Insight einrichten

OnCommand Insight

NetApp
April 01, 2024

Inhalt

Insight einrichten . . . 1
- Zugriff auf die Web-UI . . . 1
- Installieren Ihrer Insight Lizenzen . . . 2
- Einrichten und Verwalten von Benutzerkonten . . . 7
- Festlegen einer Warnmeldung für die Anmeldung . . . 15
- Insight Sicherheit . . . 16
- Unterstützung für Smart Card- und Zertifikatanmeldung . . . 30
- Konfigurieren des Data Warehouse für die Smart Card- und Zertifikatanmeldung . . . 43
- Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.5 bis 7.3.9) . . . 44
- Konfigurieren von Cognos für Smart Card- und Zertifikatanmeldung (OnCommand Insight 7.3.10 und höher) . . . 46
- Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.5 auf 7.3.9) . . . 47
- Importieren von CA-signierten SSL-Zertifikaten für Cognos und DWH (Insight 7.3.10 und höher) . . . 50
- SSL-Zertifikate werden importiert . . . 52
- Einrichtung wöchentlicher Backups für Ihre Insight-Datenbank . . . 55
- Archivierung von Performance-Daten . . . 56
- Konfigurieren Ihrer E-Mail-Adresse . . . 58
- Konfigurieren von SNMP-Benachrichtigungen . . . 59
- Aktivieren der Syslog-Funktion . . . 60
- Konfiguration der Performance und Sicherstellung von Benachrichtigungen über Verstöße . . . 61
- Konfigurieren von Ereignisbenachrichtigungen auf Systemebene . . . 62
- Konfigurieren der ASUP Verarbeitung . . . 63
- Definieren von Anwendungen . . . 64
- Die Hierarchie Ihrer Geschäftseinheiten . . . 67
- Anmerkungen definieren . . . 70
- Elemente werden abgefragt . . . 86
- Management von Performance-Richtlinien . . . 93
- Importieren und Exportieren von Benutzerdaten . . . 98

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
     ```

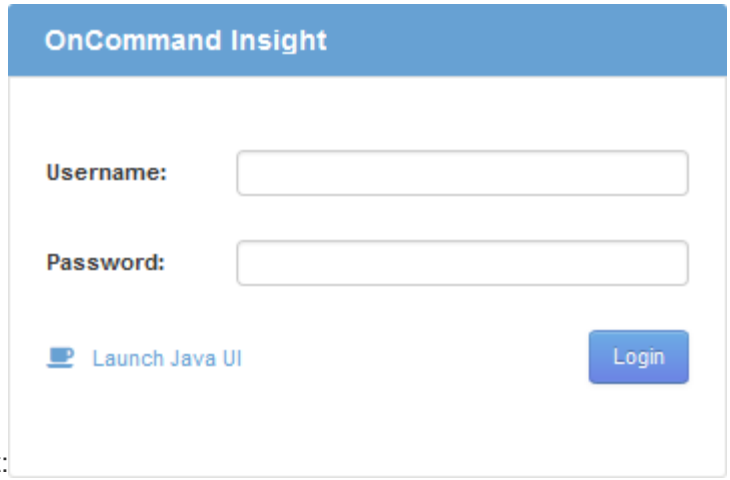
   - Insight von jedem beliebigen anderen Speicherort aus öffnen:

     ```
     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.

> 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.

> 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.

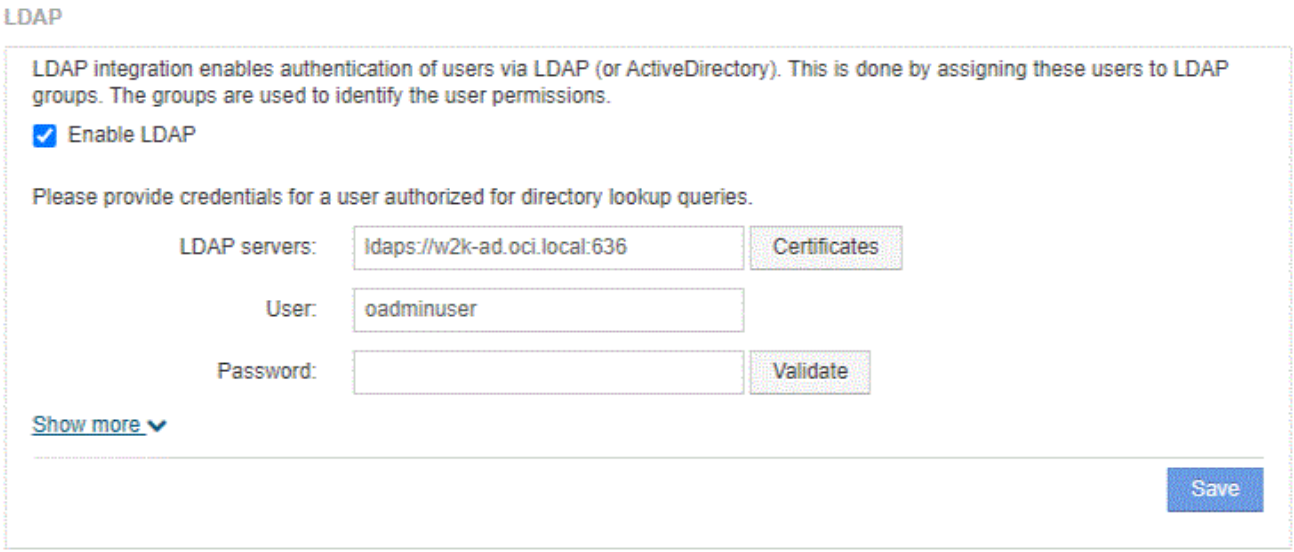
Über diese Aufgabe

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. Scrollen Sie zum LDAP-Abschnitt, wie hier gezeigt.



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.

Insight Sicherheit

In Version 7.3.1 von OnCommand Insight wurden Sicherheitsfunktionen eingeführt, mit denen Insight Umgebungen noch sicherer arbeiten können. Zu den Funktionen gehören Verbesserungen der Verschlüsselung, das Hashing von Passwörtern und die Möglichkeit, interne Benutzer-Passwörter und Schlüsselpaare zu ändern, die Passwörter verschlüsseln und entschlüsseln. Sie können diese Funktionen auf allen Servern in der Insight-Umgebung verwalten.

Die Standardinstallation von Insight beinhaltet eine Sicherheitskonfiguration, bei der alle Standorte in Ihrer Umgebung dieselben Schlüssel und dieselben Standardpasswörter verwenden. Zum Schutz sensibler Daten empfiehlt NetApp, die Standardschlüssel und das Erfassungs-Benutzerpasswort nach einer Installation oder einem Upgrade zu ändern.

Verschlüsselte Passwörter der Datenquelle werden in der Insight Server-Datenbank gespeichert. Der Server verfügt über einen öffentlichen Schlüssel und verschlüsselt Passwörter, wenn ein Benutzer sie auf einer WebUI-Datenquellkonfigurationsseite eingibt. Der Server verfügt nicht über die privaten Schlüssel, die zum Entschlüsseln der in der Server-Datenbank gespeicherten Datenquellkennwörter erforderlich sind. Nur Acquisition Units (LAU, rau) verfügen über den privaten Schlüssel der Datenquelle, der zum Entschlüsseln von Passwörtern für Datenquellen erforderlich ist.

Server werden neu keying

Die Verwendung von Standardschlüsseln führt zu einer Sicherheitsanfälligkeit in Ihrer Umgebung. Standardmäßig werden Datenquellkennwörter in der Insight-Datenbank verschlüsselt gespeichert. Sie werden verschlüsselt und verwenden einen Schlüssel, der für alle Insight-Installationen verwendet wird. In einer Standardkonfiguration enthält eine an NetApp gesendete Insight Datenbank Passwörter, die theoretisch von NetApp entschlüsselt werden können.

Ändern des Benutzerpassworts für die Erfassung

Durch die Verwendung des standardmäßigen Benutzerpasswords für die Akquisition wird die Sicherheitslücke in Ihrer Umgebung behoben. Alle Akquisitionseinheiten verwenden den Benutzer „`Acquisition`“, um mit dem Server zu kommunizieren. Raus mit Standardpasswörtern kann theoretisch eine Verbindung zu jedem Insight-

Server herstellen, wobei Standardpasswörter verwendet werden.

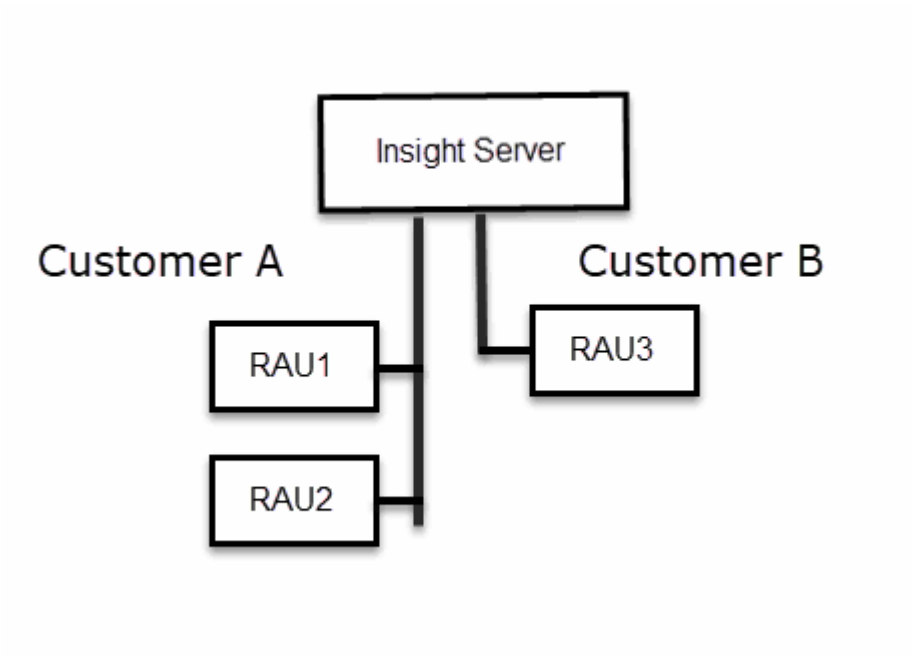
Überlegungen zu Upgrades und Installationen

Wenn Ihr Insight-System nicht standardmäßige Sicherheitskonfigurationen enthält (Sie haben ein Rekeying durchgeführt oder Passwörter geändert), müssen Sie Ihre Sicherheitskonfigurationen sichern. Durch die Installation neuer Software oder in einigen Fällen eines Software-Upgrades wird das System auf eine Standardsicherheitskonfiguration zurückgesetzt. Wenn Ihr System auf die Standardkonfiguration zurückgesetzt wird, müssen Sie die nicht voreingestellte Konfiguration wiederherstellen, damit das System ordnungsgemäß funktioniert.

Schlüsselmanagement in einer komplexen Service-Provider-Umgebung

Ein Service-Provider kann mehrere OnCommand Insight-Kunden hosten, die Daten erfassen. Die Schlüssel schützen Kundendaten vor unberechtigtem Zugriff durch mehrere Kunden auf dem Insight Server. Die Daten jedes Kunden werden durch spezifische Schlüsselpaare geschützt.

Diese Implementierung von Insight kann wie in der folgenden Abbildung dargestellt konfiguriert werden.



Sie müssen in dieser Konfiguration für jeden Kunden individuelle Schlüssel erstellen. Kunde A benötigt identische Schlüssel für beide raus. Kunde B benötigt einen einzigen Schlüsselsatz.

Die Schritte, die Sie Unternehmen würden, um die Verschlüsselungsschlüssel für Kunde A zu ändern:

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU1 gehostet wird.
2. Starten Sie das Sicherheitsadministrator-Tool.
3. Wählen Sie Verschlüsselungsschlüssel ändern, um die Standardschlüssel zu ersetzen.
4. Wählen Sie Backup, um eine ZIP-Sicherungsdatei der Sicherheitskonfiguration zu erstellen.
5. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU2 gehostet wird.
6. Kopieren Sie die Sicherungszip-Datei der Sicherheitskonfiguration auf RAU2.
7. Starten Sie das Sicherheitsadministrator-Tool.

8. Stellen Sie die Sicherheitssicherung von RAU1 auf dem aktuellen Server wieder her.

Die Schritte, die Sie Unternehmen würden, um die Verschlüsselungsschlüssel für Kunde B zu ändern:

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem RAU3 gehostet wird.
2. Starten Sie das Sicherheitsadministrator-Tool.
3. Wählen Sie Verschlüsselungsschlüssel ändern, um die Standardschlüssel zu ersetzen.
4. Wählen Sie Backup, um eine ZIP-Sicherungsdatei der Sicherheitskonfiguration zu erstellen.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Insight-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.
4. Wählen Sie **Server**.

   Die folgenden Serverkonfigurationsoptionen stehen zur Verfügung:

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

> Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Ändern des Server-Verschlüsselungsschlüssels auf einem Server - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server

- **Verschlüsselungsschlüssel Ändern**

  Ändern Sie den Server-Verschlüsselungsschlüssel, der zum Verschlüsseln oder Entschlüsseln von Proxy-Benutzerpasswörtern, SMTP-Benutzerpasswörtern, LDAP-Benutzerpasswörtern usw. verwendet wird.

  > Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Passwort Aktualisieren**

  Ändern Sie das Passwort für die internen Konten, die von Insight verwendet werden. Folgende Optionen werden angezeigt:

  - _Intern
  - Akquisition
  - cognos_admin
  - dwh_intern
  - Hosts
  - Inventar
  - Stamm

> Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt Schlüssel und Passwörter auf die Standardwerte zurück. Standardwerte sind die Werte, die während der Installation angegeben werden.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

  a. Wählen Sie die Option aus, die Sie ändern möchten, und folgen Sie den Anweisungen.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Insight-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.
4. Wählen Sie **Local Acquisition Unit** aus, um die Sicherheitskonfiguration der Local Acquisition Unit neu zu konfigurieren.

   Folgende Optionen werden angezeigt:

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

> Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf DEM LAU ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf jedem der Raus

- **Verschlüsselungsschlüssel Ändern**

  Ändern Sie die AU-Verschlüsselungsschlüssel, die zum Verschlüsseln oder Entschlüsseln von Gerätepasswörtern verwendet werden.

  > Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Passwort Aktualisieren**

  Passwort für 'Acquisition'-Benutzerkonto ändern.

  > Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt das Erfassungs-Benutzerpasswort und die Erfassungs-Benutzerverschlüsselungsschlüssel auf die Standardwerte zurück. Bei der Installation werden die Standardwerte angegeben.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

5. Wählen Sie die Option aus, die Sie konfigurieren möchten, und befolgen Sie die 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

Benutzerpasswords für die 'Erfassung', wenn das Passwort für diesen Benutzer auf dem Server geändert wurde. Für die Kommunikation mit dem Server verwenden alle RAUS und DIE LAU dasselbe Passwort wie das des Benutzers „Acquisition“ des Servers.

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.

Gehen Sie wie folgt vor, um Sicherheitsoptionen auf einer rau zu verwalten:

Schritte

1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem die rau ausgeführt wird
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.

   Das System zeigt das Menü für die rau an.

   - **Backup**

     Erstellt eine Sicherungszip-Datei des Tresors, die alle Passwörter und Schlüssel enthält und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an den folgenden Standardstandorten ab:

     - Fenster – `C:\Program Files\SANscreen\backup\vault`
     - Linux `/var/log/netapp/oci/backup/vault`
   - **Wiederherstellen**

     Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

     > Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf einem Server ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server
   - **Verschlüsselungsschlüssel Ändern**

     Ändern Sie die rau-Verschlüsselungsschlüssel, die zum Verschlüsseln oder Entschlüsseln von Gerätekennwörtern verwendet werden.

     > Wenn Sie die Verschlüsselungsschlüssel ändern, sollten Sie Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.
   - **Passwort Aktualisieren**

Passwort für 'Acquisition'-Benutzerkonto ändern.

> Einige Konten müssen synchronisiert werden, wenn Passwörter geändert werden. Wenn Sie beispielsweise das Passwort für den Benutzer „Acquisition“ auf dem Server ändern, müssen Sie das Kennwort für den Benutzer „Acquisition“ auf DER LAU, rau und DWH ändern, damit es übereinstimmt. Wenn Sie Kennwörter ändern, sollten Sie außerdem Ihre neue Sicherheitskonfiguration sichern, damit Sie sie nach einem Upgrade oder einer Installation wiederherstellen können.

- **Auf die Standardeinstellungen zurücksetzen**

  Setzt die Verschlüsselungsschlüssel und Passwörter auf die Standardwerte zurück. Standardwerte sind die Werte, die während der Installation angegeben werden.

- **Ausgang**

  Beenden Sie das `securityadmin` Werkzeug.

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`

Schritte

1. Führen Sie eine Remote-Anmeldung beim Data Warehouse-Server durch.
2. Starten Sie das Sicherheitsadministrator-Tool im interaktiven Modus:
   - Fenster – `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux `/bin/oci-securityadmin.sh -i`

     Das System fordert Anmeldeinformationen an.
3. Geben Sie den Benutzernamen und das Kennwort für ein Konto mit „`Admin`“-Anmeldeinformationen ein.

   Das System zeigt das Menü Sicherheitsverwaltung für das Data Warehouse an:

   - **Backup**

     Erstellt eine ZIP-Sicherungsdatei des Tresors, die alle Kennwörter und Schlüssel enthält, und legt die Datei an einem vom Benutzer angegebenen Speicherort oder an dem Standardspeicherort ab:

- Fenster – `C:\Program Files\SANscreen\backup\vault`
- Linux `/var/log/netapp/oci/backup/vault`

◦ **Wiederherstellen**

Stellt die Zip-Sicherung des erstellten Tresors wieder her. Nach der Wiederherstellung werden alle Passwörter und Schlüssel zum Zeitpunkt der Backup-Erstellung auf die vorhandenen Werte zurückgesetzt.

> Restore kann verwendet werden, um Passwörter und Schlüssel auf mehreren Servern zu synchronisieren, zum Beispiel: - Verschlüsselungsschlüssel auf einem Server ändern - Erstellen einer Sicherung des Tresors - Wiederherstellen der Vault-Sicherung auf dem zweiten Server
>
> +

◦ **Chiffrierschlüssel ändern**

Ändern Sie den DWH-Verschlüsselungsschlüssel, der zum Verschlüsseln oder Entschlüsseln von Kennwörtern wie Verbindungskennwörtern und SMPT-Kennwörtern verwendet wird.

◦ **Passwort Aktualisieren**

Kennwort für ein bestimmtes Benutzerkonto ändern.

- _Intern
- Akquisition
- cognos_admin
- dwh
- dwh_intern
- Whuser
- Hosts
- Inventar
- Stamm

> Wenn Sie die Kennwörter für dwhuser, Hosts, Inventar oder Root ändern, haben Sie die Möglichkeit, SHA-256-Passwort-Hashing zu verwenden. Für diese Optionen müssen alle Clients, die auf die Konten zugreifen, SSL-Verbindungen verwenden.

+

◦ **Auf die Standardeinstellungen zurücksetzen**

Setzt die Verschlüsselungsschlüssel und Passwörter auf die Standardwerte zurück. Standardwerte sind die Werte, die während der Installation angegeben werden.

◦ **Ausgang**

Beenden Sie das `securityadmin` Werkzeug.

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.

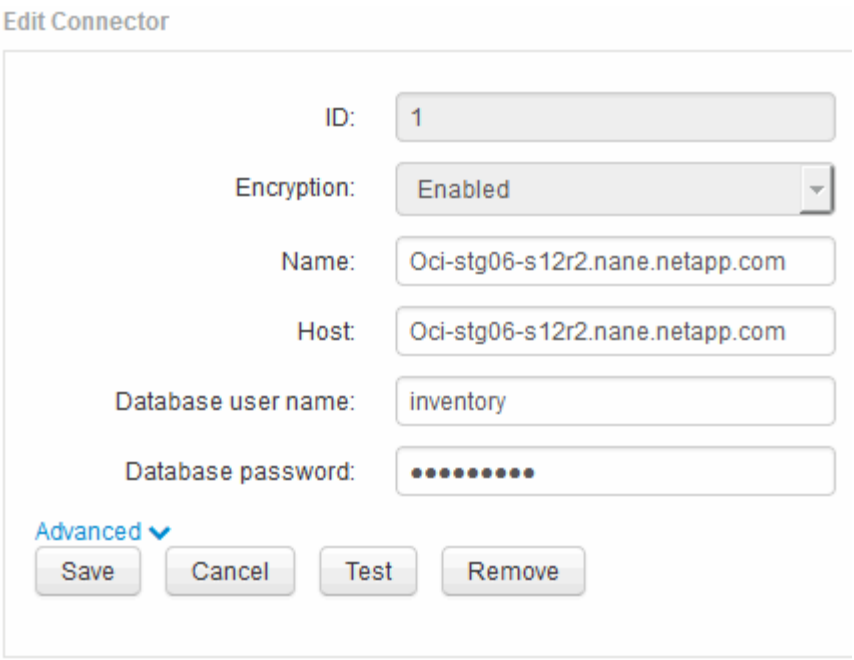
Bevor Sie beginnen

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

Schritte

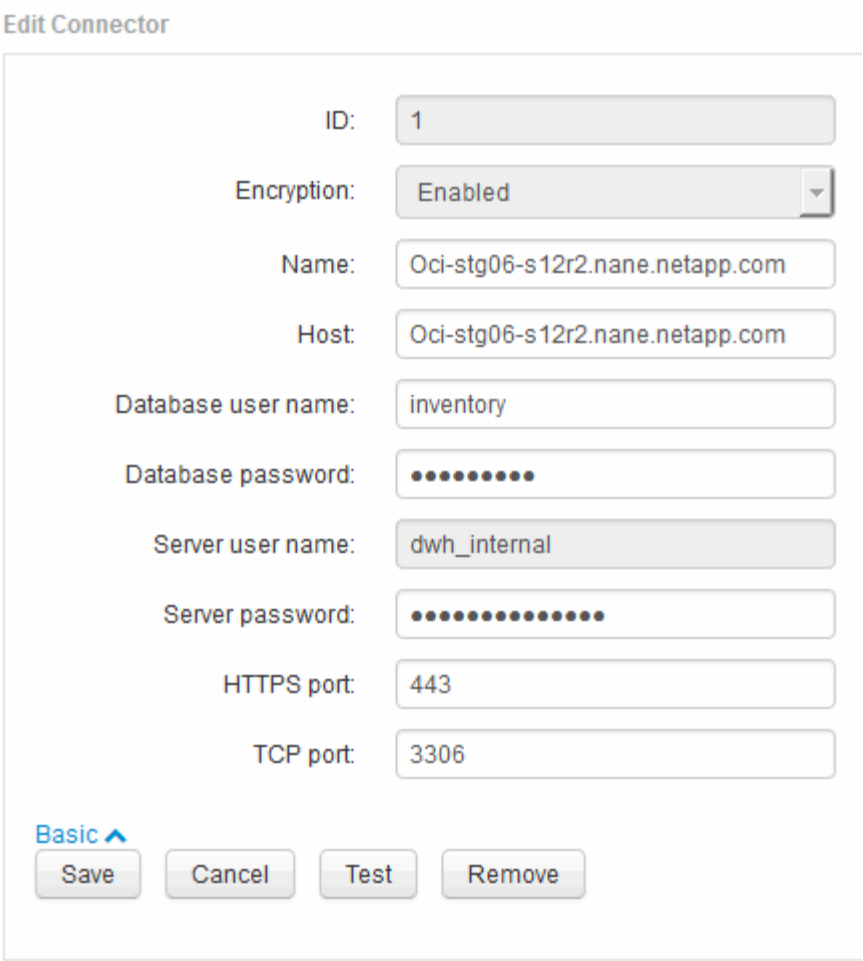
1. Melden Sie sich beim Data Warehouse Portal unter an https://hostname/dwh, Wobei Hostname der Name des Systems ist, auf dem OnCommand Insight Data Warehouse installiert ist.
2. Klicken Sie im Navigationsfenster auf der linken Seite auf **Connectors**.

   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.

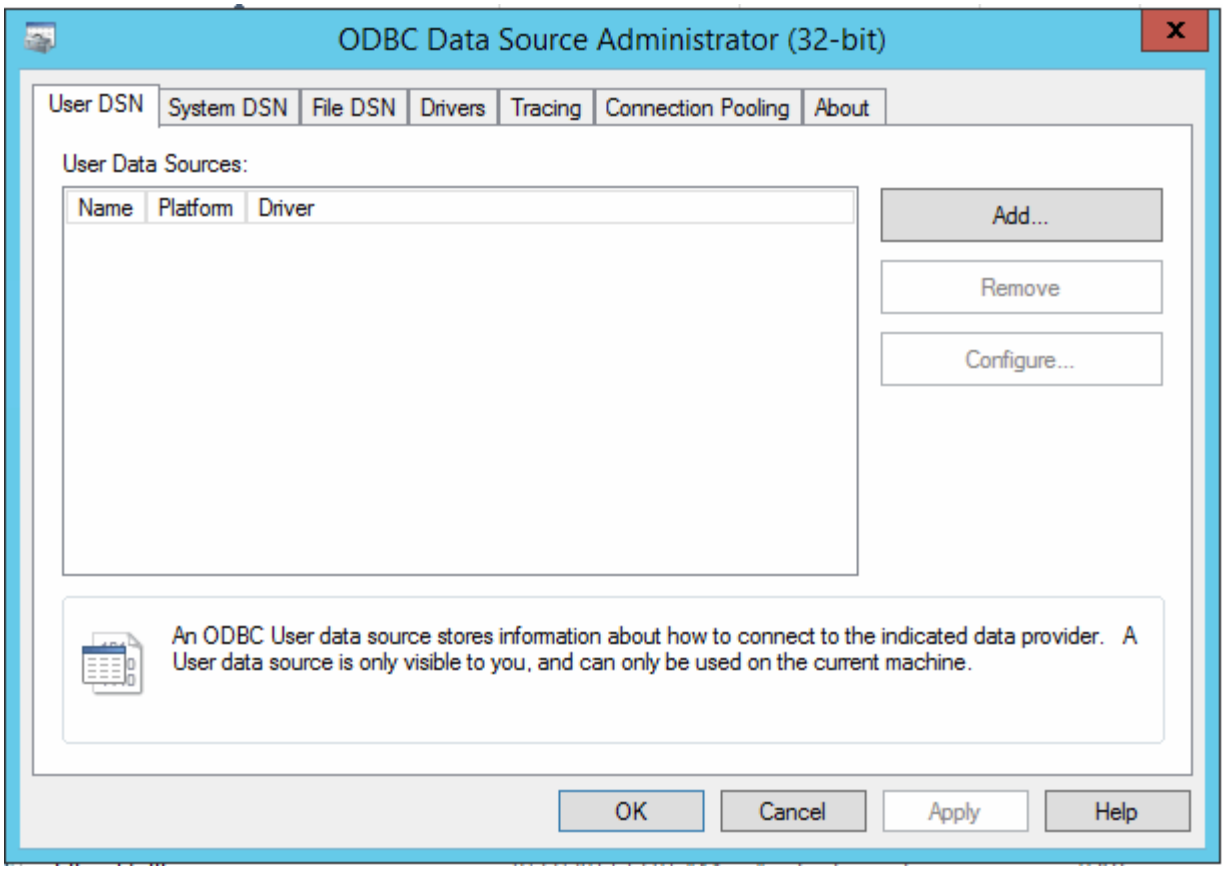
Bevor Sie beginnen

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

Schritte

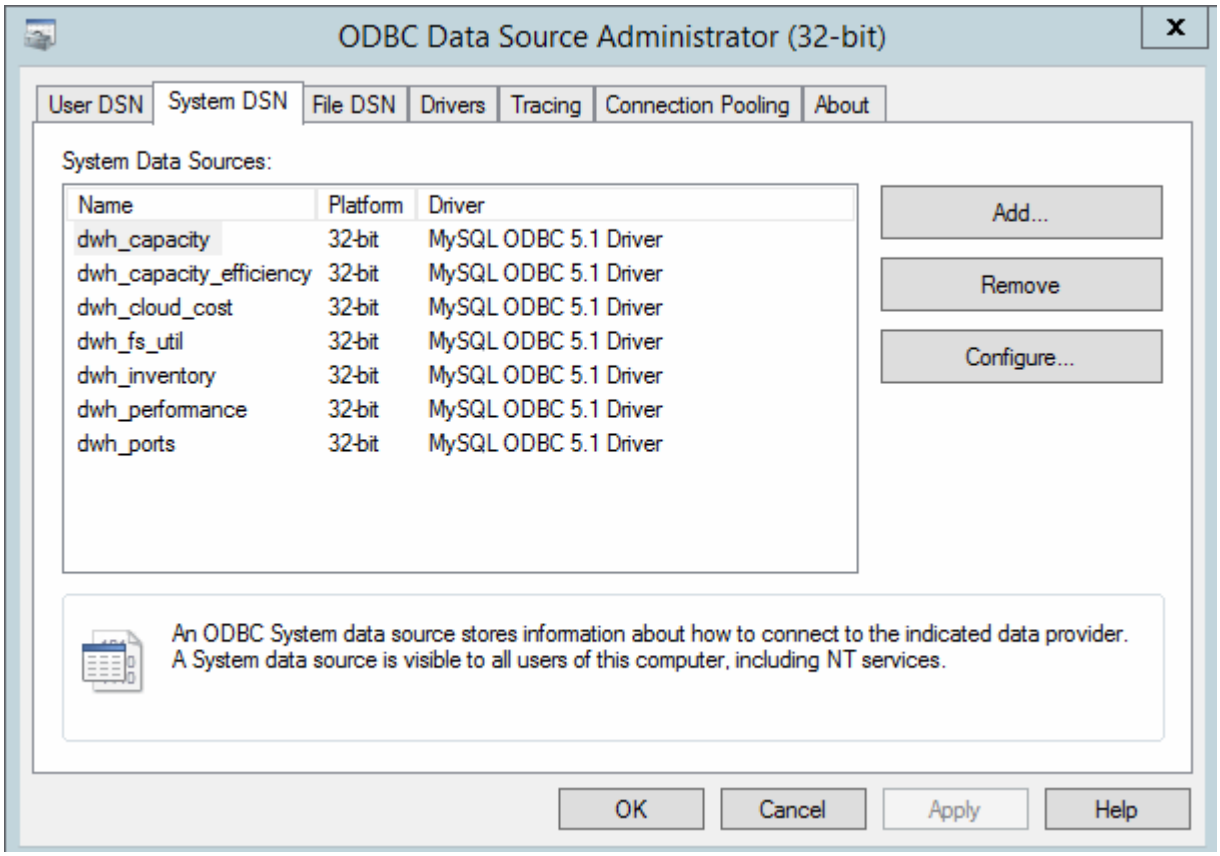
1. Führen Sie eine Remote-Anmeldung beim Server durch, auf dem das Data Warehouse gehostet wird.
2. Rufen Sie das ODBC-Verwaltungstool unter auf `C:\Windows\SysWOW64\odbcad32.exe`

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



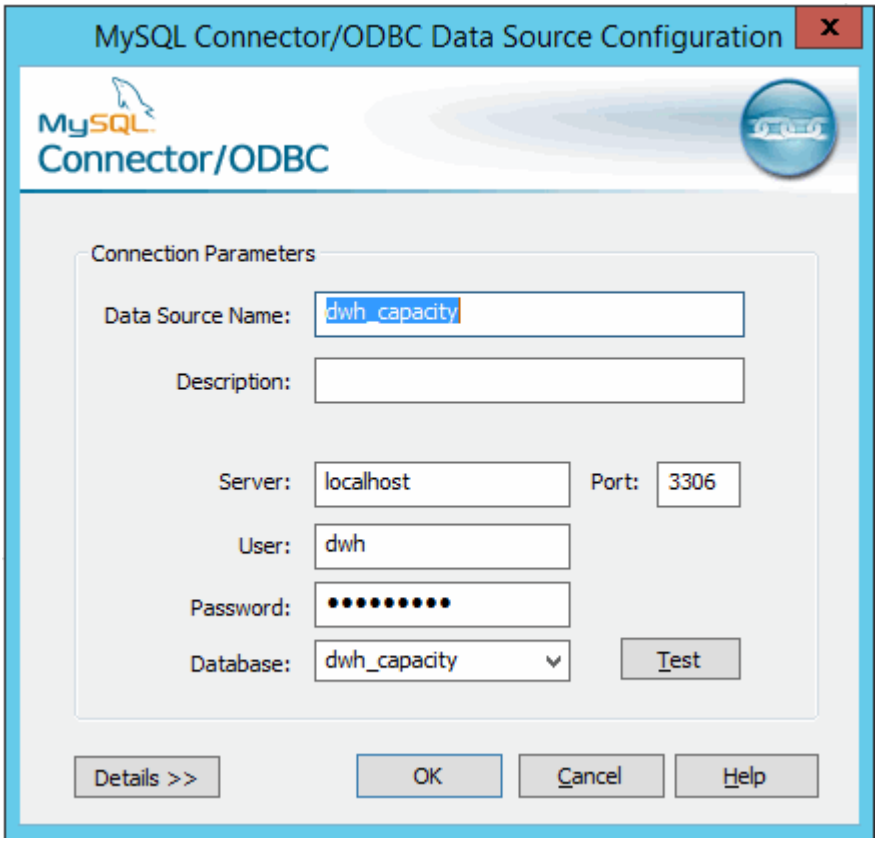
3. Klicken Sie auf **System DSN**

   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.

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.

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.keystore`

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.

> 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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

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 7.3.5 bis 7.3.9)

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 7.3.5 bis 7.3.9.

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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS:
   ```
   ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet
   ```
   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:
   ```
   ..\..\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 leicht identifizieren würde`keytool -list` Betrieb.
   f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Um den CAC-Modus zu aktivieren, führen Sie aus `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Um den CAC-Modus zu deaktivieren, führen Sie aus `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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 leicht identifizieren würde`keytool -list` Betrieb.
   f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.

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 7.3.5 auf 7.3.9)

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 OnCommnand Insight 7.3.5 bis 7.3.9.

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. Erstellen Sie ein Backup von `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Erstellen Sie unter eine Sicherungskopie der Ordner „`certs`“ und „`csk`“ `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Senden Sie die cryptRequest.csr an die Zertifizierungsstelle (CA), um ein SSL-Zertifikat zu erhalten.

   Fügen Sie zusätzliche Attribute wie „`SAN:dns=FQDN“ hinzu (z. B. hostname.netapp.com)`", um den SubjectAltName hinzuzufügen. Google Chrome Version 58 und später beschwert sich, wenn die SubjectAltName fehlt aus dem Zertifikat.

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 8c, 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. Intermediate.cer mit Notepad öffnen und Inhalt kopieren.

   b. Öffnen Sie root.cer mit Notepad und speichern Sie den Inhalt aus 9a.

   c. Speichern Sie die Datei unter CA.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\CA.cer

       Dadurch wird CA.cer als Stammzertifizierungsstelle festgelegt.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

       Dadurch wird Cognos.cer als von CA.cer signiertes Verschlüsselungszertifikat festgelegt.

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. „D:\Programme\SANscreen\java\bin\keytool.exe“ -exportcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\cognos\Analytics\Configuration\certs\CAMKeystore“ -storetype PKCS12 -storepass NoPassWordSet -alias-Verschlüsselung

13. Importieren Sie „`c:\temp\cognos.crt`“ in dwh trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.

    a. „D:\Programme\SANscreen\java\bin\keytool.exe“ -importcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\wildfly\Standalone\Configuration\Server.trustore“ -storepass changeit -alias cognoscert

14. Starten Sie den SANscreen-Dienst neu.

15. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

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 NoPassWordSet -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.
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 NoPassWordSet -alias-Verschlüsselung
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 changeit -alias cognos3rdca
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 changeit -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.

> 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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      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 7.3.5 bis 7.3.9)

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 7.3.5 bis 7.3.9.

> 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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS:
      ```
      ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet
      ```
      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:
      ```
      ..\..\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 leicht identifizieren würde`keytool -list` Betrieb.
   f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.
   g. Antwort `yes` Wenn Sie aufgefordert werden, dem Zertifikat zu vertrauen.
2. Um den CAC-Modus zu aktivieren, führen Sie aus `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Um den CAC-Modus zu deaktivieren, führen Sie aus `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 die `keytool` Dienstprogramm zum Auflisten der vertrauenswürdigen CAS: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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 leicht identifizieren würde`keytool -list` Betrieb.

   f. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `NoPassWordSet`.
   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 7.3.5 auf 7.3.9)

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 OnCommnand Insight 7.3.5 bis 7.3.9.

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. Erstellen Sie ein Backup von `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Erstellen Sie unter eine Sicherungskopie der Ordner „`certs`“ und „`csk`“ `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. Öffnen Sie das `c:\temp\encryptRequest.csr` Datei und kopieren Sie den generierten Inhalt.
5. Senden Sie die cryptRequest.csr an die Zertifizierungsstelle (CA), um ein SSL-Zertifikat zu erhalten.

   Fügen Sie zusätzliche Attribute wie „`SAN:dns=FQDN“ hinzu (z. B. hostname.netapp.com)`", um den SubjectAltName hinzuzufügen. Google Chrome Version 58 und später beschwert sich, wenn die SubjectAltName fehlt aus dem Zertifikat.

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 8c, 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. Intermediate.cer mit Notepad öffnen und Inhalt kopieren.
   b. Öffnen Sie root.cer mit Notepad und speichern Sie den Inhalt aus 9a.
   c. Speichern Sie die Datei unter CA.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\CA.cer

      Dadurch wird CA.cer als Stammzertifizierungsstelle festgelegt.

   c. ThirdPartyCertificateTool.bat -java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

      Dadurch wird Cognos.cer als von CA.cer signiertes Verschlüsselungszertifikat festgelegt.
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. „D:\Programme\SANscreen\java\bin\keytool.exe“ -exportcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\cognos\Analytics\Configuration\certs\CAMKeystore“ -storetype PKCS12 -storepass NoPassWordSet -alias-Verschlüsselung
13. Importieren Sie „`c:\temp\cognos.crt`“ in dwh trustore, um mithilfe des Admin CMD-Eingabefensters die SSL-Kommunikation zwischen Cognos und DWH herzustellen.
   a. „D:\Programme\SANscreen\java\bin\keytool.exe“ -importcert -file „`c:\temp\cognos.crt`“ -keystore „D:\Programme\SANscreen\wildfly\Standalone\Configuration\Server.trustore“ -storepass changeit -alias cognoscert
14. Starten Sie den SANscreen-Dienst neu.
15. Führen Sie eine Sicherungskopie des DWH durch, um sicherzustellen, dass DWH mit Cognos kommuniziert.

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 NoPassWordSet -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.
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 NoPassWordSet -alias-Verschlüsselung
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 changeit -alias cognos3rdca

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 changeit -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

> Bevor Sie diesen Vorgang durchführen, sollten Sie das vorhandene sichern `server.keystore` Datei und benennen Sie die Sicherung `server.keystore.old`. Korrumpieren oder beschädigen `server.keystore` Die Datei kann zu einem nicht funktionsfähigen Insight-Server führen, nachdem der Insight-Server neu gestartet wurde. Wenn Sie ein Backup erstellen, können Sie bei Problemen auf die alte Datei zurücksetzen.

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"`

    a. Wenn Sie zur Eingabe eines Passworts aufgefordert werden, geben Sie ein `changeit`.

    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 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 + 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 + Add .

   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 + Add 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 More 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 More ▾, 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.

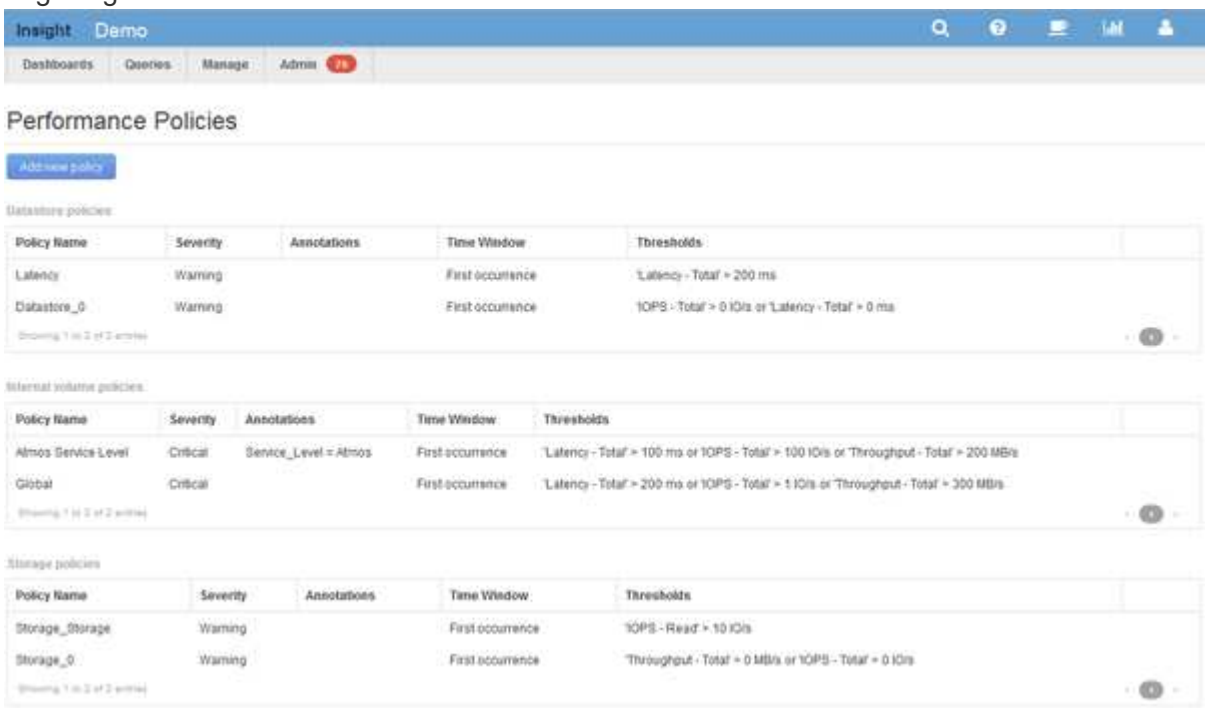
Erstellung von Performance-Richtlinien

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.
>
> +

Copyright-Informationen

Markeninformationen