
| | | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | SSH | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Sonstige Gesamtkapazität | Implementiert | SSH | |
| | | Andere Genutzte Kapazität | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VNX SSH UND CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

## EMC VNXe und Unity Unisphere (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 650F Unity 680 Unity 680F Unity 880 Unity 880F VNXe3200 | 3.1.17.10223906 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.7.0.5.008 5.1.0.0.5.394 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.4.0.0.5.094 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Ziel-Volume | Implementiert | HTTPS | |
|---|---|---|---|---|---|
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verwendet |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Festplatte | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VNXe und Unisphere CLI | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## EMC VPLEX

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| VPLEX | 6.1.0.00.00.23 6.1.0.01.00.13 6.1.0.02.00.04 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTP/S | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTP/S | Verwendete Kapazität des Snapshot in MB |
| | | Name | Implementiert | HTTP/S | |
| | | Gesamtbruttokapazität | Implementiert | HTTP/S | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTP/S | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTP/S | |
| | | Thin Provisioning | Implementiert | HTTP/S | |
| | | UUID | Implementiert | HTTP/S | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTP/S | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | IOPS insgesamt | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Latenzleseszeit | Implementiert | SSH | |
| | | Latenz Insgesamt | Implementiert | SSH | |
| | | Latenz – Schreiben | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | | Durchsatz Beim Lesen | Implementiert | SSH | |
| | | Gesamtdurchsatz | Implementiert | SSH | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC VPLEX-CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |
| EMC VPLEX-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

## EMC XtremIO (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
| --- | --- | --- |
| 4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0 | 1 Bricks und 48 TB 1 x 20 TB 2 Bricks und 251 TB 2 x 20 TB 3 Bricks und 283 TB 4 Bricks und 503 TB 4 x 10 TB 6 x 20 TB 8 x 20 TB | 4.0.25-27 4.0.31-11 6.1.0-99_X2 6.2.1-36_X2 6.3.3-8_X2 6.4.0-36_HOTFIX_2_X2 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Ziel-Volume | Implementiert | HTTPS | |
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verwendet |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Festplattengröße | Implementiert | HTTPS | Kommagetrennte Liste der Festplattengrößen (GB) |
| | | Festplattengeschwindigkeit | Implementiert | HTTPS | Kommagetrennte Liste von Festplattengeschwindigkeiten (rpm) |
| | | Festplattentyp | Nicht Verfügbar | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Server-ID | Implementiert | HTTPS | |
| | Storage-Node-Daten | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Bruttokapazität | Implementiert | HTTPS | |
| | | Gesamtkapazität | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC XTREMIO REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## NetApp E-Series

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 2650 2660 2704 2806 5600 5700 | 8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | RMI | |
| | | Einheitliche | Implementiert | RMI | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | RMI | Verwendete Kapazität des Snapshot in MB |
| | | Festplattentyp | Nicht Verfügbar | RMI | |
| | | Name | Implementiert | RMI | |
| | | Gesamtbruttokapazität | Implementiert | RMI | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | RMI | Redundanzebene |
| | | Speicherpool-Id | Implementiert | RMI | |
| | | Thin Provisioning | Implementiert | RMI | |
| | | Typ | Lücke | RMI | |
| | | UUID | Implementiert | RMI | |
| | | Genutzte Kapazität | Implementiert | RMI | |
| | | Einheitliche | Implementiert | RMI | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | | Geschriebene Kapazität | Implementiert | RMI | Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde |
| | Volume-Zuordnung | LUN | Implementiert | RMI | Der Name der Backend-lun |
| | Volume-Maske | Initiator | Implementiert | RMI | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Gesamtkapazität | | | |
|---|---|---|---|---|---|
| | | Andere Genutzte Kapazität | Implementiert | RMI | |
| | | Server-ID | Implementiert | RMI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Cache-Trefferverhältnis Lesen | Implementiert | RMI | |
| | | Cache-Trefferverhältnis Insgesamt | Implementiert | RMI | |
| | | Cache-Trefferverhältnis Schreiben | Implementiert | RMI | |
| | | Bruttokapazität | Implementiert | RMI | |
| | | Gesamtkapazität | Implementiert | RMI | |
| | | Genutzte Kapazität | Implementiert | RMI | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | RMI | |
| | | IOPS Lesen | Implementiert | RMI | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | RMI | |
| | | IOPS Schreiben | Implementiert | RMI | |
| | | Taste | Implementiert | RMI | |
| | | Latenzleseszeit | Implementiert | RMI | |
| | | Latenz Insgesamt | Implementiert | RMI | |
| | | Latenz – Schreiben | Implementiert | RMI | |
| | | Server-ID | Implementiert | RMI | |
| | | Durchsatz Beim Lesen | Implementiert | RMI | |
| | | Gesamtdurchsatz | Implementiert | RMI | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | RMI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| SANtricity API | RMI | TCP | | | Richtig | Richtig | Falsch | Falsch |

## HDS HCP (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Hitachi Content Platform | 9.6.2.37 9.6.3.33 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 600 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| **Produkt** | **Kategorie** | **Funktion/Attribut Typ** | **Status Lücke** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | Storage-Node-Daten | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Durchsatz Beim Lesen | Implementiert | | |
| | | Gesamtdurchsatz | Implementiert | | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | | |
| | | Auslastung Insgesamt | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HDS HCP REST API | HTTPS | HTTPS | 9090 | | Richtig | Richtig | Richtig | Richtig |

## HiCommand Device Manager

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 8.6.4 8.7.7 8.8.1 8.8.3 8.8.5 | D850XS HM700 HM800M R800 | 0988/J-W DKC:73-03-83-52 DKC:00/00-05-05-83 DKC:06-68/00-80-03 DKC:40/00-73-50-83 SVP:05-40/00-87/00 SVP:48-83-92 SVP:40/00-06-00/00-80 SVP:69-05-54-40/00 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Speicherpool-Id | Implementiert | HDS-XML-API | |
| | | Thin Provisioning | Implementiert | HDS-XML-API | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HDS-XML-API | |
| | | Genutzte Kapazität | Implementiert | HDS-XML-API | |
| | Volume-Zuordnung | LUN | Implementiert | HDS-XML-API | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HDS-XML-API | |
| | | Protokoll-Controller | Implementiert | HDS-XML-API | |
| | | Storage-Port | Implementiert | HDS-XML-API | |
| | Volume-Maske | Initiator | Implementiert | HDS-XML-API | |
| | | Protokoll-Controller | Implementiert | HDS-XML-API | |
| | | Storage-Port | Implementiert | HDS-XML-API | |
| | Volumenmitglied | Name | Implementiert | HDS-XML-API | |
| | | Speicherpool-Id | Implementiert | HDS-XML-API | |
| | | Rang | Implementiert | HDS-XML-API | |
| | | Zylinder | Implementiert | HDS-XML-API | |
| | | Kapazität | Implementiert | HDS-XML-API | Verwendete Kapazität des Snapshot in MB |
| | | Gesamtbruttokapazität | Implementiert | HDS-XML-API | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Genutzte Kapazität | Implementiert | HDS-XML-API | |
| | WWN-Alias | Host-Aliase | Implementiert | HDS-XML-API | |
| | | Objekttyp | Implementiert | HDS-XML-API | |
| | | Quelle | Implementiert | HDS-XML-API | |
| | | WWN | Implementiert | HDS-XML-API | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Festplatte | IOPS Lesen | Implementiert | Export/CLI | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | Export/CLI | |
| | | IOPS Schreiben | Implementiert | Export/CLI | |
| | | Taste | Implementiert | Export/CLI | |
| | | Server-ID | Implementiert | Export/CLI | |
| | | Durchsatz Beim Lesen | Implementiert | Export/CLI | |
| | | Gesamtdurchsatz | Implementiert | Export/CLI | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | Export/CLI | |
| | | Auslastung Insgesamt | Implementiert | Export/CLI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Exportdienstprogramm (USPV) / SNM CLI (AMS) | Export/CLI | | | | Falsch | Falsch | Falsch | Falsch |
| HiCommand Device Manager-XML-API | HDS-XML-API | HTTP/HTTPS | 2001 | | Richtig | Richtig | Richtig | Richtig |

## HDS HNAS (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| G600 HNAS 4100 | 14.6.7520,04 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HDS HNAS CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |

## HPE Nimble/Alletra 6000 Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| v1 | AF40 AF80 HF60 | 5.0.3.100-575430-OPT 5.2.1.600-841103-OPT |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | HTTPS | |
| | | Bruttokapazität | Implementiert | HTTPS | |
| | | Freie Rohkapazität | Implementiert | HTTPS | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | HTTPS | |
| | | IOPS Sonstiges | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HP NIMBLE REST API | HTTPS | HTTPS | 5392 | | Richtig | Falsch | Richtig | Richtig |

## Huawei OceanStor (REST/HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 5500 V3 6800 V3 | V300R006C50 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Huawei OceanStor REST-API | HTTPS | HTTPS | 8088 | | Richtig | Richtig | Richtig | Richtig |
| Huawei OceanStor Performance REST API | HTTPS | HTTPS | 8088 | | Richtig | Falsch | Richtig | Richtig |

## IBM SVC (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 2076-112 2076-124 2076-12F 2076-212 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2077-24F 2077-324 4657-924 4662-6H2 9840-AE1 9843-AE2 9843-AE3 SVC | 1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13 7.8.1.5 7.8.1.7 7.8.1.8 8.1.3.5 8.1.3.6 8.2.1.11 8.2.1.8 8.3.1.2 8.3.1.5 8.4.0.10 8.4.0.11 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.9 8.5.3.1 8.6.0.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Kapazität | | | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen?** |
| | | Geschriebene Kapazität | Implementiert | SSH | Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde |
| | | Komprimierung Aktiviert | Implementiert | SSH | |
| | | Verschlüsselt | Implementiert | SSH | |
| | Volume-Zuordnung | LUN | Implementiert | SSH | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt | Implementiert | SSH | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | SSH | |
| | | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | SSH | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Geschriebene Kapazität | Implementiert | SSH | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | KapazitätRatio geschrieben | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| IBM SVC-CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

## Infiniat Infinibox (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| F4304 F4304T F6260 F6306 | 7.1.14.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | HTTPS | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Infinidat REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## Microsoft Hyper-V

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Bereitgestellte Kapazität | Implementiert | WMI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Bereitgestellte Kapazität | Implementiert | WMI | |
| | VirtualMachine Disk | OID | Implementiert | WMI | |
| | | VirtualisierungsDisk OID | Implementiert | WMI | |
| | | OID der Virtual Machine | Implementiert | WMI | |
| | Host | Host-Cpu-Anzahl | Implementiert | WMI | |
| | | Host-Cpu-Geschwindigkeit | Implementiert | WMI | |
| | | Host Domain | Implementiert | WMI | |
| | | Host-Installierter Speicher | Implementiert | WMI | |
| | | Host-Modell | Implementiert | WMI | |
| | | Anzahl der NIC | Implementiert | WMI | |
| | | NIC-Geschwindigkeit | Implementiert | WMI | |
| | | IPS | Implementiert | WMI | |
| | | Hersteller | Implementiert | WMI | |
| | | Name | Implementiert | WMI | |
| | | OID | Implementiert | WMI | |
| | | Plattformtyp | Implementiert | WMI | |
| | Info | Name der Datenquelle | Implementiert | WMI | Info |
| | | Datum | Implementiert | WMI | |
| | | Ersteller-ID | Implementiert | WMI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| PowerShell | WS-Verwaltung | HTTP | 5985 | | Richtig | Falsch | Falsch | Richtig |
| WMI | WMI | WMI | 135 | | Richtig | Falsch | Richtig | Richtig |

## NetApp 7-Modus

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 1.12 1.17 1.19 1.20 1.21 | FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS3250 FAS3270 FAS6240 FAS8040 FAS8060 N6070 | 8.1.1 7-Mode 8.1.4P6 7-Mode 8.2.3P2 7-Mode 7.3P3 7-Mode 8.2.3P6 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.5P3 8.2-Mode 8.2.5P5 7-Mode 8.2P4 7-Mode Data ONTAP Version 7.3.3 Data ONTAP Version 7.3.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 660 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
| --- | --- | --- | --- | --- | --- |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Zuordnung | | | | Backend-lun |
| | | Protokoll-Controller | Implementiert | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | | | |
| | | Bruttokapazität | Implementiert | | | |
| | | Gesamtkapazität | Implementiert | | | |
| | | Genutzte Kapazität | Implementiert | | | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | | Als Zeitreihe gemeldet | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | | | |
| | | Gesamtkapazität Daten | Implementiert | | | |
| | | Genutzte Kapazität Von Daten | Implementiert | | | |
| | | Taste | Implementiert | | | |
| | | Server-ID | Implementiert | | | |
| | | Reservierte Snapshot-Kapazität | Implementiert | | | |
| | | Verwendete Snapshot-Kapazität | Implementiert | | | |
| | | Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie | Implementiert | | Als Zeitreihe gemeldet | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| NetApp 7 Modus ZAPI | ZAPI | ZAPI | | | Richtig | Richtig | Richtig | Richtig |

## NetApp Clustered Data ONTAP 8.1 und höher

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| AFF-A150 AFF-A200 AFF-A220 AFF-A250 AFF-A300 AFF-A400 AFF-A700 AFF-A700s AFF-A800 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF8040 AFF8080 CDvM200 DM5100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3250 FAS500f FAS6220 FAS8020 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 DvM300 | 8.2.P13.P5 8.2 9.12.1.4P3 8.3 9.14.1.1P2 9.1.2P12 8.3.2P5 8.3.2P8 9.1.0 9.1.0P15 9.1.0P19 9.1.0P2 8.3.2 8.3.0P20 9.10.1P11 9.10.1P12 9.10.1P13 9.10.1P13 9.10.1P13 9.10.1P14 9.10.1P14 9.10.1P14 9.15.1 9.3 9.3 9.3 9.4 9.4 9.5.0 9.5 9.5 9.5 9.7 9.7 9.7 9.7 9.7 9.7 9.7 9.7 9.7 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.9 9.9 9.9 9.9 9.9 9.9 9.9 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Virtualisierung? |
| | | Verschlüsselt | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | IOPS | Implementiert | HTTPS | |
| | | QoS begrenzt MB/S | Implementiert | HTTPS | |
| | | Qos-Limit: Raw | Implementiert | HTTPS | |
| | | QoS: Richtlinie | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Leseauslastung | Implementiert | HTTPS | |
| | | Auslastung Insgesamt | Implementiert | HTTPS | |
| | | Auslastung Schreiben | Implementiert | HTTPS | |
| | Datenmenge | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| NetApp ONTAP-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

## NetApp SolidFire 8.1 oder höher

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCN001 H410S-0 H610S-1 SF19210 SF2405 SF38410 SF4805 | 11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | IOPS | | | |
| | | qos-Minimum für IOPS | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | QoS: Richtlinie | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Gesamtkapazität | | | |
| | | Andere Genutzte Kapazität | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | HTTPS | |
| | Datenmenge | Bruttokapazität | Implementiert | HTTPS | |
| | | Gesamtkapazität | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | HTTPS | |
| | | Gesamteinsparungen Durch Komprimierung | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | Auslastung Insgesamt | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| SolidFire REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## NetApp StorageGRID (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Webscale | 11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3.1 3.4 3.5 4.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | tung des Knotens verwendete Metadaten in MB | | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Standortname | Implementiert | HTTPS | |
| | Storage-Pool | In Dwh-Kapazität Einbeziehen | Implementiert | HTTPS | Ein Weg von ACQ zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind |
| | | Name | Implementiert | HTTPS | |
| | | Kapazität der physischen Festplatte (MB) | Implementiert | HTTPS | Wird als Rohkapazität für den Storage-Pool verwendet |
| | | Raid-Gruppe | Implementiert | HTTPS | Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt |
| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | HTTPS | Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | HTTPS | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | HTTPS | |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | auf allen Festplatten) in MB/s |
| **Produkt** | **Kategorie** | **Funktion/Attribut schreiben** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Gesamtkapazität | Implementiert | | |
| | | Genutzte Kapazität | Implementiert | | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| StorageGRID REST API | HTTPS | HTTPS | 443 | | Richtig | Falsch | Richtig | Richtig |

## Nutanix Storage (REST)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| HX3310 NX-8150-G5 HX3310 HX321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10 CORE XC740XD-12 XC740XD-12 CORE | 5.20.2.1 5.20.4.6 6.5.4 6.5.5 6.5.5.6 6.5.5.7 6.5.6.5 6.7.1.7 6.8 6.8.1 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Zugehöriges Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Qtree-Id | Implementiert | HTTPS | Eindeutige id des qtree |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Storage-Port | Implementiert | HTTPS | |
| | | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | HTTPS | |
| | | Bruttokapazität | Implementiert | HTTPS | |
| | | Freie Rohkapazität | Implementiert | HTTPS | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | HTTPS | |
| | | IOPS Sonstiges | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Nutanix REST API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

## Oracle ZFS (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430 | 1-1.1 2013.06.05.7.28 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Kapazität | | | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen?** |
| | Volume-Zuordnung | LUN | Implementiert | HTTP/S | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| Performance | Storage-Node-Daten | Cache-Trefferverhältnis Insgesamt | Implementiert | | |
| | | IOPS insgesamt | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Auslastung Insgesamt | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| ORACLE ZFS REST API | HTTP/HTTPS | HTTP/HTTPS | 215 | | Richtig | Richtig | Richtig | Richtig |

## Pure Storage FlashArray (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| DFSC1 FA-X20R3 FA-X50R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 | 6.1.21 6.3.1 6.3.10 6.3.9 6.5.1 6.5.2 6.5.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | HTTP/S | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | HTTP/S | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTP/S | |
| | | Objekttyp | Implementiert | HTTP/S | |
| | | Quelle | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | IOPS Sonstiges | Implementiert | | |
| | | IOPS Lesen | Implementiert | | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | | |
| | | IOPS Schreiben | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Latenzleseszeit | Implementiert | | |
| | | Latenz Insgesamt | Implementiert | | |
| | | Latenz – Schreiben | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Durchsatz Beim Lesen | Implementiert | | |
| | | Gesamtdurchsatz | Implementiert | | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Pure Storage REST-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

## VMware vSphere (Web Services)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- VMware vCenter Server 5.5.0 Build-1750787
- VMware vCenter Server 5.5.0 Build-3252642
- VMware vCenter Server 5.5.0 Build-4180647
- VMware vCenter Server 5.5.0 Build-9911218
- VMware vCenter Server 6.0.0 Build-13638472
- VMware vCenter Server 6.0.0 Build-14510545
- VMware vCenter Server 6.0.0 Build-4541947
- VMware vCenter Server 6.0.0 Build-5318200
- VMware vCenter Server 6.0.0 Build-9313458
- VMware vCenter Server 6.5.0 Build-10964411
- VMware vCenter Server 6.5.0 Build-17994927
- VMware vCenter Server 6.5.0 Build-18499837
- VMware vCenter Server 6.5.0 Build-18711281
- VMware vCenter Server 6.5.0 Build-19757181
- VMware vCenter Server 6.5.0 Build-22499743
- VMware vCenter Server 6.5.0 Build-7515524
- VMware vCenter Server 6.5.0 Build-9451637
- VMware vCenter Server 6.7.0 Build-16046713
- VMware vCenter Server 6.7.0 Build-18485185
- VMware vCenter Server 6.7.0 Build-19299595
- VMware vCenter Server 6.7.0 Build-19832280
- VMware vCenter Server 6.7.0 Build-20504362
- VMware vCenter Server 6.7.0 Build-22509732
- VMware vCenter Server 6.7.0 Build-22509751
- VMware vCenter Server 7.0.1 Build-17491160

- VMware vCenter Server 7.0.3 Build-19234570
- VMware vCenter Server 7.0.3 Build-19717403
- VMware vCenter Server 7.0.3 Build-20051473
- VMware vCenter Server 7.0.3 Build-20150588
- VMware vCenter Server 7.0.3 Build-20395099
- VMware vCenter Server 7.0.3 Build-20845200
- VMware vCenter Server 7.0.3 Build-20990077
- VMware vCenter Server 7.0.3 Build-21290409
- VMware vCenter Server 7.0.3 Build-21477706
- VMware vCenter Server 7.0.3 Build-21784236
- VMware vCenter Server 7.0.3 Build-22357613
- VMware vCenter Server 7.0.3 Build-22837322
- VMware vCenter Server 7.0.3 Build-23788036
- VMware vCenter Server 7.0.3 Build-24026615
- VMware vCenter Server 8.0.1 Build-22368047
- VMware vCenter Server 8.0.1 Build-22742005
- VMware vCenter Server 8.0.1 Build-23525738
- VMware vCenter Server 8.0.1 Build-24005165
- VMware vCenter Server 8.0.2 Build-22385739
- VMware vCenter Server 8.0.2 Build-22617221
- VMware vCenter Server 8.0.2 Build-23319993
- VMware vCenter Server 8.0.2 Build-23504390
- VMware vCenter Server 8.0.2 Build-23929136
- VMware vCenter Server 8.0.3 Build-24022515
- VMware vCenter Server 8.0.3 Build-24091160

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Bereitgestellte Kapazität | Implementiert | Web-Services | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | VirtualMachine Disk | OID | Implementiert | Web-Services | |
| | | VirtualisierungsDisk OID | Implementiert | Web-Services | |
| | | OID der Virtual Machine | Implementiert | Web-Services | |
| | Host | Host-Cpu-Anzahl | Implementiert | Web-Services | |
| | | Host-Cpu-Geschwindigkeit | Implementiert | Web-Services | |
| | | Host Domain | Implementiert | Web-Services | |
| | | Host-Installierter Speicher | Implementiert | Web-Services | |
| | | Host-Modell | Implementiert | Web-Services | |
| | | Anzahl der NIC | Implementiert | Web-Services | |
| | | NIC-Geschwindigkeit | Implementiert | Web-Services | |
| | | IPS | Implementiert | Web-Services | |
| | | Hersteller | Implementiert | Web-Services | |
| | | Name | Implementiert | Web-Services | |
| | | OID | Implementiert | Web-Services | |
| | | Plattformtyp | Implementiert | Web-Services | |
| | ISCSI-Knoten | Host-Aliase | Implementiert | Web-Services | |
| | | Node-Name | Implementiert | Web-Services | |
| | | OID | Implementiert | Web-Services | |
| | | Typ | Lücke | Web-Services | |
| | Info | Api-Beschreibung | Implementiert | Web-Services | |
| | | Api-Name | Implementiert | Web-Services | |
| | | Api-Version | Implementiert | Web-Services | |
| | | Client-Api-Name | Implementiert | Web-Services | |
| | | Client-Api-Version | Implementiert | Web-Services | |
| | | Name der Datenquelle | Implementiert | Web-Services | Info |
| | | Datum | Implementiert | Web-Services | |
| | | Ersteller-ID | Implementiert | Web-Services | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VMware REST-API | Web-Services | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# Data Warehouse-Administration

## Willkommen im OnCommand Insight Data Warehouse

Das OnCommand Insight Data Warehouse ist ein zentralisiertes Repository, das Daten von mehreren OnCommand Insight Servern speichert und Daten zu einem gemeinsamen, mehrdimensionalen Datenmodell für Abfrage und Analyse umwandelt.

Das OnCommand Insight Data Warehouse ermöglicht den Zugriff auf eine offene Datenbank mit mehreren Datentabellen, mit denen Sie benutzerdefinierte Kapazitäts- und Performance-Berichte generieren können, beispielsweise Chargeback-Berichte, Trendberichte mit Archivdaten, Verbrauchsanalysen und Prognoseberichte.

### Data Warehouse-Funktionen

Das OnCommand Insight Data Warehouse ist eine unabhängige Datenbank, die aus mehreren Data Marts besteht.

Data Warehouse umfasst folgende Funktionen:

- Aktuelle und historische Konfigurations- und Bestandsdaten, mit denen Sie Trendberichte erstellen können, die für Prognosen und Planungen nützlich sind
- Mehrere mehrdimensionale historische Datentabellen und ein zusätzlicher aktueller Bestandsdatenbestand
- Eine optimierte Datenbank für vordefinierte Abfragen oder benutzerdefinierte Abfragen
- Eine Plattform für die Integration in Reporting- und Business Intelligence-Engines von Drittanbietern, einschließlich:
  - Konfigurationsmanagement-Datenbanken
  - Finanzbuchhaltungssysteme
  - Asset Management-Systeme

### Data Warehouse-Komponenten

Data Warehouse enthält mehrere Komponenten.

- Data Warehouse-Portal
- OnCommand Insight-Berichtsportal
- Tools zur Berichterstellung

#### Was Sie mit dem Data Warehouse Portal tun können

Das Data Warehouse Portal ist eine webbasierte Benutzeroberfläche, mit der Sie Optionen konfigurieren und feste Zeitpläne zum Abrufen von Daten einrichten können. Über das Data Warehouse-Portal können Sie auch auf das OnCommand Insight-Berichtsportal zugreifen.

Mit dem Data Warehouse-Portal können Sie Folgendes tun:

- Über das OnCommand Insight Reporting-Portal können Sie vordefinierte Berichte anzeigen oder mithilfe von Tools zur Berichterstellung individuelle Berichte erstellen.
- Konsolidierung mehrerer OnCommand Insight-Datenbanken.
- Managen von Verbindungen zu OnCommand Insight-Servern
- Überprüfen Sie den Status aktueller Jobs oder Abfragen, die ausgeführt werden.
- Planung von Data Warehouse-Builds
- Bearbeiten Sie den Standortnamen.
- Anzeigen der Data Warehouse-Version und des Upgrade-Verlaufs, einschließlich spezifischer Informationen wie Modulversionen, Standorte und Lizenzen.
- Anmerkungen importieren.
- Konfigurieren eines Builds anhand des Verlaufs.
- Zeigen Sie die Data Warehouse-Dokumentation und das Datenbankschema an.
- Die Data Warehouse-Datenbank zurücksetzen.
- Sichern Sie die Data Warehouse-Datenbank und stellen Sie sie wieder her.
- Fehlerbehebung bei Problemen mit Data Warehouse.
- Verwalten von Benutzerkonten

#### Softwarekomponenten von Data Warehouse

Das OnCommand Insight Data Warehouse umfasst mehrere Softwarekomponenten.

- MySQL Datenbank

  Das Back-End-Repository für Datentabellen

- IBM Cognos

  Die Reporting Engine für OnCommand Insight

- Apache Derby Database

  Wird zum Speichern von Cognos-Konfiguration und -Inhalt verwendet

- WildFly

  Der Java Enterprise-Anwendungsserver, der OnCommand Insight-Komponenten hostet

## Data Warehouse-Prozesse

Data Warehouse führt viele Prozessarten durch.

- **ETL-Prozess**

  Der ETL-Prozess (Extract Transform and Load) ruft Daten aus mehreren OnCommand Insight-Datenbanken ab, transformiert die Daten und speichert sie in Data Mart. Der Build-Prozess für Data Warehouse ist ein ETL-Prozess.

- **Jobs**

Data Warehouse führt Jobs wie die folgenden aus und erstellt Berichte dazu: Inventar, Dimensionen, Kapazität, Port-Kapazität, VM-Kapazität Auslastung des Filesystems, Performance, Kapazitätseffizienz, Lizenzen, Verlaufsdaten, Dynamische Anmerkungen, Entfernen von Konnektoren, übersprungene Erstellung, ASUP Option und Wartungsaufträge.

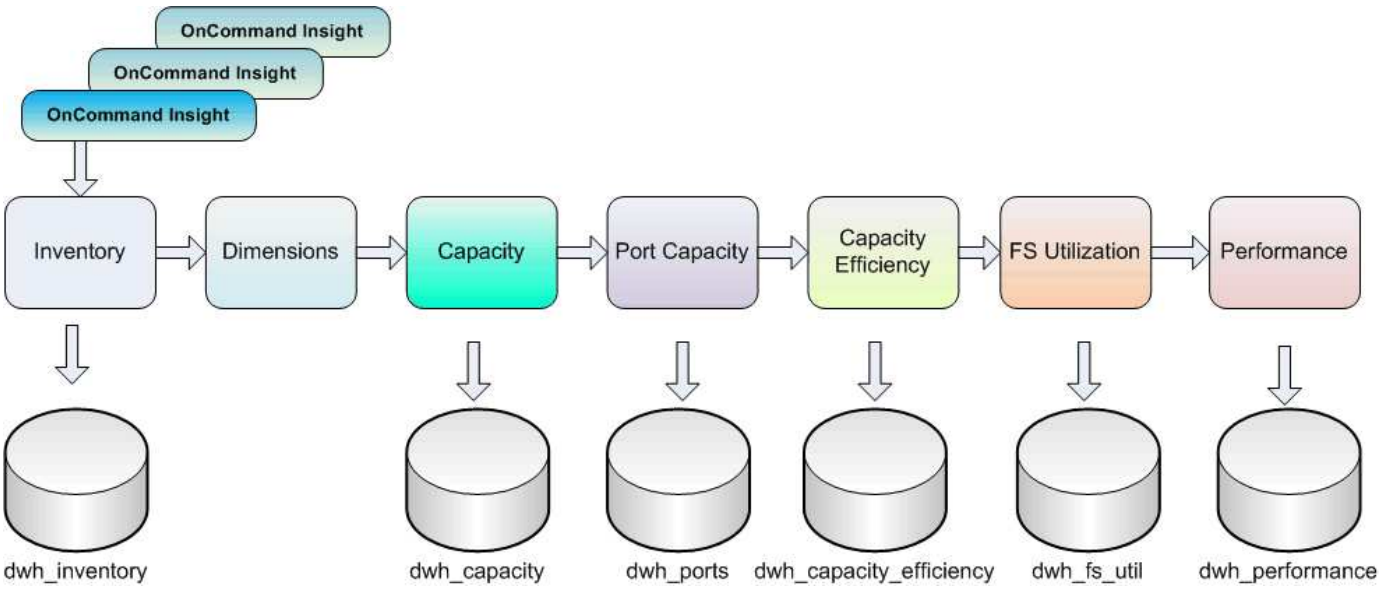
- **Konsolidierungsprozess**

  Data Warehouse unterstützt die Konsolidierung mehrerer OnCommand Insight-Server in derselben Data Warehouse-Datenbank. In vielen Konfigurationen kann es vorkommen, dass dasselbe Objekt von mehreren Konnektoren gemeldet wird (d. h., derselbe Switch existiert in zwei OnCommand Insight-Instanzen). In diesem Fall konsolidiert Data Warehouse mehrere Objekte zu einem (ein primärer Konnektor wird ausgewählt und die Daten des Objekts werden nur von diesem Konnektor übernommen).

## Wie Data Warehouse Daten extrahiert

Der ETL-Prozess (Extrahieren, Transformieren und Laden) ruft Daten aus mehreren OnCommand Insight-Datenbanken ab, wandelt die Daten um und speichert sie in Data Marts.

OnCommand Insight Connectors rufen eine Reihe von Batch-Jobs auf, um Daten aus mehreren OnCommand Insight MySQL-Datenbanken zu extrahieren und die Daten in verschiedenen Data Marts zu veröffentlichen, wie im folgenden Diagramm dargestellt.




Der ETL-Prozess umfasst folgende Einzelprozesse:

- **Auszug**

  Dieser Prozess nimmt Daten aus mehreren OnCommand Insight-Datenbanken, wandelt die Daten um und speichert sie in den Data Mart. Dieser Prozess wird für jede OnCommand Insight Instanz gleichzeitig durchgeführt. Um sicherzustellen, dass die Datenbereinigung und -Deduplizierung durchgeführt wird, ist es nicht möglich, den ETL-Prozess in mehrere geplante ETL-Vorgänge zu teilen.

- * Transform*

  Dieser Prozess wendet Regeln oder Funktionen der Geschäftslogik an, um die Daten aus der OnCommand Insight-Datenbank zu extrahieren.

- **Laden**

  Bei diesem Prozess werden die transformierten Daten in öffentliche Data Marts geladen.

## ETL-Frequenz- und Datumsdaten

Sie sollten den ETL-Prozess (Extrahieren, Transformieren und Laden) mindestens einmal pro Tag ausführen. Sie können ETL jedoch bei Bedarf mehrmals ausführen.

Standardmäßig behandelt die Cognos Reporting Engine alle Kapazitäts- und Leistungsdaten als additiv. Dadurch besteht die Gefahr, dass Kapazitätsdaten doppelt gezählt werden, wenn der ETL-Prozess mehrmals täglich ohne die richtigen Zeitfilter ausgeführt wird.

Zwei Datumsdatenelemente in der Datumsdimension stehen im Zusammenhang mit dem täglichen ETL-Prozess. Die Datumsdimension, die in mehreren Datenmodellen verwendet wird, umfasst die folgenden Datenelemente, die von der ETL betroffen sind:

- **Ist Tagesvertreter**

  Das Datenelement „is Day Representative“ wird während der ersten Ausführung des ETL-Prozesses an einem beliebigen Tag auf den Wert 1 (TRUE) gesetzt. Wenn der erste ETL-Prozess um 1:00 Uhr ausgeführt wird, ist der Tagesvertreter für alle während der 1:00 Uhr geladenen Daten auf 1 eingestellt ETL-Prozess. Wenn eine zweite ETL später geplant wird (z. B. um 1:00 Uhr), wird für die während dieses ETL-Prozesses geladenen Daten der Wert 0 (FALSE) als Tagesvertreter festgelegt.

- **Ist Neuestes**

  Das „is Latest“-Mitglied wird nach Abschluss jedes ETL-Prozesses auf den Wert 1 (TRUE) gesetzt. Wenn der erste ETL-Prozess um 1:00 Uhr morgens ausgeführt wird, ist „Letzte“ für alle Daten, die während der 1:00 Uhr morgens geladen wurden, auf „1“ gesetzt ETL-Prozess. Wenn ein anderer ETL-Prozess später geplant wird (z. B. 1:00 Uhr), wird für Daten, die während der 13 Uhr geladen werden, die Einstellung „Letzte“ auf „1“ gesetzt ETL-Prozess. Der ETL-Prozess setzt auch die 1:00 Uhr morgens ETL-Lasten sind der letzte Eintrag auf 0 (FALSE).

## Wie historische Daten im Data Warehouse aufbewahrt werden

Die Daten werden im Data Warehouse gemäß einem Zeitplan verwaltet. Mit zunehmendem Alter der Daten wird die Aufbewahrung von Datensätzen reduziert.

Data Warehouse speichert historische Daten basierend auf den Daten und Granularität der Daten, wie in der folgenden Tabelle dargestellt.

| Datentabellen | Gemessenes Objekt | Granularität | Aufbewahrungszeitraum |
|---|---|---|---|
| Performance Marts | Volumes und interne Volumes | Stündlich | 14 Tage |
| Performance Marts | Volumes und interne Volumes | Täglich | 13 Monaten |
| Performance Marts | Applikation | Stündlich | 13 Monaten |

| | | | |
|---|---|---|---|
| Performance Marts | Host | Stündlich | 13 Monaten |
| Performance Marts | Switch-Leistung für Port | Stündlich | 5 Wochen |
| Performance Marts | Performance-Switch für Host, Storage und Tape | Stündlich | 13 Monaten |
| Performance Marts | Storage-Node | Stündlich | 14 Tage |
| Performance Marts | Storage-Node | Täglich | 13 Monaten |
| Performance Marts | VM-Performance | Stündlich | 14 Tage |
| Performance Marts | VM-Performance | Täglich | 13 Monaten |
| Performance Marts | Hypervisor-Performance | Stündlich | 14 Tage |
| Performance Marts | Hypervisor-Performance | Täglich | 13 Monaten |
| Performance Marts | VMDK-Performance | Stündlich | 14 Tage |
| Performance Marts | VMDK-Performance | Täglich | 13 Monaten |
| Performance Marts | Disk Performance | Stündlich | 14 Tage |
| Performance Marts | Disk Performance | Täglich | 13 Monaten |
| Capacity Marts | Alle (außer einzelne Volumes) | Täglich | 13 Monaten |
| Capacity Marts | Alle (außer einzelne Volumes) | Monatlicher Vertreter | 14 Monaten und darüber hinaus |
| Inventarmarke | Einzelne Volumes | Aktueller Stand | 1 Tag (oder bis zum nächsten ETL) |

Nach 13 Monaten (konfigurierbar) speichert Data Warehouse in den folgenden Faktentabellen nur einen Datensatz pro Monat anstatt einen Datensatz pro Tag für Kapazitäts-, Leistungs- und Ressourcendaten:

- Tabelle mit Fakten zur Rückberechnung (dwh_capacity.chargeback_fact)
- Tabelle „Kennzahl der Dateisystemauslastung“ (dwh_fs_util.fs_util_Fact)
- Host-Faktentabelle (dwh_sa.sa_Host_Fact)
- Faktentabelle für interne Volumenkapazität (dwh_capacity.internal_volume_capacity_fact)
- Ports Faktentabelle (dwh_Ports.Ports_Fact)
- Faktentabelle für qtree-Kapazität (dwh_Capacity.qtree_Capacity_Fact)

- Faktentabelle für Speicher- und Speicherpool-Kapazität (dwh_Capacity.Storage_and_Storage_Pool_Capacity_Fact)
- Faktentabelle für Volumenkapazität (dwh_Capacity.vm_Capacity_Fact)
- Tabellen mit stündlicher Storage-Node-Performance (Storage_Node_hourly_Performance_FACT) und täglicher Storage-Node-Performance (Storage_Node_Daily_Performance_FACT)

### Datenaufbewahrung, ETL und Zeiträume

Das OnCommand Insight Data Warehouse speichert Daten, die aus dem ETL-Prozess (Extract, Transform, Load) gewonnen werden, für verschiedene Zeiträume, basierend auf den unterschiedlichen Datentabellen und der Zeitgranularität der Daten.

#### Performance Marts und stündliche Granularität für Volumes und interne Volumes

Das OnCommand Insight Data Warehouse zeichnet 14 Tage lang die stündlichen Durchschnittswerte, die Stundenmaxima und das Zugriffs-Bit für jede Stunde des Tages (24 Datenpunkte) auf. Das Access Bit ist ein boolescher Wert, der wahr ist, wenn auf das Volume zugegriffen wird, oder falsch, wenn während des stündlichen Intervalls kein Zugriff auf das Volume erfolgt. Alle 24 Datenpunkte für den Vortag werden während des ersten ETL-Prozesses des Tages ermittelt.

Sie müssen nicht einen ETL-Prozess pro Stunde ausführen, um die stündlichen Datenpunkte zu erfassen. Beim Ausführen zusätzlicher ETL-Prozesse während des Tages werden keine Leistungsinformationen von den OnCommand Insight-Servern abgerufen.

#### Performance Marts und tägliche Granularität für Volumes und interne Volumes

An jedem Tag, an dem die ETL verarbeitet wird, werden die Tagesdurchschnittswerte für den vorhergehenden Tag berechnet und in Data Warehouse eingetragen. Der Tagesdurchschnitt ist eine Zusammenfassung der 24 Datenpunkte des Vortages. Die Performance-Datentabellen speichern täglich Zusammenfassungen für Volumes und interne Volumes über 13 Monate.

#### Kapazität und tägliche Granularität

Die Capacity Marts liefern täglich Messungen für verschiedene Kapazitätsfakten über einen Zeitraum von 13 Monaten. Die Kapazitätsdaten in Data Warehouse sind aktuell bei der letzten Datenquellenerfassung für das Gerät vor der ETL.

#### KapazitätsMärz und monatliche Granularität

Data Warehouse speichert tägliche Kapazitätsdaten über 13 Monate. Nach Erreichen der 13-monatigen Schwelle werden die Kapazitätsdaten monatlich zusammengefasst. Die monatlichen Daten basieren auf den Werten, die durch das Datum, das das repräsentative Datum des Monats darstellt, reflektiert werden.

Die folgende Tabelle zeigt, welche monatlichen Daten in der monatlichen Zusammenfassung enthalten sind:

| Datum | Ist der Wert des Vertreters für den Monat | Zugewiesene Kapazität |
|---|---|---|
| Januar | 1 (Wahr) | 50 TB |
| Januar 2 | 0 (Falsch) | 52 TB |

| … | … | … |
|---|---|---|
| Januar 31 | 0 (Falsch) | 65 TB |
| Februar | 1 (Wahr) | 65 TB |

Auf der Grundlage dieser Tabelle würde ein Monatsbericht 50 TB für Januar und 65 TB für Februar anzeigen. Alle anderen Kapazitätswerte für Januar würden nicht in der monatlichen Zusammenfassung enthalten sein.

#### Inventory Mart

Der Bestandsdatenbestand ist nicht historisch. Jedes Mal, wenn ein ETL-Prozess ausgeführt wird, wird der Inventory Mart gelöscht und neu erstellt. Daher spiegeln alle Berichte, die aus dem Inventory Mart generiert wurden, nicht die historische Bestandskonfiguration wider.

# Erste Schritte mit Data Warehouse

Mit dem OnCommand Insight Data Warehouse können Sie die erforderlichen Optionen konfigurieren, bevor Sie Berichte mit Ihren Daten erstellen. Data Warehouse enthält viele Funktionen, allerdings müssen Sie nur wenige von ihnen für den Einstieg verwenden. Zum Einrichten von Data Warehouse verwenden Sie Optionen im Data Warehouse Portal.

## Über diese Aufgabe

Zur Einrichtung des OnCommand Insight Data Warehouse sollte ein Storage-Administrator folgende Schritte durchführen:

- Zugriff auf das Data Warehouse-Portal
- Verbinden von Data Warehouse mit OnCommand Insight-Servern
- Erstellen der Datenbank aus dem Verlauf
- Backup- und Wiederherstellungsprozesse einrichten

Darüber hinaus muss ein Storage-Administrator möglicherweise die folgenden Verfahren ausführen.

- Zugriff auf MySQL über die Befehlszeilenschnittstelle
- Planung täglicher Builds
- Einrichtung mehrerer Mandanten in Berichten
- Fehlerbehebung bei Setup-Problemen
  - Warum kann ich meine Anmerkungen nicht sehen?
  - Was soll ich mit fehlgeschlagenen historischen Baustellen tun?

Wenn Sie das Data Warehouse Portal zum ersten Mal verwenden, müssen Sie Data Warehouse einrichten, bevor Informationen auf der Seite Jobs angezeigt werden können. Sie müssen diesen Einrichtungsvorgang auch wiederholen, nachdem Sie die Data Warehouse-Datenbank zurückgesetzt haben.

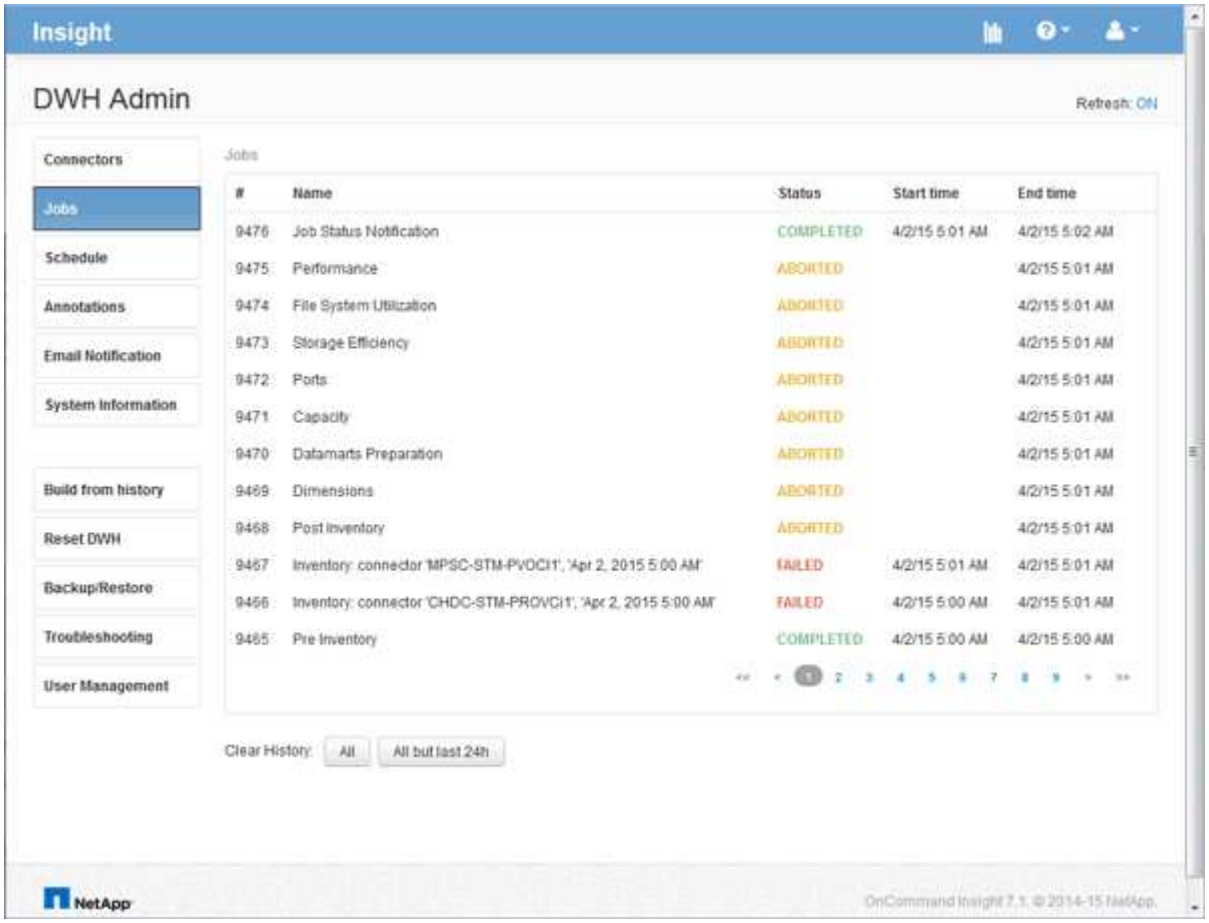
## Zugriff auf das Data Warehouse-Portal

Das OnCommand Insight-Data-Warehouse-Portal ist eine webbasierte Benutzeroberfläche, mit der Sie Connector-Informationen aktualisieren, Jobwarteschlangen anzeigen, tägliche Builds planen, Anmerkungen auswählen, E-Mail-Benachrichtigungen einrichten, Systeminformationen anzeigen, die Datenbank erstellen, Data Warehouse zurücksetzen, die Datenbank sichern und wiederherstellen, Probleme beheben, Verwalten von Benutzerkonten im Data Warehouse- und Reporting-Portal sowie Zugriff auf Dokumentation und Schemadokumentationen.

### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
3. Klicken Sie Auf **Login**.

   Das Data Warehouse-Portal wird geöffnet:




## Verwalten von Benutzerkonten für Data Warehouse und Reporting

Benutzerkonten, Benutzerauthentifizierung und Benutzerautorisierung für die OnCommand Insight-Berichtstools werden über das Data Warehouse (DWH) definiert

und verwaltet. Basierend auf diesen Konfigurationen erhalten Benutzer und Administratoren Zugriff auf einige oder alle verfügbaren OnCommand Insight-Berichte.

Für den Zugriff auf die Benutzerverwaltung im Data Warehouse ist ein Konto mit Systemadministratorrechten erforderlich. Hierzu zählen folgende Optionen:

- Vollständige Administrationsfunktionen für das Data Warehouse
- Konfiguration und Pflege aller Benutzerkonten
- Lesezugriff auf die Datenbank
- Möglichkeit zum Einrichten von Connectors in der ETL, Planen von Data Warehouse-Jobs, Zurücksetzen der Datenbank, Zuweisen oder Ändern von Rollen sowie Hinzufügen und Entfernen von Benutzerkonten

### Zugriff auf das Data Warehouse- und Reporting-Portal

Das Data Warehouse-Portal bietet Zugriff auf Verwaltungsoptionen. Über das Data Warehouse-Portal können Sie auch auf das Reporting-Portal zugreifen.

#### Schritte

1. Melden Sie sich als Administrator beim Data Warehouse-Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Reporting-Portal zu öffnen.

### Reporting-Benutzerrollen

Jedem Benutzerkonto wird eine Rolle mit einem Satz von Berechtigungen zugewiesen. Die Anzahl der Benutzer wird durch die Anzahl der Reporting-Lizenzen begrenzt, die jeder Rolle zugeordnet sind.

Jede Rolle kann die folgenden Aktionen ausführen:

- **Empfänger**

  Zeigt Berichte im OnCommand Insight-Reporting-Portal an und legt persönliche Einstellungen wie die für Sprachen und Zeitzonen fest.

  Empfänger können keine Berichte erstellen, Berichte ausführen, Berichte planen, Berichte exportieren oder administrative Aufgaben ausführen.

- **Business Consumer**

  Führt Berichte aus und führt alle Empfängeroptionen aus.

- **Business Author**

  Zeigt geplante Berichte an, führt Berichte interaktiv aus, erstellt Meldungen und führt alle Business Consumer-Optionen aus.

- **Pro Author**

  Erstellt Berichte, erstellt Pakete und Datenmodule sowie alle Optionen für Business Author.

- **Administrator**

  Führt Verwaltungsaufgaben für Berichte durch, wie z. B. Import und Export von Berichtsdefinitionen, Konfiguration von Berichten, Konfiguration von Datenquellen und Herunterfahren und Neustart von Berichtsaufgaben.

Die folgende Tabelle zeigt die Berechtigungen und die maximale Anzahl von Benutzern, die für jede Rolle zulässig sind:

| Merkmal | Empfänger | Geschäftsverbraucher | Wirtschaftautor | Pro Author | Admin |
|---|---|---|---|---|---|
| Anzeigen von Berichten auf der Registerkarte „Teaminhalt“ | Ja. | Ja. | Ja. | Ja. | Ja. |
| Berichte erstellen | Nein | Ja. | Ja. | Ja. | Ja. |
| Planen von Berichten | Nein | Ja. | Ja. | Ja. | Ja. |
| Externe Dateien hochladen | Nein | Nein | Ja. | Ja. | Nein |
| Erstellen von Geschichten | Nein | Nein | Ja. | Ja. | Nein |
| Erstellen von Berichten | Nein | Nein | Ja. | Ja. | Nein |
| Erstellen von Paketen und Datenmodulen | Nein | Nein | Nein | Ja. | Nein |
| Ausführung administrativer Aufgaben | Nein | Nein | Nein | Nein | Ja. |
| Anzahl der Benutzer | Anzahl der OnCommand Insight Benutzer | 20 | 2 | 1 | 1 |

Wenn Sie einen neuen Benutzer für Data Warehouse und Reporting hinzufügen und das Limit in einer Rolle überschreiten, wird der Benutzer als „`deactivated`,“ hinzugefügt und Sie müssen einen anderen Benutzer mit dieser Rolle deaktivieren oder entfernen, um eine neue Benutzermitgliedschaft zu erhalten.

Für die Funktionen zur Berichterstellung ist eine Insight Plan-Lizenz erforderlich. Sie können zusätzliche Benutzer von Business Author und Pro Author hinzufügen, indem Sie DAS ARAP (Additional Report Authoring Package) erwerben. Wenden Sie sich an Ihren OnCommand Insight Ansprechpartner.

Diese berichtstellungsweisen Benutzerrollen haben keinen Einfluss auf den direkten Datenbankzugriff. Diese berichtenden Benutzerrollen haben keinen Einfluss auf Ihre Fähigkeit, SQL-Abfragen mithilfe der Data Marts zu erstellen.

### Hinzufügen eines Reporting-Benutzers

Sie müssen für jede Person, die Zugriff auf das Reporting-Portal benötigt, ein neues Benutzerkonto hinzufügen. Die Verwendung eines anderen Benutzerkontos für jede Person ermöglicht die Kontrolle von Zugriffsrechten, individuellen Einstellungen und Verantwortlichkeit.

#### Bevor Sie beginnen

Bevor Sie einen Reporting-Benutzer hinzufügen, müssen Sie einen eindeutigen Benutzernamen zugewiesen haben, das zu verwendende Kennwort festgelegt und die korrekte Benutzerrolle bzw. -Rolle überprüft haben. Diese Rollen sind auf das Reporting-Portal spezialisiert.

#### Schritte

1. Melden Sie sich als Administrator beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Benutzerverwaltung**.
3. Klicken Sie im Fenster **Benutzerverwaltung** auf **Neuen Benutzer hinzufügen**.
4. Geben Sie die folgenden Informationen für den neuen Reporting-Benutzer ein:
   - **Benutzername**

     Benutzername (alphanumerisch, einschließlich a-z, A-Z und 0-9) für das Konto
   - **E-Mail-Adresse**

     Mit dem Benutzerkonto verknüpfte E-Mail-Adresse, die erforderlich ist, wenn der Benutzer Berichte abonniert
   - **Passwort**

     Passwort zur Anmeldung bei OnCommand Insight mit diesem Benutzerkonto, das normalerweise vom Benutzer ausgewählt und in der Benutzeroberfläche bestätigt wird
   - **Insight-Rolle**

     Rollen, die dem Benutzer mit entsprechenden Berechtigungen zur Verfügung stehen

     Die Optionen für die OnCommand Insight-Rolle werden nur angezeigt, wenn OnCommand Insight auf demselben Rechner wie die Berichtsfunktionen installiert ist, was nicht typisch ist.

- **Berichtsrollen**

  Berichtsfunktion für dieses Benutzerkonto (z. B. Pro Author)

  Die Administratorrolle ist eindeutig. Sie können diese Rolle jedem Benutzer hinzufügen.

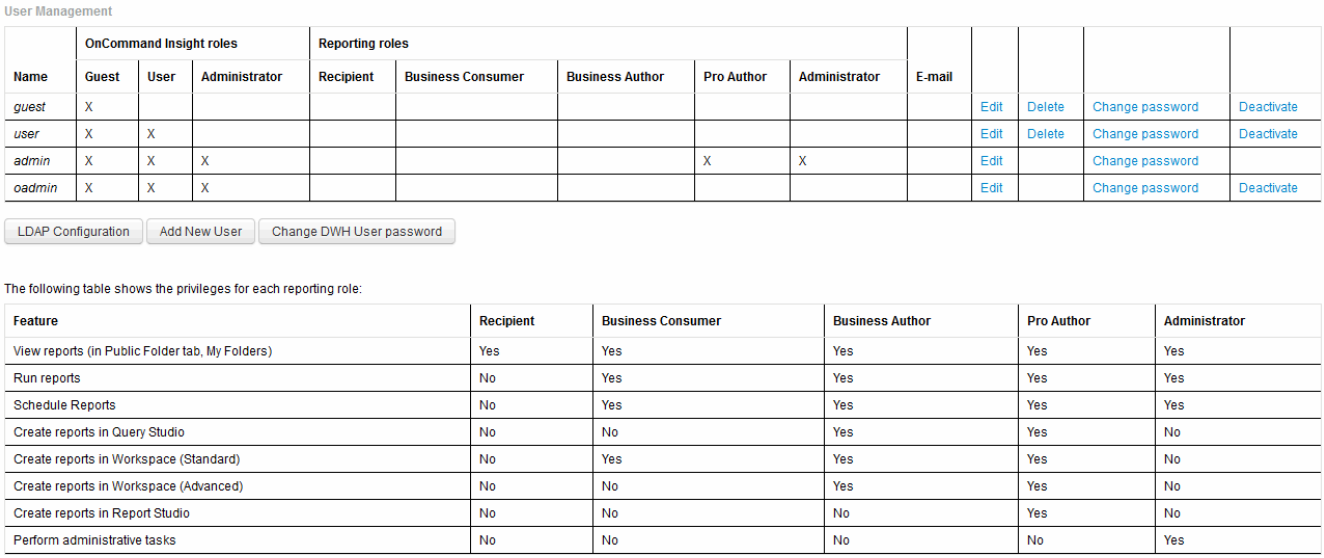
5. Klicken Sie Auf **Hinzufügen**.

### Verwalten von Benutzerkonten

Sie können Benutzerkonten, Benutzerauthentifizierung und Benutzerautorisierung über das Data Warehouse-Portal konfigurieren. Jedem Benutzerkonto wird eine Rolle mit einer der folgenden Berechtigungsstufen zugewiesen. Die Anzahl der Benutzer wird durch die Anzahl der Reporting-Lizenzen begrenzt, die jeder Rolle zugeordnet sind.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Benutzerverwaltung**.


User Management

| | OnCommand Insight roles | | | Reporting roles | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Guest | User | Administrator | Recipient | Business Consumer | Business Author | Pro Author | Administrator | E-mail | | | | |
| *guest* | X | | | | | | | | | Edit | Delete | Change password | Deactivate |
| *user* | X | X | | | | | | | | Edit | Delete | Change password | Deactivate |
| *admin* | X | X | X | | | | X | X | | Edit | | Change password | |
| *oadmin* | X | X | X | | | | | | | Edit | | Change password | Deactivate |

LDAP Configuration | Add New User | Change DWH User password

The following table shows the privileges for each reporting role:

| Feature | Recipient | Business Consumer | Business Author | Pro Author | Administrator |
|---|---|---|---|---|---|
| View reports (in Public Folder tab, My Folders) | Yes | Yes | Yes | Yes | Yes |
| Run reports | No | Yes | Yes | Yes | Yes |
| Schedule Reports | No | Yes | Yes | Yes | Yes |
| Create reports in Query Studio | No | No | Yes | Yes | No |
| Create reports in Workspace (Standard) | No | Yes | Yes | Yes | No |
| Create reports in Workspace (Advanced) | No | No | Yes | Yes | No |
| Create reports in Report Studio | No | No | No | Yes | No |
| Perform administrative tasks | No | No | No | No | Yes |

3. Führen Sie einen der folgenden Schritte aus:
   - Um einen vorhandenen Benutzer zu bearbeiten, wählen Sie die Zeile für den Benutzer aus und klicken Sie auf **Bearbeiten**.
   - Um das Passwort eines Benutzers zu ändern, wählen Sie die Zeile für den Benutzer aus und klicken Sie auf **Passwort ändern**.
   - Um einen Benutzer zu löschen, wählen Sie die Zeile für den Benutzer aus und klicken auf **Löschen**
4. Um einen Benutzer zu aktivieren oder zu deaktivieren, wählen Sie die Zeile für den Benutzer aus und klicken Sie auf **Aktivieren** oder **Deaktivieren**.

### Konfigurieren von LDAP für die Berichterstellung

Über das Data Warehouse-Portal kann der Administrator die LDAP-Nutzung für Data

# Warehouse und Reporting konfigurieren.

**Bevor Sie beginnen**

Sie müssen sich bei Insight als Administrator anmelden, um diese Aufgabe auszuführen.

Für alle Secure Active Directory (d. h. LDAPS)-Benutzer müssen Sie den AD-Servernamen genau so verwenden, wie er im Zertifikat definiert ist. Sie können die IP-Adresse nicht für die sichere AD-Anmeldung verwenden.

Wenn Sie *Server.keystore* und/oder *Server.trustore* Passwörter mit geändert "Sicherheitsadministration"haben, starten Sie den *SANscreen*-Dienst neu, bevor Sie das LDAP-Zertifikat importieren.

**Schritte**

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Benutzerverwaltung**.
3. Klicken Sie auf **LDAP-Konfiguration**.
4. Wählen Sie **LDAP aktivieren**, um die LDAP-Benutzerauthentifizierung und -Autorisierung zu starten.
5. Nehmen Sie alle erforderlichen Änderungen vor, um LDAP zu konfigurieren.

   Die meisten Felder enthalten Standardwerte. Die Standardeinstellungen sind für das Active Directory gültig.

   - **Attribut des Hauptnamens des Benutzers**

     Attribut, das jeden Benutzer im LDAP-Server identifiziert. Standard ist `userPrincipalName`, Die weltweit einzigartig ist. OnCommand Insight versucht, den Inhalt dieses Attributs mit dem oben angegebenen Benutzernamen abzugleichen.

   - **Rollenattribut**

     LDAP-Attribut, das die Passung des Benutzers innerhalb der angegebenen Gruppe identifiziert. Standard ist `memberOf`.

   - **Mail-Attribut**

     LDAP-Attribut, das die E-Mail-Adresse des Benutzers identifiziert. Standard ist `mail`. Dies ist nützlich, wenn Sie Berichte von OnCommand Insight abonnieren möchten. Insight erfasst die E-Mail-Adresse des Benutzers bei der ersten Anmeldung und sucht danach nicht mehr.

     Wenn sich die E-Mail-Adresse des Benutzers auf dem LDAP-Server ändert, müssen Sie sie in Insight aktualisieren.

   - **Distinguished Name Attribut**

     LDAP-Attribut, das den Distinguished Name des Benutzers identifiziert. Der Standardwert ist `distinguishedName`.

   - **Empfehlung**

Gibt an, ob dem Pfad zu anderen Domänen folgen soll, wenn sich mehrere Domänen im Unternehmen befinden. Sie müssen immer die Standardeinstellung verwenden `follow` Einstellung.

- **Timeout**

  Dauer der Wartezeit auf eine Antwort vom LDAP-Server vor der Zeitüberschreitung in Millisekunden. Der Standardwert ist 2,000, was in allen Fällen angemessen ist und nicht geändert werden sollte.

- **LDAP-Server**

  Dies ist die IP-Adresse oder der DNS-Name zur Identifizierung des LDAP-Servers. Um einen bestimmten Port zu identifizieren, wobei `ldap-server-address` Ist der Name des LDAP-Servers. Sie können das folgende Format verwenden:

  ```
  ldap://ldap-server-address:port
  ```

  Um den Standardport zu verwenden, können Sie das folgende Format verwenden:

  ```
  ldap://ldap-server-address
  ```

  ```
   When entering multiple LDAP servers in this field,
  separate entries with a comma, and ensure that the correct
  port number is used in each entry.
  + um die LDAP-Zertifikate zu importieren, klicken Sie auf
  *Zertifikate importieren* und importieren bzw. suchen Sie
  die Zertifikatdateien manuell.
  ```

- **Domäne**

  LDAP-Knoten, auf dem OnCommand Insight nach dem LDAP-Benutzer suchen soll. Dies ist in der Regel die Domäne der obersten Ebene für das Unternehmen. Beispiel:

```
DC=<enterprise>,DC=com
```

- **Insight Server Admins-Gruppe**

  LDAP-Gruppe für Benutzer mit Insight Server Administrator-Berechtigungen. Standard ist `insight.server.admins`.

- **Gruppe der Insight-Administratoren**

  LDAP-Gruppe für Benutzer mit Insight Administrator-Berechtigungen. Standard ist `insight.admins`.

- **Insight Benutzergruppe**

  LDAP-Gruppe für Benutzer mit Insight-Benutzerberechtigungen. Standard ist `insight.users`.

- **Insight Gästegruppe**

  LDAP-Gruppe für Benutzer mit Insight Gastberechtigungen. Standard ist `insight.guests`.

- **Gruppe der Reporting-Administratoren**

  LDAP-Gruppe für Benutzer mit Administratorrechten für Insight Reporting. Standard ist `insight.report.admins`.

- **Reporting pro Autorengruppe**

  LDAP-Gruppe für Benutzer mit Insight Reporting Pro-Autorenrechten. Standard ist `insight.report.proauthors`.

- **Reporting Business Authors-Gruppe**

  LDAP-Gruppe für Benutzer mit Berechtigungen für Business-Autoren von Insight Reporting. Standard ist `insight.report.business.authors`.

- **Gruppe der Geschäftskonsumenten melden**

  LDAP-Gruppe für Benutzer mit Insight Reporting-Rechten für Geschäftskunden. Standard ist `insight.report.business.consumers`.

- **Empfängergruppe melden**

  LDAP-Gruppe für Benutzer mit Insight Reporting-Empfängerberechtigungen. Standard ist `insight.report.recipients`.

6. Geben Sie Werte in die Felder **Directory Lookup user** und **Directory Lookup user password** ein, wenn Sie Änderungen vorgenommen haben.

   Wenn Sie die überarbeiteten Werte nicht in diese Felder eingeben, werden Ihre Änderungen nicht gespeichert.

7. Geben Sie das Passwort für die Verzeichnissuche erneut in das Feld **Confirm Directory lookup user password** ein, und klicken Sie auf **Validate Password**, um das Passwort auf dem Server zu validieren.
8. Klicken Sie auf **Update**, um die Änderungen zu speichern. Klicken Sie auf **Abbrechen**, um die Änderungen zu entfernen.

## Verbinden von Data Warehouse mit OnCommand Insight-Servern

Konnektoren stellen Verbindungen vom OnCommand Insight Data Warehouse zu den OnCommand Insight-Servern her. Sie können Data Warehouse mit einem oder mehreren OnCommand Insight-Servern verbinden. Sie können Verbindungen zu oder aus OnCommand Insight-Datenbanken hinzufügen oder entfernen.

### Über diese Aufgabe

Data Warehouse weist dem Konnektor, der zusammen mit dem Anschlussnamen verwendet wird, eine globale eindeutige ID zu. Nach dem Hinzufügen eines Konnektors fragt Data Warehouse die OnCommand Insight-Datenbank nach dem Namen und der Version des OnCommand Insight-Standorts ab.

Sie können eine Verbindung zu einer Datenquelle mit oder ohne SSL herstellen. Durch die Auswahl der sicheren Datenquelle wird bei der Kommunikation mit der OnCommand Insight Remote-Datenbank SSL verwendet.

Data Warehouse kann eine konsolidierte Ansicht der Daten mehrerer OnCommand Insight Installationen bereitstellen. Diese konsolidierte Datenbank bietet folgende Informationen:

- Global Eindeutige Identifizierungsmerkmale

  Jedem Objekt wird eine global eindeutige ID zugewiesen, die unabhängig von den von den einzelnen Standorten verwendeten IDs ist, um widersprüchliche IDs zu vermeiden und die doppelte Erkennung zu ermöglichen. Diese IDs werden von allen Data Marts gemeinsam genutzt. Diese ID ist die global eindeutige ID (GUID) in der Spalte Kommentar der Inventory Data Mart-Tabellen.

- Keine Duplizierung

  Entitäten, die in mehreren OnCommand Insight-Datenbanken vorhanden sind, werden nur einmal in der konsolidierten Datenbank registriert.

- Aktueller Datensatz

  Die Daten in der konsolidierten Datenbank (Inventory Data Mart) sind immer am aktuellsten Stand.

Wenn Sie eine Verbindung hinzufügen oder bearbeiten, können Sie die Verbindung auch testen. Der Test führt Folgendes aus:

- Überprüft die Host-IP-Adresse, den Benutzernamen und das Passwort und stellt sicher, dass eine Verbindung hergestellt werden kann.

  Ungültige Verbindungen werden rot angezeigt.

- Vergleicht die OnCommand Insight-Version mit der Data Warehouse-Version.

  Wenn die Versionen nicht kompatibel sind, wird eine Fehlermeldung angezeigt.

- Stellt sicher, dass die OnCommand Insight-Datenbank nicht geändert oder in einer anderen Datenbank wiederhergestellt wurde, wie dies bei der letzten Data Warehouse-Verarbeitung der Fall ist. Wenn eine Änderung vorgenommen wurde, wird eine Fehlermeldung angezeigt.

**Schritte**

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   Die Tabelle Connectors wird zunächst leer angezeigt und zeigt nach dem Hinzufügen eines Connectors die Verbindungsinformationen an.

3. Klicken Sie auf **Neu**, um einen neuen Konnektor hinzuzufügen.
4. Geben Sie Folgendes ein:

   - **Verschlüsselung**

     Wählen Sie aus, um Data Warehouse-Anfragen mit SSL-Verschlüsselung zu aktivieren `Enabled`.

- **Name**

  Ein Anschlussname, der den Anschluss in der Ansicht Connectors identifiziert.

- **Gastgeber**

  Host-IP-Adresse

- **Benutzername**

  „Inventory“

  Mit diesem Benutzernamen und Passwort können Sie sich bei der Remote-OnCommand Insight-Datenbank anmelden und Abfragen zu den Daten durchführen.

- **Passwort**

  SANscreen

5. Um den Port anzugeben, der für TCP-Verbindungen zum Host verwendet werden soll, klicken Sie auf **Erweitert** und geben Sie die TCP-Portnummer ein.
6. Um den Port (außer dem Standardport) anzugeben, der für HTTPS-Verbindungen zum Host verwendet werden soll, klicken Sie auf **Erweitert** und geben Sie die Portnummer ein.
7. Klicken Sie Auf **Test**.

   Data Warehouse testet die Verbindung.

8. Klicken Sie Auf **Speichern**.

   Wenn Sie mehrere Verbindungen für mehrere Installationen eingeben, ruft Data Warehouse unabhängige Build-Prozesse auf, einen für jede Datenbank, aus der Daten extrahiert werden sollen. Jeder dieser Build-Prozesse extrahiert Daten aus einer OnCommand Insight-Datenbank und lädt sie in die konsolidierte Datenbank.

## Data Warehouse-Datenbank aus Verlaufsübersicht erstellen

Sie können die Data Warehouse-Datenbank mithilfe von historischen Daten auf Ihrem OnCommand Insight-Server erstellen. Data Warehouse extrahiert Daten von den OnCommand Insight-Servern und erstellt die Data Warehouse-Data Marts gemäß dem Zeitplan für die Erstellung aus dem Verlauf.

Für diese Option ist keine spezielle Lizenz erforderlich, und Bestandsdaten sind im Build enthalten. Für die Erstellung von Kapazitätsinformationen sind jedoch der OnCommand Insight-Plan und die OnCommand Insight Perform Lizenzen erforderlich.

Wenn bereits ein Build (aus dem Verlauf oder der aktuellen Version) ausgeführt wurde, kann der Build nicht an Daten vor dem letzten Job ausgeführt werden. Dies bedeutet, dass Sie bei der Ausführung eines aktuellen Builds nicht aus dem Verlauf erstellen können. Genauer gesagt, wenn Sie Builds aus der Geschichte durchgeführt haben, die am 1. Januar 2012 endete, können Sie keine Build auf dem Jahr 2011 durchführen.

Wenn der Verlauf nicht ein oder zwei der erfolglosen ETL-Prozesse enthält, versuchen Sie nicht, einen Verlauf für nur diese Tage zu erstellen. Historische Daten sind für längere Zeiträume, und ein oder zwei Tage wird sich

der Trend nicht signifikant ändern. Wenn Sie aus dem Verlauf neu erstellen möchten, erstellen Sie den gesamten Verlauf neu.

In der Ansicht Build from History werden alle Build-Jobs von allen Connectors angezeigt. Beispielsweise kann die Ansicht einen Bestandsjob für jeden Konnektor, einen Port-Kapazitätsjob für jeden Build-Lauf und einen Job mit Anmerkungen anzeigen.

Bevor Sie das Build aus dem Verlauf konfigurieren, müssen Sie Folgendes ausführen:

- Anschlüsse müssen konfiguriert werden.
- Anmerkungen sollten in OnCommand Insight eingegeben werden und können manuell über die Option **Aktualisierung von Anmerkungen für DWH erzwingen** im alten OnCommand Insight-Portal aktualisiert werden oder werden automatisch 15 Minuten nach ihrer Einstellung aktualisiert.

### Hinzufügen eines Jobs, der aus dem Verlauf eine Data Warehouse-Datenbank erstellt

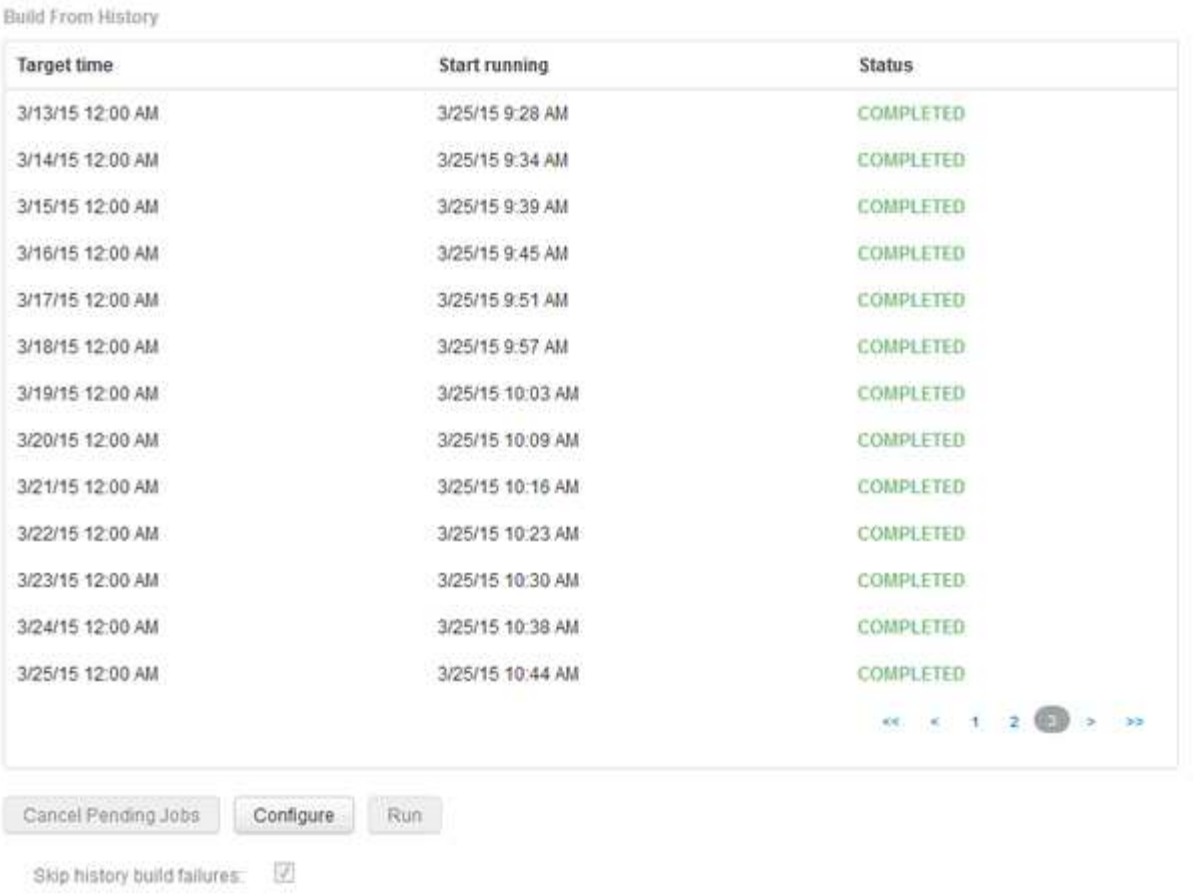
Sie können die Data Warehouse-Datenbank mithilfe von historischen Daten erstellen, die auf dem OnCommand Insight-Server gespeichert sind, sodass Sie Projektionsberichte ausführen können.

#### Bevor Sie beginnen

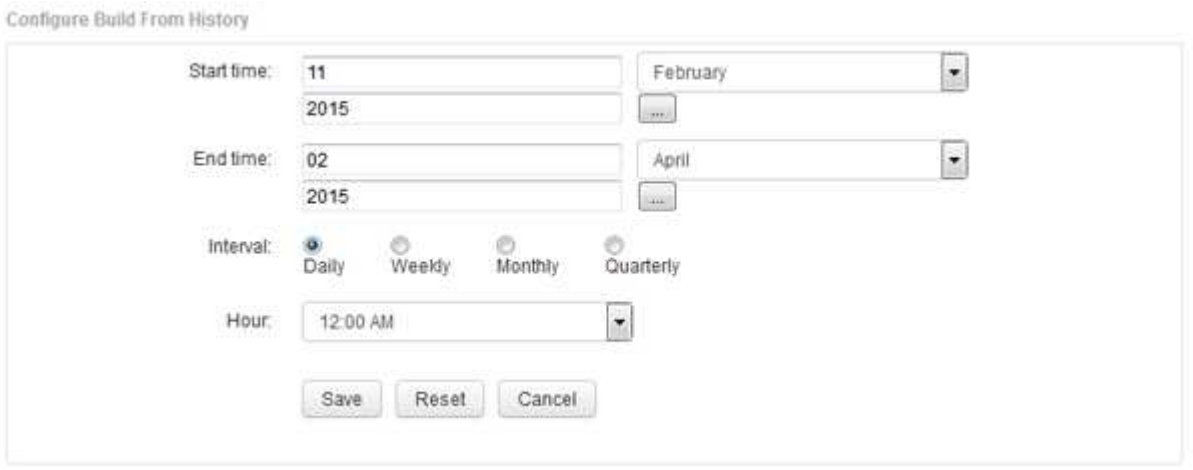
Sie müssen Anmerkungen auf dem OnCommand Insight-Server aktualisiert und eine Aktualisierung der Anmerkungsinformationen für das Data Warehouse erzwungen haben.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Build from History**.




3. Klicken Sie Auf **Konfigurieren**.




4. Geben Sie die Start- und Endzeit ein.

   Um einen Kalender anzuzeigen, aus dem Sie diese Daten auswählen können, klicken Sie auf den Abwärtspfeil neben dem Namen des Monats.

   Das Zeitformat hängt vom Gebietsschema des Data Warehouse-Servers ab.

   Die Start- und Endzeiten müssen innerhalb des Verlaufsbereichs liegen, der in allen OnCommand Insight-Servern enthalten ist, mit denen das Data Warehouse verbunden ist, wie in der Option Connectors des Data Warehouse-Portals festgelegt. Die Standard-Start- und Endzeiten geben den maximal gültigen Zeitraum an. Der Data Warehouse-Build-Job wird automatisch zu dem von Ihnen angegebenen Zeitpunkt

ausgeführt.

> Die Konfiguration eines nicht realistischen Zeitplans wie „`Täglich für 4 Jahre`“ führt zu 1460 Build-Zyklen, was 10 Tage dauern kann.

5. Wählen Sie das Intervall aus.

   Wenn Sie ein Monats- oder Wochenintervall auswählen, wird das Feld Tag angezeigt. Wenn Sie monatlich ausgewählt haben, ist Tag ein Datum. Wenn Sie wöchentlich ausgewählt haben, ist Tag Sonntag bis Samstag.

6. Wählen Sie die Stunde, zu der der Build stattfinden soll.
7. Um die Optionen auf die Standardeinstellungen zurückzusetzen, klicken Sie optional auf **Reset**.
8. Klicken Sie Auf **Speichern**.
9. Klicken Sie auf der Seite **Build from History** auf **Run**, um einen Build außerhalb des automatischen Schedule Builds durchzuführen.

   In der Spalte Zielzeit wird die Zeit angezeigt, zu der dieser Eintrag erstellt wurde. In der Spalte Status wird angezeigt, ob der Build abgeschlossen oder fehlgeschlagen ist.

#### Abbrechen eines Builds aus einem Verlaufsjob

Sie können alle geplanten Jobs abbrechen. Der Jobstatus lautet „`Ababgebrochen`“.

##### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Build from History**.
3. Klicken Sie Auf **Abbrechen**.

## Sichern der Data Warehouse-Datenbank

Sie können die Data Warehouse-Datenbank, die auch ein Cognos-Backup enthält, in einer Datei sichern und später mithilfe des Data Warehouse-Portals wiederherstellen. Mit einem solchen Backup können Sie auf einen anderen Data Warehouse-Server migrieren oder auf eine neue Data Warehouse-Version aktualisieren.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://fqdn/dwh`.
2. Wählen Sie im Navigationsfenster links **Backup/Restore** aus.
3. Klicken Sie auf **Backup** und wählen Sie Ihre Backup-Konfiguration aus:

   a. Alle Datamarts außer Performance Datamart

   b. Alle Datamarts

      Dieser Vorgang kann 30 Minuten oder länger dauern.

+ Data Warehouse erstellt eine Sicherungsdatei und zeigt ihren Namen an.

4. Klicken Sie mit der rechten Maustaste auf die Sicherungsdatei, und speichern Sie sie an einem gewünschten Speicherort.

   Sie möchten den Dateinamen möglicherweise nicht ändern. Sie sollten die Datei jedoch außerhalb des Installationspfads des Data Warehouse speichern.

   Die Data Warehouse Backup-Datei enthält MySQL der DWH-Instanz; benutzerdefinierte Schemas (MySQL DBs) und Tabellen; LDAP-Konfiguration; die Datenquellen, die Cognos mit der MySQL-Datenbank verbinden (nicht die Datenquellen, die den Insight-Server mit Geräten verbinden, um Daten zu erfassen); Importieren und Exportieren von Aufgaben, die Berichte importiert oder exportiert haben; Reporting von Sicherheitsrollen, Gruppen und Namespaces; Benutzerkonten; Alle geänderten Reporting Portal-Berichte sowie alle benutzerdefinierten Berichte, unabhängig davon, wo sie gespeichert sind, selbst im Verzeichnis „Meine Ordner“. Cognos-Systemkonfigurationsparameter wie SMTP-Servereinstellungen und Cognos-Einstellungen für benutzerdefinierten Speicher werden nicht gesichert.

   Die Standardschemas, in denen benutzerdefinierte Tabellen gesichert werden, umfassen Folgendes:

| |
|---|
| dwh_Capacity |
| dwh_Capacity_Staging |
| dwh_Bemaßungen |
| dwh_fs_util |
| dwh_Inventory |
| dwh_Inventory_Staging |
| dwh_Inventory_transient |
| dwh_Management |
| dwh_Performance |
| dwh_Performance_Staging |
| dwh_Ports |
| dwh_Reports |
| dwh_sa_Staging |
| |
| |
| |

   Schemas, bei denen benutzerdefinierte Tabellen vom Backup ausgeschlossen werden, umfassen Folgendes:

| |
|---|
| Information_Schema |
| Akquisition |
| Cloud_Modell |
| Host_Data |
| innodb |
| Inventar |
| Inventory_private |
| Inventory_Time |
| Protokolle |
| Vereinfachtes |
| mysql |
| nas |
| Performance |
| Performance_Schema |
| Performance_Views |
| SANscreen |
| Schrubben |
| Servicesicherheit |
| Test |
| Tmp |
| workbench |
| |
| |
| |

Bei manuell initiierten Backups wird ein angezeigt `.zip` Datei wird erstellt, die folgende Dateien enthält:

- Ein tägliches Backup `.zip` Datei, die Cognos-Berichtsdefinitionen enthält
- Ein meldet Backup `.zip` Datei, die alle Berichte in Cognos enthält, einschließlich der Berichte im Verzeichnis eigene Ordner
- Eine Data Warehouse-Datenbank-Sicherungsdatei Zusätzlich zu manuellen Backups, die Sie jederzeit durchführen können, erstellt Cognos täglich ein Backup (automatisch jeden Tag in einer Datei mit dem Namen generiert) `DailyBackup.zip`), das die Berichtsdefinitionen enthält. Die tägliche Sicherung umfasst die wichtigsten Ordner und Pakete, die mit dem Produkt geliefert werden. Das Verzeichnis „Meine Ordner“ und alle Verzeichnisse, die Sie außerhalb der obersten Produktordner erstellen, sind nicht im Cognos-Backup enthalten.

Aufgrund der Art und Weise, wie Insight die Dateien in benennt `.zip` Datei, zeigen einige Entpackprogramme, dass die Datei leer ist, wenn sie geöffnet wird. So lange wie die `.zip` Die Datei hat eine Größe größer als 0 und endet nicht mit einem `.bad` Erweiterung, die `.zip` Datei ist gültig. Sie können die Datei mit einem anderen Entpackprogramm wie 7-Zip oder WinZip® öffnen.

## Backup benutzerdefinierter Berichte und Artefakte in Berichten

Wenn Sie benutzerdefinierte Berichte in einer Version von Insight vor 7.0 erstellt haben und ein Upgrade auf die neueste Insight Version durchführen möchten, sollten Sie vor der Upgrade-Installation ein Backup Ihrer Berichte erstellen und Artefakte melden und diese nach der Upgrade-Installation wiederherstellen. Achten Sie auch auf die Ordner, die Sie zum Speichern von Berichtsartefakten verwenden.

### Über diese Aufgabe

Wenn Sie Änderungen an den vordefinierten Berichten vorgenommen haben, erstellen Sie Ihre eigenen Kopien dieser Berichte in einem separaten Ordner. Auf diese Weise überschreiben Sie Ihre Änderungen nicht, wenn Sie die vordefinierten Artefakte aktualisieren.

Wenn Sie Berichte im Bereich „Meine Ordner“ haben, sollten Sie sie in die Ordner „Benutzerdefinierte Berichte“ kopieren, damit sie nicht verloren gehen.

## Wiederherstellen der Data Warehouse-Datenbank

Sie können eine Data Warehouse-Datenbank mithilfe des wiederherstellen `.zip` Datei, die beim Sichern dieser Data Warehouse-Datenbank erstellt wurde.

### Über diese Aufgabe

Wenn Sie eine Data Warehouse-Datenbank wiederherstellen, haben Sie die Möglichkeit, auch Benutzerkontoinformationen aus dem Backup wiederherzustellen. Benutzerverwaltungstabellen werden von der Data Warehouse-Berichtsengine in einer reinen Data Warehouse-Installation verwendet.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Backup/Restore**.

3. Klicken Sie im Abschnitt **Datenbank und Berichte wiederherstellen** auf **Durchsuchen**, und suchen Sie den `.zip` Datei, die das Data Warehouse-Backup enthält.
4. Wenn Sie Berichte oder Benutzerkontodaten wiederherstellen möchten, aktivieren Sie eines oder beide der folgenden Kontrollkästchen:
   - **Datenbank wiederherstellen**

     Enthält Data Warehouse-Einstellungen, Data Marts, Verbindungen und Benutzerkontoinformationen.
   - **Berichte wiederherstellen**

     Umfasst benutzerdefinierte Berichte, vordefinierte Berichte, Änderungen an vordefinierten Berichten und Berichtseinstellungen, die Sie im Reporting Portal erstellt haben.

   > Wenn Ihr Datenbankbackup einen benutzerdefinierten Bericht enthält, der einen Schrägstrich (/) oder eine offene Klammer ([) im Namen hat (z. B. US IT Center Switch Port Boston/Juli), wird der Bericht durch den Wiederherstellungsvorgang umbenannt und der Schrägstrich oder die offene Klammer durch einen Unterstrich ersetzt (z. B. US IT Center Switch Port Boston_Juli).
5. Klicken Sie Auf **Wiederherstellen**.

   Nach Abschluss des Wiederherstellungsvorgangs wird unter der Schaltfläche Wiederherstellen eine Meldung angezeigt. Wenn die Wiederherstellung erfolgreich war, wird die Meldung erfolgreich angezeigt. Wenn die Wiederherstellung fehlschlägt, meldet die Meldung die spezifische Ausnahme, die den Fehler verursacht hat. Wenn eine Ausnahme auftritt und der Wiederherstellungsprozess fehlschlägt, wird die ursprüngliche Datenbank automatisch zurückgesetzt.

## Einrichtung mehrerer Mandanten in Berichten

OnCommand Insight Data Warehouse unterstützt in der Berichterstellung mehrere Mandanten (oft verkürzt auf „`mmulti-Tenancy`“ oder „`multimandancy`“), da Sie Benutzer einer oder mehreren Geschäftseinheiten zuordnen können. Mit dieser Funktion können Administratoren Daten oder Berichte nach Benutzerattributen oder Benutzerzugehörigkeit trennen.

Geschäftseinheiten nutzen eine Hierarchie für die Kapazitätszuordnung und verwenden dabei die folgenden Werte:

- Mandant: Wird in erster Linie von Service-Providern verwendet, um Ressourcen einem Kunden zuzuordnen, z. B. NetApp.
- Geschäftsbereich (Line of Business, Lob): Ein Geschäftsbereich innerhalb eines Unternehmens, z. B. „Hardware“ oder „Software“.
- Business Unit: Eine traditionelle Geschäftseinheit wie „Sales“ oder „Marketing“.
- Projekt: Ein Projekt, dem Sie möglicherweise Kapazitätszuordnung zuweisen möchten.

Der Prozess der Konfiguration mehrerer Mandanten umfasst die folgenden wichtigen Schritte:

- Konfigurieren Sie ein Data Warehouse-Benutzerkonto.
- Erstellen Sie eine Gruppe im Reporting Portal.

- Weisen Sie Benutzern eine oder mehrere Gruppen zu, die für Geschäftseinheiten stehen.
- Weisen Sie einem oder mehreren Geschäftseinheiten Benutzer zu. Beispiel: Benutzer, die mit „NetApp“ verknüpft sind, erhalten Zugriff auf alle Geschäftseinheiten, die über „`NetApp`“ als Mandant verfügen.
- Testen Sie, ob Benutzer nur die Berichte sehen können, die sie sehen sollten.

Die folgenden Punkte fassen zusammen, wie Benutzer auf Berichtsdaten zugreifen:

- Ein Benutzer, der keiner Gruppe zugewiesen ist, erhält Zugriff auf alle Daten.
- Ein Benutzer, der einer Gruppe zugewiesen ist, kann ohne eine Geschäftseinheit keinen Zugriff auf Datensätze erhalten.

Beispielsweise könnten Sie über die folgenden Abteilungen verfügen und müssen Berichte für Benutzer in diesen Abteilungen trennen.

| Benutzer | Engineering | Unterstützung | Finanzen | Legal |
|---|---|---|---|---|
| Benutzer1 | X | X | | |
| Benutzer2 | | | X | X |
| Benutzer3 | | X | | |

#### Benutzerkonten werden konfiguriert

Sie müssen mehrere Schritte ausführen, um Benutzerkonten zu konfigurieren.

##### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Benutzerverwaltung**.
3. Konfigurieren Sie jedes Benutzerkonto.

#### Zuweisen von Benutzern zu Geschäftseinheiten

Sie müssen eine Reihe von Schritten ausführen, um Benutzer Business Entities zuzuweisen. Data Warehouse unterstützt in der Berichterstellung mehrere Mandanten (oft verkürzt auf „`mmulti-Tenancy`“ oder „`multimandancy`“), da Sie Benutzer einer oder mehreren Geschäftseinheiten zuordnen können. So können Administratoren Daten oder Berichte je nach Benutzerattributen oder Benutzerzugehörigkeit trennen.

##### Schritte

1. Melden Sie sich beim Data Warehouse Portal als Administrator unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Reporting Portal zu öffnen.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.

4. Wählen Sie im Menü Start die Option **IBM Cognos Administration**.
5. Klicken Sie auf die Registerkarte **Sicherheit**:
6. Wählen Sie im Verzeichnis **Cognos** aus.
7. Erstellen Sie einen neuen Unterordner im Cognos-Ordner mit dem Namen „`BES`“ für Geschäftseinheiten.
8. Öffnen Sie den BES-Ordner.
9. Klicken Sie auf das Symbol **Neue Gruppe**, um Gruppen hinzuzufügen, die unterschiedlichen Berechtigungsstufen entsprechen.

   Diese Berechtigungsstufen können entweder den vollständigen Namen der Geschäftseinheit (z. B. NetApp.N/A) oder ein Präfix (z. B. NetApp.N/A. Finance) sein. In beiden Formaten erhalten Sie den Zugriff auf alle Projekte innerhalb der Geschäftseinheit (NetApp.N/A.Finance).

   Der Assistent Neue Gruppe wird angezeigt.
10. Füllen Sie die Seiten des Assistenten aus.
11. Wählen Sie eine Geschäftseinheit aus und klicken Sie auf **Mehr**.
12. Klicken Sie auf **set members**.
13. Klicken Sie Auf **Hinzufügen**.
14. Wählen Sie das SANscreen-Verzeichnis aus.
15. Wählen Sie aus der Liste der Benutzer jeden Benutzer aus, der in die Business-Einheit aufgenommen werden soll, und fügen Sie den Benutzer dem Feld Ausgewählte Einträge hinzu.
16. Klicken Sie auf **OK**.
17. Wiederholen Sie den Vorgang, bei dem jeder der Business-Entity-Gruppen Mitglieder hinzugefügt werden.

## Fehlerbehebung bei Setup-Problemen

Es gibt mehrere häufige Probleme mit Anmerkungen, Builds und Berichten, die Sie während der Einrichtung haben können. Sie können diese Probleme beheben, indem Sie die beschriebenen Schritte ausführen.

#### Warum ich meine Anmerkungen nicht sehen kann

Wenn Sie Anmerkungen in Data Warehouse nicht sehen können, müssen Sie möglicherweise eine Aktualisierung der Anmerkungen erzwingen und dann ein Data Warehouse Build starten.

Fehlende Anmerkungen beeinflussen die Art und Weise, wie Daten in das Data Warehouse importiert und in den Berichten angezeigt werden. Wenn beispielsweise die Anmerkung „`Tier`“ nicht verfügbar ist, können Sie Speichersysteme in Data Warehouse-Berichten nicht nach Ebene gruppieren.

##### Erzwingen einer Aktualisierung von Anmerkungen für Data Warehouse

Sie können eine Aktualisierung der Anmerkungen von OnCommand Insight in Data Warehouse initiieren.

### Über diese Aufgabe

Sie können Anmerkungen mit einer der beiden Optionen aktualisieren:

- Einschließlich gelöschter Objekte: Dies umfasst Daten über Geräte, die nicht mehr vorhanden sind, wie Hosts, Speicher-Arrays oder Switches, die entfernt wurden. Dies ist erforderlich, wenn Sie Data Warehouse-Daten mit historischen Datenpunkten erstellen möchten.
- Gelöschte Objekte nicht eingeschlossen: Wählen Sie diese Option, wenn Sie gelöschte Objekte ausschließen möchten.

### Schritte

1. Melden Sie sich beim OnCommand Insight-Portal als Administrator an `https://hostname`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight installiert ist.
2. Klicken Sie auf **Admin** > **Troubleshooting**. Klicken Sie unten auf der Seite auf **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Registerkarte **Aktionen** auf **DWH-Anmerkungen aktualisieren (gelöscht einbeziehen)**.

#### Generieren eines manuellen Data Warehouse-Builds

Nach dem Erzwingen einer Aktualisierung von Anmerkungen (Ausführen transienter Daten) in OnCommand Insight müssen Sie ein Data Warehouse Build initiieren. Sie können bis zum nächsten geplanten Build warten oder jetzt einen Build starten.

### Schritte

1. Melden Sie sich als Administrator beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan**.
3. Klicken Sie auf **Build now**.

#### Benutzerdefinierte Anmerkungen werden in Data Warehouse importiert

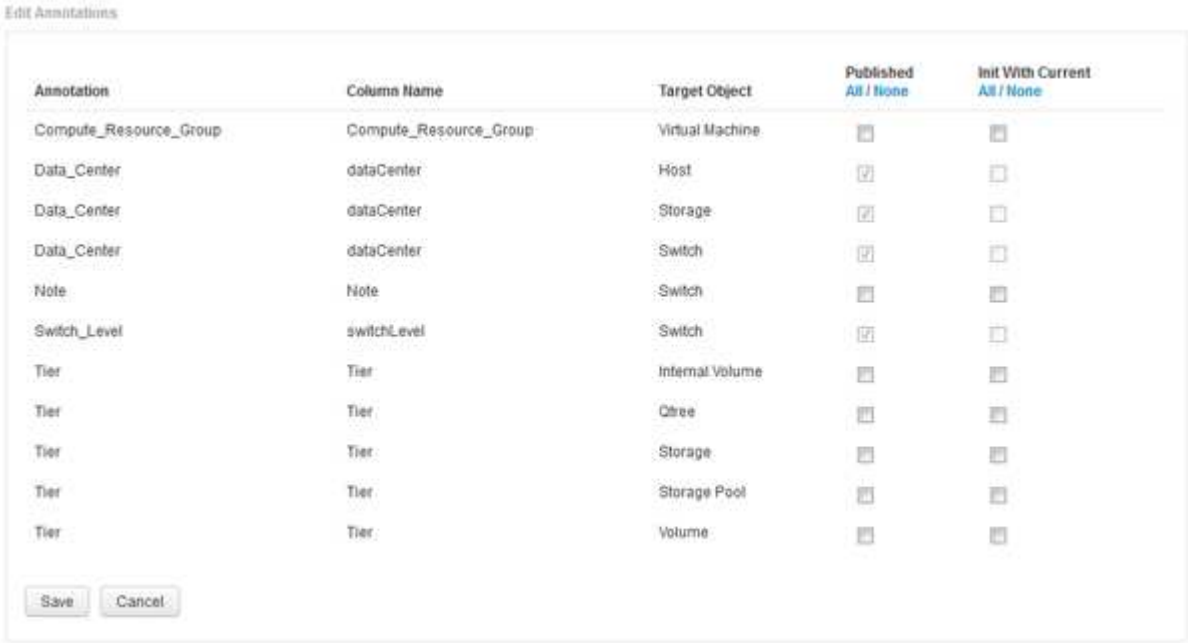
Nachdem Sie eine Aktualisierung der Anmerkungen in OnCommand Insight erzwungen haben, müssen Sie die gewünschten Anmerkungen in Data Warehouse auswählen und einen Data Warehouse Build starten. Sie können bis zum nächsten geplanten Build warten oder jetzt einen Build starten.

### Schritte

1. Melden Sie sich als Administrator beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Anmerkungen**.

Die Liste zeigt eine Zeile für jeden Anmerkungstyp und ein Zielobjekt an, dem die Anmerkung zugeordnet werden kann. Ein Häkchen in der Spalte Veröffentlicht zeigt an, dass die Anmerkung bereits für das bestimmte Zielobjekt ausgewählt wurde und bereits über die Data Warehouse Data Marts verfügbar ist.

3. Klicken Sie auf **Bearbeiten**, um zu bearbeiten, wie Anmerkungen aus OnCommand Insight importiert werden.




4. Gehen Sie wie folgt vor, um den Anmerkungsprozess zu bearbeiten:
   - Wählen Sie **Veröffentlicht**, um aus OnCommand Insight abgerufene Anmerkungen in die Data Warehouse-Datenbank hinzuzufügen. Klicken Sie auf **Alle**, um alle Anmerkungen auf allen Objekten auszuwählen. Klicken Sie auf **Keine**, um sicherzustellen, dass keine Optionen ausgewählt sind.

Deaktivieren Sie diese Option, um die Anmerkungsspalte aus der Bestandstabelle des jeweiligen Objekts und den zugehörigen Datentabellen zu entfernen. Wenn benutzerdefinierte Berichte Anmerkungsdaten verwenden, werden die Berichte nicht erfolgreich ausgeführt.

◦ Aktivieren Sie **Init with Current**, um historische Daten in Data Warehouse-Dimensionstabellen mit dem aktuellen Anmerkungswert zu initialisieren. Klicken Sie auf **Alle**, um alle Anmerkungen auf allen Objekten auszuwählen. Klicken Sie auf **Keine**, um sicherzustellen, dass keine Optionen ausgewählt sind. Dieses Kontrollkästchen ist deaktiviert, nachdem eine Anmerkung veröffentlicht wurde. Das Kontrollkästchen ist für nicht veröffentlichte Anmerkungen aktiviert. Wenn beispielsweise ein Host mit dem Anmerkungstyp „`floor`“ beschriftet wird und den Wert „`1`“ erhält und in der Tabelle Host_Dimension 3 Zeilen für diesen Host vorhanden sind, wird bei Auswahl von **Init with Current** der Wert „`1`“ in der Spalte „`floor`“ für alle 3 Zeilen in der Tabelle Host_Dimension zugeordnet. Wenn **Init with Current** nicht ausgewählt ist, wird nur die letzte Zeile für diesen Host den Wert „`1`“ in der Spalte „Floor“ haben.

5. Klicken Sie Auf **Speichern**.

   Eine Warnmeldung wird angezeigt, die darauf hinweist, dass dadurch Änderungen an der Struktur der Daten oder Datenverlust verursacht werden, wenn Sie Anmerkungen entfernen.

6. Klicken Sie auf **Ja**, um fortzufahren.

   Data Warehouse initiiert einen Job mit asynchronen Anmerkungen, der die angeforderten Änderungen anwendet. Sie können den Job auf der Seite Jobs anzeigen. Sie können auch die Änderungen im Data Warehouse-Datenbankschema sehen.

#### Was tun mit fehlgeschlagenen historischen Build-Punkten

Sie können aus dem Verlauf erstellen, indem Sie die Option **Historie überspringen Build-Fehler** aktivieren, um fehlgeschlagene Builds zu vermeiden.

Wenn Sie dies tun, wird der Build aus der Geschichte fortgesetzt. Wenn ein Build fehlschlägt und diese Option aktiviert ist, setzt Data Warehouse die Erstellung fort und ignoriert alle fehlgeschlagenen Builds. In solchen Fällen gibt es keinen Datenpunkt in den historischen Daten für übersprungene Builds. Wenn Sie diese Option nicht aktivieren und das Build fehlschlägt, werden alle nachfolgenden Jobs abgebrochen.

# Administrative Aufgaben, die Sie mit Data Warehouse durchführen können

OnCommand Insight Data Warehouse ist eine webbasierte Benutzeroberfläche, über die Benutzer Daten in OnCommand Insight Data Warehouse konfigurieren und Fehler beheben und Zeitpläne für den Abruf von Daten aus OnCommand Insight einrichten können.

Mit dem Data Warehouse-Portal können Sie die folgenden administrativen Aufgaben ausführen:

- Überprüfen Sie den Status aktueller Jobs oder Abfragen, die ausgeführt werden
- Verwalten von Anmerkungen
- Konfigurieren Sie E-Mail-Benachrichtigungen
- Aufrufen und Erstellen von benutzerdefinierten Berichten
- Überprüfung der Data Warehouse-Dokumentation und des Datenbankschemas
- Bearbeiten Sie den Standortnamen
- Identifizieren Sie die Data Warehouse-Version und den Upgrade-Verlauf

- Erstellen Sie die Data Warehouse-Daten aus dem Verlauf
- Die Data Warehouse-Datenbank zurücksetzen
- Sichern Sie die Data Warehouse-Datenbank und stellen Sie sie wieder her
- Beheben Sie Fehler bei Data Warehouse-Problemen und sehen Sie sich OnCommand Insight-Protokolle an
- Benutzerkonten verwalten

## Verwalten von Jobs

Sie können eine Liste der aktuellen Jobs und deren Status anzeigen. Der erste Job in einem Build-Zyklus ist fett gedruckt. Das Build, das Data Warehouse für jeden Konnektor und für jeden Data Mart ausführt, wird als Job betrachtet.

### Über diese Aufgabe

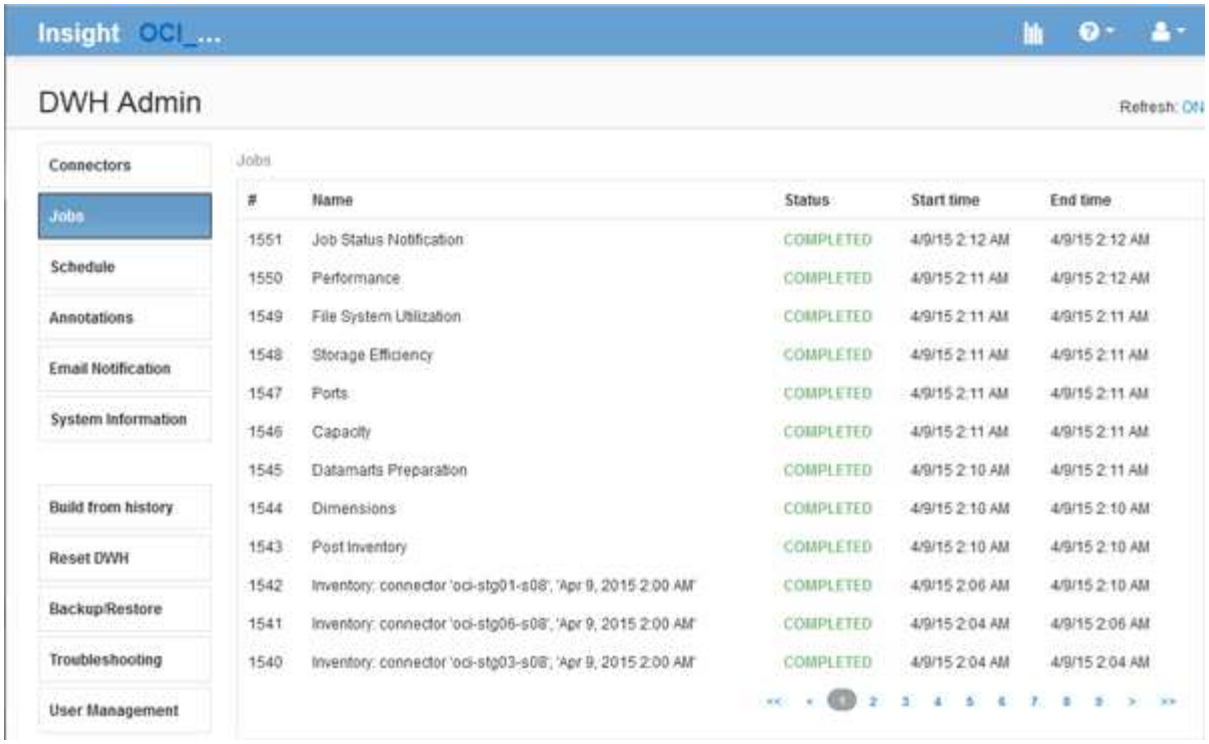
Sie können alle ausstehenden Aufträge abbrechen, die Sie geplant oder begonnen haben. Sie können auch den Verlauf der zuvor ausgeführten Jobs löschen. Sie können den Verlauf von Jobs löschen, die nicht ausstehen, ausgeführt werden oder gerade abgebrochen werden. Sie können den gesamten Verlauf oder den gesamten Verlauf außer den letzten 24 Stunden löschen, um alle Einträge außer dem letzten Tag zu entfernen.

Sie können Informationen zu den folgenden Jobtypen sehen: Lizenz, Vorbestand, Inventar, Nachbestand, Abmessungen, Datenvorbereitung, Kapazität, Ports, Speichereffizienz, Auslastung Des Dateisystems, Leistung, Job Status Notification, History Build, dynamische Anmerkungen, Connector entfernen, Build, Phone Home und Maintenance wurden übersprungen.

Ein Wartungsauftrag wird wöchentlich ausgeführt und verwendet MySQL-Tools zur Optimierung der Datenbank.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Jobs**.




Wenn der Status „Ausstehend“ angezeigt wird, wird ein Link zum Abbrechen angezeigt.

3. Um einen ausstehenden Auftrag abzubrechen, klicken Sie auf **Abbrechen**.
4. Um den Job-Verlauf zu entfernen, klicken Sie auf **Alle** oder **Alle außer letzte 24h**.

## Überwachung des Zustands von Data Warehouses

Das Data Warehouse (DWH) umfasst eine Systemzustandsüberwachung, die Informationen zum Status der DWH anzeigt. Alarmmeldungen werden auf den Seiten **Connectors** und **Jobs** des DWH angezeigt und an den angeschlossenen Insight-Server gesendet, wo sie auf der Seite **Admin** > **Health** angezeigt werden.

Das DWH sammelt alle zehn Minuten Messwerte und zeigt unter folgenden Bedingungen einen Alarm an:

- Die Verbindung zum Insight Server ist unterbrochen
- Festplattenauslastung liegt über 90 %
- Der Dienst Reporting (Cognos) ist ausgefallen
- Eine Abfrage hält eine Sperre auf einem beliebigen Tisch für eine längere Zeit
- Ein Wartungsauftrag ist deaktiviert
- Die automatische Sicherung ist deaktiviert
- Sicherheitsrisiko: Standardmäßige Verschlüsselungsschlüssel erkannt

Warnungen der Systemzustandsüberwachung im Data Warehouse können bis zu 30 Tage lang unterdrückt werden.

Wenn die E-Mail-Benachrichtigung aktiviert ist, werden diese Ereignisse auch per E-Mail gemeldet. Beachten Sie, dass die E-Mail keine Anhänge enthält.

Diese Ereignisse werden im protokolliert `dwh_troubleshoot.log` Datei an folgenden Speicherorten:

- Windows: `<install dir>\SANscreen\Wildfly\Standalone\Logs`
- Linux `/var/log/netapp/oci/wildfly/`

## Planung täglicher Builds

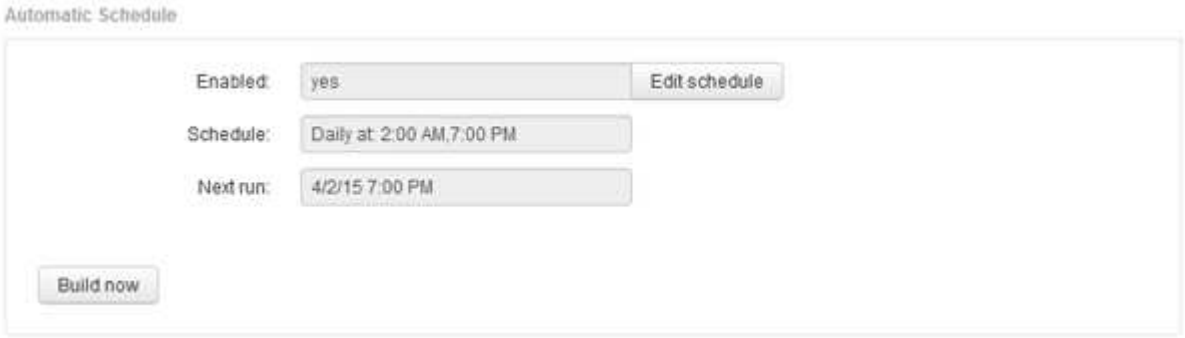
Obwohl Sie das Data Warehouse manuell erstellen können, indem Sie das Steuerelement Build NOW jederzeit verwenden, empfiehlt es sich, automatische Builds zu planen und zu definieren, wann und wie oft die Data Warehouse-Datenbank erstellt werden soll. Data Warehouse führt einen Build-Job für jeden Konnektor und für jeden Data Mart durch. Data Warehouse führt einen Build-Job für jeden Konnektor für Lizenzen und Inventar aus, und alle anderen Build-Jobs (z. B. Kapazität) werden auf der konsolidierten Datenbank ausgeführt.

### Über diese Aufgabe

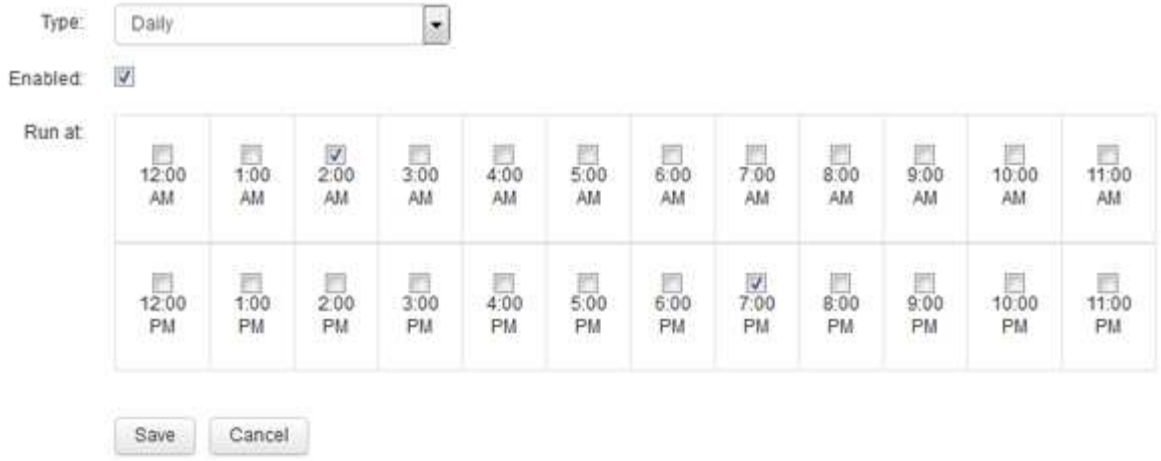
Jedes Mal, wenn das Data Warehouse erstellt wird, führt es einen Bestandsauftrag für jeden Konnektor aus. Nachdem die Bestandsaufnahmeaufträge abgeschlossen sind, führt Data Warehouse Jobs für Abmessungen, Kapazität und die übrigen Datentabellen durch.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan bearbeiten**.




3. Klicken Sie im Dialogfeld **Build Schedule** auf **Edit**, um einen neuen Zeitplan hinzuzufügen.




4. Wählen Sie die Frequenz - wöchentlich.
5. Wählen Sie die Uhrzeit für jeden Tag aus, an dem der Job ausgeführt werden soll.
6. Wählen Sie N/A für Tage aus, die Sie nicht ausführen möchten.
7. Um den Zeitplan zu aktivieren, wählen Sie **aktiviert**.

   Wenn Sie diese Option nicht aktivieren, wird der Zeitplan nicht erstellt.

8. Klicken Sie Auf **Speichern**.
9. Um Data Warehouse außerhalb des automatischen geplanten Builds zu erstellen, klicken Sie auf **Build now**.

## Konfigurieren eines wöchentlichen Zeitplans

Obwohl Sie das Data Warehouse manuell erstellen können, indem Sie das Steuerelement Build NOW jederzeit verwenden, empfiehlt es sich, automatische Builds zu planen und zu definieren, wann und wie oft die Data Warehouse-Datenbank erstellt werden soll. Data Warehouse führt einen Build-Job für jeden Konnektor und für jeden Data Mart durch. Data Warehouse führt einen Build-Job für jeden Konnektor für Lizenzen und Inventar aus, und alle anderen Build-Jobs (z. B. Kapazität) werden auf der konsolidierten Datenbank ausgeführt. Mit einem wöchentlichen Zeitplan können Sie festlegen, wann der Build für jeden Wochentag ausgeführt werden soll.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan bearbeiten**.
3. Wählen Sie die Frequenz - wöchentlich.
4. Wählen Sie die Uhrzeit für jeden Tag aus, an dem der Job ausgeführt werden soll.
5. Wählen Sie N/A für Tage aus, die Sie nicht ausführen möchten.
6. Um den Zeitplan zu aktivieren, wählen Sie **aktiviert**.

Wenn Sie diese Option nicht aktivieren, wird der Zeitplan nicht erstellt.

7. Klicken Sie Auf **Speichern**.
8. Um Data Warehouse außerhalb des automatischen geplanten Builds zu erstellen, klicken Sie auf **Build now**.

## Planen täglicher Backups

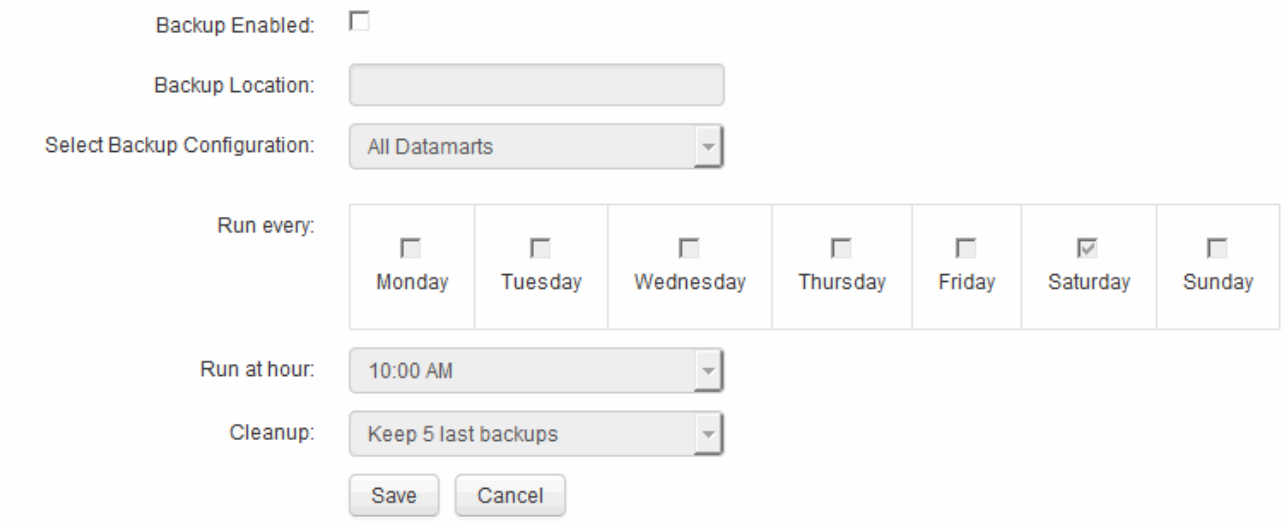
Obwohl Sie das Data Warehouse manuell mithilfe der Steuerung Backup/Wiederherstellung jederzeit sichern können, empfiehlt es sich, automatische Backups zu planen und zu definieren, wann und wie oft das Backup der Data Warehouse-Datenbank und des Cognos-Content-Speichers durchgeführt werden soll. Backups schützen vor Datenverlust, sodass Sie bei Bedarf die Data Warehouse-Datenbank wiederherstellen können. Sie verwenden auch ein Backup, wenn Sie zu einem neuen Data Warehouse-Server migrieren oder auf eine neue Data Warehouse-Version aktualisieren.

### Über diese Aufgabe

Die Planung von Backups in Zeiten, in denen der Data Warehouse-Server nicht ausgelastet ist, verbessert die Backup-Performance und verringert die Auswirkungen auf Benutzer.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Zeitplan**.
3. Klicken Sie im Dialogfeld **Sicherungsplan** auf **Bearbeiten**, um einen neuen Zeitplan hinzuzufügen.




4. Um die geplanten Backups zu aktivieren, wählen Sie **Backup aktiviert**.
5. Geben Sie den Speicherort an, an dem die Sicherungsdateien gespeichert werden sollen.
6. Geben Sie die zu sichernden Daten an.

7. Geben Sie den Tag oder die Tage an, an denen die Sicherung durchgeführt werden soll.
8. Geben Sie an, zu welcher Tageszeit das Backup gestartet werden soll.
9. Geben Sie an, wie viele frühere Backup-Kopien Sie behalten möchten.
10. Klicken Sie Auf **Speichern**.

## Ausführen von benutzerdefinierten Skripts in Data Warehouse

Mit Data Warehouse können Kunden Jobs erstellen, mit denen benutzerdefinierte Skripte ausgeführt werden können, die benutzerdefinierte Daten in Data Warehouse vorbereiten.

### Bevor Sie beginnen

Um zu verhindern, dass das benutzerdefinierte Skript während einer Data Warehouse-Aktualisierung gelöscht wird, dürfen Sie das Skript nicht im SANscreen-Verzeichnis speichern.

### Über diese Aufgabe

Der Job kann nur ein Skript angeben. Sie können mehrere Skripts und Befehle von einem Skript ausführen.

### Schritte

1. Wählen Sie in Data Warehouse **DWH Admin** > **Schedule** aus.
2. Aktivieren Sie das Kontrollkästchen **Script enabled**.
3. Geben Sie den absoluten Pfad des Skriptnamens in das Textfeld **Script Location** ein.
4. Klicken Sie Auf **Speichern**.

### Ergebnisse

Die Job Engine des Data Warehouse plant die Ausführung eines Jobs „`Custom Scripting`“. Der Job wird nach einer ETL ausgeführt und andere widersprüchliche Hintergrundprozesse werden vermieden. Der Job wird nicht von einer Operation „`aus Historie erstellen`“ ausgeführt.

## Was Sie mit Anmerkungen tun können

Anmerkungen bieten eine Methode zum Definieren von Informationen, die sich auf Objekte in Ihrer Umgebung beziehen, und ermöglichen Ihnen dann, Objekte basierend auf der Anmerkung zu verfolgen. Beispielsweise können Sie Geräten in Ihrer Umgebung Gebäude- oder Bodennummernkommentare hinzufügen und anschließend eine Abfrage erstellen, die alle Geräte im ersten Stock eines Datacenters zurückgibt.

Darüber hinaus können Sie sich alle Geräte eines bestimmten Datacenters oder einer Geschäftseinheit ansehen und ermitteln, welche Geschäftseinheit den meisten Tier-1-Storage verwendet. Dazu weisen Sie dem Gerät über die Web-UI von OnCommand Insight eine Anmerkung zu Datacentern, Unternehmenseinheiten oder Ebenen zu. Anschließend können Sie ausgewählte benutzerdefinierte Anmerkungen aus OnCommand Insight in das Data Warehouse übertragen. Dies soll dazu führen, dass die dem Objekt zugewiesenen Anmerkungswerte in Ihren benutzerdefinierten Berichten angezeigt werden.

Sie können festlegen, welche benutzerdefinierten Anmerkungen an das Data Warehouse übertragen werden. Anmerkungen werden als zusätzliche Spalten zur Objekttabelle im Inventar und zur entsprechenden

Dimensionstabelle in den Datentabellen hinzugefügt. Wenn Sie die Anmerkungen zu Ressourcen über die OnCommand Insight-Benutzeroberfläche aktualisieren und das nächste Data Warehouse-Build starten oder warten, werden die Ergebnisse in den folgenden Tabellen angezeigt:

- dwh_Inventory.annotation_value
- dwh_Inventory.Object_to_annotation

Um sicherzustellen, dass in OnCommand Insight eingegebene Anmerkungen in Data Warehouse enthalten sind, sind die folgenden wichtigen Prozesse erforderlich:

- Bevor Sie Anmerkungen in das Data Warehouse importieren, müssen Sie sicherstellen, dass sie in OnCommand Insight vorbereitet werden.

  Dazu können Sie die Option **Troubleshooting** > **Aktualisierung von Anmerkungen für Data Warehouse** manuell ausführen oder bis zum nächsten geplanten transienten Datenlauf warten. Wenn Sie die Aktualisierung von Anmerkungen erzwingen, erzwingen Sie, dass der OnCommand Insight-Server die transienten Daten (z. B. Anmerkungswerte) berechnet und in Datenbanktabellen platziert, damit der Data Warehouse ETL-Prozess die Daten lesen kann. Die Aktualisierung der Beschriftungsdaten erfolgt automatisch alle 15 Minuten. Sie können sie jedoch häufiger ausführen.

- Anschließend importieren Sie Anmerkungen in Data Warehouse mithilfe der Option Data Warehouse **Anmerkungen**.
- Wenn Sie Anmerkungen in Berichte aufnehmen möchten, die Sie mithilfe der Berichterstellungs-Tools des OnCommand Insight Reporting Portals erstellen, müssen Sie das Metadatenmodell für die OnCommand Insight-Berichterstellung aktualisieren.

Wenn Sie ein Data Warehouse aktualisieren, wird der Job mit Anmerkungen während der Wiederherstellung der Datenbank automatisch ausgeführt. Der Anmerkungsjob wird auch automatisch ausgeführt, wenn WildFly gestartet wird.

WildFly ist ein Anwendungsserver, auf dem der OnCommand Insight-Java-Code ausgeführt wird und sowohl für den OnCommand Insight-Server als auch für das Data Warehouse benötigt wird.

#### Anmerkungen werden in OnCommand Insight vorbereitet

## Anmerkungen müssen in OnCommand Insight vorbereitet werden, bevor sie in das Data Warehouse importiert werden können.

##### Schritte

1. Melden Sie sich beim OnCommand Insight-Portal als Administrator an `https://hostname`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight installiert ist.
2. Klicken Sie auf **Admin** > **Troubleshooting**. Klicken Sie unten auf der Seite auf **Erweiterte Fehlerbehebung**.
3. Klicken Sie auf der Registerkarte **Aktionen** auf **DWH-Anmerkungen aktualisieren (gelöscht einbeziehen)**.

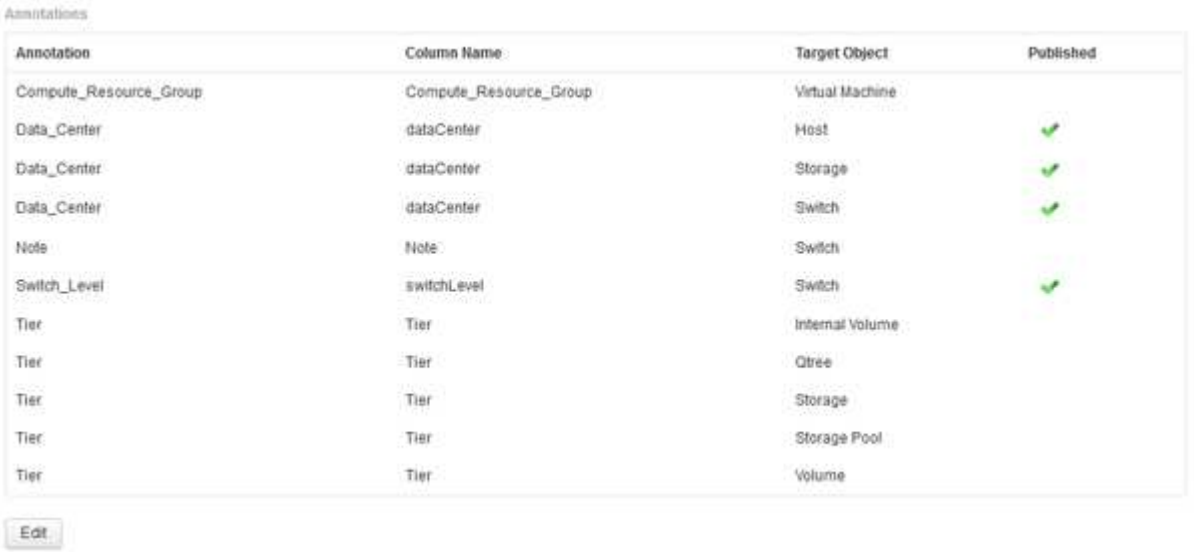
#### Benutzerdefinierte Anmerkungen werden in Data Warehouse importiert

## Nachdem Sie eine Aktualisierung der Anmerkungen in OnCommand Insight erzwungen haben, müssen Sie die gewünschten Anmerkungen in Data Warehouse auswählen und

einen Data Warehouse Build starten. Sie können bis zum nächsten geplanten Build warten oder jetzt einen Build starten.

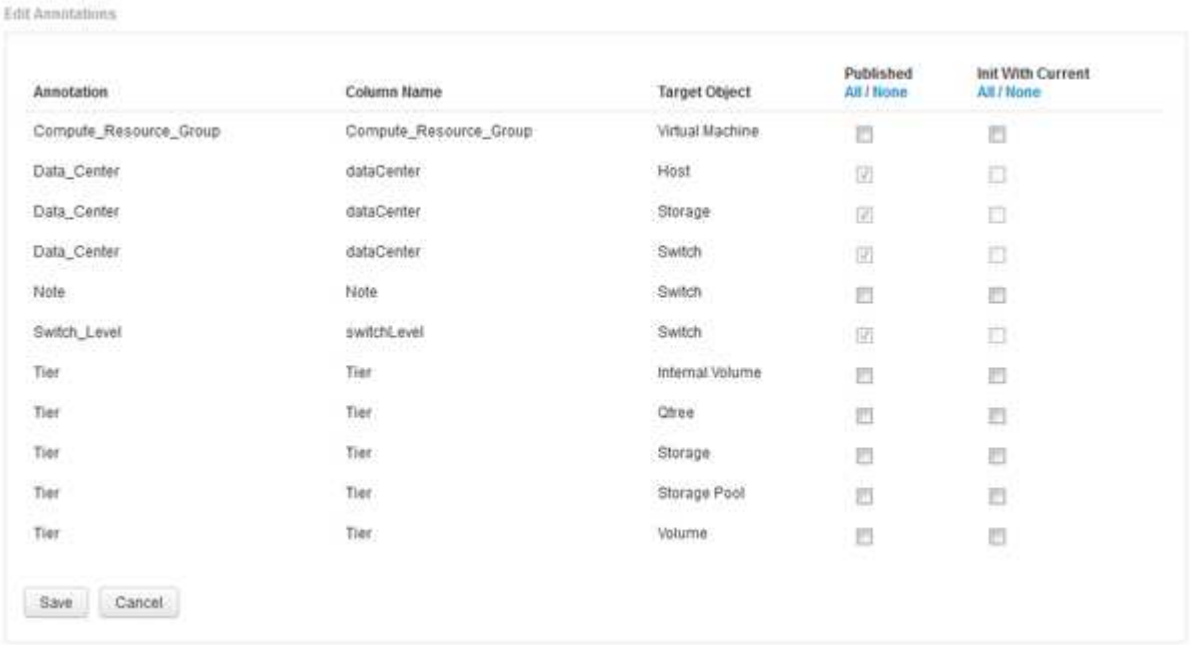
**Schritte**

1. Melden Sie sich als Administrator beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Anmerkungen**.




Die Liste zeigt eine Zeile für jeden Anmerkungstyp und ein Zielobjekt an, dem die Anmerkung zugeordnet werden kann. Ein Häkchen in der Spalte Veröffentlicht zeigt an, dass die Anmerkung bereits für das bestimmte Zielobjekt ausgewählt wurde und bereits über die Data Warehouse Data Marts verfügbar ist.

3. Klicken Sie auf **Bearbeiten**, um zu bearbeiten, wie Anmerkungen aus OnCommand Insight importiert werden.




4. Gehen Sie wie folgt vor, um den Anmerkungsprozess zu bearbeiten:

- Wählen Sie **Veröffentlicht**, um aus OnCommand Insight abgerufene Anmerkungen in die Data Warehouse-Datenbank hinzuzufügen. Klicken Sie auf **Alle**, um alle Anmerkungen auf allen Objekten auszuwählen. Klicken Sie auf **Keine**, um sicherzustellen, dass keine Optionen ausgewählt sind.

  Deaktivieren Sie diese Option, um die Anmerkungsspalte aus der Bestandstabelle des jeweiligen Objekts und den zugehörigen Datentabellen zu entfernen. Wenn benutzerdefinierte Berichte Anmerkungsdaten verwenden, werden die Berichte nicht erfolgreich ausgeführt.

- Aktivieren Sie **Init with Current**, um historische Daten in Data Warehouse-Dimensionstabellen mit dem aktuellen Anmerkungswert zu initialisieren. Klicken Sie auf **Alle**, um alle Anmerkungen auf allen Objekten auszuwählen. Klicken Sie auf **Keine**, um sicherzustellen, dass keine Optionen ausgewählt sind. Dieses Kontrollkästchen ist deaktiviert, nachdem eine Anmerkung veröffentlicht wurde. Das Kontrollkästchen ist für nicht veröffentlichte Anmerkungen aktiviert. Wenn beispielsweise ein Host mit dem Anmerkungstyp „`floor`“ beschriftet wird und den Wert „`1`“ erhält und in der Tabelle Host_Dimension 3 Zeilen für diesen Host vorhanden sind, wird bei Auswahl von **Init with Current** der Wert „`1`“ in der Spalte „`floor`“ für alle 3 Zeilen in der Tabelle Host_Dimension zugeordnet. Wenn **Init with Current** nicht ausgewählt ist, wird nur die letzte Zeile für diesen Host den Wert „`1`“ in der Spalte „Floor“ haben.

5. Klicken Sie Auf **Speichern**.

   Eine Warnmeldung wird angezeigt, die darauf hinweist, dass dadurch Änderungen an der Struktur der Daten oder Datenverlust verursacht werden, wenn Sie Anmerkungen entfernen.

6. Klicken Sie auf **Ja**, um fortzufahren.

   Data Warehouse initiiert einen Job mit asynchronen Anmerkungen, der die angeforderten Änderungen anwendet. Sie können den Job auf der Seite Jobs anzeigen. Sie können auch die Änderungen im Data Warehouse-Datenbankschema sehen.

### Anzeigen des Jobs mit Anmerkungen in der Liste Jobs

Sie können den Job Anmerkungen in der Liste Jobs anzeigen und die Änderungen der Anmerkungen auf Data Warehouse Data Marts anwenden.

#### Schritte

1. Melden Sie sich als Administrator beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Jobs**.

### Anzeigen von Anmerkungsänderungen im Datenbankschema

Das Datenbankschema spiegelt die Änderungen in der spezifischen Tabelle wider.

#### Über diese Aufgabe

Wenn Sie beispielsweise Anmerkungen zu einem Speicher-Array hinzufügen, werden diese in der Speicher- oder Schaltertabelle im Inventar oder anderen Data Marts angezeigt.

Wenn Sie die Anmerkungen zu Ressourcen über die OnCommand Insight-Benutzeroberfläche aktualisieren und den nächsten Data Warehouse-Build starten oder warten, wird eine neue Spalte im entsprechenden

Objekt in Inventory (dwh_Inventory) und in der entsprechenden Dimensionstabelle hinzugefügt oder entfernt (In der entsprechenden Datentabelle). Die Ergebnisse werden in den folgenden Tabellen angezeigt:

- dwh_Inventory.annotation_value
- dwh_Inventory.Object_to_annotation

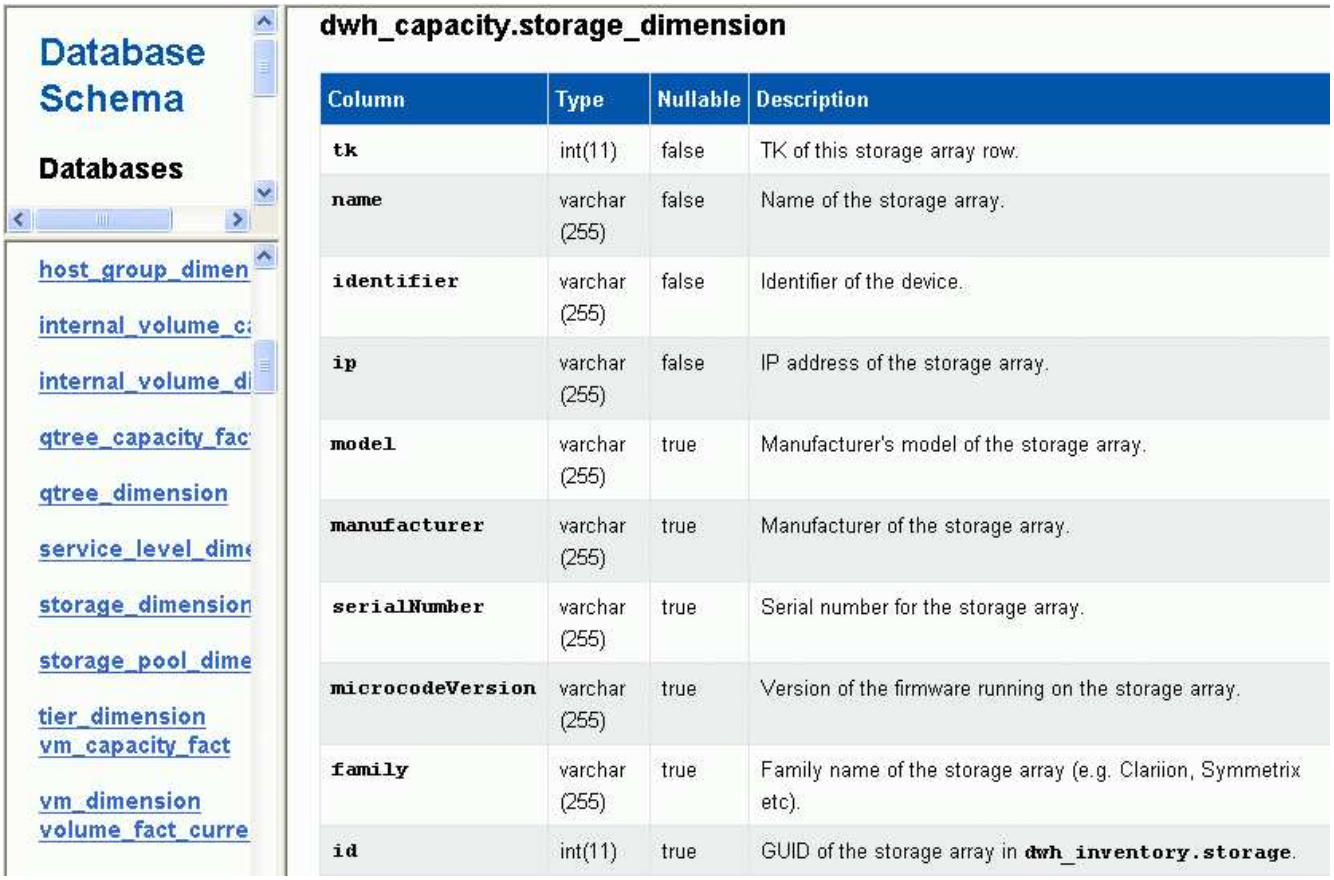
#### Schritte

1. Klicken Sie Auf Klicken Sie in der Data Warehouse-Symbolleiste auf **Dokumentation**.
2. Wählen Sie **Datenbankschema**.
3. Blättern Sie im Bereich **Datenbankschema** links zum Abschnitt **DWH_INVENTORY** und klicken Sie auf **Switch**.

**dwh_inventory.switch**

| Column | Type | Nullable | Description |
|---|---|---|---|
| **id** | int(11) | false | GUID of the switch. |
| **fabricId** | int(11) | true | GUID of the fabric on which this switch is configured to operate.<br>References:<br>• **id** in dwh_inventory.fabric |
| **identifier** | varchar (255) | false | Identifier of the device. |
| **wwn** | varchar (255) | false | WWN of the switch. |
| **ip** | varchar (255) | false | IP address of the switch. |
| **Name** | varchar (255) | false | Name of the switch. |
| **Manufacturer** | varchar (255) | true | Manufacturer of the switch |
| **Model** | varchar (255) | true | Manufacturer's model of the switch. |
| **Firmware** | varchar (255) | true | Firmware version running on the switch. |

4. Die Tabelle **dwh_Inventory.Switch** spiegelt die Änderungen wider:




**dwh_capacity.storage_dimension**

| Column | Type | Nullable | Description |
|---|---|---|---|
| **tk** | int(11) | false | TK of this storage array row. |
| **name** | varchar (255) | false | Name of the storage array. |
| **identifier** | varchar (255) | false | Identifier of the device. |
| **ip** | varchar (255) | false | IP address of the storage array. |
| **model** | varchar (255) | true | Manufacturer's model of the storage array. |
| **manufacturer** | varchar (255) | true | Manufacturer of the storage array. |
| **serialNumber** | varchar (255) | true | Serial number for the storage array. |
| **microcodeVersion** | varchar (255) | true | Version of the firmware running on the storage array. |
| **family** | varchar (255) | true | Family name of the storage array (e.g. Clariion, Symmetrix etc). |
| **id** | int(11) | true | GUID of the storage array in **dwh_inventory.storage**. |

Die Spalte mit den Anmerkungen zum Rechenzentrum wird in der Tabelle Storage_Dimensions angezeigt.

## Einstellen von E-Mail-Benachrichtigungen

Sie können Data Warehouse E-Mails an eine bestimmte E-Mail-Adresse senden lassen, wenn Data Warehouse-Jobs nicht erfolgreich abgeschlossen werden.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **E-Mail-Benachrichtigung**.
3. Geben Sie Folgendes ein:
   - SMTP-Serveradresse

     Gibt den Server an, der als SMTP-Server in Ihrer Organisation fungiert. Er wird entweder mit einem Hostnamen oder mit einer IP-Adresse im Format nnn.nnn.nnn.nnn identifiziert. Wenn Sie einen Hostnamen angeben, stellen Sie sicher, dass DNS ihn auflösen kann.

   - Benutzername und Kennwort des SMTP-Servers

     Gibt den Benutzernamen für den Zugriff auf den E-Mail-Server an und ist nur erforderlich, wenn der SMTP-Server einen Benutzer zum Anmelden am Server benötigt. Dies ist derselbe Benutzername, mit dem Sie sich bei der Anwendung anmelden und auf Ihre E-Mail zugreifen.

- Benachrichtigungen aktiviert

  **Ja** aktiviert die Benachrichtigungen; **Nein** deaktiviert die Benachrichtigungen.

- E-Mail des Absenders

  Gibt die E-Mail-Adresse an, die zum Senden der Benachrichtigungen verwendet wird. Dies muss eine gültige E-Mail-Adresse in Ihrem Unternehmen sein.

- E-Mail-Adresse des Empfängers

  Gibt die E-Mail-Adresse oder die Adressen der Person oder der Personen an, die die E-Mail immer erhalten. Trennen Sie mehrere Adressen durch Kommas.

- E-Mail-Betreff

  Gibt den Betreff für die Benachrichtigung an.

- E-Mail-Signatur

  Gibt die Informationen an, die unten in der E-Mail angezeigt werden, z. B. den Abteilungsnamen.

## Zugriff auf das Reporting Portal

Über das Data Warehouse Portal können Sie auf das Reporting Portal zugreifen, wo Sie mit Tools zur Berichterstellung wie Workspace Advanced und Report Studio benutzerdefinierte Berichte erstellen können.

### Schritte

1. Klicken Sie in der Symbolleiste Data Warehouse auf Um das Insight Reporting Portal zu öffnen.
2. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.

## Anzeigen der Dokumentation des Data Warehouse-Datenbankschemas

Sie können die Schemainformationen der Data Warehouse-Datenbank überprüfen.

### Schritte

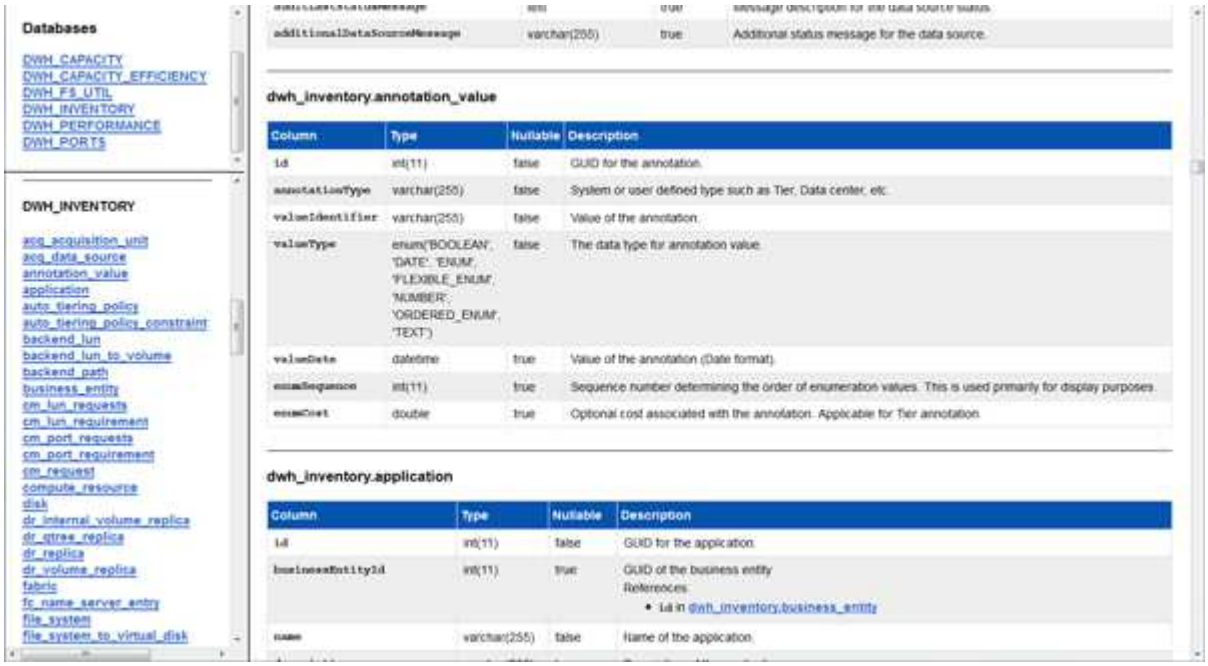
1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie in der Symbolleiste Data Warehouse auf Und wählen Sie **Schema**.

## Anzeigen des Data Warehouse-Datenbankschemas

Sie können das Datenbankschema anzeigen, um zu verstehen, wie die Daten in einer anderen API verwendet werden oder um SQL-Abfragen zu entwickeln. Die Schemaoption listet alle Datenbanken, Tabellen und Spalten im Schema auf. Sie können auch die Datenbankschemamdiagramme mit den Tabellenbeziehungen überprüfen.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie Auf Wählen Sie in der Data Warehouse-Symbolleiste **Dokumentation**.
3. Wählen Sie **Datenbankschema**.
4. Klicken Sie beispielsweise im Bereich **Databases** auf **DWH_INVENTORY**.
5. Blättern Sie im Bereich **Alle Tabellen** nach unten zum Abschnitt **DWH_INVENTORY**, und klicken Sie auf die Tabelle **annotation_value**.




Die Tabelle dwh_Inventory.Annotation wird angezeigt.

## Anzeigen von Systeminformationen

Sie können System-, Modul-, Lizenz- und Data Warehouse-Upgrade-Informationen anzeigen.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Systeminformationen**.
3. Überprüfen Sie auf der Registerkarte **System** die Systeminformationen, und bearbeiten Sie ggf. den Standortnamen, indem Sie die folgenden Schritte ausführen:
   a. Klicken Sie Auf **Standortnamen Bearbeiten**
   b. Geben Sie den neuen Standortnamen ein und klicken Sie auf **Speichern**.
4. Um Informationen zur Anwendung (Anwendungsname, Modul, Version und Installationsdatum) anzuzeigen, klicken Sie auf die Registerkarte **Anwendungsinfo**.

5. Um Lizenzinformationen (Protokoll, Code, Ablaufdatum und Menge) anzuzeigen, klicken Sie auf die Registerkarte **Lizenzen**.
6. So zeigen Sie Informationen zum Anwendungsupgrade an (Anwendungsname, von Datum, bis Datum, Uhrzeit, Benutzer, Und Dateigröße), klicken Sie auf **Aktualisierungsverlauf**.

## Erweiterte Optionen

Data Warehouse umfasst verschiedene erweiterte Optionen.

#### Fehlgeschlagene Builds werden übersprungen

Nach dem ersten Build kann es manchmal zu einem erfolglosen Build kommen. Um sicherzustellen, dass alle Jobs nach einem erfolglosen Build erfolgreich abgeschlossen wurden, können Sie die Option **Historie überspringen Fehler erstellen** aktivieren.

##### Über diese Aufgabe

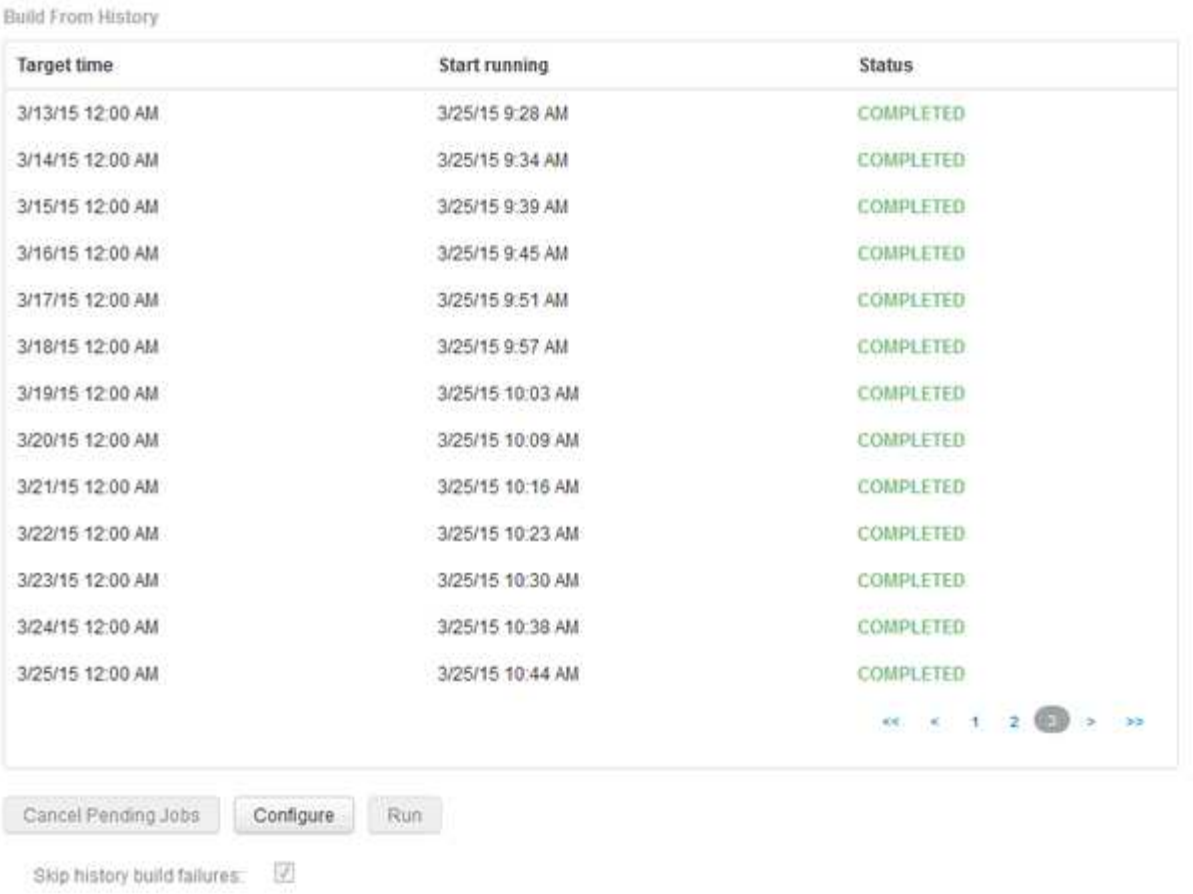
Wenn ein Build fehlschlägt und die Option **Historie überspringen Buildfehler** aktiviert ist, setzt Data Warehouse die Erstellung fort und ignoriert alle fehlgeschlagenen Builds. In diesem Fall gibt es in den historischen Daten keinen Datenpunkt für übersprungene Builds.

Verwenden Sie diese Option nur, wenn der Build nicht erfolgreich war.

Wenn ein Build in Build from History fehlschlägt und das Kontrollkästchen **Historie überspringen Buildfehler** nicht aktiviert ist, werden alle nachfolgenden Jobs abgebrochen.

##### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Build from history**.




3. Klicken Sie Auf **Konfigurieren**.
4. Konfigurieren Sie den Build.
5. Klicken Sie Auf **Speichern**.
6. Um fehlgeschlagene Builds zu überspringen, aktivieren Sie **Fehler beim Erstellen des Verlaufs überspringen**.

   Sie können dieses Kontrollkästchen nur sehen, wenn die Schaltfläche **Run** aktiviert ist.

7. Um einen Build außerhalb des automatischen geplanten Builds auszuführen, klicken Sie auf **Ausführen**.

#### Zurücksetzen der Data Warehouse-Datenbank oder des Reporting-Servers

Sie können den Inhalt der Data Warehouse Data Marts löschen und alle konfigurierten Konnektoren löschen. Sie können dies tun, wenn eine Installation oder ein Upgrade nicht erfolgreich abgeschlossen wurde und die Data Warehouse-Datenbank in einem Zwischenzustand belassen wurde. Sie können auch nur das Bestandsdatenmodell oder das Cognos Reporting-Datenmodell löschen.

##### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **DWH-Datenbank zurücksetzen**.
3. Klicken Sie auf eine der folgenden Optionen:

- **DWH-Datenbank zurücksetzen**

  Dadurch werden die Inhalte aller Data Warehouse Data Marts und aller konfigurierten Konnektoren gelöscht und das Data Warehouse wird ohne benutzerdefinierte Konfigurationen in den Standard-Installationszustand versetzt. Sie können diese Option wählen, wenn Sie zum Beispiel Ihre verbundenen Server geändert haben, aber versehentlich eine andere Data Warehouse-Datenbank auf Ihrem Server wiederhergestellt haben und in einen standardmäßig installierten Zustand zurückkehren müssen. Dadurch werden keine Berichte gelöscht. (Berichte werden im Cognos Content Store gespeichert.)

- **Nur Lagerbestand Zurücksetzen**

  Dadurch wird nur der Inhalt des Bestandsdatenmodells gelöscht. Dadurch werden keine historischen Daten gelöscht.

- **Berichtsinhalt Zurücksetzen**

  Dadurch wird der Inhalt des Reporting-Servers zurückgesetzt. Dadurch werden alle benutzerdefinierten Berichte gelöscht, die Sie möglicherweise haben. Sichern Sie Ihre Berichte, bevor Sie diese Option wählen.

Eine Warnmeldung wird angezeigt.

4. Klicken Sie auf **Ja**, um fortzufahren.

#### Wiederherstellen und Aktualisieren von Berichten für Versionen vor 6.3

## Wenn Sie ein Upgrade einer Insight-Version vor Version 6.3 durchführen, müssen Sie Artefakte in der Berichterstellung manuell wiederherstellen.

##### Bevor Sie beginnen

Befolgen Sie die Anweisungen unter „Aktualisieren des Data Warehouse (DWH)“ und „Sichern von benutzerdefinierten Berichten und Berichten von Artefakten“.

##### Schritte

1. Um Reporting-Artefakte aus Versionen vor Version 6.3 wiederherzustellen, kopieren Sie die Datei Export Backup.zip, die Sie im erstellt und gespeichert haben `<install>\cognos\c10_64\deployment` Verzeichnis.
2. Öffnen Sie einen Browser, und gehen Sie zu `http://<server>:<port>/reporting` Für den Server und Port, den Sie bei der Installation verwendet haben.
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein und klicken Sie auf **Login**.
4. Wählen Sie im Menü **Start** die Option **Insight Reporting Administration**.
5. Klicken Sie auf die Registerkarte **Konfiguration**.

   Aufgrund von Änderungen im Datenmodell werden die Berichte in den alten Paketen möglicherweise nicht ausgeführt und müssen aktualisiert werden.

6. Klicken Sie Auf **Content Administration**.
7. Klicken Sie auf die Schaltfläche **Neuer Import**.
8. Stellen Sie sicher, dass Sie das Archiv in das Bereitstellungsverzeichnis kopiert haben (z. B.

`backup6.0.zip`) Ausgewählt ist, und klicken Sie auf **Weiter**.

9. Wenn Sie ein Passwort zum Schutz des Archivs eingegeben haben, geben Sie das Passwort ein und klicken Sie auf **OK**.
10. Ändern Sie den Namen `Export...` Bis `Import Backup` Und klicken Sie auf **Weiter**.
11. Klicken Sie auf das Bleistiftsymbol neben jedem Paketnamen und geben Sie ggf. einen neuen Zielnamen ein. Fügen Sie beispielsweise einen hinzu `_original` Suffix auf den vorhandenen Namen. Klicken Sie dann auf **OK**.
12. Nachdem Sie die Zielpaketnamen für alle Pakete umbenannt haben, wählen Sie alle blauen Ordner aus und klicken Sie auf **Weiter**, um fortzufahren.
13. Alle Standardwerte übernehmen.
14. Klicken Sie auf **Finish** und wählen Sie dann **Run**.
15. Überprüfen Sie die Details dieses Imports und klicken Sie auf **OK**.
16. Klicken Sie auf **Aktualisieren**, um den Status des Imports anzuzeigen.
17. Klicken Sie nach dem Import auf **Schließen**.

#### Ergebnisse

Auf der Registerkarte Öffentliche Ordner werden zwei Pakete angezeigt. Beispiel: Einer mit einem `7.0` Suffix (für die neuere Version) und eines mit einem `_original` (Oder was auch immer Sie während des Sicherungs-/Wiederherstellungsvorgangs eingegeben haben) Suffix, das Ihre alten Berichte enthält. Aufgrund von Änderungen im Datenmodell werden die Berichte in den alten Paketen möglicherweise nicht ausgeführt und müssen aktualisiert werden. Ihre Portalregisterkarten zeigen nun auf die aktuelle Version der Portalseiten.

### Zugriff auf MySQL über die Befehlszeilenschnittstelle

Zusätzlich zum Zugriff auf Data Warehouse-Datenelemente über die Tools zur Berichterstellung können Sie direkt über eine Verbindung als MySQL-Benutzer auf Data Warehouse-Datenelemente zugreifen. Sie können sich als MySQL-Benutzer verbinden, um die Datenelemente in Ihren eigenen Anwendungen zu verwenden.

#### Über diese Aufgabe

Es gibt viele Möglichkeiten, sich zu verbinden. Die folgenden Schritte zeigen einen Weg.

Stellen Sie beim Zugriff auf MySQL eine Verbindung zur MySQL-Datenbank auf dem Rechner her, auf dem Data Warehouse installiert ist. Der MySQL-Port ist standardmäßig 3306; Sie können ihn jedoch während der Installation ändern. Der Benutzername und das Passwort sind dwhuser/netapp123.

#### Schritte

1. Öffnen Sie auf dem Rechner, auf dem Data Warehouse installiert ist, ein Befehlszeilenfenster.
2. Greifen Sie im OnCommand Insight-Verzeichnis auf das MySQL-Verzeichnis zu.
3. Geben Sie den folgenden Benutzernamen und das folgende Kennwort ein: `mysql -udwhuser -pnetapp123`

   Je nachdem, wo Data Warehouse installiert ist, wird Folgendes angezeigt:

```
c:\Program Files\SANscreen\mysql\bin> mysql -udwhuser -pnetapp123
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 882
Server version: 5.1.28-rc-community MySQL Community Server (GPL)
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

4. Anzeigen der Data Warehouse-Datenbanken: `show databases;`

   Folgendes wird angezeigt:

```
mysql> show databases;
+--------------------------+
| Database                 |
+--------------------------+
| information_schema       |
| dwh_capacity             |
| dwh_capacity_efficiency  |
| dwh_fs_util              |
| dwh_inventory            |
| dwh_performance          |
| dwh_ports                |
+--------------------------+
```

#### Fehlerbehebung Bei Data Warehouse

## Sie können verschiedene Aufgaben im Zusammenhang mit der Fehlerbehebung bei Data Warehouse ausführen.

- Verwenden Sie OnCommand Insight ASUP.
- Anzeigen von OnCommand Insight-Protokollen
- Beheben von Problemen im Zusammenhang mit Upgrades und Geschäftseinheiten.
- Beheben von Problemen im Zusammenhang mit der Konsolidierung mehrerer OnCommand Insight-Server

Sie können mehrere OnCommand Insight Server in derselben Data Warehouse-Datenbank konsolidieren. In vielen Konfigurationen wird dasselbe Objekt von mehreren Konnektoren gemeldet (d. h., derselbe Switch existiert in zwei OnCommand Insight-Instanzen). In solchen Fällen konsolidiert Data Warehouse die mehrere Objekte in einem (ein primärer Konnektor wird ausgewählt und die Daten des Objekts werden nur von diesem Konnektor übernommen).

Der Speicheradministrator kann auf der Seite Fehlerbehebung Probleme im Zusammenhang mit Konsolidierungsproblemen beheben.

# Sie können ASUP-Protokolle an den technischen Support senden, um Hilfe bei der Fehlerbehebung zu erhalten. ASUP für Data Warehouse wird für die automatische Ausführung konfiguriert. Im Data Warehouse Portal können Sie den automatischen Sendevorgang deaktivieren, ein Backup der Data Warehouse-Datenbank einschließen oder eine Übertragung an ASUP initiieren.

Die Informationen in den Protokollen werden mithilfe des HTTPS-Protokolls an den technischen Support weitergeleitet. Es werden keine Daten über ASUP weitergeleitet, es sei denn, Sie haben sie zuerst auf dem Insight Server konfiguriert.

Data Warehouse sendet die Protokolle an den OnCommand Insight-Server, der der erste Konnektor ist, der auf der Seite Data Warehouse Portal Connectors aufgeführt ist. Der automatische Prozess sendet die folgenden Dateien:

- Data Warehouse-Protokolle, die Folgendes umfassen:
  - boot.log (mit Backups)
  - dwh.log (einschließlich Backups wie dwh.log.1)
  - dhw_troubleshoot.log
  - dwh_upgrade.log (mit Backups)
  - WildFly.log (mit Backups)
  - ldap.log (mit Backups)
  - SQL-Dump der Data Warehouse Management-Datenbank
  - mysql: My.cnf, .err und langsame Abfrageprotokolle
  - Voller innodb-Status
- Cognos-Protokolle, die Folgendes enthalten:
  - cognos-logs.zip

    Enthält die Cognos-Protokolldateien aus dem `<install>\cognos\c10_64\logs` Verzeichnis. Es enthält auch die von Cognos generierten Protokolle sowie die OnCommand InsightAP.log-Datei, die alle Protokolle von Benutzern enthält, die sich an und aus OnCommand Insight-Berichten anmelden.
  - DailyBackup.zip

    Enthält die Sicherung der Reporting-Artefakte in den öffentlichen Ordnern. Der Inhalt von „Meine Ordner“ ist hier nicht enthalten.
  - cognos`_version_site name_`content_store.zip

    Enthält eine vollständige Sicherung des Cognos Content Store.

Sie können einen Fehlerbehebungsbericht manuell erstellen. Die ZIP-Datei für den Fehlerbehebungsbericht enthält die folgenden Data Warehouse-Informationen:

- boot.log (mit Backups)
- dwh.log (einschließlich Backups wie dwh.log.1)

- dwh_upgrade.log (mit Backups)
- wildfly.log (mit Backups)
- ldap.log (mit Backups)
- Dump-Dateien in c:\Program Files\SANscreen\wildfly\Standalone\log\dwh\
- SQL-Dump der Data Warehouse Management-Datenbank
- mysql: My.cnf, .err und langsame Abfrageprotokolle
- Voller innodb-Status

ASUP sendet nicht automatisch eine Sicherung der OnCommand Insight-Datenbank an den technischen Support.

#### Deaktivieren der automatischen ASUP-Übertragung

Alle NetApp Produkte sind mit automatisierten Funktionen ausgestattet, die den bestmöglichen Support bei der Fehlerbehebung in Ihrer Umgebung gewährleisten. ASUP sendet in regelmäßigen Abständen vordefinierte, spezifische Informationen an den Kunden-Support. ASUP ist standardmäßig für Data Warehouse aktiviert. Sie können es jedoch deaktivieren, wenn die Informationen nicht mehr gesendet werden sollen.

**Schritte**

1. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
2. Klicken Sie auf **Disable**, um zu verhindern, dass ASUP einen täglichen Bericht sendet.

   Es wird eine Meldung angezeigt, die besagt, dass ASUP deaktiviert ist.

#### Einschließlich einer Sicherung der Data Warehouse-Datenbank

Standardmäßig sendet ASUP nur die Data Warehouse-Protokolldateien an den technischen Support zur Unterstützung bei der Fehlerbehebung. Sie können jedoch auch wählen, ob Sie ein Backup der Data Warehouse-Datenbank einschließen und den Typ der gesendeten Daten auswählen möchten.

**Schritte**

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
3. Um festzulegen, dass ASUP ein Backup der Data Warehouse-Datenbank enthalten soll, klicken Sie auf die Liste **DWH-Datenbanksicherung einbeziehen** und wählen Sie eine der folgenden Optionen für den Datentyp aus, den das Backup enthalten soll:
   - Alle (inkl. Performance)
   - Alle Außer Leistung
   - Nur Inventar
4. Klicken Sie Auf **Aktualisieren**.

#### Senden von Insight Protokollen an ASUP

Sie können ASUP-Protokolle an den technischen Support senden, um Hilfe bei der Fehlerbehebung zu erhalten. ASUP für Data Warehouse wird für die automatische Ausführung konfiguriert. Im Data Warehouse-Portal können Sie den automatischen Sendevorgang deaktivieren, ein Backup der Data Warehouse-Datenbank aufnehmen oder eine Übertragung an ASUP initiieren. Wenn Sie einen ASUP-Bericht anfordern, wird die Berichtsanfrage auf der Seite Jobs im Data Warehouse-Portal als Job angezeigt.

##### Über diese Aufgabe

Der Job wird von der Jobwarteschlange verwaltet, ähnlich wie die Verarbeitung anderer Jobs. Wenn ein ASUP Job bereits den Status Ausstehend oder ausgeführt hat, wird eine Fehlermeldung angezeigt, die angibt, dass die ASUP Berichtsanforderung der Jobanforderung nicht hinzugefügt werden kann, da die Jobwarteschlange ausstehende oder laufende Anforderungen enthält.

##### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt **OnCommand Insight ASUP** auf der Seite **Fehlerbehebung** auf **DWH-Problembehandlungs-Bericht herunterladen**, um den Problembehebungsbericht abzurufen.
4. Um den Bericht an den OnCommand Insight-Server zu senden, der als erster Konnektor auf der Seite Data Warehouse Portal **Connectors** aufgeführt ist, klicken Sie auf **Jetzt senden**.

#### Anzeigen von OnCommand Insight-Protokollen

Sie können verschiedene Data Warehouse- und Cognos-Protokolle in OnCommand Insight anzeigen.

##### Über diese Aufgabe

Sie können Fehlerbehebungs- und Statusinformationen in Cognos- und Data Warehouse-Protokolldateien untersuchen.

##### Schritte

1. Melden Sie sich beim Data Warehouse-Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt **Logs** auf **Log Files**.

   Die folgenden Protokolldateien werden angezeigt:

| | |
|---|---|
| dwh.log | |
| Listet den Status von Data Warehouse-Jobs auf | |

| | |
|---|---|
| wildfly.log | |
| Stellt Informationen über den WildFly-Anwendungsserver bereit | |
| dwh_Upgrade-Protokoll | |
| Enthält Informationen zum Upgrade auf Data Warehouse | |
| ldap.log | |
| Protokolliert Nachrichten im Zusammenhang mit der LDAP-Authentifizierung | |
| dwh_troubleshoot.log | |
| Protokolliert Meldungen, die bei der Fehlerbehebung von DWH-Problemen helfen können | |
| sanscreenap.log | |
| Bietet Informationen über die Verbindung zum Server, Authentifizierung und Zugriff auf das Cognos-Repository sowie Informationen über andere Prozesse | |
| cognosserver.log | |
| Cognos-Protokoll | |

4. Klicken Sie auf den Namen der Protokolldatei, die Sie anzeigen möchten.

#### Probleme bei der Konsolidierung mehrerer Server-Chassis

Sie können die Konnektoren anzeigen, die Hosts und Adapter sowie SAN-Switches und Speicher-Arrays berichten. Sie können auch die verschiedenen Konnektoren sehen, die über ein Objekt berichten, und den primären Konnektor identifizieren, den Konnektor, der für das Objekt ausgewählt wurde.

### Anzeigen von Problemen mit der Konsolidierung von Hosts und Adaptern

Die gemeldeten Daten für Hosts und ihre zugehörigen Adapter werden aus dem Inventory Data Mart abgeleitet.

#### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster links auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt **Gehäusekonsolidierung** auf **Hosts und Adapter**.

Die in diesem Beispiel dargestellte Konfiguration ist keine gültige Konfiguration. Principal und Available Connectors auf localhost legen nahe, dass Insight Server und DWH auf demselben Server installiert sind. In diesem Beispiel möchten wir Sie mit der Konsolidierungspabelle vertraut machen.

Hosts and Adapters Consolidation

Filter

| Host GUID | Host Name | Host IP | Adapter GUID | Adapter WWN | Principal Connector | Available Connectors | Insight ID | Insight Change Time |
|---|---|---|---|---|---|---|---|---|
| 288 | Agassi | 192.1.168.71 | | | localhost (1) | localhost (1) | 9927 | 11/18/10 1:36 PM |
| | | | 576 | 40:A0:00:00:00:00:00:84 | localhost (1) | localhost (1) | 9928 | 11/18/10 1:36 PM |
| | | | 577 | 40:A0:00:00:00:00:00:85 | localhost (1) | localhost (1) | 9930 | 11/18/10 1:36 PM |
| 305 | Al_Host1 | 192.1.168.88 | | | localhost (1) | localhost (1) | 12254 | 11/18/10 1:38 PM |
| | | | 597 | 40:A0:00:00:00:00:01:05 | localhost (1) | localhost (1) | 12255 | 11/18/10 1:38 PM |
| 306 | Al_Host2 | 192.1.168.89 | | | localhost (1) | localhost (1) | 12257 | 11/18/10 1:38 PM |
| | | | 598 | 40:A0:00:00:00:00:01:06 | localhost (1) | localhost (1) | 12258 | 11/18/10 1:38 PM |
| 307 | Al_Host3 | 192.1.168.90 | | | localhost (1) | localhost (1) | 12260 | 11/18/10 1:38 PM |

Für alle Hosts und Adapter gibt es eine Zeile für jeden Connector, der über sie berichtet, sowie den primären Connector, von dem der Host und der Adapter genommen werden. Nur für Hosts und Adapter können für einen Host, der von einem Anschluss gemeldet wird, seine Adapter von einem anderen Anschluss gemeldet werden.

Sie sehen auch die OnCommand Insight-Änderungszeit eines Hosts/Adapters für jeden Anschluss. Mit diesem Parameter können Sie ermitteln, wann ein Update in OnCommand Insight für den Host/Adapter erfolgt ist und wann derselbe Host/Adapter auf anderen OnCommand Insight-Servern aktualisiert wurde.

4. Optional können Sie Daten in dieser Ansicht filtern, indem Sie einen Teil des Textes eingeben und auf **Filter** klicken. Um den Filter zu löschen, löschen Sie den Text im Feld **Filter** und klicken Sie auf **Filter**. Sie können nach Host-Name, Host-IP, Adapter-WWN oder OnCommand Insight-Objekt-ID filtern.

   Der Filter ist Groß-/Kleinschreibung beachten.

5. Überprüfen Sie die folgenden Daten:

- **Host-GUID**

  Global Unique Identifier für diesen konsolidierten Gerätetyp (Hosts)

- **Hostname**

  Name des konsolidierten Hosts, wie er im Data Warehouse angezeigt wird

- **Host-IP**

  IP-Adresse des konsolidierten Hosts

- **Adapter-GUID**

  Globale eindeutige Kennung für den Host-Adapter

- **Adapter WWN**

  WWN des Host-Adapters

- **Principal Connector**

  Der Name des OnCommand Insight-Connectors, der die eigentliche Datenquelle war

- **Verfügbare Anschlüsse**

  Alle OnCommand Insight-Anschlüsse, auf denen sich der konsolidierte Host/Adapter befindet

- **Insight-ID**

  OnCommand Insight-ID des konsolidierten Hosts/Adapters für den entsprechenden Reporting Connector

- * Insight Change Time*

  Wenn in OnCommand Insight ein Update für den Host/Adapter erfolgt ist und derselbe Host/Adapter auf anderen OnCommand Insight-Servern aktualisiert wurde

6. Klicken Sie auf den Anschluss, um Details zum Anschluss zu erhalten.

   Die folgenden Informationen für den Anschluss werden angezeigt:

   - Host-Name
   - Das letzte Mal, wenn ein Data Warehouse-Job auf diesem Connector ausgeführt wurde
   - Das letzte Mal, wenn eine Änderung von diesem Konnektor empfangen wurde
   - Die Version des OnCommand Insight-Servers, auf die dieser Connector verweist

**Anzeigen von Problemen bei der Konsolidierung von Speicher-Arrays**

Die gemeldeten Daten für Speicher-Arrays werden aus dem Inventory Data Mart abgeleitet. Für alle Speicher-Arrays gibt es eine Zeile für jeden Connector, der über sie berichtet, sowie den primären Connector, von dem jedes Array genommen wird.

**Schritte**

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt **Gehäusekonsolidierung** auf **SAN-Speicher-Arrays**.
4. Um Daten in dieser Ansicht zu filtern, geben Sie optional einen Teil des Textes in das Filterfeld ein und klicken auf **Filter**. Um den Filter zu löschen, löschen Sie den Text im Feld Filter und klicken Sie auf **Filter**. Sie können nach Speichername, Speicher-IP, Anbietermodell oder OnCommand Insight-Objekt-ID filtern.

   Der Filter ist Groß-/Kleinschreibung beachten.

5. Überprüfen Sie die folgenden Daten:
   - **GUID**

     Global Unique Identifier für diesen konsolidierten Gerätetyp (Speicher-Array)

   - **Name**

     Name des konsolidierten Speicherarrays, wie er im Data Warehouse angezeigt wird

   - **IP**

     IP-Adresse des konsolidierten Speicher-Arrays

   - **Hersteller und Modell**

     Name des Anbieters, der das konsolidierte Speicher-Array verkauft, und Modellnummer des Herstellers

   - **Principal Connector**

     Der Name des OnCommand Insight-Connectors, der die eigentliche Datenquelle war

   - **Verfügbare Anschlüsse**

     Alle OnCommand Insight-Connectors, in denen sich das konsolidierte Storage-Array befindet

   - **Insight-ID**

     ID des konsolidierten Speicher-Arrays auf dem OnCommand Insight-Gehäuse, in dem sich der Hauptanschluss befindet

   - * Insight Change Time*

     Wenn in OnCommand Insight ein Update für das Speicher-Array durchgeführt wurde und dasselbe Speicher-Array auf anderen OnCommand Insight-Servern aktualisiert wurde

**Anzeigen von Problemen mit der Konsolidierung von Switches**

Die gemeldeten Daten für Switches werden aus dem Inventory Data Mart abgeleitet. Für alle Switches gibt es eine Zeile für jeden Anschluss, der über sie berichtet, sowie den primären Anschluss, aus dem jeder Switch entnommen wird.

**Schritte**

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie vom Navigationsfenster links auf**Fehlersuche**.
3. Klicken Sie im Abschnitt **Gehäusekonsolidierung** auf **SAN-Switches**.
4. Optional können Sie Daten in dieser Ansicht filtern, indem Sie einen Teil des Textes eingeben und auf **Filter** klicken. Um den Filter zu löschen, deaktivieren Sie das Filterfeld und klicken Sie auf **Filter**. Sie können nach Switch-Name, Switch-IP, Anbietermodell oder OnCommand Insight-Objekt-ID filtern.

   Der Filter ist Groß-/Kleinschreibung beachten.

5. Überprüfen Sie die folgenden Daten:
   - **GUID**

     Global Unique Identifier für diesen konsolidierten Gerätetyp (Speicher-Array)

   - **Name**

     Name des konsolidierten Speicher-Arrays, wie er im Data Warehouse angezeigt wird

   - **IP**

     IP-Adresse des konsolidierten Speicher-Arrays

   - **Hersteller und Modell**

     Name des Anbieters, der das konsolidierte Speicher-Array verkauft, und Modellnummer des Herstellers

   - * WWN*

     WWN für den Konsolidierungs-Switch

   - **Principal Connector**

     Der Name des OnCommand Insight-Connectors, der die eigentliche Datenquelle war

   - **Verfügbare Anschlüsse**

     Alle OnCommand Insight-Connectors, in denen sich das konsolidierte Storage-Array befindet

   - **Insight-ID**

     ID des konsolidierten Speicher-Arrays auf dem OnCommand Insight-Gehäuse, in dem sich der Hauptanschluss befindet

   - * Insight Change Time*

     Wenn in OnCommand Insight ein Update für das Speicher-Array durchgeführt wurde und dasselbe Speicher-Array auf anderen OnCommand Insight-Servern aktualisiert wurde

In der Ansicht Anmerkungskonsolidierung in der Ansicht Fehlerbehebung in Data Warehouse wird eine Tabelle angezeigt, die alle verfügbaren Anmerkungstypen und die Objekttypen enthält, auf die sie angewendet werden können.

### Über diese Aufgabe

Die Konsolidierung der Anmerkungswerte basiert auf dem Wert des Anmerkungstyps. Ein Speicher-Array kann zwei verschiedene Tier-Werte haben, die jeweils von einem anderen Konnektor stammen. Wenn also in einem Konnektor ein Tier mit dem Namen Gold definiert ist und in einem zweiten Konnektor ein Tier mit dem Namen Goldy definiert ist, erscheint diese Information im Data Warehouse als zwei separate Tiers.

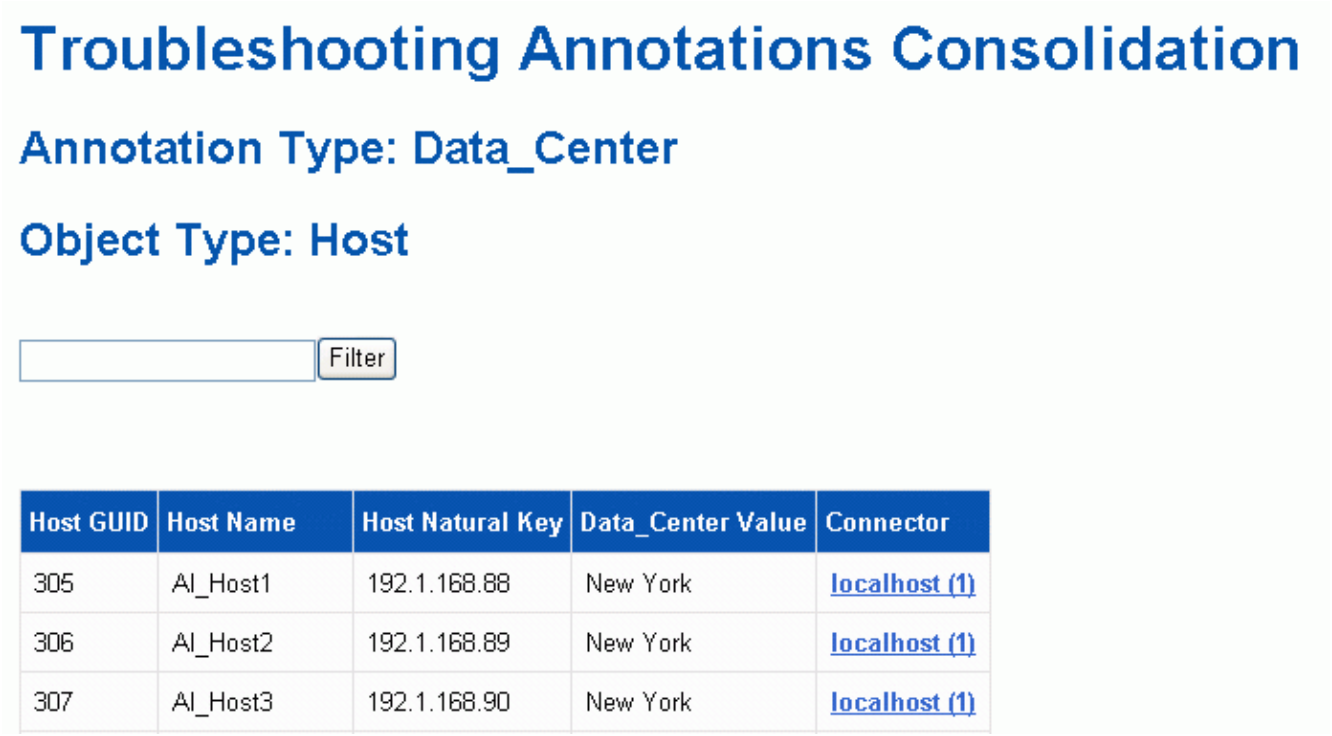
Da einige Anmerkungstypen die Zuordnung mehrerer Anmerkungswerte zu demselben Objekt ermöglichen, erlaubt Data Warehouse den Objekten (z. B. „`Host`“), ihnen mehrere Anmerkungswerte zuzuweisen (z. B. können „`data Center 1`“ und „`data Center 2“ demselben Host zugewiesen werden).

Die Funktion der Ebenenanmerkung auf Volumes unterscheidet sich etwas von den allgemeinen Anmerkungstabellen. Möglicherweise könnte es eine sehr große Anzahl von Volumes in der Umgebung geben, und die Anzeige aller Volumes im Data Warehouse würde sich auf die Nutzbarkeit der Informationen auswirken. Daher werden in der Ansicht Konsolidierung von Anmerkungen nur die Volumes angezeigt, denen mehrere Tier-Werte zugewiesen sind, und der Speicher, der jedes Volume enthält.

### Schritte

1. Melden Sie sich beim Data Warehouse Portal unter an `https://hostname/dwh`, Wo `hostname` Ist der Name des Systems, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt **Konsolidierung von Anmerkungen** in der Zeile für das Objekt auf **Anzeigen**.

   Im Folgenden sehen Sie ein Beispiel für die Anmerkungen zu Data_Center:



# Berichterstellung

## Willkommen beim OnCommand Insight Reporting

OnCommand Insight Reporting ist ein Business Intelligence-Tool, mit dem Sie vordefinierte Berichte anzeigen oder benutzerdefinierte Berichte erstellen können. OnCommand Insight Reporting generiert Berichte aus den DWH-Daten (Data Warehouse).

Mit OnCommand Insight Reporting können Sie folgende Aufgaben ausführen:

- Führen Sie einen vordefinierten Bericht aus
- Erstellen Sie einen benutzerdefinierten Bericht
- Passen Sie das Berichtsformat und die Bereitstellungsmethode an
- Planen Sie die automatische Ausführung von Berichten
- E-Mail-Berichte
- Verwenden Sie Farben, um Schwellenwerte für Daten darzustellen

Vordefinierte Berichte sind die OnCommand Insight-Standardberichte. In diesem Handbuch werden die vordefinierten Berichte beschrieben, die mit allen Produktlizenzen verfügbar sind.

### Zugriff auf das OnCommand Insight-Berichtsportal

Sie können das OnCommand Insight-Berichtsportal direkt über einen Webbrowser, über das Data Warehouse oder über den Insight-Server aufrufen. Über das Reporting Portal können Sie auf vordefinierte Berichte zugreifen oder eigene Berichte mithilfe von Data Warehouse-Daten erstellen.

#### Greifen Sie über einen Webbrowser auf das Reporting-Portal zu

##### Schritte

1. Öffnen Sie einen Webbrowser.
2. Geben Sie die folgende URL ein: `https://server-name:9300/bi`

   9300 steht für den Standardport, der während der Installation angegeben wurde. Wenn ein anderer Port angegeben wurde, müssen Sie den Port ändern.

3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, und klicken Sie dann auf **OK**.

#### Zugriff auf das Berichtsportal vom Insight Server aus

##### Schritte

1. Öffnen Sie einen Webbrowser.
2. Geben Sie die folgende URL ein, um auf den Insight-Server zuzugreifen: `https://server-name`
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, und klicken Sie dann auf **OK**.

4. Klicken Sie in der Symbolleiste Insight auf .
5. Geben Sie auf der angezeigten Anmeldeseite Ihren Benutzernamen und Ihr Passwort ein, und klicken Sie dann auf **OK**.

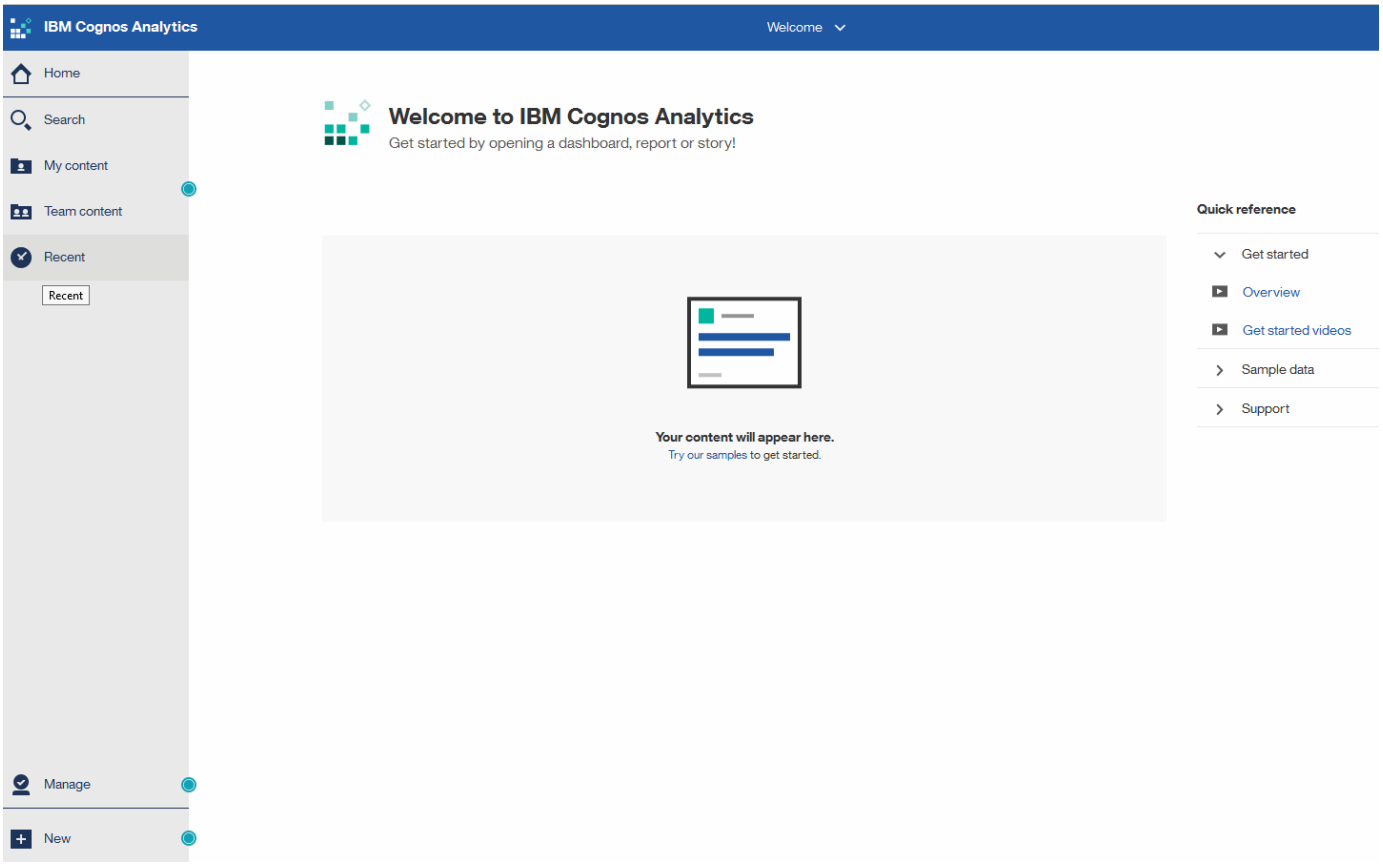
### Zugriff auf das Berichtsportal über das Data Warehouse

#### Schritte

1. Öffnen Sie einen Webbrowser.
2. Geben Sie die folgende URL ein, um auf das Data Warehouse zuzugreifen: `https://server-name/dwh`
3. Geben Sie Ihren Benutzernamen und Ihr Passwort ein, und klicken Sie dann auf **OK**.
4. Klicken Sie in der Symbolleiste Data Warehouse auf .
5. Geben Sie auf der angezeigten Anmeldeseite Ihren Benutzernamen und Ihr Passwort ein, und klicken Sie dann auf **OK**.

#### Ergebnisse

Die Startseite von IBM Cognos Analytics wird angezeigt. Dies ist die Standard-Landing Page des OnCommand Insight-Berichtsportals.




## Abweichungen aufgrund von installierten Lizenzen

Die Daten in den OnCommand Insight-Berichten basieren auf den von Ihnen erworbenen OnCommand Insight Lizenzen. Ohne die Planlizenz erhalten Sie beispielsweise Point-in-Time-Daten (heute) im Bestandsdatamart für Kapazität und Leistung, aber Sie haben

nicht die Möglichkeit, die Kapazitäts- oder Leistungsdaten für jedes Gerät zu tendenziieren (über einen Zeitraum berichten).

Wenn keine Planlizenz vorhanden ist, können keine neuen Berichte erstellt oder vorhandene Berichte bearbeitet werden. Möglicherweise werden Unterschiede zwischen den verfügbaren Berichten in Ihrem OnCommand Insight-System und den Abbildungen in der Dokumentation angezeigt. Diese Abweichungen sind auf Unterschiede zwischen den installierten Lizenzen auf Ihrem System und den Lizenzen auf dem System zurückzuführen, mit denen die Illustrationen erstellt wurden.

Weitere Informationen zu Lizenzen finden Sie im OnCommand Insight Installationshandbuch.

## Reporting-Benutzerrollen

Jedem Benutzerkonto wird eine Rolle mit einem Satz von Berechtigungen zugewiesen. Die Anzahl der Benutzer wird durch die Anzahl der Reporting-Lizenzen begrenzt, die jeder Rolle zugeordnet sind.

Jede Rolle kann die folgenden Aktionen ausführen:

- **Empfänger**

  Zeigt Berichte im OnCommand Insight-Reporting-Portal an und legt persönliche Einstellungen wie die für Sprachen und Zeitzonen fest.

  Empfänger können keine Berichte erstellen, Berichte ausführen, Berichte planen, Berichte exportieren oder administrative Aufgaben ausführen.

- **Business Consumer**

  Führt Berichte aus und führt alle Empfängeroptionen aus.

- **Business Author**

  Zeigt geplante Berichte an, führt Berichte interaktiv aus, erstellt Meldungen und führt alle Business Consumer-Optionen aus.

- **Pro Author**

  Erstellt Berichte, erstellt Pakete und Datenmodule sowie alle Optionen für Business Author.

- **Administrator**

  Führt Verwaltungsaufgaben für Berichte durch, wie z. B. Import und Export von Berichtsdefinitionen, Konfiguration von Berichten, Konfiguration von Datenquellen und Herunterfahren und Neustart von Berichtsaufgaben.

Die folgende Tabelle zeigt die Berechtigungen und die maximale Anzahl von Benutzern, die für jede Rolle zulässig sind:

| Merkmal | Empfänger | Geschäftsverbraucher | Wirtschaftautor | Pro Author | Admin |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| Anzeigen von Berichten auf der Registerkarte „Teaminhalt“ | Ja. | Ja. | Ja. | Ja. | Ja. |
| Berichte erstellen | Nein | Ja. | Ja. | Ja. | Ja. |
| Planen von Berichten | Nein | Ja. | Ja. | Ja. | Ja. |
| Externe Dateien hochladen | Nein | Nein | Ja. | Ja. | Nein |
| Erstellen von Geschichten | Nein | Nein | Ja. | Ja. | Nein |
| Erstellen von Berichten | Nein | Nein | Nein | Ja. | Nein |
| Erstellen von Paketen und Datenmodulen | Nein | Nein | Nein | Ja. | Nein |
| Ausführung administrativer Aufgaben | Nein | Nein | Nein | Nein | Ja. |
| Anzahl der Benutzer | Anzahl der OnCommand Insight Benutzer | 20 | 2 | 1 | 1 |

Wenn Sie einen neuen Benutzer für Data Warehouse und Reporting hinzufügen und das Limit in einer Rolle überschreiten, wird der Benutzer als „`deactivated`,“ hinzugefügt und Sie müssen einen anderen Benutzer mit dieser Rolle deaktivieren oder entfernen, um eine neue Benutzermitgliedschaft zu erhalten.

Für die Funktionen zur Berichterstellung ist eine Insight Plan-Lizenz erforderlich. Sie können zusätzliche Benutzer von Business Author und Pro Author hinzufügen, indem Sie DAS ARAP (Additional Report Authoring Package) erwerben. Wenden Sie sich an Ihren OnCommand Insight Ansprechpartner.

Diese berichtstellungsweisen Benutzerrollen haben keinen Einfluss auf den direkten Datenbankzugriff. Diese berichtenden Benutzerrollen haben keinen Einfluss auf Ihre Fähigkeit, SQL-Abfragen mithilfe der Data Marts zu erstellen.

## Aktivieren Von Sicherheitsüberschriften

HTTP-Header können so konfiguriert werden, dass die allgemeine Sicherheit der Cognos Analytics-Webanwendung erhöht wird.

So fügen Sie die Antwortkopfzeilen hinzu:

- Melden Sie sich bei der Cognos Analytics-Benutzeroberfläche an und navigieren Sie zu **Verwalten -> Konfiguration -> System -> Erweiterte Einstellungen**
- Fügen Sie den folgenden Schlüssel/Wert hinzu, und wenden Sie sie an:
  - Schlüssel: `BIHeaderFilter.responseHeaders`
  - Wert: `[{"name":"X-FRAME-OPTIONS","value":"SAMEORIGIN"},{"name":"X-XSS-Protection","value":"1"},{"name":"X-Content-Type-Options","value":"nosniff"}]`
- Aktualisiere deinen Browser, um die Header zu aktivieren.

# Berichterstellung leicht gemacht

Sie können vordefinierte Berichte über das OnCommand Insight-Berichtsportal erstellen, diese per E-Mail an andere Benutzer senden und sogar ändern. Mithilfe mehrerer Berichte können Sie nach Gerät, Geschäftseinheit oder Tier filtern. Die Berichterstellungs-Tools verwenden IBM Cognos als Grundlage und bieten Ihnen viele Möglichkeiten zur Datenpräsentation.

- Die vordefinierten OnCommand Insight Berichte zeigen Ihren Bestand, Ihre Storage-Kapazität, Kostenverrechnung, Performance, Storage-Effizienz, Und Daten zu Cloud-Kosten. Sie können diese vordefinierten Berichte ändern und Ihre Änderungen speichern.

Die Ihnen zur Verfügung stehenden Berichtsdaten werden von verschiedenen Faktoren gesteuert, darunter:

- Melden Sie sich beim OnCommand Insight-Reporting-Portal an, das durch Rollen definiert ist.
- Die Einrichtung des OnCommand InsightData Warehouse, das die Daten für die Berichte speichert.

Sie können Berichte in verschiedenen Formaten generieren, darunter HTML, PDF, CSV, XML, Und Excel.

OnCommand Insight unterstützt mehrere Mandanten in der Berichterstellung, da Sie Benutzer Geschäftseinheiten zuordnen können. Mit dieser Funktion können Administratoren Daten oder Berichte nach den Attributen eines Benutzers oder seiner Zugehörigkeit trennen.

Ab Cognos Version 11.1.2 gelten Reporting-URLs nicht als „stabil“ und können sich ändern. Wenn Sie mit einem Lesezeichen versehene Berichts-URLs haben, können diese Lesezeichen später fehlschlagen. Weitere Informationen finden Sie hier: http://queryvision.com/ibm-analytics-11-x-urls-they-are-a-changing/

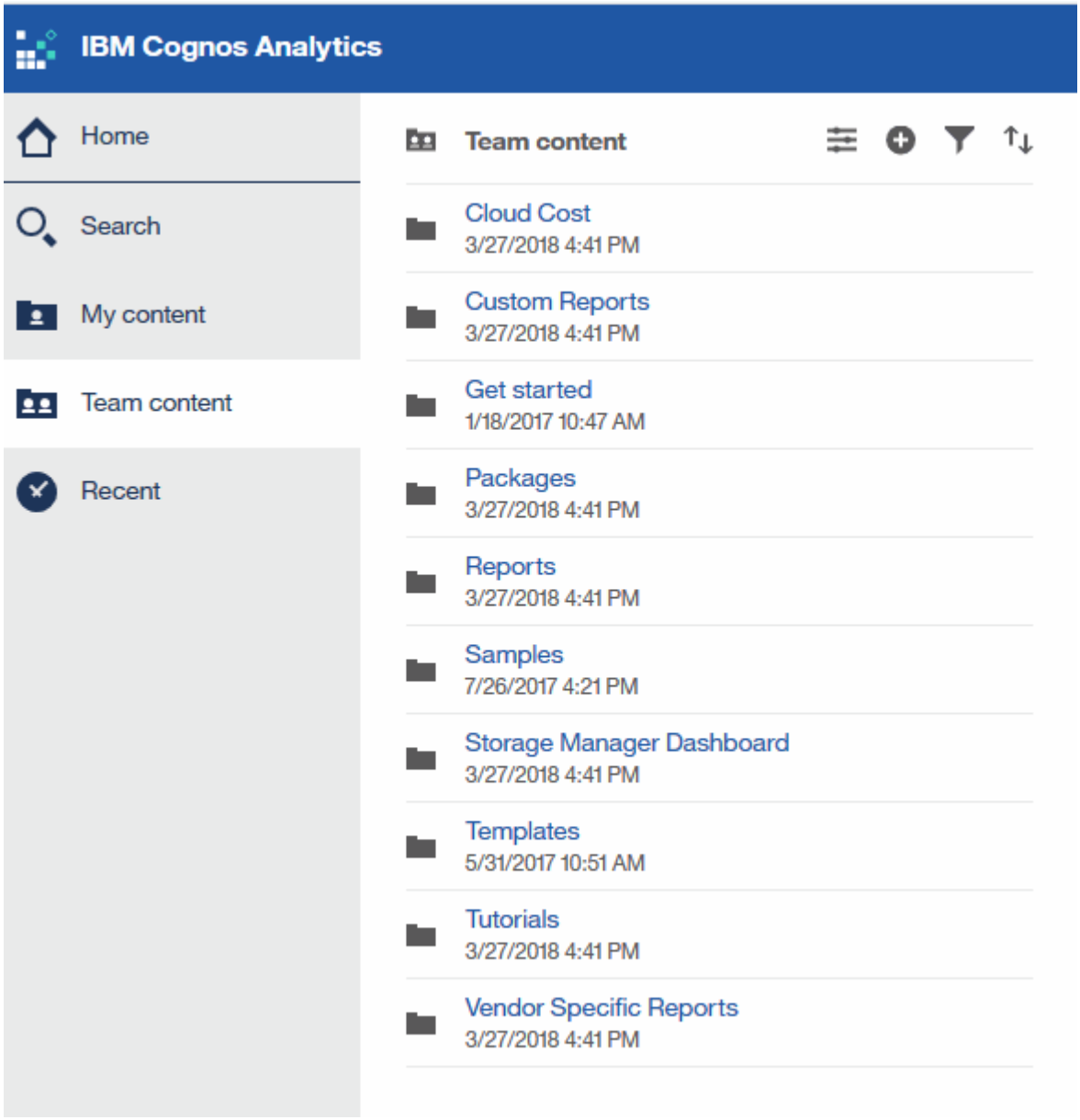
OnCommand Insight unterstützt keine Dashboards, die mit Paketen in IBM Cognos erstellt wurden, es sei denn, die neue Datenmodulfunktion wird verwendet.

## Navigieren zu vordefinierten OnCommand Insight-Berichten

Wenn Sie das Reporting-Portal öffnen, können Sie im Ordner Team Content den Informationstyp auswählen, den Sie in den OnCommand Insight-Berichten benötigen.

**Schritte**

1. Klicken Sie im linken Navigationsbereich auf **Team content** und wählen Sie die Informationskategorie aus, die Sie verwenden möchten.




2. Klicken Sie auf **Berichte**, um auf die vordefinierten Berichte zuzugreifen.
3. Klicken Sie auf **erste Schritte**, **Beispiele** oder **Tutorials**, um zu erfahren, wie Sie Berichte erstellen.

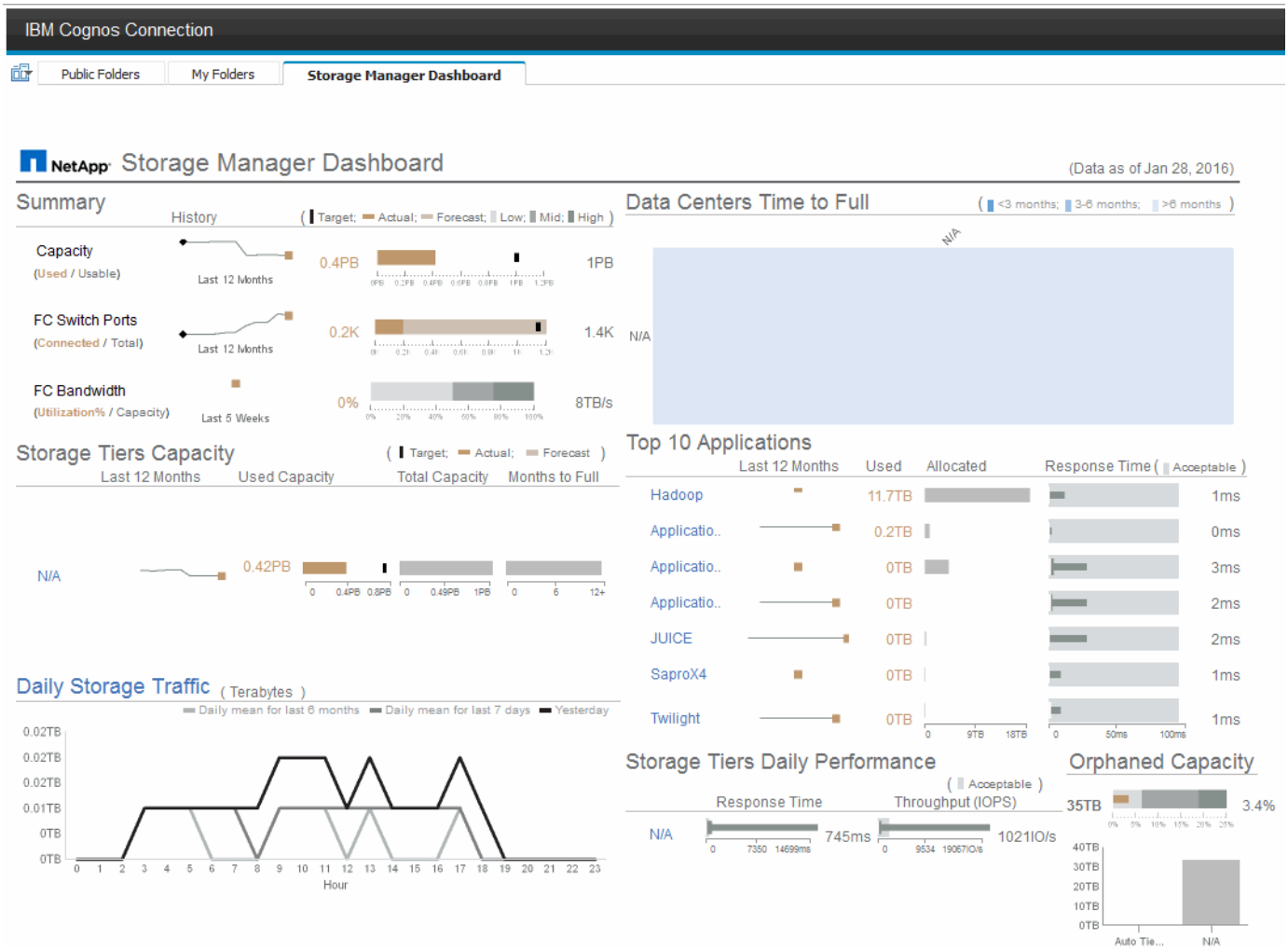
## Funktionen des Storage Manager Dashboards

### Mit dem Storage Manager Dashboard können Sie Ihre Storage-Services täglich managen.

Das Storage Manager Dashboard bietet Ihnen eine zentrale Visualisierung, mit der Sie die Ressourcennutzung im Laufe der Zeit mit dem akzeptablen Bereich und den vorherigen Aktivitätstagen vergleichen und kontrastieren können. Wenn nur die wichtigsten Performance-Metriken für Ihre Storage-Services angezeigt werden, können Sie Entscheidungen zur Wartung Ihres Datacenters treffen.

Das Dashboard besteht aus sieben Komponenten, die kontextbezogene Informationen zu bestimmten Aspekten Ihrer Storage-Umgebung enthalten. Sie können die Aspekte Ihrer Storage-Services detailliert analysieren und einen Abschnitt, der für Sie am wichtigsten ist, analysieren.

### Zusammenfassung




Diese Komponente zeigt die genutzte im Vergleich zur nutzbaren Storage-Kapazität, die Switch-Ports insgesamt gegenüber der Anzahl der verbundenen Switch-Ports sowie die Gesamtauslastung des verbundenen Switch-Ports gegenüber der Bandbreite und die jeweiligen Trends im Laufe der Zeit an. Sie können die tatsächliche Auslastung im Vergleich zum niedrigen, mittleren und hohen Bereich anzeigen. So können Sie anhand eines Ziels den Verbrauch zwischen Insight-Prognosen und den gewünschten ist-Werten vergleichen. Für Kapazität und Switch Ports können Sie dieses Ziel konfigurieren. Die Prognose basiert auf einer Extrapolation der aktuellen Wachstumsrate und des festgelegten Datums. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, das Ziel überschreitet, wird neben der Kapazität eine Warnmeldung (roter Kreis) angezeigt.

### Kapazität Des Storage-Tiers

Diese Komponente zeigt die genutzte Tier-Kapazität im Vergleich zur dem Tier zugewiesenen Kapazität. Dadurch wird angegeben, wie die genutzte Kapazität über einen Zeitraum von 12 Monaten erhöht oder verringert wird und wie viele Monate für die volle Kapazität übrig sind. Die Kapazitätsauslastung wird mit Werten angezeigt, die für die tatsächliche Nutzung angegeben sind, mit Prognosen zur Nutzung von Insight und mit einem Kapazitätsziel, das Sie konfigurieren können. Wenn die prognostizierte genutzte Kapazität, die auf dem zukünftigen Projektionsdatum der Nutzung basiert, die Zielkapazität überschreitet, wird neben einer

Tier eine Warnmeldung (roter Kreis) angezeigt.

Sie können auf eine beliebige Ebene klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen, in dem freie Kapazitäten und nicht genutzte Kapazitäten, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier angezeigt werden. Sie können auch auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

**Täglicher Storage-Traffic**

Diese Komponente zeigt die Performance der Umgebung, falls ein großes Wachstum, Änderungen oder potenzielle Probleme im Vergleich zu den vorangegangenen sechs Monaten auftreten. Es zeigt auch den durchschnittlichen Verkehr gegenüber dem Verkehr für die letzten sieben Tage, und für den Vortag. Sie können Anomalien in der Performance der Infrastruktur visualisieren, da sie Informationen liefert, die sowohl zyklische (vorherige sieben Tage) als auch saisonale Schwankungen (vorherige sechs Monate) hervorheben.

Sie können auf den Titel (**Daily Storage Traffic**) klicken, um den Bericht Storage Traffic Details anzuzeigen, der die Heatmap des stündlichen Speicherverkehrs für den vorherigen Tag für jedes Speichersystem anzeigt. Klicken Sie auf einen beliebigen Speichernamen in diesem Bericht, um die Seite „Anlage“ anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

**Datacenter voll Zeit**

Diese Komponente zeigt alle Datacenter und nicht alle Tiers an und zeigt, wie viel Kapazität in den einzelnen Datacentern für die einzelnen Storage-Tiers auf der Grundlage von prognostizierten Wachstumsraten von Insight verbleibt. Die Füllstandkapazität wird blau angezeigt. Je dunkler die Farbe ist, desto geringer ist die Zeit, die die Tier an der Position verlassen hat, bevor sie voll ist.

Sie können auf einen Abschnitt einer Ebene klicken, um den Bericht „Storage Pools Days to Full Details“ anzuzeigen. Dieser zeigt die Gesamtkapazität, die freie Kapazität und die Anzahl der Tage an, die für alle Pools in der ausgewählten Tier und im Datacenter voll werden sollen. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool-Namen in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der der aktuelle Status dieser Ressource zusammengefasst wird.

**Top 10 Applikationen**

Diese Komponente zeigt die 10 wichtigsten Applikationen auf Grundlage der genutzten Kapazität an. Unabhängig davon, wie der Tier die Daten organisiert, werden in diesem Bereich die aktuelle Kapazität und der Anteil der Infrastruktur angezeigt. Sie können die Benutzerfreundlichkeit der letzten sieben Tage visualisieren, um zu sehen, ob der Verbraucher akzeptable (oder, was noch wichtiger ist, nicht akzeptable) Reaktionszeiten hat.

In diesem Bereich werden auch Trendanalysen angezeigt, die angeben, ob die Applikationen ihre Service Level Objectives (SLOs) hinsichtlich der Performance erfüllen. Sie können die Mindestreaktionszeit der letzten Woche, das erste Quartil, das dritte Quartil und die maximale Reaktionszeit anzeigen, wobei ein Median im Vergleich zu einer akzeptablen SLO angezeigt wird, die Sie konfigurieren können. Wenn die mittlere Antwortzeit für eine Applikation außerhalb des zulässigen SLO-Bereichs liegt, wird neben der Applikation ein Alarm (ein roter Kreis) angezeigt. Sie können auf eine Anwendung klicken, um die Asset-Seite anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

**Storage Tiers Tägliche Performance**

Diese Komponente zeigt eine Zusammenfassung der Performance der Tier für Reaktionszeit und IOPS für die letzten sieben Tage. Die Performance wird mit einer SLO verglichen, die Sie konfigurieren können. Dadurch

sehen Sie, ob es Möglichkeiten gibt, die Storage Tiers zu konsolidieren, die von diesen Tiers bereitgestellten Workloads neu auszurichten oder Probleme mit bestimmten Tiers zu identifizieren. Wenn sich die mittlere Antwortzeit oder der mittlere IOPS außerhalb des akzeptablen SLO-Bereichs befindet, wird eine Warnmeldung (ein roter Kreis) neben einer Tier angezeigt.

Sie können auf einen Tier-Namen klicken, um den Bericht Storage Pools Capacity and Performance Details anzuzeigen. Er enthält Angaben zu freier und genutzter Kapazität, Anzahl der Tage bis zur vollen Auslastung sowie Angaben zur Performance (IOPS und Reaktionszeit) für alle Pools in der ausgewählten Tier. Klicken Sie auf einen beliebigen Speicher- oder Speicherpool in diesem Bericht, um die Seite Anlage anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

**„Verlorene“ Kapazität**

Diese Komponente zeigt die gesamte verwaiste Kapazität und verwaiste Kapazität je Tier. Sie wird verglichen mit einem akzeptablen Bereich für die gesamte nutzbare Kapazität und zeigt die tatsächliche verwaiste Kapazität an. Verwaiste Kapazität wird durch die Konfiguration und die Performance definiert. *Durch Konfiguration verwaister Speicher* beschreibt eine Situation, in der einem Host Speicher zugewiesen ist. Die Konfiguration wurde jedoch nicht ordnungsgemäß ausgeführt, und der Host kann nicht auf den Speicher zugreifen. *Verwaist durch Performance* ist, wenn der Speicher korrekt konfiguriert ist, um von einem Host darauf zugegriffen zu werden. Es gab jedoch keinen Lagerverkehr.

Der horizontale gestapelte Balken zeigt die zulässigen Bereiche an. Je dunkler das Grau ist, desto unannehmbarer ist die Situation. Die tatsächliche Situation wird mit dem schmalen Bronzebalken angezeigt, der die tatsächliche verwaiste Kapazität anzeigt.

Sie können auf eine Tier klicken, um den Bericht „Verlorene Storage-Details“ anzuzeigen. In diesem Bericht werden alle Volumes angezeigt, die nach Konfiguration und Performance der ausgewählten Tier als „verwaist“ identifiziert wurden. Klicken Sie in diesem Bericht auf eine beliebige Ablage, einen Speicherpool oder ein beliebiges Volume, um die Seite „Asset“ anzuzeigen, auf der der aktuelle Status dieser Ressource zusammengefasst wird.

## Verwenden von vordefinierten Berichten zur Beantwortung häufiger Fragen

OnCommand Insight enthält vordefinierte Berichte, die verschiedene allgemeine Berichtsanforderungen berücksichtigen und wichtige Einblicke bieten, die die Grundlage für fundierte Entscheidungen zur Storage-Infrastruktur bilden.

Die folgenden vordefinierten Berichte sind unter **Team content** > **Reports** oder **Team content** > **Vendor Specific Reports** verfügbar.

Neuere Versionen von Berichten sind möglicherweise im NetApp Storage Automation Store verfügbar. Im Automation Store sollten Sie regelmäßig nach Berichten suchen.

- **AWS Cloud Cost Data**

  Der Cloud-Kostenbericht bietet eine konsolidierte Ansicht aller Ressourcen, sodass Sie die Nutzung und die Kosten von Cloud- und On-Premises-Services nachverfolgen, analysieren und optimieren können. Außerdem können Sie sie in Ihrer Umgebung dynamisch skalieren.

  Der Bericht korreliert Kosten zwischen der Infrastruktur und erstellt eindeutige und verwertbare Berichte, um mittels gezielter Kapazitätsplanung und Abfallentsorgung das richtige Sizing zu gewährleisten.

- **Kapazität und Performance des Anwendungs-Service-Levels**

Der Bericht Application Service Level Capacity and Performance liefert einen allgemeinen Überblick über die Applikationen. Diese Informationen können für die Kapazitätsplanung oder für einen Migrationsplan verwendet werden.

- **Rückbelastung**

  Der Bericht Chargeback liefert Informationen zur Rückberechnung von Storage-Kapazitäten nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein.

  Um zu verhindern, dass die Doppelzählung keine ESX Server beinhaltet, überwachen Sie nur die VMs.

  Eine aktualisierte Version dieses Berichts finden Sie im NetApp Storage Automation Store.

- **Datenquellen**

  Der Bericht „Datenquellen“ zeigt alle Datenquellen an, die auf Ihrem Standort installiert sind, den Status der Datenquelle (Erfolg/Fehler) und Statusmeldungen. Der Bericht enthält Informationen darüber, wo mit der Fehlerbehebung von Datenquellen begonnen werden soll. Fehlerhafte Datenquellen wirken sich auf die Genauigkeit von Insight-Berichten und die allgemeine Benutzerfreundlichkeit des Produkts aus.

- **ESX vs. VM-Performance**

  Der Bericht ESX vs VM Performance zeigt einen Vergleich der ESX Server und VMs und zeigt die durchschnittliche und Spitzen-IOPS, den Durchsatz und die Latenz sowie die Auslastungen für ESX-Server und VMs an. Um eine Doppelzählung zu verhindern, schließen Sie die ESX Server aus; schließen Sie nur die VMs ein.

  Eine aktualisierte Version dieses Berichts finden Sie im NetApp Storage Automation Store.

- **Stoff Zusammenfassung**

  Der Bericht Fabric Summary identifiziert Switches und Switch-Informationen, einschließlich der Anzahl von Ports, Firmware-Versionen und Lizenzstatus. Der Bericht enthält keine NPV Switch-Ports.

- **Host-HBAs**

  Der Bericht Host HBAs bietet einen Überblick über die Hosts in der Umgebung und bietet die Hersteller-, Modell- und Firmware-Version von HBAs sowie die Firmware-Ebene der Switches, mit denen sie verbunden sind. Dieser Bericht kann zur Analyse der Firmware-Kompatibilität bei der Planung eines Firmware-Upgrades für einen Switch oder einen HBA verwendet werden.

- **Kapazität und Leistung des Host Service Levels**

  Der Bericht über Kapazität und Performance auf Host Service Level bietet einen Überblick über die Storage-Auslastung je Host für rein Block-beschränkte Applikationen.

- **Host Zusammenfassung**

  Der Host Summary Report bietet einen Überblick über die Speichernutzung für jeden ausgewählten Host mit Informationen für Fibre Channel- und iSCSI-Hosts. Der Bericht ermöglicht den Vergleich von Ports und Pfaden, der Fibre Channel- und ISCSI-Kapazität und der Anzahl der Verstöße.

- **Lizenzdetails**

  Im Bericht Lizenzdetails wird die berechtigte Menge an Ressourcen angezeigt, die Sie für alle Standorte mit aktiven Lizenzen lizenziert haben. Der Bericht zeigt außerdem eine Zusammenfassung der

tatsächlichen Menge an allen Standorten mit aktiven Lizenzen. Die Zusammenfassung kann Überschneidungen von Storage Arrays umfassen, die von mehreren Servern gemanagt werden.

- **Mapped but not masked Volumes**

  Der Bericht zugeordnete, jedoch nicht maskierte Volumes enthält die Volumes, deren Logical Unit Number (LUN) von einem bestimmten Host zur Verwendung zugeordnet wurde, jedoch nicht für diesen Host maskiert ist. In einigen Fällen können diese LUNs deaktiviert werden, die nicht maskiert wurden. Auf nicht maskierte Volumes kann jeder Host zugegriffen werden, wodurch sie anfällig für Datenkorruption sind.

- **NetApp Kapazität und Performance**

  Der Bericht NetApp Capacity and Performance liefert globale Daten für zugewiesene, genutzte und zugeteilte Kapazitäten im Rahmen von Trend- und Performance-Daten zur NetApp Kapazität.

- **OCI Scorecard**

  Der Bericht „OCI Scorecard“ bietet eine Zusammenfassung und einen allgemeinen Status aller von OnCommand Insight erkannten Assets. Der Status wird mit grünen, gelben und roten Markierungen angezeigt:

  - Grün zeigt den normalen Zustand an
  - Gelb zeigt ein potenzielles Problem in der Umgebung an
  - Rot zeigt ein Problem an, das Aufmerksamkeit erfordert Alle Felder im Bericht werden im Datenwörterbuch beschrieben, das dem Bericht beiliegt.

- **Speicherzusammenfassung**

  Der Bericht „Storage Summary“ bietet eine vollständige Übersicht über genutzte und nicht genutzte Kapazitätsdaten für Brutto-, zugewiesene Storage-Pools und Volumes. Dieser Bericht bietet einen Überblick über den gesamten erkannten Storage.

  Eine neuere Version dieses Berichts finden Sie im NetApp Storage Automation Store.

- **VM Kapazität und Performance**

  Beschreibt die VM-Umgebung (Virtual Machine) und ihre Kapazitätsauslastung. VM-Tools müssen aktiviert sein, um einige Daten anzuzeigen, z. B. wenn die VMs heruntergefahren wurden.

- **VM-Pfade**

  Der Bericht zu VM-Pfaden enthält Daten zur Storage-Kapazität und Performancemetriken, wobei Virtual Machines auf welchem Host ausgeführt werden, welche Hosts auf welche gemeinsam genutzten Volumes zugreifen, was der aktive Zugriffspfad ist und welche Kapazitätszuweisung und -Nutzung umfasst.

- **HDS-Kapazität nach Thin Pool**

  Der HDS Bericht zur Kapazität nach Thin Pool zeigt die Menge der nutzbaren Kapazität in einem Storage-Pool, der per Thin Provisioning bereitgestellt ist.

- **NetApp Kapazität nach Aggregat**

  Der Bericht NetApp-Kapazität nach Aggregaten zeigt die Gesamtmenge, die Gesamtzahl der genutzten, verfügbaren und den engagierten Speicherplatz von Aggregaten.

- **Symmetrix-Kapazität durch Thick Array**

  Der Bericht Symmetrix Capacity by Thick Array zeigt die Rohkapazität, nutzbare Kapazität, freie Kapazität, zugeordnet, maskiert, Und der gesamten freien Kapazität.

- **Symmetrix-Kapazität nach Thin Pool**

  Der Bericht Symmetrix Capacity by Thin Pool zeigt die Rohkapazität, nutzbare Kapazität, genutzte Kapazität, freie Kapazität, verwendeter Prozentsatz, Abonnierte Kapazitäten und Abonnementtarif.

- **XIV Kapazität nach Array**

  Der Bericht XIV Capacity by Array zeigt genutzte und ungenutzte Kapazität des Arrays an.

- **XIV Kapazität pro Pool**

  Der Bericht zur Nutzung der XIV-Kapazität anhand von Pools zeigt genutzte und nicht genutzte Kapazität für Storage Pools an.

## Erstellen eines Berichts mit Cognos 11

Das Erstellen von Berichten mit Cognos 11 unterscheidet sich von früheren Versionen von Cognos. Verwenden Sie dieses Verfahren, um einen Bericht mithilfe der vordefinierten OnCommand Insight-Berichte zu erstellen.

### Über diese Aufgabe

Mithilfe der folgenden Schritte erstellen Sie einen einfachen Bericht über die physische Kapazität von Speicher und Speicherpools in einer Reihe von Rechenzentren.

### Schritte

1. Klicken Sie in der Symbolleiste auf
2. Klicken Sie Auf **Bericht**
3. Klicken Sie Auf **Vorlagen** > **Leer**
4. Klicken Sie auf **Themes** > **Cool Blue** > **OK**

   Die Registerkarte „Quelle und Daten“ wird angezeigt

5. Klicken Sie Auf **Quelle** >
6. Klicken Sie im Dialogfeld Datei öffnen auf **Teaminhalt** > **Pakete**

   Eine Liste der verfügbaren Pakete wird angezeigt.

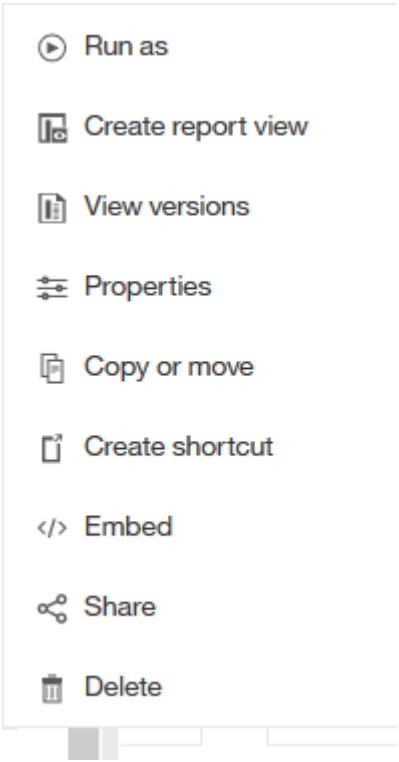
7. Klicken Sie auf **Storage and Storage Pool Capacity** > **Open**
8. Klicken Sie Auf

   Die verfügbaren Stile für Ihren Bericht werden angezeigt.

9. Klicken Sie Auf **Liste**

   Fügen Sie entsprechende Namen für Liste und Abfrage hinzu

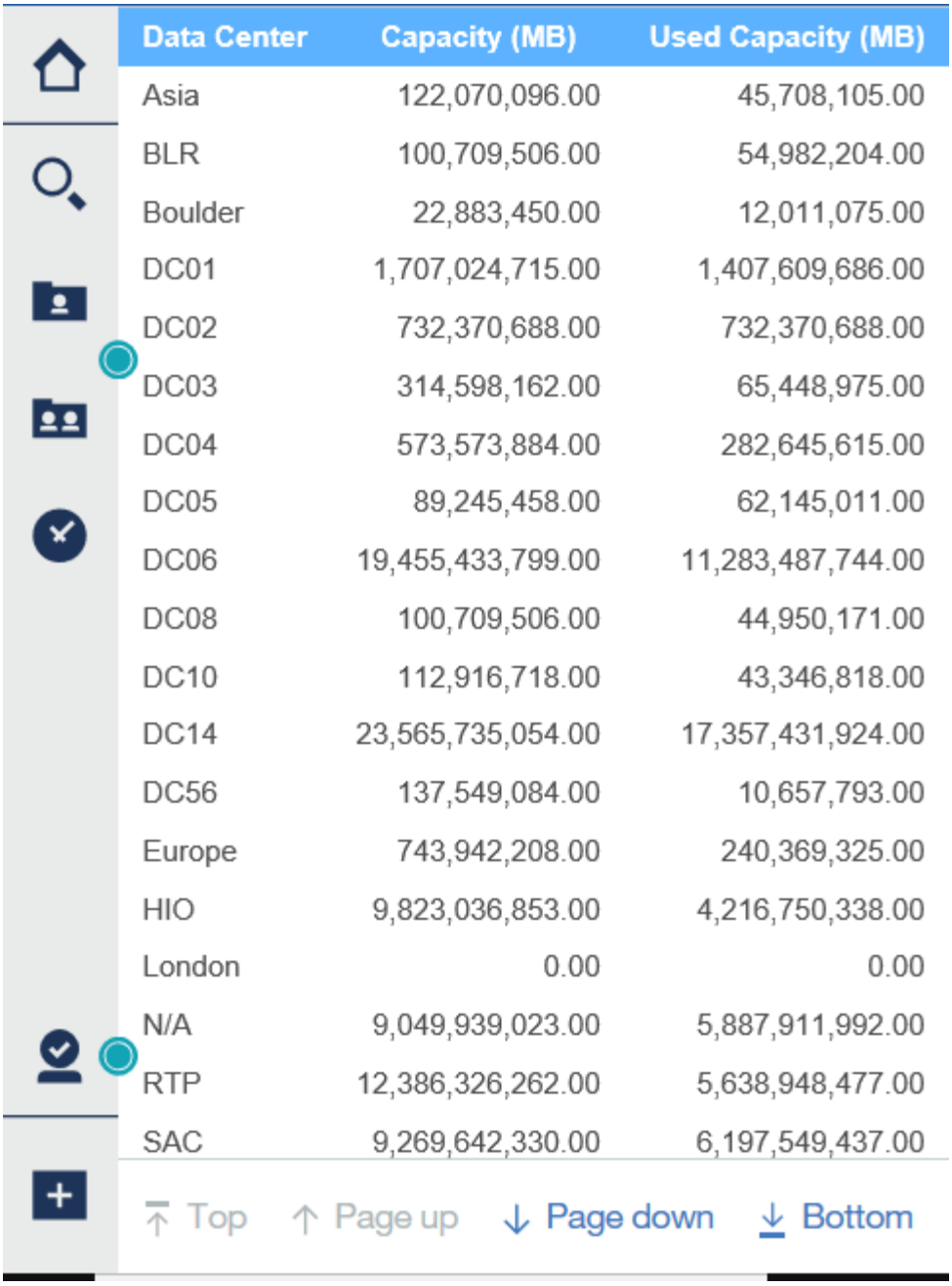
10. Klicken Sie auf **OK**
11. Erweitern Sie **Physische Kapazität**
12. Erweitern Sie sich auf die unterste Ebene von **Data Center**
13. Ziehen

Am Gaumen melden.
14. Erweitern Sie * Kapazität (MB)*
15. Ziehen Sie **Capacity (MB)** auf den Meldungs-Gaumen.
16. Ziehen Sie **Used Capacity (MB)** auf den Meldenden Gaumen.
17. 


    Führen Sie den Bericht aus, indem Sie auf klicken Und Auswahl eines Ausgabetyps.

**Ergebnisse**

Ein Bericht wie der folgende wird erstellt:



| Data Center | Capacity (MB) | Used Capacity (MB) |
|---|---|---|
| Asia | 122,070,096.00 | 45,708,105.00 |
| BLR | 100,709,506.00 | 54,982,204.00 |
| Boulder | 22,883,450.00 | 12,011,075.00 |
| DC01 | 1,707,024,715.00 | 1,407,609,686.00 |
| DC02 | 732,370,688.00 | 732,370,688.00 |
| DC03 | 314,598,162.00 | 65,448,975.00 |
| DC04 | 573,573,884.00 | 282,645,615.00 |
| DC05 | 89,245,458.00 | 62,145,011.00 |
| DC06 | 19,455,433,799.00 | 11,283,487,744.00 |
| DC08 | 100,709,506.00 | 44,950,171.00 |
| DC10 | 112,916,718.00 | 43,346,818.00 |
| DC14 | 23,565,735,054.00 | 17,357,431,924.00 |
| DC56 | 137,549,084.00 | 10,657,793.00 |
| Europe | 743,942,208.00 | 240,369,325.00 |
| HIO | 9,823,036,853.00 | 4,216,750,338.00 |
| London | 0.00 | 0.00 |
| N/A | 9,049,939,023.00 | 5,887,911,992.00 |
| RTP | 12,386,326,262.00 | 5,638,948,477.00 |
| SAC | 9,269,642,330.00 | 6,197,549,437.00 |

Top Page up Page down Bottom

# Verwalten von Berichten

Für jeden Bericht können Sie den Link **Mehr** in der Spalte Aktionen auswählen und auf alle Berichtsvorgänge zugreifen, wie beispielsweise das Festlegen von Berichtseigenschaften, das Planen von Berichten oder das Versenden von Berichten per E-Mail. Administratoren haben mehr Managementoptionen als andere Benutzer.

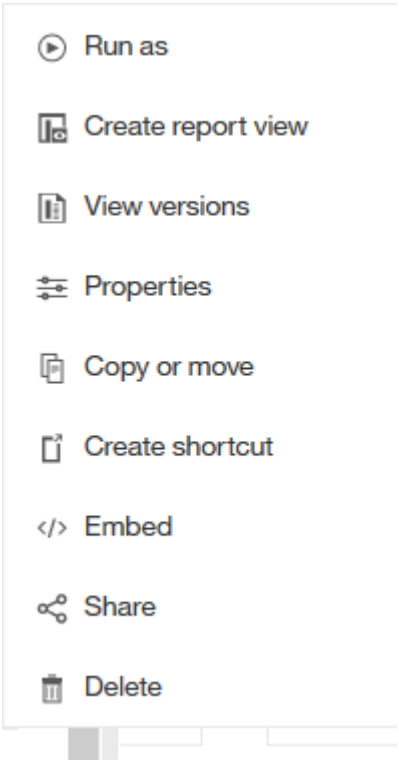
Administratoren können Berechtigungen für andere Berichtsbenutzer entsprechend ihrer OnCommand Insight-Rollen festlegen.

### Anpassen des Ausgabeformats und der Bereitstellung eines Berichts

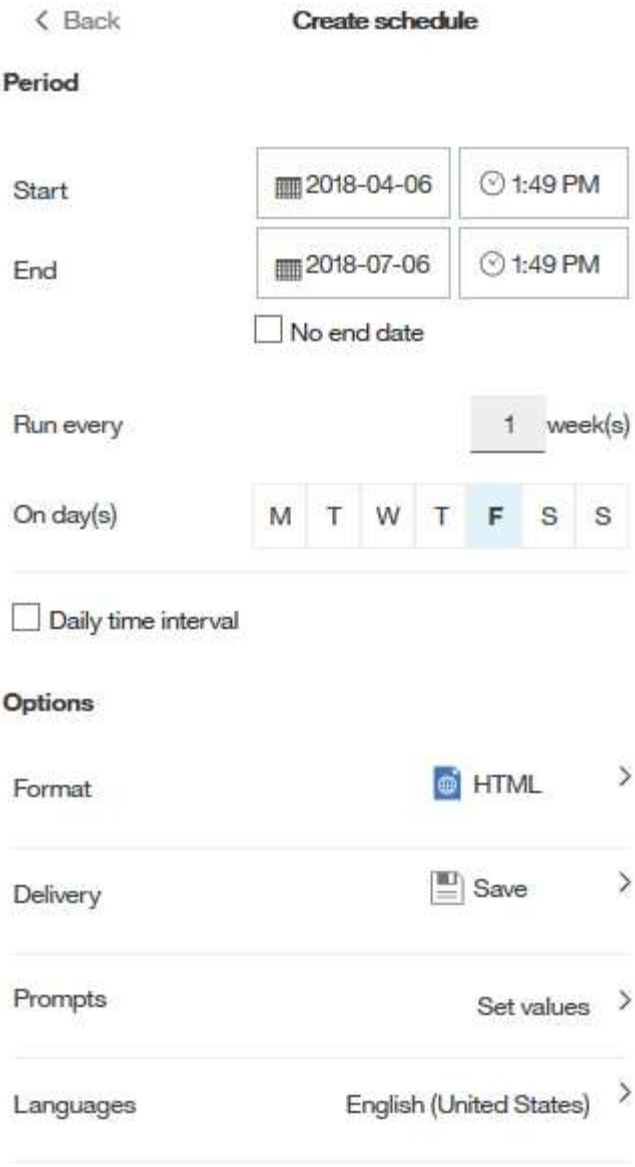
Sie können das Format und die Bereitstellungsmethode von Berichten anpassen.

**Schritte**

1. Öffnen Sie das OnCommand Insight-Berichtsportal, wählen Sie den Bericht aus, den Sie anpassen möchten, und klicken Sie auf **[...]**.




2. Klicken Sie Auf **Eigenschaften** > **Zeitplan**




3. Sie können folgende Optionen festlegen:
   - **Zeitplan**, wenn Sie Berichte ausführen möchten.
   - **Format** die Berichtausgabe.
   - **Lieferung** Drucken, speichern oder senden Sie den Bericht per E-Mail.
   - **Sprachen** definiert die Sprache, in der der Bericht geliefert wird.
4. Klicken Sie auf **Erstellen**, um den Bericht anhand der von Ihnen getroffene Auswahl zu erstellen.

## Kopieren eines Berichts in die Zwischenablage

Verwenden Sie diesen Vorgang, um einen Bericht in die Zwischenablage zu kopieren.

### Schritte

1. Öffnen Sie das Cognos 11 Reporting Portal: https://server-name:9300/bi/
2. Klicken Sie in der Symbolleiste auf

3. Klicken Sie Auf **Bericht**
4. Klicken Sie auf das Symbol *Seiten*

   Das Symbol **Report** Wird angezeigt
5. Klicken Sie mit der linken Maustaste auf das Symbol **Report**

   Berichtsoptionen werden angezeigt.
6. Klicken Sie auf **Bericht in Zwischenablage kopieren**.

### Öffnen von Berichten (XML) aus der Zwischenablage

Sie können eine Berichtsspezifikation öffnen, die zuvor in die Zwischenablage kopiert wurde.

#### Über diese Aufgabe

Sie rufen die Benutzeroberfläche „Reporting“ auf, indem Sie einen neuen Bericht erstellen oder einen vorhandenen Bericht öffnen

#### Schritte

1. Öffnen Sie das Cognos 11 Reporting Portal: https://server-name:9300/bi/
2. Klicken Sie in der Symbolleiste auf
3. Klicken Sie Auf **Bericht**
4. Klicken Sie auf das Symbol *Seiten*

   Das Symbol **Report** Wird angezeigt
5. Klicken Sie mit der linken Maustaste auf das Symbol **Report**

   Berichtsoptionen werden angezeigt.
6. Klicken Sie auf **Bericht aus Zwischenablage öffnen**.

# Erstellen benutzerdefinierter Ad-hoc-Berichte

Sie können die Tools zur Erstellung benutzerdefinierter Berichte verwenden. Nachdem Sie Berichte erstellt haben, können Sie sie speichern und regelmäßig ausführen. Die Ergebnisse der Berichte können automatisch per E-Mail an sich selbst und andere gesendet werden.

Die Beispiele in diesem Abschnitt veranschaulichen den folgenden Prozess, der für jedes der OnCommand Insight-Datenmodelle verwendet werden kann:

- Ermitteln einer Frage, die mit einem Bericht beantwortet werden soll
- Ermitteln der für die Ergebnisse erforderlichen Daten

- Auswählen von Datenelementen für den Bericht

## Was Sie vor dem Entwurf Ihres Berichts tun müssen

Bevor Sie Ihren benutzerdefinierten Bericht erstellen, müssen Sie einige erforderliche Aufgaben ausführen. Wenn Sie diese nicht ausfüllen, können die Berichte ungenau oder unvollständig sein.

Wenn Sie beispielsweise den Gerätekennungsprozess nicht abschließen, sind die Kapazitätsberichte nicht korrekt. Oder wenn Sie die Erstellung von Annotationen (z. B. Tiers, Geschäftseinheiten und Datacenter) nicht abschließen, werden in Ihren benutzerdefinierten Berichten möglicherweise Daten nicht präzise domänenübergreifend erfasst und für einige Datenpunkte „k. A.“ angezeigt.

Bevor Sie Ihre Berichte entwerfen, führen Sie die folgenden Aufgaben aus:

- Konfigurieren Sie alle Datenquellen. Weitere Informationen finden Sie im *OnCommand Insight Konfigurations- und Administrationshandbuch*.
- Geben Sie Annotationen (z. B. Tiers, Datacenter und Geschäftsbereiche) auf Geräten und Ressourcen in Ihrer Umgebung ein. Vor der Berichterstellung ist es von Vorteil, dass die Annotationen stabil sind, da das OnCommand Insight Data Warehouse historische Informationen sammelt.
- Konfigurieren Sie das OnCommand Insight Data Warehouse so, dass die Daten vom OnCommand Insight-Server im ETL-Prozess (Extrahieren, Transformieren und Laden) akzeptiert werden.

## Prozess der Erstellung von Berichten

Das Erstellen von Ad-hoc-Berichten umfasst mehrere Aufgaben.

- Planen Sie die Ergebnisse Ihres Berichts.
- Daten identifizieren, um Ergebnisse zu unterstützen
- Wählen Sie das Datenmodell aus (z. B. Chargeback-Datenmodell, Bestandsdatenmodell usw.), das die Daten enthält.
- Datenelemente für den Bericht auswählen.
- Optional können Sie Berichtsergebnisse formatieren, sortieren und filtern.

#### So planen Sie die Ergebnisse Ihres benutzerdefinierten Berichts

Bevor Sie die Berichtdesign-Tools öffnen, können Sie die gewünschten Ergebnisse aus dem Bericht planen. Mit den Tools zur Erstellung von Berichten können Sie problemlos Berichte erstellen und benötigen möglicherweise keine umfangreiche Planung. Es ist jedoch sinnvoll, den Berichtsinfragesteller zu den Berichtanforderungen zu verstehen.

- Geben Sie die genaue Frage an, die Sie beantworten möchten. Beispiel:
  - Wie viel Kapazität habe ich noch übrig?
  - Wie hoch sind die Kosten für die Rückberechnung pro Geschäftsbereich?
  - Wie groß ist die Kapazität je Tier, um sicherzustellen, dass die Geschäftsbereiche auf die richtige Storage-Tier ausgerichtet sind?
  - Wie kann ich einen Strom- und Kühlungsbedarf vorhersagen? (Fügen Sie benutzerdefinierte Metadaten durch Hinzufügen von Annotationen zu Ressourcen hinzu.)

- Ermitteln Sie die Datenelemente, die Sie zur Unterstützung der Antwort benötigen.
- Identifizieren Sie die Beziehungen zwischen Daten, die in der Antwort angezeigt werden sollen. Nehmen Sie keine unlogischen Beziehungen in Ihre Frage auf, zum Beispiel “Ich möchte die Ports sehen, die sich auf die Kapazität beziehen.”
- Ermitteln der für Daten erforderlichen Berechnungen
- Bestimmen Sie, welche Filtertypen erforderlich sind, um die Ergebnisse zu begrenzen.
- Bestimmen, ob aktuelle oder historische Daten verwendet werden müssen.
- Legen Sie fest, ob Sie Zugriffsberechtigungen für Berichte festlegen müssen, um die Daten auf bestimmte Zielgruppen zu beschränken.
- Ermitteln Sie, wie der Bericht verteilt werden soll. Sollte er beispielsweise per E-Mail an einen festgelegten Zeitplan gesendet oder im Bereich „Team Content Folder“ enthalten sein?
- Bestimmen Sie, wer den Bericht verwalten soll. Dies kann sich auf die Komplexität des Designs auswirken.
- Erstellen Sie ein Modell des Berichts.

#### Tipps für das Design von Berichten

Bei der Erstellung von Berichten sind einige Tipps hilfreich.

- Legen Sie fest, ob Sie aktuelle oder historische Daten verwenden müssen.

  Die meisten Berichte müssen nur über die neuesten im Data Warehouse verfügbaren Daten berichten.

- Data Warehouse bietet historische Informationen zu Kapazität und Leistung, jedoch nicht zu Bestandsdaten.
- Jeder sieht alle Daten, aber möglicherweise müssen Sie die Daten auf bestimmte Zielgruppen beschränken.

  Um die Informationen für verschiedene Benutzer zu segmentieren, können Sie Berichte erstellen und Zugriffsberechtigungen für sie festlegen.

# Datenmodell für die Berichterstellung

Ihr Unternehmen profitiert von den Daten, die im OnCommand Insight Data Warehouse erkannt und gespeichert werden. Das OnCommand Insight Data Warehouse ist ein zentralisiertes Repository, das Daten aus mehreren Informationsquellen speichert und in ein gemeinsames, mehrdimensionales Datenmodell für effizientes Abfragen und Analysieren umwandelt.

Aus diesem Repository können Sie benutzerdefinierte Berichte generieren, die beispielsweise für Kostenverrechnung, Verbrauchsanalyse und Prognosen verwendet werden, um Fragen wie die folgenden zu beantworten:

- Welche Bestände habe ich?
- Wo ist mein Inventar?
- Wer nutzt unsere Ressourcen?
- Wie sieht die Rückberechnung von zugewiesenem Storage für einen Geschäftsbereich aus?

- Wie viel Spielraum habe ich bei Switch Ports?
- Wie lange dauert es, bis ich zusätzliche Storage-Kapazität anschaffen muss?
- Werden die Geschäftseinheiten auf die entsprechenden Storage Tiers abgestimmt?
- Inwiefern ändert sich die Storage-Zuweisung über einen Monat, ein Quartal oder ein Jahr?

Mithilfe des Datenmodells, das mit OnCommand Insight-Berichten bereitgestellt wird, können Sie Berichte mithilfe von Tools zur Berichterstellung entwerfen und planen.

## Datenmodell im Überblick

OnCommand Insight bietet mehrere Datenmodelle für die Berichtentwicklung. Jedes Datenmodell ist eine Aggregation, die Daten zusammenfasst, sodass sie abgefragt und durchsucht werden können. Berichte zur Kapazitätsplanung verwenden beispielsweise das Kapazitätsdatenmodell.

Die Datenmodelle für die Unternehmensberichterstattung von OnCommand Insight bieten Datenelemente und interaktive Beziehungen zwischen Datenelementen, die eine geschäftliche Sicht der Daten ermöglichen. Mithilfe der Datenelemente und Beziehungen können Sie Berichte mit den von NetApp empfohlenen Berichterzeugungstools von IBM Cognos Analytics erstellen.

OnCommand Insight bietet auch Data Marts, mit denen Sie Ihre eigenen SQL-Abfragen entwickeln können. Es besteht eine Unterscheidung zwischen diesen SQL-Abfragedaten und den in der Berichterstellung verwendeten Datenmodellen. Die einzelnen OnCommand Insight-Berichtsdatenmodelle verwenden das zugrunde liegende OnCommand Insight-Datenbankschema, das in den Data Marts angegeben ist; allerdings verwenden die Datenmodelle zusätzliche Tabellen und manchmal neue Elemente in den Tabellen. Das Datenmodell umfasst beispielsweise eine Tabelle mit den monatlichen Kapazitätsinfaktdaten im Datenmodell für die Storage-Kapazität, die auf der Tabelle mit den Kapazitätsinfaktanzen aus dem Datenbankschema und dem Data Mart basiert. Das Datenmodell filtert die Werte aus der Datenbank-Schematabelle heraus, um nur Monatsinformationen anzuzeigen.

Ein weiteres Beispiel für einen Unterschied zwischen dem Datenbankschema, das in Data Marts verwendet wird, und dem Datenmodell ist in der Verletzungstabelle und in der Spalte „Typ der Verletzung“ zu finden. Das Datenmodell übersetzt programmatisch benannte Werte in die Datenbank, um den in der OnCommand Insight-Webbenutzeroberfläche angezeigten Text abzugleichen.

#### OnCommand Insight Datenmodelle

OnCommand Insight umfasst mehrere Datenmodelle, aus denen Sie entweder vordefinierte Berichte auswählen oder Ihren eigenen benutzerdefinierten Bericht erstellen können.

Jedes Datenmodell enthält einen einfachen Data Marts und einen erweiterten Data Marts:

- Der einfache Data Mart bietet schnellen Zugriff auf die am häufigsten verwendeten Datenelemente und umfasst nur den letzten Snapshot der Data Warehouse-Daten; er enthält keine historischen Daten.
- Advanced Data Mart bietet alle Werte und Details, die aus dem einfachen Data Mart zur Verfügung stehen, und beinhaltet den Zugriff auf historische Datenwerte.
- **Kapazitätsdatenmodell**

  Mit können Sie Fragen zur Storage-Kapazität, Auslastung des Filesystems, zur internen Volume-Kapazität, Port-Kapazität, qtree-Kapazität, beantworten. Und Kapazität von Virtual Machines (VMs). Das

Kapazitätsdatenmodell ist ein Container für mehrere Kapazitätsmodelle. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen beantworten:

- **Storage- und Storage-Pool-Kapazitätsdatenmodell**

  Ermöglicht das Antworten auf Fragen zur Ressourcenplanung von Storage-Kapazitäten, einschließlich Storage- und Storage-Pools, und umfasst sowohl physische als auch virtuelle Storage-Pool-Daten. Dieses einfache Datenmodell unterstützt Sie bei der Beantwortung von Fragen hinsichtlich Kapazität im Boden und der Kapazitätsauslastung von Storage-Pools nach Tier und Datacenter im Laufe der Zeit.

  Neue Kapazitätsberichte sind die Basis für ein Datenmodell, da es sich um ein einfacheres, zielgerichtetes Datenmodell handelt. Sie können Fragen wie die folgenden beantworten, indem Sie dieses Datenmodell verwenden:

  - Welches ist der voraussichtliche Termin für die Erreichung der Kapazitätsgrenze von 80 % meines physischen Storage?
  - Wie hoch ist die physische Storage-Kapazität auf einem Array für eine bestimmte Tier?
  - Wie groß ist meine Speicherkapazität nach Hersteller und Familie sowie nach Rechenzentrum?
  - Welchen Trend geht zur Storage-Auslastung bei einem Array für alle Tiers?
  - Welches sind meine 10 wichtigsten Storage-Systeme bei höchster Auslastung?
  - Wie sieht der Trend zur Storage-Auslastung der Storage Pools aus?
  - Wie viel Kapazität ist bereits zugewiesen?
  - Welche Kapazität ist für die Zuweisung verfügbar?
- **Datenmodell für die Auslastung des Dateisystems**

  Ermöglicht die Beantwortung von Fragen zur Auslastung des Dateisystems. Dieses Datenmodell bietet eine Übersicht über die Kapazitätsauslastung durch Hosts auf Filesystem-Ebene. Administratoren können zugewiesene und genutzte Kapazität pro Filesystem ermitteln, den Typ des Filesystems festlegen und Trendstatistiken nach Filesystem-Typ ermitteln. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

  - Wie groß ist das Filesystem?
  - Wo sind die Daten aufbewahrt und wie wird auf sie zugegriffen, z. B. lokal oder SAN?
  - Was sind historische Trends für die Kapazität des Filesystems? Und was können wir dann, basierend auf diesen, für zukünftige Anforderungen erwarten?
- **Kapazitäts-Datenmodell des internen Volumes**

  Hier können Sie Fragen zur verwendeten Kapazität des internen Volume, zu der zugewiesenen Kapazität und zur Kapazitätsauslastung beantworten:

  - Welche internen Volumes haben eine Auslastung über einem vordefinierten Schwellenwert?
  - Welche internen Volumes besteht in der Gefahr, dass die Kapazität aufgrund von Trends nicht mehr verfügbar ist?
  - Welche Kapazität haben wir im Vergleich zur zugewiesenen Kapazität in unseren internen Volumes?
- **Datenmodell der Portkapazität**

  Mit dieser Option können Sie Fragen zu Switch-Port-Konnektivität, Portstatus und Portgeschwindigkeit

im Laufe der Zeit beantworten. Sie können Fragen wie die folgenden beantworten, um die Anschaffung neuer Switches zu planen:

- Wie kann ich eine Portverbrauchsprognose erstellen, die Ressourcenverfügbarkeit (Port) prognostiziert (nach Rechenzentrum, Switch-Anbieter und Port-Geschwindigkeit)?
- Welche Ports werden wahrscheinlich zu Kapazitätsknapp, wenn es um Datengeschwindigkeit, Datacenter, Anbieter und Anzahl der Host- und Storage-Ports geht?
- Welche Trends haben die Switch-Port-Kapazität im Laufe der Zeit?
- Welche Port-Geschwindigkeiten werden verwendet?
- Welche Art von Port-Kapazität ist erforderlich und welches Unternehmen wird gerade dabei sein, einen bestimmten Port-Typ oder einen bestimmten Anbieter zu nutzen?
- Wie lange kann diese Kapazität optimal erworben und verfügbar gemacht werden?

◦ **Qtree Kapazitätsdatenmodell**

Ermöglicht die Trend-Nutzung von qtree (mit Daten wie genutzter bzw. zugewiesener Kapazität) im Laufe der Zeit. Sie können die Informationen nach verschiedenen Dimensionen anzeigen, z. B. nach Geschäftseinheit, Applikation, Stufe und Service-Level. Folgende Fragen können Sie mit diesem Datenmodell beantworten:

- Wie hoch ist die genutzte Kapazität von qtrees im Vergleich zu den Limits, die pro Applikation oder Geschäftseinheit gesetzt werden?
- Welche Trends haben wir bei unserer genutzten und freien Kapazität, sodass wir Kapazitäten planen können?
- Welche Geschäftseinheiten nutzen die größte Kapazität?
- Welche Applikationen belegen die größte Kapazität?

◦ **Modell der VM-Kapazitätsdaten**

Ermöglicht Ihnen, Berichte über Ihre virtuelle Umgebung und deren Kapazitätsauslastung zu erstellen. Mit diesem Datenmodell können Sie Änderungen des Kapazitätsverbrauchs über die Zeit für VMs und Datenspeicher berichten. Das Datenmodell bietet außerdem Thin Provisioning und Chargeback-Daten für Virtual Machines.

- Wie kann ich das Kapazitätszuordnungsberechnung basierend auf der Kapazität bestimmen, die für VMs und Datenspeicher bereitgestellt wird?
- Welche Kapazitäten werden nicht von VMs genutzt, und welcher Anteil ungenutzte Kapazitäten ist frei, verwaist oder anderer?
- Welche Anschaffungen müssen wir anhand von Verbrauchstrends erwerben?
- Wie hoch sind meine Storage-Effizienzeinsparungen durch Storage Thin Provisioning und Deduplizierungstechnologien? Die Kapazitäten im VM-Kapazitätsdatenmodell werden von virtuellen Festplatten (VMDKs) genutzt. Das bedeutet, dass die bereitgestellte Größe einer VM mit dem VM-Kapazitätsdatenmodell die Größe der virtuellen Festplatten entspricht. Dies unterscheidet sich von der bereitgestellten Kapazität in der Ansicht der Virtual Machines in OnCommand Insight, in der die bereitgestellte Größe für die VM selbst angezeigt wird.

◦ **Datenmodell der Volume-Kapazität**

Ermöglicht die Analyse sämtlicher Volumes in Ihrer Umgebung und die Organisation von Daten nach Anbieter, Modell, Tier, Service Level und Datacenter. Sie können die Kapazität für verwaiste Volumes, ungenutzte Volumes und Datensicherungs-Volumes (zur Replizierung genutzt) anzeigen. Außerdem

können Sie unterschiedliche Volume-Technologien (iSCSI oder FC) sehen und virtuelle Volumes mit nicht-virtuellen Volumes vergleichen, um Probleme bei der Array-Virtualisierung zu beheben. Sie können Fragen wie die folgenden mit diesem Datenmodell beantworten:

  - Welche Volumes haben eine Auslastung, die über einem vordefinierten Schwellenwert liegt?
  - Welchen Trend geht in meinem Datacenter hinsichtlich verwaister Volume-Kapazität?
  - Wie viel meiner Datacenter-Kapazität ist virtualisiert oder Thin Provisioning?
  - Wie viel meiner Datacenter-Kapazität muss für die Replizierung reserviert werden?

- **Chargeback-Datenmodell**

  Ermöglicht das Antworten auf Fragen zur genutzten Kapazität und zugewiesenen Kapazität in Storage-Ressourcen (Volumes, interne Volumes und qtrees). Dieses Datenmodell liefert Informationen zur Kostenverrechnung und Transparenz der Storage-Kapazität nach Hosts, Applikationen und Geschäftseinheiten und schließt sowohl aktuelle als auch historische Daten ein. Berichtsdaten können nach Service Level und Storage Tier kategorisiert werden.

  Sie können dieses Datenmodell verwenden, um Berichte zur Rückberechnung zu erstellen, indem Sie die Menge an Kapazität ermitteln, die von einer Geschäftseinheit verwendet wird. Dieses Datenmodell ermöglicht Ihnen die Erstellung einheitlicher Berichte für verschiedene Protokolle (einschließlich NAS, SAN, FC und iSCSI).

  - Bei Storage ohne interne Volumes werden Berichte zur Kostenverrechnung nach Volumes angezeigt.
  - Zur Speicherung mit internen Volumes:

    - Wenn den Volumes Geschäftseinheiten zugewiesen sind, werden Chargeback-Berichte nach Volumes angezeigt.
    - Wenn Geschäftseinheiten nicht Volumes zugewiesen, aber qtrees zugewiesen sind, werden Chargeback-Berichte durch qtrees angezeigt.
    - Wenn Geschäftseinheiten nicht Volumes zugewiesen und nicht qtrees zugewiesen sind, wird das interne Volume durch Chargeback-Berichte angezeigt.
    - Die Entscheidung, ob die Kostenzuordnung nach Volume, qtree oder internem Volume angezeigt werden soll, wird für jedes interne Volume getroffen. Somit ist es möglich, dass verschiedene interne Volumes im selben Storage Pool die Chargeback auf verschiedenen Ebenen zur Verfügung stehen. Kapazitätfakten werden nach einem Standard-Zeitintervall gelöscht. Weitere Informationen finden Sie unter Data Warehouse-Prozesse.

    Berichte, die das Chargeback-Datenmodell verwenden, können andere Werte anzeigen als die Berichte, die das Storage Capacity-Datenmodell verwenden.

  - Bei Storage Arrays, die keine NetApp Storage-Systeme sind, bleiben die Daten beider Datenmodelle gleich.
  - Bei Storage-Systemen von NetApp und Celerra verwendet das Chargeback-Datenmodell eine einzelne Schicht (von Volumes, internen Volumes oder qtrees), um die Gebühren zu senken. Das Storage-Kapazitätsdatenmodell nutzt dagegen mehrere Schichten (von Volumes und internen Volumes), um ihre Gebühren zu sichern.

- **Bestandsdatenmodell**

  Mit Hilfe von Antworten auf Fragen zu Bestandsressourcen, einschließlich Hosts, Speichersystemen, Switches, Festplatten, Tapes Qtrees, Quotas, Virtual Machines und Server sowie generische Geräte. Das Bestandsdatenmodell enthält mehrere Unterverzeichnis, mit denen Sie Informationen zu Replikationen, FC-Pfaden, iSCSI-Pfaden, NFS-Pfaden und Verstößen anzeigen können. Das Bestandsdatenmodell

enthält keine historischen Daten. Fragen, die Sie mit diesem Data Mart beantworten können, können die folgenden sein:

- Welche Assets habe ich und wo sind sie?
- Wer nutzt die Ressourcen?
- Welche Gerätetypen habe ich und welche Komponenten sind diese Geräte?
- Wie viele Hosts je Betriebssystem habe ich und wie viele Ports sind auf diesen Hosts vorhanden?
- Welche Storage-Arrays pro Anbieter gibt es in den einzelnen Datacentern?
- Über wie viele Switches je Anbieter verfügt ich in jedem Datacenter?
- Wie viele Ports sind nicht lizenziert?
- Welche Tapes von welchem Anbieter verwenden wir und wie viele Ports sind auf jedem Tape vorhanden?
- Werden alle generischen Geräte identifiziert, bevor wir mit der Arbeit an Berichten beginnen?
- Welche Pfade sind zwischen den Hosts und Storage Volumes oder Tapes?
- Welche Pfade gibt es zwischen generischen Geräten und Speicher-Volumes oder Bändern?
- Wie viele Verstöße gegen die einzelnen Typen gibt es pro Datacenter?
- Was sind die Quell- und Ziel-Volumes für jedes replizierte Volume?
- Erhalte ich Firmware-Inkompatibilitäten oder falsche Portgeschwindigkeiten zwischen Fibre Channel Host HBAs und Switches?

- **Modell der Leistungsdaten**

  Antworten auf Fragen zur Performance von Volumes, Applikations-Volumes, internen Volumes, Switches, Applikationen VMs, VMDKs, ESX und VM, Hosts und Applikations-Nodes. Mit diesem Datenmodell können Sie Berichte erstellen, die verschiedene Arten von Fragen zum Performance-Management beantworten:

  - Auf welche Volumes oder internen Volumes wurde in einem bestimmten Zeitraum nicht zugegriffen?
  - Können wir mögliche Fehlkonfigurationen beim Storage für eine (nicht verwendete) Applikation ermitteln?
  - Wie sieht das Zugriffsverhalten einer Applikation insgesamt aus?
  - Werden für eine bestimmte Applikation entsprechend Tiered Volumes zugewiesen?
  - Könnten wir für eine Applikation, die derzeit läuft, einen günstigeren Storage nutzen, ohne die Applikations-Performance zu beeinträchtigen?
  - Welche Applikationen bieten mehr Zugriffe auf den derzeit konfigurierten Storage? Wenn Sie die Switch-Leistungstabellen verwenden, können Sie folgende Informationen abrufen:
  - Ist mein Host-Verkehr durch verbundene Ports ausgeglichen?
  - Welche Switches oder Ports weisen eine hohe Anzahl an Fehlern auf?
  - Welche Switches werden am häufigsten an der Port-Performance verwendet?
  - Welche nicht ausgelasteten Switches basieren auf der Port-Performance?
  - Welcher Durchsatz beim Trending des Hosts basiert auf der Port-Performance?
  - Wie hoch ist die Performance-Auslastung der letzten X Tage für einen angegebenen Host, ein Storage-System, ein Tape oder Switch?
  - Welche Geräte erzeugen Datenverkehr auf einem bestimmten Switch (z. B. welche Geräte sind für den Einsatz eines stark genutzten Switches verantwortlich)?

- Wie hoch ist der Durchsatz für einen bestimmten Geschäftsbereich in unserer Umgebung? Wenn Sie die Tabellen zur Festplatten-Performance verwenden, erhalten Sie folgende Informationen:
- Wie ist der Durchsatz für einen angegebenen Storage-Pool auf Basis von Festplatten-Performance-Daten?
- Was ist der am höchsten genutzte Storage-Pool?
- Wie hoch ist die durchschnittliche Festplattenauslastung für einen bestimmten Storage?
- Was ist der Trend zur Nutzung eines Storage-Systems oder eines Storage-Pools basierend auf den Festplatten-Performance-Daten?
- Wie sieht der Trend zur Festplattennutzung für einen bestimmten Storage Pool aus? Wenn Sie VM- und VMDK-Performance-Tabellen verwenden, erhalten Sie folgende Informationen:
- Arbeitet meine virtuelle Umgebung mit optimaler Performance?
- Welche VMDKs stellen die höchsten Workloads dar?
- Wie kann ich die von VMDs gemeldete Performance bei verschiedenen Datastores nutzen, um Entscheidungen zum Re-Tiering zu treffen. Das Performance-Datenmodell enthält Informationen, mit denen Sie die Angemessenheit von Tiers, Storage-Fehlkonfigurationen für Applikationen und die letzten Zugriffszeiten von Volumes und internen Volumes ermitteln können. Dieses Datenmodell bietet Daten wie Reaktionszeiten, IOPS, Durchsatz, Anzahl der ausstehenden Schreibvorgänge und den Status des Datenzugriffs.

- **Datenmodell Storage-Effizienz**

  Nachverfolgung des Storage-Effizienz-Ergebnisses und des Potenzials im Laufe der Zeit Dieses Datenmodell speichert Messungen nicht nur der bereitgestellten Kapazität, sondern auch der genutzten oder verbrauchten Menge (der physischen Messung). Wenn beispielsweise Thin Provisioning aktiviert ist, zeigt OnCommand Insight an, wie viel Kapazität vom Gerät genommen wird. Mithilfe dieses Modells lässt sich außerdem die Effizienz bei aktivierter Deduplizierung bestimmen. Sie können verschiedene Fragen mithilfe des Storage-Effizienz-Data Marts beantworten:

  - Wie hoch sind unsere Storage-Effizienzeinsparungen als Ergebnis der Implementierung von Thin Provisioning und Deduplizierungstechnologien?
  - Wie hoch sind die Storage-Einsparungen in den gesamten Datacentern?
  - Wann müssen wir, basierend auf Trends bei früheren Kapazitäten, zusätzlichen Storage erwerben?
  - Was würde der Kapazitätsgewinn bedeuten, wenn wir Technologien wie Thin Provisioning und Deduplizierung aktivieren würden?
  - Sind Sie hinsichtlich der Storage-Kapazität aktuell in Gefahr?

**Daten-Modell-Fakt- und Bemaßungstabellen**

Jedes Datenmodell enthält Fakt- und Bemaßungstabellen.

- Fact-Tabellen: Enthalten Daten, die gemessen werden, z. B. Menge, Rohkapazität und nutzbare Kapazität. Fremdschlüssel in Bemaßungstabellen enthalten.
- Bemaßungstabellen: Enthalten beschreibende Informationen zu Fakten, beispielsweise Datacenter und Geschäftseinheiten. Eine Dimension ist eine Struktur, die häufig aus Hierarchien besteht, die Daten kategorisiert. Maßattribute helfen, die Maßwerte zu beschreiben.

Mithilfe verschiedener oder mehrerer Bemaßungsattribute (siehe Spalten in den Berichten) erstellen Sie Berichte, die für jede im Datenmodell beschriebene Dimension auf Daten zugreifen.

Erläuterungen zu allen Datenelementen, die beim Erstellen von Berichten verwendet werden, finden Sie im Datenglossar.

#### Farben, die in Datenmodellelementen verwendet werden

Farben auf Datenmodellelementen haben unterschiedliche Indikationen.

- Gelbe Werte: Stellen Messungen dar.
- Nicht-gelbe Werte: Repräsentieren Attribute. Diese Werte aggregieren nicht.

#### Verwenden mehrerer Datenmodelle in einem Bericht

Normalerweise verwenden Sie ein Datenmodell pro Bericht. Sie können jedoch einen Bericht schreiben, in dem Daten aus mehreren Datenmodellen kombiniert werden.

Um einen Bericht zu schreiben, der Daten aus mehreren Datenmodellen zusammenfasst, wählen Sie eines der Datenmodelle aus, die als Basis verwendet werden sollen, und schreiben Sie dann SQL-Abfragen, um auf die Daten der zusätzlichen Datentabellen zuzugreifen. Sie können die SQL-Join-Funktion verwenden, um die Daten aus den verschiedenen Abfragen in einer einzigen Abfrage zu kombinieren, mit der Sie den Bericht schreiben können.

Beispielsweise möchten Sie die aktuelle Kapazität für jedes Storage Array bereitstellen und benutzerdefinierte Anmerkungen zu den Arrays erfassen. Sie können den Bericht mithilfe des Datenmodells für die Storage-Kapazität erstellen. Sie können die Elemente aus den Tabellen „Aktuelle Kapazität und Dimension“ verwenden und eine separate SQL-Abfrage hinzufügen, um auf die Annotationsinformationen im Bestandsdatenmodell zuzugreifen. Abschließend können Sie die Daten kombinieren, indem Sie die Bestandsspeicherdaten mit der Tabelle Speicherdimension verknüpfen, indem Sie den Speichernamen und die Kriterien für den Beitritt verwenden.

# Häufig gestellte Fragen

## Allgemeine Fragen

Diese FAQ beantwortet allgemeine Fragen zu OnCommand Insight.

### Wann wurde OnCommand Insight (OCI) eingeführt?

OCI ist mit über zehn Jahren aktiver Entwicklung eines der ausgereiftesten Produkte für das Infrastruktur-Monitoring der Branche. Der früher als Onaro oder SANscreen bekannte Name von SANscreen wurde bei der Aufnahme in die OnCommand Portfolio Suite geändert und wird jetzt als OnCommand Insight oder – in der Regel – als Insight oder OCI bezeichnet.

### Wie lange dauert die Implementierung von OCI in meiner Umgebung?

OCI ist einfach ein Software-Download. Software wird auf zwei dedizierten virtuellen oder physischen Servern installiert. Typische Installationen sind in nur 2 Stunden möglich, und Daten zu Bestands-, Kapazitäts- und Performance werden nahezu sofort bereitgestellt. Alle zusätzlichen Richtlinien für Performance und Best Practices, Benutzeranmerkungen und eine Einrichtung zur Kostenbewusstsein erfordern zusätzliche Planungsgespräche.

### Erfordert OCI Agenten, Kollektoren oder Sonden?

OCI ist zu 100 % agentenlos und erfordert keine Agenten, Taps oder Sonden. Die Geräteerkennung ist schreibgeschützt, bandextern und über IP ausgeführt.

### Wie erkennt OCI Geräte und stellt eine Verbindung zu ihnen her?

Das OCI Setup nutzt die nativen APIs und Protokolle, die häufig bereits in der Datacenter-Umgebung vorhanden sind, ohne Agenten oder Sonden zu benötigen. SSH, HTTP, SMIS und CLI sind nur ein paar Beispiele. Wenn bereits Geräte-Element-Manager vorhanden sind (z. B. Unisphere von EMC), kommuniziert OCI mit den Element-Managern, um die vorhandenen Umgebungsdaten zu erfassen. Für die meisten Geräteermittlungen sind nur eine IP-Adresse und ein schreibgeschützter Benutzername und ein Kennwort erforderlich. Diese Geräteerkennungen können „`1:n`“ sein, beispielsweise mit der VMware Datenquelle von OCI. Durch die Erkennung von VMware vCenter erkennt OCI wiederum alle ESXi Hosts und zugehörigen VMs, wobei nur eine IP-Adresse und Zugangsdaten vorhanden sind.

### Ist für OCI Professional Services erforderlich? Ist das verfügbar, und was bieten sie an?

Für Umgebungen mittlerer Größe empfehlen wir Professional Services für die Implementierung, Konfiguration und Integration sowie eine Vielzahl von Möglichkeiten für benutzerdefinierte Berichte und Datenvalidierungen. Eine kurze Diskussion mit dem OCI-Team und dem Account Engagement Manager kann helfen zu ermitteln, welche Services am meisten von Ihnen profitieren.

### Wie oft wird OCI im Hinblick auf neue Funktionen und Verbesserungen aktualisiert?

Produkt-Updates und Service-Pakete sind für OCI-Versionen erhältlich. Major Releases oder Minor Releases werden in der Regel alle paar Monate bereitgestellt, wobei Service Packs einschließlich neuer Geräte-Support und Firmware häufiger veröffentlicht werden. Beide sind auf der support.netapp.com Download-Seite

verfügbar. Bestimmte Updates, z. B. neue Festplattenmodelle, die häufiger von Herstellern angeboten werden, werden automatisch an die OCI Software weitergegeben. Darüber hinaus kann die Erfassung der OCI-Datenquellengeräte sofort nach einer Entwicklungsphase oder -Aktualisierung vor Ort gepatcht werden.

## Wie priorisiert das OCI-Managementteam Anfragen nach neuen Datenquellen?

Das Produktmanagement-Team von OCI verfolgt aktiv alle Anfragen zu Verbesserungen und Interoperabilitätsfunktionen (IFR) von Kunden. Jede Anfrage wird detailliert beschrieben, auf ihre Machbarkeit überprüft und anhand der Kundennachfrage und der strategischen Auswirkungen auf das Geschäft priorisiert. Sobald die Anforderungen akzeptiert wurden, werden sie basierend auf dem Arbeitsaufwand und der Planung für die zukünftige Entwicklung bestimmt. Der agile Charakter des OCIs-Entwicklungsprozesses ermöglicht es routinemäßig, neue Datenquellen außerhalb der regulären geplanten Release-Zyklen zur Verfügung zu stellen. NetApp Ansprechpartner können Ihnen bei Kundenanfragen und beim Einreichen neuer Anfragen in Ihrem Namen helfen. Datenquellen können vor Ort gepatcht werden, ohne dass ein Upgrade von OCI erforderlich ist.

## Mein Unternehmen läuft komplett unter Linux. Kann OCI auf Linux verwendet werden?

Ja, OCI unterstützt mehrere Versionen von Linux und Windows. Beachten Sie, dass Cognos (das von OCI in Verbindung mit dem Data Warehouse verwendete Reporting-Tool von IBM) nur unter Windows unterstützt wird. Wenn Sie OCI für die Berichterstellung verwenden, müssen Sie das Reporting-Tool auf einem Windows-Server ausführen. Der OCI-Installationsleitfaden führt die Serveranforderungen und die unterstützten Betriebssysteme der einzelnen OCI-Komponenten auf.

## Ist OCI für sichere Umgebungen ohne Internetzugang geeignet?

Ja, OCI wird von den 10 führenden Fortune 500-Unternehmen sowie von führenden Banken, Gesundheitswesen, Forschung und Behörden weltweit genutzt. OCI unterstützt US Military Common Access Cards (CAC) und bietet Lösungen für geografisch verteilte und stark Firewall-Umgebungen.

## Ich habe immer wieder erfahren, dass OnCommand Unified Manager (OCUM) die Managementlösung für cDOT ist. Können Sie mir helfen zu verstehen, warum ich auch OCI verwenden würde?

OnCommand Unified Manager arbeitet auf der Storage-Array-Ebene „`device Management`“. Er bietet detaillierte Incident- und Event-basierte Analysen von Clustered Data ONTAP (cDOT) Arrays und deren Cluster Interconnects. OCI bietet eine ganzheitliche Übersicht über lokale und global verteilte Umgebungen mit 7-Mode, Clustered Data ONTAP und Arrays von Drittanbietern. Die umfassende Transparenz – von der VM bis zur Spindel – ermöglicht historische Trendanalysen und Prognosen zur Kapazität, Performance und Kostenmodellierung, die einen proaktiven Ansatz zur Servicequalität für das Datacenter Management fördern.

## Was ist der sekundäre OnCommand Insight ETL?

Der Begriff „sekundäre ETL“ bezieht sich auf eine entwickelte Implementierung von Professional Services, die zum Aufrufen zusätzlicher ETL (Extract, Transform and Load) der erfassten Daten zur Einfüllung in das OnCommand Insight Data Warehouse verwendet wird.

Der sekundäre ETL-Prozess dient primär dem Prefetch von „Batch“-Daten, sodass komplexere Berichte schneller generiert oder für die tägliche Ausführung geplant werden können.

Diese sekundäre ETL wird zusätzlich zu der empfohlenen ETL „einmal pro Tag“ im OnCommand Insight Data Warehouse-Administrationshandbuch beschrieben.

NetApp Professional Services sind qualifiziert, sekundäres ETL-Scripting zu konfigurieren, um Auswirkungen auf bestehende Zeitpläne für OnCommand Insight-Berichte, automatisierte Backups, Skalierbarkeit oder andere Aktivitäten im Bereich der System-Performance zu vermeiden. Weitere Informationen zu Anforderungen an ETL-Skripts oder Datenvalidierungen erhalten Sie bei Ihrem NetApp Ansprechpartner. Dort erfahren Sie, wie die NetApp Professional Services Sie unterstützen können.

# OnCommand Insight-Lizenzierung

Antworten auf häufig gestellte Fragen zur OnCommand Insight-Lizenzierung.

## OCI-Lizenzierungsübersicht

OCI wird nach Kapazität lizenziert. Kunden müssen für jedes Modul eine Lizenz erwerben, das sie aktivieren möchten:

**Discover** ist eine Voraussetzung für Assure, Perform und Plan und wird nicht alleine angeboten. Discover wird nach TB gemanagter Kapazität lizenziert.

**Assure** wird nach TB gemanagter Kapazität lizenziert (als eine einzige Einheit für die gesamte Speicherinfrastruktur: FC, NAS, iSCSI, FCoE).

**Perform** wird nach TB verwalteter Kapazität lizenziert.

**Plan** wird nach TB verwalteter Kapazität lizenziert.

„`Managed Capacity`“ ist definiert als die Rohkapazität der physischen Laufwerke, virtuellen Laufwerke und Bänder vor der Formatierung. Dies gilt für alle von Insight erkannten Storage sowohl lokal als auch in der Cloud.

Die meisten Datenquellen nehmen die Bruttokapazität von 2 auf der Festplatte an. Die Festplattenrolle, z. B. eine Ersatzfestplatte, nicht zugewiesene Festplatte oder eine RAID-Festplatte, wird nicht berücksichtigt.

Es gibt zwei Arten von Insight-Lizenzen: **Perpetual** und **Subscription**.

**Perpetual-Lizenzen** ermöglichen Ihnen die unbegrenzte Nutzung der spezifischen Version/Freigabe der Software, die Sie erhalten, vorbehaltlich der geltenden Lizenzbedingungen. Wenn Sie einen Software Support-Plan (SSP) erworben haben, bietet NetApp über die NetApp Support Site Zugang zu kommerziell verfügbaren Software Updates, sobald und sofern Updates gemäß den Bedingungen der Support Services verfügbar sind. NetApp bietet darüber hinaus den Zugang zu speziellen Patches, die vom NetApp Technical Support Center festgelegt werden.

**Abonnement** ist eine befristete Lizenz von Software, die das Recht auf:

- Verwenden Sie die Software nur für einen begrenzten Zeitraum (in der Regel 12 Monate) vor Ort unter Einhaltung der geltenden Lizenzbedingungen
- Software-Support (bisher als SSP bezeichnet) für die Dauer der Laufzeit erhalten
- Der Lizenznehmer darf zwar die aktuellste im Handel erhältliche Version, Veröffentlichung oder Aktualisierung verwenden, sollte diese verfügbar gemacht werden und erhält Unterstützung für die Software

Am Ende jeder festen Laufzeit (meistens 12 Monate) kann die Lizenz um einen zusätzlichen, festen Zeitraum verlängert werden (meistens 12 Monate). Wenn die Lizenz nicht verlängert wird, hat der Lizenznehmer nicht mehr die Rechte zur Nutzung der Software, hat keinen Anspruch mehr auf die Vorteile von SSP und muss alle

Kopien der Software vernichten.

### Weitere Informationen zu OCI-Lizenzmodulen

OCI verfügt über 4 zentrale Lizenzmodule, um heutige Datacenter-Umgebungen zu erfüllen. Diese Module sind **Discover, Perform, Assure und Plan**. Discover ist das Basismodul und für alle anderen Modulkäufe erforderlich.

Mit dem Modul **Discover** kann OCI die Assets im Rechenzentrum lokalisieren und die Servicepfade des Geräts dynamisch abbilden. Es werden Informationen wie Kapazität, Herstellerinformationen, Modell, Firmware und Seriennummern bereitgestellt.

**Perform** ist das Performance-Erfassungsmodul von OCI. Performance erfasst IOPS, Durchsatz, Latenz sowie Informationen zu CPU und Arbeitsspeicher und liefert andere Analysen.

**Assure** ist in Richtung Fibre-Channel-Umgebungen und Effizienztechnologien positioniert. Sie hilft bei der Erkennung und dem Management von Risiken in Fibre Channel- und iSCSI-Umgebungen. Unterstützung bei der Identifizierung, Zuordnung und Ausgabe von Warnmeldungen bei Masking, Mapping und Zoning von Servicepfadeinträgen und Best Practice-Richtlinien für Effizienz wie Fabric-Redundanz, Switch Hops, Fan-out-Verhältnissen und Thin Provisioning

**Plan** bietet die Möglichkeit, Trends bei Computing, Fabric und verschiedenen Storage-Typen (cDOT, 7-Mode, Drittanbieter) in hybriden On-Premises- und global verteilten Data Center-Umgebungen zu erkennen und vorherzusagen. Es ermöglicht längere Aufbewahrungszeiten. Das Data Warehouse besteht aus einer integrierten Intelligenz zur Erstellung von Berichten und vermeidet die doppelte Zählung von Kennzahlen in gemeinsam genutzten Speicherumgebungen. Es kann ein Kompliment von „`Out of the box`“-Berichten generieren und planen oder eigene Berichte mit den integrierten “ `Drag-and-Drop`“-Tools zur Berichterstellung erstellen.

# Konfiguration und unterstützte Geräte

In diesen FAQ werden häufig gestellte Fragen zur OnCommand Insight-Konfiguration und zu unterstützten Geräten beantwortet.

### Nimmt OCI Änderungen an der Umgebung vor?

Nein OCI ist ein schreibgeschütztes Tool, das Informationen zur Umgebung des Kunden erfasst. OCI nimmt keine Änderungen an Ihren Assets oder Konfigurationen vor.

### Welchen Zugriff auf Berechtigungsebene benötigt OCI für meine Geräte?

In den meisten Fällen, in denen das Gerät es unterstützt, ist ein schreibgeschützter Zugriff alles erforderlich. Es gibt einige Lösungen, die keinen schreibgeschützten Zugriff erlauben und somit die entsprechenden erhöhten Berechtigungen benötigen würden.

### Wie oft erfasst OCI Informationen?

OCI erfasst in der Regel alle 5 Minuten Performance-Daten sowie alle ½ Stunden eine Erkennung der logischen und physischen Konstrukte OCI bestimmt die standardmäßigen Abrufintervalle gemäß den empfohlenen Best Practices und der Skalierbarkeit, erlaubt dem Benutzer jedoch die vollständige Kontrolle über diese Intervalle.

## Welche Auswirkungen hat OCI auf meine Umgebung?

Die agentenlose, Out-of-Band- und passive IP-Kommunikation von OCI minimiert die Einrichtung, Wartung und Auswirkungen auf das Datacenter-Ecosystem. Das Performance-Entwicklungsteam von OCI ergreift hervorragende Maßnahmen, um die Auswirkungen auf die Performance des Datacenters bei Aktivitäten zur Überwachung der Performance selbst zu minimieren. Die Auswirkungen werden in normalen Betriebsumgebungen als unwesentlich angesehen und können in stark ausgelasteten oder leistungsschwächer ausgelasteten Technologieplattformen entspannt oder verschärft werden. Weitere Informationen finden Sie im OnCommand Insight Installationshandbuch.

## Wie kann ich alle Hosts/VMs in OCI auflisten?

Die Ergänzung von Widgets und Abfrageoptionen von OCI kann dazu verwendet werden, Einträge im Bestandsstil für Datacenter-Ressourcen bereitzustellen. Einträge von virtuellen Maschinen bis auf die Spindeln und zahlreiche Konstrukte dazwischen können alle Anfragen, Widgets, Dashboards und Data Warehouse-Berichterstellung zur Verfügung gestellt werden und sind über die RESTful API zugänglich.

## Bietet OCI dieselbe Unterstützung für verwandte Hosts ohne Hypervisor (d. h. physische Server)?

Hypervisoren wie VMware bieten detaillierte Informationen über DIE ESXI-Hosts und ihre zugehörigen Virtual Machines (VMs). Bei physischen Servern sammelt OCI Kennzahlen bis zum Host-HBA. OCI nutzt eine einzigartige Methode zur Erkennung physischer Server über eine zum Patent angemeldete Technologie. Sobald Storage und/oder Switches erkannt wurden, sind Hostnamen für physische Server in den Fabric-Alias-Informationen enthalten. OCI wählt diese Host-Namen aus, stimmt sie in DNS ab und bringt die Hosts automatisch in OCI. Durch diese Technik wird die Notwendigkeit von manuellen Aktualisierungen bei der Eingabe und der Wartung des Werkzeugbestands erheblich reduziert.

## Bietet OCI die gleiche metrische Tiefe (Parität) des Geräts in heterogenen Umgebungen?

Die Standardisierung, die Gemeinsamkeit und Terminologie bei Plattformen und Technologien von Drittanbietern gibt es immer unterschiedliches Maß. OCI versucht, Kapazitäts- und Performance-Informationen in einem konsistenten Framework zu normalisieren. Einige Kapazitäts- und Performance-Kennzahlen werden nativ von den Zählern des Geräts bereitgestellt, wie z. B. IOPS, Latenz und Rohkapazität. Wenn keine Zähler bereitgestellt werden, kann OCI versuchen, die Werte zusammenzufassen (beispielsweise durch eine Zusammenfassung der IOPS oder Kapazitäten der zugrunde liegenden Volumes). In Fällen, in denen keine dieser Werte verfügbar sind, versucht OCI, die metrischen Werte durch verschiedene Algorithmen abzuleiten. OCI bietet eine allgemeine SNMP-Integrationsfunktion, mit der zusätzliche Kennzahlen integriert werden, die derzeit nicht von OCI erfasst werden.

## Unterstützt OCI Fibre Channel Switches?

Ja, neben der Erfassung von Daten aus Storage-Ressourcen erfasst OCI auch Bestands- und Performance-Daten von Cisco, Brocade und QLogic Switches in der Umgebung.

## Stehen Topologieansichten der gesamten Infrastruktur zur Verfügung? Zeigt OCI „End-to-End-Sichtbarkeit“ an?

Ja, OCI erkennt und ordnet die logischen und physischen Konstrukte dynamisch zu und bietet eine interaktive End-to-End-Topologieansicht für Computing, Fabrics, Virtualisierungen und Back-End Storage. Topologiesymbole ermöglichen die schnelle Navigation zu betroffenen Ressourcen und unterstützen die Identifikation von Workloads und Verstößen in Shared Storage-Umgebungen.

# Skalierbarkeit und Benutzerfreundlichkeit

Dieses FAQ beantwortet häufig gestellte Fragen zur Skalierbarkeit und Benutzerfreundlichkeit von OnCommand Insight.

## Wie skaliert OCI?

OCI ist hinsichtlich Interoperabilität und der Anzahl der Assets, die es bei minimalem Platzbedarf erwerben kann, führend. Im Kern benötigt OCI 2 virtuelle oder physische Server: Einen für den Operationsserver, auf dem alle Datacenter-Ressourcen erfasst werden, und einen für das konsolidierte Data Warehouse für die langfristige Verlaufsberichte. Die Unternehmensabdeckung von OCI unterstützt Hunderte von Arrays, Zehntausende Virtual Machines, 100,000 Fibre-Channel-Pfade und mehr als 10,000 Fibre-Channel-Ports – und all das in einer einzigen Server-Instanz.

## Wie viele Mitarbeiter sind für das Management der OCI-Applikation erforderlich?

OCI kann von einer einzelnen Person gemanagt werden. OCI bietet jedoch Funktionen, die von mehreren Personas innerhalb der Geschäftsumgebung verwendet werden können, von denen jede unterschiedliche Rollen hat, die jeweils unterschiedliche Anforderungen an Berichterstellung, Fehlerbehebung und Analyse haben. Mit allen Maßnahmen wird die Tool-Wartung auf ein Minimum reduziert – von Menüs für den Systemzustand und die Benachrichtigung, in denen Konfigurationsprobleme angezeigt werden, bis hin zur automatischen Erkennung physischer, mit einer Fabric verbundener Hosts. Flexible Annotationen ermöglichen für alle Benutzertypen den geschäftlichen Kontext der Ökosystemdaten. Von Storage-, Fabric- und Virtualisierungsadministratoren bis hin zu Kapazitätsplanern, Geschäftsanalysten und Führungskräften – OCI vereint die gemeinsame Nutzung von Informationen über Unternehmenssilos und Technologien hinweg in einer zentralen Konsole.

## Unterstützt OCI individuelle Berichte?

Ja. OCI bietet Reporting über das Business Intelligence-Tool IBM Cognos, mit dem Kunden eigene, vollständig angepasste Berichte zu Daten erstellen können, die im Data Warehouse von OCI erfasst werden.

## Wie einfach ist die Erstellung benutzerdefinierter Berichte?

OCI Berichterstellung bietet Funktionen sowohl für neue als auch für fortgeschrittene Benutzer. OCI bietet eine Reihe von Funktionen zur Berichterstellung, darunter die Berichterstellung „`dRAG and Drop`“ und abfragebasierte SQL-Berichte für komplexere Benutzerprojekte oder professionelle Serviceaktivitäten. Die integrierte Business Intelligence-Lösung (IBM Cognos) von OCI vermeidet häufige Fehler wie das Doppelten der Kapazität. Mit einer Kombination aus sofort einsatzbereiten Berichten, Widgets, Abfragen und Dashboards gibt es Angebote, die den Berichtsanforderungen von jedermann entsprechen.

Außerdem stehen Berichtsvorlagen zum Herunterladen im OCI Community Store zur Verfügung.

## Kann OCI dank der Einfachheit des Traffics Performance und Verfügbarkeit anzeigen?

Ja. OCI Data Warehouse und Reporting ermöglichen Berichte mit Farbverbesserungen, z. B. rot/gelb/grün „`bedingtes Styling`“ von Werten. Das Generieren einer farbigen Schriftart oder eines Hintergrunds in einem Bericht kann sowohl von Endbenutzern als auch von Professional Services implementiert werden. OCIs-Widget-Bibliotheken ermöglichen die Anzeige von geschäftsspezifischen Leistungsmetriken in Dashboards.

# Fehlerbehebung bei der Performance

In diesem FAQ werden häufig gestellte Fragen zur Fehlerbehebung bei OnCommand Insight-Performance beantwortet.

## Wie kann ich eine Liste aller gierigen Ressourcen in meiner Umgebung erstellen?

Die Korrelationsanalyse von OCI hilft bei der Identifizierung übergriffiger und beeinträchtigter Ressourcen für einen bestimmten Service-Pfad. Die von der Korrelationsfunktion generierte Analyse wird in Echtzeit durchgeführt, während jedes Objekt angezeigt wird. Die Analyse ermöglicht es, Performance-Probleme schneller zu beheben und die Ursache zu identifizieren. Die Untersuchung generierter Verstöße gegen definierte Performance-Richtlinien sind ein Ansatzpunkt für die Erkennung übergriffiger und beeinträchtigter Ressourcen. Sowohl Widgets als auch Dashboards, die die neueste Abfragefunktion verwenden, helfen beim Filtern, Sortieren und Visualisieren von Ressourcen mit mehr als erwarteten IOPS (übergriffige), Auslastung oder Latenz.

## Kann OCI an einen Ort zur Diagnose von Performance-Problemen helfen?

Ja. Die Performance-Fehlerbehebung in OCI kann auf verschiedene Weise erreicht werden. OCI bietet verschiedene Alarmmethoden. Häufig werden SNMP-, Syslog- und E-Mail-Alarme verwendet. Per E-Mail versandte Warnmeldungen ermöglichen Benutzern das schnelle Klicken auf die betroffenen Ressourcen in OCI. In einem globalen Suchfenster können Administratoren einfach einen Ressourcennamen eingeben, um mit der Analyse der Situation zu beginnen.

Das OCI Dashboard für Verstöße ermöglicht Benutzern eine Priorisierung von Vorgängen basierend auf Anzahl der Ereignisse, Dauer und Tageszeit. Ein Beispiel für verschiedene Alarmtypen sind Latenz, IOPS, Auslastung, Schweregrad, Geschäftsbereich oder sogar zugehörige Applikationen.

Die Korrelationsanalyse von OCI hilft Administratoren, Objekte der betroffenen Ressource zu vergleichen und ihre Auswirkungen auf IOPS, Latenz, Auslastung, CPU- und BB-Gutschriften zu bestimmen.

Die Query-Technologie und Widget Dashboards von OCI ermöglichen das genaue Auffinden von Details in organisierten Ansichten, die auf Problembereiche im Datacenter abzielen.

## Bietet OCI Unterstützung bei Migrationen von 7-Mode zu cDOT?

Ja, OCI bietet ein umfassendes Verständnis für die vorhandenen Workload-Anforderungen und Validierungen nach der Migration. Die Rolle von OCI bei der Modernisierung heutiger Datacenter ermöglicht Simulationen beim Änderungsmanagement, die Planung der Optimierung vor der Migration und die Festlegung der richtigen Serviceklasse. OCI erfasst und korreliert die Auswirkungen auf das Geschäft in Umgebungen mit mehreren Anbietern mühelos mit nur wenigen Klicks über Tausende NFS-Shares und Fibre Channel-Pfade hinweg. Von der Migration bis hin zur Technologieaktualisierung – OCI bietet den Weg zu zuverlässigen, auf das richtige Sizing ausdimensionierten Migrationen und verhindert ungeplante Serviceunterbrechungen.

## Wie „`real Time`“ überwacht OCI die Performance?

OCI wird sowohl für das Management von On-Premises- als auch von Hybrid-Cloud-Datacentern als **nahezu in Echtzeit** bezeichnet. Während die Abfrage von Datenquellen für eine häufigere Ausführung konfiguriert werden kann, profitieren die meisten Benutzer nicht von einem erheblichen analytischen Nutzen, wenn ein Intervall für die Leistungserfassung für die meisten Geräte von weniger als 5 Minuten besteht. Eine häufigere Sammlung kann die zu managenden Objekte und die durchgeführten Analysen unnötig belasten. Natürlich kann es Situationen geben, in denen eine granularere Erfassung erforderlich ist. Glücklicherweise bietet OCI vollständige Flexibilität, einschließlich konfigurierbarer Gerätebestandsdaten und Performance-

Abfrageintervalle, die an die Anforderungen Ihrer Datacenter-Umgebung angepasst sind.

### Warum unterscheidet sich mein „Total“ von meinem „Read“ plus „Write“?

In einigen Fällen können Sie feststellen, dass *Total* für einen Zähler nicht gleich der Summe von *reads* plus *writes* für diesen Zähler ist. Es gibt einige Fälle, in denen dies geschehen könnte.

**IOPS**: Zusätzlich zu Lese- und Schreibvorgängen verarbeitet ein Speicher-Array oder ein anderes Asset interne Vorgänge ohne Bezug zum Workload-Datenfluss. Diese werden manchmal als „`sSystem`“, „`metadata`“ oder einfach als „`andere`“ Vorgänge bezeichnet und können internen Prozessen wie Snapshots, Deduplizierung oder Neuzuordnung zugeordnet werden. Um die Anzahl der Systemoperationen für eine bestimmte Ressource zu ermitteln, subtrahieren Sie in diesen Fällen die Summe der IOPS *Read* und *Write* von den IOPS *Total*. Die Summe aus Lese- und Schreib-IOPS ergibt sich aus den IOPS, die direkt mit Ihrem Datenfluss verbunden sind.

**Latenz**: Die gesamte Reaktionszeit (Latenz) für einen Vorgang kann manchmal als *weniger als* die Schreibreaktionszeit gemeldet werden, da die gesamte Reaktionszeit ein zeitgewichteter Durchschnitt ist. I/O-Workloads bestehen oft aus mehr Lese- als Schreiboperationen, wobei Schreibvorgänge in der Regel größere Latenzen beobachten. Wenn ein Workload beispielsweise 10 Lesevorgänge mit einer durchschnittlichen Latenz von 5 ms und 5 Schreibvorgänge mit einer durchschnittlichen Latenz von 10 ms durchführte, wird die gewichtete durchschnittliche Gesamtlatenz als Anzahl der Lesezeiten die durchschnittliche Leselatenz berechnet, Plus die Anzahl der Schreibvorgänge mal die durchschnittliche Schreiblatenz, geteilt durch die Gesamtzahl der I/O-Vorgänge, z. B. (10 * 5 + 5 * 10) / (10 + 5) = 6,33 ms.

### Warum zeigen OCI und OCUM unterschiedliche Werte für überbelegten Speicherplatz?

Der OnCommand Unified Manager (OCUM) Begriff des „bereitgestellten“ Speicherplatzes kann Autogrow-Limits enthalten, auf die FlexVols (interne OnCommand Insight Volumes) wachsen können. Die OCI „Kapazität“ spiegelt diese Autogrow-Grenzen nicht wider. Daher wird in einer Umgebung mit Autogrow FlexVols die mit OCUM bereitgestellte Gesamtkapazität das OCI Storage-Level über dem Gesamtvolumen mit überprovisionierter Kapazität übersteigen. Das Delta ergibt den Unterschied zwischen der FlexVols Kapazität und ihrer Autogrow Kapazität.

# Management Ihrer Umgebung

Diese FAQ enthält Antworten auf häufig gestellte Fragen zum Management von OnCommand Insight-Umgebungen.

### Kann ich einem bestimmten Benutzer Zugriff auf OCI geben, während die Ansicht auf bestimmte Ressourcen beschränkt wird (d. h. SVM und zugehörige Volumes, VMs, Server)?

OCI bietet rollenbasierten Zugriff. Der Zugriff auf die Berichterstellung wird beispielsweise über die Data Warehouse-Berichte von OCI gesteuert. Berichte können geplant, per E-Mail als PDF, HTML oder CSV oder an eine Dateifreigabe oder sogar eine URL gesendet werden, bei der der Benutzer sich vor der Anzeige authentifizieren muss. Der benutzerbasierte Zugriff wird in Form von Administratoren, Benutzern und Gästen gewährt. Active Directory/ldap-Unterstützung ist ebenfalls verfügbar.

# Integration von Insight in andere Tools

In diesen FAQ werden häufig gestellte Fragen zur Integration von OnCommand Insight in andere Tools beantwortet.

## Kann OCI mit anderen Tools integriert werden und welche Integrationspunkte sind verfügbar?

Ja, OCI ist eine erweiterbare (weit offene) Lösung, die Integrationen in Orchestrierungs-, Business-Management-, Änderungs- und Ticketsysteme von Drittanbietern sowie benutzerdefinierte CMDB-Integrationen ermöglicht. Die vollständig veröffentlichte RESTful API von OCI und die offenen Integrationspunkte der MySQL Datenbank ermöglichen ein einfaches und effektives Verschieben von Daten, sodass Benutzer nahtlos auf ihre Daten zugreifen können.

Die Swagger-basierte API-Dokumentation von Insight finden Sie im Produkt unter **(?) Hilfe > REST API Dokumentation**.

## Was ist der Insight BMC Connector?

Der OnCommand Insight Connector für BMC integriert das OnCommand Insight Data Warehouse (DWH) und die BMC Atrium Configuration Management Database (CMDB). Insight Connector für BMC ordnet physische und logische gespeicherte Daten zu Netzwerk-Storage-Systemen (z. B. Storage-Einheiten, Host Storage-Services, VS Storage Service und VM Storage Service) und ihre Beziehungen zu Geräten (Hosts, Storage Switches, Und Tapes) und importiert sie als Konfigurationselemente und -Beziehungen in die BMC-CMDB. Weitere Informationen zum OnCommand Insight Connector für BMC erhalten Sie auf der NetApp Support-Website.

## Funktioniert OCI mit SCOM oder VROPs?

Ja, OCI ergänzt eine Reihe von Geschäftsmanagementlösungen und wird als maßgebliche Quelle für Informationen zu Storage, Computing, Hypervisor und Fabric für das Datacenter angesehen. OCI Kunden nutzen die RESTful API und die erweiterbare MySQL Datenbank von OCI, um zahlreiche Applikationen wie BMC Remedy, ServiceNow, SCOM, Vrops und Splunk zu erweitern. Um nur einige zu nennen. OCI erweitert die Integration, indem Informationen aus nahezu jeder Datenquelle importiert und/oder die erfassten Umgebungsmetriken an beliebte Monitoring-, Ticketing-, CMDB-Abrechnungs- und Orchestrierungssysteme von Drittanbietern gesendet werden.

## Kann OCI mit Cloud-Services verwendet werden, die ich bereits verwendet habe oder die ich in Betracht ziehe?

Ja, das Management von OCI sowohl für herkömmliche lokale als auch für flexible Hybrid-Cloud-Umgebungen bietet Transparenz bei der Ermittlung der besten, kostengünstigsten Plattform für die Anforderungen von Business-Services. OCI kann für Analysen vor und nach der Migration genutzt werden, um Workloads zu ermitteln, die sich für die Cloud eignen. Zur Auswahl des geeigneten Cloud-Services sind historische Kapazitätstrends, Performance und Kosten erforderlich. Workshops für das Servicedesign mit der I/O-Dichte von OCI und anderen Metriken können Sie zudem bei der Beantwortung von Fragen wie der Optimierung Ihrer Umgebung und der Frage, ob die Cloud sinnvoll ist, unterstützen. OCI unterstützt NetApp Private Storage, Cloud ONTAP, Amazon S3 und OpenStack KVM und erweitert damit seine Abdeckung weiter. OCI spielt weiterhin eine wichtige Rolle bei der Cloud-Management-Kampagne von NetApp, insbesondere in den Bereichen Kapazitätsplanung, Performance, Service-Qualität und Chargeback.

### Kann OCI Vorfälle in unserer Vorfallmanagement-Lösung eröffnen?

Ja, OCI-Verstoßereignisse können über SNMP als Trap oder per Syslog an einen Server und einige über RESTful API ausgelöst und gesendet werden. Die Details, die innerhalb der bereitgestellten Ereignisse enthalten sind, können von vielen Incident Management- und Ticketing-Lösungen von Drittanbietern interpretiert werden.

### Können Sie einer Geschäftseinheit oder Abteilung Ressourcen zuweisen?

Ja, OCI umfasst eine Methode des Metadaten-Tagging namens Annotationen. Geschäftseinheiten, Geschäftsbereiche, Mandanten und Projekte können Datacenter-Ressourcen zugewiesen werden, um einen umfassenderen Geschäftskontext zu Ressourcen, Kapazitätsplanung, Fehlerbehebung und Berichterstellung zu erhalten.

### Funktioniert OCI mit Work Flow Automator (WFA)?

Die Integrationsfunktionen von OCI mit CMDB-, Abrechnungs- und Orchestrierungstechnologien von Drittanbietern sind ein wichtiger Wert für seinen Erfolg, und WFA ist keine Ausnahme. NetApp Professional Services haben verschiedene erfolgreiche Integrationen mit WFA Workflows und OCI durchgeführt.

### Wie lange dauert die OCI-Aufbewahrungsdauer für Performance-Daten?

Der OCI Server hält 90 Tage Performance nahezu in Echtzeit sowie den aktuellen (Point-in-Time) Bestand (logische und physische Konstrukte).

Die Performance-Polling-Intervalle von OCI lassen sich vom Benutzer konfigurieren. Die Storage-Performance wird bei den meisten Anbietern in der Regel alle 5 Minuten konfiguriert. Performance-/Bestandsdaten werden täglich zum OCI Data Warehouse (DWH) gesendet, um langfristige Verlaufsberichte und Prognosen zu erstellen. DWH wandelt diese Daten in zusammengefasste Daten um (stündliche, tägliche, monatliche Rollup-Daten). Unsere Fähigkeit, „`changes`“ nachzuverfolgen, z. B. den überwachten Umgebungsverlauf für Storage-/Compute-/Fabric-Konfigurationen/Zuordnungen, hat derzeit keine definierten Grenzen.

Data Warehouse speichert historische Daten auf der Grundlage der Daten und Granularität.

### Gibt es Berichte zur Performance-Planung?

Ja, es gibt mehrere Berichte für OCI und viele andere in unserem Katalog der Professional Services basierend auf einem Anwendungsfall. Das Data Warehouse-Modul enthält außerdem eine Reihe von Cognos-Tools zur Berichterstellung, mit denen Benutzer ihre eigenen Berichte erstellen können.

# Data ONTAP Storage-IOPS

In diesen FAQ werden häufig gestellte Fragen beantwortet, die zeigen, wie IOPS-Werte von Data ONTAP Storage-Systemen abgeleitet werden.

### Die abgeleitet von Storage-IOPS aus Data ONTAP Storage-Systemen

- IOPS auf Storage Array-Ebene werden von den internen IOPS-Volumes aggregiert
- IOPS auf Storage Node-Ebene umfassen Metadaten-OPS
- IOPS auf Storage Pool-Ebene schließt Metadaten-OPS aus; misst nur die Festplatten
- Die internen IOPS auf Volume-Ebene umfassen Lese- und Schreib-OPS (Operationen) + andere OPS

## Frage - wie können die aggregierten IOPS manchmal höher sein als Knoten-IOPS?

Vor Clustered Data ONTAP 8.3.1 setzen sich Node-IOPS aus Protokoll-IOPS zusammen. Mit Clustered Data ONTAP 8.3.1. Und später setzen sie sich aus Kennzahlen der Systemkomponenten zusammen. Sie beinhalten „nur“ Anfragen nach Daten, Anfragen die durch die Eingangstür kommen, aber keine Backend-Aufgaben wie Snapmirrors, Deduplizierung usw. Andererseits produzieren diese Aufgaben Festplatten-IOPS und somit IOPS-Aggregate. Daher könnten Sie aggregierte IOPS sehen, die höher sind als die Knoten-IOPS.

## Frage: Wie werden Meta-Daten oder andere OPS berechnet

Sonstige Vorgänge = Gesamt - (Lesen + Schreiben)

# Anleitungen

## Erste Schritte mit Insight

Nachdem OnCommand Insight installiert und ordnungsgemäß lizenziert wurde, sollten Sie einige Aufgaben durchführen, um die Umgebung auf die Darstellung der für Sie wichtigen Daten vorzubereiten.

In einer typischen Umgebung werden u. a. folgende Aufgaben ausgeführt:

1. **Anmerkungen zu Ihren Assets**, um sie für Abfragen und Berichte vorzubereiten. Nützliche erste Annotationen umfassen in der Regel Datacenter, Tiering und Service Level.
2. **Abfragen erstellen**, um wichtige Daten anzuzeigen und bei der Fehlersuche zu helfen
3. **Zuweisen von Anwendungen** und **Geschäftseinheiten** zu Assets
4. **Erstellen von Leistungsrichtlinien** und **Alerts** für Verstöße gegen diese Richtlinien
5. **Erstellen von benutzerdefinierten Dashboards**, um Daten je nach Bedarf oder Benutzerrolle hervorzuheben

### Einrichten von Benachrichtigungen

Sie können Insight so konfigurieren, dass Benachrichtigungen bei auslösenden Ereignissen wie Performance-Richtlinie, globalem Pfad oder Kapazitätsverletzungen per E-Mail, SNMP oder Syslog gesendet werden. Sie können Insight auch so konfigurieren, dass E-Mail-Benachrichtigungen bei Ereignissen auf Systemebene wie Datenquellfehlern oder Ausfällen der Erfassungseinheiten gesendet werden.

Dies sind grundlegende Anweisungen. Weitere Informationen zu Benachrichtigungen finden Sie unter Konfiguration und Administration > Insight-Konfiguration und -Administration > Einrichten von Insight.

#### Einrichten von E-Mails für Benachrichtigungen

Insight kann bei auslösenden Ereignissen, z. B. bei Verstößen gegen Performance-Richtlinien, E-Mail-Benachrichtigungen senden.

##### Über diese Aufgabe

Führen Sie die folgenden grundlegenden Schritte aus, um E-Mail-Benachrichtigungen zu konfigurieren:

##### Schritte

1. Klicken Sie auf **Admin** > **Benachrichtigungen** und gehen Sie zum Abschnitt **E-Mail**.
2. Geben Sie im Feld **Server** den Namen Ihres SMTP-Servers ein. Sie können entweder einen vollständig qualifizierten Domänennamen oder eine IP-Adresse eingeben.
3. Geben Sie Ihren SMTP-Benutzernamen und (falls von Ihrem SMTP-Server erforderlich) das Kennwort ein.
4. Geben Sie im Feld **Absender-E-Mail** das E-Mail-Konto des Absenders ein, das in den Benachrichtigungen als Absender identifiziert wird.

   Dieses Konto muss ein gültiges E-Mail-Konto in Ihrem Unternehmen sein.

5. Geben Sie in das Feld **Email Signature** einen beliebigen Text ein, der in jede gesendete E-Mail eingefügt werden soll.
6. Klicken Sie im Feld **Empfänger** auf + Um eine E-Mail-Adresse einzugeben, und klicken Sie auf **OK**.
7. Klicken Sie Auf **Speichern**.

   Um eine E-Mail-Adresse zu bearbeiten oder zu entfernen oder eine Test-E-Mail zu senden, wählen Sie die Adresse aus, und klicken Sie auf die entsprechende Schaltfläche, die angezeigt wird.

   Beachten Sie, dass Sie Insight so konfigurieren können, dass E-Mail-Benachrichtigungen für bestimmte Verstöße gegen Performance-Richtlinien an bestimmte Personen oder Gruppen gesendet werden. Beispielsweise können Sie Verstöße gegen Cloud-Ressourcen an eine Gruppe und physische Hostereignisse an eine andere Gruppe senden. Gehen Sie zu **Verwalten** > **Leistungsrichtlinien**, um einzelne Richtlinienbenachrichtigungen zu konfigurieren.

### Einrichten von Syslog für die Protokollierung

Insight kann Syslog-Ereignisse bezüglich Kapazitäts- oder Pfadverletzungen und Performance-Warnmeldungen versenden.

#### Über diese Aufgabe

Führen Sie die folgenden grundlegenden Schritte aus, um die Syslog-Benachrichtigung in Insight zu konfigurieren:

#### Schritte

1. Klicken Sie auf **Admin** > **Notifications** und gehen Sie zum Abschnitt **Syslog**.
2. Aktivieren Sie das Kontrollkästchen **Syslog enabled**.
3. Geben Sie im Feld **Server** die IP-Adresse des Protokollservers ein.
4. Wählen Sie im Feld **Anlage** die Einrichtungsebene aus, die dem Programmtyp entspricht, der die Nachricht protokolliert.
5. Klicken Sie Auf **Speichern**.

### Einrichten von SNMP für Benachrichtigungen

Insight kann SNMP-Benachrichtigungen an auslösende Ereignisse senden, z. B. Verstöße oder Schwellwerte der Datenquelle.

#### Über diese Aufgabe

Führen Sie die folgenden grundlegenden Schritte aus, um SNMP in Insight zu konfigurieren:

#### Schritte

1. Klicken Sie auf **Admin** > **Notifications** und gehen Sie zum Abschnitt **SNMP**.
2. Klicken Sie auf **actions** und wählen Sie **Trap-Quelle hinzufügen**.
3. Geben Sie im Dialogfeld **SNMP-Trap-Empfänger hinzufügen** die **IP**-Adresse und **Port** ein, an die Sie SNMP-Trap-Nachrichten senden möchten. Verwenden Sie für **Community String** „`public`“ für SNMP-Trap-Nachrichten.

4. Klicken Sie Auf **Speichern**.

## Vorbereiten von Assets: Kommentieren

Mit Anmerkungen können Sie den ausgewählten Assets bestimmte Tags oder Beschriftungen zuordnen, was die Verwaltung und Berichterstellung für diese Assets erleichtert.

#### Erstellen von Anmerkungen für Ihr Unternehmen

In diesem Leitfaden wird beschrieben, wie Sie Anmerkungen für Ihre Umgebung erstellen und anpassen, die für Abfragen, Filtern, Benachrichtigungen und Berichte verwendet werden können.

Eine Annotation ist eine Notiz oder ein Tag, die Sie bestimmten Assets in Ihrer Umgebung zuordnen. OnCommand Insight enthält mehrere Annotationen, die Sie je nach Bedarf für Ihre Assets konfigurieren können oder Ihre eigenen benutzerdefinierten Annotationen basierend auf Ihren geschäftlichen Anforderungen erstellen können.

Die folgenden Beispiele sind diejenigen, die in der Regel zuerst in neuen Kundenumgebungen konfiguriert wurden, um als Grundlage für zusätzliche Aktionen zu dienen. Ihre eigenen Anforderungen an Anmerkungen können variieren, aber die hier beschriebenen Schritte können als Anleitung zur Konfiguration aller Anmerkungen verwendet werden, die Sie für die gewünschten Anlagen benötigen.

Dieser Leitfaden basiert auf folgenden Annahmen:

- Sie haben OnCommand Insight Server installiert und ordnungsgemäß lizenziert.
- Sie möchten Best Practices erkunden, nicht jede verfügbare Option.
- Sie verstehen, dass dies nur Beispiele sind und dass Ihre spezifischen Anforderungen variieren können.

In diesem Handbuch erfahren Sie, wie Sie vorhandene Anmerkungen ändern und benutzerdefinierte Anmerkungen erstellen

In unserer Beispielumgebung möchten wir Assets nach Datacenter, Tier, Service Level und Umgebung auflisten können.

#### Konfigurieren von Anmerkungen zum Rechenzentrum

Die Anmerkung des Datacenters wird in der Regel verwendet, um ein Storage-Array, einen Switch oder eine physische Host-Ressource einem Datacenter-Standort zuzuordnen. Sie können die Annotation des Datacenters auch anderen Assets in Ihrer Umgebung zuordnen.

Schritte

- Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
- Wählen Sie **Verwalten** > **Anmerkungen**.
- Wählen Sie die Anmerkung **Data Center** und klicken Sie auf das Symbol **Bearbeiten**.
- Klicken Sie auf **+Add**, und fügen Sie den Namen und die Beschreibung Ihres ersten Rechenzentrums zur Anmerkungsliste hinzu.

- Gleichen Sie für Ihre anderen Rechenzentren.
- Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Beispiele für Anmerkungen zum Rechenzentrum:

| Name | Beschreibung |
| --- | --- |
| DC1_SVL | Sunnyvale Geb. 1 |
| DC2_SVLb3 | SVL geb. 3 eng |
| DC3_NY | New York |
| DC4_London | London |
| … | |

Insight bietet mehrere Out-of-the-Box-Anmerkungstypen, mit denen Benutzer Werte gemäß ihren Anforderungen definieren oder ändern können. Diese standardmäßigen Anmerkungstypen sind immer für die Web-Benutzeroberfläche von Insight und für die Berichterstellung verfügbar. Neu erstellte benutzerdefinierte Annotationen sind auf der Web-Benutzeroberfläche von Insight sichtbar, erfordern jedoch zusätzliche Maßnahmen, um sie für die Berichterstellung zur Verfügung zu stellen. Für Informationen über das Einfügen benutzerdefinierter Anmerkungen in Berichte. Wenden Sie sich an Ihren Ansprechpartner im NetApp Customer Support.

Einige Benutzer sind möglicherweise geneigt, die Länderanmerkung zum Festlegen der Anlagenstandorte zu verwenden, im Gegensatz zu oder in Verbindung mit der Anmerkung zum Rechenzentrum. Beachten Sie jedoch, dass die Länderanmerkung im Insight Data Warehouse als benutzerdefinierter Anmerkungstyp behandelt wird und daher möglicherweise nicht in der gleichen Granularität wie das Data Center angezeigt wird.

**Konfigurieren Sie die Beschriftungen der Ebenen**

Die Tier-Annotation wird verwendet, um Anlagen ihren jeweiligen Tiers zuzuordnen, zum Beispiel für die Kostenabrechnung. Insight verfügt über eine Reihe von standardmäßigen Tiering-Annotationen. Sie können diese je nach Ihren Tiering-Namenskonventionen ändern oder Ihre eigenen Tiers nach Bedarf erstellen.

Beachten Sie beim Festlegen von Tier-Anmerkungen Folgendes:

- Die Kosten gelten pro Gigabyte.
- Tier 1, 2, 3 sind Standardebenen, die auf Speicherarrayebene nach Festplattentyp konfiguriert werden. Viele Kunden würden jedoch innerhalb eines Arrays oder über Arrays desselben Typs hinweg mehrere Festplattentypen bereitstellen.
- Als Best Practice empfiehlt es sich, Tiering-Annotationen basierend auf Festplattentyp und/oder Festplattengeschwindigkeit zu erstellen. Dies ist eine typische Tier-Methodik, von der Ihre eigenen Anforderungen abweichen können.

Schritte

- Wählen Sie die Anmerkung **Tier** und klicken Sie auf das Symbol **Bearbeiten**.
- Klicken Sie bei Bedarf auf **+Add**, und fügen Sie den Namen und die Beschreibung Ihrer ersten Schicht zur Anmerkungsliste hinzu.
- Tun Sie das gleiche für Ihre anderen Ebenen.
- Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Beispiele für Tier-Anmerkungen:

| Name | Beschreibung | Kosten pro GB |
|---|---|---|
| Auto-Tiering | Automatisiertes Storage Tiering | 0.5 |
| Tier-1-SSD | Rein Flash-Basiertes Array | 0.5 |
| Tier 2 SAS | SAS | 0.25 |
| Tier 3 SATA | SATA | 0.1 |
| … | | |

#### Konfigurieren Sie Service-Level-Anmerkungen

## Die Anmerkung zum Service-Level wird verwendet, um Anlagen ihren jeweiligen Service-Levels zuzuordnen.

Service-Level-Annotationen werden normalerweise nur in Kundenumgebungen festgelegt, die Auto-Tiering verwenden. Im Insight Data Warehouse wird Tiering bevorzugt. Als Best Practice empfiehlt es sich jedoch, den Service-Level zu verwenden, wenn Sie Details zu den bereitgestellten Kosten und zu den bereitgestellten Kosten im Detail anzeigen möchten Kundenkosten. Wenn beide in Data Warehouse vorhanden sind, ersetzt Service Level die Ebene.

Schritte

- Wählen Sie die Anmerkung **Service Level** und klicken Sie auf das Symbol **Bearbeiten**.
- Klicken Sie auf **+Add**, und fügen Sie den Namen und die Beschreibung Ihres ersten Service-Levels zur Anmerkungsliste hinzu.
- Tun Sie dasselbe für Ihre anderen Service-Level.
- Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Beispiel für Anmerkungen zum Service-Level:

| Name | Beschreibung | Kosten pro GB |
|---|---|---|
| Service-Level 1 | FAS Controller mit FC oder SAS, lokale & Remote-Spiegelung und Band | 0.93 |

| | | |
|---|---|---|
| Service-Level 2 | FAS-Controller mit FC oder SAS, lokalen und Remote-Spiegelungen | 0.85 |
| Service-Level 3 | FAS Controller mit SATA und lokaler Spiegelung | 0.48 |
| … | | |

#### Konfigurieren Sie Anmerkungen zur benutzerdefinierten Umgebung

Die Umgebungsanmerkung ist eine benutzerdefinierte Anmerkung zur Zuordnung von Anlagen zu ihrem jeweiligen Umgebungsort oder ihrer Verwendung, z. B. Labor, Forschung und Entwicklung, Produktion, Usw. Durch die Erstellung der Umgebungsanmerkung und die Einstellung auf diese Ressourcen können Sie Ihre Laborressourcen einfach separat von Ihren Produktionsanlagen finden, filtern und Berichte erstellen.

Schritte

- Wählen Sie **Verwalten** > **Anmerkungen**.
- Klicken Sie oben auf der Seite auf die Schaltfläche **+Add**.
- Geben Sie für **Name** ‘**Environment**’ ein.
- Geben Sie für **Description** ‘**Asset environment type**’ ein.
- Wählen Sie für **Typ Liste**. Neue Felder werden angezeigt, damit Sie Ihre Liste erstellen können.
- Lassen Sie jetzt **Neue Assets spontan hinzufügen** deaktiviert. Aktivieren Sie diese Option, wenn Sie der Auswahlliste neue Umgebungen hinzufügen möchten, während Sie sie gleichzeitig mit Assets verknüpfen.
- Geben Sie den Namen und die Beschreibung Ihrer ersten Umgebung ein.
- Klicken Sie auf **+Add** und tun Sie das gleiche für Ihre anderen Umgebungen.
- Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Beispiele für Umgebungskommentare:

| Name | Beschreibung |
|---|---|
| Labor | Labor |
| Abw | Entwicklung |
| Prd | Produktion |
| … | |

## Suchen von Assets: Abfragen

Mit leistungsstarken Abfragen können Sie einfach Assets in Ihrer Umgebung finden und anzeigen.

#### Verwenden von Abfragen zum Kommentieren von Assets

Nachdem Sie nun Ihre ersten Anmerkungen erstellt haben, wollen wir uns ansehen, wie Sie diese Anmerkungen mit bestimmten Assets verknüpfen.

In den folgenden Beispielen werden diese Anmerkungen auf bestimmte Assets angewendet. Beispielsweise erstellen wir eine Abfrage, um alle Storage-Arrays aufzulisten, die sich in einem bestimmten Datacenter befinden, und diese mit der entsprechenden Anmerkung zu markieren. Dies gilt auch für Ressourcen, die zu einer bestimmten Ebene und einem bestimmten Service-Level gehören.

#### Abfragen und Kommentieren von Rechenzentren

Mithilfe von Abfragen verknüpfen Sie Ihre Annotationen mit den entsprechenden Assets Ihrer Umgebung. In diesem Beispiel verknüpfen wir die Datacenter-Annotationen mit ausgewählten Assets.

Während der Datenerfassung sammelt Insight (neben anderen Informationen) die Namen der erkannten Ressourcen. In diesem Beispiel werden wir davon ausgehen, dass alle Ihre Storage-Arrays nach dem Datacenter benannt wurden, in dem sie sich befinden, wie z. B. „`SVL_NN_<label>`“ für Arrays in Sunnyvale. Mit Insight-Abfragen lassen sich diese Assets einfach kommentieren.

- Melden Sie sich bei Insight als Benutzer mit administrativen Berechtigungen an
- Wählen Sie **Abfragen** > **+Neue Abfrage**
- Drop-down das Feld **Suchen nach…** und wählen Sie **Speicher**. Eine Liste aller Speicher-Arrays wird angezeigt.
- Geben Sie im Filterfeld **Name** „`SVL`“ ein, und klicken Sie auf (Oder drücken Sie die Eingabetaste). Die Liste der Abfrageergebnisse wird jetzt aktualisiert, um nur die Arrays anzuzeigen, die die Zeichenfolge „`SVL`“ enthalten.
- Beim Filtern können Sie jedes der folgenden Zeichen allein oder kombiniert verwenden, um Ihre Suche in einem beliebigen Textfeld auf der Abfrageseite zu verfeinern:
  - Mit einem Sternchen können Sie nach allem suchen. Beispiel: „`vol*RHEL`“ zeigt Assets an, die mit „`vol`“ beginnen und mit „`RHEL`“ enden.
  - Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Wenn Sie beispielsweise nach „`SVL-PRD??-S12`“ filtern, werden SVL-PRD12-S12, SVL-PRD13-S12 usw. angezeigt.
  - Mit dem Operator ODER können Sie mehrere Einheiten angeben. Beispielsweise kann „`FAS2240 ODER CX600 ODER FAS3270`“ mehrere Storage-Modelle finden.
- Wählen Sie die Speicherarrays aus, die Sie diesem Rechenzentrum zuordnen möchten. Wenn alle gewünschten Arrays ausgewählt sind, klicken Sie auf die Schaltfläche **Aktionen** und wählen **Anmerkung bearbeiten**.
- Wählen Sie im Dialogfeld **Anmerkung hinzufügen** die Anmerkung **Data Center** aus.
- Wählen Sie den gewünschten **Wert** aus, z. B. „`DC1_SVL`“.

- Klicken Sie Auf **Speichern**.
- Wenn die Spalte Rechenzentrum auf der Seite Abfrageergebnisse nicht sichtbar ist, wählen Sie sie aus, indem Sie die Schaltfläche **Spalten** herunterfahren und **Rechenzentrum** wählen.
- Falls gewünscht, können Sie die Abfrage für die zukünftige Verwendung speichern, indem Sie oben rechts auf der Seite Abfrage auf die Schaltfläche **Speichern** klicken und ihr einen eindeutigen und expliziten Namen geben. Beispiel: „`Storage Arrays - SVL Data Center`“.

Wenn Sie die Anmerkung „`SVL`“ mit anderen Assets verknüpfen möchten, erstellen Sie eine neue Abfrage und befolgen Sie diese Schritte für jeden gewünschten Asset-Typ.

Wiederholen Sie diese Schritte für Ressourcen in jedem Ihrer Datacenter.

#### Ebenen abfragen und beschriften

## Mithilfe von Abfragen verknüpfen Sie Ihre Annotationen mit den entsprechenden Assets Ihrer Umgebung. In diesem Fall ordnen wir diese Tiers den entsprechenden Assets zu.

Lassen Sie uns Anmerkungen für Ihre Tiers erstellen. In diesem Beispiel verknüpfen wir Tiers mit Storage-Pools und nehmen an, dass Ihre Tier-Annotationen wie folgt konfiguriert sind:

| Wert | Beschreibung | Kosten pro GB |
|---|---|---|
| Tier-1-SSD | Rein Flash-Basiertes Array | 0.5 |
| Tier 2 SAS | SAS | 0.25 |
| Tier 3 SATA | SATA | 0.1 |

Suchen wir nach allen SSD-Festplatten in Ihrer Umgebung und ordnen Sie ihnen die Beschriftung „`Tier 1 SSD`“ zu.

- Melden Sie sich bei Insight als Benutzer mit administrativen Berechtigungen an
- Wählen Sie **Abfragen** > **+Neue Abfrage**
- Drop-down das Feld **Suchen nach…** und wählen Sie **Speicherpool**. Eine Liste aller Speicherpools wird angezeigt.
- Das Feld **Name** ist dieses Mal möglicherweise nicht hilfreich, also verwenden wir ein anderes Feld. Klicken Sie auf das Dropdown-Menü **Mehr** und wählen Sie „`am wenigsten performant Disk type`“ aus. In diesem Feld werden die für uns interessanten Festplattentypen aufgeführt. Geben Sie „`SSD`“ in das Feld ein, und klicken Sie auf Schaltfläche. In der Abfrageergebnisliste werden nur Ihre SSD-Speicherpools angezeigt.
- Sie können weiter filtern, indem Sie auf das Dropdown-Menü **Mehr** klicken und zusätzliche Felder auswählen.
- Wählen Sie die Speicherpools aus, die Sie diesem Tier zuordnen möchten. Wenn alle gewünschten Speicherpools ausgewählt sind, klicken Sie auf die Schaltfläche **Aktionen** und wählen **Anmerkung bearbeiten**.
- Wählen Sie im Dialogfeld **Anmerkung hinzufügen** die Anmerkung **Tier** aus.
- Wählen Sie den gewünschten **Wert** aus der Liste aus. Wählen Sie für dieses Beispiel „`Tier 1 SSD`“.

- Klicken Sie Auf **Speichern**.
- Wenn die Spalte „Ebene“ auf der Seite „Abfrageergebnisse“ nicht angezeigt wird, wählen Sie sie aus, indem Sie die Schaltfläche **Spalten** herunterfahren und **Ebene** wählen. Sie sollten die entsprechende Anmerkung sehen, die jetzt Ihren Assets zugeordnet ist.
- Speichern Sie die Abfrage, indem Sie oben rechts auf der Seite Abfrage auf die Schaltfläche **Speichern** klicken und ihr einen eindeutigen und expliziten Namen geben. Beispiel: „`Storage Pools - Tier 1 SSD`“.

Wenn Sie die Annotation „`Tier 1 SSD`“ anderen Assets zuordnen möchten, erstellen Sie eine neue Abfrage und führen Sie die folgenden Schritte für jeden gewünschten Asset-Typ aus.

Wiederholen Sie diese Schritte für die Assets in jeder Ihrer verbleibenden Tiers.

#### Anmerkungen zu Service-Level und Umgebung

Fügen Sie mithilfe der von Ihnen gelernten Schritte und Konzepte Anmerkungen zu Service-Level und Umgebung zu den entsprechenden Ressourcen hinzu.

Um den entsprechenden Assets in Ihrer Umgebung Anmerkungen zu Service-Level und Umgebung hinzuzufügen, befolgen Sie die oben aufgeführten Schritte, um die gewünschten Assets und die entsprechenden Anmerkungen zum Service-Level oder zur Umgebung auszuwählen. Sie können mit denselben Assets mehrere Annotationen verknüpft sein. In der Tat ermöglicht Ihnen dieses Verfahren mehr Flexibilität beim Management Ihrer Umgebung durch Insight.

Nachdem Sie nun Abfragen erstellt haben, um Ihre Assets mit Anmerkungen zu versehen, können Sie diese Anmerkungen auf verschiedene Weise verwenden, z. B.:

- Performance-Richtlinien zur Benachrichtigung bei Ereignissen auf gewünschten Assets
- Benutzerdefinierte Dashboards und Widgets zur Überwachung der Aktivität
- Berichterstellung

## Ihre Unternehmensstruktur: Einrichtung von Geschäftseinheiten und Anwendungen

Wenn Sie die Elemente Ihrer Unternehmensstruktur verstehen, können Sie die Ressourcennutzung verfolgen und Kostenberichte erstellen.

#### Konfigurieren von Geschäftseinheiten für Ihr Unternehmen

Wenn Sie die Geschäftselemente Ihrer Unternehmensstruktur verstehen, können Sie die Ressourcennutzung verfolgen und Kostenberichte erstellen. Hier konfigurieren wir Ihre Unternehmenseinheiten.

##### Über diese Aufgabe

Mit OnCommand Insight können Sie Geschäftseinheiten in einer Hierarchie definieren, die bis zu vier Granularitätsstufen umfasst.

- **Mieter**

  Wird in erster Linie von Dienstleistern zur Zuordnung von Ressourcen zu einem Kunden verwendet. Die

Mandantenebene ist erforderlich, wenn Ihr Unternehmen ein ISP ist und Sie die Ressourcennutzung von Kunden verfolgen möchten.

- **Geschäftsbereich**

  Ein Geschäftsbereich oder eine Produktlinie innerhalb eines Unternehmens, z. B. Storage. Geschäftsbereich ist in der Hierarchie erforderlich, wenn die Daten für verschiedene Produktlinien nachverfolgt werden müssen.

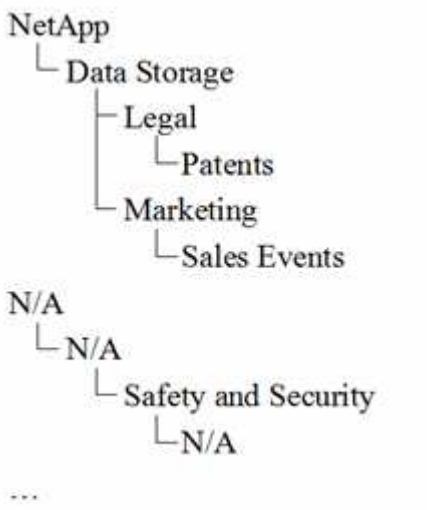
- **Geschäftsbereich**

  Repräsentiert eine traditionelle Geschäftseinheit wie Legal oder Marketing. Die Geschäftseinheit ist erforderlich, wenn Sie die Daten verschiedener Abteilungen nachverfolgen müssen. Diese Hierarchieebene ist oft wertvoll, wenn es darum geht, eine Ressource zu trennen, die von einer Abteilung genutzt wird, die von anderen Abteilungen nicht genutzt wird.

- * Projekt*

  Wird häufig zur Identifizierung eines bestimmten Projekts in einer Geschäftseinheit verwendet, für das Kapazitätszuordnung gewünscht wird. Beispielsweise kann „`Patente`“ ein Projektname für die Rechtsabteilung und „`Verkaufsveranstaltungen`“ ein Projektname für die Geschäftseinheit Marketing sein. Beachten Sie, dass die Namen der Ebenen Leerzeichen enthalten können.

Ein Beispiel für eine Unternehmenshierarchie wäre:




Best Practice: Erstellen Sie eine Tabelle mit jeder Zeile, die eine vollständige Geschäftseinheit in Ihrer Hierarchie zeigt:

| Mandant | Geschäftsbereich | Geschäftsbereich | Projekt |
|---|---|---|---|
| NetApp | Datenspeicher | Legal | Patente |
| NetApp | Datenspeicher | Marketing | Verkaufsveranstaltungen |
| 1. A. | 1. A. | Sicherheit | 1. A. |

| … | | | |
|---|---|---|---|

Sie müssen nicht alle Ebenen für das Design Ihrer Unternehmenshierarchie verwenden. Sie können „N/A“ für nicht verwendete Stufen auswählen.

So erstellen Sie eine Unternehmenshierarchie in Insight:

#### Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
2. Wählen Sie **Verwalten** > **Business Entities**.
3. Klicken Sie auf die Schaltfläche **+Add**
4. Klicken Sie in das Feld **Tenant** und geben Sie Ihren Mieternamen ein.

   Wenn Sie bereits Mandanten für Ihre Umgebung eingegeben haben, wird eine Liste der vorhandenen Mandanten angezeigt, aus der Sie auswählen können. Sie können auch „N/A“ wählen, wenn der Mandant für diese Geschäftseinheit nicht zutrifft.

5. Wiederholen Sie dies für **Geschäftsbereich**, **Geschäftsbereich** und **Projekt**.
6. Klicken Sie Auf **Speichern**

#### Nachdem Sie fertig sind

Best Practices:

- Ordnen Sie Ihre Unternehmenshierarchie in einer Tabelle zu, und überprüfen Sie, ob die Namen in der Hierarchie in den Ansichten und Berichten von Insight selbsterklärend sind.
- Erstellen Sie Ihre Geschäftseinheiten in Insight, bevor Sie Anwendungen erstellen.
- Identifizieren und Auflisten aller Applikationen, die den einzelnen Geschäftsbereichen zugeordnet werden

### Konfigurieren von Anwendungen für Ihr Unternehmen

Wenn Sie sich mit den in Ihrer Unternehmensumgebung verwendeten Applikationen auskennen, behalten Sie die Übersicht über die Asset-Nutzung und erstellen Kostenberichte. Hier konfigurieren wir die Anwendungen Ihres Unternehmens und ordnen sie den entsprechenden Assets zu.

#### Über diese Aufgabe

Im Abschnitt *Konfigurieren von Geschäftseinheiten für Ihr Unternehmen* haben wir einige Geschäftseinheiten erstellt und empfohlen, alle Anwendungen aufzulisten, die Sie mit jeder Geschäftseinheit verknüpfen. Mit OnCommand Insight können wir Daten, die mit diesen Applikationen verbunden sind, beispielsweise zur Nutzung oder Kostenberichterstellung nachverfolgen.

Bevor Sie Daten zu den in Ihrer Umgebung ausgeführten Applikationen nachverfolgen können, müssen Sie zunächst diese Applikationen definieren und sie den entsprechenden Assets zuordnen. Applikationen können folgenden Assets zugewiesen werden: Hosts, virtuelle Maschinen, Volumes, interne Volumes, qtrees, Freigaben und Hypervisoren:

In dieser Anleitung möchten wir die Verwendung virtueller Maschinen nachverfolgen, die das Marketingteam für seine Exchange-E-Mail verwendet. Sie werden sich an die folgende Tabelle erinnern, die wir bei der Definition unserer Geschäftseinheiten erstellt haben. Fügen wir diesem Arbeitsblatt eine Spalte mit den Anwendungen hinzu, die von den einzelnen Unternehmenseinheiten verwendet werden. (Diese Tabelle ist nur ein Beispiel für ein Arbeitsblatt. In der Tabelle Business Entities in Insight wird keine Spalte „`Applications`“ angezeigt.)

| Mandant | Geschäftsbereich | Geschäftsbereich | Projekt | Applikationen Unterstützt |
|---|---|---|---|---|
| NetApp | Datenspeicher | Legal | Patente | Oracle Identity Manager, Oracle On Demand, PatentWiz |
| NetApp | Datenspeicher | Marketing | Verkaufsveranstaltungen | Exchange, gemeinsam genutzte Oracle-Datenbank, BlastOff Event Planner |
| 1. A. | 1. A. | Sicherheit | 1. A. | 1. A. |
| … | | | | |

- Erstellen von Anwendungen in Insight:*

#### Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
2. Wählen Sie **Verwalten** > **Anwendungen**
3. Klicken Sie auf die Schaltfläche **+Add**
4. Geben Sie den Namen der Anwendung ein (geben Sie für unser Beispiel „`Exchange`“ ein)
5. Wählen Sie eine Priorität für die Anwendung aus
6. Wenn Sie die Anwendung einer Business Entity zuordnen möchten, wählen Sie eine aus der Dropdown-Liste **Business Entity** aus. Andernfalls können Sie diese Option als „`Keine`“ belassen.
7. Wenn Sie sicherstellen möchten, dass jeder Host Zugriff auf dieselben Volumes in einem Cluster hat, stellen Sie sicher, dass das Kontrollkästchen **Validieren der Volume-Freigabe** aktiviert ist. Beispielsweise müssen Hosts in Hochverfügbarkeits-Clustern oft für Failover auf dieselben Volumes maskiert werden, allerdings müssen Hosts in verwandten Applikationen in der Regel nicht auf dieselben physischen Volumes zugreifen. Außerdem müssen Sie gemäß den Richtlinien möglicherweise aus Sicherheitsgründen nicht in Verbindung stehende Anwendungen nicht auf dieselben physischen Volumes zugreifen können. Wenn Sie keine Volume-Freigabe verwenden, deaktivieren Sie das Kontrollkästchen **Volume-Freigabe validieren**. Dies erfordert die Assure-Lizenz.
8. Klicken Sie auf Speichern .
9. Wiederholen Sie diesen Vorgang für alle anderen Anwendungen in Ihrer Umgebung.

#### Nachdem Sie fertig sind

Wir sehen, dass das Marketingteam die Exchange-Anwendung verwendet. Wir möchten die Auslastung der Virtual Machines von Exchange überprüfen, um vorhersagen zu können, wann mehr Storage benötigt wird. Verbinden wir die Exchange-Anwendung mit allen VMs von Marketing. Der einfachste Weg, dies zu erreichen, ist durch eine Abfrage.

Wenn Sie diese Schritte befolgen, können Sie jede Ihrer Anwendungen mit den entsprechenden Assets verknüpfen.

#### Anwendungen mit Assets verknüpfen:

Nachdem Sie nun Ihre Applikationen erstellt haben (und diese je nach Bedarf an Geschäftseinheiten gebunden), können wir diese Applikationen nun Assets in Ihrer Umgebung zuordnen. In diesem Beispiel verknüpfen wir die Exchange-Anwendung mit einer Reihe von virtuellen Maschinen in Ihrem Unternehmen. Der einfachste Weg, dies zu tun ist, was eine Abfrage.

1. Wählen Sie **Abfragen** > **+Neue Abfrage**.
2. Wählen Sie in der Dropdown-Liste **Select Resource Type** die Option *Virtual Machine*
3. Wir gehen davon aus, dass das Marketingteam ihre Assets mit der Zeichenfolge „`mktg`“ benennt. Geben Sie im Feld Namensfilter „`*mktg* `“ (ohne Anführungszeichen) ein, und klicken Sie auf die Schaltfläche Übernehmen (Häkchen).
4. Es wird eine Liste aller VMs mit der Zeichenfolge „`*mktg* `“ angezeigt.
5. Wenn gewünscht, klicken Sie auf das Dropdown-Menü **Mehr** und fügen Sie weitere Filter hinzu.
6. Aktivieren Sie die für Exchange verwendeten VMs, indem Sie in das Kontrollkästchen neben jedem gewünschten VM-Namen klicken, oder aktivieren Sie alle VMs, indem Sie oben in der Spalte auf das Kontrollkästchen klicken.
7. Wenn die gewünschten VMs ausgewählt sind, klicken Sie auf die Schaltfläche **actions** und wählen **Add Application**.
8. Klicken Sie im Dialogfeld Anwendung zuweisen auf das Dropdown-Menü **Anwendung** und wählen Sie „`Exchange`“ aus.
9. Klicken Sie Auf **Speichern**.
10. Wiederholen Sie diesen Vorgang, um die Exchange Applikation mit anderen Assets (Hosts, Volumes usw.) zu verknüpfen.

## Erstellung von Performance-Richtlinien für Warnmeldungen

Mit Performance Policies können Sie überwachen und Warnmeldungen senden, wenn bestimmte Bedingungen erfüllt sind.

#### Über diese Aufgabe

Nachdem wir unsere Ressourcen mit Anmerkungen versehen haben, erstellen wir nun eine Performance-Richtlinie, mit der wir bei einer Latenz von über 2 ms in jedem Storage Array in unserem Sunnyvale (DC1_SVL) Datacenter benachrichtigt werden können. Wenn diese Bedingungen eintreten, senden wir eine E-Mail an ausgewählte Empfänger.

**Schritte**

1. Wählen Sie **Verwalten** > **Leistungsrichtlinien** aus.

   Die Seite Leistungsrichtlinien wird geöffnet. Es sind bereits mehrere Standardrichtlinien festgelegt, die Sie an Ihre Anforderungen anpassen können. Wir werden jedoch eine neue Politik schaffen.

2. Klicken Sie auf die Schaltfläche **+Add**.

   Das Dialogfeld **Richtlinie hinzufügen** wird geöffnet.

3. Geben Sie im Feld **Richtlinienname** „`SVL Data Center Latency Policy`“ ein.

   Sie müssen einen Namen verwenden, der sich von allen anderen Richtliniennamen für das Objekt unterscheidet. Sie können beispielsweise nicht zwei Richtlinien mit dem Namen „Latenz“ für ein internes Volume festlegen. Sie können jedoch eine „Latenzrichtlinie“ für ein internes Volume und eine weitere „Latenzrichtlinie“ für ein anderes Volume festlegen. Es empfiehlt sich, immer einen eindeutigen Namen für eine Richtlinie zu verwenden, unabhängig vom Objekttyp.

4. Wählen Sie für **auf Objekte des Typs anwenden Speicher** aus.
5. Wählen Sie im Feld **with annotation Data Center** is „`DC1_SVL`“ aus (oder wählen Sie hier den Namen Ihres gewünschten Rechenzentrums).
6. Anwenden nach einem Fenster von **erster Vorkommen** .

   Die Option „Erstes Auftreten“ löst eine Warnung aus, wenn ein Schwellenwert bei der ersten Datenprobe überschritten wird. Alle anderen Optionen lösen eine Warnung aus, wenn der Schwellenwert einmal überschritten wird und mindestens die angegebene Zeit lang kontinuierlich überschritten wird.

7. Wählen Sie aus der Liste **mit Schweregrad** die Option **Warnung** aus.
8. Klicken Sie unter **E-Mail-Empfänger** auf, um die globale Empfängerliste zu überschreiben. Klicken Sie auf**+**, um die E-Mail-Adresse Ihres ersten gewünschten Benachrichtigungsempfängers hinzuzufügen, und klicken Sie auf **OK**. Wiederholen Sie dies für alle weiteren gewünschten E-Mail-Empfänger.
9. Behalten Sie die Standardauswahl für Warnung erstellen bei, wenn **alle** der folgenden Werte zutreffen. Dadurch wird eine Benachrichtigung gesendet, wenn einer der festgelegten Schwellenwerte erreicht ist. Sie können auch nur dann eine Warnung ausgeben, wenn **alle** der eingestellten Schwellenwerte erfüllt sind.
10. Um Ihren ersten Schwellenwert festzulegen, wählen Sie **Latency - Total** in der Dropdown-Liste aus und setzen Sie ihn auf mehr als 2 ms.
11. Wenn gewünscht, fügen Sie zusätzliche Schwellenwerte hinzu, die Sie durch Klicken auf die Schaltfläche **Schwellenwert hinzufügen** benachrichtigen können. Wenn die Richtlinie so angepasst wird, wie Sie es wünschen, klicken Sie auf **Speichern**.
12. Sie können auch wählen, **Verarbeitung weiterer Richtlinien stoppen, wenn Alarm erzeugt wird**. Dadurch werden zusätzliche Richtlinienwarnungen gestoppt, wenn die Bedingungen dieser Richtlinie erfüllt sind.
13. Sie können beliebig viele neue Richtlinien hinzufügen und je nach Geschäftsbedarf Warnmeldungen für andere Empfänger festlegen. Alle Richtlinien, die ohne bestimmte Empfänger konfiguriert sind, senden Benachrichtigungen an die globale Empfängerliste, die auf der Seite **Admin** > **Benachrichtigungen** festgelegt ist

### Nachdem Sie fertig sind

Jede neue Richtlinie wird automatisch aktiviert, wenn sie gespeichert wird, und Empfänger erhalten Warnungen, wenn die Bedingungen der Richtlinie erfüllt sind (bekannt als *Verstoß*). Sie können diese Verstöße auch im Dashboard **Dashboards** > **Verstöße** überwachen.

## Datenhervorhebt mithilfe von Dashboards

Da Ihre Ressourcen nun mit Anmerkungen versehen sind und Performance-Richtlinien für Verstöße konfiguriert sind, können Sie Dashboards erstellen, die bestimmte Daten hervorheben, die Sie als Ziel verfolgen möchten.

### Über diese Aufgabe

In diesem Beispiel geben wir eine allgemeine Ansicht der Dashboard-Erstellung an, indem wir ein Dashboard mit nur einem Widget mit den VM-Performance-Daten erstellen. Sie können auf einem einzelnen Dashboard beliebig viele Widgets hinzufügen und so viele Dashboards erstellen, wie Sie benötigen. Widgets können nach Bedarf geändert und verschoben werden.

Weitere Informationen zu Dashboards und Widgets finden Sie in der OnCommand Insight-Dokumentation.

### Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
2. Wählen Sie im Menü **Dashboards** die Option **+Neues Dashboard**.

   Die Seite Neues Dashboard wird geöffnet.

3. Best Practice: Benennen und speichern Sie Ihr Dashboard, sobald Sie es erstellen. Klicken Sie auf die Schaltfläche **Speichern** und geben Sie einen eindeutigen Namen für das Dashboard in das Feld **Name** ein. Beispiel: „`VM Performance Dashboard`“. Klicken Sie Auf **Speichern**.
4. Schieben Sie bei Bedarf den Schalter **Bearbeiten** auf „`on`“, um den Bearbeitungsmodus zu aktivieren. Auf diese Weise können Sie beginnen, Widgets zu Ihrem Dashboard hinzuzufügen.
5. Klicken Sie auf die Schaltfläche **+Widgets** und wählen Sie **Tabelle**, um ein neues Tabellen-Widget zum Dashboard hinzuzufügen.

   Das Dialogfeld Widget bearbeiten wird geöffnet.

6. Löschen Sie im Feld Name „`Widget 1`“, und geben Sie „`Virtual Machine Performance table`“ ein.
7. Klicken Sie auf das Dropdown-Menü Asset-Typ und ändern Sie **Storage** in **Virtual Machine**.

   Die Änderungen an den Tabellendaten werden angezeigt, wenn alle Virtual Machines in Ihrer Umgebung angezeigt werden.

8. Um der Tabelle zusätzliche Spalten hinzuzufügen, klicken Sie auf *Spalten* Und wählen Sie die gewünschten Spalten aus, z. B._*Data Center*, *Storage Name* und *Tier*.Sie können die Tabelle nach einer dieser Spalten sortieren.
9. Sie können Filter nach Bedarf einstellen, um die für Sie wichtigen Daten für dieses Dashboard hervorzuheben. Sie können z. B. festlegen, dass nur virtuelle Maschinen mit „`Tier 1 - SSD`“-Annotation angezeigt werden sollen. Klicken Sie neben **Filtern nach** auf die Schaltfläche „` + “ und wählen Sie*Tier*. Klicken Sie auf **any** und geben Sie „`Tier 1 - SSD`“ ein. Klicken Sie auf das

Um den Filter zu speichern.

In der Tabelle werden jetzt nur noch virtuelle Maschinen im Tier „SSD“ angezeigt.

10. Sie können Ergebnisse gruppieren, indem Sie auf die Schaltfläche „` + `“ neben **Gruppieren nach** klicken und ein Feld auswählen, nach dem Sie gruppieren möchten, z. B. Data Center. Die Gruppierung wird automatisch auf die Tabelle angewendet.
11. Wenn Sie das Widget an Ihre Zufriedenheit angepasst haben, klicken Sie auf die Schaltfläche **Speichern**.

    Das TabellenWidget wird im Dashboard gespeichert.

12. Sie können die Größe des Widgets auf dem Dashboard ändern, indem Sie die untere rechte Ecke ziehen.
13. Um weitere Widgets hinzuzufügen, klicken Sie auf die Schaltfläche **+Widget**. Jedes Widget wird dem Dashboard hinzugefügt, wenn es gespeichert wird.
14. Wenn Sie alle gewünschten Änderungen vorgenommen haben, klicken Sie auf **Speichern**, um das Dashboard zu speichern.
15. Sie können zusätzliche Dashboards erstellen, um unterschiedliche Daten hervorzuheben.

# Erstellen benutzerdefinierter Dashboards

## OnCommand Insight 7.3 enthält erweiterte benutzerdefinierte Dashboard-Funktionen, um Benutzern eine Betriebsansicht der für sie wichtigen Daten zu ermöglichen und eine Komplettansicht der Daten bereitzustellen.

OnCommand Insight bietet Benutzern die Flexibilität, Infrastrukturdaten von Betriebsansichten über VERSCHIEDENE IT-Plattformen hinweg zu erstellen, da Sie benutzerdefinierte Dashboards mit einer Vielzahl von Widgets erstellen können, die alle eine große Flexibilität bei der Anzeige und Dokumentation Ihrer Daten bieten. In dieser Anleitung erstellen wir ein Beispiel-Dashboard, um die VM-Performance hervorzuheben.

Dieses How-To sollte nur als Beispiel dienen und deckt nicht jedes mögliche Szenario ab. Mit den hier beschriebenen Konzepten und Schritten können Sie eigene Dashboards erstellen, um die Daten hervorzuheben, die Ihren speziellen Anforderungen entsprechen.

**Übersicht**

Sie erstellen ein benutzerdefiniertes Dashboard mit einer der folgenden Methoden:

- **Dashboards** > **+Neues Dashboard**
- **Dashboards** > **Alle Dashboards anzeigen** und auf **+Hinzufügen** klicken

Der Bildschirm Neues Dashboard verfügt über mehrere Steuerelemente:

- **Zeitauswahl**: Ermöglicht die Anzeige von Dashboard-Daten für einen Zeitraum von 3 Stunden bis zu 90 Tagen mithilfe der benutzerdefinierten Datumsbereichauswahl. Sie können diesen globalen Zeitbereich in einzelnen Widgets überschreiben.
- **Bearbeiten**-Schaltfläche: Durch Auswahl von “on” wird der Bearbeitungsmodus aktiviert, mit dem Sie Änderungen am Dashboard vornehmen können. Neue Dashboards werden standardmäßig im Bearbeitungsmodus geöffnet.
- **Speichern** Button: Ermöglicht das Speichern, Umbenennen oder Löschen des Dashboards.

- **Variable** Button: Variablen können zu Dashboards hinzugefügt werden. Wenn Sie die Variable ändern, werden alle Widgets auf einmal aktualisiert. Weitere Informationen zu Variablen finden Sie unter "Konzepte des benutzerdefinierten Dashboards"
- **Widget** Button, mit dem Sie beliebig viele Tabellen, Diagramme oder andere Widgets zum Dashboard hinzufügen können.

Widgets können geändert und an verschiedene Positionen im Dashboard verschoben werden, um Ihnen die beste Ansicht Ihrer Daten entsprechend Ihren aktuellen Anforderungen zu geben.

#### Widget-Typen

Sie können aus den folgenden Widgets wählen:

**Tabelle** Widget: Eine Tabelle, die Daten nach den von Ihnen gewählten Filtern und Spalten anzeigt. Tabellendaten können in Gruppen zusammengefasst werden, die ausgeblendet und erweitert werden können.

**Linie, Spline, Fläche, gestapelte Fläche** Karten: Dies sind Zeitreihendiagramm-Widgets, auf denen Sie Leistung und andere Daten im Laufe der Zeit anzeigen können.

**Einzelner Wert** Widget: Ein Widget, mit dem Sie einen einzelnen Wert anzeigen können, der entweder direkt von einem Zähler abgeleitet oder mit einer Abfrage oder einem Ausdruck berechnet werden kann. Beispielsweise können Sie im oberen Bereich Ihres Dashboards die Summe der IOPS-Gesamtkapazität für den gesamten Storage in Ihrer Umgebung als einen einzigen Wert anzeigen.

**Balken** Diagramm: Ein Diagramm, um die oberen oder unteren 5, 10, 20 oder 50 Werte anzuzeigen.

**Box Plot**-Diagramm: Ein Plot des min, max, median und des Bereichs zwischen dem unteren und oberen Quartil von Daten in einem einzigen Diagramm.

**Scatter Plot**-Diagramm: Zeichnet verwandte Daten als Punkte, z. B. IOPS und Latenz. In diesem Beispiel würden Sie schnell Assets mit hoher Latenz und niedrigen IOPS sehen.

Darüber hinaus gibt es eine Reihe von Legacy-Widgets, die Sie wählen können. Wählen Sie in der Dropdown-Liste **Widgets Mehr anzeigen…**um diese Widgets anzuzeigen.

## Konzepte des benutzerdefinierten Dashboards

Benutzerdefinierte Dashboards und Widgets bieten große Flexibilität bei der Anzeige von Daten. Nachfolgend finden Sie einige Konzepte, mit denen Sie Ihre individuellen Dashboards optimal nutzen können. Jedes Konzept wird in den folgenden Abschnitten näher erläutert.

#### Variablen

Variablen ermöglichen es Ihnen, die in einigen oder allen Widgets auf einem Dashboard angezeigten Daten gleichzeitig zu ändern. Wenn jedes Widget auf eine gemeinsame Variable eingestellt wird, führen Änderungen an einem Ort dazu, dass die in jedem Widget angezeigten Daten automatisch aktualisiert werden.

#### Mehrere Abfragen und/oder Ausdrücke

Jedes Widget für Zeitreihen (Linien-, Spline-, Bereich- oder gestapelte Flächendiagramme) kann bis zu fünf Abfragen und/oder Ausdrücke enthalten, um zu bestimmen, welche Daten angezeigt werden sollen, sodass Sie verschiedene Datensätze auf einem einzelnen Diagramm vergleichen können. Beispielsweise können Sie ein Liniendiagramm mit IOPS sowohl für Storage als auch für VMs oder ein Einzeldiagramm mit Durchsatz und

Latenz für alle Storage-Pools erstellen.

- Rollup und Gruppieren*

Die in jedem Widget angezeigten Daten werden aus den erfassten Datenpunkten aufgerollt. Sie haben verschiedene Möglichkeiten, diese Daten einzurollen:

- AVG: Erfasst Daten als Durchschnitt der zugrunde liegenden Daten
- Max: Rollt Daten bis zum Maximum der zugrunde liegenden Daten
- Min: Rollt Daten auf das Minimum der zugrunde liegenden Daten
- Summe: Fasst Daten als Summe der zugrunde liegenden Daten zusammen

Standardmäßig werden alle zugrunde liegenden Daten in einem einzelnen Eintrag (Alle) auf dem Diagramm oder der Tabelle zusammengefasst. Sie können stattdessen Daten für ein bestimmtes Attribut, wie z. B. Data Center oder Tier, erstellen, um die zugrunde liegenden Daten in die gewünschten Gruppen zu verteilen. Ihr Widget zeigt nur die Daten für die ausgewählten Attribute an.

Sie können Daten in einem Tabellenwidget nach dem ausgewählten Attribut gruppieren. Sie können beispielsweise die Tabelle nach Rechenzentrum gruppieren. Gruppen können beliebig erweitert oder reduziert werden. Leistungsdaten in einer Tabelle werden in der Gruppenkopfzeile gemäß der im Widget festgelegten Rollup-Methode (Durchschnitt, Max, Min oder Summe) aufgerollt.

Tabellen-Widgets können nach jeder Spalte sortiert werden, und Spalten können nach Bedarf verschoben oder in der Größe geändert werden.

**Oben/Unten**

Verwenden Sie diese Option, um die Ergebnismenge in Diagramm-Widgets zu begrenzen, um auszuwählen, ob die oberen N-Ergebnisse in Ihrem Widget oder die unteren N-Ergebnisse angezeigt werden sollen. Sie können diese Option wählen, wenn Daten nicht automatisch gerollt oder von einem bestimmten Attribut aufgerollt werden.

**Dashboard-Zeit überschreiben**

Standardmäßig zeigen die meisten Widgets, die Sie einem Dashboard hinzufügen, Daten entsprechend der Einstellung des Zeitbereichs des Dashboards an (3h, 24h, 3d, 7d, 30d oder benutzerdefinierter Bereich). Sie können diese Zeiteinstellung jedoch in einzelnen Widgets überschreiben, um sie zu zwingen, Daten in einem bestimmten Zeitkontext anzuzeigen, unabhängig von der Zeiteinstellung des Dashboards.

Diese Konzepte werden im folgenden Abschnitt näher erläutert.

**Dashboard-Variablen**

## Mit Dashboard-Variablen können Sie Daten schnell und einfach über mehrere Widgets auf einem Dashboard filtern.

#### Bevor Sie beginnen

Dieses Beispiel erfordert, dass die Annotation **City** (auch City-Attribut genannt) auf mehreren Speicheranlagen festgelegt wird.

Für beste Ergebnisse, stellen Sie verschiedene Städte auf verschiedenen Lagern.

**Über diese Aufgabe**

Variablen bieten eine schnelle und einfache Möglichkeit, die in einigen oder allen Widgets auf einem benutzerdefinierten Dashboard angezeigten Daten zu filtern. Die folgenden Schritte führen Sie zum Erstellen von Widgets, die Variablen verwenden, und zeigen Ihnen, wie Sie sie auf Ihrem Dashboard verwenden.

**Schritte**

1. Melden Sie sich bei Insight als Benutzer mit administrativen Berechtigungen an
2. Klicken Sie auf **Dashboards** > **+Neues Dashboard**.
3. Bevor wir Widgets hinzufügen, möchten wir die Variablen definieren, die wir zum Filtern der Dashboard-Daten verwenden. Klicken Sie auf die Schaltfläche **Variable**.

   Die Liste der Attribute wird angezeigt.

4. Nehmen wir an, wir möchten das Dashboard so einstellen, dass es nach Stadt gefiltert wird. Wählen Sie das Attribut **City** aus der Liste aus.

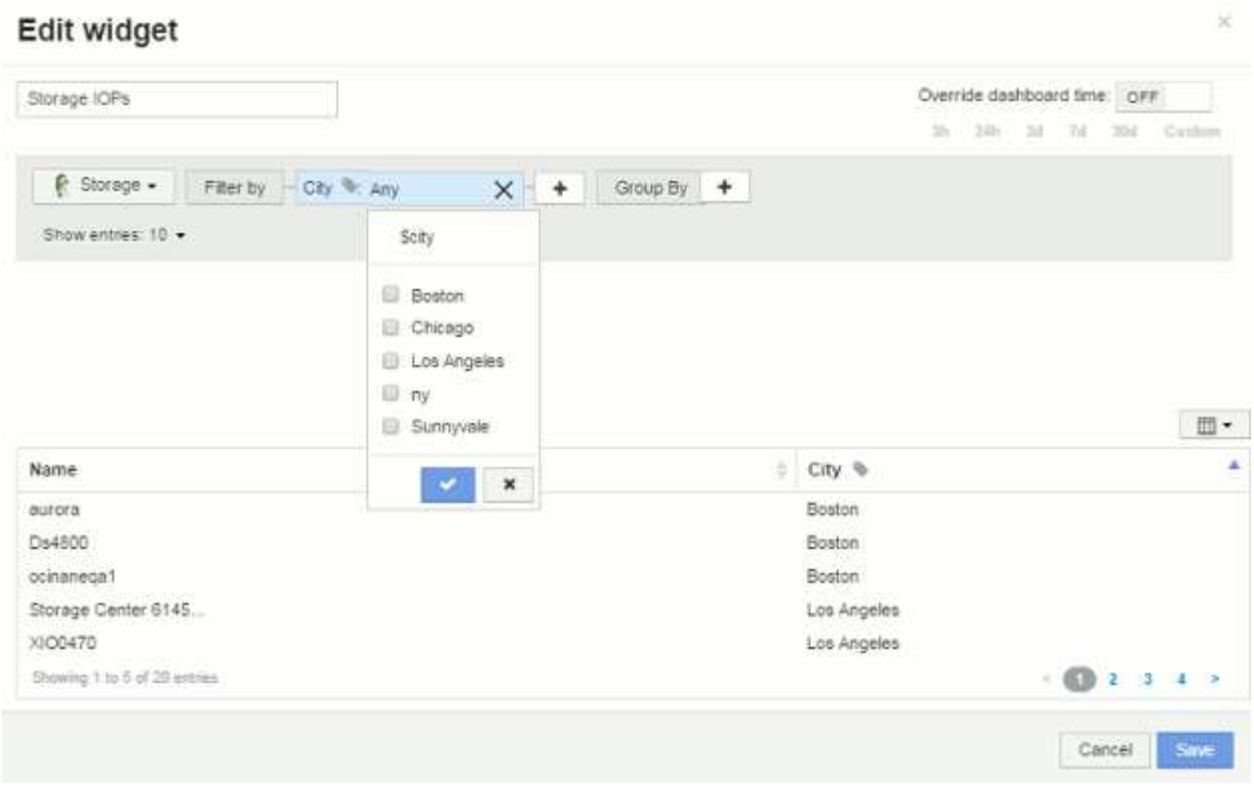
   Das Feld City Variable für den Wert von USD wird erstellt und dem Dashboard hinzugefügt.

5. Als Nächstes müssen wir unseren Widgets sagen, dass sie diese Variable verwenden sollen. Die einfachste Möglichkeit, dies zu veranschaulichen ist, eine Tabelle Widget mit der Stadt Spalte hinzufügen. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie das Widget **Tabelle** aus.
6. Fügen Sie zuerst das Feld Stadt zur Tabelle hinzu, indem Sie es aus der Spaltenauswahl auswählen Schaltfläche.

   Stadt ist ein Attribut vom Typ Liste, daher enthält es eine Liste mit zuvor definierten Auswahlmöglichkeiten. Sie können auch Text-, Boolesche oder Datumstyp-Attribute auswählen.

7. Klicken Sie dann auf die Schaltfläche **Filtern nach +** und wählen Sie **Stadt**.
8. Klicken Sie auf **any**, um die möglichen Filteroptionen für Stadt anzuzeigen. Beachten Sie, dass die Liste jetzt neben allen zuvor verfügbaren Optionen „ `City‟ an der Spitze enthält. Wählen Sie „` City“, um diese Dashboard-Variable zu verwenden.

   Die Option „``“ wird nur hier angezeigt, wenn sie zuvor auf der Dashboard-Hauptseite definiert wurde. Wenn die Variable nicht zuvor definiert wurde, werden nur die vorhandenen Auswahlmöglichkeiten für den Filter angezeigt. Nur Variablen, die für den ausgewählten Attributtyp gelten, werden in der Dropdown-Liste für diesen Filter angezeigt.




9. **Speichern** das Widget.
10. Klicken Sie auf der Dashboard-Seite auf **any** neben der Variablen für die Stadt, und wählen Sie die Stadt oder die Städte aus, die Sie sehen möchten.

    Ihr Tabellen-Widget wird aktualisiert, um nur die ausgewählten Städte anzuzeigen. Sie können die Werte in der Variablen „Stadt USD“ beliebig ändern. Alle Widgets auf Ihrem Dashboard, die auf die Variable „Stadt USD“ eingestellt sind, werden automatisch aktualisiert, sodass nur die Daten für die ausgewählten Werte angezeigt werden.

11. Achten Sie darauf, Ihr Dashboard zu speichern, wenn Sie es so konfiguriert haben, wie Sie es möchten.

#### Mehr zu Dashboard-Variablen

Dashboard-Variablen enthalten verschiedene Typen, können in verschiedenen Feldern verwendet werden und müssen Regeln für die Benennung befolgen. Diese Konzepte werden hier erläutert.

### Variabentypen

Eine Variable kann einen der folgenden Typen sein:

**Text**: Alphanumerische Zeichenfolge. Dies ist der Standard-Variablentyp.

**Numerisch**: Eine Zahl oder ein Zahlenbereich.

**Boolean**: Verwenden Sie Felder mit Werten von True/False, Yes/No, 0/1, etc Für die boolesche Variable sind die Auswahlmöglichkeiten *Yes*, *No*, *None*, *Any*.

**Datum**: Ein Datum oder ein Datumsbereich.

### „`Generic`“-Variablen

Sie können eine generische oder universelle Variable festlegen, indem Sie auf die Schaltfläche **Variable** klicken und einen der oben aufgeführten Typen auswählen. Diese Typen werden immer oben in der Dropdown-Liste angezeigt. Die Variable erhält einen Standardnamen, z. B. „` var1`“, und ist nicht an eine bestimmte Anmerkung oder ein bestimmtes Attribut gebunden.

Durch das Konfigurieren einer generischen Variable können Sie diese Variable in Widgets verwenden, um nach *any* -Feldern dieses Typs zu filtern. Wenn Sie beispielsweise ein Tabellen-Widget haben, das *Name*, *Alias* und *Vendor* (alle Textattribute) anzeigt, und „`€2var1`“ eine Textvariable ist, können Sie für jedes dieser Felder im Widget Filter festlegen, um die Variable €2var1 zu verwenden. Sie können andere Widgets so einstellen, dass sie für diese oder beliebige Textfelder var1 verwenden.

Wenn Sie auf Ihrer Dashboard-Seite einen Wert von var1 einstellen (z. B. „`NetApp`“), wird *all* der Felder in *all* Widgets filtern, die so eingestellt sind, dass sie diese Variable verwenden. Auf diese Weise können Sie mehrere Widgets gleichzeitig aktualisieren, um Dashboard-Daten hervorzuheben, die Sie nach Bedarf auswählen.

Da generische Variablen für jedes Feld dieses Typs verwendet werden können, können Sie den Namen einer generischen Variable ändern, ohne deren Funktionalität zu ändern.

> Alle Variablen werden als "generische" Variablen behandelt, auch solche, die Sie für ein bestimmtes Attribut erstellen, da alle konfigurierten Variablen eines Typs angezeigt werden, wenn Sie einen Filter für alle Attribute oder Anmerkungen dieses Typs festlegen. Es empfiehlt sich jedoch, eine generische Variable zu erstellen, wenn Sie sie zum Filtern nach einem Wert in mehreren Feldern verwenden, wie im Beispiel „*Name/Alias/Vendor*“ oben beschrieben.

#### Variablenbenennung

Variablennamen:

- Muss immer mit einem „```“ vorangestellt werden. Diese wird automatisch hinzugefügt, wenn Sie eine Variable konfigurieren.
- Sonderzeichen dürfen nicht enthalten sein. Es sind nur die Buchstaben a bis z und die Ziffern 0-9 zulässig.
- Darf nicht länger als 20 Zeichen sein, einschließlich des „```“-Symbols.
- Nicht Groß-/Kleinschreibung beachten: Cityname und Cityname im Wert von US-Dollar sind die gleiche Variable.
- Darf nicht mit einem vorhandenen Variablennamen identisch sein.
- Kann nicht nur das „```“-Symbol sein.

#### Widgets, die Variablen verwenden

Variablen können mit den folgenden Widgets verwendet werden:

- Flächendiagramm
- Balkendiagramm
- Box Plot Chart
- Liniendiagramm
- Streudiagramm

- Widget „Einzelner Wert“
- Spline-Diagramm
- Gestapeltes Flächendiagramm
- Tabellenwidget

**Widget-Legenden werden angezeigt**

## Widgets in Dashboards können mit oder ohne Legenden angezeigt werden.

Legenden in Widgets können auf einem Dashboard mit einer der beiden Methoden ein- oder ausgeschaltet werden:

1. Aktivieren Sie beim Erstellen oder Bearbeiten des Widgets selbst das Kontrollkästchen „Legenden“, und speichern Sie das Widget.
2. Wenn sich das Dashboard im Bearbeitungsmodus befindet, klicken Sie im Widget auf die Schaltfläche Optionen, und aktivieren Sie das Kontrollkästchen Legenden im Menü.

Während Sie die im Widget angezeigten Daten bearbeiten und ändern, wird die Legende für dieses Widget dynamisch aktualisiert.

Wenn Legenden angezeigt werden, wird die Legende als Link zu dieser Asset-Seite angezeigt, wenn die Landing-Page des von der Legende angegebenen Assets navigiert werden kann.

**Anfragen und Filter für das Dashboard-Widget**

## Die Abfrage in einem Dashboard-Widget ist ein leistungsstarkes Tool zur Verwaltung der Anzeige Ihrer Daten. Hier sind einige Dinge zu beachten über Widget-Abfragen.

Einige Widgets können bis zu fünf Abfragen haben. Jede Abfrage erstellt im Widget einen eigenen Satz von Linien oder Diagrammen. Das Einrichten von Rollup, Gruppierung, Ergebnissen von oben/unten usw. auf einer Abfrage hat keine Auswirkungen auf andere Abfragen für das Widget.

Sie können auf das Augensymbol klicken, um eine Abfrage vorübergehend auszublenden. Das Widget wird automatisch aktualisiert, wenn Sie eine Abfrage ausblenden oder anzeigen. Auf diese Weise können Sie die angezeigten Daten auf einzelne Abfragen überprüfen, während Sie Ihr Widget erstellen.

Die folgenden Widget-Typen können mehrere Abfragen haben:

- Diagramm Bereich
- Stapelgebietskarte
- Liniendiagramm
- Spline-Diagramm
- Widget mit einem einzelnen Wert

Die übrigen Widget-Typen können nur eine einzige Abfrage haben:

- Tabelle
- Balkendiagramm
- Box-Darstellung

- Streudiagramm

#### Filtern in Dashboard-Abfragen

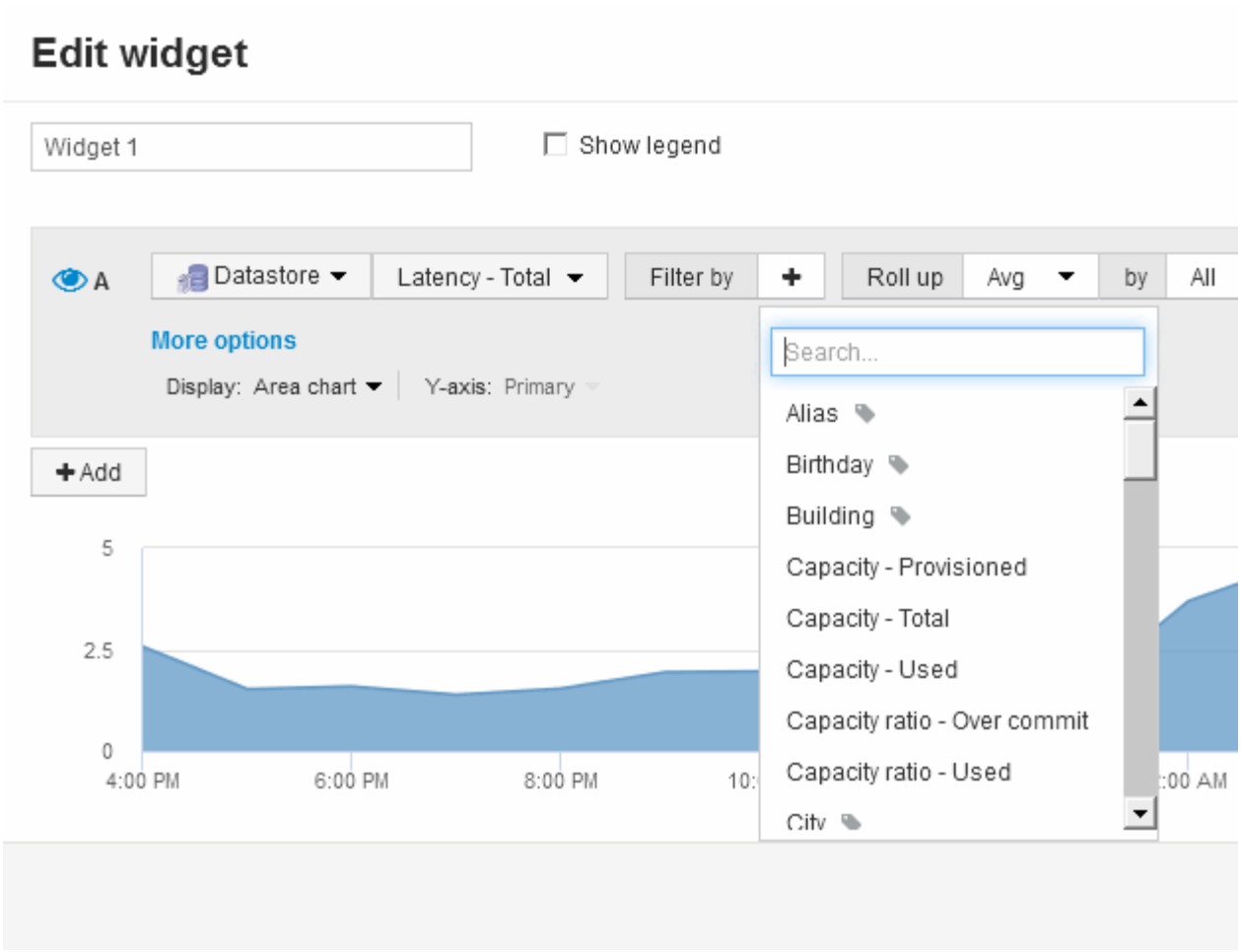
Sie können mit einer der folgenden Filter Ihre Suche in einem beliebigen **Textfeld** in der Abfrage verfeinern:

- Mit einem Sternchen können Sie nach allem suchen. Beispiel: `vol*rhel` Zeigt alle Ressourcen an, die mit „`vol`“ beginnen und mit „`RHEL`“ enden.
- Mit dem Fragezeichen können Sie nach einer bestimmten Anzahl von Zeichen suchen. Beispiel: `BOS-PRD??-S12` Zeigt BOS-PRD12-S12, BOS-PRD13-S12 usw. an.
- Mit dem Operator ODER können Sie mehrere Einheiten angeben. Beispiel: `FAS2240 OR CX600 OR FAS3270` Findet mehrere Storage-Modelle
- Der NICHT-Operator ermöglicht es Ihnen, Text aus den Suchergebnissen auszuschließen. Beispiel: `NOT EMC*` Findet alles, was nicht mit „`EMC`“ beginnt. Verwenden Sie können `NOT *` Um Felder anzuzeigen, die Null-Werte enthalten.

Wenn Sie einen Filter in doppelte Anführungszeichen einschließen, behandelt Insight alles zwischen dem ersten und dem letzten Zitat als exakte Übereinstimmung. Alle Sonderzeichen oder Operatoren in den Angeboten werden als Literale behandelt. Wenn Sie beispielsweise nach „`*`“ filtern, werden Ergebnisse zurückgegeben, die ein wörtliches Sternchen sind. Das Sternchen wird in diesem Fall nicht als Platzhalter behandelt. Die Operatoren UND, OR und NOT werden auch als Literalzeichenfolgen behandelt, wenn sie in Doppelzitate eingeschlossen sind.

#### Identifizieren von Objekten, die von Abfragen und Filtern zurückgegeben werden

Die von Abfragen und Filtern zurückgegebenen Objekte sehen ähnlich aus wie in der folgenden Abbildung. Objekte, denen Tags zugewiesen sind, sind Annotationen, während die Objekte ohne Tags Performance-Zähler oder Objektattribute sind.




**Roll-up und Aggregation**

## Die in Dashboard-Widgets angezeigten Daten werden aus den erfassten Datenpunkten gerollt, wodurch Flexibilität und Konzisilität in Ihren Dashboards ermöglicht werden.

Die in jedem Widget angezeigten Daten werden aus den zugrunde liegenden Datenpunkten, die während der Erfassung erfasst wurden, aufgerollt. Wenn Sie beispielsweise ein Liniendiagramm mit Storage-IOPS im Laufe der Zeit haben, kann es sinnvoll sein, eine separate Zeile für jedes Ihrer Datacenter zu sehen, um einen schnellen Vergleich zu erzielen. Sie haben verschiedene Möglichkeiten, diese Daten einzurollen:

- **AVG**: Zeigt jede Zeile als den *Mittelwert* der zugrunde liegenden Daten an.
- **Max**: Zeigt jede Zeile als *Maximum* der zugrunde liegenden Daten an.
- **Min**: Zeigt jede Zeile als *minimum* der zugrunde liegenden Daten an.
- **Sum**: Zeigt jede Zeile als die *Summe* der zugrunde liegenden Daten an.

Wählen Sie dazu in der Abfrage Ihres Widgets zunächst einen Asset-Typ (z. B. *Storage*) und eine Metrik (z. B. *IOPS - Total*) aus. Wählen Sie für **Roll-up** eine Rollup-Methode (wie *AVG*) und wählen Sie ein Attribut oder eine Anmerkung aus, mit dem die Daten zusammengefasst werden sollen (z. B. *Data Center*). Das Widget wird automatisch aktualisiert und zeigt eine Zeile für jedes Ihrer Rechenzentren an.

Sie können auch wählen, *all* der zugrunde liegenden Daten in das Diagramm oder die Tabelle zu Rollen. In diesem Fall erhalten Sie eine einzelne Zeile für jede Abfrage im Widget, die den Durchschnitt, die min, die max oder die Summe der gewählten Metrik für alle zugrunde liegenden Assets anzeigen wird.

Wenn Sie einen Filter für die Abfrage eingerichtet haben, basieren die gerollten Daten auf den gefilterten Daten.

Beachten Sie, dass Sie, wenn Sie ein Widget nach einem beliebigen Feld Rollen möchten (z. B. *Model*), weiterhin **Filtern nach** dieses Feld benötigen, um die Daten für dieses Feld richtig auf dem Diagramm oder der Tabelle anzuzeigen.

**Daten aggregieren:** Sie können Ihre Zeitreihendiagramme (Linie, Bereich, etc.) weiter ausrichten, indem Sie Datenpunkte in Minuten-, Stunden- oder Tagesbuckets zusammenfassen, bevor diese Daten anschließend nach Attribut (falls ausgewählt) aufgerollt werden. Sie können die Datenpunkte nach dem Durchschnitt, Max, Min oder Summe oder nach dem letzten Datenpunkt, der während des ausgewählten Intervalls erfasst wurde, aggregieren. Um eine Aggregationsmethode zu wählen, klicken Sie in der Abfrage des Widgets auf **Weitere Optionen**.

Das zulässige Mindestintervall beträgt zehn Minuten. Ein kleines Intervall kombiniert mit einem langen Zeitbereich kann zu einem "Aggregationsintervall führte zu zu zu vielen Datenpunkten" führen. Warnung. Falls Sie in einem kleinen Intervall den Zeitrahmen für das Dashboard auf 7 Tage verkürzen möchten, werden Sie diesen vielleicht feststellen. In diesem Fall erhöht Insight das Aggregationsintervall vorübergehend auf 1 Stunde, bis Sie einen kleineren Zeitrahmen auswählen.

Sie können auch Daten in Balkendiagramm-Widget und ein-Wert-Widget aggregieren.

Die meisten Asset-Zähler aggregieren standardmäßig auf *Avg*. Einige Zähler aggregieren standardmäßig auf *max*, *Min* oder *sum*. Beispiel: Port-Fehler aggregieren nach *sum* standardmäßig, wo Storage-IOPS-Aggregat zu *Avg*.

### Anzeigen der Ergebnisse von oben/unten in Dashboard-Widgets

In einem Diagramm-Widget auf einem benutzerdefinierten Dashboard können Sie entweder die oberen oder unteren Ergebnisse für aufgerollte Daten anzeigen und die Anzahl der angezeigten Ergebnisse auswählen. In einem Tabellen-Widget können Sie die Anzahl der angezeigten Zeilen auswählen und nach einer beliebigen Spalte sortieren.

#### Diagramm-Widget oben/unten

Wenn Sie in einem Diagramm-Widget Daten nach einem bestimmten Attribut einrollen möchten, haben Sie die Möglichkeit, entweder die oberen N- oder unteren N-Ergebnisse anzuzeigen. Beachten Sie, dass Sie die oberen oder unteren Ergebnisse nicht auswählen können, wenn Sie durch *all*-Attribute Rollen möchten.

Sie können wählen, welche Ergebnisse angezeigt werden sollen, indem Sie im Feld **Anzeigen** oder **unten** der Abfrage * einen Wert aus der Liste auswählen.

#### Tabelle Widget zeigt Einträge an

In einem TabellenWidget können Sie die Anzahl der in den Tabellenergebnissen angezeigten Ergebnisse auswählen. Sie können zwischen 5, 10, 20 oder 50 Ergebnissen wählen. Sie haben nicht die Möglichkeit, obere oder untere Ergebnisse zu wählen, da Sie in der Tabelle nach Bedarf aufsteigend oder absteigend sortieren können.

Sie können die Anzahl der Ergebnisse auswählen, die in der Tabelle auf dem Dashboard angezeigt werden sollen, indem Sie einen Wert aus dem Feld **Einträge anzeigen** der Abfrage auswählen.

Beachten Sie, dass je mehr Ergebnisse Sie anzeigen möchten, desto größer wird Ihr Widget, wenn Sie es auf dem Dashboard speichern. Sie können die Größe des Widgets nicht kleiner als die Anzahl der angezeigten

Zeilen ändern.

### Gruppierung in Tabellen-Widgets

Die Daten in einem TabellenWidget können nach allen verfügbaren Attributen gruppiert werden. So können Sie einen Überblick über Ihre Daten anzeigen und sie für mehr Details anzeigen. Metriken in der Tabelle werden für eine einfache Anzeige in jeder zusammenklappbaren Zeile aufgerollt.

Mit den Tabelle-Widgets können Sie Ihre Daten anhand der von Ihnen festgelegten Attribute gruppieren. Beispielsweise könnte Ihre Tabelle die Storage-IOPS insgesamt anzeigen, die nach den Datacentern gruppiert sind, in denen diese Storage gespeichert sind. Sie können auch eine Tabelle mit virtuellen Maschinen anzeigen, die nach dem Hypervisor gruppiert sind, der sie hostet. In der Liste können Sie jede Gruppe erweitern, um die Assets in dieser Gruppe anzuzeigen.

Die Gruppierung ist nur im Widget-Typ **Tabelle** verfügbar.

#### Aufkommen von Performance-Daten

Wenn Sie eine Spalte für Leistungsdaten (z. B. *IOPS - Total*) in ein TabellenWidget einfügen, können Sie bei Auswahl der Gruppierung der Daten eine Aufrollmethode für diese Spalte auswählen. Die Standard-Roll-up-Methode ist es, den *Durchschnitt* der zugrunde liegenden Daten in der Gruppenzeile anzuzeigen. Sie können auch wählen, ob die Daten *sum*, *minimum* oder *maximum* angezeigt werden sollen.

#### Beispiel für Gruppierung (mit Rollup-Erklärung)

Mit den Tabelle-Widgets können Sie Daten gruppieren, um die Anzeige zu erleichtern.

#### Über diese Aufgabe

In diesem Beispiel werden wir ein TabellenWidget erstellen, das alle VMs nach Datacenter gruppiert zeigt.

#### Schritte

1. Erstellen oder öffnen Sie ein Dashboard, und fügen Sie ein Widget mit * Table* hinzu.
2. Wählen Sie **Virtual Machine** als Asset-Typ für dieses Widget aus.
3. Klicken Sie auf die Spaltenauswahl Und wählen Sie *Hypervisor Name* und *IOPS - Total*.

   Diese Spalten werden jetzt in der Tabelle angezeigt.

4. Ignorieren Sie alle VMs ohne IOPS und schließen Sie nur VMs ein, die insgesamt IOPS mehr als 1 haben. Klicken Sie auf die Schaltfläche **Filtern nach +** und wählen Sie **IOPS - Gesamt**. Klicken Sie auf **any**, und geben Sie im Feld **von** 1 ein. Lassen Sie das Feld * to* leer. Klicken Sie auf die Schaltfläche, um den Filter anzuwenden.

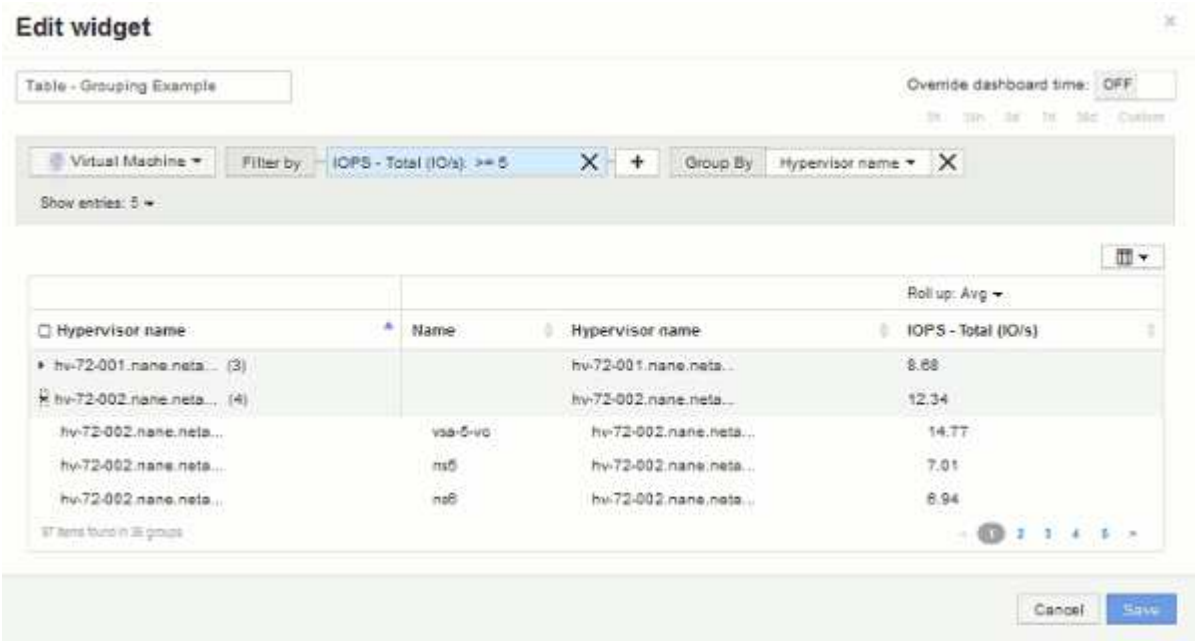
   In der Tabelle werden jetzt alle VMs mit IOPS-Gesamtwerten größer oder gleich 1 angezeigt. Beachten Sie, dass es keine Gruppierung in der Tabelle gibt. Alle VMs werden angezeigt.

5. Klicken Sie auf die Schaltfläche **Gruppieren nach +**.

   Da **All** standardmäßig als Gruppierungsmethode ausgewählt ist, werden alle VMs in eine einzelne Gruppe mit dem Namen „`All`“ verschoben.

6. Oberhalb der Spalte *IOPS - Total* ist nun eine Option **Roll Up**. Die Standard-Rollup-Methode lautet *Avg*. Das bedeutet, dass die für die Gruppe angezeigte Zahl der Durchschnitt aller gesamten IOPS ist, die für jede VM innerhalb der Gruppe gemeldet wurden. Sie können diese Spalte mit *AVG*, *Sum*, *Min* oder *Max* nach oben Rollen. Jede Spalte, die Sie anzeigen, die Leistungskennzahlen enthält, kann einzeln aufgerollt werden.
7. Klicken Sie auf **All** und wählen Sie **Hypervisor Name**.

   Die VM-Liste ist jetzt nach Hypervisor gruppiert. Sie können jeden Hypervisor erweitern, um die von ihm gehosteten VMs anzuzeigen.




8. Klicken Sie auf **Speichern**, um die Tabelle im Dashboard zu speichern. Sie können die Größe des Widgets ändern.
9. Klicken Sie auf **Speichern**, um das Dashboard zu speichern.

#### Überschreiben der Dashboard-Zeit für einzelne Widgets

Sie können die Einstellung des Haupt-Dashboard-Zeitrahmens in einzelnen Widgets außer Kraft setzen. Diese Widgets zeigen Daten basierend auf dem eingestellten Zeitrahmen an, nicht auf dem Zeitrahmen des Dashboards.

Um die Dashboard-Zeit außer Kraft zu setzen und ein Widget dazu zu zwingen, einen eigenen Zeitrahmen zu verwenden, setzen Sie im Bearbeitungsmodus des Widgets die Option **Dashboard-Zeit überschreiben** auf **ein**, und wählen Sie einen Zeitrahmen für das Widget aus. * Speichern* das Widget auf dem Dashboard.

Das Widget zeigt seine Daten entsprechend dem eingestellten Zeitrahmen an, unabhängig vom Zeitrahmen, den Sie auf dem Dashboard selbst auswählen.

Der Zeitrahmen, den Sie für ein Widget festlegen, hat keine Auswirkungen auf andere Widgets auf dem Dashboard.

#### Primäre und sekundäre Achse erklärt

Die sekundäre Achse erleichtert die Anzeige von Daten aus zwei verschiedenen

# Wertegruppen, die verschiedene Maßeinheiten verwenden.

**Über diese Aufgabe**

Verschiedene Metriken verwenden unterschiedliche Maßeinheiten für die Daten, die sie in einem Diagramm erfassen. Wenn wir beispielsweise IOPS betrachten, entspricht die Maßeinheit der Anzahl der I/O-Operationen pro Sekunde (I/O/s), während die Latenz lediglich ein Maß an Zeit ist (Millisekunden, Mikrosekunden, Sekunden usw.). Wenn Sie beide Metriken auf einem einzigen Liniendiagramm mit einem einzelnen Satz A-Werte für die Y-Achse angeben, werden die Latenzzahlen (normalerweise wenige Millisekunden) im selben Maßstab mit den IOPS (normalerweise sind Tausende) dargestellt und die Latenzzeile geht bei diesem Maßstab verloren.

Es ist jedoch möglich, beide Datensätze auf einem einzigen aussagekräftigen Diagramm zu grafisch zu gestalten, indem eine Maßeinheit auf der primären (linken) Y-Achse und die andere Maßeinheit auf der sekundären (rechten) Y-Achse eingestellt wird. Jede Metrik wird im eigenen Maßstab dokumentiert.

**Schritte**

1. Erstellen oder Öffnen eines Dashboards. Fügen Sie dem Dashboard ein Widget **Liniendiagramm**, **Spline Chart**, **Flächendiagramm** oder **gestapeltes Flächendiagramm** hinzu.
2. Wählen Sie einen Asset-Typ (z. B. **Storage**) aus und wählen Sie für Ihre erste Metrik **IOPS - Total**. Stellen Sie Ihre gewünschten Filter ein, und wählen Sie ggf. eine Roll-up-Methode aus.

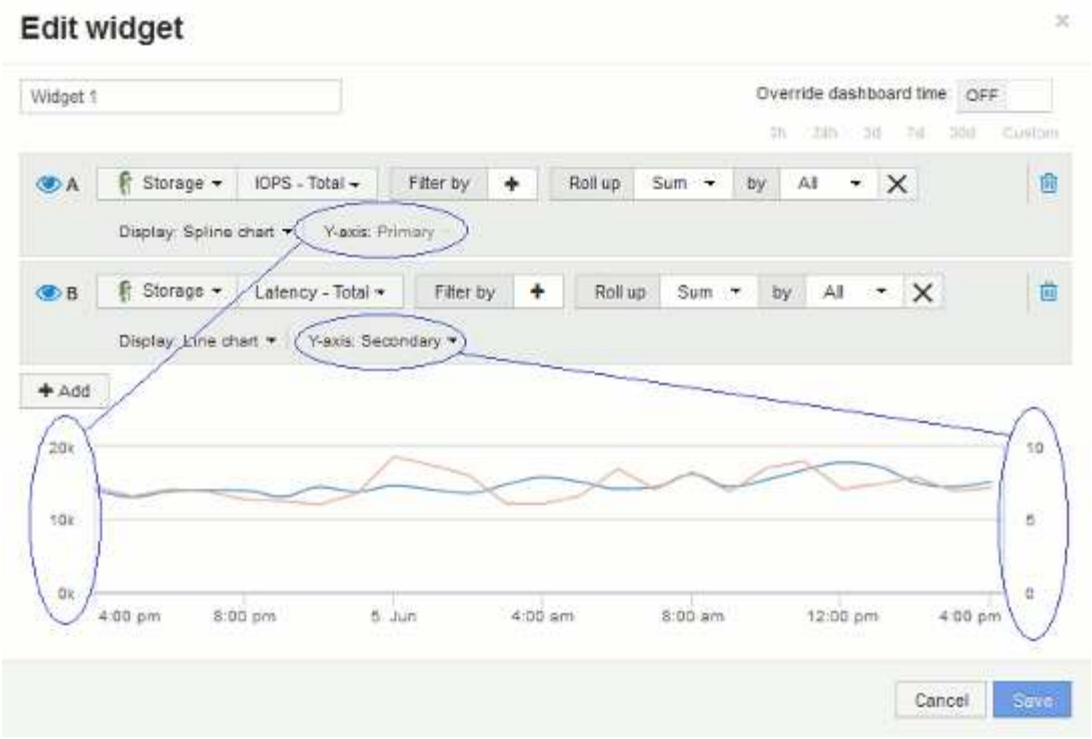
   Die IOPS-Linie wird auf dem Diagramm angezeigt, wobei ihre Skalierung auf der linken Seite dargestellt ist.

3. Klicken Sie auf **+Add**, um eine zweite Zeile zum Diagramm hinzuzufügen. Wählen Sie für diese Zeile **Latency - Total** für die Metrik.

   Beachten Sie, dass die Linie flach am unteren Rand des Diagramms angezeigt wird. Der Grund dafür ist, dass die Daten im gleichen Maßstab wie die IOPS-Linie gezeichnet werden.

4. Wählen Sie in der Latenzabfrage **Y-Achse: Sekundär** aus.

   Die Latenzlinie wird jetzt auf eigene Skala gezeichnet, die rechts im Diagramm angezeigt wird.




### Ausdrücke in Dashboard-Widgets

Ausdrücke in Zeitreihen-Widgets ermöglichen es Ihnen, Daten basierend auf Berechnungen mit Metriken Ihrer Wahl anzuzeigen.

In einem Dashboard können Sie mit einem Widget mit beliebigen Zeitreihen (Linie, Spline, Bereich, gestapelter Bereich) Ausdrücke aus von Ihnen ausgewählten Metriken erstellen und das Ergebnis dieser Ausdrücke in einem einzigen Diagramm anzeigen. Die folgenden Beispiele verwenden Ausdrücke, um bestimmte Probleme zu lösen. Im ersten Beispiel möchten wir den IOPS-Wert für alle Storage Assets in unserer Umgebung als Prozentsatz von IOPS insgesamt darstellen. Das zweite Beispiel gibt uns einen Einblick in das „System“ oder den „Overhead“ der IOPS in unserer Umgebung, d. h. die IOPS, die nicht aus dem Lesen oder Schreiben von Daten stammen.

#### Beispiel für Ausdrücke: Lese-IOPS-Prozentsatz

Mithilfe von Ausdrücken können Sie Metriken auf alternative Weise anzeigen, wie z. B. Prozentsatz der Gesamtmenge.

#### Über diese Aufgabe

In diesem Beispiel möchten wir Lese-IOPS als Prozentsatz der gesamten IOPS anzeigen. Sie können sich dies als folgende Formel vorstellen:

- Leseprozentsatz = (Lese-IOPS/Gesamt-IOPS) x 100

Diese Daten können in einem Liniendiagramm auf Ihrem Dashboard angezeigt werden. Um dies zu tun, führen Sie folgende Schritte aus:

### Schritte

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im **Edit-Modus**.
2. Fügen Sie ein Widget zum Dashboard hinzu. Wählen Sie **Flächendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage mit **IOPS - Total** für **Storage**-Assets angezeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Klicken Sie auf die Schaltfläche **in Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Beachten Sie, dass Sie den Asset-Typ im Expression-Modus nicht ändern können. Beachten Sie, dass während Sie sich im Ausdruckmodus befinden, die Schaltfläche in **revert to Query** geändert wird. Klicken Sie auf diese Option, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass durch Umschalten zwischen den Modi die Felder auf ihre Standardeinstellungen zurückgesetzt werden.

   Bleiben Sie jetzt im **Expression**-Modus.

4. Die Metrik **IOPS - Total** befindet sich jetzt im Feld „`a`“ der alphabetischen Variablen. Klicken Sie im Feld Variable „`b`“ auf **Auswählen** und wählen Sie **IOPS - Lesen**.

   Sie können insgesamt fünf alphabetische Variablen für Ihren Ausdruck hinzufügen, indem Sie auf die Schaltfläche**+**klicken, die den Variablenfeldern folgt. Für unser Beispiel mit dem Prozentsatz „Lesen“ benötigen wir nur die IOPS insgesamt („`a`“) und die IOPS für Lesevorgänge („`b`“).

5. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die jeder Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir wissen, dass *Read Percentage = (Read IOPS / Total IOPS) x 100*, daher würden wir diesen Ausdruck wie folgt schreiben: `(b / a) * 100`
6. Das Feld **Beschriftung** kennzeichnet den Ausdruck. Ändern Sie die Bezeichnung in „`Prozentsatz lesen`“, oder etwas, das für Sie gleichermaßen bedeutsam ist.
7. Ändern Sie das Feld **Einheiten** in „`%`“ oder „`percent`“.

   Das Diagramm zeigt den prozentualen IOPS-Leseanteil im Zeitverlauf für die ausgewählten Speichergeräte an. Auf Wunsch können Sie einen Filter einstellen oder eine andere Rollup-Methode auswählen. Beachten Sie, dass, wenn Sie **sum** als Rollup-Methode auswählen, alle Prozentwerte addiert werden, die potenziell über 100% liegen können.

8. Klicken Sie auf **Speichern**, um das Diagramm auf Ihrem Dashboard zu speichern.

   Sie können auch Ausdrücke in den Widgets **Liniendiagramm**, **Spline Chart** oder **Stacked Area Chart** verwenden.

#### Ausdrücke Beispiel: "System" I/O

## Ausdrücke geben Ihnen die Freiheit, Daten zu graten, die aus anderen Metriken berechnet werden können.

### Über diese Aufgabe

Beispiel 2: OnCommand Insight erwirbt viele Kennzahlen aus Datenquellen. Dazu zählen Lese-, Schreib- und IOPS-Werte. Die von der Erfassung gemeldete Gesamtzahl an IOPS umfasst jedoch manchmal „System“-IOPS. Dabei handelt es sich um solche I/O-Vorgänge, die keinen direkten Teil des Lesens und Schreibens von

Daten darstellen. Dieser System-I/O kann auch als „Overhead“-I/O bezeichnet werden, der für einen ordnungsgemäßen Systembetrieb, aber nicht direkt mit Datenoperationen benötigt wird.

Zur Anzeige dieser System-I/OS können die Lese- und Schreib-IOPS von den insgesamt gemeldeten IOPS aus der Übernahme entfernt werden. Die Formel könnte wie folgt aussehen:

- System-IOPS = IOPS insgesamt – (Lese-IOPS + Schreib-IOPS)

Diese Daten können dann in einem Liniendiagramm auf Ihrem Dashboard angezeigt werden. Um dies zu tun, führen Sie folgende Schritte aus:

**Schritte**

1. Erstellen Sie ein neues Dashboard oder öffnen Sie ein vorhandenes Dashboard im **Edit-Modus**.
2. Fügen Sie ein Widget zum Dashboard hinzu. Wählen Sie **Liniendiagramm**.

   Das Widget wird im Bearbeitungsmodus geöffnet. Standardmäßig wird eine Abfrage mit **IOPS - Total** für **Storage**-Assets angezeigt. Wählen Sie bei Bedarf einen anderen Asset-Typ aus.

3. Klicken Sie auf die Schaltfläche, um eine Kopie der Abfrage zu erstellen.

   Ein Duplikat der Abfrage wird unterhalb des Originals hinzugefügt.

4. Klicken Sie in der zweiten Abfrage auf die Schaltfläche **in Ausdruck konvertieren**.

   Die aktuelle Abfrage wird in den Ausdrucksmodus konvertiert. Klicken Sie auf **Zurücksetzen auf Abfrage**, wenn Sie jederzeit wieder in den Abfragemodus wechseln möchten. Beachten Sie, dass durch Umschalten zwischen den Modi die Felder auf ihre Standardeinstellungen zurückgesetzt werden.

   Bleiben Sie jetzt im **Expression**-Modus.

5. Die Metrik **IOPS - Total** befindet sich jetzt im Feld „`a`“ der alphabetischen Variablen. Klicken Sie auf **IOPS - Total** und ändern Sie es in **IOPS - Lesen**. .
6. Klicken Sie im Feld Variable „`b`“ auf **Auswählen** und wählen Sie **IOPS - Schreiben**.
7. Im Feld **Ausdruck** verwenden Sie die Buchstaben, die jeder Variablen entsprechen, um Ihren Ausdruck zu erstellen. Wir würden unseren Ausdruck einfach schreiben als: `a + b`. Wählen Sie im Abschnitt **Anzeige** für diesen Ausdruck**Flächendiagramm**.
8. Das Feld **Beschriftung** kennzeichnet den Ausdruck. Ändern Sie die Bezeichnung in „`System IOPS`“ oder etwas, das für Sie gleichermaßen bedeutsam ist.

   Im Diagramm wird die IOPS insgesamt als Liniendiagramm angezeigt. In einem Flächendiagramm wird die Kombination aus Lese- und Schreib-IOPS unterhalb dieser Werte angezeigt. Die Lücke zwischen den beiden gibt die IOPS an, die nicht direkt mit Lese- oder Schreibvorgängen verbunden sind.

9. Klicken Sie auf **Speichern**, um das Diagramm auf Ihrem Dashboard zu speichern.

## Benutzerdefiniertes Dashboard: Virtual Machine Performance

Benutzerdefinierte Dashboards und Widgets von OnCommand Insight ermöglichen eine Betriebsansicht von Bestands- und Performance-Trends.

### Über diese Aufgabe

IT-Abteilungen stehen heute vor zahlreichen Herausforderungen. Von Administratoren muss mit weniger Aufwand mehr erreicht werden, und eine vollständige Übersicht über dynamische Datacenter ist daher ein muss. In diesem Beispiel zeigen wir Ihnen, wie Sie ein benutzerdefiniertes Dashboard mit Widgets erstellen, die Ihnen betriebliche Einblicke in die Leistung der virtuellen Maschine in Ihrer Umgebung geben. Wenn Sie diesem Beispiel folgen und Widgets erstellen, die auf Ihre spezifischen Anforderungen zugeschnitten sind, können Sie die Back-End-Storage-Performance im Vergleich zur Front-End-VM (VM)-Performance visualisieren oder die VM-Latenz im Vergleich zur I/O-Anforderung anzeigen.

Individuelle Dashboards ermöglichen Ihnen, Prioritäten für Ihre Bemühungen zu setzen und die Verfügbarkeit von Ressourcen zu ermitteln. Sie können auf Ebbe und Flut von Workloads reagieren und die Zeit für die Erkennung und Behebung aufkommender Probleme minimieren. Benutzerdefinierte Dashboards bieten Ihnen die Flexibilität, priorisierte Ansichten in geschäftskritische Infrastrukturen zu erstellen. Sie sind nützlich, um die Performance-Verfügbarkeit in heterogenen Technologien zu ermitteln.

Hier werden wir ein Dashboard für die Performance von virtuellen Maschinen erstellen, das Folgendes enthält:

- Eine Tabelle mit VM-Namen und Performance-Daten
- Ein Diagramm, das VM-Latenz mit Storage-Latenz vergleicht
- Ein Diagramm mit den Angaben zu Lese-, Schreib- und IOPS insgesamt für VMs
- Ein Diagramm zeigt den maximalen Durchsatz für Ihre VMs

Dies ist nur ein einfaches Beispiel. Sie können Ihr Dashboard anpassen, um Performance-Daten hervorzuheben und zu vergleichen, die Sie für Ihre eigenen Best Practices im Betrieb auswählen.

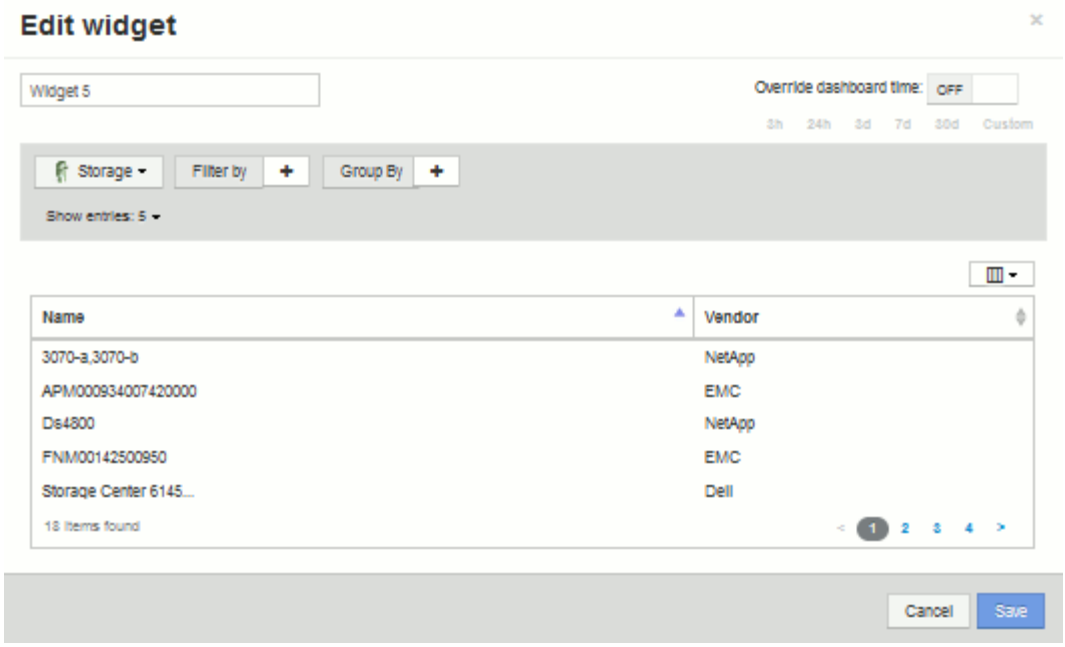
### Schritte

1. Melden Sie sich bei Insight als Benutzer mit Administratorrechten an.
2. Wählen Sie im Menü **Dashboards** die Option **+Neues Dashboard**.

   Die Seite Neues Dashboard wird geöffnet.

3. Geben wir unserem Dashboard einen aussagekräftigen Namen. Klicken Sie Auf **Speichern**. Geben Sie im Feld **Name** einen eindeutigen Namen für das Dashboard ein, z. B. „`VM Performance by Application`“.
4. Klicken Sie auf **Speichern**, um das Dashboard mit dem neuen Namen zu speichern.
5. Beginnen wir mit dem Hinzufügen unserer Widgets. Schieben Sie bei Bedarf den Schalter **Bearbeiten** auf „`on`“, um den Bearbeitungsmodus zu aktivieren.
6. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie **Tabelle Widget**, um ein neues Tabelle Widget zum Dashboard hinzuzufügen.

   Das Dialogfeld Widget bearbeiten wird geöffnet. Der Standardname ist „`Widget 1`“, und die Standarddaten werden für alle Speicher in Ihrer Umgebung angezeigt.




7. Wir können dieses Widget anpassen. Löschen Sie im Feld Name „`Widget 1`“, und geben Sie „`Virtual Machine Performance table`“ ein.
8. Klicken Sie auf das Dropdown-Menü Asset-Typ und ändern Sie **Storage** in **Virtual Machine**.

   Die Änderungen an den Tabellendaten werden angezeigt, wenn alle Virtual Machines in Ihrer Umgebung angezeigt werden. Vorerst werden in der Tabelle nur die VM-Namen angezeigt. Fügen wir der Tabelle einige Spalten hinzu.

9. Klicken Sie auf *Spalten* Und wählen Sie *Data Center*, *Storage Name* und *IOPS - Total* aus. Sie können auch versuchen, den Namen in die Suche einzugeben, um schnell die gewünschten Felder anzuzeigen.

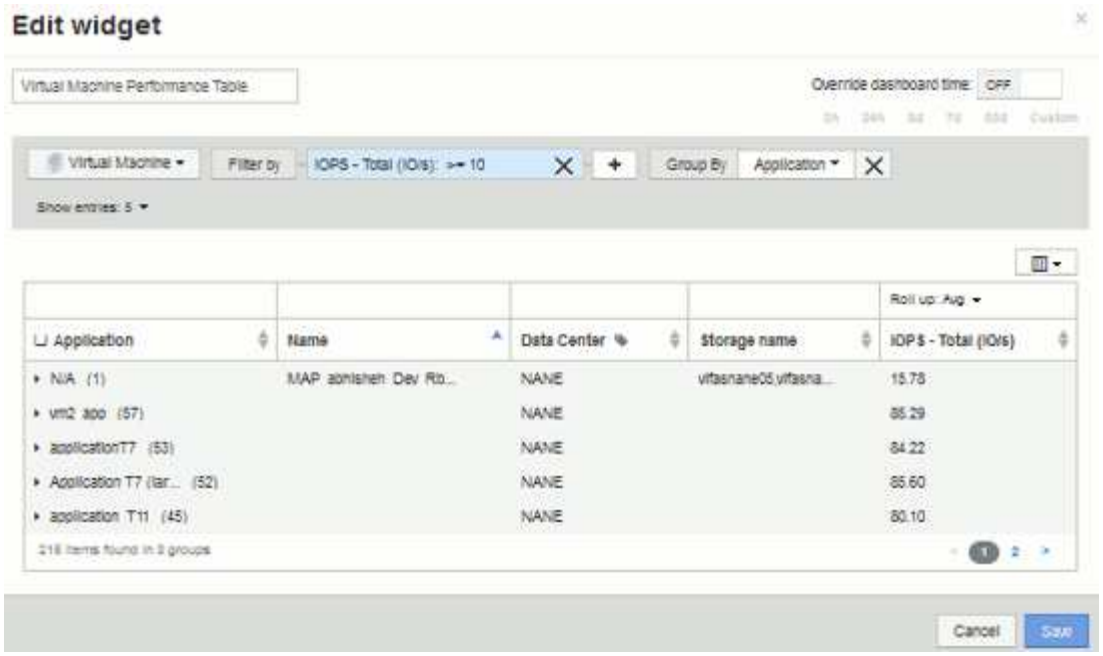
   Diese Spalten werden nun in der Tabelle angezeigt. Sie können die Tabelle nach einer dieser Spalten sortieren. Beachten Sie, dass die Spalten in der Reihenfolge angezeigt werden, in der sie dem Widget hinzugefügt wurden.

10. Bei dieser Übung werden wir VMs ausschließen, die nicht aktiv genutzt werden. Wir sollten also etwas mit weniger als 10 IOPS insgesamt herausfiltern. Klicken Sie neben **Filter by** auf die Schaltfläche` + ` und wählen Sie*IOPS - Total (IO/s)*. Klicken Sie auf **any** und geben Sie “10” in das Feld **von** ein. Lassen Sie das Feld * to* leer. Klicken Sie auf das Um den Filter zu speichern.

    Die Tabelle zeigt jetzt nur VMs mit insgesamt 10 IOPS oder mehr.

11. Wir können die Tabelle weiter reduzieren, indem wir Ergebnisse gruppieren. Klicken Sie neben **Gruppieren nach** auf die Schaltfläche „` + `“ und wählen Sie ein Feld aus, nach dem Sie gruppieren möchten, z. B. Applikation oder Cluster. Gruppierung wird automatisch angewendet.

    Die Tabellenzeilen werden nun entsprechend Ihrer Einstellung gruppiert. Sie können die Gruppen nach Bedarf erweitern und reduzieren. Gruppierte Zeilen zeigen gerollte Daten für jede der Spalten an. In einigen Spalten können Sie die Aufrollmethode für diese Spalte auswählen.



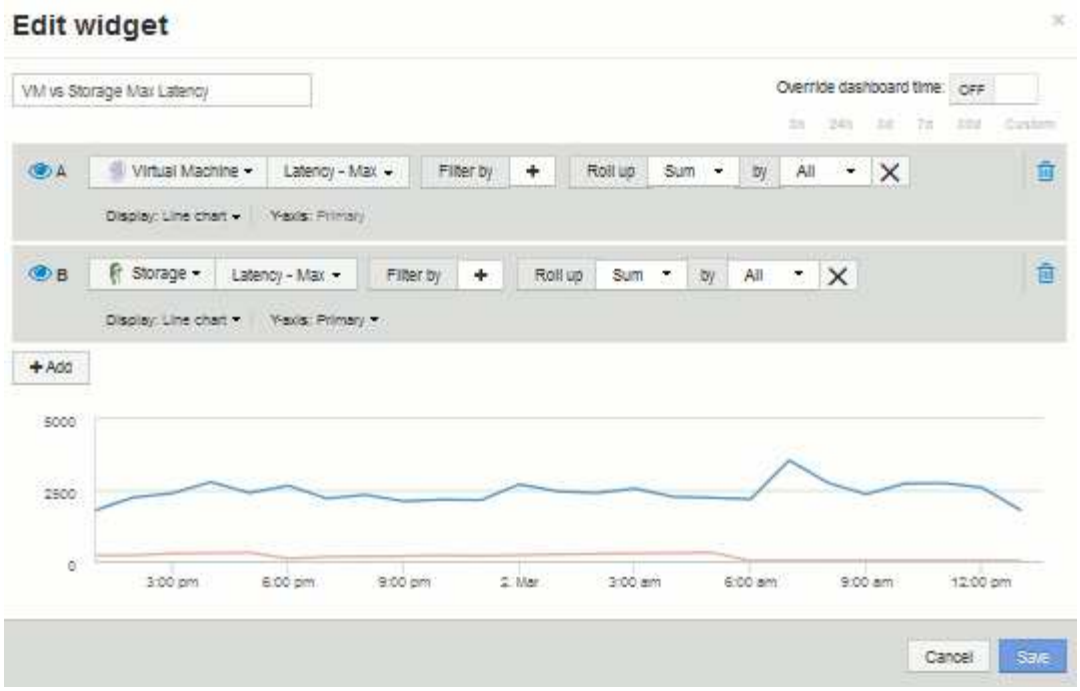

12. Wenn Sie das Tabellen-Widget an Ihre Zufriedenheit angepasst haben, klicken Sie auf die Schaltfläche **Speichern**.

    Das TabellenWidget wird im Dashboard gespeichert.

13. Sie können die Größe des Widgets auf dem Dashboard ändern, indem Sie die untere rechte Ecke ziehen. Machen Sie das Widget breiter, um alle Spalten deutlich anzuzeigen. Klicken Sie auf **Speichern**, um das aktuelle Dashboard zu speichern.
14. Als nächstes fügen wir einige Diagramme hinzu, um unsere VM-Performance anzuzeigen. Erstellen wir nun ein Liniendiagramm, in dem die VM-Latenz mit der Storage-Latenz verglichen wird.
15. Schieben Sie bei Bedarf den Schalter **Bearbeiten** auf „`on`“, um den Bearbeitungsmodus zu aktivieren.
16. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie **Liniendiagramm**, um ein neues Liniendiagramm-Widget zum Dashboard hinzuzufügen.

    Das Dialogfeld Widget bearbeiten wird geöffnet. Klicken Sie auf das Feld **Name** und benennen Sie dieses Widget „`VM vs. Storage Max Latency`“.

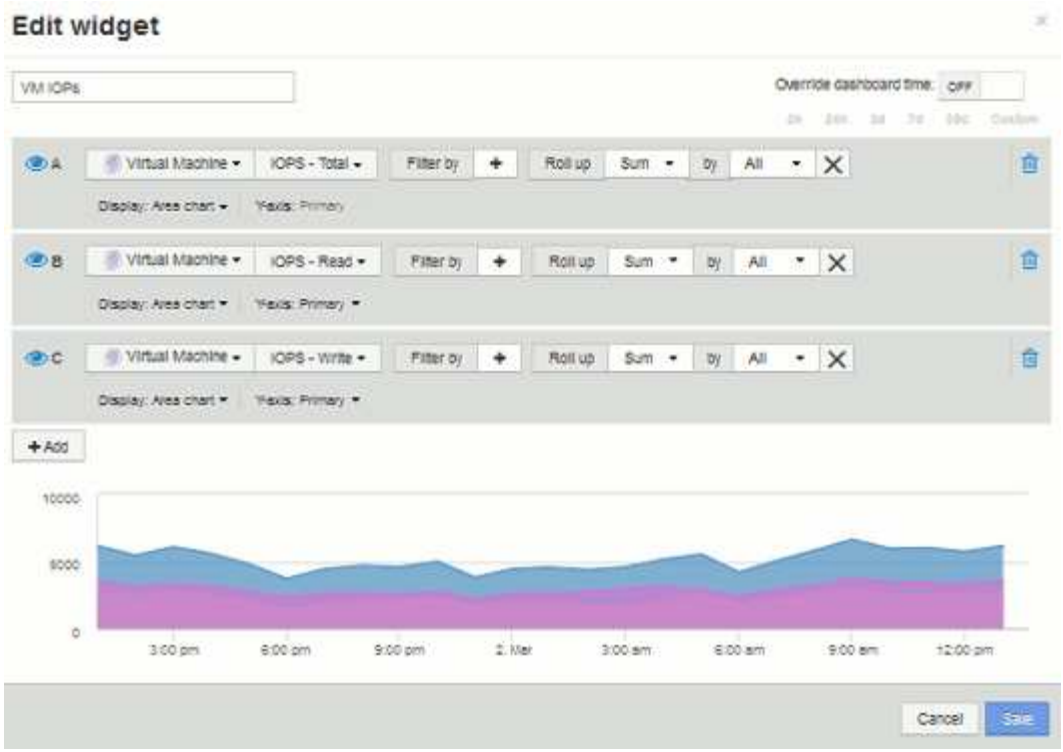
17. Wählen Sie **Virtual Machine** und wählen Sie **Latency - Max**. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Wählen Sie für **Roll-up** „`sum`“ von „`All`“. Diese Daten als**Liniendiagramm** anzeigen und die Y-Achse als **primär** belassen.
18. Klicken Sie auf die Schaltfläche **+Add**, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Storage** und **Latency - Max** aus. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Wählen Sie für **Roll-up** „`sum`“ von „`All`“. Diese Daten als**Liniendiagramm** anzeigen und die Y-Achse als **primär** belassen.




19. Klicken Sie auf **Speichern**, um dieses Widget zum Dashboard hinzuzufügen.
20. Als nächstes fügen wir ein Diagramm mit den IOPS „Lesen“, „Schreiben“ und „Gesamt“ in einem einzelnen Diagramm ein.
21. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie **Bereichsdiagramm**, um ein neues Widget für die Flächendiagramme zum Dashboard hinzuzufügen.

    Das Dialogfeld Widget bearbeiten wird geöffnet. Klicken Sie auf das Feld **Name** und benennen Sie dieses Widget „`VM IOPS`“.

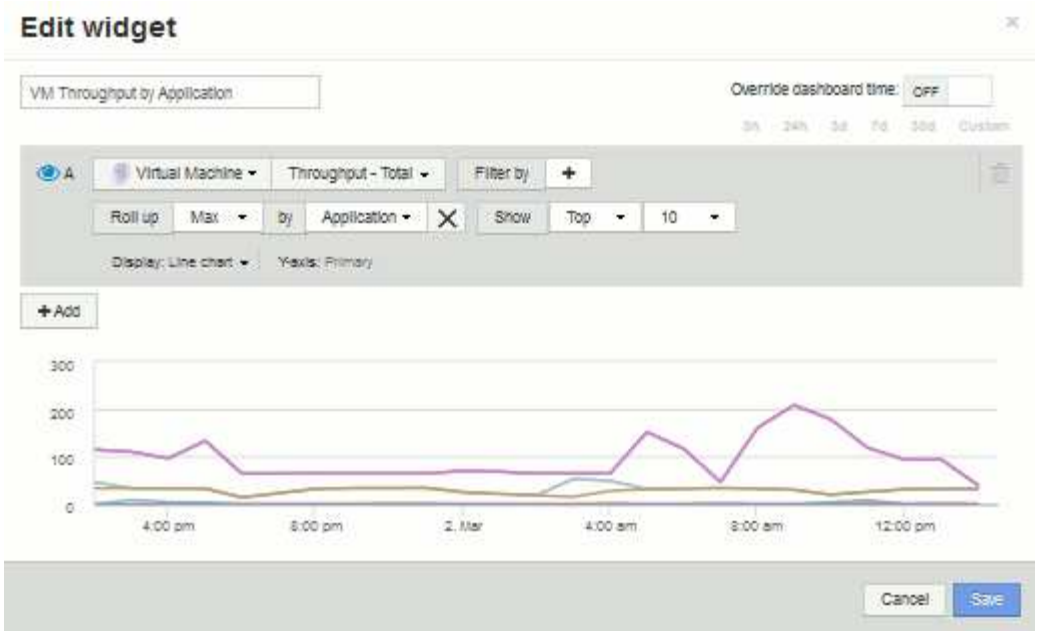
22. Wählen Sie **Virtual Machine** und wählen Sie **IOPS - Total**. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Wählen Sie für **Roll-up** „`sum`“ von „`All`“. Diese Daten als**Flächendiagramm** anzeigen und die Y-Achse als **primär** belassen.
23. Klicken Sie auf die Schaltfläche +Hinzufügen, um eine zweite Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und wählen Sie **IOPS - Lesen**. Y-Achse als **primär** belassen.
24. Klicken Sie auf die Schaltfläche +Hinzufügen, um eine dritte Datenzeile hinzuzufügen. Wählen Sie für diese Zeile **Virtual Machine** und wählen Sie **IOPS - Write**. Y-Achse als **primär** belassen.




25. Klicken Sie auf **Speichern**, um dieses Widget zum Dashboard hinzuzufügen.
26. Danach fügen wir ein Diagramm hinzu, das den VM-Durchsatz für jede mit der VM verbundene Applikation anzeigt. Dafür nutzen wir die Roll-Up-Funktion.
27. Klicken Sie auf die Schaltfläche **Widget** und wählen Sie **Liniendiagramm**, um ein neues Liniendiagramm-Widget zum Dashboard hinzuzufügen.

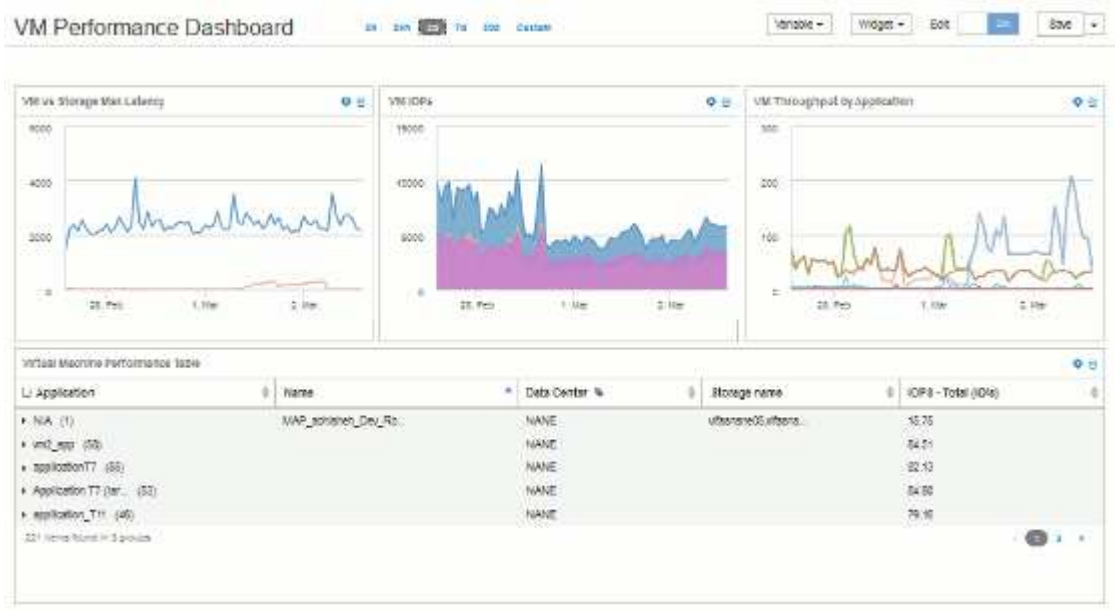
    Das Dialogfeld Widget bearbeiten wird geöffnet. Klicken Sie auf das Feld **Name** und benennen Sie dieses Widget „`VM Throughput by Application`“.

28. Wählen Sie **Virtual Machine** und wählen Sie **Throughput - Total**. Stellen Sie alle gewünschten Filter ein, oder lassen Sie **Filter durch** leer. Wählen Sie für **Roll-up** „`Max`“ und dann „`Application`“ oder „`Name`“. Zeigen Sie die **Top 10**-Anwendungen an. Diese Daten als**Liniendiagramm** anzeigen und die Y-Achse als **primär** belassen.




29. Klicken Sie auf **Speichern**, um dieses Widget zum Dashboard hinzuzufügen.
30. Sie können Widgets verschieben, indem Sie die Maustaste an einer beliebigen Stelle im oberen Bereich des Widgets gedrückt halten und an eine neue Position ziehen. Sie können die Größe von Widgets ändern, indem Sie die untere rechte Ecke ziehen. Achten Sie darauf, das Dashboard nach den Änderungen **Speichern** zu speichern.

    Ihr letztes VM Performance Dashboard sieht folgendermaßen aus:




## Beispiel für ein Dashboard zur Auslastung von Storage-Nodes mit Variablen

Erstellen Sie ein benutzerdefiniertes Dashboard für die Storage-Analyse, das Variablen für Storage, Storage-Pool, Node, Tier, Auslastung und Latenz enthält.

### Bevor Sie beginnen

Es wird empfohlen, sich mit Dashboards in Insight vertraut zu machen, jedoch nicht erforderlich.

### Über diese Aufgabe

Mit dem folgenden Verfahren wird ein benutzerdefiniertes Dashboard zur Storage-Analyse erstellt, das Variablen für Storage, Storage-Pool, Node, Tier, Auslastung und Latenz verwendet. Variablen im folgenden Beispiel werden verwendet, um die angezeigten Assets oder Metriken über ein oder mehrere Widgets zu filtern, die auf dem Dashboard verfügbar sind. Die Widgets, die diese Variablen als Filter verwenden, werden nach Bedarf mit gefiltertem Inhalt aktualisiert, entsprechend den Werten, die in den Variablenfeldern im Dashboard eingegeben wurden. So können Sie schnell mehrere Diagramme und Diagramme filtern, um einen bestimmten Bereich von Interesse zu finden.

Wenn Sie die Schritte in diesem Beispiel befolgen, erstellen Sie ein Dashboard wie das folgende. Sie können diese Widgets ändern oder eine beliebige Anzahl zusätzlicher Widgets hinzufügen, um die von Ihnen ausgewählten Daten hervorzuheben.

### Schritte

1. Erstellen Sie ein neues Dashboard und nennen Sie es „`Analyse: Storage Overview`“ – oder etwas, das ebenso aussagekräftig ist.
2. Klicken Sie auf die Dropdown-Liste **Variable** und wählen Sie den Variablentyp **Text**. Standardmäßig wird die Variable *€21.1* genannt. Klicken Sie auf _ € var1_, um den Namen zu bearbeiten, und ändern Sie ihn in _ € Storage_. Klicken Sie dann auf das Häkchen, um die Variable zu speichern. Wiederholen Sie diese Schritte, um Textvariablen für *€Knoten*, *€Pool* und *€Volumen* zu erstellen.
3. Wiederholen Sie den oben genannten Prozess, um Variablen vom Typ **Anzahl** mit den Namen _ USD Utilization_ und _ USD Latenz_ zu erstellen.
4. Klicken Sie auf die Dropdown-Liste **Variable** und suchen Sie nach der *Tier*-Anmerkung. Wählen Sie diese Option aus, um eine Variable mit dem Namen „ _ USD -Stufe_“ zu erstellen.

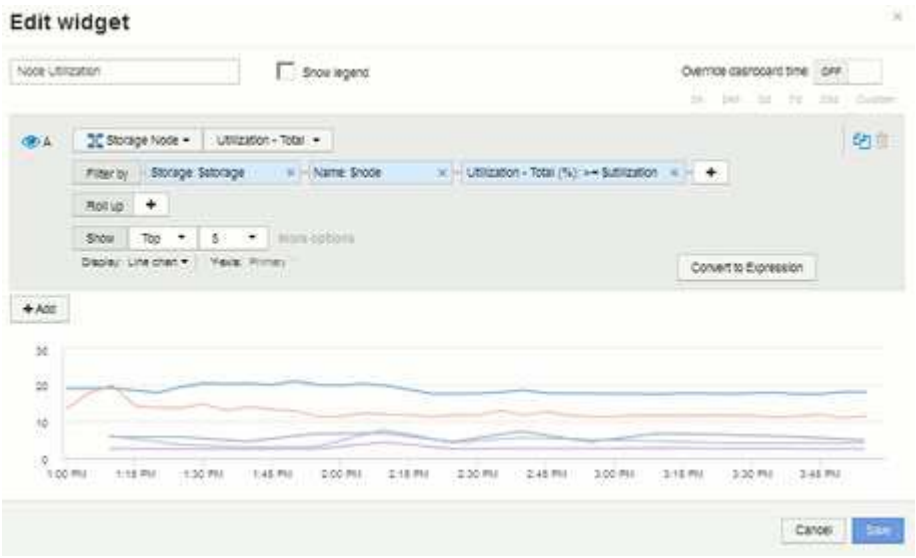
Sie können Variablen jederzeit hinzufügen, es ist jedoch einfacher, sie im Voraus zu erstellen und somit für alle Widgets verfügbar zu machen, während Sie sie erstellen.

5. Fügen Sie ein Widget hinzu, indem Sie auf das Dropdown-Menü **Widget** klicken und entweder ein **Liniendiagramm**oder **Bereichsdiagramm**-Widget auswählen. Benennen Sie das Widget „`Node Utilization`“. Klicken Sie auf den Asset-Typ **Storage** und ändern Sie ihn in **Storage Node**. Wählen Sie **Auslastung - Gesamt** für die Diagrammdaten.
6. Klicken Sie auf die Schaltfläche **Filtern nach +**, um einen Filter hinzuzufügen. Suchen und wählen Sie **Storage** aus, klicken Sie dann auf **any** und wählen Sie die Variable *€Storage* aus.
7. Klicken Sie auf die Schaltfläche**+**, um einen weiteren Filter für **Name** hinzuzufügen. Setzen Sie die Variable auf *€Knoten*.

   Dem Anmerkungsnamensfilter können verschiedene Variablen zugewiesen werden. Verwenden Sie je nach Objekt im Widget das Name/Variablenpaar auf der untersten Ebene. Beispiel:

   - Sie können die Variable *€Knoten* dem Filter **Name** für ein Knoten-fokussiertes Widget zuweisen.
   - Sie können die Variable *€Pool* dem Filter **Name** für ein Pool-orientiertes Widget zuweisen.
8. Klicken Sie auf die Schaltfläche**+**, um einen weiteren Filter für **Utilization - Total (%)** hinzuzufügen. Setzen Sie die Variable auf *>= € Utilization*.
9. Klicken Sie auf das Feld **X** nach dem**Roll Up**, um das Feld auszublenden.
10. Wählen Sie **Top 5 anzeigen** und klicken Sie auf **Speichern**, um das Widget zu speichern und zu Ihrem Dashboard zurückzukehren.

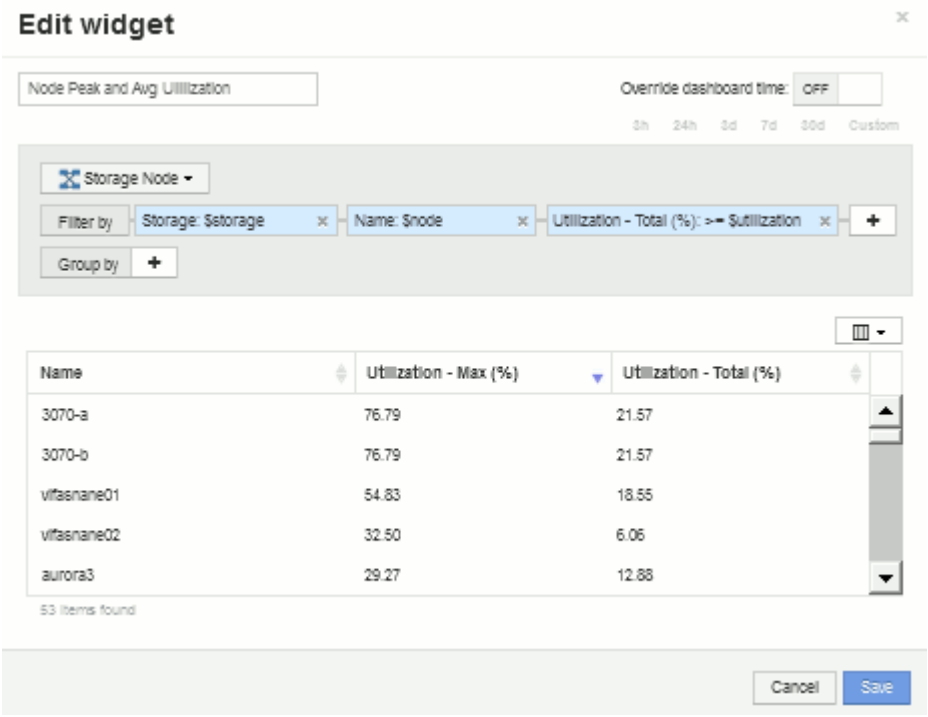
    Ihr Widget sollte so aussehen:




11. Fügen Sie Ihrem Dashboard ein weiteres Linien- oder Bereichsdiagramm-Widget hinzu. Wählen Sie **Storage Node** als Asset-Typ und **Latency - Total** als Metrik zum Diagramm aus.
12. Klicken Sie auf die Schaltfläche **Filtern nach +**, um Filter für **Speicher: € Speicher** und **Name: € Knoten** hinzuzufügen.
13. Fügen Sie einen Filter für **Latency - Total** hinzu und wählen Sie die Variable **€llatenz** aus.
14. Benennen Sie das Widget „`Node Latency`“, und speichern Sie es.
15. Sie können unterstützende Tabellen hinzufügen, um weitere Details für die erstellten Diagramme anzuzeigen, z. B. maximale oder durchschnittliche Knotenauslastung. Fügen Sie dem Dashboard ein

Widget **Tabelle** hinzu und wählen Sie **Storage Node** als Asset-Typ aus. Erstellen Sie Filter für **Storage: € Storage**, **Name: € Node** und **Utilization – Total: € Utilization**.

16. Fügen Sie der Tabelle Spalten für **Auslastung - Max**, **Auslastung - Gesamt** oder andere gewünschte Spalten hinzu.
17. Benennen Sie das Widget „`Node Peak and Average Utilization`“, und speichern Sie es.




18. Wiederholen Sie die Schritte, um eine Tabelle für Node Latency zu erstellen, wobei **Latency - max**, **Latency - Total** oder andere Spalten wie gewünscht angezeigt werden.
19. Um Ihr Dashboard abzurunden, können Sie für einige oder alle der folgenden Elemente zusätzliche Diagramm- und Tabellen-Widgets hinzufügen:

| Diagramm | Tabelle |
|---|---|
| Storage-Pool-Auslastung | Storage Pool: Maximale Auslastung und durchschn. Auslastung |
| Durchsatz Im Storage Pool | Storage Pool: Höchster und durchschn. Durchsatz |
| Volume-Latenz | Volume-Spitzenlatenz und durchschn. Latenz |
| Volume IOPS | Maximale und durchschn. IOPS des Volume |

1. Sie können die Widgets in jeder gewünschten Position auf Ihrem Dashboard verschieben und ihre Größe ändern. Wenn Sie fertig sind, achten Sie darauf, das Dashboard zu speichern.

   Ihr letztes Dashboard sieht in etwa so aus:

2. Sie können die Variablen verwenden, um sich auf bestimmte Assets in Ihrem Dashboard zu konzentrieren. Wenn Sie Werte in die Variablenfelder eingeben, werden die Widgets automatisch aktualisiert, um diese Variablen wiederzugeben. Wenn Sie beispielsweise „15“ in das Feld „Variable für die Verwendung von USD eingeben, werden für die Widgets, die diese Variable verwenden, nur Assets mit Gesamtauslastung >= 15 % angezeigt.

   Widget „Node-Auslastung“ mit den obersten 5 Nodes:

Widget „Node-Auslastung“ mit mindestens 15 % Auslastung:

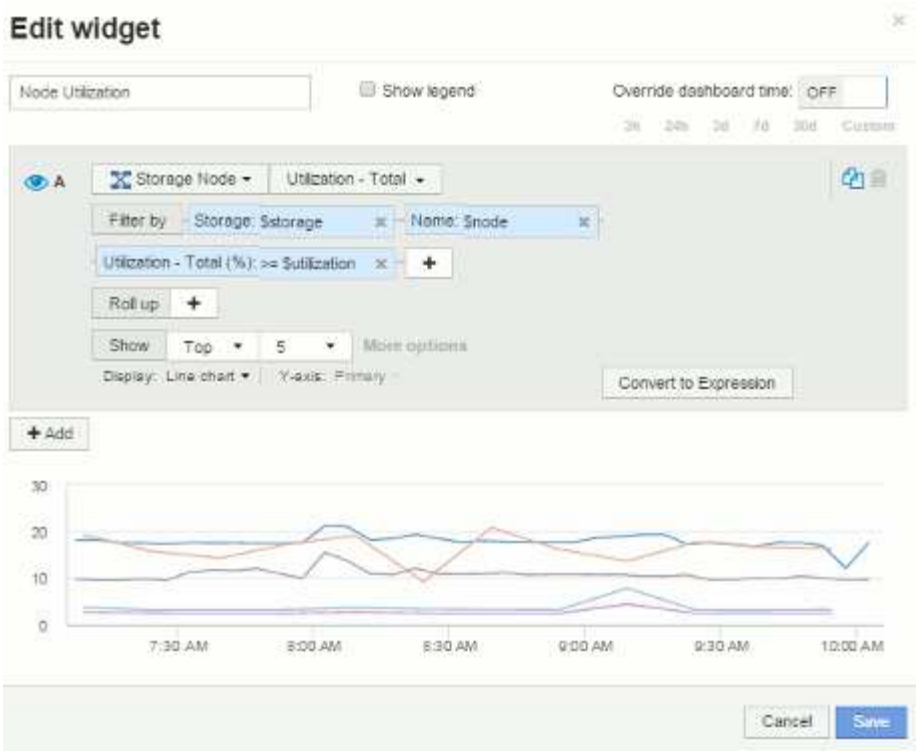
3. Beachten Sie beim Erstellen Ihrer Widgets Folgendes:
   - Die Variable „USD“ wirkt sich nur auf Ressourcen aus, die mit der Anmerkung **Tier** versehen werden.
   - Nicht alle Filter wirken sich auf alle Widgets aus, je nachdem, ob das Widget die angegebene(n) Variable(n) akzeptiert.
   - Zahlenvariablen werden als „`größer oder gleich`“ des angegebenen Werts angewendet. Beachten Sie, dass jede Variable als Filter für jedes Widget auf jeder Ebene einer Speicherhierarchie verwendet werden kann, sofern die Variable für das Asset gültig ist, für das das Widget ausgeführt wird. Wenn Sie von einer Knotenebene auf einen Speicherpool zu einem Widget „Volume“ wechseln, sind weitere Variablen für die Zuweisung als Filter vorhanden. So können beispielsweise in einem Widget auf Storage Node-Ebene die Variablen *Storage* und *Name* als Filter zugewiesen werden. Auf der Ebene des Speicherpools stehen alle *Storage*, *Nodes*, *Storage Pools* und *Name* zur Verfügung. Weisen Sie Ihre Variablen nach Bedarf zu und verwenden Sie die Variable „US-Dollar-Name“ auf der untersten Ebene im Stapel. Dadurch kann Ihre Namensvariable nach dem tatsächlichen Namen des Assets filtern, für das das Widget ausgeführt wird.

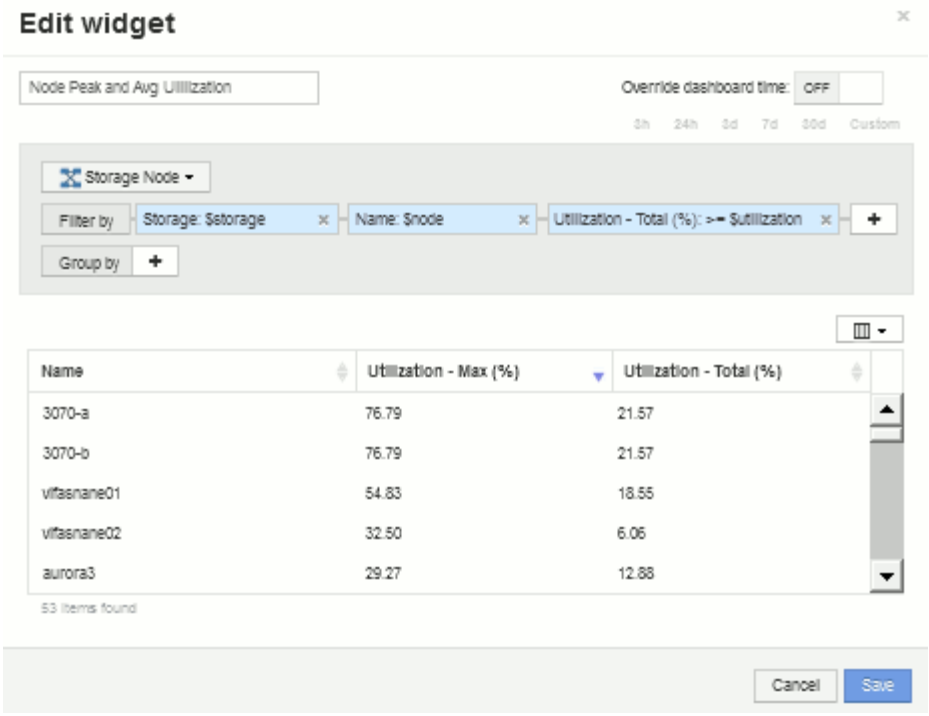
**Beispiel-Widget-Einstellungen für das Node-Dashboard**

## Widget-Einstellungen für das Node-Dashboard mit Variablen, Beispiel.

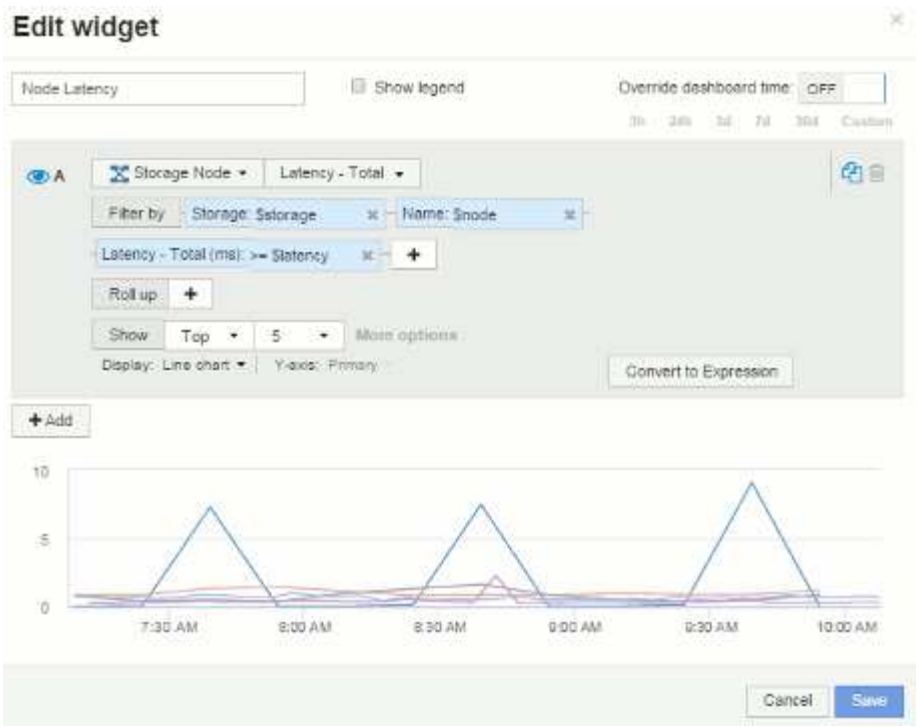
Im Folgenden finden Sie die Einstellungen für die einzelnen Widgets im Dashboard des Storage-Node.

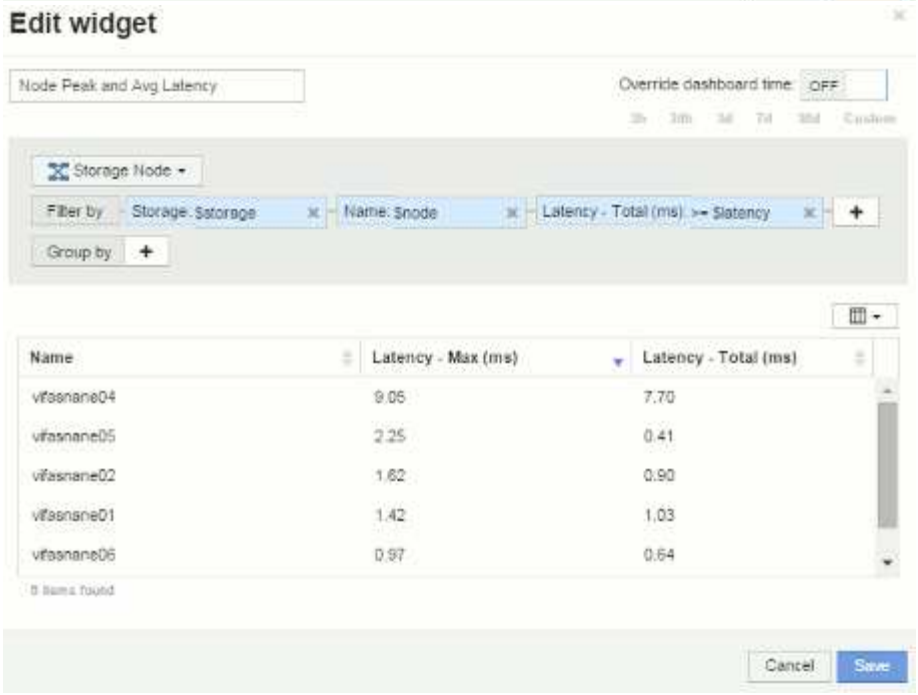
Node-Auslastung:


Edit widget
Node Utilization
Show legend
Override dashboard time:
OFF
A
Storage Node
Utilization - Total
Filter by
Storage: $storage
Name: $node
Utilization - Total (%): >= $utilization
Roll up
Show
Top
5
More options
Display: Line chart
Y-axis: Primary
Convert to Expression
+ Add
30
20
10
0
7:30 AM
8:00 AM
8:30 AM
9:00 AM
9:30 AM
10:00 AM
Cancel
Save

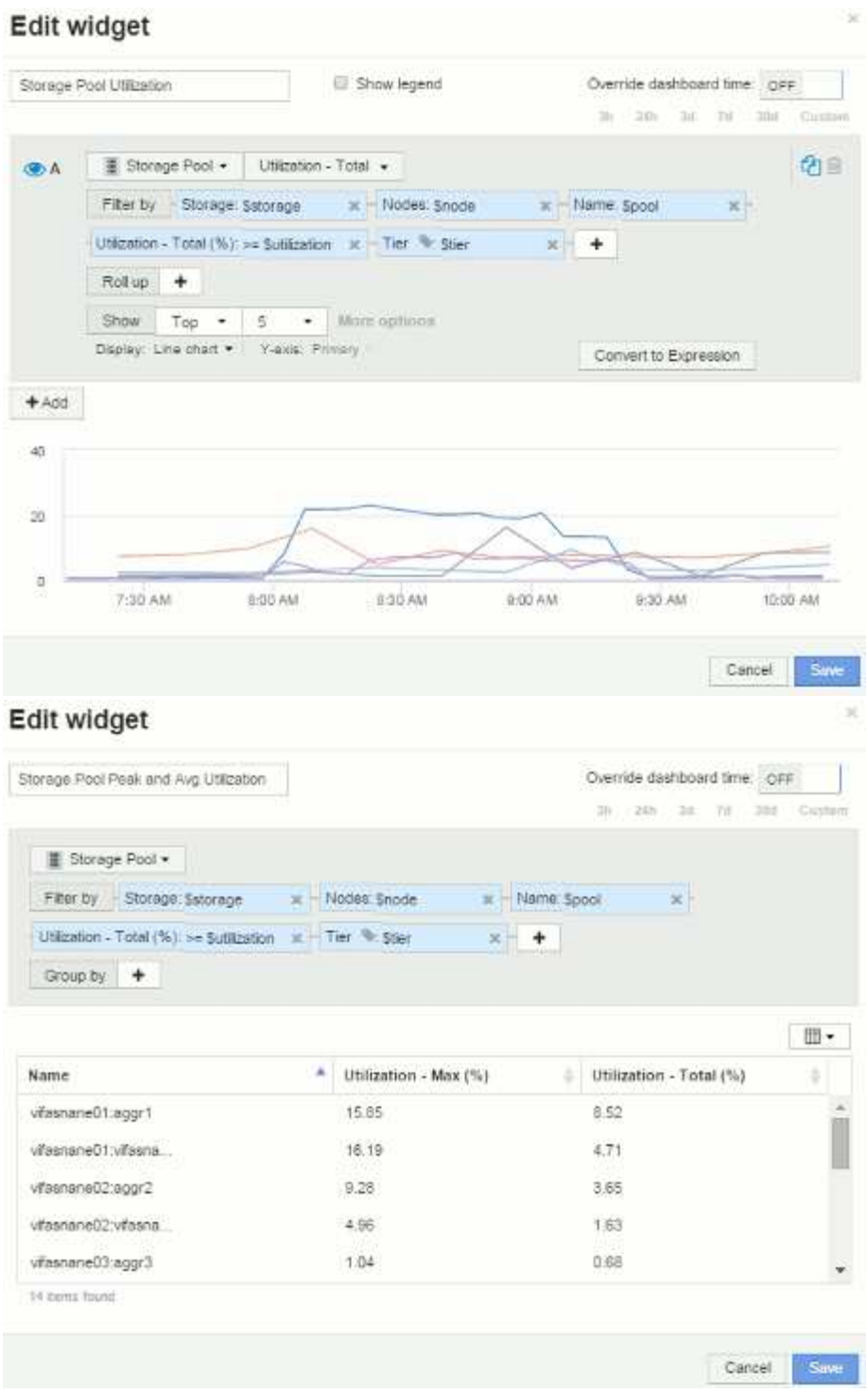

Edit widget
Node Peak and Avg Utilization
Override dashboard time:
OFF
Storage Node
Filter by
Storage: $storage
Name: $node
Utilization - Total (%): >= $utilization
Group by
Name
Utilization - Max (%)
Utilization - Total (%)
3070-a
76.79
21.57
3070-b
76.79
21.57
vifasnane01
54.83
18.55
vifasnane02
32.50
6.06
aurora3
29.27
12.88
53 items found
Cancel
Save

Node-Latenz:



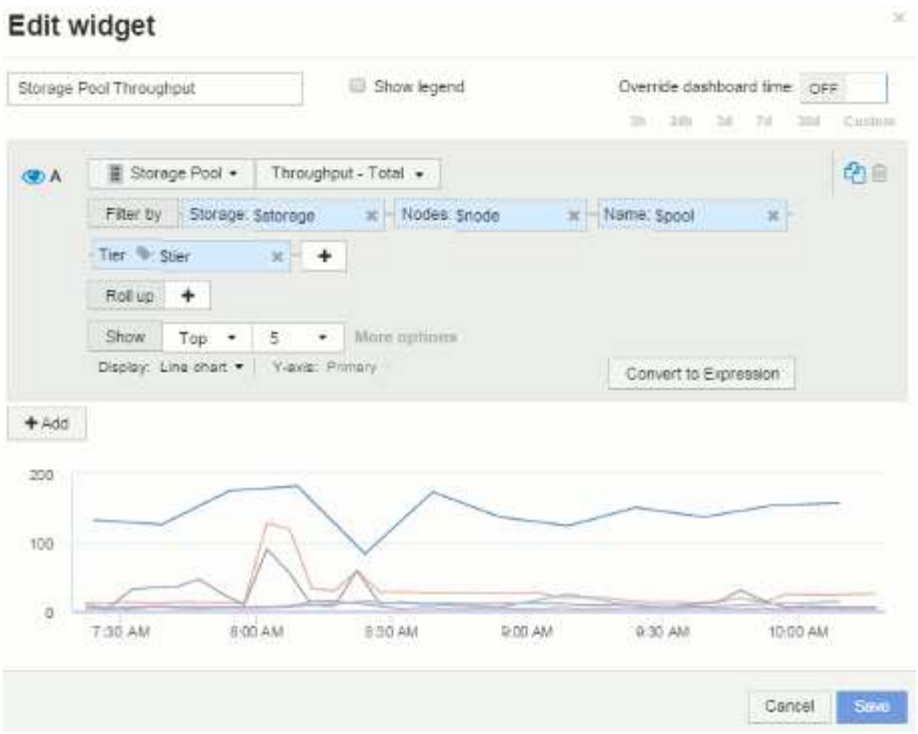

Storage-Pool-Auslastung:

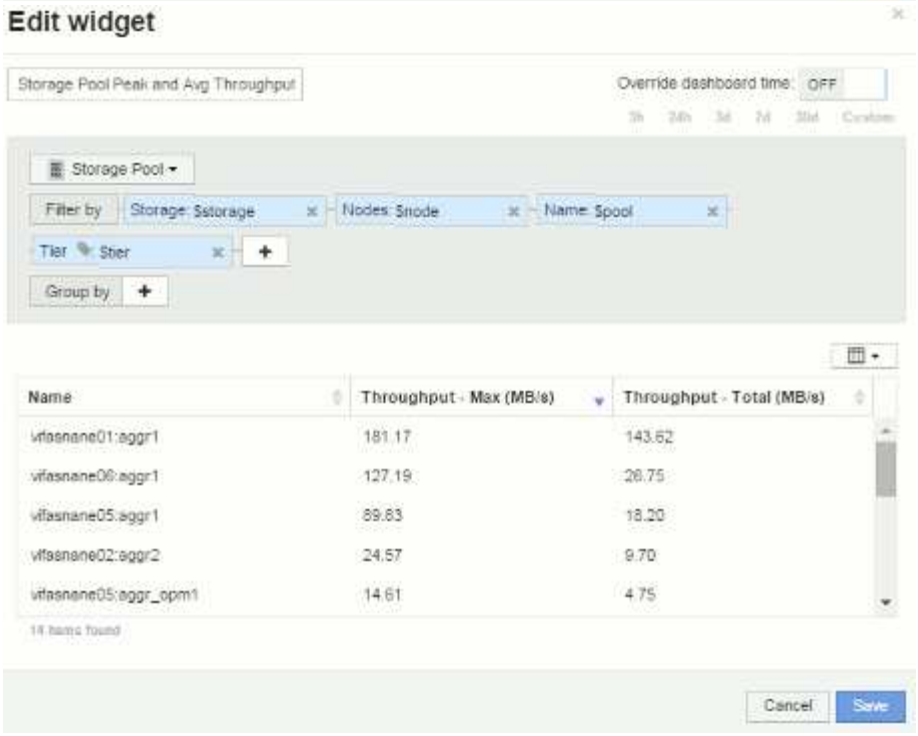




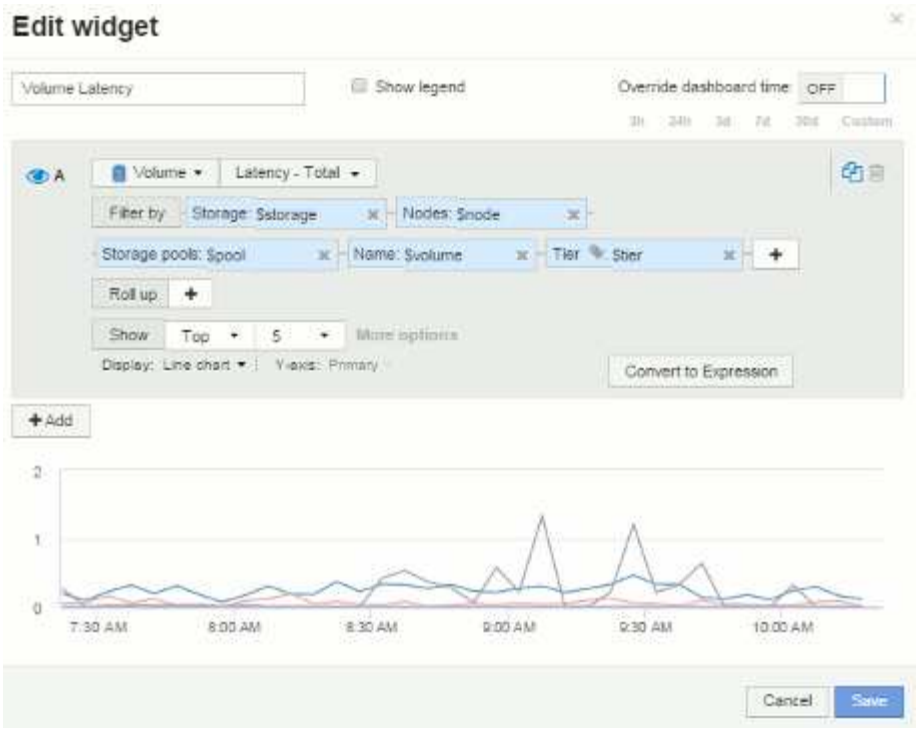


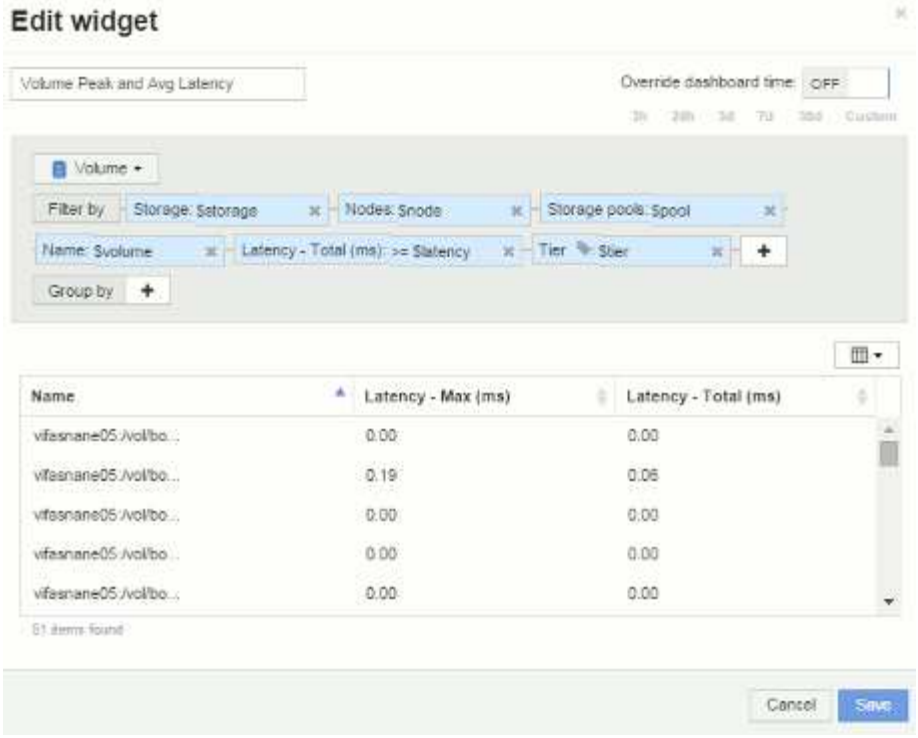
Durchsatz des Storage Pools:



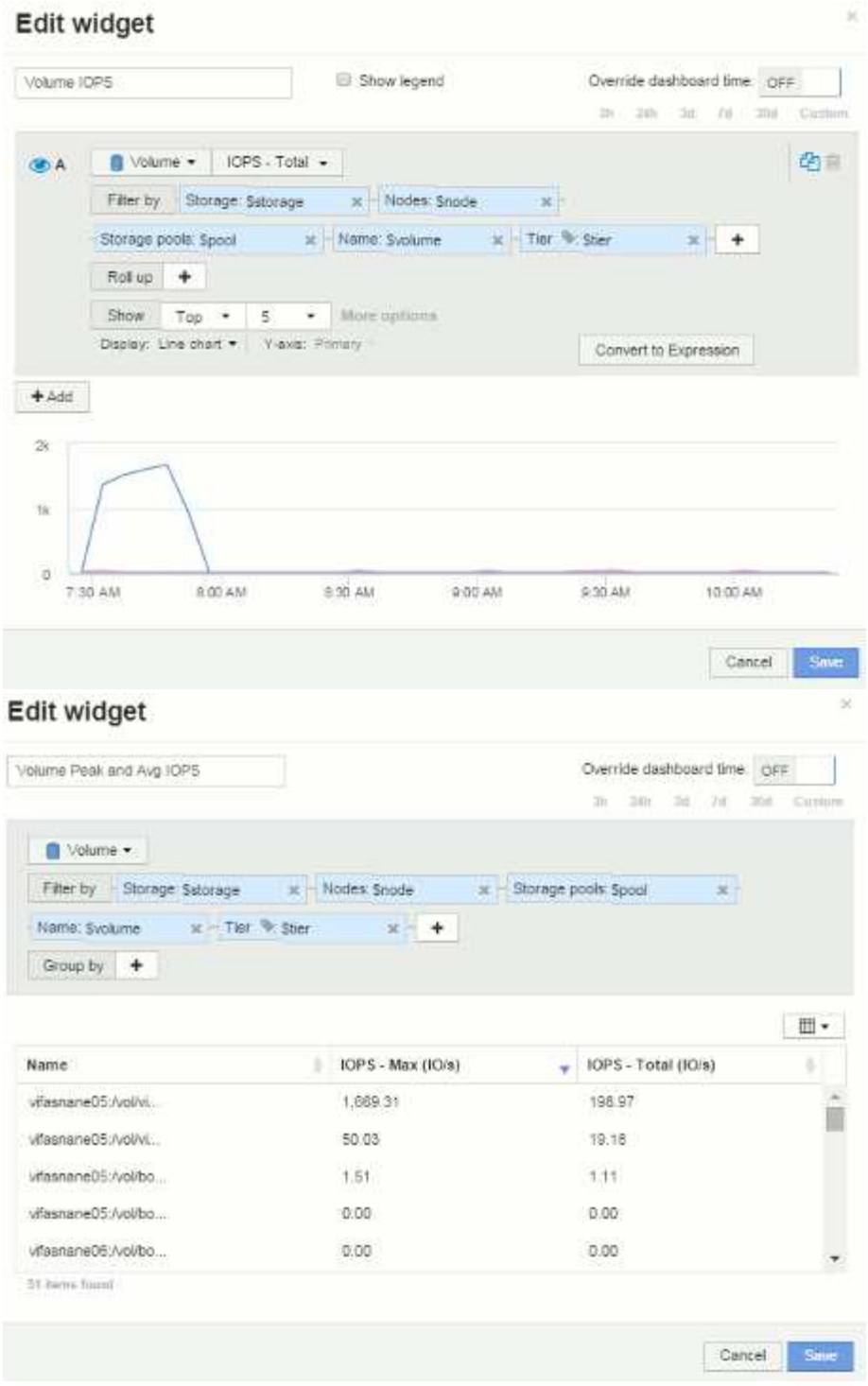




Volume-Latenz:


Edit widget
Volume Latency
Show legend
Override dashboard time
OFF
A
Volume
Latency - Total
Filter by
Storage: $storage
Nodes: $node
Storage pools: $pool
Name: $volume
Tier
$tier
Roll up
Show
Top
5
More options
Display: Line chart
Y-axis: Primary
Convert to Expression
+ Add
2
1
0
7:30 AM
8:00 AM
8:30 AM
9:00 AM
9:30 AM
10:00 AM
Cancel
Save


Edit widget
Volume Peak and Avg Latency
Override dashboard time
OFF
Volume
Filter by
Storage: $storage
Nodes: $node
Storage pools: $pool
Name: $volume
Latency - Total (ms): >= $latency
Tier
$tier
Group by
Name
Latency - Max (ms)
Latency - Total (ms)
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.19
0.06
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.00
0.00
vifasnane05:/vol/bo...
0.00
0.00
61 items found
Cancel
Save

Volume-IOPS:




## Best Practices für Dashboards und Widgets

Tipps und Tricks, damit Sie die leistungsstarken Funktionen von Dashboards und Widgets optimal nutzen können.

#### Best Practice: Die richtige Metrik finden

OnCommand Insight erfasst Zähler und Metriken anhand von Namen, die sich manchmal von Datenquelle zu Datenquelle unterscheiden.

Bei der Suche nach der richtigen Metrik oder dem Zähler für Ihr Dashboard-Widget sollten Sie bedenken, dass die Metrik, die Sie benötigen, unter einem anderen Namen als der Metrik stehen kann, an die Sie denken. Obwohl Dropdown-Listen in OnCommand Insight normalerweise alphabetisch sind, wird ein Begriff manchmal nicht in der Liste angezeigt, wo er Ihrer Meinung nach erscheinen sollte. Beispielsweise werden Begriffe wie „Rohkapazität“ und „genutzte Kapazität“ in den meisten Listen nicht zusammen angezeigt.

Best Practice: Verwenden Sie die Suchfunktion in Feldern wie **Filter by** oder Orten wie der Spaltenauswahl Um zu finden, wonach Sie suchen. Wenn Sie beispielsweise nach „Cap“ suchen, werden alle Metriken mit „Capacity“ in ihren Namen angezeigt, unabhängig davon, wo sie auftreten. Sie können dann ganz einfach die gewünschten Metriken aus dieser kurzen Liste auswählen.

Hier sind ein paar alternative Formulierungen, die Sie bei der Suche nach Metriken versuchen können:

| Wann Sie suchen möchten: | Versuchen Sie auch die Suche nach: |
|---|---|
| CPU | Prozessor |
| Kapazität | Genutzte KapazitätRohkapazität<br><br>Bereitgestellte Kapazität<br><br>Speicher-Pools Kapazität<br><br><other asset type>-Kapazität<br><br>Geschriebene Kapazität |
| Festplattengeschwindigkeit | Niedrigste FestplattenschnelleLeast performing Disk type |
| Host | HypervisorHosten |
| Hypervisor | Hostis-Hypervisor |
| Mikrocode | Firmware |
| Name | AliasHypervisor-Name<br><br>Speichername<br><br>Der Name der <other asset type><br><br>Einfacher Name<br><br>Ressourcenname<br><br>Fabric-Alias |

| | |
|---|---|
| Lesen/Schreiben | Partielles R/WAusstehende Schreibvorgänge<br>IOPS – Schreiben<br>Geschriebene Kapazität<br>Latenz – Lesen<br>Cache-Auslastung – Lesen |
| Virtual Machine | VMIS virtuell |

Dies ist keine umfassende Liste. Dies sind nur Beispiele für mögliche Suchbegriffe.

**Best Practice: Die richtigen Assets finden**

## Die Insight Ressourcen, auf die Sie in Widget-Filtern verweisen können, variieren von Asset-Typ zu Asset-Typ.

In Dashboards bestimmt der Asset-Typ, um den Sie Ihr Widget erstellen, die anderen Asset-Typ-Zähler, für die Sie eine Spalte filtern oder hinzufügen können. Beachten Sie beim Erstellen Ihres Widgets Folgendes:

| Dieser Asset-Typ / Zähler: | Kann unter diesen Assets gefiltert werden: |
|---|---|
| Virtual Machine | VMDK |
| Datenspeicher(e) | Internes VolumeVMDK<br>Virtual Machine<br>Datenmenge |
| Hypervisor | Virtual Machine |
| Für Hypervisor | Host |
| Host(s) | Internes VolumeVolume |
| Cluster | HostVirtual Machine |
| Fabric | Port |

Dies ist keine umfassende Liste.

Best Practice: Wenn Sie nach einem bestimmten Asset-Typ filtern, der nicht in der Liste angezeigt wird, versuchen Sie, Ihre Abfrage um einen alternativen Asset-Typ zu erstellen.

### Streudiagramm Beispiel: Wissen der Achse

Wenn Sie die Reihenfolge der Zähler in einem Streudiagramm-Widget ändern, werden die Achsen geändert, auf denen die Daten angezeigt werden.

#### Über diese Aufgabe

Dieses Beispiel erstellt ein Scatter-Diagramm, mit dem Sie leistungsschwache VMs sehen können, die eine hohe Latenz im Vergleich zu niedrigen IOPS haben.

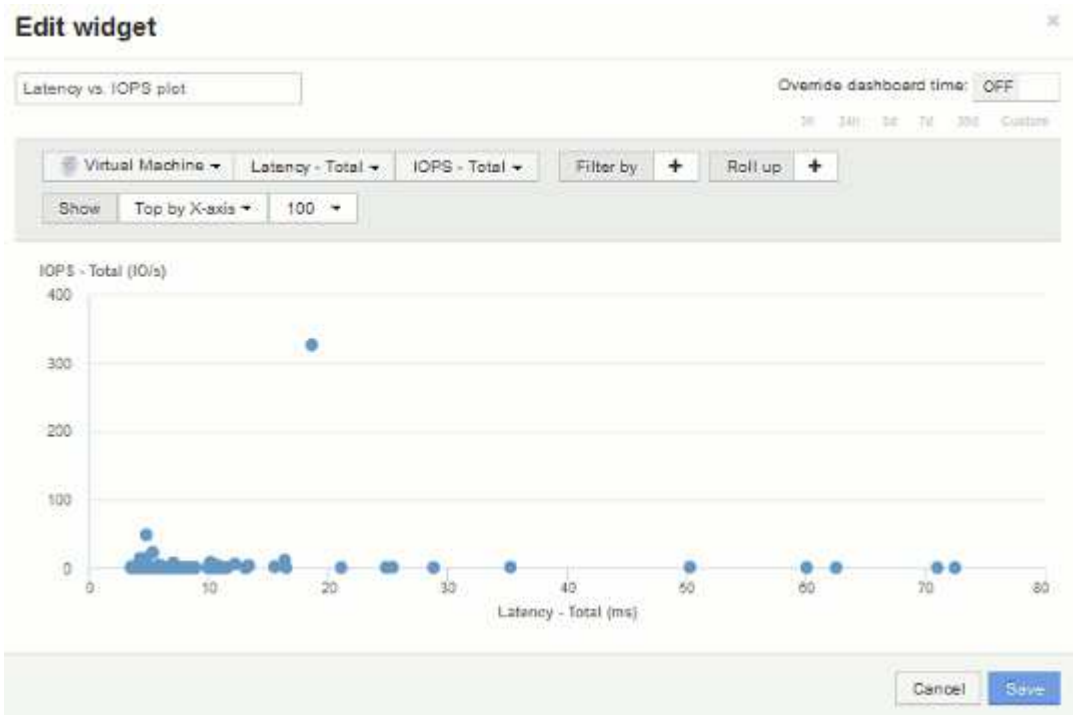
#### Schritte

1. Erstellen oder öffnen Sie ein Dashboard im Bearbeitungsmodus und fügen Sie ein Widget **Streudiagramm** hinzu.
2. Wählen Sie einen Asset-Typ aus, zum Beispiel **Virtual Machine**.
3. Wählen Sie den ersten Zähler aus, den Sie zeichnen möchten. Wählen Sie für dieses Beispiel **Latency - Total** aus.

   *Latenz - Total* wird entlang der X-Achse des Diagramms kartiert.

4. Wählen Sie den zweiten Zähler aus, den Sie zeichnen möchten. Wählen Sie in diesem Beispiel **IOPS - Total** aus.

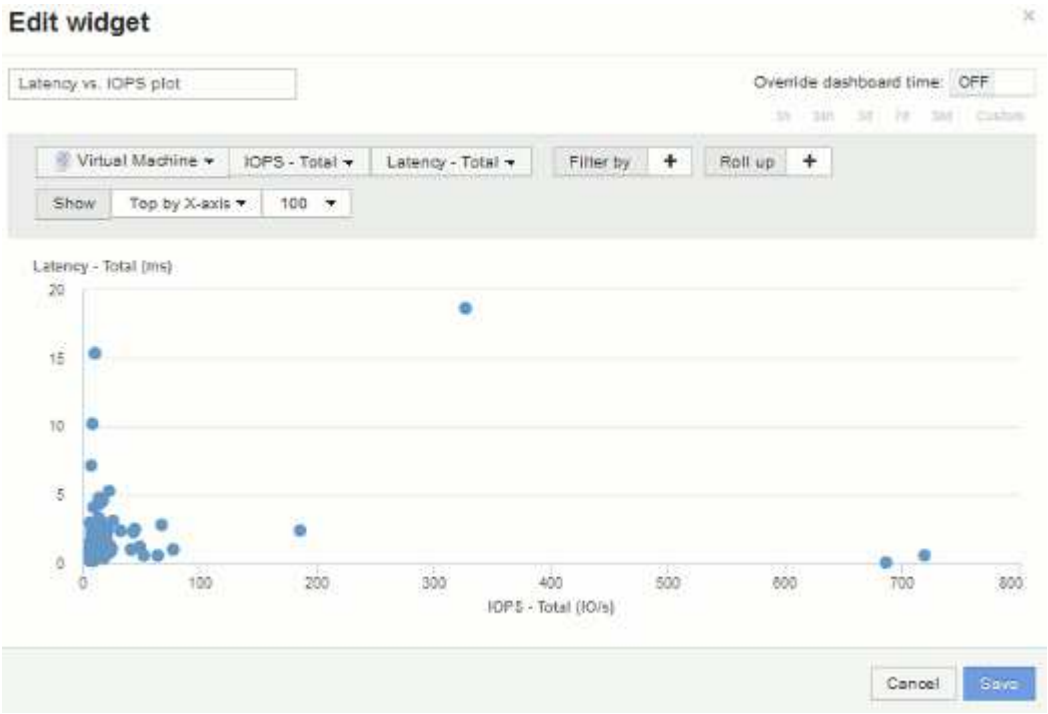
   *IOPS - Total* wird entlang der Y-Achse im Diagramm dargestellt. VMs mit höherer Latenz werden rechts im Diagramm angezeigt. Es werden nur die 100 VMs mit der höchsten Latenz angezeigt, da die Einstellung **Top by X-Axis** aktuell ist.




5. Kehren Sie nun die Reihenfolge der Zähler um, indem Sie den ersten Zähler auf **IOPS - Total** und den zweiten auf **Latency - Total** setzen.

   *latency- Total* wird nun entlang der Y-Achse im Diagramm und*IOPS - Total* entlang der X-Achse dargestellt. VMs mit höheren IOPS werden jetzt rechts im Diagramm angezeigt.

Da wir die **Top by X-Axis**-Einstellung nicht geändert haben, zeigt das Widget jetzt die Top 100 VMs mit den höchsten IOPS an, da dies das ist, was derzeit entlang der X-Achse dargestellt wird.




6. Sie können wählen, dass das Diagramm die obere N nach X-Achse, die obere N nach Y-Achse, die untere N nach X-Achse oder die untere N nach Y-Achse anzeigt. In unserem letzten Beispiel werden die 100 besten VMs angezeigt, die die höchsten *Gesamt-IOPS* haben. Wenn wir ihn auf die Y-Achse oben ändern, werden im Diagramm erneut die 100 wichtigsten VMs mit der höchsten *Gesamtlatenz* angezeigt.

   Beachten Sie, dass Sie in einem Streudiagramm-Diagramm auf einen Punkt klicken können, um die Bestandsseite für diese Ressource zu öffnen.

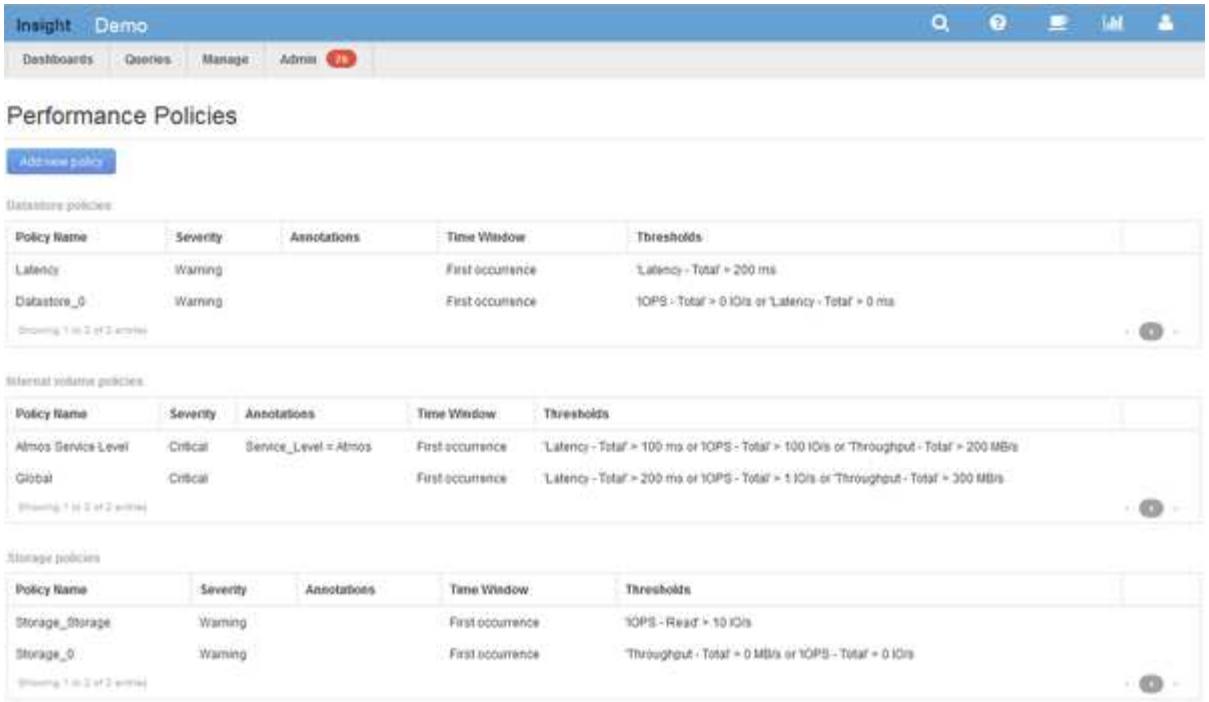
# Erstellung von Performance-Richtlinien

Sie erstellen Performance-Richtlinien, um Schwellenwerte festzulegen, die Warnmeldungen auslösen, um Sie über Probleme im Zusammenhang mit den Ressourcen in Ihrem Netzwerk zu informieren. Sie können beispielsweise eine Performance-Richtlinie erstellen, um Sie zu benachrichtigen, wenn die Gesamtauslastung für Storage-Pools über 60 % liegt.

## Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser.
2. Wählen Sie **Verwalten** > **Leistungsrichtlinien** Aus.

   Die Seite Leistungsrichtlinien wird angezeigt.




Richtlinien werden nach Objekten organisiert und in der Reihenfolge bewertet, in der sie in der Liste für das Objekt angezeigt werden.

3. Klicken Sie auf **Neue Richtlinie hinzufügen**.

   Das Dialogfeld Richtlinie hinzufügen wird angezeigt.

4. Geben Sie im Feld **Richtlinienname** einen Namen für die Richtlinie ein.

   Sie müssen einen Namen verwenden, der sich von allen anderen Richtliniennamen für das Objekt unterscheidet. Sie können beispielsweise nicht zwei Richtlinien mit dem Namen „`Latency`“ für ein internes Volume verwenden. Sie können jedoch eine „`Latency`“-Richtlinie für ein internes Volume und eine weitere „`Latency`“-Richtlinie für ein anderes Volume haben. Es empfiehlt sich, immer einen eindeutigen Namen für eine Richtlinie zu verwenden, unabhängig vom Objekttyp.

5. Wählen Sie in der Liste **auf Objekte des Typs anwenden** den Objekttyp aus, für den die Richtlinie gilt.
6. Wählen Sie in der Liste **with annotation** ggf. einen Anmerkungstyp aus und geben Sie einen Wert für die Anmerkung in das Feld **Wert** ein, um die Richtlinie nur auf Objekte anzuwenden, die diesen speziellen Anmerkungssatz haben.
7. Wenn Sie **Port** als Objekttyp ausgewählt haben, wählen Sie aus der Liste **Connected To** aus, mit welchem Port verbunden ist.
8. Wählen Sie in der Liste **Übernehmen nach einem Fenster von** aus, wann eine Warnung ausgelöst wird, um eine Schwellenverletzung anzuzeigen.

   Die Option „Erstes Auftreten“ löst eine Warnung aus, wenn ein Schwellenwert bei der ersten Datenprobe überschritten wird. Alle anderen Optionen lösen eine Warnung aus, wenn der Schwellenwert einmal überschritten wird und mindestens die angegebene Zeit lang kontinuierlich überschritten wird.

9. Wählen Sie aus der Liste **with severity** den Schweregrad für die Verletzung aus.
10. Standardmäßig werden E-Mail-Benachrichtigungen zu Richtlinienverstößen an die Empfänger in der globalen E-Mail-Liste gesendet. Sie können diese Einstellungen überschreiben, sodass Benachrichtigungen für eine bestimmte Richtlinie an bestimmte Empfänger gesendet werden.

- Klicken Sie auf den Link, um die Empfängerliste zu öffnen, und klicken Sie dann auf die Schaltfläche **+**, um Empfänger hinzuzufügen. Verstöße gegen diese Richtlinie werden an alle Empfänger in der Liste gesendet.

11. Klicken Sie auf den Link **any** im Abschnitt **Create alert if eines der folgenden sind wahr**, um zu steuern, wie Alarme ausgelöst werden:
    - **Beliebig**

      Dies ist die Standardeinstellung, die Warnungen erstellt, wenn einer der Schwellenwerte für eine Richtlinie überschritten wird.

    - * Alle*

      Durch diese Einstellung wird eine Meldung erstellt, wenn alle Schwellenwerte für eine Richtlinie überschritten werden. Wenn Sie **all** auswählen, wird der erste Schwellenwert, den Sie für eine Performance Policy erstellen, als primäre Regel bezeichnet. Sie müssen sicherstellen, dass der primäre Regelschwellenwert der Verstoß ist, den Sie für die Performance Policy am meisten befürchten.

12. Wählen Sie im Abschnitt **Warnung erstellen, wenn** einen Leistungszähler und einen Operator aus, und geben Sie dann einen Wert ein, um einen Schwellenwert zu erstellen.
13. Klicken Sie auf **Schwellenwert hinzufügen**, um weitere Schwellenwerte hinzuzufügen.
14. Um einen Schwellenwert zu entfernen, klicken Sie auf das Papierkorb-Symbol.
15. Aktivieren Sie das Kontrollkästchen **Verarbeitung weiterer Richtlinien beenden, wenn Warnung generiert wird**, wenn die Policy die Verarbeitung beenden soll, wenn eine Warnung auftritt.

    Wenn Sie beispielsweise vier Richtlinien für Datastores haben und die zweite Richtlinie so konfiguriert ist, dass sie die Verarbeitung bei Auftreten einer Meldung stoppt, werden die dritte und vierte Richtlinie nicht verarbeitet, während ein Verstoß gegen die zweite Richtlinie aktiv ist.

16. Klicken Sie Auf **Speichern**.

    Die Seite Performance Policies wird angezeigt, und die Performance Policy wird in der Liste der Policies für den Objekttyp angezeigt.

## Konfiguration der Performance und Sicherstellung von Benachrichtigungen über Verstöße

OnCommand Insight unterstützt Benachrichtigungen bei Performance-Verstößen und stellt diese sicher. Standardmäßig sendet Insight keine Benachrichtigungen für diese Verstöße. Sie müssen Insight so konfigurieren, dass E-Mails gesendet, Syslog-Meldungen an den Syslog-Server gesendet oder SNMP-Benachrichtigungen gesendet werden, wenn eine Verletzung auftritt.

### Bevor Sie beginnen

Sie müssen E-Mail-, Syslog- und SNMP-Sendemethoden für Verstöße konfiguriert haben.

### Schritte

1. Klicken Sie Auf **Admin** > **Benachrichtigungen**.

2. Klicken Sie Auf **Events**.
3. Klicken Sie im Abschnitt **Performance Violations Events** oder **Assure Violations Events** auf die Liste für die gewünschte Benachrichtigungsmethode (**Email**, **Syslog** oder **SNMP**) und wählen Sie den Schweregrad (**Warnung und höher** oder **kritisch**) für die Verletzung aus.
4. Klicken Sie Auf **Speichern**.

## Überwachung der Verstöße in Ihrem Netzwerk

Wenn Insight aufgrund der in den Performance-Richtlinien festgelegten Schwellenwerte Verstöße generiert, können Sie diese über das Dashboard für Verstöße anzeigen. Das Dashboard listet alle Verstöße auf, die in Ihrem Netzwerk auftreten, und ermöglicht es Ihnen, Probleme zu lokalisieren und zu beheben.

### Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser.
2. Klicken Sie in der Insight-Symbolleiste auf **Dashboards** und wählen Sie **Dashboard für Verstöße**.

   Das Dashboard „Verstöße“ wird angezeigt.

3. Sie können das Kreisdiagramm **Verstöße nach Richtlinien** auf folgende Weise verwenden:
   - Sie können den Cursor über einen beliebigen Diagrammabschnitt bewegen, um den Prozentsatz der Gesamtverletzungen anzuzeigen, die für eine bestimmte Richtlinie oder Metrik aufgetreten sind.
   - Sie können auf eine Schicht eines Diagramms klicken, um es „`vergrößern`“ zu öffnen. Dadurch können Sie diese Schicht hervorheben und genauer untersuchen, indem Sie sie vom Rest des Diagramms entfernen.
   - Sie können auf klicken Symbol in der oberen rechten Ecke, um das Kreisdiagramm im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren. Ein Kreisdiagramm kann maximal fünf Schichten enthalten. Wenn Sie also sechs Richtlinien haben, die Verstöße erzeugen, kombiniert Insight die fünfte und sechste Schicht in einem „`others`“-Slice. Insight weist der ersten Schicht die meisten Verstöße zu, der zweiten die zweithäufigsten Verstöße usw.
4. Sie können das Diagramm **Historie der Verstöße** auf folgende Weise verwenden:
   - Sie können den Cursor über das Diagramm bewegen, um die Gesamtzahl der zu einem bestimmten Zeitpunkt aufgetretenen Verstöße und die Anzahl der aufgetretenen Verstöße für jede angegebene Metrik anzuzeigen.
   - Sie können auf eine Legende klicken, um die mit der Legende verknüpften Daten aus dem Diagramm zu entfernen.

     Klicken Sie auf die Legende, um die Daten erneut anzuzeigen.

   - Sie können auf klicken Symbol in der oberen rechten Ecke, um die Karte im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren.
5. Sie können die **Tabelle der Verstöße** auf folgende Weise verwenden:
   - Sie können auf klicken Symbol in der oberen rechten Ecke, um die Tabelle im Vollbildmodus anzuzeigen, und klicken Sie auf Erneut, um das Kreisdiagramm zu minimieren.

     Wenn Ihre Fenstergröße zu klein ist, werden in der Tabelle „Verstöße“ nur drei Spalten angezeigt, wenn Sie jedoch auf klicken , Zusätzliche Spalten (bis zu sieben) werden angezeigt.

- Sie können Verstöße für einen bestimmten Zeitraum anzeigen (**1h**, **3h**, **24h**, **3d**, **7d**, Und **30d**), wobei Insight eine maximale Anzahl von 1000 Verstößen für den ausgewählten Zeitraum anzeigt.
- Sie können das Feld **Filter** verwenden, um nur die gewünschten Verstöße anzuzeigen.
- Sie können die Sortierreihenfolge der Spalten in einer Tabelle entweder aufsteigend (Aufwärtspfeil) oder absteigend (Abwärtspfeil) ändern, indem Sie auf den Pfeil in der Spaltenüberschrift klicken. Um zur Standardsortierreihenfolge zurückzukehren, klicken Sie auf eine beliebige andere Spaltenüberschrift.

  Standardmäßig werden die Verstöße in absteigender Reihenfolge in der Tabelle angezeigt.
- Sie können in der Spalte „ID“ auf eine Verletzung klicken, um die Seite „Anlage“ für die Dauer der Verletzung anzuzeigen.
- Sie können in der Spalte Beschreibung auf die Ressourcenverknüpfungen (z. B. Speicherpool und Speichervolume) klicken, um die mit diesen Ressourcen verknüpften Asset-Seiten anzuzeigen.
- Sie können auf den Link Leistungsrichtlinie in der Spalte Richtlinie klicken, um das Dialogfeld Richtlinie bearbeiten anzuzeigen.

  Sie können die Schwellenwerte für eine Richtlinie anpassen, wenn Sie der Ansicht sind, dass sie zu wenige oder zu viele Verstöße verursacht.
- Sie können auf eine Seitenzahl klicken, um Daten nach Seite zu durchsuchen, wenn mehr Daten als auf eine einzelne Seite passen.
- Klicken Sie auf ✖ Um den Verstoß zu verwerfen.

# Fehlerbehebung für Fibre Channel BB Credit 0-Fehler

Fibre Channel verwendet Buffer-to-Buffer Credits (BB Credits) zur Steuerung des Übertragungsflusses. Der Gutschriftwert wird verringert, wenn ein Frame von einem Port gesendet wird und der Gutschriftwert aufgefüllt wird, wenn der Port eine Antwort erhält. Wenn die BB-Credits im Port nicht aufgefüllt werden, kann der Übertragungsfluss beeinträchtigt werden. Ports benötigen Speicher oder Puffer, um Frames vorübergehend zu speichern, bis sie nacheinander zusammengebaut und ausgeliefert werden. Die Anzahl der Puffer ist die Anzahl der Frames, die ein Port speichern kann und wird als Puffergutschrift bezeichnet.

Da die verfügbaren Credits für einen bestimmten Port bei null liegen, wird durch einen Fehler darauf hingewiesen, dass der Port keine Übertragungen mehr empfängt, wenn Null erreicht wird. Er wird erst wieder aufgenommen, wenn die BB-Credits wieder aufgefüllt werden.

Insight Performance-Richtlinien ermöglichen die Festlegung von Schwellenwerten für die folgenden Port-Kennzahlen.

| |
|---|
| BB Credit Null - Rx |
| Die Anzahl der empfansenden Buffer-to-Buffer-Credits, die während des Abtastzeitraums auf Null umgestiegen ist |
| BB Credit Null - Tx |

| | |
|---|---|
| Die Anzahl der Übermittler-Puffer-Credits, die während des Abtastzeitraums auf Null umgestiegen sind | |
| BB Credit Null - Gesamt | |
| Die Anzahl der Male, die dieser Port die Übertragung stoppen musste, weil der angeschlossene Port nicht mehr über Credits verfügte | |
| BB-Gutschrift Null-Dauer - Tx | |
| Zeit in Millisekunden, während der die Tx BB-Gutschrift während des Abtastintervalls Null war | |

BB-Gutschriftfehler können durch einige der folgenden Szenarien verursacht werden:

- Wenn eine bestimmte Implementierung einen hohen Prozentsatz an FC-Frames mit Größen hat, die deutlich kleiner als die maximale Größe sind, sind möglicherweise mehr BB_Credits erforderlich.
- Workload-Änderungen an der Umgebung, die sich auf Ports oder Geräte auswirken könnten, die mit ihnen verbunden sind, z. B. Storage-Nodes.

Sie können die Fabric-, Switch- und Port-Asset-Seiten zur Überwachung Ihrer Fibre-Channel-Umgebung verwenden. Port-Asset-Seiten enthalten zusammenfassende Informationen über die Ressource, ihre Topologie (das Gerät und seine Verbindungen), Leistungsdiagramme und Tabellen der zugehörigen Ressourcen. Bei der Fehlerbehebung von Fibre-Channel-Problemen ist das Performance-Diagramm für die einzelnen Port-Assets hilfreich, da es den Datenverkehr für den ausgewählten Port mit den wichtigsten Beiträgen anzeigt. Auf den Port-Asset-Seiten werden in diesem Diagramm auch Kennzahlen für die zwischenpufferten Gutschriften und Portfehler angezeigt. Insight zeigt für jede Metrik ein separates Performance-Diagramm an.

## Erstellen von Performance-Richtlinien und Schwellenwerten für Ports

Sie können Performance-Richtlinien mit Schwellenwerten für Metriken erstellen, die einem Port zugeordnet sind. Standardmäßig gelten Performance-Richtlinien für alle Geräte des angegebenen Typs, wenn Sie sie erstellen. Sie können eine Annotation erstellen, um nur ein bestimmtes Gerät oder eine Gruppe von Geräten in die Performance-Richtlinie aufzunehmen. Aus einfachen Grund wird bei diesem Verfahren keine Beschriftung verwendet.

### Bevor Sie beginnen

Wenn Sie eine Annotation mit dieser Performance-Richtlinie verwenden möchten, müssen Sie die Annotation erstellen, bevor Sie die Performance-Richtlinie erstellen.

### Schritte

1. Klicken Sie in der Insight-Symbolleiste auf **Verwalten** > **Leistungsrichtlinien**

   Die vorhandenen Richtlinien werden angezeigt. Wenn eine Richtlinie für Switch-Ports vorhanden ist, können Sie die vorhandene Richtlinie bearbeiten und die neuen Richtlinien und Schwellenwerte hinzufügen.

2. Bearbeiten Sie eine vorhandene Portrichtlinie oder erstellen Sie eine neue Portrichtlinie

- Klicken Sie auf das Bleistiftsymbol ganz rechts neben der vorhandenen Richtlinie. Fügen Sie die in den Schritten „d“ und „e“ beschriebenen Schwellenwerte hinzu.
- Klicken Sie auf **+Hinzufügen**, um eine neue Richtlinie hinzuzufügen
  i. Fügen Sie ein „Richtlinienname“ hinzu: Gerät mit langsamer Entleerung
  ii. Port als Objekttyp auswählen
  iii. Geben Sie das erste Vorkommen für „Apply after window“ von ein
  iv. Schwellenwert eingeben: BB Credit Null - Rx > 1,000,000
  v. Schwellenwert eingeben: BB Credit Null - Tx > 1,000,000
  vi. Klicken Sie auf „Verarbeitung weiterer Richtlinien beenden, wenn eine Warnung generiert wird“.
  vii. Klicken Sie Auf „Speichern“.

Die von Ihnen erstellte Richtlinie überwacht die Schwellenwerte, die Sie über einen Zeitraum von 24 Stunden festgelegt haben. Wenn der Schwellenwert überschritten wird, wird eine Verletzung gemeldet.

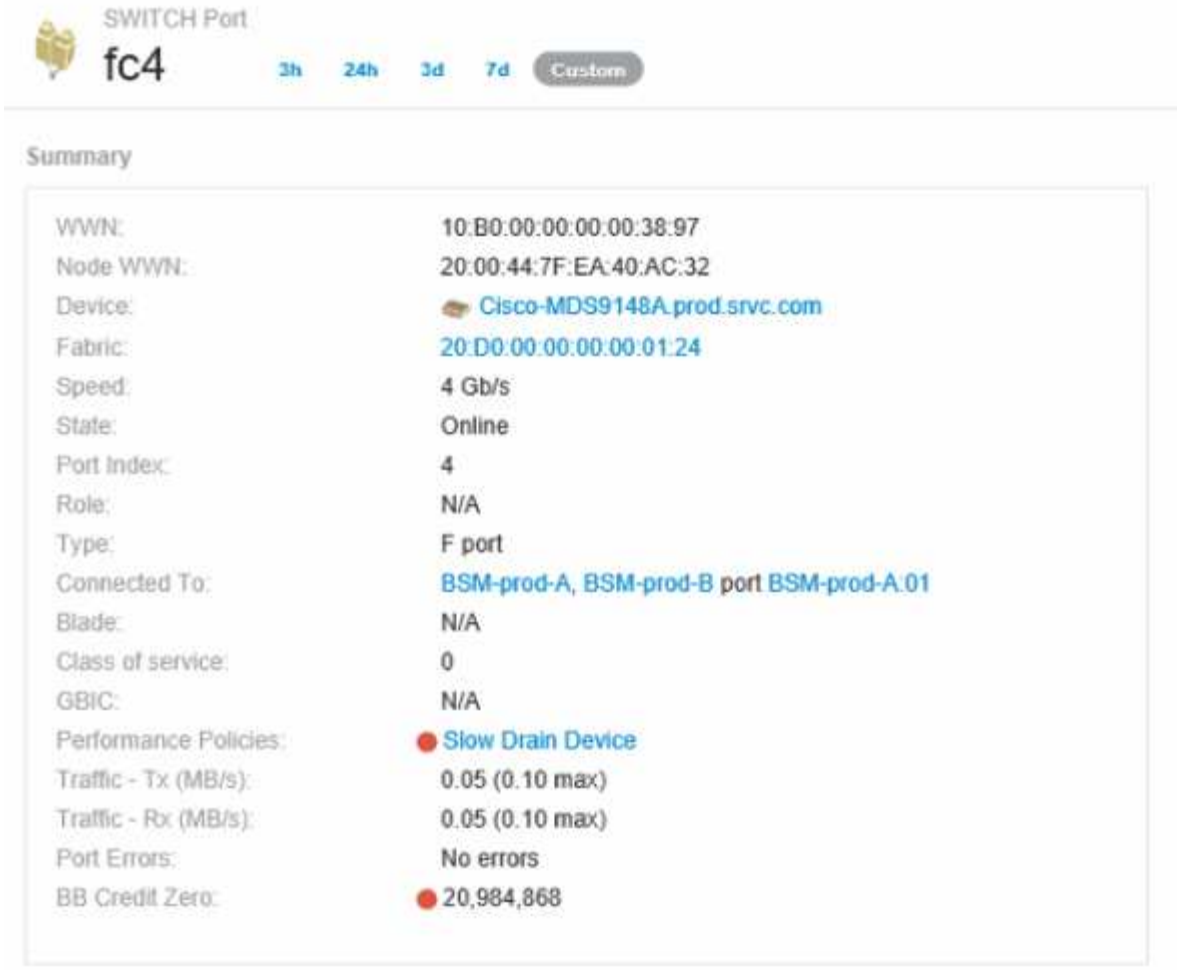
3. Klicken Sie Auf **Dashboards** > **Verstöße Dashboard**

   Das System zeigt alle auf dem System aufgetretenen Verstöße an. Suchen oder sortieren Sie die Verstöße, um die „Slow Drain Device“-Verstöße anzuzeigen. Das Dashboard „Verstöße“ zeigt alle Ports an, bei denen BB Credit 0-Fehler aufgetreten sind, die die Schwellenwerte überschreiten, die in der Performance Policy festgelegt wurden. Jeder Switch-Port, der im Dashboard für Verstöße identifiziert wurde, ist ein hervorgehobener Link zur Landing Page des Ports.

4. Klicken Sie auf einen hervorgehobenen Port-Link, um die Port-Landing-Page anzuzeigen.

   Die Zielseite des Ports wird angezeigt und enthält nützliche Informationen für die Fehlerbehebung bei BB Credit 0:

   - Geräte, mit denen der Port verbunden ist
   - Identifizierung des Ports, der den Verstoß meldet, d. h. eines Fibre-Channel-Switch-Ports.
   - Die Geschwindigkeit des Ports
   - Der zugeordnete Knoten und
     Portname




5. Blättern Sie nach unten, um die Kennzahlen für den Port anzuzeigen. Klicken Sie auf **Metriken auswählen, die angezeigt werden sollen** > **BB Credit Null**, um das BB Credit-Diagramm anzuzeigen.

6. Klicken Sie auf **Top Correlated**

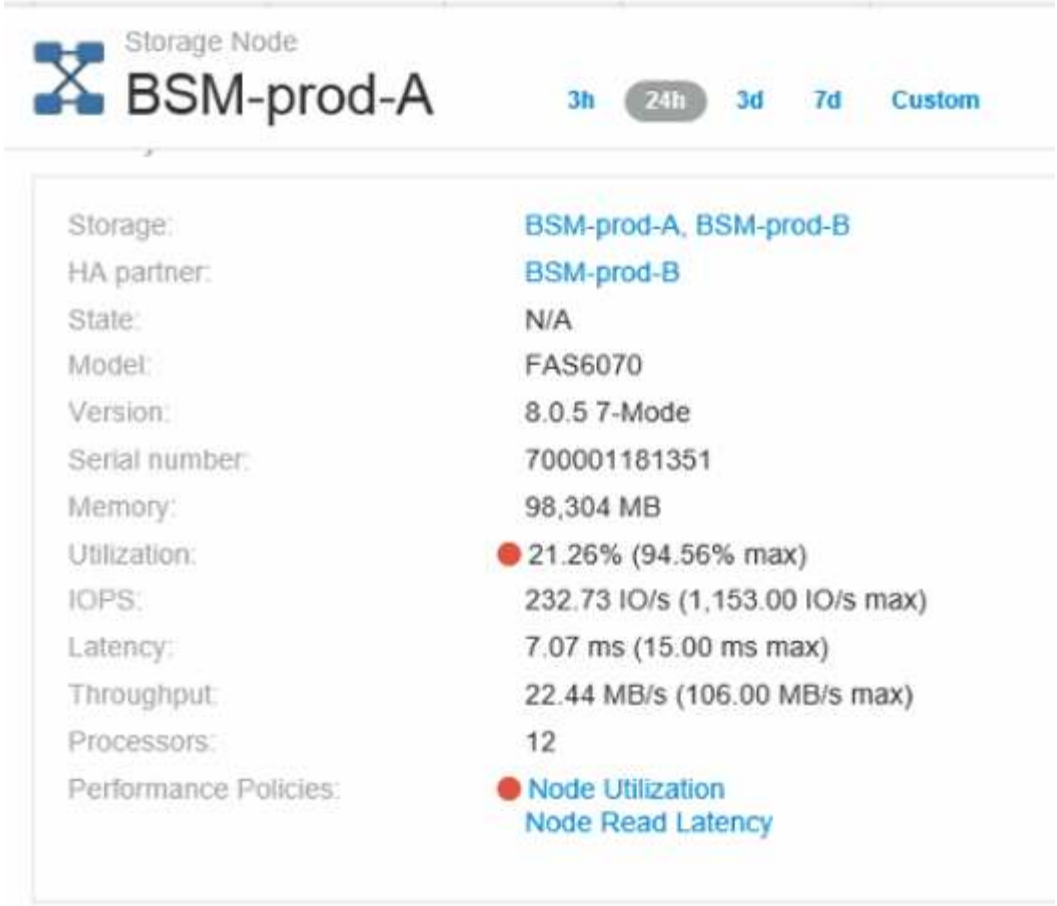
   Die Top-korrelierte Ressourcenanalyse zeigt den verbundenen Controller-Node, den der Port als die Ressource bereitstellt, die am stärksten mit der Performance korreliert. Dieser Schritt vergleicht die IOPS-Kennzahlen der Portaktivität mit der gesamten Node-Aktivität. Auf den Anzeigen werden die Kennzahlen Tx und Rx BB Credit Zero sowie die IOPS des Controller-Node angezeigt. Das Display zeigt Folgendes an:

   - Die Controller-I/O-Vorgänge sind stark mit dem Port-Verkehr korreliert

- Die Performance Policy wird verletzt, wenn der Port E/A an den Server sendet.
- In Anbetracht der Tatsache, dass unser Port Performance-Verstoß in Verbindung mit einer hohen IOPS-Belastung des Storage Controllers auftritt, ist es wahrscheinlich, dass der Verstoß durch den Workload auf dem Storage Node verursacht
wird.

7. Kehren Sie zur Landing Page des Ports zurück und greifen Sie auf die Landing Page des Storage-Controller-Node zu, um die Workload-Metriken zu analysieren.

   Der Node zeigt eine Verletzung der Auslastung an und die Kennzahlen zeigen einen hohen Wert für „ersetzte Cache-Lesevorgänge“, der im Zusammenhang mit dem „Buffer-to-Buffer-Zero“-Kreditstatus steht.




8. Auf der Landing Page Node können Sie die BB-Kreditzverenzeros vergleichen, indem Sie den Port aus der Liste der korrelierten Ressourcen auswählen und im Menü Metrics Auslastungsdaten, einschließlich Cache-Nutzungsdaten, für unseren Node auswählen.

Diese Daten machen deutlich, dass das Cache-Trefferverhältnis umgekehrt mit unseren anderen Kennzahlen korreliert wird. Anstatt auf die Serverlast aus dem Cache zu reagieren, tritt auf dem Storage-Node eine hohe Anzahl von Lesevorgängen im Cache auf. Es ist wahrscheinlich, dass das Abrufen der meisten Daten von der Festplatte statt vom Cache die Verzögerung bei der Übertragung der Daten des Ports an den Server verursacht. Die Ursache des Performance-Problems scheint wahrscheinlich eine durch Workloads generierte Änderung des I/O-Verhaltens zu sein, und dass der Node-Cache und seine Konfiguration die Ursache dafür sind. Das Problem kann gelöst werden, indem entweder die Cache-Größe des Node vergrößert oder das Verhalten des Caching-Algorithmus geändert wird.

# Analyse der Infrastruktur

Die in diesem Thema beschriebenen Verfahren dienen möglicherweise zur Analyse von Teilen der Infrastruktur in Ihrer Umgebung. Die Schritte, Ansichten und Daten, die Sie in dieser Übung sammeln, verwenden virtuelle Computing-Objekte als Beispiel. Die Analyse anderer Ressourcen in Ihrer Umgebung führt ähnliche Schritte anhand relevanter Zähler für jede spezifische Ressource aus. Ziel dieser Übung ist es, Sie mit den verschiedenen Optionen vertraut zu machen, die Insight bietet zum Monitoring und Verständnis der Eigenschaften der Assets in Ihrem Datacenter.

## Über diese Aufgabe

So können Sie den Zustand Ihrer Infrastruktur analysieren:

- Beobachten Sie das Verhalten eines Objekts im Zeitverlauf
- Vergleichen Sie die Metriken eines Objekts mit den Metriken der Top 10 ähnlichen Objekte
- Zahlen für Objekte vergleichen
- Vergleichen Sie die 10 besten Objekte mit dem Durchschnitt
- Vergleichen Sie Metriken A und B für viele Objekte, um Kategorien und Anomalien anzuzeigen
- Vergleichen Sie einen Bereich von Objekten mit anderen Objekten
- Verwenden Sie einen Ausdruck, um Metriken anzuzeigen, die in der Web-Benutzeroberfläche nicht verfügbar sind

Sie können alle diese Ansichten von Objekten in Ihrer Infrastruktur in einem Dashboard erstellen, indem Sie Widgets für jede durchgeführte Analyse verwenden. Die Dashboards können gespeichert werden, um einen schnellen Zugriff auf aktuelle Daten in der Infrastruktur zu ermöglichen.

## Beobachten Sie das Verhalten eines Objekts im Laufe der Zeit

Sie können das Verhalten eines einzelnen Objekts beobachten, um festzustellen, ob das Objekt innerhalb der erwarteten Betriebsebenen arbeitet.

### Schritte

1. Verwenden Sie eine Abfrage, um die zu analysende VM zu identifizieren: **Query** > **+ Neue Abfrage** > **Virtuelle Maschine** > **"Name"**

   Wenn Sie das Namensfeld leer lassen, werden alle VMs zurückgegeben. Wählen Sie die VM aus, die Sie in dieser Übung verwenden möchten. Sie können ihn auswählen, indem Sie durch die Liste der VMs

blättern.

2. Erstellen Sie ein neues Dashboard für die Informationen, die Sie erfassen möchten. Klicken Sie in der Symbolleiste auf **Dashboards** > **+Neues Dashboard**.
3. Wählen Sie im neuen Dashboard **Variable** > **Text** aus.

   a. Fügen Sie den VM-Namen aus Ihrer Abfrage als hinzu`$var1` Wert:

   b. Aktivieren Sie das Kontrollkästchen.

   Die Variable wird verwendet, um einfach zwischen verschiedenen Gruppen von Objekten zu wechseln, die Sie analysieren möchten. In anderen Schritten Ihrer Analyse können Sie diese Variable für zusätzliche Analysen mit der ursprünglich ausgewählten einzelnen VM verwenden. Variablen werden nützlicher, wenn sie mehrere Objekte identifizieren.

4. Fügen Sie dem neuen Dashboard ein Liniendiagramm-Widget hinzu: **Widget** > **Liniendiagramm**.

   a. Ändern Sie den Standard-Asset-Typ auf virtuelle Maschine: Klicken Sie auf **virtuelle Maschine** > **Latenz-Gesamt**.

   b. Klicken Sie auf **Filtern nach** > **Name** > **€21.1**.

   c. Ändern Sie den Zeitraum auf dem Armaturenbrett: **Dashboard-Zeit überschreiben** > **ein** > **7 Tage**.

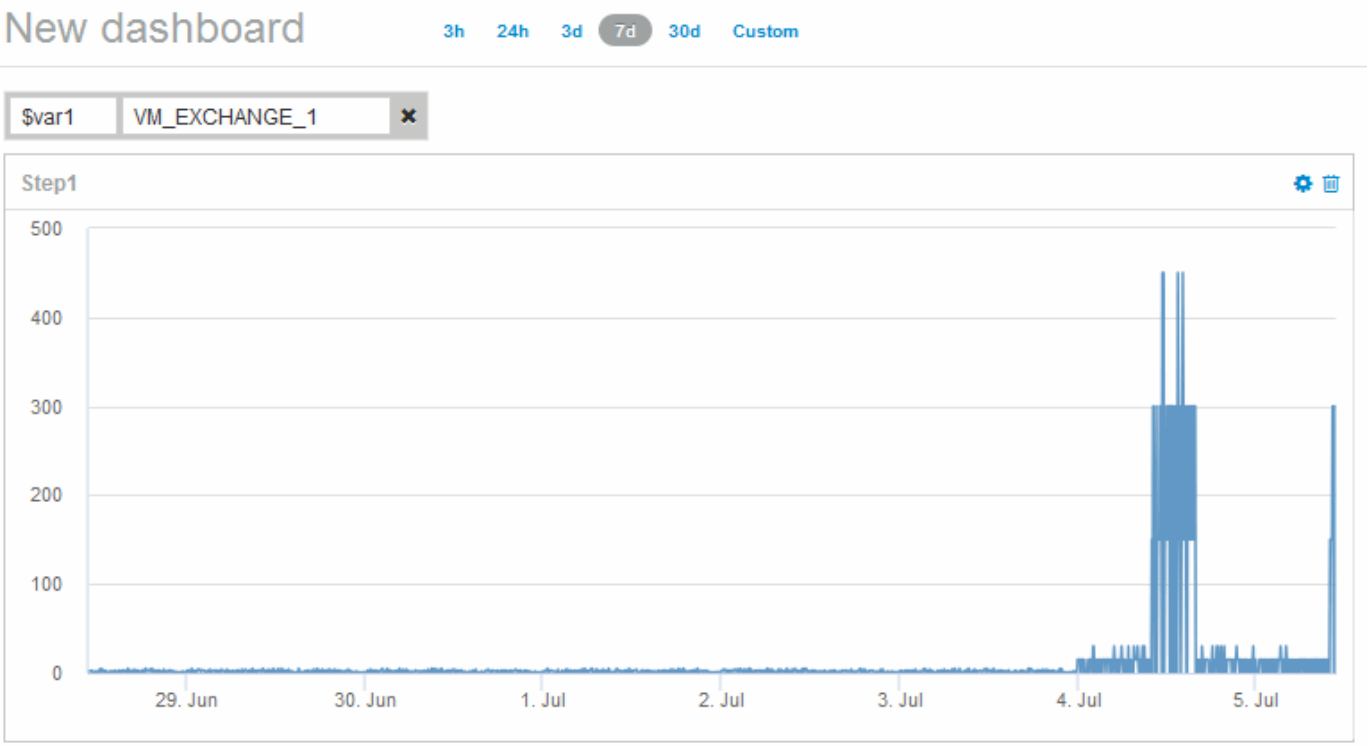
      Sie können die Dauer der Anzeige mit einer beliebigen voreingestellten Auswahl oder durch Angabe eines benutzerdefinierten Zeitbereichs ändern.

   + das Dashboard zeigt den **IOPS-Total** der VM für den von Ihnen angegebenen Zeitraum an.

5. Weisen Sie dem Widget einen Namen zu und speichern Sie das Widget.

### Ergebnisse

Ihr Widget sollte Daten wie die folgenden enthalten:



Die VM zeigt eine Periode ungewöhnlich hoher Latenz für einen kurzen Zeitraum in den angezeigten 7 Tagen an.

## Vergleichen Sie Objekte mit der Gesamtlatenz von 10 und der durchschnittlichen Latenz für alle ähnlichen Objekte

Vielleicht möchten Sie einmal die VMs mit der Gesamtlatenz von 10 und der durchschnittlichen Latenz vergleichen, um alle zu identifizieren, die außerhalb des durchschnittlichen Bereichs liegen. Diese Informationen könnten bei Entscheidungen zum Lastausgleich von Workloads auf VMs helfen.

### Schritte

1. Fügen Sie dem neuen Dashboard ein Widget mit einem gestapelten Flächendiagramm hinzu: **Widget** > **gestapeltes Flächendiagramm**

   a. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **Latency total**

      Das Widget zeigt die Latenzsumme für alle VMs für 24 Stunden in einem gestapelten Flächendiagramm an.

   b. Erstellen Sie eine zweite Anzeige in diesem Widget, die Latenz insgesamt gemittelt für alle VMs zeigt: **Widget** > **Liniendiagramm**

   c. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Virtual Machine** > **Latency-total**

      Das Widget zeigt die Latenzsumme für den standardmäßigen 24-Stunden-Zeitraum unter Verwendung eines Liniendiagramms an.

   d. Klicken Sie auf **X** in der **Roll Up**-Leiste und wählen Sie **Show** > **Top** > **10**

   Das System zeigt die 10 wichtigsten VMs basierend auf der Gesamtlatenz an.

2. Um die durchschnittliche Latenzgesamtmenge für alle VMs mit den Top 10 IOPS insgesamt zu vergleichen, verwenden Sie die folgenden Schritte:

   a. Klicken Sie Auf **+Hinzufügen**

   b. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **IOPS total**

   c. Klicken Sie auf **X** in der **Roll Up**-Leiste und wählen Sie **Show** > **Top** > **10**

      Das System zeigt die 10 Objekte mit hoher Latenz und die durchschnittliche Latenz in einem Liniendiagramm an.

      + Bild::../media/Analytics-top10-avg.gif[]

   + die durchschnittliche Latenz beträgt 1.6 ms, während in den Top Ten, die VMs mit einer Latenz von über 200 ms.

## Vergleichen Sie die Latenzgesamtmenge eines Objekts mit der Latenzgesamtmenge der Top-10-Objekte

Mit den folgenden Schritten vergleichen Sie die Latenzgesamtmenge einer einzelnen VM mit den VMs, die den Gesamtbetrag der 10 höchsten Latenz der gesamten virtuellen Infrastruktur melden.

### Schritte

1. Fügen Sie dem neuen Dashboard ein Widget mit einem Liniendiagramm hinzu: **Widget** > **Liniendiagramm**

   a. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **Latency-total**

      Das Widget zeigt die Gesamtlatenz für alle VMs für die standardmäßigen 24 Stunden in einem Flächendiagramm an.

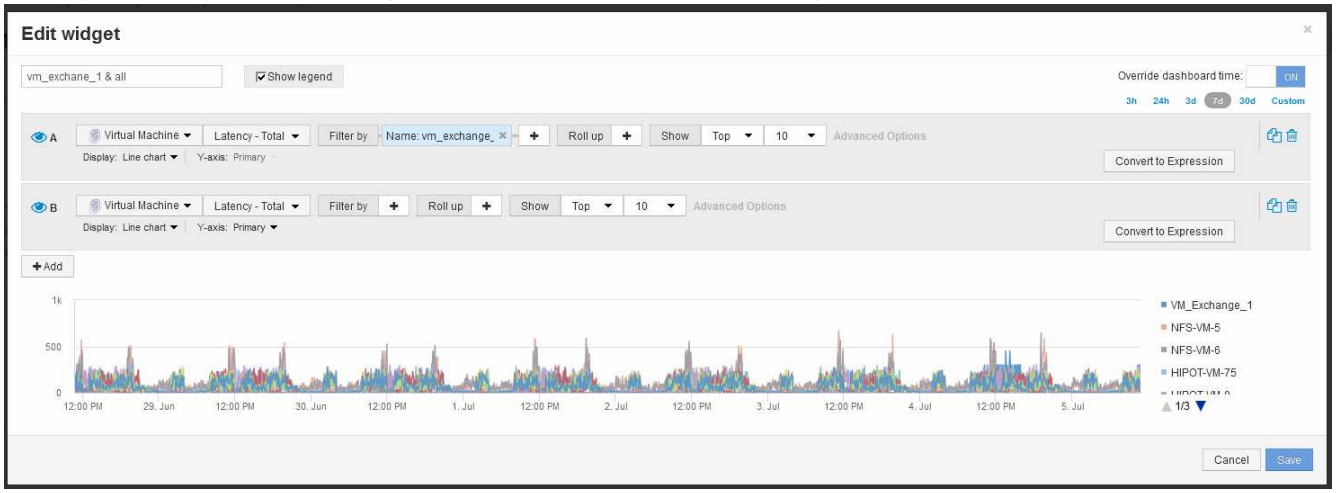
   b. Erstellen Sie eine zweite Anzeige in diesem Widget, die Latenz insgesamt gemittelt für alle VMs zeigt: **Widget** > **Liniendiagramm**

   c. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **Latency-Total**

      Das Widget zeigt die Latenzsumme für den standardmäßigen 24-Stunden-Zeitraum unter Verwendung eines Liniendiagramms an.

   d. Klicken Sie auf **X** in der **Roll Up**-Leiste und wählen Sie **Show** > **Top** > **10**

   Das System zeigt die 10 wichtigsten VMs auf Basis der Latenz – gesamt an.




2. Fügen Sie die VM hinzu, die Sie mit den Top 10 vergleichen möchten:

   a. Klicken Sie Auf **+Hinzufügen**

   b. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **Latency total**

   c. Klicken Sie auf **Filtern nach** > **Name** > **€21.1**

3. Klicken Sie auf **Legende anzeigen**

### Ergebnisse

Eine Legende gibt die einzelnen VMs an, die analysiert werden. Sie können VM_Exchange_1 leicht identifizieren und feststellen, ob eine Latenz ähnlich den zehn wichtigsten VMs der Umgebung auftritt.

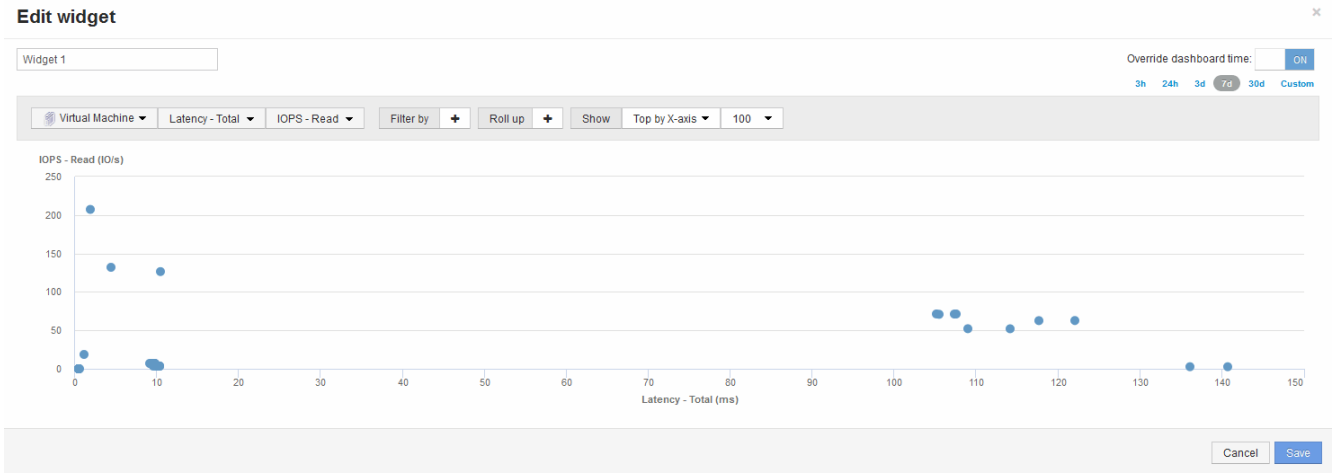
## Vergleichen Sie Metriken-A mit Metriken-B, um Kategorien und Anomalien anzuzeigen

Sie können ein Streudiagramm verwenden, um zwei Datensätze für jedes Objekt anzuzeigen. Beispielsweise können Sie festlegen, dass für jedes Objekt die Summe aus IOPS-Lese- und -Latenz angezeigt wird. Mithilfe dieses Diagramms können Sie anhand der IOPS und der Latenz zusammen das Objekt identifizieren, das Sie als lästig erachten.

### Schritte

1. Fügen Sie dem neuen Dashboard ein Widget mit einem Streudiagramm hinzu: **Widget** > **Streudiagramm**
2. Ändern Sie das Standardgerät in Virtual Machine: Klicken Sie auf **Storage** > **Virtual Machine** > **Latency total** > **IOPS Read**

   Das System zeigt einen Streudiagramm ähnlich der folgenden an:




## Verwenden Sie einen Ausdruck, um alternative Metriken zu identifizieren

Sie können Ausdrücke verwenden, um Metriken anzuzeigen, die nicht von der Web-Benutzeroberfläche bereitgestellt werden, wie z. B. die IOPS, die vom System-Overhead generiert werden.

### Über diese Aufgabe

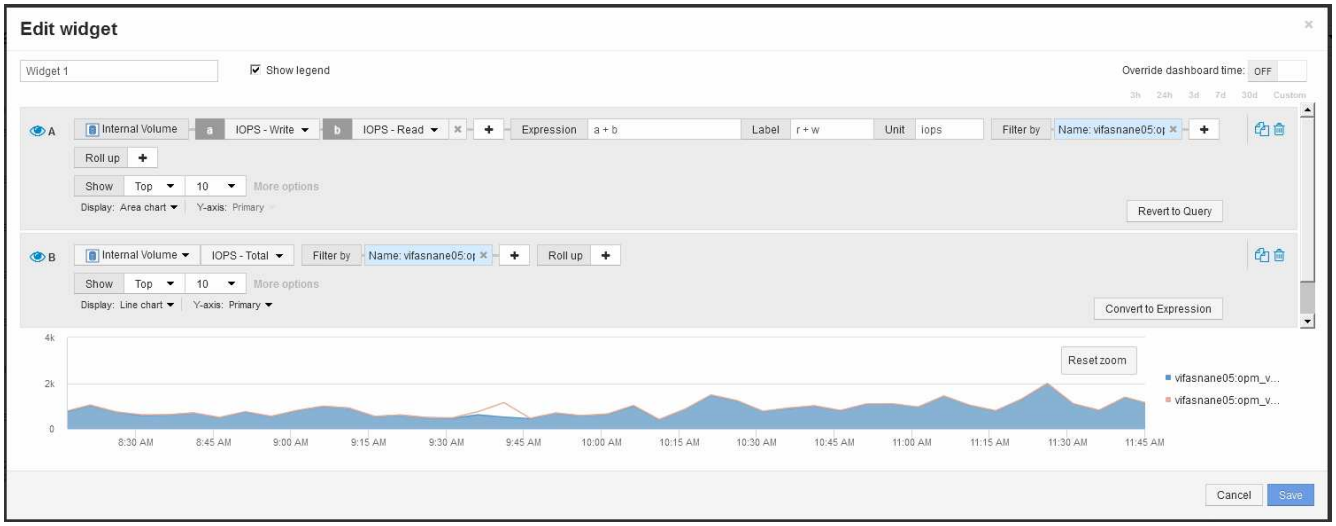
Möglicherweise möchten Sie einen Ausdruck verwenden, um die gesamten IOPS anzuzeigen, die durch nicht-Lese- oder nicht-Schreibvorgänge generiert werden, z. B. Overhead-Vorgänge für ein internes Volume.

### Schritte

1. Fügen Sie ein Widget zum Dashboard hinzu. Wählen Sie **Flächendiagramm**.
2. Ändern Sie das Standardgerät in Internes Volume: Klicken Sie auf **Speicher** > **Internes Volume** > **IOPS**

**Schreiben**

3. Klicken Sie auf die Schaltfläche **in Ausdruck konvertieren**.
4. Die Metrik **IOPS - Schreiben** befindet sich jetzt im Feld „**a**“ mit der alphabetischen Variable.
5. Klicken Sie im Variablenfeld “**b**” auf **Auswählen** und wählen Sie **IOPS - Lesen**.
6. Geben Sie im Feld **Ausdruck a + b** ein. Wählen Sie im Abschnitt **Anzeige** für den Ausdruck**Flächendiagramm**.
7. Geben Sie im Feld **Filter by** den Namen des internen Volumes ein, das Sie analysieren.
8. Das Feld **Beschriftung** kennzeichnet den Ausdruck. Ändern Sie die Bezeichnung in eine aussagekräftige Bezeichnung wie „`R + W IOPS`“.
9. Klicken Sie auf **+Add**, um dem Widget eine Zeile für die gesamten IOPS hinzuzufügen.
10. Ändern Sie das Standardgerät in Internes Volume: Klicken Sie auf **Speicher** > **Internes Volume** > **IOPS Total**
11. Geben Sie im Feld **Filter by** den Namen des internen Volumes ein, das Sie analysieren.




Im Diagramm wird die IOPS insgesamt als Linie angezeigt. Im Diagramm wird die Kombination aus Lese- und Schreib-IOPS in Blau angezeigt. Die Lücke zwischen 9:30 und 9:45 zeigt I/O-Operationen (Overhead) ohne Lese- und Schreibzugriff.

# Einführung zur Risikominimierung beim Thin Provisioning

In modernen hybriden IT-Datacentern müssen Administratoren mithilfe von Kapazitätstechnologien wie Thin Provisioning die Ressourcenauslastung überdehnen, um die Zuweisung zu steuern und die ehemals nicht verfügbaren Kapazitäten optimal zu nutzen.

OnCommand Insight sorgt für Kapazitätsnutzung und Auslastungsdetails nahezu in Echtzeit über mehrere Thin Provisioning-Ebenen des IT-Service-Stacks hinweg. Wenn das Risiko einer Überzeichnung nicht ordnungsgemäß gemanagt wird, kann dies zu Ausfallzeiten für das Unternehmen führen.

## Überwachen des Speicherpools

Jede Landing Page des Storage-Pools bietet Überzeichnungs-Verhältnisse, identifiziert

korrelierte Ressourcen, LUN- und Festplattenauslastung, Richtlinienverstöße und Verstöße gegen den Storage-Pool.

Verwenden Sie die Landing Page für Storage-Pools, um potenzielle Probleme mit den physischen Ressourcen zu identifizieren, die Ihre virtuelle Infrastruktur unterstützen. Sie können die Kapazitäts- und Kapazitätsverhältnisse von Trends über 30 Tage verfolgen oder einen individuellen Zeitrahmen verwenden. Achten Sie in den folgenden Abschnitten auf die Daten, um den Status des Speicherpools zu überwachen.

- **Zusammenfassung**

  In diesem Abschnitt erhalten Sie Informationen zu folgenden Themen:

  - Informationen zur Kapazität des Speicherpools, einschließlich der physischen Kapazität und der überbelegten Kapazität
  - Ob das Aggregat überzeichnet ist und nach wie viel.
  - Alle aufgetretenen Richtlinienverstöße.
- **Speicherressourcen und Festplatten-Abschnitte**

  Im Abschnitt Storage-Ressourcen wird die LUN-Auslastung angezeigt.

  Der Abschnitt „Festplatten“ zeigt die einzelnen Festplatten, aus denen der Speicherpool besteht.
- **Ressourcen**

  Verwenden Sie diesen Abschnitt, um die Korrelation von VMDKs zu LUNs zu verstehen und den Applikationspfad von Storage zur VM zu verstehen.
- **Abschnitt Verstöße**

  Im Abschnitt „Verstöße“ werden Verstöße gegen Performance-Richtlinien identifiziert, die für den Speicherpool festgelegt wurden.

## Überwachen der Datenspeicher

Die Datastore-Landing Page identifiziert Überzeichnungs-Verhältnisse, LUN- und Festplattenauslastung, korrelierte Ressourcen und zeigt Richtlinienverstöße und Verstöße gegen den Datastore an.

Auf dieser Landing Page lassen sich Probleme mit Ihrer virtuellen Infrastruktur erkennen. Verfolgen Sie die Trends bei den Kapazitäts- und Kapazitätsverhältnissen, um Änderungen in Ihrer Kapazität vorherzusehen.

- **Zusammenfassung**

  In diesem Abschnitt erhalten Sie Informationen zu folgenden Themen:

  - Datenspeicher-Kapazitätsinformationen einschließlich der physischen Kapazität und der zu viel belegten Kapazität
  - Der Prozentsatz der überbelegten Kapazität.
  - Kennzahlen für Latenz, IOPS und Durchsatz
- **VMDKs**

Im Abschnitt VMDKs werden die Kapazität und Performance der virtuellen Festplatte angezeigt.

- **Speicherressourcen**

  Dieser Abschnitt zeigt die genutzte Kapazität und die Performance-Kennzahlen für das interne Volume in Bezug auf den Datastore.

- **Ressourcen**

  Verwenden Sie diesen Abschnitt, um die Korrelation von VMDKs zu LUNs zu verstehen und den Applikationspfad von Storage zur VM nachzuvollziehen.

- **Abschnitt Verstöße**

  Im Abschnitt Verstöße werden Verstöße gegen Performance-Richtlinien identifiziert, die für den Datastore festgelegt wurden.

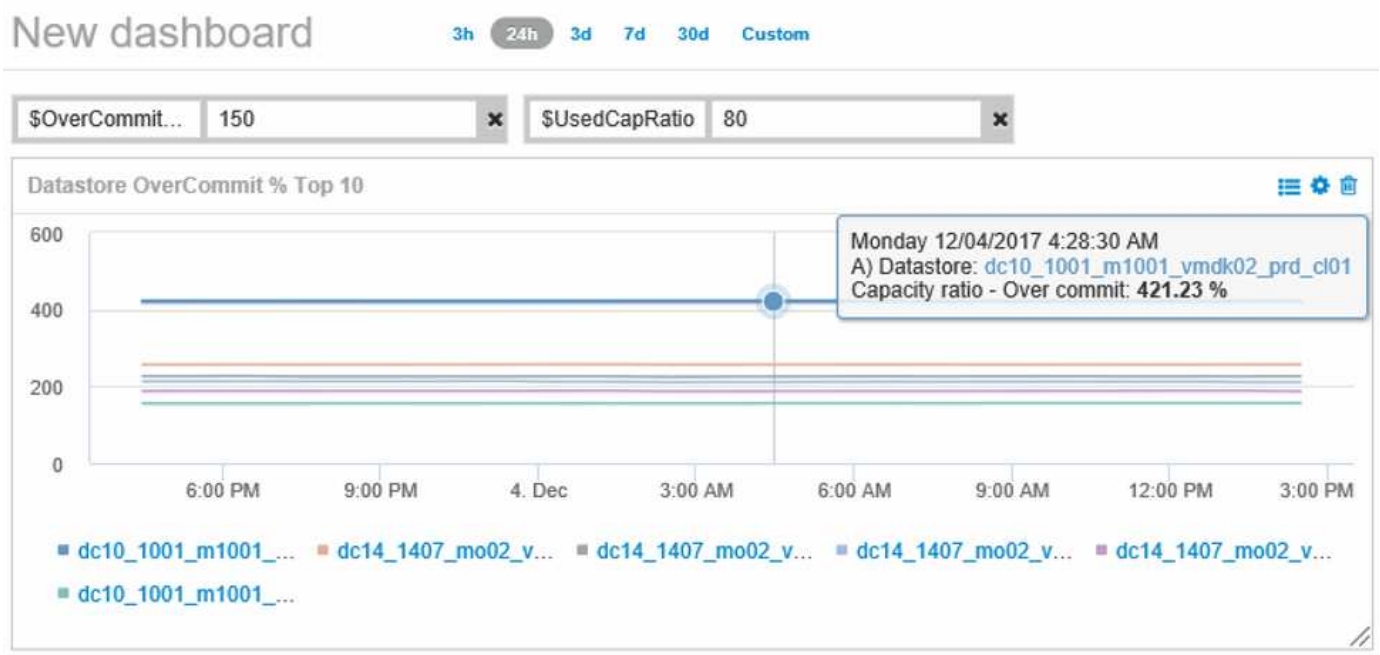
## Erstellen Sie Dashboards für das Monitoring von Thin Provisioning-Umgebungen

Die flexiblen Dashboard-Design- und Anzeigeoptionen von OnCommand Insight ermöglichen eine umfassende Analyse der Kapazitätsauslastung und -Auslastung sowie strategische Informationen zur Risikominimierung in Thin Provisioning Datacenter-Infrastrukturen.

Sie können Dashboards erstellen, die Zugriff auf Datenspeicher- und Storage-Pool-Informationen bieten, die Sie überwachen möchten.

### Verwenden von Dashboards für den Zugriff auf Datenspeicherinformationen

Möglicherweise möchten Sie Dashboards erstellen, die schnellen Zugriff auf die Daten bieten, die Sie in Ihrer virtuellen Infrastruktur überwachen möchten. Ein Dashboard könnte Widgets wie die folgenden enthalten, um die 10 wichtigsten Datastores anhand ihrer überlastenen % und ein Widget mit den Kapazitätsdaten für Datastores zu identifizieren. Die Dashboards verwenden Variablen, um Datastores hervorzuheben, die von mehr als 150 % überlastet sind, und Datastores, die mehr als 80 % ihrer genutzten Kapazität überschritten haben.




Overcommit Subscription %

| Name | Capacity - Total (GB) | Capacity - Used (GB) | Capacity - Provisioned (GB) | Capacity ratio - Over commit (%) | Capacity ratio - Used (%) |
|---|---|---|---|---|---|
| dc14_1407_...1_prd_cl03 | 5,008.00 | 4,091.04 | 12,876.38 | 257.12 | 81.69 |
| dc14_1407_...2_prd_cl03 | 6,936.69 | 5,872.31 | 14,633.80 | 210.96 | 84.66 |
| dc14_1407_...3_prd_cl03 | 9,437.03 | 7,951.36 | 17,639.86 | 186.92 | 84.26 |
| dc14_1407_...4_prd_cl03 | 7,911.09 | 6,627.00 | 17,891.24 | 226.15 | 83.77 |

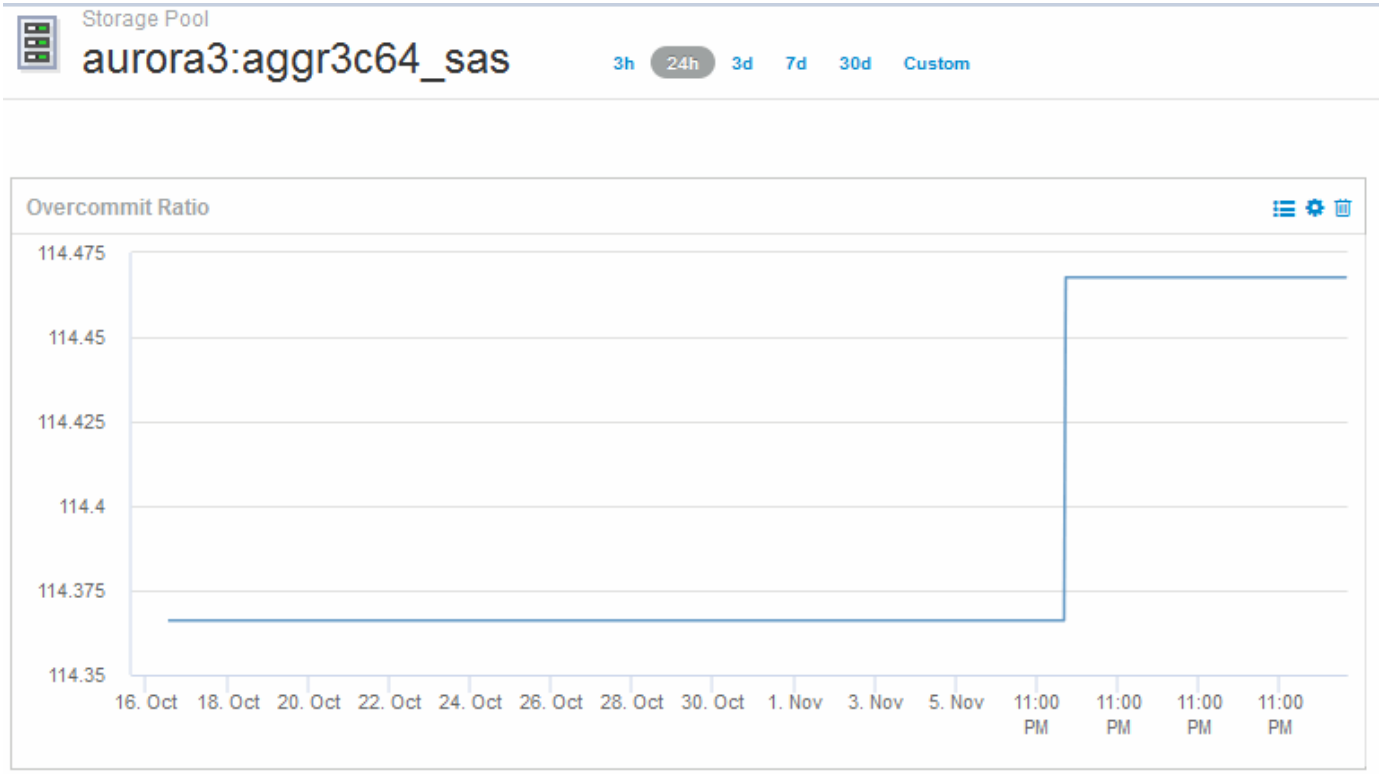
4 items found

Weitere Widgets, die zur Überwachung Ihrer Thin-Provisioning-Umgebung verwendet werden können, können einige der folgenden Informationen enthalten:

- VMDK-Kapazitäten in Beziehung zu Datenspeichern
- VM-Kapazitäten
- Trends bei der genutzten Datenspeicherkapazität

### Verwenden von Dashboards für den Zugriff auf Storage-Pool-Informationen

Ein Dashboard kann Widgets wie die folgenden enthalten, die die verwendete physische Speicherkapazität identifizieren oder die überbelegte Kapazität für einen Speicherpool identifizieren.




## Einsatz von Performance-Richtlinien zur Reduzierung des Risikos bei Thin Provisioning

Sie sollten Performance-Richtlinien erstellen, um Alarme auszugeben, wenn Schwellenwerte in Ihrer virtuellen Infrastruktur verletzt wurden. Mit diesen Warnmeldungen können Sie auf Änderungen in der Systemumgebung reagieren, bevor sie zu Unterbrechungen oder Betriebsausfällen führen.

Richtlinien zur Unterstützung des Monitorings der virtuellen Infrastruktur umfassen die folgenden:

- * Datastore*

  Sie könnten die folgenden Richtlinien auf dem Datenspeicher verwenden:

  - Kapazitätsverhältnis – Überprovisionierung
  - Kapazitätsverhältnis - verwendet
  - Kapazität – Verwendet
  - Kapazität – Gesamt
- **Speicherpool**

  Die folgenden Richtlinien schützen vor Kapazitätsausfällen in Thin Provisioning Umgebungen im Zusammenhang mit Storage:

  - Bereitgestellte Kapazität
  - Genutzte Kapazität
  - Kapazitätsverhältnis – Überprovisionierung

- Kapazitätsverhältnis - verwendet

Über diese Richtlinien lässt sich die Kapazität in der virtuellen Infrastruktur erweitern, einschließlich:

- Interne Volumes
- LUNs
- Festplatten
- VMDKs
- VMs

Richtlinien können mithilfe von Annotationen konfiguriert werden. Sie weisen die gleiche Anmerkung den spezifischen Ressourcen zu, die eine Anwendung unterstützen. Sie können beispielsweise den Datenspeichern und den Storage-Pools einer Applikation mit Thin Provisioning Anmerkungen zuweisen. Möglicherweise haben Sie Anmerkungen mit dem Namen „Produktion“ für die Produktionsumgebung, „Entwicklung“ für die Entwicklungsumgebung usw. Sie können die Schwellenwerte und die Kritikalität von Warnungen abhängig von der Art der Anwendung, die die Assets unterstützen, ändern. Beispielsweise könnte ein Verstoß gegen einen Schwellenwert für den Datastore einer Produktionsapplikation eine *kritische Warnung* erzeugen, während dieselbe Sicherheitsverletzung für eine Entwicklungsumgebung möglicherweise nur eine *Warnung* erhöht. Die Einbindung von Anmerkungen in definierte Richtlinien kann dazu beitragen, unerwünschte Warnmeldungen für nicht kritische Assets weiter zu reduzieren.

## Erstellen von Performance-Richtlinien für Speicherpools

Sie können Performance-Richtlinien erstellen, die Warnmeldungen auslösen, um Sie zu benachrichtigen, wenn die Schwellenwerte für Storage Pool Assets überschritten wurden.

### Bevor Sie beginnen

Bei diesem Verfahren wird davon ausgegangen, dass Sie den Speicherpool über Thin Provisioning bereitgestellt haben.

### Über diese Aufgabe

Sie möchten Richtlinien erstellen, um Änderungen in einem Speicherpool zu überwachen und zu melden, die zu Ausfällen führen könnten. Für den physischen Storage-Pool, der über Thin Provisioning bereitgestellt wird, soll die physische Kapazität überwacht und das Verhältnis der Überprovisionierung überwacht werden.

### Schritte

1. Öffnen Sie OnCommand Insight in Ihrem Browser.
2. Wählen Sie **Verwalten** > **Leistungsrichtlinien** Aus

   Die Seite Leistungsrichtlinien wird angezeigt. Richtlinien werden nach Objekten organisiert und in der Reihenfolge bewertet, in der sie in der Liste angezeigt werden. Wenn Benachrichtigungen aktiviert sind (**Admin** > **Benachrichtigungen**), können Sie Insight so konfigurieren, dass E-Mails gesendet werden, wenn Performance-Richtlinien verletzt werden.

3. Klicken Sie auf **+Add**, um eine neue Richtlinie zu erstellen.
4. Geben Sie unter **Richtlinienname** einen Richtliniennamen für den Speicherpool ein.
5. Wählen Sie unter **auf Objekte des Typs anwenden** den Eintrag Speicherpool aus.

6. Geben Sie in **Apply after window of** das erste Vorkommen ein.
7. Geben Sie in **with severity** kritisch ein
8. Konfigurieren Sie die E-Mail-Empfänger, die benachrichtigt werden sollen, wenn Schwellenwerte überschritten werden.

   Standardmäßig werden E-Mail-Benachrichtigungen bei Richtlinienverstößen an die Empfänger in der globalen E-Mail-Liste gesendet. Sie können diese Einstellungen überschreiben, sodass Benachrichtigungen für eine bestimmte Richtlinie an bestimmte Empfänger gesendet werden.

   Klicken Sie auf den Link, um die Empfängerliste zu öffnen, und klicken Sie dann auf die Schaltfläche +, um Empfänger hinzuzufügen. Verstöße gegen diese Richtlinie werden an alle Empfänger in der Liste gesendet.
9. Geben Sie in **Create alert if any of the following are true** das Kapazitätsverhältnis ein - used > 85%

#### Ergebnisse

Diese Konfiguration führt dazu, dass das System eine kritische Warnmeldung sendet, wenn mehr als 85 % der physischen Kapazität des Speicherpools verwendet wird. Die Verwendung von 100 % des physischen Speichers führt zu einem Anwendungsausfall.

#### Erstellen Sie zusätzliche Richtlinien für Speicherpools

##### Über diese Aufgabe

Erstellen Sie eine zusätzliche „`Capacity Ratio - used`“-Richtlinie, die eine Warnmeldung ausgibt, wenn die verwendete Storage-Pool-Kapazität 75 % überschreitet. Wenn Benachrichtigungen aktiviert sind (**Admin** > **Benachrichtigungen**), können Sie Insight so konfigurieren, dass E-Mails gesendet werden, wenn Performance-Richtlinien verletzt werden.

## Erstellen von Performance-Richtlinien für Datastores

Sie können Performance-Richtlinien mit Schwellenwerten für die Metriken der Datenspeicher erstellen, die zu den von Ihnen überwachten Storage-Pools korrelieren. Standardmäßig gelten Performance-Richtlinien für alle Geräte des angegebenen Typs, wenn Sie sie erstellen. Sie können eine Annotation erstellen, um nur ein bestimmtes Gerät oder eine Gruppe von Geräten in die Performance-Richtlinie aufzunehmen.

#### Bevor Sie beginnen

Wenn Sie eine Annotation in einer Performance-Richtlinie verwenden, muss die Annotation vorhanden sein, bevor die Richtlinie erstellt wird.

#### Über diese Aufgabe

Sie erstellen eine Performance-Richtlinie, die eine Benachrichtigung bereitstellt, wenn ein oder mehrere von Ihnen überwachten Datenspeicher einen festgelegten Schwellenwert überschreitet. Möglicherweise enthält Ihr System bereits eine globale Richtlinie, die Ihren Anforderungen entspricht. Eine Richtlinie mit Annotationen kann auch funktionieren, wenn Sie Ihre Datastores mit Anmerkungen versehen.

**Schritte**

1. Wählen Sie in der Insight-Symbolleiste **Verwalten** > **Performance Policies** aus

   Die Seite Performance-Richtlinien wird angezeigt. Prüfen Sie alle vorhandenen Performance-Richtlinien, um vorhandene Richtlinien zu ermitteln, die die Metriken für Schwellenwerte berücksichtigen, die Sie überwachen möchten.

2. Klicken Sie auf **+Hinzufügen**, um eine neue Richtlinie hinzuzufügen
3. „`Richtlinienname`“ hinzufügen

   Sie müssen einen Namen verwenden, der sich von allen anderen Richtliniennamen für das Objekt unterscheidet. Sie können beispielsweise nicht zwei Richtlinien mit dem Namen „Latenz“ für ein internes Volume festlegen. Sie können jedoch eine „Latenzrichtlinie“ für ein internes Volume und eine weitere „Latenzrichtlinie“ für einen Datenspeicher festlegen. Es empfiehlt sich, immer einen eindeutigen Namen für eine Richtlinie zu verwenden, unabhängig vom Objekttyp.

4. Wählen Sie als Objekttyp „Datastore“ aus
5. Klicken Sie Auf „`First Vorkommen`“.

   Die Option „Erstes Auftreten“ löst eine Warnung aus, wenn ein Schwellenwert bei der ersten Datenprobe überschritten wird. Alle anderen Optionen lösen eine Warnung aus, wenn der Schwellenwert einmal überschritten wird und mindestens die angegebene Zeit lang kontinuierlich überschritten wird.

6. Klicken Sie Auf „`Warnung`“.
7. Wählen Sie unter „`Warnung erstellen`“ **Kapazitätsverhältnis - Übercommit** aus und setzen Sie den Wert auf **> 150**

   Möglicherweise möchten Sie zusätzliche Warnmeldungen zur Kapazität erstellen, z. B. **Kapazität gesamt**und **genutzte Kapazität**.

# Erfassen von Host- und VM-Dateisystemauslastungs-Daten

## Die Datenquelle „Host and VM File Systems“ ermöglicht in Kombination mit der Host Utilization License die Berichterstellung und Kostenverrechnung für bekannte Hosts und VMs auf Filesystem-Ebene.

OnCommand Insight erfasst Daten von Storage-Geräten, von denen die meisten ihre Volumes als Block-Geräte melden. Dadurch kann Insight Berichte zur Auslastung auf Storage-Ebene erstellen, jedoch nicht auf Filesystem-Ebene. Storage Arrays wissen in der Regel, auf welche Blöcke geschrieben wurden, jedoch nicht, auf welche Blöcke freigegeben wurden.

Client-Hosts und VMs implementieren Dateisysteme (ntfs, ext*…) Auf diesen Blockgeräten. Die meisten Dateisysteme enthalten ein Inhaltsverzeichnis mit Verzeichnis- und Dateimetadaten. Wenn Dateien gelöscht werden, werden ihre Einträge einfach aus dem Inhaltsverzeichnis entfernt. Von diesen Dateien verbrauchte Blöcke sind jetzt für die Wiederverwendung durch das Dateisystem geeignet, aber das Speicher-Array weiß dies nicht. Damit Insight Berichte über die Dateisystemnutzung erstellen kann, müssen diese aus Sicht des Client-Hosts oder der VM gesammelt werden, um eine genaue Kostenzuordnung zu ermöglichen.

Insight ermöglicht die Erfassung von Daten zur Filesystem-Auslastung auf dieser Ebene über die Datenquelle **NetApp Host and VM File System** in Kombination mit der **Host Utilization** Lizenz. VM’s müssen mit dem entsprechenden **Compute Resource Group**-Namen versehen werden, und zugehörige Speicher-Arrays

müssen mit entsprechenden **Tier**-Anmerkungen mit den richtigen Kosten versehen werden, um eine genaue Kostenberichterstellung zu ermöglichen.

Die Host Utilization License ist ressourcenbasiert und nicht kapazitätsbasiert wie andere Insight-Lizenzen.

## Konfigurieren Sie Insight für die Dateisystemsammlung

Um Insight für die Erfassung von Dateisystemauslastungsdaten zu konfigurieren, müssen Sie die Host Utilization Pack Lizenz installieren und die Datenquelle von NetApp Host und VM File Systems konfigurieren.

### Bevor Sie beginnen

Installieren Sie die Host Utilization Pack-Lizenz, wenn Sie dies noch nicht getan haben. Sie können die Lizenz auf der Seite **Admin** > **Setup** auf der Registerkarte **Lizenzen** überprüfen.

Die Datenquelle „Host and VM File Systems“ meldet nur die Auslastung des Dateisystems und die Metadaten des Dateisystems für bekannte * Compute Resources* (Hosts und VMs), die derzeit in Insight erfasst oder erkannt werden:

- Virtual Machines werden von Hypervisor-Datenquellen wie Hyper-V und VMware erfasst.
- Hosts werden über Geräteauflösung erkannt.

Die richtigen Tier-Annotationen müssen über die entsprechenden Storage-Ressourcen vorhanden sein.

Die folgenden verbundenen Blockspeichergeräte werden unterstützt:

- NetApp Clustered Data ONTAP (cDOT)
- NetApp 7-Mode
- Clariion
- Windows: VMware Virtual Disks (VMDKs) für FC, iSCSI
- Linux: VMware VMDKs (iSCSI und FC nicht unterstützt)

Eine **Compute Resource Group** ist eine Annotation, die das Gruppieren von Hosts und/oder virtuellen Maschinen ermöglicht, die gemeinsame administrative Anmeldedaten verwenden.

### Schritte

1. Notieren Sie zunächst die Hosts und/oder virtuellen Maschinen, die in Ihre **Compute Resource Group** aufgenommen werden sollen. Gehen Sie zu **Abfragen** > **+Neue Abfrage** und suchen Sie nach *Virtual Machine* Assets.

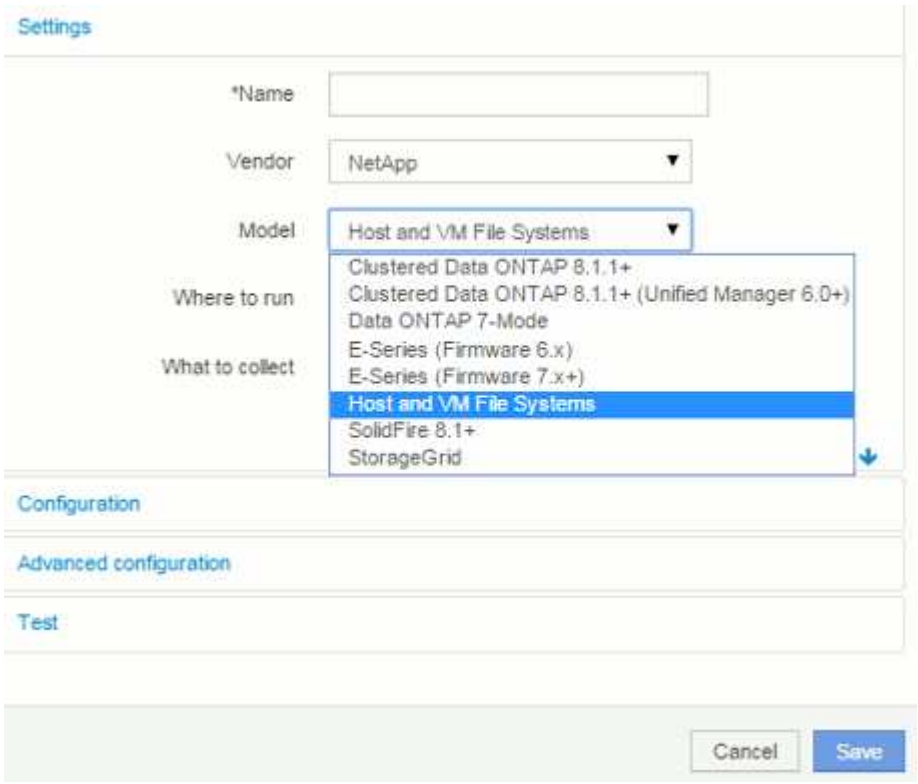
   Sie müssen diese Schritte für *Host*-Assets wiederholen.

2. Klicken Sie auf die Spaltenauswahl rechts neben der Tabelle und wählen Sie die Spalte **Compute Resource Group** aus, um sie in der Abfrageergebnistabelle anzuzeigen.
3. Wählen Sie die virtuellen Maschinen aus, die Sie der gewünschten Compute-Ressourcengruppe hinzufügen möchten. Sie können einen Filter verwenden, um nach bestimmten Assets zu suchen.
4. Klicken Sie auf die Schaltfläche **actions** und wählen Sie **Anmerkung bearbeiten**.

5. Wählen Sie die Anmerkung *Compute Resource Group* aus, und wählen Sie dann den gewünschten Namen der Ressourcengruppe im Feld *Value* aus.

   Die Annotation der Ressourcengruppe wird den ausgewählten VMs hinzugefügt. Der Name der Ressourcengruppe muss mit dem Namen übereinstimmen, den Sie später in der Datenquelle „Host“ und „VM File Systems“ konfigurieren werden.

6. Um die Datenquelle von Host und VM File Systems für eine Compute Resource Group zu konfigurieren, klicken Sie auf **Admin** > **Data Sources** und **Add** die *NetApp Host und VM File Systems* Datenquelle.




7. Geben Sie im Abschnitt **Konfiguration** einen **Benutzernamen** und ein **Passwort** für einen Betriebssystembenutzer mit entsprechenden Rechten zum Abrufen von Dateisystemdaten ein. Für Windows-Betriebssystembenutzer muss dies das Domänenpräfix enthalten, wenn es in Ihrer Windows-Umgebung verwendet wird.

   Beachten Sie, dass eine Insight Acquisition Unit (AU), die unter Linux installiert ist, Berichte über Linux-Rechenressourcen erstellen kann, während eine AU unter Windows mit Linux- oder Windows-Rechenressourcen kommunizieren kann.

8. Geben Sie den Namen der **Compute Resource Group** für die Assets ein, aus denen Sie die Dateisystemnutzungsdaten erfassen möchten. Dieser Name muss mit dem Namen der Ressourcengruppe übereinstimmen, mit der Sie die oben genannten Assets mit Anmerkungen versehen haben.

   Wenn Sie das Feld Compute Resource Group leer lassen, sammelt die Datenquelle Daten für Hosts oder VMs, die keine Anmerkungen zu Compute Resource Group haben.

9. Geben Sie im Abschnitt **Advanced Configuration**das gewünschte Abfrageintervall für diese Datenquelle ein. Der Standardwert von 6 Stunden ist in der Regel ausreichend.

10. Es wird empfohlen, die Datenquellenverbindung vor dem Speichern **zu testen**. Ein erfolgreiches Verbindungsergebnis zeigt Ihnen auch an, wie viele Compute-Ressourcenziele in der Gruppe enthalten sind.

11. Klicken Sie Auf **Speichern**. Die Datenquelle „Host and VM File Systems“ beginnt bei der nächsten Abfrage mit dem Sammeln von Daten.
12. Sobald Dateisystemdaten erfasst wurden, können Sie sie auf der Asset-Seite des Hosts oder der VM im Widget „Dateisystem“ anzeigen:

13. Wiederholen Sie diese Schritte für jede Compute Resource Group, die Sie haben werden. Jede Compute-Ressourcengruppe muss einer eigenen Host- und VM-Dateisystemquelle zugeordnet sein.

    Beachten Sie, dass Dateisysteminformationen für Hosts und VMs erfasst werden, die bereits von herkömmlichen VMware oder Hyper-V Datenquellen in Ihrer Umgebung erfasst werden.

## Chargeback und Berichterstellung für Filesysteme

Die Kostenverrechnung für File-Systeme erfolgt immer aus der Storage-Perspektive. Speicher-Arrays, die mit virtuellen Maschinen verknüpft sind, die für eine bestimmte Compute-Ressourcengruppe mit Anmerkungen versehen sind, werden in Chargeback-Berichten für diese Ressourcengruppe aufgenommen.

### Bevor Sie beginnen

Alle virtuellen Maschinen, die Sie in die Kostenzuordnung für die Dateisystemauslastung einbeziehen möchten, müssen mit dem entsprechenden Namen der Compute-Ressourcengruppe versehen werden. Storage-Arrays, die diesen Virtual Machines zugeordnet sind, müssen mit den entsprechenden Tier-Annotationen versehen werden. ETL in Data Warehouse muss nach der Erstellung dieser Anmerkungen erfolgt sein.

### Schritte

1. Öffnen Sie in der Regel einen Browser für Ihren Reporting-Server `https://<host or IP>:9300/p2pd`` `http://<host or IP\>:9300/bi (7.3.3 or later)` Und melden Sie sich an.
2. Wählen Sie das Paket **File System Utilization** und erstellen Sie einen neuen Bericht.

3. Ziehen Sie Elemente aus Ihren Data Mart(s), um Ihren Bericht zu erstellen.

   Das folgende Beispiel ist ein sehr einfacher Bericht. Sie können komplexe Berichte erstellen, die auf Ihre spezifischen Geschäftsanforderungen abgestimmt sind.

| Name | Type | Allocated Capacity GB | Used Capacity GB | Tier Name | Cost | Storage Name |
|---|---|---|---|---|---|---|
| / | xfs | 119.96 | 9.96 | N/A | | vifasnane05,vifasnane06 |
| / | xfs | 5,492.53 | 799.63 | Tier 1 | 100 | vifasnane |
| /boot | xfs | 0.48 | 0.17 | N/A | | vifasnane05,vifasnane06 |
| /boot | xfs | 8.72 | 2.41 | Tier 1 | 100 | vifasnane |
| /dev/dm-1 | swap | 7.81 | 0.00 | N/A | | vifasnane05,vifasnane06 |
| /dev/dm-1 | swap | 140.61 | 0.78 | Tier 1 | 100 | vifasnane |
| C:\ | NTFS | 948.27 | 331.98 | Tier 1 | 100 | vifasnane |
| PHYSICALDRIVE0: System Reserved | NTFS | 1.70 | 1.41 | Tier 1 | 100 | vifasnane |

# Konfigurieren des Systems zur Erstellung von Chargeback-Daten

Chargeback-Berichte stellen Informationen zu Storage Capacity Chargeback und Accountability nach Hosts, Applikationen und Geschäftseinheiten bereit. Sie umfassen sowohl aktuelle als auch historische Daten.

In diesem Leitfaden wird beschrieben, wie Insight so konfiguriert wird, dass ein Chargeback-Bericht erstellt wird, der die Kosten für Service Level und Storage-Nutzung transparent macht. Ziel des Leitfadens ist es, die Schritte zur Erstellung eines einfachen Chargeback-Berichts durchzuführen und die Insight Benutzer mit den Optionen vertraut zu machen, die bei der Konfiguration von Chargeback in ihrer speziellen Umgebung zur Verfügung stehen.

Für jede Applikation werden im Beispielbericht die bereitgestellten Ressourcen und die Kosten der Ressourcen angegeben. Die Ausgabe für den Bericht wird durch Definition der folgenden Daten in Insight erstellt

- Storage-Tiers
- Kosten im Zusammenhang mit den einzelnen Storage-Tiers
- Bereitgestellte Storage-Kapazität
- Service-Leveln
- Kosten pro Service-Level

In den folgenden Abschnitten werden die Schritte beschrieben, die erforderlich sind, um diese Daten so zu konfigurieren, dass sie von Insight Reporting aufgerufen werden können.

## Definieren von Annotationen für die Verwendung mit Chargeback

Wenn Sie OnCommand Insight zur Nachverfolgung von Daten gemäß Ihren Unternehmensanforderungen anpassen, können Sie spezielle Annotationen definieren, die erforderlich sind, um ein vollständiges Bild Ihrer Daten zu erstellen: Beispielsweise

kann durch eine Annotation das Ende des Lebenszyklus einer Ressource, das Datacenter, in dem sich die Ressource befindet, oder eine Storage Tier definiert werden, die die Kosten pro GB des Storage definiert.

### Über diese Aufgabe

Das Beispiel für einen Chargeback-Bericht in diesem Leitfaden enthält Daten für den Service-Level und die Tier-Ebene. Sie müssen Anmerkungen für jedes Service-Level und jede Tier-Ebene erstellen und anschließend die Kosten für die Service-Level und Tier-Level definieren.

### Schritte

1. Melden Sie sich bei der Web-Benutzeroberfläche von Insight an
2. Klicken Sie Auf **Verwalten** > **Anmerkungen**

   Die Seite Anmerkungen wird angezeigt.

3. Bewegen Sie den Mauszeiger über den Service-Level oder die Beschriftung der Ebene, und klicken Sie auf .

   Das Dialogfeld Anmerkung bearbeiten wird angezeigt.

4. Klicken Sie auf **ADD**, um neue Tiers und Kosten hinzuzufügen.

   Im Berichtsbeispiel verwenden die Namen der Ebenen „Stufe“ und „Service“ die Analogie aus Edelmetall: Gold, „Sliver“ und „Bronze“. Sie können beliebige Namenskonventionen verwenden, die von Ihrer Organisation gewählt wurden, z. B. Stufe 1, Stufe 2, Oberster Rang.

5. Geben Sie die Werte für die Tiers Gold-Fast, Gold, Silber und Bronze sowie die zugehörigen Kosten ein.

   Die von Ihnen eingegebenen Werte definieren die Kosten pro GB für den Speicher, der von Anwendungen verwendet wird. Die Service-Level-Kosten können die Kosten für die Bereitstellung der Dienstleistung oder der tatsächliche Preis für die Dienstleistung des Verbrauchers sein. Diese Kosten werden im Chargeback-Bericht ausgewiesen.

6. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

## Definition von Applikationen für die Verwendung mit Chargeback

Wenn Sie Kostendaten zu bestimmten Applikationen verfolgen möchten, die in Ihrer Umgebung ausgeführt werden, müssen Sie zunächst die Applikationen definieren.

### Bevor Sie beginnen

Wenn Sie eine Applikation einer Geschäftseinheit zuordnen möchten, müssen Sie die Geschäftseinheit bereits erstellt haben.

In diesem Beispiel werden keine Anwendungen mit Geschäftseinheiten verknüpft.

### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.

2. Klicken Sie Auf **Verwalten** > **Anwendung**

   Nachdem Sie eine Applikation definiert haben, werden auf der Seite Anwendungen der Name der Applikation, ihre Priorität und gegebenenfalls die mit der Applikation verknüpfte Geschäftseinheit angezeigt.

3. Klicken Sie Auf**Hinzufügen**

   Das Dialogfeld Anwendung hinzufügen wird angezeigt.

4. Geben Sie im Feld Name einen eindeutigen Namen für die Anwendung ein. Geben Sie die im Bericht „African Tours“, „APAC Commercial Sales“ usw. identifizierten Anwendungen ein.
5. Klicken Sie auf **Priorität** und wählen Sie die Priorität (kritisch, hoch, mittel oder niedrig) für die Anwendung in Ihrer Umgebung aus.
6. Wenn Sie diese Anwendung mit einer Business Entity verwenden möchten, klicken Sie auf **Business Entity** und wählen Sie die Entity aus der Liste aus.
7. Sie werden keine Volume-Freigabe verwenden, klicken Sie auf, um das Feld **Validieren** Volume-Freigabe zu deaktivieren.
8. Klicken Sie Auf **Speichern**.

   Die Anwendungen werden auf der Seite Anwendungen angezeigt. Wenn Sie auf den Namen der Anwendung klicken, zeigt Insight die Seite der Anlage für die Anwendung an. Nachdem Sie eine Anwendung definiert haben, können Sie eine Anlagenseite für Host, virtuelle Maschine, Volume, internes Volume oder Hypervisor aufrufen, um eine Anwendung einem Asset zuzuweisen.

## Zuweisen von Anwendungen zu Assets

Nachdem Sie Ihre Anwendungen definiert haben, müssen Sie die Anwendungen bestimmten Assets zuordnen. Sie können eine einfache Ad-hoc-Methode verwenden, um Anwendungen auf ein Asset anzuwenden. Benutzer, die Anwendungen in großen Mengen anwenden möchten, sollten eine Abfragemethode verwenden, um die Assets zu identifizieren, die sie einer Anwendung zuweisen möchten.

#### Zuweisen von Anwendungen zu Assets mithilfe einer Ad-hoc-Methode

Sie weisen einem Asset eine Anwendung zu, sodass Sie die Ressourcen des Assets identifizieren können, das von der Anwendung verwendet wird. Wenn einem Asset Kosten zugewiesen sind, können Sie die Kosten identifizieren, die der Applikation entstehen. Wenn die Ressource nach Größe gemessen wird, können Sie bestimmen, ob die Ressource wieder aufgefüllt werden muss.

##### Über diese Aufgabe

Verwenden Sie die folgende Methode, um Anwendungen Assets zuzuweisen.

##### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Suchen Sie das Asset (Host, virtuelle Maschine, Volume oder internes Volume), auf das Sie die Anwendung anwenden möchten, indem Sie einen der folgenden Schritte ausführen:

| Option | Beschreibung |
| --- | --- |
| Navigieren Sie zur Liste der Assets | Klicken Sie auf **Dashboard** > **Assets Dashboard** und wählen Sie das Asset aus. |
| Suchen Sie nach dem Asset | Klicken Sie Auf Geben Sie in der Symbolleiste, um das Feld **Assets suchen** anzuzeigen, den Namen des Assets ein, und wählen Sie dann das Asset aus der Liste aus. |

3. Positionieren Sie im Bereich **Benutzerdaten** der Asset-Seite den Cursor über den Namen der Applikation, die dem Asset aktuell zugewiesen ist (wenn keine Anwendung zugewiesen ist, wird **Keine** angezeigt), und klicken Sie dann auf (Anwendung bearbeiten).

   Die Liste der verfügbaren Anwendungen für das ausgewählte Asset wird angezeigt. Den Anwendungen, die derzeit mit dem Asset verknüpft sind, wird ein Häkchen vorangestellt.

4. Sie können in das Suchfeld eingeben, um die Anwendungsnamen zu filtern, oder Sie können in der Liste nach unten blättern.
5. Wählen Sie die Anwendungen aus, die Sie dem Asset zuordnen möchten.

   Sie können dem Host, der virtuellen Maschine und dem internen Volume mehrere Anwendungen zuweisen. Sie können einem Volume jedoch nur eine Anwendung zuweisen.

6. Klicken Sie Auf So weisen Sie der Anlage die ausgewählte Applikation oder die ausgewählten Anwendungen zu.

   Die Applikationsnamen werden im Abschnitt Benutzerdaten angezeigt. Wenn die Applikation mit einer Geschäftseinheit verknüpft ist, wird auch der Name der Geschäftseinheit in diesem Abschnitt angezeigt.

### Zuweisen von Anwendungen zu einem Asset mithilfe einer Abfrage

Sie weisen einem Asset eine Anwendung zu, sodass Sie die Ressourcen des Assets identifizieren können, das von der Anwendung verwendet wird. Wenn einem Asset Kosten zugewiesen sind, können Sie die Kosten identifizieren, die der Applikation entstehen. Wenn die Ressource nach Größe gemessen wird, können Sie bestimmen, ob die Ressource wieder aufgefüllt werden muss.

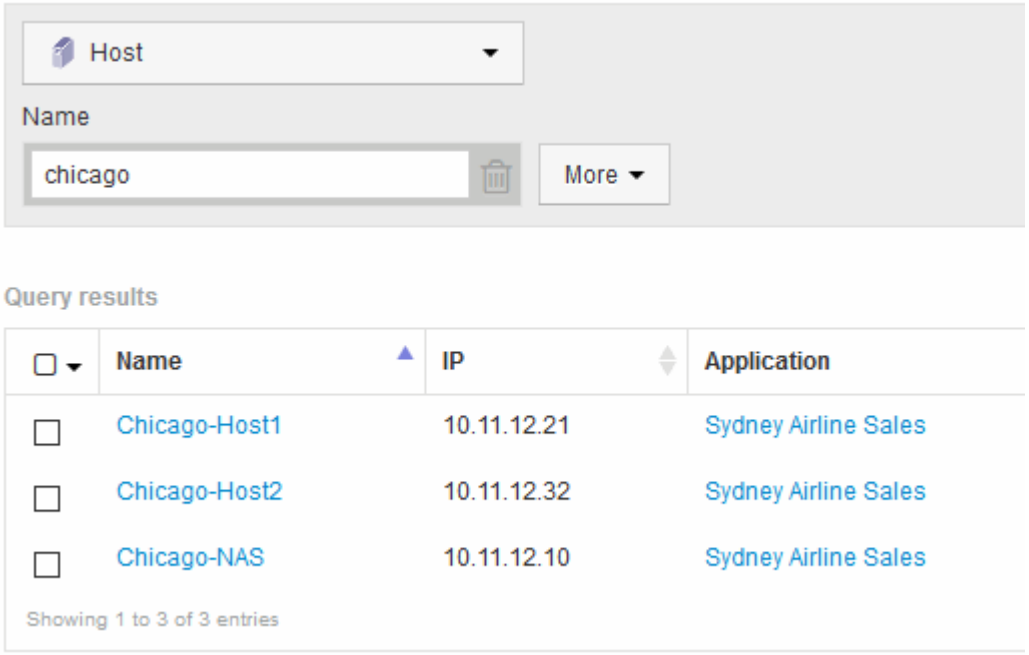
#### Über diese Aufgabe

Sie können die Zuweisung mehrerer Assets zu einer Anwendung vereinfachen, indem Sie eine Abfrage verwenden.

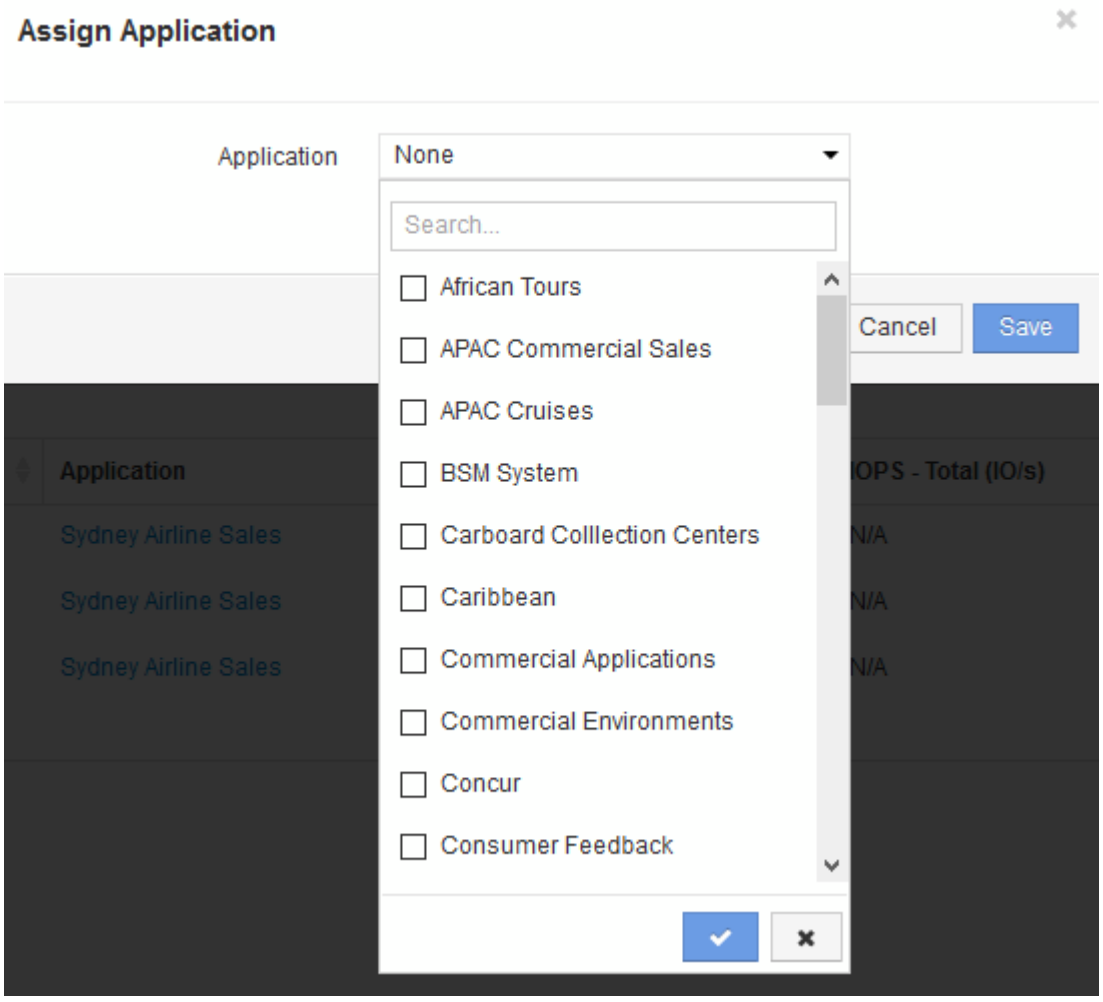
#### Schritte

1. Erstellen Sie eine neue Abfrage, um die Assets zu identifizieren, denen Sie eine Anwendung zuweisen möchten. Wenn Sie ihn beispielsweise einem Host mit einem bestimmten Namen zuweisen möchten, der sich auf einen geografischen Standort bezieht, klicken Sie auf **Abfragen** > **+Neue Abfrage**
2. Klicken Sie Auf **Host**
3. Geben Sie im Feld **Name** ein `Chicago`

Das System zeigt alle Hosts mit an `Chicago` Als Teil, wenn ihr Name.




4. Wählen Sie einen oder mehrere Hosts aus, die von Ihrer Abfrage identifiziert wurden.
5. Klicken Sie Auf **Actions** > **Add Application**



Das Dialogfeld Anwendung zuweisen wird angezeigt.

6. Wählen Sie die Anwendung aus, die Sie dem Host zuweisen möchten, und klicken Sie auf
7. Klicken Sie Auf **Speichern**

   Der Anwendungsname wird im Abschnitt Benutzerdaten angezeigt.

## Erstellen eines einfachen Chargeback-Berichts

Chargeback-Berichte ermöglichen Administratoren und Managern die Bewertung der Kapazitätsauslastung nach Applikation, Geschäftseinheit, Service Level und Tier. Die Chargeback-Berichte umfassen Angaben zu Kapazitätstransparenz, historischer Kapazitätstransparenz und Trenddaten. Die Daten für diese Berichte werden aus dem OnCommand Insight Data Warehouse erstellt und geplant.

### Bevor Sie beginnen

Ihr System muss für die Erstellung des Beispielberichts konfiguriert werden, um die Kosten für Storage-Tiers zu melden. Die folgenden Aufgaben müssen durchgeführt werden:

- Definieren Sie Anmerkungen für Ebenen.
- Kostenzuordnung zu Anmerkungen.
- Definieren Sie die Anwendungen, für die Sie Daten nachverfolgen möchten.
- Anwendungen zu Assets zuweisen.

### Über diese Aufgabe

In diesem Beispiel wird das erweiterte Reporting-Tool Cognos Workspace verwendet, um den Chargeback-Bericht zu erstellen. Mit Workspace Advanced erstellen Sie Berichte, indem Sie Datenelemente in eine Berichtpalette ziehen und ablegen.

### Schritte

1. Klicken Sie in der OnCommand Insight-Webbenutzeroberfläche auf das Berichtssymbol.
2. Melden Sie sich beim Reporting Portal an.
3. Klicken Sie in der IBM Cognos-Verbindungssymbolleiste auf **Start** > **Cognos Worksapce Advanced**

   Der Bildschirm Workspace Advanced Package wird geöffnet.

4. Klicken Sie Auf **Packages** > **Chargeback**

   Der Bildschirm IBM Workspace Advanace wird angezeigt.

5. Klicken Sie Auf **Neu**
6. Klicken Sie im Dialogfeld **New** Report auf **List**, um einen Listenbericht anzugeben.

   Die Berichtpalette wird angezeigt, und unter der Überschrift Quelle werden die Rückbelastung „`Simple Data Mart`“ und „`Advanced Data Mart`“ angezeigt.

7. Klicken Sie auf die Pfeile neben den einzelnen Data Marts, um sie zu erweitern.

   Der volle Inhalt der Data Marts wird angezeigt.

8. Ziehen Sie „`Application`“ aus dem „`Simple Data Mart `“ in die linke Spalte der Berichtpalette.

   Wenn Sie ein Element in die Palette ziehen, wird die Spalte verkleinert und hervorgehoben. Wenn Sie die Anwendungsdaten in die hervorgehobenen Spalten ablegen, werden alle Anwendungen in der Spalte korrekt aufgelistet.

9. Ziehen Sie „`Tier`“ aus dem „`Simple Data Mart `“ in die nächste Spalte der Berichtpalette.

   Die zu jeder Applikation gehörende Speicherebene wird der Palette hinzugefügt.

10. Ziehen Sie „`Tier Cost`“ aus dem „`Simple Data Mart `“ in die nächste Spalte der Berichtpalette.
11. Ziehen Sie „`Provisioned Capacity`“ aus dem „`Simple Data Mart `“ in die nächste Spalte der Berichtpalette.
12. Halten Sie die Taste **Strg** gedrückt und wählen Sie die Spalten „`Tier Cost`“ und „`Provisioned Capacity`“ in der Palette aus.
13. Klicken Sie mit der rechten Maustaste in eine der ausgewählten Spalten.
14. Klicken Sie auf **Berechnen** > **Tier-Kosten * bereitgestellte Kapazitäts-DB**

    Der Palette wird eine neue Spalte mit dem Titel „Tier Cost * Provisioning Capacity GB“ hinzugefügt.

15. Klicken Sie mit der rechten Maustaste auf die Spalte **Tier Cost * Provisioning Capacity GB**.
16. Klicken Sie Auf **Stil** > **Datentyp**
17. Klicken Sie auf **Formattyp** > **Währung**
18. Klicken Sie auf **OK**

    Die Spaltendaten werden nun als US-Währung formatiert.

19. Klicken Sie mit der rechten Maustaste auf „`Tier Cost * Provision Capacity GB`“ und wählen Sie **Edit Data Item Label** aus
20. Ersetzen Sie das Namensfeld durch „`provisionierte Kapazitätskosten`“.
21. Klicken Sie zum Ausführen des Berichts auf **Ausführen** > **Bericht ausführen - HTML**

    Es wird ein Bericht wie der folgende angezeigt.

| Application | Service Level | Service Level Cost | Tier | Tier Cost | Provisioned Capacity GB | Provisioned Capacity Cost |
|---|---|---|---|---|---|---|
| APAC Commercial Sales | Gold-Fast | 12 | Gold-Fast | 12 | 674.04 | $8,088.42 |
| APAC Commercial Sales | Silver | 10 | Silver | 7 | 1,903.83 | $13,326.82 |
| APAC Cruises | Gold-Fast | 12 | Gold-Fast | 12 | 730.20 | $8,762.44 |
| African Tours | Gold | 12 | Gold | 10 | 4,856.12 | $48,561.16 |
| African Tours | Silver | 10 | Silver | 7 | 1,480.85 | $10,365.93 |
| CRM | Bronze | 3 | Bronze | 3 | 5,689.08 | $17,067.23 |
| Caribbean | Gold | 12 | Gold | 10 | 4,590.41 | $45,904.08 |
| Commercial Applications | Bronze | 3 | Bronze | 3 | 14,312.88 | $42,938.64 |
| Commercial Applications | Gold-Fast | 12 | Gold-Fast | 12 | 40,308.42 | $483,701.05 |
| Commercial Environments | Bronze | 3 | Bronze | 3 | 16,812.27 | $50,436.81 |
| Commercial Environments | Gold | 12 | Gold | 10 | 9,313.51 | $93,135.13 |
| Commercial Environments | Silver | 10 | Silver | 7 | 1,480.79 | $10,365.54 |
| Concur | Gold | 12 | Gold | 10 | 247.39 | $2,473.91 |
| Concur | Gold-Fast | 12 | Gold-Fast | 12 | 575.17 | $6,902.09 |
| Consumer Feedback | Gold | 12 | Gold | 10 | 1,335.89 | $13,358.94 |

# Berichte zur I/O-Dichte beschreiben nur interne Daten-Volumes

Bei NetApp Storage-Systemen enthält das Root-Aggregat das Root-Volume. Das Root-Volume enthält spezielle Verzeichnisse und Konfigurationsdateien für die Verwaltung und Steuerung des Speichersystems. Die Management- und Kontrollvorgänge können zu umfangreichen Aktivitäten im Root-Aggregat führen. Wenn Sie das Insight System für die 10 besten internen Volumes mit der höchsten I/O-Dichte abfragen, können die Ergebnisse unter Umständen auch NetApp Root-Aggregate zu Mitgliedern der Top 10 gehören.

Bei der Überwachung Ihrer Umgebung ist es wichtiger, zu ermitteln, welche internen Datenvolumen eine hohe I/O-Dichte erzeugen. Damit nur die Daten-Volumes präzise ermittelt werden können, müssen die internen NetApp Volumes von Anfragen isoliert werden, die zur Überwachung der I/O-Dichte erforderlich sind.

Dieser Leitfaden beschreibt, wie NetApp Root-Aggregate leicht identifiziert, von den Ergebnissen interner Volume-Abfragen isoliert und Regeln erstellt werden können, die beim Hinzufügen zum System neue NetApp Root-Aggregate ausschließen. Die folgenden Funktionen von Insight sorgen dafür, dass die Berichte zur I/O-Dichte von internen Daten-Volumes abgeleitet werden.

- Es wird eine Abfrage erstellt, um alle NetApp Root-Aggregate zu identifizieren, die von Insight überwacht werden.
- Jedem NetApp Root-Aggregat wird eine Annotation zugewiesen.
- Eine Anmerkungsregel wird erstellt, um die NetApp Aggregate auszuschließen

## Erstellen einer Abfrage, um NetApp Root-Aggregate in Ihrer Umgebung zu identifizieren

Abfragen ermöglichen die Suche auf granularer Ebene, basierend auf vom Benutzer ausgewählten Kriterien. Mit einer Abfrage können Sie nach internen Volumes in Ihrer

Umgebung suchen, die das NetApp Root-Aggregat enthalten.

**Schritte**

1. Erstellen Sie in der Web-Benutzeroberfläche von OnCommand Insight eine Abfrage zur Identifizierung von NetApp-Root-Aggregaten in Ihrer Umgebung: **Abfragen** > **neue Abfrage** > **Ressourcentyp auswählen**
2. Klicken Sie Auf **Speicherpool**
3. Geben Sie den Namen für das Root-Aggregat ein

   In diesem Beispiel wird „`aggr0`“ für den Namen verwendet. Beim Erstellen eines Aggregats müssen nur die folgenden Anforderungen für den Namen erfüllt werden:

   - Er muss entweder mit einem Buchstaben oder einem Unterstrich (_) beginnen.
   - Er darf nur Buchstaben, Ziffern und Unterstriche enthalten.
   - Sie kann maximal 250 Zeichen umfassen. In den meisten Fällen ist das Aggregat der Name aggr0, aggr_0, oder etwas ähnliches. Es könnte einen iterativen Prozess erfordern, um alle NetApp Root-Aggregate in Ihrer Umgebung zu identifizieren.
4. Klicken Sie auf **Speichern** und geben Sie einen Namen für die neue Abfrage ein.

   Wie bereits erwähnt, könnte dies ein iterativer Prozess sein und mehrere Anfragen zur Identifizierung aller NetApp Root-Aggregate erfordern.

## Erstellen Sie eine Anmerkung für die von Ihren Abfragen zurückgegebenen Root-Volumes

Anmerkungen sind spezielle Notizen, die Sie Ihren Assets zuweisen, damit Sie Assets nach ihren Anmerkungen filtern können. Die von Ihnen erstellten Annotationen werden verwendet, um die NetApp Root-Aggregate in Ihrer Umgebung zu identifizieren und sicherzustellen, dass diese nicht in einem bestimmten Bericht enthalten sind.

**Bevor Sie beginnen**

Sie müssen alle Root-Aggregate identifiziert haben, die Sie aus dem Bericht „`High I/O Density`“ ausschließen möchten.

**Schritte**

1. Erstellen Sie eine Annotation, um alle NetApp-Root-Aggregate, die Sie identifiziert haben, mit Abfragen zu verknüpfen: **Verwalten** > **Annotationen**
2. Klicken Sie Auf **Hinzufügen**
   a. Geben Sie den Namen für die Anmerkung ein: **RootAggr**
   b. Geben Sie eine Beschreibung der Anmerkung ein: **Root-Aggregat aus dem Bericht "hohe I/O-Dichte" entfernen**
   c. Geben Sie den Typ der Anmerkung ein: **Boolean**
3. Klicken Sie Auf **Speichern**

### Erstellen einer Annotation-Regel, um bestimmte Aggregate aus Ihrem I/O-Dichtebericht zu automatisieren

Alternativ zum manuellen Anwenden von Anmerkungen auf einzelne Assets können Sie mithilfe von Anmerkungsregeln automatisch Anmerkungen auf mehrere Assets anwenden. Anmerkungsregeln basieren auf Abfragen, die Sie erstellen, und wenn sie auf dem System ausgeführt werden, fügen sie vorhandenen Assets neue Assets hinzu. Wenn diese Vermögenswerte von einem Bericht ausgeschlossen werden, werden auch die neuen Vermögenswerte automatisch ausgeschlossen.

#### Bevor Sie beginnen

Sie müssen eine Abfrage erstellt und gespeichert haben, die die NetApp Root-Aggregate identifiziert, die Sie in Ihrer Umgebung identifiziert haben.

#### Schritte

1. Melden Sie sich bei der OnCommand Insight Web UI an.
2. Klicken Sie auf **Verwalten** > **Anmerkungsregeln**
3. Klicken Sie Auf **Hinzufügen**

   Das Dialogfeld Regel hinzufügen wird angezeigt.

4. Gehen Sie wie folgt vor:
   a. Geben Sie im Feld Name einen eindeutigen Namen ein, der die Regel „`RootAggrExclude`“ beschreibt.
   b. Klicken Sie auf „Query“ und wählen Sie die Abfrage aus, die von Insight verwendet werden soll, um die Anmerkungsregel auf:“` Aggregate0`“ anzuwenden.
   c. Klicken Sie auf Anmerkung und wählen Sie „`Root agg exclude`“ aus.
   d. Klicken Sie auf Wert, und geben Sie true ein

# Erfassung von Integrationsdaten

Sie können Integrationsdaten in Ihr OnCommand Insight-System importieren. Daten können mit collectd, einer Open-Source-Software, importiert werden, die als Daemon zum Sammeln von Leistungsdaten ausgeführt wird, oder mit Hilfe der Integrations-SNMP-Datenquelle, mit der Sie allgemeine SNMP-Daten erfassen können.

## Datenfluss für Integrationsdaten

Folgendes gilt für die Gesamtmenge der Integrationsdaten, die dem OnCommand Insight-Server zur Verfügung gestellt werden dürfen:

- Eine Warteschlange mit 100 Anrufen wird beibehalten.

  Wenn ein Client länger als eine Minute in der Warteschlange wartet, tritt ein Zeitüberschreitungsfehler auf.

- Die empfohlene Aufnahmerate für Integrationsdaten beträgt einmal pro Minute und pro Client.

- Es sind maximal 300 Integrationsobjekttypen zulässig.

## Zugriff auf Software und Dokumentation für die Sammlung

Die Output Writer Plug-in-Software und die Dokumentation zur Sammlung finden Sie auf der NetApp GitHub Website: https://github.com/NetApp/OCI_collectd

## Backup und Restore von Integrationsdaten

Backup und Restore von Integrationsdaten werden nach den Backup- und Restore-Richtlinien für OnCommand Insight Performance-Daten modelliert. Wenn ein Backup für Leistungsdaten konfiguriert wird, werden auch Integrationsdaten in das Backup einbezogen. Wie beim Performance-Backup sind auch die Integrationsdaten der letzten sieben Tage im Backup enthalten. Alle in einem Backup vorhandenen Integrationsdaten werden bei einem Wiederherstellungsvorgang wiederhergestellt.

## Lizenzen Zu Haben

Für die Meldung von Integrationsdaten ist eine Perform-Lizenz erforderlich. Wenn keine Lizenz zur Durchführung vorhanden ist, tritt ein Fehler mit der Meldung „Lizenz zum Melden von Integrationsdaten erforderlich ausführen“ auf.

## Erfassen von SNMP-Integrationsdaten

Mit der integrierten SNMP-Datenquelle können Sie allgemeine SNMP-Daten in OnCommand Insight erfassen.

#### Integrationspakete

Die Datenquelle „SNMP Integration“ verwendet ein „`Integration Pack`“, um zu definieren, welche Integrationswerte erfasst werden und welche SNMP-Objekte diese Werte bereitstellen.

Ein Integration Pack besteht aus:

- Eine JSON-Konfigurationsdatei (Integration.json), die die Integration von Nutzlastinhalten in Bezug auf SNMP-Objekte eines bestimmten Gerätetyps (Switch, Router usw.) definiert.
- Eine Liste der MIB-Dateien, die das Integrationspaket abhängig ist.

Ein Integrationspaket kann mehrere Datentypen definieren. Wenn Sie beispielsweise einen RHEL-Host integrieren, kann ein Datentyp für allgemeine Systeminformationen wie Uptime, Anzahl der Benutzer und Anzahl der laufenden Prozesse definiert werden. Dadurch kann ein zweiter Datentyp für die Speichernutzung und die Auslastung des Dateisystems definiert werden. Im Allgemeinen muss jeder Datentyp „`flat`“ sein und darf keine verschachtelten Daten enthalten.

Ein einzelnes Integrationspaket sollte nicht mehr als 24 Datentypen definieren. Insight begrenzt die Menge der gesammelten Integrationsdaten. Der Versuch, mehr als 24 Berichte über einen Zeitraum von einer Minute aufzunehmen, führt zu einem Ratenfehler.

Die Namen für Integrationstypen müssen die folgenden Regeln einhalten:

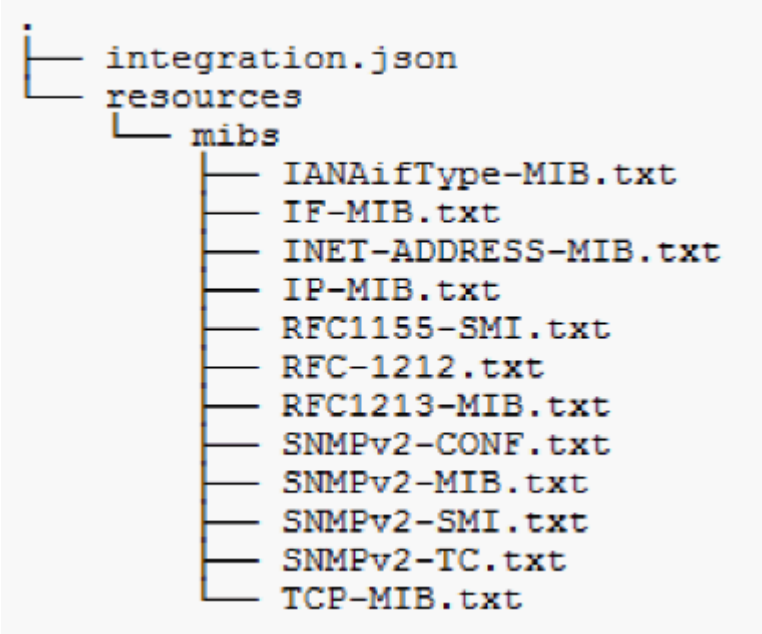
- Der Name darf nicht mit den folgenden Zeichen beginnen: _, - oder,+
- Der Name darf die folgenden Zeichen nicht enthalten: #, \, /, *, ?, „, <, >, ' , `,
- Darf nicht länger als 100 UTF-8-kodierte Bytes sein

- Kann nicht benannt werden. Oder ..

#### Integrationsdateiformat

Ein Integrationspaket ist eine ZIP-Datei, die eine JSON-Konfigurationsdatei (Integration.json) enthält, die den Inhalt der Integrations-Nutzdaten in Bezug auf SNMP-Objekte definiert. Es enthält auch einen MIBS-Ordner, der alle MIB-Dateien und ihre MIB-Abhängigkeiten enthält.

Der `integration.json` Die Datei muss auf der obersten Ebene der ZIP-Datei vorhanden sein und die MIB-Dateien müssen im Unterverzeichnis „Resources/mibs“ innerhalb der ZIP-Datei vorhanden sein. Die ZIP-Datei kann auch Dateien enthalten, wie z.B. eine "readme.txt", wenn gewünscht. Ein Beispiel für die Integration ZIP-Struktur ist:




#### Importieren von SNMP-Integrationspaketen

Sie importieren SNMP-Integrationspakete über die Web-Benutzeroberfläche in OnCommand Insight. Integrationspakete werden durch den im definierten Wert „IntegrationPackName“ identifiziert `integration.json` In der ZIP-Datei enthaltene Konfigurationsdatei.

##### Bevor Sie beginnen

Sie müssen eine richtig formatierte ZIP-Datei erstellt haben, die das Integrationspaket enthält, das Sie auf den OnCommand Insight-Server importieren möchten.

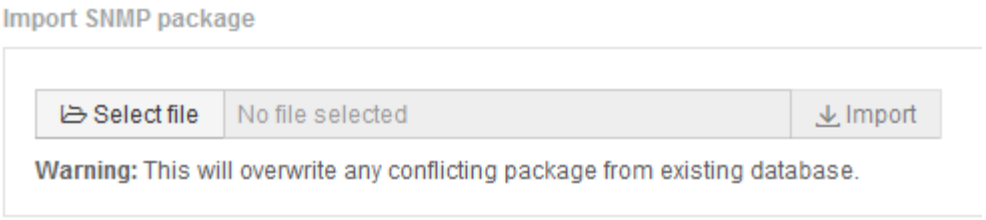
##### Über diese Aufgabe

Führen Sie die folgenden Schritte aus, um SNMP-Integrationspakete auf den Insight-Server zu importieren.

##### Schritte

1. Klicken Sie auf **Admin** > **Setup** > **SNMP-Integration**

   Das System zeigt den Bildschirm SNMP-Paket importieren an:




2. Klicken Sie auf **Select file**, um die lokale Datei auszuwählen, die das SNMP-Paket enthält.

   Die ausgewählte Datei wird im Feld Datei angezeigt.

   Alle vorhandenen Integrationspakets mit demselben Namen werden überschrieben.

3. Klicken Sie Auf **Import**

   Die Datei wird auf den Insight-Server importiert.

### Erstellen einer Datenquelle für die SNMP-Integration

Die Integrations-SNMP-Datenquelle bietet allgemeine SNMP-Konfigurationseigenschaften ähnlich wie andere SNMP-basierte Datenquellen, die in den OnCommand Insight-Datenquellen für Brocade und Cisco enthalten sind.

#### Bevor Sie beginnen

Damit die Integrations-SNMP-Datenquelle erfolgreich zum Erfassen verwendet werden kann, muss Folgendes zutreffen:

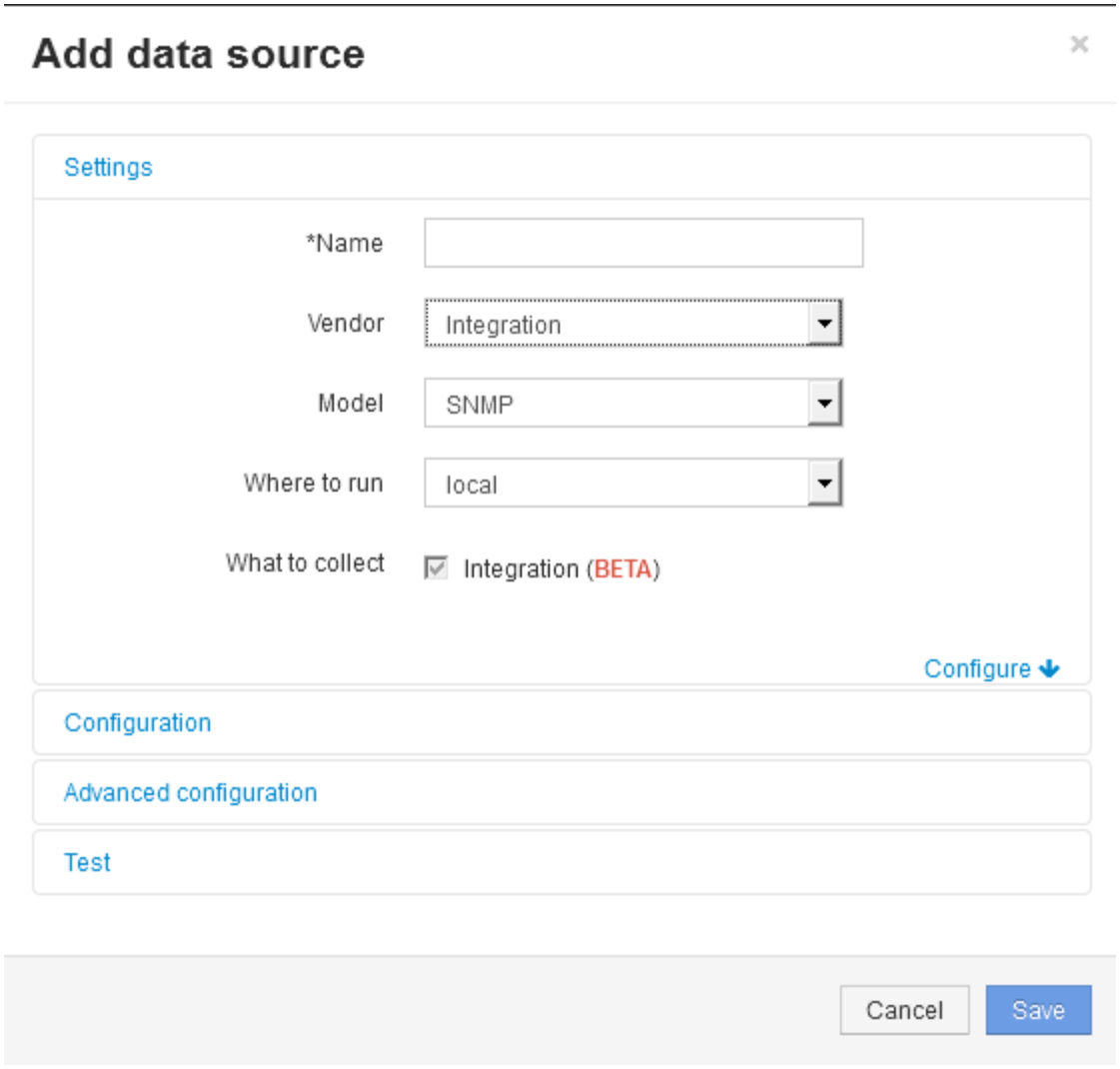
- Sie müssen bereits ein Integrationspaket importiert haben, das Sie für diese SNMP-Datenquelle verwenden.
- Alle Zielgeräte haben dieselben Anmeldeinformationen.
- Alle Zielgeräte implementieren die SNMP-Objekte, auf die das konfigurierte Integrationspaket verweist.

#### Über diese Aufgabe

Um eine Datenquelle für die SNMP-Integration zu erstellen, wählen Sie im Assistenten für die Erstellung der Datenquelle „Integration“ und „SNMP“ aus.

#### Schritte

1. Klicken Sie in der OnCommand Insight Web UI auf **Admin** > **Datenquellen**
2. Klicken Sie Auf **+Hinzufügen**
3. Geben Sie einen Namen für die Datenquelle ein
4. Wählen Sie für Anbieter **Integration** aus
5. Wählen Sie für Modell **SNMP** aus




6. Für was zu sammeln, überprüfen Sie **Integration**

   Dies ist das einzige Paket auf dieser Datenquelle und wird standardmäßig aktiviert:

7. Klicken Sie Auf **Konfiguration**
8. Geben Sie die IP-Adressen für die Systeme ein, von denen Sie SNMP-Daten erfassen
9. Wählen Sie ein importiertes SNMP Integration Pack aus
10. Legen Sie das Intervall für die Integrations-Abfrage fest
11. Wählen Sie die SNMP-Version aus
12. Geben Sie die SNMP-Community-Zeichenfolge ein

    Für SNMP V1 und V2.

13. Fügen Sie den Benutzernamen und das Kennwort für Systeme hinzu, von denen Sie Daten erfassen möchten.

    Für SNMP V3.

14. Klicken Sie Auf **Erweiterte Konfiguration**

    Die Standardeinstellungen der erweiterten Konfiguration werden angezeigt. Nehmen Sie alle erforderlichen

Änderungen an diesen Einstellungen vor.

#### Integration.json-Dateiinformationen

## Die Datei Integration.json identifiziert die Nutzlast .

Die folgende Abbildung zeigt eine farbcodierte Darstellung einer einfachen Integration.json-Datei. In der beigefügten Tabelle wird die Funktion der Objekte in der Datei angegeben.

```
{
 "integrationPackName": "WindowsSnmp",
 "description": "Generic integration for mibs supported by the default
SNMP  Agent for Windows 2012, including HOST-RESOURCES",
 "acquisitionType": "SNMP",
 "integrationTypes": [
  {
   "integrationType":       "snmp_win2012_host",
   "name": {
    "mibModuleName":     "RFC1213-MIB",
    "objectName":        "sysName"
   },
   "identifiers": {
    "hostname": {
     "mibModuleName":     "RFC1213-MIB",
    }
   },
   "attributes": {
    "description": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":        "sysDescr"
    },
    "snmp_sys_obj_id": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":        "sysObjectID"
    }
   },
   "dataPoints": {
    "uptime": {
     "num": {
      "mibModuleName":    "RFC1213-MIB",
      "objectName":       "sysUpTime"
     }
    }
   }
  }]}
```

| | |
|---|---|
| Blue | Reserved |
| Red | User customizable strings and IDs |
| Green | MIB names |
| Purple | MIB object |
| Black | JSON structure |

#### Info zu Integration.json-Dateien

Jedes Feld hat folgende Merkmale:

- Der Abschnitt „Identifiers“ bildet einen eindeutigen zusammengesetzten Schlüssel zur Erstellung eines

neuen „Objekts“ in Insight

- Die "Attribute" liefern unterstützende Metadaten zum Objekt.

  In beiden Fällen wird nur der Wert des neuesten Berichts für dieses Objekt (identifiziert durch die Kennungen) beibehalten.

- Die „Datenpunkte“ sind Zeitreihendaten und müssen numerische Werte sein. Insight speichert jeden hier gemeldeten Wert standardmäßig 90 Tage lang und verknüpft diese Zeitreihen mit dem identifizierten Objekt.

#### Numerische Ausdrücke

Standardmäßig werden alle Wertausdrücke als Strings in der Integrations-Payload gemeldet. „Identifiers“ und „Attribute“ können nur Zeichenfolgenwerte definieren. „Datapoint“ kann String- oder numerische Werte definieren. Numerische Werte werden mit einem der folgenden Zusatztasten definiert:

- num - die Gesamtzahl der empfangenen Bytes seit der letzten Initialisierung des Zählers
- delta - die Anzahl der Bytes, die während des Abfrageintervalls empfangen wurden
- Rate: Die durchschnittliche Empfangsrate während des Abfrageintervalls in Byte pro Sekunde

  Eine durchschnittliche Empfangsrate während des Abfrageintervalls in Megabyte pro Sekunde kann mithilfe einer Kombination aus Rate und mathematischen Operationen durchgeführt werden

#### Mathematische Vorgänge

Der `integration.json` File unterstützt die folgenden mathematischen Operationen: Add, subtrahieren, multiplizieren, dividieren. Das folgende Beispiel zeigt Multiplikations-, Division- und Sum-Operationen in einer JSON-Datei.

```
"network_utilization":
{
  "mult": [
    {
      "div": [
        {
          "sum": [
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCOutOctets",
              "comment":        "bytes per second out"
            },
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCInOctets",
              "comment":        "bytes per second in"
            }
          ]
        },
        {
          "num": {
            "mibModuleName":  "IF-MIB",
            "objectName":     "ifSpeed",
            "comment":        "1,000,000 bits per second"
          }
        }
      ]
    },
    {
      "const":                0.0008,
      "comment":       "normalize to ratio of bits and convert to percent:
                       8 * 100 / 1,000,000 = 0.0008"
    }
  ]
}
```

**Stichwörter**

Ein Integrationspaket-Schlüsselwort, String, wird implementiert, um OKTETT-Strings oder proprietäre Typen, die aus OKTETT-STRINGS abgeleitet werden, zu erzwingen, die normalerweise im hexadezimalen Format gerendert werden, um stattdessen als ASCII-Zeichen dargestellt zu werden.

Häufig ENTHALTEN OKTETT-Strings binäre Daten, z. B. MAC-Adressen und WWNs:

```
        "interface_mac": {
                  "mibModuleName":      "IF-MIB",
                  "objectName":         "ifPhysAddress"
                 }
```

IfPhysAddress ist der Typ PhysAddress, der nur EIN OKTETT-STRING ist:

```
  PhysAddress ::= TEXTUAL-CONVENTION
                DISPLAY-HINT "1x:"
                STATUS       current
                DESCRIPTION
                                "Represents media- or physical-level
addresses."
                SYNTAX       OCTET STRING
```

Wenn ifPhysAddress standardmäßig als Hex gerendert wird, ist das Ergebnis:

```
"interface_mac": "00:50:56:A2:07:E7"
```

Wenn Sie jedoch einen OKTETT-STRING oder einen proprietären Typ haben, der von OKTETT-STRING abgeleitet wurde, den Sie als ASCII interpretieren möchten, können Sie das Schlüsselwort „string“ verwenden:

```
        "string_test_1": {
          "string": {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
          }
        },

        "string_test_2": {
          "string": [
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            },
            {
              "const": "JSD"
            },
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            }
          ]
        }
```

Das Schlüsselwort folgt den bestehenden Regeln für die Zeichenfolgenverkettung und fügt im folgenden Beispiel ein einzelnes Leerzeichen zwischen Begriffen ein:

```
    "string_test_1": "PV¢ç",
           "string_test_2": "PV¢ç JSD PV¢ç"
```

Das Schlüsselwort „string“ wirkt auf einen einzelnen Begriff oder eine Liste von Begriffen, aber nicht auf verschachtelte Ausdrücke. Verschachtelte Ausdrücke werden nur für Datenpunkteausdrücke unterstützt. Der Versuch, einen „String“-Ausdruck in einem Datapoint-Ausdruck zu verwenden, führt zu einem Fehler, der dem folgenden ähnelt:

*java.lang.IllegalArgumentException: Integration Pack 'GenericSwitch32' Index 'snmp_generic_Interface_32' Abschnitt 'daPoints' Schlüssel 'string_Test_3' nicht unterstützter JSON-numerischer Ausdruck '{"string":{"mibModuleName":"IF-MIB","objectName":"ifPhysAddress"}}'*

Einige abgeleitete OKTETT-STRING-Typen wie DisplayString, SnmpAdminString haben einen hartkodierten Vorrang vor dem Schlüsselwort "string". Das liegt daran, dass SnmpAdminString spezifisch UTF-8-kodiert ist und wir es richtig handhaben wollen, während das "string"-Schlüsselwort die vom snmp_Framework zurückgegebene Standardzeichendarstellung erzwingt, die einzelne Byte ascii-Codepunkte pro Zeichen annimmt.

# Analyse eines Applikations-Performance-Problems

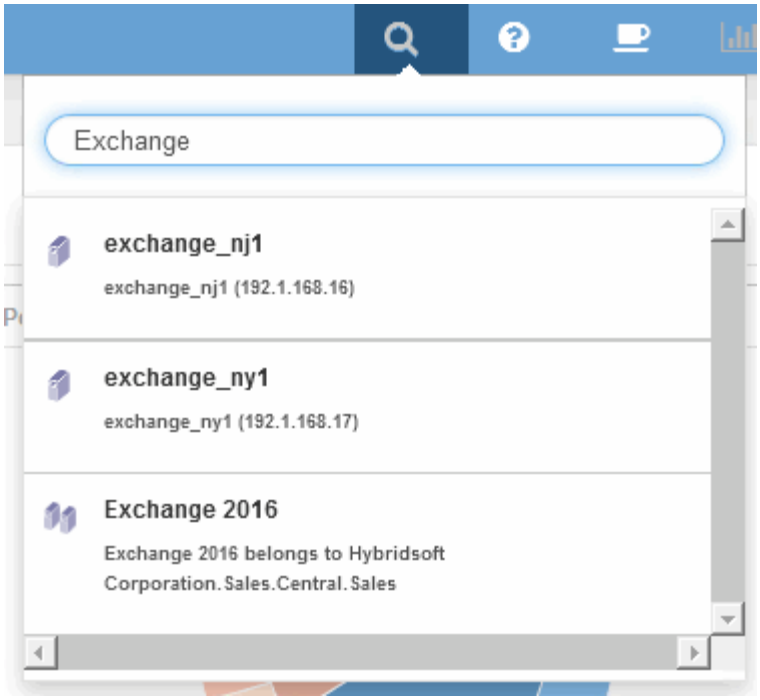
In diesem Dokument werden die Schritte beschrieben, die Sie zur Behebung von Leistungsberichten für eine Anwendung, die sich auf Benutzer oder Administratoren auswirkt, durchführen können. Benutzer beschweren sich beispielsweise darüber, dass ihre Exchange-Anwendung den ganzen Tag über langsam ist.

## Über diese Aufgabe

In OnCommand Insight ist eine Anwendung eine konfigurierte Einheit. Sie weisen der Applikation einen Namen und eine Geschäftseinheit zu und weisen der Applikation Computing- und Storage-Ressourcen zu. Dies ermöglicht einen besseren End-to-End-Überblick über den Zustand der Infrastruktur und ein proaktives Management des Infrastruktur-Asset-Managements.

## Schritte

1. Um mit der Untersuchung des Problems zu beginnen, verwenden Sie die Insight-Symbolleiste, um eine globale Suche nach der Exchange-Anwendung durchzuführen.



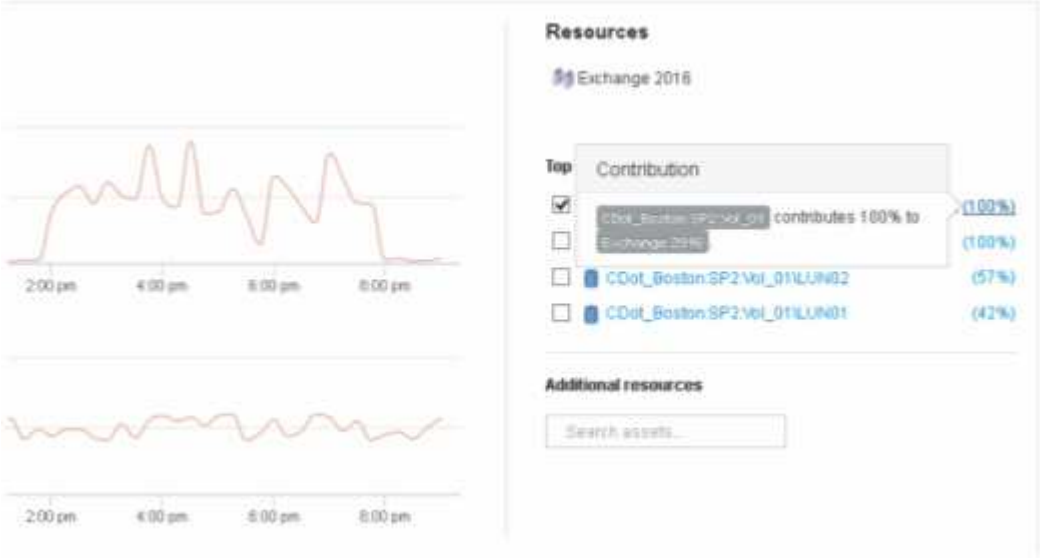

Beim Durchführen einer Suche können Sie vor dem Objektnamen einen Objektdeskriptor hinzufügen, um die Suchergebnisse zu verfeinern.

2. Wenn Sie in den Suchergebnissen „Exchange 2016“ auswählen, wird die Zielseite der Anwendung angezeigt.

Auf der Landing Page der Anwendung sind folgende Informationen von Interesse:

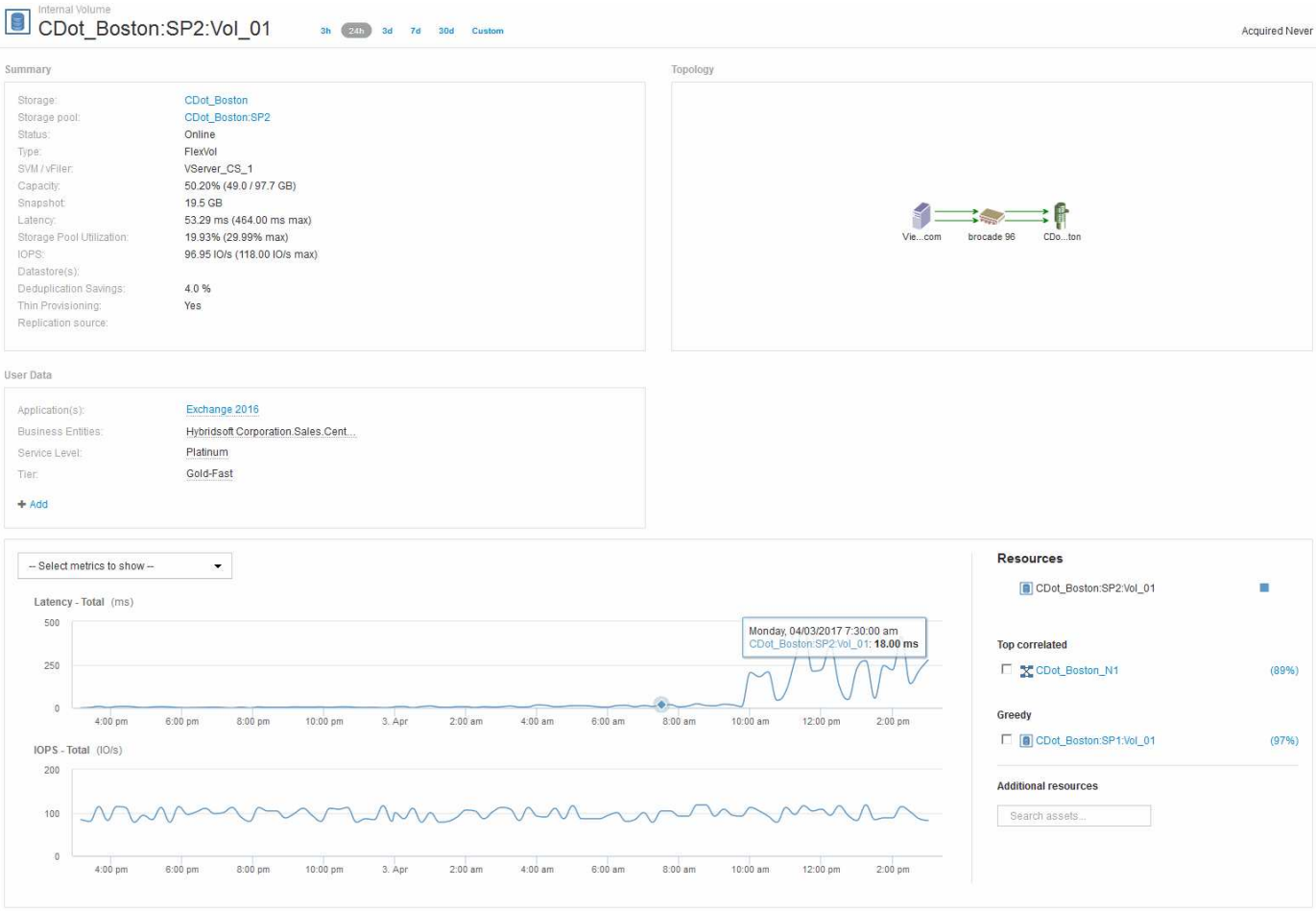
- Im ausgewählten Zeitraum von 24 Stunden wird rechts im Latenzdiagramm eine Erhöhung der Latenz angezeigt.

- Während des Zeitraums der Latenzerhöhungen gibt es keine wesentlichen Änderungen im Niveau der IOPS. Es scheint, dass die Latenzerhöhung nicht durch eine schwerere Anwendungsnutzung verursacht wird. Der Storage-Bedarf, auf den auch die Latenzspitze zählen könnte, ist nicht besonders hoch. Der Anstieg der Latenz kann auf einen externen Faktor zurückzuführen sein.
- Klicken Sie rechts neben den Diagrammen im Abschnitt Top Contributors auf 100% für das ausgewählte interne Volume (CDOT_Boston:SP2:Vol_01). Das System zeigt, dass diese Ressource 100 % zur Exchange 2016 Applikation beiträgt.




- Klicken Sie auf den Navigationslink für dieses interne Volume (CDOT_Boston:SP2:Vol_01), um auf die Zielseite für das interne Volume zuzugreifen. Die Analyse des internen Volumes kann Informationen zur Latenzspitze liefern.

## Untersuchung des internen Volumens



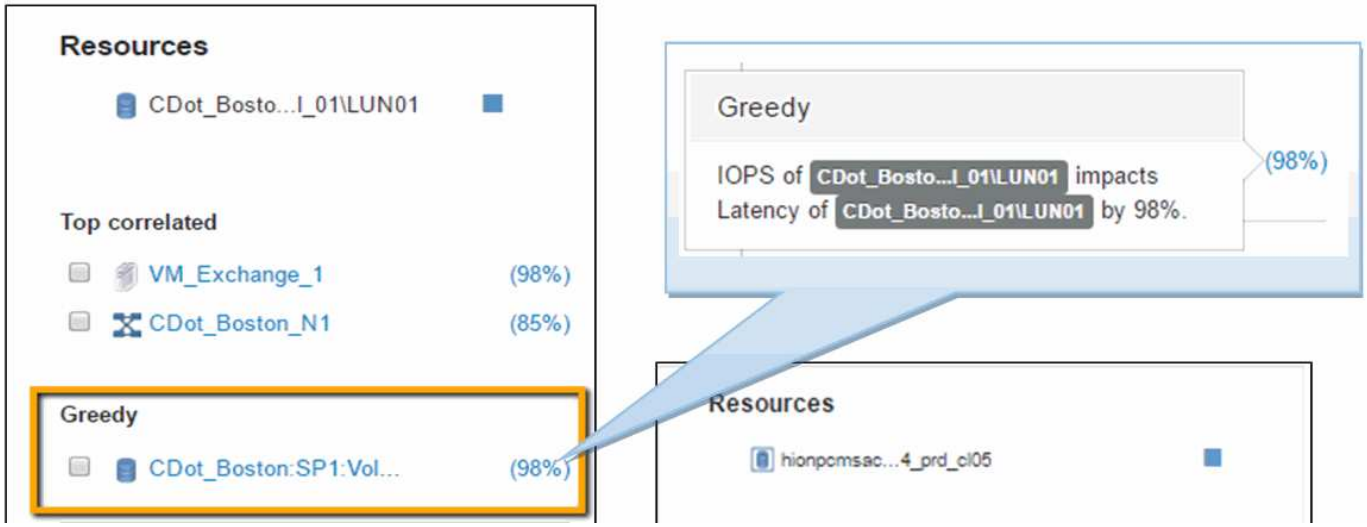

Auf der Landing Page Internes Volume wird Folgendes angezeigt:

- Die Performance-Diagramme des internen Volumes entsprechen den zuvor für die Applikations-Performance sowohl für Latenz als auch für IOPS sichtbaren Werten.
- Im Abschnitt „Ressourcen“, in dem die korrelierten Assets angezeigt werden, wird eine „`gierig`“-Ressource identifiziert (CDOT_Boston:SP1:Vol_01).

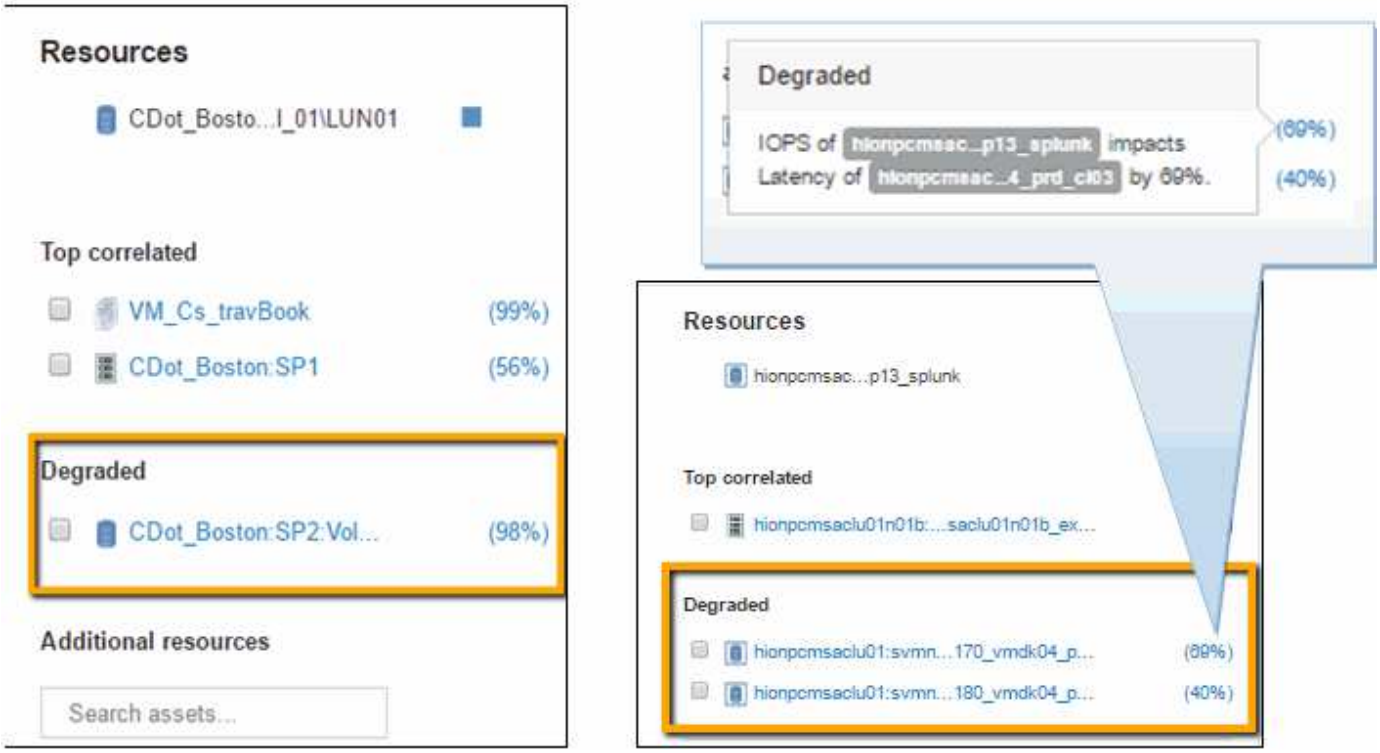
Eine gierige Ressource wird durch Analysen zur Korrelation von Einblicken identifiziert. Gierige/beeinträchtigte Ressourcen sind „`Peers`“, die dieselbe gemeinsame Ressource nutzen. Die übergriffige Ressource verfügt über IOPS-Werte oder Auslastungsraten, die sich negativ auf die IOPS oder die Latenz der beeinträchtigten Ressource auswirken.

Übergriffige und beeinträchtigte Ressourcen lassen sich auf den Landing Pages der Virtual Machine, des Volumes und des internen Volumes ermitteln. Auf jeder Landing Page werden maximal zwei gierige Ressourcen angezeigt.

Die Auswahl des Korrelationsrankings (%) liefert die gierigen Ergebnisse der Ressourcenanalyse. Wenn Sie beispielsweise auf einen übergriffigen Prozentwert klicken, wird der Vorgang für ein Asset identifiziert, das sich auf das beeinträchtigte Asset auswirkt, ähnlich wie im folgenden Beispiel dargestellt.



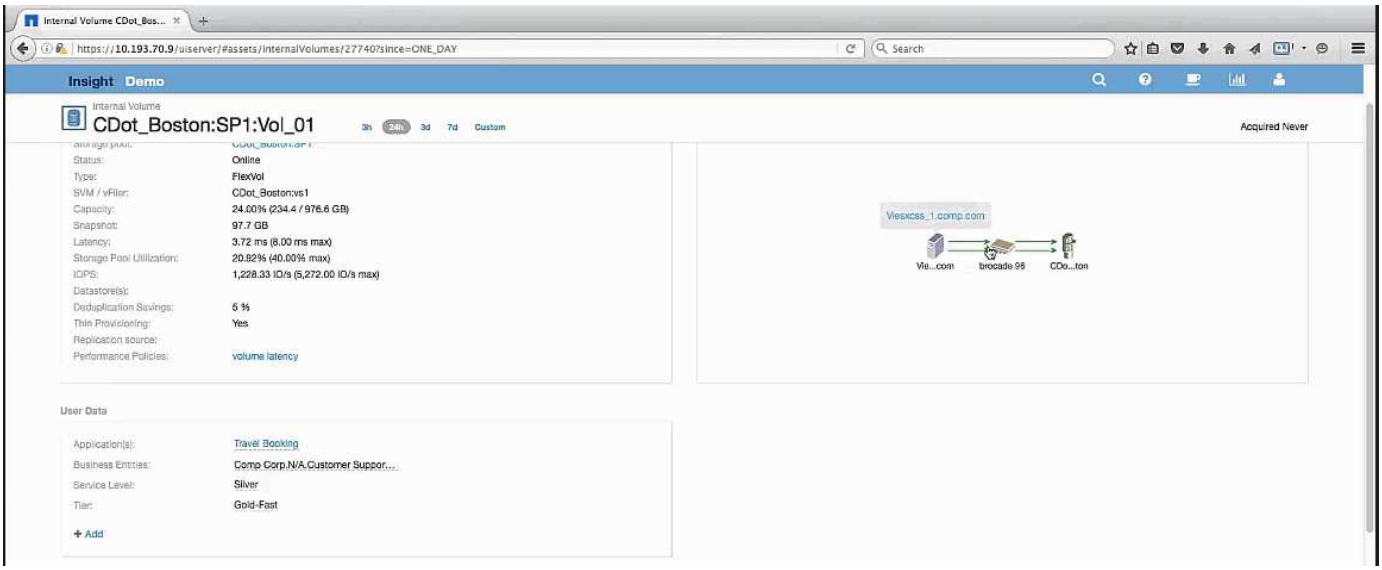

Wenn eine herabgesetzte Ressource erkannt wird, können Sie die Bewertung degraded (%) auswählen, um den Vorgang und die Ressource zu identifizieren, die sich auf die beeinträchtigte Ressource auswirkt.




## Untersuchung der gierigen Ressource

Wenn Sie auf das interne Volume klicken, das als gierige Ressource identifiziert wurde, wird die Landing Page für das Volume CDOT_Boston:SP1:Vol_01 geöffnet.

Hinweis: In der Zusammenfassung ist dieses interne Volume eine Ressource für eine andere Anwendung (Travel Booking) und obwohl es in einem anderen Speicherpool enthalten ist, befindet es sich auf demselben Knoten wie das interne Volume für Exchange 2016 (CDOT_Boston_N1).




Auf der Landing Page wird angezeigt:

- Das interne Volumen, das einer Reisebuchungsanwendung zugeordnet ist.
- In den korrelierten Ressourcen wird ein neuer Speicherpool erkannt.
- Das ursprüngliche interne Volume, das Sie untersucht haben (CDOT_Boston:SP2:Vol_01), wird als „`degradiert`“ gekennzeichnet.
- Im Performance-Diagramm weist die Applikation ein stabiles Latenzprofil auf, das in etwa gleichzeitig einen IOPS-Spitzenwert hat, während der Latenzanstieg in der Exchange Applikation festzustellen ist.

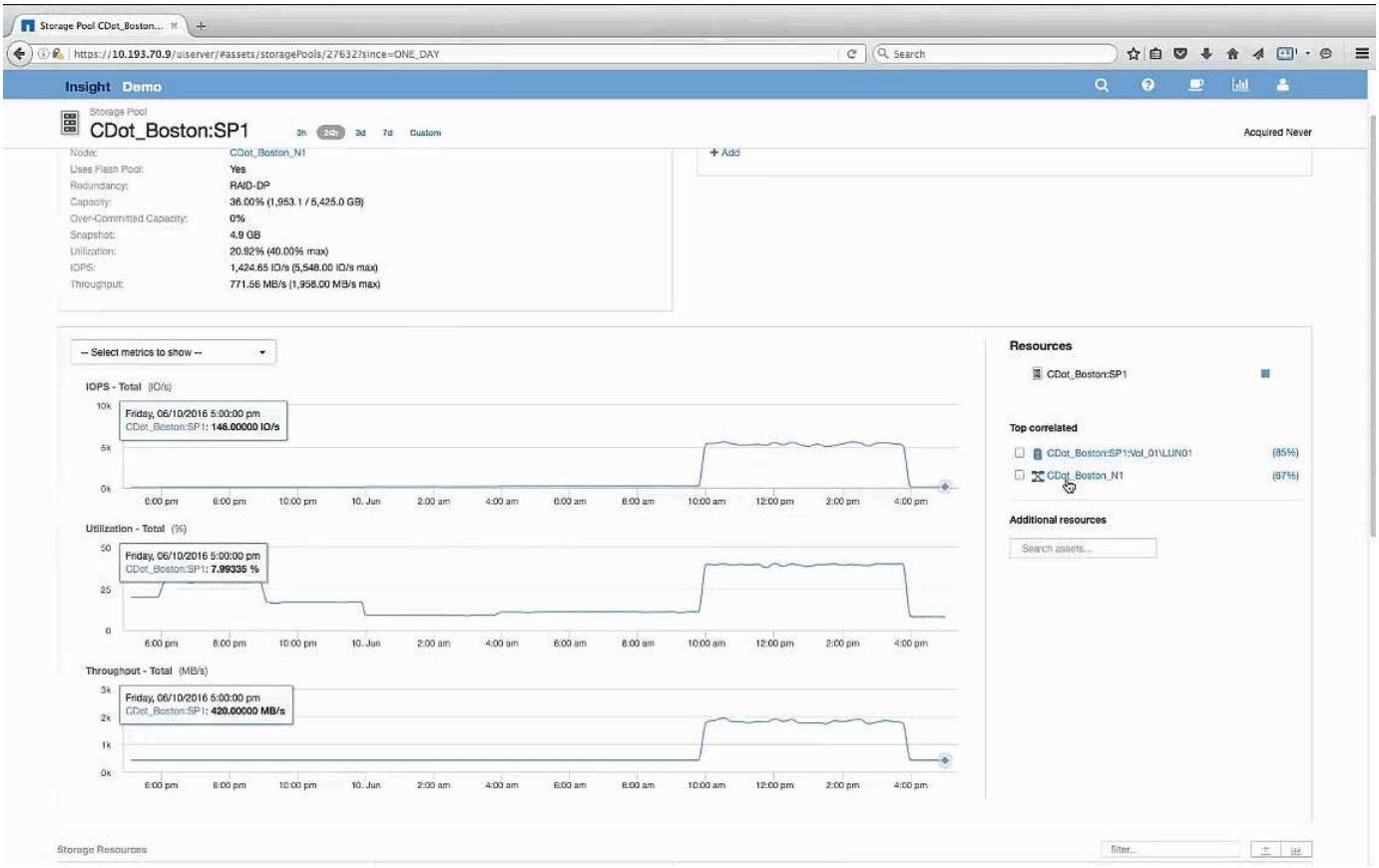
  Dies kann darauf hinweisen, dass die Latenzspitze der Exchange-Applikation wahrscheinlich durch den IOPS-Spitzenwert auf diesem Volume verursacht wird.

Rechts neben den Diagrammen im Abschnitt „Ressource“ wird die korrelierte herabgesetzte Ressource angezeigt, die das interne Exchange 2016-Volume ist (CDOT_Boston:SP2:Vol_01). Klicken Sie auf das Kontrollkästchen, um das beeinträchtigte interne Volume in die Performance-Diagramme aufzunehmen. Wenn Sie die beiden Performance-Diagramme ausrichten, zeigen Sie, dass die Latenz- und IOPS-Spitzen fast zeitgleich auftreten. Dies sagt uns, dass wir ein besseres Verständnis der Travel Booking-Anwendung bekommen wollen. Wir müssen verstehen, warum die Applikation einen so anhaltenden IOPS-Spitzenwert verzeichnet.

Die Untersuchung des mit der Travel Booking-Anwendung verknüpften Speicherpools kann ermitteln, warum die IOPS-Spitzenwerte in der Anwendung auftreten. Klicken Sie auf CDOT_Boston:SP1, um die Landing Page für Storage Pool anzuzeigen.

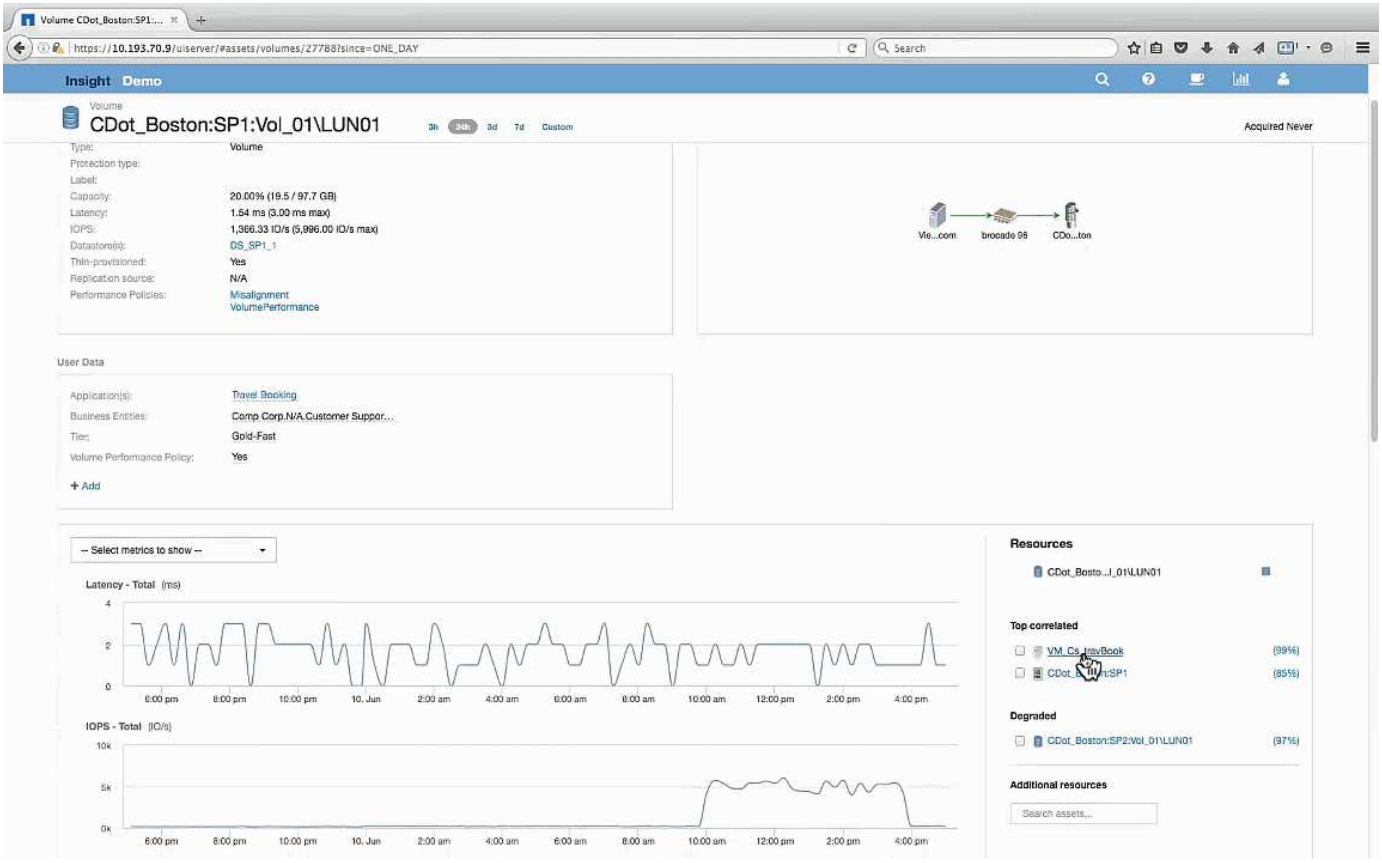
## Untersuchen Sie den Speicherpool

Bei der Untersuchung der Landing Page des Storage-Pools wird die gleiche IOPS-Spitzenauslastung angezeigt, die in den zugehörigen Assets zu beobachten ist. Im Abschnitt „Ressourcen“ sehen Sie, dass diese Landing Page des Speicherpools mit dem Volumen der Reiseanwendung verknüpft ist. Klicken Sie auf das Volume, um die Volume-Landing Page zu öffnen.




## Das Volumen wird untersucht

Die Volume-Landing-Page zeigt dieselbe bekannte IOPS-Spitze wie die zugehörigen Assets.




Im Abschnitt „Ressourcen“ wird die VM für die Anwendung „Reisebuchung“ identifiziert. Klicken Sie auf den Link VM, um die Landing Page der VM anzuzeigen.

## Untersuchen der VM

Wählen Sie auf der Landing Page der VM zusätzliche Metriken aus, die die CPU-Auslastung und Speicherauslastung anzeigen und einschließen. Die Diagramme für die CPU- und Speicherauslastung zeigen, dass beide mit fast 100 % ihrer Kapazität arbeiten. So wird uns mitgeteilt, dass das Problem mit dem Exchange Server kein Storage-Problem ist, sondern das Ergebnis der hohen CPU- und Arbeitsspeicherauslastung für VMs und des damit verbunden Arbeitsspeicheraustauschs von I/O auf die Festplatte.

Um dieses Problem zu lösen, können Sie nach weiteren ähnlichen Ressourcen suchen. Geben Sie im Eingabedialogfeld zusätzliche Ressourcen „`Node`“ ein, um Metriken für Assets anzuzeigen, die der Exchange VM ähnlich sind. Der Vergleich hilft bei der Identifizierung eines Node, der sich besser für das Hosting des Workloads eignet, falls eine Änderung erforderlich ist.

# Erfassen und Reporting von AWS-Abrechnungsdaten

Die Kostendatenquelle Amazon AWS Cloud importiert die von Amazon erstellten Abrechnungsdaten als Integrationsdaten in Insight und steht damit dem Data Warehouse

für die Berichterstellung zur Verfügung.

Es besteht aus drei Teilen, um die Daten zu Cloud-Abrechnungen für Insight verfügbar zu machen:

Überprüfen der AWS Kontoinformationen

Konfigurieren der AWS Cloud-Kostendatenquelle in Insight zur Erfassung der Daten.

Senden der Daten über ETL an Data Warehouse zur Verwendung in Berichten.

## Die Datenerfassung von AWS für Insight wird vorbereitet

Ihr AWS Konto muss ordnungsgemäß konfiguriert sein, damit Insight Cloud-Kostendaten erfassen kann.

### Über diese Aufgabe

Die folgenden Schritte werden über Ihr AWS-Konto durchgeführt. Weitere Informationen finden Sie in der Dokumentation zu Amazon: "http://docs.aws.amazon.com". Wenn Sie das Einrichten eines AWS-Cloud-Kontos nicht kennen, wenden Sie sich an Ihren Cloud-Anbieter.

Diese Schritte werden hier als Höflichkeit zur Verfügung gestellt und gelten zum Zeitpunkt der Veröffentlichung als richtig. NetApp übernimmt keine Garantie für die Richtigkeit dieser Schritte. Wenden Sie sich an Ihren Cloud-Provider oder AWS-Kontoinhaber, um Informationen oder Unterstützung bei der Konfiguration Ihres AWS-Kontos zu erhalten.

Best Practice: Insight empfiehlt, einen primären IAM-Benutzer auf demselben Konto zu erstellen, dem auch der S3-Bucket gehört, in den die Abrechnungsberichte hochgeladen werden. Verwenden Sie diesen Benutzer, um AWS-Abrechnungsdaten zu konfigurieren und zu erfassen.

So konfigurieren Sie Ihr AWS Konto so, dass Insight Daten erfassen kann:

### Schritte

1. Melden Sie sich als IAM-Benutzer (Identity Access Management) bei Ihrem AWS-Konto an. Melden Sie sich für eine ordnungsgemäße Erfassung beim primären IAM-Konto an und nicht bei einem Gruppen-IAM-Konto.
2. Gehen Sie zu **Amazon S3**, um Ihren Bucket zu erstellen. Geben Sie einen eindeutigen Bucket-Namen ein, und überprüfen Sie die richtige Region.
3. Aktivieren Sie Ihren Amazon-Kosten- und Nutzungsbericht. Siehe https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html Zur Information.
   a. Gehen Sie zum AWS **Billing and Cost Management Dashboard**und wählen Sie **Reports**.
   b. Klicken Sie auf **Report erstellen** und geben Sie den Berichtsnamen ein. Wählen Sie für **Zeiteinheit** die Option Täglich. Aktivieren Sie das Kontrollkästchen, um **Ressourcen-IDs** einzuschließen, und klicken Sie auf **Weiter**.
   c. Klicken Sie auf den Link **Beispielrichtlinie** auf der Seite Lieferoptionen auswählen. Kopieren Sie den Text der Beispielrichtlinie im Feld in die Zwischenablage. Klicken Sie Auf **Schließen**.
   d. Gehen Sie zurück zum erstellten S3-Bucket, klicken Sie auf die Registerkarte **Berechtigungen** und wählen Sie die Schaltfläche **Bucket Policy**.
   e. Fügen Sie den Text aus der Beispielrichtlinie ein, und ersetzen Sie ihn `<bucketname>` Geben Sie den

tatsächlichen Bucket-Namen in jeder Zeile ein, die Folgendes enthält: `"Resource": "arn:aws:s3:: <bucketname>"`. **Speichern** die Politik.

f. Kehren Sie zum Bildschirm Bericht erstellen zurück, geben Sie Ihren S3-Bucket ein und klicken Sie auf die Schaltfläche **Verify**. Klicken Sie Auf **Weiter**.

g. Überprüfen Sie Ihre Informationen und klicken Sie auf **Überprüfen und vervollständigen**.

4. Damit Insight Daten aus AWS erfassen kann, müssen Sie die entsprechenden Berechtigungen erteilen. Der folgende Link bietet Details dazu, wie Sie Berechtigungen für **Alle Buckets auflisten** (Schritt 4.1) und Berechtigungen für die Objekte im Ordner festlegen (Schritt 5.2): https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html.
5. Gehen Sie in der IAM-Konsole zu **Policies** und klicken Sie auf **Create Policy**.
6. Geben Sie einen Namen in das Feld **Richtlinienname** ein, und klicken Sie unten auf **Richtlinie erstellen**.
7. Wählen Sie in der IAM-Konsole Ihren Benutzer aus, und wählen Sie dann unten im Bildschirm **Inline-Richtlinie hinzufügen** aus.
8. Klicken Sie auf **Service auswählen** und wählen Sie S3.
9. Gehen Sie auf die Registerkarte **JSON**. Kopieren Sie den JSON-Beispieltext aus Schritt 5.1.2.g der AWS Walkthrough in das JSON-Feld.
10. Ersetzen Sie die Felder *companybucket* und *Development* in der JSON durch Ihre S3-Informationen.
11. Klicken Sie auf **Richtlinie prüfen**, um Ihre Richtlinieneinstellungen zu überprüfen.

## Konfiguration der AWS Cloud Cost-Datenquelle

Sie konfigurieren die AWS Cloud-Kostendatenquelle wie für jede Insight Datenquelle.

### Bevor Sie beginnen

Sie müssen Ihr Amazon AWS Konto bereits eingerichtet und auf die Datenerfassung bei Insight vorbereitet haben und über die folgenden Informationen verfügen.

- Berichtsname
- S3-Bucket-Name
- AWS Region, in der sich der S3-Bucket befindet.
- Präfix für Berichtspfad

### Über diese Aufgabe

Sobald Ihr AWS Konto bereit ist und über die entsprechenden Berechtigungen verfügt, können Sie OnCommand Insight so konfigurieren, dass Daten für den Rechnungsbericht erfasst werden.

Sie müssen für jeden abrechnungsfähigen Benutzer/Konto, von dem Sie Rechnungsdaten abrufen möchten, eine separate AWS Cloud-Kostendatenquelle hinzufügen.

### Schritte

1. Melden Sie sich als Administrator bei OnCommand Insight an.
2. Klicken Sie auf **Admin** > **Data Sources**, um die Seite Insight Data Source zu öffnen.
3. Klicken Sie auf **+Add**, um eine neue Datenquelle hinzuzufügen. Wählen Sie **Amazon** und dann **AWS**

**Cloud Cost** aus.

4. Geben Sie im Abschnitt **Konfiguration** den Namen des Berichts_, *S3 Bucket* Name, *S3 Region* (muss die Region sein, in der sich der S3-Bucket befindet), *Report path PREFIX*, *AWS IAM Access Key ID* und *AWS IAM Secret Access Key* ein. Wenn Sie sich über diese Fragen nicht sicher sind, wenden Sie sich an Ihren Cloud-Provider oder AWS-Kontoinhaber.
5. Aktivieren Sie das Kontrollkästchen, um zu überprüfen, ob AWS Sie für API-Anfragen und Datentransfers, die von der Insight Datenquelle vorgenommen werden, in Rechnung stellt.
6. Geben Sie unter **Advanced Configuration** das HTTP-Verbindungs- und Socket-Timeout ein. Der Standardwert beträgt 300 Sekunden.
7. Klicken Sie Auf **Speichern**.

## AWS Cloud-Kostendaten in Insight verarbeiten

Insight erfasst einmal pro Monat Daten aus dem AWS Abrechnungsbericht für den Vormonat und gibt die endgültigen Cloud-Kosten für diesen Monat wieder.

Wenn Sie nach der Einrichtung Ihrer AWS Cloud-Kostendatenquelle(n) bereits Abrechnungsberichte für S3 generiert haben, erhalten Sie unmittelbar nach der ersten Datenquellabfrage bis zu drei Monate vergangene Daten.

Insight erfasst einmal pro Monat AWS- „`final`“-Daten. Diese Erfassung erfolgt einige Tage nach Abschluss des Vormonats, sodass AWS Zeit hat, die tatsächlichen Daten abzuschließen.

Rechnungsdaten für AWS werden zur Berichterstellung an das Data Warehouse von Insight gesendet.

Beachten Sie, dass jede Datenquelle für ein einzelnes abrechenbares Konto/Benutzer konfiguriert werden muss.

## Berichte zu Cloud-Kostendaten in Insight

Die in Insight erfassten monatlichen Cloud-Kosten werden an das Data Warehouse gesendet, das über das Cloud-Kostendatamart zur Verwendung in Berichten zur Verfügung steht.

### Bevor Sie beginnen

Sie müssen Datenquellen konfiguriert haben, um Cloud-Kostendaten aus AWS zu erfassen. Jeder abrechenbare Benutzer/jedes abrechenbare Konto muss über eine separate Datenquelle verfügen.

Warten Sie mindestens 36 Stunden, bis Insight mit dem Erfassen von Daten beginnt.

Lassen Sie ETL nach dieser Zeit mindestens einmal ausführen, um die Daten an das Data Warehouse zu senden.

### Über diese Aufgabe

Nachdem Ihre Daten erfasst und an das Data Warehouse gesendet wurden, können Sie sie in einem der verschiedenen vorkonfigurierten Berichte anzeigen oder benutzerdefinierte Berichte erstellen. Insight speichert die Daten im eigenen Cloud-Kostendatamart.

So zeigen Sie Ihre Cloud-Kostendaten in einem der vorkonfigurierten Berichte an:

### Schritte

1. Öffnen Sie Insight Reporting mit einer der folgenden Methoden:
   - Klicken Sie auf das Symbol Reporting Portal In der Web-UI des Insight-Servers oder in der Data Warehouse-Benutzeroberfläche.
   - Starten Sie die Berichterstellung direkt, indem Sie die folgende URL eingeben: `https://<dwh_server_name\>:9300/p2pd/servlet/dispatch` Oder `https://<dwh_server_name\>:9300/bi` `(7.3.3 and later)`
2. Sobald Sie bei Reporting angemeldet sind, klicken Sie auf **Öffentliche Ordner** und wählen **Cloud-Kosten**.
3. Sie können Ihre AWS-Abrechnungsdaten in den verfügbaren Berichten im Ordner **Cloud Cost** einsehen oder Ihren eigenen benutzerdefinierten Bericht mit dem **Cloud Cost Datamart** erstellen, das im Ordner **Packages** verfügbar ist.

### Rolle auswerten

Vor der Integration in Insight müssen Sie Ihre ServiceNow Rolle zu Security_admin erweitern.

#### Schritte

1. Melden Sie sich mit Administratorrechten bei Ihrer ServiceNow-Instanz an.
2. Wählen Sie im Dropdown-Menü **Systemadministrator** die Option **Rollen heben** aus, und heben Sie Ihre Rolle auf Security_admin an. Klicken Sie auf OK.

### Update-Set installieren

Im Rahmen der Integration von ServiceNow und OnCommand Insight müssen Sie einen Updatesatz installieren, der vorkonfigurierte Daten in ServiceNow lädt, um dem Konnektor spezifische Felder und Tabellen zum Extrahieren und Laden von Daten bereitzustellen.

#### Schritte

1. Navigieren Sie in ServiceNow zur Tabelle für Remote-Update-Sets, indem Sie nach „`abgerufene Update-Sets`“ suchen.
2. Klicken Sie auf **Update Set aus XML importieren**.
3. Der Updatensatz befindet sich in der zuvor auf Ihr lokales Laufwerk heruntergeladenen Python-Connector-ZIP-Datei (in unserem Beispiel die `C:\OCI2SNOW` Ordner) im `\update_sets` Unterordner. Klicken Sie auf **Datei auswählen** und wählen Sie die .XML-Datei in diesem Ordner aus. Klicken Sie Auf **Upload**.
4. Sobald der Update-Satz geladen ist, öffnen Sie ihn und klicken Sie auf **Preview Update Set**.

   Wenn Fehler erkannt werden, müssen Sie sie korrigieren, bevor Sie den Aktualisierungssatz übertragen können.

5. Wenn keine Fehler vorliegen, klicken Sie auf **Update Set übertragen**.

   Sobald der Update-Satz übergeben wurde, wird er auf der Seite **System-Update-Sets** > **Update-Quellen** angezeigt.

### ServiceNow Integration - Benutzer einrichten

Sie müssen einen ServiceNow-Benutzer einrichten, damit Insight eine Verbindung zu den Daten herstellen und diese synchronisieren kann.

#### Über diese Aufgabe

#### Schritte

1. Erstellen Sie ein Servicekonto in ServiceNow. Melden Sie sich bei ServiceNow an und navigieren Sie zu **Systemsicherheit** > **Benutzer und Gruppen** > **Benutzer**. Klicken Sie auf **Neu**.
2. Geben Sie einen Benutzernamen ein. In diesem Beispiel verwenden wir „`OCI2SNOW`“ als Integrationsbenutzer. Geben Sie ein Kennwort für diesen Benutzer ein.

   In dieser Anleitung verwenden wir in der gesamten Dokumentation einen Servicekontobenutzer namens „`OCI2SNOW`“`. Sie können ein anderes Servicekonto verwenden, aber stellen Sie sicher, dass es in Ihrer gesamten Umgebung konsistent ist.

3. Klicken Sie mit der rechten Maustaste auf die Menüleiste und klicken Sie auf **Speichern**. Dadurch können Sie auf diesem Benutzer bleiben, um Rollen hinzuzufügen.
4. Klicken Sie auf **Bearbeiten** und fügen Sie diesem Benutzer folgende Rollen hinzu:
   - Asset
   - Import_Transformator
   - Rest_Service
5. Klicken Sie Auf **Speichern**.
6. Dieser Benutzer muss zu OnCommand Insight hinzugefügt werden. Melden Sie sich bei Insight als Benutzer mit Administratorberechtigungen an.
7. Navigieren Sie zu **Admin** > **Setup** und klicken Sie auf den Reiter **Users**.
8. Klicken Sie auf die Schaltfläche **Aktionen** und wählen Sie **Benutzer hinzufügen**.
9. Geben Sie als Name „`OCI2SNOW`“ ein. Wenn Sie oben einen anderen Benutzernamen verwendet haben, geben Sie diesen Namen hier ein. Geben Sie dasselbe Kennwort ein, das Sie für den Benutzer ServiceNow oben verwendet haben. Sie können das E-Mail-Feld leer lassen.
10. Weisen Sie diesem Benutzer die Rolle **User** zu. Klicken Sie Auf **Speichern**.

### Installieren Sie Python und Bibliotheken

Python kann auf dem Insight Server oder auf einem Standalone Host oder einer VM installiert werden.

#### Schritte

1. Laden Sie auf Ihrem VM oder Host Python 3.6 oder höher herunter.
2. Wählen Sie eine benutzerdefinierte Installation aus, und wählen Sie die folgenden Optionen aus. Diese sind entweder für den ordnungsgemäßen Betrieb des Konnektors erforderlich oder werden dringend empfohlen.
   - Startprogramm für alle Benutzer installieren

- Fügen Sie Python zum PFAD hinzu
- Installieren von Pip (wodurch Python andere Pakete installieren kann)
- Installieren Sie TK/tcl und IM LEERLAUF
- Installieren Sie die Python Test Suite
- Installieren Sie py Launcher für alle Benutzer
- Dateien mit Python verknüpfen
- Erstellen Sie Verknüpfungen für installierte Anwendungen
- Fügen Sie Python zu Umgebungsvariablen hinzu
- Standardbibliothek vorkompilieren

3. Nachdem Python installiert wurde, installieren Sie die Python-Bibliotheken “reQuests” und “psnow”. Führen Sie den folgenden Befehl aus: `python -m pip install requests pysnow`

   **HINWEIS:** dieser Befehl kann fehlschlagen, wenn Sie in einer Proxy-Umgebung arbeiten. Um dieses Problem zu umgehen, müssen Sie jede der Python-Bibliotheken manuell herunterladen und die Installationsanforderungen nacheinander und in der richtigen Reihenfolge ausführen.

   Der Befehl installiert mehrere Dateien.

4. Überprüfen Sie, ob die Python-Bibliotheken richtig installiert sind. Starten Sie Python mit einer der folgenden Methoden:
   - Öffnen Sie eine cmd-Eingabeaufforderung, und geben Sie ein `python`
   - Öffnen Sie unter Windows **Start** und wählen Sie **Python** > **Python-<version>.exe**
5. Geben Sie an der Python-Eingabeaufforderung ein `modules`

   Python wird Sie bitten, einen Moment zu warten, während es eine Liste von Modulen sammelt, die dann angezeigt werden.

#### Einrichtung von Python Middleware

## Nachdem Python und die erforderlichen Bibliotheken installiert sind, können Sie den Middleware Connector für die Kommunikation mit OnCommand Insight und ServiceNow konfigurieren.

##### Schritte

1. Öffnen Sie auf dem Host oder der VM, auf dem Sie die Connector-Software heruntergeladen haben, als Administrator ein Befehlsfenster und wechseln Sie zur `\OCI2SNOW\` Ordner.
2. Sie müssen das Skript initialisieren, um eine leere **config.ini**-Datei zu erzeugen. Führen Sie den folgenden Befehl aus: `oci_snow_sync.pyz init`
3. Öffnen Sie die **config.ini**file in einem Texteditor und nehmen Sie im Abschnitt [OCI] folgende Änderungen vor:
   - Setzen Sie url auf <code><a href="https://<name.domain&gt" class="bare">https://<name.domain&gt</a>;</code> Oder <code><a href="https://<ip" class="bare">https://<ip</a> address></code> Für die Insight Instanz.
   - Setzen Sie **user** und **password** auf den Insight-Benutzer, z.B. OCI2SNOW.

- Setzen Sie **include_off_vms** auf **false**

4. Nehmen Sie im Abschnitt [SCHNEE] folgende Änderungen vor:
   - Setzen Sie **instance** auf den FQDN oder die ip-Adresse für Ihre ServiceNow-Instanz
   - Setzen Sie **User** und **Password** auf den ServiceNow-Servicekontonutzer, zum Beispiel den OCI2SNOW.
   - Setzen Sie unter **field für die OCI-URL** das Feld **url** auf „`U_oci_url`“. Dieses Feld wird als Teil des Konnektor-OCI-Updatungssatzes erstellt. Sie können dies in der Kundenumgebung ändern, aber wenn Sie dies tun, müssen Sie es hier und in ServiceNow ändern. Als Best Practice empfiehlt es sich, dieses Feld so zu lassen wie es ist.
   - Setzen Sie das Feld **Filter_Status** auf „`installed, in Stock`“. Wenn Sie einen anderen Status haben, müssen Sie diesen Status hier festlegen, damit alle Datensätze vor dem Hochladen neuer Datensätze mit den Insight-Datensätzen übereinstimmen. In den meisten Fällen sollte dieses Feld unverändert bleiben.
   - Setzen Sie **Ind_Status**auf „`Retired`“.
5. Der Abschnitt [Proxy] ist nur erforderlich, wenn Sie einen Proxyserver verwenden. Wenn Sie diesen Abschnitt verwenden müssen, stellen Sie die folgenden Einstellungen sicher:
   - ;Https = http://<host>:<port>
   - ;Http = http://<host>:<port>
   - ;Include_oci = true
   - ;Include_Snow = wahr
6. Bearbeiten Sie den Abschnitt [Protokoll] nur, wenn Sie detailliertere Debug-Informationen benötigen.
7. Um den Konnektor zu testen, öffnen Sie als Administrator eine cmd-Eingabeaufforderung und wechseln Sie in den Ordner \OCI2SNOW. Führen Sie den folgenden Befehl aus: `oci_snow_sync.pyz test`

   Details finden Sie im `logs\` Ordner.

#### Verbindung wird synchronisiert

Sobald ServiceNow, Insight und der Connector ordnungsgemäß konfiguriert sind, können Sie den Connector synchronisieren.

##### Schritte

1. Öffnen Sie eine cmd-Eingabeaufforderung, und wechseln Sie in den Ordner \OCI2SNOW.
2. Führen Sie den folgenden Befehl zweimal aus. Bei der ersten Synchronisierung werden die Elemente aktualisiert, bei der zweiten Synchronisierung werden die Beziehungen aktualisiert: `oci_snow_sync.pyz sync`
3. Vergewissern Sie sich, dass die Tabelle Storage Server in Ihrer ServiceNow-Instanz ausgefüllt ist. Öffnen Sie einen Speicherserver, und überprüfen Sie, ob die mit diesem Speicher verbundenen Ressourcen aufgelistet sind.

#### Planen der täglichen Synchronisierung

Sie können den Windows-Taskplaner verwenden, um den ServiceNow-Konnektor automatisch zu synchronisieren.

**Über diese Aufgabe**

Die automatische Synchronisierung stellt sicher, dass Insight-Daten regelmäßig zu ServiceNow verschoben werden. Sie können jede Methode für die Planung verwenden. Die folgenden Schritte verwenden den Windows-Taskplaner, um die automatische Synchronisierung durchzuführen.

**Schritte**

1. Klicken Sie auf dem Windows-Bildschirm auf **Start** und geben Sie **Run** > **Task Scheduler** ein.
2. Klicken Sie Auf **Grundaufgabe Erstellen…**
3. Geben Sie einen aussagekräftigen Namen ein, z. B. „`OCI2SNOW Connector Sync`“. Geben Sie eine Beschreibung der Aufgabe ein. Klicken Sie Auf **Weiter**.
4. Wählen Sie diese Option, um die Aufgabe * täglich* auszuführen. Klicken Sie Auf **Weiter**.
5. Wählen Sie eine Tageszeit aus, um die Aufgabe auszuführen. Klicken Sie Auf **Weiter**.
6. Wählen Sie unter Aktion * Programm starten*. Klicken Sie Auf **Weiter**.
7. Geben Sie im Feld **Program/script** ein `C:\OCI2SNOW\oci_snow_sync_pyz`. Geben Sie im Feld **Argumente** ein `sync`. Geben Sie im Feld **Start in** ein `C:\OCI2SNOW`. Klicken Sie auf **weiter**.
8. Überprüfen Sie die Zusammenfassungsdetails, und klicken Sie auf **Fertig stellen**.

   Die Synchronisierung wird nun täglich ausgeführt.

# OCI Data Collector: Support Matrix

Die Data Collector Support Matrix bietet Referenz für Data Collectors, die von OCI unterstützt werden, einschließlich Hersteller- und Modellinformationen.

## HP Enterprise 3PAR / Alletra 9000 / Primera StoreServ Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| HPE_3PAR 20450 HPE_3PAR 7200 HPE_3PAR 7400 HPE_3PAR 7440C HPE_3PAR 7450C HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR A670 HP_3PAR 7200 HP_3PAR 7200C HP_3PAR 7400 HP_3PAR 7400C HP_3PAR 7450C HP_3PAR 8200 HP_3PAR 8440 | 3.2.2 (MU2) 3.2.2 (MU4) 3.2.2 (MU6) 3.3.1 (MU2) 3.3.1 (MU5) 4.4.1 Auslösetyp: Standard Support Release |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
| --- | --- | --- | --- | --- | --- |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Storage-Port | Implementiert | SSH | |
| | Volumenreferenz | Name | Implementiert | SSH | |
| | | Storage-Ip | Implementiert | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Verhältnis | | | |
| | | Server-ID | Implementiert | SMI-S | |
| **Produkt** | **Kategorie** | **Funktion/Attribut lesen** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Gesamtdurchsatz | Implementiert | SMI-S | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SMI-S | |
| | | „Ausstehend“ | Implementiert | SMI-S | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| 3PAR SMI-S | SMI-S | HTTP/HTTPS | 5988/5989 | | Richtig | Richtig | Richtig | Richtig |
| 3PAR-CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

# Amazon AWS EC2

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- 1 2014-10-01

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Disk | VirtualisierungsDisk OID | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Virtual Machine | Implementiert | HTTPS | |
| | Host | Host-Betriebssystem | Implementiert | HTTPS | |
| | | IPS | Implementiert | HTTPS | |
| | | Hersteller | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | OID | Implementiert | HTTPS | |
| | Info | Api-Beschreibung | Implementiert | HTTPS | |
| | | Api-Name | Implementiert | HTTPS | |
| | | Api-Version | Implementiert | HTTPS | |
| | | Name der Datenquelle | Implementiert | HTTPS | Info |
| | | Datum | Implementiert | HTTPS | |
| | | Ersteller-ID | Implementiert | HTTPS | |
| | | Erstellschlüssel | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EC2 API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# Brocade Fibre Channel Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 184.0 Brocade 200E Brocade 300E Brocade 4024 Embedded Brocade 4100 Brocade 4900 Brocade 5000 Brocade 5100 Brocade 6510 Brocade 6520 Embedded Brocade 7800 Brocade 5300 Brocade 5480 Brocade 6505 Brocade 7840 Brocade DCX8510-4 Brocade DCX8510-8 Brocade G610 Brocade G620 Brocade G630 Brocade M5224 Embedded Brocade M6505 Brocade VA-40FC Brocade X6-4 Brocade X6-8 Brocade X7-8 | v5.3.0a v6.1.0c v6.1.0h v6.2.1b v6.2.1b v6.2.2f v6.2.2f v6.3.2b v6.4.1b v6.4.1b v6.4.2b1 v7.0.2c v7.2.1c v7.2.1c v7.2.1d v8.2 01 857687 01 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Gigabits | | | |
|---|---|---|---|---|---|
| | | Unbekannte Konnektivität | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Switch | Domänen-Id | Implementiert | SSH | |
| | | Firmware-Version | Implementiert | SSH | |
| | | IP | Implementiert | SSH | |
| | | URL managen | Implementiert | SSH | |
| | | Hersteller | Implementiert | SSH | |
| | | Modell | Implementiert | SSH | |
| | | Name | Implementiert | Manuelle Eingabe | |
| | | Seriennummer | Implementiert | SSH | |
| | | Switch-Rolle | Implementiert | SSH | |
| | | Switch-Status | Implementiert | SSH | |
| | | Switch-Status | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | | VSAN aktiviert | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |
| | Zone | Zonenname | Implementiert | SSH | |
| | Zonenmitglied | Typ | Lücke | SSH | |
| | | WWN | Implementiert | SSH | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | SSH | |
| | | Konfigurationsname | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Port-Fehler | Implementiert | SNMP | Port-Fehler signalisieren Verlust |
| | | Port-Fehler | Implementiert | SNMP | Port-Fehler synchronisierung |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Port-Fehler: Zeitüberschreitung Bei Der Übertragung Des Discard-Moduls | Implementiert | SNMP | Port-Fehler Zeitüberschreitung Verwerfen |
| | | Gesamtanzahl Der Portfehler | Implementiert | SNMP | Gesamtanzahl an Port-Fehlern |
| | | Server-ID | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Gesamte Traffic Frame Rate | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Durchschnittliche Bildgröße | Implementiert | SNMP | Durchschnittliche Größe des Datenverkehrs |
| | | TX-Rahmen | Implementiert | SNMP | Durchschnittliche Größe des Verkehrsaufkommens |
| | | Rate Des Verkehrsaufkommens | Implementiert | SNMP | |
| | | Gesamte Datenverkehrrate | Implementiert | SNMP | |
| | | Übertragungsrate Des Datenverkehrs | Implementiert | SNMP | |
| | | Auslastung Des Erfressenen Datenverkehrs | Implementiert | SNMP | |
| | | Gesamtauslastung Des Datenverkehrs | Implementiert | SNMP | Gesamte Traffic-Auslastung |
| | | Auslastung Des Datenverkehrs | Implementiert | SNMP | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Brocade SNMP | SNMP | SNMPv1, SNMPv2 UND SNMPv3 | 161 | | Richtig | Richtig | Richtig | Richtig |
| Brocade SSH | SSH | SSH | 22 | | Falsch | Falsch | Richtig | Richtig |
| Konfiguration des Datenquellenassistenten | Manuelle Eingabe | | | | Richtig | Richtig | Richtig | Richtig |

# Brocade Network Advisor HTTP

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- 14.4.5

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | Fabric | Name | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Info | Api-Beschreibung | Implementiert | HTTP/S | |
| | | Api-Name | Implementiert | HTTP/S | |
| | | Api-Version | Implementiert | HTTP/S | |
| | | Name der Datenquelle | Implementiert | HTTP/S | Info |
| | | Datum | Implementiert | HTTP/S | |
| | | Ersteller-ID | Implementiert | HTTP/S | |
| | | Erstellschlüssel | Implementiert | HTTP/S | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTP/S | |
| | | Objekttyp | Implementiert | HTTP/S | |
| | | Quelle | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Zone | Zonenname | Implementiert | HTTP/S | |
| | Zonenmitglied | Typ | Lücke | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | HTTP/S | |
| | | Konfigurationsname | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Port | BB Credit Null Gesamt | Implementiert | HTTP/S | BB Credit Null Gesamt |
| | | BB Credit Zero übertragen | Implementiert | HTTP/S | BB Credit Zero übertragen |
| | | BB Credit Zero MS übertragen | Implementiert | HTTP/S | BB Credit Zero MS übertragen |
| | | Port-Fehler Klasse 3 Verwerfen | Implementiert | HTTP/S | |
| | | Port-Fehler Crc | Implementiert | HTTP/S | Port-Fehler Crc |
| | | Port-Fehler Enc In | Implementiert | HTTP/S | Port-Fehler Enc In |
| | | Port-Fehler Kurzer Rahmen | Implementiert | HTTP/S | Port-Fehler aufgrund des kurzen Rahmens |
| | | Verbindungsfehler Bei Portfehlern | Implementiert | HTTP/S | Verbindungsfehler bei Port-Fehlern |
| | | Signalverlust Bei Port-Fehler | Implementiert | HTTP/S | Port-Fehler signalisieren Verlust |
| | | Port-Fehler Sync-Verlust | Implementiert | HTTP/S | Port-Fehler Synchronisierungsverlust |
| | | Port-Fehler: Zeitüberschreitung Bei Der Übertragung Des Discard-Moduls | Implementiert | HTTP/S | Port-Fehler Zeitüberschreitung Verwerfen |
| | | Gesamtanzahl Der Portfehler | Implementiert | HTTP/S | Gesamtanzahl an Port-Fehlern |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Brocade Network Advisor REST-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# Cisco MDS und Nexus Fabric Switches

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| C97148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148 DS-C9148 DS-C9559 DS-C9488 DS-C9559 DS-C969148T C9 DS-C9559 DS-C966K9 DS-C9509 DS-C9 8978 2 | 3.2 6.2 7.1 7.3 11 7.3 7 8.1 2 8.4 8.4(2c) 9 4 7.3 7.3 7 7.3 8.3 8.4 8.4 8.4(3a) 23 6.2 33 6.2 7.3 7.3 13 7.3 8 8.3 8.4 8.4(1a) 6.2(6.2)N1(3.13e) 6.2(21)N2(4.04i) 29(17)N2(4.13j) 6.2(6.2)N1(4.21k) 6.2(1) 15(19) N1(6.2) 6.2(1) 13(8g) 6.2(5.2)N1(41a) 6.2(5.2)6.2)5.2(5.2) 5.2) 8(3) 5.2) 3) 5.0) 5.0(5.0) 3) 5.0) 3(5.0) 3) 4.1 8.4 8.4 8.5 9.2 2 9.3 9.3 2 9.3 9.4) |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | SNMP | |
| | | VSAN aktiviert | Implementiert | SNMP | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | WWN | Implementiert | SNMP | |
| | WWN-Alias | Host-Aliase | Implementiert | SNMP | |
| | | Objekttyp | Implementiert | SNMP | |
| | | Quelle | Implementiert | SNMP | |
| | | WWN | Implementiert | SNMP | |
| | Zone | Zonenname | Implementiert | SNMP | |
| | | Zonentyp | Implementiert | SNMP | |
| | Zonenmitglied | Typ | Lücke | SNMP | |
| | | WWN | Implementiert | SNMP | |
| | Zonenfunktionen | Aktive Konfiguration | Implementiert | SNMP | |
| | | Konfigurationsname | Implementiert | SNMP | |
| | | Standardverhalten Für Zoneneinzug | Implementiert | SNMP | |
| | | Steuerung Zusammenführen | Implementiert | SNMP | |
| | | WWN | Implementiert | SNMP | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | Discard-Moduls | | | |
|---|---|---|---|---|---|
| | | Gesamtanzahl Der Portfehler | Implementiert | SNMP | Gesamtanzahl an Port-Fehlern |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Gesamte Traffic Frame Rate | Implementiert | SNMP | |
| | | Verkehrsrahmenrate | Implementiert | SNMP | |
| | | Durchschnittliche Bildgröße | Implementiert | SNMP | Durchschnittliche Größe des Datenverkehrs |
| | | TX-Rahmen | Implementiert | SNMP | Durchschnittliche Größe des Verkehrsaufkommens |
| | | Rate Des Verkehrsaufkommens | Implementiert | SNMP | |
| | | Gesamte Datenverkehrrate | Implementiert | SNMP | |
| | | Übertragungsrate Des Datenverkehrs | Implementiert | SNMP | |
| | | Auslastung Des Erfressenen Datenverkehrs | Implementiert | SNMP | |
| | | Gesamtauslastung Des Datenverkehrs | Implementiert | SNMP | Gesamte Traffic-Auslastung |
| | | Auslastung Des Datenverkehrs | Implementiert | SNMP | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Cisco SNMP | SNMP | SNMPv1 (nur Inventar), SNMPv2, SNMPv3 | 161 | | Richtig | Richtig | Richtig | Richtig |

# EMC Celerra (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| NSX VG8 VNX5600 | 5.5.38-1 7.1.76-4 7.1.79-8 8.1.9-184 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Zugehöriges Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Celerra-CLI | SSH | SSH | | | Richtig | Falsch | Richtig | Richtig |

# EMC CLARiiON (NaviCLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 6.28 7.32 7.33 | CX4-120 VNX5200 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000 | 04.28.000.5.008 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.249 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.238 05.33.021.5.256 05.33.021.5.266 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Speicherpool-Id | Implementiert | CLI | |
| | | Thin Provisioning | Implementiert | CLI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | CLI | |
| | | UUID | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | Volume-Zuordnung | LUN | Implementiert | CLI | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | CLI | |
| | | Storage-Port | Implementiert | CLI | |
| | | Typ | Lücke | CLI | |
| | Volume-Maske | Initiator | Implementiert | CLI | |
| | | Protokoll-Controller | Implementiert | CLI | |
| | | Storage-Port | Implementiert | CLI | |
| | | Typ | Lücke | CLI | |
| | Volumenmitglied | Kapazität | Implementiert | CLI | Verwendete Kapazität des Snapshot in MB |
| | | Name | Implementiert | CLI | |
| | | Rang | Implementiert | CLI | |
| | | Gesamtbruttokapazität | Implementiert | CLI | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | CLI | Redundanzebene |
| | | Speicherpool-Id | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | WWN-Alias | Host-Aliase | Implementiert | CLI | |
| | | IP | Implementiert | CLI | |
| | | Objekttyp | Implementiert | CLI | |
| | | Quelle | Implementiert | CLI | |
| | | WWN | Implementiert | CLI | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | Storage Pools: Kapazität | Implementiert | CLI | |
|---|---|---|---|---|---|
| | | Taste | Implementiert | CLI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | CLI | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | CLI | |
| | | Bruttokapazität | Implementiert | CLI | |
| | | Gesamtkapazität | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | CLI | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | CLI | |
| | | Taste | Implementiert | CLI | |
| | | Sonstige Gesamtkapazität | Implementiert | CLI | |
| | | Andere Genutzte Kapazität | Implementiert | CLI | |
| | | Server-ID | Implementiert | CLI | |
| | | Reservierte Snapshot-Kapazität | Implementiert | CLI | |
| | | Verwendete Snapshot-Kapazität | Implementiert | CLI | |
| | | Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie | Implementiert | CLI | Als Zeitreihe gemeldet |
| | Datenmenge | Bruttokapazität | Implementiert | CLI | |
| | | Gesamtkapazität | Implementiert | CLI | |
| | | Genutzte Kapazität | Implementiert | CLI | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | CLI | |
| | | Taste | Implementiert | CLI | |
| | | Server-ID | Implementiert | CLI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Navi CLI | CLI | | 6389,2162,2163,443 (HTTPS)/80 (HTTP) | | Richtig | Richtig | Richtig | Falsch |

# EMC Data Domain (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| DD2500 DD4200 DD4500 DD6300 DD670 DD6800 DD6900 DD9300 DD9400 DD990 | 5.4.6.0-503967 5.5.0.9-471508 5.5.2.1-486308 6.1.0.5-567091 6.2.1.30-663869 6.2.1.50-680189 7.10.1.15-1078832 7.10.1.20-1090468 7.2.0.70-686759 7.6.5.25-1078970.4.0-1017976 7.7.5.11-1046187 7.7.0.40-691389 7.7 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1016 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | SSH | Verhältnis zur Konvertierung von nutzbarer |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Rohkapazität zur Informationen** |
| | | Speicherpool-Id | Implementiert | SSH | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | SSH | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | SSH | |
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Data Domain CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |

# EMC ECS

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| ECS | 3.6.1.3 3.7.0.6 3.8.0.6 3.8.1.1 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1024 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | Storage-Node | Name | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Version | Implementiert | HTTPS | Softwareversion |
| | Storage-Pool | In Dwh-Kapazität Einbeziehen | Implementiert | HTTPS | Ein Weg von ACQ zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind |
| | | Name | Implementiert | HTTPS | |
| | | Kapazität der physischen Festplatte (MB) | Implementiert | HTTPS | Wird als Rohkapazität für den Storage-Pool verwendet |
| | | Raid-Gruppe | Implementiert | HTTPS | Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt |
| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | HTTPS | Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | HTTPS | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | HTTPS | |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC ECS REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# Dell EMC Isilon/PowerScale (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| A200 A2000 A300 A3000 F800 H400 H500 H500-4U-Single-128 GB-1 x 1 GE-2 x 10 GE SFP+-30 TB-1638 GB SSD H700 NL400 NL410 Traceback (letzter Anruf zuletzt): X210 X400 Sudo Python | 9.2.1.12 9.4.0.14 9.4.0.17 9.5.0.7 v8.0.0.6 v8.0.0.7 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Zugehöriges Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| 1040 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Fehlerhafte Bruttokapazität | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktionsattribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Storage-Node-Daten | IOPS Lesen | Implementiert | SSH | Anzahl der Lese-IOPS im Dateisystem |
| | | IOPS Schreiben | Implementiert | SSH | IOPS Schreiben des Dateisystems |
| | | Lesedurchsatz Des Dateidurchsatzes | Implementiert | SSH | |
| | | Durchsatz des Dateisystems | Implementiert | SSH | Dateisystem-Durchsatz schreiben |
| | | IOPS Lesen | Implementiert | SSH | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | SSH | |
| | | IOPS Schreiben | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Latenz Insgesamt | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | | Durchsatz Beim Lesen | Implementiert | SSH | |
| | | Gesamtdurchsatz | Implementiert | SSH | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SSH | |
| | | Auslastung Insgesamt | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Isilon SSH | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

# EMC PowerStore REST

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| PowerStore 1000T PowerStore 5000T PowerStore 5200T | 2.1.1.1 3.2.1.0 3.5.0.2 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | | |
| | | Einheitliche | Implementiert | | Handelt es sich um ein Gerät zur |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen? |
|---|---|---|---|---|---|
| | Datenmenge | Kapazität | Implementiert | | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | | |
| | | Name | Implementiert | | |
| | | Gesamtbruttokapazität | Implementiert | | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Speicherpool-Id | Implementiert | | |
| | | Thin Provisioning | Implementiert | | |
| | | Typ | Lücke | | |
| | | UUID | Implementiert | | |
| | | Genutzte Kapazität | Implementiert | | |
| | | QoS: Richtlinie | Implementiert | | |
| | Volume-Zuordnung | LUN | Implementiert | | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Typ | Lücke | | |
| | WWN-Alias | Host-Aliase | Implementiert | | |
| | | Objekttyp | Implementiert | | |
| | | Quelle | Implementiert | | |
| | | WWN | Implementiert | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | IOPS Sonstiges | Implementiert | | |
| | | IOPS Lesen | Implementiert | | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | | |
| | | IOPS Schreiben | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Latenzleseszeit | Implementiert | | |
| | | Latenz Insgesamt | Implementiert | | |
| | | Latenz – Schreiben | Implementiert | | |
| | | Server-ID | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC POWERSTORE REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# EMC RecoverPoint (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| RecoverPoint | 5.1.SP3.P1(g. 69) 5.1.SP4.HF1(h.83)<br>5.1.SP4.P1(h.89) |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1050 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Festplatten) | | | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | Storage-Node | Speichergröße | Lücke | HTTPS | Gerätespeicher in MB |
| | | Modell | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Prozessoranzahl | Implementiert | HTTPS | Geräte-CPU |
| | | Seriennummer | Implementiert | HTTPS | |
| | | Status | Implementiert | HTTPS | Kostenloser Text, der den Gerätestatus beschreibt |
| | | UUID | Implementiert | HTTPS | |
| | | Version | Implementiert | HTTPS | Softwareversion |
| | Storage-Synchronisierung | Modus | Implementiert | HTTPS | |
| | | Modus Enum | Implementiert | HTTPS | |
| | | Quell-Storage | Implementiert | HTTPS | |
| | | Quell-Volume | Implementiert | HTTPS | |
| | | Status | Implementiert | HTTPS | Kostenloser Text, der den Gerätestatus beschreibt |
| | | Staatsummen | Implementiert | HTTPS | |
| | | Ziel-Storage | Implementiert | HTTPS | |
| | | Ziel-Volume | Implementiert | HTTPS | |
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verändert |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| RecoverPoint-REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# EMC Symmetrix CLI

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| V10.0.0.0 V10.0.0.3 V10.0.1.0 V10.0.1.3 V10.1.0.0 V10.1.0.3 V8.3.0.6 V9.1.0.15 V9.2.0.0 V9.2.3.0 V9.2.3.4 V9.2.3.6 V9.2.4.1 V9.2.4.2 V9.2.4.6 | PMax8000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX250F VMAX40K VMAX450F VMAX950F | 5876.286.194 6 5978.714.714 (16F40000) Build 115 5978.479.479 34 5978.714.714 61 5978.714.714 (175A0000) Build 372 5978.711.711 85 (175A0000) Build 179 5978.711.711 (175A0000) Build 205 5978.711.711 (175A0000) Build 49 5978.714.714 (175A0000) Build 365 5978.711.711 (175A0000) Build 374 5978.711.711 (175A0000) Build 448 5978.711.711 (175A0000) Build 484 5978.711.711 (1750000) Build 539 5978.711.711 (1750000) Build 239 5978.711.711 A00517500 542 5978.714.714) A0000 5978.714.714) A17500 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |
| | Volumenmitglied | Automatisiertes Tiering | Implementiert | | Gibt an, ob dieser storagepool an Auto-Tiering mit anderen Pools beteiligt ist |
| | | Kapazität | Implementiert | | Verwendete Kapazität des Snapshot in MB |
| | | Zylinder | Implementiert | | |
| | | Name | Implementiert | | |
| | | Rang | Implementiert | | |
| | | Gesamtbruttokapazität | Implementiert | | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | | Redundanzebene |
| | | Speicherpool-Id | Implementiert | | |
| | | UUID | Implementiert | | |
| | WWN-Alias | Host-Aliase | Implementiert | | |
| | | Objekttyp | Implementiert | | |
| | | Quelle | Implementiert | | |
| | | WWN | Implementiert | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | auf allen Festplatten) in MB/s |
| **Produkt** | **Kategorie** | **Funktion/Attribut schreiben** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | „Ausstehend“ | Implementiert | | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| symcli | CLI | | 2707 | | Richtig | Richtig | Richtig | Richtig |
| Symmetrix SMI-S | SMI-S | HTTP/HTTPS | 5988/5989 | | Richtig | Falsch | Falsch | Richtig |

# Dell Unisphere-REST

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| V10.0.1.3 V10.1.0.1 V10.1.0.5 V10.1.0.6 V9.2.4.7 V9.2.4.9 | PowerMax_2000 PowerMax_2500 PowerMax_8000 PowerMax_8500 VMAX250F VMAX950F | 5978.714.714 5978.714.714 Build 6 5978.714.714 Build 61 5978.714.714 Build 85 6079.225.0 Build 127 6079.225.0 Build 216 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | um ein Gerät zur Storage-Virtualisierung? |
|---|---|---|---|---|---|
| **Produkt** | **Kategorie** | **Funktionen/Attribute Gruppen** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| 1070 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Schreiben | | | |
| | | Server-ID | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktionsattribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Durchsatz lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | „Ausstehend“ | Implementiert | HTTPS | Insgesamt ausstehend |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Dell Unisphere-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# EMC VNX (SSH)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| VNX5300 VNX5400 VNX5800 VNX7500 | 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.33.009.5.186 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | SSH | |
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | IP | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | Storage Pools: Kapazität | Implementiert | SSH | |
|---|---|---|---|---|---|
| | | Taste | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | SSH | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | SSH | |
| | | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | SSH | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Sonstige Gesamtkapazität | Implementiert | SSH | |
| | | Andere Genutzte Kapazität | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VNX SSH UND CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

# EMC VNXe und Unity Unisphere (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Unity 300 Unity 300F Unity 350F Unity 450F Unity 480F Unity 550F Unity 600 Unity 600F Unity 650F Unity 680 Unity 680F Unity 880 Unity 880F VNXe3200 | 3.1.17.10223906 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.7.0.5.008 5.1.0.0.5.394 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.3.0.0.5.120 5.3.1.0.5.008 5.4.0.0.5.094 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1084 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Ziel-Volume | Implementiert | HTTPS | |
|---|---|---|---|---|---|
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verwendet |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Festplatte | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VNXe und Unisphere CLI | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# EMC VPLEX

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| VPLEX | 6.1.0.00.00.23 6.1.0.01.00.13 6.1.0.02.00.04 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1096 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTP/S | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTP/S | Verwendete Kapazität des Snapshot in MB |
| | | Name | Implementiert | HTTP/S | |
| | | Gesamtbruttokapazität | Implementiert | HTTP/S | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTP/S | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTP/S | |
| | | Thin Provisioning | Implementiert | HTTP/S | |
| | | UUID | Implementiert | HTTP/S | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTP/S | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| 1100 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | IOPS insgesamt | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Latenzleseszeit | Implementiert | SSH | |
| | | Latenz Insgesamt | Implementiert | SSH | |
| | | Latenz – Schreiben | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | | Durchsatz Beim Lesen | Implementiert | SSH | |
| | | Gesamtdurchsatz | Implementiert | SSH | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC VPLEX-CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |
| EMC VPLEX-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# EMC XtremIO (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
| --- | --- | --- |
| 4.2.2 6.2.1 6.3.1 6.3.2 6.3.3 6.4.0 | 1 Bricks und 48 TB 1 x 20 TB 2 Bricks und 251 TB 2 x 20 TB 3 Bricks und 283 TB 4 Bricks und 503 TB 4 x 10 TB 6 x 20 TB 8 x 20 TB | 4.0.25-27 4.0.31-11 6.1.0-99_X2 6.2.1-36_X2 6.3.3-8_X2 6.4.0-36_HOTFIX_2_X2 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Ziel-Volume | Implementiert | HTTPS | |
| | | Technologie | Implementiert | HTTPS | Technologie, die Storage-Effizienz verwendet |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Festplattengröße | Implementiert | HTTPS | Kommagetrennte Liste der Festplattengrößen (GB) |
| | | Festplattengeschwindigkeit | Implementiert | HTTPS | Kommagetrennte Liste von Festplattengeschwindigkeiten (rpm) |
| | | Festplattentyp | Nicht Verfügbar | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |
| 1110 | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Server-ID | Implementiert | HTTPS | |
| | Storage-Node-Daten | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | Datenmenge | Bruttokapazität | Implementiert | HTTPS | |
| | | Gesamtkapazität | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| EMC XTREMIO REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# NetApp E-Series

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 2650 2660 2704 2806 5600 5700 | 8.10.15.0 8.20.11.60 8.20.16.0 8.20.5.60 8.40.0.3 8.40.60.2 8.63.0.2 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.2.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | RMI | |
| | | Einheitliche | Implementiert | RMI | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | RMI | Verwendete Kapazität des Snapshot in MB |
| | | Festplattentyp | Nicht Verfügbar | RMI | |
| | | Name | Implementiert | RMI | |
| | | Gesamtbruttokapazität | Implementiert | RMI | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | RMI | Redundanzebene |
| | | Speicherpool-Id | Implementiert | RMI | |
| | | Thin Provisioning | Implementiert | RMI | |
| | | Typ | Lücke | RMI | |
| | | UUID | Implementiert | RMI | |
| | | Genutzte Kapazität | Implementiert | RMI | |
| | | Einheitliche | Implementiert | RMI | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | | Geschriebene Kapazität | Implementiert | RMI | Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde |
| | Volume-Zuordnung | LUN | Implementiert | RMI | Der Name der Backend-lun |
| | Volume-Maske | Initiator | Implementiert | RMI | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Gesamtkapazität | | | |
| | | Andere Genutzte Kapazität | Implementiert | RMI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | RMI | |
| | Datenmenge | Cache-Trefferverhältnis Lesen | Implementiert | RMI | |
| | | Cache-Trefferverhältnis Insgesamt | Implementiert | RMI | |
| | | Cache-Trefferverhältnis Schreiben | Implementiert | RMI | |
| | | Bruttokapazität | Implementiert | RMI | |
| | | Gesamtkapazität | Implementiert | RMI | |
| | | Genutzte Kapazität | Implementiert | RMI | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | RMI | |
| | | IOPS Lesen | Implementiert | RMI | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | RMI | |
| | | IOPS Schreiben | Implementiert | RMI | |
| | | Taste | Implementiert | RMI | |
| | | Latenzleseszeit | Implementiert | RMI | |
| | | Latenz Insgesamt | Implementiert | RMI | |
| | | Latenz – Schreiben | Implementiert | RMI | |
| | | Server-ID | Implementiert | RMI | |
| | | Durchsatz Beim Lesen | Implementiert | RMI | |
| | | Gesamtdurchsatz | Implementiert | RMI | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | RMI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| SANtricity API | RMI | TCP | | | Richtig | Richtig | Falsch | Falsch |

# HDS HCP (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Hitachi Content Platform | 9.6.2.37 9.6.3.33 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | Storage-Node-Daten | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Durchsatz Beim Lesen | Implementiert | | |
| | | Gesamtdurchsatz | Implementiert | | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | | |
| | | Auslastung Insgesamt | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HDS HCP REST API | HTTPS | HTTPS | 9090 | | Richtig | Richtig | Richtig | Richtig |

# HiCommand Device Manager

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 8.6.4 8.7.7 8.8.1 8.8.3 8.8.5 | D850XS HM700 HM800M R800 | 0988/J-W DKC:73-03-83-52 DKC:00/00-05-05-83 DKC:06-68/00-80-03 DKC:40/00-73-50-83 SVP:05-40/00-87/00 SVP:48-83-92 SVP:40/00-06-00/00-80 SVP:69-05-54-40/00 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1128 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Speicherpool-Id | Implementiert | HDS-XML-API | |
| | | Thin Provisioning | Implementiert | HDS-XML-API | |
| **Produkt** | **Kategorie** | **Funktion/Attribut Typ** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HDS-XML-API | |
| | | Genutzte Kapazität | Implementiert | HDS-XML-API | |
| | Volume-Zuordnung | LUN | Implementiert | HDS-XML-API | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HDS-XML-API | |
| | | Protokoll-Controller | Implementiert | HDS-XML-API | |
| | | Storage-Port | Implementiert | HDS-XML-API | |
| | Volume-Maske | Initiator | Implementiert | HDS-XML-API | |
| | | Protokoll-Controller | Implementiert | HDS-XML-API | |
| | | Storage-Port | Implementiert | HDS-XML-API | |
| | Volumenmitglied | Name | Implementiert | HDS-XML-API | |
| | | Speicherpool-Id | Implementiert | HDS-XML-API | |
| | | Rang | Implementiert | HDS-XML-API | |
| | | Zylinder | Implementiert | HDS-XML-API | |
| | | Kapazität | Implementiert | HDS-XML-API | Verwendete Kapazität des Snapshot in MB |
| | | Gesamtbruttokapazität | Implementiert | HDS-XML-API | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Genutzte Kapazität | Implementiert | HDS-XML-API | |
| | WWN-Alias | Host-Aliase | Implementiert | HDS-XML-API | |
| | | Objekttyp | Implementiert | HDS-XML-API | |
| | | Quelle | Implementiert | HDS-XML-API | |
| | | WWN | Implementiert | HDS-XML-API | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Festplatte | IOPS Lesen | Implementiert | Export/CLI | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | Export/CLI | |
| | | IOPS Schreiben | Implementiert | Export/CLI | |
| | | Taste | Implementiert | Export/CLI | |
| | | Server-ID | Implementiert | Export/CLI | |
| | | Durchsatz Beim Lesen | Implementiert | Export/CLI | |
| | | Gesamtdurchsatz | Implementiert | Export/CLI | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | Export/CLI | |
| | | Auslastung Insgesamt | Implementiert | Export/CLI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Exportdienstprogramm (USPV) / SNM CLI (AMS) | Export/CLI | | | | Falsch | Falsch | Falsch | Falsch |
| HiCommand Device Manager-XML-API | HDS-XML-API | HTTP/HTTPS | 2001 | | Richtig | Richtig | Richtig | Richtig |

# HDS HNAS (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| G600 HNAS 4100 | 14.6.7520,04 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1138 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Insgesamt Genutzte Kapazität | Implementiert | SSH | Gesamtkapazität in MB |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | SSH | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HDS HNAS CLI | SSH | SSH | 22 | | Richtig | Richtig | Richtig | Richtig |

# HPE Nimble/Alletra 6000 Storage

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| v1 | AF40 AF80 HF60 | 5.0.3.100-575430-OPT 5.2.1.600-841103-OPT |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut Typ** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | HTTPS | |
| | | Bruttokapazität | Implementiert | HTTPS | |
| | | Freie Rohkapazität | Implementiert | HTTPS | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | HTTPS | |
| | | IOPS Sonstiges | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| HP NIMBLE REST API | HTTPS | HTTPS | 5392 | | Richtig | Falsch | Richtig | Richtig |

# Huawei OceanStor (REST/HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 5500 V3 6800 V3 | V300R006C50 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Huawei OceanStor REST-API | HTTPS | HTTPS | 8088 | | Richtig | Richtig | Richtig | Richtig |
| Huawei OceanStor Performance REST API | HTTPS | HTTPS | 8088 | | Richtig | Falsch | Richtig | Richtig |

# IBM SVC (CLI)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| 2076-112 2076-124 2076-12F 2076-212 2076-224 2076-24F 2076-24G 2076-524 2076-624 2076-724 2076-824 2077-24F 2077-324 4657-924 4662-6H2 9840-AE1 9843-AE2 9843-AE3 SVC | 1.5.2.5 1.6.1.0 1.6.1.5 7.8.1.11 7.8.1.13 7.8.1.5 7.8.1.7 7.8.1.8 8.1.3.5 8.1.3.6 8.2.1.11 8.2.1.8 8.3.1.2 8.3.1.5 8.4.0.10 8.4.0.11 8.5.0.10 8.5.0.11 8.5.0.12 8.5.0.9 8.5.3.1 8.6.0.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1160 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Kapazität | | | |
| | | Einheitliche | Implementiert | SSH | Handelt es sich um ein Gerät zur |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen?** |
| | | Geschriebene Kapazität | Implementiert | SSH | Gesamtkapazität, die von einem Host in MB auf dieses Volume geschrieben wurde |
| | | Komprimierung Aktiviert | Implementiert | SSH | |
| | | Verschlüsselt | Implementiert | SSH | |
| | Volume-Zuordnung | LUN | Implementiert | SSH | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | Volume-Maske | Initiator | Implementiert | SSH | |
| | | Protokoll-Controller | Implementiert | SSH | |
| | | Storage-Port | Implementiert | SSH | |
| | | Typ | Lücke | SSH | |
| | WWN-Alias | Host-Aliase | Implementiert | SSH | |
| | | Objekttyp | Implementiert | SSH | |
| | | Quelle | Implementiert | SSH | |
| | | WWN | Implementiert | SSH | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | SSH | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Auslastung insgesamt | Implementiert | SSH | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | SSH | |
| | | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | SSH | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |
| | Datenmenge | Bruttokapazität | Implementiert | SSH | |
| | | Gesamtkapazität | Implementiert | SSH | |
| | | Genutzte Kapazität | Implementiert | SSH | |
| | | Geschriebene Kapazität | Implementiert | SSH | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | SSH | |
| | | KapazitätRatio geschrieben | Implementiert | SSH | |
| | | Taste | Implementiert | SSH | |
| | | Server-ID | Implementiert | SSH | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| IBM SVC-CLI | SSH | SSH | 22 | | Richtig | Falsch | Richtig | Richtig |

# Infiniat Infinibox (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
| --- | --- |
| F4304 F4304T F6260 F6306 | 7.1.14.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | HTTPS | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut-Typ | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| | | Typ | Lücke | HTTPS | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTPS | |
| | | Objekttyp | Implementiert | HTTPS | |
| | | Quelle | Implementiert | HTTPS | |
| | | WWN | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Infinidat REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# Microsoft Hyper-V

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Bereitgestellte Kapazität | Implementiert | WMI | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Bereitgestellte Kapazität | Implementiert | WMI | |
| | VirtualMachine Disk | OID | Implementiert | WMI | |
| | | VirtualisierungsDisk OID | Implementiert | WMI | |
| | | OID der Virtual Machine | Implementiert | WMI | |
| | Host | Host-Cpu-Anzahl | Implementiert | WMI | |
| | | Host-Cpu-Geschwindigkeit | Implementiert | WMI | |
| | | Host Domain | Implementiert | WMI | |
| | | Host-Installierter Speicher | Implementiert | WMI | |
| | | Host-Modell | Implementiert | WMI | |
| | | Anzahl der NIC | Implementiert | WMI | |
| | | NIC-Geschwindigkeit | Implementiert | WMI | |
| | | IPS | Implementiert | WMI | |
| | | Hersteller | Implementiert | WMI | |
| | | Name | Implementiert | WMI | |
| | | OID | Implementiert | WMI | |
| | | Plattformtyp | Implementiert | WMI | |
| | Info | Name der Datenquelle | Implementiert | WMI | Info |
| | | Datum | Implementiert | WMI | |
| | | Ersteller-ID | Implementiert | WMI | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| PowerShell | WS-Verwaltung | HTTP | 5985 | | Richtig | Falsch | Falsch | Richtig |
| WMI | WMI | WMI | 135 | | Richtig | Falsch | Richtig | Richtig |

# NetApp 7-Modus

Von diesem Datensammler unterstützte Modelle und Versionen:

| API-Versionen | Modelle | Firmware-Versionen |
|---|---|---|
| 1.12 1.17 1.19 1.20 1.21 | FAS2220 FAS2240-2 FAS2240-4 FAS2554 FAS3210 FAS3250 FAS3270 FAS6240 FAS8040 FAS8060 N6070 | 8.1.1 7-Mode 8.1.4P6 7-Mode 8.2.3P2 7-Mode 7.3P3 7-Mode 8.2.3P6 7-Mode 8.2.4P4 7-Mode 8.2.4P5 7-Mode 8.2.5P3 8.2-Mode 8.2.5P5 7-Mode 8.2P4 7-Mode Data ONTAP Version 7.3.3 Data ONTAP Version 7.3.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | Zuordnung | | | | Backend-lun |
| | | Protokoll-Controller | Implementiert | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | | |
| | Volume-Maske | Initiator | Implementiert | | |
| | | Protokoll-Controller | Implementiert | | |
| | | Storage-Port | Implementiert | | |
| | | Typ | Lücke | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Durchsatz Schreiben | Implementiert | | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** | |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | | | |
| | | Bruttokapazität | Implementiert | | | |
| | | Gesamtkapazität | Implementiert | | | |
| | | Genutzte Kapazität | Implementiert | | | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | | Als Zeitreihe gemeldet | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | | | |
| | | Gesamtkapazität Daten | Implementiert | | | |
| | | Genutzte Kapazität Von Daten | Implementiert | | | |
| | | Taste | Implementiert | | | |
| | | Server-ID | Implementiert | | | |
| | | Reservierte Snapshot-Kapazität | Implementiert | | | |
| | | Verwendete Snapshot-Kapazität | Implementiert | | | |
| | | Kapazitätsverhältnis Der Verwendeten Snapshot-Technologie | Implementiert | | Als Zeitreihe gemeldet | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| NetApp 7 Modus ZAPI | ZAPI | ZAPI | | | Richtig | Richtig | Richtig | Richtig |

# NetApp Clustered Data ONTAP 8.1 und höher

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| AFF-A150 AFF-A200 AFF-A220 AFF-A250 AFF-A300 AFF-A400 AFF-A700 AFF-A700s AFF-A800 AFF-A900 AFF-C190 AFF-C250 AFF-C400 AFF-C800 AFF8040 AFF8080 CDvM200 DM5100F FAS2240-2 FAS2520 FAS2552 FAS2554 FAS2620 FAS2650 FAS2720 FAS2750 FAS3250 FAS500f FAS6220 FAS8020 FAS8060 FAS8080 FAS8200 FAS8300 FAS8700 FAS9000 FAS9500 DvM300 | 8.2.P13.P5 8.2 9.12.1.4P3 8.3 9.14.1.1P2 9.1.2P12 8.3.2P5 8.3.2P8 9.1.0 9.1.0P15 9.1.0P19 9.1.0P2 8.3.2 8.3.0P20 9.10.1P11 9.10.1P12 9.10.1P13 9.10.1P13 9.10.1P13 9.10.1P14 9.10.1P14 9.10.1P14 9.15.1 9.3 9.3 9.3 9.4 9.4 9.5.0 9.5 9.5 9.5 9.7 9.7 9.7 9.7 9.7 9.7 9.7 9.7 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.8 9.9 9.9 9.9 9.9 9.9 9.9 9.9 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1200 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Virtualisierung? |
| | | Verschlüsselt | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | IOPS | Implementiert | HTTPS | |
| | | QoS begrenzt MB/S | Implementiert | HTTPS | |
| | | Qos-Limit: Raw | Implementiert | HTTPS | |
| | | QoS: Richtlinie | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Leseauslastung | Implementiert | HTTPS | |
| | | Auslastung Insgesamt | Implementiert | HTTPS | |
| | | Auslastung Schreiben | Implementiert | HTTPS | |
| | Datenmenge | Taste | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| NetApp ONTAP-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# NetApp SolidFire 8.1 oder höher

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| H410S-1 SF19210 SF2405 SF38410 SF4805 FC0025 FCN001 H410S-0 H610S-1 SF19210 SF2405 SF38410 SF4805 | 11.1.0.72 11.3.1.5 12.3.0.958 12.3.1.103 12.3.2.3 12.5.0.897 12.7.0.380 9.3.0.40 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1224 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | IOPS | | | |
| | | qos-Minimum für IOPS | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | QoS: Richtlinie | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | Gesamtkapazität | | | |
| | | Andere Genutzte Kapazität | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Server-ID | Implementiert | HTTPS | |
| | Datenmenge | Bruttokapazität | Implementiert | HTTPS | |
| | | Gesamtkapazität | Implementiert | HTTPS | |
| | | Genutzte Kapazität | Implementiert | HTTPS | |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | HTTPS | |
| | | Gesamteinsparungen Durch Komprimierung | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Teilweise Blockielles Verhältnis | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |
| | | Auslastung Insgesamt | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| SolidFire REST-API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# NetApp StorageGRID (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Webscale | 11.6.0.11 11.6.0.7 11.7.0.4 11.7.0.8 11.8.0.5 3.1 3.4 3.5 4.0 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | tung des Knotens verwendete Metadaten in MB | | | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Standortname | Implementiert | HTTPS | |
| | Storage-Pool | In Dwh-Kapazität Einbeziehen | Implementiert | HTTPS | Ein Weg von ACQ zu steuern, welche Speicherpools in der DWH-Kapazität interessant sind |
| | | Name | Implementiert | HTTPS | |
| | | Kapazität der physischen Festplatte (MB) | Implementiert | HTTPS | Wird als Rohkapazität für den Storage-Pool verwendet |
| | | Raid-Gruppe | Implementiert | HTTPS | Zeigt an, ob es sich bei diesem StoragePool um eine RAID-Gruppe handelt |
| | | Verhältnis „Rohkapazität“ zu „nutzbar“ | Implementiert | HTTPS | Verhältnis zur Konvertierung von nutzbarer Kapazität zur Rohkapazität |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning Wird Unterstützt | Implementiert | HTTPS | Ob dieses interne Volume Thin Provisioning für die Volume-Ebene zusätzlich unterstützt |
| | | Insgesamt Zugewiesene Kapazität | Implementiert | HTTPS | |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | auf allen Festplatten) in MB/s |
| **Produkt** | **Kategorie** | **Funktion/Attribut schreiben** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | Storage-Pool | Bereitgestellte Kapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Gesamtkapazität | Implementiert | | |
| | | Genutzte Kapazität | Implementiert | | |
| | | Kapazitätsverhältnis Zu Hoch Festsetzen | Implementiert | | Als Zeitreihe gemeldet |
| | | Verhältnis Der Verwendeten Kapazität | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| StorageGRID REST API | HTTPS | HTTPS | 443 | | Richtig | Falsch | Richtig | Richtig |

# Nutanix Storage (REST)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| HX3310 NX-8150-G5 HX3310 HX321 HX5510 NX-8155-G6 NX-8155-G7 XC640-10 CORE XC740XD-12 XC740XD-12 CORE | 5.20.2.1 5.20.4.6 6.5.4 6.5.5 6.5.5.6 6.5.5.7 6.5.6.5 6.7.1.7 6.8 6.8.1 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1244 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | | | | Ebene zusätzlich unterstützt |
| | | Insgesamt | Implementiert | HTTPS | |
| **Produkt** | **Kategorie** | **Zugehöriges Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Insgesamt Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Insgesamt Genutzte Kapazität | Implementiert | HTTPS | Gesamtkapazität in MB |
| | | Typ | Lücke | HTTPS | |
| | | Einheitliche | Implementiert | HTTPS | Handelt es sich um ein Gerät zur Storage-Virtualisierung? |
| | Datenmenge | Kapazität | Implementiert | HTTPS | Verwendete Kapazität des Snapshot in MB |
| | | Verbindungspfad | Implementiert | HTTPS | |
| | | Name | Implementiert | HTTPS | |
| | | Qtree-Id | Implementiert | HTTPS | Eindeutige id des qtree |
| | | Gesamtbruttokapazität | Implementiert | HTTPS | Gesamte Rohkapazität (Summe aller Festplatten im Array) |
| | | Redundanz | Implementiert | HTTPS | Redundanzebene |
| | | Speicherpool-Id | Implementiert | HTTPS | |
| | | Thin Provisioning | Implementiert | HTTPS | |
| | | UUID | Implementiert | HTTPS | |
| | Volume-Zuordnung | LUN | Implementiert | HTTPS | Der Name der Backend-lun |
| | | Storage-Port | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |
| | Volume-Maske | Storage-Port | Implementiert | HTTPS | |
| | | Initiator | Implementiert | HTTPS | |
| | | Protokoll-Controller | Implementiert | HTTPS | |
| | | Typ | Lücke | HTTPS | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | HTTPS | |
| | | Bruttokapazität | Implementiert | HTTPS | |
| | | Freie Rohkapazität | Implementiert | HTTPS | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | HTTPS | |
| | | IOPS Sonstiges | Implementiert | HTTPS | |
| | | IOPS Lesen | Implementiert | HTTPS | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | HTTPS | |
| | | IOPS Schreiben | Implementiert | HTTPS | |
| | | Taste | Implementiert | HTTPS | |
| | | Latenzleseszeit | Implementiert | HTTPS | |
| | | Latenz Insgesamt | Implementiert | HTTPS | |
| | | Latenz – Schreiben | Implementiert | HTTPS | |
| | | Server-ID | Implementiert | HTTPS | |
| | | Durchsatz Beim Lesen | Implementiert | HTTPS | |
| | | Gesamtdurchsatz | Implementiert | HTTPS | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | HTTPS | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Nutanix REST API | HTTPS | HTTPS | 443 | | Richtig | Richtig | Richtig | Richtig |

# Oracle ZFS (HTTPS)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| Sun ZFS Storage 7330 Sun ZFS Storage 7420 Sun ZFS Storage 7430 | 1-1.1 2013.06.05.7.28 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Kapazität | | | |
| | | Einheitliche | Implementiert | HTTP/S | Handelt es sich um ein Gerät zur |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen?** |
| | Volume-Zuordnung | LUN | Implementiert | HTTP/S | Der Name der Backend-lun |
| | | Maskierung Erforderlich | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| Performance | Storage-Node-Daten | Cache-Trefferverhältnis Insgesamt | Implementiert | | |
| | | IOPS insgesamt | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Auslastung Insgesamt | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| ORACLE ZFS REST API | HTTP/HTTPS | HTTP/HTTPS | 215 | | Richtig | Richtig | Richtig | Richtig |

# Pure Storage FlashArray (HTTP)

Von diesem Datensammler unterstützte Modelle und Versionen:

| Modelle | Firmware-Versionen |
|---|---|
| DFSC1 FA-X20R3 FA-X50R2 FA-X70R3 FA-X70R4 FA-X90R2 FA-X90R3 FA-X90R4 | 6.1.21 6.3.1 6.3.10 6.3.9 6.5.1 6.5.2 6.5.4 |

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |
| 1266 | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | Protokoll-Controller | Implementiert | HTTP/S | |
|---|---|---|---|---|---|
| | | Storage-Port | Implementiert | HTTP/S | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | | Typ | Lücke | HTTP/S | |
| | Volume-Maske | Initiator | Implementiert | HTTP/S | |
| | | Protokoll-Controller | Implementiert | HTTP/S | |
| | | Storage-Port | Implementiert | HTTP/S | |
| | | Typ | Lücke | HTTP/S | |
| | WWN-Alias | Host-Aliase | Implementiert | HTTP/S | |
| | | Objekttyp | Implementiert | HTTP/S | |
| | | Quelle | Implementiert | HTTP/S | |
| | | WWN | Implementiert | HTTP/S | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| Performance | Storage | Fehlerhafte Bruttokapazität | Implementiert | | |
| | | Bruttokapazität | Implementiert | | |
| | | Freie Rohkapazität | Implementiert | | Rohkapazität von Spare-Festplatten (Summe aller freien Festplatten) |
| | | Storage Pools: Kapazität | Implementiert | | |
| | | IOPS Sonstiges | Implementiert | | |
| | | IOPS Lesen | Implementiert | | Anzahl der Lese-IOPS auf der Festplatte |
| | | IOPS insgesamt | Implementiert | | |
| | | IOPS Schreiben | Implementiert | | |
| | | Taste | Implementiert | | |
| | | Latenzleseszeit | Implementiert | | |
| | | Latenz Insgesamt | Implementiert | | |
| | | Latenz – Schreiben | Implementiert | | |
| | | Server-ID | Implementiert | | |
| | | Durchsatz Beim Lesen | Implementiert | | |
| | | Gesamtdurchsatz | Implementiert | | Durchschnittliche Gesamtrate der Festplatte (Lese- und Schreibvorgänge auf allen Festplatten) in MB/s |
| | | Durchsatz Schreiben | Implementiert | | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| Pure Storage REST-API | HTTP/HTTPS | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# VMware vSphere (Web Services)

Von diesem Datensammler unterstützte Modelle und Versionen:

API-Versionen:

- VMware vCenter Server 5.5.0 Build-1750787
- VMware vCenter Server 5.5.0 Build-3252642
- VMware vCenter Server 5.5.0 Build-4180647
- VMware vCenter Server 5.5.0 Build-9911218
- VMware vCenter Server 6.0.0 Build-13638472
- VMware vCenter Server 6.0.0 Build-14510545
- VMware vCenter Server 6.0.0 Build-4541947
- VMware vCenter Server 6.0.0 Build-5318200
- VMware vCenter Server 6.0.0 Build-9313458
- VMware vCenter Server 6.5.0 Build-10964411
- VMware vCenter Server 6.5.0 Build-17994927
- VMware vCenter Server 6.5.0 Build-18499837
- VMware vCenter Server 6.5.0 Build-18711281
- VMware vCenter Server 6.5.0 Build-19757181
- VMware vCenter Server 6.5.0 Build-22499743
- VMware vCenter Server 6.5.0 Build-7515524
- VMware vCenter Server 6.5.0 Build-9451637
- VMware vCenter Server 6.7.0 Build-16046713
- VMware vCenter Server 6.7.0 Build-18485185
- VMware vCenter Server 6.7.0 Build-19299595
- VMware vCenter Server 6.7.0 Build-19832280
- VMware vCenter Server 6.7.0 Build-20504362
- VMware vCenter Server 6.7.0 Build-22509732
- VMware vCenter Server 6.7.0 Build-22509751
- VMware vCenter Server 7.0.1 Build-17491160

- VMware vCenter Server 7.0.3 Build-19234570
- VMware vCenter Server 7.0.3 Build-19717403
- VMware vCenter Server 7.0.3 Build-20051473
- VMware vCenter Server 7.0.3 Build-20150588
- VMware vCenter Server 7.0.3 Build-20395099
- VMware vCenter Server 7.0.3 Build-20845200
- VMware vCenter Server 7.0.3 Build-20990077
- VMware vCenter Server 7.0.3 Build-21290409
- VMware vCenter Server 7.0.3 Build-21477706
- VMware vCenter Server 7.0.3 Build-21784236
- VMware vCenter Server 7.0.3 Build-22357613
- VMware vCenter Server 7.0.3 Build-22837322
- VMware vCenter Server 7.0.3 Build-23788036
- VMware vCenter Server 7.0.3 Build-24026615
- VMware vCenter Server 8.0.1 Build-22368047
- VMware vCenter Server 8.0.1 Build-22742005
- VMware vCenter Server 8.0.1 Build-23525738
- VMware vCenter Server 8.0.1 Build-24005165
- VMware vCenter Server 8.0.2 Build-22385739
- VMware vCenter Server 8.0.2 Build-22617221
- VMware vCenter Server 8.0.2 Build-23319993
- VMware vCenter Server 8.0.2 Build-23504390
- VMware vCenter Server 8.0.2 Build-23929136
- VMware vCenter Server 8.0.3 Build-24022515
- VMware vCenter Server 8.0.3 Build-24091160

Von diesem Datensammler unterstützte Produkte:

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|
| grundlage | | | | | |

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| Produkt | Kategorie | Funktion/Attribut | Status | Verwendetes Protokoll | Weitere Informationen |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Bereitgestellte Kapazität | Implementiert | Web-Services | |
| **Produkt** | **Kategorie** | **Funktion/Attribut** | **Status** | **Verwendetes Protokoll** | **Weitere Informationen** |
| | VirtualMachine Disk | OID | Implementiert | Web-Services | |
| | | VirtualisierungsDisk OID | Implementiert | Web-Services | |
| | | OID der Virtual Machine | Implementiert | Web-Services | |
| | Host | Host-Cpu-Anzahl | Implementiert | Web-Services | |
| | | Host-Cpu-Geschwindigkeit | Implementiert | Web-Services | |
| | | Host Domain | Implementiert | Web-Services | |
| | | Host-Installierter Speicher | Implementiert | Web-Services | |
| | | Host-Modell | Implementiert | Web-Services | |
| | | Anzahl der NIC | Implementiert | Web-Services | |
| | | NIC-Geschwindigkeit | Implementiert | Web-Services | |
| | | IPS | Implementiert | Web-Services | |
| | | Hersteller | Implementiert | Web-Services | |
| | | Name | Implementiert | Web-Services | |
| | | OID | Implementiert | Web-Services | |
| | | Plattformtyp | Implementiert | Web-Services | |
| | ISCSI-Knoten | Host-Aliase | Implementiert | Web-Services | |
| | | Node-Name | Implementiert | Web-Services | |
| | | OID | Implementiert | Web-Services | |
| | | Typ | Lücke | Web-Services | |
| | Info | Api-Beschreibung | Implementiert | Web-Services | |
| | | Api-Name | Implementiert | Web-Services | |
| | | Api-Version | Implementiert | Web-Services | |
| | | Client-Api-Name | Implementiert | Web-Services | |
| | | Client-Api-Version | Implementiert | Web-Services | |
| | | Name der Datenquelle | Implementiert | Web-Services | Info |
| | | Datum | Implementiert | Web-Services | |
| | | Ersteller-ID | Implementiert | Web-Services | |

Von diesem Datensammler verwendete Management-APIs:

| API | Verwendetes Protokoll | Verwendetes Transportschicht-Protokoll | Eingehende Ports verwendet | Verwendete ausgehende Ports | Unterstützt Authentifizierung | Erfordert nur die „Schreibgeschützt“-Anmeldedaten | Unterstützung Von Verschlüsselung | Firewall-freundlich (statische Ports) |
|---|---|---|---|---|---|---|---|---|
| VMware REST-API | Web-Services | HTTP/HTTPS | 80/443 | | Richtig | Richtig | Richtig | Richtig |

# Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

## Urheberrecht

http://www.netapp.com/us/legal/copyright.aspx

## 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.

http://www.netapp.com/us/legal/netapptmlist.aspx

## Patente

Eine aktuelle Liste der NetApp Patente finden Sie unter:

https://www.netapp.com/us/media/patents-page.pdf

## Datenschutzrichtlinie

https://www.netapp.com/us/legal/privacypolicy/index.aspx

## Hinweis

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis für OnCommand Insight 7.3.16"

"Hinweis für OnCommand Insight 7.3.15"

"Hinweis für OnCommand Insight 7.3.14"

"Hinweis für OnCommand Insight 7.3.13"

**Copyright-Informationen**

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

**Markeninformationen**

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