Configurazione di Insight

OnCommand Insight

NetApp
October 24, 2024

Sommario

Configurazione di Insight

Per configurare Insight, è necessario attivare le licenze Insight, configurare le origini dati, definire utenti e notifiche, abilitare i backup ed eseguire le procedure di configurazione avanzate richieste.

Una volta installato il sistema OnCommand Insight, è necessario eseguire le seguenti operazioni di installazione:

- Installare le licenze Insight.
- Configura le origini dati in Insight.
- Configurare gli account utente.
- Configurare l'e-mail.
- Definire le notifiche SNMP, e-mail o syslog, se necessario.
- Abilita backup settimanali automatici del tuo database Insight.
- Eseguire qualsiasi procedura di configurazione avanzata richiesta, inclusa la definizione di annotazioni e soglie.

Accesso all'interfaccia utente Web

Dopo aver installato OnCommand Insight, è necessario installare le licenze e configurare Insight per il monitoraggio dell'ambiente. A tale scopo, utilizzare un browser Web per accedere all'interfaccia utente Web di Insight.

Fasi

1. Effettuare una delle seguenti operazioni:
    - Aprire Insight sul server Insight:

      `https://fqdn`

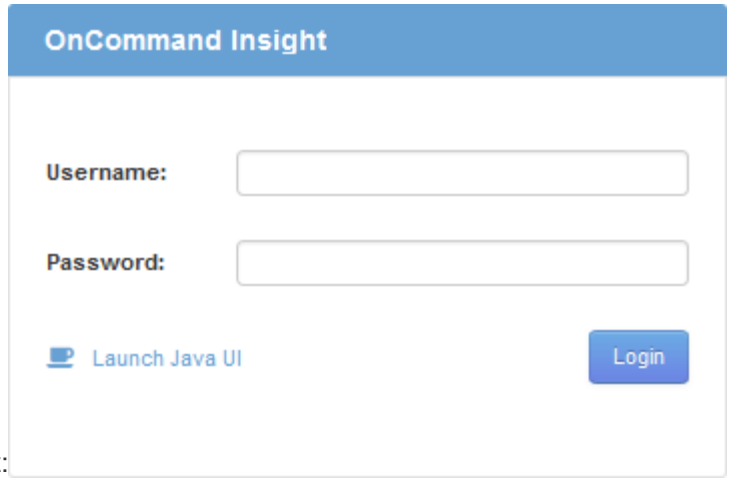
    - Apri Insight da qualsiasi altra posizione:

      `https://fqdn:port`

      Il numero della porta è 443 o un'altra porta configurata al momento dell'installazione del server Insight. Il numero di porta predefinito è 443 se non viene specificato nell'URL.

   Viene visualizzata la finestra di dialogo OnCommand

Insight:



2. Inserire il nome utente e la password e fare clic su **Login**.

   Se le licenze sono state installate, viene visualizzata la pagina di configurazione dell'origine dati.

   Una sessione del browser Insight inattiva per 30 minuti è scaduta e l'utente viene disconnesso automaticamente dal sistema. Per una maggiore sicurezza, si consiglia di chiudere il browser dopo la disconnessione da Insight.

Installazione delle licenze Insight

Una volta ricevuto il file di licenza contenente le chiavi di licenza Insight da NetApp, è possibile utilizzare le funzioni di configurazione per installare tutte le licenze contemporaneamente.

A proposito di questa attività

Le chiavi di licenza Insight sono memorizzate in `.txt` oppure `.lcn` file.

Fasi

1. Aprire il file di licenza in un editor di testo e copiare il testo.
2. Aprire Insight nel browser.
3. Nella barra degli strumenti Insight, fare clic su **Admin**.
4. Fare clic su **Setup**.
5. Fare clic sulla scheda **Licenses** (licenze).
6. Fare clic su **Update License** (Aggiorna licenza).
7. Copiare il testo della chiave di licenza nella casella di testo **licenza**.
8. Selezionare l'operazione **Update (più comune)**.
9. Fare clic su **Save** (Salva).
10. Se si utilizza il modello di licenza Insight Consumption, selezionare la casella **Enable sending usage information to NetApp** (attiva invio delle informazioni sull'utilizzo a NetApp*) nella sezione **Send usage information** (Invia informazioni sull'utilizzo). Il proxy deve essere configurato e attivato correttamente per l'ambiente in uso.

Al termine

Dopo aver installato le licenze, è possibile eseguire le seguenti attività di configurazione:

- Configurare le origini dati.
- Creare account utente OnCommand Insight.

Licenze OnCommand Insight

OnCommand Insight opera con licenze che abilitano funzionalità specifiche sul server Insight.

- **Scoprire**

  Discover è la licenza Insight di base che supporta l'inventario. Per utilizzare OnCommand Insight, è necessario disporre di una licenza Discover e la licenza Discover deve essere associata ad almeno una delle licenze di assicurazione, esecuzione o piano.

- **Rassicurare**

  Una licenza Assurance fornisce supporto per la funzionalità Assurance, incluse policy di percorso globali e SAN e gestione delle violazioni. Una licenza di assicurazione consente inoltre di visualizzare e gestire le vulnerabilità.

- **Eseguire**

  Una licenza Perform supporta il monitoraggio delle performance su pagine di risorse, widget dashboard, query e così via, oltre a gestire policy e violazioni delle performance.

- **Piano**

  Una licenza Plan supporta le funzioni di pianificazione, incluso l'utilizzo e l'allocazione delle risorse.

- **Pacchetto di utilizzo host**

  Una licenza di utilizzo host supporta l'utilizzo del file system su host e macchine virtuali.

- **Creazione report**

  Una licenza per la creazione di report supporta altri autori per la creazione di report. Questa licenza richiede la licenza Plan.

I moduli OnCommand Insight sono concessi in licenza per un periodo annuale o perpetuo:

- Per terabyte di capacità monitorata per i moduli di rilevamento, assicurazione, pianificazione ed esecuzione
- In base al numero di host per il pacchetto di utilizzo host
- In base al numero di unità aggiuntive di pro-autori Cognos richieste per l'authoring dei report

Le chiavi di licenza sono un insieme di stringhe univoche generate per ciascun cliente. È possibile ottenere le chiavi di licenza dal proprio rappresentante OnCommand Insight.

Le licenze installate controllano le seguenti opzioni disponibili nel software:

- **Scoprire**

  Acquisire e gestire l’inventario (base)

  Monitorare le modifiche e gestire le policy di inventario

- **Rassicurare**

  Visualizza e gestisci le violazioni e le policy dei percorsi SAN

  Visualizzare e gestire le vulnerabilità

  Visualizza e gestisci task e migrazioni

- **Piano**

  Visualizzare e gestire le richieste

  Visualizzare e gestire le attività in sospeso

  Visualizzare e gestire le violazioni delle prenotazioni

  Visualizzare e gestire le violazioni del bilanciamento delle porte

- **Eseguire**

  Monitorare i dati delle performance, inclusi i dati nei widget dashboard, nelle pagine di risorse e nelle query

  Visualizza e gestisci le policy e le violazioni delle performance

Le seguenti tabelle forniscono informazioni dettagliate sulle funzionalità disponibili con e senza la licenza Perform per gli utenti admin e non-admin.

Funzione (admin)	Con Perform License	Senza licenza di esecuzione
Applicazione	Sì	Nessun grafico o dati sulle performance
Macchina virtuale	Sì	Nessun grafico o dati sulle performance
Hypervisor	Sì	Nessun grafico o dati sulle performance
Host	Sì	Nessun grafico o dati sulle performance
Datastore	Sì	Nessun grafico o dati sulle performance
VMDK	Sì	Nessun grafico o dati sulle performance

Volume interno	Sì	Nessun grafico o dati sulle performance
Volume	Sì	Nessun grafico o dati sulle performance
Pool di storage	Sì	Nessun grafico o dati sulle performance
Disco	Sì	Nessun grafico o dati sulle performance
Storage	Sì	Nessun grafico o dati sulle performance
Nodo storage	Sì	Nessun grafico o dati sulle performance
Fabric	Sì	Nessun grafico o dati sulle performance
Porta dello switch	Sì	Nessun grafico o dati sulle prestazioni; “Port Errors” mostra “N/A”
Porta di storage	Sì	Sì
Porta NPV	Sì	Nessun grafico o dati sulle performance
Switch	Sì	Nessun grafico o dati sulle performance
Switch NPV	Sì	Nessun grafico o dati sulle performance
Qtree	Sì	Nessun grafico o dati sulle performance
Quota	Sì	Nessun grafico o dati sulle performance
Percorso	Sì	Nessun grafico o dati sulle performance
Zona	Sì	Nessun grafico o dati sulle performance

Membro della zona	Sì	Nessun grafico o dati sulle performance
Dispositivo generico	Sì	Nessun grafico o dati sulle performance
Nastro	Sì	Nessun grafico o dati sulle performance
Mascheratura	Sì	Nessun grafico o dati sulle performance
Sessioni ISCSI	Sì	Nessun grafico o dati sulle performance
Portali di rete ICSI	Sì	Nessun grafico o dati sulle performance
Cerca	Sì	Sì
Amministratore	Sì	Sì
Dashboard	Sì	Sì
Widget	Sì	Parzialmente disponibile (sono disponibili solo i widget asset, query e admin)
Dashboard delle violazioni	Sì	Nascosto
Dashboard delle risorse	Sì	Parzialmente disponibile (i widget IOPS di storage e IOPS delle macchine virtuali sono nascosti)
Gestire le policy sulle performance	Sì	Nascosto
Gestire le annotazioni	Sì	Sì
Gestire le regole di annotazione	Sì	Sì
Gestire le applicazioni	Sì	Sì
Query	Sì	Sì
Gestire le entità di business	Sì	Sì

Funzione	Utente - con licenza Perform	Guest - con licenza Perform	Utente - senza licenza Perform	Guest - senza licenza di esecuzione
Dashboard delle risorse	Sì	Sì	Parzialmente disponibile (i widget IOPS di storage e IOPS delle macchine virtuali sono nascosti)	Parzialmente disponibile (i widget IOPS di storage e IOPS delle macchine virtuali sono nascosti)
Dashboard personalizzato	Sola visualizzazione (nessuna opzione di creazione, modifica o salvataggio)	Sola visualizzazione (nessuna opzione di creazione, modifica o salvataggio)	Sola visualizzazione (nessuna opzione di creazione, modifica o salvataggio)	Sola visualizzazione (nessuna opzione di creazione, modifica o salvataggio)
Gestire le policy sulle performance	Sì	Nascosto	Nascosto	Nascosto
Gestire le annotazioni	Sì	Nascosto	Sì	Nascosto
Gestire le applicazioni	Sì	Nascosto	Sì	Nascosto
Gestire le entità di business	Sì	Nascosto	Sì	Nascosto
Query	Sì	Solo visualizzazione e modifica (nessuna opzione di salvataggio)	Sì	Solo visualizzazione e modifica (nessuna opzione di salvataggio)

Impostazione e gestione degli account utente

Gli account utente, l'autenticazione utente e l'autorizzazione utente possono essere definiti e gestiti in due modi: Nel server LDAP (protocollo di accesso alle directory leggero) di Microsoft Active Directory (versione 2 o 3) o in un database utente OnCommand Insight interno. La disponibilità di un account utente diverso per ciascuna persona consente di controllare i diritti di accesso, le preferenze individuali e la responsabilità. Utilizzare un account con privilegi di amministratore per questa operazione.

Prima di iniziare

È necessario aver completato le seguenti attività:

- Installare le licenze OnCommand Insight.

- Assegnare un nome utente univoco per ciascun utente.
- Determinare le password da utilizzare.
- Assegnare i ruoli utente corretti.

Se si sta importando un certificato LDAP e sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

Le Best practice di sicurezza impongono agli amministratori di configurare il sistema operativo host per impedire l'accesso interattivo di utenti non amministratori/standard.

Fasi

1. Aprire Insight nel browser.
2. Nella barra degli strumenti Insight, fare clic su **Admin**.
3. Fare clic su **Setup**.
4. Selezionare la scheda **utenti**.
5. Per creare un nuovo utente, fare clic sul pulsante **azioni** e selezionare **Aggiungi utente**.

   Immettere **Nome**, **Password**, **Indirizzo e-mail** e selezionare uno degli utenti **ruoli** come Amministratore, utente o ospite.

6. Per modificare le informazioni di un utente, selezionarlo dall'elenco e fare clic sul simbolo **Edit user account** (Modifica account utente) a destra della descrizione dell'utente.
7. Per rimuovere un utente dal sistema OnCommand Insight, selezionarlo dall'elenco e fare clic su **Delete user account** (Elimina account utente) a destra della descrizione dell'utente.

Risultati

Quando un utente accede a OnCommand Insight, il server tenta per primo di autenticarsi tramite LDAP, se LDAP è attivato. Se OnCommand Insight non riesce a individuare l'utente sul server LDAP, esegue la ricerca nel database Insight locale.

Ruoli utente Insight

A ciascun account utente viene assegnato uno dei tre livelli di autorizzazione possibili.

- Guest consente di accedere a Insight e di visualizzare le varie pagine.
- L'utente consente tutti i privilegi di livello guest, oltre all'accesso alle operazioni Insight, come la definizione di policy e l'identificazione di dispositivi generici. Il tipo di account utente non consente di eseguire operazioni di origine dati, né di aggiungere o modificare account utente diversi dal proprio.
- Administrator (Amministratore) consente di eseguire qualsiasi operazione, inclusi l'aggiunta di nuovi utenti e la gestione delle origini dati.

Best practice: limita il numero di utenti con autorizzazioni di amministratore creando la maggior parte degli account per utenti o ospiti.

Configurazione di Insight per LDAP

OnCommand Insight deve essere configurato con le impostazioni LDAP (Lightweight Directory Access Protocol) così come sono configurate nel dominio LDAP aziendale.

Prima di configurare Insight per l'utilizzo con LDAP o LDAP sicuro (LDAPS), prendere nota della configurazione di Active Directory nell'ambiente aziendale. Le impostazioni di Insight devono corrispondere a quelle della configurazione di dominio LDAP dell'organizzazione. Prima di configurare Insight per l'utilizzo con LDAP, consultare i seguenti concetti e rivolgersi all'amministratore di dominio LDAP per conoscere gli attributi appropriati da utilizzare nell'ambiente.

Per tutti gli utenti di Secure Active Directory (ad esempio LDAPS), è necessario utilizzare il nome del server ad esattamente come definito nel certificato. Non è possibile utilizzare l'indirizzo IP per l'accesso ad sicuro.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

OnCommand Insight supporta LDAP e LDAPS tramite server Microsoft Active Directory o Azure ad. Ulteriori implementazioni LDAP potrebbero funzionare, ma non sono state qualificate con Insight. Le procedure descritte in queste guide presuppongono l'utilizzo di Microsoft Active Directory versione 2 o 3 LDAP (Lightweight Directory Access Protocol).

User Principal Name Attribute:

L'attributo LDAP User Principal Name (userPrincipalName) è quello che Insight utilizza come attributo Username. Il nome principale dell'utente è garantito per essere univoco a livello globale in una foresta Active Directory (ad), ma in molte grandi organizzazioni il nome principale di un utente potrebbe non essere immediatamente ovvio o noto. L'organizzazione potrebbe utilizzare un'alternativa all'attributo User Principal Name per il nome utente principale.

Di seguito sono riportati alcuni valori alternativi per il campo User Principal Name Attribute (attributo nome principale utente):

- **SAMAccountName**

  Questo attributo utente è il nome utente precedente a Windows 2000 NT legacy, ovvero la maggior parte degli utenti è abituata ad accedere alla propria macchina Windows personale. Non è garantito che questo sia globalmente unico in un insieme di strutture ad.

  SAMAccountName rileva la distinzione tra maiuscole e minuscole per l'attributo User Principal Name.

- **mail**

  Negli ambienti ad con MS Exchange, questo attributo rappresenta l'indirizzo e-mail principale dell'utente finale. A differenza dell'attributo userPrincipalName, questo deve essere univoco a livello globale in un insieme di strutture ad (e familiare anche per gli utenti finali). L'attributo mail non esiste nella maggior parte degli ambienti non MS Exchange.

- **riferimento**

  Un riferimento LDAP è il modo in cui un controller di dominio indica a un'applicazione client che non dispone di una copia di un oggetto richiesto (o, più precisamente, che non contiene la sezione della

struttura di directory in cui si trova l'oggetto, se effettivamente esiste) e che fornisce al client una posizione che è più probabile contenere l'oggetto. A sua volta, il client utilizza il riferimento come base per una ricerca DNS di un controller di dominio. Idealmente, i riferimenti fanno sempre riferimento a un controller di dominio che contiene effettivamente l'oggetto. Tuttavia, è possibile che il controller di dominio indicato generi un altro riferimento, anche se di solito non richiede molto tempo per scoprire che l'oggetto non esiste e per informare il client.

SAMAccountName è generalmente preferito rispetto a User Principal Name. SAMAccountName è univoco nel dominio (anche se potrebbe non essere univoco nella foresta di domini), ma è la stringa utilizzata dagli utenti del dominio per l'accesso (ad esempio,*netapp_Username*). Il nome distinto è il nome univoco nella foresta, ma generalmente non è noto agli utenti.

Nella parte del sistema Windows dello stesso dominio, è sempre possibile aprire un prompt dei comandi e digitare SET per trovare il nome di dominio corretto (USERDOMAIN=). Il nome di accesso OCI sarà quindi `USERDOMAIN\sAMAccountName`.

Per il nome di dominio **mydomain.x.y.z.com**, utilizzare `DC=x,DC=y,DC=z,DC=com` Nel campo dominio di Insight.

Porte:

La porta predefinita per LDAP è 389 e la porta predefinita per LDAPS è 636

URL tipico per LDAPS: `ldaps://<ldap_server_host_name>:636`

I log sono:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

Per impostazione predefinita, Insight si aspetta i valori annotati nei seguenti campi. Se questi cambiamenti si verificano nell'ambiente Active Directory, assicurarsi di modificarli nella configurazione Insight LDAP.

Attributo ruolo
MemberOf
Attributo mail
mail
Attributo nome distinto
DistinguishedName
Riferimento
segui

Gruppi:

Per autenticare gli utenti con ruoli di accesso diversi nei server OnCommand Insight e DWH, è necessario

creare gruppi in Active Directory e immettere i nomi dei gruppi nei server OnCommand Insight e DWH. I nomi dei gruppi riportati di seguito sono solo di esempio; i nomi configurati per LDAP in Insight devono corrispondere a quelli impostati per l'ambiente Active Directory.

Gruppo Insight	Esempio
Gruppo di amministratori del server Insight	insight.server.admins
Gruppo di amministratori di Insight	insight.admins
Gruppo di utenti Insight	insight.users
Gruppo di ospiti Insight	insight.guest
Gruppo di amministratori dei report	insight.report.admins
Gruppo di autori di report pro	insight.report.proauthors
Gruppo di autori di report	insight.report.business.authors
Gruppo di clienti di reporting	insight.report.business.consumer
Gruppo di destinatari dei report	insight.report.destinatari

Configurazione delle definizioni utente mediante LDAP

Per configurare OnCommand Insight (OCI) per l'autenticazione utente e l'autorizzazione da un server LDAP, è necessario definire nel server LDAP l'amministratore del server OnCommand Insight.

Prima di iniziare

È necessario conoscere gli attributi utente e gruppo configurati per Insight nel dominio LDAP.

Per tutti gli utenti di Secure Active Directory (ad esempio LDAPS), è necessario utilizzare il nome del server ad esattamente come definito nel certificato. Non è possibile utilizzare l'indirizzo IP per l'accesso ad sicuro.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

A proposito di questa attività

OnCommand Insight supporta LDAP e LDAPS tramite server Microsoft Active Directory. Ulteriori implementazioni LDAP potrebbero funzionare, ma non sono state qualificate con Insight. Questa procedura presuppone che si stia utilizzando Microsoft Active Directory versione 2 o 3 LDAP (Lightweight Directory Access Protocol).

Gli utenti LDAP vengono visualizzati insieme agli utenti definiti localmente nell'elenco **Admin** > **Setup** › **Users**.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Setup**.
3. Fare clic sulla scheda **utenti**.
4. Scorrere fino alla sezione LDAP.
5. Fare clic su **Enable LDAP** (attiva LDAP) per consentire l'autenticazione e l'autorizzazione dell'utente LDAP.
6. Compilare i campi:

   ◦ `LDAP servers`: Insight accetta un elenco separato da virgole di URL LDAP. Insight tenta di connettersi agli URL forniti senza eseguire la convalida per il protocollo LDAP.

   > Per importare i certificati LDAP, fare clic su **certificati** e importare automaticamente o individuare manualmente i file dei certificati.

   L'indirizzo IP o il nome DNS utilizzato per identificare il server LDAP viene in genere inserito nel seguente formato:

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

   oppure, se si utilizza la porta predefinita:

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

   + Quando si immettono più server LDAP in questo campo, assicurarsi di utilizzare il numero di porta corretto in ciascuna voce.

   ◦ `User name`: Immettere le credenziali di un utente autorizzato per le query di ricerca directory sui server LDAP.

   ◦ `Password`: Inserire la password per l'utente precedente. Per confermare la password sul server LDAP, fare clic su **convalida**.

7. Se si desidera definire questo utente LDAP con maggiore precisione, fare clic su **Mostra altri** e compilare i campi degli attributi elencati.

   Queste impostazioni devono corrispondere agli attributi configurati nel dominio LDAP. In caso di dubbi sui valori da inserire per questi campi, rivolgersi all'amministratore di Active Directory.

   ◦ **Gruppo amministratori**

     Gruppo LDAP per utenti con privilegi Insight Administrator. Il valore predefinito è `insight.admins`.

   ◦ **Gruppo utenti**

     Gruppo LDAP per utenti con privilegi Insight User. Il valore predefinito è `insight.users`.

   ◦ **Gruppo ospiti**

Gruppo LDAP per utenti con privilegi Insight Guest. Il valore predefinito è `insight.guests`.

- Gruppo **Server Admins**

  Gruppo LDAP per utenti con privilegi di amministratore di Insight Server. Il valore predefinito è `insight.server.admins`.

- **Timeout**

  Tempo di attesa di una risposta dal server LDAP prima del timeout, espresso in millisecondi. il valore predefinito è 2,000, che è adeguato in tutti i casi e non deve essere modificato.

- **Dominio**

  Nodo LDAP in cui OnCommand Insight dovrebbe iniziare a cercare l'utente LDAP. In genere si tratta del dominio di primo livello dell'organizzazione. Ad esempio:

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

- **Attributo nome principale utente**

  Attributo che identifica ciascun utente nel server LDAP. Il valore predefinito è `userPrincipalName`, che è unico a livello globale. OnCommand Insight tenta di far corrispondere il contenuto di questo attributo con il nome utente fornito in precedenza.

- **Attributo ruolo**

  Attributo LDAP che identifica la misura dell'utente all'interno del gruppo specificato. Il valore predefinito è `memberOf`.

- **Attributo Mail**

  Attributo LDAP che identifica l'indirizzo e-mail dell'utente. Il valore predefinito è `mail`. Questa opzione è utile se si desidera iscriversi ai report disponibili presso OnCommand Insight. Insight rileva l'indirizzo e-mail dell'utente la prima volta che ciascun utente effettua l'accesso e non lo cerca dopo.

  Se l'indirizzo e-mail dell'utente cambia sul server LDAP, assicurarsi di aggiornarlo in Insight.

- **Attributo nome distinto**

  Attributo LDAP che identifica il nome distinto dell'utente. il valore predefinito è `distinguishedName`.

8. Fare clic su **Save** (Salva).

Modifica delle password dell'utente

Un utente con privilegi di amministratore può modificare la password per qualsiasi account utente OnCommand Insight definito sul server locale.

Prima di iniziare

Devono essere stati completati i seguenti elementi:

- Notifiche a chiunque acceda all'account utente che si sta modificando.
- Nuova password da utilizzare dopo questa modifica.

A proposito di questa attività

Quando si utilizza questo metodo, non è possibile modificare la password di un utente validato tramite LDAP.

Fasi

1. Accedere con privilegi di amministratore.
2. Nella barra degli strumenti Insight, fare clic su **Admin**.
3. Fare clic su **Setup**.
4. Fare clic sulla scheda **utenti**.
5. Individuare la riga che visualizza l'account utente che si desidera modificare.
6. A destra delle informazioni sull'utente, fare clic su **Edit user account** (Modifica account utente).
7. Inserire la nuova **Password**, quindi immetterla di nuovo nel campo di verifica.
8. Fare clic su **Save** (Salva).

Modifica di una definizione utente

Un utente con privilegi di amministratore può modificare un account utente per modificare l'indirizzo e-mail o i ruoli per OnCommand Insight o DWH e le funzioni di reporting.

Prima di iniziare

Determinare il tipo di account utente (OnCommand Insight, DWH o una combinazione) da modificare.

A proposito di questa attività

Per gli utenti LDAP, è possibile modificare l'indirizzo e-mail solo utilizzando questo metodo.

Fasi

1. Accedere con privilegi di amministratore.
2. Nella barra degli strumenti Insight, fare clic su **Admin**.
3. Fare clic su **Setup**.
4. Fare clic sulla scheda **utenti**.
5. Individuare la riga che visualizza l'account utente che si desidera modificare.
6. A destra delle informazioni sull'utente, fare clic sull'icona **Edit user account** (Modifica account utente).
7. Apportare le modifiche necessarie.
8. Fare clic su **Save** (Salva).

Eliminazione di un account utente

Qualsiasi utente con privilegi di amministratore può eliminare un account utente quando non viene più utilizzato (per una definizione utente locale) o forzare OnCommand Insight a riscoprire le informazioni utente al successivo accesso (per un utente LDAP).

Fasi

1. Accedere a OnCommand Insight con privilegi di amministratore.
2. Nella barra degli strumenti Insight, fare clic su **Admin**.
3. Fare clic su **Setup**.
4. Fare clic sulla scheda **utenti**.
5. Individuare la riga che visualizza l'account utente che si desidera eliminare.
6. A destra delle informazioni utente, fare clic sull'icona **Delete user account "x"**.
7. Fare clic su **Save** (Salva).

Impostazione di un messaggio di avviso di accesso

OnCommand Insight consente agli amministratori di impostare un messaggio di testo personalizzato che viene visualizzato quando gli utenti accedono.

Fasi

1. Per impostare il messaggio nel server OnCommand Insight:
   a. Accedere al **Admin › risoluzione dei problemi › risoluzione dei problemi avanzata › Impostazioni avanzate**.
   b. Inserire il messaggio di accesso nell'area di testo.
   c. Fare clic sulla casella di controllo **il client visualizza il messaggio di avviso di accesso**.
   d. Fare clic su **Save** (Salva).

      Il messaggio viene visualizzato al momento dell'accesso per tutti gli utenti.
2. Per impostare il messaggio in Data Warehouse (DWH) e Reporting (Cognos):
   a. Selezionare **System Information** (informazioni di sistema) e fare clic sulla scheda **Login Warning** (Avviso di accesso).
   b. Inserire il messaggio di accesso nell'area di testo.
   c. Fare clic su **Save** (Salva).

      Il messaggio viene visualizzato quando si accede a DWH e Cognos Reporting per tutti gli utenti.

Strumento securityadmin

OnCommand Insight fornisce funzionalità che consentono agli ambienti Insight di operare con una maggiore sicurezza. Queste funzioni includono crittografia, hash delle password e la possibilità di modificare le password interne degli utenti e le coppie di chiavi che

crittografano e decrittografano le password. È possibile gestire queste funzionalità su tutti i server dell'ambiente Insight utilizzando **securityadmin Tool**.

Che cos'è lo strumento securityadmin?

Lo strumento di amministrazione della protezione supporta l'esecuzione di modifiche al contenuto dei vault e l'esecuzione di modifiche coordinate all'installazione di OnCommand Insight.

Gli usi principali dello strumento securityadmin sono **Backup** e **Restore** della configurazione di protezione (ad esempio, vault) e delle password. Ad esempio, è possibile eseguire il backup del vault su un'unità di acquisizione locale e ripristinarlo su un'unità di acquisizione remota, assicurando la coordinazione delle password in tutto l'ambiente. In alternativa, se nell'ambiente sono presenti più server OnCommand Insight, è possibile eseguire un backup del vault dei server e ripristinarlo in altri server per mantenere le stesse password. Questi sono solo due esempi dei modi in cui è possibile utilizzare securityadmin per garantire la coesione negli ambienti.

Si consiglia vivamente di **eseguire il backup del vault** ogni volta che si esegue il backup di un database OnCommand Insight. In caso contrario, si potrebbe perdere l'accesso.

Lo strumento fornisce entrambe le modalità **interactive** e **command line**.

Molte operazioni dello strumento securityadmin modificano il contenuto del vault e apportano modifiche all'installazione, assicurando che il vault e l'installazione rimangano sincronizzati.

Ad esempio,

- Quando si modifica la password di un utente Insight, la voce dell'utente nella tabella SANscreen.users viene aggiornata con il nuovo hash.
- Quando si modifica la password di un utente MySQL, verrà eseguita l'istruzione SQL appropriata per aggiornare la password dell'utente nell'istanza MySQL.

In alcune situazioni, verranno apportate diverse modifiche all'installazione:

- Quando si modifica l'utente dwh MySQL, oltre ad aggiornare la password nel database MySQL, verranno aggiornate anche più voci di registro per ODBC.

Nelle sezioni seguenti il termine "cambiamenti coordinati" viene utilizzato per descrivere tali cambiamenti.

Modalità di esecuzione

- Funzionamento normale/predefinito - il servizio server SANscreen deve essere in esecuzione

  Per la modalità di esecuzione predefinita, lo strumento securityadmin richiede l'esecuzione del servizio **server SANscreen**. Il server viene utilizzato per l'autenticazione e molte modifiche coordinate all'installazione vengono effettuate tramite chiamate al server.

- Funzionamento diretto - il servizio del server SANscreen potrebbe essere in esecuzione o interrotto.

  Se eseguito su un'installazione OCI Server o DWH, lo strumento può essere eseguito anche in modalità "diretta". In questa modalità, l'autenticazione e le modifiche coordinate vengono eseguite utilizzando il database. Il servizio Server non viene utilizzato.

  Il funzionamento è identico alla modalità normale, con le seguenti eccezioni:

- L’autenticazione è supportata solo per gli utenti non amministratori di dominio. (Utenti con password e ruoli nel database, non LDAP).
- L’operazione "sostituzione delle chiavi" non è supportata.
- La fase di ri-crittografia del ripristino del vault viene ignorata.
- Modalità di ripristino lo strumento può essere eseguito anche quando l’accesso al server e al database non è possibile (ad esempio perché la password principale nel vault non è corretta).

  Quando viene eseguito in questa modalità, l’autenticazione non è possibile e, quindi, non può essere eseguita alcuna operazione con una modifica coordinata dell’installazione.

  La modalità di recupero può essere utilizzata per:

- determinare quali voci del vault sono errate (utilizzando l’operazione di verifica)
- sostituire la password di root non corretta con il valore corretto. (Questa operazione non modifica la password. L’utente deve inserire la password corrente).

> Se la password di root nel vault non è corretta e la password non è nota e non è presente alcun backup del vault con la password di root corretta, l’installazione non può essere recuperata utilizzando lo strumento securityadmin. L’unico modo per recuperare l’installazione è quello di reimpostare la password dell’istanza MySQL seguendo la procedura documentata all’indirizzo https://dev.mysql.com/doc/refman/8.4/en/resetting-permissions.html. Dopo aver eseguito la procedura di ripristino, utilizzare l’operazione password memorizzata corretta per immettere la nuova password nel vault.

Comandi

Comandi senza restrizioni

I comandi senza restrizioni apportano modifiche coordinate all’installazione (ad eccezione degli archivi di trust). I comandi senza restrizioni possono essere eseguiti senza autenticazione dell’utente.

Comando	Descrizione
vault di backup	Creare un file zip contenente il vault. Il percorso relativo ai file del vault corrisponderà al percorso dei vault rispetto alla radice di installazione. • wildfly/standalone/configuration/vault/* • acq/conf/vault/* Si consiglia vivamente di eseguire il backup del vault ogni volta che si esegue il backup di un database OnCommand Insight.
controlla-per-chiavi-predefinite	Verificare se le chiavi del vault corrispondono a quelle del vault di default usato nelle istanze precedenti alla versione 7.3.16.

password-memorizzata-corretta	Sostituire una password (errata) memorizzata nel vault con la password corretta nota all'utente. Questo può essere utilizzato quando il vault e l'installazione non sono coerenti. **Notare che non modifica la password effettiva nell'installazione.**
	Change-trust-store-password modificare la password utilizzata per un trust-store e memorizzare la nuova password nel vault. La password corrente dell'archivio di fiducia deve essere "conosciuta".
verify-keystore	controllare se i valori nel vault sono corretti: • Per gli utenti OCI, l'hash della password corrisponde al valore nel database • Per gli utenti MySQL, può essere effettuata una connessione al database • per i keystore, è possibile caricare il keystore e leggere le relative chiavi (se presenti)
tasti elenco	elencare le voci nel vault (senza mostrare il valore memorizzato)

Comandi limitati

L'autenticazione è necessaria per qualsiasi comando non nascosto che apporta modifiche coordinate all'installazione:

Comando	Descrizione
restore-vault-backup	Sostituisce il vault corrente con il vault contenuto nel file di backup del vault specificato. Esegue tutte le azioni coordinate per aggiornare l'installazione in modo che corrisponda alle password nel vault ripristinato: • Aggiornare le password degli utenti di comunicazione OCI • Aggiornare le password utente MySQL, incluso root • per ogni keystore, se la password del keystore è "conosciuta", aggiornare il keystore usando le password del vault ripristinato. Quando viene eseguito in modalità normale, legge anche ciascun valore crittografato dall'istanza, lo decrittografa utilizzando il servizio di crittografia del vault corrente, lo crittografa nuovamente utilizzando il servizio di crittografia del vault ripristinato e memorizza il valore crittografato nuovamente.
sincronizza con vault	Esegue tutte le azioni coordinate per aggiornare l'installazione in modo che corrisponda alle password utente nel vault ripristinato: • Aggiorna le password degli utenti di comunicazione OCI • Aggiorna le password utente MySQL, incluso root

change-password (cambia password)	Modifica la password nel vault ed esegue le azioni coordinate.
sostituire le chiavi	Creare un nuovo vault vuoto (che avrà chiavi diverse da quelle esistenti). Quindi copiare le voci dal vault corrente al nuovo vault. Quindi legge ciascun valore crittografato dall'istanza, decrittografarlo utilizzando il servizio di crittografia del vault corrente, crittografarlo nuovamente utilizzando il servizio di crittografia del vault ripristinato e memorizzare il valore crittografato nuovamente.

Azioni coordinate

Vault dei server

_interno	aggiorna hash password per l'utente nel database
acquisizione	aggiorna hash password per l'utente nel database se il vault di acquisizione è presente, aggiornare anche la voce nel vault di acquisizione
dwh_internal	aggiorna hash password per l'utente nel database
cognos_admin	aggiorna hash password per l'utente nel database Se DWH e Windows, aggiornare SANscreen/cognos/Analytics/Configuration/SANscreenAP.properties per impostare la proprietà cognos.admin sulla password.
root	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
inventario	Eseguire SQL per aggiornare la password utente nell'istanza MySQL

dwh	Eseguire SQL per aggiornare la password utente nell'istanza MySQL Se DWH e Windows, aggiornare il registro di Windows per impostare le seguenti voci ODBC sulla nuova password: • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Capacity_Efficiency\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_fs_util\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Inventory\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_performance\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_Ports\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_sa\PWD • HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\ODBC\ODBC.INI\dwh_cloud_cost\PWD
dwhuser	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
host	Eseguire SQL per aggiornare la password utente nell'istanza MySQL
password_keystore	riscrivere il keystore con la nuova password - wildfly/standalone/configuration/server.keystore
truststore_password	riscrivere il keystore con la nuova password - wildfly/standalone/configuration/server.trustore
password_chiave	riscrivere il keystore con la nuova password - wildfly/standalone/configuration/sso.jks
archivio_cognos	nessuno

Vault di acquisizione

acquisizione	nessuno
truststore_password	riscrivere il keystore con la nuova password (se esiste) - acq/conf/cert/client.keystore

Esecuzione di Security Admin Tool - riga di comando

La sintassi per eseguire lo strumento SA in modalità riga di comando è la seguente:

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

where

-s                      selects server vault
-au                     selects acquisition vault

-db                     selects direct operation mode

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

Note:

- L'opzione "-i" potrebbe non essere presente sulla riga di comando (in quanto questo seleziona la modalità interattiva).
- per le opzioni "-s" e "-au":
  - "-s" non è consentito su una RAU
  - "-au" non è consentito su DWH
  - se nessuno dei due è presente, allora
    - Il vault del server è selezionato su Server, DWH e Dual
    - Il vault di acquisizione viene selezionato su RAU
- Le opzioni -lu e -lp vengono utilizzate per l'autenticazione dell'utente.
  - Se viene specificato <user> e <password> non lo è, all'utente verrà richiesta la password.
  - Se <user> non viene fornito ed è richiesta l'autenticazione, all'utente verranno richiesti sia <user> che <password>.

Comandi:

Comando	Utilizzo
password-memorizzata-corretta	`securityadmin [-s`

-au] [-db] -pt <key> [<value>]
 	
`where`
 	
-pt specifies the command ("put") <key> is the key <value> is the value. If not present, user will be prompted for value
 	
` `
	vault di backup

`securityadmin [-s`	-au] [-db] -b [<backup-dir>] where -b specified command <backup-dir> is the output directory. If not present, default location of SANscreen/backup/vault is used The backup file will be named ServerSecurityBackup-yyyy-MM-dd-HH-mm.zip ` `
vault di backup	`securityadmin [-s`
-au] [-db] -ub <backup-file> where -ub specified command ("upgrade-backup") <backup-file> The location to write the backup file ` `	tasti elenco

`securityadmin [-s`	-au] [-db] -l where -l specified command ``
tasti di controllo	`securityadmin [-s`
-au] [-db] -ck where -ck specified command exit code: 1 error 2 default key(s) 3 unique keys ``	verify-keystore (server)

`securityadmin [-s] [-db] -v`
 	
`where`
 	
`-v specified command`
	eseguire l'upgrade

`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -u where -u specified command For server vault, if -lu is not present, then authentication will be performed for <user> =_internal and <password> = _internal's password from vault. For acquisition vault, if -lu is not present, then no authentication will be attempted ``

sostituire le chiavi	`securityadmin [-s`
-au] [-db] [-lu <user>] [-lp <password>] -rk where -rk specified command ``	restore-vault-backup
`securityadmin [-s`	-au] [-db] [-lu <user>] [-lp <password>] -r <backup-file> where -r specified command <backup-file> the backup file location ``

modifica-password (server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -up -un <user> -p [<password>] [-sh]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-un <user> entry ("user") name to update`
	`-p <password> new password. If <password not supplied, user will be prompted.`
	`-sh for mySQL user, use strong hash`

modifica password per l'utente di acquisizione (acquisizione)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -up -p [<password>]`
	
	`where`
	
	`-up specified command ("update-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

change-password per truststore-_password (acquisizione)	`securityadmin [-au] [-db] [-lu <user>] [-lp <password>] -utp -p [<password>]`
	
	`where`
	
	`-utp specified command ("update-truststore-password")`
	`-p <password> new password. If <password not supplied, user will be prompted.`

sincronizza con vault (server)	`securityadmin [-s] [-db] [-lu <user>] [-lp <password>] -sv <backup-file>`
	
	`where`
	
	`-sv specified command`

Esecuzione dello strumento di amministrazione della protezione - modalità interattiva

Interattivo - Menu principale

Per eseguire lo strumento SA in modalità interattiva, immettere il seguente comando:

```
 securityadmin -i
In un server o in un'installazione doppia, securityadmin richiederà
all'utente di selezionare il server o l'unità di acquisizione locale.
```

Rilevati nodi server e unità di acquisizione. Selezionare il nodo di cui si desidera riconfigurare la protezione:

```
1 - Server

2 - Local Acquisition Unit

9 - Exit

Enter your choice:
```

In DWH, "Server" viene selezionato automaticamente. Su un'unità AU remota, viene selezionata automaticamente l'opzione "Acquisition Unit" (unità di acquisizione).

Interactive - Server: Recupero della password di root

In modalità Server, lo strumento securityadmin controlla innanzitutto che la password root memorizzata sia corretta. In caso contrario, viene visualizzata la schermata di ripristino della password principale.

```
ERROR: Database is not accessible

1 - Enter root password

2 - Get root password from vault backup

9 - Exit

Enter your choice:
```

Se si seleziona l'opzione 1, all'utente verrà richiesta la password corretta.

```
 Enter password (blank = don't change)
 Enter correct password for 'root':
Se viene inserita la password corretta, viene visualizzato quanto segue.
```

```
 Password verified.  Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se viene immessa una password errata, viene visualizzato quanto segue

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Premere invio per tornare al menu di ripristino.
```

Se si seleziona l'opzione 2, all'utente verrà richiesto di specificare il nome di un file di backup da cui leggere la password corretta:

```
 Enter Backup File Location:
Se la password del backup è corretta, viene visualizzato quanto segue.
```

```
 Password verified.  Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se la password nel backup non è corretta, viene visualizzato quanto segue

```
 Password verification failed - Access denied for user 'root'@'localhost'
(using password: YES)
Premere invio per tornare al menu di ripristino.
```

Interactive - Server: Password corretta

L'azione "Password corretta" viene utilizzata per modificare la password memorizzata nel vault in modo che corrisponda alla password effettiva richiesta dall'installazione. Questo comando è utile in situazioni in cui è stata apportata una modifica all'installazione da qualcosa di diverso dallo strumento securityadmin. Alcuni esempi sono:

- La password per un utente SQL è stata modificata mediante l'accesso diretto a MySQL.
- Viene sostituito un archivio chiavi o la password di un archivio chiavi viene modificata utilizzando keytool.
- Un database OCI è stato ripristinato e tale database ha password diverse per gli utenti interni

"Correct Password" (Password corretta) richiede innanzitutto all'utente di selezionare la password per memorizzare il valore corretto.

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

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Dopo aver selezionato la voce da correggere, all'utente viene richiesto come desidera fornire il valore.

```
1 - Enter {user} password

2 - Get {user} password from vault backup

9 - Exit

Enter your choice:
```

Se si seleziona l'opzione 1, all'utente verrà richiesta la password corretta.

```
 Enter password (blank = don't change)
 Enter correct password for '{user}':
Se viene inserita la password corretta, viene visualizzato quanto segue.
```

```
 Password verified.  Vault updated
Premendo invio si torna al menu senza restrizioni del server.
```

Se viene immessa una password errata, viene visualizzato quanto segue

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

Premendo invio si torna al menu senza restrizioni del server.

Se si seleziona l'opzione 2, all'utente verrà richiesto di specificare il nome di un file di backup da cui leggere la password corretta:

```
 Enter Backup File Location:
Se la password del backup è corretta, viene visualizzato quanto segue.
```

```
 Password verified.  Vault updated
Premendo invio viene visualizzato il menu senza restrizioni del server.
```

Se la password nel backup non è corretta, viene visualizzato quanto segue

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

Premendo invio viene visualizzato il menu senza restrizioni del server.

Interactive - Server: Verifica del contenuto del vault

Verificare che il contenuto del vault verifichi se il vault dispone di chiavi corrispondenti al vault predefinito distribuito con le versioni OCI precedenti e verifichi se ciascun valore nel vault corrisponde all'installazione.

I possibili risultati per ogni chiave sono:

OK	Il valore del vault è corretto
Non selezionato	Impossibile verificare il valore rispetto all'installazione
PESSIMO	Il valore non corrisponde all'installazione

Mancante	Manca una voce prevista.

```
Encryption keys secure: unique, non-default encryption keys detected

             cognos_admin: OK
                    hosts: OK
             dwh_internal: OK
                inventory: OK
                  dwhuser: OK
        keystore_password: OK
                      dwh: OK
      truststore_password: OK
                     root: OK
                _internal: OK
          cognos_internal: Not Checked
             key_password: OK
              acquisition: OK
           cognos_archive: Not Checked
 cognos_keystore_password: Missing


Press enter to continue
```

Interactive - Server: Backup

Backup richiede la directory in cui deve essere memorizzato il file zip di backup. La directory deve già esistere e il nome del file sarà ServerSecurityBackup-yyyy-mm-dd-hh-mm.zip.

```
Enter backup directory location [C:\Program Files\SANscreen\backup\vault]
:

Backup Succeeded!   Backup File: C:\Program
Files\SANscreen\backup\vault\ServerSecurityBackup-2024-08-09-12-02.zip
```

Interactive - Server: Login

L'azione di accesso viene utilizzata per autenticare un utente e ottenere l'accesso alle operazioni che modificano l'installazione. L'utente deve disporre di un Privileges di amministrazione. Quando viene eseguito con il server, può essere utilizzato qualsiasi utente amministratore; quando viene eseguito in modalità diretta, l'utente deve essere un utente locale piuttosto che un utente LDAP.

```
Authenticating via server. Enter user and password

UserName: admin

Password:
```

oppure

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:
```

Se la password è corretta e l'utente è un utente amministratore, viene visualizzato il menu limitato.

Se la password non è corretta, viene visualizzato quanto segue:

```
Authenticating via database.  Enter local user and password.

UserName: admin

Password:

Login Failed!
```

Se l'utente non è un amministratore, viene visualizzato quanto segue:

```
Authenticating via server. Enter user and password

UserName: user

Password:

User 'user' does not have 'admin' role!
```

Interactive - Server: Menu limitato

Una volta effettuato l'accesso, lo strumento visualizza il menu limitato.

```
Logged in as: admin
Select Action:

2 - Change Password

3 - Verify Vault Contents

4 - Backup

5 - Restore

6 - Change Encryption Keys

7 - Fix installation to match vault

9 - Exit

Enter your choice:
```

Interactive - Server: Cambia password

L’azione "Cambia password" viene utilizzata per modificare una password di installazione in un nuovo valore.

"Cambia password" richiede innanzitutto all’utente di selezionare la password da modificare.

```
Change Password
Select User:  (Enter 'b' to go Back)

1 - _internal

2 - acquisition

3 - cognos_admin

4 - cognos keystore

5 - dwh

6 - dwh_internal

7 - dwhuser

8 - hosts

9 - inventory

10 - sso keystore

11 - server keystore

12 - root

13 - server truststore

14 - AU truststore

Enter your choice:
```

Dopo aver selezionato la voce da correggere, se l'utente è un utente MySQL, all'utente verrà chiesto se eseguire un hash sicuro per la password

```
MySQL supports SHA-1 and SHA-256 password hashes. SHA-256 is stronger but
requires all clients use SSL connections

Use strong password hash? (Y/n): y
```

Quindi, all'utente viene richiesta la nuova password.

```
New Password for '{user}':
If the password is empty, the operation is cancelled.

Password is empty - cancelling operation
```

Se viene immessa una password non vuota, all'utente viene richiesto di confermarla.

```
New Password for '{user}':

Confirm New Password for '{user}':

Password successfully updated for 'dwhuser'!
```

Se la modifica non riesce, viene visualizzato l'errore o l'eccezione.

Interactive - Server: Ripristino

Interactive - Server (interattivo - Server): Modifica delle chiavi di crittografia

L'azione Modifica chiavi di crittografia sostituirà la chiave di crittografia utilizzata per crittografare le voci del vault e sostituirà la chiave di crittografia utilizzata per il servizio di crittografia del vault. Poiché la chiave del servizio di crittografia viene modificata, i valori crittografati nel database vengono nuovamente crittografati; vengono letti, decrittografati con la chiave corrente, crittografati con la nuova chiave e salvati nuovamente nel database.

Questa azione non è supportata in modalità diretta poiché il server fornisce l'operazione di ricodifica per alcuni contenuti del database.

```
Replace encryption key with new key and update encrypted database values

Confirm (y/N): y

Change Encryption Keys succeeded! Restart 'Server' Service!
```

Interactive - Server: Installazione fix

L'azione Correggi installazione aggiornerà l'installazione. Tutte le password di installazione che possono essere modificate tramite lo strumento securityadmin, ad eccezione di root, saranno impostate sulle password nel vault.

- Le password degli utenti interni di OCI verranno aggiornate.
- Le password degli utenti MySQL, ad eccezione di root, verranno aggiornate.
- Le password dei keystore verranno aggiornate.

```
Fix installation - update installation passwords to match values in vault

Confirm:  (y/N): y

Installation update succeeded! Restart 'Server' Service.
```

L'azione si interrompe al primo aggiornamento non riuscito e visualizza l'errore o l'eccezione.

Gestione della sicurezza sul server Insight

Il `securityadmin` Consente di gestire le opzioni di sicurezza sul server Insight. La gestione della sicurezza include la modifica delle password, la generazione di nuove chiavi, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle configurazioni alle impostazioni predefinite.

A proposito di questa attività

Si utilizza `securityadmin` tool per gestire la sicurezza:

- Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Per ulteriori informazioni, consultare la "Securityadmin"documentazione.

Gestione della sicurezza sull'unità di acquisizione locale

Il `securityadmin` Tool consente di gestire le opzioni di sicurezza sull'utente di acquisizione locale (LAU). La gestione della sicurezza include la gestione di chiavi e password, il salvataggio e il ripristino delle configurazioni di sicurezza create o il ripristino delle impostazioni predefinite delle configurazioni.

Prima di iniziare

Devi avere `admin` privilegi per eseguire attività di configurazione della sicurezza.

A proposito di questa attività

Si utilizza `securityadmin` tool per gestire la sicurezza:

- Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Per ulteriori informazioni, vedere le "Strumento securityadmin"istruzioni.

Gestione della sicurezza su una RAU

Il `securityadmin` Tool consente di gestire le opzioni di sicurezza su Raus. Potrebbe

essere necessario eseguire il backup o il ripristino di una configurazione del vault, modificare le chiavi di crittografia o aggiornare le password per le unità di acquisizione.

A proposito di questa attività

Si utilizza `securityadmin` tool per gestire la sicurezza:

- Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Uno scenario per aggiornare la configurazione di protezione per LAU/RAU è l'aggiornamento della password utente di 'acquisizione' quando la password per quell'utente è stata modificata sul server. LAU e tutti i Raus utilizzano la stessa password dell'utente 'acquisizione' del server per comunicare con il server.

L'utente di "acquisizione" esiste solo sul server Insight. RAU o LAU accedono come tale utente quando si connettono al server.

Per ulteriori informazioni, vedere le "Strumento securityadmin"istruzioni.

Gestione della sicurezza nel Data Warehouse

Il `securityadmin` Consente di gestire le opzioni di sicurezza sul server Data Warehouse. La gestione della sicurezza include l'aggiornamento delle password interne per gli utenti interni sul server DWH, la creazione di backup della configurazione di sicurezza o il ripristino delle configurazioni alle impostazioni predefinite.

A proposito di questa attività

Si utilizza `securityadmin` tool per gestire la sicurezza:

- Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat`
- Linux - `/bin/oci-securityadmin.sh`

Per ulteriori informazioni, consultare la "Securityadmin"documentazione.

Modifica delle password utente interne di OnCommand Insight

Le policy di sicurezza potrebbero richiedere la modifica delle password nell'ambiente OnCommand Insight. Alcune delle password di un server si trovano su un server diverso dell'ambiente, che richiede la modifica della password su entrambi i server. Ad esempio, quando si modifica la password utente "Inventory" su Insight Server, è necessario corrispondere alla password utente "Inventory" sul connettore del server Data Warehouse configurato per Insight Server.

Prima di iniziare

Prima di modificare le password, è necessario comprendere le dipendenze degli account utente. Il mancato aggiornamento delle password su tutti i server richiesti causerà errori di comunicazione tra i componenti Insight.

A proposito di questa attività

La seguente tabella elenca le password utente interne per Insight Server e i componenti Insight con password dipendenti che devono corrispondere alla nuova password.

Password di Insight Server	Modifiche richieste
_interno	
acquisizione	LAU, RAU
dwh_internal	Data Warehouse
host	
inventario	Data Warehouse
root	

La seguente tabella elenca le password utente interne per Data Warehouse ed elenca i componenti Insight che hanno password dipendenti che devono corrispondere alla nuova password.

Password Data Warehouse	Modifiche richieste
cognos_admin	
dwh	
dwh_internal (modificato utilizzando l'interfaccia utente di configurazione di Server Connector)	Server Insight
dwhuser	
host	
Inventario (modificato utilizzando l'interfaccia utente di configurazione di Server Connector)	Server Insight
root	

Modifica delle password nell'interfaccia utente di configurazione della connessione del server DWH

La seguente tabella elenca la password utente per LAU ed elenca i componenti Insight con password dipendenti che devono corrispondere alla nuova password.

LAU password	Modifiche richieste
acquisizione	Insight Server, RAU

Modifica delle password "inventario" e "dwh_internal" utilizzando l'interfaccia utente di configurazione della connessione al server

Se è necessario modificare le password "Inventory" o "dwh_internal" in modo che corrispondano a quelle del server Insight, utilizzare l'interfaccia utente di Data Warehouse.

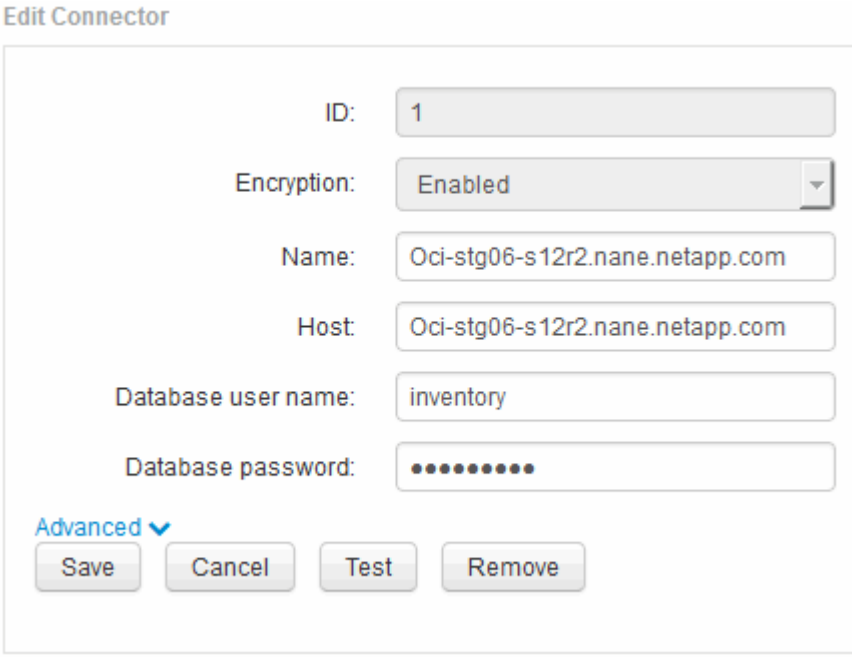
Prima di iniziare

Per eseguire questa attività, è necessario essere connessi come amministratore.

Fasi

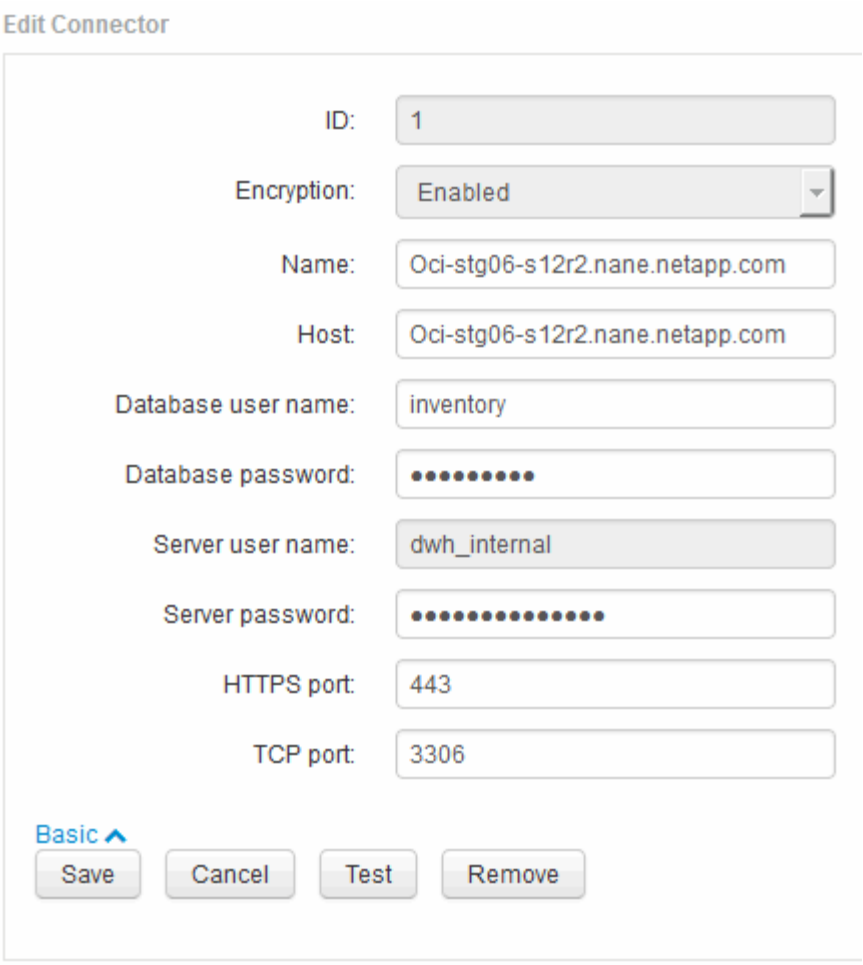
1. Accedere al Data Warehouse Portal all'indirizzo https://hostname/dwh, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

   Viene visualizzata la schermata **Edit Connector** (Modifica connettore).



3. Immettere una nuova password "Inventory" per il campo **Database password**.
4. Fare clic su **Save** (Salva)
5. Per modificare la password "dwh_internal", fare clic su **Advanced.**

   Viene visualizzata la schermata Edit Connector Advanced (Modifica avanzate connettore).



6. Inserire la nuova password nel campo **Server password**:
7. Fare clic su Save (Salva)

Modifica della password dwh mediante lo strumento di amministrazione ODBC

Quando si modifica la password per l'utente dwh sul server Insight, la password deve essere modificata anche sul server Data Warehouse. Utilizzare lo strumento Amministratore origine dati ODBC per modificare la password nel Data Warehouse.

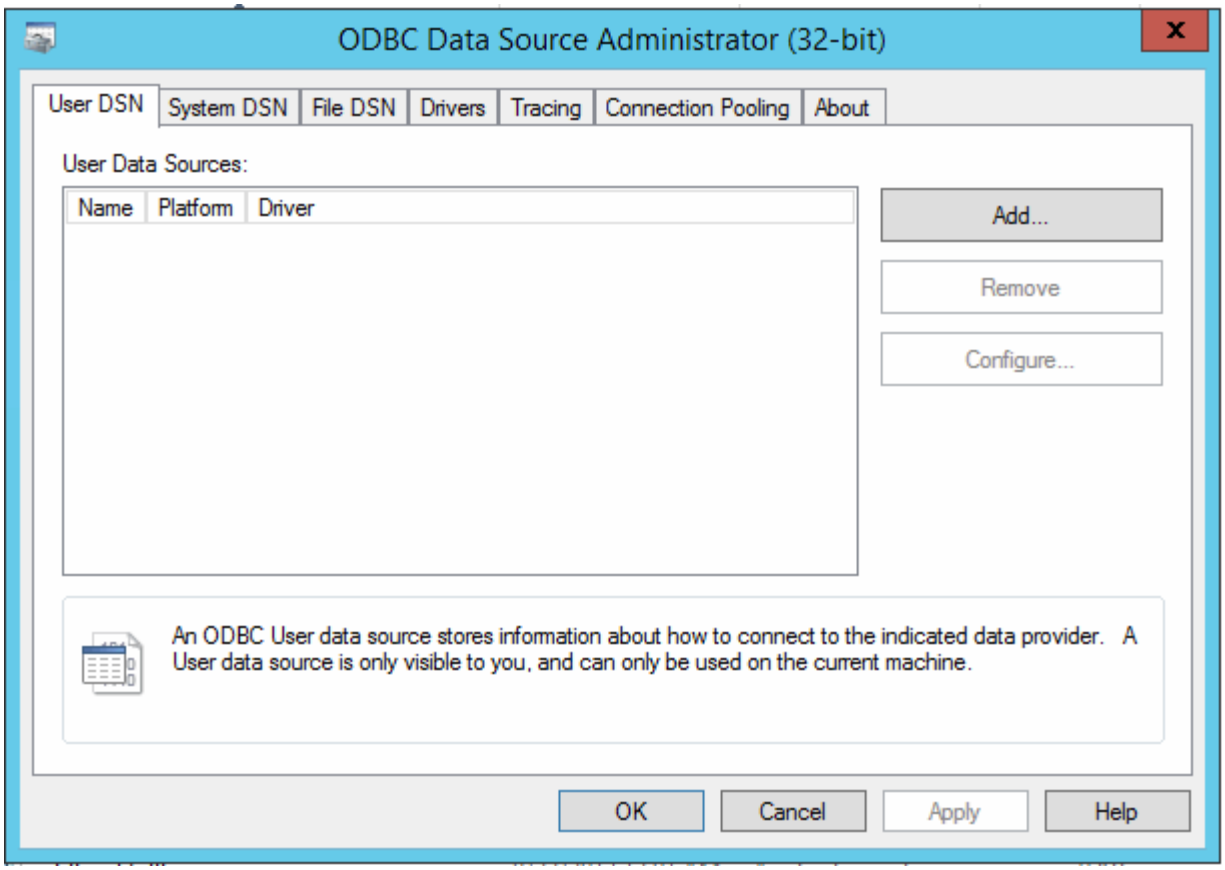
Prima di iniziare

È necessario eseguire un accesso remoto al server Data Warehouse utilizzando un account con privilegi di amministratore.

Fasi

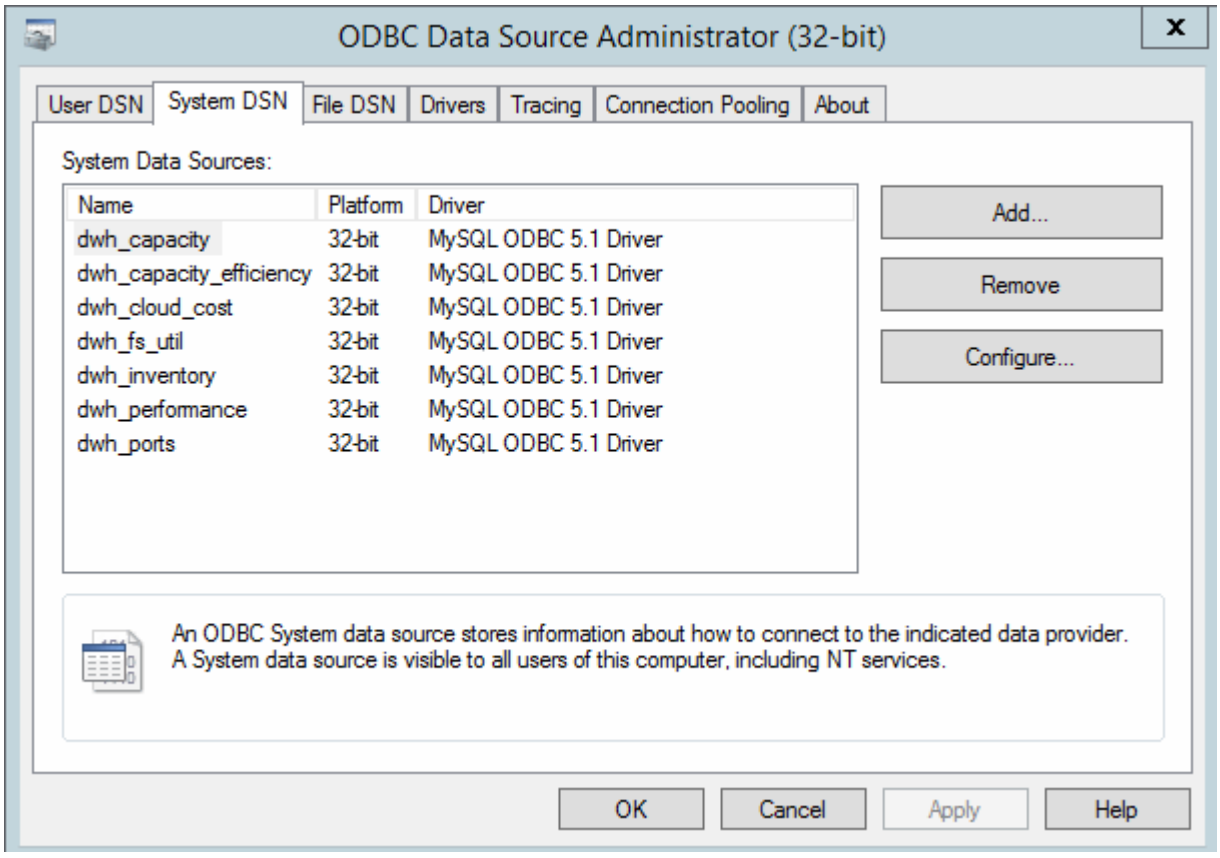
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

   Viene visualizzata la schermata Amministratore origine dati ODBC.



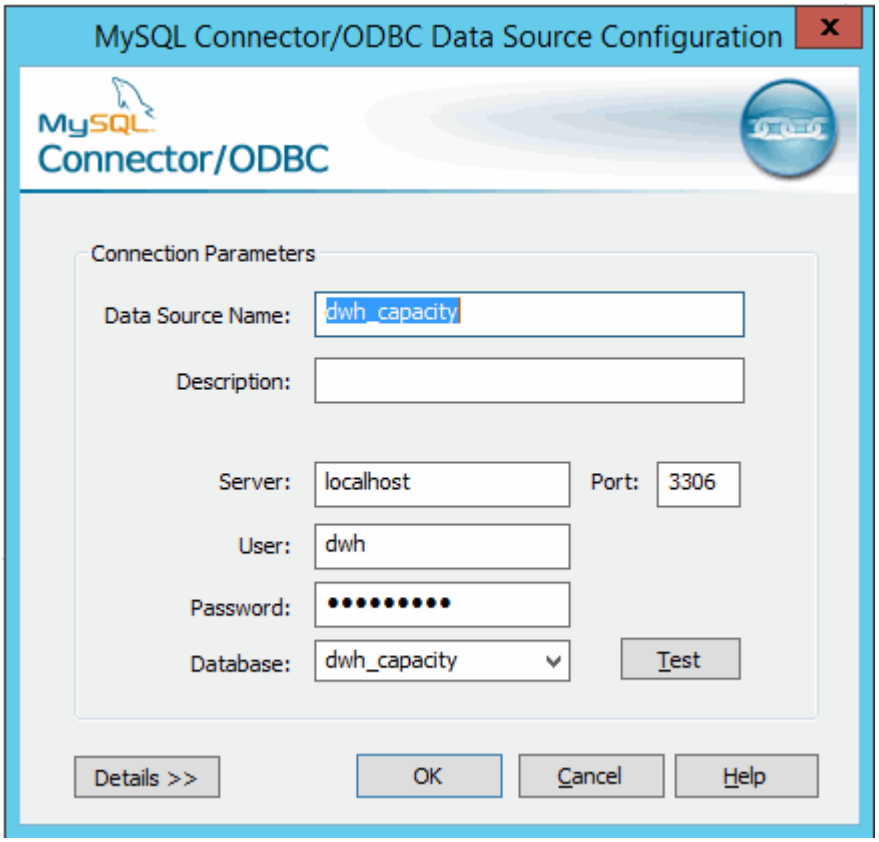
3. Fare clic su **DSN di sistema**

   Vengono visualizzate le origini dati di sistema.



4. Selezionare un'origine dati OnCommand Insight dall'elenco.
5. Fare clic su **Configura**

   Viene visualizzata la schermata Data Source Configuration (Configurazione origine dati).



6. Inserire la nuova password nel campo **Password**.

Supporto di accesso con smart card e certificato

OnCommand Insight supporta l'utilizzo di smart card (CAC) e certificati per autenticare gli utenti che accedono ai server Insight. È necessario configurare il sistema per abilitare queste funzioni.

Dopo aver configurato il sistema per il supporto di CAC e certificati, la navigazione verso una nuova sessione di OnCommand Insight comporta la visualizzazione di una finestra di dialogo nativa che fornisce all'utente un elenco di certificati personali tra cui scegliere. Questi certificati vengono filtrati in base al set di certificati personali emessi dalle CA attendibili dal server OnCommand Insight. La maggior parte delle volte, esiste una singola scelta. Per impostazione predefinita, Internet Explorer salta questa finestra di dialogo se esiste una sola scelta.

Per gli utenti CAC, le smart card contengono più certificati, uno solo dei quali può corrispondere alla CA attendibile. Il certificato CAC per `identification` deve essere utilizzato.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Configurazione degli host per l'accesso a smart card e certificati

È necessario apportare modifiche alla configurazione dell'host OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati.

Prima di iniziare

- LDAP deve essere attivato nel sistema.
- LDAP `User principal account name` L'attributo deve corrispondere al campo LDAP che contiene l'ID dell'utente.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Utilizzare `regedit` utility per modificare i valori del registro di sistema in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`:

a. Modificare l'opzione JVM_Option `DclientAuth=false` a. `DclientAuth=true.`

2. Eseguire il backup del file keystore: `C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Aprire un prompt dei comandi specificando `Run as administrator`
4. Eliminare il certificato autogenerato: `C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
5. Generare un nuovo certificato: `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. Generare una richiesta di firma del certificato (CSR): `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. Una volta restituito il CSR nel passaggio 6, importare il certificato, quindi esportarlo in formato base-64 e collocarlo in `"C:\temp" named servername.cer`.
8. Estrarre il certificato dal keystore:`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. Estrarre una chiave privata dal file p12: `openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"`
10. Unire il certificato base-64 esportato al punto 7 con la chiave privata: `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. Importare il certificato Unito nel keystore: `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. Importare il certificato root: `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. Importare il certificato root nel 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. Importare il certificato intermedio: `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"`

Ripetere questo passaggio per tutti i certificati intermedi.

15. Specificare il dominio in LDAP da associare a questo esempio.
16. Riavviare il server.

Configurazione di un client per il supporto dell'accesso con smart card e certificato

I computer client richiedono middleware e modifiche ai browser per consentire l'utilizzo di Smart Card e per l'accesso ai certificati. I clienti che utilizzano già Smart Card non devono richiedere ulteriori modifiche ai computer client.

Prima di iniziare

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

A proposito di questa attività

Di seguito sono riportati i requisiti di configurazione del client più comuni:

- Installazione del middleware Smart Card, ad esempio ActivClient (vedere http://militarycac.com/activclient.htm)
- Modifica del browser IE (vedere http://militarycac.com/files/Making_AKO_work_with_Internet_Explorer_color.pdf)
- Modifica del browser Firefox (vedere https://militarycac.com/firefox2.htm)

Abilitazione del CAC su un server Linux

Alcune modifiche sono necessarie per abilitare il CAC su un server Linux OnCommand Insight.

La CA principale deve essere importata nel truststore.

Fasi

1. Selezionare `/opt/netapp/oci/conf/`
2. Modifica `wildfly.properties` e modificare il valore di `CLIENT_AUTH_ENABLED` A "vero"

3. Importare il "`certificato di origine" esistente in `/opt/netapp/oci/wildfly/standalone/configuration/server.truststore`
4. Riavviare il server

Configurazione di Data Warehouse per l'accesso a smart card e certificati

È necessario modificare la configurazione del data warehouse di OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati.

Prima di iniziare

- LDAP deve essere attivato nel sistema.
- LDAP `User principal account name` L'attributo deve corrispondere al campo LDAP che contiene il numero dell'ID governativo di un utente.

  Il nome comune (CN) memorizzato nei CAC emessi dal governo è normalmente nel seguente formato: `first.last.ID`. Per alcuni campi LDAP, ad esempio `sAMAccountName`, questo formato è troppo lungo. Per questi campi, OnCommand Insight estrae solo il numero ID dal CNS.

Se sono state modificate le password *server.keystore* e/o *server.trustore* utilizzando "securityadmin", riavviare il servizio *SANscreen* prima di importare il certificato LDAP.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Utilizzare regedit per modificare i valori del Registro di sistema in `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java`

   a. Modificare l'opzione JVM_Option `-DclientAuth=false` a. `-DclientAuth=true`.

   Per Linux, modificare `clientAuth` parametro in `/opt/netapp/oci/scripts/wildfly.server`

2. Aggiungere le autorità di certificazione (CA) al trustore del Data Warehouse:

   a. In una finestra di comando, passare a. `..\SANscreen\wildfly\standalone\configuration`.

b. Utilizzare l' `keytool`utilità per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass <password>` + consultare la "Securityadmin"documentazione per ulteriori informazioni sull'impostazione o la modifica della password per server_trustore.

   La prima parola in ciascuna riga indica l'alias della CA.

c. Se necessario, fornire un file di certificato CA, di solito un `.pem` file. Per includere le CA del cliente con le CA attendibili del Data Warehouse, visitare il sito `..\SANscreen\wildfly\standalone\configuration` e utilizzare `keytool` comando di importazione: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

   My_alias è in genere un alias che identificherebbe facilmente la CA in`keytool -list` operazione.

3. Sul server OnCommand Insight, la `wildfly/standalone/configuration/standalone-full.xml` Il file deve essere modificato aggiornando verify-client su "REQUESTED" in `/subsystem=undertow/server=default-server/https-listener=default-https`Per attivare CAC. Accedere al server Insight ed eseguire il comando appropriato:

SISTEMA OPERATIVO	Script
Windows	<install dir>/SANscreen/wildfly/bin/enableCACforRemoteEJB.bat
Linux	/Opt/netapp/oci/wildfly/bin/enableCACforRemoteEJB.sh

   Dopo aver eseguito lo script, attendere il completamento del ricaricamento del server wildfly prima di passare al punto successivo.

4. Riavviare il server OnCommand Insight.

Configurazione dei Cognos per l'accesso con smart card e certificato (OnCommand Insight 7.3.10 e versioni successive)

È necessario modificare la configurazione del data warehouse di OnCommand Insight per supportare gli accessi con smart card (CAC) e certificati per il server Cognos.

Prima di iniziare

Questa procedura riguarda i sistemi che eseguono OnCommand Insight 7.3.10 e versioni successive.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Fasi

1. Aggiungere le autorità di certificazione (CA) al trustore Cognos.
   a. In una finestra di comando, passare a. `..\SANscreen\cognos\analytics\configuration\certs\`
   b. Utilizzare l' `keytool`utilità per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass <password>`

      La prima parola in ciascuna riga indica l'alias della CA.

   c. Se non esistono file adatti, fornire un file di certificato CA, di solito un `.pem` file.
   d. Per includere le CA del cliente con le CA attendibili di OnCommand Insight, visitare il sito Web all'indirizzo `..\SANscreen\cognos\analytics\configuration\certs\`.
   e. Utilizzare `keytool` utility per importare `.pem` file: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

      `my_alias` È in genere un alias che identifica facilmente la CA nell'`keytool -list`operazione.

   f. Quando viene richiesta una password, immetterla nel file */SANscreen/bin/cognos_info.dat*.
   g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.
2. Per attivare la modalità CAC, procedere come segue:
   a. Configurare la pagina di disconnessione CAC, seguendo questa procedura:
      - Accesso al portale Cognos (l'utente deve far parte del gruppo System Administrators, ad esempio cognos_admin)
      - (Solo per 7.3.10 e 7.3.11) fare clic su Manage (Gestisci)→ Configuration (Configurazione)→ System (sistema)→ Security (sicurezza)
      - (Solo per 7.3.10 e 7.3.11) inserire cacLogout.html rispetto all'URL di reindirizzamento disconnessione /→ richiedere
      - Chiudere il browser.
   b. Eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

c. Avviare il servizio IBM Cognos. Attendere l'avvio del servizio Cognos.

3. Per disattivare la modalità CAC, procedere come segue:
   a. Eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
   b. Avviare il servizio IBM Cognos. Attendere l'avvio del servizio Cognos.
   c. (Solo per 7.3.10 e 7.3.11) Disconfigurare la pagina di disconnessione CAC, seguendo la procedura riportata di seguito:
      - Accesso al portale Cognos (l'utente deve far parte del gruppo System Administrators, ad esempio cognos_admin)
      - Fare clic su Manage (Gestisci)→ Configuration (Configurazione)→ System (sistema)→ Security (sicurezza)
      - Inserire cacLogout.html nell'URL di reindirizzamento disconnessione
      - Chiudere il browser.

Importazione di certificati SSL con firma CA per Cognos e DWH (Insight 7.3.10 e versioni successive)

È possibile aggiungere certificati SSL per abilitare l'autenticazione e la crittografia avanzate per l'ambiente Data Warehouse e Cognos.

Prima di iniziare

Questa procedura riguarda i sistemi che eseguono OnCommand Insight 7.3.10 e versioni successive.

Per le istruzioni più aggiornate sul CAC e sul certificato, consulta i seguenti articoli della Knowledge base (è richiesto l'accesso al supporto):

- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per OnCommand Insight"
- "Come configurare l'autenticazione della scheda di accesso comune (CAC) per il data warehouse OnCommand Insight"
- "Come creare e importare un certificato firmato dall'autorità di certificazione (CA) in OnComand Insight e OnCommand Insight Data Warehouse 7.3.x"
- "Come creare un certificato autofirmato in OnCommand Insight 7.3.X installato su un host Windows"
- "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

A proposito di questa attività

Per eseguire questa procedura, è necessario disporre dei privilegi di amministratore.

Fasi

1. Arrestare Cognos utilizzando lo strumento di configurazione IBM Cognos. Chiudere Cognos.
2. Creare backup di `..\SANScreen\cognos\analytics\configuration` e. `..\SANScreen\cognos\analytics\temp\cam\freshness` cartelle.

3. Generare una richiesta di crittografia del certificato da Cognos. In una finestra Admin CMD, eseguire:
   a. cd "`\Program Files\sanscreen\cognos\analytics\bin`"
   b. `ThirdPartyCertificateTool.bat -java:local -c -e -p <password> -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. Nota: In questo caso -H e -i devono aggiungere subjectAltNames come dns e ipaddress.
   c. Per <password>, utilizzare la password del file */SANscreen/bin/cognos_info.dat*.
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inserire il contenuto EncryptRequest.csr e generare il certificato utilizzando il portale per la firma CA.
6. Scarica i certificati della catena includendo il certificato root utilizzando il formato PKCS7

   In questo modo si scarica il file fqdn.p7b
7. Ottenere un certificato in formato .p7b dalla CA. Utilizzare un nome che lo contrassegna come certificato per il server Web Cognos.
8. ThirdPartyCertificateTool.bat non riesce ad importare l'intera catena, pertanto sono necessari più passaggi per esportare tutti i certificati. Suddividere la catena esportandole singolarmente come segue:
   a. Aprire il certificato .p7b in "Crypto Shell Extensions".
   b. Selezionare "Certificates" nel riquadro sinistro.
   c. Fare clic con il pulsante destro del mouse su CA principale > tutte le attività > Esporta.
   d. Selezionare l'output Base64.
   e. Immettere un nome di file che lo identifichi come certificato root.
   f. Ripetere i passaggi da 8a a 8e per esportare tutti i certificati separatamente in file .cer.
   g. Assegnare un nome ai file intermediateX.cer e cognos.cer.
9. Ignorare questo passaggio se si dispone di un solo certificato CA, altrimenti unire sia root.cer che intermediateX.cer in un unico file.
   a. Aprire root.cer con blocco note e copiare il contenuto.
   b. Aprire intermediate.cer con blocco note e aggiungere il contenuto da 9a (intermedio prima e root avanti).
   c. Salvare il file come chain.cer.
10. Importare i certificati nel keystore Cognos utilizzando il prompt Admin CMD:
    a. cd "`Program Files/sanscreen/cognos/Analytics` bin"
    b. ThirdPartyCertificateTool.bat -java:local -i -T -r c
    c. ThirdPartyCertificateTool.bat -java:local -i -T -r c
    d. ThirdPartyCertificateTool.bat -java:local -i -e -r c
11. Aprire IBM Cognos Configuration.
    a. Selezionare Local Configuration (Configurazione locale)-→ Security (protezione) -→ Cryptography (crittografia) -→ Cognos
    b. Modifica "Usa CA di terze parti?" Su vero.
    c. Salvare la configurazione.
    d. Riavviare Cognos

12. Esportare il certificato Cognos più recente in cognos.crt utilizzando il prompt Admin CMD:
    a. cd "`C: Programmi/SANscreen"
    b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\Configuration\certs\CAMKeystore -storetype PKCS12 -storepass <password> -alias Encryption
    c. Per <password>, utilizzare la password del file */SANscreen/bin/cognos_info.dat*.
13. Eseguire il backup del trustore del server DWH all'indirizzo `..\SANscreen\wildfly\standalone\configuration\server.trustore`
14. Importare "`c:` temp cognos.crt" in DWH trustore per stabilire la comunicazione SSL tra Cognos e DWH, utilizzando la finestra del prompt Admin CMD.
    a. cd "`C: Programmi/SANscreen"
    b. java\bin\keytool.exe -importcert -file c:\temp\cognos.crt -keystore wildfly\standalone\configuration\server.trustore -storepass <password> -alias cognos3rdca
    c. Per <password>, utilizzare la password del file */SANscreen/bin/cognos_info.dat*.
15. Riavviare il servizio SANscreen.
16. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.
17. I seguenti passaggi devono essere eseguiti anche quando viene modificato solo il "sSL certificate" e i certificati Cognos predefiniti rimangono invariati. In caso contrario, Cognos potrebbe lamentarsi del nuovo certificato SANscreen o non essere in grado di creare un backup DWH.

    a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
    b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass <password> -alias "ssl certificate"`
    c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

    In genere, questi passaggi vengono eseguiti nell'ambito del processo di importazione dei certificati Cognos descritto in "Come importare un certificato firmato dall'autorità di certificazione (CA) di Cognos in OnCommand DataWarehouse 7.3.3 e versioni successive"

Importazione di certificati SSL

È possibile aggiungere certificati SSL per abilitare l'autenticazione e la crittografia avanzate per migliorare la sicurezza dell'ambiente OnCommand Insight.

Prima di iniziare

Assicurarsi che il sistema soddisfi il livello di bit minimo richiesto (1024 bit).

A proposito di questa attività

Si consiglia vivamente di eseguire il backup del vault prima dell'aggiornamento.

Vedere le "Strumento securityadmin" istruzioni per ulteriori informazioni sul vault e sulla gestione delle password.

Fasi

1. Creare una copia del file keystore originale: `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old`
2. Elencare i contenuti del keystore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

   Il sistema visualizza il contenuto del keystore. Deve essere presente almeno un certificato nel keystore, `"ssl certificate"`.

3. Eliminare `"ssl certificate"`: `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. Generare una nuova chiave: `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. Quando viene richiesto di inserire il nome e il cognome, immettere il nome di dominio completo (FQDN) che si desidera utilizzare.
   b. Fornire le seguenti informazioni sull'organizzazione e sulla struttura organizzativa:
      - Paese: Abbreviazione ISO di due lettere per il proprio paese (ad esempio, Stati Uniti)
      - Stato o provincia: Nome dello stato o della provincia in cui si trova la sede centrale dell'organizzazione (ad esempio, Massachusetts)
      - Località: Nome della città in cui si trova la sede centrale dell'organizzazione (ad esempio, Waltham)
      - Nome dell'organizzazione: Nome dell'organizzazione proprietaria del nome di dominio (ad esempio, NetApp)
      - Nome dell'unità organizzativa: Nome del reparto o del gruppo che utilizzerà il certificato (ad esempio, supporto)
      - Domain Name/ Common Name (Nome dominio/Nome comune): Il nome FQDN utilizzato per le ricerche DNS del server (ad esempio, www.example.com). Il sistema risponde con informazioni simili a quanto segue: `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
   c. Invio `Yes` Quando il nome comune (CN) è uguale all'FQDN.
   d. Quando viene richiesta la password della chiave, immetterla o premere il tasto Invio per utilizzare la password del keystore esistente.
5. Generare un file di richiesta del certificato: `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`

   Il `c:\localhost.csr` file è il file di richiesta del certificato appena generato.

6. Inviare il `c:\localhost.csr` File all'autorità di certificazione (CA) per l'approvazione.

   Una volta approvato il file di richiesta del certificato, si desidera che il certificato venga restituito in `.der`

formato. Il file potrebbe essere restituito o meno come `.der` file. Il formato file predefinito è `.cer` Per i servizi Microsoft CA.

La maggior parte delle CA delle organizzazioni utilizza un modello di catena di trust, inclusa una CA principale, che spesso non è in linea. Ha firmato i certificati solo per alcune CA figlio, note come CA intermedie.

È necessario ottenere la chiave pubblica (certificati) per l'intera catena di trust, ovvero il certificato per la CA che ha firmato il certificato per il server OnCommand Insight e tutti i certificati compresi tra la CA che ha firmato e la CA principale dell'organizzazione.

In alcune organizzazioni, quando invii una richiesta di firma, potresti ricevere una delle seguenti informazioni:

- Un file PKCS12 contenente il certificato firmato e tutti i certificati pubblici nella catena di trust
- R `.zip` file contenente singoli file (incluso il certificato firmato) e tutti i certificati pubblici nella catena di trust
- Solo il certificato firmato

  È necessario ottenere i certificati pubblici.

7. Importare il certificato approvato per 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. Quando richiesto, inserire la password del keystore.

      Viene visualizzato il seguente messaggio: `Certificate reply was installed in keystore`
8. Importare il certificato approvato per 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. Quando richiesto, inserire la password trustore.

      Viene visualizzato il seguente messaggio: `Certificate reply was installed in trustore`
9. Modificare il `SANscreen\wildfly\standalone\configuration\standalone-full.xml` file:

   Sostituire la seguente stringa alias: `alias="cbc-oci-02.muccbc.hq.netapp.com"`. Ad esempio:

   ```
   <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. Riavviare il servizio del server SANscreen.

    Una volta eseguito Insight, fare clic sull'icona del lucchetto per visualizzare i certificati installati nel sistema.

    Se viene visualizzato un certificato contenente informazioni "emesse a" che corrispondono alle informazioni "emesse da", è ancora installato un certificato autofirmato. I certificati autofirmati generati dal

programma di installazione Insight hanno una scadenza di 100 anni.

NetApp non può garantire che questa procedura rimuoverà gli avvisi dei certificati digitali. NetApp non può controllare la configurazione delle workstation degli utenti finali. Considerare i seguenti scenari:

- Microsoft Internet Explorer e Google Chrome utilizzano la funzionalità di certificazione nativa di Microsoft su Windows.

  Ciò significa che se gli amministratori di Active Directory spingono i certificati CA dell'organizzazione nei trust dei certificati dell'utente finale, gli utenti di questi browser vedranno scomparire gli avvisi dei certificati quando i certificati autofirmati di OnCommand Insight sono stati sostituiti con quelli firmati dall'infrastruttura CA interna.

- Java e Mozilla Firefox dispongono di archivi di certificati personalizzati.

  Se gli amministratori di sistema non automatizzano l'acquisizione dei certificati CA negli archivi di certificati attendibili di queste applicazioni, l'utilizzo del browser Firefox potrebbe continuare a generare avvisi sui certificati a causa di un certificato non attendibile, anche quando il certificato autofirmato è stato sostituito. L'installazione della catena di certificati della tua organizzazione nel trustore è un requisito aggiuntivo.

Configurazione di backup settimanali per il database Insight

È possibile impostare backup settimanali automatici per il database Insight per proteggere i dati. Questi backup automatici sovrascrivono i file nella directory di backup specificata.

A proposito di questa attività

Best practice: Quando si imposta il backup settimanale del database OCI, è necessario memorizzare i backup su un server diverso da quello utilizzato da Insight, in caso di guasto del server. Non memorizzare alcun backup manuale nella directory di backup settimanale perché ogni backup settimanale sovrascrive i file nella directory.

Il file di backup conterrà quanto segue:

- Dati di inventario
- Fino a 7 giorni di dati sulle performance

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** > **Setup**.
2. Fare clic sulla scheda **Backup & Archive**.
3. Nella sezione Weekly Backup (Backup settimanale), selezionare **Enable weekly backup** (attiva backup settimanale).
4. Immettere il percorso per la **posizione di backup**. Può trovarsi sul server Insight locale o su un server remoto accessibile dal server Insight.

L’impostazione della posizione di backup è inclusa nel backup stesso, pertanto se si ripristina il backup su un altro sistema, tenere presente che la posizione della cartella di backup potrebbe non essere valida sul nuovo sistema. Controllare le impostazioni della posizione di backup dopo aver ripristinato un backup.

5. Selezionare l’opzione **Cleanup** per conservare gli ultimi due o gli ultimi cinque backup.
6. Fare clic su **Save** (Salva).

Risultati

Per creare un backup on-demand, accedere a **Admin** > **Troubleshooting**.

Cosa include il backup

È possibile utilizzare backup settimanali e on-demand per la risoluzione dei problemi o la migrazione.

Il backup settimanale o on-demand include quanto segue:

- Dati di inventario
- Dati sulle performance (se selezionati per l’inclusione nel backup)
- Origini dati e impostazioni dell’origine dati
- Pacchetti di integrazione
- Unità di acquisizione remota
- Impostazioni ASUP/proxy
- Impostazioni della posizione di backup
- Impostazioni della posizione di archiviazione
- Impostazioni di notifica
- Utenti
- Policy sulle performance
- Entità aziendali e applicazioni
- Regole e impostazioni di risoluzione del dispositivo
- Dashboard e widget
- Dashboard e widget personalizzati della pagina delle risorse
- Query
- Annotazioni e regole di annotazione

Il backup settimanale non include:

- Impostazioni dello strumento di sicurezza / informazioni sul vault (backup tramite processo CLI separato)
- Log (possono essere salvati su un file .zip su richiesta)
- Dati sulle performance (se non selezionati per l’inclusione nel backup)
- Licenze

Se si sceglie di includere i dati delle performance nel backup, viene eseguito il backup dei dati più recenti per sette giorni. I dati rimanenti saranno presenti nell'archivio, se la funzione è attivata.

Archiviazione dei dati delle performance

OnCommand Insight 7.3 introduce la possibilità di archiviare quotidianamente i dati relativi alle performance. Ciò integra la configurazione e i backup dei dati con performance limitate.

OnCommand Insight conserva fino a 90 giorni di dati relativi a performance e violazioni. Tuttavia, quando si crea un backup di tali dati, nel backup vengono incluse solo le informazioni più recenti. L'archiviazione consente di salvare il resto dei dati relativi alle performance e di caricarli secondo necessità.

Una volta configurata la posizione di archiviazione e attivata l'archiviazione, Insight archivia una volta al giorno i dati delle performance del giorno precedente per tutti gli oggetti nella posizione di archiviazione. Ogni giorno l'archivio viene conservato nella cartella di archiviazione in un file separato. L'archiviazione avviene in background e continuerà fino a quando Insight è in esecuzione.

I 90 giorni più recenti di archivi vengono conservati; i file di archivio più vecchi di 90 giorni vengono cancellati quando vengono creati quelli più recenti.

Abilitazione dell'archiviazione delle performance

Per abilitare l'archiviazione dei dati sulle performance, attenersi alla seguente procedura.

Fasi

1. Sulla barra degli strumenti, fare clic su **Admin** > **Setup**.
2. Selezionare la scheda **Backup & Archive**.
3. Nella sezione Performance Archive (Archivio delle performance), assicurarsi che sia selezionata l'opzione**Enable performance archive** (attiva archivio delle performance).
4. Specificare un percorso di archiviazione valido.

   Non è possibile specificare una cartella nella cartella di installazione di Insight.

   Procedura consigliata: Non specificare la stessa cartella per l'archiviazione della posizione di backup di Insight.

5. Fare clic su **Save** (Salva).

   Il processo di archiviazione viene gestito in background e non interferisce con altre attività Insight.

Caricamento dell'archivio delle performance

Per caricare l'archivio dei dati sulle prestazioni, attenersi alla procedura descritta di seguito.

Prima di iniziare

Prima di caricare l'archivio dei dati sulle prestazioni, è necessario ripristinare un backup settimanale o manuale valido.

Fasi

1. Sulla barra degli strumenti, fare clic su **Admin** > **Troubleshooting**.
2. Nella sezione Restore (Ripristino), in **Load performance archive** (carica archivio prestazioni), fare clic su **Load** (carica).

> Il caricamento dell'archivio viene gestito in background. Il caricamento dell'archivio completo può richiedere molto tempo poiché i dati delle performance archiviati di ogni giorno vengono inseriti in Insight. Lo stato del caricamento dell'archivio viene visualizzato nella sezione archivio di questa pagina.

Configurazione dell'e-mail

Devi configurare OnCommand Insight per accedere al tuo sistema di posta elettronica in modo che il server possa utilizzare la tua email per inviare i report ai quali ti iscrivi e trasferire le informazioni di supporto per la risoluzione dei problemi al supporto tecnico di NetApp.

Prerequisiti per la configurazione della posta elettronica

Prima di poter configurare OnCommand Insight per l'accesso al sistema di posta elettronica, è necessario individuare il nome host o l'indirizzo IP per identificare il server di posta (SMTP o Exchange) e assegnare un account di posta elettronica per i report OnCommand Insight.

Chiedere all'amministratore dell'e-mail di creare un account e-mail per OnCommand Insight. Sono necessarie le seguenti informazioni:

- Il nome host o l'indirizzo IP per identificare il server di posta (SMTP o Exchange) utilizzato dall'organizzazione. Queste informazioni sono disponibili nell'applicazione utilizzata per leggere l'e-mail. In Microsoft Outlook, ad esempio, è possibile trovare il nome del server visualizzando la configurazione dell'account: Strumenti - account di posta elettronica - Visualizza o modifica l'account di posta elettronica esistente.
- Nome dell'account e-mail tramite il quale OnCommand Insight invierà regolarmente i report. L'account deve essere un indirizzo e-mail valido all'interno dell'organizzazione. (La maggior parte dei sistemi di posta non invia messaggi a meno che non vengano inviati da un utente valido). Se il server di posta elettronica richiede un nome utente e una password per inviare la posta, richiedere queste informazioni all'amministratore di sistema.

Configurazione dell'e-mail per Insight

Se gli utenti desiderano ricevere i report Insight nei propri account di posta elettronica, è necessario configurare il server di posta elettronica per attivare questa funzione.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Notifications**.
2. Scorrere verso il basso fino alla sezione **Email** della pagina.
3. Nella casella **Server**, immettere il nome del server SMTP dell'organizzazione, identificato utilizzando un nome host o un indirizzo IP (formato_nnn.nnn.nnn.nnn.nnn_).

   Se si specifica un nome host, assicurarsi che il nome possa essere risolto tramite DNS.
4. Nella casella **Nome utente**, immettere il proprio nome utente.
5. Nella casella **Password**, immettere la password per accedere al server di posta elettronica, necessaria solo se il server SMTP è protetto da password. Si tratta della stessa password utilizzata per accedere all'applicazione che consente di leggere l'e-mail. Se è richiesta una password, è necessario immetterla una seconda volta per la verifica.
6. Nella casella **e-mail mittente**, immettere l'account e-mail del mittente che verrà identificato come mittente in tutti i report OnCommand Insight.

   Questo account deve essere un account e-mail valido all'interno dell'organizzazione.
7. Nella casella **Firma email**, immettere il testo che si desidera inserire in ogni messaggio inviato.
8. Nella casella destinatari, fare clic su ✚, Inserire un indirizzo e-mail e fare clic su **OK**.

   Per modificare un indirizzo e-mail, selezionarlo e fare clic su . Per eliminare un indirizzo e-mail, selezionarlo e fare clic su ✖.
9. Per inviare un messaggio di posta elettronica di prova a destinatari specifici, fare clic su ✔.
10. Fare clic su **Save** (Salva).

Configurazione delle notifiche SNMP

OnCommand Insight supporta le notifiche SNMP per le modifiche alla configurazione e ai criteri di percorso globale, nonché per le violazioni. Ad esempio, le notifiche SNMP vengono inviate quando vengono superate le soglie dell'origine dati.

Prima di iniziare

È necessario completare le seguenti operazioni:

- Identificazione dell'indirizzo IP del server che consolida i trap per ciascun tipo di evento.

  Potrebbe essere necessario consultare l'amministratore di sistema per ottenere queste informazioni.
- Identificazione del numero di porta attraverso il quale il computer designato ottiene i trap SNMP per ciascun tipo di evento.

  La porta predefinita per i trap SNMP è 162.
- Compilazione del MIB presso il sito.

  Il MIB proprietario viene fornito con il software di installazione per supportare le trap OnCommand Insight. NetApp MIB è compatibile con tutti i software di gestione SNMP standard ed è disponibile sul server Insight

in `<install dir>\SANscreen\MIBS\sanscreen.mib`.

Fasi

1. Fare clic su **Admin** e selezionare **Notifications**.
2. Scorrere verso il basso fino alla sezione **SNMP** della pagina.
3. Fare clic su **azioni** e selezionare **Aggiungi origine trap**.
4. Nella finestra di dialogo **Aggiungi destinatari trap SNMP**, immettere i seguenti valori:
   - **IP**

     L'indirizzo IP a cui OnCommand Insight invia i messaggi trap SNMP.

   - **Porta**

     Il numero di porta a cui OnCommand Insight invia i messaggi trap SNMP.

   - **Stringa di comunità**

     Utilizzare "public" per i messaggi trap SNMP.
5. Fare clic su **Save** (Salva).

Attivazione della funzione syslog

È possibile identificare una posizione per il registro delle violazioni OnCommand Insight e degli avvisi sulle prestazioni, nonché i messaggi di controllo e attivare il processo di registrazione.

Prima di iniziare

- È necessario disporre dell'indirizzo IP del server su cui memorizzare il log di sistema.
- È necessario conoscere il livello di struttura che corrisponde al tipo di programma che registra il messaggio, ad esempio LOCAL1 o USER.

A proposito di questa attività

Il syslog include i seguenti tipi di informazioni:

- Messaggi di violazione
- Avvisi sulle prestazioni
- Facoltativamente, i messaggi del registro di controllo

Nel syslog vengono utilizzate le seguenti unità:

- Metriche di utilizzo: Percentuale
- Metriche di traffico: MB
- Velocità di traffico: MB/s.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Notifications**.
2. Scorrere verso il basso fino alla sezione **Syslog** della pagina.
3. Selezionare la casella di controllo **Enable syslog** (attiva syslog).
4. Se si desidera, selezionare la casella di controllo **Invia audit**. I nuovi messaggi del registro di controllo verranno inviati a syslog oltre a essere visualizzati nella pagina Audit. Si noti che i messaggi del registro di controllo già esistenti non verranno inviati a syslog; verranno inviati solo i messaggi di registro generati di recente.
5. Nel campo **Server**, immettere l'indirizzo IP del server di log.

   È possibile specificare una porta personalizzata aggiungendo i due punti alla fine dell'IP del server (ad esempio server:porta). Se la porta non è specificata, viene utilizzata la porta syslog predefinita 514.
6. Nel campo **Facility**, selezionare il livello di struttura corrispondente al tipo di programma che sta registrando il messaggio.
7. Fare clic su **Save** (Salva).

Contenuti di Insight syslog

È possibile abilitare un syslog su un server per raccogliere messaggi di avviso relativi alle violazioni Insight e alle performance che includono dati di utilizzo e traffico.

Tipi di messaggio

Insight syslog elenca tre tipi di messaggi:

- Violazioni del percorso SAN
- Violazioni generali
- Avvisi sulle prestazioni

Dati forniti

Le descrizioni delle violazioni includono gli elementi coinvolti, l'ora dell'evento e la relativa severità o priorità della violazione.

Gli avvisi relativi alle performance includono i seguenti dati:

- Percentuali di utilizzo
- Tipi di traffico
- Velocità di traffico misurata in MB

Configurazione delle performance e garanzia delle notifiche di violazione

OnCommand Insight supporta le notifiche per le performance e garantisce le violazioni. Per impostazione predefinita, Insight non invia notifiche per queste violazioni; è necessario configurare Insight per inviare e-mail, messaggi syslog al server syslog o per

inviare notifiche SNMP in caso di violazione.

Prima di iniziare

È necessario aver configurato i metodi di invio di email, syslog e SNMP per le violazioni.

Fasi

1. Fare clic su **Admin** > **Notifications**.
2. Fare clic su **Eventi**.
3. Nella sezione **Performance Inviaces events** o **Inrassicurare Violaves events**, fare clic sull'elenco del metodo di notifica (**Email**, **Syslog** o **SNMP**) desiderato e selezionare il livello di severità (**Warning and above** or **critical**) per la violazione.
4. Fare clic su **Save** (Salva).

Configurazione delle notifiche degli eventi a livello di sistema

OnCommand Insight supporta le notifiche per eventi a livello di sistema, come guasti delle unità di acquisizione o errori delle origini dati. Per ricevere le notifiche, è necessario configurare Insight in modo che invii e-mail quando si verifica uno o più di questi eventi.

Prima di iniziare

È necessario aver configurato i destinatari e-mail per ricevere le notifiche in **Admin** > **Notifiche** > **metodi di invio**.

Fasi

1. Fare clic su **Admin** > **Notifications**.
2. Fare clic su **Eventi**.
3. Nella sezione **Eventi avviso di sistema** e-mail, selezionare il livello di gravità (**Avviso e superiore** o **critico**) per la notifica oppure scegliere **non inviare** se non si desidera ricevere notifiche di eventi a livello di sistema.
4. Fare clic su **Save** (Salva).
5. Fare clic su **Admin** > **System Alerts** per configurare gli avvisi.
6. Per aggiungere un nuovo avviso, fare clic su **+Aggiungi** e assegnare all'avviso un **Nome** univoco. È inoltre possibile fare clic sull'icona a destra per **modificare** un avviso esistente.
7. Scegliere il **tipo di evento** su cui avvisare, ad esempio *Acquisition Unit Failure*.
8. Scegliere un intervallo **Snooze** per eliminare le notifiche sugli eventi duplicati del tipo selezionato per l'intervallo di tempo selezionato. Se si seleziona *mai*, si riceveranno notifiche ripetute una volta al minuto fino a quando l'evento non si verifica più.
9. Scegliere **severità** (Avviso o critico) per la notifica dell'evento.
10. Per impostazione predefinita, le notifiche e-mail verranno inviate all'elenco globale dei destinatari di posta elettronica oppure è possibile fare clic sul collegamento fornito per ignorare l'elenco globale e inviare notifiche a destinatari specifici.

11. Fare clic su Save (Salva) per aggiungere l'avviso.

Configurazione dell'elaborazione ASUP

Tutti i prodotti NetApp sono dotati di funzionalità automatizzate per fornire il miglior supporto possibile ai clienti. Il supporto automatizzato (ASUP) invia periodicamente informazioni specifiche e predefinite al supporto clienti. È possibile controllare le informazioni da inoltrare a NetApp e la frequenza con cui vengono inviate.

Prima di iniziare

È necessario configurare OnCommand Insight per l'inoltro dei dati prima di inviarli.

A proposito di questa attività

I dati ASUP vengono inoltrati utilizzando il protocollo HTTPS.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Setup**.
3. Fare clic sulla scheda **ASUP & Proxy**.
4. Nella sezione **ASUP**, selezionare **Enable ASUP** (attiva ASUP) per attivare la funzione ASUP.
5. Se si desidera modificare le informazioni aziendali, aggiornare i seguenti campi:
   - **Nome dell'azienda**
   - **Nome del sito**
   - **Cosa inviare**: Log, dati di configurazione, dati sulle performance
6. Fare clic su **Test Connection** (verifica connessione) per verificare che la connessione specificata funzioni.
7. Fare clic su **Save** (Salva).
8. Nella sezione **Proxy**, scegliere se attivare **Proxy** e specificare le informazioni relative al proxy **host**, **porta** e **utente**.
9. Fare clic su **Test Connection** (verifica connessione) per verificare che il proxy specificato funzioni.
10. Fare clic su **Save** (Salva).

Contenuto del pacchetto ASUP (AutoSupport)

Il pacchetto AutoSupport contiene il backup del database e informazioni estese.

Il pacchetto AutoSupport include quanto segue:

- Dati di inventario
- Dati sulle performance (se selezionati per l'inclusione in ASUP)
- Origini dati e impostazioni dell'origine dati
- Pacchetti di integrazione

- Unità di acquisizione remota
- Impostazioni ASUP/proxy
- Impostazioni della posizione di backup
- Impostazioni della posizione di archiviazione
- Impostazioni di notifica
- Utenti
- Policy sulle performance
- Entità aziendali e applicazioni
- Regole e impostazioni di risoluzione del dispositivo
- Dashboard e widget
- Dashboard e widget personalizzati della pagina delle risorse
- Query
- Annotazioni e regole di annotazione
- Registri
- Licenze
- Stato di acquisizione/origine dei dati
- Stato di MySQL
- Informazioni di sistema

Il pacchetto AutoSupport non include:

- Impostazioni dello strumento di sicurezza / informazioni sul vault (backup tramite processo CLI separato)
- Dati sulle performance (se non selezionati per l'inclusione in ASUP)

Se si sceglie di includere i dati delle performance nell'ASUP, vengono inclusi i sette giorni più recenti di dati. I dati rimanenti saranno presenti nell'archivio, se la funzione è attivata. I dati di archivio non sono inclusi in ASUP.

Definizione delle applicazioni

Se si desidera tenere traccia dei dati associati a applicazioni specifiche in esecuzione nell'ambiente, è necessario definire tali applicazioni.

Prima di iniziare

Se si desidera associare l'applicazione a un'entità aziendale, è necessario che l'entità aziendale sia già stata creata.

A proposito di questa attività

È possibile associare le applicazioni alle seguenti risorse: Host, macchine virtuali, volumi, volumi interni, qtree, condivisioni e hypervisor.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Manage** (Gestisci) e selezionare **Applications** (applicazioni).

   Dopo aver definito un'applicazione, la pagina applicazioni visualizza il nome dell'applicazione, la relativa priorità e, se applicabile, l'entità aziendale associata all'applicazione.

3. Fare clic su **Aggiungi**.

   Viene visualizzata la finestra di dialogo Add Application (Aggiungi applicazione).

4. Inserire un nome univoco per l'applicazione nella casella **Nome**.
5. Fare clic su **priorità** e selezionare la priorità (critica, alta, media o bassa) per l'applicazione nell'ambiente in uso.
6. Se si intende utilizzare questa applicazione con un'entità commerciale, fare clic su **entità commerciale** e selezionare l'entità dall'elenco.
7. **Opzionale**: Se non si utilizza la condivisione del volume, deselezionare la casella **convalida condivisione volume**.

   Ciò richiede la licenza di assicurazione. Impostare questa opzione quando si desidera garantire che ciascun host abbia accesso agli stessi volumi in un cluster. Ad esempio, gli host dei cluster ad alta disponibilità spesso devono essere mascherati sugli stessi volumi per consentire il failover; tuttavia, gli host delle applicazioni non correlate non hanno solitamente la necessità di accedere agli stessi volumi fisici. Inoltre, le policy normative potrebbero richiedere l'esplicitamente di impedire alle applicazioni non correlate di accedere agli stessi volumi fisici per motivi di sicurezza.

8. Fare clic su **Save** (Salva).

   L'applicazione viene visualizzata nella pagina applicazioni. Facendo clic sul nome dell'applicazione, Insight visualizza la pagina delle risorse dell'applicazione.

Al termine

Dopo aver definito un'applicazione, è possibile accedere a una pagina di risorse per host, macchina virtuale, volume, volume interno o hypervisor per assegnare un'applicazione a una risorsa.

Assegnazione di applicazioni alle risorse

Dopo aver definito le applicazioni con o senza entità di business, è possibile associarle alle risorse.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare la risorsa (host, macchina virtuale, volume o volume interno) a cui si desidera applicare l'applicazione effettuando una delle seguenti operazioni:
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse** e fare clic sulla risorsa.
   - Fare clic su Nella barra degli strumenti per visualizzare la casella **Cerca risorse**, digitare il nome della risorsa, quindi selezionarla dall'elenco.

3. Nella sezione **dati utente** della pagina risorse, posizionare il cursore sul nome dell'applicazione attualmente assegnata alla risorsa (se non è stata assegnata alcuna applicazione, viene visualizzato **Nessuno**), quindi fare clic su (Modifica applicazione).

   Viene visualizzato l'elenco delle applicazioni disponibili per la risorsa selezionata. Le applicazioni attualmente associate alla risorsa sono precedute da un segno di spunta.

4. È possibile digitare nella casella Cerca per filtrare i nomi delle applicazioni oppure scorrere l'elenco.
5. Selezionare le applicazioni che si desidera associare alla risorsa.

   È possibile assegnare più applicazioni all'host, alla macchina virtuale e al volume interno; tuttavia, è possibile assegnare una sola applicazione al volume.

6. Fare clic su per assegnare l'applicazione o le applicazioni selezionate alla risorsa.

   I nomi delle applicazioni vengono visualizzati nella sezione User Data (dati utente); se l'applicazione è associata a un'entità aziendale, anche il nome dell'entità aziendale viene visualizzato in questa sezione.

Applicazioni di editing

È possibile modificare la priorità di un'applicazione, l'entità aziendale associata a un'applicazione o lo stato della condivisione del volume.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Manage** (Gestisci) e selezionare **Applications** (applicazioni).
3. Posizionare il cursore sull'applicazione che si desidera modificare e fare clic su .

   Viene visualizzata la finestra di dialogo Edit Application (Modifica applicazione).

4. Effettuare una delle seguenti operazioni:
   - Fare clic su **priorità** e selezionare una priorità diversa.

     Non è possibile modificare il nome dell'applicazione.

   - Fare clic su **entità aziendale** e selezionare un'entità aziendale diversa a cui associare l'applicazione o selezionare **Nessuno** per rimuovere l'associazione dell'applicazione all'entità aziendale.
   - Fare clic per deselezionare o selezionare **Validate volume sharing** (convalida condivisione volume).

     Questa opzione è disponibile solo se si dispone della licenza di assicurazione.

5. Fare clic su **Save** (Salva).

Eliminazione delle applicazioni

È possibile eliminare un'applicazione quando non soddisfa più le esigenze dell'ambiente.

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Manage** (Gestisci) e selezionare **Applications** (applicazioni).
3. Posizionare il cursore sull'applicazione che si desidera eliminare e fare clic su .

   Viene visualizzata una finestra di dialogo di conferma che chiede se si desidera eliminare l'applicazione.

4. Fare clic su **OK**.

Gerarchia delle entità di business

È possibile definire entità di business per tenere traccia e generare report sui dati dell'ambiente a un livello più granulare.

In OnCommand Insight, la gerarchia delle entità di business contiene i seguenti livelli:

- **Il tenant** viene utilizzato principalmente dai service provider per associare le risorse a un cliente, ad esempio NetApp.
- **Line of Business (LOB)** è una linea di business o di prodotto all'interno di un'azienda, ad esempio lo storage dei dati.
- **Business Unit** rappresenta una business unit tradizionale, ad esempio legale o marketing.
- **Project** viene spesso utilizzato per identificare un progetto specifico all'interno di una business unit per cui si desidera un chargeback della capacità. Ad esempio, "brevetti" potrebbe essere un nome di progetto per l'unità aziendale legale e "Eventi commerciali" potrebbe essere un nome di progetto per l'unità aziendale di marketing. I nomi dei livelli possono includere spazi.

Non è necessario utilizzare tutti i livelli nella progettazione della gerarchia aziendale.

Progettazione della gerarchia delle entità di business

È necessario comprendere gli elementi della struttura aziendale e i componenti da rappresentare nelle entità aziendali perché diventano una struttura fissa nel database OnCommand Insight. È possibile utilizzare le seguenti informazioni per configurare le entità aziendali. Non è necessario utilizzare tutti i livelli di gerarchia per raccogliere i dati in queste categorie.

Fasi

1. Esaminare ciascun livello della gerarchia delle entità di business per determinare se tale livello deve essere incluso nella gerarchia delle entità di business della propria azienda:
   - Il livello **tenant** è necessario se la tua azienda è un ISP e vuoi monitorare l'utilizzo delle risorse da parte dei clienti.
   - **La linea di business (LOB)** è necessaria nella gerarchia se è necessario tenere traccia dei dati delle diverse linee di prodotti.
   - **Business Unit** è necessaria per tenere traccia dei dati di diversi reparti. Questo livello della gerarchia è spesso utile per separare una risorsa che un reparto utilizza, ma non gli altri reparti.
   - Il livello **Project** può essere utilizzato per lavori specializzati all'interno di un reparto. Questi dati

potrebbero essere utili per individuare, definire e monitorare le esigenze tecnologiche di un progetto separato rispetto ad altri progetti di un'azienda o di un reparto.

2. Creare un grafico che mostri ogni entità aziendale con i nomi di tutti i livelli all'interno dell'entità.
3. Controllare i nomi nella gerarchia per assicurarsi che siano intuitivi nelle visualizzazioni e nei report di OnCommand Insight.
4. Identificare tutte le applicazioni associate a ciascuna entità aziendale.

Creazione di entità di business

Dopo aver progettato la gerarchia delle entità di business per la tua azienda, puoi impostare le applicazioni e associare le entità di business alle applicazioni. Questo processo crea la struttura delle entità di business nel database OnCommand Insight.

A proposito di questa attività

L'associazione delle applicazioni alle entità aziendali è facoltativa; tuttavia, si tratta di una procedura consigliata.

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Manage** (Gestisci) e selezionare **Business Entities** (entità aziendali).

   Viene visualizzata la pagina entità di business.
3. Fare clic su + Add per iniziare a costruire una nuova entità.

   Viene visualizzata la finestra di dialogo **Aggiungi entità aziendale**.
4. Per ogni livello di entità (tenant, line of business, business unit e progetto), è possibile eseguire una delle seguenti operazioni:
   - Fare clic sull'elenco a livello di entità e selezionare un valore.
   - Digitare un nuovo valore e premere Invio.
   - Lasciare il valore del livello di entità come N/A se non si desidera utilizzare il livello di entità per l'entità aziendale.
5. Fare clic su **Save** (Salva).

Assegnazione di entità aziendali alle risorse

È possibile assegnare un'entità aziendale a una risorsa (host, porta, storage, switch, macchina virtuale, qtree, share, volume o volume interno) senza aver associato l'entità aziendale a un'applicazione; tuttavia, le entità aziendali vengono assegnate automaticamente a un asset se tale risorsa è associata a un'applicazione correlata a un'entità aziendale.

Prima di iniziare

È necessario aver già creato un'entità aziendale.

A proposito di questa attività

Sebbene sia possibile assegnare le entità aziendali direttamente alle risorse, si consiglia di assegnare le applicazioni alle risorse e quindi assegnare le entità aziendali alle risorse.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare la risorsa a cui si desidera applicare l'entità aziendale effettuando una delle seguenti operazioni:
   - Fare clic sulla risorsa nella dashboard delle risorse.
   - Fare clic su Nella barra degli strumenti per visualizzare la casella **Cerca risorse**, digitare il nome della risorsa, quindi selezionarla dall'elenco.
3. Nella sezione **dati utente** della pagina delle risorse, posizionare il cursore su **Nessuno** accanto a **entità aziendali** e fare clic su .

   Viene visualizzato l'elenco delle entità di business disponibili.

4. Digitare la casella **Search** per filtrare l'elenco per un'entità specifica o scorrere l'elenco verso il basso; selezionare un'entità aziendale dall'elenco.

   Se l'entità aziendale scelta è associata a un'applicazione, viene visualizzato il nome dell'applicazione. In questo caso, la parola "derived" viene visualizzata accanto al nome dell'entità aziendale. Se si desidera mantenere l'entità solo per la risorsa e non per l'applicazione associata, è possibile eseguire manualmente l'override dell'assegnazione dell'applicazione.

5. Per eseguire l'override di un'applicazione derivata da un'entità aziendale, posizionare il cursore sul nome dell'applicazione e fare clic su , selezionare un'altra entità aziendale e selezionare un'altra applicazione dall'elenco.

Assegnazione o rimozione di entità aziendali da più risorse

È possibile assegnare o rimuovere entità aziendali da più risorse utilizzando una query invece di dover assegnarle o rimuoverle manualmente.

Prima di iniziare

È necessario aver già creato le entità aziendali da aggiungere alle risorse desiderate.

Fasi

1. Creare una nuova query o aprire una query esistente.
2. Se lo si desidera, filtrare le risorse a cui si desidera aggiungere entità aziendali.
3. Selezionare le risorse desiderate nell'elenco o fare clic su Per selezionare **tutto**.

   Viene visualizzato il pulsante **azioni**.

4. Per aggiungere un'entità aziendale alle risorse selezionate, fare clic su Actions. Se al tipo di risorsa selezionato possono essere assegnate entità aziendali, viene visualizzata la voce di menu **Add Business Entity** (Aggiungi entità aziendale). Selezionare questa opzione.

5. Selezionare l'entità aziendale desiderata dall'elenco e fare clic su **Save** (Salva).

   Qualsiasi nuova entità aziendale assegnata ha la priorità su tutte le entità aziendali già assegnate alla risorsa. L'assegnazione delle applicazioni alle risorse sovrascriverà anche le entità aziendali assegnate nello stesso modo. L'assegnazione di entità aziendali a come risorsa può anche sovrascrivere qualsiasi applicazione assegnata a tale risorsa.

6. Per rimuovere un'entità aziendale assegnata alle risorse, fare clic su 

E selezionare **Remove Business Entity**.
7. Selezionare l'entità aziendale desiderata dall'elenco e fare clic su **Delete** (Elimina).

Definizione delle annotazioni

Quando si personalizza OnCommand Insight per tenere traccia dei dati in base ai requisiti aziendali, è possibile definire eventuali annotazioni specializzate necessarie per fornire un quadro completo dei dati: Ad esempio, fine del ciclo di vita delle risorse, data center, ubicazione dell'edificio, Tier di storage o volume, e livello di servizio del volume interno.

Fasi

1. Elencare qualsiasi terminologia del settore a cui devono essere associati i dati dell'ambiente.
2. Elencare la terminologia aziendale a cui devono essere associati i dati dell'ambiente, che non sono già stati monitorati utilizzando le entità aziendali.
3. Identificare i tipi di annotazione predefiniti che potrebbero essere utilizzabili.
4. Identificare le annotazioni personalizzate da creare.

Utilizzo delle annotazioni per monitorare l'ambiente

Quando si personalizza OnCommand Insight per tenere traccia dei dati in base ai requisiti aziendali, è possibile definire note specializzate, denominate *annotazioni*, e assegnarle alle risorse. Ad esempio, è possibile annotare le risorse con informazioni come fine del ciclo di vita delle risorse, data center, posizione dell'edificio, Tier di storage o livello di servizio del volume.

L'utilizzo delle annotazioni per il monitoraggio dell'ambiente include le seguenti attività di alto livello:

- Creazione o modifica delle definizioni per tutti i tipi di annotazione.
- Visualizzazione delle pagine delle risorse e associazione di ciascuna risorsa a una o più annotazioni.

  Ad esempio, se una risorsa viene affittata e il leasing scade entro due mesi, potrebbe essere necessario applicare un'annotazione di fine ciclo di vita alla risorsa. In questo modo si impedisce ad altri di utilizzare tale risorsa per un periodo di tempo prolungato.

- Creazione di regole per applicare automaticamente le annotazioni a più risorse dello stesso tipo.
- Utilizzo dell'utility di importazione delle annotazioni per importare le annotazioni.
- Filtrare le risorse in base alle annotazioni.

- Raggruppare i dati nei report in base alle annotazioni e generare tali report.

  Per ulteriori informazioni sui report, consulta la *Guida ai report di OnCommand Insight*.

Gestione dei tipi di annotazione

OnCommand Insight fornisce alcuni tipi di annotazione predefiniti, come il ciclo di vita delle risorse (compleanno o fine del ciclo di vita), la posizione dell'edificio o del data center e il Tier, che è possibile personalizzare per visualizzare nei report. È possibile definire i valori per i tipi di annotazione predefiniti o creare tipi di annotazione personalizzati. È possibile modificare questi valori in un secondo momento.

Tipi di annotazione predefiniti

OnCommandInsight offre alcuni tipi di annotazione predefiniti. Queste annotazioni possono essere utilizzate per filtrare o raggruppare i dati e per filtrare i report dei dati.

È possibile associare le risorse ai tipi di annotazione predefiniti, ad esempio:

- Ciclo di vita delle risorse, ad esempio compleanno, tramonto o fine vita
- Informazioni sulla posizione di un dispositivo, ad esempio data center, edificio o piano
- Classificazione delle risorse, ad esempio per qualità (Tier), per dispositivi connessi (livello di switch) o per livello di servizio
- Stato, ad esempio hot (utilizzo elevato)

La tabella seguente elenca i tipi di annotazione predefiniti. È possibile modificare i nomi delle annotazioni in base alle proprie esigenze.

Tipi di annotazione	Descrizione	Tipo
Alias	Nome intuitivo per una risorsa.	Testo
Compleanno	Data in cui il dispositivo è stato o sarà portato online.	Data
Edificio	Posizione fisica delle risorse di host, storage, switch e nastro.	Elenco
Città	Posizione in comune di host, storage, switch e risorse su nastro.	Elenco
Gruppo di risorse di calcolo	Assegnazione del gruppo utilizzata dall'origine dati dei filesystem host e VM.	Elenco
Continente	Posizione geografica delle risorse di host, storage, switch e nastro.	Elenco

Paese	Posizione nazionale di host, storage, switch e risorse su nastro.	Elenco
Data center	Posizione fisica della risorsa ed è disponibile per host, storage array, switch e nastri.	Elenco
Collegamento diretto	Indica (Sì o No) se una risorsa di storage è connessa direttamente agli host.	Booleano
Fine del ciclo di vita	Data in cui un dispositivo verrà portato offline, ad esempio, se il leasing è scaduto o l'hardware viene ritirato.	Data
Alias fabric	Nome intuitivo per un fabric.	Testo
Piano	Posizione di un dispositivo su un piano di un edificio. Può essere impostato per host, storage array, switch e nastri.	Elenco
Caldo	Dispositivi già in uso su base regolare o alla soglia di capacità.	Booleano
Nota	Commenti che si desidera associare a una risorsa.	Testo
Rack	Rack in cui risiede la risorsa.	Testo
Camera	Spazio all'interno di un edificio o di un'altra ubicazione di risorse host, storage, switch e nastro.	Elenco
SAN	Partizione logica della rete. Disponibile su host, storage array, nastri, switch e applicazioni.	Elenco
Livello di servizio	Un insieme di livelli di servizio supportati che è possibile assegnare alle risorse. Fornisce un elenco di opzioni ordinate per volumi interni, qtree e volumi. Modificare i livelli di servizio per impostare le policy di performance per diversi livelli.	Elenco

Stato/Provincia	Stato o provincia in cui si trova la risorsa.	Elenco
Tramonto	Soglia impostata dopo la quale non è possibile assegnare nuove allocazioni a quel dispositivo. Utile per migrazioni pianificate e altre modifiche di rete in sospeso.	Data
Livello switch	Include opzioni predefinite per l'impostazione delle categorie per gli switch. In genere, queste designazioni rimangono valide per la durata del dispositivo, anche se è possibile modificarle, se necessario. Disponibile solo per gli switch.	Elenco
Tier	Può essere utilizzato per definire diversi livelli di servizio all'interno del proprio ambiente. I Tier possono definire il tipo di livello, ad esempio la velocità necessaria (ad esempio, oro o argento). Questa funzione è disponibile solo su volumi interni, qtree, storage array, storage pool e volumi.	Elenco
Severità della violazione	Classificazione (ad esempio, maggiore) di una violazione (ad esempio, porte host mancanti o ridondanza mancante), in una gerarchia di importanza da massima a minima.	Elenco

Alias, data center, hot, livello di servizio, Sunset, Livello switch, livello di servizio, livello e severità delle violazioni sono annotazioni a livello di sistema che non è possibile eliminare o rinominare; è possibile modificare solo i valori assegnati.

Modalità di assegnazione delle annotazioni

È possibile assegnare le annotazioni manualmente o automaticamente utilizzando le regole di annotazione. OnCommand Insight assegna inoltre automaticamente alcune annotazioni all'acquisizione delle risorse e in base all'ereditarietà. Le annotazioni assegnate a una risorsa vengono visualizzate nella sezione User Data (dati utente) della pagina delle risorse.

Le annotazioni vengono assegnate nei seguenti modi:

- È possibile assegnare manualmente un'annotazione a una risorsa.

Se un'annotazione viene assegnata direttamente a una risorsa, l'annotazione viene visualizzata come testo normale su una pagina risorsa. Le annotazioni assegnate manualmente hanno sempre la precedenza sulle annotazioni ereditate o assegnate dalle regole di annotazione.

- È possibile creare una regola di annotazione per assegnare automaticamente le annotazioni alle risorse dello stesso tipo.

  Se l'annotazione viene assegnata in base alla regola, Insight visualizza il nome della regola accanto al nome dell'annotazione in una pagina asset.

- Insight associa automaticamente un livello di Tier a un modello di Tier storage per accelerare l'assegnazione delle annotazioni di storage alle risorse al momento dell'acquisizione delle risorse.

  Alcune risorse di storage vengono automaticamente associate a un Tier predefinito (Tier 1 e Tier 2). Ad esempio, il Tier di storage Symmetrix si basa sulla famiglia Symmetrix e VMAX ed è associato al Tier 1. È possibile modificare i valori predefiniti in base ai requisiti del livello. Se l'annotazione è assegnata da Insight (ad esempio, Tier), viene visualizzato "System-defined `S`" quando si posiziona il cursore sul nome dell'annotazione in una pagina di risorse.

- Alcune risorse (figli di una risorsa) possono derivare l'annotazione Tier predefinita dalla risorsa (principale).

  Ad esempio, se si assegna un'annotazione a uno storage, l'annotazione Tier viene derivata da tutti i pool di storage, volumi interni, volumi, qtree e condivisioni appartenenti allo storage. Se viene applicata un'annotazione diversa a un volume interno dello storage, l'annotazione viene successivamente derivata da tutti i volumi, qtree e condivisioni. "derived" viene visualizzato accanto al nome dell'annotazione in una pagina di risorse.

Associare i costi alle annotazioni

Prima di eseguire i report relativi ai costi, è necessario associare i costi alle annotazioni a livello di sistema livello di servizio, livello switch e livello, che consentono agli utenti dello storage di addebitarsi i costi in base all'effettivo utilizzo della produzione e della capacità replicata. Ad esempio, per il livello Tier, è possibile avere valori di livello Gold e Silver e assegnare un costo più elevato al livello Gold rispetto al livello Silver.

Fasi

1. Accedere all'interfaccia utente di Insightweb.
2. Fare clic su Gestisci e selezionare **Annotazioni**.

   Viene visualizzata la pagina Annotation (Annotazione).

3. Posizionare il cursore sull'annotazione Service Level (livello di servizio), Switch Level (livello switch) o Tier (livello Tier) e fare clic su .

   Viene visualizzata la finestra di dialogo Edit Annotation (Modifica annotazione).

4. Inserire i valori per i livelli esistenti nel campo **costo**.

   Le annotazioni Tier e Service Level presentano valori di Auto Tier e Object Storage, rispettivamente, che non è possibile rimuovere.

5.

Fare clic su  per aggiungere altri livelli.

6. Al termine, fare clic su **Save** (Salva).

Creazione di annotazioni personalizzate

Utilizzando le annotazioni, è possibile aggiungere dati personalizzati specifici del business che corrispondano alle esigenze del business alle risorse. Sebbene OnCommand Insight fornisca una serie di annotazioni predefinite, è possibile che si desideri visualizzare i dati in altri modi. I dati contenuti nelle annotazioni personalizzate integrano i dati dei dispositivi già raccolti, ad esempio il produttore dello switch, il numero di porte e le statistiche sulle prestazioni. I dati aggiunti utilizzando le annotazioni non vengono rilevati da Insight.

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** e selezionare **Annotazioni**.

   La pagina Annotazioni visualizza l'elenco delle annotazioni.

3. Fare clic su  .

   Viene visualizzata la finestra di dialogo **Add Annotation** (Aggiungi annotazione).

4. Immettere un nome e una descrizione nei campi **Nome** e **Descrizione**.

   È possibile inserire fino a 255 caratteri in questi campi.

   I nomi delle annotazioni che iniziano o terminano con un punto "." non sono supportati.

5. Fare clic su **Type** (tipo), quindi selezionare una delle seguenti opzioni che rappresentano il tipo di dati consentiti in questa annotazione:

   - Booleano

     In questo modo viene creato un elenco a discesa con le opzioni Sì e No Ad esempio, l'annotazione "Dirett attached" è booleana.

   - Data

     In questo modo viene creato un campo che contiene una data. Ad esempio, se l'annotazione sarà una data, selezionare questa opzione.

   - Elenco

     In questo modo è possibile creare una delle seguenti opzioni:

     - Un elenco a discesa fisso

       Quando altri utenti assegnano questo tipo di annotazione su un dispositivo, non possono aggiungere altri valori all'elenco.

- Un elenco a discesa flessibile

  Se si seleziona l'opzione **Aggiungi nuovi valori al volo** quando si crea questo elenco, altri utenti assegnano questo tipo di annotazione su un dispositivo possono aggiungere altri valori all'elenco.

◦ Numero

In questo modo si crea un campo in cui l'utente che assegna l'annotazione può inserire un numero. Ad esempio, se il tipo di annotazione è "Floor", l'utente può selezionare il tipo di valore "number" e inserire il numero di piano.

◦ Testo

In questo modo viene creato un campo che consente il testo in formato libero. Ad esempio, è possibile immettere "Language" come tipo di annotazione, selezionare "Text" come tipo di valore e immettere una lingua come valore.

> Dopo aver impostato il tipo e salvato le modifiche, non è possibile modificare il tipo di annotazione. Se è necessario modificare il tipo, eliminare l'annotazione e crearne una nuova.

6. Se si seleziona **Elenca**come tipo di annotazione, procedere come segue:
   a. Selezionare **Add new values on the fly** (Aggiungi nuovi valori in tempo reale) se si desidera aggiungere altri valori all'annotazione quando ci si trova in una pagina di risorse, che crea un elenco flessibile.

      Si supponga, ad esempio, di trovarsi in una pagina di risorse e di avere l'annotazione City (Città) con i valori Detroit, Tampa e Boston. Se è stata selezionata l'opzione **Aggiungi nuovi valori al volo**, è possibile aggiungere valori aggiuntivi a Città come San Francisco e Chicago direttamente nella pagina delle risorse, invece di andare alla pagina Annotazioni per aggiungerli. Se non si sceglie questa opzione, non è possibile aggiungere nuovi valori di annotazione quando si applica l'annotazione; in questo modo si crea un elenco fisso.

   b. Immettere un valore e un nome nei campi **valore** e **Descrizione**.
   c. Fare clic su 

per aggiungere altri valori.
   d. Fare clic su per rimuovere un valore.
7. Fare clic su **Save** (Salva).

Le annotazioni vengono visualizzate nell'elenco della pagina Annotazioni.

Informazioni correlate

"Importazione ed esportazione dei dati utente"

Assegnazione manuale delle annotazioni alle risorse

L'assegnazione di annotazioni alle risorse consente di ordinare, raggruppare e creare report sulle risorse in modi rilevanti per la tua azienda. Sebbene sia possibile assegnare automaticamente annotazioni a risorse di un tipo particolare, utilizzando le regole di annotazione, è possibile assegnare annotazioni a una singola risorsa utilizzando la

relativa pagina delle risorse.

Prima di iniziare

È necessario aver creato l'annotazione che si desidera assegnare.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare la risorsa a cui si desidera applicare l'annotazione effettuando una delle seguenti operazioni:
   - Fare clic sulla risorsa nella dashboard delle risorse.
   - Fare clic su Nella barra degli strumenti per visualizzare la casella **Cerca risorse**, digitare il tipo o il nome della risorsa, quindi selezionare la risorsa dall'elenco visualizzato.

     Viene visualizzata la pagina delle risorse.
3. Nella sezione **dati utente** della pagina delle risorse, fare clic su + Add.

   Viene visualizzata la finestra di dialogo Add Annotation (Aggiungi annotazione).
4. Fare clic su **Annotation** (Annotazione) e selezionare un'annotazione dall'elenco.
5. Fare clic su **valore** ed eseguire una delle seguenti operazioni, a seconda del tipo di annotazione selezionato:
   - Se il tipo di annotazione è list, date o booleano, selezionare un valore dall'elenco.
   - Se il tipo di annotazione è testo, digitare un valore.
6. Fare clic su **Save** (Salva).
7. Se si desidera modificare il valore dell'annotazione dopo l'assegnazione, fare clic su e selezionare un valore diverso.

   Se l'annotazione è di tipo elenco per cui è selezionata l'opzione **Aggiungi valori dinamicamente all'assegnazione dell'annotazione**, è possibile digitare per aggiungere un nuovo valore oltre alla selezione di un valore esistente.

Modifica delle annotazioni

È possibile modificare il nome, la descrizione o i valori di un'annotazione oppure eliminare un'annotazione che non si desidera più utilizzare.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insightweb.
2. Fare clic su **Gestisci** e selezionare **Annotazioni**.

   Viene visualizzata la pagina Annotazioni.
3. Posizionare il cursore sull'annotazione che si desidera modificare e fare clic su .

   Viene visualizzata la finestra di dialogo **Edit Annotation** (Modifica annotazione).
4. È possibile apportare le seguenti modifiche a un'annotazione:

a. Modificare il nome, la descrizione o entrambi.

   Tuttavia, è possibile inserire un massimo di 255 caratteri per il nome e la descrizione e non modificare il tipo di annotazione. Inoltre, per le annotazioni a livello di sistema, non è possibile modificare il nome o la descrizione; tuttavia, è possibile aggiungere o rimuovere valori se l'annotazione è un tipo di elenco.

   Se un'annotazione personalizzata viene pubblicata nel Data Warehouse e viene rinominata, i dati storici andranno persi.

a. Per aggiungere un altro valore a un'annotazione di tipo di elenco, fare clic su + Add .
b. Per rimuovere un valore da un'annotazione di tipo di elenco, fare clic su .

   Non è possibile eliminare un valore di annotazione se tale valore è associato a un'annotazione contenuta in una regola di annotazione, una query o una policy di performance.

5. Al termine, fare clic su **Save** (Salva).

Al termine

Se si intende utilizzare le annotazioni nel Data Warehouse, è necessario forzare un aggiornamento delle annotazioni nel Data Warehouse. Fare riferimento alla *Guida all'amministrazione del data warehouse di OnCommand Insight*.

Eliminazione delle annotazioni

È possibile eliminare un'annotazione che non si desidera più utilizzare. Non è possibile eliminare un'annotazione a livello di sistema o un'annotazione utilizzata in una regola di annotazione, in una query o in un criterio di performance.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Gestisci** e selezionare **Annotazioni**.

   Viene visualizzata la pagina Annotazioni.

3. Posizionare il cursore sull'annotazione che si desidera eliminare e fare clic su .

   Viene visualizzata una finestra di dialogo di conferma.

4. Fare clic su **OK**.

Assegnazione di annotazioni alle risorse utilizzando le regole di annotazione

Per assegnare automaticamente le annotazioni alle risorse in base ai criteri definiti, configurare le regole di annotazione. OnCommand Insight assegna le annotazioni alle risorse in base a queste regole. Insight offre anche due regole di annotazione predefinite, che è possibile modificare in base alle proprie esigenze o rimuovere se non si desidera utilizzarle.

Regole di annotazione dello storage predefinite

Per accelerare l'assegnazione delle annotazioni di storage alle risorse, OnCommand Insight include 21 regole di annotazione predefinite, che associano un livello di Tier a un modello di Tier di storage. Tutte le risorse di storage vengono automaticamente associate a un Tier al momento dell'acquisizione delle risorse nell'ambiente.

Le regole di annotazione predefinite applicano le annotazioni di un livello nel seguente modo:

- Tier 1, Tier di qualità dello storage

  L'annotazione Tier 1 viene applicata ai seguenti vendor e alle loro famiglie specificate: EMC (Symmetrix), HDS (HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM (DS8000), NetApp (FAS6000 o FAS6200) e violino (memoria).

- Tier 2, Tier di qualità dello storage

  L'annotazione Tier 2 viene applicata ai seguenti vendor e alle loro famiglie specificate: HP (3PAR StoreServ o EVA), EMC (CLARiiON), HDS (AMS o D800), IBM (XIV) e NetApp (FAS3000, FAS3100 e FAS3200).

È possibile modificare le impostazioni predefinite di queste regole in modo che corrispondano ai requisiti del livello o rimuoverle se non sono necessarie.

Creazione di regole di annotazione

In alternativa all'applicazione manuale delle annotazioni a singole risorse, è possibile applicare automaticamente le annotazioni a più risorse utilizzando le regole di annotazione. Le annotazioni impostate manualmente su una singola pagina di risorse hanno la precedenza sulle annotazioni basate su regole quando Insight valuta le regole di annotazione.

Prima di iniziare

È necessario aver creato una query per la regola di annotazione.

A proposito di questa attività

Sebbene sia possibile modificare i tipi di annotazione durante la creazione delle regole, i tipi dovrebbero essere stati definiti in anticipo.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Manage** (Gestisci) e selezionare **Annotation rules** (regole annotazione).

   La pagina Annotation Rules (regole di annotazione) visualizza l'elenco delle regole di annotazione esistenti.

3. Fare clic su + Add.

   Viene visualizzata la finestra di dialogo Add Rule (Aggiungi regola).

4. Effettuare le seguenti operazioni:
   a. Nella casella **Nome**, immettere un nome univoco che descriva la regola.

      Questo nome viene visualizzato nella pagina Annotation Rules (regole di annotazione).

   b. Fare clic su **Query** e selezionare la query che OnCommand Insight deve utilizzare per applicare l'annotazione alle risorse.
   c. Fare clic su **Annotation** (Annotazione) e selezionare l'annotazione da applicare.
   d. Fare clic su **valore** e selezionare un valore per l'annotazione.

      Ad esempio, se si sceglie compleanno come annotazione, si specifica una data per il valore.
5. Fare clic su **Save** (Salva).
6. Fare clic su **Run All rules** (Esegui tutte le regole) se si desidera eseguire tutte le regole immediatamente; in caso contrario, le regole vengono eseguite a intervalli regolari pianificati.

Impostazione della precedenza della regola di annotazione

Per impostazione predefinita, OnCommand Insight valuta le regole di annotazione in modo sequenziale; tuttavia, è possibile configurare l'ordine in cui OnCommand Insight valuta le regole di annotazione se si desidera che Insight valuti le regole in un ordine specifico.

Fasi

1. Accedere all'interfaccia utente di Insightweb.
2. Fare clic su **Manage** (Gestisci) e selezionare **Annotation rules** (regole annotazione).

   La pagina Annotation Rules (regole di annotazione) visualizza l'elenco delle regole di annotazione esistenti.
3. Posizionare il cursore su una regola di annotazione.

   Le frecce di precedenza vengono visualizzate a destra della regola.
4. Per spostare una regola verso l'alto o verso il basso nell'elenco, fare clic sulla freccia verso l'alto o verso il basso.

   Per impostazione predefinita, le nuove regole vengono aggiunte in sequenza all'elenco di regole. Le annotazioni impostate manualmente su una singola pagina di risorse hanno la precedenza sulle annotazioni basate su regole quando Insight valuta le regole di annotazione.

Modifica delle regole di annotazione

È possibile modificare una regola di annotazione per modificare il nome della regola, la relativa annotazione, il valore dell'annotazione o la query associata alla regola.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insightweb.

2. Fare clic su **Manage** (Gestisci) e selezionare **Annotation rules** (regole annotazione).

   La pagina Annotation Rules (regole di annotazione) visualizza l'elenco delle regole di annotazione esistenti.

3. Individuare la regola che si desidera modificare:
   - Nella pagina Annotation Rules (regole di annotazione), è possibile filtrare le regole di annotazione immettendo un valore nella casella di filtro.
   - Fare clic su un numero di pagina per sfogliare le regole di annotazione per pagina se sono presenti più regole che si adattano a una pagina.
4. Per visualizzare la finestra di dialogo **Modifica regola**, eseguire una delle seguenti operazioni:
   - Nella pagina Annotation Rules (regole di annotazione), posizionare il cursore sulla regola di annotazione e fare clic su .
   - Se ci si trova in una pagina di risorse, posizionare il cursore sull'annotazione associata alla regola, posizionare il cursore sul nome della regola quando viene visualizzata, quindi fare clic sul nome della regola.
5. Apportare le modifiche richieste e fare clic su **Save** (Salva).

Eliminazione delle regole di annotazione

È possibile eliminare una regola di annotazione quando non è più necessaria per monitorare gli oggetti nella rete.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insightweb.
2. Fare clic su **Manage** (Gestisci) e selezionare **Annotation rules** (regole annotazione).

   La pagina Annotation Rules (regole di annotazione) visualizza l'elenco delle regole di annotazione esistenti.

3. Individuare la regola che si desidera eliminare:
   - Nella pagina Annotation Rules (regole di annotazione), è possibile filtrare le regole di annotazione immettendo un valore nella casella di filtro.
   - Fare clic su un numero di pagina per sfogliare le regole di annotazione per pagina se sono presenti più regole che si adattano a una singola pagina.
4. Posizionare il cursore sulla regola che si desidera eliminare, quindi fare clic su .

   Viene visualizzato un messaggio di conferma che richiede se si desidera eliminare la regola.

5. Fare clic su **OK**.

Importazione dei valori di annotazione

Se si mantengono annotazioni su oggetti SAN (come storage, host e macchine virtuali) in un file CSV, è possibile importare tali informazioni in OnCommand Insight. È possibile importare applicazioni, entità aziendali o annotazioni, ad esempio Tier e building.

A proposito di questa attività

Si applicano le seguenti regole:

- Se un valore di annotazione è vuoto, l'annotazione viene rimossa dall'oggetto.
- Quando si annotano volumi o volumi interni, il nome dell'oggetto è una combinazione di nome dello storage e nome del volume utilizzando il separatore trattino e freccia (→):

  ```
  <storage_name>-><volume_name>
  ```

- Quando lo storage, gli switch o le porte sono annotati, la colonna Application (applicazione) viene ignorata.
- Le colonne di tenant, Line_of_Business, Business_Unit e Project costituiscono un'entità aziendale.

  I valori possono essere lasciati vuoti. Se un'applicazione è già correlata a un'entità aziendale diversa dai valori di input, l'applicazione viene assegnata alla nuova entità aziendale.

L'utility di importazione supporta i seguenti tipi di oggetti e chiavi:

Tipo	Chiave
Host	`id-><id>` oppure `<Name>` oppure `<IP>`
MACCHINA VIRTUALE	`id-><id>` oppure `<Name>`
Pool di storage	`id-><id>` oppure `<Storage_name>` `/→<Storage_Pool_name>`
Volume interno	`id-><id>` oppure `<Storage_name>` `/→<Internal_volume_name>`
Volume	`id-><id>` oppure `<Storage_name>` `/→<Volume_name>`
Storage	`id-><id>` oppure `<Name>` oppure `<IP>`
Switch	`id-><id>` oppure `<Name>` oppure `<IP>`
Porta	`id-><id>` oppure `<WWN>`
Condividere	`id-><id>` oppure `<Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol>` `<Qtree>` è facoltativo se esiste un qtree predefinito.
Qtree	`id-><id>` oppure `<Storage Name>-><Internal Volume Name>-><Qtree Name>`

Il file CSV deve avere il seguente formato:

```
, , <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>]
```

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Admin** e selezionare **Troubleshooting**.

   Viene visualizzata la pagina risoluzione dei problemi.
3. Nella sezione **altre attività** della pagina, fare clic sul collegamento **Portale OnCommand Insight**.
4. Fare clic su **Insight Connect API**.
5. Accedere al portale.
6. Fare clic su **Annotation Import Utility**.
7. Salvare `.zip` file, decomprimerlo e leggere `readme.txt` file per ulteriori informazioni ed esempi.
8. Posizionare il file CSV nella stessa cartella di `.zip` file.
9. Nella finestra della riga di comando, immettere quanto segue:

   ```
   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
   ```

   Per impostazione predefinita, l'opzione -l, che attiva la registrazione aggiuntiva, e l'opzione -c, che attiva la distinzione tra maiuscole e minuscole, sono impostate su false. Pertanto, è necessario specificarli solo quando si desidera utilizzare le funzioni.

   Non ci sono spazi tra le opzioni e i relativi valori.

Le seguenti parole chiave sono riservate e impediscono agli utenti di specificarle come nomi di annotazione: - Applicazione - priorità_applicazione - tenant - linea_di_business - unità_business - errori di progetto vengono generati se si tenta di importare un tipo di annotazione utilizzando una delle parole chiave riservate. Se i nomi delle annotazioni sono stati creati utilizzando queste parole chiave, è necessario modificarli in modo che lo strumento di importazione funzioni correttamente.

L'utilità di importazione delle annotazioni richiede Java 8 o Java 11. Assicurarsi che uno di questi sia installato prima di eseguire l'utilità di importazione. Si consiglia di utilizzare l'ultima versione di OpenJDK 11.

Assegnazione di annotazioni a più risorse utilizzando una query

L'assegnazione di un'annotazione a un gruppo di risorse consente di identificare o utilizzare più facilmente tali risorse correlate in query o dashboard.

Prima di iniziare

Le annotazioni che si desidera assegnare alle risorse devono essere state create in precedenza.

A proposito di questa attività

È possibile semplificare l'attività di assegnazione di un'annotazione a più risorse utilizzando una query. Ad esempio, se si desidera assegnare un'annotazione di indirizzo personalizzata a tutti gli array in una posizione specifica del data center.

Fasi

1. Creare una nuova query per identificare le risorse su cui si desidera assegnare un'annotazione. Fare clic su **Query** > **+Nuova query**.
2. Nell'elenco a discesa **Cerca…**, selezionare **Storage**. È possibile impostare i filtri in modo da restringere ulteriormente l'elenco delle memorie visualizzate.
3. Nell'elenco di archivi visualizzato, selezionare uno o più archivi facendo clic sulla casella di controllo accanto al nome dello storage. È inoltre possibile selezionare tutti gli storage visualizzati facendo clic sulla casella di controllo principale nella parte superiore dell'elenco.
4. Una volta selezionati tutti gli storage desiderati, fare clic su **azioni** > **Modifica annotazione**.

   Viene visualizzata la finestra di dialogo Add Annotation (Aggiungi annotazione).

5. Selezionare **Annotation** (Annotazione) e **value** che si desidera assegnare alle memorie e fare clic su **Save** (Salva).

   Se si visualizza la colonna per l'annotazione, questa viene visualizzata su tutti gli storage selezionati.

6. È ora possibile utilizzare l'annotazione per filtrare le memorie in un widget o in una query. In un widget, è possibile effettuare le seguenti operazioni:

   a. Creare una dashboard o aprirne una esistente. Aggiungere una **variabile** e scegliere l'annotazione impostata sui dati memorizzati sopra. La variabile viene aggiunta alla dashboard.

   b. Nel campo della variabile appena aggiunto, fare clic su **Any** e immettere il valore appropriato su cui filtrare. Fare clic sul segno di spunta per salvare il valore della variabile.

c. Aggiungere un widget. Nella query del widget, fare clic sul pulsante**Filtra per+**e selezionare l'annotazione appropriata dall'elenco.

d. Fare clic su **Any** e selezionare la variabile di annotazione aggiunta in precedenza. Le variabili create iniziano con "``" e vengono visualizzate nell'elenco a discesa.

e. Impostare gli altri filtri o campi desiderati, quindi fare clic su **Save** (Salva) quando il widget viene personalizzato in base alle proprie preferenze.

Il widget sulla dashboard visualizza i dati solo per le memorie a cui è stata assegnata l'annotazione.

Esecuzione di query sulle risorse

Le query consentono di monitorare e risolvere i problemi della rete effettuando una ricerca delle risorse nell'ambiente a un livello granulare in base a criteri selezionati dall'utente (annotazioni e metriche delle performance). Inoltre, le regole di annotazione, che assegnano automaticamente le annotazioni alle risorse, richiedono una query.

Risorse utilizzate in query e dashboard

Le query Insight e i widget della dashboard possono essere utilizzati con un'ampia gamma di tipi di risorse

I seguenti tipi di risorse possono essere utilizzati in query, widget dashboard e pagine di risorse personalizzate. I campi e i contatori disponibili per i filtri, le espressioni e la visualizzazione variano in base al tipo di risorsa. Non tutte le risorse possono essere utilizzate in tutti i tipi di widget.

- Applicazione
- Datastore
- Disco
- Fabric
- Dispositivo generico
- Host
- Volume interno
- Sessione iSCSI
- Portale di rete iSCSI
- Percorso
- Porta
- Qtree
- Quota
- Condividere
- Storage
- Nodo di storage
- Pool di storage
- Switch

- Nastro
- VMDK
- Macchina virtuale
- Volume
- Zona
- Membro di zona

Creazione di una query

È possibile creare una query per consentire la ricerca delle risorse nell'ambiente a un livello granulare. Le query consentono di suddividere i dati aggiungendo filtri e quindi ordinando i risultati per visualizzare i dati di inventario e performance in un'unica vista.

A proposito di questa attività

Ad esempio, è possibile creare una query per i volumi, aggiungere un filtro per trovare i dati memorizzati associati al volume selezionato, aggiungere un filtro per trovare un'annotazione particolare, ad esempio Tier 1, sugli storage selezionati, Infine, Aggiungi un altro filtro per trovare tutti gli storage con IOPS - Read (io/s) superiori a 25. Una volta visualizzati i risultati, è possibile ordinare le colonne delle informazioni associate alla query in ordine crescente o decrescente.

Quando viene aggiunta una nuova origine dati che acquisisce le risorse o vengono effettuate annotazioni o assegnazioni di applicazioni, è possibile eseguire query per tali risorse, annotazioni o applicazioni dopo che le query sono state indicizzate, che si verifica a intervalli pianificati regolarmente.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Query** e selezionare **+ Nuova query**.
3. Fare clic su **Select Resource Type** (Seleziona tipo di risorsa) e selezionare un tipo di risorsa.

   Quando si seleziona una risorsa per una query, vengono visualizzate automaticamente diverse colonne predefinite; è possibile rimuovere queste colonne o aggiungerne di nuove in qualsiasi momento.

4. Nella casella di testo **Nome**, digitare il nome della risorsa o una parte di testo da filtrare attraverso i nomi delle risorse.

   È possibile utilizzare una delle seguenti opzioni da sola o combinate per perfezionare la ricerca in qualsiasi casella di testo della pagina Nuova query:

   - Un asterisco consente di cercare tutto. Ad esempio, `vol*rhel` visualizza tutte le risorse che iniziano con "vol" e terminano con "rhel".
   - Il punto interrogativo consente di cercare un numero specifico di caratteri. Ad esempio, `BOS-PRD??-S12` Visualizza BOS-PRD12-S12, BOS-PRD13-S12 e così via.
   - L'operatore OR consente di specificare più entità. Ad esempio, `FAS2240 OR CX600 OR FAS3270` trova più modelli di storage.
   - L'operatore NOT consente di escludere il testo dai risultati della ricerca. Ad esempio, `NOT EMC*` Trova tutto ciò che non inizia con "EMC". È possibile utilizzare `NOT *` per visualizzare i campi che non contengono valori.

5. Fare clic su  per visualizzare le risorse.
6. Per aggiungere un criterio, fare clic su 

ed eseguire una delle seguenti operazioni:
   - Digitare per cercare un criterio specifico, quindi selezionarlo.
   - Scorrere l'elenco e selezionare un criterio.
   - Inserire un intervallo di valori se si sceglie una metrica delle performance come IOPS - Read (io/s). Le annotazioni predefinite fornite da Insight sono indicate da ; è possibile avere annotazioni con nomi duplicati.

   Viene aggiunta una colonna all'elenco risultati query per i criteri e i risultati della query nell'elenco vengono aggiornati.
7. Se si desidera, fare clic su per rimuovere un'annotazione o una metrica delle prestazioni dai risultati della query.

   Ad esempio, se la query mostra la latenza massima e il throughput massimo per gli archivi dati e si desidera visualizzare solo la latenza massima nell'elenco dei risultati della query, fare clic su questo pulsante e deselezionare la casella di controllo **throughput - Max**. La colonna throughput - Max (MB/s) viene rimossa dall'elenco risultati query.

   A seconda del numero di colonne visualizzate nella tabella dei risultati della query, potrebbe non essere possibile visualizzare ulteriori colonne aggiunte. È possibile rimuovere una o più colonne fino a quando le colonne desiderate non diventano visibili.
8. Fare clic su **Save** (Salva), immettere un nome per la query e fare nuovamente clic su **Save** (Salva).

   Se si dispone di un account con ruolo di amministratore, è possibile creare dashboard personalizzate. Una dashboard personalizzata può comprendere qualsiasi widget della libreria di widget, molti dei quali consentono di rappresentare i risultati delle query in una dashboard personalizzata. Per ulteriori informazioni sui dashboard personalizzati, consulta la *Guida introduttiva di OnCommand Insight*.

Informazioni correlate

"Importazione ed esportazione dei dati utente"

Visualizzazione delle query

È possibile visualizzare le query per monitorare le risorse e modificare il modo in cui le query visualizzano i dati relativi alle risorse.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**.
3. È possibile modificare la modalità di visualizzazione delle query effettuando una delle seguenti operazioni:
   - È possibile inserire del testo nella casella **filter** per eseguire la ricerca e visualizzare query specifiche.
   - È possibile modificare l'ordinamento delle colonne nella tabella delle query in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.

- Per ridimensionare una colonna, passare il mouse sull'intestazione della colonna fino a visualizzare una barra blu. Posizionare il mouse sulla barra e trascinarla verso destra o verso sinistra.
- Per spostare una colonna, fare clic sull'intestazione della colonna e trascinarla verso destra o verso sinistra.
- Quando si scorrono i risultati della query, tenere presente che i risultati potrebbero cambiare poiché Insight esegue automaticamente il polling delle origini dati. Ciò potrebbe causare la mancanza di alcuni elementi o la mancata visualizzazione di alcuni elementi in base all'ordinamento.

Esportazione dei risultati della query in un file .CSV

È possibile esportare i risultati di una query in un file .CSV per importare i dati in un'altra applicazione.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

3. Fare clic su una query.
4. Fare clic su per esportare i risultati della query in un `.CSV` file.
5. Effettuare una delle seguenti operazioni:
   - Fare clic su **Apri con**, quindi su **OK** per aprire il file con Microsoft Excel e salvarlo in una posizione specifica.
   - Fare clic su **Save file** (Salva file), quindi su **OK** per salvare il file nella cartella Downloads (Download). Verranno esportati solo gli attributi delle colonne visualizzate. Alcune colonne visualizzate, in particolare quelle che fanno parte di relazioni nidificate complesse, non vengono esportate.

     Quando viene visualizzata una virgola nel nome di una risorsa, l'esportazione racchiude il nome tra virgolette, conservando il nome della risorsa e il formato .csv appropriato.

     + quando si esportano i risultati delle query, tenere presente che **tutte le** righe della tabella dei risultati verranno esportate, non solo quelle selezionate o visualizzate sullo schermo, fino a un massimo di 10,000 righe.

Quando si apre un file .CSV esportato con Excel, se si dispone di un nome oggetto o di un altro campo nel formato NN:NN (due cifre seguite da due punti e altre due cifre), Excel a volte interpreta tale nome come formato orario, anziché come formato testo. Ciò può causare la visualizzazione di valori errati in tali colonne in Excel. Ad esempio, un oggetto denominato "81:45" viene visualizzato in Excel come "81:45:00". Per risolvere questo problema, importare il file .CSV in Excel seguendo la procedura riportata di seguito:

+

```
-   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.
```

+

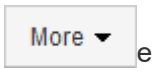
Modifica delle query

È possibile modificare i criteri associati a una query quando si desidera modificare i criteri di ricerca per le risorse che si stanno interrogando.

Fasi

1. Accedere all'interfaccia utente di Insightweb.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

3. Fare clic sul nome della query.
4. Per rimuovere un criterio dalla query, fare clic su .
5. Per aggiungere un criterio alla query, fare clic su 

e selezionare un criterio dall'elenco.
6. Effettuare una delle seguenti operazioni:
   - Fare clic su **Save** (Salva) per salvare la query con il nome utilizzato inizialmente.
   - Fare clic su **Save As** (Salva con nome) per salvare la query con un altro nome.
   - Fare clic su **Rename** (Rinomina) per modificare il nome della query utilizzato inizialmente.
   - Fare clic su **Ripristina** per ripristinare il nome della query a quello utilizzato inizialmente.

Eliminazione delle query

È possibile eliminare le query quando non raccolgono più informazioni utili sulle risorse. Non è possibile eliminare una query se utilizzata in una regola di annotazione.

Fasi

1. Accedere all'interfaccia utente di Insightweb.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

3. Posizionare il cursore sulla query che si desidera eliminare e fare clic su .

   Viene visualizzato un messaggio di conferma che chiede se si desidera eliminare la query.

4. Fare clic su **OK**.

Assegnazione di più applicazioni o rimozione di più applicazioni dalle risorse

È possibile assegnare o rimuovere più applicazioni dalle risorse utilizzando una query invece di dover assegnarle o rimuoverle manualmente.

Prima di iniziare

È necessario aver già creato una query che trovi tutte le risorse da modificare.

Fasi

1. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

2. Fare clic sul nome della query che trova le risorse.

   Viene visualizzato l'elenco delle risorse associate alla query.

3. Selezionare le risorse desiderate nell'elenco o fare clic su Per selezionare **tutto**.

   Viene visualizzato il pulsante **azioni**.

4. Per aggiungere un'applicazione alle risorse selezionate, fare clic su Actions E selezionare **Modifica applicazione**.
   a. Fare clic su **applicazione** e selezionare una o più applicazioni.

      È possibile selezionare più applicazioni per host, volumi interni e macchine virtuali; tuttavia, è possibile selezionare solo un'applicazione per un volume.

   b. Fare clic su **Save** (Salva).

5. Per rimuovere un'applicazione assegnata alle risorse, fare clic su Actions E selezionare **Rimuovi applicazione**.

a. Selezionare l'applicazione o le applicazioni che si desidera rimuovere.

b. Fare clic su **Delete** (Elimina).

Tutte le nuove applicazioni assegnate hanno la precedenza su quelle derivate da un'altra risorsa. Ad esempio, i volumi ereditano le applicazioni dagli host e, quando vengono assegnate nuove applicazioni a un volume, la nuova applicazione ha la precedenza sull'applicazione derivata.

Modifica o rimozione di più annotazioni dalle risorse

È possibile modificare più annotazioni per le risorse o rimuovere più annotazioni dalle risorse utilizzando una query invece di doverle modificare o rimuovere manualmente.

Prima di iniziare

È necessario aver già creato una query che trovi tutte le risorse che si desidera modificare.

Fasi

1. Fare clic su **Query** e selezionare **Mostra tutte le query**.

   Viene visualizzata la pagina Query.

2. Fare clic sul nome della query che trova le risorse.

   Viene visualizzato l'elenco delle risorse associate alla query.

3. Selezionare le risorse desiderate nell'elenco o fare clic su ☐ ▾ Per selezionare **tutto**.

   Viene visualizzato il pulsante **azioni**.

4. Per aggiungere un'annotazione alle risorse o modificare il valore di un'annotazione assegnata alle risorse, fare clic su Actions ▾ E selezionare **Edit Annotation** (Modifica annotazione).

   a. Fare clic su **Annotation** (Annotazione) e selezionare un'annotazione per la quale si desidera modificare il valore oppure selezionare una nuova annotazione per assegnarla a tutte le risorse.

   b. Fare clic su **valore** e selezionare un valore per l'annotazione.

   c. Fare clic su **Save** (Salva).

5. Per rimuovere un'annotazione assegnata alle risorse, fare clic su Actions ▾ E selezionare **Remove Annotation** (Rimuovi annotazione).

   a. Fare clic su **Annotation** (Annotazione) e selezionare l'annotazione che si desidera rimuovere dalle risorse.

   b. Fare clic su **Delete** (Elimina).

Copia dei valori della tabella

È possibile copiare i valori nelle tabelle per utilizzarli nelle caselle di ricerca o in altre applicazioni.

A proposito di questa attività

Esistono due metodi per copiare i valori dalle tabelle o dai risultati delle query.

Fasi

1. Metodo 1: Evidenziare il testo desiderato con il mouse, copiarlo e incollarlo nei campi di ricerca o in altre applicazioni.
2. Metodo 2: Per i campi a valore singolo la cui lunghezza supera la larghezza della colonna della tabella, indicata da ellissi (…), posizionare il puntatore del mouse sul campo e fare clic sull'icona degli Appunti. Il valore viene copiato negli Appunti per essere utilizzato nei campi di ricerca o in altre applicazioni.

   Si noti che è possibile copiare solo i valori che sono collegamenti alle risorse. Si noti inoltre che solo i campi che includono valori singoli (ad esempio, non elenchi) hanno l'icona di copia.

Gestione delle policy sulle performance

OnCommand Insight consente di creare policy sulle performance per monitorare la rete alla ricerca di diverse soglie e per generare avvisi quando tali soglie vengono superate. Utilizzando le policy sulle performance, è possibile rilevare immediatamente una violazione di una soglia, identificare l'implicazione e analizzare l'impatto e la causa del problema in modo da consentire una correzione rapida ed efficace.

Una policy sulle performance consente di impostare soglie su qualsiasi oggetto (datastore, disco, hypervisor, volume interno, porta, Storage, nodo storage, pool storage, VMDK, macchina virtuale, E volume) con i contatori delle performance riportati (ad esempio, IOPS totali). Quando si verifica una violazione di una soglia, Insight la rileva e la segnala nella pagina delle risorse associate, visualizzando un cerchio rosso continuo, un avviso via e-mail, se configurato, e nella dashboard delle violazioni o in qualsiasi dashboard personalizzata che segnala le violazioni.

Insight fornisce alcune policy di performance predefinite, che è possibile modificare o eliminare se non applicabili all'ambiente in uso, per i seguenti oggetti:

- Hypervisor

  Esistono policy di swapping ESX e utilizzo ESX.

- Volume e volume interni

  Sono disponibili due policy di latenza per ciascuna risorsa, una annotata per il Tier 1 e l'altra per il Tier 2.

- Porta

  Esiste una policy per lo zero del credito BB.

- Nodo storage

  Esiste una policy per l'utilizzo del nodo.

- Macchina virtuale

  Esistono lo swapping delle macchine virtuali e policy di memoria e CPU ESX.

- Volume

  Vi sono latenza per Tier e policy di volume disallineate.

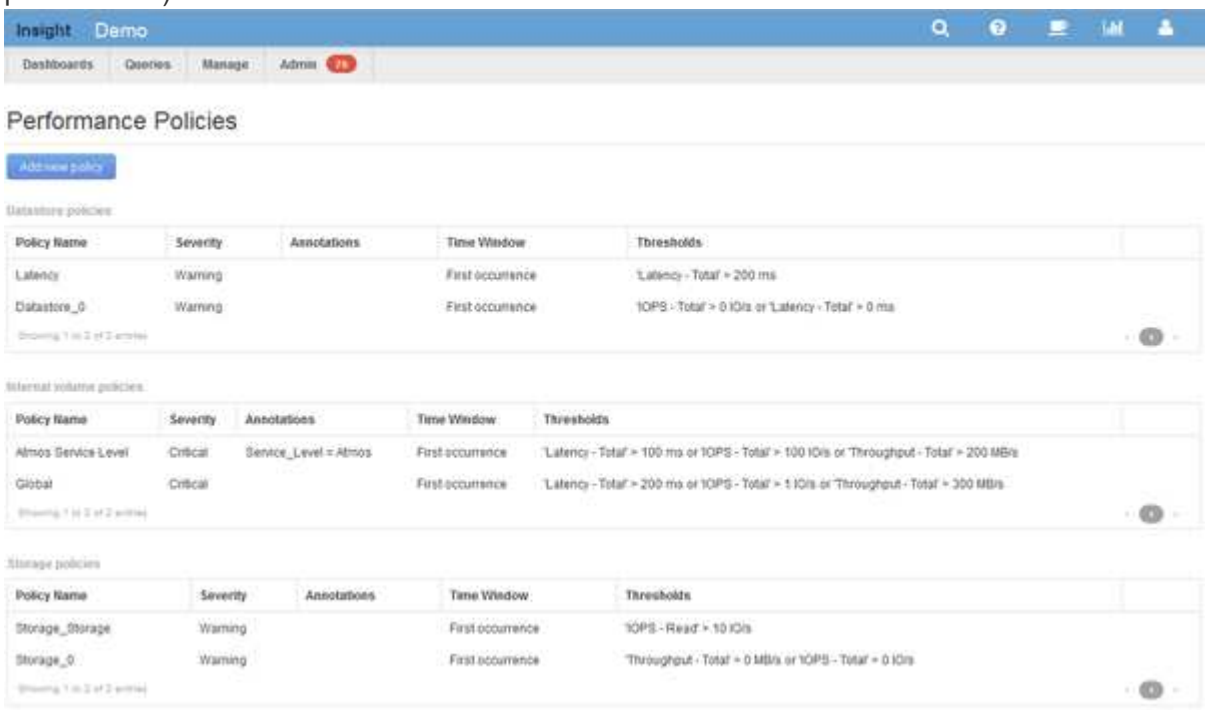
Creazione di policy sulle performance

Vengono create policy di performance per impostare soglie che attivano avvisi per segnalare problemi relativi alle risorse della rete. Ad esempio, è possibile creare una policy sulle performance per avvisare l'utente quando l'utilizzo totale per i pool di storage è superiore al 60%.

Fasi

1. Aprire OnCommand Insight nel browser.
2. Selezionare **Gestisci** > **Criteri di performance**.

   Viene visualizzata la pagina Performance Policies (Criteri di performance).



   I criteri sono organizzati in base all'oggetto e vengono valutati nell'ordine in cui vengono visualizzati nell'elenco relativo a tale oggetto.

3. Fare clic su **Aggiungi nuovo criterio**.

   Viene visualizzata la finestra di dialogo Add Policy (Aggiungi policy).

4. Nel campo **Nome policy**, immettere un nome per la policy.

   È necessario utilizzare un nome diverso da tutti gli altri nomi di policy per l'oggetto. Ad esempio, non è possibile avere due criteri denominati "latenza" per un volume interno; tuttavia, è possibile disporre di un criterio "latenza" per un volume interno e di un altro criterio "latenza" per un volume diverso. La procedura consigliata consiste nell'utilizzare sempre un nome univoco per qualsiasi policy, indipendentemente dal tipo

di oggetto.

5. Dall'elenco **Apply to objects of type** (Applica a oggetti di tipo), selezionare il tipo di oggetto a cui si applica il criterio.
6. Dall'elenco **con annotazione**, selezionare un tipo di annotazione, se applicabile, e inserire un valore per l'annotazione nella casella **valore** per applicare la policy solo agli oggetti che hanno questo particolare set di annotazioni.
7. Se si seleziona **Port** come tipo di oggetto, dall'elenco **Connected to** (connesso a), selezionare la porta a cui è connessa.
8. Dall'elenco **Apply after a window of** (Applica dopo una finestra di*), selezionare quando viene generato un avviso per indicare una violazione di soglia.

   L'opzione First ricorrenza attiva un avviso quando viene superata una soglia sul primo campione di dati. Tutte le altre opzioni attivano un avviso quando la soglia viene superata una volta e viene continuamente superata per almeno il periodo di tempo specificato.

9. Dall'elenco **con severità**, selezionare la severità per la violazione.
10. Per impostazione predefinita, gli avvisi e-mail sulle violazioni delle policy verranno inviati ai destinatari nell'elenco e-mail globale. È possibile ignorare queste impostazioni in modo che gli avvisi relativi a una determinata policy vengano inviati a destinatari specifici.
    - Fare clic sul collegamento per aprire l'elenco dei destinatari, quindi fare clic sul pulsante **+** per aggiungere i destinatari. Gli avvisi di violazione per tale policy verranno inviati a tutti i destinatari dell'elenco.
11. Fare clic sul collegamento **Any** nella sezione **Create alert if any of the following are true** (Crea avviso se una delle seguenti affermazioni è vera) per controllare la modalità di attivazione degli avvisi:
    - **qualsiasi**

      Questa è l'impostazione predefinita, che crea avvisi quando una qualsiasi delle soglie relative a un criterio viene superata.

    - **tutto**

      Questa impostazione crea un avviso quando tutte le soglie di un criterio vengono superate. Quando si seleziona **tutto**, la prima soglia creata per un criterio di performance viene definita regola primaria. È necessario assicurarsi che la soglia della regola principale sia la violazione di cui si è maggiormente preoccupati per la policy sulle performance.

12. Nella sezione **Create alert if**, selezionare un contatore delle prestazioni e un operatore, quindi immettere un valore per creare una soglia.
13. Fare clic su **Add threshold** (Aggiungi soglia) per aggiungere altre soglie.
14. Per rimuovere una soglia, fare clic sull'icona del cestino.
15. Selezionare la casella di controllo **Arresta l'elaborazione di ulteriori criteri se viene generato un avviso** se si desidera che il criterio interrompa l'elaborazione quando si verifica un avviso.

    Ad esempio, se si dispone di quattro criteri per gli archivi dati e il secondo è configurato per interrompere l'elaborazione quando si verifica un avviso, il terzo e il quarto criterio non vengono elaborati mentre è attiva una violazione del secondo criterio.

16. Fare clic su **Save** (Salva).

    Viene visualizzata la pagina Performance Policies (Criteri di performance) e il criterio di performance viene

visualizzato nell'elenco dei criteri per il tipo di oggetto.

Precedenza della valutazione dei criteri di performance

La pagina Performance Policies raggruppa i criteri in base al tipo di oggetto e Insight valuta i criteri nell'ordine in cui vengono visualizzati nell'elenco dei criteri di performance dell'oggetto. Puoi modificare l'ordine in cui Insight valuta le policy per mostrare le informazioni più importanti per te nella tua rete.

Insight valuta tutte le policy applicabili a un oggetto in sequenza quando vengono presi campioni di dati delle performance nel sistema per quell'oggetto; tuttavia, a seconda delle annotazioni, non tutte le policy si applicano a un gruppo di oggetti. Si supponga, ad esempio, che il volume interno abbia i seguenti criteri:

- Policy 1 (policy predefinita fornita da Insight)
- Policy 2 (con un'annotazione "SService Level = Silver" con l'opzione **Stop Processing further policies if alert is generated**
- Policy 3 (con un'annotazione "SService Level = Gold")
- Policy 4

Per un Tier di volume interno con un'annotazione Gold, Insight valuta Policy 1, ignora Policy 2 e quindi valuta Policy 3 e Policy 4. Per un Tier senza annotazioni, Insight valuta in base all'ordine delle policy; pertanto, Insight valuta solo Policy 1 e Policy 4. Per un Tier di volume interno con un'annotazione Silver, Insight valuta Policy 1 e Policy 2; Tuttavia, se un avviso viene attivato quando la soglia del criterio viene superata una volta e viene continuamente attraversato per la finestra di tempo specificata nel criterio, Insight non valuta più gli altri criteri nell'elenco mentre valuta i contatori correnti per l'oggetto. Quando Insight acquisisce il successivo set di esempi di performance per l'oggetto, inizia di nuovo a valutare le policy di performance per l'oggetto in base al filtro e quindi a ordinare.

Modifica della precedenza di una policy di performance

Per impostazione predefinita, Insight valuta in sequenza le policy di un oggetto. Puoi configurare l'ordine in cui Insight valuta le policy di performance. Ad esempio, se si dispone di una policy configurata per interrompere l'elaborazione quando si verifica una violazione per lo storage di livello Gold, è possibile inserire tale policy prima nell'elenco ed evitare di visualizzare violazioni più generiche per la stessa risorsa di storage.

Fasi

1. Aprire Insight nel browser.
2. Dal menu **Gestisci**, selezionare **Criteri di performance**.

   Viene visualizzata la pagina Performance Policies.

3. Posizionare il cursore del mouse sul nome di un criterio nell'elenco dei criteri di performance di un tipo di oggetto.

   Le frecce di precedenza vengono visualizzate a destra del criterio.

4. Per spostare un criterio in alto nell'elenco, fare clic sulla freccia verso l'alto; per spostarlo in basso nell'elenco, fare clic sulla freccia verso il basso.

Per impostazione predefinita, i nuovi criteri vengono aggiunti in sequenza all'elenco di criteri di un oggetto.

Modifica delle policy sulle performance

Puoi modificare le policy sulle performance esistenti e predefinite per modificare il modo in cui Insight monitora le condizioni di interesse nella tua rete. Ad esempio, è possibile modificare la soglia di un criterio.

Fasi

1. Aprire Insight nel browser.
2. Dal menu **Gestisci**, selezionare **Criteri di performance**.

   Viene visualizzata la pagina Performance Policies.
3. Posizionare il cursore del mouse sul nome di un criterio nell'elenco dei criteri di performance di un oggetto.
4. Fare clic su .

   Viene visualizzata la finestra di dialogo Edit Policy (Modifica policy).
5. Apportare le modifiche richieste.

   Se si modifica un'opzione diversa dal nome della policy, Insight elimina tutte le violazioni esistenti per tale policy.
6. Fare clic su **Save.** (Salva)

Eliminazione delle policy sulle performance

È possibile eliminare un criterio di performance se si ritiene che non sia più applicabile al monitoraggio degli oggetti nella rete.

Fasi

1. Aprire Insight nel browser.
2. Dal menu **Gestisci**, selezionare **Criteri di performance**.

   Viene visualizzata la pagina Performance Policies.
3. Posizionare il cursore del mouse sul nome di un criterio nell'elenco dei criteri di performance di un oggetto.
4. Fare clic su .

   Viene visualizzato un messaggio che chiede se si desidera eliminare il criterio.
5. Fare clic su **OK**.

Importazione ed esportazione dei dati utente

Le funzioni di importazione ed esportazione consentono di esportare annotazioni, regole di annotazione, query, policy di performance e dashboard personalizzati in un unico file.

Questo file può quindi essere importato in server OnCommand Insight diversi.

Le funzioni di esportazione e importazione sono supportate solo tra server che eseguono la stessa versione di OnCommand Insight.

Per esportare o importare i dati utente, fare clic su **Admin** e selezionare **Setup**, quindi selezionare la scheda **Import/Export user data** (Importa/Esporta dati utente).

Durante l'operazione di importazione, i dati vengono aggiunti, Uniti o sostituiti, a seconda degli oggetti e dei tipi di oggetti importati.

- Tipi di annotazione
  - Aggiunge un'annotazione se nel sistema di destinazione non esiste alcuna annotazione con lo stesso nome.
  - Unisce un'annotazione se il tipo di annotazione è un elenco e un'annotazione con lo stesso nome esiste nel sistema di destinazione.
  - Sostituisce un'annotazione se il tipo di annotazione è diverso da un elenco ed esiste un'annotazione con lo stesso nome nel sistema di destinazione.

    Se nel sistema di destinazione esiste un'annotazione con lo stesso nome ma con un tipo diverso, l'importazione non riesce. Se gli oggetti dipendono dall'annotazione non riuscita, potrebbero mostrare informazioni non corrette o indesiderate. Al termine dell'operazione di importazione, è necessario controllare tutte le dipendenze delle annotazioni.

- Regole di annotazione
  - Aggiunge una regola di annotazione se nel sistema di destinazione non esiste alcuna regola di annotazione con lo stesso nome.
  - Sostituisce una regola di annotazione se esiste una regola di annotazione con lo stesso nome nel sistema di destinazione.

    Le regole di annotazione dipendono da query e annotazioni. Al termine dell'operazione di importazione, è necessario verificare la precisione di tutte le regole di annotazione.

- Policy
  - Aggiunge un criterio se nel sistema di destinazione non esiste alcun criterio con lo stesso nome.
  - Sostituisce un criterio se esiste un criterio con lo stesso nome nel sistema di destinazione.

    Una volta completata l'operazione di importazione, i criteri potrebbero non essere in ordine. È necessario controllare l'ordine dei criteri dopo l'importazione. Se le annotazioni non sono corrette, le policy che dipendono dalle annotazioni potrebbero non riuscire. È necessario controllare tutte le dipendenze delle annotazioni dopo l'importazione.

    +

- Query
  - Aggiunge una query se nel sistema di destinazione non esiste alcuna query con lo stesso nome.
  - Sostituisce una query se esiste una query con lo stesso nome nel sistema di destinazione, anche se il tipo di risorsa della query è diverso.

Se il tipo di risorsa di una query è diverso, dopo l'importazione, i widget della dashboard che utilizzano tale query potrebbero visualizzare risultati indesiderati o non corretti. Dopo l'importazione, è necessario controllare la precisione di tutti i widget basati su query. Se le annotazioni non sono corrette, le query che dipendono dalle annotazioni potrebbero non riuscire. È necessario controllare tutte le dipendenze delle annotazioni dopo l'importazione.

+

- Dashboard
  - Aggiunge una dashboard se nel sistema di destinazione non esiste una dashboard con lo stesso nome.
  - Sostituisce una dashboard se nel sistema di destinazione esiste una dashboard con lo stesso nome, anche se il tipo di risorsa della query è diverso.

Dopo l'importazione, è necessario controllare la precisione di tutti i widget basati su query nei dashboard. Se il server di origine ha più dashboard con lo stesso nome, vengono tutti esportati. Tuttavia, solo il primo verrà importato nel server di destinazione. Per evitare errori durante l'importazione, assicurarsi che i dashboard abbiano nomi univoci prima di esportarli.

+

Informazioni sul copyright

Informazioni sul marchio commerciale