Konfiguration und Administration

OnCommand Insight

NetApp
October 24, 2024

Inhalt

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`

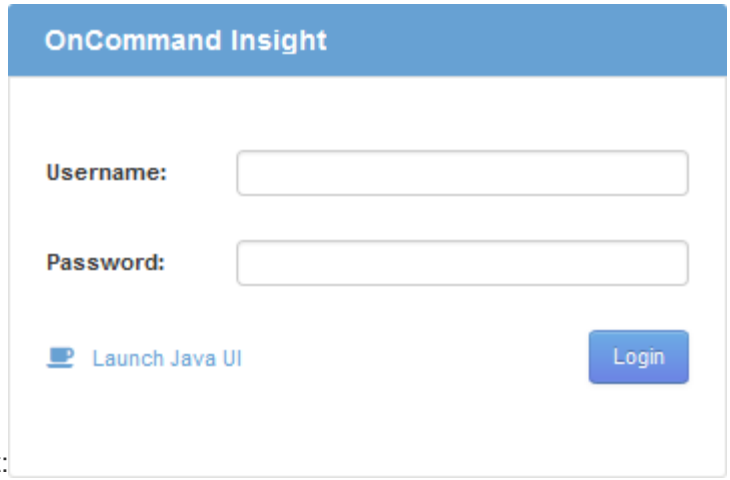
   - Insight von jedem beliebigen anderen Speicherort aus öffnen:

     `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. • wildfly/Standalone/Configuration/Vault/* • acq/conf/Vault/* 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. 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: • Stimmt der Hash des Passworts für OCI-Benutzer mit dem Wert in der Datenbank überein • Für MySQL-Benutzer kann eine Datenbankverbindung hergestellt werden • 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. Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Kennwörtern im wiederhergestellten Tresor entspricht: • Aktualisieren Sie die Benutzerpasswörter für die OCI-Kommunikation • Aktualisieren Sie die MySQL-Benutzerpasswörter, einschließlich Root • Wenn das Schlüsselspeicher-Passwort „bekannt“ ist, aktualisieren Sie den Schlüsselspeicher mit den Kennwörtern aus dem wiederhergestellten Tresor. 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: • Aktualisiert die Benutzerpasswörter für die OCI-Kommunikation • 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 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 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 Wenn DWH und Windows, aktualisieren Sie die Windows-Registrierung, um die folgenden ODBC-bezogenen Einträge auf das neue Passwort zu setzen: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • 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>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value	Backup-Vault
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip
Backup-Vault	`securityadmin [-s`

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

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

Change-Passwort für Akquisitionsbenutzer (Akquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]` `where` `-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>]` `where` `-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>` `where` `-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.

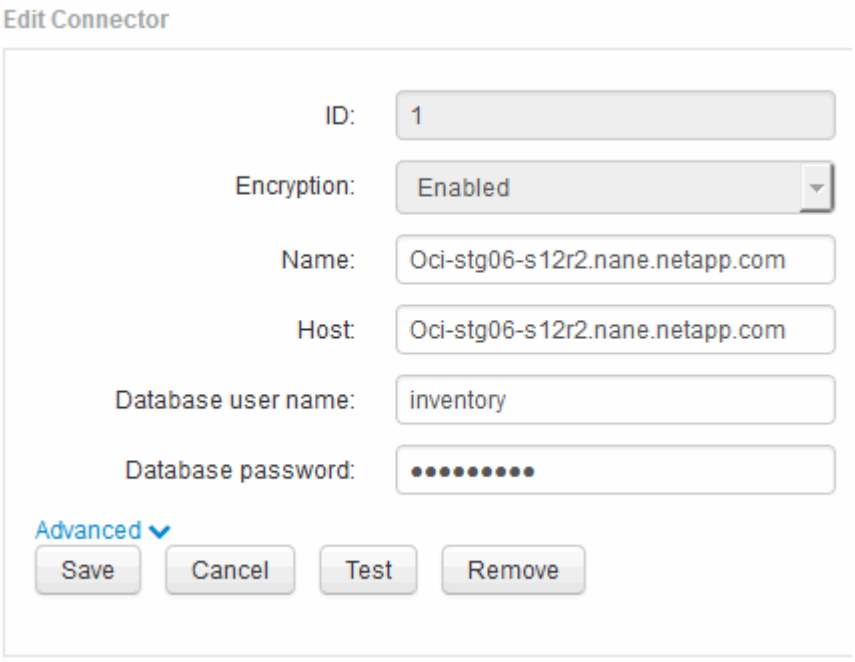
Bevor Sie beginnen

Sie müssen als Administrator angemeldet sein, um diese Aufgabe ausführen zu können.

Schritte

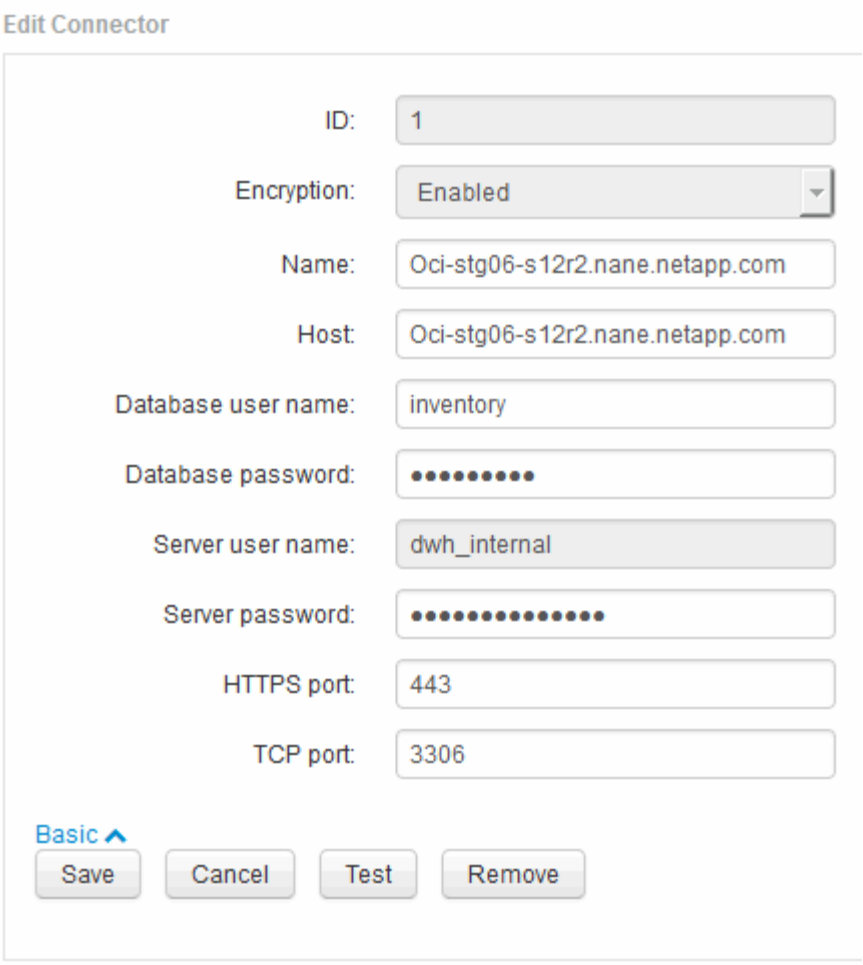
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   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.

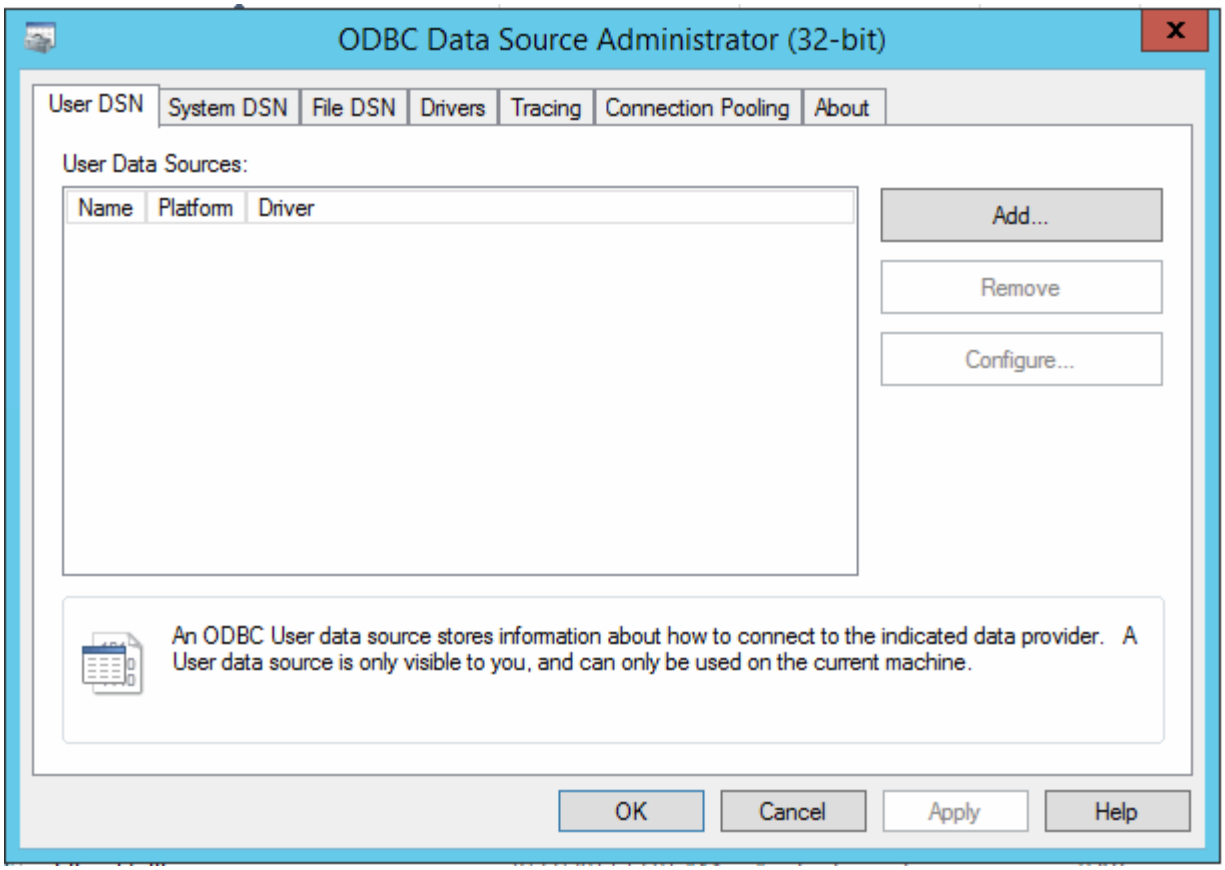
Bevor Sie beginnen

Sie müssen eine Remote-Anmeldung beim Data Warehouse-Server mit einem Konto mit Administratorrechten durchführen.

Schritte

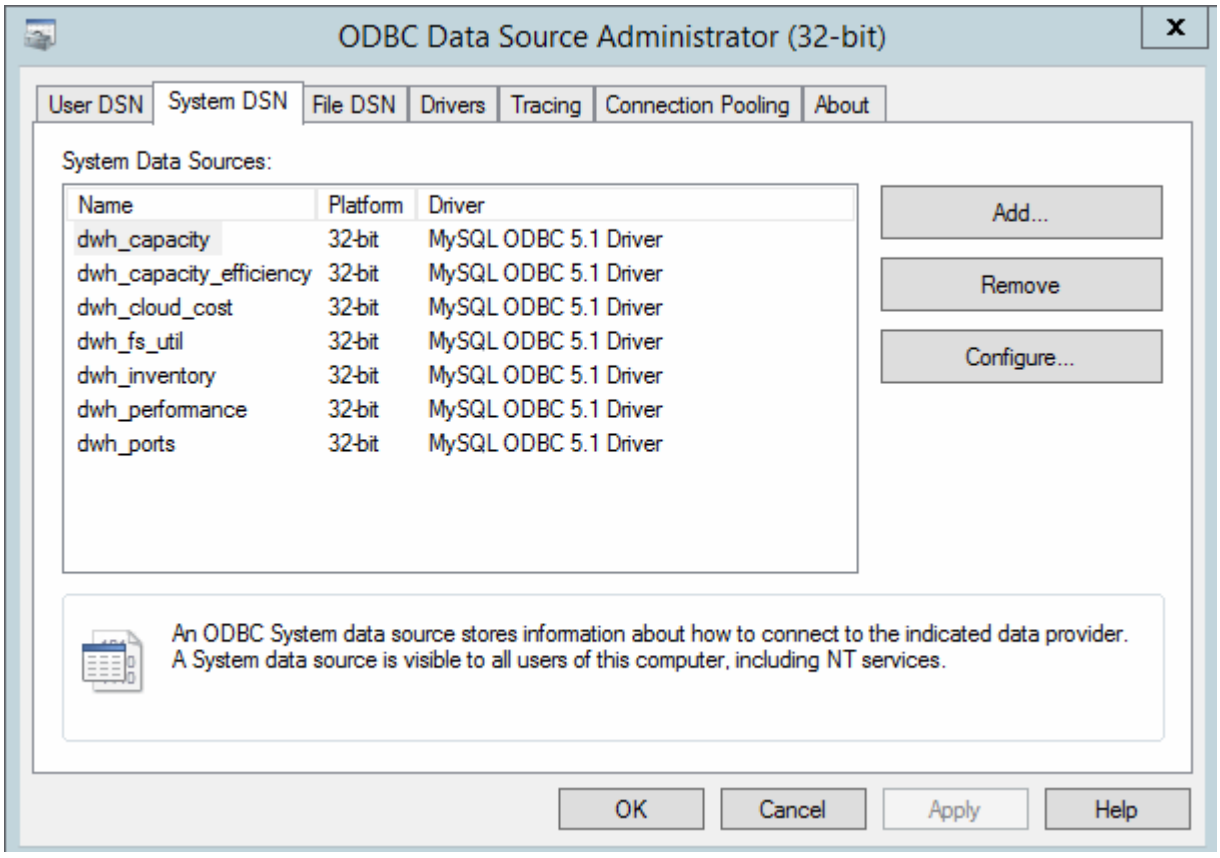
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

   Das System zeigt den ODBC-Bildschirm „Data Source Administrator“ an.



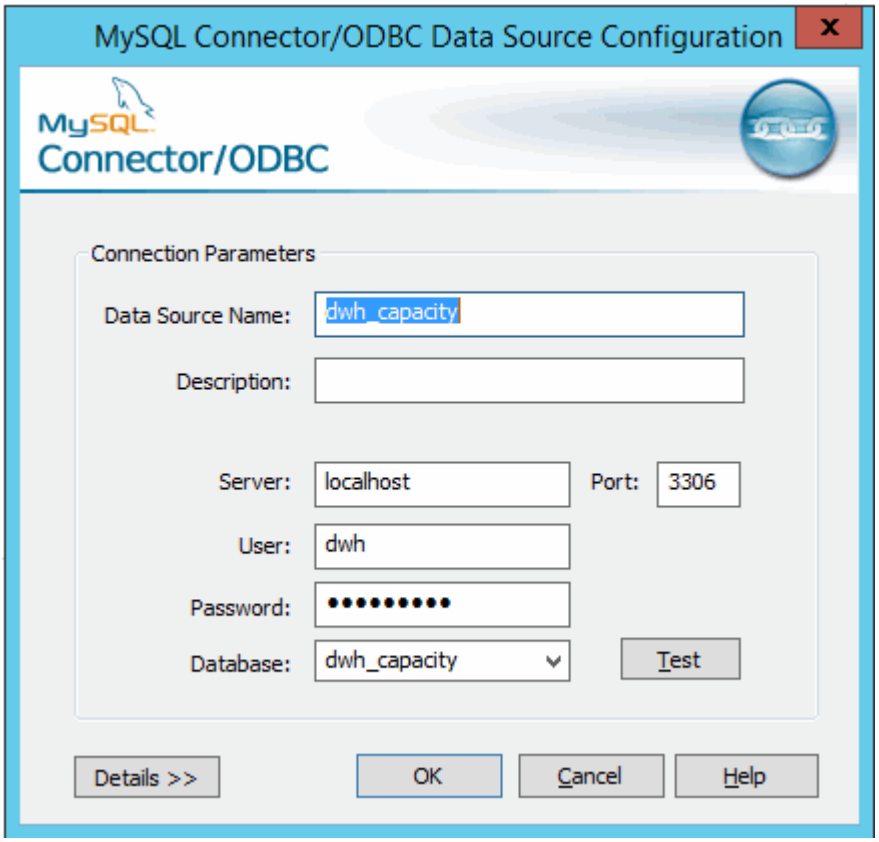
3. Klicken Sie auf **System DSN**

   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.
```

+

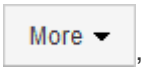
Ändern von Abfragen

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.

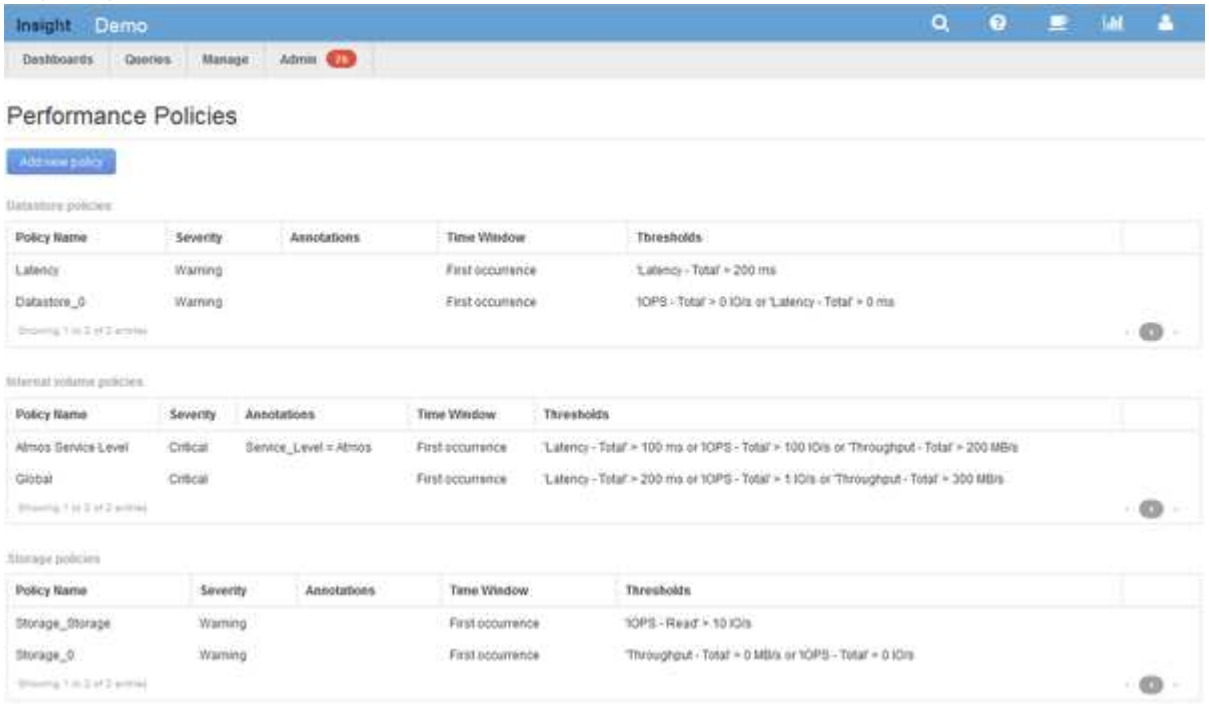
Erstellung von Performance-Richtlinien

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. • wildfly/Standalone/Configuration/Vault/* • 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. 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: • Stimmt der Hash des Passworts für OCI-Benutzer mit dem Wert in der Datenbank überein • Für MySQL-Benutzer kann eine Datenbankverbindung hergestellt werden • 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. Führt alle koordinierten Aktionen durch, um die Installation so zu aktualisieren, dass sie den Kennwörtern im wiederhergestellten Tresor entspricht: • Aktualisieren Sie die Benutzerpasswörter für die OCI-Kommunikation • Aktualisieren Sie die MySQL-Benutzerpasswörter, einschließlich Root • Wenn das Schlüsselspeicher-Passwort „bekannt“ ist, aktualisieren Sie den Schlüsselspeicher mit den Kennwörtern aus dem wiederhergestellten Tresor. 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: • Aktualisiert die Benutzerpasswörter für die OCI-Kommunikation • 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 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 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 Wenn DWH und Windows, aktualisieren Sie die Windows-Registrierung, um die folgenden ODBC-bezogenen Einträge auf das neue Passwort zu setzen: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • 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>] `where` -pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value	Backup-Vault
`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip
Backup-Vault	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file	Listentasten

`` securityadmin [-s ```	-au] [-db] -l where -l specified command ```
Prüfschlüssel	``` securityadmin [-s ```
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ```	Verify-keystore (Server)
`` securityadmin [-s] [-db] -v where -v specified command ```	Upgrade
`` securityadmin [-s ```	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ```

Schlüssel ersetzen	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	Restore-Vault-Backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``
Change-Password (Server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]` `where` `-up specified command ("update-password")` `-un <user> entry ("user") name to update` `-p <password> new password. If <password not supplied, user will be prompted.` `-sh for mySQL user, use strong hash`
Change-Passwort für Akquisitionsbenutzer (Akquisition)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]` `where` `-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>]` `where` `-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>` `where` `-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.

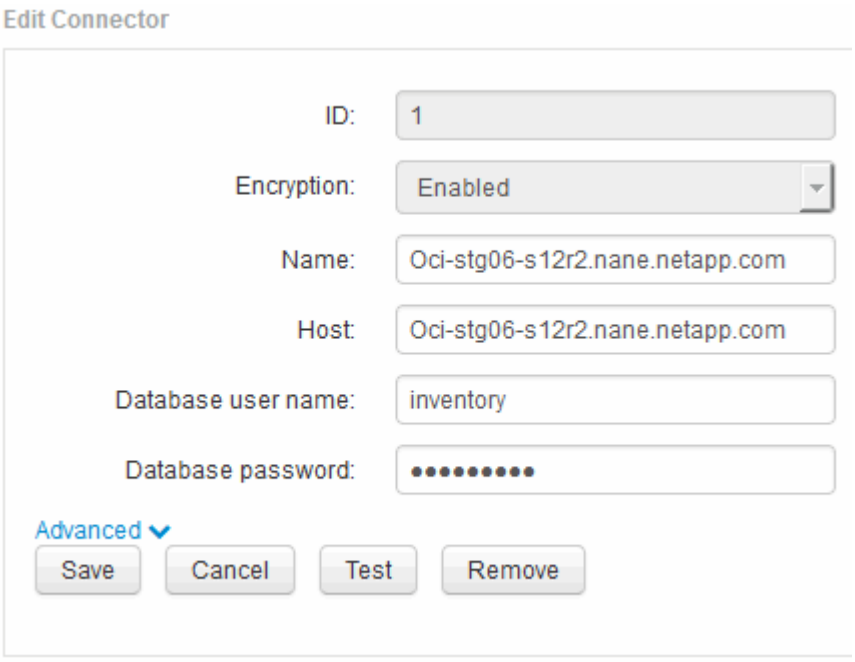
Bevor Sie beginnen

Sie müssen als Administrator angemeldet sein, um diese Aufgabe ausführen zu können.

Schritte

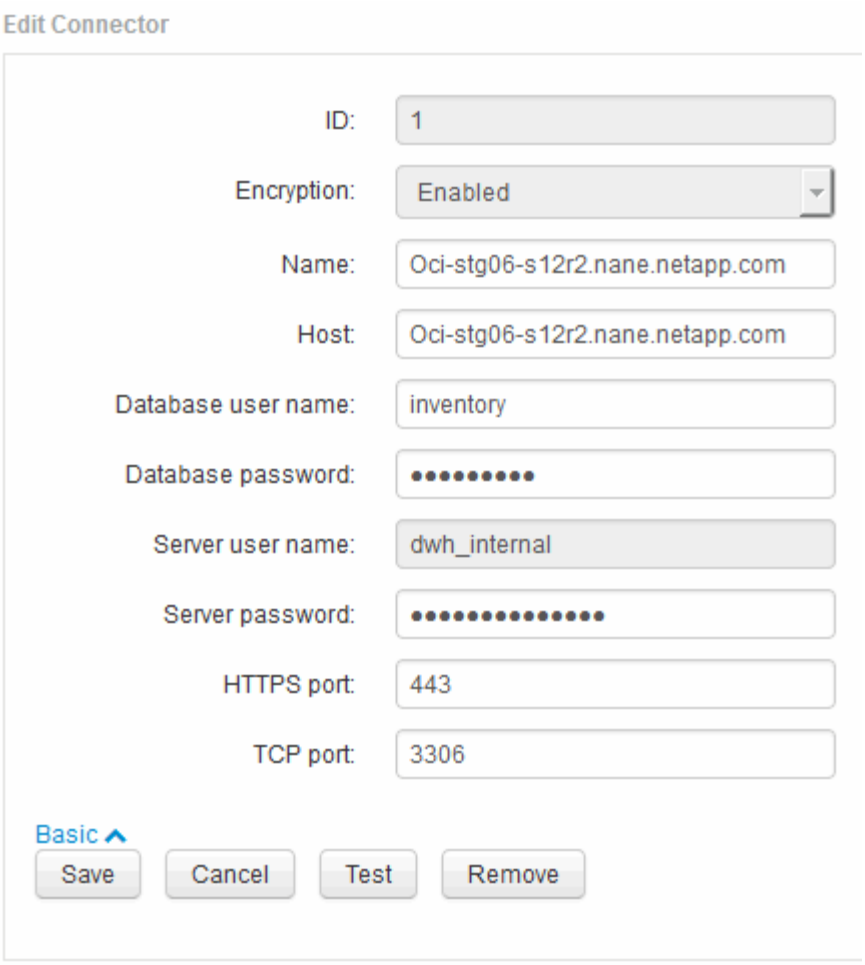
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   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.

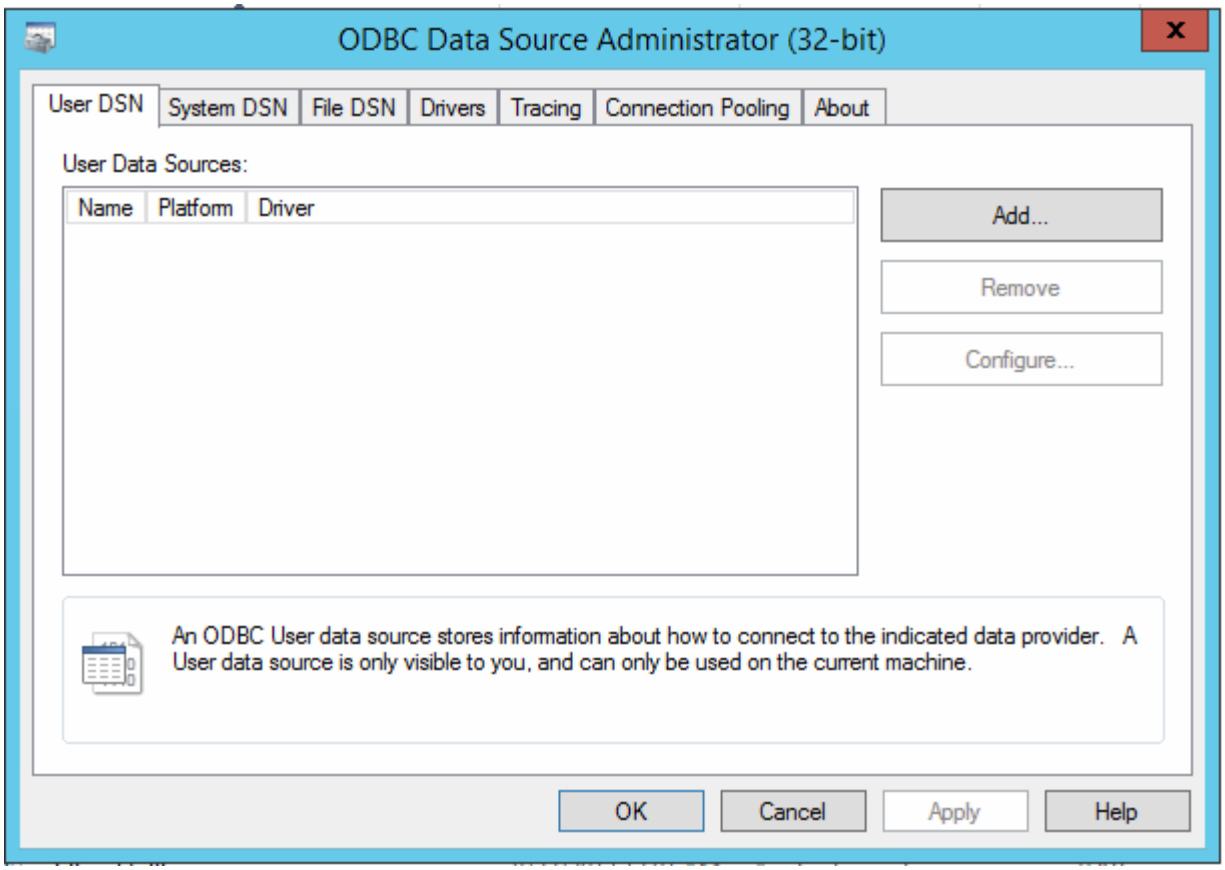
Bevor Sie beginnen

Sie müssen eine Remote-Anmeldung beim Data Warehouse-Server mit einem Konto mit Administratorrechten durchführen.

Schritte

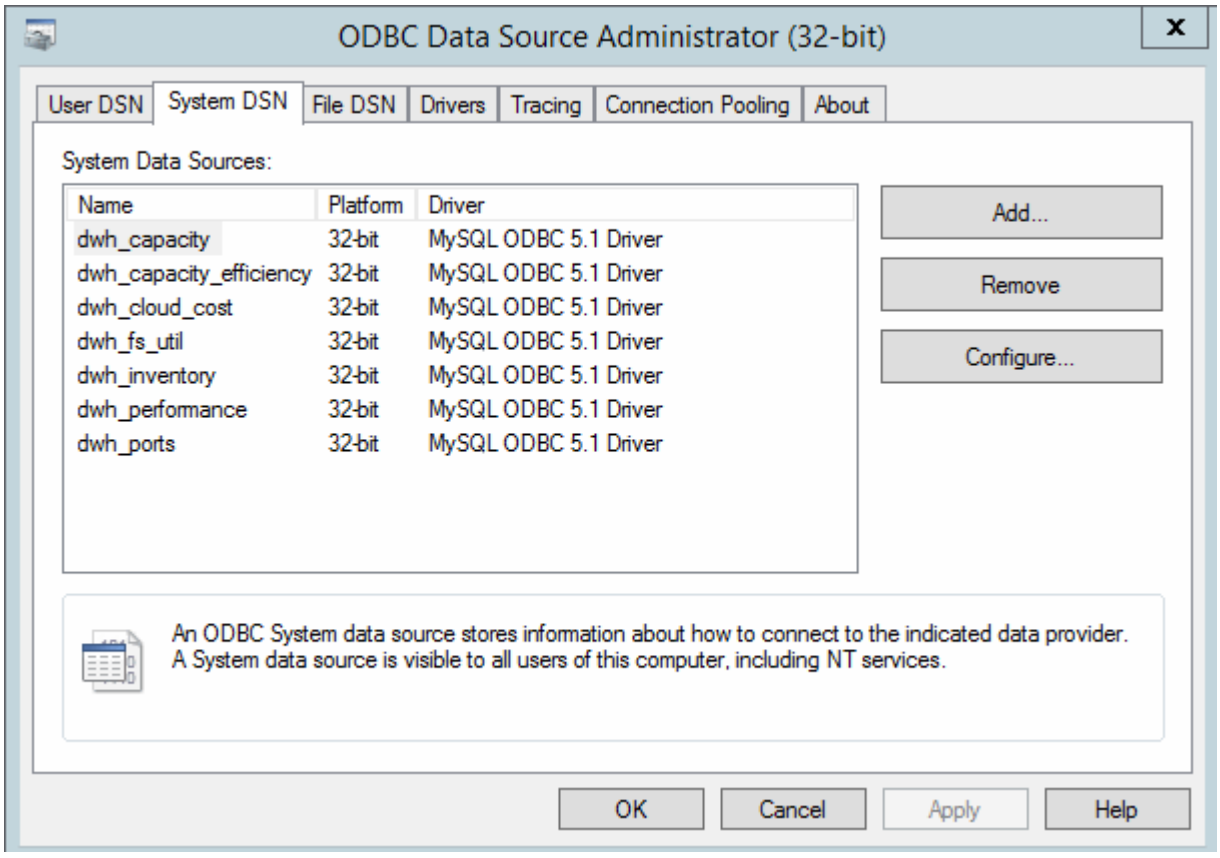
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

   Das System zeigt den ODBC-Bildschirm „Data Source Administrator“ an.



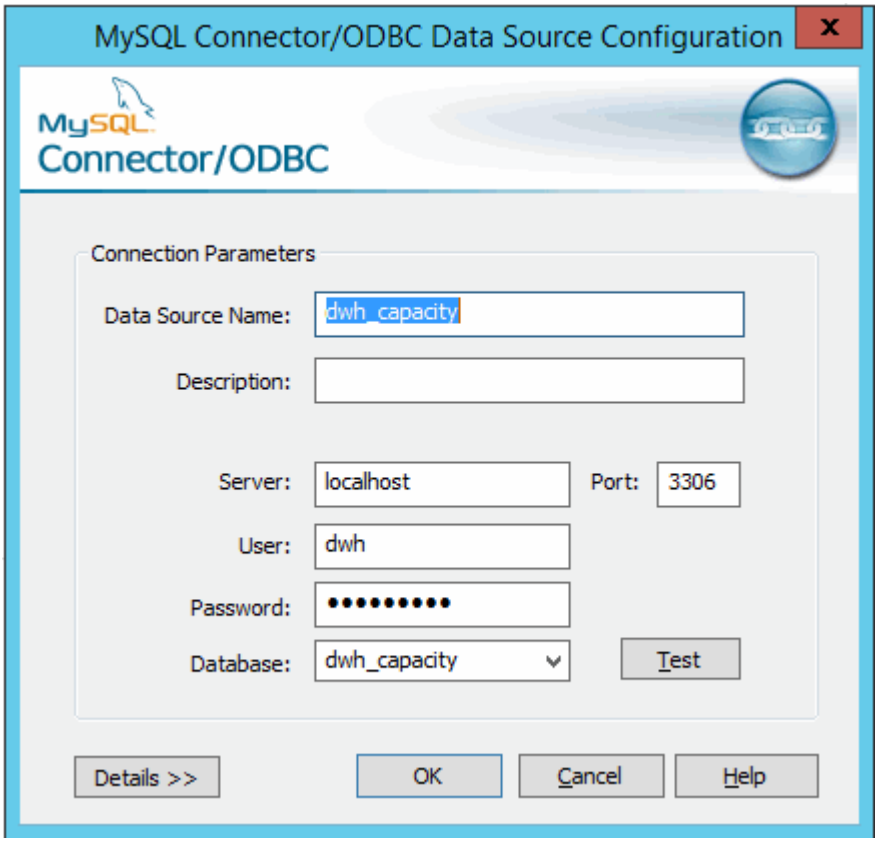
3. Klicken Sie auf **System DSN**

   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 

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 

, 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 

, 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.

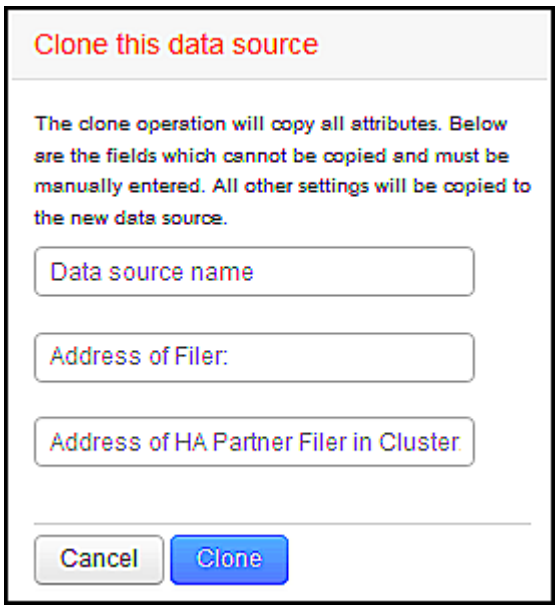
Schritte

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: • **Geräte-Alias** 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). • **Keine** Melden Sie keinen Alias • **Port-Beschreibung** Eine Beschreibung zur Identifizierung des Ports in einer Liste von Ports • **Zone Alias (alle)** Ein benutzerfreundlicher Name für einen Port, der nur für die Zonenkonfiguration verwendet werden kann • **Zone Alias (nur aktiv)** 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: • 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. • 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. • 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. 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 Raid-Gruppe	Storage-Pool
Standard-Volume, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), 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: • IP-Adresse des Arrays: IP-Adresse des Speichers • Benutzername: Benutzername für den Speicher • Passwort: Passwort für den Speicher • 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: • IP-Adresse des Arrays: IP-Adresse des Speichers • Speicher Navigator CLI-Pfad: SNM2 CLI-Pfad • Kontoauthentifizierung gültig: Wählen Sie die Option zur Auswahl einer gültigen Kontokertifizierung aus • Benutzername: Benutzername für den Speicher • 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: • IP-Adresse des Arrays: IP-Adresse des Speichers • Benutzername: Benutzername für den Speicher • Passwort: Passwort für den Speicher • 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: • IP-Adresse des Arrays: IP-Adresse des Speichers • Speicher Navigator CLI-Pfad: SNM2 CLI-Pfad • Kontoauthentifizierung gültig: Wählen Sie die Option zur Auswahl einer gültigen Kontokertifizierung aus • Benutzername: Benutzername für den Speicher • 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: • 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 • Wählen Sie im Dropdown-Menü „Bereich“ die Option „Analyse“ aus. Eine Liste der möglichen Eigenschaften wird angezeigt. • Klicken Sie auf das oberste Kontrollkästchen und es werden alle drei Eigenschaften ausgewählt.- Klicken Sie auf die Schaltfläche Hinzufügen auf der rechten Seite. • 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

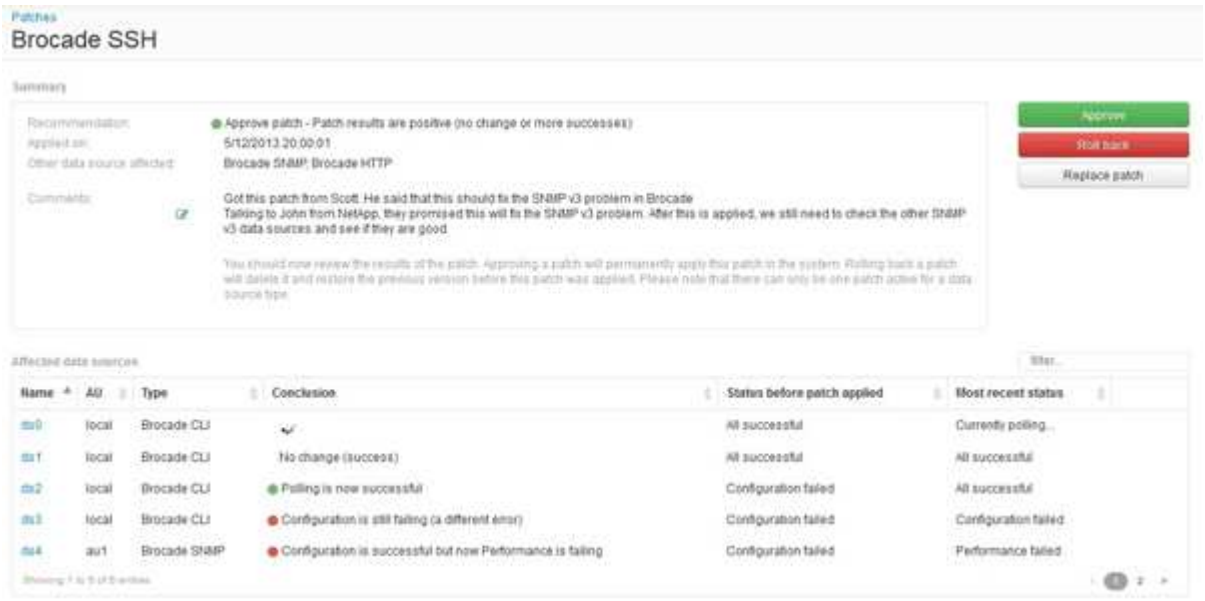
Sie haben einen Patch installiert und müssen entscheiden, ob der Patch erfolgreich ist und genehmigt werden sollte.

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.

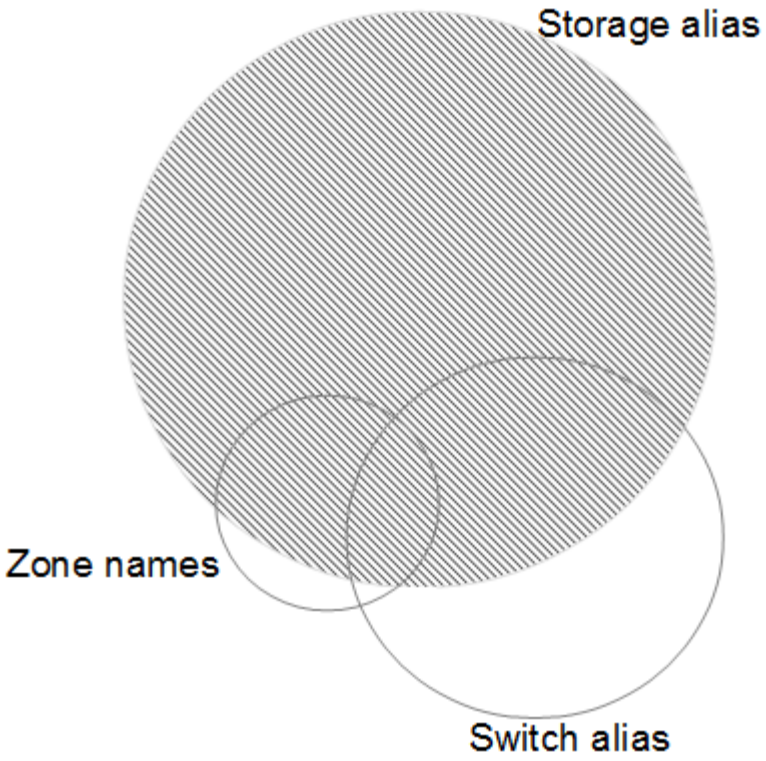
Bevor Sie beginnen

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?

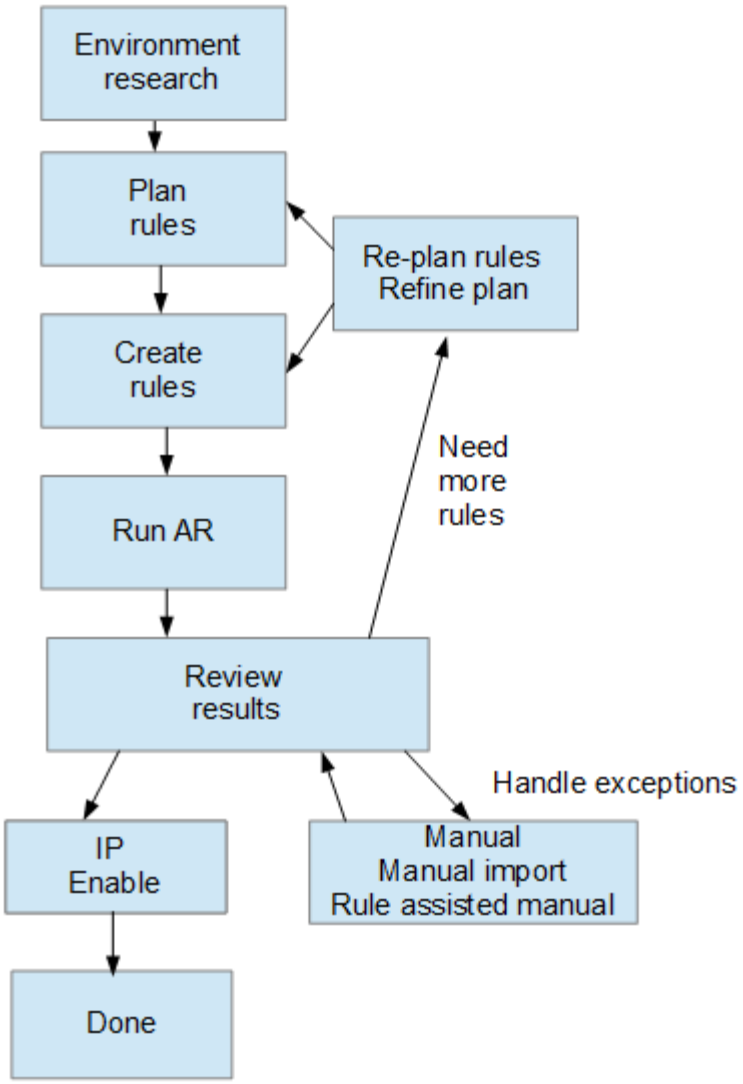
Nach der Analyse Ihrer Umgebung sollten Sie in der Lage sein, zu identifizieren, welche Benennungsstandards existieren, die Sie mit der Zuverlässigkeit rechnen können. Die gesammelten Informationen können grafisch in einer Abbildung dargestellt werden, die der folgenden ähnelt:



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 • Speicheralias, der einen eingebetteten Host- oder Bandnamen enthält • Switch-Alias, der einen eingebetteten Host- oder Bandnamen enthält • 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) • Trennzeichen • 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.

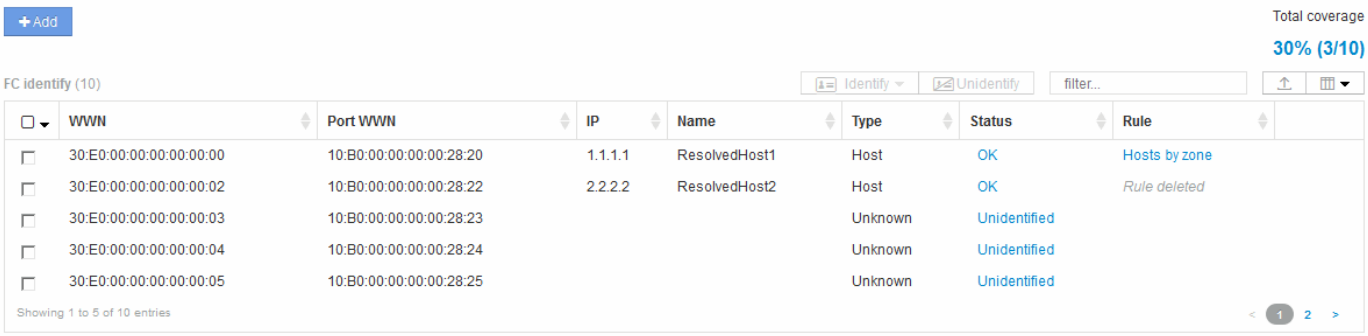
   OnCommand Insight führt den Host-Auflösungsprozess in der Reihenfolge aus, in der die Methoden angezeigt werden, beginnend mit den Methoden oben.

   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:

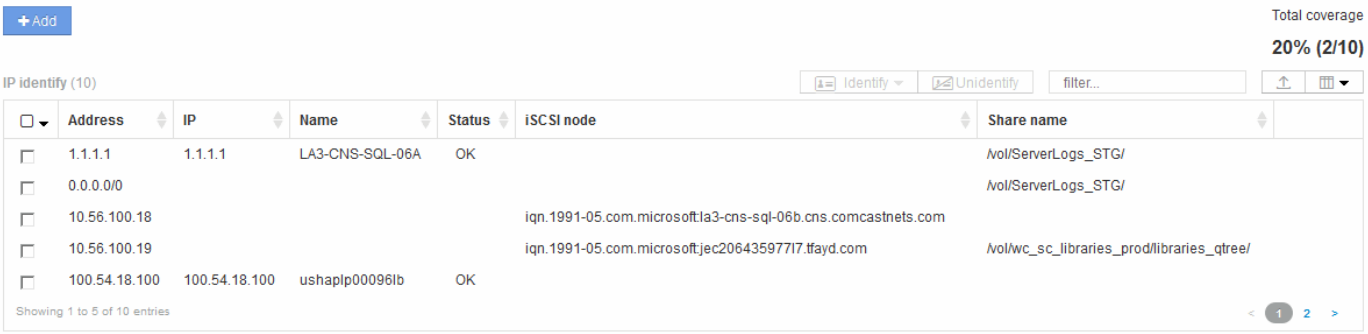
WWN
IP
Name
Typ

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. + „Ungültiger Sicherungsort“, wenn das Sicherungsverzeichnis ungültig ist. + zeigt die letzte erfolgreiche Telefonhomezeit sowie die Zeit des letzten fehlgeschlagenen Versuchs an, falls verfügbar. + „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. + „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. + „Cluster Mode detected“, wenn mehr als ein Knoten erkannt wird. + „hohe Speicherauslastung“, wenn der genutzte Heap-Speicherplatz mehr als 85 % beträgt. + "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. + "`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. + 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. + „Verletzungsmanager ist blockiert“, wenn die Anzahl der offenen Verstöße am Grenzwert für Verstöße liegt. + 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

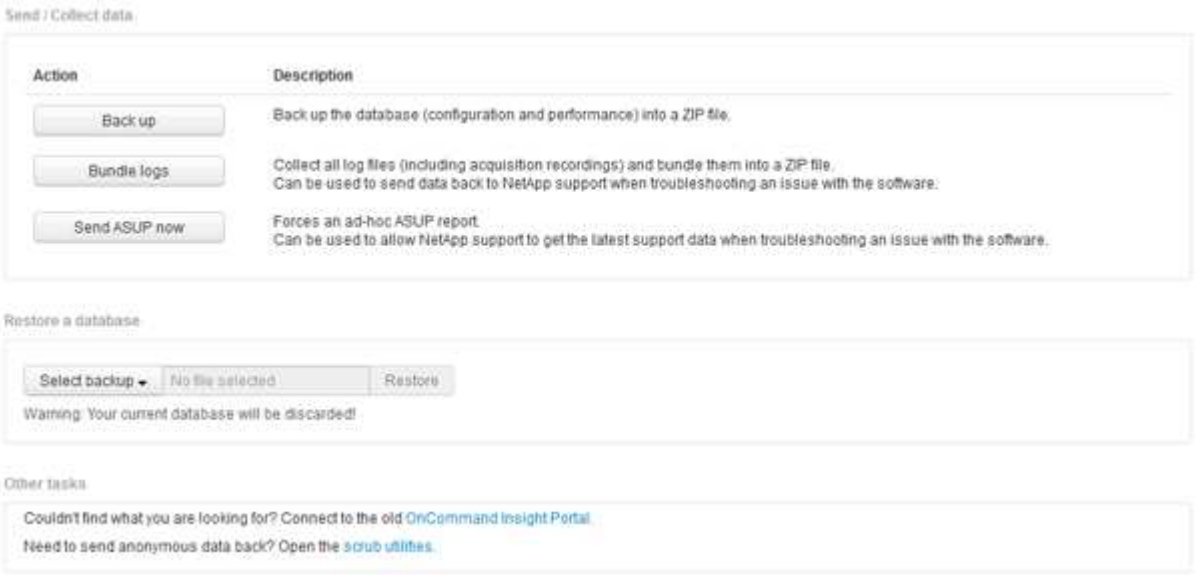
Um Ihre Insight-Datenbank aus einer verifizierten Sicherungsdatei wiederherzustellen, verwenden Sie die Fehlerbehebungsoptionen. Dieser Vorgang ersetzt Ihre aktuellen OnCommand Insight-Daten vollständig.

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

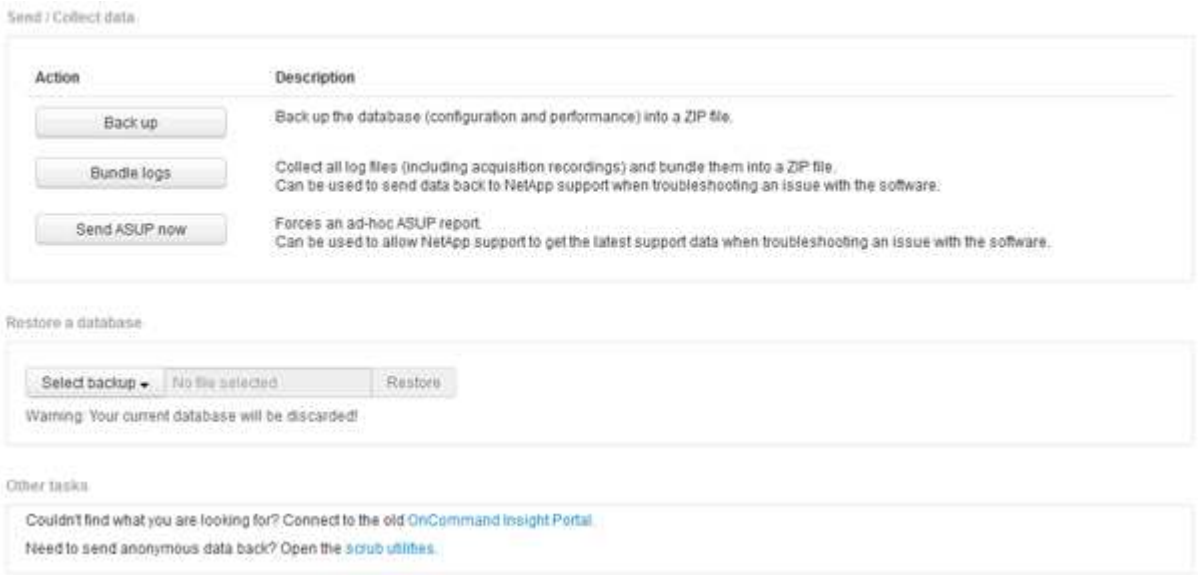
1. Klicken Sie in der Insight-Symbolleiste auf **Admin**.
2. Klicken Sie Auf **Fehlerbehebung**.
3. Klicken Sie im Abschnitt Daten senden/erfassen auf **Paketprotokolle**.
4. Klicken Sie Auf **Datei Speichern**.
5. Klicken Sie auf **OK**.

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`“ • Name • Anbieter • Modell

Storage Pool	• „storagepool“ • Name • Name des Speichers • IP-Adressen des Speichers • Seriennummer des Speichers • Storage-Anbieter • Storage-Modell • Namen für alle zugeordneten internen Volumes • Namen für alle zugeordneten Festplatten
Internes Volumen	• „internalvolume“ • Name • Name des Speichers • IP-Adressen des Speichers • Seriennummer des Speichers • Storage-Anbieter • Storage-Modell • Name des Speicherpools • Namen aller zugeordneten Freigaben • Namen aller zugehörigen Applikationen und Geschäftseinheiten
Datenmenge	• „Volume“ • Name • Etikett • Namen aller internen Volumes • Name des Speicherpools • Name des Speichers • IP-Adressen des Speichers • Seriennummer des Speichers • Storage-Anbieter • Storage-Modell

Storage-Node	• „storagenode“ • Name • Name des Speichers • IP-Adressen des Speichers • Seriennummer des Storage • Storage-Anbieter • Storage-Modell
Host	• „Host“ • Name • IP-Adressen • Namen aller zugehörigen Applikationen und Geschäftseinheiten
Datenspeicher	• „Datastore“ • Name • IP des virtuellen Zentrums • Namen aller Volumes • Namen aller internen Volumes
Virtual Machines	• „virtualmachine“ • Name • DNS-Name • IP-Adressen • Name des Hosts • IP-Adressen des Hosts • Namen aller Datastores • Namen aller zugehörigen Applikationen und Geschäftseinheiten

Switches (normal und Kapitalwert)	• „sHexe“ • IP-Adresse • wwn • Name • Seriennummer • Modell • Domänen-ID • Name der Fabric • wwn der Fabric
Applikation	• „Anwendung“ • Name • Mandant • Geschäftsbereich • Geschäftseinheit • Projekt
Tape	• „Tape“ • IP-Adresse • Name • Seriennummer • Anbieter
Port	• „Port“ • wwn • Name
Fabric	• „Stoff“ • wwn • 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.

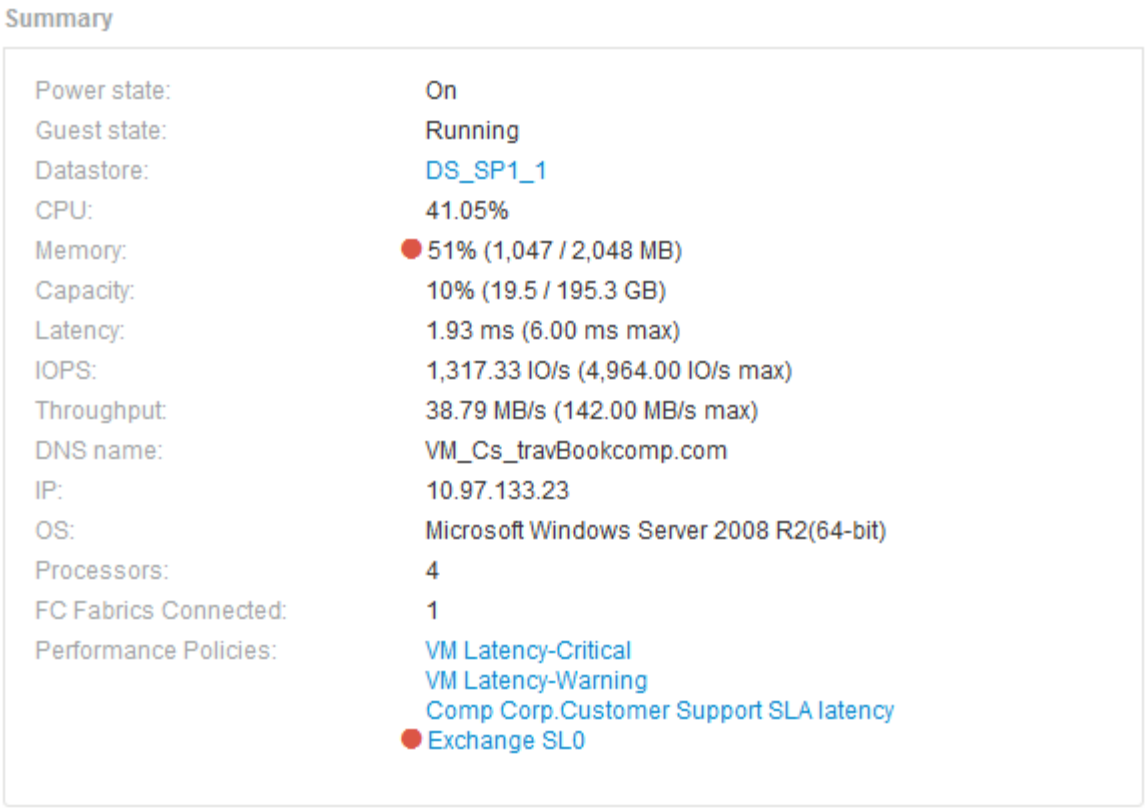
Abschnitte der Anlagenseite

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.

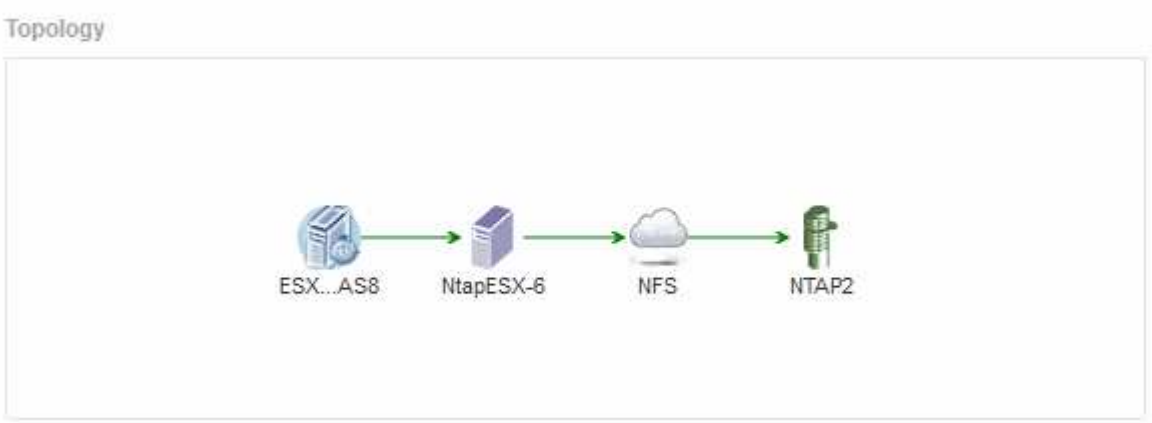
5. Falls zutreffend, können Sie auf einen Link zu einer Leistungsrichtlinie klicken, um die mit der Ressource verbundenen Leistungsrichtlinien oder -Richtlinien anzuzeigen.

   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.

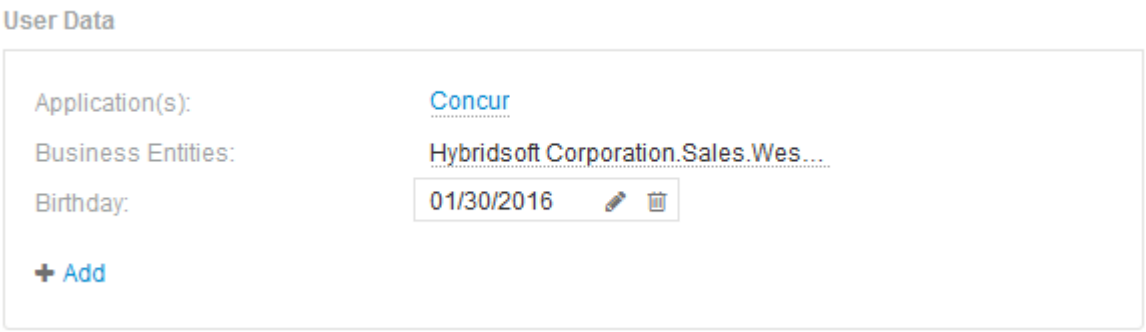
Wenn die Topologie für das Asset größer ist, als in den Abschnitt passt, klicken Sie auf den Link *Klicken, um den Topologie-Hyperlink zu sehen.

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. 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. Latenz: Durchschnittliche Antwortzeit der Virtual Machines in einem Datenspeicher. 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). 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.

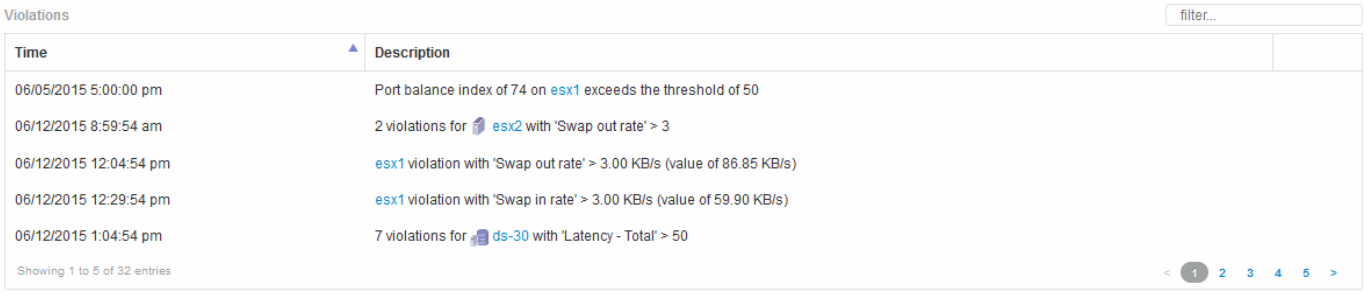
3. So steuern Sie, wie Assets in der Tabelle angezeigt werden:
   - Klicken Sie auf den Namen einer Anlage, um die zugehörige Anlagenseite anzuzeigen.
   - Verwenden Sie das Feld **Filter**, um nur bestimmte Assets anzuzeigen.
   - Klicken Sie auf eine Seitenzahl, um die Assets nach Seite zu durchsuchen, 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.

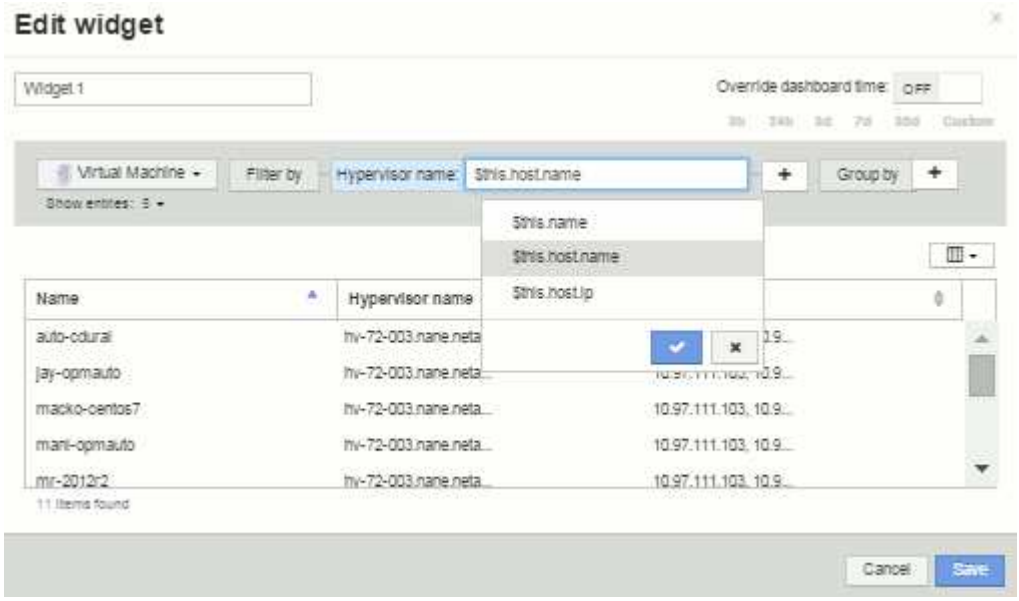
4. Wir wollen alle virtuellen Maschinen anzeigen. Klicken Sie auf die Asset Selector und ändern Sie **Storage** in **Virtual Machine**.

   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

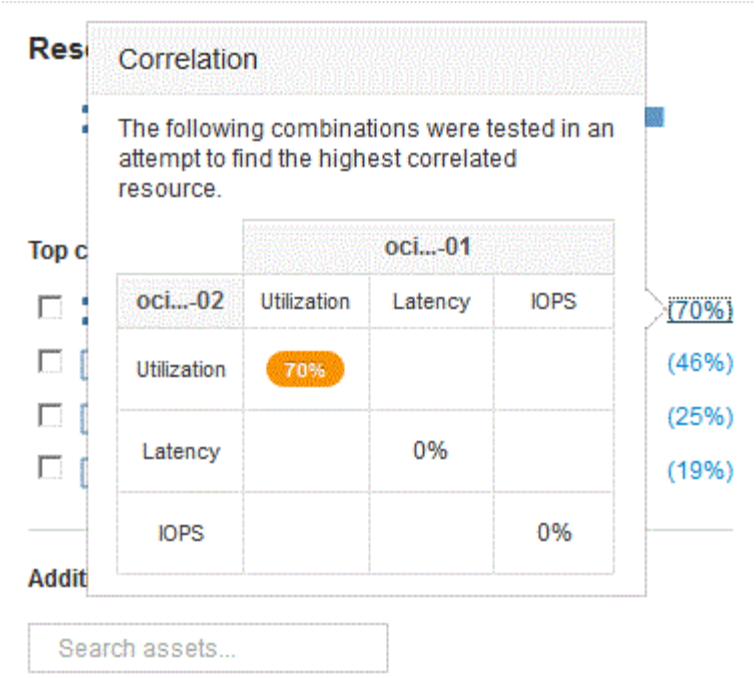
Wenn Sie Leistungsprobleme untersuchen und die *Asset-Seite* für ein Gerät öffnen, sollten Sie die Liste Top Correlated Resources verwenden, um die in den Leistungsdiagrammen angezeigten Daten zu verfeinern. Eine Ressource mit einem hohen Prozentsatz zeigt an, dass die Ressource ähnliche Vorgänge wie 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.

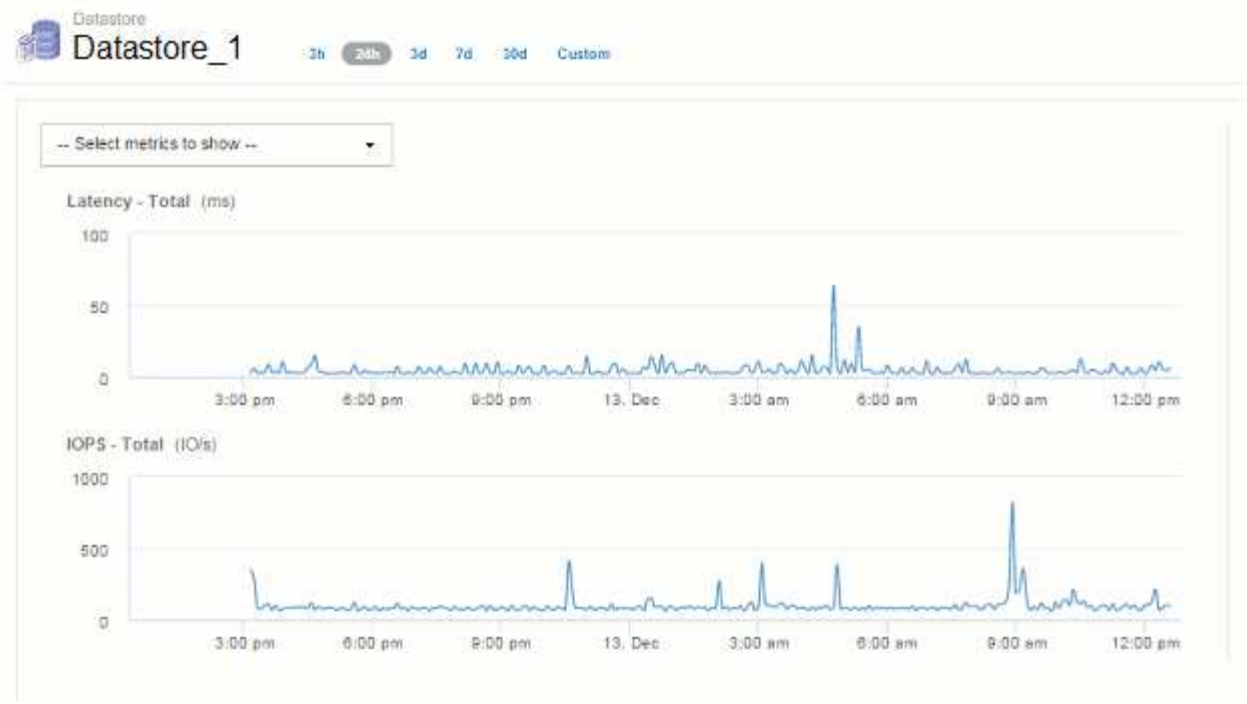
Funktionsweise von Downsampling

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	
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 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					

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**	**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) 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**	**Funktion/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					
450					

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**	**Funktion/Attribut**	**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					

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	
	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 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

Produkt	Kategorie	Funktion/Attribut	Status	Verwendetes Protokoll	Weitere Informationen
		Speicherpool-Id	Implementiert	HDS-XML-API	
		Thin Provisioning Typ	Implementiert	HDS-XML-API	
		Tiering Lücke	Implementiert	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					

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**
		QoS begrenzt 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/Attrib ut**	**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					
640					

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