Configurazione e amministrazione

OnCommand Insight

NetApp
April 01, 2024

Sommario

Configurazione e amministrazione

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:

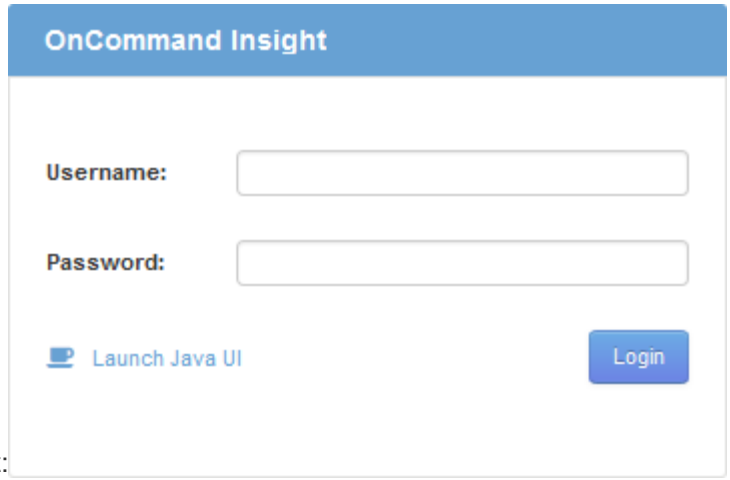
     `https://fqdn`

   - 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.

> 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.

> 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.

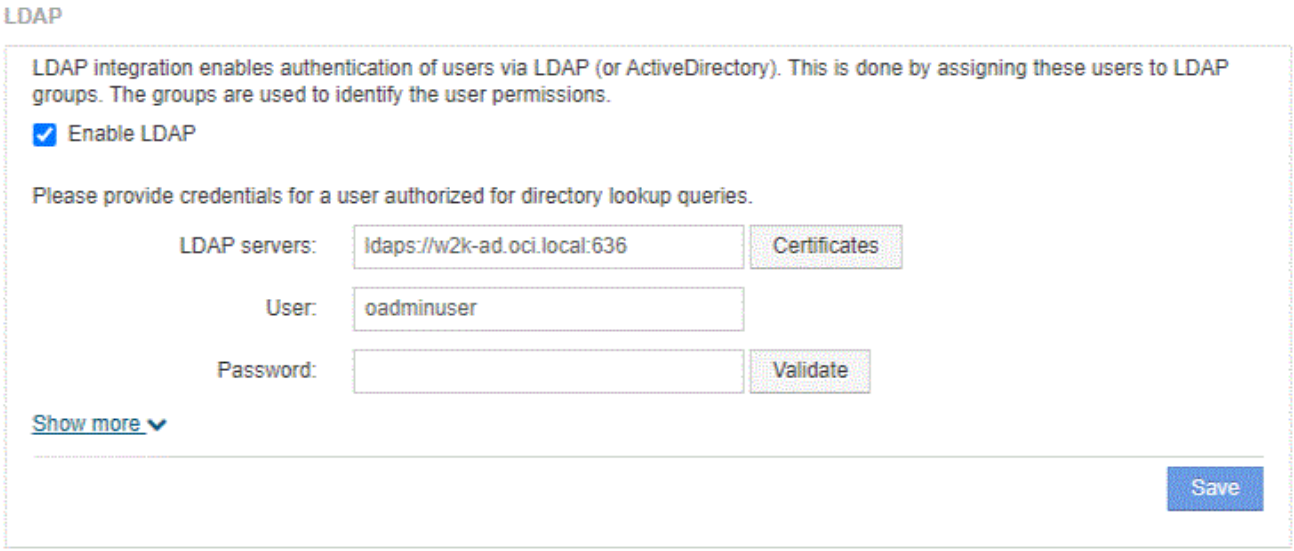
A proposito di questa attività

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, come illustrato di seguito.



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.

Insight Security

La versione 7.3.1 di OnCommand Insight ha introdotto funzionalità di sicurezza che consentono agli ambienti Insight di funzionare con una maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne e le coppie di chiavi che crittografano e decrittare le password. È possibile gestire queste funzionalità su tutti i server dell'ambiente Insight.

L'installazione predefinita di Insight include una configurazione di sicurezza in cui tutti i siti dell'ambiente condividono le stesse chiavi e le stesse password predefinite. Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente di acquisizione dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono memorizzate nel database di Insight Server. Il server dispone di una chiave pubblica e crittografa le password quando un utente le inserisce in una pagina di configurazione dell'origine dati WebUI. Il server non dispone delle chiavi private necessarie per decrittare le password dell'origine dati memorizzate nel database del server. Solo le unità di acquisizione (LAU, RAU) dispongono della chiave privata dell'origine dati necessaria per decrittare le password dell'origine dati.

Codifica dei server

L'utilizzo delle chiavi predefinite introduce una vulnerabilità a livello di sicurezza nell'ambiente in uso. Per impostazione predefinita, le password dell'origine dati vengono memorizzate crittografate nel database Insight. Vengono crittografati utilizzando una chiave comune a tutte le installazioni Insight. In una configurazione predefinita, un database Insight inviato a NetApp include password che in teoria potrebbero essere decifrate da NetApp.

Modifica della password utente di acquisizione

L'utilizzo della password utente predefinita "Acquisition" (acquisizione) introduce una vulnerabilità di sicurezza nell'ambiente. Tutte le unità di acquisizione utilizzano l'utente "Acquisition" per comunicare con il server. Raus con password predefinite può in teoria connettersi a qualsiasi server Insight utilizzando password predefinite.

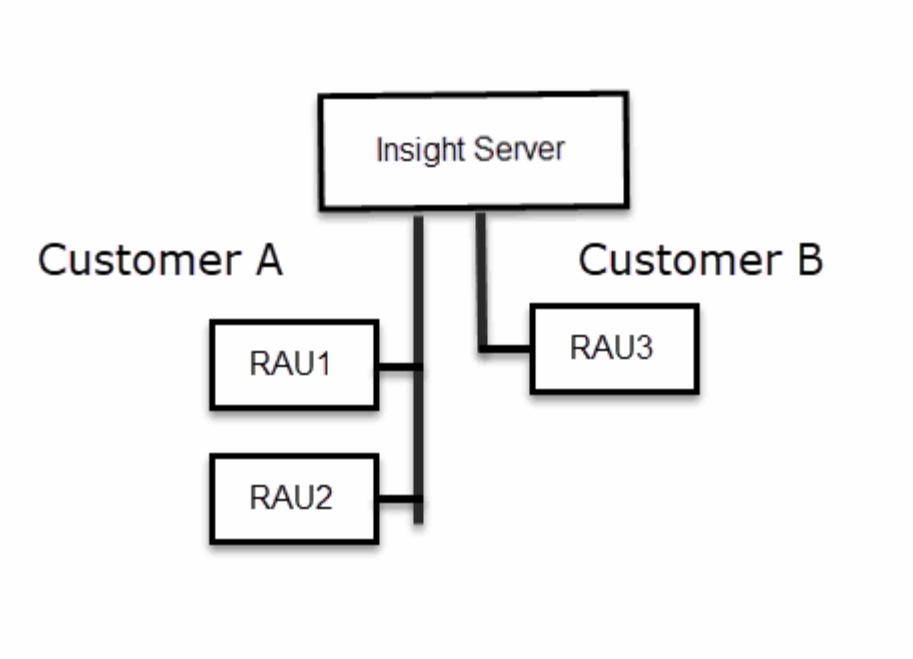
Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (password ridigettate o modificate), è necessario eseguire il backup delle configurazioni di sicurezza. L'installazione di un nuovo software o, in alcuni casi, l'aggiornamento del software ripristina la configurazione di sicurezza predefinita del sistema. Quando il sistema torna alla configurazione predefinita, è necessario ripristinare la configurazione non predefinita per il corretto funzionamento del sistema.

Gestione delle chiavi in un ambiente di service provider complesso

Un service provider può ospitare più clienti OnCommand Insight che raccolgono dati. Le chiavi proteggono i dati dei clienti dall'accesso non autorizzato da parte di più clienti sul server Insight. I dati di ciascun cliente sono protetti dalle coppie di chiavi specifiche.

Questa implementazione di Insight può essere configurata come mostrato nell'illustrazione seguente.



In questa configurazione, è necessario creare singole chiavi per ciascun cliente. Il cliente A richiede chiavi identiche per entrambi i Raus. Il cliente B richiede un singolo set di chiavi.

La procedura da seguire per modificare le chiavi di crittografia per il cliente A:

1. Eseguire un login remoto al server che ospita RAU1.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.
5. Eseguire un login remoto al server che ospita RAU2.
6. Copiare il file zip di backup della configurazione di sicurezza in RAU2.
7. Avviare lo strumento di amministrazione della protezione.
8. Ripristinare il backup di sicurezza da RAU1 al server corrente.

La procedura da seguire per modificare le chiavi di crittografia per il cliente B:

1. Eseguire un login remoto al server che ospita RAU3.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.

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`

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali “Admin”.
4. Selezionare **Server**.

   Sono disponibili le seguenti opzioni di configurazione del server:

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall’utente o nelle seguenti posizioni predefinite:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Ripristina**

     Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

     > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare la chiave di crittografia del server su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server
   - **Cambia chiave di crittografia**

     Modificare la chiave di crittografia del server utilizzata per crittografare o decrittare le password utente proxy, le password utente SMTP, le password utente LDAP e così via.

     > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un’installazione.
   - **Aggiorna password**

     Modificare la password per gli account interni utilizzati da Insight. Vengono visualizzate le seguenti opzioni:

- _interno
- acquisizione
- cognos_admin
- dwh_internal
- host
- inventario
- root

> Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

  Ripristina i valori predefiniti delle chiavi e delle password. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

  a. Scegliere l'opzione che si desidera modificare e seguire le istruzioni.

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`

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`

- Linux - `/bin/oci-securityadmin.sh -i`

  Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali “Admin”.
4. Selezionare **Local Acquisition Unit** (unità di acquisizione locale) per riconfigurare la configurazione di sicurezza dell’unità di acquisizione locale.

   Vengono visualizzate le seguenti opzioni:

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall’utente o nelle seguenti posizioni predefinite:

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

   - **Ripristina**

     Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

     > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia sul LAU - creare un backup del vault - ripristinare il backup del vault su ciascuno dei Raus

   - **Modifica delle chiavi di crittografia**

     Modificare le chiavi di crittografia AU utilizzate per crittografare o decrittare le password del dispositivo.

     > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un’installazione.

   - **Aggiorna password**

     Modificare la password per l’account utente di 'acquisizione'.

     > Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l’utente di "acquisizione" sul server, è necessario modificare la password per l’utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un’installazione.

   - **Ripristina impostazioni predefinite**

     Ripristina la password utente di acquisizione e le chiavi di crittografia dell’utente di acquisizione sui valori predefiniti. I valori predefiniti sono quelli forniti durante l’installazione.

   - **Esci**

Uscire da `securityadmin` tool.

5. Scegliere l'opzione che si desidera configurare e seguire le 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 l'aggiornamento della configurazione di sicurezza per LAU, RAU, è quello di aggiornare la password utente di 'acquisizione' quando la password per quell'utente è stata modificata sul server. Tutti i sistemi Raus e LAU utilizzano la stessa password dell'utente di '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 gestire le opzioni di sicurezza su una RAU, attenersi alla procedura riportata di seguito:

Fasi

1. Eseguire un accesso remoto al server che esegue RAU
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali "Admin".

   Il sistema visualizza il menu della RAU.

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Ripristina**

     Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

> Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

- **Modifica delle chiavi di crittografia**

  Modificare le chiavi di crittografia RAU utilizzate per crittografare o decrittare le password del dispositivo.

  > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

  Modificare la password per l'account utente di 'acquisizione'.

  > Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

  Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

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`

Fasi

1. Eseguire un login remoto al server Data Warehouse.

2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.

3. Immettere il nome utente e la password di un account con credenziali “Admin”.

   Il sistema visualizza il menu Security admin per Data Warehouse:

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall’utente o nella posizione predefinita:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Ripristina**

     Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

     > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server
     >
     > +

   - **Modificare le chiavi di crittografia**

     Modificare la chiave di crittografia DWH utilizzata per crittografare o decrittare password come le password del connettore e le password SMPT.

   - **Aggiorna password**

     Modificare la password per un account utente specifico.

     - _interno
     - acquisizione
     - cognos_admin
     - dwh
     - dwh_internal
     - dwhuser
     - host
     - inventario
     - root

> Quando si modificano le password di dwhuser, host, inventario o root, è possibile utilizzare l'hashing delle password SHA-256. Questa opzione richiede che tutti i client che accedono agli account utilizzino connessioni SSL.

+

- **Ripristina impostazioni predefinite**

  Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

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.

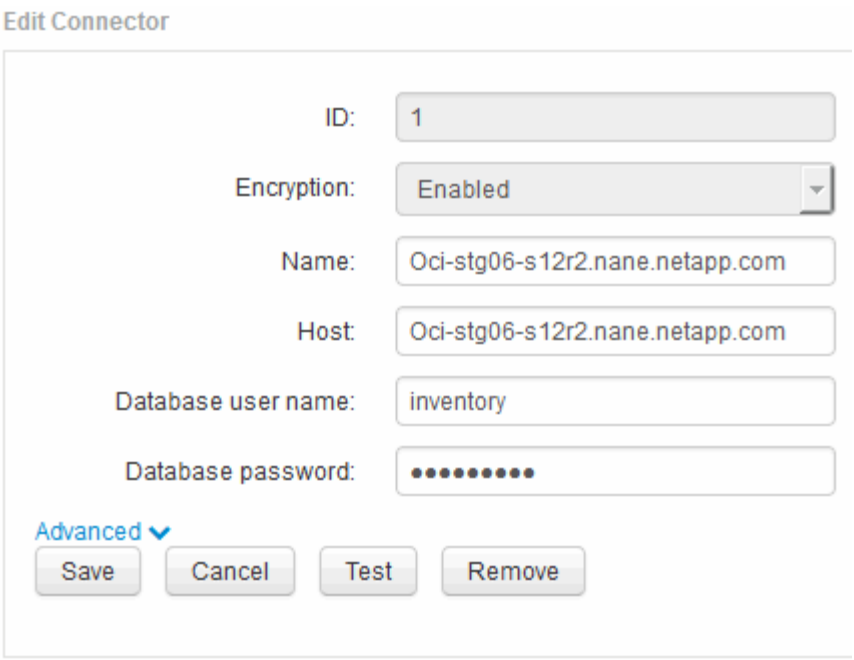
Prima di iniziare

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

Fasi

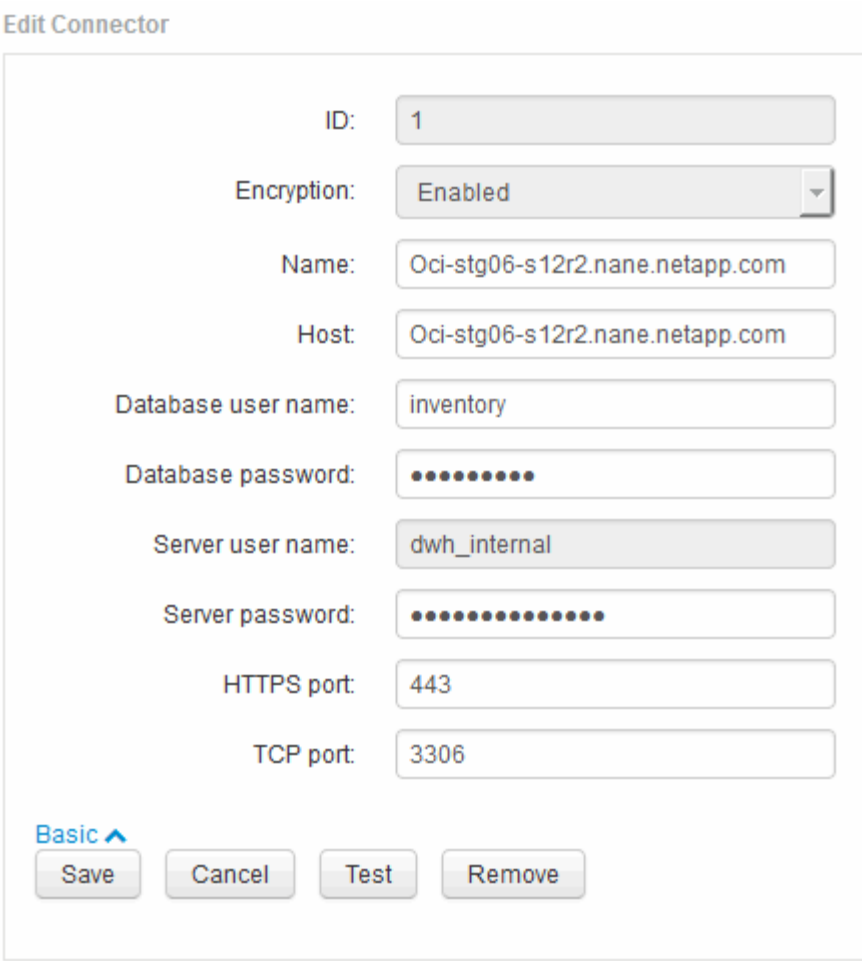
1. Accedere al Data Warehouse Portal all'indirizzo https://hostname/dwh, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

   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.

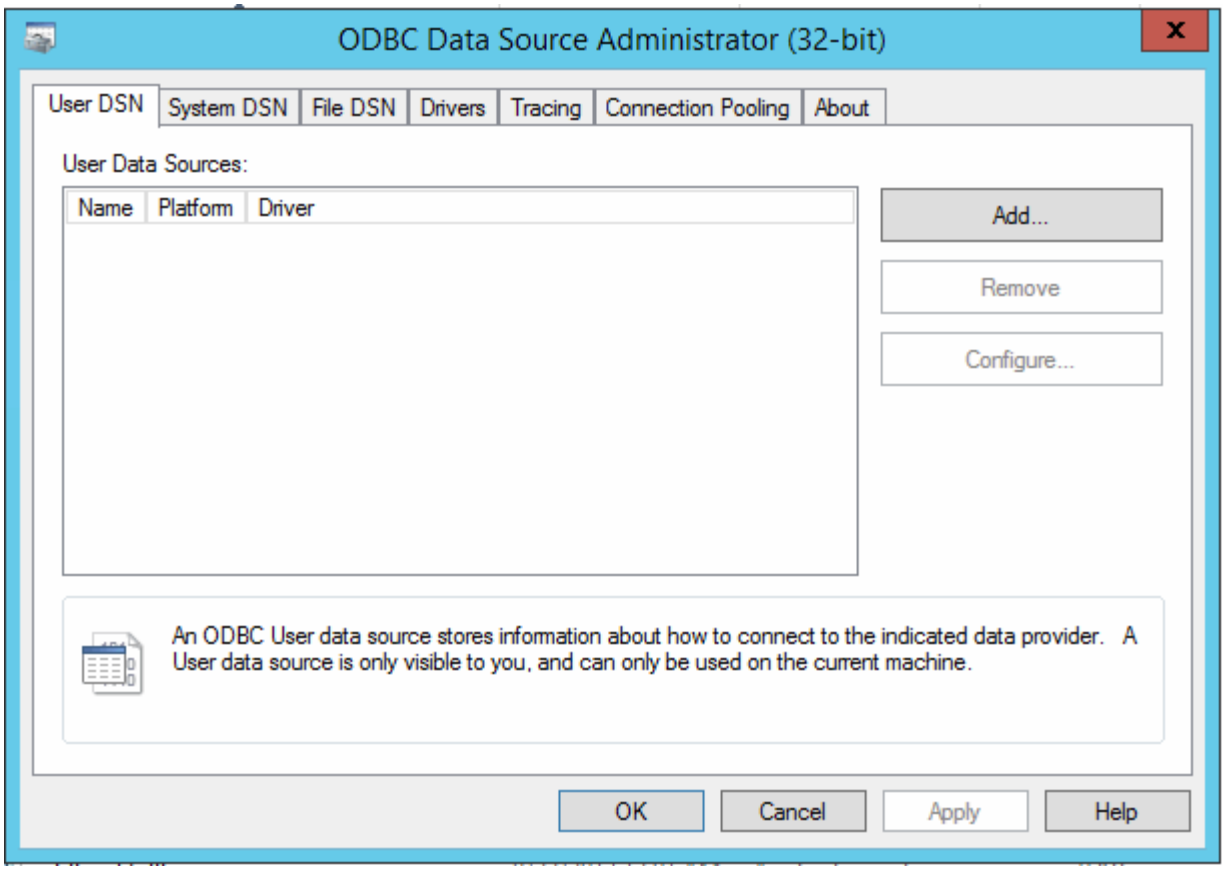
Prima di iniziare

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

Fasi

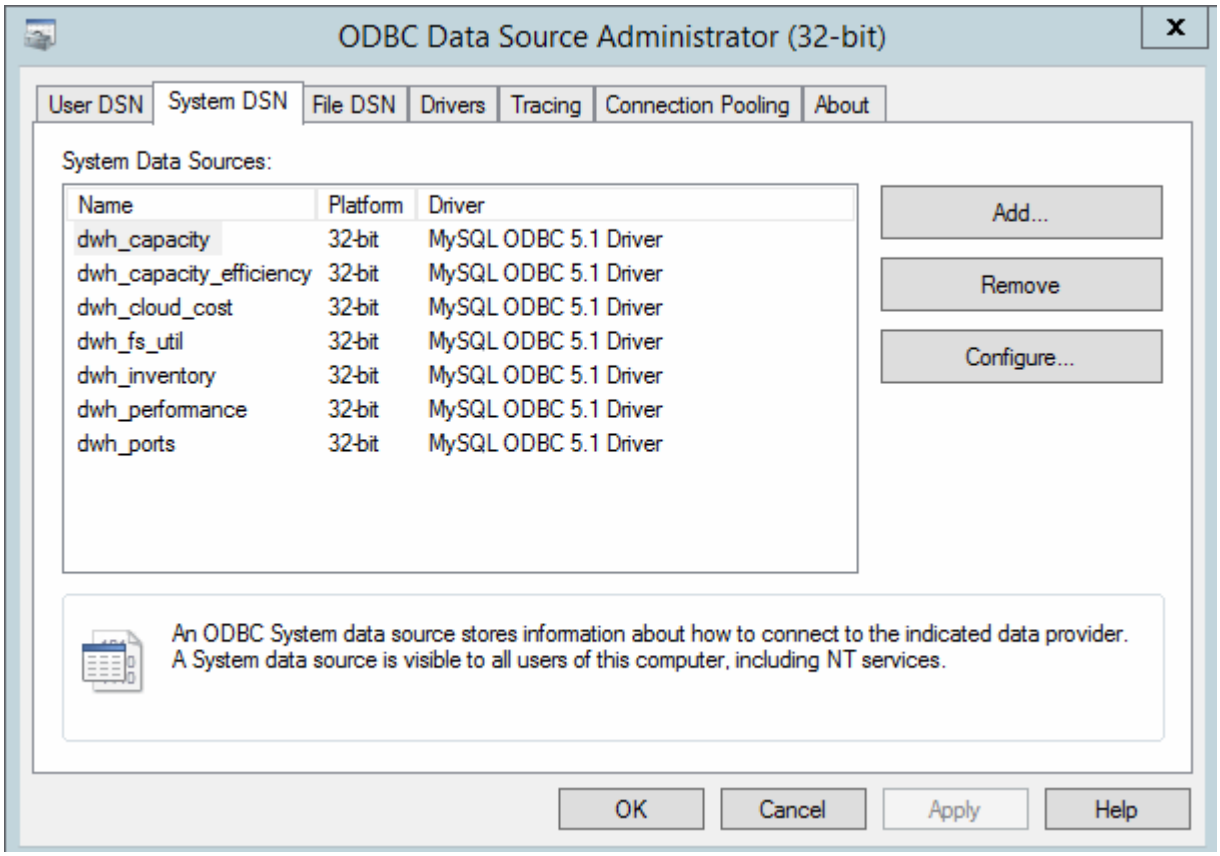
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

   Viene visualizzata la schermata Amministratore origine dati ODBC.



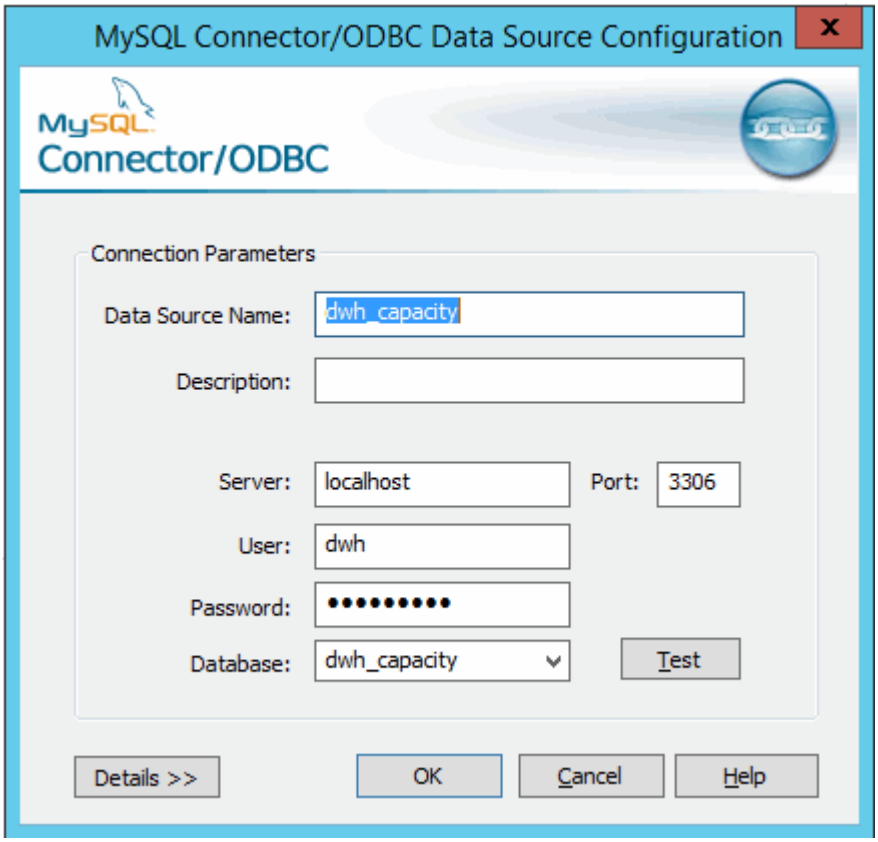
3. Fare clic su **DSN di sistema**

   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.

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.

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 root" esistente in `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
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.

> 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 `keytool` Utility per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      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 (da OnCommand Insight 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommand Insight dalla versione 7.3.5 alla 7.3.9.

> 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 `keytool` Utility per elencare le CA attendibili: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   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: `..\..\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 identificherebbe facilmente la CA in`keytool -list` operazione.

f. Quando viene richiesta una password, immettere `NoPassWordSet`.

g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.

2. Per attivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. Per disattivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 `keytool` Utility per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

   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 identificherebbe facilmente la CA in`keytool -list` operazione.

f. Quando viene richiesta una password, immettere `NoPassWordSet`.

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 da 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommnand Insight dalla versione 7.3.5 alla 7.3.9.

> 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. Creare un backup di `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Creare un backup delle cartelle "certs" e "csk" in `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inviare il file EncryptRequest.csr all'autorità di certificazione (CA) per ottenere un certificato SSL.

   Assicurarsi di aggiungere altri attributi come "SAN:dns=FQDN (ad esempio, hostname.netapp.com)" per aggiungere SubjectAltName). Google Chrome versione 58 e successive si lamenta se SubjectAltName non è presente nel certificato.

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 8c 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 Intermediate.cer con blocco note e copiare il contenuto.
   b. Aprire root.cer con blocco note e salvare il contenuto da 9a.
   c. Salvare il file come CA.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

      In questo modo, CA.cer viene impostato come autorità di certificazione principale.

   c. ThirdPartyCertificateTool.bat -java:local -i -e -r c

      In questo modo, Cognos.cer viene impostato come certificato di crittografia firmato da CA.cer.

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. "D: File di programma/SANscreen/java/bin/keytool.exe" -exportcert -file "c: Temp/cognos.crt" -keystore "D: File di programma/SANscreen/cognos/analytics/Configuration/CAMKeystore" -storetype PKCS12 -storepass NoPassSet -alias Encryption
13. 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. "D: File di programma/SANscreen/java/bin/keytool.exe" -importcert -file "c: Temp/cognos.crt" -keystore "D: File di programma/SANscreen/wildfly/standalone/configurazione/server.trustore" -storepass changeit -alias cognoschert
14. Riavviare il servizio SANscreen.
15. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.

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 NoPassWordSet -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.
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 keytool.exe -exportcert -file c: Temp cognos.crt -keystore cognos/analytics/Configuration/certs/CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias Encryption
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/configurazione/server.trustore -storepass changeit -alias codnos3rdca
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 changeit -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"

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.

> 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 `keytool` Utility per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

   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 (da OnCommand Insight 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommand Insight dalla versione 7.3.5 alla 7.3.9.

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 `keytool` Utility per elencare le CA attendibili: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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: `..\..\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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.
2. Per attivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Per disattivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 `keytool` Utility per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   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 da 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommnand Insight dalla versione 7.3.5 alla 7.3.9.

> 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. Creare un backup di `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.

2. Creare un backup delle cartelle “certs” e “csk” in `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d “CN=FQDN,O=orgname,C=US” -r c:\temp\encryptRequest.csr`
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inviare il file EncryptRequest.csr all’autorità di certificazione (CA) per ottenere un certificato SSL.

   Assicurarsi di aggiungere altri attributi come “SAN:dns=FQDN (ad esempio, hostname.netapp.com)” per aggiungere SubjectAltName). Google Chrome versione 58 e successive si lamenta se SubjectAltName non è presente nel certificato.

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 8c 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 Intermediate.cer con blocco note e copiare il contenuto.
   b. Aprire root.cer con blocco note e salvare il contenuto da 9a.
   c. Salvare il file come CA.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

       In questo modo, CA.cer viene impostato come autorità di certificazione principale.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c

       In questo modo, Cognos.cer viene impostato come certificato di crittografia firmato da CA.cer.

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. "D: File di programma/SANscreen/java/bin/keytool.exe" -exportcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/cognos/analytics/Configuration/CAMKeystore" -storetype PKCS12 -storepass NoPassSet -alias Encryption

13. 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. "D: File di programma/SANscreen/java/bin/keytool.exe" -importcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/wildfly/standalone/configurazione/server.trustore" -storepass changeit -alias cognoschert

14. Riavviare il servizio SANscreen.

15. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.

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 NoPassWordSet -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.
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 keytool.exe -exportcert -file c: Temp cognos.crt -keystore cognos/analytics/Configuration/certs/CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias Encryption

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/configurazione/server.trustore -storepass changeit -alias codnos3rdca

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 changeit -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

> Prima di tentare di eseguire questa procedura, è necessario eseguire il backup di quella esistente `server.keystore` e assegnare un nome al backup `server.keystore.old`. Corrompendo o danneggiando `server.keystore` Dopo il riavvio del server Insight, il file potrebbe causare l'inoperabilità di un server Insight. Se si crea un backup, è possibile ripristinare il file precedente in caso di problemi.

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"`
   a. Quando viene richiesta una password, immettere `changeit`.

   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 Actions 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 + Add 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 + Add.

   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 + Add 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 More 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 More 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.

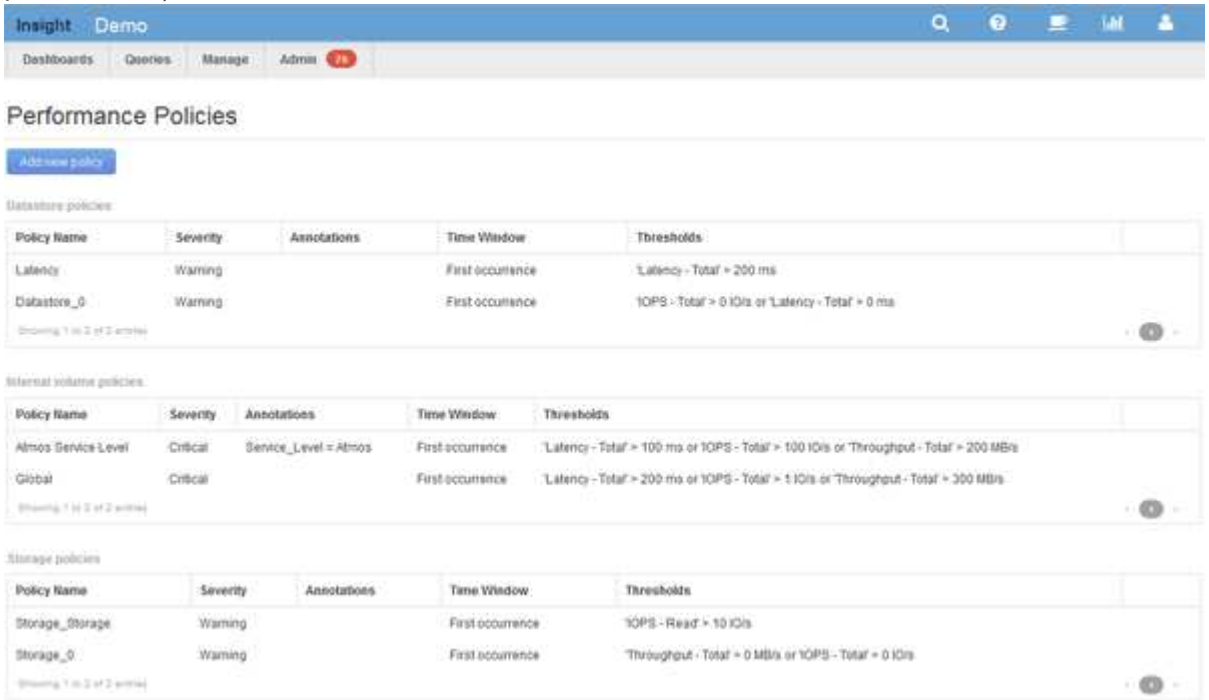
Creazione di policy sulle performance

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.
>
> +

Insight Security

La versione 7.3.1 di OnCommand Insight ha introdotto funzionalità di sicurezza che consentono agli ambienti Insight di funzionare con una maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne e le coppie di chiavi che crittografano e decrittare le password. È possibile gestire queste funzionalità su tutti i server dell'ambiente Insight.

L'installazione predefinita di Insight include una configurazione di sicurezza in cui tutti i siti dell'ambiente condividono le stesse chiavi e le stesse password predefinite. Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente di acquisizione dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono memorizzate nel database di Insight Server. Il server dispone di una chiave pubblica e crittografa le password quando un utente le inserisce in una pagina di

configurazione dell'origine dati WebUI. Il server non dispone delle chiavi private necessarie per decrittare le password dell'origine dati memorizzate nel database del server. Solo le unità di acquisizione (LAU, RAU) dispongono della chiave privata dell'origine dati necessaria per decrittare le password dell'origine dati.

Codifica dei server

L'utilizzo delle chiavi predefinite introduce una vulnerabilità a livello di sicurezza nell'ambiente in uso. Per impostazione predefinita, le password dell'origine dati vengono memorizzate crittografate nel database Insight. Vengono crittografati utilizzando una chiave comune a tutte le installazioni Insight. In una configurazione predefinita, un database Insight inviato a NetApp include password che in teoria potrebbero essere decifrate da NetApp.

Modifica della password utente di acquisizione

L'utilizzo della password utente predefinita "Acquisition" (acquisizione) introduce una vulnerabilità di sicurezza nell'ambiente. Tutte le unità di acquisizione utilizzano l'utente "Acquisition" per comunicare con il server. Raus con password predefinite può in teoria connettersi a qualsiasi server Insight utilizzando password predefinite.

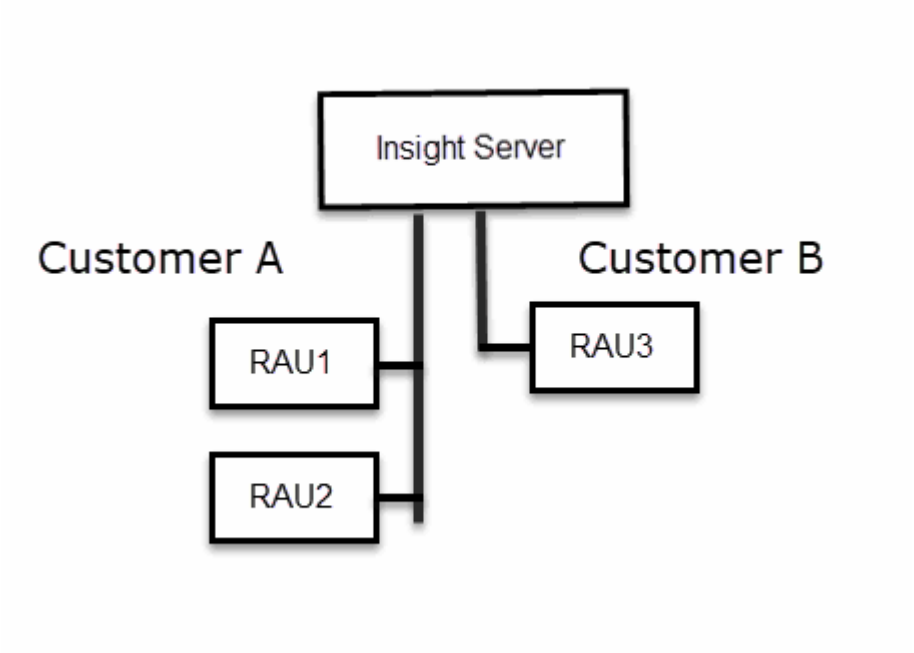
Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (password ridigettate o modificate), è necessario eseguire il backup delle configurazioni di sicurezza. L'installazione di un nuovo software o, in alcuni casi, l'aggiornamento del software ripristina la configurazione di sicurezza predefinita del sistema. Quando il sistema torna alla configurazione predefinita, è necessario ripristinare la configurazione non predefinita per il corretto funzionamento del sistema.

Gestione delle chiavi in un ambiente di service provider complesso

Un service provider può ospitare più clienti OnCommand Insight che raccolgono dati. Le chiavi proteggono i dati dei clienti dall'accesso non autorizzato da parte di più clienti sul server Insight. I dati di ciascun cliente sono protetti dalle coppie di chiavi specifiche.

Questa implementazione di Insight può essere configurata come mostrato nell'illustrazione seguente.



In questa configurazione, è necessario creare singole chiavi per ciascun cliente. Il cliente A richiede chiavi identiche per entrambi i Raus. Il cliente B richiede un singolo set di chiavi.

La procedura da seguire per modificare le chiavi di crittografia per il cliente A:

1. Eseguire un login remoto al server che ospita RAU1.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.
5. Eseguire un login remoto al server che ospita RAU2.
6. Copiare il file zip di backup della configurazione di sicurezza in RAU2.
7. Avviare lo strumento di amministrazione della protezione.
8. Ripristinare il backup di sicurezza da RAU1 al server corrente.

La procedura da seguire per modificare le chiavi di crittografia per il cliente B:

1. Eseguire un login remoto al server che ospita RAU3.
2. Avviare lo strumento di amministrazione della protezione.
3. Selezionare Change Encryption Key (Cambia chiave di crittografia) per sostituire le chiavi predefinite.
4. Selezionare Backup per creare un file zip di backup della configurazione di sicurezza.

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`

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali “Admin”.
4. Selezionare **Server**.

Sono disponibili le seguenti opzioni di configurazione del server:

- **Backup**

  Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

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

- **Ripristina**

  Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

  > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare la chiave di crittografia del server su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

- **Cambia chiave di crittografia**

  Modificare la chiave di crittografia del server utilizzata per crittografare o decrittare le password utente proxy, le password utente SMTP, le password utente LDAP e così via.

  > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

  Modificare la password per gli account interni utilizzati da Insight. Vengono visualizzate le seguenti opzioni:

  - _interno
  - acquisizione
  - cognos_admin
  - dwh_internal
  - host
  - inventario
  - root

> Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

Ripristina i valori predefiniti delle chiavi e delle password. I valori predefiniti sono quelli forniti durante

l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

  a. Scegliere l'opzione che si desidera modificare e seguire le istruzioni.

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`

Fasi

1. Eseguire un accesso remoto al server Insight.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali "Admin".
4. Selezionare **Local Acquisition Unit** (unità di acquisizione locale) per riconfigurare la configurazione di sicurezza dell'unità di acquisizione locale.

   Vengono visualizzate le seguenti opzioni:

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Ripristina**

Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

> Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia sul LAU - creare un backup del vault - ripristinare il backup del vault su ciascuno dei Raus

- **Modifica delle chiavi di crittografia**

  Modificare le chiavi di crittografia AU utilizzate per crittografare o decrittare le password del dispositivo.

  > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Aggiorna password**

  Modificare la password per l'account utente di 'acquisizione'.

  > Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

  Ripristina la password utente di acquisizione e le chiavi di crittografia dell'utente di acquisizione sui valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

5. Scegliere l'opzione che si desidera configurare e seguire le 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 l'aggiornamento della configurazione di sicurezza per LAU, RAU, è quello di aggiornare la

password utente di 'acquisizione' quando la password per quell'utente è stata modificata sul server. Tutti i sistemi Raus e LAU utilizzano la stessa password dell'utente di '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 gestire le opzioni di sicurezza su una RAU, attenersi alla procedura riportata di seguito:

Fasi

1. Eseguire un accesso remoto al server che esegue RAU
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali "Admin".

   Il sistema visualizza il menu della RAU.

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nelle seguenti posizioni predefinite:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`
     - Linux - `/var/log/netapp/oci/backup/vault`
   - **Ripristina**

     Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

     > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server

   - **Modifica delle chiavi di crittografia**

     Modificare le chiavi di crittografia RAU utilizzate per crittografare o decrittare le password del dispositivo.

     > Quando si modificano le chiavi di crittografia, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

   - **Aggiorna password**

     Modificare la password per l'account utente di 'acquisizione'.

> Alcuni account devono essere sincronizzati quando si modificano le password. Ad esempio, se si modifica la password per l'utente di "acquisizione" sul server, è necessario modificare la password per l'utente di "acquisizione" su LAU, RAU e DWH in modo che corrisponda. Inoltre, quando si modificano le password, è necessario eseguire il backup della nuova configurazione di protezione in modo da poterla ripristinare dopo un aggiornamento o un'installazione.

- **Ripristina impostazioni predefinite**

  Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

- **Esci**

  Uscire da `securityadmin` tool.

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`

Fasi

1. Eseguire un login remoto al server Data Warehouse.
2. Avviare lo strumento di amministrazione della protezione in modalità interattiva:
   - Finestre - `C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i`
   - Linux - `/bin/oci-securityadmin.sh -i`

     Il sistema richiede le credenziali di accesso.
3. Immettere il nome utente e la password di un account con credenziali "Admin".

   Il sistema visualizza il menu Security admin per Data Warehouse:

   - **Backup**

     Crea un file zip di backup del vault contenente tutte le password e le chiavi e colloca il file in una posizione specificata dall'utente o nella posizione predefinita:

     - Finestre - `C:\Program Files\SANscreen\backup\vault`

    - Linux - `/var/log/netapp/oci/backup/vault`

  - **Ripristina**

    Ripristina il backup zip del vault creato. Una volta ripristinato, tutte le password e le chiavi vengono ripristinate ai valori esistenti al momento della creazione del backup.

    > Il ripristino può essere utilizzato per sincronizzare password e chiavi su più server, ad esempio: - Modificare le chiavi di crittografia su un server - creare un backup del vault - ripristinare il backup del vault sul secondo server
    >
    > +

  - **Modificare le chiavi di crittografia**

    Modificare la chiave di crittografia DWH utilizzata per crittografare o decrittare password come le password del connettore e le password SMPT.

  - **Aggiorna password**

    Modificare la password per un account utente specifico.

    - _interno
    - acquisizione
    - cognos_admin
    - dwh
    - dwh_internal
    - dwhuser
    - host
    - inventario
    - root

    > Quando si modificano le password di dwhuser, host, inventario o root, è possibile utilizzare l'hashing delle password SHA-256. Questa opzione richiede che tutti i client che accedono agli account utilizzino connessioni SSL.

+

  - **Ripristina impostazioni predefinite**

    Ripristina le chiavi di crittografia e le password ai valori predefiniti. I valori predefiniti sono quelli forniti durante l'installazione.

  - **Esci**

    Uscire da `securityadmin` tool.

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.

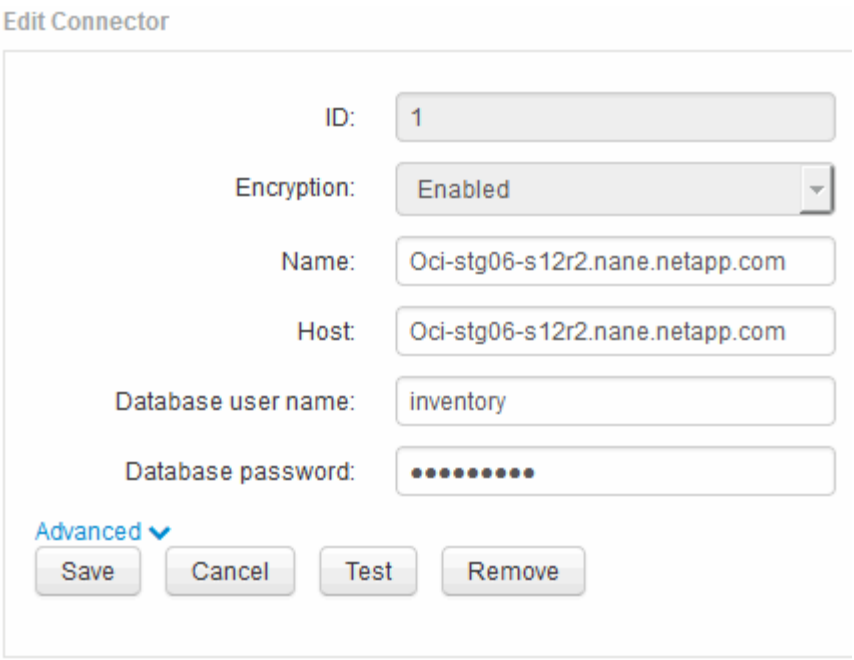
Prima di iniziare

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

Fasi

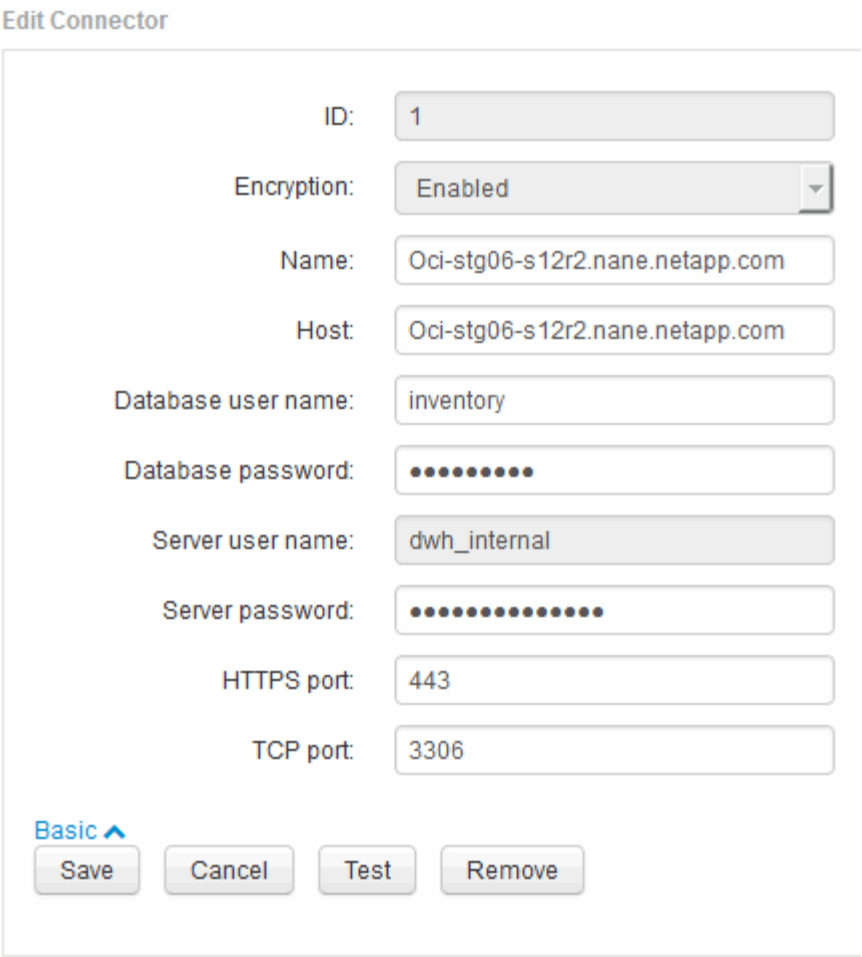
1. Accedere al Data Warehouse Portal all'indirizzo https://hostname/dwh, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

   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.

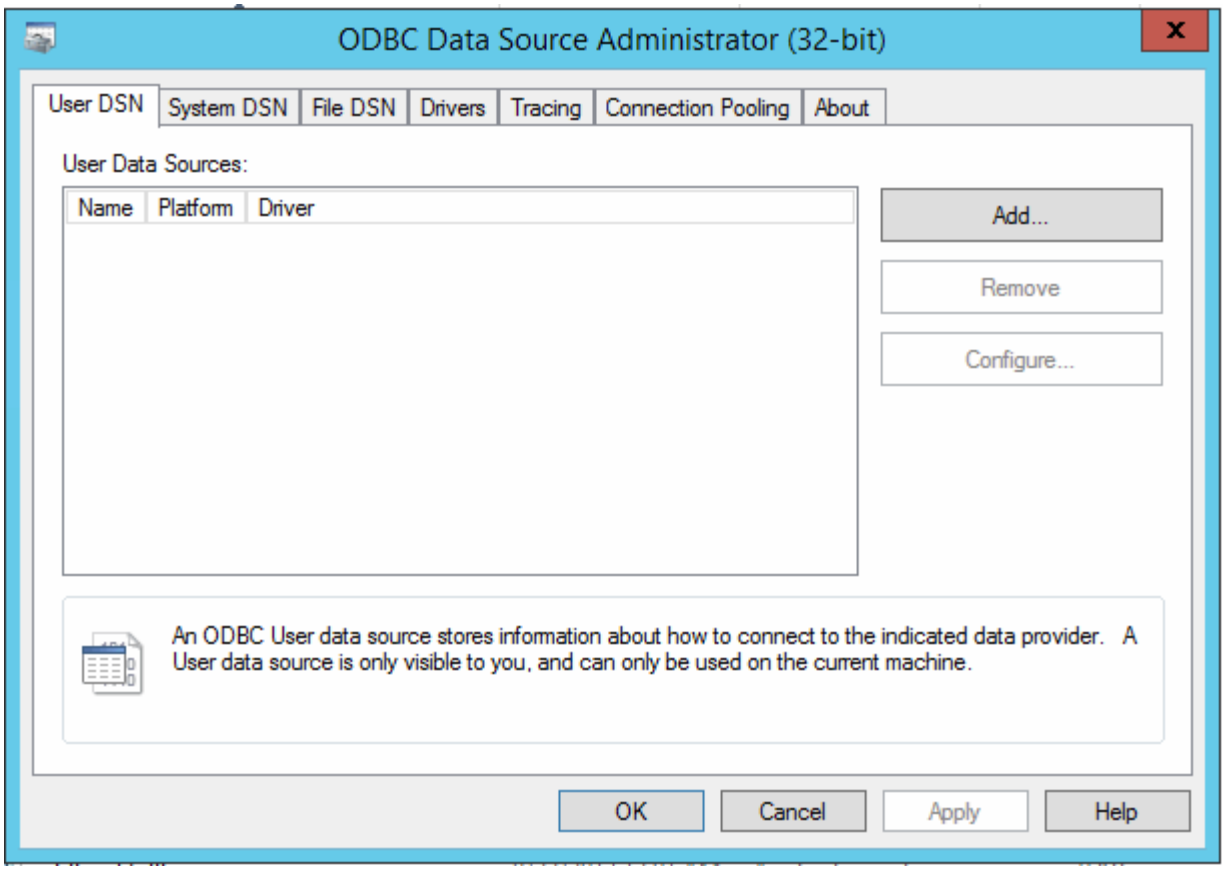
Prima di iniziare

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

Fasi

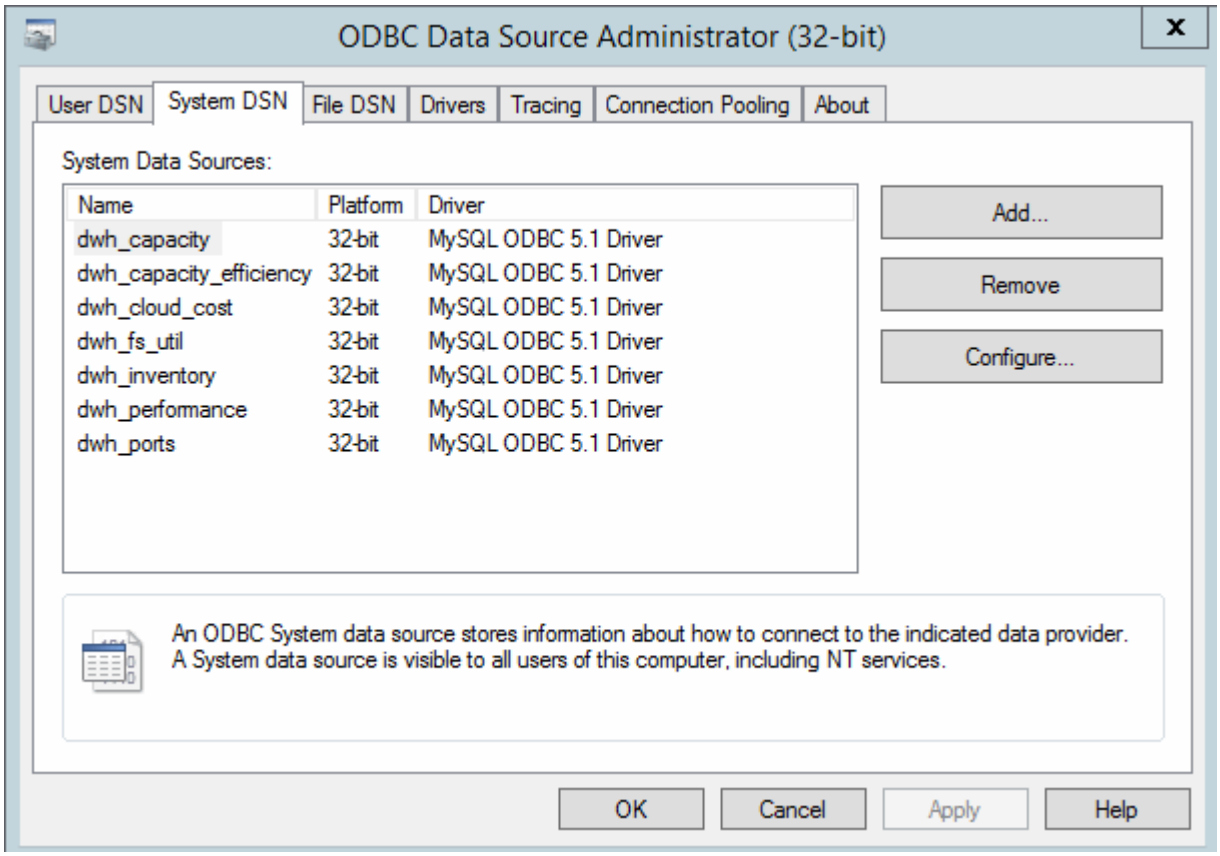
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

   Viene visualizzata la schermata Amministratore origine dati ODBC.



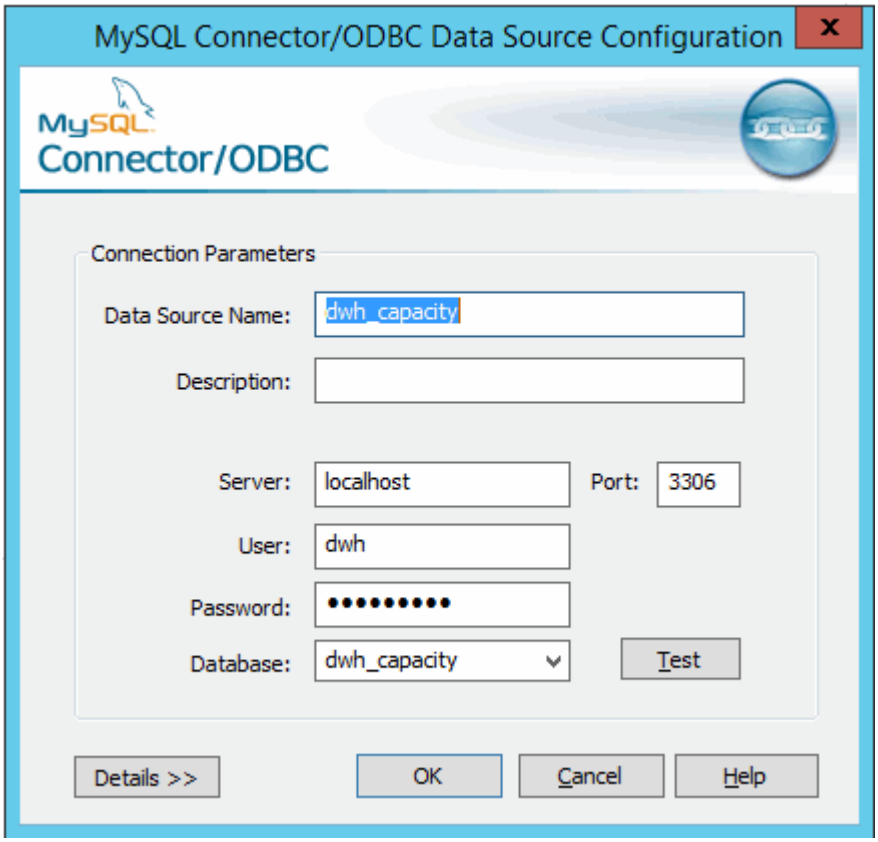
3. Fare clic su **DSN di sistema**

   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.

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.

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 root" esistente in `/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
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.

> 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 `keytool` Utility per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      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 (da OnCommand Insight 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommand Insight dalla versione 7.3.5 alla 7.3.9.

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 `keytool` Utility per elencare le CA attendibili: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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: `..\..\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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.
2. Per attivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Per disattivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 `keytool` Utility per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   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 da 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommnand Insight dalla versione 7.3.5 alla 7.3.9.

> 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. Creare un backup di `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Creare un backup delle cartelle "certs" e "csk" in `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inviare il file EncryptRequest.csr all'autorità di certificazione (CA) per ottenere un certificato SSL.

   Assicurarsi di aggiungere altri attributi come "SAN:dns=FQDN (ad esempio, hostname.netapp.com)" per aggiungere SubjectAltName). Google Chrome versione 58 e successive si lamenta se SubjectAltName non è presente nel certificato.

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 8c 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 Intermediate.cer con blocco note e copiare il contenuto.
   b. Aprire root.cer con blocco note e salvare il contenuto da 9a.
   c. Salvare il file come CA.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

       In questo modo, CA.cer viene impostato come autorità di certificazione principale.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c

       In questo modo, Cognos.cer viene impostato come certificato di crittografia firmato da CA.cer.

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. "D: File di programma/SANscreen/java/bin/keytool.exe" -exportcert -file "c: Temp/cognos.crt" -keystore "D: File di programma/SANscreen/cognos/analytics/Configuration/CAMKeystore" -storetype PKCS12 -storepass NoPassSet -alias Encryption
13. 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. "D: File di programma/SANscreen/java/bin/keytool.exe" -importcert -file "c: Temp/cognos.crt" -keystore "D: File di programma/SANscreen/wildfly/standalone/configurazione/server.trustore" -storepass changeit -alias cognoschert
14. Riavviare il servizio SANscreen.
15. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.

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 NoPassWordSet -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.
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 keytool.exe -exportcert -file c: Temp cognos.crt -keystore cognos/analytics/Configuration/certs/CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias Encryption
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/configurazione/server.trustore -storepass changeit -alias codnos3rdca
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 changeit -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"

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.

> 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 `keytool` Utility per elencare le CA attendibili: `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit`

      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 (da OnCommand Insight 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommand Insight dalla versione 7.3.5 alla 7.3.9.

> 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 `keytool` Utility per elencare le CA attendibili: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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: `..\..\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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   g. Risposta `yes` quando viene richiesto di considerare attendibile il certificato.
2. Per attivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
3. Per disattivare la modalità CAC, eseguire `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

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 `keytool` Utility per elencare le CA attendibili: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

      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 identificherebbe facilmente la CA in`keytool -list` operazione.
   f. Quando viene richiesta una password, immettere `NoPassWordSet`.
   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 da 7.3.5 a 7.3.9)

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 si applica ai sistemi che eseguono OnCommnand Insight dalla versione 7.3.5 alla 7.3.9.

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. Creare un backup di `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. Creare un backup delle cartelle "certs" e "csk" in `..\SANScreen\cognos\analytics\configuration`.
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 NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. Aprire `c:\temp\encryptRequest.csr` archiviare e copiare il contenuto generato.
5. Inviare il file EncryptRequest.csr all'autorità di certificazione (CA) per ottenere un certificato SSL.

   Assicurarsi di aggiungere altri attributi come "SAN:dns=FQDN (ad esempio, hostname.netapp.com)" per aggiungere SubjectAltName). Google Chrome versione 58 e successive si lamenta se SubjectAltName non è presente nel certificato.

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 8c 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 Intermediate.cer con blocco note e copiare il contenuto.
   b. Aprire root.cer con blocco note e salvare il contenuto da 9a.
   c. Salvare il file come CA.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

       In questo modo, CA.cer viene impostato come autorità di certificazione principale.

    c. ThirdPartyCertificateTool.bat -java:local -i -e -r c

       In questo modo, Cognos.cer viene impostato come certificato di crittografia firmato da CA.cer.
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. "D: File di programma/SANscreen/java/bin/keytool.exe" -exportcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/cognos/analytics/Configuration/CAMKeystore" -storetype PKCS12 -storepass NoPassSet -alias Encryption
13. 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. "D: File di programma/SANscreen/java/bin/keytool.exe" -importcert -file “c: Temp/cognos.crt” -keystore "D: File di programma/SANscreen/wildfly/standalone/configurazione/server.trustore" -storepass changeit -alias cognoschert
14. Riavviare il servizio SANscreen.
15. Eseguire un backup di DWH per assicurarsi che DWH comunichi con Cognos.

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 NoPassWordSet -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.
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 keytool.exe -exportcert -file c: Temp cognos.crt -keystore cognos/analytics/Configuration/certs/CAMKeystore -storetype PKCS12 -storepass NoPassWordSet -alias Encryption
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/configurazione/server.trustore -storepass changeit -alias codnos3rdca
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 changeit -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

> Prima di tentare di eseguire questa procedura, è necessario eseguire il backup di quella esistente `server.keystore` e assegnare un nome al backup `server.keystore.old`. Corrompendo o danneggiando `server.keystore` Dopo il riavvio del server Insight, il file potrebbe causare l'inoperabilità di un server Insight. Se si crea un backup, è possibile ripristinare il file precedente in caso di problemi.

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"`

   a. Quando viene richiesta una password, immettere `changeit`.

   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.

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 Actions 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 + Add 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 + Add.

   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 + Add 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 More 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 More 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 origini dati Insight

Le origini dati sono il componente più critico utilizzato per la manutenzione di un ambiente OnCommand Insight. Poiché sono la principale fonte di informazioni per Insight, è fondamentale mantenere le origini dati in uno stato di esecuzione.

È possibile monitorare le origini dati nella rete selezionando un'origine dati per controllare gli eventi relativi al relativo stato e annotando eventuali modifiche che potrebbero aver causato problemi.

Oltre a esaminare una singola origine dati, è possibile eseguire le seguenti operazioni:

- Clonare un'origine dati per creare molte origini dati simili in Insight
- Modificare le informazioni dell'origine dati
- Modificare le credenziali
- Polling del controllo
- Eliminare l'origine dati
- Installare le patch di origine dei dati
- Installare una nuova origine dati da una patch
- Preparare un report degli errori per il supporto clienti NetApp

Configurazione delle origini dati in Insight

Le origini dati sono il componente più critico quando si tenta di mantenere un ambiente Insight. Le origini dati rilevano le informazioni di rete utilizzate per l'analisi e la convalida. È necessario configurare le origini dati in Insight in modo che possano essere monitorate all'interno della rete.

Per ciascuna origine dati, i requisiti specifici per definire l'origine dati dipendono dal vendor e dal modello dei dispositivi corrispondenti. Prima di aggiungere le origini dati, è necessario disporre di indirizzi di rete, informazioni sull'account e password per tutti i dispositivi e, eventualmente, di questi dettagli aggiuntivi:

- Switch
- Stazioni di gestione dei dispositivi

- Sistemi storage dotati di connettività IP
- Stazioni di gestione dello storage
- Server host che eseguono software di gestione per dispositivi storage che non dispongono di connettività IP

Per ulteriori informazioni sulle definizioni delle origini dati, vedere le informazioni "riferimento alle origini dati specifiche del vendor" in questa sezione.

Informazioni di supporto dell'origine dati

Nell'ambito della pianificazione della configurazione, è necessario assicurarsi che i dispositivi nel proprio ambiente possano essere monitorati da Insight. A tale scopo, è possibile consultare la matrice di supporto dell'origine dati per informazioni dettagliate su sistemi operativi, dispositivi specifici e protocolli. Alcune origini dati potrebbero non essere disponibili su tutti i sistemi operativi.

Posizione della versione più aggiornata della matrice di supporto Data Source

La matrice di supporto origine dati OnCommand Insight viene aggiornata con ogni release di service pack. La versione più recente del documento è disponibile nella "Sito di supporto NetApp". .

Aggiunta di origini dati

È possibile aggiungere rapidamente origini dati utilizzando la finestra di dialogo Aggiungi origine dati.

Fasi

1. Aprire OnCommand Insight nel browser e accedere come utente con autorizzazioni amministrative.
2. Selezionare **Admin** e scegliere **origini dati**.
3. Fare clic sul pulsante **+Aggiungi**.

   Viene visualizzata la procedura guidata Add data source (Aggiungi origine dati).

4. Nella sezione **Impostazioni**, immettere le seguenti informazioni:

Campo	Descrizione
Nome	Immettere un nome di rete univoco per questa origine dati. NOTA: Nel nome dell'origine dati sono consentiti solo lettere, numeri e il carattere di sottolineatura (_).
Vendor	Scegliere il vendor dell'origine dati dal menu a discesa.
Modello	Scegliere il modello dell'origine dati dal menu a discesa.

Dove correre	Scegliere locale oppure scegliere un'unità di acquisizione remota se le RAU sono configurate nell'ambiente in uso.
Cosa raccogliere	Per la maggior parte delle origini dati, queste opzioni saranno inventario e prestazioni. L'inventario è sempre selezionato per impostazione predefinita e non può essere deselezionato. Si noti che alcune origini dati potrebbero avere opzioni diverse. Le opzioni di raccolta selezionate modificano i campi disponibili nelle sezioni Configurazione e Configurazione avanzata.

5. Fare clic sul collegamento **Configuration** (Configurazione) e immettere le informazioni di configurazione di base richieste per l'origine dati con il tipo di raccolta dati selezionato.
6. Se questo tipo di origine dati richiede di solito informazioni più dettagliate per la configurazione nella rete, fare clic sul collegamento **Advanced Configuration** (Configurazione avanzata) per inserire ulteriori informazioni.
7. Per ulteriori informazioni sulla configurazione o sulle informazioni di configurazione avanzate richieste o disponibili per l'origine dati specifica, consultare la "Riferimento all'origine dati specifica del vendor".
8. Fare clic sul collegamento **Test** per verificare che l'origine dati sia configurata correttamente.
9. Fare clic su **Save** (Salva).

Importazione di origini dati da un foglio di calcolo

È possibile importare più origini dati in OnCommand Insight da un foglio di calcolo. Questo potrebbe essere utile se si mantengono già le periferiche di rilevamento in un foglio di calcolo. Questo processo aggiunge nuove origini dati, ma non può essere utilizzato per aggiornare le origini dati esistenti.

A proposito di questa attività

OnCommand Insight include un foglio di calcolo che consente di creare origini dati. Questo foglio di calcolo presenta i seguenti attributi:

- Il foglio di calcolo può essere utilizzato con Microsoft Excel 2003 o versioni successive.
- Ciascuna scheda contiene un tipo di origine dati, ad esempio Brocade SSH/CLI.
- Ogni riga rappresenta un'istanza di una nuova origine dati da creare.

Il foglio di calcolo include una macro che crea una nuova origine dati in OnCommand Insight.

Fasi

1. Individuare il foglio di calcolo in `<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip`.
2. Nel foglio di calcolo, inserire le informazioni relative all'origine dei dati nelle celle a colori.
3. Elimina righe vuote.

4. Dal foglio di calcolo, eseguire `CreateDataSources` macro per creare le origini dati.
5. Quando vengono richieste le credenziali, immettere il nome utente e la password di amministrazione del server OnCommand Insight.

   I risultati vengono registrati nel registro di acquisizione.

6. Viene visualizzato un messaggio che chiede se sul computer che esegue la macro è installato OnCommand Insight.

   Selezionare una delle seguenti opzioni:

   - No: Selezionare "No" se viene creato un file batch che deve essere eseguito sulla macchina OnCommand Insight. Eseguire questo file batch dalla directory di installazione.
   - Sì: Selezionare "Sì" se OnCommand Insight è già installato e non sono necessari ulteriori passaggi per generare le informazioni sull'origine dati.
7. Per verificare l'aggiunta delle origini dati, aprire Insight nel browser.
8. Nella barra degli strumenti Insight, fare clic su **Admin**.
9. Controllare l'elenco origini dati per le origini dati importate.

Aggiunta di una nuova origine dati tramite patch

Le nuove origini dati vengono rilasciate come file di patch che possono essere caricati nel sistema utilizzando il processo di patch. Questo processo consente di rendere disponibili nuove origini dati tra le release pianificate di OnCommand Insight.

Prima di iniziare

È necessario aver caricato il file di patch che si desidera installare.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Selezionare **Patch**.
3. Selezionare **azioni** > **Installa service pack o patch**.
4. Nella finestra di dialogo **Installa Service Pack o Patch**, fare clic su **Sfoglia** per individuare e selezionare il file di patch caricato.
5. Fare clic su **Avanti** nella finestra di dialogo **Riepilogo patch**.
6. Esaminare le informazioni **Leggimi** e fare clic su **Avanti** per continuare.
7. Nella finestra di dialogo **Installa**, fare clic su **fine**.

Clonazione di un'origine dati

Utilizzando la funzione di clonazione, è possibile aggiungere rapidamente un'origine dati con le stesse credenziali e attributi di un'altra origine dati. La clonazione consente di configurare facilmente più istanze dello stesso tipo di dispositivo.

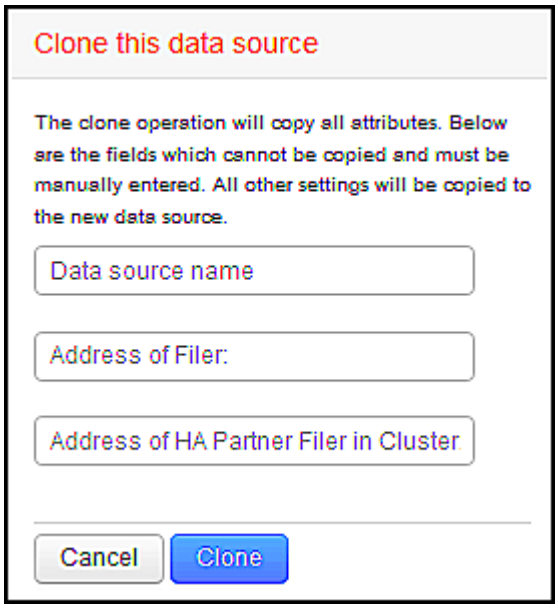
Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.

   Viene visualizzato l'elenco origini dati.

2. Evidenziare l'origine dati con le informazioni di configurazione che si desidera utilizzare per la nuova origine dati.
3. A destra dell'origine dati evidenziata, fare clic sull'icona **Clone**.

   La finestra di dialogo Clone this data source (Clona questa origine dati) elenca le informazioni da fornire per l'origine dati selezionata, come mostrato in questo esempio per un'origine dati NetApp:



4. Inserire le informazioni richieste nei campi; tali informazioni non possono essere copiate dall'origine dati esistente.
5. Fare clic su **Clone**.

Risultati

L'operazione di clonazione copia tutti gli altri attributi e impostazioni per creare la nuova origine dati.

Verifica della configurazione dell'origine dati

Quando si aggiunge un'origine dati, è possibile verificare la correttezza della configurazione per comunicare con il dispositivo prima di salvare o aggiornare tale origine dati.

Quando si fa clic sul pulsante **Test** nella procedura guidata origine dati, viene selezionata la comunicazione con il dispositivo specificato. Il test produce uno dei seguenti risultati:

- SUPERATO: L'origine dati è configurata correttamente.
- ATTENZIONE: Il test è stato incompleto, probabilmente a causa del timeout durante l'elaborazione o dell'acquisizione non in esecuzione.
- ERRORE: L'origine dati, come configurata, non può comunicare con il dispositivo specificato. Controllare le

impostazioni di configurazione e ripetere il test.

Riferimento all'origine dati specifica del vendor

I dettagli della configurazione variano a seconda del vendor e del modello dell'origine dati da aggiungere.

Se l'origine dati di un vendor richiede istruzioni di configurazione avanzate di Insight, come requisiti speciali e comandi specifici, tali informazioni sono incluse in questa sezione.

Origine dati InServ 3PAR

OnCommand Insight utilizza l'origine dati 3PAR InServ (firmware 2.2.2+, SSH) per rilevare l'inventario degli storage array HP 3PAR StoreServ.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati InServ 3PAR. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco fisico	Disco
Sistema storage	Storage
Nodo controller	Nodo di storage
Gruppo di provisioning comune	Pool di storage
Volume virtuale	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP o FQDN del cluster InServ
- Per l'inventario, nome utente e password di sola lettura per InServ Server.
- Per le performance, leggere e scrivere nome utente e password su InServ Server.
- Requisiti delle porte: 22 (inventario), 5988 o 5989 (performance collection) [Nota: 3PAR Performance is supported for InServ OS 3.x+]
- Per la raccolta delle performance, verificare che SMI-S sia abilitato effettuando l'accesso all'array 3PAR tramite SSH.

Configurazione

Campo	Descrizione
IP del cluster	Indirizzo IP o nome di dominio completo del cluster InServ
Nome utente	Nome utente del server InServ
Password	Password utilizzata per il server InServ
IP HOST SMI-S.	Indirizzo IP dell'host del provider SMI-S.
Nome utente SMI-S.	Nome utente dell'host del provider SMI-S.
Password SMI-S.	Password utilizzata per l'host del provider SMI-S.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Escludi dispositivi	Elenco separato da virgole degli IP delle periferiche da escludere
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 60 secondi)
Numero di tentativi SSH	Numero di tentativi SSH
Timeout attesa banner SSH (sec)	Timeout di attesa banner SSH (impostazione predefinita: 20 secondi)
Porta SMI-S.	Porta utilizzata dall'host del provider SMI-S.
Protocollo	Protocollo utilizzato per connettersi al provider SMI-S.
Spazio dei nomi SMI-S.	Spazio dei nomi SMI-S.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Numero di tentativi di connessione SMI-S.	Numero di tentativi di connessione SMI-S.

Fonte dati Amazon AWS EC2

OnCommand Insight utilizza questa origine dati per rilevare l'inventario e le performance di Amazon AWS EC2.

Prerequisiti:

Per raccogliere dati dai dispositivi Amazon EC2, devi disporre delle seguenti informazioni:

- È necessario disporre dell'ID della chiave di accesso IAM
- Devi disporre della chiave di accesso segreta per il tuo account cloud Amazon EC2
- È necessario disporre del privilegio "list organization"
- Porta 433 HTTPS
- Le istanze di EC2 possono essere segnalate come macchina virtuale o (meno naturalmente) come host. I volumi EBS possono essere riportati sia come VirtualDisk utilizzato dalla macchina virtuale, sia come datastore che fornisce la capacità per VirtualDisk.

Le chiavi di accesso sono costituite da un ID della chiave di accesso (ad esempio, AKIAIOSFONN7EXAMPLE) e da una chiave di accesso segreta (ad esempio, wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY). Le chiavi di accesso vengono utilizzate per firmare le richieste programmatiche inviate a EC@ se si utilizzano le operazioni Amanzon EC2 SDK, REST o Query API. Queste chiavi vengono fornite con il contratto di Amazon.

Come configurare questa origine dati

Per configurare l'origine dati Amazon AWS EC2, sono necessari l'ID della chiave di accesso AWS IAM e la chiave di accesso segreta per l'account AWS.

Compilare i campi dell'origine dati in base alle tabelle seguenti:

Configurazione:

Campo	Descrizione
Regione AWS	Scegliere la regione AWS
Ruolo IAM	Da utilizzare solo se acquisito su un AU in AWS. Per ulteriori informazioni sui ruoli IAM, consulta la sezione riportata di seguito.
ID chiave di accesso AWS IAM	Inserire l'ID della chiave di accesso AWS IAM. Obbligatorio se non si utilizza il ruolo IAM.
Chiave di accesso segreta AWS IAM	Immettere la chiave di accesso segreta AWS IAM. Obbligatorio se non si utilizza il ruolo IAM.
Sono consapevole che AWS mi fatturerà per le richieste API	Controllare questa opzione per verificare che AWS ti presenti la fattura per le richieste API effettuate tramite il polling Insight

Configurazione avanzata:

Campo	Descrizione
Includi aree geografiche aggiuntive	Specificare aree aggiuntive da includere nel polling.
Ruolo multiaccount	Ruolo per l'accesso alle risorse in diversi account AWS.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Timeout connessione HTTP e socket (sec)	Timeout connessione HTTP (impostazione predefinita: 300 secondi)
Includere tag AWS	Selezionare questa opzione per abilitare il supporto dei tag AWS nelle annotazioni Insight
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 1800 secondi)

Mappatura dei tag AWS alle annotazioni Insight

L'origine dati AWS EC2 include un'opzione che consente di popolare le annotazioni Insight con tag configurati su AWS. Le annotazioni devono essere denominate esattamente come i tag AWS. Insight popolerà sempre le annotazioni di tipo testo con lo stesso nome e farà un "miglior tentativo" di popolare le annotazioni di altri tipi (numero, booleano, ecc.). Se l'annotazione è di tipo diverso e l'origine dati non riesce a compilarla, potrebbe essere necessario rimuovere l'annotazione e ricrearla come tipo di testo.

Si noti che AWS fa distinzione tra maiuscole e minuscole, mentre Insight non fa distinzione tra maiuscole e minuscole. Pertanto, se si crea un'annotazione denominata "OWNER" in Insight e i tag denominati "OWNER", "Owner" e "Owner" in AWS, tutte le variazioni AWS di "Owner" verranno mappate all'annotazione "OWNER" di Insight.

Informazioni correlate:

"Gestione delle chiavi di accesso per gli utenti IAM"

Includi aree geografiche aggiuntive

Nella sezione AWS Data Collector **Advanced Configuration**, è possibile impostare il campo **include extra regions** in modo da includere regioni aggiuntive, separate da virgola o punto e virgola. Per impostazione predefinita, questo campo è impostato su ***us-.****, che raccoglie su tutte le regioni US AWS. Per eseguire la raccolta su *tutte* regioni, impostare questo campo su ***.****.

Se il campo **include extra regions** è vuoto, il data collector raccoglierà le risorse specificate nel campo **AWS Region** come specificato nella sezione **Configuration**.

Raccolta da account secondari AWS

Insight supporta la raccolta di account figlio per AWS all'interno di un singolo data collector AWS. La configurazione per questa raccolta viene eseguita nell'ambiente AWS:

- È necessario configurare ciascun account figlio in modo che disponga di un ruolo AWS che consenta all'ID account primario di accedere ai dettagli EC2 dall'account figlio.
- Ogni account figlio deve avere il nome del ruolo configurato come la stessa stringa
- Inserire questa stringa di nome ruolo nella sezione Insight AWS Data Collector **Advanced Configuration**, nel campo **Cross account role**.

Best practice: Si consiglia vivamente di assegnare il criterio AWS predefinito AmazonEC2ReadOnlyAccess all'account primario ECS. Inoltre, l'utente configurato nell'origine dati deve avere almeno il *AWSOrganizationsReadOnlyAccess*policy predefinito assegnato, per eseguire query su AWS.

Per informazioni sulla configurazione dell'ambiente in modo da consentire a Insight di raccogliere dagli account figlio AWS, consultare quanto segue:

"Esercitazione: Delegare l'accesso tra gli account AWS utilizzando i ruoli IAM"

"Configurazione AWS: Accesso a un utente IAM in un altro account AWS di proprietà dell'utente"

"Creazione di un ruolo per delegare le autorizzazioni a un utente IAM"

Ruoli IAM

Quando si utilizza la protezione di *ruolo* IAM, è necessario assicurarsi che il ruolo creato o specificato disponga delle autorizzazioni appropriate necessarie per accedere alle risorse.

Ad esempio, se si crea un ruolo IAM denominato *InstanceEC2ReadOnly*, è necessario impostare il criterio per concedere l'autorizzazione di accesso in sola lettura a tutte le risorse EC2 per questo ruolo IAM. Inoltre, è necessario concedere l'accesso a STS (Security Token Service) in modo che questo ruolo possa assumere ruoli diversi account.

Dopo aver creato un ruolo IAM, è possibile allegarlo quando si crea una nuova istanza EC2 o un'istanza EC2 esistente.

Dopo aver associato il ruolo IAM *InstanceEc2ReadOnly* a un'istanza EC2, sarà possibile recuperare la credenziale temporanea attraverso i metadati dell'istanza in base al nome del ruolo IAM e utilizzarla per accedere alle risorse AWS da qualsiasi applicazione in esecuzione su questa istanza EC2.

> Il ruolo IAM può essere utilizzato solo quando l'unità di acquisizione è in esecuzione in un'istanza AWS.

Fonte dei dati Brocade Enterprise Fabric Connectivity Manager

OnCommand Insight utilizza l'origine dati di Brocade Enterprise Fabric Connectivity Manager (EFCM) per rilevare l'inventario degli switch Brocade EFCM. Insight supporta le versioni EFCM 9.5, 9.6 e 9.7.

Requisiti

> Questo data collector non è disponibile a partire da OnCommand Insight 7.3.11.

- Indirizzo di rete o nome di dominio completo per il server EFCM
- La versione dell'EFCM deve essere 9.5, 9.6 o 9.7

- Indirizzo IP del server EFCM
- Nome utente e password di sola lettura per il server EFCM
- Accesso convalidato allo switch Connectrix da Telnet dal server Insight, utilizzando il nome utente e la password di sola lettura sulla porta 51512

Configurazione

Campo	Descrizione
Server EFC	Indirizzo IP o nome di dominio completo del server EFC
Nome utente	Nome utente dello switch
Password	Password utilizzata per lo switch

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 15 minuti)
Nome fabric	Nome del fabric che deve essere segnalato dall'origine dati EFCM. Lasciare vuoto per riportare il nome del fabric come WWN.
Porta di comunicazione	Porta utilizzata per la comunicazione con lo switch
Attivare il trapping	Selezionare questa opzione per abilitare l'acquisizione alla ricezione di una trap SNMP dal dispositivo. Se si seleziona enable trapping (attiva trap), è necessario attivare anche SNMP.
Tempo minimo tra trap (sec)	Tempo minimo tra i tentativi di acquisizione attivati da trap (impostazione predefinita: 15 secondi)
Zonesets inattivi	Elenco separato da virgole di zone inattive su cui eseguire l'acquisizione, oltre a eseguire l'acquisizione sui set di zone attive
NIC da utilizzare	Specificare l'interfaccia di rete da utilizzare sulla RAU quando si esegue la creazione di report sui dispositivi SAN
Escludi dispositivi	Elenco separato da virgole dei nomi di unità da includere o escludere dal polling

Utilizzare il nome alternativo dello switch EFCM come nome dello switch Insight	Selezionare per utilizzare il nome alternativo dello switch EFCM come nome dello switch Insight
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Origine dati dello switch FC Brocade

OnCommand Insight utilizza l'origine dati dello switch FC Brocade (SSH) per rilevare l'inventario dei dispositivi switch Brocade o rebranded con firmware FOS 4.2 e versioni successive. Sono supportati i dispositivi in entrambe le modalità switch FC e Access Gateway.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati dello switch FC Brocade. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Switch	Switch
Porta	Porta
Fabric virtuale, fabric fisico	Fabric
Zona	Zona
Switch logico	Switch logico
Zona LSAN	Zona IVR

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- L'unità di acquisizione (locale o remota) avvia le connessioni alla porta TCP 22 sugli switch Brocade per raccogliere i dati di inventario. L'AU avvierà inoltre le connessioni alla porta UDP 161 per la raccolta dei dati sulle prestazioni.
- Deve essere presente una connettività IP a tutti gli switch del fabric. Se si seleziona la casella di controllo Discover All switch in the Fabric (rileva tutti gli switch nel fabric), OCI identifica tutti gli switch nel fabric; tuttavia, per rilevarli, richiede la connettività IP a questi switch aggiuntivi.
- Lo stesso account è necessario a livello globale per tutti gli switch del fabric. È possibile utilizzare putty (emulatore di terminale open source) per confermare l'accesso.

- Se è installata la licenza Perform, le porte 161 e 162 devono essere aperte per tutti gli switch del fabric per il polling delle prestazioni SNMP.
- Stringa di comunità di sola lettura SNMP

Configurazione

Campo	Descrizione
IP dello switch	Indirizzo IP o nome di dominio completo dello switch
Nome utente	Nome utente dello switch
Password	Password utilizzata per lo switch
Versione SNMP	Versione SNMP
Stringa di comunità SNMP	Stringa di comunità di sola lettura SNMP utilizzata per accedere allo switch
Nome utente SNMP	Nome utente del protocollo della versione SNMP (valido solo per SNMP v3)
Password SNMP	Password del protocollo della versione SNMP (applicabile solo a SNMP v3)

Configurazione avanzata

Campo	Descrizione
Nome fabric	Nome del fabric che deve essere segnalato dall'origine dati. Lasciare vuoto per riportare il nome del fabric come WWN.
Escludi dispositivi	Elenco separato da virgole degli ID dei dispositivi da escludere dal polling
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 15 minuti)
Timeout (sec)	Timeout di connessione (impostazione predefinita: 30 secondi)
Timeout attesa banner (sec)	Timeout di attesa banner SSH (impostazione predefinita: 5 secondi)
Domini amministrativi attivi	Selezionare se si utilizzano i domini di amministrazione

Recuperare i dati MPR	Selezionare per acquisire i dati di routing dal router multiprotocollo (MPR)
Attivare il trapping	Selezionare questa opzione per abilitare l'acquisizione alla ricezione di una trap SNMP dal dispositivo. Se si seleziona enable trapping (attiva trap), è necessario attivare anche SNMP.
Tempo minimo tra trap (sec)	Tempo minimo tra i tentativi di acquisizione attivati da trap (impostazione predefinita: 10 secondi)
Scopri tutti gli switch del fabric	Selezionare per rilevare tutti gli switch nel fabric
Scegli di favorire HBA vs Alias zona	Scegliere se favorire gli alias HBA o di zona
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Protocollo SNMP Auth	Protocollo di autenticazione SNMP (solo SNMP v3)
SNMP Privacy Protocol	Protocollo di privacy SNMP (solo SNMP v3)
Password per la privacy SNMP	Password per la privacy SNMP (solo SNMP v3)
Tentativi SNMP	Numero di tentativi SNMP
Timeout SNMP (ms)	Timeout SNMP (impostazione predefinita: 5000 ms)

Origine dati Brocade Sphereon/Intrepid Switch

OnCommand Insight utilizza l'origine dati Brocade Sphereon/Intrepid Switch (SNMP) per rilevare l'inventario degli switch Brocade Sphereon o Intrepid.

Requisiti

Questo data collector non è disponibile a partire da OnCommand Insight 7.3.11.

- Deve essere presente una connettività IP a tutti gli switch del fabric. Se si seleziona la casella di controllo Discover All switch in the Fabric (rileva tutti gli switch nel fabric), OCI identifica tutti gli switch nel fabric; tuttavia, per rilevarli, richiede la connettività IP a questi switch aggiuntivi.
- Stringa di comunità di sola lettura se si utilizza SNMP V1 o SNMP V2.
- Accesso HTTP allo switch per ottenere informazioni sullo zoning.
- Convalida dell'accesso eseguendo `snmpwalk` utility per lo switch (vedere `<install_path\>\bin\)`.

Configurazione

Campo	Descrizione
Switch Sphereon	Indirizzo IP o nome di dominio completo dello switch
Versione SNMP	Versione SNMP
Community SNMP	Stringa di comunità di sola lettura SNMP utilizzata per accedere allo switch
Nome utente	Nome utente SMI-S per lo switch (solo SNMP v3)
Password	Password SMI-S per lo switch (solo SNMP v3)

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 15 minuti)
Protocollo SNMP Auth	Protocollo di autenticazione SNMP (solo SNMPv3)
SNMP Privacy Protocol	Protocollo di privacy SNMP (solo SNMPv3)
Password per la privacy SNMP	Password per la privacy SNMP
Numero di tentativi SNMP	Numero di tentativi SNMP
Timeout SNMP (ms)	Timeout SNMP (impostazione predefinita: 5000 ms)
Nome fabric	Nome del fabric che deve essere segnalato dall'origine dati. Lasciare vuoto per riportare il nome del fabric come WWN.
Attivare il trapping	Selezionare questa opzione per abilitare l'acquisizione alla ricezione di una trap SNMP dal dispositivo. Se si seleziona enable trapping (attiva trap), è necessario attivare anche SNMP.
Tempo minimo tra Ttrap (secondi)	Tempo minimo tra i tentativi di acquisizione attivati da trap (impostazione predefinita: 10 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Origine dati Cisco FC Switch firmware (SNMP)

OnCommand Insight utilizza l'origine dati Cisco FC Switch firmware 2.0+ (SNMP) per rilevare l'inventario degli switch Fibre Channel Cisco MDS e una serie di switch Cisco Nexus FCoE su cui è abilitato il servizio FC. Inoltre, è possibile scoprire molti modelli di dispositivi Cisco in esecuzione in modalità NPV con questa origine dati.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati dello switch FC Cisco. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Switch	Switch
Porta	Porta
VSAN	Fabric
Zona	Zona
Switch logico	Switch logico
Voce del server dei nomi	Voce del server dei nomi
Area di routing inter-VSAN (IVR)	Zona IVR

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP di uno switch nel fabric o di singoli switch
- Rilevamento dello chassis, per abilitare il rilevamento fabric
- Se si utilizza SNMP V2, stringa di comunità di sola lettura
- La porta 161 viene utilizzata per accedere al dispositivo
- Convalida degli accessi mediante `snmpwalk` utility per lo switch (vedere `<install_path\>\bin\`)

Configurazione

Campo	Descrizione
IP switch Cisco	Indirizzo IP o nome di dominio completo dello switch

Versione SNMP	Per l'acquisizione delle prestazioni è necessario SNMP versione v2 o successiva
Stringa di comunità SNMP	Stringa di comunità di sola lettura SNMP utilizzata per accedere allo switch (non applicabile per SNMP v3)
Nome utente	Nome utente dello switch (solo SNMP v3)
Password	Password utilizzata per lo switch (solo SNMPv3)

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Protocollo SNMP Auth	Protocollo di autenticazione SNMP (solo SNMPv3)
SNMP Privacy Protocol	Protocollo di privacy SNMP (solo SNMPv3)
Password per la privacy SNMP	Password per la privacy SNMP
Tentativi SNMP	Numero di tentativi SNMP
Timeout SNMP (ms)	Timeout SNMP (impostazione predefinita: 5000 ms)
Attivare il trapping	Selezionare per attivare il trapping. Se si attiva il trapping, è necessario attivare anche le notifiche SNMP.
Tempo minimo tra trap (sec)	Tempo minimo tra i tentativi di acquisizione attivati da trap (impostazione predefinita: 10 secondi)
Scopri tutti gli switch fabric	Selezionare per rilevare tutti gli switch nel fabric
Escludi dispositivi	Elenco separato da virgole degli IP delle periferiche da escludere dal polling
Includi dispositivi	Elenco separato da virgole degli IP delle periferiche da includere nel polling
Verificare il tipo di dispositivo	Selezionare questa opzione per accettare solo i dispositivi che si pubblicizzano esplicitamente come dispositivi Cisco

Tipo di alias primario	Fornire una prima preferenza per la risoluzione dell'alias. Scegliere tra le seguenti opzioni: • **Alias periferica** Si tratta di un nome di facile utilizzo per una porta WWN (pWWN) che può essere utilizzata in tutti i comandi di configurazione, come richiesto. Tutti gli switch della famiglia Cisco MDS 9000 supportano i servizi Distributed Device Alias (alias del dispositivo). • **Nessuno** Non segnalare alias • **Descrizione della porta** Una descrizione che consente di identificare la porta in un elenco di porte • **Alias zona (tutti)** Un nome di facile utilizzo per una porta che può essere utilizzata solo per la configurazione dello zoning • **Alias zona (solo attivo)** Un nome di facile utilizzo per una porta che può essere utilizzata solo per la configurazione attiva. Questa è l'impostazione predefinita.
Tipo di alias secondario	Specificare una seconda preferenza per la risoluzione dell'alias
Tipo di alias terzo	Fornire una terza preferenza per la risoluzione dell'alias
Abilitare il supporto della modalità proxy SANTap	Selezionare se lo switch Cisco utilizza SANTap in modalità proxy. Se si utilizza EMC RecoverPoint, probabilmente si utilizza SANTap.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Fonte dei dati EMC Celerra

L'origine dati Celerra (SSH) raccoglie le informazioni di inventario dallo storage Celerra. Per la configurazione, questa origine dati richiede l'indirizzo IP dei processori di storage e un nome utente e una password di sola lettura.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC Celerra. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Server di rete Celerra	Storage
Celerra Meta Volume/Pool di storage Celerra	Pool di storage
File System	Volume interno
Data Mover. (Mover dati	Controller
File System montato su un Data Mover	Condivisione file
Esportazioni CIFS e NFS	Condividere
Volume del disco	LUN back-end

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- L'indirizzo IP del processore di storage
- Nome utente e password di sola lettura
- Porta SSH 22

Configurazione

Campo	Descrizione
Indirizzo di Celerra	Indirizzo IP o nome di dominio completo del dispositivo Celerra
Nome utente	Nome utilizzato per accedere al dispositivo Celerra
Password	Password utilizzata per accedere al dispositivo Celerra

Configurazione avanzata

Campo	Descrizione

Intervallo polling inventario (minuti)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 600 secondi)
Numero di tentativi	Numero di tentativi di inventario
Timeout attesa banner SSH (sec)	Timeout di attesa banner SSH (impostazione predefinita: 20 secondi)

Origine dati EMC CLARiiON (navicli)

Prima di configurare questa origine dati, assicurarsi che EMC Navisphere CLI sia installato sul dispositivo di destinazione e sul server Insight. La versione di Navisphere CLI deve corrispondere alla versione del firmware sul controller. Per la raccolta dei dati sulle performance, la registrazione delle statistiche deve essere attivata.

Sintassi dell'interfaccia della riga di comando di Navisphere

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope,use 0 for global scope> -port <use 443 by default> command
```

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC CLARiiON. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Storage	Storage
Processore per lo storage	Nodo di storage
Thin Pool, RAID Group	Pool di storage
LUN	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Un indirizzo IP di ciascun processore di storage CLARiiON
- Nome utente e password Navisphere di sola lettura per gli array CLARiiON
- Navicli deve essere installato sul server Insight/RAU
- Convalida dell'accesso: Eseguire navicli dal server Insight a ciascun array utilizzando il nome utente e la password indicati sopra.
- La versione di navicli deve corrispondere al nuovo codice FLARE dell'array
- Per le performance, la registrazione delle statistiche deve essere attivata.
- Requisiti delle porte: 80, 443

Configurazione

Campo	Descrizione
Storage CLARiiON	Indirizzo IP o nome di dominio completo dello storage CLARiiON
Nome utente	Nome utilizzato per accedere al dispositivo di storage CLARiiON.
Password	Password utilizzata per accedere al dispositivo di storage CLARiiON.
Percorso CLI su percorso navicli.exe o percorso naviseccli.exe	Percorso completo di `navicli.exe` OPPURE `naviseccli.exe` eseguibile

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
USA client sicuro (navigcli)	Selezionare per utilizzare il client sicuro (navcli)
Scopo	L'ambito del client sicuro. L'impostazione predefinita è Globale.
Porta CLI CLARiiON	Porta utilizzata per CLARiiON CLI
Timeout processo esterno inventario (sec)	Timeout processo esterno (impostazione predefinita: 1800 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Performance External Process timeout (sec) (Timeout processo esterno performance	Timeout processo esterno (impostazione predefinita: 1800 secondi)

Origine dati EMC Data Domain

Questa origine dati raccoglie le informazioni di storage e configurazione dai sistemi storage di deduplica EMC Data Domain. Per aggiungere l'origine dati, è necessario utilizzare istruzioni e comandi di configurazione specifici e conoscere i requisiti dell'origine dati e le raccomandazioni sull'utilizzo.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati del dominio dati EMC. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Array	Storage
Porta	Porta
File	Volume interno
Mtree	Qtree
Quota	Quota
Condivisione NFS e CIFS	FileShare

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP del dispositivo Data Domain
- Nome utente e password di sola lettura per lo storage Data Domain
- Porta SSH 22

Configurazione

Campo	Descrizione

Indirizzo IP	L'indirizzo IP o il nome di dominio completo dell'array di storage Data Domain
Nome utente	Il nome utente dell'array di storage Data Domain
Password	La password per l'array di storage Data Domain

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 180 secondi)
Porta SSH	Porta di servizio SSH

Fonte dei dati EMC ECC StorageScope

Il dispositivo EMC ECC StorageScope dispone di tre tipi di origini dati: 5.x, 6.0 e 6.1.

Configurazione

Questo data collector non è più disponibile a partire da OnCommand Insight 7.3.11.

Campo	Descrizione
Server ECC	Indirizzo IP o nome di dominio completo del server ECC
Nome utente	Nome utente del server ECC
Password	Password del server ECC

Configurazione avanzata

Campo	Descrizione
Porta ECC	Porta utilizzata per il server ECC
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 30 minuti)
Protocollo per la connessione al database	Protocollo utilizzato per la connessione al database

Eseguire una query sulle informazioni del file system	Selezionare questa opzione per recuperare i dettagli relativi agli alias WWN e ai file system.

Origine dati Dell EMC ECS

Questo data collector acquisisce i dati di inventario e performance dai sistemi storage EMC ECS. Per la configurazione, il data collector richiede un indirizzo IP del server ECS e un account di dominio di livello amministrativo.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC ECS. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Cluser	Storage
Tenant	Pool di storage
Bucket	Volume interno
Disco	Disco

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP della console di gestione ECS
- Account di dominio di livello amministrativo per il sistema ECS
- Porta 443 (HTTPS). Richiede la connettività in uscita alla porta TCP 443 sul sistema ECS.
- Per le performance, nome utente e password di sola lettura per l'accesso ssh/SCP.
- Per le prestazioni, è necessaria la porta 22.

Configurazione

Campo	Descrizione
Host ECS	Indirizzi IP o nomi di dominio pienamente qualificati del sistema ECS
Porta host ECS	Porta utilizzata per la comunicazione con l'host ECS
ID fornitore ECS	ID vendor per ECS

Password	Password utilizzata per ECS

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (minuti)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 360 minuti.

Fonte dei dati EMC Isilon

L'origine dati ISILON SSH raccoglie l'inventario e le performance dallo storage NAS scale-out EMC Isilon.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC Isilon. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
File System	Volume interno

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Autorizzazioni di amministratore per lo storage Isilon
- Accesso validato tramite `telnet` alla porta 22

Configurazione

Campo	Descrizione
Indirizzo IP	L'indirizzo IP o il nome di dominio completo del cluster Isilon
Nome utente	Il nome utente del cluster Isilon

Password	La password per il cluster Isilon

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Timeout di attesa processo SSH	Timeout processo SSH (impostazione predefinita: 60 secondi)
Porta SSH	Porta di servizio SSH

Esecuzione dei comandi CLI

A partire da OnCommand Insight versione 7.3.11 e Service Pack 9, l'origine dati EMC Isilon contiene un miglioramento che consentirà a Insight di eseguire più comandi CLI. Se si utilizza un utente non root all'interno dell'origine dati, è probabile che sia stato configurato un file "sudoers" per consentire a tale account utente di eseguire comandi CLI specifici tramite SSH.

Per consentire a Insight di comprendere la funzione "Access Zones" di EMC, Insight eseguirà ora anche i seguenti nuovi comandi CLI:

- `sudo isi zone zones list --format json –verbose`
- `sudo isi zone zones list`

Insight analizza l'output di questi comandi ed esegue più istanze di comandi esistenti per ottenere la configurazione logica di oggetti come qtree, quote e condivisioni/esportazioni NAS che risiedono in zone di accesso non predefinite. Insight ora riporta questi oggetti per le zone di accesso non predefinite come risultato di questo miglioramento. Poiché Insight ottiene tali dati eseguendo comandi esistenti (con opzioni diverse), non è necessario modificare il file dei sostutori per il funzionamento; è solo con l'introduzione dei nuovi comandi sopra descritti che la modifica è necessaria.

Aggiorna il file di supporto per consentire all'account del servizio Insight di eseguire questi comandi prima di eseguire l'aggiornamento a questa versione di Insight. In caso contrario, le origini dati Isilon si guasteranno.

Statistiche del "file system"

A partire da OnCommand Insight 7.3.12, il data collector EMC Isilon introduce le statistiche del "file system" sull'oggetto nodo per EMC Isilon. Le statistiche dei nodi esistenti riportate da OnCommand Insight sono basate su "disco", ad esempio, per gli IOPS e il throughput di un nodo di storage, cosa fanno i dischi in questo nodo in aggregato? Tuttavia, per i carichi di lavoro in cui le letture sono memorizzate nella cache e/o la compressione è in uso, il carico di lavoro del file system potrebbe essere sostanzialmente superiore a quello effettivamente presente sui dischi: Un set di dati che comprime 5:1 potrebbe quindi avere un valore di "throughput di lettura del file system" 5 volte il nodo di storage throughput di lettura, poiché quest'ultimo misura le letture del disco, che si espandono di 5 volte quando il nodo decomprime i dati per servire la richiesta di lettura del client.

Fonte dei dati Dell EMC PowerStore

Il data collector Dell EMC PowerStore raccoglie le informazioni di inventario dallo storage Dell EMC PowerStore. Per la configurazione, il data collector richiede l'indirizzo IP dei processori di storage e un nome utente e una password di sola lettura.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati del dominio dati EMC. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
host	host
host_volume_mapping	host_volume_mapping
Hardware (contiene dischi sotto l'oggetto "extra_details"): Dischi	Disco
Appliance	StoragePool
Cluster	Array di storage
Nodo	StorageNode
porta_fc	Porta
volume	Volume
Volume interno	file_system
File	Volume interno
Mtree	Qtree
Quota	Quota
Condivisione NFS e CIFS	FileShare

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP o nome di dominio completo del processore di storage

- Nome utente e password di sola lettura

Spiegazione del numero di serie principale

Tradizionalmente Insight è in grado di riportare il numero di serie dello storage array o i numeri di serie dei singoli nodi di storage. Tuttavia, alcune architetture di storage array non sono perfettamente allineate a questo. Un cluster PowerStore può essere composto da 1-4 appliance e ogni appliance ha 2 nodi. Se l'appliance dispone di un numero di serie, tale numero non corrisponde né al numero di serie del cluster né ai nodi.

L'attributo "Parent Serial Number" (numero di serie principale) sull'oggetto del nodo di storage viene popolato in modo appropriato per gli array Dell/EMC PowerStore quando i singoli nodi si trovano all'interno di un'appliance/enclosure intermedia che fa parte di un cluster più grande.

Configurazione

Campo	Descrizione
Gateway PowerStore	Indirizzi IP o nomi di dominio pienamente qualificati dello storage PowerStore
Nome utente	Nome utente di PowerStore
Password	Password utilizzata per PowerStore

Configurazione avanzata

Campo	Descrizione
Porta HTTPS	Il valore predefinito è 443
Intervallo polling inventario (minuti)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.

La raccolta di performance di PowerStore di OnCommand utilizza i dati di origine della granularità di 5 minuti. Pertanto, Insight esegue il polling dei dati ogni cinque minuti e questo non è configurabile.

Fonte dei dati EMC RecoverPoint

L'origine dati EMC RecoverPoint raccoglie le informazioni di inventario dallo storage EMC RecoverPoint. Per la configurazione, l'origine dati richiede l'indirizzo IP dei processori di storage e un nome utente e una password di sola lettura.

L'origine dati EMC RecoverPoint raccoglie le relazioni di replica volume-volume che RecoverPoint coordina tra altri array di storage. OnCommand Insight mostra un array di storage per ogni cluster RecoverPoint e raccoglie i dati di inventario per i nodi e le porte di storage su quel cluster. Non vengono raccolti dati di volumi o pool di storage.

Requisiti

- Indirizzo IP o nome di dominio completo del processore di storage

- Nome utente e password di sola lettura
- Accesso API REST tramite la porta 443
- Accesso SSH tramite putty

Configurazione

Campo	Descrizione
Indirizzo di RecoverPoint	Indirizzo IP o nome di dominio completo del cluster RecoverPoint
Nome utente	Nome utente del cluster RecoverPoint
Password	Password per il cluster RecoverPoint

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione al cluster Recoverpoint
Intervallo polling inventario (minuti)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Cluster esclusi	Elenco separato da virgole di ID cluster o nomi da escludere durante il polling

EMC Solutions Enabler con fonte di dati SMI-S Performance

OnCommand Insight rileva gli array di storage Symmetrix utilizzando Solutions Enabler `symcli` Comandi in combinazione con un server Solutions Enabler esistente nel tuo ambiente. Il server Solutions Enabler esistente dispone della connettività all'array di storage Symmetrix attraverso l'accesso ai volumi di gatekeeper. Per accedere a questo dispositivo sono necessarie le autorizzazioni di amministratore.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC Solutions Enabler. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Gruppo di dischi	Gruppo di dischi

Array di storage	Storage
Direttore	Nodo di storage
Pool di dispositivi, Storage Resource Pool (SRP)	Pool di storage
Dispositivo, TDev	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

Prima di configurare questa origine dati, assicurarsi che il server OnCommand Insight disponga della connettività TCP alla porta 2707 sul server di abilitazione soluzioni esistente. OnCommand Insight rileva tutti gli array Symmetrix che sono “locali” per questo server, come si vede nell’output “symcfg list” da quel server.

- L’applicazione EMC Solutions Enabler (CLI) con provider SMI-S deve essere installata e la versione deve corrispondere o essere precedente alla versione in esecuzione su Solutions Enabler Server.
- Un configurato correttamente `{installdir}\EMC\SYMAPI\config\netcnfg` il file è obbligatorio. Questo file definisce i nomi dei servizi per i server Solutions Enabler e il metodo di accesso (SICURO / NOSECURE /ANY).
- Se si richiede una latenza di lettura/scrittura a livello di nodo di storage, il provider SMI-S deve comunicare con un’istanza in esecuzione dell’applicazione UNISPHERE per VMAX.
- Autorizzazioni di amministratore per il server Solutions Enabler (se)
- Nome utente e password di sola lettura per il software se
- Solutions Enabler Server 6.5 requisiti:
  - SMI-S provider 3.3.1 per SMC-S V1.2 installato
  - Dopo l’installazione, eseguire `\Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd`
- L’applicazione UNISPHERE per VMAX deve essere in esecuzione e raccogliere le statistiche per gli array di storage Symmetrix VMAX gestiti dall’installazione del provider SMI-S.
- Access validation (convalida accesso): Verificare che il provider SMI-S sia in esecuzione: `telnet <se_server\> 5988`

Configurazione

Se l’autenticazione utente SMI-S non è attivata, i valori predefiniti nell’origine dati OnCommand Insight vengono ignorati.

L’attivazione di symauth sugli array Symmetrix potrebbe impedire a OnCommand Insight di rilevarli. Acquisizione OnCommand Insight viene eseguita come utente DI SISTEMA sul server OnCommand Insight/unità di acquisizione remota che comunica con il server di abilitazione soluzioni. Se il nome host o IL SISTEMA non dispone di privilegi symauth, OnCommand Insight non riesce a rilevare l’array.

L’origine dati EMC Solutions Enabler Symmetrix CLI include il supporto per la configurazione dei dispositivi per

il thin provisioning e Symmetrix Remote Data Facility (SRDF).

Le definizioni sono fornite per i pacchetti Fibre Channel e Switch Performance.

Campo	Descrizione
Nome servizio	Nome del servizio specificato nel file netcnfg
Percorso completo alla CLI	Percorso completo alla CLI di Symmetrix

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati
Inventario Escludi i dispositivi	Elenco separato da virgole degli ID dei dispositivi da includere o escludere

Caching della connessione	Scegliere il metodo di caching della connessione: • LOCALE indica che il servizio di acquisizione OnCommand Insight è in esecuzione sul server Solutions Enabler, che dispone di connettività Fibre Channel agli array Symmetrix che si desidera rilevare e ha accesso ai volumi gatekeeper. Questo problema potrebbe verificarsi in alcune configurazioni dell'unità di acquisizione remota (RAU). • REMOTE_CACHED è l'impostazione predefinita e dovrebbe essere utilizzata nella maggior parte dei casi. In questo modo vengono utilizzate le impostazioni del file NETCNFG per connettersi tramite IP al server Solutions Enabler, che deve disporre di connettività Fibre Channel agli array Symmetrix che si desidera rilevare e avere accesso ai volumi di Gatekeeper. • Nel caso in cui le opzioni REMOTE_CACHED rendano non disponibili i comandi CLI, utilizzare L'opzione REMOTA. Tenere presente che rallenterà il processo di acquisizione (possibilmente fino a ore o persino giorni in casi estremi). Le impostazioni del file NETCNFG vengono ancora utilizzate per una connessione IP al server Solutions Enabler che dispone di connettività Fibre Channel agli array Symmetrix rilevati. Questa impostazione non modifica il comportamento di OnCommand Insight rispetto agli array elencati come REMOTI dall'output "symcfg list". OnCommand Insight raccoglie i dati solo sui dispositivi indicati COME LOCALI da questo comando.
Timeout CLI (sec)	Timeout del processo CLI (impostazione predefinita: 7200 secondi)
IP HOST SMI-S.	Indirizzo IP dell'host del provider SMI-S.
Porta SMI-S.	Porta utilizzata dall'host del provider SMI-S.
Protocollo	Protocollo utilizzato per connettersi al provider SMI-S.
Spazio dei nomi SMI-S.	Namespace di interoperabilità configurato per l'utilizzo da parte del provider SMI-S.

Nome utente SMI-S.	Nome utente dell'host del provider SMI-S.
Password SMI-S.	Nome utente dell'host del provider SMI-S.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 1000 secondi)
Tipo di filtro delle prestazioni	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati sulle prestazioni
Elenco dispositivi filtro prestazioni	Elenco separato da virgole degli ID dei dispositivi da includere o escludere
Intervallo di polling RPO (sec)	Intervallo tra i sondaggi RPO (impostazione predefinita: 300 secondi)

Origine dati EMC VNX

Per la configurazione, l'origine dati EMC VNX (SSH) richiede l'indirizzo IP della stazione di controllo e un nome utente e una password di sola lettura.

Configurazione

Campo	Descrizione
IP VNX	Indirizzo IP o nome di dominio completo della stazione di controllo VNX
Nome utente VNX	Nome utente della stazione di controllo VNX
Password VNX	Password per la stazione di controllo VNX

Requisiti

- Indirizzo IP della stazione di controllo
- Nome utente e password di sola lettura.
- Convalida degli accessi: Verifica dell'accesso SSH tramite PuTTY.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)

Timeout attesa processo VNX SSH (sec)	Timeout del processo VNX SSH (impostazione predefinita: 600 secondi)
Tentativi di tentativo del comando Celerra	Numero di tentativi di comando Celerra
Timeout processo esterno CLARiiON per inventario (sec)	Timeout processo esterno CLARiiON per inventario (valore predefinito: 1800 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Timeout processo esterno CLARiiON per le prestazioni (sec)	Timeout processo esterno CLARiiON per le prestazioni (impostazione predefinita: 1800 secondi)

Fonte dei dati EMC VNXe

L'origine dati EMC VNXe fornisce il supporto dell'inventario per gli array storage unificati EMC VNXe e Unity.

Questa origine dati è basata su CLI e richiede l'installazione di Unisphere per VNXe CLI (uemcli.exe) sull'unità di acquisizione su cui risiede l'origine dati VNXe. uemcli.exe utilizza HTTPS come protocollo di trasporto, quindi l'unità di acquisizione deve essere in grado di avviare connessioni HTTPS agli array VNXe/Unity. È necessario disporre di almeno un utente di sola lettura per l'utilizzo da parte dell'origine dati.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC VNXe. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Array di storage	Storage
Del processore	Nodo di storage
Pool di storage	Pool di storage
Informazioni generali sul blocco iSCSI, VMware VMFS	Volume
Cartella condivisa	Volume interno
Condivisione CIFS, condivisione NFS, condivisione dal datastore VMware NFS	Condividere

Sistema remoto di replica	Sincronizzazione
Nodo iSCSI	Nodo di destinazione iSCSI
ISCSI Initiator	ISCSI Target Initiator

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questa origine dati:

- Il data collector VNXe è basato su CLI; è necessario installare Unisphere per VNXe CLI (uemcli.exe) sull'unità di acquisizione in cui risiede il data collector VNXe.
- uemcli.exe utilizza HTTPS come protocollo di trasporto, quindi l'unità di acquisizione deve essere in grado di avviare connessioni HTTPS a VNXe.
- È necessario disporre di almeno un utente di sola lettura per l'utilizzo da parte dell'origine dati.
- Indirizzo IP del server di abilitazione delle soluzioni di gestione.
- HTTPS sulla porta 443 è obbligatorio
- Il data collector EMC VNXe fornisce supporto NAS e iSCSI per l'inventario; verranno rilevati volumi Fibre Channel, ma Insight non esegue report su mappatura FC, mascheratura o porte di storage.

Configurazione

Campo	Descrizione
Storage VNXe	Indirizzo IP o nome di dominio completo del dispositivo VNXe
Nome utente	Nome utente del dispositivo VNXe
Password	Password per il dispositivo VNXe
Percorso completo dell'eseguibile uemcli	Percorso completo di `uemcli.exe` eseguibile

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Porta CLI VNXe	Porta utilizzata per la CLI VNXe

Timeout processo esterno inventario (sec)	Timeout processo esterno (impostazione predefinita: 1800 secondi)

Origine dati EMC VPLEX

Per la configurazione, questa origine dati richiede un indirizzo IP del server VPLEX e un account di dominio di livello amministrativo.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC VPLEX. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Cluster	Storage
Motore	Nodo di storage
Device, System Extend	Pool di storage back-end
Volume virtuale	Volume
Porta front-end, porta back-end	Porta
Dispositivo distribuito	Sincronizzazione dello storage
Vista storage	Mappa del volume, maschera del volume
Volume di storage	LUN back-end
ITL	Percorso back-end

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP del server VPLEX
- Account di dominio a livello amministrativo per il server VPLEX
- Porta 443 (HTTPS). Richiede la connettività in uscita alla porta TCP 443 sulla stazione di gestione VPLEX.
- Per le performance, nome utente e password di sola lettura per l'accesso ssh/SCP.
- Per le prestazioni, è necessaria la porta 22.

- Validare l'accesso: Verificare utilizzando `telnet` alla porta 443. Per una porta diversa da quella predefinita, con qualsiasi utilizzo da parte del browser

Configurazione

Campo	Descrizione
Indirizzo IP della console di gestione VPLEX	Indirizzo IP o nome di dominio completo della console di gestione VPLEX
Nome utente	Nome utente per VPLEX CLI
Password	Password utilizzata per VPLEX CLI
Performance Remote IP Address (Indirizzo IP remoto delle prestazioni) della console di gestione VPLEX	Performance Remote IP address (Indirizzo IP remoto delle performance) della console di gestione VPLEX
Performance Remote User Name (Nome utente remoto performance)	Performance Remote user name of VPLEX Management Console (Nome utente remoto delle performance di VPLEX Management
Password remota delle performance	Performance Remote Password di VPLEX Management Console

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione	Porta utilizzata per VPLEX CLI
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)
Numero di tentativi	Numero di tentativi di inventario
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 600 secondi)
Timeout attesa processo SSH performance (sec)	Timeout processo SSH (impostazione predefinita: 600 secondi)
Timeout attesa banner SSH (sec)	Timeout di attesa banner SSH (impostazione predefinita: 20 secondi)
Numero di tentativi	Numero di tentativi di esecuzione

Fonte dei dati EMC XtremIO

Per configurare l'origine dati EMC XtremIO (HTTP), è necessario disporre dell'indirizzo host XtremIO Management Server (XMS) e di un account con privilegi di amministratore.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati EMC XtremIO. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco (SSD)	Disco
Cluster	Storage
Controller	Nodo di storage
Volume	Volume
Mappa LUN	Mappa del volume
Iniziatore, destinazione	Maschera di volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Un indirizzo IP di ogni XtremIO Management Server
- Un account con privilegi di amministratore
- Accesso alla porta 443 (HTTPS)

Configurazione

Campo	Descrizione
Host XMS	Indirizzo IP o nome di dominio completo di XtremIO Management Server
Nome utente	Nome utente di XtremIO Management Server
Password	Password per XtremIO Management Server

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione a XTremIO Management Server (impostazione predefinita: 443)
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Fonte dei dati Fujitsu Eternus

L'origine dati di Fujitsu Eternus richiede l'indirizzo IP dello storage. Non può essere delimitato da virgole.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati di Fujitsu Eternus. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Storage	Storage
Thin Pool, Tier Pool flessibile, Gruppo RAID	Pool di storage
Volume standard, volume dati snap (SDV), Volume del pool di dati Snap (SDPV), Volume di thin provisioning (TPV)	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP dello storage Eternus, che non può essere delimitato da virgole
- Nome utente e password a livello di amministrazione SSH
- Porta 22
- Assicurarsi che lo scorrimento della pagina sia disattivato. (clienv-show-more-scroll disattiva)

Configurazione

Campo	Descrizione
Indirizzo IP dello storage Eternus	Indirizzo IP dello storage Eternus
Nome utente	Nome utente dello storage Eternus
Password	Password utilizzata per lo sterno

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 600 secondi)

Fonte dei dati Hitachi Content Platform (HCP)

Questo data collector supporta Hitachi Content Platform (HCP) utilizzando l'API di gestione HCP.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati HCP. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Cluster HCP	Storage
Tenant	Pool di storage
Namespace	Volume interno
Nodo	Nodo

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti di inventario

- Indirizzo IP del server HCP
- Nome utente e password di sola lettura per il software HCP e privilegi peer

Configurazione

Campo	Descrizione
Host HCP	Indirizzo IP o nome di dominio completo dell'host HCP
Porta HCP	Il valore predefinito è 9090
ID utente HCP	Nome utente dell'host HCP
Password HCP	Password utilizzata per l'host HCP
Tipo di autenticazione HCP	Scegliere HCP_LOCAL o ACTIVE_DIRECTORY

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 900 secondi)

Origine dati di HDS HiCommand Device Manager

Le origini dati HDS HiCommand e HiCommand Lite supportano il server HiCommand Device Manager. OnCommand Insight comunica con il server di gestione dispositivi HiCommand utilizzando l'API HiCommand standard.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dalle origini dati HDS HiCommand e HiCommand Lite. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight

PDEV	Disco
Pool di giornale	Gruppo di dischi
Array di storage	Storage
Port Controller (Controller porta)	Nodo di storage
Gruppo di array, DP Pool	Pool di storage
Unità logica, LDEV	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti di inventario

- Indirizzo IP del server HiCommand Device Manager
- Nome utente e password di sola lettura per il software HiCommand Device Manager e privilegi peer
- Requisiti delle porte: 2001 (http) o 2443 (https)
- Convalidare l'accesso:
  - Accedere al software HiCommand Device Manager utilizzando il nome utente e la password peer.
  - Verificare l'accesso all'API di HiCommand Device Manager: `telnet <HiCommand Device_Manager_server_ip\> 2001`

Requisiti relativi alle performance

- Prestazioni di HDS USP, USP V e VSP
  - Performance Monitor deve essere concesso in licenza.
  - Lo switch di monitoraggio deve essere attivato.
  - Lo strumento di esportazione (`Export.exe`) Deve essere copiato sul server OnCommand Insight.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell'array di destinazione.
- Performance di HDS AMS
  - Performance Monitor deve essere concesso in licenza.
  - L'utility CLI Storage Navigator Modular 2 (SNM2) deve essere installata sul server OnCommand Insight.
  - È necessario registrare tutti gli storage array AMS, WMS e SMS le cui performance devono essere acquisite da OnCommand Insight utilizzando il seguente comando:
  - Assicurarsi che tutti gli array registrati siano elencati nell'output di questo comando: `auunitref.exe`.

Configurazione

Campo	Descrizione
Server HiCommand	Indirizzo IP o nome di dominio completo del server HiCommand Device Manager
Nome utente	Nome utente del server HiCommand Device Manager.
Password	Password utilizzata per il server HiCommand Device Manager.
DISPOSITIVI: STORAGE VSP G1000 (R800), VSP (R700), HUS VM (HM700) E USP	Elenco dei dispositivi per storage VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Ogni storage richiede: • IP dell'array: Indirizzo IP dello storage • User Name (Nome utente): Nome utente dello storage • Password: Password per lo storage • Cartella contenente file JAR dell'utility di esportazione: La cartella contenente l'utility di esportazione `.jar` file
SNM2Devices - Storage WMS/SMS/AMS	Elenco dei dispositivi per gli storage WMS/SMS/AMS. Ogni storage richiede: • IP dell'array: Indirizzo IP dello storage • Percorso CLI di Storage Navigator: Percorso CLI SNM2 • Account Authentication Valid (autenticazione account valida): Selezionare questa opzione per scegliere un'autenticazione account valida • User Name (Nome utente): Nome utente dello storage • Password: Password per lo storage
Scegli Tuning Manager per le performance	Scegliere Tuning Manager per le performance e ignorare altre opzioni di performance
Tuning Manager host	Indirizzo IP o nome di dominio completo del tuning manager
Porta Tuning Manager	Porta utilizzata per Tuning Manager
Nome utente Tuning Manager	Nome utente di Tuning Manager

Password Tuning Manager	Password per Tuning Manager

In HDS USP, USP V e VSP, qualsiasi disco può appartenere a più di un gruppo di array.

Configurazione avanzata

Campo	Descrizione
Porta del server HiCommand	Porta utilizzata per HiCommand Device Manager
HTTPS attivato	Selezionare per attivare HTTPS
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati
Escludere o includere i dispositivi	Elenco separato da virgole di ID dispositivo o nomi di array da includere o escludere
Query host Manager (Gestore host query)	Selezionare per eseguire query sul gestore host
Timeout HTTP (sec)	Timeout connessione HTTP (impostazione predefinita: 60 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Timeout di esportazione in secondi	Timeout utility di esportazione (impostazione predefinita: 300 secondi)

Data collector Hitachi Ops Center

Questo data collector utilizza la suite integrata di applicazioni di Hitachi Ops Center per accedere ai dati di inventario e performance di più dispositivi storage. Per il rilevamento dell'inventario e della capacità, l'installazione di Ops Center deve includere i componenti "Common Services" e "Administrator". Per la raccolta delle performance, è necessario implementare anche "Analyzer".

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine OnCommand Insight
Sistemi storage	Storage
Volume	Volume
Gruppi di parità	Pool di storage (RAID), gruppi di dischi
Disco	Disco
Pool di storage	Pool di storage (sottile, SNAP)
Gruppi di parità esterni	Pool di storage (back-end), gruppi di dischi
Porta	Nodo di storage → nodo controller → porta
Gruppi di host	Mappatura e mascheramento dei volumi
Coppie di volumi	Sincronizzazione dello storage

Nota: Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo data collector.

Requisiti di inventario

Per raccogliere i dati di inventario, è necessario disporre di quanto segue:

- Indirizzo IP o nome host del server Ops Center che ospita il componente "servizi comuni"
- Account utente root/sysadmin e password presenti su tutti i server che ospitano i componenti di Ops Center. HDS non ha implementato il supporto API REST per l'utilizzo da parte degli utenti LDAP/SSO fino a quando Ops Center 10.8+

Requisiti relativi alle performance

Per raccogliere i dati sulle performance, è necessario soddisfare i seguenti requisiti:

- È necessario installare il modulo "Analyzer" di HDS Ops Center
- Gli storage array devono alimentare il modulo "Analyzer" di Ops Center

Configurazione

Campo	Descrizione
Hitachi Ops Center IP Address (Indirizzo IP centro Hitachi Ops)	Indirizzo IP o nome di dominio completo del server Ops Center che ospita il componente "servizi comuni"
Nome utente	Nome utente del server Ops Center.
Password	Password utilizzata per il server Ops Center.

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS (porta 443) è l'impostazione predefinita
Sovrascrivere la porta TCP	Specificare la porta da utilizzare se non quella predefinita

Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40.
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati.
Filtra elenco dispositivi	Elenco separato da virgole dei numeri di serie delle periferiche da includere o escludere
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. Il valore predefinito è 300.

Storage HDS

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse di storage HDS.

Terminologia dello storage HDS

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse di storage HDS. Molti di questi termini si applicano anche ad altri data collezionisti.

- Name — deriva direttamente dall'attributo "name" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- Modello - viene fornito direttamente dall'attributo "arrayType" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- Vendor — HDS
- Famiglia - proviene direttamente dall'attributo "arrayFamily" di HDS HiCommand Device Manager tramite la chiamata API XML GetStorageArray
- IP — Indirizzo IP di gestione dell'array, non un elenco completo di tutti gli indirizzi IP dell'array
- Capacità raw - un valore base2 che rappresenta la somma della capacità totale di tutti i dischi di questo sistema, indipendentemente dal ruolo del disco.

Pool di storage HDS

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse del pool di storage HDS.

Terminologia del pool di storage HDS

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse del pool di storage HDS. Molti di questi termini si applicano anche ad altri data collezionisti.

- Type (tipo): Il valore qui sarà uno dei seguenti:
  - RISERVATO — se questo pool è dedicato per scopi diversi dai volumi di dati, ad esempio, journaling, snapshot
  - Thin Provisioning — se si tratta di un pool HDP
  - RAID Group — probabilmente non si vedranno questi per alcuni motivi:

    OCI adotta una posizione forte per evitare il doppio conteggio della capacità a tutti i costi. Su HDS, in

genere è necessario creare gruppi RAID dai dischi, creare volumi di pool su tali gruppi RAID e costruire pool (spesso HDP, ma potrebbe essere uno scopo speciale) da tali volumi di pool. Se OCI riportasse i gruppi RAID sottostanti così come i pool, la somma della loro capacità raw supererebbe enormemente la somma dei dischi.

Invece, il data collector HDS HiCommand di OCI riduce arbitrariamente le dimensioni dei gruppi RAID in base alla capacità dei volumi del pool. Ciò potrebbe causare il mancato reporting del gruppo RAID da parte di OCI. Inoltre, tutti i gruppi RAID risultanti vengono contrassegnati in modo che non siano visibili nell'interfaccia Web OCI, ma fluiscano nel data warehouse OCI (DWH). Lo scopo di queste decisioni è di evitare il disordine dell'interfaccia utente per le cose che la maggior parte degli utenti non si preoccupano — se il vostro array HDS dispone di gruppi RAID con 50 MB liberi, probabilmente non è possibile utilizzare tale spazio libero per qualsiasi risultato significativo.

- Nodo - N/D, in quanto i pool HDS non sono legati a uno specifico nodo
- Ridondanza - il livello RAID del pool. Possibili valori multipli per un pool HDP composto da più tipi RAID
- Capacity % - percentuale utilizzata dal pool per l'utilizzo dei dati, con il GB utilizzato e le dimensioni logiche totali del pool
- Capacità con overcommit - un valore derivato che indica "la capacità logica di questo pool viene sovrascritta da questa percentuale in virtù della somma dei volumi logici che superano la capacità logica del pool di questa percentuale"
- Snapshot: Mostra la capacità riservata all'utilizzo dello snapshot in questo pool

Nodo storage HDS

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse dei nodi di storage HDS.

Terminologia dei nodi di storage HDS

I seguenti termini si applicano agli oggetti o ai riferimenti che si possono trovare nelle landing page delle risorse dei nodi di storage HDS. Molti di questi termini si applicano anche ad altri data collezionisti.

- Name (Nome) - il nome del Front-End Director (FED) o dell'adattatore di canale sugli array monolitici o il nome del controller su un array modulare. Un determinato array HDS avrà 2 o più nodi di storage
- Volumes (volumi) - la tabella Volume mostra qualsiasi volume mappato a qualsiasi porta di proprietà di questo nodo di storage

Data collector Hitachi Ops Center

Questo data collector utilizza la suite integrata di applicazioni di Hitachi Ops Center per accedere ai dati di inventario e performance di più dispositivi storage. Per il rilevamento dell'inventario e della capacità, l'installazione di Ops Center deve includere i componenti "Common Services" e "Administrator". Per la raccolta delle performance, è necessario implementare anche "Analyzer".

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine OnCommand Insight
Sistemi storage	Storage
Volume	Volume
Gruppi di parità	Pool di storage (RAID), gruppi di dischi
Disco	Disco
Pool di storage	Pool di storage (sottile, SNAP)
Gruppi di parità esterni	Pool di storage (back-end), gruppi di dischi
Porta	Nodo di storage → nodo controller → porta
Gruppi di host	Mappatura e mascheramento dei volumi
Coppie di volumi	Sincronizzazione dello storage

Nota: Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questo data collector.

Requisiti di inventario

Per raccogliere i dati di inventario, è necessario disporre di quanto segue:

- Indirizzo IP o nome host del server Ops Center che ospita il componente "servizi comuni"
- Account utente root/sysadmin e password presenti su tutti i server che ospitano i componenti di Ops Center. HDS non ha implementato il supporto API REST per l'utilizzo da parte degli utenti LDAP/SSO fino a quando Ops Center 10.8+

Requisiti relativi alle performance

Per raccogliere i dati sulle performance, è necessario soddisfare i seguenti requisiti:

- È necessario installare il modulo "Analyzer" di HDS Ops Center
- Gli storage array devono alimentare il modulo "Analyzer" di Ops Center

Configurazione

Campo	Descrizione
Hitachi Ops Center IP Address (Indirizzo IP centro Hitachi Ops)	Indirizzo IP o nome di dominio completo del server Ops Center che ospita il componente "servizi comuni"
Nome utente	Nome utente del server Ops Center.
Password	Password utilizzata per il server Ops Center.

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS (porta 443) è l'impostazione predefinita
Sovrascrivere la porta TCP	Specificare la porta da utilizzare se non quella predefinita

Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40.
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati.
Filtra elenco dispositivi	Elenco separato da virgole dei numeri di serie delle periferiche da includere o escludere
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. Il valore predefinito è 300.

Origine dati HDS NAS (HNAS)

L'origine dati HDS NAS (HNAS) è un'origine dati di inventario e configurazione per supportare il rilevamento di cluster HDS NAS. Insight supporta il rilevamento di condivisioni NFS e CIFS, file system (Insight Internal Volumes) e span (Insight Storage Pools).

Questa origine dati è basata su SSH, pertanto l'unità di acquisizione che la ospiterà deve essere in grado di avviare sessioni SSH su TCP 22 sull'HNAS stesso o sull'unità di gestione dei sistemi (SMU) a cui è connesso il cluster.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati HNAS. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Tier	Gruppo di dischi
Cluster	Storage
Nodo	Nodo di storage
Intervallo	Pool di storage
File System	Volume interno

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questa origine dati:

- Indirizzo IP del dispositivo
- Porta 22, protocollo SSH

- Nome utente e password - livello di privilegio: Supervisore
- NOTA: Questo data collector è basato su SSH, quindi l'AU che lo ospita deve essere in grado di avviare sessioni SSH su TCP 22 sull'HNAS stesso o sull'unità di gestione dei sistemi (SMU) a cui è connesso il cluster.

> Questo data collector è basato su SSH, quindi l'AU che lo ospita deve essere in grado di avviare sessioni SSH su TCP 22 sull'HNAS stesso o sull'unità di gestione dei sistemi (SMU) a cui è connesso il cluster.

Configurazione

Campo	Descrizione
Host HNAS	Indirizzo IP o nome di dominio completo di HNAS Management host
Nome utente	Nome utente per CLI HNAS
Password	Password utilizzata per CLI HNAS

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 30 minuti)
Timeout attesa banner SSH (sec)	Timeout di attesa banner SSH (impostazione predefinita: 15 secondi)
Timeout comando SSH (sec)	Timeout comando SSH (impostazione predefinita: 30 secondi)

Origine dati HP CommandView AE

Le origini dati HP CommandView Advanced Edition (AE) e CommandView AE CLI/SMI (AE Lite) supportano l'inventario e le prestazioni da un server Device Manager CommandView (chiamato anche HiCommand).

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dalle origini dati di HP CommandView AE e AE Lite. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight

PDEV	Disco
Pool di giornale	Gruppo di dischi
Array di storage	Storage
Port Controller (Controller porta)	Nodo di storage
Gruppo di array, DP Pool	Pool di storage
Unità logica, LDEV	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti di inventario

- Indirizzo IP del server HiCommand Device Manager
- Nome utente e password di sola lettura per il software CommandView AE e privilegi peer
- La versione CommandView AE Lite di Device Manager dispone solo della licenza CLI
- Requisiti delle porte: 2001

Requisiti relativi alle performance

- Prestazioni di HDS USP, USP V e VSP
  - Performance Monitor deve essere concesso in licenza.
  - Lo switch di monitoraggio deve essere attivato.
  - Lo strumento di esportazione (`Export.exe`) Deve essere copiato sul server OnCommand Insight.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell'array di destinazione.
- Performance di HDS AMS
  - Performance Monitor deve essere concesso in licenza.
  - L'utility CLI Storage Navigator Modular 2 (SNM2) deve essere installata sul server OnCommand Insight.
  - È necessario registrare tutti gli storage array AMS, WMS e SMS le cui performance devono essere acquisite da OnCommand Insight utilizzando il seguente comando:
  - Assicurarsi che tutti gli array registrati siano elencati nell'output di questo comando: `auunitref.exe`.

Configurazione

Campo	Descrizione
Server HiCommand	Indirizzo IP o nome di dominio completo del server HiCommand Device Manager

Nome utente	Nome utente del server HiCommand Device Manager.
Password	Password utilizzata per il server HiCommand Device Manager.
Dispositivi - Storage USP, USP V, VSP/R600	Elenco dei dispositivi per storage VSP G1000 (R800), VSP (R700), HUS VM (HM700) e USP. Ogni storage richiede: • IP dell'array: Indirizzo IP dello storage • User Name (Nome utente): Nome utente dello storage • Password: Password per lo storage • Cartella contenente file JAR dell'utility di esportazione: La cartella contenente l'utility di esportazione `.jar` file
SNM2Devices - Storage WMS/SMS/AMS	Elenco dei dispositivi per gli storage WMS/SMS/AMS. Ogni storage richiede: • IP dell'array: Indirizzo IP dello storage • Percorso CLI di Storage Navigator: Percorso CLI SNM2 • Account Authentication Valid (autenticazione account valida): Selezionare questa opzione per scegliere un'autenticazione account valida • User Name (Nome utente): Nome utente dello storage • Password: Password per lo storage
Scegli Tuning Manager per le performance	Scegliere Tuning Manager per le performance e ignorare altre opzioni di performance
Tuning Manager host	Indirizzo IP o nome di dominio completo del tuning manager
Porta Tuning Manager	Porta utilizzata per Tuning Manager
Nome utente Tuning Manager	Nome utente di Tuning Manager
Password Tuning Manager	Password per Tuning Manager

In HDS USP, USP V e VSP, qualsiasi disco può appartenere a più di un gruppo di array.

Configurazione avanzata

Campo	Descrizione
Porta del server HiCommand	Porta utilizzata per HiCommand Device Manager
HTTPS attivato	Selezionare per attivare HTTPS
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco di array riportato di seguito durante la raccolta dei dati
Escludere o includere i dispositivi	Elenco separato da virgole di ID dispositivo o nomi di array da includere o escludere
Query host Manager (Gestore host query)	Selezionare per eseguire query sul gestore host
Timeout HTTP (sec)	Timeout connessione HTTP (impostazione predefinita: 60 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Timeout di esportazione in secondi	Timeout utility di esportazione (impostazione predefinita: 300 secondi)

Origine dati storage HP EVA

Per la configurazione, l'origine dati EVA Storage (SSSU) richiede l'indirizzo IP del server Command View (CV) e un nome utente e una password di sola lettura per il software CV. L'utente deve essere definito nel software CV.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati HP EVA. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Gruppo di dischi	Gruppo di dischi (non modellato)
Cella di storage	Storage

Disco virtuale	Pool di storage
Disco virtuale	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti di inventario

- Indirizzo IP del server CV
- Nome utente e password di sola lettura per il software CV. L'utente deve essere definito nel software CV.
- Software di terze parti installato sul server/RAU OnCommand Insight: `sssu.exe`. Il `sssu.exe` La versione deve corrispondere alla versione del CV.
- Convalida dell'accesso: Eseguire `sssu.exe` comandi che utilizzano nome utente e password.

Requisiti relativi alle performance

La suite software HP StorageWorks Command View EVA deve essere installata sul server OnCommand Insight. In alternativa, è possibile installare un'unità di acquisizione remota (RAU) sul server EVA:

1. Installare la suite software HP StorageWorks Command View EVA sul server OnCommand Insight o installare un'unità di acquisizione remota sul server Command View EVA.
2. Individuare il `evaperf.exe` comando. Ad esempio, `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Utilizzando l'indirizzo IP del server Command View, attenersi alla seguente procedura:
   a. Eseguire questo comando, dove 860 è la porta predefinita `Evaperf.exe server <Command View Server IP\> 860 <username\>`
   b. Inserire la password del server Command View al prompt della password.

      Questo dovrebbe restituire un prompt della riga di comando e nient'altro.
4. Verificare la configurazione eseguendo `evaperf.exe ls`.

   Viene visualizzato un elenco di array o controller gestiti dal server Command View. Ogni riga mostra un controller su un array EVA.

Configurazione

Campo	Descrizione
Server CommandView	Indirizzo IP o nome di dominio completo di EVA Storage Manager
Nome utente	Nome utente del gestore Command View. Il nome deve essere definito nella visualizzazione dei comandi.

Password	Password utilizzata per Command View Manager.
Performance User Name (Nome utente performance)	Per le prestazioni, il nome utente del gestore Command View. Il nome deve essere definito nella visualizzazione dei comandi.
Password delle performance	Per le prestazioni, la password utilizzata per il gestore Command View.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Home page di CLI	Percorso completo alla home directory CLI dove `sssu.exe` si trova
Inventario Escludi i dispositivi	Elenco separato da virgole dei nomi dei dispositivi da includere
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Performance CLI Home	Per Array Performance, nome percorso completo della home directory CLI dove si trova sssu.exe. Per convalidare l'accesso, eseguire `sssu.exe`
Timeout comando (sec)	`evaperf` timeout di attesa del comando (impostazione predefinita: 600 secondi)
Performance Escludi i dispositivi	Elenco separato da virgole dei nomi dei dispositivi da escludere dalla raccolta dei dati sulle prestazioni

Origine dei dati agile HPE

L'agile data collector HPE supporta dati di inventario e performance per gli array storage agili HPE.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati HPE agile. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight

Array	Storage
Disco	Disco
Piscina	Pool di storage
Volume	Volume
Iniziatore	Alias host storage
Controller	Nodo di storage
Interfaccia Fibre Channel	Controller

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- L'array deve essere installato e configurato e raggiungibile dal client tramite il relativo FQDN (Fully Qualified Domain Name) o l'indirizzo IP di gestione dell'array.
- L'array deve eseguire NimbleOS 2.3.x o versione successiva.
- È necessario disporre di un nome utente e di una password validi per l'array.
- La porta 5392 deve essere aperta sull'array.

Configurazione

Campo	Descrizione
Array Management IP Address (Indirizzo IP gestione array)	FQDN (Fully Qualified Domain Name) o indirizzo IP di gestione dell'array.
Nome utente	Nome utente dell'array nimble
Password	Password per l'array nimble

Configurazione avanzata

Campo	Descrizione
Porta	Porta utilizzata da nimble REST API. Il valore predefinito è 5392.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)

Nota: L'intervallo di polling delle prestazioni predefinito è di 300 secondi e non può essere modificato. Questo è l'unico intervallo supportato da nimble.

Fonte dei dati di Huawei OceanStor

OnCommand Insight utilizza l'origine dati REST/HTTPS (Huawei OceanStor) per rilevare l'inventario dello storage Huawei OceanStor.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario e performance da Huawei OceanStor. Per ogni tipo di risorsa acquisita da OnCommand Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine OnCommand Insight
Pool di storage	Pool di storage
File System	Volume interno
Controller	Nodo di storage
Porta FC (mappata)	Mappa del volume
Iniziatore FC host (mappato)	Maschera di volume
Condivisione NFS/CIFS	Condividere
Condividere	Nodo di destinazione iSCSI
ISCSI link Initiator	Nodo iniziatore iSCSI
Disco	Disco
LUN	Volume

Requisiti

Di seguito sono riportati i requisiti per configurare e utilizzare questo data collector:

- IP del dispositivo
- Credenziali per accedere a OceanStor Device Manager
- La porta 8088 deve essere disponibile

Configurazione

Campo	Descrizione

Indirizzo IP host OceanStor	Indirizzo IP o nome di dominio completo di OceanStor Device Manager
Nome utente	Nome utilizzato per accedere a OceanStor Device Manager
Password	Password utilizzata per accedere a OceanStor Device Manager

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione a OceanStor Device Manager (impostazione predefinita: 8088)
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)

Fonte di dati IBM Cleversafe

Questa fonte di dati raccoglie i dati di inventario e performance per IBM Cleversafe.

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Manager IP Address (Indirizzo IP gestore) o host Name (Nome host
- Un nome utente e una password per lo stesso
- Porta 9440

Configurazione

Campo	Descrizione
Nome host o indirizzo IP del gestore Cleversafe	Indirizzo IP host del dispositivo CleverSafe
Nome utente	Nome utilizzato per accedere a Cleversafe
Password	Password utilizzata per accedere a Cleversafe

Configurazione avanzata

Campo	Descrizione

Intervallo polling inventario (min)	Il valore predefinito è 60 minuti
Timeout connessione HTTP)	Il valore predefinito è 60 secondi

Origine dati IBM DS

L'origine dati IBM DS (CLI) supporta solo i dispositivi DS6xxx e DS8xxx. I dispositivi DS3xxx, DS4xxx e DS5xxx sono supportati dall'origine dati NetApp e-Series. Per i modelli e le versioni del firmware supportati, fare riferimento alla matrice di supporto di Insight Data Source.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati IBM DS. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Modulo unità disco	Disco
Immagine di storage	Storage
Pool di estensione	Pool di storage
Volume a blocchi fisso	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP di ciascun array DS
- Storage Display Name è opzionale e solo cosmetico
- Nome utente e password di sola lettura su ciascun array DS
- Software di terze parti installato sul server Insight: IBM dscli
- Convalida dell'accesso: Eseguire `dscli` comandi che utilizzano il nome utente e la password
- Requisiti delle porte: 80, 443 e 1750

Configurazione

Campo	Descrizione
Storage DS	Indirizzo IP o nome di dominio completo di DS Storage host

Nome utente	Nome utilizzato per la CLI DS
Password	Password utilizzata per la CLI DS
Percorso eseguibile dscli.exe	Percorso completo di `dscli.exe`utility.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Nome visualizzato dello storage	Nome dello storage array IBM DS
Inventario Escludi i dispositivi	Elenco separato da virgole dei numeri di serie dei dispositivi da escludere dalla raccolta dell'inventario
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Tipo di filtro delle prestazioni	Includi: Dati raccolti solo dai dispositivi presenti nell'elenco. Escludi: Non vengono raccolti dati da questi dispositivi
Elenco dispositivi filtro prestazioni	Elenco separato da virgole degli ID dei dispositivi da includere o escludere dalla raccolta delle performance

Origine dati IBM PowerVM

L'origine dati IBM PowerVM (SSH) raccoglie informazioni sulle partizioni virtuali in esecuzione sulle istanze hardware IBM POWER gestite da una console di gestione hardware (HMC). Per la configurazione, questa origine dati richiede il nome utente per accedere a HMC tramite SSH e l'autorizzazione a livello di visualizzazione per le configurazioni HMC.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati di IBM PowerVM. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
hdisk	Disco virtuale

Sistema gestito	Host
Server LPAR, VIO	Macchina virtuale
Gruppo di volumi	Data Store
Volume fisico	LUN

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP della console di gestione hardware (HMC)
- Nome utente e password che forniscono l'accesso a HMC tramite SSH
- Requisito di porta SSH-22
- Visualizzare l'autorizzazione su tutti i sistemi di gestione e i domini di protezione delle partizioni logiche

  L'utente deve anche disporre dell'autorizzazione View per le configurazioni HMC e della capacità di raccogliere le informazioni VPD per il raggruppamento di sicurezza della console HMC. L'utente deve anche essere autorizzato all'accesso a Virtual io Server Command nel gruppo di protezione partizione logica. È consigliabile iniziare da un ruolo di operatore e rimuovere tutti i ruoli. Gli utenti di sola lettura su HMC non dispongono dei privilegi necessari per eseguire i comandi proxy sugli host AIX.

- La Best practice di IBM consiste nel fare in modo che i dispositivi siano monitorati da due o più HMCS. Tenere presente che questo potrebbe causare la segnalazione di dispositivi duplicati da parte di OnCommand Insight, pertanto si consiglia vivamente di aggiungere dispositivi ridondanti all'elenco "Escludi dispositivi" nella configurazione avanzata per questo data collector.

Configurazione

Campo	Descrizione
Indirizzo HMC (hardware Management Console)	Indirizzo IP o nome di dominio completo della console di gestione hardware PowerVM
Utente HMC	Nome utente della console di gestione hardware
Password	Password utilizzata per la console di gestione hardware

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)

Porta SSH	Porta utilizzata per SSH su PowerVM
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 600 secondi)
Numero di tentativi	Numero di tentativi di inventario
Escludi dispositivi	Elenco separato da virgole degli ID dei dispositivi o dei nomi visualizzati da escludere

Origine dati IBM SVC

L'origine dati IBM SVC raccoglie dati di inventario e performance utilizzando SSH, supportando una varietà di dispositivi che eseguono il sistema operativo SVC. L'elenco dei dispositivi supportati include modelli come SVC, v7000, v5000 e v3700. Per informazioni sui modelli e le versioni del firmware supportati, fare riferimento alla matrice di supporto di Insight Data Source.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati IBM SVC. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
Gruppo Mdisk	Pool di storage
Disco virtuale	Volume
Mdisk	LUN back-end

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti di inventario

- Indirizzo IP di ciascun cluster SVC
- Porta 22 disponibile
- Coppia di chiavi pubbliche e private generate con Insight o riutilizzate una coppia di chiavi già in uso nel

vostro SVC

Se stai riutilizzando una coppia di chiavi esistente, devi convertirle dal formato Putty al formato OpenSSH.

- Chiave pubblica installata nel cluster SVC
- La chiave privata deve essere identificata nell'origine dati
- Convalida dell'accesso: Aprire `ssh` Sessione al cluster SVC utilizzando la chiave privata

> Non è necessario installare software di terze parti.

Requisiti relativi alle performance

- SVC Console, obbligatoria per qualsiasi cluster SVC e richiesta per il pacchetto di base Discovery SVC.
- Livello di accesso amministrativo richiesto solo per la copia dei file di dati delle performance dai nodi del cluster al nodo di configurazione.

> Poiché questo livello di accesso non è richiesto per il pacchetto di rilevamento della base SVC, l'utente della base SVC potrebbe non funzionare correttamente.

- Porta 22 richiesta
- Per questo utente deve essere generata una chiave SSH pubblica e privata, in modo che sia accessibile dall'unità di acquisizione. Se l'utente di base SVC dispone delle autorizzazioni appropriate, lo stesso utente e la stessa chiave funzionano. La stessa chiave SSH può essere utilizzata per i dati di inventario e performance.
- Abilitare la raccolta dati connettendosi al cluster SVC tramite SSH ed eseguendo: `svctask startstats -interval 1`

> In alternativa, abilitare la raccolta dati utilizzando l'interfaccia utente di gestione SVC.

Spiegazione del numero di serie principale

Tradizionalmente Insight è in grado di riportare il numero di serie dello storage array o i numeri di serie dei singoli nodi di storage. Tuttavia, alcune architetture di storage array non sono perfettamente allineate a questo. Un cluster SVC può essere composto da 1-4 appliance e ogni appliance ha 2 nodi. Se l'appliance dispone di un numero di serie, tale numero non corrisponde né al numero di serie del cluster né ai nodi.

L'attributo "Parent Serial Number" (numero di serie principale) sull'oggetto del nodo di storage viene popolato in modo appropriato per gli array IBM SVC quando i singoli nodi si trovano all'interno di un'appliance/enclosure intermedia che fa parte di un cluster più grande.

Configurazione

Campo	Descrizione
IP cluster/s.	Indirizzo IP del nome di dominio completo per lo storage SVC
Scegliere 'Password' o 'OpenSSH Key file' per specificare il tipo di credenziale	Il tipo di credenziale utilizzato per la connessione al dispositivo tramite SSH

Nome utente inventario	Nome utente per la CLI SVC
Password inventario	Password per la CLI SVC
Percorso completo alla chiave privata di inventario	Percorso completo al file delle chiavi private di inventario
Performance User Name (Nome utente performance)	Nome utente di SVC CLC per la raccolta delle performance
Password delle performance	Password per SVC CLC per la raccolta delle performance
Percorso completo alla chiave privata delle performance	Percorso completo del file delle chiavi private Performance

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Escludi dispositivi	Elenco separato da virgole degli ID dei dispositivi da escludere dalla raccolta dell'inventario
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 200 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)
Performance Escludi i dispositivi	Elenco separato da virgole degli ID dei dispositivi da escludere dalla raccolta delle performance
Timeout attesa processo SSH performance (sec)	Timeout processo SSH (impostazione predefinita: 200 secondi)
Per ripulire i file stats scaricati	Selezionare per eliminare i file di statistiche scaricati

Origine dati IBM Tivoli Monitoring

Questa origine dati viene utilizzata esclusivamente per l'utilizzo del file system. Comunica direttamente con il database di monitoraggio di Tivoli, noto anche come database di monitoraggio di Tivoli. Sono supportati i database Oracle e DB2.

Messaggio di errore Oracle

Questo data collector non è più disponibile a partire da OnCommand Insight 7.3.11.

Se il SID specificato genera il messaggio di errore "ora-12154" quando si tenta di connettersi, controllare due volte la configurazione del servizio di rete Oracle DB. Se la configurazione di accesso specifica un nome host completo (ad esempio, "NAMES.DEFAULT_DOMAIN"), provare a inserire il nome del servizio completo nel campo SID. Un semplice esempio è che la connessione al SID `testdb` Si sta guastando e la configurazione Oracle specifica un dominio di`company.com`. È possibile utilizzare la seguente stringa al posto del SID di base per tentare la connessione: `testdb.company.com`.

Configurazione

Campo	Descrizione
IP del database di monitoraggio Tivoli	Indirizzo IP o nome di dominio completo del server di monitoraggio Tivoli
Nome utente	Nome utente del server di monitoraggio Tivoli
Password	Password per il server di monitoraggio Tivoli

Configurazione avanzata

Campo	Descrizione
Porta del database di monitoraggio Tivoli	Porta utilizzata per il database di monitoraggio Tivoli
Oracle SID o DB2 Database Name (Nome database DB2)	ID servizio listener Oracle o nome database DB2
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Driver di database da utilizzare	Scegliere driver database da utilizzare
Protocollo utilizzato per la connessione al database	Protocollo utilizzato per la connessione al database
Schema del database	Inserire lo schema del database

Origine dati IBM TotalStorage DS4000

Questa fonte di dati raccoglie informazioni sull'inventario e sulle performance. Esistono due configurazioni possibili (firmware 6.x e 7.x+), entrambe con gli stessi valori. L'API raccoglie le statistiche dei dati del volume.

Configurazione

Campo	Descrizione
Elenco separato da virgole degli IP controller SANtricity array	Indirizzi IP o nomi di dominio pienamente qualificati dei controller, separati da virgole

Requisiti

- Indirizzo IP di ciascun array DS5 o FAStT
- Access validation (convalida accesso): Ping dell'indirizzo IP di entrambi i controller su ciascun array.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 30 minuti)
Intervallo di polling delle performance (fino a 3600 secondi)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Origine dati IBM XIV

L'inventario delle origini dati IBM XIV (CLI) viene eseguito utilizzando l'interfaccia della riga di comando XIV. Le prestazioni di XIV si possono ottenere effettuando chiamate SMI-S all'array XIV, che esegue un provider SMI-S sulla porta 5989.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati di IBM XIV. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Sistema storage	Storage
Pool di storage	Pool di storage
Volume	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Requisiti della porta: Porta TCP 7778
- Indirizzo IP dell'interfaccia di gestione XIV
- Nome utente e password di sola lettura
- XIV CLI deve essere installato sul server Insight o RAU
- Convalida dell'accesso: Accedere all'interfaccia utente XIV dal server Insight utilizzando il nome utente e la password.

Configurazione

Campo	Descrizione
Indirizzo IP	Indirizzo IP o nome di dominio completo per lo storage XIV
Nome utente	Nome utente dello storage XIV
Password	Password per lo storage XIV
Percorso completo alla directory CLI XIV	Percorso completo alla directory XIV CLI

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 40 minuti)
Timeout attesa processo CLI (ms)	Timeout processo CLI (impostazione predefinita: 7200000 ms)
IP HOST SMI-S.	Indirizzo IP dell'host del provider SMI-S.
Porta SMI-S.	Porta utilizzata dall'host del provider SMI-S.
Protocollo SMI-S.	Protocollo utilizzato per connettersi al provider SMI-S.
Spazio dei nomi SMI-S.	Spazio dei nomi SMI-S.
Nome utente	Nome utente dell'host del provider SMI-S.
Password	Password per l'host del provider SMI-S.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Numero di tentativi di connessione SMI-S.	Numero di tentativi di connessione SMI-S.

Fonte di dati Infinidat InfiniBox

L'origine dati Infinidat InfiniBox (HTTP) viene utilizzata per raccogliere informazioni dallo storage Infinidat InfiniBox. È necessario disporre dell'accesso a InfiniBox Management Node.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati InfiniBox. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
InfiniBox	Storage
Nodo	Nodo di storage
Piscina	Pool di storage
Volume	Volume
Porta FC	Porta
Filesystem	Volume interno
Filesystem	FileShare
Esportazioni di file system	Condividere

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Configurazione

Campo	Descrizione
Host InfiniBox	Indirizzo IP o nome di dominio completo di InfiniBox Management Node
Nome utente	Nome utente di InfiniBox Management Node

Password	Password per InfiniBox Management Node

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione a InfiniBox Server (impostazione predefinita: 443)
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Timeout connessione	Timeout di connessione (impostazione predefinita: 60 secondi)

Origine dei dati di calcolo di Microsoft Azure

OnCommand Insights utilizza Azure Compute Data Collector per acquisire dati di inventario e performance dalle istanze di calcolo di Azure.

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Requisito porta: 443 HTTPS
- IP REST di Azure Management (management.azure.com)
- Azure Service Principal Application (Client) ID (account utente)
- Chiave di autenticazione Azure Service Principal (password utente)

Devi configurare un account Azure per Insight Discovery. Una volta configurato correttamente l'account e registrato l'applicazione in Azure, si disporranno delle credenziali necessarie per rilevare l'istanza di Azure con Insight. Il seguente collegamento descrive come configurare l'account per il rilevamento:https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configurazione

Inserire i dati nei campi dell'origine dati in base alla tabella riportata di seguito:

Campo	Descrizione
Azure Service Principal Application (Client) ID (ruolo di lettore richiesto)	ID di accesso ad Azure. Richiede l'accesso al ruolo Reader.
ID tenant Azure	ID tenant Microsoft
Chiave di autenticazione principale del servizio Azure	Chiave di autenticazione per l'accesso

Ho capito che Microsoft mi ha dato la bolletta per le richieste API	Controlla questa sezione per verificare che Microsoft ti presenti la fattura per le richieste API effettuate tramite il polling Insight.

Configurazione avanzata

Inserire i dati nei campi dell'origine dati in base alla tabella riportata di seguito:

Campo	Descrizione
Intervallo polling inventario (min)	Il valore predefinito è 60
Scegliere "Escludi" o "Includi" per applicare il filtro delle macchine virtuali in base ai tag	Specificare se includere o escludere le macchine virtuali in base ai tag durante la raccolta dei dati. Se si seleziona 'include', il campo Tag Key non può essere vuoto.
Tag Key e valori su cui filtrare le macchine virtuali	Fare clic su **+ Filter Tag** (Tag filtro) per scegliere quali macchine virtuali (e dischi associati) includere/escludere filtrando le chiavi e i valori corrispondenti alle chiavi e ai valori dei tag sulla macchina virtuale. Tag Key è obbligatorio, Tag Value è facoltativo. Quando il valore Tag è vuoto, la VM viene filtrata finché corrisponde alla chiave Tag.
Performance poll Interval (sec)	

Origine dati Azure NetApp Files

Questa origine dati acquisisce i dati di inventario e performance per Azure NetApp Files (ANF).

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Requisito porta: 443 HTTPS
- IP REST di Azure Management (management.azure.com)
- Azure Service Principal Application (Client) ID (account utente)
- Chiave di autenticazione Azure Service Principal (password utente)
- È necessario impostare un account Azure per il rilevamento Cloud Insights.

  Una volta configurato correttamente l'account e registrata l'applicazione in Azure, si disporranno delle credenziali necessarie per rilevare l'istanza di Azure con Cloud Insights. Il seguente collegamento descrive come configurare l'account per il rilevamento:

  https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal

Configurazione

Campo	Descrizione
Azure Service Principal Application (Client) ID	ID di accesso ad Azure
ID tenant Azure	ID tenant Azure
Chiave di autenticazione principale del servizio Azure	Chiave di autenticazione per l'accesso
Ho capito che Microsoft mi ha dato la bolletta per le richieste API	Controlla questa sezione per verificare che Microsoft ti presenti la fattura per le richieste API effettuate tramite il polling Insight.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Il valore predefinito è 60 minuti

Origine dati Microsoft Hyper-V.

Per la configurazione, l'origine dati Microsoft Hyper-V richiede l'indirizzo IP o il nome DNS risolvibile per l'host fisico (hypervisor). Questa origine dati utilizza PowerShell (precedentemente utilizzato WMI).

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati Hyper-V. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco rigido virtuale	Disco virtuale
Host	Host
Macchina virtuale	Macchina virtuale
Cluster Shared Volumes (CSV), Volume di partizione	Data Store
Dispositivo SCSI Internet, LUN SCSI Multi Path	LUN
Porta Fibre Channel	Porta

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Hyper-V richiede l'apertura della porta 5985 per la raccolta dei dati e l'accesso/gestione remota.
- Indirizzo IP del nodo del gruppo di clustering
- User e password dell'amministratore locale sull'hypervisor
- Account utente di livello amministrativo
- Requisiti delle porte: Porta 135 e porte TCP dinamiche assegnate 1024-65535 per Windows 2003 e versioni precedenti e 49152-65535 per Windows 2008.
- La risoluzione DNS deve avere successo, anche se il data collector è rivolto solo a un indirizzo IP.
- Ogni hypervisor Hyper-V deve avere "Resource Metering" attivato per ogni macchina virtuale, su ogni host. Ciò consente a ciascun hypervisor di avere più dati disponibili per Cloud Insights su ciascun guest. In caso contrario, vengono acquisite meno metriche di performance per ciascun ospite. Per ulteriori informazioni sulla misurazione delle risorse, consultare la documentazione microsoft:

  "Panoramica sulla misurazione delle risorse Hyper-V."

  "Enable-VMResourceMetering"

Configurazione

Campo	Descrizione
Indirizzo IP host fisico	L'indirizzo IP o il nome di dominio completo per l'host fisico (hypervisor)
Nome utente	Nome utente amministratore dell'hypervisor
Password	Password per l'hypervisor
Dominio NT	Il nome DNS utilizzato dai nodi nel cluster

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout connessione (ms)	Timeout connessione (impostazione predefinita: 60000 ms)

Fonte dei dati NetApp Clustered Data ONTAP

Questa origine dati deve essere utilizzata per i sistemi storage che utilizzano Clustered Data ONTAP e richiede un account amministratore utilizzato per le chiamate API di sola lettura.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati Clustered Data ONTAP. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Gruppo RAID	Gruppo di dischi
Cluster	Storage
Nodo	Nodo di storage
Aggregato	Pool di storage
LUN	Volume
Volume	Volume interno

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Account amministratore utilizzato per le chiamate API di sola lettura
- L'IP di destinazione è la LIF di gestione del cluster
- Nome utente (con nome ruolo di sola lettura per l'applicazione ontapi sul Vserver predefinito) e password per accedere al cluster NetApp
- Requisiti delle porte: 80 o 443
- Requisiti di licenza: Licenza FCP e volumi mappati/mascherati necessari per il rilevamento

Configurazione

Campo	Descrizione
IP di gestione NetApp	Indirizzo IP o nome di dominio completo del cluster NetApp
Nome utente	Nome utente del cluster NetApp
Password	Password per il cluster NetApp

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Storage Clustered Data ONTAP

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse di storage NetApp Clustered Data ONTAP.

Terminologia dello storage Clustered Data ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse di storage NetApp Clustered Data ONTAP. Molti di questi termini si applicano anche ad altri data collezionisti.

- Modello — un elenco delimitato da virgole dei nomi dei modelli di nodi discreti univoci all'interno di questo cluster. Se tutti i nodi nei cluster sono dello stesso tipo di modello, viene visualizzato un solo nome di modello.
- Vendor — stesso nome del vendor che si vedrebbe se si configurasse una nuova origine dati.
- Serial number (numero di serie) - il numero di serie dell'array. Nei sistemi di storage con architettura cluster come NetApp Clustered Data ONTAP, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie "nodi di torage `S`".
- IP — in genere sono gli IP o i nomi host configurati nell'origine dati.
- Versione del microcodice — firmware.
- Capacità raw — somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza — una rappresentazione di ciò che stanno sperimentando i carichi di lavoro dell'host, sia in lettura che in scrittura. Idealmente, OCI sta reperendo questo valore direttamente, ma spesso non è così. Al posto dell'array che offre questo up, OCI sta generalmente eseguendo un calcolo ponderato per gli IOPS derivato dalle statistiche dei singoli volumi interni'.
- Throughput — aggregato da volumi interni.
- Gestione — potrebbe contenere un collegamento ipertestuale per l'interfaccia di gestione del dispositivo. Creato a livello di programmazione dall'origine dati Insight come parte del reporting dell'inventario.

Pool di storage Clustered Data ONTAP

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse del pool di storage NetApp Clustered Data ONTAP.

Terminologia del pool di storage Clustered Data ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse del pool di NetApp Clustered Data ONTAPstorage. Molti di questi termini si applicano anche ad altri data collezionisti.

- Storage — su quale array di storage vive questo pool. Obbligatorio.

- Type — un valore descrittivo da un elenco di un elenco enumerato di possibilità. Il più comunemente sarà “aggregate” o “RAID Group”`".
- Nodo — se l’architettura di questo array di storage è tale che i pool appartengano a un nodo di storage specifico, il suo nome verrà visualizzato qui come un collegamento ipertestuale alla propria landing page.
- Utilizza Flash Pool — valore Sì/No — questo pool basato su SATA/SAS dispone di SSD utilizzati per l’accelerazione del caching?
- Ridondanza — livello RAID o schema di protezione. RAID_DP è a doppia parità, RAID_TP è a tripla parità.
- Capacità — i valori qui sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, e la percentuale utilizzata per questi.
- Capacità con overcommit — se utilizzando le tecnologie di efficienza è stata allocata una somma totale di capacità di volume o volume interno superiore alla capacità logica del pool di storage, il valore percentuale qui sarà maggiore dello 0%.
- Snapshot — le capacità di snapshot utilizzate e totali, se l’architettura del pool di storage dedica parte della sua capacità a segmentare le aree esclusivamente per le snapshot. È probabile che le configurazioni ONTAP in MetroCluster mostrino questo aspetto, mentre le altre configurazioni ONTAP lo dimostrano meno.
- Utilizzo — un valore percentuale che indica la percentuale massima di occupato su disco di qualsiasi disco che contribuisce alla capacità di questo pool di storage. L’utilizzo dei dischi non ha necessariamente una forte correlazione con le performance degli array: L’utilizzo potrebbe essere elevato a causa di ricostruzioni dei dischi, attività di deduplica, ecc. in assenza di carichi di lavoro basati su host. Inoltre, le implementazioni di replica di molti array` possono guidare l’utilizzo dei dischi senza essere visualizzati come volumi interni o carichi di lavoro di volume.
- IOPS - la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di storage.
- Throughput - la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di storage.

Nodo di storage Clustered Data ONTAP

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse dei nodi di storage NetApp Clustered Data ONTAP.

Terminologia dei nodi di storage Clustered Data ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse del pool di storage NetApp Clustered Data ONTAP. Molti di questi termini si applicano anche ad altri data collezionisti.

- Storage — a quale array di storage fa parte questo nodo. Obbligatorio.
- Partner HA — sulle piattaforme in cui un nodo eseguirà il failover su un nodo e solo su un altro nodo, in genere viene visualizzato qui.
- Stato — integrità del nodo. Disponibile solo quando l’array è abbastanza integro da essere inventorato da un’origine dati.
- Modello — nome del modello del nodo.
- Version — nome della versione del dispositivo.
- Serial number (numero di serie) - il numero di serie del nodo.
- Memoria — memoria base 2, se disponibile.
- Utilizzo — in ONTAP, si tratta di un indice di stress del controller da un algoritmo proprietario. Con ogni sondaggio sulle performance, viene riportato un numero compreso tra 0 e 100%, che è il più alto tra il

conflitto del disco WAFL o l'utilizzo medio della CPU. Se si osservano valori sostenuti > 50%, ciò è indicativo di un sottodimensionamento — potenzialmente un controller/nodo non sufficientemente grande o non abbastanza dischi rotanti per assorbire il carico di lavoro di scrittura.

- IOPS — derivato direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Latenza — derivata direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Throughput — derivato direttamente dalle chiamate ONTAP ZAPI sull'oggetto nodo.
- Processori — numero di CPU.

NetApp Clustered Data ONTAP per l'origine dati di Unified Manager

Questa origine dati raccoglie i dati di ONTAP 8.1.x dal database Unified Manager (UM) 6.0+. Utilizzando questa origine dati, Insight rileva tutti i cluster configurati e popolati in UM. Per l'efficienza, Insight non chiama ZAPI sul cluster stesso. Le performance non sono supportate in questa origine dati.

Configurazione

Questo data collector non è più disponibile a partire da OnCommand Insight 7.3.11.

Campo	Descrizione
IP di Unified Manager	Indirizzo IP o nome di dominio completo di Unified Manager
Nome utente	Nome utente di Unified Manager
Password	Password per Unified Manager
Porta	Porta utilizzata per la comunicazione con Unified Manager (impostazione predefinita: 3306)

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 15 minuti)
Escludi cluster	Elenco separato da virgole degli IP del cluster da escludere

NetApp Data ONTAP che opera in un'origine dati 7-Mode

Per i sistemi storage che utilizzano il software Data ONTAP in 7-Mode, è necessario utilizzare l'origine dati ONTAPI, che utilizza l'interfaccia CLI per ottenere i numeri di capacità.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati NetApp Data ONTAP 7-Mode. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Gruppo RAID	Gruppo di dischi
Filer	Storage
Filer	Nodo di storage
Aggregato	Pool di storage
LUN	Volume
Volume	Volume interno

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP del partner e del controller di storage FAS
- Porta 443
- Nome utente e password del controller e del partner
- Un nome utente e una password personalizzati a livello di amministratore per controller e partner controller con le seguenti funzionalità di ruolo per 7-Mode:
  - "api-*": Utilizzare questa opzione per consentire a OnCommand Insight di eseguire tutti i comandi API dello storage NetApp.
  - "Login-http-admin": Consente a OnCommand Insight di connettersi allo storage NetApp tramite HTTP.
  - "Security-api-vfiler": Utilizzare questa opzione per consentire a OnCommand Insight di eseguire i comandi API dello storage NetApp per recuperare le informazioni sull'unità vFiler.
  - "cli-options" (Opzioni cli): Consente di leggere le opzioni del sistema di storage.
  - "cli-lun": Consente di accedere a questi comandi per la gestione delle LUN. Visualizza lo stato (percorso LUN, dimensione, stato online/offline e stato condiviso) del LUN o della classe di LUN.
  - "cli-df": Consente di visualizzare lo spazio libero su disco.
  - "cli-ifconfig": Consente di visualizzare interfacce e indirizzi IP.

Configurazione

Campo	Descrizione
Indirizzo del filer	Indirizzo IP o nome di dominio completo per NetApp Filer
Nome utente	Nome utente del filer NetApp
Password	Password per NetApp Filer
Indirizzo di ha Partner Filer nel cluster	Indirizzo IP o nome di dominio completo per ha Partner Filer
Nome utente di ha Partner Filer nel cluster	Nome utente per NetApp ha Partner Filer
Password di ha Partner Filer nel cluster	Password per NetApp ha Partner Filer

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Tipo di connessione	Scegliere il tipo di connessione
Porta di connessione	Porta utilizzata per le API NetApp
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Connessione ai sistemi storage

In alternativa all'utilizzo dell'utente amministrativo predefinito per questa origine dati, è possibile configurare un utente con diritti amministrativi direttamente sui sistemi storage NetApp in modo che questa origine dati possa acquisire dati dai sistemi storage NetApp.

La connessione ai sistemi storage NetApp richiede che l'utente, specificato al momento dell'acquisizione del filer principale (su cui è presente il sistema storage), soddisfi le seguenti condizioni:

- L'utente deve trovarsi su vfiler0 (root filer/pfiler).

  I sistemi storage vengono acquisiti quando si acquisisce il pfiler principale.

- I seguenti comandi definiscono le funzionalità del ruolo utente:
  - "api-*": Utilizzare questa opzione per consentire a OnCommand Insight di eseguire tutti i comandi API dello storage NetApp. Questo comando è necessario per utilizzare ZAPI.
  - "Login-http-admin": Consente a OnCommand Insight di connettersi allo storage NetApp tramite HTTP.

Questo comando è necessario per utilizzare ZAPI.

- "Security-api-vfiler": Utilizzare questa opzione per consentire a OnCommand Insight di eseguire i comandi API dello storage NetApp per recuperare le informazioni sull'unità vFiler.
- "cli-options": Per il comando "options" e utilizzato per l'IP del partner e le licenze abilitate.
- " cli-lun": Consente di accedere a questi comandi per la gestione delle LUN. Visualizza lo stato (percorso LUN, dimensione, stato online/offline e stato condiviso) del LUN o della classe di LUN.
- "cli-df": Per i comandi "df -s", "df -r", "df -A -r" e utilizzato per visualizzare lo spazio libero.
- "cli-ifconfig": Per il comando "ifconfig -a" e utilizzato per ottenere l'indirizzo IP del filer.
- "cli-rdfile": Per il comando "rdfile /etc/netgroup" e utilizzato per ottenere netgroup.
- "cli-date": Per il comando "date" e utilizzato per ottenere la data completa per ottenere le copie Snapshot.
- "cli-SNAP": Per il comando "snap-list" e utilizzato per ottenere le copie Snapshot.

Se non vengono fornite le autorizzazioni cli-date o cli-SNAP, l'acquisizione può terminare, ma le copie Snapshot non vengono segnalate.

Per acquisire correttamente un'origine dati 7-Mode e non generare avvisi sul sistema di storage, è necessario utilizzare una delle seguenti stringhe di comando per definire i ruoli utente. La seconda stringa qui elencata è una versione semplificata della prima:

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-
df,cli-lun,cli-ifconfig,cli-date,cli-snap,
or
login-http-admin,api-*,security-api-vfile,cli-*
```

Fonte di dati NetApp e-Series

L'origine dei dati NetApp e-Series raccoglie informazioni sull'inventario e sulle performance. Esistono due configurazioni possibili (firmware 6.x e firmware 7.x+), entrambe con gli stessi valori.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati NetApp e-Series. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Gruppo di volumi	Gruppo di dischi
Array di storage	Storage

Controller	Nodo di storage
Gruppo di volumi	Pool di storage
Volume	Volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- L'indirizzo IP di ciascun controller dell'array
- Requisito di porta 2463

Configurazione

Campo	Descrizione
Elenco separato da virgole degli IP controller SANtricity array	Indirizzi IP e/o nomi di dominio pienamente qualificati per i controller degli array

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 30 minuti)
Intervallo di polling delle performance (fino a 3600 secondi)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Storage e-Series

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse di storage NetApp e-Series.

Terminologia dello storage e-Series

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse di storage NetApp e-Series. Molti di questi termini si applicano anche ad altri data collezionisti.

- Modello — nome del modello del dispositivo.
- Vendor — stesso nome del vendor che si vedrebbe se si configurasse una nuova origine dati.
- Serial number (numero di serie) - il numero di serie dell'array. Nei sistemi di storage con architettura cluster come NetApp Clustered Data ONTAP, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie "nodi di torage `S`".
- IP — in genere sono gli IP o i nomi host configurati nell'origine dati.

- Versione del microcodice — firmware.
- Capacità raw — somma di base 2 di tutti i dischi fisici nel sistema, indipendentemente dal loro ruolo.
- Latenza — una rappresentazione di ciò che stanno sperimentando i carichi di lavoro dell'host, sia in lettura che in scrittura. Insight calcola una media ponderata degli IOPS derivata dai volumi nello storage.
- Throughput: Il throughput totale dell'host dell'array. Insight somma il throughput dei volumi` per derivare questo valore.
- Gestione — potrebbe contenere un collegamento ipertestuale per l'interfaccia di gestione del dispositivo. Creato a livello di programmazione dall'origine dati Insight come parte del reporting dell'inventario.

Pool di storage e-Series

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse del pool di storage NetApp e-Series.

Terminologia del pool di storage e-Series

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse del pool di storage NetApp e-Series. Molti di questi termini si applicano anche ad altri data collezionisti.

- Storage — su quale array di storage vive questo pool. Obbligatorio.
- Type — un valore descrittivo da un elenco di un elenco enumerato di possibilità. La maggior parte dei casi sarà "Thin Provisioning" o "RAID Group".
- Nodo — se l'architettura di questo array di storage è tale che i pool appartengano a un nodo di storage specifico, il suo nome verrà visualizzato qui come un collegamento ipertestuale alla propria landing page.
- Utilizza il valore di Flash Pool — Sì/No.
- Ridondanza — livello RAID o schema di protezione. E-Series riporta "RAID 7" per i pool DDP.
- Capacità — i valori qui sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, e la percentuale utilizzata per questi. Entrambi questi valori includono la capacità "preservation" di e-Series, che consente di ottenere numeri e percentuali superiori a quelli visualizzati dall'interfaccia utente di e-Series.
- Capacità con overcommit — se utilizzando le tecnologie di efficienza è stata allocata una somma totale di capacità di volume superiore alla capacità logica del pool di storage, il valore percentuale qui sarà maggiore dello 0%.
- Snapshot — le capacità di snapshot utilizzate e totali, se l'architettura del pool di storage dedica parte della sua capacità a segmentare le aree esclusivamente per le snapshot.
- Utilizzo - valore percentuale che indica la percentuale massima di occupato su disco di qualsiasi disco che contribuisce alla capacità di questo pool di storage. L'utilizzo dei dischi non ha necessariamente una forte correlazione con le performance degli array: L'utilizzo potrebbe essere elevato a causa di ricostruzioni dei dischi, attività di deduplica, ecc. in assenza di carichi di lavoro basati su host. Inoltre, le implementazioni di replica di molti array` possono guidare l'utilizzo del disco senza essere visualizzate come workload di volume.
- IOPS - la somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di storage.
- Throughput - la somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di storage.

Nodo storage e-Series

Termini applicabili a oggetti o riferimenti che si possono trovare nelle landing page delle risorse dei nodi di storage NetApp e-Series.

Terminologia dei nodi di storage e-Series

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse del pool di storage NetApp e-Series. Molti di questi termini si applicano anche ad altri data collezionisti.

- Storage — a quale array di storage fa parte questo nodo. Obbligatorio.
- Partner HA — sulle piattaforme in cui un nodo eseguirà il failover su un nodo e solo su un altro nodo, in genere viene visualizzato qui.
- Stato — integrità del nodo. Disponibile solo quando l'array è abbastanza integro da essere inventorato da un'origine dati.
- Modello — nome del modello del nodo.
- Version — nome della versione del dispositivo.
- Serial number (numero di serie) - il numero di serie del nodo.
- Memoria — memoria base 2, se disponibile.
- Utilizzo — l'utilizzo non è attualmente disponibile per NetApp e-Series.
- IOPS — calcolato sommando tutti gli IOPS per i volumi che appartengono esclusivamente a questo nodo.
- Latency (latenza) - un numero che rappresenta la latenza tipica dell'host o il tempo di risposta su questo controller. Insight calcola una media ponderata degli IOPS dai volumi che appartengono esclusivamente a questo nodo.
- Throughput - un numero che rappresenta il throughput basato su host su questo controller. Calcolato sommando tutto il throughput per i volumi che appartengono esclusivamente a questo nodo.
- Processori — numero di CPU.

Origine dei dati dei file system host e VM di NetApp

È possibile utilizzare l'origine dati dei file system VM e host di NetApp per recuperare i dettagli del file system e le mappature delle risorse di storage per tutti i file system host e VM (macchine virtuali) di Microsoft Windows e per tutte le macchine virtuali Linux supportate (solo quelle virtualmente mappate) Esistenti nel server Insight annotati con il gruppo di risorse di calcolo (CRG) configurato.

Requisiti generali

- Questa funzione deve essere acquistata separatamente.

  Per assistenza, contatta il tuo rappresentante Insight.

- Controllare la matrice di supporto Insight per verificare che il sistema operativo host o della macchina virtuale sia supportato.

  Per verificare che vengano creati collegamenti dai file system alle risorse di storage, verificare che il tipo e la versione del vendor di storage o virtualizzazione rilevanti segnalino i dati di identificazione del volume o del disco virtuale richiesti.

Requisiti di Microsoft Windows

- Questa origine dati utilizza strutture di dati WMI (Window Management Instrumentation) per recuperare i dati.

  Questo servizio deve essere operativo e disponibile in remoto. In particolare, la porta 135 deve essere accessibile e deve essere aperta se dietro un firewall.

- Gli utenti di dominio Windows devono disporre delle autorizzazioni appropriate per accedere alle strutture WMI.
- Sono necessarie le autorizzazioni di amministratore.
- Porte TCP dinamiche assegnate 1024-65535 per Windows 2003 e versioni precedenti
- Porte 49152-65535 per Windows 2008

> Come regola generale, quando si tenta di utilizzare un firewall tra Insight, un AU e questa origine dati, è necessario consultare il team Microsoft per identificare le porte che ritengono necessarie.

Requisiti Linux

- Questa origine dati utilizza una connessione Secure Shell (SSH) per eseguire comandi sulle macchine virtuali Linux.

  Il servizio SSH deve essere operativo e disponibile in remoto. In particolare, la porta 22 deve essere accessibile e deve essere aperta se dietro un firewall.

- Gli utenti SSH devono disporre dei permessi sudo per eseguire i comandi di sola lettura sulle macchine virtuali Linux.

  Devi utilizzare la stessa password per accedere a SSH e per rispondere a qualsiasi sfida relativa alla password di sudo.

Consigli per l'utilizzo

- Annotare un gruppo di host e macchine virtuali con credenziali comuni del sistema operativo utilizzando la stessa annotazione del gruppo di risorse di calcolo.

  Ogni gruppo dispone di un'istanza di questa origine dati che individua i dettagli del file system da tali host e macchine virtuali.

- Se si dispone di un'istanza di questa origine dati per la quale il tasso di successo è basso (ad esempio, OnCommand Insight sta rilevando i dettagli del file system solo per 50 host su 1000 e macchine virtuali in un gruppo), È necessario spostare gli host e le macchine virtuali per cui il rilevamento ha esito positivo in un gruppo di risorse di calcolo separato.

Configurazione

Campo	Descrizione

Nome utente	Utente del sistema operativo con diritti appropriati per recuperare i dati del file system per gli utenti del sistema operativo Windows, questo deve includere il prefisso di dominio.
Password	Password per l'utente del sistema operativo
Gruppo di risorse di calcolo	Il valore di annotazione utilizzato per contrassegnare le macchine host e virtuali per l'origine dati rileva i file system.Un valore vuoto indica che l'origine dati rileva i file system per tutti gli host e le macchine virtuali non attualmente annotati con alcun gruppo di risorse di calcolo.

Configurazione avanzata

Campo	Descrizione
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 360 minuti)

Fonte dei dati NetApp SolidFire

L'origine dati NetApp SolidFire supporta configurazioni iSCSI e Fibre Channel SolidFire, sia per l'inventario che per la raccolta delle performance.

L'origine dati SolidFire utilizza l'API REST di SolidFire. L'unità di acquisizione in cui risiede l'origine dati deve essere in grado di avviare connessioni HTTPS alla porta TCP 443 sull'indirizzo IP di gestione del cluster SolidFire. L'origine dati necessita di credenziali in grado di eseguire query API REST sul cluster SolidFire.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati NetApp SolidFire. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
Volume	Volume
Porta Fibre Channel	Porta

Gruppo di accesso al volume, assegnazione LUN	Mappa del volume
Sessione iSCSI	Maschera di volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Indirizzo IP virtuale di gestione
- Porta 443

Configurazione

Campo	Descrizione
Management Virtual IP Address (MVIP) (Indirizzo IP virtuale di gestione)	Indirizzo IP virtuale di gestione del cluster SolidFire
Nome utente	Nome utilizzato per accedere al cluster SolidFire
Password	Password utilizzata per accedere al cluster SolidFire

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Porta TCP	Porta TCP utilizzata per la connessione al server SolidFire (impostazione predefinita: 443)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Risoluzione dei problemi

Quando SolidFire segnala un errore, viene visualizzato in OnCommand Insight come segue:

```
An error message was received from a SolidFire device while trying to retrieve
data. The call was <method> (<parameterString> ). The error message from the
device was (check the device manual): <message>
```

Dove:

- <method> è un metodo HTTP, ad esempio GET o PUT.
- <parameterString> è un elenco separato da virgole di parametri inclusi nella chiamata DI PAUSA.
- Il <message> corrisponde a quello che il dispositivo ha restituito come messaggio di errore.

Fonte dei dati NetApp StorageGRID

Questa fonte di dati raccoglie i dati di inventario e performance per StorageGRID.

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Indirizzo IP host StorageGRID
- Nome utente e password per un utente a cui sono stati assegnati i ruoli di Metric Query e accesso tenant
- Porta 443

Configurazione

Campo	Descrizione
Indirizzo IP host StorageGRID (MVIP)	Host IP address (Indirizzo IP host) di StorageGRID
Nome utente	Nome utilizzato per accedere a StorageGRID
Password	Password utilizzata per accedere a StorageGRID

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 900 secondi)

Origine dati OpenStack

L'origine dati OpenStack (REST API / KVM) raccoglie informazioni sulle istanze hardware di OpenStack. Questa origine dati raccoglie i dati di inventario per tutte le istanze di OpenStack e, facoltativamente, i dati sulle performance delle macchine virtuali.

Requisiti

Di seguito sono riportati i requisiti per la configurazione dell'origine dati OpenStack.

- Indirizzo IP del controller OpenStack

- Si consigliano le credenziali del ruolo di amministratore di OpenStack e l'accesso sudo all'hypervisor KVM Linux.

> Se non si utilizza un account admin o privilegi equivalenti, è comunque possibile acquisire dati dall'origine dati. Sarà necessario modificare il file di configurazione dei criteri (ad esempio etc/nova/policy.json) per consentire agli utenti con ruolo non amministrativo di chiamare l'API:

  - "os_compute_api:os-availability-zone:detail": ""
  - "os_compute_api:hypervisor del sistema operativo": ""
  - os_compute_api:server:dettaglio:get_all_tenant": ""
- Per la raccolta delle performance, il modulo OpenStack Ceilometer deve essere installato e configurato. La configurazione del Ceilometer viene eseguita modificando il `nova.conf` File per ciascun hypervisor e riavviare il servizio Nova Compute su ciascun hypervisor. Il nome dell'opzione cambia per le diverse versioni di OpenStack:
  - Icehouse
  - Juno
  - Chilo
  - Libertà
  - Mitaka
  - Newton
  - Ocata
- Per le statistiche CPU, "compute_monitors=ComputeDriverCPUMonitor" deve essere attivato in /etc/nova/nova.conf sui nodi di calcolo.
- Requisiti delle porte:
  - 5000 per http e 13000 per https, per il servizio Keystone
  - 22 per KVM SSH
  - 8774 per Nova Compute Service
  - 8776 per Cinder Block Service
  - 8777 per Ceilometer Performance Service
  - 9292 per Glance Image Service

> La porta viene associata al servizio specifico e il servizio può essere eseguito sul controller o su un altro host in ambienti più grandi.

Configurazione

Campo	Descrizione
Indirizzo IP controller OpenStack	Indirizzo IP o nome di dominio completo del controller OpenStack
Amministratore di OpenStack	Nome utente di un amministratore OpenStack

Password OpenStack	Password utilizzata per OpenStack Admin
Tenant amministratore OpenStack	Tenant amministratore OpenStack
Utente KVM sudo	Nome utente di KVM sudo
Scegliere 'Password' o 'OpenSSH Key file' per specificare il tipo di credenziale	Il tipo di credenziale utilizzato per la connessione al dispositivo tramite SSH
Percorso completo alla chiave privata di inventario	Percorso completo alla chiave privata di inventario
Password KVM sudo	Password KVM sudo

Configurazione avanzata

Campo	Descrizione
Abilita il rilevamento dell'inventario dell'hypervisor tramite SSH	Selezionare questa opzione per abilitare il rilevamento dell'inventario dell'hypervisor tramite SSH
Porta URL OpenStack Admin	Porta URL OpenStack Admin
Utilizzare HTTPS	Selezionare per utilizzare HTTP sicuro
Timeout connessione HTTP (sec)	Timeout per connessione HTTP (impostazione predefinita: 300 secondi)
Porta SSH	Porta utilizzata per SSH
Timeout attesa processo SSH (sec)	Timeout processo SSH (impostazione predefinita: 30 secondi)
Tentativi di processo SSH	Numero di tentativi di inventario
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)

Origine dati Oracle ZFS

L'origine dati Oracle ZFS supporta la raccolta di inventario e performance.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario da questa origine dati. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco (SDD)	Disco
Cluster	Storage
Controller	Nodo di storage
LUN	Volume
Mappa LUN	Mappa del volume
Iniziatore, destinazione	Maschera di volume
Condividere	Volume interno

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questa origine dati:

- Nomi host per ZFS Controller-1 e ZFS Controller-2
- Nome utente e credenziali dell'amministratore
- Requisito porta: 215 HTTP/HTTPS

Configurazione

Nome host controller-1 ZFS	Nome host del controller di storage 1
Nome host controller-2 ZFS	Nome host del controller di storage 2
Nome utente	Nome utente dell'account utente amministratore del sistema di storage
Password	Password per l'account utente amministratore

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione a ZFS (impostazione predefinita: 215)

Tipo di connessione	HTTP o HTTPS
Intervallo di polling dell'inventario	Intervallo di polling dell'inventario (impostazione predefinita: 60 minuti)
Timeout connessione	Il valore predefinito è 60 secondi
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Risoluzione dei problemi

Alcune operazioni da eseguire in caso di problemi con questo data collector:

Problema:	Prova:
"Credenziali di accesso non valide"	Convalidare l'account utente e la password ZFS
"Errore di configurazione" con messaggio di errore "reServizio ST disattivato"	Verificare che il servizio REST sia attivato su questo dispositivo.
"Errore di configurazione " con messaggio di errore "utente non autorizzato per il comando"	Probabilmente a causa di determinati ruoli (ad esempio, "Advanced_analytics") non sono inclusi per l'utente configurato <userName>.soluzione possibile: • Correggere l'ambito di Analytics (statistica) per l'utente{user} con il ruolo di sola lettura:- dalla schermata Configuration → Users (Configurazione utenti), posizionare il mouse sul ruolo e fare doppio clic per consentire la modifica • Selezionare "Analytics" (analisi) dal menu a discesa Scope (ambito). Viene visualizzato un elenco delle proprietà possibili. • Fare clic sulla casella di controllo più in alto per selezionare tutte e tre le proprietà.- fare clic sul pulsante Add (Aggiungi) sul lato destro. • Fare clic sul pulsante Apply (Applica) nella parte superiore destra della finestra a comparsa. La finestra a comparsa si chiude.

Origine dati pure Storage FlashArray

L'origine dati pure Storage FlashArray (HTTP) viene utilizzata per raccogliere informazioni da pure Storage Flash Array. Insight supporta sia l'inventario che la raccolta delle performance.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati pure Storage FlashArray. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco (SSD)	Disco
Array	Storage
Controller	Nodo di storage
Volume	Volume
Porta	Porta
LUN Map (host, gruppo host, porta di destinazione)	Mappa del volume, maschera del volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP del sistema di storage
- Nome utente e password dell'account Administrator del sistema di storage pure.
- Requisito porta: HTTP/HTTPS 80/443

Configurazione

Campo	Descrizione
Host FlashArray	Indirizzo IIP o nome di dominio completo di FlashArray Management Server
Nome utente	Nome utente di FlashArray Management Server
Password	Password per FlashArray Management Server

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Server di gestione

Porta TCP	Porta TCP utilizzata per la connessione al server FlashArray (impostazione predefinita: 443)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 60 minuti)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi di perfromance (impostazione predefinita: 300 secondi)

Origine dati QLogic FC Switch

Per la configurazione, l'origine dati QLogic FC Switch (SNMP) richiede l'indirizzo di rete del dispositivo FC Switch, specificato come indirizzo IP, e una stringa di comunità SNMP di sola lettura utilizzata per accedere al dispositivo.

Configurazione

Campo	Descrizione
Switch SANsurfer	Indirizzo IP o nome di dominio completo per lo switch SANSurfer
Versione SNMP	Versione SNMP
Community SNMP	Stringa di comunità SNMP
Nome utente	Nome utente dello switch SANSurfer
Password	Password per lo switch SANSurfer

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 15 minuti)
Protocollo SNMP Auth	Protocollo di autenticazione SNMP (solo SNMPv3)
Tentativi SNMP	Numero di tentativi SNMP
Timeout SNMP (ms)	Timeout SNMP (impostazione predefinita: 5000 ms)

Attivare il trapping	Selezionare per attivare il trapping
Tempo minimo tra trap (sec)	Tempo minimo tra i tentativi di acquisizione attivati da trap (impostazione predefinita: 10 secondi)
Nome fabric	Nome del fabric che deve essere segnalato dall'origine dati. Lasciare vuoto per riportare il nome del fabric come WWN.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Origine dati Red Hat (RHEV)

L'origine dati Red Hat Enterprise Virtualization (REST) raccoglie informazioni sulle istanze RHEV tramite HTTPS.

Requisiti

- Indirizzo IP del server RHEV sulla porta 443 tramite API REST
- Nome utente e password di sola lettura
- RHEV versione 3.0+

Configurazione

Campo	Descrizione
Indirizzo IP del server RHEV	Indirizzo IP o nome di dominio completo del server RHEV
Nome utente	Nome utente del server RHEV
Password	Password utilizzata per il server RHEV

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione HTTPS	Porta utilizzata per la comunicazione HTTPS con RHEV
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)

Origine dati Violin Flash Memory Array

L'origine dati HTTP (Flash Memory Array) di Violin 6000-Series raccoglie le informazioni di rete per l'analisi e la convalida dagli array di memoria flash serie 6000 di Violin.

Terminologia

Questo data collector non è più disponibile a partire da OnCommand Insight 7.3.11.

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati dell'array di memoria flash serie 6000 di Violin. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Modulo VIMM (Intelligent Memory Module) per violino	Disco
Container	Storage
Gateway di memoria	Nodo di storage
LUN	Volume
Initiator, Initiator Group, Target	Mappa del volume, maschera del volume

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Sono necessari un nome utente e una password di sola lettura per lo storage.
- Convalidare l'accesso con un browser Web utilizzando l'indirizzo IP dello storage.

Configurazione

Campo	Descrizione
Indirizzo IP o FQDN del gateway principale dell'array di memoria violino	Indirizzo IP o nome di dominio completo del gateway principale di Violin Memory Array
Nome utente	Nome utente del gateway principale di Violin Memory Array
Password	Password per il gateway principale di Violin Memory Array

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione	Porta utilizzata per la comunicazione con array Violin
HTTPS attivato	Selezionare per utilizzare HTTPS
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout connessione (sec)	Timeout di connessione (impostazione predefinita: 60 secondi)
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Fonte dei dati VMware vSphere

L'origine dati di VMware vSphere (Web Services) raccoglie le informazioni dell'host ESX e richiede privilegi di sola lettura su tutti gli oggetti all'interno del Virtual Center.

Terminologia

OnCommand Insight acquisisce le seguenti informazioni di inventario dall'origine dati di VMware vSphere. Per ogni tipo di risorsa acquisita da Insight, viene mostrata la terminologia più comune utilizzata per questa risorsa. Durante la visualizzazione o la risoluzione dei problemi di questa origine dati, tenere presente la seguente terminologia:

Vendor/modello	Termine Insight
Disco virtuale	Disco
Host	Host
Macchina virtuale	Macchina virtuale
Data Store	Data Store
LUN	LUN
Porta Fibre Channel	Porta

Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa origine dati.

Requisiti

- Indirizzo IP del server Virtual Center
- Nome utente e password di sola lettura in Virtual Center
- Privilegi di sola lettura su tutti gli oggetti all'interno del Virtual Center.
- Accesso all'SDK sul server Virtual Center
- Requisiti delle porte: http-80 https-443
- Convalidare l'accesso accedendo a Virtual Center Client utilizzando il nome utente e la password e verificando che l'SDK sia abilitato immettendo `telnet <vc_ip\> 443`.

Configurazione

Campo	Descrizione
Virtual Center Address (Indirizzo centro virtuale)	Indirizzo di rete del Virtual Center o del server vSphere, specificato come indirizzo IP *(nnn.nnn.nnn.nnn.nnn* format) o come nome host che può essere risolto tramite DNS.
Nome utente	Nome utente del server VMware.
Password	Password per il server VMware.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (impostazione predefinita: 20 minuti)
Timeout connessione (ms)	Timeout connessione (impostazione predefinita: 60000 ms)
Filtra le VM in base a.	Scegliere come filtrare le macchine virtuali
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere l'elenco delle macchine virtuali riportato di seguito durante la raccolta dei dati

Elenco di macchine virtuali da filtrare (separate da virgole o separate da punto e virgola se nel valore viene utilizzata una virgola)	Elenco di macchine virtuali separate da virgole o da punto e virgola da includere o escludere dal polling
Numero di tentativi per le richieste a vCenter	Numero di tentativi di richiesta vCenter
Porta di comunicazione	Porta utilizzata per il server VMware
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle prestazioni (impostazione predefinita: 300 secondi)

Modifica delle credenziali dell'origine dati

Se più origini dati dello stesso tipo condividono un nome utente e una password, è possibile modificare la password per tutte le periferiche del gruppo contemporaneamente.

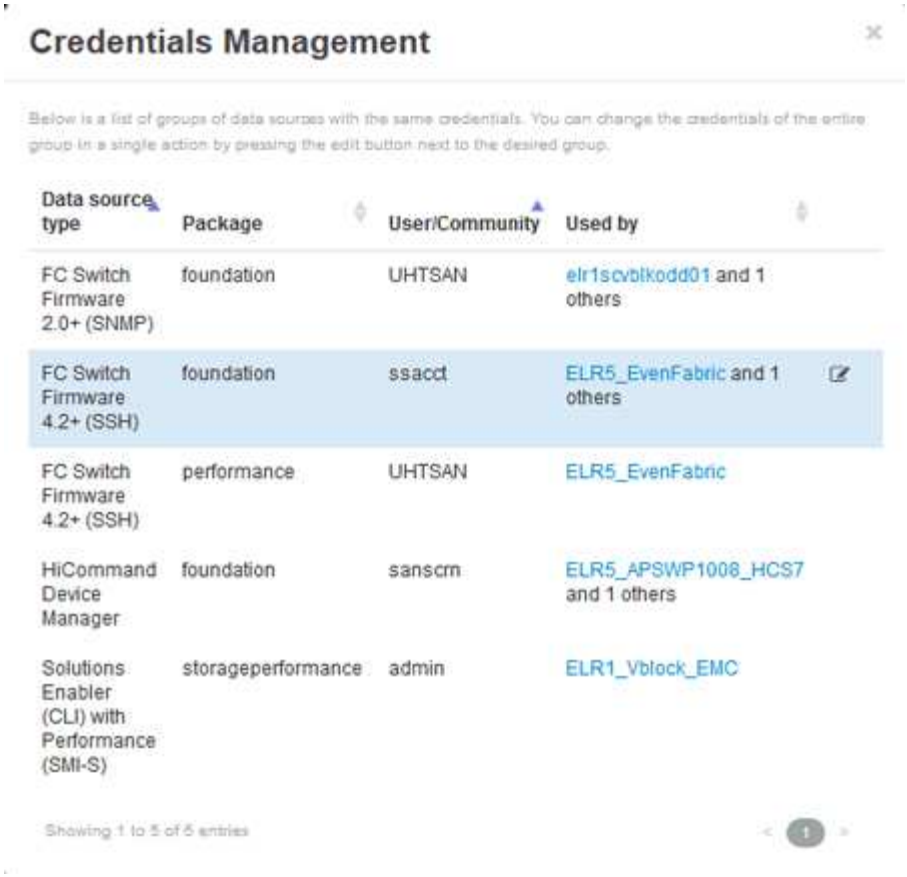
Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.

   Viene visualizzato l'elenco **origini dati**.

2. Fare clic sul pulsante **azioni** e selezionare l'opzione **Modifica credenziali**.
3. Nella finestra di dialogo Credentials Management (Gestione credenziali), selezionare uno dei gruppi di origine dati dall'elenco.

   L'icona Modifica, una penna su un foglio di carta, diventa attiva a destra.



4. Fare clic su **Edit** (Modifica).
5. Inserire la nuova password e confermarla.

Modifiche che causano problemi di raccolta dei dati

Se si verificano problemi di raccolta dati in OnCommand Insight, è probabile che le modifiche nell'ambiente siano la causa principale. Come regola generale di manutenzione, è necessario tenere conto anche di eventuali modifiche nell'ambiente in Insight.

È possibile utilizzare questo elenco di controllo per identificare le modifiche alla rete che potrebbero causare problemi:

- Hai modificato le password? Tali password sono state modificate in Insight?
- Hai rimosso una periferica dalla rete? È inoltre necessario rimuovere il dispositivo da OnCommand Insight per evitare che venga riscoperto e reintrodotto.
- Hai aggiornato il software dell'infrastruttura (ad esempio HP CommandView EVA o EMC Solutions Enabler)?

  Assicurarsi che sull'unità di acquisizione siano installate le versioni appropriate degli strumenti client. Se i guasti dell'origine dati persistono, è necessario contattare il supporto tecnico per richiedere assistenza ed eventualmente una patch dell'origine dati.

- Tutte le unità di acquisizione OnCommand Insight utilizzano la stessa versione di OnCommand Insight? Se le unità di acquisizione remota e l'unità di acquisizione locale utilizzano versioni OnCommand Insight diverse, installare la stessa versione su tutte le unità per correggere il problema di raccolta dei dati.

Se è necessario installare una nuova versione di OnCommand Insight su tutte le unità di acquisizione, accedere al sito di supporto e scaricare la versione corretta.

- Sono stati modificati nomi di dominio o aggiunti nuovi domini? È necessario aggiornare i metodi di risoluzione del dispositivo (in precedenza Auto Resolution).

Analisi dettagliata di un'origine dati

Se si rileva un errore o un rallentamento di un'origine dati, è possibile esaminare un riepilogo dettagliato delle informazioni relative a tale origine dati per determinare la causa del problema. Le origini dati con condizioni che richiedono attenzione sono contrassegnate da un cerchio rosso pieno.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.

   Viene visualizzato l'elenco **origini dati**. Tutte le origini dati elencate con potenziali problemi sono contrassegnate da un cerchio rosso fisso. I problemi più gravi sono in cima alla lista.

2. Selezionare l'origine dati che causa il problema.
3. Fare clic sul collegamento relativo al nome dell'origine dati.
4. Nella pagina di riepilogo dell'origine dati, controllare le informazioni in una delle seguenti sezioni:
   - **Timeline dell'evento**

     Elenca gli eventi legati allo stato corrente visualizzato nell'elenco origini dati. Gli eventi in questo riepilogo vengono visualizzati per dispositivo. Gli errori sono visualizzati in rosso. È possibile posizionare il puntatore del mouse sugli elementi della timeline per visualizzare ulteriori informazioni.

   - **Dispositivi segnalati da questa origine dati**

     Elenca i tipi di periferiche, i relativi indirizzi IP e i collegamenti a informazioni più dettagliate per ciascuna periferica.

   - **Modifiche segnalate da questa fonte di dati (ultime 3 settimane)**

     Elenca tutti i dispositivi aggiunti o rimossi o che hanno subito modifiche alla configurazione.

5. Dopo aver esaminato le informazioni relative all'origine dati, è possibile eseguire una di queste operazioni utilizzando i pulsanti nella parte superiore della pagina:
   - **Modifica** la descrizione dell'origine dati per correggere il problema.
   - **Polling again** forza il polling a rivelare se il problema era persistente o intermittente.
   - **Posticipare** il polling dell'origine dati per 3, 7 o 30 giorni per consentirti di cercare il problema e interrompere i messaggi di avviso.
   - **Installare una patch** sull'origine dati per risolvere il problema.
   - Preparare un **report degli errori** per il supporto tecnico.
   - **Elimina** l'origine dati dall'ambiente di monitoraggio Insight.

Ricerca di un’origine dati guasta

Se un’origine dati visualizza il messaggio "**Inventory failed !**" o "**Performance failed !**" e un impatto alto o medio, è necessario ricercare questo problema utilizzando la pagina di riepilogo dell’origine dati con le relative informazioni collegate.

Fasi

1. Fare clic sul collegamento **Nome** dell’origine dati per aprire la pagina Riepilogo.
2. Nella pagina Summary (Riepilogo), consultare l’area **Comments** (commenti) per leggere eventuali note lasciate da un altro tecnico che potrebbe anche indagare su questo guasto.
3. Annotare eventuali messaggi relativi alle prestazioni.
4. Se è stata applicata una patch a questa origine dati, fare clic sul collegamento per controllare la pagina **patch** per verificare se il problema è stato causato.
5. Spostare il puntatore del mouse sui segmenti del grafico **Timeline evento** per visualizzare ulteriori informazioni.
6. Selezionare un messaggio di errore per un dispositivo e visualizzato sotto la timeline dell’evento, quindi fare clic sull’icona **Dettagli errore** visualizzata a destra del messaggio.

   I dettagli relativi all’errore includono il testo del messaggio di errore, le cause più probabili, le informazioni in uso e i suggerimenti su come risolvere il problema.

7. Nell’area periferiche segnalate da questa origine dati, è possibile filtrare l’elenco in modo da visualizzare solo le periferiche di interesse, quindi fare clic sul collegamento **Nome** di una periferica per visualizzare la *pagina risorse* relativa a tale periferica.
8. Per tornare alle pagine visualizzate in precedenza, utilizzare una delle seguenti tecniche:
   - Fare clic sulla freccia indietro del browser.
   - Fare clic con il pulsante destro del mouse sulla freccia indietro per visualizzare un elenco delle pagine e selezionare la pagina desiderata.
9. Per visualizzare informazioni dettagliate sulle altre risorse, fare clic su altri nomi collegati.
10. Quando si torna alla pagina di riepilogo dell’origine dati, controllare l’area **Changes** nella parte inferiore della pagina per verificare se il problema è stato causato da modifiche recenti.

Controllo del polling dell’origine dati

Dopo aver apportato una modifica a un’origine dati, potrebbe essere necessario eseguire immediatamente il polling per verificare le modifiche oppure posticipare la raccolta di dati su un’origine dati per uno, tre o cinque giorni mentre si lavora su un problema.

Fasi

1. Fare clic su **Admin** e passare alla vista elenco origine dati
2. Selezionare l’origine dati per cui si desidera controllare il polling.
3. Fare clic sul collegamento relativo al nome dell’origine dati.
4. Nella pagina di riepilogo dell’origine dati, controllare le informazioni e fare clic su una di queste due opzioni di polling:

- **Eseguire nuovamente il polling** per forzare l'origine dati a raccogliere immediatamente i dati.
- **Posticipare** e selezionare la durata del ritardo di polling da 3, 7 o 30 giorni.

Al termine

Se la raccolta dati è stata posticipata su un'origine dati e si desidera riavviare la raccolta, fare clic su **Riprendi** nella pagina di riepilogo.

Modifica delle informazioni dell'origine dati

È possibile modificare rapidamente le informazioni di configurazione dell'origine dati.

Fasi

1. Fare clic su **Admin** e passare alla vista elenco origine dati
2. Individuare l'origine dati che si desidera modificare.
3. Utilizzare uno dei seguenti metodi per iniziare le modifiche:
   - Fare clic su **Edit data source** (Modifica origine dati) a destra dell'origine dati selezionata.
   - Fare clic sul nome collegato dell'origine dati selezionata e fare clic su **Edit** (Modifica). Entrambi i metodi aprono la finestra di dialogo Modifica origine dati.
4. Apportare le modifiche desiderate e fare clic su **Save** (Salva).

Modifica delle informazioni per più origini dati

È possibile modificare la maggior parte delle informazioni per più origini dati dello stesso fornitore e modello contemporaneamente. Ad esempio, se queste origini dati condividono un nome utente e una password, è possibile modificare la password in un'unica posizione e aggiornare la password per tutte le origini dati selezionate.

A proposito di questa attività

Le opzioni che non è possibile modificare per le origini dati selezionate appaiono in grigio o non vengono visualizzate nella finestra di dialogo Modifica origine dati. Inoltre, quando un'opzione visualizza il valore **Mixed**, il valore dell'opzione varia tra le origini dati selezionate. Ad esempio, se l'opzione **Timeout (sec)** per due origini dati selezionate è **Mixed**, un'origine dati potrebbe avere un valore di timeout pari a 60 e l'altra potrebbe avere un valore pari a 90; pertanto, se si modifica questo valore in 120 e si salvano le modifiche alle origini dati, l'impostazione di timeout per entrambe le origini dati diventa 120.

Fasi

1. Fare clic su **Admin** e passare alla vista elenco origine dati
2. Selezionare le origini dati che si desidera modificare. Le origini dati selezionate devono appartenere allo stesso vendor, modello e unità di acquisizione.
3. Fare clic sul pulsante **azioni** e selezionare l'opzione **Modifica**.
4. Nella finestra di dialogo di modifica, modificare le **Impostazioni** in base alle esigenze.
5. Fare clic sul collegamento **Configuration** (Configurazione) per modificare le opzioni di base per le origini dati.

6. Fare clic sul collegamento **Advanced Configuration** (Configurazione avanzata) per modificare le opzioni avanzate per le origini dati.
7. Fare clic su **Save** (Salva).

Mappatura dei tag di origine dei dati alle annotazioni

Quando un'origine dati è configurata per eseguire il polling dei dati dei tag, Insight imposta automaticamente i valori di annotazione per un'annotazione Insight esistente con lo stesso nome di un tag.

Quando l'annotazione Insight esiste prima che i tag siano attivati nell'origine dati, i dati del tag origine dati vengono aggiunti automaticamente all'annotazione Insight.

Quando si crea un'annotazione dopo l'attivazione del tag, il polling iniziale dell'origine dati non aggiorna automaticamente l'annotazione. Si verifica un ritardo nel tempo necessario per sostituire o popolare l'annotazione Insight. Per evitare il ritardo, è possibile forzare l'aggiornamento delle annotazioni posticipando e riprendendo l'origine dati.

Eliminazione di un'origine dati

Se è stata rimossa un'origine dati dall'ambiente, è necessario eliminarla anche dall'ambiente di monitoraggio di OnCommand Insight.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.

   Viene visualizzato l'elenco origini dati.

2. Selezionare l'origine dati che si desidera eliminare.
3. Fare clic sul nome dell'origine dati collegata.
4. Controllare le informazioni relative all'origine dati selezionata nella pagina di riepilogo per assicurarsi che si tratti dell'origine che si desidera eliminare.
5. Fare clic su **Delete** (Elimina).
6. Fare clic su **OK** per confermare l'operazione.

Quali patch di origine dati sono

Le patch di origine dati risolvono i problemi con le patch esistenti e consentono inoltre di aggiungere facilmente nuovi tipi di origine dati (vendor e modelli). Per ogni tipo di origine dati nella rete, è possibile caricare patch di origine dati. È inoltre possibile installare, testare e gestire il processo di patch. Tuttavia, per un tipo di origine dati può essere attiva una sola patch alla volta.

Per ciascuna patch, è possibile eseguire le seguenti operazioni:

- Controllare prima e dopo il confronto di ciascuna origine dati che riceve la patch.
- Scrivere commenti per spiegare le decisioni o riepilogare la ricerca.

- Apportare modifiche a un'origine dati che non risponde correttamente alla patch.
- Approvare la patch da applicare al server Insight.
- Eseguire il rollback di una patch che non funziona come desiderato.
- Sostituire una patch guasta con una diversa.

Applicazione di una patch di origine dati

Le patch per l'origine dei dati sono periodicamente disponibili e consentono di risolvere problemi con un'origine dati esistente, aggiungere un'origine dati per un nuovo vendor o aggiungere un nuovo modello per un vendor.

Prima di iniziare

È necessario aver ottenuto il `.zip` file che contiene l'origine dati più recente `.patch` file dal supporto tecnico.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.
3. Dal pulsante Actions (azioni), selezionare **Apply patch** (Applica patch).
4. Nella finestra di dialogo **Apply data source patch** (Applica patch origine dati), fare clic su **Browse** (Sfoglia) per individuare `.patch` file.
5. Esaminare i tipi di origine dei dati * * Patch name*, * Description* e * interessati*.
6. Se la patch selezionata è corretta, fare clic su **Apply Patch** (Applica patch).

   Se si sta applicando una patch che risolve i problemi con un'origine dati, tutte le origini dati dello stesso tipo vengono aggiornate con la patch ed è necessario approvare la patch. Le patch che non influiscono sulle origini dati configurate vengono approvate automaticamente.

Al termine

Se si applica una patch che aggiunge un'origine dati per un nuovo vendor o un nuovo modello, è necessario aggiungere l'origine dati dopo l'applicazione della patch.

Installazione di una patch su un tipo di origine dati

Dopo aver caricato una patch di origine dati, è possibile installarla su tutte le origini dati dello stesso tipo.

Prima di iniziare

È necessario aver caricato un file di patch che si desidera installare su un tipo di origine dati.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.
3. Dal pulsante Actions (azioni), selezionare **Apply patch** (Applica patch).

4. Nella finestra di dialogo **Apply data source patch** (Applica patch origine dati), fare clic su **Browse** (Sfoglia) per individuare il file di patch caricato.
5. Controllare i tipi di origine dati * * * Nome patch*, **Descrizione** e **origine dati interessata**.
6. Se la patch selezionata è corretta, fare clic su **Apply Patch** (Applica patch).

   Tutte le origini dati dello stesso tipo vengono aggiornate con questa patch.

Gestione delle patch

È possibile esaminare lo stato corrente di tutte le patch di origine dati applicate alla rete. Se si desidera eseguire un'azione su una patch, fare clic sul nome collegato nella tabella delle patch attualmente in esame.

Prima di iniziare

È necessario aver già caricato e installato almeno una patch.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.

   Se non viene installata alcuna patch, la tabella delle patch attualmente in esame è vuota.

3. In **patch attualmente in fase di revisione**, controllare lo stato delle patch dell'origine dati attualmente applicate.
4. Per esaminare i dettagli associati a una patch specifica, fare clic sul nome collegato della patch.
5. Per la patch selezionata, fare clic su una di queste opzioni per eseguire l'azione successiva sulla patch:
   - **Approva patch** commuta la patch alle origini dati.
   - **Rollback** rimuove la patch.
   - **Sostituisci patch** consente di selezionare una patch diversa per tali origini dati.

Eseguire il commit di una patch di origine dati

Le informazioni contenute nel riepilogo delle patch consentono di stabilire se le prestazioni della patch sono corrette e quindi di assegnare la patch alla rete.

Prima di iniziare

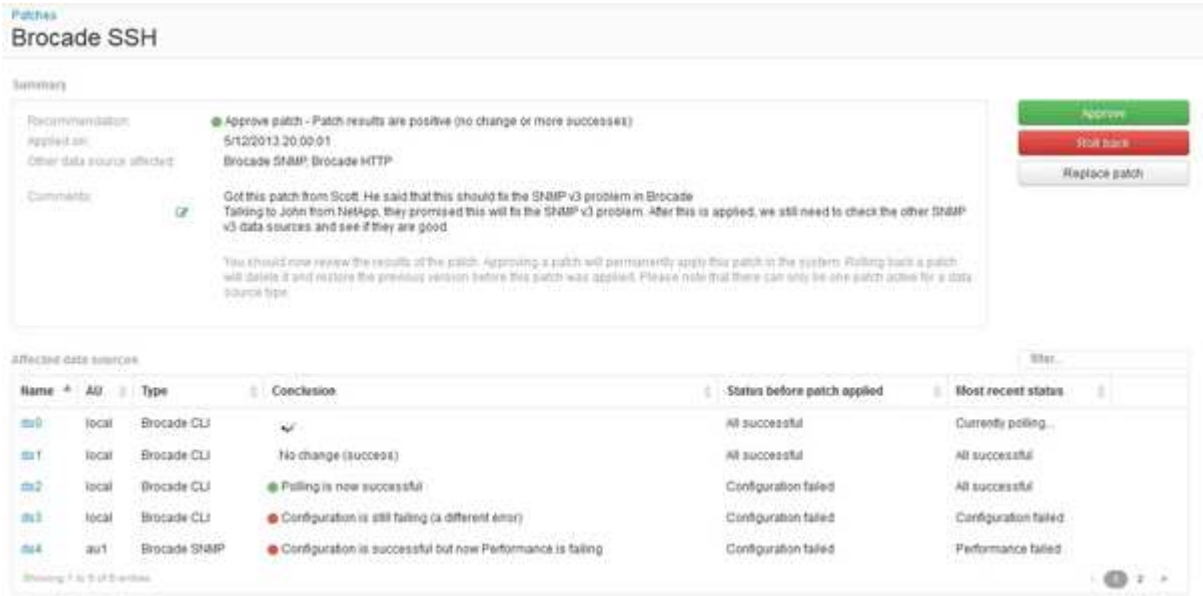
È stata installata una patch e occorre decidere se la patch è stata installata correttamente e deve essere approvata.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.

   Se non vengono installate patch, le patch attualmente in fase di revisione sono vuote.

3. In **patch attualmente in fase di revisione**, controllare lo stato delle patch dell'origine dati attualmente applicate.
4. Per esaminare i dettagli associati a una patch specifica, fare clic sul nome collegato della patch.
5. Nelle informazioni riepilogative sulle patch, mostrate in questo esempio, controllare i termini **Recommendation** e **Comments** per valutare l'avanzamento della patch.



6. Consultare la tabella **origini dati interessate** per visualizzare lo stato di ciascuna origine dati interessata prima e dopo la patch.

   Se si teme che si sia verificato un problema con una delle origini dati da applicare alle patch, fare clic sul nome collegato nella tabella origini dati interessate.

7. Se si conclude che la patch deve essere applicata a quel tipo di origine dati, fare clic su **approva**.

   Le origini dati vengono modificate e la patch viene rimossa dalle patch attualmente in fase di revisione.

Eseguire il rollback di una patch di origine dati

Se una patch di origine dati non funziona nel modo previsto, è possibile eseguire il rollback. Il rollback di una patch lo elimina e ripristina la versione precedente come prima dell'applicazione della patch.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.
3. In **Patch attualmente in fase di revisione**, fare clic sul nome collegato della patch che sembra non essere riuscita.
4. Nella pagina delle patch per l'origine dati, esaminare le seguenti informazioni:
   - **Summary** descrive quando è stata applicata la patch, le origini dati interessate e i commenti sulla patch forniti da te o da altri membri del tuo team.
   - **Origini dati interessate** elenca tutte le origini dati con patch e include un confronto dello stato prima e

dopo l'applicazione delle patch.

5. Per visualizzare i dettagli di un'origine dati che non sta elaborando correttamente la patch, fare clic sul collegamento **Nome**.
   a. Controllare le informazioni di riepilogo.
   b. Controllare la * timeline evento* per visualizzare eventuali dati di configurazione o performance che potrebbero influire su questa origine dati.
6. Se si conclude che la patch non avrà esito positivo, fare clic sulla freccia indietro del browser per tornare alla pagina di riepilogo delle patch.
7. Fare clic su **Ripristina** per rimuovere la patch.

   Se si conosce una patch diversa che potrebbe avere successo, fare clic su **Sostituisci patch** e caricare la nuova patch.

Risoluzione del dispositivo

È necessario individuare tutti i dispositivi che si desidera monitorare con OnCommand Insight. Il rilevamento è necessario per tenere traccia con precisione delle performance e dell'inventario nel tuo ambiente. In genere, la maggior parte dei dispositivi nell'ambiente viene rilevata tramite la risoluzione automatica dei dispositivi.

> Se si sta eseguendo un aggiornamento e nel sistema da cui si sta eseguendo l'aggiornamento sono presenti regole di risoluzione automatica inattive, queste verranno eliminate durante l'aggiornamento. Per mantenere le regole di risoluzione automatica inattive, attivare le regole (selezionare la casella) prima di eseguire l'aggiornamento.

Dopo aver installato e configurato le origini dati, vengono identificati i dispositivi nell'ambiente, inclusi switch, storage array e l'infrastruttura virtuale di hypervisor e macchine virtuali. Tuttavia, questo non identifica normalmente il 100% dei dispositivi nell'ambiente in uso.

Dopo aver configurato i dispositivi di origine dati, la procedura consigliata consiste nell'utilizzare le regole di risoluzione dei dispositivi per identificare i dispositivi sconosciuti rimanenti nell'ambiente. La risoluzione dei dispositivi può aiutare a risolvere i dispositivi sconosciuti come i seguenti tipi di dispositivi:

- host fisici
- storage array
- nastri
- switch

I dispositivi che rimangono come "sconosciuti" dopo la risoluzione del dispositivo sono considerati dispositivi generici, che è possibile visualizzare anche nelle query e nei dashboard.

Le regole create a loro volta identificheranno automaticamente i nuovi dispositivi con attributi simili man mano che vengono aggiunti all'ambiente. In alcuni casi, la risoluzione del dispositivo consente anche l'identificazione manuale ignorando le regole di risoluzione del dispositivo per i dispositivi non rilevati in Insight.

L'identificazione incompleta dei dispositivi può causare problemi quali:

- Percorsi incompleti

- Connessioni multipath non identificate
- L'impossibilità di raggruppare le applicazioni
- Viste topopologie imprecise
- Dati imprecisi nel data warehouse e report

La funzione di risoluzione del dispositivo (**Gestisci** > **risoluzione del dispositivo**) include le seguenti schede, ciascuna delle quali svolge un ruolo nella pianificazione della risoluzione del dispositivo e nella visualizzazione dei risultati:

- "FC Identify" contiene un elenco di WWN e informazioni sulle porte dei dispositivi Fibre Channel che non sono stati risolti mediante la risoluzione automatica dei dispositivi. La scheda identifica inoltre la percentuale di dispositivi identificati.
- "IP Identify" contiene un elenco di dispositivi che accedono alle condivisioni CIFS e NFS e che non sono stati identificati tramite la risoluzione automatica del dispositivo. La scheda identifica inoltre la percentuale di dispositivi identificati.
- "Auto resolution rules" (regole di risoluzione automatica) contiene l'elenco delle regole eseguite durante l'esecuzione della risoluzione del dispositivo Fibre Channel. Si tratta di regole create per risolvere i dispositivi Fibre Channel non identificati.
- "Preferences" (Preferenze) fornisce le opzioni di configurazione utilizzate per personalizzare la risoluzione del dispositivo per l'ambiente in uso.

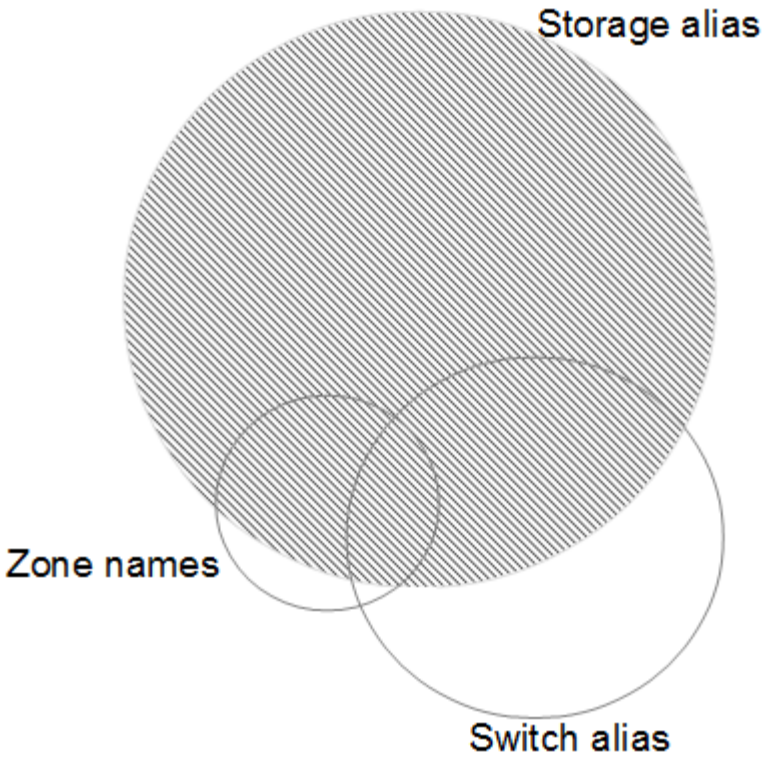
Prima di iniziare

Prima di definire le regole per l'identificazione dei dispositivi, è necessario conoscere la configurazione dell'ambiente. Più informazioni sull'ambiente, più facile sarà l'identificazione dei dispositivi.

Devi rispondere a domande simili a quelle riportate di seguito per aiutarti a creare regole precise:

- Il tuo ambiente dispone di standard di denominazione per zone o host e quale percentuale di questi è accurata?
- L'ambiente utilizza un alias dello switch o uno storage e corrispondono al nome host?
- Il tuo ambiente utilizza uno strumento SRM ed è possibile utilizzarlo per identificare i nomi host? Quale copertura offre l'SRM?
- Con quale frequenza cambiano gli schemi di denominazione nel tuo ambiente?
- Ci sono state acquisizioni o fusioni che hanno introdotto diversi schemi di denominazione?

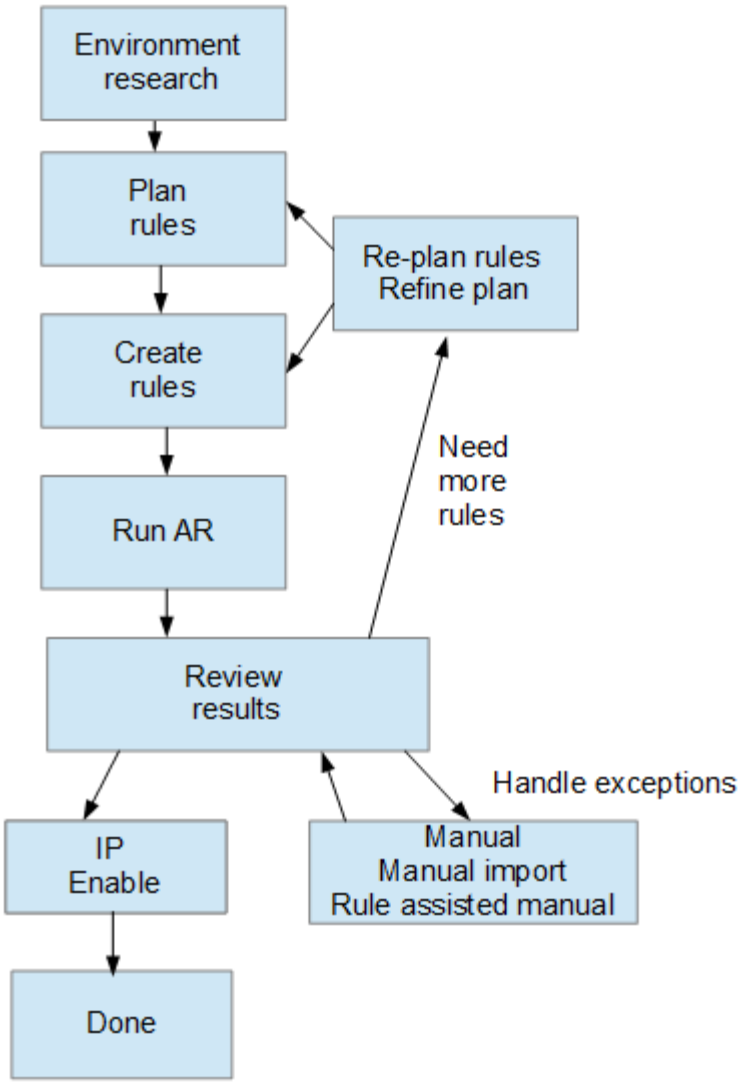
Dopo aver analizzato l'ambiente, dovresti essere in grado di identificare gli standard di denominazione esistenti che ci si può aspettare di incontrare in termini di affidabilità. Le informazioni raccolte potrebbero essere rappresentate graficamente in una figura simile alla seguente:



In questo esempio, il maggior numero di dispositivi è rappresentato in modo affidabile dagli alias dello storage. Le regole che identificano gli host che utilizzano gli alias dello storage devono essere scritte per prime, le regole che utilizzano gli alias switch devono essere scritte per poi essere scritte per prime e le ultime regole create devono utilizzare gli alias della zona. A causa della sovrapposizione dell'utilizzo di alias di zona e switch, alcune regole di alias dello storage potrebbero identificare dispositivi aggiuntivi, lasciando meno regole richieste per alias di zona e switch.

Procedura per la definizione dei dispositivi nell'ambiente

In genere, per identificare i dispositivi nell'ambiente in uso, si utilizza un flusso di lavoro simile a quello riportato di seguito. L'identificazione è un processo iterativo e potrebbe richiedere più fasi di pianificazione e definizione delle regole.



Se nell'ambiente sono presenti dispositivi non identificati (noti anche come "sconosciuti" o generici) e successivamente si configura un'origine dati che li identifichi al momento del polling, questi non verranno più visualizzati o conteggiati come dispositivi generici.

Pianificazione delle regole di risoluzione dei dispositivi per l'ambiente in uso

L'utilizzo di regole per identificare i dispositivi nell'ambiente è in genere un processo iterativo che richiede un'analisi completa dell'ambiente e la creazione di più regole per identificare il maggior numero possibile di dispositivi. Lo scenario migliore consiste nell'impostare l'obiettivo di identificare il 100% dei dispositivi nell'ambiente in uso.

L'ordine più efficiente per le regole consiste nel posizionare prima le regole più restrittive, con la conseguenza che la maggior parte delle voci non corrisponde al modello, mentre il processo procede a regole meno restrittive. Ciò consente a Insight di applicare più modelli a ciascuna voce, aumentando la possibilità di corrispondenza dei modelli e di identificazione positiva dell'host.

Quando si creano regole, l'obiettivo deve essere quello di creare regole che affrontino il maggior numero possibile di dispositivi non identificati. Ad esempio, la creazione di regole che seguono un modello di copertura simile a quello riportato di seguito è molto più efficiente rispetto alla creazione di 30 regole con percentuali di copertura inferiori:

Regola	Percentuale di copertura
Regola 1	60%
Articolo 2	25%
Articolo 3	8%
Articolo 4	4%
Articolo 5	1%

Creazione di regole di risoluzione dei dispositivi

Vengono create regole di risoluzione dei dispositivi per identificare host, storage e nastri che non vengono identificati automaticamente da OnCommand Insight. Le regole create consentono di identificare i dispositivi attualmente presenti nell'ambiente e i dispositivi simili man mano che vengono aggiunti all'ambiente.

A proposito di questa attività

Quando si creano regole, si inizia identificando l'origine delle informazioni su cui viene eseguita la regola, il metodo utilizzato per estrarre informazioni e se la ricerca DNS viene applicata ai risultati della regola.

Origine utilizzata per identificare il dispositivo
• Alias SRM per gli host • Alias dello storage contenente un nome host o nastro incorporato • Alias dello switch contenente un nome host o nastro incorporato • Nomi di zone contenenti un nome host incorporato
Metodo utilizzato per estrarre il nome del dispositivo dall'origine
• Così com'è (estrarre un nome da un SRM) • Delimitatori • Espressioni regolari
Ricerca DNS
Specifica se si utilizza il DNS per verificare il nome host.

Le regole vengono create nella scheda regole di risoluzione automatica. I passaggi seguenti descrivono il processo di creazione delle regole.

Fasi

1. Fare clic su **Gestisci** > **risoluzione del dispositivo**
2. Nella scheda **regole di risoluzione automatica**, fare clic su **+Aggiungi**

   Viene visualizzata la schermata New Rule (Nuova regola).

   > La schermata New Rule (Nuova regola) include un'icona **?**, che fornisce aiuto ed esempi per la creazione di espressioni regolari.

3. Nell'elenco **Type** (tipo), selezionare il dispositivo che si desidera identificare.

   È possibile selezionare host o Tape.

4. Nell'elenco **Source** (origine), selezionare l'origine che si desidera utilizzare per identificare l'host.

   In base all'origine scelta, Insight visualizza la seguente risposta:

   - Zones (zone) elenca le zone e il WWN che devono essere identificati da Insight.
   - SRM elenca gli alias non identificati che devono essere identificati da Insight
   - L'alias dello storage elenca gli alias dello storage e il WWN che devono essere identificati da Insight
   - L'alias dello switch elenca gli alias dello switch che devono essere identificati da Insight
5. Nell'elenco **Method** (metodo), selezionare il metodo da utilizzare per identificare l'host.

Origine	Metodo
SRM	"As is", "Delimiters", "Regular Expressions"
Alias storage	"delimiters" o "Regular Expressions"
Cambiare alias	"delimiters" o "Regular Expressions"
Zone	"delimiters" o "Regular Expressions"

   - Le regole che utilizzano "Delimiters" richiedono i delimitatori e la lunghezza minima del nome host.

     La lunghezza minima del nome host è il numero di caratteri che Insight deve utilizzare per identificare un host. Insight esegue ricerche DNS solo per nomi host lunghi o più lunghi.

     Per le regole che utilizzano i delimitatori, la stringa di input viene token dal delimitatore e viene creato un elenco di nomi host candidati creando diverse combinazioni del token adiacente. L'elenco viene quindi ordinato, dal più grande al più piccolo. Ad esempio, per vipsnq03_hba3_emc3_12ep0 l'elenco risulterà nel seguente:

     - vipsnq03_hba3_emc3_12ep0
     - vipsnq03_hba3_emc3
     - hba3 emc3_12ep0
     - vipsnq03_hba3

        - emc3_12ep0
        - hba3_emc3
        - vipsnq03
        - 12p0
        - emc3
        - hba3
    - Le regole che utilizzano “Regular Expression” richiedono un’espressione regolare, il formato e la selezione della distinzione tra maiuscole e minuscole.
6. Fare clic su 

Per eseguire tutte le regole, oppure fare clic sulla freccia rivolta verso il basso nel pulsante per eseguire la regola creata (e qualsiasi altra regola creata dall’ultima esecuzione completa di AR).

Risultati

I risultati dell’esecuzione della regola vengono visualizzati nella scheda FC Identify (identificazione FC).

Avvio di un aggiornamento automatico della risoluzione del dispositivo

Un aggiornamento della risoluzione del dispositivo commuta le modifiche manuali aggiunte dall’ultima esecuzione automatica della risoluzione del dispositivo. L’esecuzione di un aggiornamento può essere utilizzata per salvare ed eseguire solo le nuove voci manuali della configurazione della risoluzione del dispositivo. Non viene eseguita alcuna risoluzione completa del dispositivo.

Fasi

1. Accedere all’interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione periferica**
3. Nella schermata **Device resolution** (risoluzione periferica), fare clic sulla freccia verso il basso nel pulsante **Run AR** (Esegui AR*).
4. Fare clic su **Aggiorna** per avviare l’aggiornamento.

Identificazione manuale assistita da regole

Questa funzione viene utilizzata nei casi speciali in cui si desidera eseguire una regola specifica o un elenco di regole (con o senza un riordinamento singolo) per risolvere host, dispositivi di storage e nastri sconosciuti o gruppi di essi.

Prima di iniziare

Sono presenti diversi dispositivi non identificati e più regole che consentono di identificare correttamente altri dispositivi.

A proposito di questa attività

Se l'origine contiene solo una parte del nome di un host o di un dispositivo, utilizzare una regola di espressione regolare e formattarla per aggiungere il testo mancante.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Gestisci** > **risoluzione del dispositivo**
3. Fare clic sulla scheda **FC Identify** (identificazione FC).

   Il sistema visualizza i dispositivi identificati e non identificati.

4. Selezionare più dispositivi non identificati.
5. Fare clic su **Identify** > **set host resolution** o **> set tape resolution**

   Il sistema visualizza la schermata Identify (identificazione) che contiene un elenco di tutte le regole che hanno identificato correttamente i dispositivi.

6. Modificare l'ordine delle regole in un ordine che soddisfi le proprie esigenze.

   L'ordine delle regole viene modificato nella schermata Identify (identificazione), ma non globalmente.

7. Selezionare il metodo più adatto alle proprie esigenze.

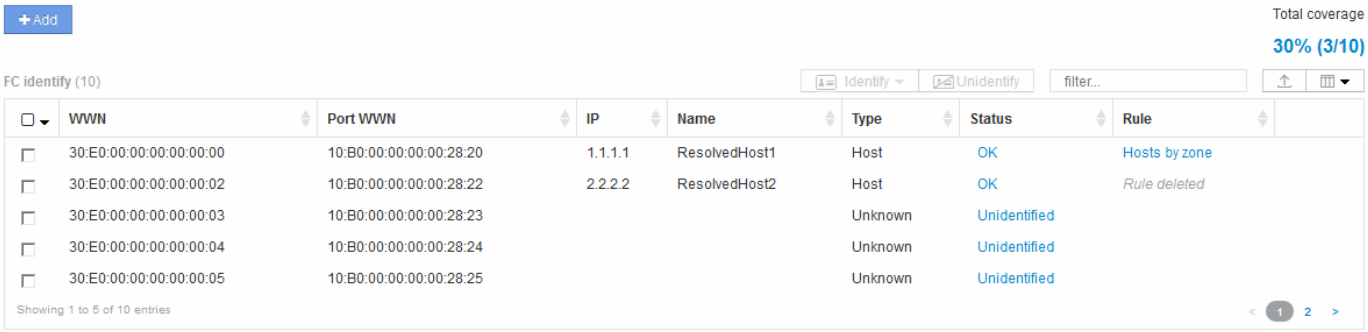
   OnCommand Insight esegue il processo di risoluzione dell'host nell'ordine in cui vengono visualizzati i metodi, iniziando da quelli in alto.

   Quando si incontrano le regole applicabili, i nomi delle regole vengono visualizzati nella colonna rules (regole) e identificati come manual (manuale).

Risoluzione del dispositivo Fibre Channel

La schermata FC Identify (identificazione FC) visualizza il WWN e il WWPN dei dispositivi Fibre Channel i cui host non sono stati identificati dalla risoluzione automatica del dispositivo. Lo schermo visualizza anche tutti i dispositivi che sono stati risolti con la risoluzione manuale del dispositivo.

I dispositivi che sono stati risolti mediante risoluzione manuale contengono lo stato "OK" e identificano la regola utilizzata per identificare il dispositivo. Lo stato dei dispositivi mancanti è "Unidentified". La copertura totale per l'identificazione dei dispositivi è riportata in questa pagina.



È possibile eseguire operazioni in blocco selezionando più dispositivi sul lato sinistro della schermata di

identificazione FC. È possibile eseguire azioni su un singolo dispositivo passando il mouse su un dispositivo e selezionando i pulsanti identifica o Annulla identificazione all'estrema destra dell'elenco.

Il collegamento Total Coverage (copertura totale) visualizza un elenco del "numero di dispositivi identificati/numero di dispositivi disponibili" per la configurazione:

- Alias SRM
- Alias storage
- Cambiare alias
- Zone
- Definito dall'utente

Aggiunta manuale di un dispositivo Fibre Channel

È possibile aggiungere manualmente un dispositivo Fibre Channel a OnCommand Insight utilizzando la funzione di aggiunta manuale disponibile nella scheda Device resolution FC Identify (identificazione FC risoluzione dispositivo). Questo processo potrebbe essere utilizzato per la pre-identificazione di un dispositivo che si prevede venga scoperto in futuro.

Prima di iniziare

Per aggiungere correttamente un identificativo del dispositivo al sistema, è necessario conoscere l'indirizzo WWN o IP e il nome del dispositivo.

A proposito di questa attività

È possibile aggiungere manualmente un host, uno storage, un nastro o un dispositivo Fibre Channel sconosciuto.

Fasi

1. Accedere all'interfaccia utente Web di Insight
2. Fare clic su **Gestisci** > **risoluzione del dispositivo**
3. Fare clic sulla scheda **FC Identify** (identificazione FC).
4. Fare clic sul pulsante Aggiungi.

   Viene visualizzata la finestra di dialogo Add Device (Aggiungi dispositivo)

5. Immettere il numero WWN o l'indirizzo IP, il nome della periferica e selezionare il tipo di periferica.

Risultati

Il dispositivo inserito viene aggiunto all'elenco dei dispositivi nella scheda FC Identify (identificazione FC). La "regola" è identificata come Manuale.

Importazione dell'identificativo del dispositivo Fibre Channel da un file CSV

È possibile importare manualmente l'identificazione del dispositivo Fibre Channel nella funzione di risoluzione del dispositivo OnCommand Insight utilizzando un elenco di

dispositivi in un file CSV.

Prima di iniziare

È necessario disporre di un file CSV formattato correttamente per importare gli identificatori dei dispositivi direttamente nella funzione risoluzione periferica. Il file CSV per le periferiche Fibre Channel richiede le seguenti informazioni:

WWN
IP
Nome
Tipo

> Come procedura consigliata, si consiglia di esportare prima le informazioni di identificazione FC in un file CSV, apportare le modifiche desiderate in tale file, quindi importare nuovamente il file in FC Identify. In questo modo, le colonne previste sono presenti e nell'ordine corretto.

Per importare le informazioni di identificazione FC:

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione periferica**
3. Selezionare la scheda **FC Identify**.
4. Fare clic su **identifica** > **identifica dal file** .
   a. Accedere alla cartella contenente i file CSV da importare e selezionare il file desiderato.

   I dispositivi immessi vengono aggiunti all'elenco dei dispositivi nella scheda FC Identify (identificazione FC). La "regola" è identificata come "Manuale".

Esportazione degli identificatori dei dispositivi Fibre Channel in un file CSV

È possibile esportare gli identificativi dei dispositivi Fibre Channel esistenti in un file CSV dalla funzione di risoluzione dei dispositivi OnCommand Insight. È possibile esportare un identificativo del dispositivo in modo da poterlo modificare e quindi importarlo nuovamente in Insight, dove viene utilizzato per identificare i dispositivi simili a quelli che corrispondono originariamente all'identificativo esportato.

A proposito di questa attività

Questo scenario può essere utilizzato quando le periferiche hanno attributi simili che possono essere facilmente modificati nel file CSV e quindi reimportati nel sistema.

Quando si esporta un'identificazione del dispositivo Fibre Channel in un file CSV, il file contiene le seguenti informazioni nell'ordine indicato:

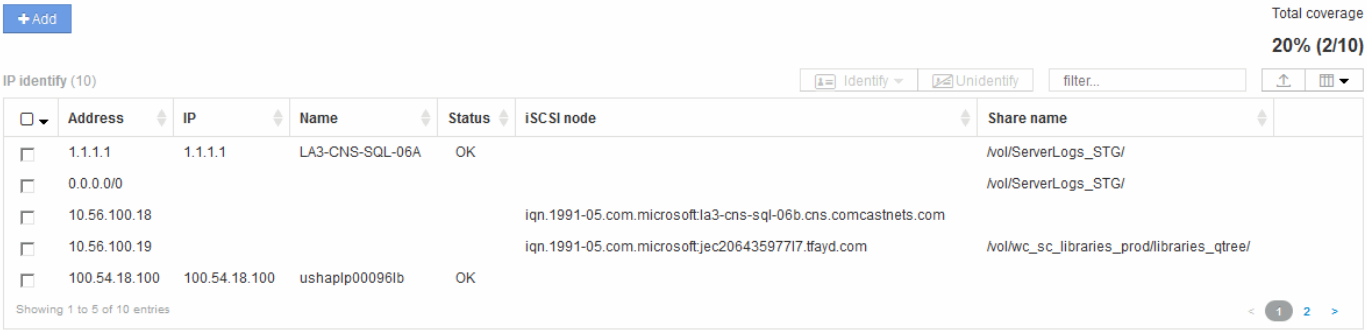
WWN	
IP	
Nome	
Tipo	

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione periferica**
3. Selezionare la scheda **FC Identify**.
4. Selezionare il dispositivo Fibre Channel o i dispositivi di cui si desidera esportare l'identificativo.
5. Fare clic sull'esportazione icona.
6. Scegliere se si desidera aprire il file CSV o salvarlo.

Risoluzione del dispositivo IP

La schermata IP Identify (identificazione IP) visualizza tutte le condivisioni iSCSI e CIFS o NFS identificate dalla risoluzione automatica del dispositivo o dalla risoluzione manuale del dispositivo. Vengono visualizzati anche i dispositivi non identificati. La schermata include l'indirizzo IP, il nome, lo stato, il nodo iSCSI e il nome di condivisione dei dispositivi. Viene visualizzata anche la percentuale di dispositivi identificati correttamente.



Aggiunta manuale di dispositivi IP

È possibile aggiungere manualmente un dispositivo IP a OnCommand Insight utilizzando la funzione di aggiunta manuale disponibile nella schermata di identificazione IP.

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione del dispositivo**
3. Fare clic sulla scheda **IP Identify** (identificazione IP).

4. Fare clic sul pulsante Aggiungi.

   Viene visualizzata la finestra di dialogo Add Device (Aggiungi dispositivo)

5. Immettere l'indirizzo, l'indirizzo IP e un nome di periferica univoco.

Risultati

Il dispositivo inserito viene aggiunto all'elenco dei dispositivi nella scheda IP Identify (identificazione IP).

Importazione dell'identificativo del dispositivo IP da un file CSV

È possibile importare manualmente gli identificatori dei dispositivi IP nella funzione risoluzione periferica utilizzando un elenco di identificatori dei dispositivi in un file CSV.

Prima di iniziare

Per importare gli identificatori dei dispositivi, è necessario disporre di un file CSV formattato correttamente. Il file CSV per le periferiche IP richiede le seguenti informazioni:

Indirizzo
IP
Nome

> Come procedura consigliata, si consiglia di esportare prima le informazioni di identificazione IP in un file CSV, apportare le modifiche desiderate in tale file, quindi importare nuovamente il file in identificazione IP. In questo modo, le colonne previste sono presenti e nell'ordine corretto.

Per importare le informazioni di identificazione IP:

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione periferica**
3. Selezionare la scheda **IP Identify** (identificazione IP).
4. Fare clic su **identifica** > **identifica dal file** .

   a. Accedere alla cartella contenente i file CSV da importare e selezionare il file desiderato.

   I dispositivi immessi vengono aggiunti all'elenco dei dispositivi nella scheda IP Identify (identificazione IP).

Esportazione dell'identificativo del dispositivo IP in un file CSV

È possibile esportare gli identificativi dei dispositivi IP esistenti da Insight utilizzando la funzione risoluzione dispositivo. È possibile esportare l'identificazione di un dispositivo in modo che sia possibile modificarla e importarla nuovamente in Insight in modo da poterla utilizzare per identificare i dispositivi simili a quelli dell'identificativo esportato.

A proposito di questa attività

Quando si esporta un identificativo del dispositivo IP in un file CSV, il file contiene le seguenti informazioni nell'ordine indicato:

Indirizzo
IP
Nome

Fasi

1. Accedere all'interfaccia utente Web di Insight.
2. Fare clic su **Gestisci** > **risoluzione periferica**
3. Selezionare la scheda **IP Identify** (identificazione IP).
4. Selezionare il dispositivo IP o i dispositivi di cui si desidera esportare l'identificativo.
5. Fare clic sull'esportazione icona.
6. Scegliere se si desidera aprire il file CSV o salvarlo.

Impostazione delle opzioni nella scheda Preferenze

La scheda Device resolution preferences (Preferenze risoluzione dispositivo) consente di creare una pianificazione di risoluzione automatica, specificare i vender di storage e nastri da includere o escludere dall'identificazione e impostare le opzioni di ricerca DNS.

Pianificazione automatica della risoluzione

Un programma di risoluzione automatica può specificare quando eseguire la risoluzione automatica del dispositivo:

Opzione	Descrizione
Ogni	Utilizzare questa opzione per eseguire la risoluzione automatica del dispositivo a intervalli di giorni, ore o minuti.
Ogni giorno	Utilizzare questa opzione per eseguire la risoluzione automatica giornaliera del dispositivo a un orario specifico.
Manualmente	Utilizzare questa opzione solo per eseguire manualmente la risoluzione automatica del dispositivo.

Ad ogni cambiamento di ambiente	Utilizzare questa opzione per eseguire la risoluzione automatica del dispositivo ogni volta che si verifica un cambiamento nell'ambiente.

Se si specifica manualmente, la risoluzione automatica notturna del dispositivo viene disattivata.

Opzioni di elaborazione DNS

Le opzioni di elaborazione DNS consentono di selezionare le seguenti funzioni:

- Quando l'elaborazione dei risultati della ricerca DNS è attivata, è possibile aggiungere un elenco di nomi DNS da aggiungere ai dispositivi risolti.
- È possibile selezionare "Auto resolution of IP:" (risoluzione automatica degli IP:) per abilitare la risoluzione automatica degli host per gli iniziatori iSCSI e gli host che accedono alle condivisioni NFS utilizzando la ricerca DNS. Se non viene specificato, viene eseguita solo la risoluzione basata su FC.
- È possibile scegliere di consentire i caratteri di sottolineatura nei nomi host e di utilizzare un alias "connesso a" invece dell'alias della porta standard nei risultati.

Inclusi o esclusi vendor di storage e nastri specifici

È possibile includere o escludere vendor di storage e nastri specifici per la risoluzione automatica. È possibile escludere vendor specifici se, ad esempio, si sa che un host specifico diventerà un host legacy e dovrebbe essere escluso dal nuovo ambiente. Puoi anche aggiungere di nuovo i vendor che hai precedentemente escluso, ma che non vuoi più escludere.

> Le regole di risoluzione dei dispositivi per il nastro funzionano solo per i WWN in cui il fornitore per quel WWN è impostato su **incluso solo come nastro** nelle preferenze del vendor.

Esempi di espressioni regolari

Se è stato selezionato l'approccio alle espressioni regolari come strategia di denominazione di origine, è possibile utilizzare gli esempi di espressioni regolari come guide per le proprie espressioni utilizzate nei metodi di risoluzione automatica di OnCommand Insight.

Formattazione delle espressioni regolari

Quando si creano espressioni regolari per la risoluzione automatica OnCommand Insight, è possibile configurare il formato di output immettendo i valori in un campo denominato `FORMAT`.

L'impostazione predefinita è `\1`, ovvero il nome di una zona che corrisponde all'espressione regolare viene sostituito dal contenuto della prima variabile creata dall'espressione regolare. In un'espressione regolare, i valori delle variabili vengono creati dalle istruzioni tra parentesi. Se si verificano più istruzioni tra parentesi, le variabili vengono referenziate numericamente, da sinistra a destra. Le variabili possono essere utilizzate nel formato di output in qualsiasi ordine. Il testo costante può anche essere inserito nell'output, aggiungendolo al `FORMAT` campo.

Ad esempio, per questa convenzione di denominazione delle zone potrebbero essere presenti i seguenti nomi di zona:

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_solaris_FC1

Inoltre, è possibile che l'output sia nel seguente formato:

```
        [hostname]-[data center]-[device type]
```

A tale scopo, è necessario acquisire i campi nome host, data center e tipo di dispositivo nelle variabili e utilizzarli nell'output. La seguente espressione regolare consente di eseguire questa operazione:

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

Poiché ci sono tre gruppi di parentesi, le variabili `\1`, `\2` e. `\3` verrà popolato.

È quindi possibile utilizzare il seguente formato per ricevere l'output nel formato preferito:

```
\2-\1-\3
```

L'output sarà il seguente:

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

I trattini tra le variabili forniscono un esempio di testo costante inserito nell'output formattato.

Esempio 1 che mostra i nomi delle zone

In questo esempio, si utilizza l'espressione regolare per estrarre un nome host dal nome della zona. È possibile creare un'espressione regolare se si dispone di un'espressione simile ai seguenti nomi di zona:

- S0032_myComputer1Name-HBA0
- S0434_myComputer1Name-HBA1
- S0432_myComputer1Name-HBA3

L'espressione regolare che è possibile utilizzare per acquisire il nome host è:

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

Il risultato è una corrispondenza di tutte le zone che iniziano con S seguite da qualsiasi combinazione di cifre , seguite da un carattere di sottolineatura, dal nome host alfanumerico (myComputer1Name), da un carattere di sottolineatura o trattino, dalle lettere maiuscole HBA e da una singola cifra (0-9). Il solo nome host è memorizzato nella variabile * 1*.

L'espressione regolare può essere suddivisa nei suoi componenti:

- "S" rappresenta il nome della zona e inizia l'espressione. Corrisponde solo a una "S" all'inizio del nome della zona.
- I caratteri [0-9] tra parentesi indicano che la seguente "S" deve essere una cifra compresa tra 0 e 9, inclusi.
- Il segno + indica che l'occorrenza delle informazioni tra parentesi precedenti deve essere 1 o più volte.
- _ (Carattere di sottolineatura) significa che le cifre dopo S devono essere immediatamente seguite da un carattere di sottolineatura nel nome della zona. In questo esempio, la convenzione di denominazione delle zone utilizza il carattere di sottolineatura per separare il nome della zona dal nome host.
- Dopo il carattere di sottolineatura richiesto, le parentesi indicano che il modello contenuto in verrà memorizzato nella variabile 1.
- I caratteri tra parentesi [a-za-Z0-9] indicano che i caratteri corrispondenti sono tutte lettere (indipendentemente dal maiuscolo/minuscolo) e numeri.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi si verificano 0 o più volte.
- I caratteri tra parentesi [_-] (sottolineatura e trattino) indicano che il modello alfanumerico deve essere seguito da un trattino basso o un trattino.
- Le lettere HBA nell'espressione regolare indicano che questa sequenza esatta di caratteri deve essere presente nel nome della zona.
- Il set finale di caratteri tra parentesi [0-9] corrisponde a una singola cifra compresa tra 0 e 9.

Esempio 2

In questo esempio, saltare fino al primo carattere di sottolineatura "*", quindi abbinare e e tutto ciò che segue fino al secondo "*", quindi saltare tutto ciò che segue.

Zona: `Z_E2FHDBS01_E1NETAPP`

Nome host: `E2FHDBS01`

RegExp: `.?(E.?).*?`

Esempio 3

Le parentesi "( )" intorno all'ultima sezione dell'espressione regolare (di seguito) identificano quale parte è il nome host. Se si desidera che VSAN3 sia il nome host, si tratterebbe di: _([a-za-Z0-9]).*

Zona: `A_VSAN3_SR48KENT_A_CX2578_SPA0`

Nome host: `SR48KENT`

RegExp: `_[a-zA-Z0-9]+_([a-zA-Z0-9]).*`

Esempio 4 che mostra un modello di denominazione più complicato

È possibile creare un'espressione regolare se si dispone di un'espressione simile ai seguenti nomi di zona:

- MyComputerName123-HBA1_Symm1_FA3
- MyComputerName123-HBA2_Symm1_FA5
- MyComputerName123-HBA3_Symm1_FA7

L'espressione regolare che è possibile utilizzare per acquisire questi elementi è:

```
([a-zA-Z0-9]*)_.*
```

Il `\1` la variabile contiene solo `myComputerName123` dopo essere stato valutato da questa espressione.

L'espressione regolare può essere suddivisa nei suoi componenti:

- Le parentesi indicano che il modello contenuto in verrà memorizzato nella variabile 1.
- I caratteri tra parentesi [a-za-Z0-9] indicano che qualsiasi lettera (indipendentemente dal caso) o cifra corrisponde.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi si verificano 0 o più volte.
- Il carattere _ (carattere di sottolineatura) nell'espressione regolare indica che il nome della zona deve avere un carattere di sottolineatura immediatamente dopo la stringa alfanumerica associata dalle parentesi precedenti.
- Il . (punto) corrisponde a qualsiasi carattere (carattere jolly).
- Il simbolo * (asterisco) indica che il carattere jolly del punto precedente può verificarsi 0 o più volte.

  In altre parole, la combinazione .* indica qualsiasi carattere, qualsiasi numero di volte.

Esempio 5 che mostra i nomi delle zone senza schema

È possibile creare un'espressione regolare se si dispone di un'espressione simile ai seguenti nomi di zona:

- MyComputerName_HBA1_Symm1_FA1
- MyComputerName123_HBA1_Symm1_FA1

L'espressione regolare che è possibile utilizzare per acquisire questi elementi è:

```
(.*?)_.*
```

La variabile conterrà *MyComputerName* (nel primo esempio di nome di zona) o *myComputerName123* (nell'esempio di nome della seconda zona). Questa espressione regolare corrisponde quindi a tutto ciò che precede il primo carattere di sottolineatura.

L'espressione regolare può essere suddivisa nei suoi componenti:

- Le parentesi indicano che il modello contenuto in verrà memorizzato nella variabile 1.
- Il simbolo .* (punto asterisco) corrisponde a qualsiasi carattere, qualsiasi numero di volte.

- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi si verificano 0 o più volte.
- Il ? il carattere rende la partita non avida. Questo costringe l'IT a interrompere la corrispondenza al primo underscore, piuttosto che all'ultimo.
- I caratteri _.* corrispondono al primo carattere di sottolineatura trovato e a tutti i caratteri che lo seguono.

Esempio 6 che mostra i nomi dei computer con un modello

È possibile creare un'espressione regolare se si dispone di un'espressione simile ai seguenti nomi di zona:

- Storage1_Switch1_myComputerName123A_A1_FC1
- Storage2_Switch2_myComputerName123B_A2_FC2
- Storage3_Switch3_myComputerName123T_A3_FC3

L'espressione regolare che è possibile utilizzare per acquisire questi elementi è:

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

Poiché la convenzione di denominazione delle zone ha un modello più ampio, è possibile utilizzare l'espressione di cui sopra, che corrisponde a tutte le istanze di un nome host (MyComputerName nell'esempio) che termina con A, a B o a T, inserendo tale nome host nella variabile 1.

L'espressione regolare può essere suddivisa nei suoi componenti:

- Il simbolo .* (punto asterisco) corrisponde a qualsiasi carattere, qualsiasi numero di volte.
- Il ? il carattere rende la partita non avida. Questo costringe l'IT a interrompere la corrispondenza al primo underscore, piuttosto che all'ultimo.
- Il carattere di sottolineatura corrisponde al primo carattere di sottolineatura nel nome della zona.
- Pertanto, la prima combinazione di .*?_ corrisponde ai caratteri *storage1_* nell'esempio del nome della prima zona.
- La seconda combinazione .*?_ si comporta come la prima, ma corrisponde a *Switch1_* nell'esempio del nome della prima zona.
- Le parentesi indicano che il modello contenuto in verrà memorizzato nella variabile 1.
- I caratteri tra parentesi [a-za-Z0-9] indicano che qualsiasi lettera (indipendentemente dal caso) o cifra corrisponde.
- Il simbolo * (asterisco) che segue le parentesi indica che i caratteri tra parentesi si verificano 0 o più volte.
- I caratteri tra parentesi nell'espressione regolare [ABT] corrispondono a un singolo carattere nel nome della zona che deve essere A, B o T.
- Il _ (carattere di sottolineatura) che segue le parentesi indica che la corrispondenza del carattere [ABT] deve essere seguita da un carattere di sottolineatura.
- Il simbolo .* (punto asterisco) corrisponde a qualsiasi carattere, qualsiasi numero di volte.

Di conseguenza, la variabile 1 contiene una stringa alfanumerica che:

- è stato preceduto da un numero di caratteri alfanumerici e da due caratteri di sottolineatura
- seguito da un carattere di sottolineatura (e da un numero qualsiasi di caratteri alfanumerici)

- Aveva un carattere finale di A, B o T, prima del terzo trattino di sottolineatura.

Esempio 7

Zona: `myComputerName123_HBA1_Symm1_FA1`

Nome host: `myComputerName123`

RegExp: `([a-zA-Z0-9]+)_.*`

Esempio 8

Questo esempio trova tutto prima del primo _.

Zona: `MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

Nome host: `MyComputerName`

RegExp: `(.?)_.`

Esempio 9

Questo esempio trova tutto dopo il primo _ e fino al secondo _.

Zona: `Z_MyComputerName_StorageName`

Nome host: `MyComputerName`

RegExp: `.?(.?).*?`

Esempio 10

Questo esempio estrae "MyComputerName123" dagli esempi di zona.

Zona: `Storage1_Switch1_MyComputerName123A_A1_FC1`

`Storage2_Switch2_MyComputerName123B_A2_FC2`

`Storage3_Switch3_MyComputerName123T_A3_FC3`

Nome host: `MyComputerName123`

RegExp: `.?.?([a-zA-Z0-9]+)[ABT]_.`

Esempio 11

Zona: `Storage1_Switch1_MyComputerName123A_A1_FC1`

Nome host: `MyComputerName123A`

RegExp: `.?.?([a-zA-z0-9]+).*?`

Esempio 12

Il termine ^ (circumflex o caret) **all'interno delle parentesi quadre** nega l'espressione, ad esempio [^FF] indica qualsiasi elemento tranne la lettera F maiuscola o minuscola, mentre [^a-z] indica tutto tranne la lettera a-z minuscola e, nel caso precedente, qualsiasi elemento ad eccezione di _. L'istruzione format aggiunge "-" al nome host di output.

Zona: `mhs_apps44_d_A_10a0_0429`

Nome host: `mhs-apps44-d`

RegExp: `([^_])_([AB]).*`+Formato in OnCommand Insight:

`([^_])_().*`Formato in OnCommand Insight:

Esempio 13

In questo esempio, l'alias dello storage è delimitato da "" e l'espressione deve utilizzare "" per definire che la stringa è effettivamente utilizzata e che non fanno parte dell'espressione stessa.

Alias storage: `\Hosts\E2DOC01C1\E2DOC01N1`

Nome host: `E2DOC01N1`

RegExp: `\\.?\\.?\\(.*?)`

Esempio 14

Questo esempio estrae "PD-RV-W-ad-2" dagli esempi di zona.

Zona: `PD_D-PD-RV-W-AD-2_01`

Nome host: `PD-RV-W-AD-2`

RegExp: `[^-]-(.-\d+).+`

Esempio 15

In questo caso, l'impostazione del formato aggiunge "US-BV-" al nome host.

Zona: `SRV_USBVM11_F1`

Nome host: `US-BV-M11`

RegExp: `SRV_USBV([A-Za-z0-9]+)_F[12]`

Formato: `US-BV-\1`

Gestione delle informazioni

Che tu sia un nuovo utente di Insight e abbia un nuovo sistema da configurare o che il tuo sistema sia in funzione da qualche tempo, devi adottare le misure necessarie per

garantire il funzionamento corretto di Insight e della tua rete. Il concetto chiave di manutenzione è che le modifiche della rete devono essere di solito soddisfatte in Insight.

Di seguito sono riportate le attività di manutenzione più comuni:

- Gestione dei backup Insight
- Aggiornamento delle licenze Insight scadute
- Coordinamento delle patch di origine dei dati
- Aggiornamento della versione Insight su tutte le unità di acquisizione
- Eliminazione delle origini dati rimosse da Insight

Gestione delle informazioni

OnCommand Insight monitora il tuo ambiente, consentendoti di cercare potenziali problemi prima che venga segnalata una crisi. La dashboard delle risorse fornisce grafici a torta riepilogativi, mappe termiche per IOPS e un grafico interattivo dei primi 10 pool di storage utilizzati.

Fasi

1. Apri la dashboard Insight**Assets** e sposta il cursore sui grafici a torta per esaminare la distribuzione delle risorse in questi tre grafici:
   - La capacità per vendor indica la capacità raw totale dello storage di ciascun vendor.
   - Capacity by Tier (capacità per Tier): Indica la capacità totale utilizzabile per ciascun Tier di storage.
   - Il grafico a torta delle porte dello switch mostra i produttori di porte e la percentuale di porte utilizzate.
2. Visualizza **fatti sull'ambiente** per visualizzare informazioni sulla capacità utilizzata dell'ambiente, sull'efficienza della capacità, sulle risorse FC consumate e sulle statistiche dell'infrastruttura virtuale.
3. Posizionare il cursore su una barra del pool di storage nel grafico **Top 10 Used Pools** per visualizzare la capacità utilizzata e inutilizzata del pool di storage.
4. Fare clic su un nome di risorsa visualizzato in grande testo (che indica che la risorsa presenta problemi) nella mappa termica **Storage IOP** per visualizzare una pagina che riepiloga lo stato corrente della risorsa.
5. Nell'angolo in basso a destra della dashboard delle risorse*, fare clic sul nome di una risorsa che appare in grande formato (che indica che la risorsa presenta problemi) nella mappa termica di **Virtual Machine IOPS** per visualizzare una pagina che riepiloga lo stato corrente della risorsa.
6. Nella barra degli strumenti Insight, fare clic su **Admin**.
7. Notare le aree che mostrano cerchi rossi pieni.

   Nell'interfaccia utente di OnCommand Insightweb, i potenziali problemi sono contrassegnati da un cerchio rosso pieno.

8. Fare clic su **origini dati** per esaminare un elenco di tutte le origini dati monitorate.

   Esaminare qualsiasi origine dati con una colonna **Status** contenente un messaggio con un cerchio rosso pieno e con un **Impact** elencato come Alto o Medio. Questi sono nella parte superiore del tavolo. I problemi relativi a tali origini dati influiscono su una parte significativa della rete, che è necessario risolvere.

9. Fare clic su **Acquisition Units** (unità di acquisizione) per annotare lo stato di ciascun indirizzo IP che

esegue Insight e, se necessario, riavviare un'unità di acquisizione

10. Fare clic su **Health** per visualizzare il monitoraggio delle istanze di alto livello dei server Insight.

Monitoraggio dello stato di salute del sistema OnCommand Insight

Controllare periodicamente lo stato attuale dei componenti del sistema Insight visualizzando la pagina Health, che mostra lo stato di ciascun componente e avvisa l'utente in caso di problemi.

Fasi

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

   Viene visualizzata la pagina Health.

3. Visualizzare il riepilogo dello stato corrente dei componenti prestando particolare attenzione a qualsiasi stato di attenzione nella colonna **Dettagli** preceduto da un cerchio rosso, che indica un problema che richiede attenzione immediata.

   La pagina Health (Stato) visualizza informazioni su uno o tutti i seguenti componenti Insight in base alla configurazione del sistema:

Componente	Test	Dettagli	Viene visualizzato
Acquisizione	Elaborazione dei dati di inventario	Stato dell'unità di acquisizione locale	"OK" se il numero di origini dati di polling simultaneo è inferiore al 75% del numero massimo di pool di esecuzione (il valore predefinito massimo è 30). "Acquisition is busy" (acquisizione occupata) se l'utilizzo è superiore al 75% e consiglia di aumentare l'intervallo di polling o di aggiungere altre unità di acquisizione remota.
DWH	Backup	Stato del backup pianificato Data Warehouse	"OK" e l'ultimo backup DWH riuscito se è attivato il backup pianificato DWH. In caso contrario, visualizza le informazioni relative agli errori rilevati.

DWH	ETL	Stato del Data Warehouse ETL	“OK” e l’ultimo tempo di creazione DWH riuscito se non si verificano errori. In caso contrario, visualizza le informazioni relative agli errori rilevati.
Server	ASUP	Stato di ASUP	“ASUP Enabled” (ASUP abilitato) e l’ultimo orario di residenza del telefono, se disponibile. “ASUP Failed” se phonehome è abilitato ma si è verificato un problema. + "percorso di backup non valido" se la directory di backup non è valida. + Visualizza l’ora dell’ultimo tentativo non riuscito e l’ora dell’ultimo tentativo non riuscito, se disponibile. + “ASUP Disabled” (ASUP disattivato) se phonehome è disattivato.
Server	Risoluzione automatica	Stato della risoluzione automatica del dispositivo	“OK” se non si verificano errori. “la risoluzione automatica è bloccata” se gli errori di identificazione impediscono l’avanzamento della risoluzione. + “tasso di successo basso” se è possibile identificare meno del 75% dei dispositivi generici.

Server	Elasticsearch	Stato dell’archivio di dati di ricerca elastico	“OK” se non si verificano errori. “sservizio non disponibile” se non è possibile connettersi al servizio di ricerca elastico. + "Cluster mode detected" (rilevata modalità cluster) se viene rilevato più di un nodo. + "elevato utilizzo della memoria" se lo spazio di heap utilizzato è superiore al 85%. + "Status: RED" (Stato: ROSSO) indica un errore segnalato dalla ricerca elastica. Visualizza informazioni sull’errore e consiglia di contattare l’assistenza clienti.
Server	CPU	Utilizzo della CPU Insight	“OK” se il carico della CPU è inferiore al 65%. "Il carico della CPU del `ssystem è elevato. Riduci il carico della CPU.`" Se il carico della CPU è superiore al 65%.
Server	Spazio su disco	Stato dello spazio su disco	Spazio libero su disco, spazio su disco in uso da Insight e spazio su disco consigliato riservato a Insight. “spazio su disco insufficiente” se l’utilizzo del disco è superiore al 80%.
Server	EventBus	Stato di EventBus	“EventBus è vuoto” se la coda EventBus è vuota, altrimenti visualizza lo stato della coda EventBus.

Server	Elaborazione dei dati di inventario	Stato della funzionalità di elaborazione dei dati di inventario del server Insight	“OK” se il server Insight non è occupato. “sserver is busy” (Server occupato) se il server è occupato per almeno il 75% del tempo dell’ultima ora. Consiglia di non aggiungere più origini dati e di suddividere l’ambiente in più server.
Server	MySQL	Stato del database MySQL	“OK” se non vengono rilevati problemi. “il database presenta problemi di performance. Alcune query richiedono troppo tempo per essere eseguite” se il numero di query lente è superiore al 5%. + “il file di log del database è cresciuto più di <size> nell’ultima ora. Controllare il file di log MySQL” se il log degli errori supera i 20 KB.
Server	Archivio delle performance	Stato dell’archivio delle performance	“l’archivio delle prestazioni è abilitato” o “l’archivio delle prestazioni non è abilitato”.
Server	Memoria fisica	Stato della memoria fisica	“OK” se l’utilizzo della memoria è inferiore al 85%. “ml’utilizzo è elevato. Riduci l’impatto della memoria complessiva per la stabilità del sistema” se l’utilizzo della memoria è superiore al 85%.
Server	Service Pack	Disponibilità dei service pack	Visualizza se è disponibile un service pack per Insight. Se è disponibile un service pack, visualizza le istruzioni.

Server	Informazioni sull’utilizzo	Stato dell’invio delle informazioni sull’utilizzo	Visualizza se l’invio di informazioni sull’utilizzo a NetApp è attivato o disattivato. Consiglia di attivare se disattivato. Visualizza l’ora dell’ultimo tentativo o dell’ultimo invio riuscito. + Visualizza informazioni su eventuali problemi riscontrati.
Server	Violazione	Stato delle violazioni aperte	“OK” se il numero di violazioni aperte è inferiore al 75% del limite di violazioni. "Il numero massimo di violazioni aperte consentite è <number> `m`" se il numero di violazioni aperte è superiore al 75% del limite di violazioni. Consiglia di rivedere la configurazione dei criteri di performance. + “Violation manager is blocked” (il gestore delle violazioni è bloccato) se il numero di violazioni aperte è al limite. + tenere presente che il gestore delle violazioni non può creare nuove violazioni e consiglia di rivedere la configurazione delle policy sulle performance.
Server	Backup settimanale	Stato del backup settimanale	“OK” se è attivato il backup settimanale, altrimenti viene visualizzato “Weekly backup is not enabled” (il backup settimanale non è abilitato).

Eliminazione dei dispositivi inattivi

L'eliminazione dei dispositivi inattivi consente di mantenere i dati più puliti e facili da navigare.

A proposito di questa attività

Per eliminare i dispositivi inattivi da Insight, procedere come segue:

Fasi

1. Creare una nuova query o aprire una query esistente.
2. Scegliere il tipo di risorsa *generic device*, *host*, *storage*,*switch* o *tape*.
3. Aggiungi un filtro per **è attivo** e imposta il filtro su **No**.

   Nella tabella dei risultati vengono visualizzate solo le risorse non attive.

4. Selezionare i dispositivi che si desidera eliminare.
5. Fare clic sul pulsante **azioni** e selezionare **Elimina dispositivi inattivi**.

   I dispositivi inattivi vengono cancellati e non verranno più visualizzati in Insight.

Controllo delle attività del sistema e dell'utente

Se si desidera individuare modifiche impreviste, è possibile visualizzare un audit trail del sistema OnCommand Insight e delle relative attività utente. I messaggi del registro di controllo possono essere inviati a syslog in aggiunta alla visualizzazione nella pagina Audit.

A proposito di questa attività

Insight genera voci di audit per le attività degli utenti che influiscono sulla rete di storage o sulla sua gestione, tra cui:

- Accesso in corso
- Autorizzare o annullare l'autorizzazione di un percorso
- Aggiornamento di un percorso autorizzato
- Impostazione di policy o soglie globali
- Aggiunta o rimozione di un'origine dati
- Avvio o interruzione di un'origine dati
- Aggiornamento delle proprietà dell'origine dati
- Aggiunta, modifica o eliminazione di un'attività
- Rimozione di un gruppo di applicazioni
- Identificazione o modifica dell'identificazione di un dispositivo
- Creare un utente
- Eliminare un utente

- Modifica del ruolo dell'utente
- Modifica di un utente (Guest à Admin)
- Disconnessione di un utente (disconnessione forzata o disconnessione manuale)
- Eliminazione di un'unità di acquisizione
- Aggiorna licenza
- Attivazione del backup
- Disattivazione del backup in corso
- Abilitazione di ASUP (l'abilitazione del proxy sulla stessa pagina viene riportata nel registro di controllo)
- Disattivazione di ASUP (la disattivazione del proxy sulla stessa pagina viene riportata nel registro di controllo)
- Security (sicurezza) - digitare nuovamente le password di sistema e modificarle.
- Rimozione/aggiunta di annotazioni sulle risorse
- Accesso/disconnessione utente CAC
- Timeout sessione utente CAC

Fasi

1. Aprire Insight nel browser.
2. Fare clic su **Admin** e selezionare **Audit**.

   La pagina Audit visualizza le voci di audit in una tabella.

3. È possibile visualizzare i seguenti dettagli nella tabella:

   - **Ora**

     Data e ora in cui sono state apportate le modifiche

   - **Utente**

     Nome dell'utente associato alla voce di audit

   - **Ruolo**

     Ruolo dell'account utente, guest, utente o amministratore

   - **IP**

     Indirizzo IP associato alla voce di audit

   - **Azione**

     Tipo di attività nella voce di audit

   - **Dettagli**

     Dettagli della voce di audit

     Se un'attività dell'utente influisce su una risorsa, ad esempio un'origine dati o un'applicazione, i dettagli

includono un collegamento alla landing page della risorsa.

> Quando un'origine dati viene eliminata, i dettagli dell'attività dell'utente relativi all'origine dati non contengono più un collegamento alla landing page dell'origine dati.

4. È possibile visualizzare le voci di audit scegliendo un determinato periodo di tempo (1 ora, 3 ore, 24 ore, 3 giorni e 7 giorni), Con Insight che mostra un numero massimo di 1000 violazioni per il periodo di tempo selezionato.

   È possibile fare clic su un numero di pagina sotto la tabella per sfogliare i dati per pagina se sono presenti più dati che si adattano a una singola pagina.

5. È possibile modificare l'ordinamento delle colonne di una tabella in ordine crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna; per tornare all'ordinamento predefinito, fare clic su un'altra intestazione di colonna.

   Per impostazione predefinita, la tabella visualizza le voci in ordine decrescente.

6. È possibile utilizzare la casella **filter** per visualizzare solo le voci desiderate nella tabella.

   Per visualizzare solo le voci di audit da parte dell'utente `izzyk`, digitare `izzyk` nella casella **filter**.

Monitoraggio delle violazioni nella rete

Quando Insight genera violazioni a causa delle soglie impostate nelle policy sulle performance, puoi visualizzarle utilizzando la dashboard delle violazioni. La dashboard elenca tutte le violazioni che si verificano nella rete e consente di individuare e risolvere i problemi.

Fasi

1. Aprire OnCommand Insight nel browser.
2. Nella barra degli strumenti di Insight, fare clic su **Dashboard** e selezionare **dashboard violazioni**.

   Viene visualizzata la dashboard delle violazioni.

3. È possibile utilizzare il grafico a torta **violazioni per policy** nei seguenti modi:
   - È possibile posizionare il cursore su qualsiasi sezione di un grafico per visualizzare la percentuale delle violazioni totali che si sono verificate per una determinata policy o metrica.
   - È possibile fare clic su una sezione di un grafico per "ingrandire", che consente di enfatizzare e studiare più attentamente la sezione spostandola dal resto del grafico.
   - Fare clic su ⤢ nell'angolo in alto a destra per visualizzare il grafico a torta in modalità a schermo intero, quindi fare clic su ⤡ di nuovo per ridurre a icona il grafico a torta. Un grafico a torta può contenere un massimo di cinque sezioni; pertanto, se si dispone di sei policy che generano violazioni, Insight combina la quinta e la sesta sezione in una sezione "altre". Insight assegna il maggior numero di violazioni alla prima sezione, la seconda più violazioni alla seconda sezione e così via.
4. Puoi utilizzare il grafico **Cronologia violazioni** nei seguenti modi:
   - È possibile posizionare il cursore sul grafico per visualizzare il numero totale di violazioni che si sono verificate in un determinato momento e il numero che si è verificato al di fuori del totale per ciascuna metrica specificata.

- È possibile fare clic su un'etichetta della legenda per rimuovere i dati associati alla legenda dal grafico.

  Fare clic sulla legenda per visualizzare nuovamente i dati.

- Fare clic su ⤢ nell'angolo in alto a destra per visualizzare il grafico a schermo intero, quindi fare clic su ⤡ di nuovo per ridurre a icona il grafico a torta.

5. È possibile utilizzare la **Tabella delle violazioni** nei seguenti modi:
   - Fare clic su ⤢ nell'angolo in alto a destra per visualizzare la tabella in modalità a schermo intero, quindi fare clic su ⤡ di nuovo per ridurre a icona il grafico a torta.

     Se le dimensioni della finestra sono troppo piccole, la tabella delle violazioni visualizza solo tre colonne, tuttavia quando si fa clic su ⤢, vengono visualizzate colonne aggiuntive (fino a sette).

   - È possibile visualizzare le violazioni per un determinato periodo di tempo (**1h**, **3h**, **24h**, **3d**, **7d**, E **30d**), con Insight che mostra un numero massimo di 1000 violazioni per il periodo di tempo selezionato.
   - È possibile utilizzare la casella **filter** per visualizzare solo le violazioni desiderate.
   - È possibile modificare l'ordinamento delle colonne in una tabella in modo che sia crescente (freccia verso l'alto) o decrescente (freccia verso il basso) facendo clic sulla freccia nell'intestazione della colonna; per tornare all'ordinamento predefinito, fare clic su un'altra intestazione di colonna.

     Per impostazione predefinita, la tabella visualizza le violazioni in ordine decrescente.

   - È possibile fare clic su una violazione nella colonna ID per visualizzare la pagina delle risorse per la durata della violazione.
   - È possibile fare clic sui collegamenti alle risorse (ad esempio, pool di storage e volume di storage) nella colonna Description (Descrizione) per visualizzare le pagine delle risorse associate a tali risorse.
   - È possibile fare clic sul collegamento al criterio di performance nella colonna Policy (criterio) per visualizzare la finestra di dialogo Edit Policy (Modifica criterio).

     È possibile modificare le soglie di una policy se si ritiene che generi troppe o poche violazioni.

   - È possibile fare clic su un numero di pagina per sfogliare i dati per pagina se sono presenti più dati di quelli contenuti in una singola pagina.
   - Fare clic su ✖ per eliminare la violazione.

Stato dell'unità di acquisizione

La schermata Acquisition Unit (unità di acquisizione) fornisce una vista di tutte le unità di acquisizione, inclusi lo stato e gli eventuali errori presenti.

Lo stato delle unità di acquisizione Insight collegate al server viene visualizzato nella tabella **Admin** > **Acquisition Units** (unità di acquisizione). Questa tabella mostra le seguenti informazioni per ciascuna unità di acquisizione:

- **Nome**
- **IP**
- **Status** è lo stato operativo dell'unità di acquisizione.
- **Ultimo report**Visualizza l'ultima volta in cui un'origine dati si è connessa all'unità di acquisizione segnalata.

- **Nota** Visualizza una nota inserita dall'utente relativa all'AU.

Se un'unità di acquisizione nell'elenco presenta un problema, nel campo Status (Stato) viene visualizzato un cerchio rosso con brevi informazioni sul problema. È necessario esaminare eventuali problemi delle unità di acquisizione, poiché potrebbero influire sulla raccolta dei dati.

Per riavviare un'unità di acquisizione, passare il mouse sull'unità e fare clic sul pulsante *Restart Acquisition Unit* (Riavvia unità di acquisizione) visualizzato.

Per aggiungere una nota di testo, passare il mouse su un'unità di acquisizione e fare clic sul pulsante *Add Note* (Aggiungi nota) visualizzato. Viene visualizzata solo la nota inserita più di recente.

Ripristino del database Insight

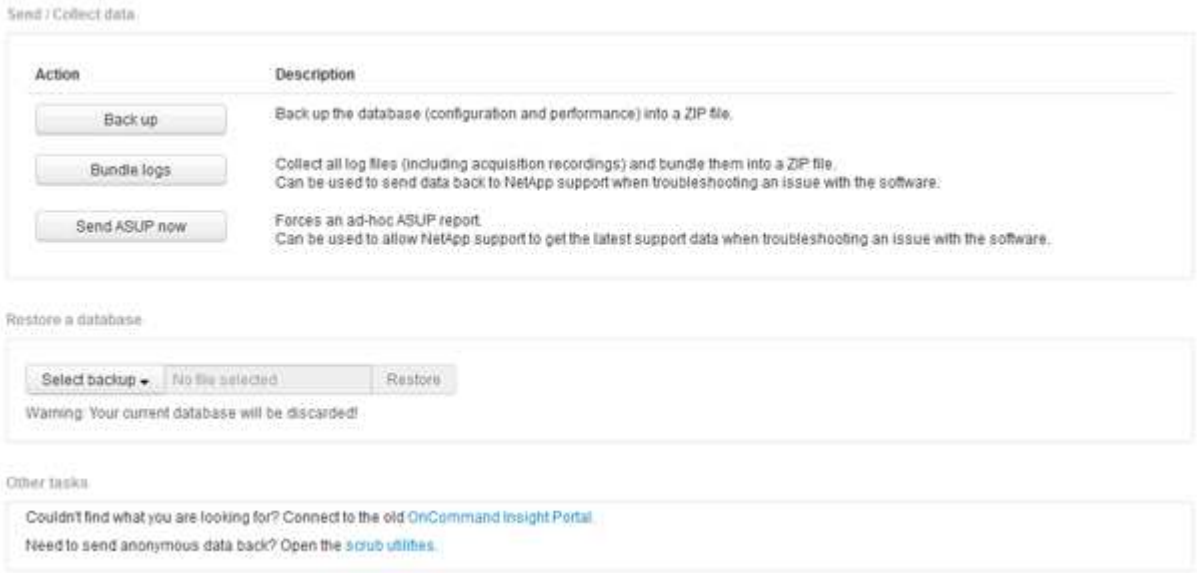
Per ripristinare il database Insight da un file di backup verificato, utilizzare le opzioni di risoluzione dei problemi. Questa operazione sostituisce completamente i dati OnCommand Insight correnti.

Prima di iniziare

Best practice:prima di ripristinare il database OnCommand Insight, utilizzare il processo di backup manuale per creare una copia del database corrente. Controllare il file di backup che si desidera ripristinare per assicurarsi che sia stato eseguito correttamente il backup contenente i file che si desidera ripristinare.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **risoluzione dei problemi**.



3. Nella sezione Restore a database (Ripristina database), selezionare il file di backup che si desidera ripristinare dal menu **Select Backup** (Seleziona backup).
4. Fare clic su **Restore** (Ripristina).
5. Quando viene visualizzato l'avviso che tutti i dati verranno sostituiti, fare clic su **OK**

   Lo stato dell'attività di ripristino viene visualizzato nella pagina di ripristino.

Aggiornamento delle licenze scadute in corso

Se una o più licenze Insight sono scadute, è possibile aggiornarle rapidamente utilizzando la stessa procedura utilizzata per installare le licenze originali.

Fasi

1. In un editor di testo, ad esempio blocco note, aprire il nuovo file di licenza ricevuto dal supporto NetApp e copiare il testo della chiave di licenza negli Appunti di Windows.
2. Aprire OnCommand Insight nel browser.
3. Fare clic su **Admin** nella barra degli strumenti.
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)**.

   Questa operazione aggiunge le nuove licenze a tutte le licenze Insight attualmente attive.

9. Fare clic su **Save** (Salva).
10. Se si utilizza il modello di licenza Insight Consumption, è necessario selezionare la casella **Enable sending usage information to NetApp** (attiva invio delle informazioni sull'utilizzo a NetApp*) nella sezione Usage (utilizzo). Il proxy deve essere configurato e attivato correttamente per l'ambiente in uso.

Licenze non più conformi

Se viene visualizzato il messaggio "non conforme" nella pagina delle licenze Insight, Insight gestisce più terabyte di quelli concessi in licenza dall'azienda.

Il messaggio "non conforme" indica che la tua azienda ha pagato meno terabyte di quanto Insight stia attualmente gestendo. La differenza tra i terabyte gestiti e il numero di terabyte concessi in licenza viene visualizzata accanto al messaggio di non conformità.

Il funzionamento del sistema Insight non viene compromesso, ma è necessario contattare il rappresentante NetApp per aumentare la copertura della licenza e aggiornare la licenza appropriata.

Sostituzione delle licenze per le versioni Insight precedenti

Se è stata acquistata una nuova versione di Insight non compatibile con le versioni precedenti del prodotto, è necessario sostituire le licenze precedenti con quelle nuove.

Quando si installano le nuove licenze, è necessario selezionare l'operazione **Sostituisci** prima di salvare il testo della chiave di licenza.

Applicazione di un service pack

Periodicamente, sono disponibili service pack che è possibile applicare per sfruttare le correzioni e i miglioramenti apportati a OnCommand Insight.

Prima di iniziare

- È necessario aver scaricato il file del service pack (ad esempio, `7.2service_pack_1.patch`) Dal sito NOW.
- È necessario aver approvato tutte le patch.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Patch**.
3. Dal pulsante Actions (azioni), selezionare **Apply patch** (Applica patch).
4. Nella finestra di dialogo **Applica patch origine dati**, fare clic su **Sfoglia** per individuare il file del service pack.
5. Esaminare **Patch name**, **Description**, **tipi di origine dati interessati**, che mostrano se sono interessate origini dati, e **Details**, che descrive i miglioramenti contenuti nel service pack.
6. Se il service pack selezionato è corretto, fare clic su **Apply Patch** (Applica patch).

   I service pack vengono approvati automaticamente; non sono necessarie ulteriori azioni.

Preparazione di un report speciale per la risoluzione dei problemi

Insight invia automaticamente le informazioni al supporto clienti NetApp attraverso il sistema ASUP configurato dopo l'installazione del software. Tuttavia, è possibile creare un report per la risoluzione dei problemi e aprire un caso con il team di supporto per un problema specifico.

È possibile utilizzare gli strumenti di Insight per eseguire un backup manuale di Insight, raggruppare i registri e inviare tali informazioni al supporto clienti di NetApp.

Backup manuale del database OnCommand Insight

Se sono stati attivati backup settimanali per il database OnCommand Insight, vengono generate automaticamente copie che è possibile utilizzare per ripristinare il database, se necessario. Se è necessario creare un backup prima di un'operazione di ripristino o inviare un backup al supporto tecnico NetApp per ricevere assistenza, è possibile creare un backup `.zip` file manualmente.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **risoluzione dei problemi**.
3. Nella sezione Send/Collect data (Invia/raccogli dati), fare clic su **Backup**.
4. Fare clic su **Save file** (Salva file).
5. Fare clic su **OK**.

Log in bundle per il supporto

Durante la risoluzione di un problema con il software Insight, è possibile generare rapidamente un file zip (utilizzando il formato "gz") dei registri e delle registrazioni di acquisizione da inviare al supporto clienti NetApp.

Fasi

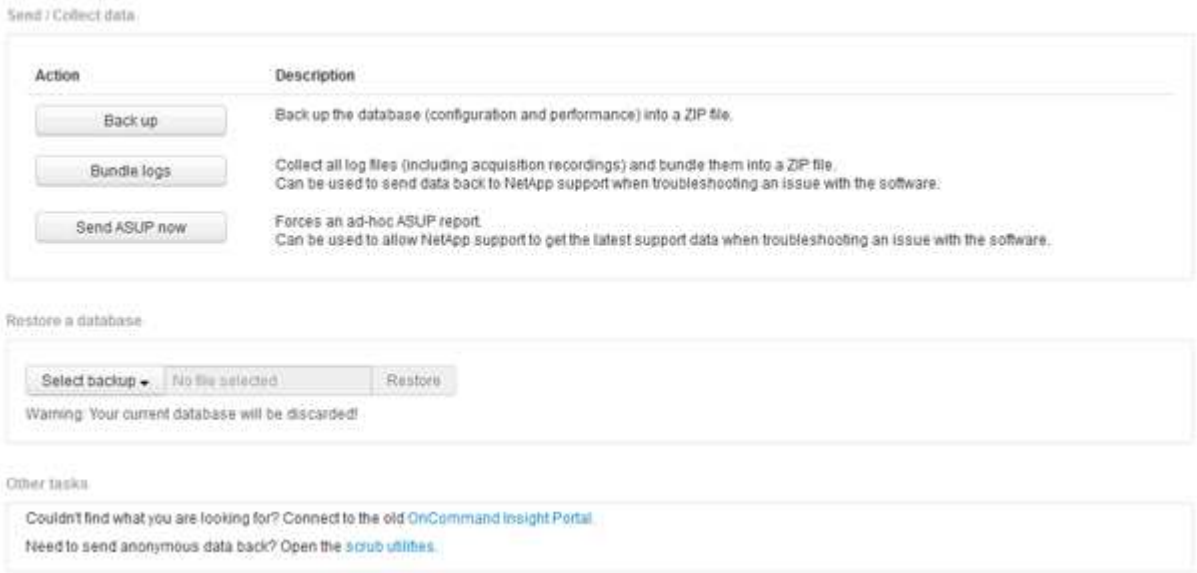
1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **risoluzione dei problemi**.
3. Nella sezione Send / Collect data (Invia/raccogli dati), fare clic su **Bundle logs** (registri bundle).
4. Fare clic su **Save file** (Salva file).
5. Fare clic su **OK**.

Invio di informazioni al supporto NetApp

La struttura di supporto automatizzato (ASUP) di NetApp invia informazioni sulla risoluzione dei problemi direttamente al team di assistenza clienti di NetApp. È possibile forzare l'invio di un report speciale.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **Setup**.
3. Fare clic sulla scheda **Backup/ASUP**.
4. Nell'area Send/Collect data (Invia/raccogli dati), fare clic su **Send ASUP now** (Invia ASUP ora) per inviare registri, registrazioni e backup al supporto NetApp.



Scrubbing dei dati per il trasferimento al supporto

I clienti che dispongono di ambienti sicuri devono comunicare con il Servizio clienti

NetApp per risolvere i problemi che si verificano senza compromettere le informazioni del database. Le utility di scrubbing di OnCommand Insight consentono di impostare un dizionario completo di parole chiave e modelli in modo da poter "pulire" i dati sensibili e inviare file scrubbed al supporto clienti.

Fasi

1. Nell'interfaccia utente Web, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **Utilità di scrub**.

   Esistono diverse sezioni di scrubbing: Ricerca nel dizionario, dati di scrubbing e dizionario di creazione, parole chiave personalizzate ed espressioni regolari.

.

+ .. Nella sezione**Lookup in dictionary**, inserire un codice per visualizzare il valore che sostituisce o un valore per visualizzare il codice che lo sostituisce. Nota: Prima di eseguire una ricerca, è necessario **creare** il dizionario per identificare i valori da utilizzare per la pulizia dai dati di supporto.

1. Per aggiungere parole chiave personalizzate per eseguire lo scrubbing dai dati di supporto, nella sezione **parole chiave personalizzate**, fare clic su **azioni › Aggiungi parola chiave personalizzata**. Inserire una parola chiave e fare clic su **Save** (Salva). La parola chiave viene aggiunta al dizionario.
2. Espandere **modelli (regexp)**. Fare clic su **Aggiungi** per visualizzare la finestra di dialogo per l'immissione di un nuovo modello.
3. Per utilizzare un'espressione regolare per identificare le parole o le frasi da scrubbing, immettere uno o più modelli nella sezione **espressioni regolari**. Fare clic su **azioni › Aggiungi espressione regolare**, immettere un Nome per il modello e l'espressione regolare nei campi e fare clic su **Salva**. Le informazioni sono state aggiunte al dizionario.

   > I modelli devono essere racchiusi tra parentesi di arrotondamento per identificare un gruppo di cattura di espressioni regolari.

4. Nella sezione**Build Dictionary**, fare clic su **Build** per avviare la compilazione del dizionario di tutte le parole identificate come sensibili dal database OnCommand Insight.

   Al termine, viene visualizzato un prompt che informa che il dizionario aggiornato è disponibile. La descrizione del database include una riga che indica il numero di parole chiave presenti nel dizionario. Verificare la precisione delle parole chiave nel dizionario. Se si riscontrano problemi e si desidera ricostruire il dizionario, fare clic su **Ripristina** nel blocco database per rimuovere tutte le parole chiave raccolte dal database OnCommand Insight dal dizionario. Come indicato dal prompt, non verranno eliminate altre parole chiave. Tornare alle utilità di scrubbing e immettere nuovamente le parole chiave personalizzate.

5. Dopo aver creato un dizionario Scrub, è possibile utilizzarlo per eseguire lo scrubbing di un log, XML o di un altro file di testo per rendere i dati anonimi.
6. Per eseguire lo scrubbing di un file di log, XML o altro file di testo, nella sezione **dati di scrubbing**, selezionare Sfoglia per individuare il file e fare clic su **file di scrubbing**.

Risoluzione avanzata dei problemi

Per completare la configurazione di OnCommand Insight, è necessario utilizzare gli strumenti avanzati per la risoluzione dei problemi. Questi strumenti vengono eseguiti nel browser e vengono aperti dalla pagina **Admin** > **Troubleshooting**.

Per aprire gli strumenti avanzati per la risoluzione dei problemi nel browser, fare clic sul collegamento **risoluzione avanzata dei problemi** nella parte inferiore della pagina.

I tool avanzati per la risoluzione dei problemi consentono di visualizzare vari report, informazioni di sistema, pacchetti installati e log, nonché di eseguire numerose azioni, come il riavvio del server o delle unità di acquisizione, l'aggiornamento delle annotazioni DWH e l'importazione di annotazioni.

Per tutte le opzioni disponibili, consultare la pagina risoluzione avanzata dei problemi.

Configurazione del numero di ore per ignorare i dati dinamici

È possibile configurare il numero di ore durante le quali OnCommand Insight ignora l'aggiornamento dei dati dinamici, ad esempio la capacità utilizzata. Se si utilizza il valore predefinito di sei ore e non si verificano modifiche alla configurazione, i report non verranno aggiornati con dati dinamici fino a quando non saranno trascorsi il numero predefinito di ore. Questa opzione migliora le performance perché questa opzione run gli aggiornamenti quando cambiano solo i dati dinamici.

A proposito di questa attività

Se viene impostato un valore per questa opzione, OnCommand Insight aggiorna i dati dinamici in base alle seguenti regole:

- Se non si verificano modifiche alla configurazione, ma i dati della capacità cambiano, i dati non verranno aggiornati.
- I dati dinamici (diversi dalle modifiche di configurazione) verranno aggiornati solo dopo il timeout specificato in questa opzione.
- Se si verificano modifiche alla configurazione, i dati dinamici e di configurazione vengono aggiornati.

I dati dinamici interessati da questa opzione includono quanto segue:

- Dati di violazione della capacità
- Capacità allocata dei file system e capacità utilizzata
- Hypervisor
  - Capacità utilizzata del disco virtuale
  - Capacità utilizzata della macchina virtuale
- Volume interno
  - Capacità allocata dei dati
  - Data used Capacity (capacità utilizzata dati)
  - Risparmi sulla deduplica
  - Ultimo tempo di accesso noto

    - Ora ultima istantanea
    - Altra capacità utilizzata
    - Numero di snapshot
    - Capacità utilizzata di Snapshot
    - Capacità totale utilizzata
- IP iSCSI Session Initiator, ID sessione di destinazione e ID sessione initiator
- Capacità utilizzata quota qtree
- Quota di file utilizzati e capacità utilizzata
- Tecnologia per l'efficienza dello storage, guadagno/perdita e potenziale guadagno/perdita
- Pool di storage
    - Data used Capacity (capacità utilizzata dati)
    - Risparmi sulla deduplica
    - Altra capacità utilizzata
    - Capacità utilizzata di Snapshot
    - Capacità totale utilizzata
- Volume
    - Risparmi sulla deduplica
    - Ultimo tempo di accesso noto
    - Capacità utilizzata

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Fare clic sulla scheda **Advanced Settings** (Impostazioni avanzate), nella sezione Acquisition Dynamic Attributes (attributi dinamici di acquisizione) inserire il numero di ore in cui OnCommand Insight deve ignorare i dati dinamici per gli attributi dinamici di acquisizione.
4. Fare clic su **Save** (Salva).
5. (Facoltativo) per riavviare l'unità di acquisizione, fare clic sul collegamento **Restart Acquisition Unit** (Riavvia unità di acquisizione).

   Il ripristino dell'unità di acquisizione locale ricarica tutte le viste dell'origine dati OnCommand Insight. Questa modifica viene applicata durante il polling successivo, quindi non è necessario riavviare l'unità di acquisizione.

Generazione di log per il supporto clienti

Se richiesto dal supporto clienti, generare un server, un'acquisizione o un log remoto per la risoluzione dei problemi.

A proposito di questa attività

Se il supporto clienti NetApp richiede, utilizzare questa opzione per generare i registri.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic su **risoluzione avanzata dei problemi**.
3. Nella pagina successiva del menu Avanzate, fare clic sul collegamento **risoluzione dei problemi**.
4. Fare clic sulla scheda **Logs** e selezionare il file di log da scaricare.

   Viene visualizzata una finestra di dialogo che consente di aprire il log o di salvarlo localmente.

Visualizzazione delle informazioni di sistema

È possibile visualizzare le informazioni di configurazione IP di Microsoft Windows relative al sistema su cui viene implementato il server OnCommand Insight.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Nella pagina Advanced Troubleshooting (risoluzione avanzata dei problemi), fare clic sulla scheda **Report**.
4. Fare clic su **System Information** (informazioni di sistema).

   La configurazione IP di Windows include informazioni quali nome host, DNS, indirizzo IP, subnet mask, informazioni sul sistema operativo, memoria, dispositivo di avvio e nome della connessione.

Elenco dei componenti OnCommand Insight installati

È possibile visualizzare un elenco dei componenti OnCommand Insight installati, inclusi, tra gli altri, inventario, capacità, dimensioni, E le viste del Data Warehouse. L'assistenza clienti potrebbe richiedere queste informazioni oppure potrebbe essere necessario verificare quali versioni software sono state installate e quando sono state installate.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Nella pagina Advanced Troubleshooting (risoluzione avanzata dei problemi), fare clic sulla scheda **Report**.
4. Fare clic su **pacchetti software installati**.

Calcolo del numero di oggetti di database

Per determinare il numero di oggetti nel database OnCommand Insight, utilizzare la funzione Calcola scala.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Nella pagina Advanced Troubleshooting (risoluzione avanzata dei problemi), fare clic sulla scheda **Report**.
4. Fare clic su **Calculated Scale**.

Riavvio del server OnCommand Insight

Quando si riavvia il server OnCommand Insight, aggiornare la pagina e accedere nuovamente al portale OnCommand Insight.

A proposito di questa attività

> Entrambe queste opzioni devono essere utilizzate solo su richiesta del supporto clienti NetApp. Prima del riavvio non viene ricevuta alcuna conferma.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Nella pagina successiva del menu Avanzate, fare clic sulla scheda **azioni**.
4. Fare clic su **Riavvia server**.

Spostamento dei dati MySQL tramite l'opzione di migrazione

È possibile utilizzare la migrazione della directory dei dati MySQL in un'altra directory. È possibile conservare la directory dei dati corrente. È possibile utilizzare l'opzione Migrate (migrazione) nel menu Troubleshooting (risoluzione dei problemi) oppure la riga di comando. Questa procedura descrive come utilizzare l'opzione **risoluzione dei problemi** > **migrazione dei dati MySQL**.

A proposito di questa attività

Se si conserva la directory dei dati corrente, questa viene conservata come backup e rinominata.

Fasi

1. Nell'interfaccia utente Web, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Fare clic su **risoluzione avanzata dei problemi**.
3. Selezionare la scheda **azioni**
4. Selezionare **Migrate MySQL Data**.
5. Immettere il percorso in cui si desidera migrare i dati.
6. Per conservare la directory dei dati esistente, selezionare **Mantieni directory dei dati esistente.**
7. Fare clic su **Migra**.

Spostamento dei dati MySQL tramite la riga di comando

È possibile utilizzare la migrazione della directory dei dati MySQL in un'altra directory. È possibile conservare la directory dei dati corrente. È possibile utilizzare l'opzione Migrate (migrazione) nel menu Troubleshooting (risoluzione dei problemi) oppure la riga di comando. Questa procedura descrive come utilizzare la riga di comando.

A proposito di questa attività

Se si conserva la directory dei dati corrente, questa viene conservata come backup e rinominata.

È possibile utilizzare l'utility Migrate MySQL Data o un `java -jar mysqldatamigrator.jar` Nel percorso OnCommand Insight di `\bin\mysqldatamigrator` dove devono essere utilizzati i seguenti parametri:

- Parametri obbligatori
  - **-path**

    Il nuovo percorso di dati in cui verrà copiata la cartella di dati.
- Parametri opzionali
  - **-myCnf <my .cnf file>**

    Il percorso del file .cnf. L'impostazione predefinita è `<install path>\mysql\my.cnf`. Utilizzare questo flag solo se si utilizza un MySQL non predefinito.
  - **-doBackup**

    Se questo indicatore è impostato, la cartella dei dati corrente verrà rinominata ma non eliminata.

Fasi

1. Accedere allo strumento della riga di comando qui: `<installation path>` mysqldatamigrator``

Esempio di utilizzo

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

Forzatura degli aggiornamenti delle annotazioni

Se le annotazioni sono state modificate e si desidera utilizzarle immediatamente nei report, utilizzare una delle opzioni di annotazione forzata.

Fasi

1. Nell'interfaccia utente Web, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Fare clic sulla scheda **azioni**.
4. Selezionare una delle seguenti opzioni:

- **Aggiornare le annotazioni DWH** per forzare l'aggiornamento delle annotazioni nel data warehouse da utilizzare per i report.
- **Aggiorna annotazioni DWH (incl cancellato)** per forzare l'aggiornamento delle annotazioni (inclusi gli oggetti cancellati) nel data warehouse da utilizzare per i report.

Verifica dello stato delle risorse del server

Questa opzione consente di visualizzare le informazioni del server OnCommand Insight, tra cui memoria del server, spazio su disco, sistema operativo e informazioni su CPU e database OnCommand Insight, incluse le dimensioni dei dati InnoDB e lo spazio libero su disco in cui risiede il database.

Fasi

1. Sulla barra degli strumenti di Insight, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **Portale OnCommand Insight**.
3. Nella pagina successiva del menu Avanzate, fare clic sul collegamento **risoluzione dei problemi**.
4. Fare clic su **Stato risorse server**.

   Per gli utenti OnCommand Insight avanzati: l'amministratore può eseguire alcuni test SQL per controllare il tempo di risposta del database e del server dal pulsante alla fine del riepilogo delle informazioni. Questa opzione visualizza un avviso se le risorse del server sono in esaurimento.

Individuazione di origini dati fantasma

Se è stata rimossa una periferica ma i dati rimangono, è possibile individuare eventuali origini dati fantasma in modo da poterle rimuovere.

Fasi

1. Nell'interfaccia utente Web, fare clic su **Admin** e selezionare **Troubleshooting**.
2. Nella parte inferiore della pagina dell'area altre attività, fare clic sul collegamento **risoluzione avanzata dei problemi**.
3. Nella scheda **Report**, fare clic sul collegamento **origini dati fantasma**.

   OnCommand Insight crea un elenco di utenti che hanno generato le informazioni sul dispositivo.

Aggiunta di un modello di disco mancante

Se l'acquisizione non riesce a causa di un modello di disco sconosciuto, è possibile aggiungere il modello di disco mancante al `new_disk_models.txt` archiviare ed eseguire nuovamente l'acquisizione.

A proposito di questa attività

Nell'ambito di un sondaggio di un dispositivo di storage da parte dell'acquisizione di OnCommand Insight, vengono letti i modelli di disco sul dispositivo di storage. Se un vendor ha aggiunto nuovi modelli di dischi al proprio array di cui Insight non è a conoscenza, o se c'è una discrepanza tra il numero di modello che Insight

cerca e quello restituito dal dispositivo di storage, l'acquisizione di tale origine dati non riuscirà e si verificherà un errore. Per evitare questi errori, è necessario aggiornare le informazioni sul modello di disco note a Insight. Nuovi modelli di dischi vengono aggiunti a Insight con aggiornamenti, patch e release di manutenzione. Tuttavia, è possibile decidere di aggiornare queste informazioni manualmente invece di attendere una patch o un aggiornamento.

Poiché OnCommand Insight legge il file del modello di disco ogni cinque minuti, tutte le informazioni del nuovo modello di dati inserite vengono aggiornate automaticamente. Non è necessario riavviare il server per rendere effettive le modifiche, ma è possibile scegliere di riavviare il server e qualsiasi unità di acquisizione remota (Raus) per rendere effettive le modifiche prima del prossimo aggiornamento.

Gli aggiornamenti del modello di disco vengono aggiunti a `new_disk_models.txt` file che si trova in`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directory. Comprendere le informazioni necessarie per descrivere il nuovo modello di disco prima di aggiornare `new_disk_models.txt` file. Informazioni imprecise nel file producono dati di sistema non corretti e potrebbero causare un'acquisizione non riuscita.

Seguire queste istruzioni per aggiornare manualmente i modelli di dischi Insight:

Fasi

1. Individuare le informazioni appropriate per il modello di disco in uso.
2. Utilizzando un editor di testo, aprire `new_disk_models.txt` file.
3. Aggiungere le informazioni richieste per la nuova origine dati.
4. Salvare il file in `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` directory sul server.
5. Eseguire il backup di `new_disk_models.txt` file in una posizione sicura. Durante qualsiasi successivo aggiornamento di OnCommand Insight, questo file verrà sovrascritto. Se le informazioni sul modello di disco non sono presenti nel file aggiornato, sarà necessario immetterle nuovamente.

Individuazione delle informazioni richieste per il nuovo modello di disco

Per individuare le informazioni sul modello del disco, identificare il fornitore e il numero di modello ed eseguire una ricerca su Internet.

A proposito di questa attività

Individuare le informazioni sul modello di disco è semplice quanto eseguire una ricerca su Internet. Annotare il nome del vendor e il numero del modello del disco prima di eseguire la ricerca.

Fasi

1. Si consiglia di utilizzare una ricerca avanzata su Internet per il vendor, il modello e il tipo di documento "PDF" per trovare la scheda tecnica del vendor e/o la guida all'installazione del disco. Queste schede tecniche sono di solito la fonte migliore per le informazioni sui dischi dei vendor.
2. Le specifiche del vendor non forniscono sempre tutte le informazioni necessarie in base al numero di modello completo. Spesso è utile cercare diverse parti della stringa del numero di modello sul sito del vendor per individuare tutte le informazioni.
3. Individuare il nome del produttore del disco, il numero completo del modello, le dimensioni e la velocità del disco e il tipo di interfaccia per definire il nuovo modello di disco in OnCommand Insight, è possibile

utilizzare la seguente tabella come guida per annotare queste informazioni man mano che vengono trovate:

Per questo campo:	Che è:	Inserire questo:
Numero di modello (noto anche come chiave)	Obbligatorio	
Vendor	Obbligatorio	
Velocità del disco (giri/min)	Obbligatorio	
Dimensioni (in GB)	Obbligatorio	
Tipo di interfaccia (selezionarne una)	Obbligatorio	ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, ALTRO
Tempo di ricerca in ms.	Opzionale	
Massima velocità di trasferimento in MB/sec	Opzionale	
Velocità di trasferimento dell'interfaccia in MB/sec	Opzionale	
Collegamento alle informazioni sul fornitore/modello	Facoltativo ma consigliato	

4. Immettere tali informazioni in `new_disk_models.txt` file. Vedere "Contenuto del file new_disk_models.txt" per formato, ordine ed esempi.

Contenuto del file new_disk_models.txt

Il `new_disk_models.txt` il file contiene campi obbligatori e facoltativi. I campi sono separati da virgole, quindi non utilizzare virgole all'interno dei campi.

Tutti i campi sono obbligatori, ad eccezione del tempo di ricerca, delle velocità di trasferimento e delle informazioni_aggiuntive. Se disponibile, includere il collegamento al sito Web vendor/model nel campo additional_info.

Utilizzando un editor di testo, inserire le seguenti informazioni in questo ordine, separate da virgole, per ogni nuovo modello di disco che si desidera aggiungere:

1. **key**: usa il numero di modello (obbligatorio)
2. **vendor**: nome (obbligatorio)
3. **numero di modello**: numero completo (di solito lo stesso valore della "chiave") (obbligatorio)
4. **rpm del disco**: ad esempio 10000 o 15000 (richiesto)
5. **Size**: Capacità in GB (richiesta)

6. **Tipo di interfaccia**: ATA, SATA, FC, SAS, FATA, SSD, ALTRO (obbligatorio)
7. **tempo di ricerca**: in ms (opzionale)
8. **Potenziale velocità di trasferimento**: La potenziale velocità di trasferimento in MB/sec. Velocità massima di trasferimento del disco stesso. (opzionale)
9. **Velocità di trasferimento dell'interfaccia**: La velocità da e verso l'host in MB/sec (opzionale).
10. **Informazioni aggiuntive**: Qualsiasi informazione aggiuntiva che si desidera acquisire. La procedura consigliata consiste nell'inserire il collegamento alla pagina del vendor in cui sono trovate le specifiche, come riferimento (facoltativo)

Per i campi facoltativi lasciati vuoti, assicurati di includere la virgola.

Esempi (ciascuno su una riga senza spazi):

```
ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,http://www.seagate.com/staticfil
es/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,,https://storage.to
shiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf
```

Monitoraggio dell'ambiente

Insight ti aiuta a prevenire i problemi nel tuo ambiente e a risolvere rapidamente i potenziali problemi.

Dati della pagina delle risorse

Le pagine delle risorse forniscono dati sulla risoluzione dei problemi relativi alle performance e presentano informazioni riepilogative su una risorsa di base (ad esempio una macchina virtuale o un volume) e sulle risorse correlate utilizzate (ad esempio pool di storage, nodi di storage e porte switch connesse), con collegamenti a informazioni aggiuntive.

A partire da OnCommand Insight 7.3.1, tutte le pagine delle risorse hanno una pagina **principale** e una pagina **dati aggiuntivi**. Nella pagina principale sono riportati un riepilogo delle risorse e diverse sezioni relative a grafici, topologia e altre informazioni. La pagina **dati aggiuntivi** consente di configurare una pagina dashboard personalizzabile per il tipo di risorsa corrente.

Un cerchio rosso fisso accanto a una riga o a un messaggio nella scheda principale della pagina delle risorse indica potenziali problemi con l'ambiente monitorato.

Tipi di pagine di risorse

Le pagine delle risorse riepilogano lo stato corrente di una risorsa e contengono collegamenti a informazioni aggiuntive sulla risorsa e sulle risorse correlate.

OnCommand Insight fornisce pagine di risorse per le seguenti risorse:

- Macchina virtuale
- Volume
- Volume interno
- Host fisico
- Pool di storage
- Storage
- Datastore
- Hypervisor
- Applicazione
- Nodo storage
- Qtree
- Disco
- VMDK
- Porta
- Switch
- Fabric
- Storage a oggetti (ad esempio, Atmos, Centera, Amazon S3)
- Zona

Le informazioni di mappatura e mascheratura possono essere visualizzate nelle tabelle delle pagine delle risorse zone, Volume, VM e host/hypervisor.

> Le informazioni di riepilogo sono disponibili per le risorse di storage a oggetti; tuttavia, è possibile accedere a queste informazioni solo dalla pagina Dettagli origini dati.

Ricerca di risorse specifiche nel tuo ambiente

È possibile individuare informazioni su risorse specifiche utilizzando la funzione di ricerca. Ad esempio, se un utente del sistema contatta l'amministratore dello storage per un reclamo relativo a un determinato server, l'amministratore può cercare il nome del server e visualizzare una pagina delle risorse che riepiloga lo stato e fornisce ulteriori informazioni collegate.

Fasi

1. Aprire l'interfaccia utente Web di OnCommand.
2. Sulla barra degli strumenti, fare clic su .

   Viene visualizzata la casella **Cerca risorse**.

3. Immettere il nome di una risorsa o parte del nome.
4. Selezionare la risorsa desiderata dai risultati della ricerca.

   Viene visualizzata la pagina delle risorse per tale risorsa.

È possibile utilizzare più tecniche di ricerca per cercare dati o oggetti nell'ambiente monitorato.

Ricerca con caratteri jolly

È possibile eseguire la ricerca di più caratteri jolly utilizzando il carattere *. Ad esempio, *appic*n* restituirebbe l'applicazione.

Frasi utilizzate nella ricerca

Una frase è un gruppo di parole racchiuse tra virgolette doppie, ad esempio "PAW VNX LUN 5". Puoi utilizzare le virgolette doppie per cercare documenti che contengono spazi nei loro nomi o attributi.

Operatori booleani

Utilizzando gli operatori booleani, è possibile combinare più termini per formare una query più complessa.

- **O**
  - L'operatore OR è l'operatore di congiunzione predefinito.

    Se non esiste un operatore booleano tra due termini, viene utilizzato L'operatore OR.
  - L'operatore OR collega due termini e trova un documento corrispondente se uno dei termini esiste in un documento.

    Ad esempio, "storage OR netapp" cerca i documenti che contengono "storage" o "netapp".
  - I punteggi più alti vengono assegnati ai documenti che corrispondono alla maggior parte dei termini.
- **E**

  È possibile utilizzare L'operatore AND per trovare i documenti in cui entrambi i termini di ricerca esistono in un singolo documento. Ad esempio, "aurora E netapp" ricerca i documenti che contengono "storage" e "netapp".

  È possibile utilizzare il simbolo && invece della parola E.
- **NON**

  Quando si utilizza L'operatore NOT, tutti i documenti che contengono il termine After NOT vengono esclusi dai risultati della ricerca. Ad esempio, "storage NOT netapp" ricerca i documenti che contengono solo "storage" e non "netapp".

  È possibile utilizzare il simbolo ! Invece della parola NO.

Ricerca di prefisso e suffisso

- Non appena si inizia a digitare una stringa di ricerca, il motore di ricerca esegue una ricerca di prefisso e suffisso per trovare la corrispondenza migliore.
- Alle corrispondenze esatte viene assegnato un punteggio più elevato rispetto a una corrispondenza con prefisso o suffisso. Il punteggio viene calcolato in base alla distanza del termine di ricerca dal risultato effettivo della ricerca. Ad esempio, abbiamo tre storage: "aurora", "aurora1" e "aurora11". La ricerca di "aur"

restituirà tutti e tre gli storage. Tuttavia, il risultato della ricerca per “aurora” avrà il punteggio più alto perché ha la distanza più vicina alla stringa di ricerca del prefisso.

- Il motore di ricerca cerca anche i termini in ordine inverso, che consente di eseguire una ricerca di suffissi. Ad esempio, quando si digita “345” nella casella di ricerca, il motore di ricerca cerca “345”.
- La ricerca non fa distinzione tra maiuscole e minuscole.

Ricerca con termini indicizzati

Le ricerche che corrispondono a un maggior numero di termini indicizzati determinano punteggi più elevati.

La stringa di ricerca viene divisa in termini di ricerca separati per spazio. Ad esempio, la stringa di ricerca “storage aurora netapp” è divisa in tre parole chiave: “storage”, “aurora” e “netapp”. La ricerca viene eseguita utilizzando tutti e tre i termini. I documenti che corrispondono alla maggior parte di questi termini avranno il punteggio più alto. Maggiori sono le informazioni fornite, migliori sono i risultati della ricerca. Ad esempio, è possibile cercare uno storage in base al nome e alla modalità.

L’interfaccia utente visualizza i risultati della ricerca in diverse categorie, con i tre risultati principali per categoria. Se non è stato trovato un documento previsto, è possibile includere più termini nella stringa di ricerca per migliorare i risultati della ricerca.

La tabella seguente fornisce un elenco di termini indicizzati che è possibile aggiungere alla stringa di ricerca.

Categoria	Termini indicizzati
Storage	• “storage” • nome • vendor • modello
StoragePool	• “storagepool” • nome • nome dello storage • Indirizzi IP dello storage • numero di serie dello storage • vendor di soluzioni storage • modello di storage • nomi di tutti i volumi interni associati • nomi di tutti i dischi associati

Volume interno	• “internalvolume” • nome • nome dello storage • Indirizzi IP dello storage • numero di serie dello storage • vendor di soluzioni storage • modello di storage • nome del pool di storage • nomi di tutte le condivisioni associate • nomi di tutte le applicazioni e le entità aziendali associate
Volume	• “volume” • nome • etichetta • nomi di tutti i volumi interni • nome del pool di storage • nome dello storage • Indirizzi IP dello storage • numero di serie dello storage • vendor di soluzioni storage • modello di storage
Nodo di storage	• “storagenode” • nome • nome dello storage • Indirizzi IP dello storage • serialnumber dello storage • vendor di soluzioni storage • modello di storage
Host	• “host” • nome • Indirizzi IP • nomi di tutte le applicazioni e le entità aziendali associate

Datastore	• “datastore” • nome • IP del centro virtuale • nomi di tutti i volumi • nomi di tutti i volumi interni
Macchine virtuali	• “virtualmachine” • nome • Nome DNS • Indirizzi IP • nome dell’host • Indirizzi IP dell’host • nomi di tutti i datastore • nomi di tutte le applicazioni e le entità aziendali associate
Switch (Regular e NPV)	• “sstrega” • Indirizzo IP • wwn • nome • numero di serie • modello • ID dominio • nome del fabric • wwn del fabric
Applicazione	• “application” • nome • tenant • linea di business • unità aziendale • progetto
Nastro	• “tape” • Indirizzo IP • nome • numero di serie • vendor

Porta	• “porta” • wwn • nome
Fabric	• “fabric” • wwn • nome

Modifica dell’intervallo di tempo dei dati visualizzati

Per impostazione predefinita, una pagina delle risorse visualizza le ultime 24 ore di dati; tuttavia, è possibile modificare il segmento di dati visualizzato selezionando un altro tempo fisso o un intervallo di tempo personalizzato per visualizzare un numero inferiore o superiore di dati.

A proposito di questa attività

È possibile modificare l’intervallo temporale dei dati visualizzati utilizzando un’opzione che si trova in ogni pagina di risorsa, indipendentemente dal tipo di risorsa.

Fasi

1. Accedere all’interfaccia utente Web di OnCommand Insightweb.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall’elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse.
3. Nell’angolo superiore sinistro della pagina, fare clic su una delle seguenti icone temporali per modificare il segmento di dati visualizzato:
   - **3 ore**

     Visualizza le ultime tre ore di dati.

   - **24 ore**

     Visualizza le ultime 24 ore di dati.

   - **3d**

     Visualizza gli ultimi tre giorni di dati.

   - **7d**

     Visualizza gli ultimi sette giorni di dati.

   - **30d**

Visualizza gli ultimi trenta giorni di dati.

- **Personalizzato**

  Visualizza una finestra di dialogo che consente di scegliere un intervallo di tempo personalizzato. È possibile visualizzare fino a 31 giorni di dati alla volta.

4. Se si sceglie **Custom**, procedere come segue:
   a. Fare clic sul campo della data e selezionare un mese, un giorno e un anno per la data di inizio.
   b. Fare clic sull'elenco delle ore e selezionare un'ora di inizio.
   c. Ripetere i passaggi a e b per i dati e l'ora di fine.
   d. Fare clic su .

Determinazione dello stato di acquisizione dell'origine dati

Poiché le origini dati sono la principale fonte di informazioni per Insight, è fondamentale assicurarsi che rimangano in uno stato di esecuzione.

La possibilità di visualizzare lo stato di acquisizione dell'origine dati è disponibile in ogni pagina delle risorse per tutte le risorse acquisite direttamente. È possibile che si verifichi uno dei seguenti scenari di acquisizione, in cui lo stato viene visualizzato nell'angolo superiore destro della pagina delle risorse:

- Acquisizione riuscita dall'origine dati

  Visualizza lo stato "acquisito `xxxx`", where `xxxx` indica il tempo di acquisizione più recente delle origini dati dell'asset.

- Si è verificato un errore di acquisizione.

  Visualizza lo stato "acquisito `xxxx`", where `xxxx` indica il tempo di acquisizione più recente di una o più origini dati dell'asset con . Quando si fa clic su , una finestra visualizza ogni origine dati per l'asset, lo stato dell'origine dati e l'ultima volta che i dati sono stati acquisiti. Facendo clic su un'origine dati viene visualizzata la pagina dei dettagli dell'origine dati.

Se un asset non viene acquisito direttamente, non viene visualizzato alcun stato.

Sezioni della pagina delle risorse

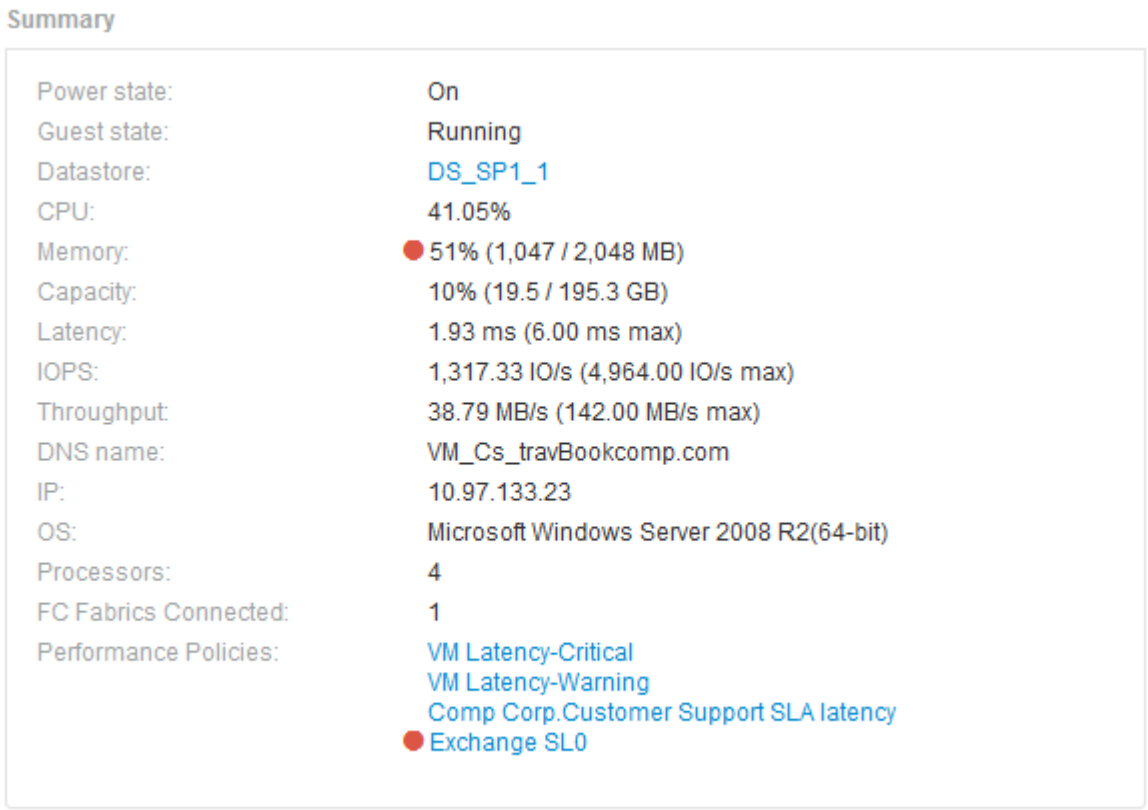
Una pagina delle risorse visualizza diverse sezioni contenenti informazioni relative alla risorsa. Le sezioni visualizzate dipendono dal tipo di risorsa.

Riepilogo

La sezione Summary (Riepilogo) di una pagina asset visualizza un riepilogo delle informazioni relative alla risorsa specifica e mostra i problemi relativi alla risorsa, indicati da un cerchio rosso, con collegamenti ipertestuali a informazioni aggiuntive sulle risorse correlate e a eventuali policy di performance assegnate alla risorsa.

Nell'esempio riportato di seguito vengono illustrati alcuni tipi di informazioni disponibili nella sezione Summary (Riepilogo) di una pagina di risorse per una macchina virtuale. Qualsiasi elemento con un cerchio rosso fisso

accanto ad esso indica potenziali problemi con l'ambiente monitorato.



Utilizzando la sezione Summary (Riepilogo)

È possibile visualizzare la sezione Summary (Riepilogo) per visualizzare informazioni generali su una risorsa. In particolare, è utile verificare se le metriche (ad esempio, memoria, capacità e latenza) o le policy sulle performance sono fonte di preoccupazione, come indicato da OnCommand Insight visualizzando un cerchio rosso accanto alla metrica o alla policy sulle performance.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse.

     Le informazioni visualizzate nella sezione Riepilogo dipendono dal tipo di pagina delle risorse che si sta visualizzando.

3. È possibile fare clic su uno dei collegamenti alle risorse per visualizzarne le pagine.

   Ad esempio, se si sta visualizzando un nodo di storage, è possibile fare clic su un collegamento per

visualizzare la pagina delle risorse dello storage a cui è associato oppure fare clic per visualizzare la pagina delle risorse del partner ha.

4. È possibile visualizzare le metriche associate alla risorsa.

   Un cerchio rosso accanto a una metrica indica che potrebbe essere necessario diagnosticare e risolvere potenziali problemi.

   > È possibile che la capacità del volume sia superiore al 100% su alcune risorse di storage. Ciò è dovuto ai metadati relativi alla capacità del volume che fa parte dei dati di capacità consumata riportati dall'asset.

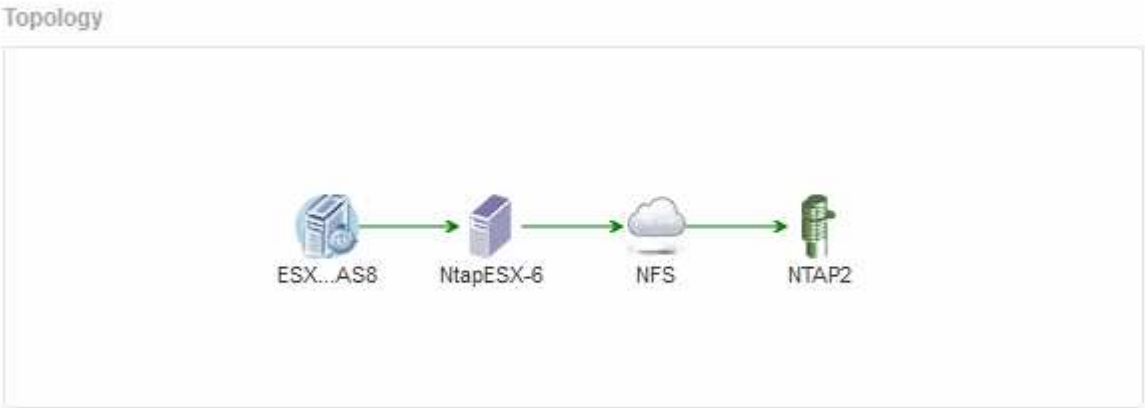
5. Se applicabile, è possibile fare clic su un collegamento al criterio di performance per visualizzare il criterio o i criteri di performance associati alla risorsa.

   Se viene visualizzato un cerchio rosso accanto a un criterio di performance, significa che un asset ha superato la soglia definita dal criterio di performance. Per diagnosticare ulteriormente il problema, è necessario esaminare la policy sulle performance.

Topologia

La sezione topologia, se applicabile a una risorsa, consente di vedere come una risorsa di base è connessa alle risorse correlate.

Di seguito viene riportato un esempio di ciò che potrebbe essere visualizzato nella sezione topologia della pagina delle risorse di una macchina virtuale.



Se la topologia della risorsa è più grande di quella che si adatta alla sezione, viene visualizzato il collegamento **Click per visualizzare la topologia**.

Utilizzo della sezione topologia

La sezione topologia consente di visualizzare le modalità di connessione tra le risorse della rete e le informazioni relative alle risorse correlate.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:

- Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
- Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse. La sezione topologia si trova nell'angolo in alto a destra della pagina delle risorse.

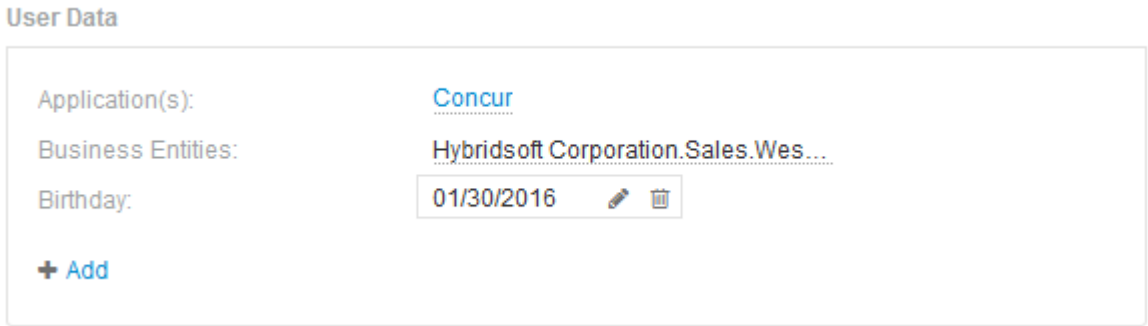
Se la topologia della risorsa è più grande di quella che si adatta alla sezione, fare clic sul collegamento **fare clic per visualizzare il collegamento ipertestuale topologia**.

3. Per visualizzare ulteriori informazioni sulle risorse correlate alla risorsa di base, posizionare il cursore su una risorsa correlata nella topologia e fare clic sul relativo nome, che visualizza la relativa pagina.

Dati dell'utente

Viene visualizzata la sezione User Data (dati utente) di una pagina di risorse che consente di modificare i dati definiti dall'utente, ad esempio applicazioni, entità aziendali e annotazioni.

Di seguito viene riportato un esempio di ciò che potrebbe essere visualizzato nella sezione User Data (dati utente) della pagina delle risorse di una macchina virtuale quando un'applicazione, un'entità aziendale e un'annotazione vengono assegnati alla risorsa:



Utilizzo della sezione User Data (dati utente) per assegnare o modificare le applicazioni

È possibile assegnare le applicazioni in esecuzione nel proprio ambiente a determinate risorse (host, macchine virtuali, volumi, volumi interni e hypervisor). La sezione User Data (dati utente) consente di modificare l'applicazione assegnata a una risorsa o di assegnare un'applicazione o applicazioni aggiuntive a una risorsa.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse.
3. È possibile effettuare le seguenti operazioni:
   - Per visualizzare la pagina delle risorse dell'applicazione, fare clic sul nome dell'applicazione.

- Per modificare l'applicazione assegnata o per assegnare un'applicazione o altre applicazioni, posizionare il cursore sul nome dell'applicazione, se è assegnata un'applicazione, oppure su **Nessuno**, se non è assegnata alcuna applicazione, fare clic su , digitare per cercare un'applicazione o selezionarne una dall'elenco, quindi fare clic su .

  Se si sceglie un'applicazione associata a un'entità aziendale, l'entità aziendale viene assegnata automaticamente all'asset. In questo caso, quando si posiziona il cursore sul nome dell'entità aziendale, viene visualizzata la parola *derived*. 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.

- Per rimuovere un'applicazione, fare clic su .

Utilizzo della sezione dati utente per assegnare o modificare le entità aziendali

È possibile definire entità di business per tenere traccia e generare report sui dati dell'ambiente a un livello più granulare. La sezione User Data (dati utente) di una pagina asset consente di modificare l'entità aziendale assegnata a un asset o di rimuovere un'entità aziendale da un asset.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse.
3. È possibile effettuare le seguenti operazioni:
   - Per modificare l'entità assegnata o per assegnarla, fare clic su e selezionare un'entità dall'elenco.
   - Per rimuovere un'entità aziendale, fare clic su .

     Non è possibile rimuovere un'entità derivata da un'applicazione assegnata alla risorsa.

Utilizzare la sezione User Data (dati utente) per assegnare o modificare le annotazioni

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. La sezione User Data (dati utente) di una pagina asset visualizza le annotazioni assegnate a una risorsa e consente di modificare le annotazioni assegnate a tale risorsa.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la

risorsa dall'elenco.

- Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. 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).

   L'annotazione viene assegnata alla risorsa. È possibile filtrare le risorse in un secondo momento mediante un'annotazione utilizzando una query.

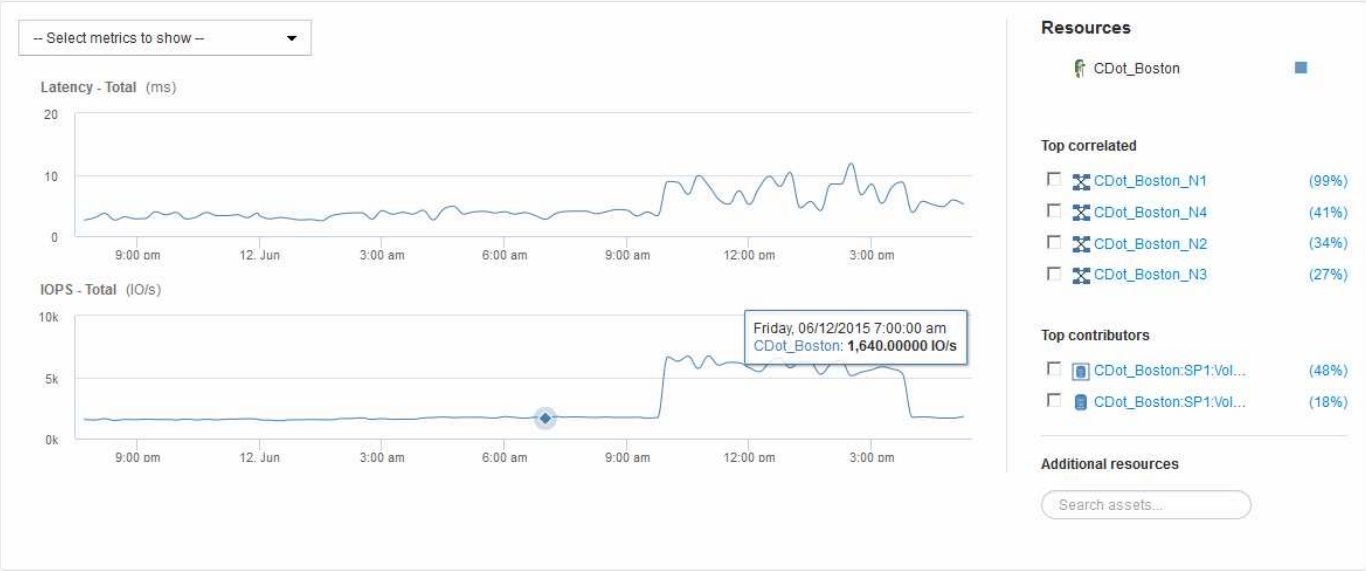
7. Se si desidera modificare il valore dell'annotazione dopo l'assegnazione, fare clic su e selezionare un valore diverso.

   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.

Vista degli esperti

La sezione Expert View di una pagina di risorse consente di visualizzare un esempio di performance per la risorsa di base in base a un numero qualsiasi di metriche applicabili nel contesto con un periodo di tempo scelto (3 ore, 24 ore, 3 giorni, 7 giorni, o un periodo di tempo personalizzato) nel grafico delle performance e nelle risorse ad esso correlate.

Di seguito viene riportato un esempio della sezione visualizzazione avanzata in una pagina di risorse per volumi:



È possibile selezionare le metriche che si desidera visualizzare nel grafico delle performance per il periodo di tempo selezionato.

La sezione risorse mostra il nome della risorsa di base e il colore che rappresenta la risorsa di base nel grafico delle performance. Se la sezione Top Correlated non contiene una risorsa che si desidera visualizzare nel grafico delle performance, è possibile utilizzare la casella **Search Assets** (Cerca risorse) nella sezione Additional Resources (risorse aggiuntive) per individuare la risorsa e aggiungerla al grafico delle performance. Quando si aggiungono risorse, queste vengono visualizzate nella sezione risorse aggiuntive.

Nella sezione risorse, se applicabile, sono inoltre riportate le risorse correlate alla risorsa di base nelle seguenti categorie:

- Correlato in alto

  Mostra le risorse con un'elevata correlazione (percentuale) con una o più metriche delle performance rispetto alla risorsa di base.

- Principali collaboratori

  Mostra le risorse che contribuiscono (percentuale) alla risorsa di base.

- Avido

  Mostra le risorse che allontanano le risorse di sistema dalla risorsa attraverso la condivisione delle stesse risorse, come host, reti e storage.

- Degradato

  Mostra le risorse che sono esaurite dalle risorse di sistema a causa di questa risorsa.

Definizioni metriche Expert View

La sezione visualizzazione avanzata di una pagina di risorse visualizza diverse metriche in base al periodo di tempo selezionato per la risorsa. Ogni metrica viene visualizzata nel proprio grafico delle performance. Puoi aggiungere o rimuovere metriche e risorse correlate dai grafici a seconda dei dati che desideri visualizzare.

Metrico	Descrizione
BB Credit zero Rx, Tx	Numero di volte in cui il conteggio del credito buffer-to-buffer di ricezione/trasmissione è passato a zero durante il periodo di campionamento. Questa metrica rappresenta il numero di volte in cui la porta collegata ha dovuto interrompere la trasmissione perché questa porta non era in credito da fornire.
Durata zero credito BB Tx	Tempo in millisecondi durante il quale il credito BB trasmesso era pari a zero durante l'intervallo di campionamento.

Percentuale di hit della cache (totale, lettura, scrittura) %	Percentuale di richieste che generano riscontri nella cache. Maggiore è il numero di accessi rispetto agli accessi al volume, migliori sono le performance. Questa colonna è vuota per gli array di storage che non raccolgono le informazioni di accesso alla cache.
Utilizzo della cache (totale) %	Percentuale totale di richieste di cache che determinano accessi alla cache
Scartati di classe 3	Numero di scarti di trasporto dati Fibre Channel di classe 3.
Utilizzo della CPU (totale) %	Quantità di risorse CPU utilizzate attivamente, come percentuale del totale disponibile (su tutte le CPU virtuali).
Errore CRC	Numero di frame con CRC (Cyclic Redundancy Check) non validi rilevati dalla porta durante il periodo di campionamento
Frame rate	Frame rate di trasmissione in frame al secondo (FPS)
Dimensione media frame (Rx, Tx)	Rapporto tra traffico e dimensione del frame. Questa metrica consente di identificare la presenza di frame overhead nel fabric.
Dimensione frame troppo lunga	Numero di frame di trasmissione dati Fibre Channel troppo lunghi.
Dimensione del frame troppo breve	Numero di frame di trasmissione dati Fibre Channel troppo brevi.
Densità i/o (totale, lettura, scrittura)	Numero di IOPS diviso per la capacità utilizzata (acquisita dall'ultimo sondaggio di inventario dell'origine dati) per il volume, il volume interno o l'elemento di storage. Misurato in numero di operazioni di i/o al secondo per TB.
IOPS (totale, lettura, scrittura)	Numero di richieste di servizio i/o in lettura/scrittura che passano attraverso il canale i/o o una parte di tale canale per unità di tempo (misurato in i/o al secondo)
Throughput IP (totale, lettura, scrittura)	Total (totale): Tasso aggregato alla quale i dati IP sono stati trasmessi e ricevuti in megabyte al secondo. Lettura: Throughput IP (ricezione): Velocità media di ricezione dei dati IP in megabyte al secondo. Write: Throughput IP (trasmissione): Velocità media di trasmissione dei dati IP in megabyte al secondo.

Latenza (totale, lettura, scrittura)	Latenza (R&W): Velocità con cui i dati vengono letti o scritti sulle macchine virtuali in un periodo di tempo fisso. Il valore viene misurato in megabyte al secondo. Latenza: Tempo di risposta medio delle macchine virtuali in un archivio dati. Latenza massima: Il tempo di risposta più elevato dalle macchine virtuali in un archivio dati.
Errore di collegamento	Numero di errori di collegamento rilevati dalla porta durante il periodo di campionamento.
Link RESET Rx, Tx	Numero di ripristini del collegamento di ricezione o trasmissione durante il periodo di campionamento. Questa metrica rappresenta il numero di ripristini del collegamento emessi dalla porta collegata a questa porta.
Utilizzo della memoria (totale) %	Soglia per la memoria utilizzata dall'host.
% Parziale R/W (totale)	Numero totale di volte in cui un'operazione di lettura/scrittura attraversa un limite di stripe su qualsiasi modulo di disco in un LUN RAID 5, RAID 1/0 o RAID 0 generalmente, gli attraversamenti di stripe non sono vantaggiosi, perché ciascuno richiede un i/O. aggiuntivo Una percentuale bassa indica una dimensione efficiente degli elementi di stripe e indica un allineamento non corretto di un volume (o di un LUN NetApp). Per CLARiiON, questo valore è il numero di passaggi di stripe diviso per il numero totale di IOPS.
Errori di porta	Report degli errori di porta nel periodo di campionamento/intervallo di tempo specificato.
Conteggio delle perdite di segnale	Numero di errori di perdita del segnale. Se si verifica un errore di perdita del segnale, non è presente alcun collegamento elettrico e si è verificato un problema fisico.
Tasso di swap (tasso totale, tasso in entrata, tasso in uscita)	Velocità con cui la memoria viene scambiata in entrata, in uscita o entrambe le cose da disco a memoria attiva durante il periodo di campionamento. Questo contatore si applica alle macchine virtuali.

Numero di perdite di sincronizzazione	Numero di errori di perdita della sincronizzazione. Se si verifica un errore di perdita della sincronizzazione, l'hardware non può rilevare il traffico o bloccarsi su di esso. Tutte le apparecchiature potrebbero non utilizzare la stessa velocità di trasmissione dati oppure le ottiche o le connessioni fisiche potrebbero essere di scarsa qualità. La porta deve risincronizzarsi dopo ogni errore, con un impatto sulle prestazioni del sistema. Misurato in KB/sec.
Throughput (totale, lettura, scrittura)	Velocità con cui i dati vengono trasmessi, ricevuti o entrambi in un periodo di tempo fisso in risposta alle richieste di servizio i/o (misurata in MB al secondo).
Timeout Discard frames - Tx	Numero di frame di trasmissione scartati a causa del timeout.
Velocità di traffico (totale, lettura, scrittura)	Traffico trasmesso, ricevuto o entrambi ricevuti durante il periodo di campionamento, in megibyte al secondo.
Utilizzo del traffico (totale, lettura, scrittura)	Rapporto tra traffico ricevuto/trasmesso/totale e capacità di ricezione/trasmissione/totale, durante il periodo di campionamento.
Utilizzo (totale, lettura, scrittura) %	Percentuale della larghezza di banda disponibile utilizzata per la trasmissione (Tx) e la ricezione (Rx).
Scrittura in sospeso (totale)	Numero di richieste di servizio i/o in scrittura in sospeso.

Utilizzando la sezione visualizzazione avanzata

La sezione visualizzazione avanzata consente di visualizzare i grafici delle performance di una risorsa in base a un numero qualsiasi di metriche applicabili in un determinato periodo di tempo e di aggiungere risorse correlate per confrontare e confrontare le performance delle risorse e delle risorse correlate in diversi periodi di tempo.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
    - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
    - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse. Per impostazione predefinita, il grafico delle performance mostra due metriche per il periodo di tempo selezionato per la pagina delle risorse. Ad esempio, per uno storage, il grafico delle performance mostra la latenza e gli IOPS totali per

impostazione predefinita. La sezione risorse visualizza il nome della risorsa e una sezione risorse aggiuntive, che consente di cercare le risorse. A seconda della risorsa, è possibile visualizzare le risorse anche nelle sezioni Top Correlated, Top Contributor, Greedy e Degraded.

3. È possibile fare clic su **Select metrics to show** (Seleziona metriche da visualizzare) e selezionare una metrica per aggiungere un grafico delle performance per una metrica.

   Viene aggiunto un grafico delle performance per la metrica selezionata. Il grafico visualizza i dati relativi al periodo di tempo selezionato. È possibile modificare il periodo di tempo facendo clic su un altro periodo di tempo nell'angolo in alto a sinistra della pagina delle risorse.

   È possibile eseguire di nuovo il passo e fare clic su per cancellare una metrica. Il grafico delle prestazioni per la metrica viene rimosso.

4. È possibile posizionare il cursore sul grafico e modificare i dati metrici visualizzati facendo clic su una delle seguenti opzioni, a seconda della risorsa:
   - **Read** o **Write**
   - **Tx**o **Rx Total** è l'impostazione predefinita.
5. È possibile trascinare il cursore sui punti dati nel grafico per vedere come cambia il valore della metrica nel periodo di tempo selezionato.
6. Nella sezione **risorse**, è possibile effettuare una delle seguenti operazioni, se applicabile, per aggiungere eventuali risorse correlate ai grafici delle performance:
   - È possibile selezionare una risorsa correlata nelle sezioni Top Correlated, Top Contributors, Greedy o Degraded per aggiungere i dati da tale risorsa al grafico delle performance per ciascuna metrica selezionata. Le risorse devono avere una correlazione o un contributo minimo del 15% per essere mostrate.

     Dopo aver selezionato la risorsa, viene visualizzato un blocco di colori accanto alla risorsa per indicare il colore dei punti dati nel grafico.

   - Per qualsiasi risorsa visualizzata, è possibile fare clic sul nome della risorsa per visualizzarne la pagina oppure fare clic sulla percentuale in cui la risorsa è correlata o contribuisce alla risorsa di base per visualizzare ulteriori informazioni sulle risorse correlate alla risorsa di base.

     Ad esempio, facendo clic sulla percentuale collegata accanto a una risorsa correlata in alto viene visualizzato un messaggio informativo che confronta il tipo di correlazione della risorsa con la risorsa di base.

   - Se la sezione Top Correlated non contiene una risorsa che si desidera visualizzare in un grafico delle performance a scopo di confronto, è possibile utilizzare la casella **Search Assets** (Cerca risorse) nella sezione Additional Resources (risorse aggiuntive) per individuare altre risorse. Una volta selezionata, la risorsa viene visualizzata nella sezione risorse aggiuntive. Se non si desidera più visualizzare informazioni sulla risorsa, fare clic su 🗑 .

Risorse correlate

Se applicabile, una pagina di risorse visualizza una sezione risorse correlate. Ad esempio, una pagina delle risorse di un volume potrebbe mostrare informazioni su risorse come i pool di storage, le porte degli switch connessi e le risorse di calcolo. Ciascuna sezione comprende una tabella che elenca le risorse correlate di tale categoria, con collegamenti alle rispettive pagine di risorse e diverse statistiche sulle performance correlate.

Utilizzando la sezione risorse correlate

La sezione risorse correlate consente di visualizzare le risorse correlate alla risorsa di base. Ogni risorsa correlata viene visualizzata in una tabella insieme alle statistiche pertinenti per la risorsa. È possibile esportare le informazioni sulle risorse, visualizzare le statistiche delle risorse nei grafici delle prestazioni di Expert View o visualizzare un grafico che visualizza le statistiche solo per le risorse correlate.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su , digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse.
3. Per controllare il modo in cui le risorse vengono visualizzate nella tabella:
   - Fare clic sul nome di una risorsa per visualizzarne la pagina.
   - Utilizzare la casella **filter** per visualizzare solo risorse specifiche.
   - Se nella tabella sono presenti più di cinque risorse, fare clic su un numero di pagina per sfogliare le risorse per pagina.
   - Modificare l'ordinamento delle colonne di una tabella in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.
   - Aggiungi una risorsa correlata a qualsiasi grafico delle performance nella sezione visualizzazione esperto posizionando il cursore sulla risorsa correlata e facendo clic su .
4. Per esportare le informazioni visualizzate nella tabella in un `.CSV` file:
   a. Fare clic su .
   b. Fare clic su **Apri con**, quindi su **OK** per aprire il file con Microsoft Excel e salvarlo in una posizione specifica oppure fare clic su **Salva file** e quindi su **OK** per salvare il file nella cartella Download.

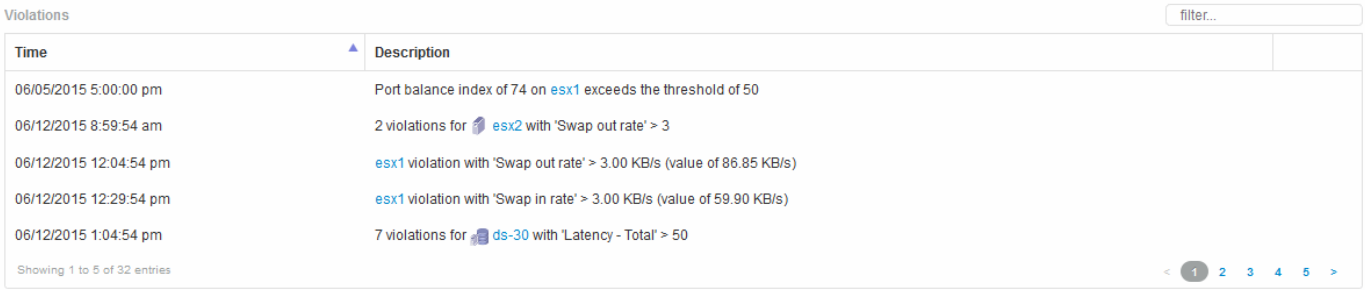
      Tutti gli attributi degli oggetti per le colonne attualmente selezionate per la visualizzazione vengono esportati nel file. Verranno esportati solo gli attributi delle colonne visualizzate. Si noti che vengono esportate solo le prime 10,000 righe della tabella.
5. Per visualizzare le informazioni relative alle risorse in un grafico sotto la tabella, fare clic su ed eseguire una delle seguenti operazioni:
   - Fare clic su **Read**,**Write** o **Total** per modificare i dati metrici visualizzati. **Total** è l'impostazione predefinita.
   - Fare clic su per selezionare una metrica diversa.
   - Fare clic su per modificare il tipo di grafico. **Grafico a linee** è l'impostazione predefinita.
   - Spostare il cursore sui punti dati nel grafico per vedere come cambia il valore della metrica nel periodo di tempo selezionato per ogni risorsa correlata.
   - Fare clic su una risorsa correlata nella legenda del grafico per aggiungerla o rimuoverla dal grafico.
   - Fare clic su un numero di pagina nella tabella delle risorse correlate per visualizzare altre risorse correlate nel grafico.

- Fare clic su ✖ per chiudere il grafico.

Violazioni

È possibile utilizzare la sezione violazioni di una pagina di risorse per visualizzare le eventuali violazioni che si verificano nell'ambiente in seguito a una policy di performance assegnata a una risorsa. Le policy sulle performance monitorano le soglie di rete e consentono di rilevare immediatamente una violazione di una soglia, identificare le implicazioni e analizzare l'impatto e la causa del problema in modo da consentire una correzione rapida ed efficace.

L'esempio seguente mostra la sezione delle violazioni che viene visualizzata in una pagina delle risorse per un hypervisor:



Utilizzando la sezione violazioni

La sezione violazioni consente di visualizzare e gestire le violazioni che si verificano nella rete in seguito a una policy di performance assegnata a una risorsa.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Nella barra degli strumenti Insight, fare clic su 🔍, digitare il nome della risorsa, quindi selezionare la risorsa dall'elenco.
   - Fare clic su **Dashboard**, selezionare **Dashboard delle risorse**, individuare il nome di una risorsa e fare clic su di essa. Viene visualizzata la pagina delle risorse. La sezione violazioni visualizza l'ora in cui si è verificata la violazione e una descrizione della soglia superata, insieme a un collegamento ipertestuale alla risorsa in cui si è verificata la violazione (ad esempio "2 viols abete ds-30 with latency - Total > 50").
3. È possibile eseguire una delle seguenti attività facoltative:
   - Utilizzare la casella **filter** per visualizzare solo violazioni specifiche.
   - Se nella tabella sono presenti più di cinque violazioni, fare clic su un numero di pagina per scorrere le violazioni per pagina.
   - Modificare l'ordinamento delle colonne di una tabella in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell'intestazione della colonna.
   - Fare clic sul nome della risorsa in una descrizione per visualizzarne la pagina; un cerchio rosso indica i problemi che richiedono ulteriori analisi.

È possibile fare clic sul criterio di performance, che visualizza la finestra di dialogo Modifica criterio, per esaminare il criterio di performance e apportare modifiche al criterio, se necessario.

- Fare clic su ✖ rimuovere una violazione dall'elenco se si stabilisce che il problema non è più motivo di preoccupazione.

Pagina delle risorse personalizzabile

È possibile visualizzare dati aggiuntivi in widget personalizzabili su ciascuna pagina di risorse. La personalizzazione della pagina per una risorsa applica la personalizzazione alle pagine per tutte le risorse di quel tipo.

È possibile personalizzare i widget della pagina delle risorse eseguendo le seguenti operazioni:

1. Aggiungere un widget alla pagina
2. Creare una query o un'espressione per il widget per mostrare i dati desiderati
3. Scegliere un filtro se si desidera
4. Scegliere un metodo di rollup o raggruppamento
5. Salvare il widget
6. Ripetere l'operazione per tutti i widget desiderati
7. Salvare la pagina delle risorse

È inoltre possibile aggiungere variabili alla pagina delle risorse personalizzate che possono essere utilizzate per perfezionare ulteriormente i dati esposti nei widget. Oltre alle variabili normali, ogni tipo di risorsa può utilizzare un insieme di variabili "€this" per identificare rapidamente le risorse direttamente correlate alla risorsa corrente, ad esempio, tutte le macchine virtuali ospitate dallo stesso hypervisor che ospita la macchina virtuale corrente.

Questa pagina di risorse personalizzate è unica per ogni utente e per ogni tipo di risorsa. Ad esempio, se l'utente A crea una pagina di risorse personalizzata per una macchina virtuale, tale pagina personalizzata verrà visualizzata per qualsiasi pagina di risorse della macchina virtuale per tale utente.

Gli utenti possono solo visualizzare, modificare o eliminare le pagine di risorse personalizzate create.

Le pagine di risorse personalizzate non sono incluse nella funzionalità di esportazione/importazione di Insight.

Comprendere le variabili

Le variabili speciali sulla pagina personalizzabile "dati aggiuntivi" di una risorsa consentono di mostrare facilmente informazioni aggiuntive direttamente correlate alla risorsa corrente.

A proposito di questa attività

Per utilizzare le variabili "` questo`" nei widget nella landing page personalizzabile della risorsa, segui la procedura riportata di seguito. Per questo esempio, aggiungeremo un widget di tabella.

> le variabili "`"` `sono valide solo per la landing page personalizzabile di una risorsa. Non sono disponibili per altre dashboard Insight. Le variabili "` this" disponibili variano in base al tipo di risorsa.

Fasi

1. Accedere a una pagina di risorse per una risorsa di propria scelta. Per questo esempio, scegliamo una pagina di risorse della macchina virtuale (VM). Eseguire una query o cercare una macchina virtuale e fare clic sul collegamento per accedere alla pagina delle risorse della macchina virtuale.

   Viene visualizzata la pagina delle risorse per la macchina virtuale.

2. Fare clic sull'elenco a discesa **Change view:** > **Additional Virtual Machine data** (dati macchina virtuale aggiuntivi) per accedere alla landing page personalizzabile della risorsa.
3. Fai clic sul pulsante **Widget** e scegli **Table widget**.

   Viene visualizzato il widget Table per la modifica. Per impostazione predefinita, tutti gli storage vengono visualizzati nella tabella.

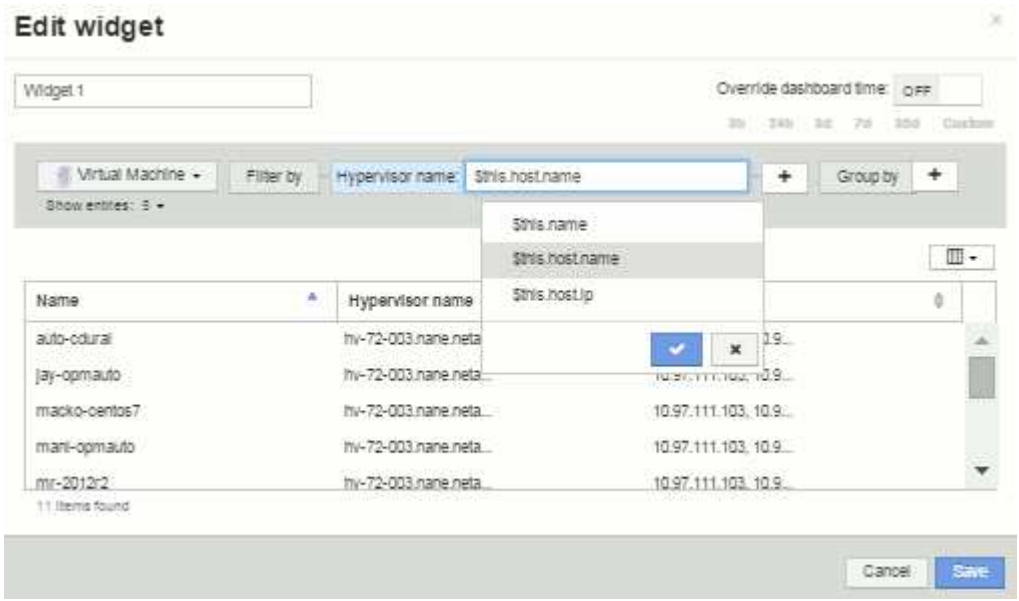
4. Vogliamo mostrare tutte le macchine virtuali. Fare clic sul selettore delle risorse e modificare **Storage** in **Virtual Machine**.

   Tutte le macchine virtuali sono ora visualizzate nella tabella.

5. Fare clic sul pulsante **selettore colonna*** **e aggiungere il campo *hypervisor name** alla tabella.

   Il nome dell'hypervisor viene visualizzato per ogni VM nella tabella.

6. Ci interessa solo l'hypervisor che ospita la macchina virtuale corrente. Fare clic sul pulsante**+**del campo **Filtra per** e selezionare **nome hypervisor**.
7. Fare clic su **qualsiasi** e selezionare la variabile * this.host.name*. Fare clic sul pulsante di controllo per salvare il filtro.



8. La tabella mostra ora tutte le macchine virtuali ospitate dall'hypervisor della macchina virtuale corrente. Fare clic su **Save** (Salva).

Risultati

La tabella creata per questa pagina di risorse della macchina virtuale verrà visualizzata per qualsiasi pagina di risorse della macchina virtuale visualizzata. L'utilizzo della variabile * this.host.name* nel widget significa che

nella tabella verranno visualizzate solo le macchine virtuali di proprietà dell'hypervisor delle risorse correnti.

Bilanciamento delle risorse di rete

Per risolvere i problemi di bilanciamento, utilizzare le pagine delle risorse per individuare i problemi e identificare i volumi ad alta capacità sottoutilizzati.

Fasi

1. Aprire la dashboard delle risorse nel browser.
2. Nella mappa termica IOPS delle macchine virtuali, si nota il nome di una macchina virtuale in stampe molto grandi che spesso segnala problemi.
3. Fare clic sul nome della macchina virtuale per visualizzare la pagina delle risorse.
4. Verificare la presenza di messaggi di errore nel riepilogo.
5. Controllare i grafici delle performance e in particolare le principali risorse correlate per individuare eventuali volumi in conflitto.
6. Aggiungi volumi al grafico delle performance per confrontare i modelli di attività e visualizzare più pagine di risorse per altre risorse coinvolte nel problema.
7. Scorrere fino alla fine della pagina delle risorse per visualizzare gli elenchi di tutte le risorse associate alla macchina virtuale. Nota: Qualsiasi VMDK eseguito ad alta capacità. Questo è probabilmente la causa del conflitto.
8. Per risolvere il problema di bilanciamento, identificare una risorsa sottoutilizzata per ricevere il carico da una risorsa sovrautilizzata o rimuovere un'applicazione meno impegnativa dalla risorsa maggiormente utilizzata.

Analisi delle performance di rete

È possibile esaminare le performance del proprio ambiente di storage, identificare le risorse sottoutilizzate e sovrautilizzate e identificare i rischi prima che si trasformino in problemi.

Insight ti aiuta a risolvere o prevenire i problemi di performance e disponibilità che vengono rivelati attraverso i dati di storage raccolti.

Puoi utilizzare Insight per eseguire queste attività di gestione delle performance:

- Monitorare le performance nell'intero ambiente
- Identificare le risorse che influenzano le performance di altri dispositivi

L'importanza dei porti

Il server Insight Server e Data Warehouse (DWH) potrebbe richiedere la presenza di una serie di porte TCP per poter funzionare in modo affidabile. Alcune di queste porte vengono utilizzate solo per i processi associati all'adattatore localhost (127.0.0.1), ma sono comunque necessarie per il funzionamento affidabile dei servizi principali. Il numero di porte richieste è un superset delle porte utilizzate nella rete.

Porte server Insight

I server Insight possono avere firewall software installati. I "fori" da aprire sono quelli descritti di seguito.

Inbound HTTPS 443 - presupponendo che Insight WebUI sia in esecuzione su TCP 443, è necessario esporre questa funzionalità per consentire a tutti i seguenti utenti:

- Utenti di Insight di WebUI
- Unità di acquisizione remota che cercano di connettersi al server Insight
- Server OCI DWH con connettori per questo server Insight.
- Qualsiasi interazione programmatica con l'API REST Insight

Il nostro consiglio generale per chiunque desideri implementare il firewalling a livello di host del server Insight è consentire l'accesso HTTPS a tutti i blocchi IP della rete aziendale.

MySQL in entrata (TCP 3306). Questa porta deve essere esposta solo a qualsiasi server Insight DWH dotato di connettore

Sebbene Insight disponga di decine di data raccoglitori, tutti sono basati su sondaggi: Insight avvierà la comunicazione in uscita verso diversi dispositivi dalle sue unità di acquisizione (aus). Finché il firewall basato su host è "stateful" in modo da consentire il traffico di ritorno attraverso il firewall, i firewall basati su host su Insight Server non dovrebbero influire sull'acquisizione dei dati.

Porte Data Warehouse

Per i server Insight DWH:

Inbound HTTPS 443 - presupponendo che Insight WebUI sia in esecuzione su TCP 443, è necessario esporre questa funzionalità per consentire ai seguenti utenti:

- Utenti amministrativi Insight del portale di amministrazione DWH

Inbound HTTPS (TCP 9300) - interfaccia di reporting di Cognos. Se gli utenti interagiranno con l'interfaccia di reporting di Cognos, questa deve essere esposta in remoto.

Possiamo immaginare ambienti in cui il DWH potrebbe non essere esposto: Forse gli autori del report devono semplicemente stabilire connessioni RDP al server DWH e creare e pianificare report in tale ambiente, mentre tutti i report devono essere inviati tramite SMTP o scritti su un file system remoto.

MySQL in entrata (TCP 3306). Questa porta deve essere esposta solo se l'organizzazione dispone di integrazioni basate su MySQL con dati DWH, ovvero se si estraggono dati dai vari data mart DWH per l'acquisizione in altre applicazioni come CMDB, sistemi di chargeback e così via

Analisi delle performance lente del PC

Se si ricevono chiamate da utenti di rete che lamentano un funzionamento lento dei computer, è necessario analizzare le prestazioni degli host e identificare le risorse interessate.

Prima di iniziare

In questo esempio, il chiamante ha fornito il nome host.

Fasi

1. Aprire Insight nel browser.

2. Inserire il nome host nella casella **Cerca risorse** e fare clic sul nome host nei risultati della ricerca.

   Viene visualizzata la *pagina risorse* della risorsa.

3. Nella pagina delle risorse dell'host, esaminare i grafici delle prestazioni al centro della pagina. È possibile visualizzare diversi tipi di dati oltre alla latenza e agli IOPS generalmente preselezionati. Fare clic sulle caselle di controllo per altri tipi di dati, ad esempio throughput, memoria, CPU o throughput IP, a seconda del tipo di dispositivo.
4. Per visualizzare una descrizione di un punto su un grafico, posizionare il puntatore del mouse sul punto.
5. È inoltre possibile modificare l'intervallo di tempo con la selezione nella parte superiore della pagina in modo che sia compreso tra 3 ore e 7 giorni o tutti i dati disponibili.
6. Esaminare l'elenco delle risorse correlate **principali** per verificare se sono presenti altre risorse con lo stesso modello di attività della risorsa di base.

   La prima risorsa nell'elenco è sempre la risorsa di base.

   a. Fare clic su una percentuale collegata accanto a una risorsa correlata per vedere se il modello di attività correlato è per IOPS o CPU per la risorsa di base e un'altra risorsa.
   b. Fare clic sulla casella di controllo relativa a una risorsa correlata per aggiungere i dati ai grafici delle performance.
   c. Fare clic sul nome collegato della risorsa correlata per visualizzarne la pagina delle risorse.
7. Per una macchina virtuale, come in questo esempio, individuare il pool di storage nella sezione **Top Correlated Resources** (risorse correlate principali) e fare clic sul nome del pool di storage.

Analisi delle risorse correlate

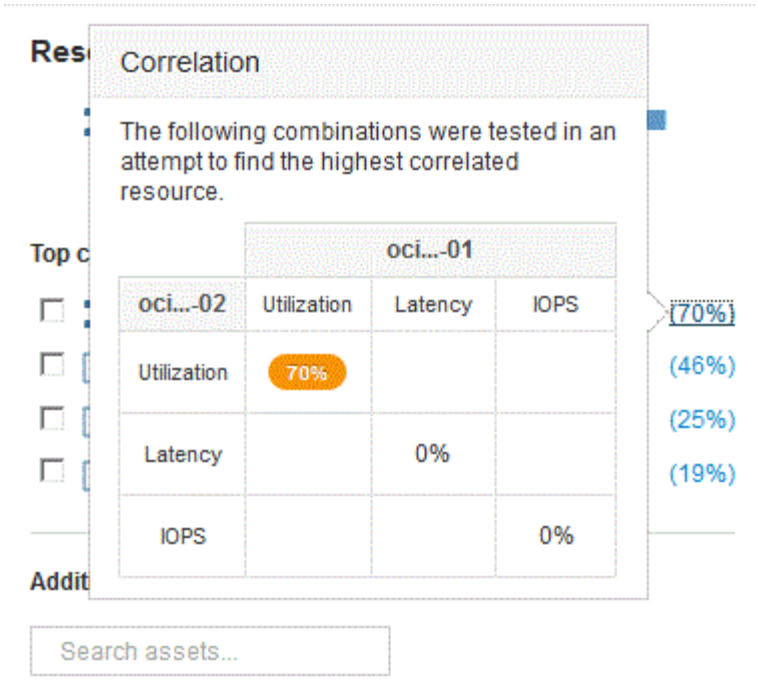
Quando si ricercano problemi di performance e si apre la *pagina delle risorse* per un dispositivo, utilizzare l'elenco delle risorse correlate principali per perfezionare i dati visualizzati nei grafici delle performance. Una risorsa con una percentuale elevata indica che la risorsa ha un'attività simile a quella della risorsa di base.

A proposito di questa attività

Si sta esaminando un problema di performance e si apre la pagina delle risorse di un dispositivo.

Fasi

1. Nell'elenco **Top Correlated Resources**, la prima risorsa è la risorsa di base. Le risorse correlate nell'elenco sono classificate in base alla percentuale di attività correlate al primo dispositivo. Fare clic sulla percentuale di correlazione collegata per visualizzare i dettagli. In questo esempio, la correlazione del 70% è in uso, quindi sia la risorsa di base che questa risorsa correlata hanno un utilizzo altrettanto elevato.



2. Per aggiungere una risorsa correlata ai grafici delle performance, selezionare la casella di controllo nell'elenco **Top Correlated Resources** (risorse correlate principali) per la risorsa che si desidera aggiungere. Per impostazione predefinita, ciascuna risorsa fornisce i dati totali disponibili, ma è possibile selezionare solo dati di lettura o solo dati di scrittura dal menu della casella di controllo.

   Ogni risorsa nei grafici ha un colore diverso, in modo da poter confrontare le misurazioni delle performance per ogni risorsa. Per le metriche di misurazione selezionate viene plottato solo il tipo di dati appropriato. Ad esempio, i dati della CPU non includono le metriche di lettura o scrittura, pertanto sono disponibili solo i dati totali.

3. Fare clic sul nome collegato della risorsa correlata per visualizzarne la pagina delle risorse.
4. Se non viene visualizzata una risorsa elencata nelle risorse correlate principali che si ritiene debba essere considerata nell'analisi, è possibile utilizzare la casella **Cerca risorse** per trovare tale risorsa.

Monitoraggio dell'ambiente Fibre Channel

Utilizzando le pagine delle risorse Fibre Channel di OnCommand, è possibile monitorare le performance e l'inventario dei fabric nel proprio ambiente ed essere consapevoli di eventuali modifiche che potrebbero causare problemi.

Pagine di risorse Fibre Channel

Le pagine delle risorse di Insight contengono informazioni riepilogative sulla risorsa, sulla sua topologia (il dispositivo e le sue connessioni), sui grafici delle performance e sulle tabelle delle risorse associate. È possibile utilizzare le pagine delle risorse relative a fabric, switch e porte per monitorare l'ambiente Fibre Channel. Particolarmente utile per la risoluzione di un problema Fibre Channel è il grafico delle performance per ogni risorsa di porta, che mostra il traffico per la porta principale contributore selezionata. Inoltre, in questo grafico è possibile visualizzare anche le metriche di credito buffer-to-buffer e gli errori di porta, con Insight che visualizza un grafico delle performance separato per ciascuna metrica.

Policy sulle performance per le metriche delle porte

Insight consente di creare policy sulle performance per monitorare la rete per rilevare diverse soglie e generare avvisi quando tali soglie vengono superate. È possibile creare criteri di performance per le porte in base alle metriche delle porte disponibili. Quando si verifica una violazione di una soglia, Insight la rileva e la segnala nella pagina delle risorse associata visualizzando un cerchio rosso continuo, un avviso via email, se configurato, e nella dashboard delle violazioni o in qualsiasi dashboard personalizzata che segnala le violazioni.

TTL (Time-to-live) e dati downsampled

A partire da OnCommand Insight 7.3, la conservazione dei dati o il time-to-live (TTL) è stato aumentato da 7 a 90 giorni. Poiché ciò significa che vengono elaborati molti più dati per grafici e tabelle e il potenziale di decine di migliaia di datapoint, i dati vengono sottoposti a downsampling prima di essere visualizzati.

Il downsampling fornisce un'approssimazione statistica dei dati nei grafici, offrendo una panoramica efficiente dei dati senza dover visualizzare ogni punto dati, mantenendo al contempo una visione accurata dei dati raccolti.

Perché è necessario eseguire il downsampling?

Insight 7.3 aumenta il time-to-live (TTL) dei dati fino a 90 giorni. Ciò significa un aumento della quantità di elaborazione necessaria per preparare i dati per la visualizzazione in grafici e grafici. Per consentire la visualizzazione rapida ed efficiente dei grafici, i dati vengono sottoposti a downsampling in modo da mantenere la forma generale di un grafico senza dover elaborare ogni singolo punto dati per quel grafico.

> Nessun dato effettivo viene perso durante il downsampling. È possibile scegliere di visualizzare i dati effettivi del grafico invece dei dati sottocampionati seguendo la procedura illustrata di seguito.

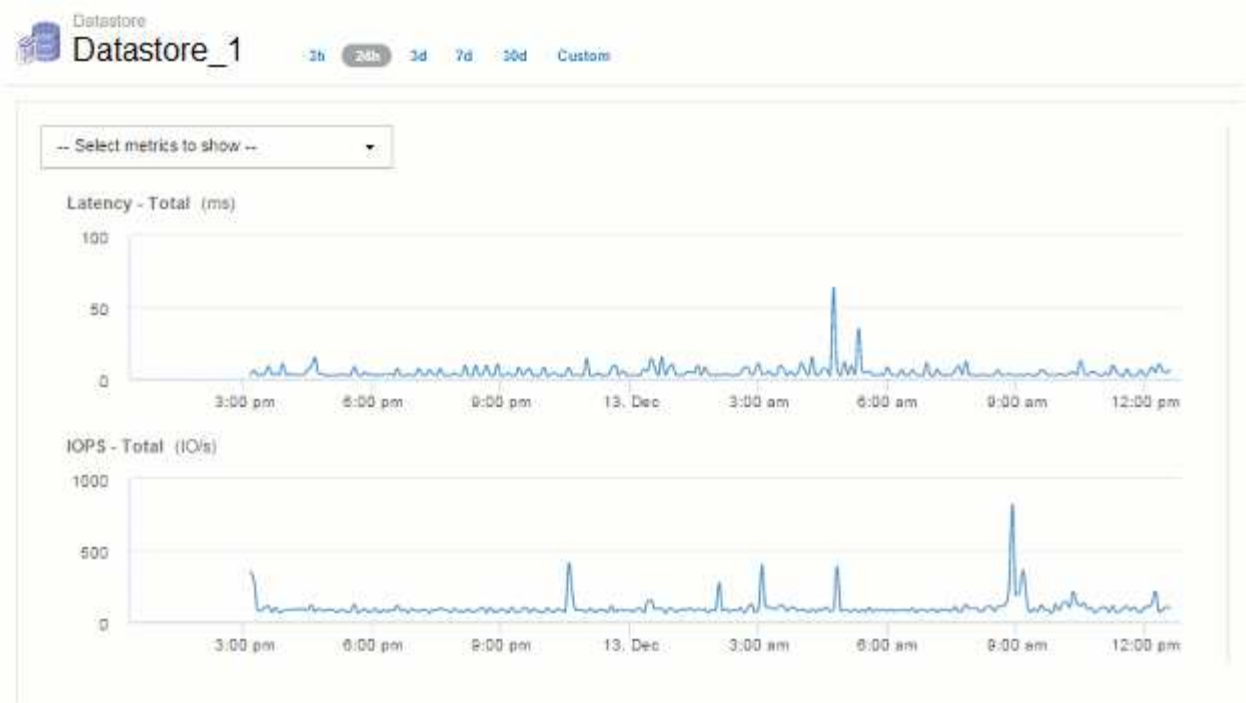
Come funziona il downsampling

I dati vengono sottoposti a downsampling nelle seguenti condizioni:

- Quando l'intervallo di tempo selezionato include almeno 7 giorni di dati, non si verifica alcun downsampling. I grafici visualizzano i dati effettivi.
- Quando l'intervallo di tempo selezionato include più di 7 giorni di dati ma meno di 1,000 punti dati, non si verifica alcun downsampling. I grafici visualizzano i dati effettivi.
- Quando l'intervallo di tempo selezionato include più di 7 giorni di dati e più di 1,000 punti dati, i dati vengono sottoposti a downsampling. I grafici visualizzano i dati approssimati.

I seguenti esempi mostrano il downsampling in azione. La prima illustrazione mostra i grafici di latenza e IOPS su una pagina di risorse Datastore per un periodo di 24 ore, come mostrato selezionando **24h** nel selettore di tempo della pagina delle risorse. È inoltre possibile visualizzare gli stessi dati selezionando **Custom** e impostando l'intervallo di tempo sullo stesso periodo di 24 ore.

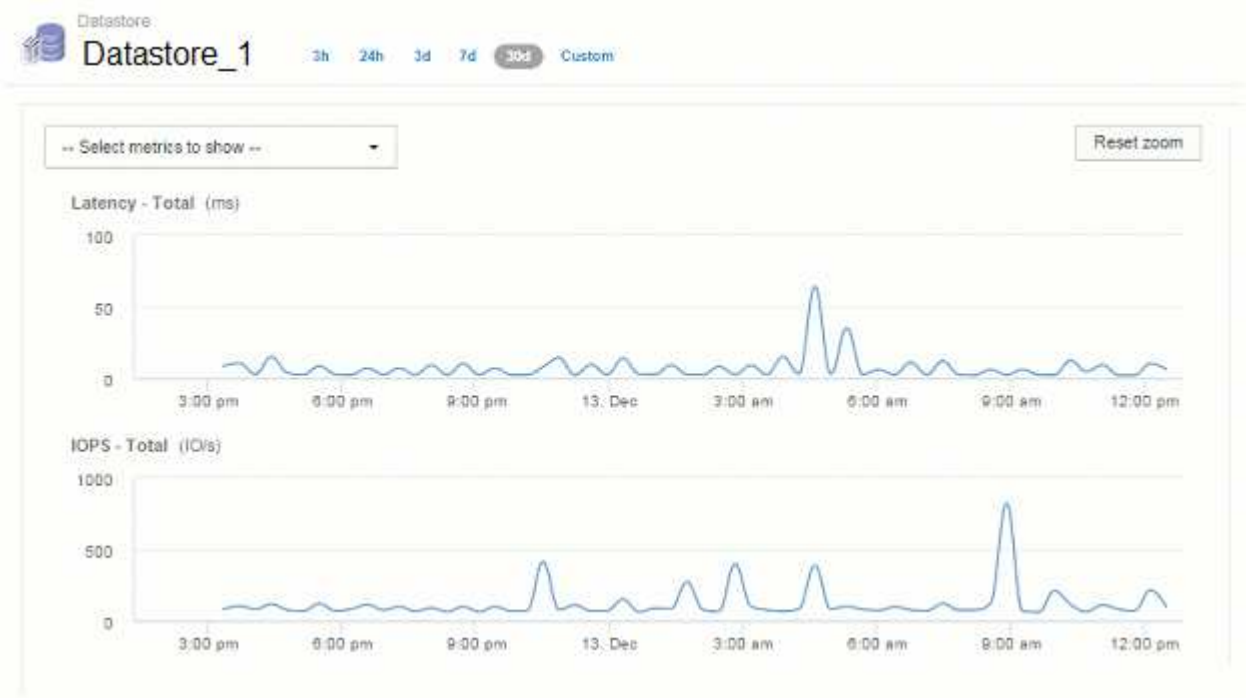
Poiché stiamo scegliendo un intervallo di tempo inferiore a 7 giorni e abbiamo meno di 1,000 punti dati da inserire nel grafico, i dati visualizzati sono dati effettivi. Non si verifica alcun downsampling.



Tuttavia, se si visualizzano i dati scegliendo **30d** nel selettore di tempo della pagina delle risorse, Oppure impostando un intervallo di tempo personalizzato di oltre 7 giorni (o nel caso in cui Insight abbia raccolto più di 1,000 campioni di dati per il periodo di tempo scelto), i dati vengono sottoposti a downsampling prima di essere visualizzati. Quando si esegue lo zoom avanti su un grafico sottocampionato, il display continua a mostrare i dati approssimati.

> Quando si esegue lo zoom avanti su una mappa con sottocampionatura, lo zoom è uno zoom digitale. Il display continua a visualizzare i dati approssimati.

La figura seguente mostra l'intervallo di tempo impostato su 30d, quindi il grafico viene ingrandito per visualizzare lo stesso periodo di 24 ore di cui sopra.



I grafici sottocampionati mostrano lo stesso periodo di 24 ore dei grafici "effettivi" di cui sopra, quindi le linee seguono la stessa forma generale, consentendo di individuare rapidamente picchi o valli interessanti nei dati delle performance.

> A causa del modo in cui i dati vengono approssimati per il downsampling, le linee del grafico potrebbero essere leggermente disattivate quando si confronta il downsampling con il dati effettivi, per consentire un migliore allineamento nei grafici. Tuttavia, la differenza è minima e non influisce sulla precisione complessiva dei dati visualizzati.

Violazioni sui grafici downsampled

Quando si visualizzano i grafici sottocampionati, tenere presente che le violazioni non vengono visualizzate. Per vedere le violazioni, è possibile eseguire una delle seguenti operazioni:

- Visualizzare i dati effettivi per quell'intervallo di tempo selezionando Custom (personalizzato) nel selettore di tempo della pagina asset e immettendo un intervallo di tempo inferiore a 7 giorni. Passare il mouse su ciascun punto rosso. La descrizione del comando mostra la violazione che si è verificata.
- Annotare l'intervallo di tempo e individuare le violazioni nella dashboard delle violazioni.

Eliminazione della cronologia dell'inventario

A partire dalla versione 7.3.2, Insight mantiene la cronologia delle modifiche dell'inventario (base) per 90 giorni. Le versioni precedenti di Insight conservavano tutta la cronologia delle modifiche dell'inventario dal momento dell'installazione. A seguito di un aggiornamento da una versione precedente di Insight, la cronologia dell'inventario precedente viene ridotta e mantenuta a 90 giorni.

Dopo aver eseguito l'aggiornamento alla versione corrente di OnCommand Insight, la cronologia viene aggiornata ai 90 giorni più recenti. Insight pota la storia in 30 giorni di pezzi che si verificano una volta al giorno, a partire dalla più vecchia, fino a 90 giorni di storia rimane. Quindi, la cronologia viene annullata ogni giorno, per mantenere solo 90 giorni' di cronologia delle modifiche dell'inventario.

Percorso NAS per macchine virtuali

OnCommand Insight 7.3 supporta i percorsi NAS per le macchine virtuali e le condivisioni di storage. Questi percorsi sono simili ai percorsi NAS per gli host alle condivisioni di storage. Quando l'indirizzo IP di una macchina virtuale è autorizzato ad accedere a una condivisione, viene creato un percorso NAS.

I percorsi NAS per le macchine virtuali vengono visualizzati nella landing page dei volumi interni. Questa pagina contiene un widget risorse di storage montate su guest che identifica i volumi interni a cui hanno accesso le macchine virtuali.

- I percorsi NAS vengono creati quando le macchine virtuali hanno accesso alle condivisioni back-end. Non viene riconosciuto se le macchine virtuali accedono alle condivisioni o meno.
- Il calcolo della correlazione si basa su latenze e IOPS e non include i casi in cui le macchine virtuali hanno percorsi NAS verso lo storage back-end.
- L'utente può eseguire query sulla condivisione in base all'indirizzo IP dell'iniziatore, ma non è supportata la query in base al percorso.

La tabella Compute Resources del volume interno ora visualizza anche le macchine virtuali con percorsi NAS. Per ogni macchina virtuale, CPU e memoria, vengono forniti dati relativi a utilizzo e performance.

Impatto del data warehouse

Le modifiche apportate al data warehouse dopo l'aggiornamento a OnCommand Insight 7.3 includono quanto segue:

- la tabella dwh_Inventory.nas_Logical viene rimossa dal data mart di inventario e sostituita con una vista.

  Tutti i report Insight 7.2.x contenenti la tabella dei percorsi NFS vengono conservati.

- La tabella dwh_Inventory.nas_cr_Logical viene aggiunta al data mart di inventario e include quanto segue:
  - Risorsa di calcolo
  - Volume interno
  - Storage
  - Condivisione NAS

Capacità come Time Series

Con OnCommand Insight 7.3.1, le informazioni sulla capacità vengono riportate e inserite come dati di serie temporali.

In precedenza, le informazioni sulla capacità acquisite dalle origini dati erano esclusivamente dati "point-in-time" (PIT), il che significa che non potevano essere utilizzate nei grafici come dati delle serie temporali. Ora, i valori di capacità per le risorse possono essere utilizzati come dati delle serie temporali nei seguenti modi:

- Grafico in tabelle, widget, viste avanzate e qualsiasi luogo in cui vengono visualizzati i dati delle serie temporali
- Applicato alle soglie di performance con violazioni utilizzando la semantica esistente
- Utilizzato nelle espressioni con altri contatori delle prestazioni, se appropriato

Si noti che se si esegue l'aggiornamento da una versione precedente di Insight, i valori di capacità DEI BOX precedenti utilizzati nelle query o nei filtri per i dashboard personalizzati verranno sostituiti con i dati di capacità delle serie temporali. Ciò potrebbe comportare piccole modifiche nel modo in cui i dati di capacità vengono riportati o filtrati rispetto ai dati equivalenti nelle versioni precedenti di Insight.