Documentazione OnCommand Insight

OnCommand Insight

NetApp
April 01, 2024

Sommario

Documentazione OnCommand Insight

OnCommand Insight è una singola soluzione per consentire la gestione e l'analisi delle risorse multi-vendor su più domini in reti, storage e server in ambienti fisici e virtuali. Insight può aiutarti a ottimizzare la tua infrastruttura attuale, consentendoti di dimensionare correttamente le operazioni per soddisfare le esigenze del business. Semplifica il processo di determinazione di cosa e quando acquistare. Inoltre, riduce i rischi durante complesse migrazioni tecnologiche, come ad esempio il passaggio a un cloud ibrido, identificando i carichi di lavoro candidati alla migrazione del cloud. Con Insight, puoi gestire l'infrastruttura IT come servizio end-to-end integrando le risorse nell'intera catena di erogazione dei servizi IT dell'azienda.

Note di rilascio

Note di rilascio

Le note di rilascio di OnCommand Insight sono disponibili al di fuori del Centro documentazione. Ti verrà richiesto di effettuare l'accesso utilizzando le credenziali del sito di supporto NetApp.

"Note sulla versione .PDF" (si apre in una nuova finestra)

Che cos’è OnCommand Insight?

Panoramica di OnCommand Insight

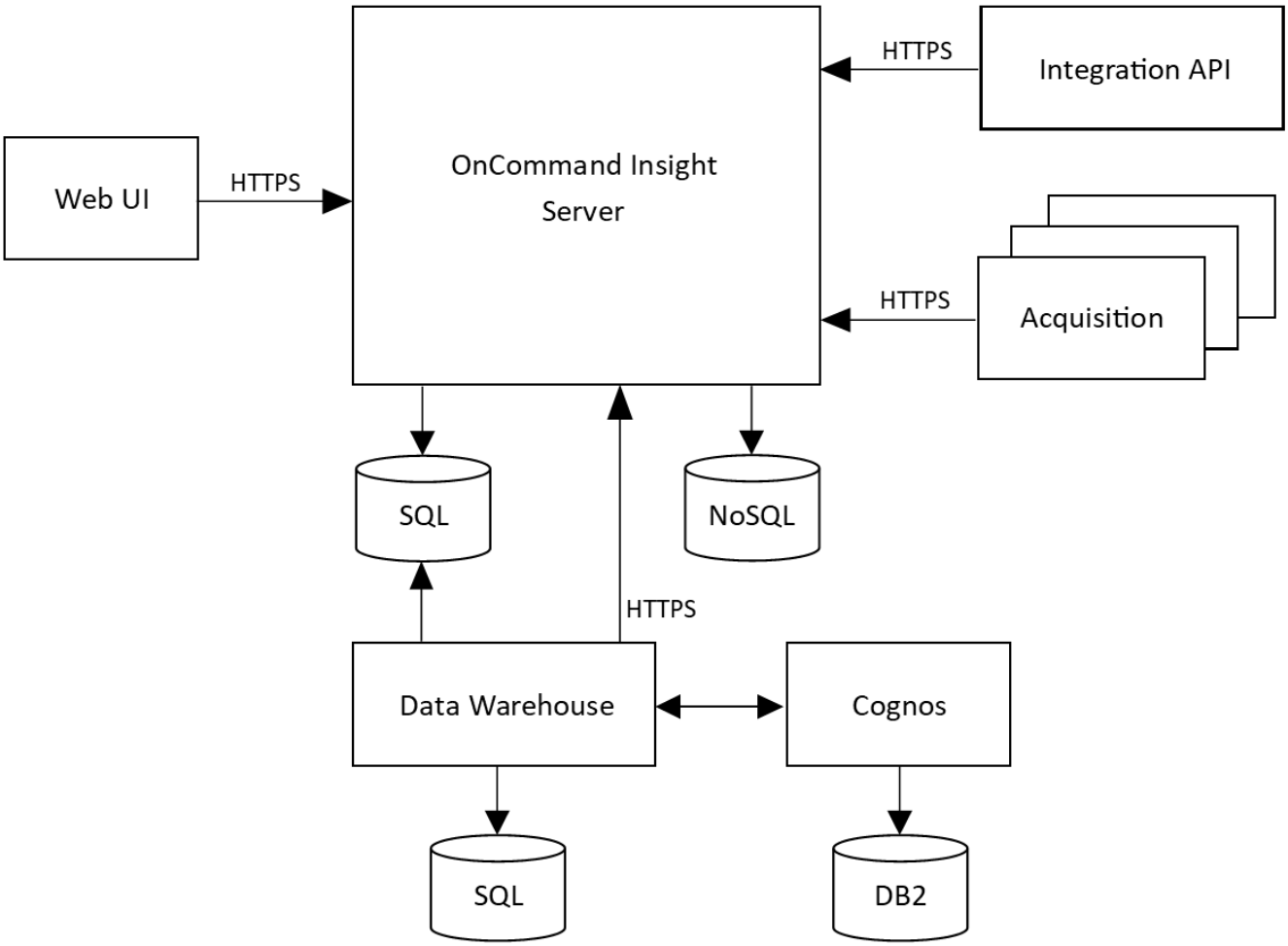
OnCommand Insight consente di semplificare la gestione operativa di ambienti IT virtuali e cloud ibridi e privati complessi. Insight è un’unica soluzione per consentire la gestione e l’analisi delle risorse multi-vendor su più domini in reti, storage e server in ambienti fisici e virtuali.

Insight può aiutarti a ottimizzare la tua infrastruttura attuale, consentendoti di dimensionare correttamente le operazioni per soddisfare le esigenze del business. Semplifica il processo di determinazione di cosa e quando acquistare. Inoltre, riduce i rischi durante complesse migrazioni tecnologiche, come ad esempio il passaggio a un cloud ibrido, identificando i carichi di lavoro candidati alla migrazione del cloud. Con Insight, puoi gestire l’infrastruttura IT come servizio end-to-end integrando le risorse nell’intera catena di erogazione dei servizi IT dell’azienda.

Architettura Insight

Un’installazione tipica di OnCommand Insight include acquisizione dei dati e data warehousing con report, tutti facilmente accessibili da un’interfaccia utente basata su web. Per ambienti più sicuri, l’acquisizione può essere eseguita tramite un’unità di acquisizione remota.

I componenti principali dell’architettura Insight sono illustrati nel seguente diagramma:



- **Server OnCommand Insight**

  Il server OnCommand Insight contiene i principali componenti di analisi e repository di dati. Il server sta continuamente creando una topologia end-to-end dell'ambiente, analizzando l'ambiente e generando avvisi quando viene rilevato un incidente o una violazione.

- **Acquisizione**

  Il motore di raccolta Insight si basa su una o più unità di acquisizione. Ogni server Insight contiene un'unità di acquisizione locale e può supportare unità di acquisizione remota. Ogni unità è un servizio in esecuzione sulla rete che accede (attraverso moduli denominati *origini dati*) e raccoglie i dati dai dispositivi nel data center. Le informazioni raccolte dalle unità di acquisizione vengono quindi inviate al server per l'analisi.

  Il motore di raccolta è progettato per essere altamente modulare e facilmente patchato.

- **API di integrazione**

  Un'API consente la raccolta di dati da agenti esterni. I dati di integrazione possono essere visualizzati nell'interfaccia utente Web utilizzando query e widget. Le dashboard possono contenere dati Insight "nativi" e dati di integrazione. È possibile applicare filtri, roll-up e raggruppamenti ai dati in queste dashboard.

- **Interfaccia utente Web**

  L'interfaccia utente basata su Web di HTML5 per Insight consente di configurare le origini dati e l'ambiente

di monitoraggio, inclusi criteri, soglie e avvisi. Quindi, utilizza la dashboard UIAsset Web e le pagine delle risorse per identificare e ricercare potenziali problemi. Puoi creare dashboard personalizzati con una vasta gamma di widget, ciascuno dei quali offre una flessibilità estesa nella visualizzazione, analisi e inserimento dei dati.

- **Data Warehouse**

  Il data warehouse di OnCommand Insight è un repository centralizzato che memorizza i dati provenienti da più server Insight e li trasforma in un modello di dati comune e multidimensionale per le query e l'analisi.

  Il data warehouse di OnCommand Insight consente di accedere a un database aperto costituito da diversi data mart che consentono di generare report personalizzati sulla capacità e sulle performance, come report di chargeback, report sui trend con dati storici, analisi dei consumi e report di previsione.

  Il Data Warehouse consolida e prepara i dati per la creazione di report per una o più installazioni di Insight. I dati includono cronologia, trend, inventario, chargeback, show back e presentazioni di dati per supportare la pianificazione a lungo termine dell'infrastruttura del data center.

- **Cognos**

  Cognos è il motore di reporting per Insight, uno strumento di business intelligence IBM che consente di visualizzare report predefiniti o di creare report personalizzati. Il reporting di Insight genera report dai dati del Data Warehouse.

Come Insight viene utilizzato da amministratori, manager e pianificatori

OnCommand Insight fornisce informazioni essenziali per amministratori dello storage, manager e architetti dello storage per l'esecuzione di analisi e troubleshooting.

Gli amministratori dello storage esperti utilizzano OnCommand Insight insieme alle proprie conoscenze in materia di storage di rete per eseguire le seguenti attività tipiche:

- Gestire l'ambiente SAN e NAS.
- Collaborare con i tecnici SAN per risolvere i problemi di rete.
- Valutare, testare e integrare nuove tecnologie di storage nell'ambiente.
- Risolvere problemi di performance, avvisi, violazioni di policy, violazioni e vulnerabilità.

I manager e i pianificatori di rete utilizzano OnCommand Insight per eseguire le seguenti attività di business:

- Pianificazione della capacità
- Sviluppo di budget e tempistiche dei progetti.
- Valuta e rivedi i piani di progetto per soddisfare le mutevoli esigenze dei progetti.
- Gestire la pianificazione e le spese del progetto.
- Acquistare hardware e software.
- Fornire report di business per la gestione della capacità, la fatturazione di riaccredito, il dimensionamento corretto e gli accordi sui livelli di servizio.

Installazione per Linux

Prerequisiti per l'installazione

Prima di installare OnCommand Insight, è necessario scaricare la versione corrente del software, acquistare la licenza appropriata e configurare l'ambiente.

Prima di installare OnCommand Insight, assicurarsi di disporre di quanto segue:

- File del software OnCommand Insight nel pacchetto di installazione scaricato per la versione corrente
- Licenza per il funzionamento della versione di OnCommand Insight scaricata
- L'ambiente hardware e software minimo

  Il prodotto corrente potrebbe consumare risorse hardware aggiuntive (a causa delle funzionalità avanzate del prodotto OnCommand Insight) che non erano utilizzate con le versioni precedenti del prodotto OnCommand Insight.

- Un piano di implementazione che include le configurazioni hardware e di rete per il server OnCommand Insight, il data warehouse e il reporting e le unità di acquisizione remota.

Pianificazione dell'implementazione

Per garantire una corretta implementazione, è necessario prendere in considerazione alcuni elementi di sistema prima di installare OnCommand Insight.

A proposito di questa attività

La pianificazione dell'implementazione di Insight include la valutazione di questi elementi di sistema:

- Architettura Insight
- I componenti di rete da monitorare
- Prerequisiti per l'installazione di Insight e requisiti del server
- Requisiti del browser Web Insight

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". .

Identificazione dei dispositivi e pianificazione dell'origine dei dati

Nell'ambito della pianificazione dell'implementazione, è necessario raccogliere informazioni sui dispositivi presenti nell'ambiente.

Sono necessari i seguenti software, connettività e informazioni su ciascun dispositivo nell'ambiente:

- Indirizzo IP o nome host risolvibile dal server OCI
- Nome di accesso e password
- Tipo di accesso al dispositivo, ad esempio controller e stazione di gestione

> L'accesso in sola lettura sarà sufficiente per la maggior parte dei dispositivi, ma alcuni richiedono autorizzazioni di amministratore.

- Connettività della porta al dispositivo in base ai requisiti della porta di origine dati
- Per gli switch, stringa di comunità di sola lettura SNMP (ID utente o password per consentire l'accesso agli switch)
- Qualsiasi software di terze parti richiesto sul dispositivo, ad esempio Solutions Enabler.
- Per ulteriori informazioni sui requisiti e sulle autorizzazioni dell'origine dati, consultare la sezione "riferimento all'origine dati specifico del vendor" nella Guida dell'interfaccia utente Web o nella *Guida alla configurazione e all'amministrazione di OnCommand Insight*.

Traffico di rete generato da OnCommand Insight

Il traffico di rete generato da OnCommand Insight, la quantità di dati elaborati che attraversano la rete e il carico che OnCommand Insight carica sui dispositivi variano in base a diversi fattori.

Il traffico, i dati e il carico differiscono tra gli ambienti in base ai seguenti fattori:

- I dati raw
- Configurazione dei dispositivi
- Topologia di implementazione di OnCommand Insight
- Intervalli di polling diversi per l'origine dati di inventario e performance, che possono essere ridotti per consentire il rilevamento di dispositivi lenti o la conservazione della larghezza di banda

I dati di configurazione raw raccolti da OnCommand Insight possono variare in modo significativo.

Nell'esempio seguente viene illustrato come i dati di configurazione possono variare e come il traffico, i dati e il carico sono influenzati da molti fattori di configurazione. Ad esempio, potrebbero essere presenti due array con 1,000 dischi ciascuno:

- Array 1: Dispone di 1,000 dischi SATA di dimensioni pari a 1 TB. Tutti i 1,000 dischi si trovano in un unico pool di storage e sono presenti 1,000 LUN, tutte presentate (mappate e mascherate) agli stessi 32 nodi in un cluster ESX.
- Array 2: Dispone di 400 dischi dati da 2 TB, dischi FC da 560 600 GB e 40 SSD. Esistono 3 pool di storage, ma 320 dischi FC vengono utilizzati nei gruppi RAID tradizionali. Le LUN scavate nei gruppi RAID utilizzano un tipo di mascheramento tradizionale (symmaskdb), mentre le LUN basate su pool con thin provisioning utilizzano un tipo di mascheramento più recente (symaccess). Sono disponibili 600 LUN per

150 host diversi. Sono disponibili 200 BCVs (volumi di replica a blocchi completi di 200 delle 600 LUN). Esistono anche 200 volumi R2, volumi di replica remoti di volumi che esistono su un array in un sito diverso.

Ciascuno di questi array dispone di 1,000 dischi e 1,000 volumi logici. Potrebbero essere fisicamente identici nella quantità di spazio rack consumata nel data center e potrebbero anche eseguire lo stesso firmware, ma il secondo array è molto più complesso nella sua configurazione rispetto al primo array.

Disinstallazione di MariaDB

È necessario disinstallare MariaDB sui server Insight o Data Warehouse prima di installare OnCommand Insight o Data Warehouse; in caso contrario, non è possibile procedere con l'installazione. MySQL non è compatibile con MariaDB. Se si tenta di eseguire un'installazione su uno dei server senza rimuovere MariaDB, l'installazione termina con un messaggio di errore che indica di disinstallare MariaDB.

Prima di iniziare

È necessario disporre dei privilegi sudo.

Fasi

1. Accedere al server Insight.
2. Ottenere un elenco dei componenti MariaDB:

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

3. Digitare quanto segue per ogni componente MariaDB installato sul server:

   ```
   yum remove component_name
   ```

Requisiti di Insight Server

Si consiglia di utilizzare un server dedicato. Non installare Insight su un server in cui sono installate altre applicazioni. Sono supportati server fisici e virtuali, a condizione che i requisiti del prodotto siano soddisfatti.

Per installare il software del server OnCommand Insight, è necessario disporre delle autorizzazioni sudo.

Alcuni componenti Insight potrebbero richiedere pacchetti dipendenti durante l'installazione. Assicurarsi che il repository YUM sia accessibile prima di installare Insight.

> Il dimensionamento per OnCommand Insight prevede diverse dipendenze, come tipo e dimensione dell'origine dati, numero di risorse nell'ambiente, intervalli di polling e altro ancora. I seguenti esempi di dimensionamento sono solo linee guida e rappresentano alcuni degli ambienti in cui Insight è stato testato. La modifica di questi o altri fattori nell'ambiente può modificare i requisiti di dimensionamento di Insight. Queste linee guida includono spazio su disco per un massimo di 90 giorni di dati di archiviazione delle performance.

Prima di installare o aggiornare Insight, si consiglia di contattare il Sales Engineer per ottenere informazioni dettagliate sul dimensionamento.

Esempi:

Fattori ambientali:	Spazio su disco, CPU e memoria testati:
80 volumi di storage 4,000 VM 4,000 porte switch	250 GB di spazio su disco 8 core 32 GB DI RAM
160 unità di storage 40.000 volumi 8,000 VM 8,000 porte switch	1 TB di spazio su disco 12 core 48 GB DI RAM

Requisiti:

Componente	Obbligatorio
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti sistemi, che non esegue altro software a livello di applicazione: • Red Hat Enterprise Linux 7,3, 7,4, 7,5, 7,6, 7,7, 7,8, 7,9, 8,1, 8,2, 8,3, 8,4, 8,5, 8,8, 9,2 • CentOS 7,2, 7,5, 7,6, 7,7, 7,8, 7,9, CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,5, 7,6, 7,7, 7,8, 7,9 8,1, 8,2, 8,3, 8,4, 8,5, 8,8 Una versione con licenza garantisce che le dipendenze richieste dall'installazione vengano risolte automaticamente dal sistema operativo. È necessario disinstallare MariaDB prima di installare Insight. La disinstallazione di MariaDB rimuove anche Postfix Mail Transport Agent. Si consiglia di utilizzare un server dedicato.
Macchina virtuale (VM)	Questo componente può essere eseguito in un ambiente virtuale, a condizione che le risorse di CPU e memoria per l'istanza siano riservate.
Memoria e CPU	24 - 256 GB DI RAM 8 - 32 core

Spazio su disco disponibile	100 GB - 3 TB di spazio su disco per l'installazione 50 GB - 1 TB di spazio su disco per l'archiviazione delle performance Per un ambiente da 500 GB di esempio, si consigliano i seguenti guasti alle partizioni: • Directory /opt — 50 GB • Directory /var/log — 100 GB • Directory /var/lib — 350 GB Si tratta di una Best practice da montare `/opt` e. `/var` su dischi separati dal file system root (`/`). I dischi SSD sono consigliati per lo spazio di installazione Insight.
Rete	Connessione Ethernet e porte: • Connessione Ethernet a 100 Mbps o 1 Gbps con indirizzo IP dedicato (statico) e connettività IP a tutti i componenti della SAN, inclusi i dispositivi FC e le unità di acquisizione remota. • I requisiti delle porte per il processo del server OnCommand Insight sono 80, 443, 1090 - 1100, 3873, 8083, da 4444 a 4446, 5445, 5455, da 4712 a 4714, 5500, e 5501. • I requisiti delle porte per il processo di acquisizione sono 12123 e 5679. • Il requisito di porta per MySQL è 3306. • I requisiti delle porte per Elasticsearch sono 9200 e 9310 Le porte 443 e 3306 richiedono l'accesso esterno attraverso qualsiasi firewall presente.
Permessi	Le autorizzazioni sudo sono richieste sul server OnCommand Insight. Se una delle seguenti cartelle è un collegamento simbolico, assicurarsi che le directory di destinazione dispongano dei permessi '755'. • /opt/netapp • /var/lib/netapp • /var/log/netapp

Connettività remota	Connettività Internet per consentire l'accesso a WebEx o una connessione desktop remota per facilitare l'installazione e il supporto post-installazione.
Accessibilità	È richiesto l'accesso HTTPS.
Server HTTP o HTTPS	I server HTTP Apache o altri server HTTPS non devono competere per le stesse porte (443) del server OnCommand Insight e non devono avviarsi automaticamente. Se devono ascoltare la porta 443, è necessario configurare il server OnCommand Insight in modo che utilizzi altre porte.

Requisiti del server Data Warehouse

Il server Data Warehouse deve essere eseguito su un computer compatibile con i requisiti hardware e software stabiliti. Assicurarsi che il server Web Apache o il software di reporting non siano già installati su questa macchina.

> Il dimensionamento per OnCommand Insight prevede più dipendenze, ad esempio il numero di risorse nell'ambiente, la quantità di dati storici conservati e molto altro ancora. I seguenti esempi di dimensionamento del data warehouse sono solo linee guida e rappresentano alcuni degli ambienti in cui Insight è stato testato. La modifica di questi o altri fattori nell'ambiente può modificare i requisiti di dimensionamento di Insight.

Prima di installare o aggiornare Insight, si consiglia di contattare il Sales Engineer per ottenere informazioni dettagliate sul dimensionamento.

Esempi:

Fattori ambientali:	Spazio su disco, CPU e memoria testati:
18 storage array3,400 VM 4,500 porte switch	Disco rigido da 200 GB 8 core 32 GB DI RAM
110 array di storage 11,500 VM 14,500 porte switch	Disco rigido da 300 GB 8 core 48 GB DI RAM

Requisiti:

Componente	Obbligatorio

Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti sistemi, che non esegue altro software a livello di applicazione: • Red Hat Enterprise Linux 7,3, 7,4, 7,5, 7,6, 7,7, 7,8, 7,9, 8,1, 8,2, 8,3, 8,4, 8,5, 8,8, 9,2 • CentOS 7,2, 7,5, 7,6, 7,7, 7,8, 7,9, CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,5, 7,6, 7,7, 7,8, 7,9 8,1, 8,2, 8,3, 8,4, 8,5, 8,8
Macchina virtuale (VM)	Questo componente può essere eseguito in un ambiente virtuale, a condizione che le risorse di CPU e memoria per l'istanza siano riservate.
CPU	8 - 40 core CPU
Memoria	32 GB - 2 TB DI RAM
Spazio su disco disponibile	200 GB - 512 GB di spazio su disco nel sistema devono essere presenti almeno 50 GB di spazio libero su disco `/var/lib` E 25 GB di spazio libero su disco in `/opt` e. `/var/log` partizioni.
Rete	• Connessione Ethernet a 100 Mbps o 1 Gbps • Indirizzo IP statico • Per il processo del server DWH OnCommand Insight, porte 80, 443, 1098, 1099, 3873, 8083 e da 4444 a 4446 • Per MySQL, porta 3306

Requisiti del server Remote Acquisition Unit

È necessario installare un'unità di acquisizione remota (RAU) per acquisire informazioni da dispositivi SAN protetti da firewall, siti remoti, reti private o in segmenti di rete diversi. Prima di installare la RAU, assicurarsi che l'ambiente soddisfi i requisiti di sistema operativo RAU, CPU, memoria e spazio su disco.

Componente	Requisito

Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti sistemi, che non esegue altro software a livello di applicazione: • Red Hat Enterprise Linux 7,3, 7,4, 7,5, 7,6, 7,7, 7,8, 7,9, 8,1, 8,2, 8,3, 8,4, 8,5, 8,8, 9,2 • CentOS 7,2, 7,5, 7,6, 7,7, 7,8, 7,9, CentOS 8 Stream, CentOS 9 Stream • Oracle Enterprise Linux 7,5, 7,6, 7,7, 7,8, 7,9 8,1, 8,2, 8,3, 8,4, 8,5, 8,8 Si consiglia di utilizzare un server dedicato.
CPU	4 core CPU
Memoria	16 GB DI RAM
Spazio su disco disponibile	40 GB
Rete	Connessione Ethernet a 100 Mbps/1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi FC e porta richiesta al server OnCommand Insight (80 o 443).
Permessi	Sudo permessi sul server RAU

Browser supportati da OnCommand Insight

L'interfaccia utente di OnCommand Insightweb basata su browser può funzionare con diversi browser.

Insight supporta versioni non beta più recenti dei seguenti browser:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Per un elenco completo delle versioni del browser idonee per OnCommand Insight, consultare la "Tool di matrice di interoperabilità NetApp".

Istruzioni di installazione di Insight

L'installazione richiede l'installazione di diversi componenti OnCommand Insight, Insight Server e Data Warehouse.

L'installazione include le seguenti attività principali:

- Download del programma di installazione di OnCommand Insight

- Installazione del server OnCommand Insight
- Installazione delle licenze
- Se si desidera, installare DWH e Reporting (deve essere installato su una macchina virtuale o su una macchina virtuale separata. La creazione di report richiede Microsoft Windows).
- Facoltativamente, l'installazione di un'unità di acquisizione remota (RAU), che acquisisce informazioni dalle risorse del dispositivo che risiedono dietro un firewall, si trovano in un sito remoto o si trovano in una rete privata

Dopo l'installazione, è necessario configurare Insight per acquisire informazioni sull'ambiente. Le attività richieste sono descritte nella *Guida alla configurazione e all'amministrazione di OnCommand Insight*.

Download del programma di installazione di OnCommand Insight

È possibile scaricare il programma di installazione di OnCommand Insight dal sito del supporto NetApp.

Prima di iniziare

È necessario disporre di un accesso al sito di supporto NetApp all'indirizzo "mysupport.netapp.com".

Inoltre, è necessario disporre di un'utility di decompressione con la quale aprire l'installazione `.ZIP` file.

Fasi

1. Accedere al server su cui si desidera installare OnCommand Insight.
2. Scaricare il file di installazione dal sito del supporto NetApp.

Installazione del server OnCommand Insight

Il server OnCommand Insight viene installato utilizzando la riga di comando.

Prima di iniziare

È necessario aver completato tutti i prerequisiti di installazione.

Fasi

1. Accedere al server Insight utilizzando un account con privilegi sudo.
2. Accedere alla directory del server in cui si trovano i file di installazione e digitare il seguente comando:

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

   Verificare il numero di versione del file di installazione; il numero di versione potrebbe essere diverso da quello visualizzato nel comando.

3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh`:

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

4. Eseguire lo script di installazione:

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

5. Leggere il Contratto di licenza, accettarlo e seguire le istruzioni.
6. Se si utilizza il modello di licenza Insight Consumption, è necessario abilitare l'invio di informazioni sull'utilizzo a NetApp. Invio `Y` a questo prompt.

Risultati

Dopo aver risposto a tutte le richieste, l'installazione inizia e richiede circa 10 minuti, a seconda delle applicazioni installate.

Installazione del data warehouse di OnCommand Insight

L'installazione è autonoma e include gli elementi necessari per eseguire e utilizzare il data warehouse di OnCommand Insight (DWH).

Prima di iniziare

È necessario aver completato tutti i prerequisiti di installazione.

A proposito di questa attività

Data Warehouse dispone di funzionalità di reporting di Cognos. Se si installa Insight su un server Linux, è tuttavia possibile utilizzare queste funzionalità solo se si installa Data Warehouse su un server Windows. Per informazioni sull'installazione del data warehouse su Windows e sulle funzionalità di reporting di Cognos, fare riferimento alla *Guida all'installazione di OnCommand Insight per Microsoft Windows*.

Fasi

1. Accedere al server Data Warehouse utilizzando un account con privilegi sudo.
2. Accedere alla directory del server in cui si trovano i file di installazione e digitare il seguente comando:

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

   Verificare il numero di versione del file di installazione; il numero di versione potrebbe essere diverso da quello visualizzato nel comando.

3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh` prima di iniziare l'installazione:

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

4. Eseguire lo script di installazione:

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

5. Leggere il Contratto di licenza, accettarlo e seguire le istruzioni.

Risultati

Dopo aver risposto a tutte le richieste, l'installazione inizia e richiede circa 10 minuti, a seconda delle applicazioni installate.

Installazione di un'unità di acquisizione remota

È possibile installare una o più unità di acquisizione remota (RAUS) nel proprio ambiente OnCommand Insight. Le unità di acquisizione vengono eseguite nella rete che accede (tramite moduli denominati data *sources*) e raccolgono i dati da diversi dispositivi nel data center.

Prima di iniziare

È necessario aver completato tutti i prerequisiti di installazione.

Almeno una porta deve essere aperta e disponibile tra il server RAU e il server OnCommand Insight per inoltrare le informazioni sulle modifiche al server. In caso di dubbi, convalidarlo aprendo un browser Web sul computer RAU e indirizzandolo al server OnCommand Insight:

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

La porta di acquisizione predefinita è 443, ma potrebbe essere cambiata durante l'installazione del server. Se la connessione viene stabilita correttamente, viene visualizzata una pagina di risposta OnCommand Insight che indica una porta aperta e disponibile tra RAU e server OnCommand Insight.

Per gli ambienti che utilizzano Network Address Translation o Port Address Translation (NAT/PAT: I.e, qualsiasi conversione di indirizzi IP), Insight supporta solo l'inserimento di una RAU tra NAT e il dispositivo.

- Supportato: Dispositivo OnCommand Insight /→ NAT /→ RAU /→
- Non supportato: Dispositivo OnCommand Insight /→ RAU /→ NAT /→

Fasi

1. Accedere al server RAU utilizzando un account con privilegi sudo.
2. Accedere alla directory del server in cui si trovano i file di installazione e digitare il seguente comando:

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

3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh`:

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

4. Eseguire lo script di installazione:

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

5. Leggere il Contratto di licenza, accettarlo e seguire le istruzioni.

   Dopo aver risposto a tutte le richieste, l'installazione inizia e richiede circa 10 minuti, a seconda delle

applicazioni installate.

Convalida dell'installazione dell'unità di acquisizione remota

Per convalidare l'installazione corretta dell'unità di acquisizione remota, è possibile visualizzare lo stato delle unità di acquisizione remota collegate al server.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su *Acquisition Units (unità di acquisizione)
3. Verificare che la nuova unità di acquisizione remota sia stata registrata correttamente e che abbia uno stato di connessione.

   Se lo stato non è connesso, provare a riavviare il servizio. Accedere al sistema unità di acquisizione remota ed eseguire il comando seguente:

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

   Se il problema persiste, contattare l'assistenza tecnica.

Verifica dell'installazione

Una volta completata l'installazione, la directory di installazione si trova in `/opt/netapp/oci`. È possibile aprire Insight in un browser supportato per verificare l'installazione. È possibile controllare anche i file di log di Insight.

Quando si apre Insight per la prima volta, viene visualizzata la pagina di configurazione della licenza. Dopo aver inserito le informazioni sulla licenza, è necessario configurare le origini dati. Consultare la *Guida alla configurazione e all'amministrazione di OnCommand Insight* per informazioni sull'immissione delle definizioni delle origini dati e sull'impostazione degli utenti e delle notifiche di Insight.

In caso di problemi di installazione, contattare il supporto tecnico e fornire le informazioni richieste.

Verifica dell'installazione dei nuovi componenti Insight

Dopo l'installazione, verificare l'esistenza dei nuovi componenti sul server.

Fasi

1. Per visualizzare un elenco dei servizi attualmente operativi sul server a cui si è connessi, digitare:

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

2. A seconda del server a cui hai effettuato l'accesso, controlla i seguenti servizi Insight nell'elenco e assicurati che abbiano lo stato "running".
   - Server Insight: Wildfly, acquisizione, mysql, elasticsearch
   - Server Data Warehouse: Wildfly, mysql

- Remote Acquisition Server (Server di acquisizione remoto): Acquisizione

Risultati

Se questi componenti non sono elencati, contattare il supporto tecnico.

Registri Insight

Insight fornisce molti file di log per facilitare la ricerca e la risoluzione dei problemi. I registri disponibili sono elencati nella directory dei registri. È possibile utilizzare uno strumento per il monitoraggio dei log, ad esempio BareTail, per visualizzare tutti i log contemporaneamente.

I file di log si trovano in `/var/log/netapp/oci/wildfly/` directory. I registri di acquisizione si trovano in `/var/log/netapp/oci/acq` directory. I file di dati si trovano in `/var/lib/netapp/oci`.

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:

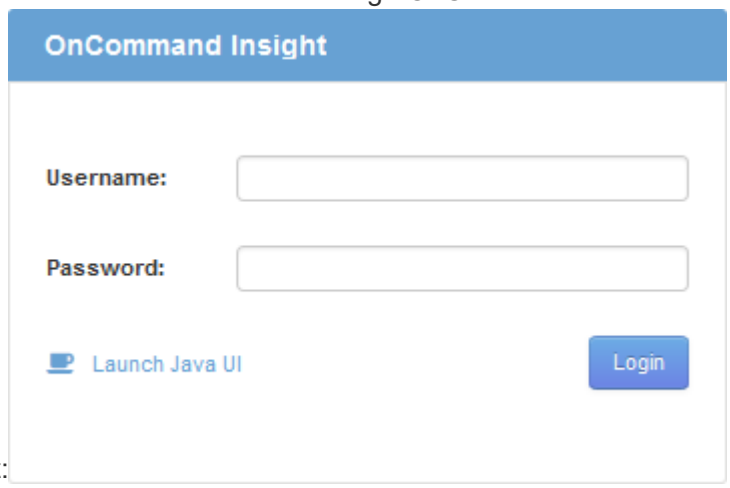
     ```
     https://fqdn
     ```

   - 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)

Risoluzione dei problemi di installazione

Le installazioni di OnCommand Insight vengono generalmente gestite attraverso le procedure guidate di installazione. Tuttavia, i clienti potrebbero riscontrare problemi durante gli aggiornamenti o conflitti dovuti agli ambienti informatici.

Assicurarsi inoltre di installare tutte le licenze OnCommand Insight necessarie per l'installazione del software.

Licenze mancanti

Per diverse funzionalità di OnCommand Insight sono necessarie licenze diverse. Le informazioni visualizzate in OnCommand Insight sono controllate dalle licenze installate. Fare riferimento alla sezione delle licenze OnCommand Insight per informazioni sulle funzionalità controllate da ciascuna licenza.

Fare riferimento alla sezione delle licenze OnCommand Insight per informazioni sulle funzionalità controllate da ciascuna licenza.

Invio di una richiesta di supporto tecnico online

In caso di problemi con l'installazione di Insight, in qualità di cliente registrato, puoi inviare una richiesta di supporto tecnico online.

Prima di iniziare

Utilizzando l'indirizzo e-mail aziendale, è necessario registrarsi come cliente del supporto per ottenere servizi di supporto online. La registrazione viene eseguita tramite il sito di supporto (http://support.netapp.com).

A proposito di questa attività

Per aiutare il supporto clienti a risolvere il problema di installazione, è necessario raccogliere il maggior numero possibile di informazioni, tra cui:

- Numero di serie di Insight
- Descrizione del problema
- Tutti i file di log Insight
- Cattura dello schermo di eventuali messaggi di errore

Fasi

1. Creare un `.zip` file delle informazioni raccolte per creare un pacchetto di risoluzione dei problemi.
2. Accedere al sito di supporto all'indirizzo "mysupport.netapp.com" E selezionare **Assistenza tecnica**.
3. Fare clic su **Apri un caso**.
4. Seguire le istruzioni del pacchetto di dati.

Al termine

Per seguire la richiesta, puoi utilizzare **verifica stato caso** nella pagina Assistenza tecnica.

Aggiornamento di Insight

Quando è disponibile una nuova versione di OnCommand Insight, è possibile eseguire l'aggiornamento per sfruttare le nuove funzionalità e risolvere i problemi. È necessario aggiornare il server Insight e il data warehouse (DWH) separatamente.

> Non memorizzare alcun backup automatico o manuale nelle directory di installazione di Insight, perché l'intera cartella di installazione viene sovrascritta durante il processo di aggiornamento. Se sono stati memorizzati file di backup in una di queste directory, è necessario spostare i backup in una posizione diversa prima di eseguire qualsiasi processo di aggiornamento o disinstallazione.

Le versioni più recenti di Insight hanno maggiori requisiti di spazio su disco, memoria e CPU. Prima di eseguire l'aggiornamento alla versione più recente di Insight, esaminare i requisiti di installazione. Prima di installare o aggiornare Insight, si consiglia di contattare il Sales Engineer per ottenere informazioni dettagliate sul dimensionamento.

È consigliabile eseguire un backup di sicurezza e un backup del database prima di aggiornare il software Insight.

Aggiornamento di Insight alla versione 7.3.12 o successiva - Linux

Prima di eseguire l'aggiornamento da OnCommand Insight 7.3.10 - 7.3.11 alla versione 7.3.12 o successiva, è necessario eseguire lo strumento di migrazione dei dati OCI.

Sfondo

OnCommand Insight versione 7.3.12 e successive utilizzano software sottostante che potrebbero essere incompatibili con le versioni precedenti. Le versioni 7.3.12 e successive di Insight includono un **Data Migration**

Tool per l'aggiornamento.

> Le versioni di OnCommand Insight 7.3.9 e precedenti non sono più supportate. Se si utilizza una di queste versioni, *è necessario* eseguire l'aggiornamento a Insight versione 7.3.10 o successiva (si consiglia vivamente la versione 7.3.11) prima di eseguire l'aggiornamento alla versione 7.3.12 o successiva.

Quali sono le funzioni di Data Migration Tool?

Lo strumento di migrazione esegue un controllo iniziale della compatibilità e segue uno dei tre diversi percorsi di aggiornamento. Il percorso selezionato si basa sulla compatibilità dei dati della versione corrente.

> Prima di eseguire l'aggiornamento, è necessario eseguire Data Migration Tool e seguire i passaggi consigliati.

Prima di iniziare

- Si consiglia vivamente di eseguire il backup del sistema OnCommand Insight prima di eseguire lo strumento di migrazione dei dati.
- Il servizio Elasticsearch sul server deve essere attivo e funzionante.
- Prima di aggiornare Insight, è necessario eseguire Data Migration Tool per il database e gli archivi delle performance.

Esecuzione dello strumento di migrazione dei dati

1. Scaricare la versione più recente del Data Migration Tool (ad esempio, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) sul server Insight e il file di installazione Insight appropriato. Decomprimere in una cartella di lavoro. I download sono disponibili sul "Sito di supporto NetApp".
2. Aprire una finestra di comando e accedere alla cartella di lavoro.
   - Si consiglia di utilizzare la shell bash.
3. Eseguire lo strumento di migrazione dei dati utilizzando il seguente comando:
   - `*sudo ./SANScreenDataMigrationTool.sh*`
4. Seguire le istruzioni, se necessario. Di seguito viene riportato un esempio.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking Elasticsearch service...
Elasticsearch service is up

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

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

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

Il Data Migration Tool verificherà la presenza di indici obsoleti nel sistema e ne riferirà l'eventuale presenza. Se non sono presenti, lo strumento si chiude.

Alcuni indici possono essere migrati mentre il servizio del server SANscreen è in esecuzione. È possibile eseguire la migrazione di altri utenti solo quando il server viene arrestato. Se non sono presenti indici che possono essere migrati, lo strumento viene chiuso. In caso contrario, seguire le istruzioni come richiesto.

Una volta completato il Data Migration Tool, si verificherà nuovamente la presenza di indici obsoleti. Se tutti gli indici sono stati migrati, lo strumento informa che l'aggiornamento a OnCommand Insight 7.3.12 è supportato. Ora puoi procedere con l'aggiornamento di Insight.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

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

SANscreen Server service is running

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

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

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

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

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

Se viene richiesto di interrompere il servizio SANscreen, riavviarlo prima di eseguire l'aggiornamento.

Errori di convalida

Nel caso in cui la convalida dell'indice non riesca, lo strumento di migrazione informa l'utente del problema prima di uscire.

OnCommand Insight non presente:

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool V1.0

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

Versione Insight non valida:

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-105

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

Il servizio Elasticsearch non è in esecuzione:

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

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

Getting installation parameters...
Elasticsearch Rest Port: 9200

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

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

Opzioni della riga di comando

Il Data Migration Tool include alcuni parametri opzionali che ne influenzano il funzionamento.

Opzione (Linux)	Funzione
-s	--silenzioso
Elimina tutti i prompt	-a
--archivio	Se specificato, le voci di archivio esistenti per qualsiasi data di cui vengono migrati gli indici verranno sostituite. Il percorso deve puntare alla directory contenente i file zip della voce di archiviazione. È possibile specificare un argomento "-" per indicare che non è necessario aggiornare l'archivio delle performance. Se questo argomento è presente, il prompt per la posizione di archiviazione verrà eliminato.
-c	--check
Se presente, lo script viene chiuso immediatamente dopo aver segnalato i conteggi degli indici.	-d
--dryrun	Se presente, l'eseguibile di migrazione riporta le azioni che verranno intraprese (per migrare i dati e aggiornare le voci di archivio) ma non eseguirà le operazioni.
-p	--porta
Se presente, utilizzare il valore fornito come porta REST di Elasticsearch. Se assente, ottenere il valore dall'installazione, se possibile; in caso contrario, utilizzare il valore predefinito 9200. In alcune installazioni di Linux OnCommand Insight, la porta REST di Elasticsearch potrebbe non essere in esecuzione sulla porta predefinita 9200. in questo caso, utilizzare l'opzione --port per fornire il valore	-h
--help	Visualizzare le informazioni sull'utilizzo

Risoluzione dei problemi

Se le voci di archivio sono state aggiornate, è *necessario* assicurarsi che la proprietà e le autorizzazioni degli archivi aggiornati siano corrette. Dovrebbero essere **ocisys ocisys 644**. In caso contrario, accedere alla cartella di archiviazione delle prestazioni ed eseguire i seguenti comandi:

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

Aggiornamento del software Insight Server

Dopo aver effettuato l'accesso al server, è possibile verificare la disponibilità di aggiornamenti del server OnCommand Insight.

Fasi

1. Nella barra degli strumenti di Insight, fare clic sull'icona **Help** (Guida).
2. Selezionare **Controlla aggiornamenti**.
3. Fare clic su **OK** se `Version is up to date` viene visualizzato il messaggio.
4. Se viene rilevata una versione più recente, fare clic sul collegamento **scarica qui** nella finestra del messaggio.
5. Nella pagina **Download**, fare clic su **download**. Annotare la posizione della directory di download.

   È inoltre possibile scaricare la versione più recente dal sito di supporto NetApp.

6. Accedere al server Insight utilizzando un account con privilegi sudo.
7. Accedere alla directory di download e digitare il seguente comando:

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

   Assicurarsi di disporre del numero di versione corretto del file di installazione.

8. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh`：

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

9. Eseguire lo script di installazione:

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

10. Accettare il Contratto di licenza e seguire le istruzioni.

Aggiornamento del software Data Warehouse

Dopo aver aggiornato il software del server Insight, è necessario aggiornare il software del data warehouse.

Fasi

1. Accedere al server Data Warehouse (DWH) utilizzando un account con privilegi sudo.
2. Scarica il software Insight DWH dal sito di supporto di NetApp.

3. Accedere alla directory di download e digitare il seguente comando:

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

   Assicurarsi di disporre del numero di versione corretto del file di installazione.

4. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh`:

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

5. Eseguire lo script di installazione:

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

6. Accettare il Contratto di licenza e seguire le istruzioni.

Aggiornamento del software Remote Acquisition Unit

Dopo aver aggiornato il software del server Insight, è necessario aggiornare il software di acquisizione remota.

Fasi

1. Accedere al server RAU (Remote Acquisition Unit) utilizzando un account con privilegi sudo.
2. Scarica il software Insight RAU dal sito di supporto di NetApp.
3. Accedere alla directory di download e digitare il seguente comando:

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

   Assicurarsi di disporre del numero di versione corretto del file di installazione.

4. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-install.sh`:

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

5. Eseguire lo script di installazione:

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

6. Accettare il Contratto di licenza e seguire le istruzioni.

Migrazione da Windows a Linux

Per utilizzare Insight su Linux con un'installazione Windows esistente, è necessario eseguire una migrazione. È necessario eseguire questa procedura sia sul server Insight che sui componenti Data Warehouse.

Fasi

1. Eseguire il backup dell'attuale installazione Insight sul server.

   Consultare la *Guida alla configurazione e all'amministrazione di OnCommand Insight* per informazioni su come eseguire il backup del database OCI.

2. Installare Insight per Linux.
3. Ripristinare il database per la versione precedente.

   Consultare la *Guida alla configurazione e all'amministrazione di OnCommand Insight* per informazioni su come ripristinare il database OCI.

4. Disinstallare la versione precedente di Insight per Windows.

Disinstallazione di OnCommand Insight

Se necessario, è possibile disinstallare i componenti di OnCommand Insight. È necessario disinstallare i componenti di OnCommand Insight separatamente.

Ogni componente viene disinstallato separatamente.

Disinstallazione del server OnCommand Insight

Se necessario, è possibile disinstallare il server OnCommand Insight.

Prima di iniziare

Procedura consigliata: Prima di disinstallare Insight, eseguire il backup del database OnCommand Insight.

Fasi

1. Accedere al server OnCommand Insight utilizzando un account con privilegi sudo.
2. Assicurarsi che tutte le finestre di OnCommand Insight siano chiuse.
3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `oci-uninstall.sh` immettendo il seguente comando:

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

   Una normale disinstallazione non rimuove la licenza Insight o i backup giornalieri. Per rimuovere l'intera installazione, utilizzare `--purge` optioon con`oci-install.sh` comando.

4. Digitare il seguente comando:

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

Disinstallazione di Data Warehouse

Se necessario, è possibile disinstallare Data Warehouse.

Prima di iniziare

Eseguire il backup della versione corrente del database di data warehouse (DWH) di OnCommand Insight.

A proposito di questa attività

La disinstallazione del data warehouse di OnCommand Insight elimina in modo permanente tutti i dati precedentemente raccolti.

Fasi

1. Accedere al server Data Warehouse utilizzando un account con privilegi sudo.
2. Assicurarsi che tutte le finestre di OnCommand Insight siano chiuse.
3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `uninstall.sh` immettendo il seguente comando: `sudo /usr/bin/oci-uninstall.sh --help`
4. Digitare il seguente comando: `sudo /usr/bin/oci-uninstall.sh`

Disinstallazione di un'unità di acquisizione remota

È possibile disinstallare un'unità di acquisizione remota quando non è più necessaria.

Fasi

1. Accedere al server Remote Acquisition Unit utilizzando un account con privilegi sudo.
2. Assicurarsi che tutte le finestre di OnCommand Insight siano chiuse.
3. È possibile visualizzare la sintassi, gli argomenti dei comandi e l'utilizzo dei parametri per `uninstall.sh` immettendo il seguente comando: `sudo /usr/bin/oci-uninstall.sh --help`
4. Digitare il seguente comando: `sudo /usr/bin/oci-uninstall.sh`

   Viene eseguito lo script di disinstallazione. Seguire le istruzioni.

Installazione per Microsoft Windows

Prerequisiti per l'installazione

Prima di installare OnCommand Insight, è necessario scaricare la versione corrente del software, acquistare la licenza appropriata e configurare l'ambiente.

Prima di installare OnCommand Insight, assicurarsi di disporre di quanto segue:

- File del software OnCommand Insight nel pacchetto di installazione scaricato per la versione corrente
- Licenza per il funzionamento della versione di OnCommand Insight scaricata
- L'ambiente hardware e software minimo

  Il prodotto corrente potrebbe consumare risorse hardware aggiuntive (a causa delle funzionalità avanzate del prodotto OnCommand Insight) che non erano utilizzate con le versioni precedenti del prodotto OnCommand Insight.

- Un piano di implementazione che include le configurazioni hardware e di rete per il server OnCommand Insight, il data warehouse e il reporting e le unità di acquisizione remota.
- Software antivirus disattivato

  Durante l'installazione di OnCommand Insight, è necessario disattivare completamente tutti i programmi antivirus. Dopo l'installazione, i percorsi utilizzati dal componente Insight (percorsi di installazione, backup e archiviazione) devono essere esclusi dalla scansione dei virus, oltre ad escludere l'intero `sanscreen` directory dalla scansione.

  Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio *C: Programmi IBM DB2*) dalla scansione antivirus dopo l'installazione.

> Se si esegue un'installazione completa come aggiornamento o come migrazione a un nuovo hardware e il sistema esistente contiene una configurazione di sicurezza non predefinita, è necessario eseguire il backup della configurazione di sicurezza prima di eseguire l'installazione. Una volta completata l'installazione, è necessario ripristinare la configurazione di sicurezza prima di ripristinare il server (che include l'unità di acquisizione locale) o il database di Data Warehouse.prima di ripristinare il database DWH, è necessario ripristinare la configurazione di sicurezza su tutti i server Insight.
>
> Per l'aggiornamento in-place (disponibile solo per Insight Server), la configurazione della sicurezza viene gestita correttamente e non è necessario ripristinarla.
>
> Si utilizza `securityadmin` per creare un backup della configurazione e ripristinare la configurazione salvata. Per ulteriori informazioni, cercare `securityadmin` Nel Centro documentazione OnCommand Insight: http://docs.netapp.com/oci-73/index.jsp

Pianificazione dell'implementazione

Per garantire una corretta implementazione, è necessario prendere in considerazione alcuni elementi di sistema prima di installare OnCommand Insight.

A proposito di questa attività

La pianificazione dell'implementazione di Insight include la valutazione di questi elementi di sistema:

- Architettura Insight
- I componenti di rete da monitorare
- Prerequisiti per l'installazione di Insight e requisiti del server
- Requisiti del browser Web Insight

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". .

Identificazione dei dispositivi e pianificazione dell'origine dei dati

Nell'ambito della pianificazione dell'implementazione, è necessario raccogliere informazioni sui dispositivi presenti nell'ambiente.

Sono necessari i seguenti software, connettività e informazioni su ciascun dispositivo nell'ambiente:

- Indirizzo IP o nome host risolvibile dal server OCI
- Nome di accesso e password
- Tipo di accesso al dispositivo, ad esempio controller e stazione di gestione

> L'accesso in sola lettura sarà sufficiente per la maggior parte dei dispositivi, ma alcuni richiedono autorizzazioni di amministratore.

- Connettività della porta al dispositivo in base ai requisiti della porta di origine dati
- Per gli switch, stringa di comunità di sola lettura SNMP (ID utente o password per consentire l'accesso agli switch)
- Qualsiasi software di terze parti richiesto sul dispositivo, ad esempio Solutions Enabler.
- Per ulteriori informazioni sui requisiti e sulle autorizzazioni dell'origine dati, consultare la sezione "riferimento all'origine dati specifico del vendor" nella Guida dell'interfaccia utente Web o nella *Guida alla configurazione e all'amministrazione di OnCommand Insight*.

Traffico di rete generato da OnCommand Insight

Il traffico di rete generato da OnCommand Insight, la quantità di dati elaborati che attraversano la rete e il carico che OnCommand Insight carica sui dispositivi variano in

base a diversi fattori.

Il traffico, i dati e il carico differiscono tra gli ambienti in base ai seguenti fattori:

- I dati raw
- Configurazione dei dispositivi
- Topologia di implementazione di OnCommand Insight
- Intervalli di polling diversi per l'origine dati di inventario e performance, che possono essere ridotti per consentire il rilevamento di dispositivi lenti o la conservazione della larghezza di banda

I dati di configurazione raw raccolti da OnCommand Insight possono variare in modo significativo.

Nell'esempio seguente viene illustrato come i dati di configurazione possono variare e come il traffico, i dati e il carico sono influenzati da molti fattori di configurazione. Ad esempio, potrebbero essere presenti due array con 1,000 dischi ciascuno:

- Array 1: Dispone di 1,000 dischi SATA di dimensioni pari a 1 TB. Tutti i 1,000 dischi si trovano in un unico pool di storage e sono presenti 1,000 LUN, tutte presentate (mappate e mascherate) agli stessi 32 nodi in un cluster ESX.
- Array 2: Dispone di 400 dischi dati da 2 TB, dischi FC da 560 600 GB e 40 SSD. Esistono 3 pool di storage, ma 320 dischi FC vengono utilizzati nei gruppi RAID tradizionali. Le LUN scavate nei gruppi RAID utilizzano un tipo di mascheramento tradizionale (symmaskdb), mentre le LUN basate su pool con thin provisioning utilizzano un tipo di mascheramento più recente (symaccess). Sono disponibili 600 LUN per 150 host diversi. Sono disponibili 200 BCVs (volumi di replica a blocchi completi di 200 delle 600 LUN). Esistono anche 200 volumi R2, volumi di replica remoti di volumi che esistono su un array in un sito diverso.

Ciascuno di questi array dispone di 1,000 dischi e 1,000 volumi logici. Potrebbero essere fisicamente identici nella quantità di spazio rack consumata nel data center e potrebbero anche eseguire lo stesso firmware, ma il secondo array è molto più complesso nella sua configurazione rispetto al primo array.

Software di scansione virus non disponibile

Se sul sistema è attivo un software antivirus, l'installazione di OnCommand Insight non riesce. È possibile evitare questo problema disattivando il software antivirus prima dell'installazione.

Per evitare un errore di installazione dovuto a un software di scansione virus attivo, durante l'installazione di ciascun componente di OnCommand Insight, è necessario disattivare completamente tutti i programmi antivirus. Dopo l'installazione, i percorsi utilizzati dal componente Insight (percorsi di installazione, backup e archiviazione) devono essere esclusi dalla scansione antivirus.

Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio *C: Programmi IBM DB2*) dalla scansione antivirus dopo l'installazione.

Requisiti di Insight Server

Si consiglia di utilizzare un server dedicato. Non installare Insight su un server in cui sono installate altre applicazioni. Sono supportati server fisici e virtuali, a condizione che i requisiti del prodotto siano soddisfatti.

Per installare il software del server OnCommand Insight, è necessario disporre delle autorizzazioni di amministratore locale.

> Il dimensionamento per OnCommand Insight prevede diverse dipendenze, come tipo e dimensione dell'origine dati, numero di risorse nell'ambiente, intervalli di polling e altro ancora. I seguenti esempi di dimensionamento sono solo linee guida e rappresentano alcuni degli ambienti in cui Insight è stato testato. La modifica di questi o altri fattori nell'ambiente può modificare i requisiti di dimensionamento di Insight. Queste linee guida includono spazio su disco per un massimo di 90 giorni di dati di archiviazione delle performance.

Prima di installare o aggiornare Insight, si consiglia di contattare il Sales Engineer per ottenere informazioni dettagliate sul dimensionamento.

Esempi:

Fattori ambientali:	Spazio su disco, CPU e memoria testati:
80 volumi di storage 4,000 VM 4,000 porte switch	250 GB di spazio su disco 8 core 32 GB DI RAM
160 unità di storage 40.000 volumi 8,000 VM 8,000 porte switch	1 TB di spazio su disco 12 core 48 GB DI RAM

Requisiti:

Componente	Obbligatorio
Sistema operativo	Un computer con Microsoft Windows Server 2016, 2019 o 2022 a 64 bit con il Service Pack più recente. Il file system resiliente (REF) introdotto con Windows Server 2012 non è compatibile con OnCommand Insight. L'installazione di OnCommand Insight in Windows è supportata solo sul file system NTFS. Si consiglia di utilizzare un server dedicato.
Macchina virtuale (VM)	Questo componente può essere eseguito in un ambiente virtuale, a condizione che le risorse di CPU e memoria per l'istanza siano riservate.

Memoria e CPU	24 - 256 GB DI RAM 8 - 32 core Si consiglia di impostare la dimensione del file di paging su “Windows Managed”. I file di paging di piccole dimensioni possono interferire con la corretta memorizzazione dei dati delle performance Insight.
Spazio su disco disponibile	100 GB - 3 TB di spazio su disco per l’installazione 50 GB - 1 TB di spazio su disco per l’archiviazione delle performance I dischi SSD sono consigliati per lo spazio di installazione Insight.
Rete	Connessione Ethernet e porte: • Connessione Ethernet a 100 Mbps o 1 Gbps con indirizzo IP dedicato (statico) e connettività IP a tutti i componenti della SAN, inclusi i dispositivi FC e le unità di acquisizione remota. • I requisiti delle porte per il processo del server OnCommand Insight sono 80, 443, 1090 - 1100, 3873, 8083, da 4444 a 4446, 5445, 5455, da 4712 a 4714, 5500, e 5501. • I requisiti delle porte per il processo di acquisizione sono 12123 e 5679. • Il requisito di porta per MySQL è 3306. • I requisiti delle porte per Elasticsearch sono 9200 e 9310 • I requisiti delle porte dinamiche per Win2008/2012 vanno dalla versione 49152 alla 65535 Le porte 443 e 3306 richiedono l’accesso esterno attraverso qualsiasi firewall presente.
Permessi	Sul server OnCommand Insight sono richieste le autorizzazioni di amministratore locale. Se una delle seguenti cartelle è un collegamento simbolico, assicurarsi che le directory di destinazione dispongano dei permessi '755'. • /opt/netapp • /var/lib/netapp • /var/log/netapp

Connettività remota	Connettività Internet per consentire l'accesso a WebEx o una connessione desktop remota per facilitare l'installazione e il supporto post-installazione.
Accessibilità	È richiesto l'accesso HTTPS.
Scansione virus	Durante l'installazione di questo componente di OnCommand Insight, è necessario disattivare completamente tutti i programmi antivirus. Dopo l'installazione, i percorsi utilizzati dal componente Insight (percorsi di installazione, backup e archiviazione) devono essere esclusi dalla scansione antivirus. Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio *C: Programmi IBM DB2*) dalla scansione antivirus dopo l'installazione.
Server HTTP o HTTPS	Microsoft Internet Information Services (IIS) o altri server HTTPS non devono competere per le stesse porte (443) del server OnCommand Insight e non devono avviarsi automaticamente. Se devono ascoltare la porta 443, è necessario configurare il server OnCommand Insight in modo che utilizzi altre porte.

Requisiti del data warehouse e del server di reporting

È necessario eseguire il Data Warehouse e il server di reporting su un computer compatibile con i requisiti hardware e software stabiliti, assicurandosi che il server Web Apache o il software di reporting non siano già installati su questa macchina.

> Il dimensionamento per OnCommand Insight prevede più dipendenze, ad esempio il numero di risorse nell'ambiente, la quantità di dati storici conservati e molto altro ancora. I seguenti esempi di dimensionamento del data warehouse sono solo linee guida e rappresentano alcuni degli ambienti in cui Insight è stato testato. La modifica di questi o altri fattori nell'ambiente può modificare i requisiti di dimensionamento di Insight.

Prima di installare o aggiornare Insight, si consiglia di contattare il Sales Engineer per ottenere informazioni dettagliate sul dimensionamento.

Esempi:

Fattori ambientali:	Spazio su disco, CPU e memoria testati:
18 storage array3,400 VM 4,500 porte switch	Disco rigido da 200 GB 8 core 32 GB DI RAM

110 array di storage 11,500 VM 14,500 porte switch	Disco rigido da 300 GB 8 core 48 GB DI RAM

Requisiti:

Componente	Obbligatorio
Sistema operativo	Un computer con Microsoft Windows Server 2016, 2019 o 2022 a 64 bit con il Service Pack più recente.
Macchina virtuale (VM)	Questo componente può essere eseguito in un ambiente virtuale, a condizione che le risorse di CPU e memoria per l'istanza siano riservate.
CPU	8 - 40 core CPU
Memoria	32 GB - 2 TB di RAM Best practice: Si consiglia di impostare la dimensione del file di paging su "Windows Managed". I file di paging di piccole dimensioni possono interferire con la corretta memorizzazione dei dati delle performance Insight.
Spazio su disco disponibile	200 GB - 2 TB di spazio su disco. L'installazione richiede almeno 20 GB di spazio libero sull'unità C. In Windows, Insight Data Warehouse con Reporting richiede che il supporto per la creazione del nome 8dot3 sia abilitato sul disco di installazione prima dell'installazione. L'unità C: In genere ha questa opzione attivata per impostazione predefinita. È possibile verificare se la creazione del nome 8dot3 è attivata sul disco di installazione di destinazione eseguendo il seguente comando (sostituire D: Con il disco di installazione di destinazione): fsutil 8dot3name query D: Per abilitare la creazione del nome 8dot3, eseguire il seguente comando (sostituire D: Con il disco di installazione di destinazione): fsutil 8dot3name set D: 0

Rete	• Connessione Ethernet a 100 Mbps o 1 Gbps • Indirizzo IP statico • La porta 50000 deve essere disponibile prima di installare Data Warehouse con Reporting su Windows • Per il processo del server DWH OnCommand Insight, porte 80, 443, 1098, 1099, 3873, 8083 e da 4444 a 4446 • Per il motore di reporting, porte 1527, 9362, 9300 e 9399 • Per MySQL, porta 3306 • Assicurarsi che il DNS funzioni correttamente eseguendo una `nslookup` rispetto all'host
Virus Scan (scansione virus)	Durante l'installazione di questo componente di OnCommand Insight, è necessario disattivare completamente tutti i programmi antivirus. Dopo l'installazione, i percorsi utilizzati dal componente Insight (percorsi di installazione, backup e archiviazione) e tutti i percorsi di installazione dei componenti DWH (SANscreen, DB2 e percorsi di backup) devono essere esclusi dalla scansione antivirus.
Visual Studio	Visual Studio 2019 "ridistribuibili" Deve essere installato prima di installare Data Warehouse con Reporting su Windows.

Requisiti del server Remote Acquisition Unit

È necessario installare un'unità di acquisizione remota (RAU) per acquisire informazioni da dispositivi SAN protetti da firewall, siti remoti, reti private o in segmenti di rete diversi. Prima di installare la RAU, assicurarsi che l'ambiente soddisfi i requisiti di sistema operativo RAU, CPU, memoria e spazio su disco.

Componente	Requisito
Sistema operativo	Un computer con Microsoft Windows Server 2016, 2019 o 2022 a 64 bit con il Service Pack più recente.
CPU	4 core CPU
Memoria	16 GB DI RAM
Spazio su disco disponibile	40 GB

Rete	Connessione Ethernet a 100 Mbps/1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi FC e porta richiesta al server OnCommand Insight (80 o 443).
Permessi	Autorizzazioni di amministratore locale sul server RAU
Scansione virus	Durante l'installazione di questo componente di OnCommand Insight, è necessario disattivare completamente tutti i programmi antivirus. Dopo l'installazione, i percorsi utilizzati dal componente Insight devono essere esclusi dalla scansione antivirus. Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio *C: Programmi IBM DB2*) dalla scansione antivirus dopo l'installazione.

Browser supportati da OnCommand Insight

L'interfaccia utente di OnCommand Insightweb basata su browser può funzionare con diversi browser.

Insight supporta versioni non beta più recenti dei seguenti browser:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

Per un elenco completo delle versioni del browser idonee per OnCommand Insight, consultare la "Tool di matrice di interoperabilità NetApp".

Istruzioni di installazione di Insight

L'installazione richiede l'installazione di diversi componenti OnCommand Insight, tra cui Insight Server, Data Warehouse e Reporting.
L'installazione include le seguenti attività principali:

- Download del programma di installazione di OnCommand Insight
- Installazione del server OnCommand Insight
- Installazione delle licenze
- Come opzione, installazione di DWH e Reporting (deve essere installato su una macchina virtuale o su una macchina virtuale separata)
- Facoltativamente, l'installazione di un'unità di acquisizione remota (RAU), che acquisisce informazioni dalle risorse del dispositivo che risiedono dietro un firewall, si trovano in un sito remoto o si trovano in una rete privata
- Per gli aggiornamenti, l'aggiornamento dei report OnCommand Insight.

Dopo l'installazione, è necessario configurare Insight per acquisire informazioni sull'ambiente. Le attività

richieste sono descritte nella *Guida alla configurazione e all'amministrazione di OnCommand Insight*.

Download del programma di installazione di OnCommand Insight

È possibile scaricare il programma di installazione di OnCommand Insight dal sito del supporto NetApp.

Prima di iniziare

È necessario disporre di un accesso al sito di supporto NetApp all'indirizzo "mysupport.netapp.com".

Fasi

1. Accedere al server su cui si desidera installare OnCommand Insight.
2. Scaricare il file di installazione dal sito del supporto NetApp.

Installazione del server OnCommand Insight

È possibile installare facilmente il server OnCommand Insight utilizzando l'installazione guidata di OnCommand Insight.

Prima di iniziare

È necessario aver completato tutti i prerequisiti di installazione.

Fasi

1. Accedere al server Insight utilizzando un account con privilegi di amministratore.
2. Aprire Esplora risorse e accedere alla directory in cui si trovano i file di installazione.
3. Fare doppio clic su `.MSI` file scaricato.
4. Fare clic su **Avanti** per continuare.
5. Leggere il Contratto di licenza, selezionare la casella di controllo **Accetto i termini del Contratto di licenza**, quindi fare clic su **Avanti**.
6. Inserire il nome del cliente e il nome del sito nella finestra **informazioni sul cliente**, quindi fare clic su **Avanti**.

   Best practice: utilizzare il nome del cliente come prefisso per il sito, ad esempio NetApp.

7. Nella finestra **Customer Information: Configure NetApp ASUP** (informazioni sul cliente: Configurazione di NetApp ASUP*), procedere come segue:

   a. Selezionare il database contenente i dati che si desidera caricare in ASUP selezionando una delle seguenti opzioni:

      - **Nessun backup del database**: Non viene inviato un backup ad ASUP.
      - **Backup senza dati sulle prestazioni**: Viene eseguito un backup e inviato ad ASUP ma non include i dati sulle prestazioni.
      - **Backup con dati sulle performance**: Viene eseguito un backup che include dati sulle performance, ma questo potrebbe generare un enorme `*.gz` file.

ASUP viene fornito utilizzando il protocollo HTTPS.

+

a. In **Logs**, selezionare se non si desidera alcun log, log di base o log esteso che contenga una registrazione dell'origine dati.
b. Fare clic su **Avanti**.

8. 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).
9. Fare clic su **Avanti**
10. Nella finestra **Configura server**, selezionare o impostare i parametri di configurazione appropriati per configurare il server OnCommand Insight:

Opzione	Descrizione
Porta portale (HTTP)	Porte utilizzate dal server OnCommand Insight per supportare i servizi Web dell'utente, incluso un portale per eseguire attività di amministrazione. Utilizzare il valore predefinito (80); tuttavia, se la porta predefinita è in uso, cambiarla con un'altra porta.
Porta portale (HTTPS)	Porta utilizzata dalle unità di acquisizione remote per inviare informazioni sulle modifiche SAN al server OnCommand Insight attraverso un canale sicuro. Utilizzare il valore predefinito (443); tuttavia, se la porta predefinita è in uso, cambiarla con un'altra porta. Specificare lo stesso numero di porta durante la configurazione di Raus.
Porta database interna (SQL)	Porta utilizzata internamente dal PC in cui è in esecuzione il server OnCommand Insight, per fungere da punto di accesso al database. Utilizzare il valore predefinito (3306); tuttavia, se la porta predefinita è in uso, cambiarla con un'altra porta.

11. Fare clic su **Avanti**.
12. Fare clic su **Install** (Installa) per continuare.

    L'installazione richiede circa 20 minuti, a seconda delle applicazioni installate.

13. Fare clic su **fine**.

Installazione di data warehouse e report OnCommand Insight

L'installazione è autonoma e include gli elementi necessari per eseguire e utilizzare il data warehouse di OnCommand Insight e le utility di reporting.

Prima di iniziare

Prima di installare o aggiornare, tenere presente quanto segue.

- Se si esegue l'aggiornamento, eseguire il backup di DWH.
- Per installare il data warehouse di OnCommand Insight con Reporting, è necessario disporre delle autorizzazioni locali *Administrator*.
- Assicurarsi che il servizio Windows Modules Installer sia attivato (automaticamente o manualmente).
- Se si esegue l'installazione su un disco non C:, è necessario attivare i nomi file brevi. Se non è abilitato, il programma di installazione lo attiverà.
- Per il componente DB2, l'utente DB2 può essere *domain* user o *local* user.
  - Se l'utente DB2 è un utente *dominio*, è necessario disporre di quanto segue:
    - L'utente DB2 deve essere già stato creato ed è necessario conoscere il nome utente e la password
    - In qualità di utente che sta installando DWH con Reporting, è necessario essere in grado di eseguire query all'utente DB2. È possibile validarlo utilizzando il comando:
      - `net user <db2 user name> /domain`
  - Se l'utente DB2 è un utente *locale*, è necessario disporre di quanto segue:
    - Nome utente e password dell'utente che verrà utilizzato per l'esecuzione come utente DB2. Se questo utente non esiste, verrà creato dall'installazione.
  - [NOTA]

Il nome utente DB2 e il nome di accesso Windows hanno le seguenti restrizioni: * I caratteri validi sono: Da 'A' a 'Z'; da 'A' a 'z'; da '0' a '9'; ' N.'; '@'; *''; '!'; '('; ')'; '{'; '}'; '-'; e '.'. * Se si utilizzano i caratteri speciali '!'; '('; ')'; '{'; '}'; '-'; e '.' il nome utente deve essere composto da lettere maiuscole. * Il primo carattere della stringa deve essere un carattere alfabetico, @, N. o €; non può essere un numero o le sequenze di lettere* _*SYS*, *DBM* o *IBM* * e non può superare i 128 byte di lunghezza. * Non possono essere UTENTI, AMMINISTRATORI, OSPITI, PUBBLICO, LOCALE o qualsiasi parola riservata SQL.

- L'utente DB2 non può essere lo stesso dell'utente che esegue l'installazione.

Fasi

1. Accedere al server Data Warehouse utilizzando un account con privilegi di amministratore.
2. Scarica il file .zip di Data Warehouse con Reporting ed estrarlo in una cartella di installazione.
3. Accedere alla cartella <download location> ed eseguire lo script *install_oci_dwh.bat*.

   Con OnCommand Insight 7.3.10 e versioni successive, è necessario eseguire lo script per l'installazione corretta di DWH/Reporting. Non eseguire l'eseguibile di installazione .MSI.

4. Immettere il dominio DB2 o premere Invio per il dominio locale.
5. Inserire il nome utente DB2. Vedere sopra per le restrizioni relative al nome utente.
6. Inserire la password per l'utente DB2. Inserire nuovamente la password quando richiesto.
7. Immettere il percorso di installazione del componente DB2 o premere Invio per impostazione predefinita.
8. Vengono visualizzate le informazioni immesse. Verificare attentamente tutte le impostazioni. Premere Invio

per avviare l'installazione.

9. Se richiesto, consentire a Windows di procedere con l'installazione di DB2.
10. Dopo l'installazione di DB2, viene eseguita l'installazione guidata di DWH. Seguire le istruzioni per installare DWH con Reporting.

    Il completamento di Data Warehouse con creazione di report può richiedere fino a un'ora.

Individuazione della documentazione di IBM Cognos

Per informazioni di base, ad esempio come avviare e arrestare il software del portale Reporting, consultare la documentazione di IBM Cognos installata con il prodotto. È possibile cercare con un browser Web informazioni su qualsiasi prodotto di reporting IBM Cognos, ad esempio Query Studio, Report Studio, Business Insight o Business Insight Advanced sul sito Web di IBM negli Information Center di tali prodotti software.

Fasi

1. Per individuare la documentazione di IBM Cognos installata con OnCommand Insight, accedere a questa directory.

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

2. È inoltre possibile visualizzare gli argomenti che descrivono le singole finestre di IBM Cognos utilizzate nel portale di reporting di OnCommand Insight. Fare clic sull'icona **?** sulla barra degli strumenti della finestra.

Verifica dell'installazione di Data Warehouse e Reporting

Dopo aver installato correttamente il data warehouse di OnCommand Insight, è necessario assicurarsi che tutti i servizi DWH e di reporting siano disponibili nei servizi Microsoft Windows.

Fasi

1. Dal menu Start di Windows, selezionare **pannello di controllo › sistema e sicurezza › Strumenti di amministrazione › servizi**.
2. Verificare che nell'elenco dei servizi siano presenti le seguenti voci:

Nome/Stato	Descrizione
Server SANscreen / in esecuzione	Il server DWH di OnCommand Insight
MySQL / in esecuzione	Il database SQL di OnCommand Insight
IBM Cognos / in esecuzione	IBM Cognos Content Database
DB2- DB2COPY1 - DB2-0 / IN ESECUZIONE	Gestire i database DB2

DB2 Governor (DB2COPY1) / non in esecuzione	Raccoglie le statistiche per le applicazioni connesse ai database DB2.
Server di licenza DB2 (DB2COPY1) / non in esecuzione	Monitora la conformità alle licenze DB2.
DB2 Management Service (DB2COPY1) / in esecuzione	Gestisce le voci di registro DB2 per la compatibilità con le versioni precedenti delle copie DB2.
DB2 Remote Command Server (DB2COPY1) / in esecuzione	Supporta l'esecuzione remota dei comandi DB2.
IBM Secure Shell Server per Windows / non in esecuzione	IBM Secure Shell Server per Windows

Installazione di un'unità di acquisizione remota (RAU)

Installare uno o più RAUS nel proprio ambiente OnCommand Insight.

Prima di iniziare

È necessario aver completato tutti i prerequisiti di installazione.

Almeno una porta deve essere aperta e disponibile tra il server RAU e il server OnCommand Insight per inoltrare le informazioni sulle modifiche al server. In caso di dubbi, convalidarlo aprendo un browser Web sul computer RAU e indirizzandolo al server OnCommand Insight:

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

Per impostazione predefinita, la porta di acquisizione è 443, ma potrebbe essere stata modificata durante l'installazione del server. Se la connessione viene stabilita correttamente, viene visualizzata una pagina di risposta OnCommand Insight che indica una porta aperta e disponibile tra RAU e server OnCommand Insight.

Fasi

1. Accedere al server RAU utilizzando un account con privilegi di amministratore.
2. Aprire Esplora risorse e accedere alla directory in cui si trova il file di installazione RAU.
3. Fare doppio clic `.MSI` per avviare l'installazione.
4. Fare clic su **Avanti** per passare alla finestra che mostra il Contratto di licenza. Leggere e accettare i termini del Contratto di licenza e fare clic su **Avanti**.
5. Selezionare per installare la RAU su un disco rigido locale o l'intera funzione su un disco rigido locale. Controllare il collegamento Disk Usage (utilizzo disco) per assicurarsi di disporre di spazio sufficiente (sono necessari 116 MB). Fare clic su **Avanti**.
6. Nella finestra Configure (Configura), impostare i seguenti parametri specifici del sito:
   - **OnCommand Insight Nome o indirizzo del server -** Nome host o indirizzo IP per identificare il server OnCommand Insight. La RAU utilizza questo nome/IP per aprire un collegamento di comunicazione

con il server. Se si specifica un nome host, assicurarsi che sia possibile risolverlo tramite DNS.

- **Acquisition Unit Name** (Nome unità di acquisizione) - Nome univoco che identifica la RAU.
- **Porta di acquisizione remota protetta OnCommand Insight (HTTPS)** - porta utilizzata dalle unità di acquisizione remota per inviare informazioni sulle modifiche dell'ambiente al server OnCommand Insight. Questa impostazione deve corrispondere al valore immesso durante l'installazione del server OnCommand Insight e deve essere la stessa su tutti i server Raus.

7. Rivedere le selezioni. Fare clic su **Indietro** per tornare indietro e apportare modifiche. Fare clic su **Avanti**.
8. Fare clic su **Installa** per avviare l'installazione.

   Attendere il completamento dell'installazione. Questa operazione dovrebbe richiedere da 5 a 10 minuti circa.

Al termine

Al termine dell'installazione, viene visualizzata una finestra finale. Fare clic sulla casella **Start Remote Acquisition Service** (Avvia servizio di acquisizione remota) per avviare la RAU, quindi fare clic su **Finish** (fine) per terminare l'operazione.

Verifica del servizio dell'unità di acquisizione remota

Una volta completata correttamente l'installazione di un'unità di acquisizione remota (RAU), il servizio RAU di OnCommand Insight dovrebbe essere disponibile nell'ambiente dei servizi Microsoft Windows.

Fasi

1. Per verificare che la RAU sia stata aggiunta ai servizi Windows, aprire il menu Start di Windows e selezionare **pannello di controllo** > **Strumenti di amministrazione** > **servizi**.
2. Individuare **OnCommand Insight acq - unità di acquisizione remota (RAU) di OnCommand Insight** nell'elenco.

Convalida dell'installazione dell'unità di acquisizione remota

Per convalidare l'installazione corretta dell'unità di acquisizione remota, è possibile visualizzare lo stato delle unità di acquisizione remota collegate al server.

Fasi

1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su *Acquisition Units (unità di acquisizione)
3. Verificare che la nuova unità di acquisizione remota sia stata registrata correttamente e che abbia uno stato di connessione.

   In caso contrario, contattare il supporto tecnico.

Verifica dell'installazione

È possibile aprire Insight in un browser supportato per verificare l'installazione. È possibile controllare anche i file di log di Insight.

Quando si apre Insight per la prima volta, viene visualizzata la pagina di configurazione della licenza. Dopo aver inserito le informazioni sulla licenza, è necessario configurare le origini dati. Consultare la *Guida alla configurazione e all'amministrazione di OnCommand Insight* per informazioni sull'immissione delle definizioni delle origini dati e sull'impostazione degli utenti e delle notifiche di Insight.

In caso di problemi di installazione, contattare il supporto tecnico e fornire le informazioni richieste.

Verifica dei nuovi servizi Insight

Una volta completata l'installazione, verificare che i servizi per i componenti Insight funzionino sul server.

Fasi

1. Per visualizzare un elenco dei servizi attualmente in funzione:
   a. Fare clic sul pulsante **Start**.
   b. Fare clic su **Esegui**.
   c. Digitare quanto segue:

      ```
      cmd
      ```

   d. Premere Invio.
   e. Digitare quanto segue nella finestra **prompt dei comandi**:

      ```
      net start
      ```

2. Verificare la presenza di questi servizi Insight nell'elenco:
   - **Server SANscreen**
   - **SANscreen acq** (processo di acquisizione)
   - **MySQL** (database Insight SQL)
   - **Elasticsearch** (Data store per dati Insight) se questi servizi non vengono visualizzati nell'elenco, contattare il supporto tecnico.

Registri Insight

Insight fornisce molti file di log per facilitare la ricerca e la risoluzione dei problemi. I registri disponibili sono elencati nella directory dei registri. È possibile utilizzare uno strumento per il monitoraggio dei log, ad esempio BareTail, per visualizzare tutti i log contemporaneamente.

I file di log si trovano in `<install directory>\SANscreen\wildfly\standalone\log` directory. I registri di acquisizione si trovano in `<install directory>\SANscreen\Acq\Log` directory.

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:

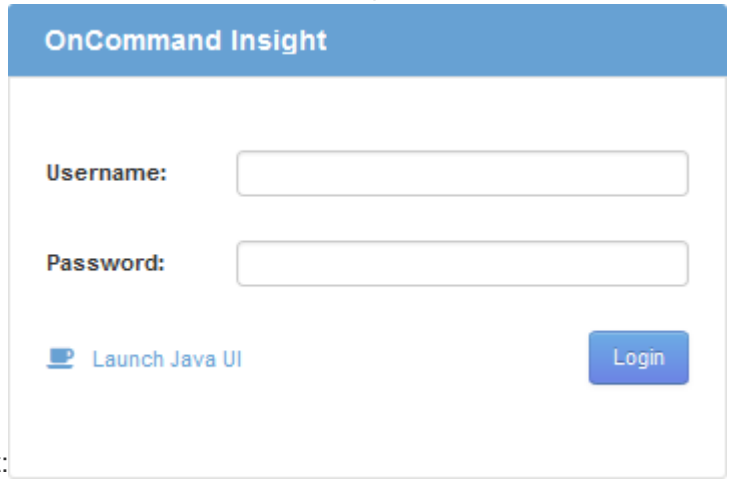
     `https://fqdn`

   - 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)

Risoluzione dei problemi di installazione

Le installazioni di OnCommand Insight vengono generalmente gestite attraverso le procedure guidate di installazione. Tuttavia, i clienti potrebbero riscontrare problemi durante gli aggiornamenti o conflitti dovuti agli ambienti informatici.

Assicurarsi inoltre di installare tutte le licenze OnCommand Insight necessarie per l'installazione del software.

Licenze mancanti

Per diverse funzionalità di OnCommand Insight sono necessarie licenze diverse. Le informazioni visualizzate in OnCommand Insight sono controllate dalle licenze installate. Fare riferimento alla sezione delle licenze OnCommand Insight per informazioni sulle funzionalità controllate da ciascuna licenza.

Fare riferimento alla sezione delle licenze OnCommand Insight per informazioni sulle funzionalità controllate da ciascuna licenza.

Invio di una richiesta di supporto tecnico online

In caso di problemi con l'installazione di Insight, in qualità di cliente registrato, puoi inviare una richiesta di supporto tecnico online.

Prima di iniziare

Utilizzando l'indirizzo e-mail aziendale, è necessario registrarsi come cliente del supporto per ottenere servizi di supporto online. La registrazione viene eseguita tramite il sito di supporto (http://support.netapp.com).

A proposito di questa attività

Per aiutare il supporto clienti a risolvere il problema di installazione, è necessario raccogliere il maggior numero possibile di informazioni, tra cui:

- Numero di serie di Insight
- Descrizione del problema
- Tutti i file di log Insight
- Cattura dello schermo di eventuali messaggi di errore

Fasi

1. Creare un `.zip` file delle informazioni raccolte per creare un pacchetto di risoluzione dei problemi.
2. Accedere al sito di supporto all'indirizzo "mysupport.netapp.com" E selezionare **Assistenza tecnica**.
3. Fare clic su **Apri un caso**.

4. Seguire le istruzioni del pacchetto di dati.

Al termine

Per seguire la richiesta, puoi utilizzare **verifica stato caso** nella pagina Assistenza tecnica.

Aggiornamento di OnCommand Insight

Normalmente, è necessario eseguire un aggiornamento su tutti i server Insight (server Insight, server Data Warehouse, unità di acquisizione remota). Consultare sempre le Note di rilascio per i requisiti di aggiornamento per una nuova release di OnCommand Insight.

Se non diversamente indicato, i requisiti e le procedure si applicano all'aggiornamento da Insight 7.x alla versione corrente di Insight. Se si esegue l'aggiornamento da una versione precedente alla 7.0, contattare il proprio rappresentante commerciale.

Aggiornamento di Insight alla versione 7.3.12 o successiva - Windows

Prima di eseguire l'aggiornamento da OnCommand Insight 7.3.10 - 7.3.11 alla versione 7.3.12 o successiva, è necessario eseguire lo strumento di migrazione dei dati OCI.

Sfondo

OnCommand Insight versione 7.3.12 e successive utilizzano software sottostante che potrebbero essere incompatibili con le versioni precedenti. Le versioni 7.3.12 e successive di Insight includono un **Data Migration Tool** per l'aggiornamento.

> Le versioni di OnCommand Insight 7.3.9 e precedenti non sono più supportate. Se si utilizza una di queste versioni, *è necessario* eseguire l'aggiornamento a Insight versione 7.3.10 o successiva (si consiglia vivamente la versione 7.3.11) prima di eseguire l'aggiornamento alla versione 7.3.12 o successiva.

Quali sono le funzioni di Data Migration Tool?

Lo strumento di migrazione esegue un controllo iniziale della compatibilità e segue uno dei tre diversi percorsi di aggiornamento. Il percorso selezionato si basa sulla compatibilità dei dati della versione corrente.

> Prima di eseguire l'aggiornamento, è necessario eseguire Data Migration Tool e seguire i passaggi consigliati.

Prima di iniziare

- Si consiglia vivamente di eseguire il backup del sistema OnCommand Insight prima di eseguire lo strumento di migrazione dei dati.
- Il servizio Elasticsearch sul server deve essere attivo e funzionante.
- Prima di aggiornare Insight, è necessario eseguire Data Migration Tool per il database e gli archivi delle performance.

Esecuzione dello strumento di migrazione dei dati

1. Scaricare la versione più recente del Data Migration Tool (ad esempio, *SANScreenDataMigrationTool-x86-7.3.12-97.zip*) sul server Insight e il file di installazione Insight appropriato. Decomprimere in una cartella di lavoro. I download sono disponibili sul "Sito di supporto NetApp".
2. Aprire una finestra di comando e accedere alla cartella di lavoro.
   - Aprire PowerShell come amministratore.
3. Eseguire lo strumento di migrazione dei dati utilizzando il seguente comando:
   - `.` *SANScreenDataMigrationTool.ps1*
4. Seguire le istruzioni, se necessario. Di seguito viene riportato un esempio.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-121

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

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

Checking Elasticsearch service...
Elasticsearch service is up

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

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

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

Il Data Migration Tool verificherà la presenza di indici obsoleti nel sistema e ne riferirà l'eventuale presenza. Se non sono presenti, lo strumento si chiude.

Alcuni indici possono essere migrati mentre il servizio del server SANscreen è in esecuzione. È possibile eseguire la migrazione di altri utenti solo quando il server viene arrestato. Se non sono presenti indici che possono essere migrati, lo strumento viene chiuso. In caso contrario, seguire le istruzioni come richiesto.

Una volta completato il Data Migration Tool, si verificherà nuovamente la presenza di indici obsoleti. Se tutti gli indici sono stati migrati, lo strumento informa che l'aggiornamento a OnCommand Insight 7.3.12 è supportato. Ora puoi procedere con l'aggiornamento di Insight.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-127

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

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

Checking Elasticsearch service...
Elasticsearch service is up

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

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

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

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

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

Se viene richiesto di interrompere il servizio SANscreen, riavviarlo prima di eseguire l'aggiornamento.

Errori di convalida

Nel caso in cui la convalida dell'indice non riesca, lo strumento di migrazione informa l'utente del problema prima di uscire.

OnCommand Insight non presente:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool V1.0

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

Versione Insight non valida:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

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

Il servizio Elasticsearch non è in esecuzione:

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-105

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

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

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

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

Opzioni della riga di comando

Il Data Migration Tool include alcuni parametri opzionali che ne influenzano il funzionamento.

Opzione (Windows)	Funzione

-s	Elimina tutti i prompt
-perf_archive	Se specificato, le voci di archivio esistenti per qualsiasi data di cui vengono migrati gli indici verranno sostituite. Il percorso deve puntare alla directory contenente i file zip della voce di archiviazione. È possibile specificare un argomento "-" per indicare che non è necessario aggiornare l'archivio delle performance. Se questo argomento è presente, il prompt per la posizione di archiviazione verrà eliminato.
-check	Se presente, lo script viene chiuso immediatamente dopo aver segnalato i conteggi degli indici.
-dryrun	Se presente, l'eseguibile di migrazione riporta le azioni che verranno intraprese (per migrare i dati e aggiornare le voci di archivio) ma non eseguirà le operazioni.

Panoramica del processo di aggiornamento di OnCommand Insight

Prima di iniziare l'aggiornamento di Insight, è importante comprendere il processo di aggiornamento. Il processo di aggiornamento è lo stesso per la maggior parte delle versioni di Insight.

Il processo di aggiornamento di Insight include le seguenti attività di alto livello:

- Scaricare i pacchetti di installazione
- Backup del database Data Warehouse

  Per evitare la possibilità di generare report errati dei dati, è necessario eseguire il backup del database Data Warehouse prima di eseguire il backup del database Insight.

- Backup del database Insight

  Il backup del database Insight viene eseguito automaticamente quando si esegue l'aggiornamento in-place. È consigliabile eseguire il backup del database prima dell'aggiornamento e collocarlo in una posizione diversa da quella del server Insight. Durante il processo di aggiornamento, Insight non raccoglie nuovi dati. Per ridurre al minimo la quantità di dati non raccolti, è necessario avviare il backup del database entro un'ora o due del tempo di aggiornamento pianificato.

- Eseguire il backup della configurazione di sicurezza Data Warehouse e Remote Acquisition Unit se la configurazione è stata modificata dalla configurazione predefinita.

  La configurazione di sicurezza non predefinita deve essere ripristinata nel Data Warehouse e nel server RAU al termine dell'aggiornamento e prima che il database Data Warehouse venga ripristinato nel sistema.

- Backup di report personalizzati di Data Warehouse

  Quando si esegue il backup del database Data Warehouse, vengono inclusi report personalizzati. Il file di backup viene creato sul server Data Warehouse. Si consiglia di eseguire il backup dei report personalizzati in una posizione diversa dal server Data Warehouse.

- Disinstallazione del software Data Warehouse e dell'unità di acquisizione remota, se applicabile

  Il server Insight dispone di un aggiornamento in-place; non è necessario disinstallare il software. L'aggiornamento in-place esegue il backup del database, disinstalla il software, installa la nuova versione e ripristina il database.

- Aggiornamento del software sul server Insight, sul data warehouse e sulle unità di acquisizione remota

  Tutte le licenze applicate in precedenza rimangono nel registro; non è necessario riapplicarle.

- Completamento delle attività di post-aggiornamento

Checklist per l'upgrade di OnCommand Insight

È possibile utilizzare gli elenchi di controllo forniti per registrare i progressi durante la preparazione all'aggiornamento. Queste attività hanno lo scopo di ridurre il rischio di errori di upgrade e accelerare le attività di recovery e ripristino.

Checklist per la preparazione all'aggiornamento (obbligatorio)

Condizione	Completato?
Assicurarsi di disporre delle autorizzazioni di amministratore locale di Windows, necessarie per eseguire il processo di aggiornamento, su tutti i server Insight.	
Se i server Insight, Data Warehouse o Remote Acquisition Unit risiedono su piattaforme a 32 bit, è necessario aggiornare i server alle piattaforme a 64 bit. A partire da Insight 7.x, gli aggiornamenti sono disponibili solo per le piattaforme a 64 bit.	

Assicurarsi di disporre delle autorizzazioni necessarie per modificare o disattivare il software antivirus su tutti i server dell'ambiente. Per evitare un errore di aggiornamento dovuto a un software di scansione virus attivo, è necessario escludere la directory di installazione Insight (`disk drive:\install directory\sanscreen` dall'accesso alla scansione antivirus durante l'aggiornamento. Dopo aver aggiornato tutti i componenti, è possibile riattivare il software antivirus in modo sicuro; tuttavia, assicurarsi di configurare la scansione in modo da escludere tutti i componenti presenti nella directory di installazione di Insight. Inoltre, è necessario escludere la cartella IBM/DB2 (ad esempio *C: Programmi IBM DB2*) dalla scansione antivirus dopo l'installazione.	

Checklist per la preparazione all'aggiornamento (Best practice)

Condizione	Completato?
Pianifica quando intendi eseguire l'upgrade, tenendo conto del fatto che la maggior parte degli aggiornamenti richiede un minimo di 4-8 ore; le aziende più grandi richiederanno più tempo. I tempi di aggiornamento possono variare in base alle risorse disponibili (architettura, CPU e memoria), alle dimensioni dei database e al numero di oggetti monitorati nell'ambiente.	
Contatta il tuo account representative per informazioni sui tuoi piani di aggiornamento e fornisci la versione di Insight installata e a quale versione desideri eseguire l'aggiornamento.	
Assicurarsi che le risorse correnti allocate a Insight, Data Warehouse e Remote Acquisition Unit soddisfino ancora le specifiche consigliate. Consulta le linee guida per il dimensionamento consigliato per tutti i server.in alternativa, puoi contattare il tuo rappresentante commerciale per discutere delle linee guida per il dimensionamento.	
Assicurarsi di disporre di spazio su disco sufficiente per il processo di backup e ripristino del database. I processi di backup e ripristino richiedono circa cinque volte lo spazio su disco utilizzato dal file di backup sui server Insight e Data Warehouse. Ad esempio, un backup da 50 GB richiede da 250 a 300 GB di spazio libero su disco.	

Assicurarsi di avere accesso a Firefox® o al browser Chrome™ quando si esegue il backup dei database Insight e Data Warehouse. Internet Explorer non è consigliato, perché si verificano alcuni problemi durante il caricamento e il download di file di dimensioni superiori a 4 GB.	
Eliminare `.tmp` File sul server Insight, che si trovano nella seguente posizione: `<install directory>\SANscreen\wildfly\standalone\tmp`.	
Rimuovere le origini dati duplicate e le origini dati decommissionate dal client Insight. La rimozione di origini dati dismesse o duplicate riduce il tempo necessario per eseguire l'aggiornamento e riduce l'opportunità di corruzione dei dati.	
Se sono stati modificati i report predefiniti forniti con Insight, è necessario salvarli con un nome diverso e salvarli nella cartella Report clienti in modo da non perdere il report modificato durante l'aggiornamento o il ripristino del sistema.	
Se si dispone di report personalizzati o modificati di Data Warehouse creati dall'utente o da servizi professionali, creare un backup di tali report esportandoli in XML e spostandoli nella cartella Report clienti. Assicurarsi che il backup non si trovi sul server Data Warehouse. Se i report non vengono spostati nelle cartelle consigliate, il processo di aggiornamento potrebbe non eseguire il backup di tali report. Per le versioni precedenti di Insight, la mancata individuazione dei report nelle cartelle appropriate può causare la perdita di report personalizzati e modificati.	
Registrare tutte le impostazioni nell'utility di configurazione di IBM Cognos, poiché non sono incluse nel backup di Data Warehouse; è necessario riconfigurare queste impostazioni dopo l'aggiornamento. L'utility si trova in `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` Sul server Data Warehouse ed è possibile eseguirlo utilizzando `cogconfigw` Command.in alternativa, è possibile eseguire un backup completo di Cognos e importare tutte le impostazioni. Per ulteriori informazioni, consultare la documentazione di IBM Cognos.	

Checklist per la preparazione all'aggiornamento (se applicabile)

Condizione	Completato?
Se sono stati sostituiti i certificati autofirmati creati dall'installazione di Insight a causa di avvisi di sicurezza del browser con certificati firmati dall'autorità di certificazione interna, eseguire il backup del file keystore, che si trova nella seguente posizione: `disk drive:\install directory\SANscreen\wildfly\standalone\configuration` e ripristinarlo dopo l'aggiornamento. Questo sostituisce i certificati autofirmati creati da Insight con i certificati firmati.	
Se una delle origini dati è stata modificata per l'ambiente in uso e non si è certi che queste modifiche siano disponibili nella versione Insight alla quale si sta eseguendo l'aggiornamento, creare una copia della seguente directory, che consente di risolvere eventuali problemi di ripristino: `disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war`.	
Eseguire il backup di tutte le tabelle e le viste del database personalizzate utilizzando `mysqldump` Tool della riga di comando.il ripristino di tabelle di database personalizzate richiede un accesso privilegiato al database. Contattare il supporto tecnico per assistenza sul ripristino di queste tabelle.	
Assicurarsi che non siano memorizzati in script di integrazione personalizzati, componenti di terze parti necessari per origini dati Insight, backup o altri dati richiesti `disk drive:\install directory\sanscreen` Poiché il contenuto di questa directory viene cancellato dal processo di aggiornamento.assicurarsi di spostare tali elementi da `\sanscreen` directory in un'altra posizione. Ad esempio, se l'ambiente contiene script di integrazione personalizzati, assicurarsi di copiare il seguente file in una directory diversa da `\sanscreen` directory: `\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt`.	

Download dei pacchetti di installazione di OnCommand Insight

È necessario scaricare i pacchetti di installazione per Insight, Data Warehouse e Remote

Acquisition Unit (se applicabile) prima del giorno in cui si sceglie di eseguire l'aggiornamento. Tempi di download dei pacchetti (`.msi` file) variano in base alla larghezza di banda disponibile.

A proposito di questa attività

È possibile scaricare i pacchetti di installazione utilizzando la WebUI Insight o accedendo al link OnCommand Insight appropriato all'indirizzo http://support.netapp.com/NOW/cgi-bin/software.

Per scaricare il pacchetto di installazione dal server Insight, procedere come segue:

Fasi

1. Aprire l'interfaccia utente Web di Insight aprendo un browser Web e immettendo una delle seguenti informazioni:
   - Sul server Insight: `https://localhost`
   - Da qualsiasi ubicazione: `https://IP Address:port or fqdn:port`

     Il numero della porta è 443 o la porta configurata al momento dell'installazione del server Insight. Il numero di porta predefinito è 443 se non si specifica il numero di porta nell'URL.
2. Accedi a Insight.
3. Fare clic sull'icona della Guida e selezionare **Controlla aggiornamenti**.
4. Se viene rilevata una versione più recente, seguire le istruzioni nella finestra del messaggio.

   Verrà visualizzata la pagina di descrizione dell'analisi per la versione più recente.
5. Nella pagina **Descrizione**, fare clic su **continua**.
6. Quando viene visualizzato il contratto di licenza con l'utente finale (EULA), fare clic su **Accept** (Accetta).
7. Fare clic sul collegamento al pacchetto di installazione per ciascun componente (server Insight, Data Warehouse, Remote Acquisition Unit), ecc.) e fare clic su **Save As** (Salva con nome) per salvare il pacchetto di installazione.

   Prima di eseguire l'aggiornamento, assicurarsi di copiare i pacchetti di installazione di Data Warehouse e Remote Acquisition Unit su dischi locali nei rispettivi server.
8. Fare clic su **CHECKSUM** e annotare i valori numerici associati a ciascun pacchetto di installazione.
9. Verificare che i pacchetti di installazione siano completi e senza errori dopo averli scaricati.

   I trasferimenti incompleti dei file possono causare problemi con il processo di aggiornamento.

   Per generare valori hash MD5 per i pacchetti di installazione, è possibile utilizzare un'utilità di terze parti come quella di Microsoft"File ChecksumIntegrity Verifier" utility.

Backup dei database

Prima di eseguire l'aggiornamento, è necessario eseguire il backup dei database Data Warehouse e OnCommand Insight. L'aggiornamento richiede un backup del database Data Warehouse in modo da poter ripristinare il database in un secondo momento del

processo di aggiornamento. L'aggiornamento in-place per Insight esegue il backup del database; tuttavia, è necessario eseguire il backup del database prima dell'aggiornamento come Best practice.

Per evitare errori di reporting dei dati, è necessario eseguire il backup del database Data Warehouse prima di eseguire il backup del database Insight. Inoltre, se si dispone di un ambiente di test, si consiglia di assicurarsi di poter ripristinare il backup prima di continuare con l'aggiornamento.

Backup del database Data Warehouse

È possibile eseguire il backup del database Data Warehouse, che include anche un backup di Cognos, su un file e ripristinarlo successivamente utilizzando il portale Data Warehouse. Un backup di questo tipo consente di migrare a un server Data Warehouse diverso o di eseguire l'aggiornamento a una nuova versione di Data Warehouse.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://fqdn/dwh`.
2. Dal riquadro di navigazione a sinistra, selezionare **Backup/Ripristino**.
3. Fare clic su **Backup** e selezionare la configurazione di backup:

   a. Tutti i Datamart tranne Performance Datamart

   b. Tutti i Datamart

   Questa operazione può richiedere 30 minuti o più.

   + Data Warehouse crea un file di backup e ne visualizza il nome.

4. Fare clic con il pulsante destro del mouse sul file di backup e salvarlo nella posizione desiderata.

   Potrebbe non essere necessario modificare il nome del file; tuttavia, è necessario memorizzare il file al di fuori del percorso di installazione di Data Warehouse.

   Il file di backup di Data Warehouse include MySQL dell'istanza DWH; schemi personalizzati (MySQL DBS) e tabelle; configurazione LDAP; origini dati che collegano Cognos al database MySQL (non le origini dati che collegano il server Insight ai dispositivi per acquisire dati); importazione ed esportazione di task che importavano o esportavano report; creazione di report su ruoli, gruppi e spazi dei nomi di sicurezza; account utente; Qualsiasi report modificato del portale di reporting e qualsiasi report personalizzato, indipendentemente dalla posizione in cui sono memorizzati, anche nella directory cartelle personali. Non viene eseguito il backup dei parametri di configurazione del sistema di Cognos, ad esempio le impostazioni del server SMTP e della memoria personalizzata di Cognos.

   Gli schemi predefiniti in cui viene eseguito il backup delle tabelle personalizzate includono quanto segue:

dwh_capacity
dwh_capacity_staging
dimensioni_dwh

dwh_fs_util
dwh_inventory
dwh_inventory_staging
dwh_inventory_transitori
gestione_dwh
dwh_performance
dwh_performance_staging
porte_dwh
report_dwh
dwh_sa_staging

Gli schemi in cui le tabelle personalizzate sono escluse dal backup includono quanto segue:

schema_informazioni
acquisizione
cloud_model
host_data
innodb
inventario
inventory_private
tempo_inventario
registri
gestione
mysql

nas
performance
schema_performance
performance_views
SANscreen
scrub
serviceassurance
test
tmp
banco di lavoro

In qualsiasi backup avviato manualmente, un `.zip` viene creato un file contenente i seguenti file:

- Un backup giornaliero `.zip` File, che contiene le definizioni dei report di Cognos
- Un backup dei report `.zip` File, che contiene tutti i report in Cognos, inclusi quelli nella directory cartelle personali
- Un file di backup del database Data Warehouse oltre ai backup manuali, che è possibile eseguire in qualsiasi momento, Cognos crea un backup giornaliero (generato automaticamente ogni giorno in un file chiamato `DailyBackup.zip`) che include le definizioni del report. Il backup giornaliero include le cartelle principali e i pacchetti forniti con il prodotto. La directory cartelle personali e le directory create al di fuori delle cartelle principali del prodotto non sono incluse nel backup di Cognos.

> A causa del modo in cui Insight nomina i file in `.zip` file, alcuni programmi di decompressione mostrano che il file è vuoto all'apertura. Fino a quando `.zip` il file ha una dimensione maggiore di 0 e non termina con a. `.bad` interno, il `.zip` il file è valido. È possibile aprire il file con un altro programma di decompressione come 7-zip o WinZip®.

Backup del database OnCommand Insight

Eseguire il backup del database Insight per assicurarsi di disporre di un backup recente se si verifica un problema dopo l'aggiornamento. Durante la fase di backup e ripristino, i dati relativi alle performance non vengono raccolti; pertanto, il backup deve avvenire il più vicino possibile al tempo di aggiornamento.

Fasi

1. Aprire Insight nel browser.
2. Fare clic su **Admin** > **Troubleshooting**.
3. Nella pagina **risoluzione dei problemi**, fare clic su **Backup**.

   Il tempo necessario per eseguire il backup del database può variare in base alle risorse disponibili (architettura, CPU e memoria), alle dimensioni del database e al numero di oggetti monitorati nell'ambiente.

   Una volta completato il backup, viene richiesto se si desidera scaricare il file.

4. Scaricare il file di backup.

Backup della configurazione di sicurezza

Quando i componenti Insight utilizzano una configurazione di sicurezza non predefinita, è necessario eseguire il backup della configurazione di sicurezza e ripristinare la configurazione su tutti i componenti dopo l'installazione del nuovo software. Prima di ripristinare il backup del database Data Warehouse, è necessario ripristinare la configurazione di sicurezza.

A proposito di questa attività

Si utilizza `securityadmin` per creare un backup della configurazione e ripristinare la configurazione salvata. Per ulteriori informazioni, cercare `securityadmin` Nel Centro documentazione OnCommand Insight: http://docs.netapp.com/oci-73/index.jsp

Backup dei report personalizzati di Data Warehouse

Se sono stati creati report personalizzati e non si dispone di `.xml` file di origine, quindi eseguire il backup di questi report prima dell'aggiornamento. Quindi, è necessario copiarli su un server diverso dal server Data Warehouse.

Fasi

1. Accedere al portale Data Warehouse all'indirizzo `https://fqdn/dwh`.
2. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire il portale di reporting ed effettuare l'accesso.
3. Selezionare **file** > **Apri**.
4. Selezionare la cartella in cui si trova il report, selezionarlo e fare clic su **Apri**.
5. Selezionare **Strumenti** > **Copia report negli Appunti**.
6. Aprire un editor di testo, incollare il contenuto del report e salvare il file con nome `report_name.txt`, dove `report _name` è il nome del report.
7. Memorizzare i report su un server diverso dal server Data Warehouse.

Esecuzione dell'aggiornamento del software

Dopo aver completato tutte le attività dei prerequisiti, è possibile aggiornare tutti i componenti Insight a una nuova release scaricando ed eseguendo il pacchetto di installazione applicabile su ciascun server.

Aggiornamento di Insight

Dopo aver completato tutte le attività dei prerequisiti, accedere al server Insight ed eseguire il pacchetto di installazione per completare l'aggiornamento. Il processo di aggiornamento disinstalla il software esistente, installa il nuovo software e riavvia il server.

Prima di iniziare

Il pacchetto di installazione di Insight deve trovarsi sul server.

Fasi

1. Accedere al server Insight utilizzando un account che dispone delle autorizzazioni di amministratore locale di Windows.
2. Individuare il pacchetto di installazione Insight (`SANscreenServer-x64-version_number-build_number.msi`) Utilizzando Esplora risorse e fare doppio clic su di esso.

   Viene visualizzata la procedura guidata di installazione guidata di OnCommand.
3. Spostare la finestra di avanzamento dal centro dello schermo e allontanarla dalla finestra dell'installazione guidata **Setup** in modo che gli errori generati non vengano nascosti.
4. Seguire le istruzioni dell'installazione guidata.

   Si consiglia di lasciare selezionate tutte le impostazioni predefinite.

Al termine

Per verificare se l'aggiornamento è stato eseguito correttamente o se sono stati generati errori, controllare il log di aggiornamento nella seguente posizione: `<install directory>\SANscreen\wildfly\standalone\log`.

Aggiornamento del data warehouse

Dopo aver completato tutte le attività dei prerequisiti, è possibile accedere al server Data Warehouse ed eseguire il pacchetto di installazione per completare l'aggiornamento.

A proposito di questa attività

L'aggiornamento inline non è supportato dal Data Warehouse (DWH). Per eseguire l'aggiornamento alla nuova versione del software DWH, procedere come segue.

Quando si aggiorna DWH, la cartella contenente il backup del vault dello strumento *securityadmin* viene eliminata. Si consiglia vivamente di eseguire il backup del vault prima di aggiornare DWH. Per riferimento, le cartelle predefinite del vault sono le seguenti:

- Cartella del vault (vault in uso):`%SANSCREEN_HOME%\wildfly\standalone\configuration\vault`
- Backup del vault: `%SANSCREEN_HOME%\backup\vault`

Vedere "Gestione della sicurezza nel Data Warehouse" per ulteriori informazioni.

Fasi

1. Accedere al server DWH utilizzando un account che dispone delle autorizzazioni di amministratore locale di Windows.
2. Eseguire il backup di DWH DB e Reports utilizzando l'interfaccia del portale DWH.
3. Eseguire il backup della configurazione di protezione se il server utilizza una configurazione di protezione non predefinita.
4. Disinstallare il software DWH dal server.
5. Riavviare il server per rimuovere i componenti dalla memoria.
6. Installare la nuova versione di DWH sul server.

   L'installazione richiede circa 2 ore. Si consiglia di lasciare selezionate tutte le impostazioni predefinite.

7. Ripristinare la configurazione di sicurezza non predefinita sul server DWH.
8. Ripristinare il database DWH sul server.

Al termine

Dopo l'aggiornamento, è necessario ripristinare il database Data Warehouse, che può richiedere più tempo o meno dell'aggiornamento.

Durante un aggiornamento di OnCommand Insight, non è raro che un cliente passi a un server Insight diverso. Se il server Insight è stato modificato, dopo il ripristino del database del data warehouse i connettori esistenti puntano all'indirizzo IP o al nome host del server precedente. Si consiglia di eliminare il connettore e crearne uno nuovo, per evitare possibili errori.

Conservazione delle impostazioni Cognos personalizzate durante un aggiornamento del Data Warehouse

Le impostazioni Cognos personalizzate, come le impostazioni e-mail SMTP non predefinite, non vengono automaticamente sottoposte a backup come parte di un aggiornamento di Data Warehouse. È necessario documentare e ripristinare manualmente le impostazioni personalizzate dopo un aggiornamento.

Prima di aggiornare Data Warehouse, preparare un elenco di controllo con tutte le impostazioni Cognos personalizzate che si desidera conservare e rivedere l'elenco prima di aggiornare il sistema. Una volta completato l'aggiornamento, è possibile ripristinare manualmente i valori per ripristinarli nelle impostazioni della configurazione originale.

Backup della configurazione di sicurezza

Quando l'ambiente Insight utilizza una configurazione di sicurezza non predefinita, è necessario eseguire il backup della configurazione di sicurezza e ripristinare la configurazione di sicurezza dopo l'installazione del nuovo software. Prima di ripristinare il backup del database Data Warehouse, è necessario ripristinare la configurazione di sicurezza.

A proposito di questa attività

Si utilizza `securityadmin` per creare un backup della configurazione e ripristinare la configurazione salvata. Per ulteriori informazioni, cercare `securityadmin` Nel Centro documentazione OnCommand Insight: http://docs.netapp.com/oci-73/index.jsp

Aggiornamento dei server delle unità di acquisizione remota

Dopo aver completato tutte le attività dei prerequisiti, è possibile accedere al server dell'unità di acquisizione remota ed eseguire il pacchetto di installazione per completare l'aggiornamento. Questa attività deve essere eseguita su tutti i server di acquisizione remoti del proprio ambiente.

Prima di iniziare

- È necessario aver aggiornato OnCommand Insight.
- Il pacchetto di installazione di OnCommand Insight deve trovarsi sul server.

Fasi

1. Accedere al server dell'unità di acquisizione remota utilizzando un account che dispone delle autorizzazioni di amministratore locale di Windows.
2. Individuare il pacchetto di installazione Insight (`RAU-x64-version_number-build_number.msi`) Utilizzando Esplora risorse e fare doppio clic su di esso.

   Viene visualizzata l'installazione guidata di OnCommand Insight.
3. Spostare la finestra di avanzamento dell'installazione guidata dal centro della schermata e allontanarla dalla finestra dell'installazione guidata in modo che gli errori generati non vengano nascosti.
4. Seguire le istruzioni dell'installazione guidata.

   Si consiglia di lasciare selezionate tutte le impostazioni predefinite.

Al termine

- Per verificare se l'aggiornamento è stato eseguito correttamente o se sono stati generati errori, controllare il log di aggiornamento nella seguente posizione: `<install directory>\SANscreen\bin\log`.
- Utilizzare `securityadmin` tool per ripristinare la sicurezza salvata

  configurazione. Per ulteriori informazioni, cercare securityadmin in OnCommand Insight

  Centro di documentazione: http://docs.netapp.com/oci-73/index.jsp

- Cancellare la cache e la cronologia del browser per assicurarsi di ricevere i dati più recenti dal server.

Completamento delle attività post-aggiornamento

Dopo aver eseguito l'aggiornamento alla versione più recente di Insight, è necessario completare attività aggiuntive.

Installazione delle patch di origine dati

Se applicabile, è necessario installare le patch più recenti disponibili per le origini dati per sfruttare le funzionalità e i miglioramenti più recenti. Dopo aver caricato una patch di origine dati, è possibile installarla su tutte le origini dati dello stesso tipo.

Prima di iniziare

Devi aver contattato il supporto tecnico e aver ottenuto il `.zip` che contiene le patch di origine dati più recenti, fornendo la versione da cui si sta eseguendo l'aggiornamento e la versione da cui si desidera eseguire l'aggiornamento.

Fasi

1. Posizionare il file di patch sul server Insight.
2. Nella barra degli strumenti Insight, fare clic su **Admin**.
3. Fare clic su **Patch**.
4. Dal pulsante Actions (azioni), selezionare **Apply patch** (Applica patch).
5. Nella finestra di dialogo **Apply data source patch** (Applica patch origine dati), fare clic su **Browse** (Sfoglia) per individuare il file di patch caricato.
6. Esaminare i tipi di origine dei dati * * Patch name*, * Description* e * interessati*.
7. 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. Insight impone automaticamente il riavvio dell'acquisizione quando si aggiunge un'origine dati. Il rilevamento include il rilevamento delle modifiche nella topologia di rete, inclusa l'aggiunta o l'eliminazione di nodi o interfacce.

8. Per forzare il processo di rilevamento manualmente, fare clic su **origini dati** e fare clic su **Esegui nuovamente il polling** accanto all'origine dati per forzare la raccolta dei dati immediatamente.

   Se l'origine dati è già in un processo di acquisizione, Insight ignora la richiesta di nuovo polling.

Sostituzione di un certificato dopo l'aggiornamento di OnCommand Insight

L'apertura dell'interfaccia utente Web di OnCommand Insight dopo un aggiornamento genera un avviso di certificazione. Il messaggio di avviso viene visualizzato perché un certificato autofirmato valido non è disponibile dopo l'aggiornamento. Per evitare che il messaggio di avviso venga visualizzato in futuro, è possibile installare un certificato autofirmato valido per sostituire il certificato originale.

Prima di iniziare

Il sistema deve soddisfare il livello minimo di crittografia (1024 bit).

A proposito di questa attività

L'avviso di certificazione non influisce sull'usabilità del sistema. Quando viene visualizzato il messaggio, è possibile indicare di aver compreso il rischio e quindi di utilizzare Insight.

Fasi

1. 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"`

   Quando viene richiesta una password, immettere `changeit`.

   Deve essere presente almeno un certificato nel keystore, `ssl certificate`.

2. Eliminare `ssl certificate`: `keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`
3. Generare una nuova chiave: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\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.
4. Generare un file di richiesta del certificato: `keytool -certreq -alias localhost -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.

5. 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.

6. Importare il certificato approvato: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
   a. Quando viene richiesta una password, inserire la password del keystore.

      Il sistema visualizza il seguente messaggio: `Certificate reply was installed in keystore`

7. Riavviare il servizio del server SANscreen.

Risultati

Il browser Web non riporta più avvisi di certificato.

Aumento della memoria Cognos

Prima di ripristinare il database Data Warehouse, è necessario aumentare l'allocazione Java per Cognos da 768 MB a 2048 MB per ridurre il tempo di generazione dei report.

Fasi

1. Aprire una finestra del prompt dei comandi come amministratore sul server Data Warehouse.
2. Passare a. `disk drive:\install directory\SANscreen\cognos\c10_64\bin64` directory.
3. Digitare il seguente comando: `cogconfigw`

   Viene visualizzata la finestra IBM Cognos Configuration (Configurazione IBM Cognos).

   > L'applicazione di scelta rapida IBM Cognos Configuration punta a. `disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat`. Se Insight è installato nella directory Program Files (spazio tra), che è l'impostazione predefinita, invece di ProgramFiles (senza spazio), il `.bat` il file non funziona. In questo caso, fare clic con il pulsante destro del mouse sul collegamento dell'applicazione e modificare `cognosconfigw.bat` a. `cognosconfig.exe` per correggere il collegamento.

4. Dal riquadro di navigazione a sinistra, espandere **ambiente**, espandere **servizi IBM Cognos**, quindi fare clic su **IBM Cognos**.
5. Selezionare **memoria massima per Tomcat in MB** e modificare da 768 MB a 2048 MB.
6. Nella barra degli strumenti di configurazione di IBM Cognos, fare clic su (Salva).

   Viene visualizzato un messaggio informativo per informare dell'esecuzione delle attività di Cognos.

7. Fare clic su **Chiudi**.
8. Nella barra degli strumenti di configurazione di IBM Cognos, fare clic su (Stop).
9. Nella barra degli strumenti di configurazione di IBM Cognos, fare clic su (Inizio).

Ripristino del database Data Warehouse

Quando si esegue il backup del database Data Warehouse, Data Warehouse crea un `.zip` file che è possibile utilizzare in seguito per ripristinare lo stesso database.

A proposito di questa attività

Quando si ripristina il database Data Warehouse, è possibile ripristinare anche le informazioni dell'account utente dal backup. Le tabelle di gestione degli utenti vengono utilizzate dal motore di report Data Warehouse in un'installazione solo Data Warehouse.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://fqdn/dwh`.
2. Dal riquadro di navigazione a sinistra, fare clic su **Backup/Restore**.
3. Nella sezione **Restore Database and Reports** (Ripristina database e report), fare clic su **Browse** (Sfoglia) e individuare `.zip` File che contiene il backup del Data Warehouse.
4. È consigliabile lasciare entrambe le seguenti opzioni selezionate:
   - **Ripristinare il database**

     Include le impostazioni del Data Warehouse, i data mart, le connessioni e le informazioni sull'account utente.

   - **Ripristina report**

     Include report personalizzati, report predefiniti, modifiche apportate ai report predefiniti e impostazioni di reporting effettuate in Reporting Connection.
5. Fare clic su **Restore** (Ripristina).

   Non allontanarsi dallo stato di ripristino. In questo caso, lo stato di ripristino non viene più visualizzato e non viene visualizzata alcuna indicazione al termine dell'operazione di ripristino.
6. Per controllare il processo di aggiornamento, consultare `dwh_upgrade.log` file, che si trova nella seguente posizione: `<install directory>\SANscreen\wildfly\standalone\log`.

   Al termine del processo di ripristino, viene visualizzato un messaggio sotto il pulsante **Restore** (Ripristina). Se il processo di ripristino ha esito positivo, viene visualizzato il messaggio Success (riuscito). Se il processo di ripristino non riesce, il messaggio indica l'eccezione specifica che ha causato l'errore. In questo caso, contattare il supporto tecnico e fornirgli `dwh_upgrade.log` file. Se si verifica un'eccezione e l'operazione di ripristino non riesce, il database originale viene ripristinato automaticamente.

   > Se l'operazione di ripristino non riesce e viene visualizzato il messaggio "Failed upding cognos content store" (aggiornamento archivio contenuti cognos non riuscito), ripristinare il database Data Warehouse senza i relativi report (solo database) e utilizzare i backup dei report XML per importare i report.

Ripristino di report personalizzati di Data Warehouse

Se applicabile, è possibile ripristinare manualmente tutti i report personalizzati di cui è stato eseguito il backup prima dell'aggiornamento; tuttavia, è necessario eseguire questa

operazione solo se si perdono i report di se sono stati danneggiati.

Fasi

1. Aprire il report con un editor di testo, quindi selezionarne e copiarne il contenuto.
2. Accedere al portale di reporting all'indirizzo `https://fqdn/reporting`.
3. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire il portale Insight Reporting.
4. Dal menu Avvio, selezionare **Report Studio**.
5. Selezionare qualsiasi pacchetto.

   Viene visualizzato Report Studio.

6. Fare clic su **Crea nuovo**.
7. Selezionare **elenco**.
8. Dal menu Strumenti, selezionare **Apri report dagli Appunti**.

   Viene visualizzata la finestra di dialogo **Apri report dagli Appunti**.

9. Dal menu file, selezionare **Salva con nome** e salvare il report nella cartella rapporti personalizzati.
10. Aprire il report per verificare che sia stato importato.

    Ripetere questa attività per ciascun report.

> Potrebbe essere visualizzato un "errore di analisi dell'espressione" quando si carica un report. Ciò significa che la query contiene un riferimento ad almeno un oggetto non esistente, il che significa che non è stato selezionato alcun pacchetto nella finestra origine per validare il report. In questo caso, fare clic con il pulsante destro del mouse su una dimensione del data mart nella finestra Source (origine), selezionare Report Package (pacchetto report), Quindi selezionare il pacchetto associato al report (ad esempio, il pacchetto di inventario se si tratta di un report di inventario o di uno dei pacchetti di performance se si tratta di un report sulle performance) in modo che Report Studio possa convalidarlo e quindi salvarlo.

Verificare che Data Warehouse disponga di dati storici

Dopo aver ripristinato i report personalizzati, è necessario verificare che Data Warehouse stia raccogliendo dati storici visualizzando i report personalizzati.

Fasi

1. Accedere al portale Data Warehouse all'indirizzo `https://fqdn/dwh`.
2. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire il portale Insight Reporting ed effettuare l'accesso.
3. Aprire la cartella contenente i report personalizzati (ad esempio, Report personalizzati).
4. Fare clic su per aprire le opzioni del formato di output per questo report.
5. Selezionare le opzioni desiderate e fare clic su **Esegui** per assicurarsi che siano popolate con dati storici di storage, calcolo e switch.

Ripristino dell'archivio delle performance

Per i sistemi che eseguono l'archiviazione delle performance, il processo di aggiornamento ripristina solo sette giorni di dati di archivio. Una volta completato l'aggiornamento, è possibile ripristinare i dati di archivio rimanenti.

A proposito di questa attività

Per ripristinare l'archivio delle prestazioni, attenersi alla procedura descritta di seguito.

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.

Verifica dei connettori

Dopo l'aggiornamento, verificare i connettori per assicurarsi di disporre di una connessione tra il data warehouse OnCommand Insight e il server OnCommand Insight.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://fqdn/dwh`.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.
3. Selezionare il primo connettore.

   Viene visualizzata la pagina Edit Connector (Modifica connettore).

4. Fare clic su **Test**.
5. Se il test ha esito positivo, fare clic su **Close** (Chiudi); in caso contrario, inserire il nome del server Insight nel campo **Name** (Nome) e il relativo indirizzo IP nel campo **host** (host), quindi fare clic su **Test** (Test).
6. Una volta stabilita la connessione tra il Data Warehouse e il server Insight, fare clic su **Save** (Salva).

   In caso contrario, controllare la configurazione della connessione e assicurarsi che il server Insight non presenti problemi.

7. Fare clic su **Test**.

   Data Warehouse verifica la connessione.

Verifica della pianificazione di estrazione, trasformazione e caricamento

Dopo l'aggiornamento, assicurarsi che il processo di estrazione, trasformazione e caricamento (ETL) stia recuperando i dati dai database OnCommand Insight, trasformandoli e salvandoli nei data mart.

Fasi

1. Accedere al portale Data Warehouse all'indirizzo `https://fqdn/dwh`.
2. Dal riquadro di navigazione a sinistra, fare clic su **Schedule** (Pianificazione).
3. Fare clic su **Modifica pianificazione**.
4. Selezionare **giornaliero** o **settimanale** dall'elenco **tipo**.

   Si consiglia di programmare l'esecuzione di ETL una volta al giorno.

5. Verificare che l'ora selezionata sia l'ora in cui si desidera eseguire il lavoro.

   In questo modo, il processo di creazione viene eseguito automaticamente.

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

Aggiornamento dei modelli di dischi

Dopo l'aggiornamento, è necessario disporre di modelli di dischi aggiornati; tuttavia, se per qualche motivo Insight non è riuscito a rilevare nuovi modelli di dischi, è possibile aggiornarli manualmente.

Prima di iniziare

È necessario aver ottenuto dal supporto tecnico `.zip` file che contiene le patch più recenti per l'origine dei dati.

Fasi

1. Arrestare il servizio SANscreen acq.
2. Accedere alla seguente directory: `<install directory>\SANscreen\wildfly\standalone\deployments\datasources.war`.
3. Spostare la corrente `diskmodels.jar` file in una posizione diversa.
4. Copiare il nuovo `diskmodels.jar` file in `datasources.war` directory.
5. Avviare il servizio SANscreen acq.

Verifica dell'esecuzione degli strumenti di business intelligence

Se applicabile, è necessario verificare che i propri strumenti di business intelligence siano in esecuzione e che i dati vengano recuperati dopo l'aggiornamento.

Verificare che gli strumenti di business intelligence come BMC Atrium e ServiceNow siano in esecuzione e in grado di recuperare i dati. Ciò include BMC Connector e le soluzioni che sfruttano REST.

Risoluzione dei problemi di un aggiornamento

Se si verificano problemi dopo un aggiornamento del OnCommand Insight, potrebbe essere utile consultare le informazioni per la risoluzione dei problemi relative ad alcuni possibili problemi.

Impossibile avviare Cognos dal menu Start di Windows

L'esistenza di uno spazio prima `\SANscreen\cognos` nel nome del percorso è un problema. Per ulteriori informazioni, consulta la community NetApp Customer Success: https://forums.netapp.com/thread/62721.

Messaggio di errore "Not a valid win32 application" (applicazione win32 non valida)

Si tratta di un problema con Microsoft Windows. Per risolvere questo problema, è necessario inserire delle virgolette intorno al percorso dell'immagine nel registro. Per ulteriori informazioni, consultare la seguente documentazione: https://support.microsoft.com/en-us/kb/812486/en-us.

Le annotazioni non sono presenti

Quando un processo ETL di Data Warehouse richiede annotazioni da un'istanza Insight, a volte riceve una risposta vuota (risultato 0) per errore. Questo errore determina lo spostamento delle annotazioni per alcuni oggetti tra uno stato "presente" e "non presente" in Data Warehouse. Per ulteriori informazioni, vedere quanto segue: https://forums.netapp.com/docs/DOC-44167

Differenze nei valori visualizzati nei report

Prima del 7.0, i report erano basati su numeri interi. Sono ora basati su cifre decimali; pertanto, dopo l'aggiornamento, si potrebbe notare un aumento o una diminuzione della visualizzazione dei valori.

I dati non vengono visualizzati nei report

Nella versione 7.0.1, sono stati modificati diversi nomi di modelli (ad esempio, Symmetrix è stato modificato in Symmetrix VMAX). Di conseguenza, se un report contiene un filtro per "Symmetrix", non verranno visualizzati dati quando si esegue il report. Per modificare il report, aprire il report con Query Explorer in Report Studio, cercare il nome del modello, sostituirlo con il nuovo nome del modello e salvare il report.

Disinstallazione del software

Per installare le nuove versioni, è necessario disinstallare le versioni precedenti del software Data Warehouse e Remote Acquisition. Questa operazione deve essere eseguita prima di tentare di aggiornare uno qualsiasi di questi componenti. Il software sul server Insight viene disinstallato durante l'aggiornamento in-place.

Disinstallazione del server OnCommand Insight

Se necessario, è possibile disinstallare il server OnCommand Insight.

Prima di iniziare

Procedura consigliata: Prima di disinstallare Insight, eseguire il backup del database OnCommand Insight.

Fasi

1. Accedere al server OnCommand Insight utilizzando un account con privilegi di amministratore.
2. Assicurarsi che tutte le finestre Insight sul server siano chiuse.
3. Aprire la funzione **Disinstalla un programma** dal pannello di controllo e selezionare l'applicazione OnCommand Insight da rimuovere.

4. Fare clic su **Disinstalla** e seguire le istruzioni.

Disinstallazione del software Data Warehouse

Prima di eseguire l'aggiornamento, è necessario disinstallare il software Data Warehouse.

Prima di iniziare

Se sono state apportate modifiche ai report che si desidera conservare, è fondamentale creare un backup prima di disinstallare Data Warehouse. La disinstallazione di Data Warehouse elimina in modo permanente tutti i dati precedentemente raccolti e rimuove tutti i report, inclusi quelli appena creati o modificati.

Fasi

1. Accedere al server Data Warehouse.
2. Assicurarsi che tutte le finestre Insight sul server siano chiuse.
3. Per eseguire la disinstallazione utilizzando il pannello di controllo:
   a. Aprire **Disinstalla un programma** dal pannello di controllo e selezionare l'applicazione OnCommand Insight da rimuovere. Fare clic su **Disinstalla** e seguire le istruzioni.
   b. Selezionare l'applicazione IBM DB2 da rimuovere. Fare clic su **Disinstalla** e seguire le istruzioni.
   c. Eliminare la cartella di installazione DB2 (ad esempio *C: File di programma IBM DB2*) per rimuovere completamente il database DB2.
4. Per eseguire la disinstallazione utilizzando lo script fornito:
   a. Accedere alla cartella *<download location>_dwh_uninstall* ed eseguire lo script *uninstall_oci_dwh.bat*.
5. Riavviare il server.

Disinstallazione del software dell'unità di acquisizione remota

Prima di eseguire l'aggiornamento a una nuova versione, è necessario disinstallare la versione esistente del software dell'unità di acquisizione remota. Questa attività deve essere eseguita su tutti i server delle unità di acquisizione remote del proprio ambiente.

Fasi

1. Accedere al server dell'unità di acquisizione remota.
2. Assicurarsi che tutte le finestre di OnCommand Insight sul server siano chiuse.
3. Aprire la funzione **Disinstalla un programma** dal pannello di controllo e selezionare il programma dell'unità di acquisizione remota OnCommand Insight da rimuovere.
4. Fare clic su **Disinstalla** e seguire le istruzioni.

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:

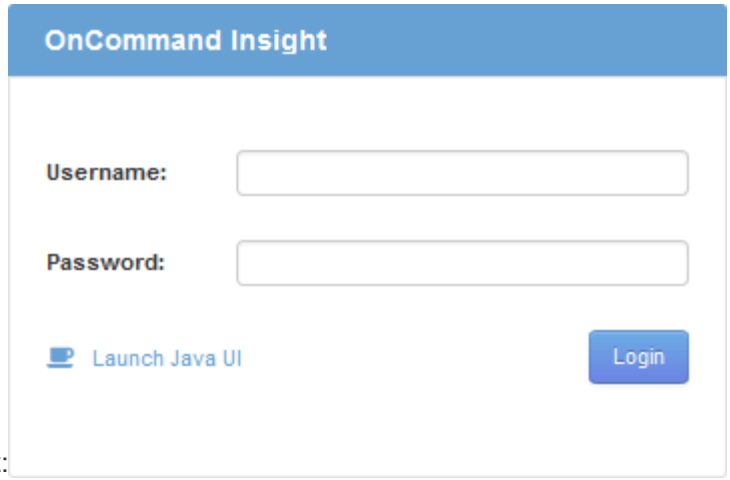
     `https://fqdn`

   - 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.

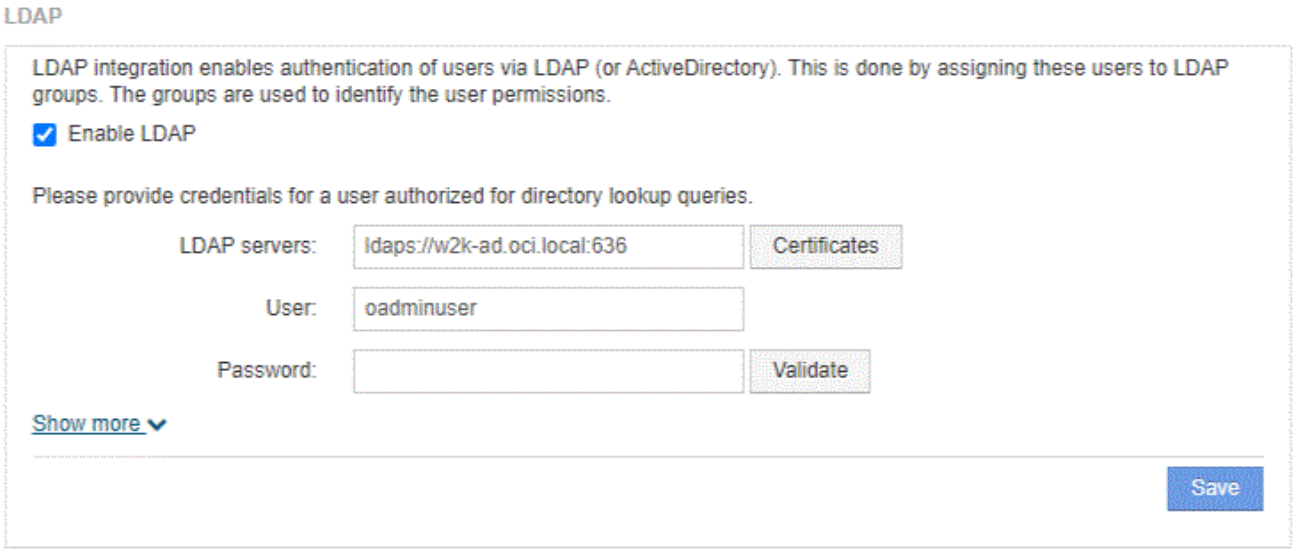
A proposito di questa attività

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.

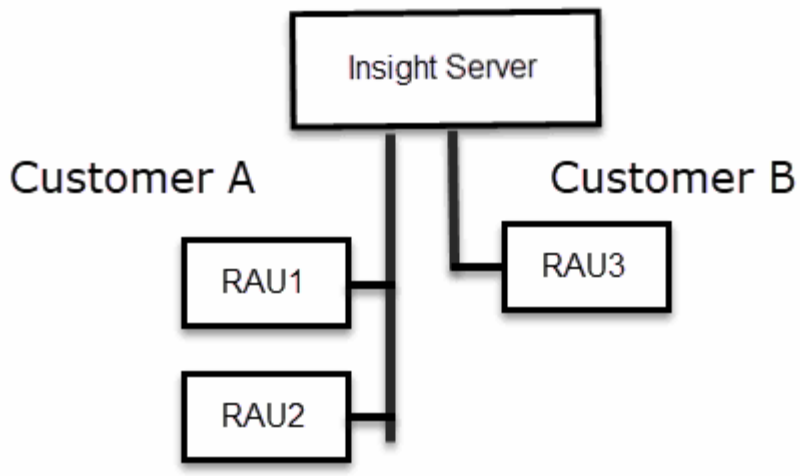
Considerazioni sull'aggiornamento e l'installazione

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.

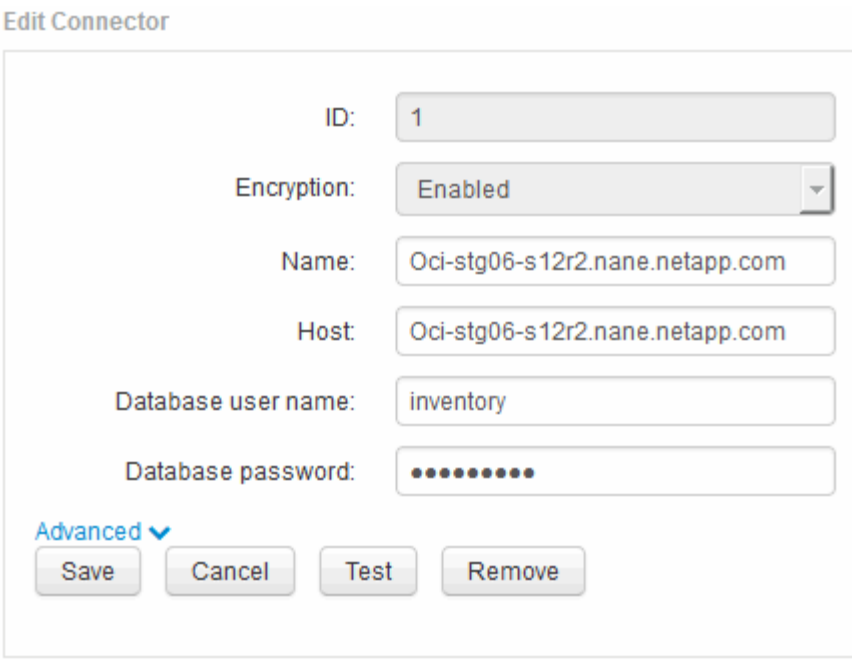
Prima di iniziare

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

Fasi

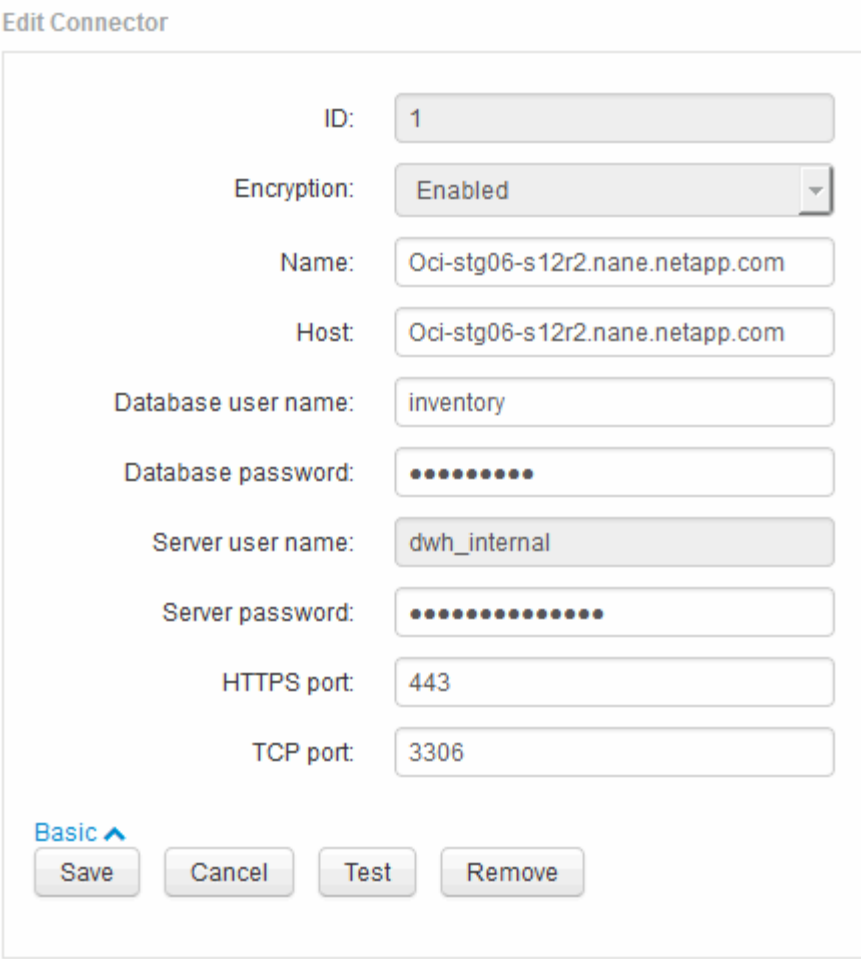
1. Accedere al Data Warehouse Portal all'indirizzo https://hostname/dwh, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

   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.

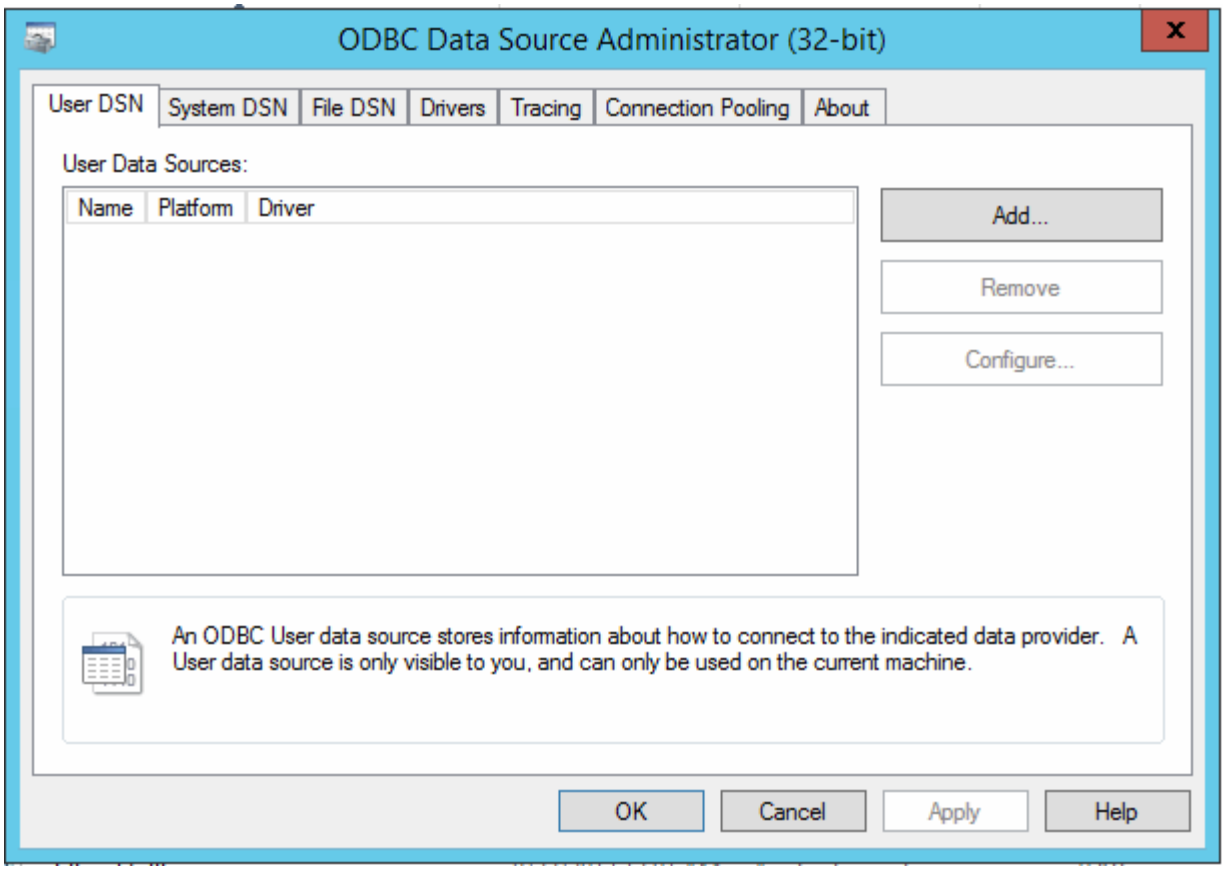
Prima di iniziare

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

Fasi

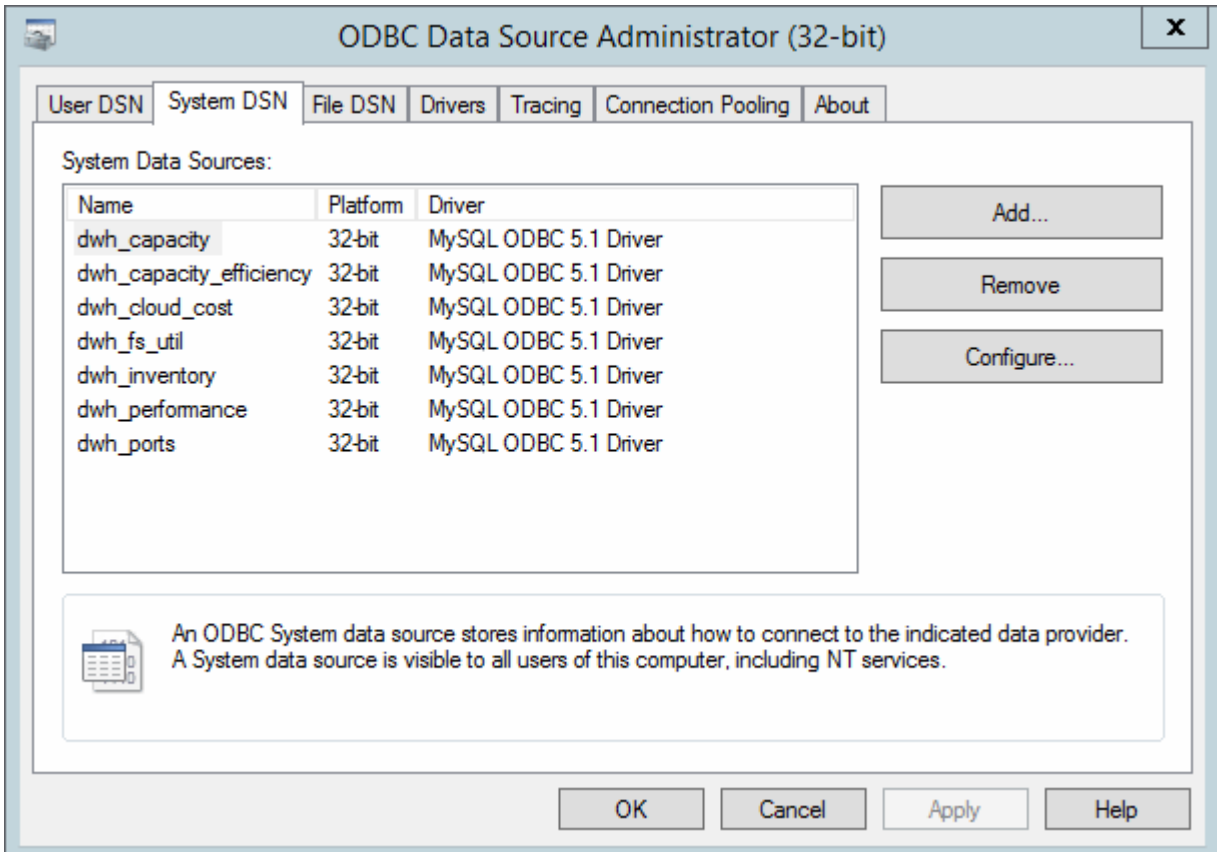
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

   Viene visualizzata la schermata Amministratore origine dati ODBC.



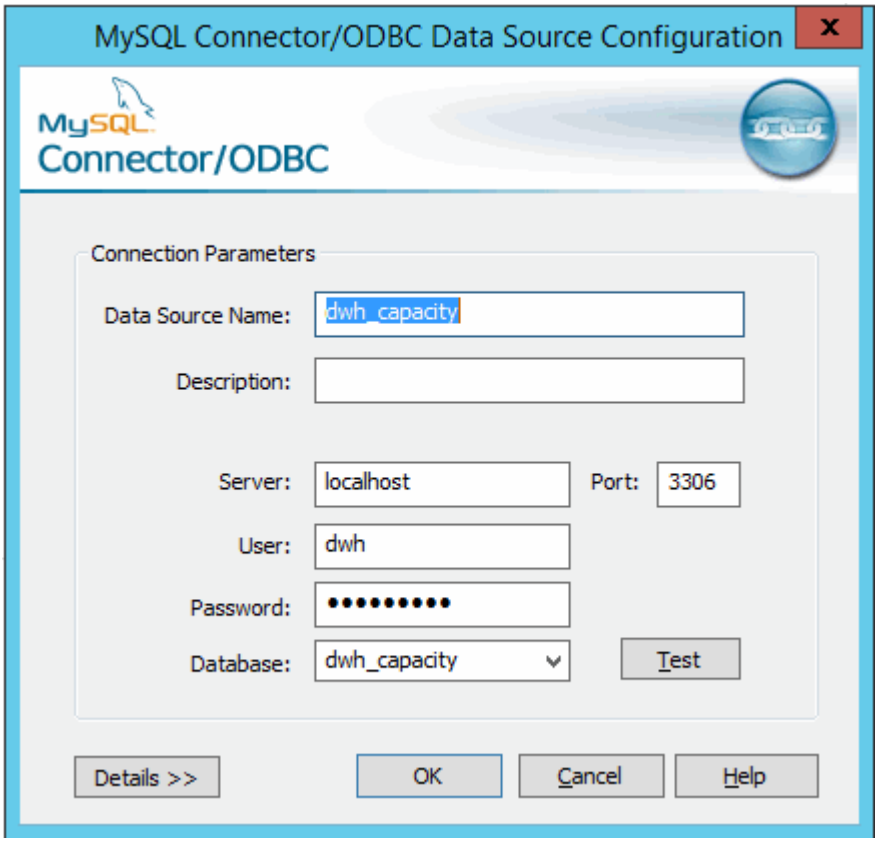
3. Fare clic su **DSN di sistema**

   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.

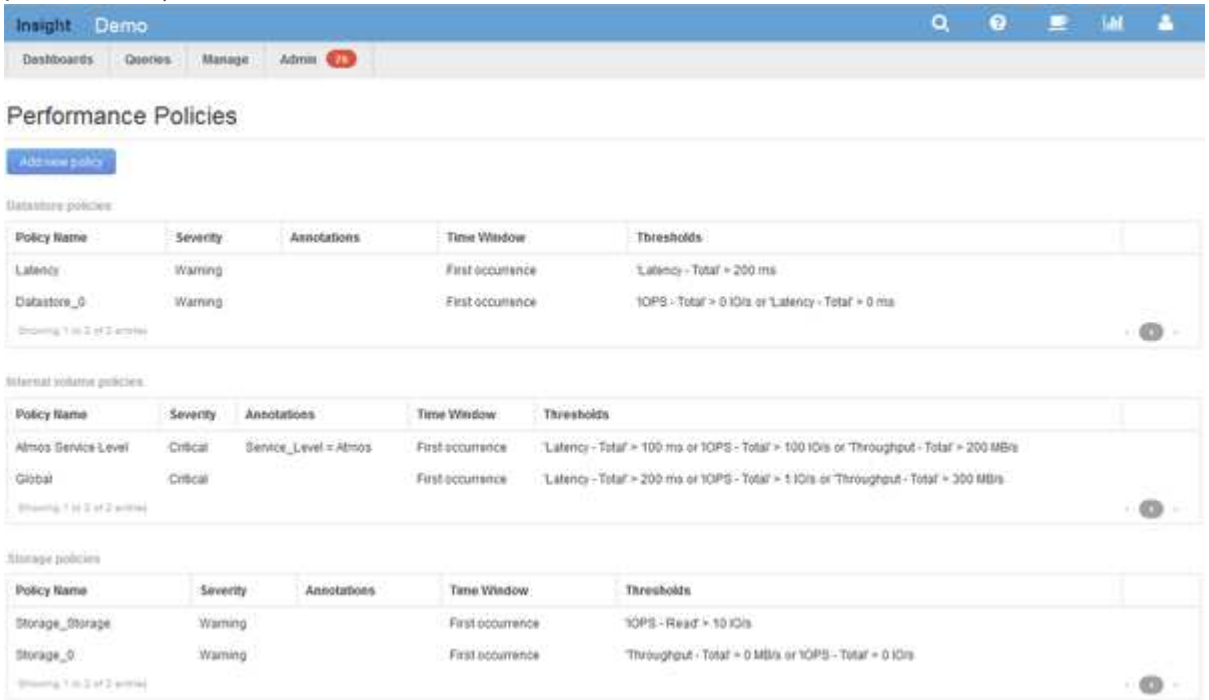
Creazione di policy sulle performance

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.

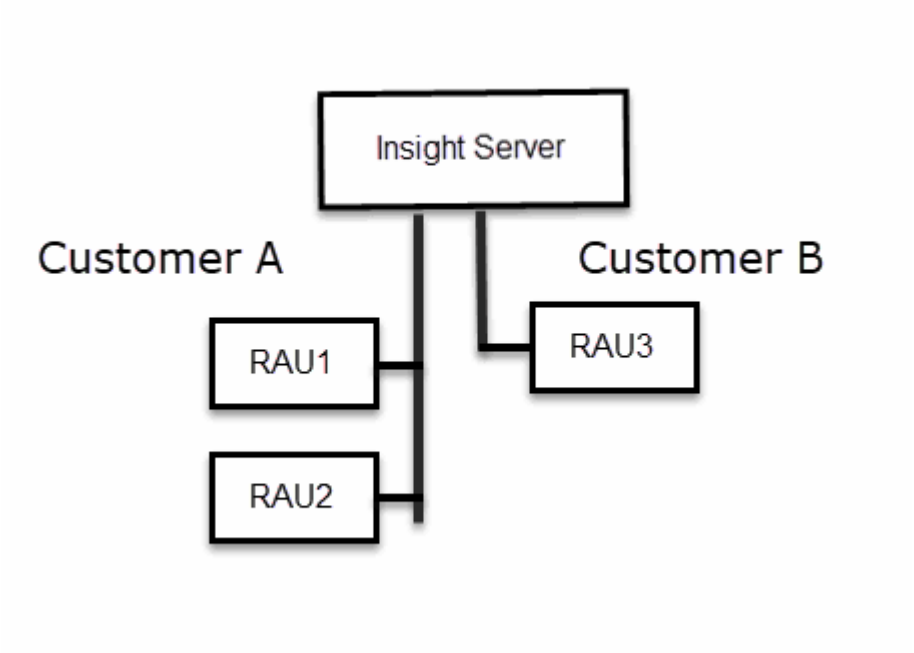
Considerazioni sull'aggiornamento e l'installazione

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.

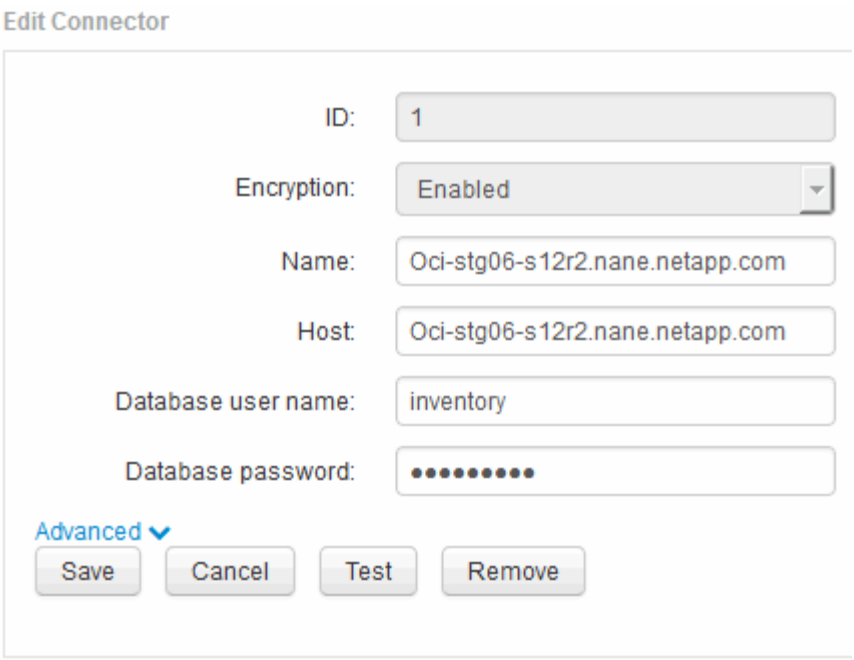
Prima di iniziare

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

Fasi

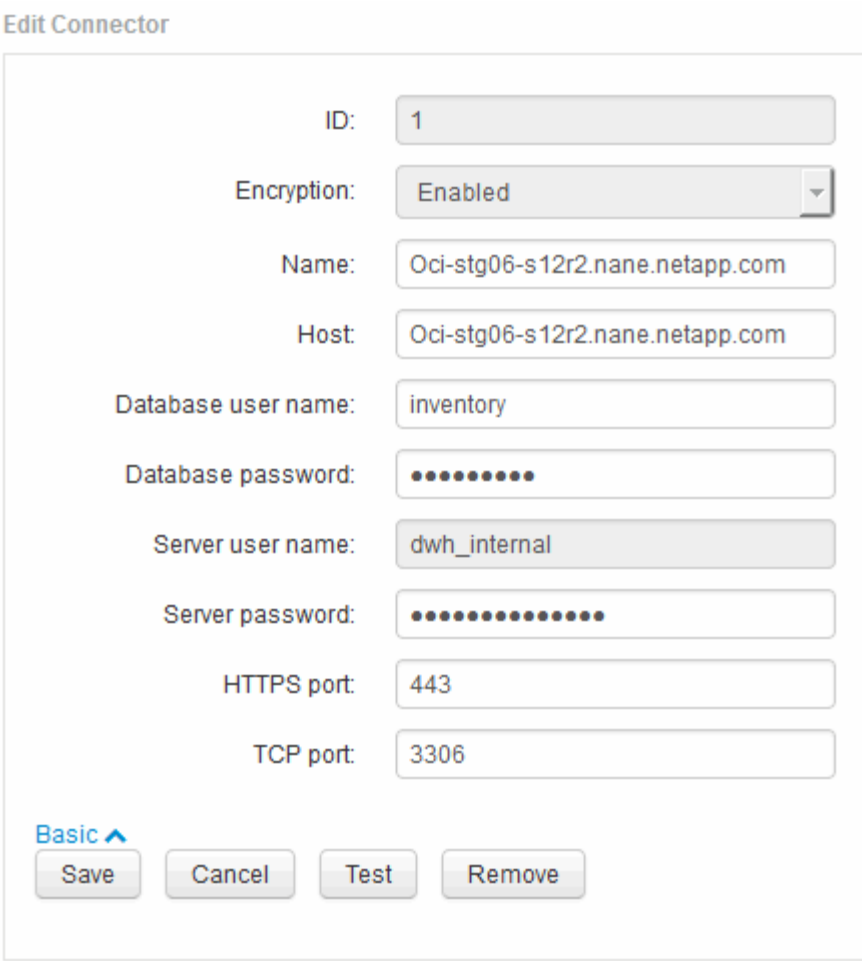
1. Accedere al Data Warehouse Portal all'indirizzo https://hostname/dwh, Dove hostname è il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **connettori**.

   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.

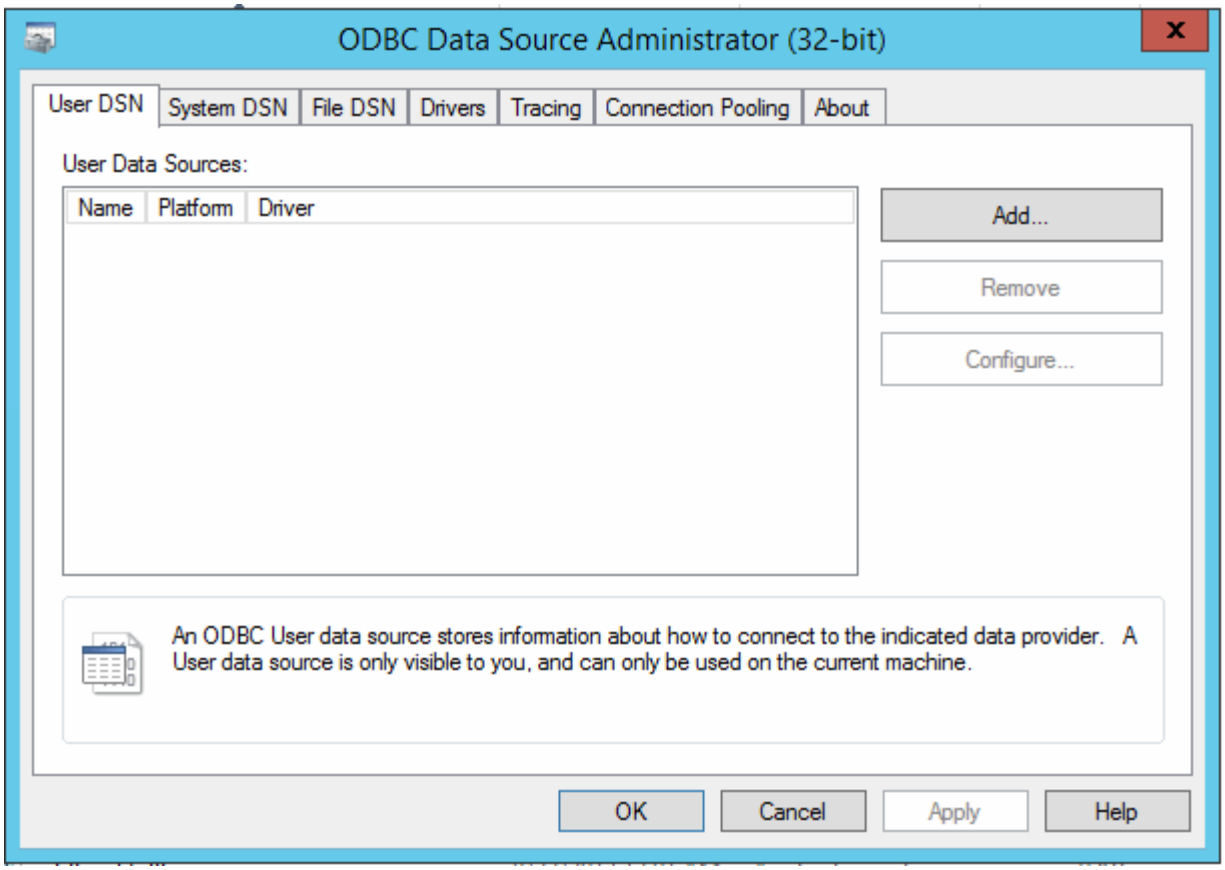
Prima di iniziare

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

Fasi

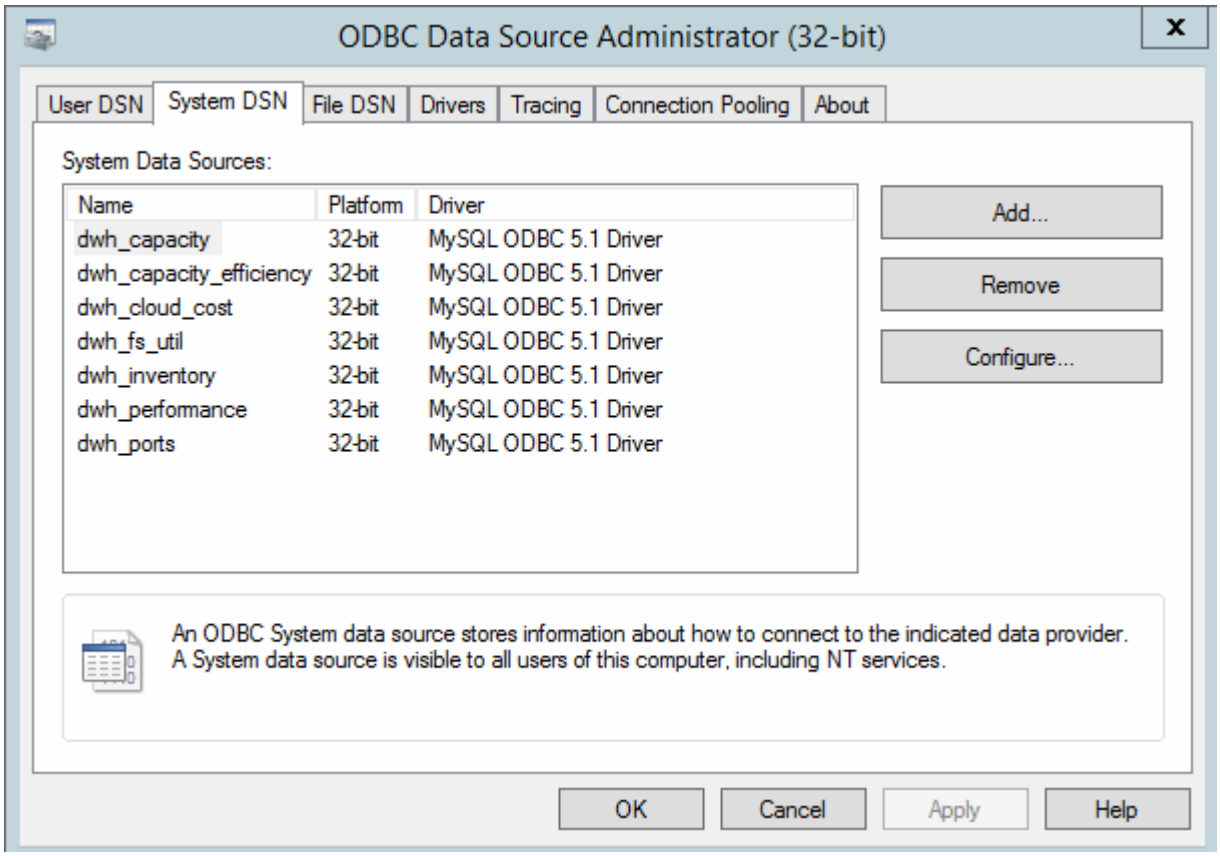
1. Eseguire un login remoto al server che ospita il Data Warehouse.
2. Accedere allo strumento di amministrazione ODBC all'indirizzo `C:\Windows\SysWOW64\odbcad32.exe`

   Viene visualizzata la schermata Amministratore origine dati ODBC.



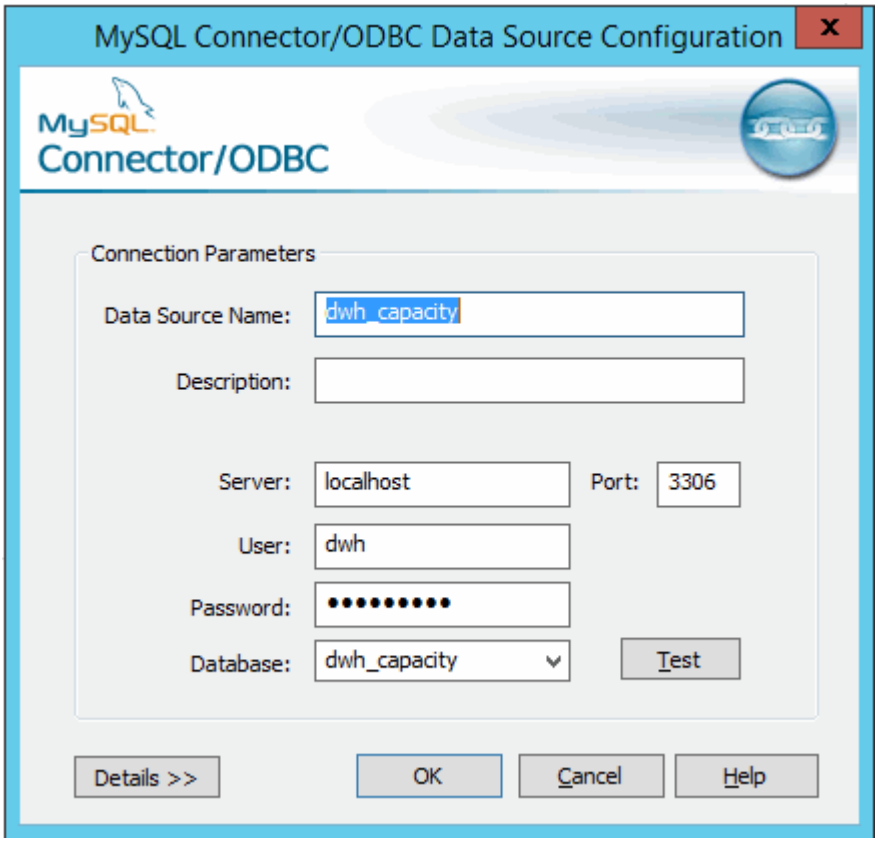
3. Fare clic su **DSN di sistema**

   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 

.

   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.

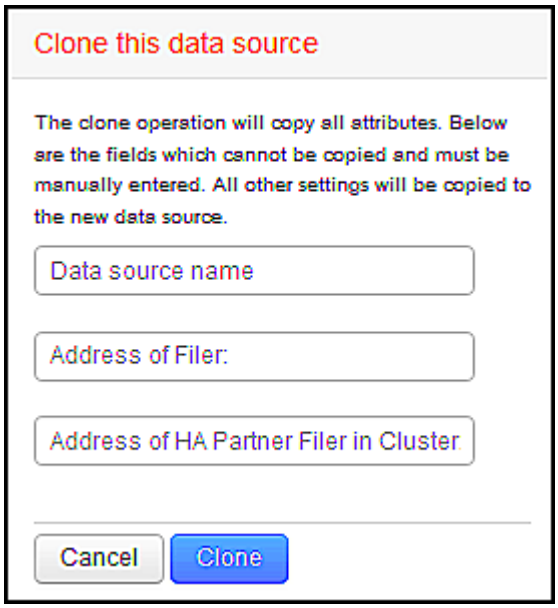
Fasi

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.

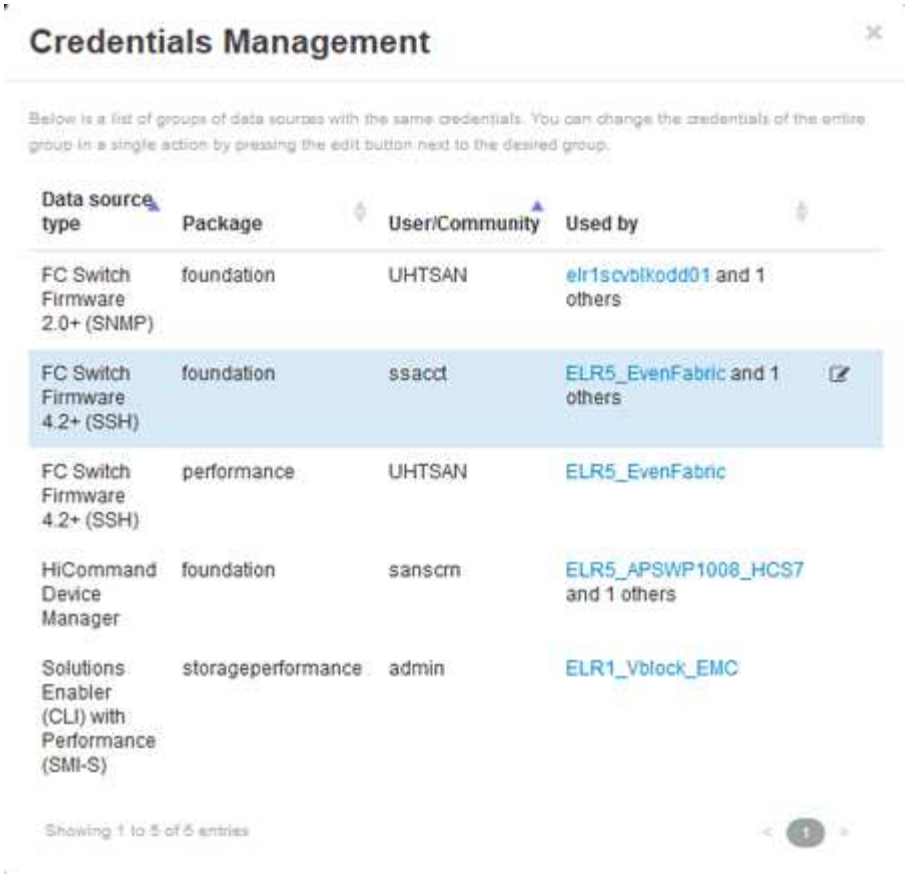
Fasi

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

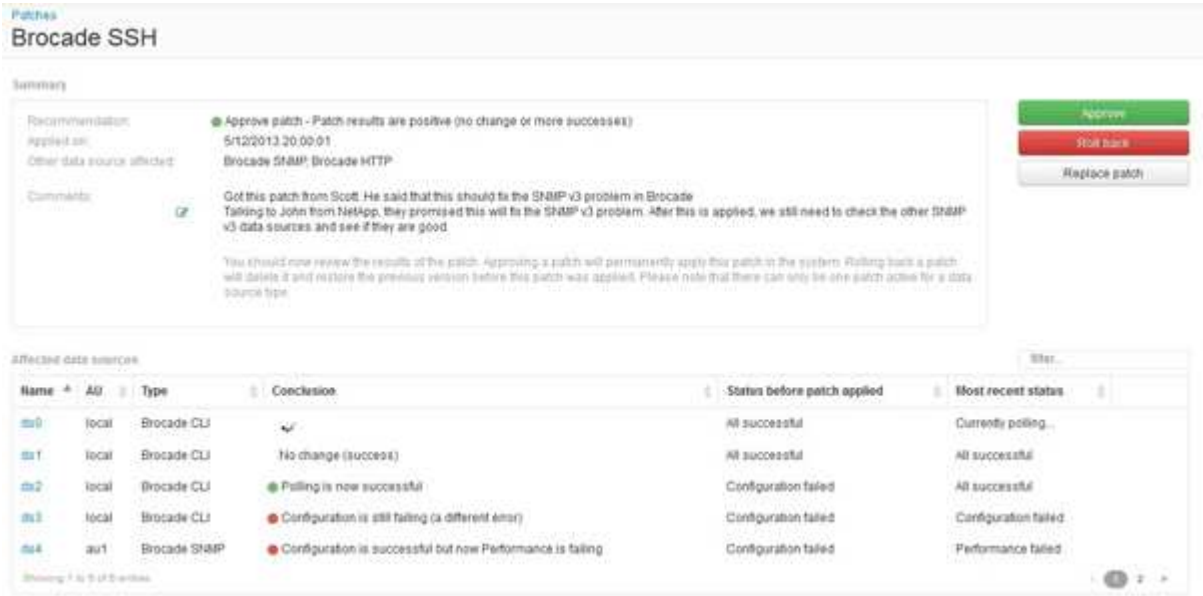
È stata installata una patch e occorre decidere se la patch è stata installata correttamente e deve essere approvata.

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.

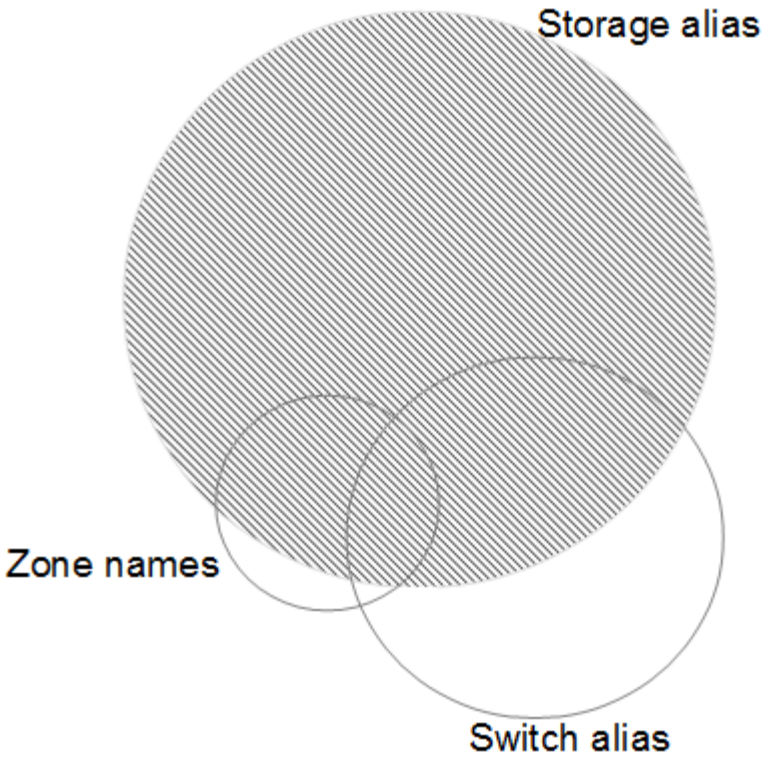
Prima di iniziare

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?

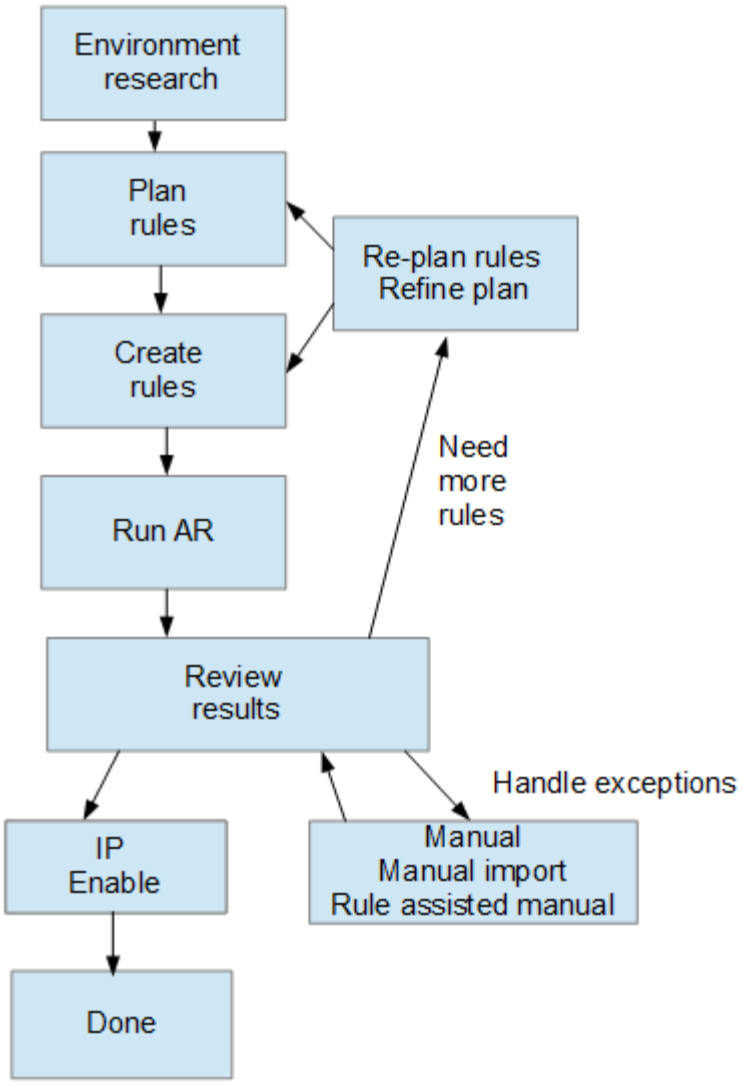
Dopo aver analizzato l'ambiente, dovresti essere in grado di identificare gli standard di denominazione esistenti che ci si può aspettare di incontrare in termini di affidabilità. Le informazioni raccolte potrebbero essere rappresentate graficamente in una figura simile alla seguente:



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.

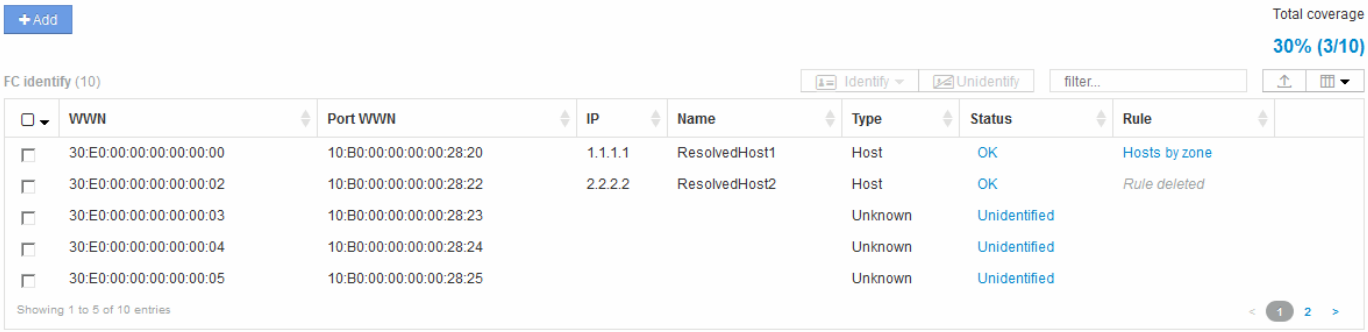
   OnCommand Insight esegue il processo di risoluzione dell'host nell'ordine in cui vengono visualizzati i metodi, iniziando da quelli in alto.

   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:

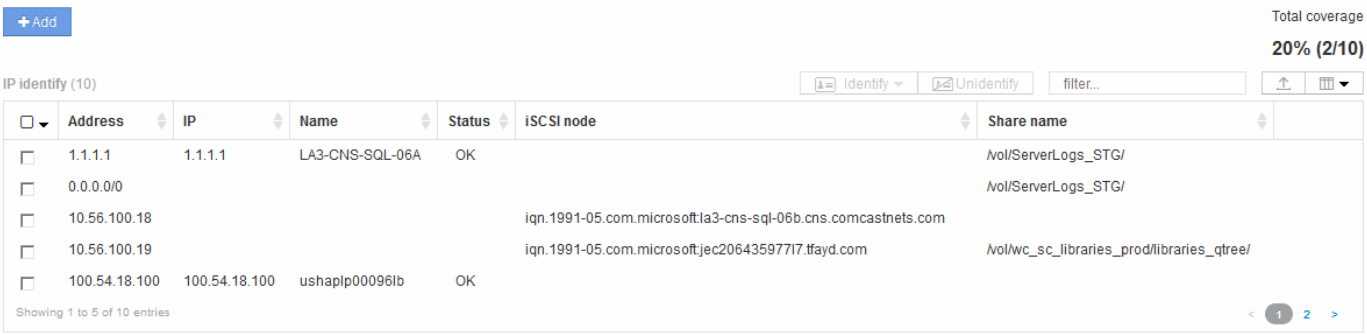
WWN
IP
Nome
Tipo

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

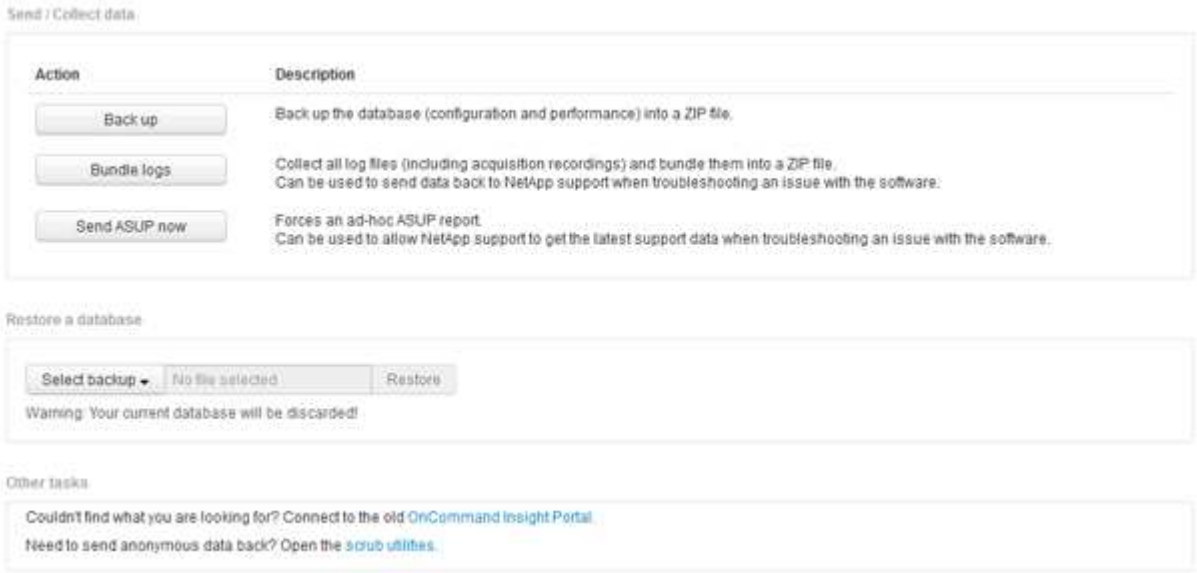
Per ripristinare il database Insight da un file di backup verificato, utilizzare le opzioni di risoluzione dei problemi. Questa operazione sostituisce completamente i dati OnCommand Insight correnti.

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

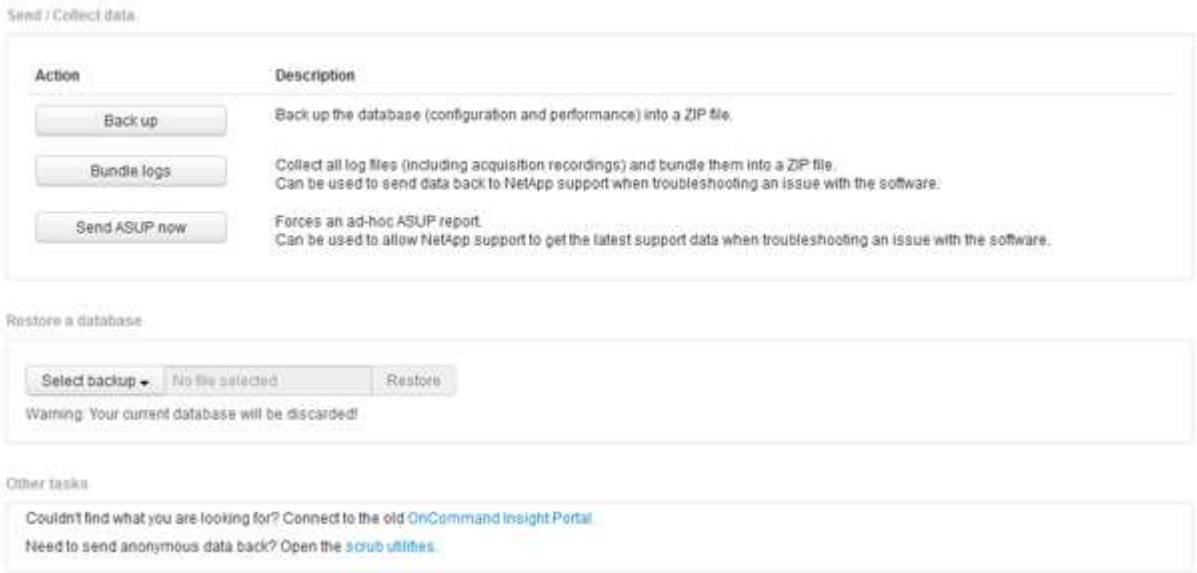
1. Nella barra degli strumenti Insight, fare clic su **Admin**.
2. Fare clic su **risoluzione dei problemi**.
3. Nella sezione Send / Collect data (Invia/raccogli dati), fare clic su **Bundle logs** (registri bundle).
4. Fare clic su **Save file** (Salva file).
5. Fare clic su **OK**.

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

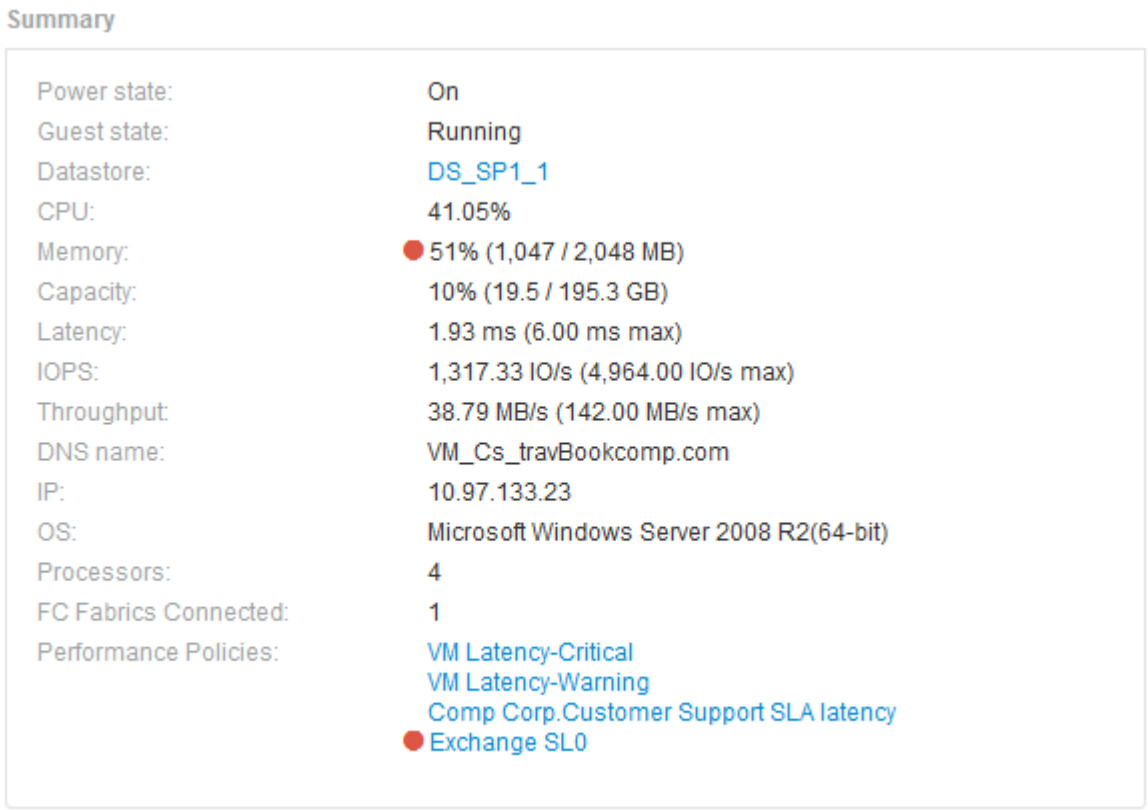
Una pagina delle risorse visualizza diverse sezioni contenenti informazioni relative alla risorsa. Le sezioni visualizzate dipendono dal tipo di risorsa.

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.

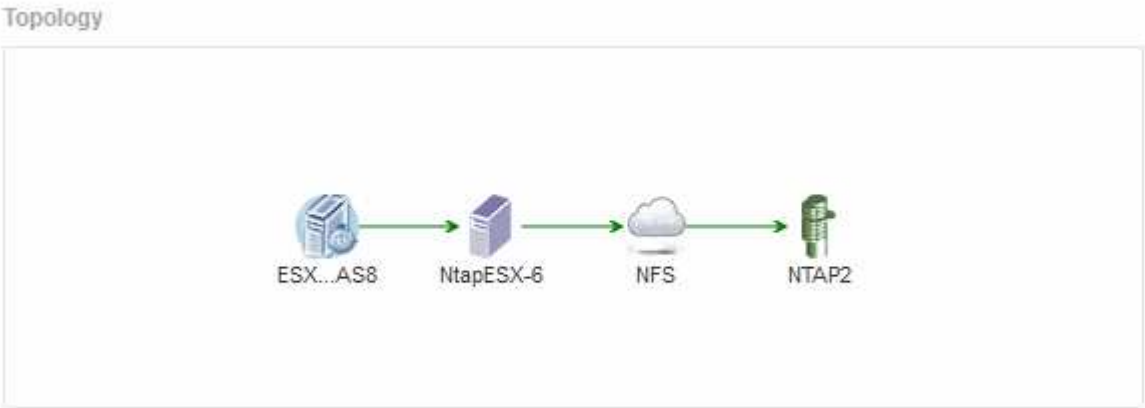
5. Se applicabile, è possibile fare clic su un collegamento al criterio di performance per visualizzare il criterio o i criteri di performance associati alla risorsa.

   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.

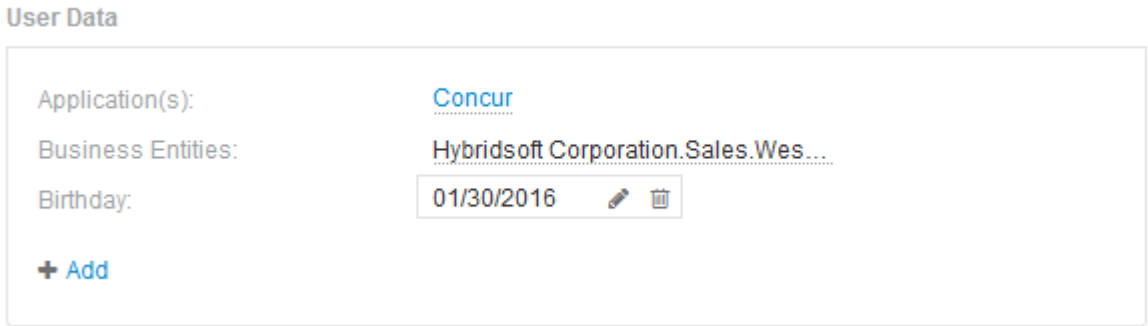
Se la topologia della risorsa è più grande di quella che si adatta alla sezione, fare clic sul collegamento **fare clic per visualizzare il collegamento ipertestuale topologia**.

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.

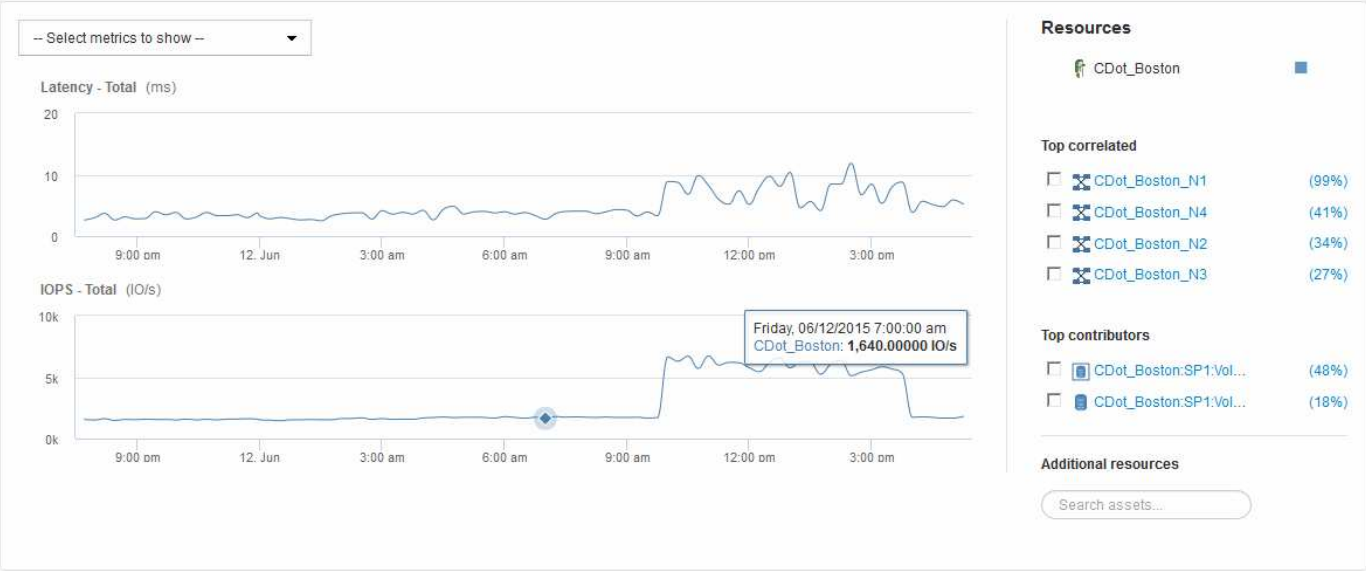
7. Se si desidera modificare il valore dell'annotazione dopo l'assegnazione, fare clic su e selezionare un valore diverso.

   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.

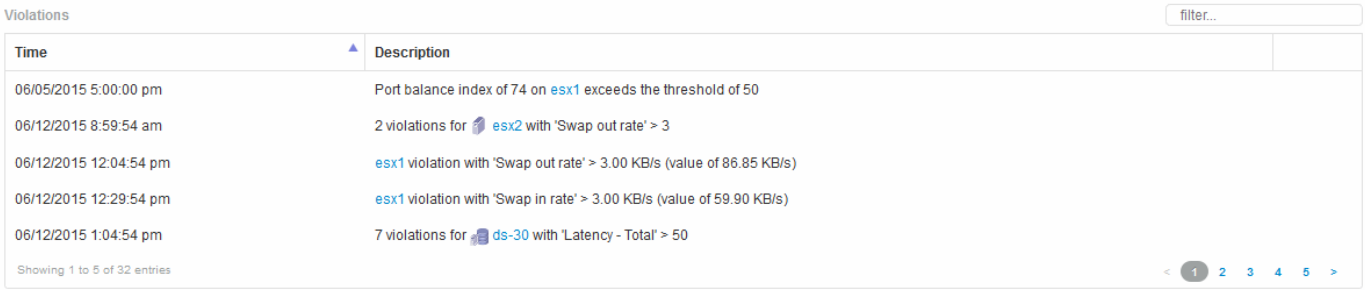
      Tutti gli attributi degli oggetti per le colonne attualmente selezionate per la visualizzazione vengono esportati nel file. Verranno esportati solo gli attributi delle colonne visualizzate. Si noti che vengono esportate solo le prime 10,000 righe della tabella.
5. Per visualizzare le informazioni relative 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.

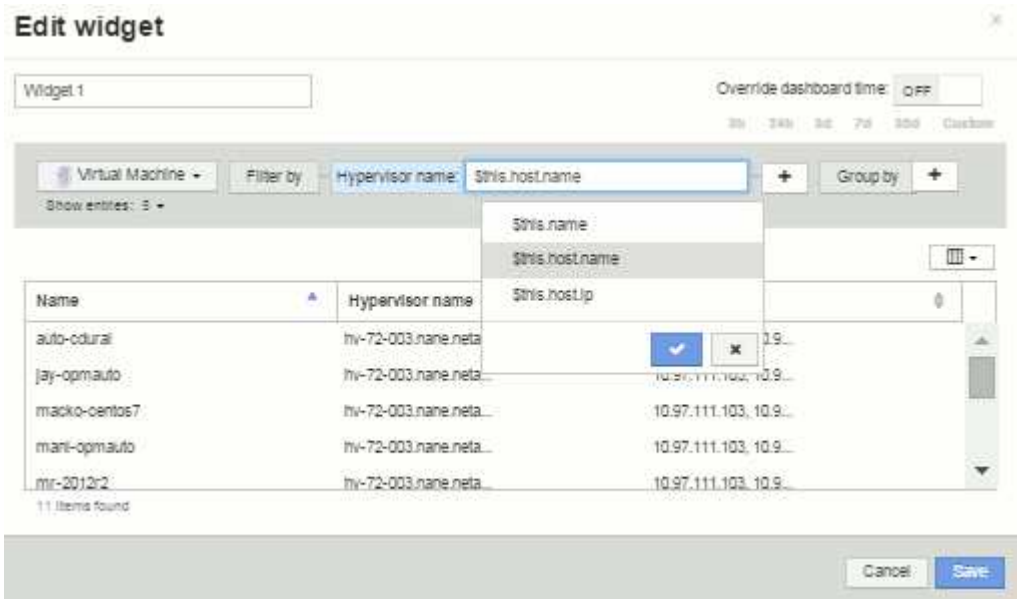
4. Vogliamo mostrare tutte le macchine virtuali. Fare clic sul selettore delle risorse e modificare **Storage** in **Virtual Machine**.

   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

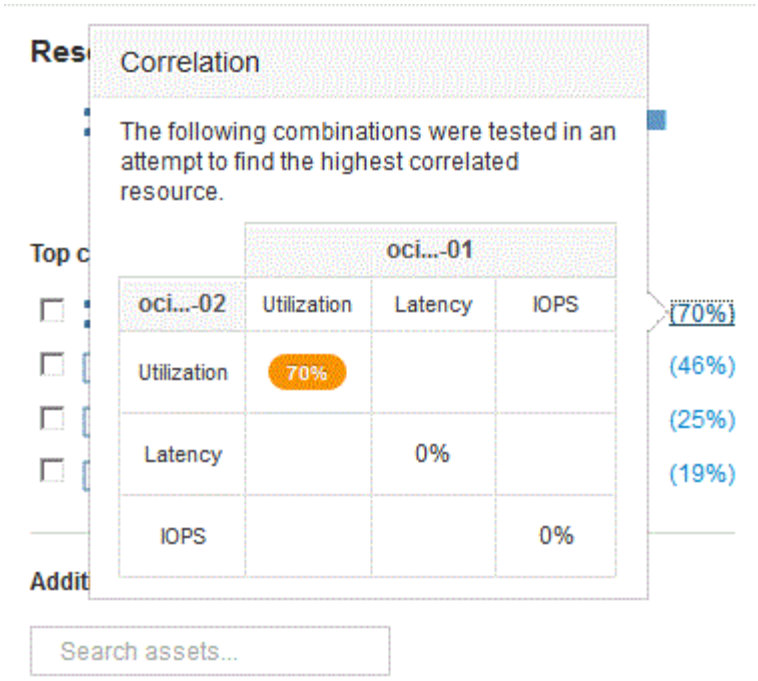
Quando si ricercano problemi di performance e si apre la *pagina delle risorse* per un dispositivo, utilizzare l'elenco delle risorse correlate principali per perfezionare i dati visualizzati nei grafici delle performance. Una risorsa con una percentuale elevata indica che la risorsa ha un'attività simile 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.

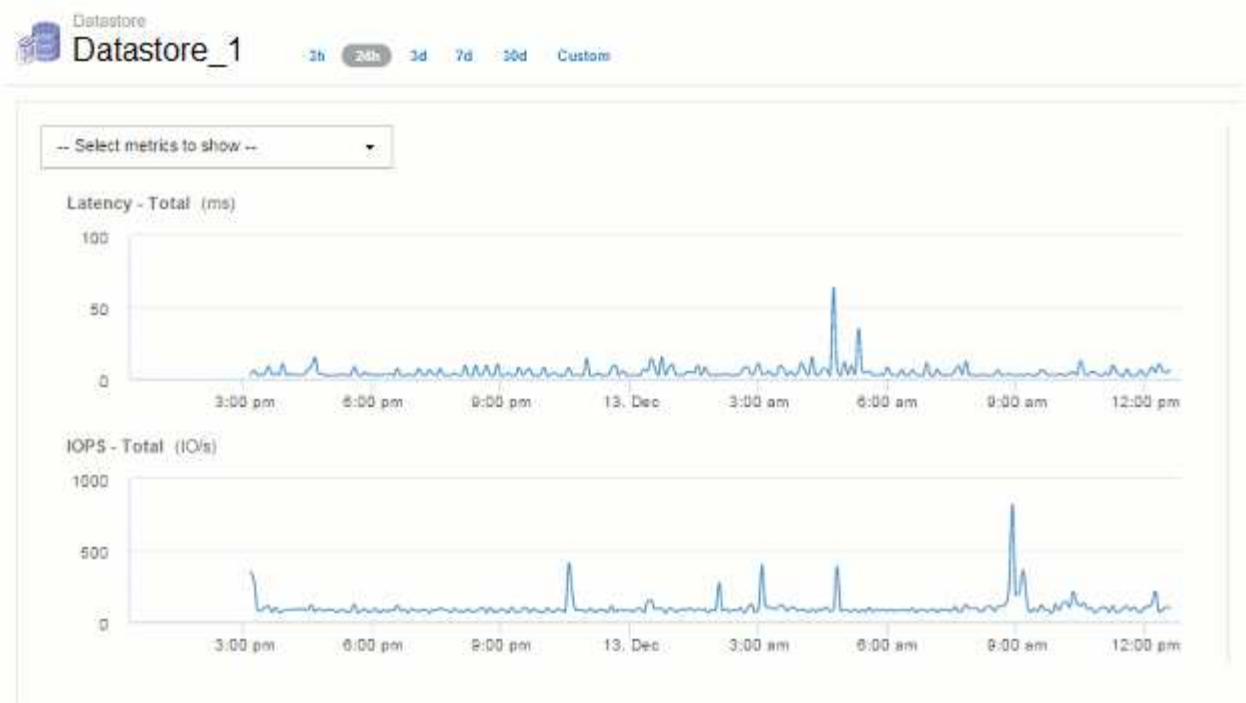
Come funziona il downsampling

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.

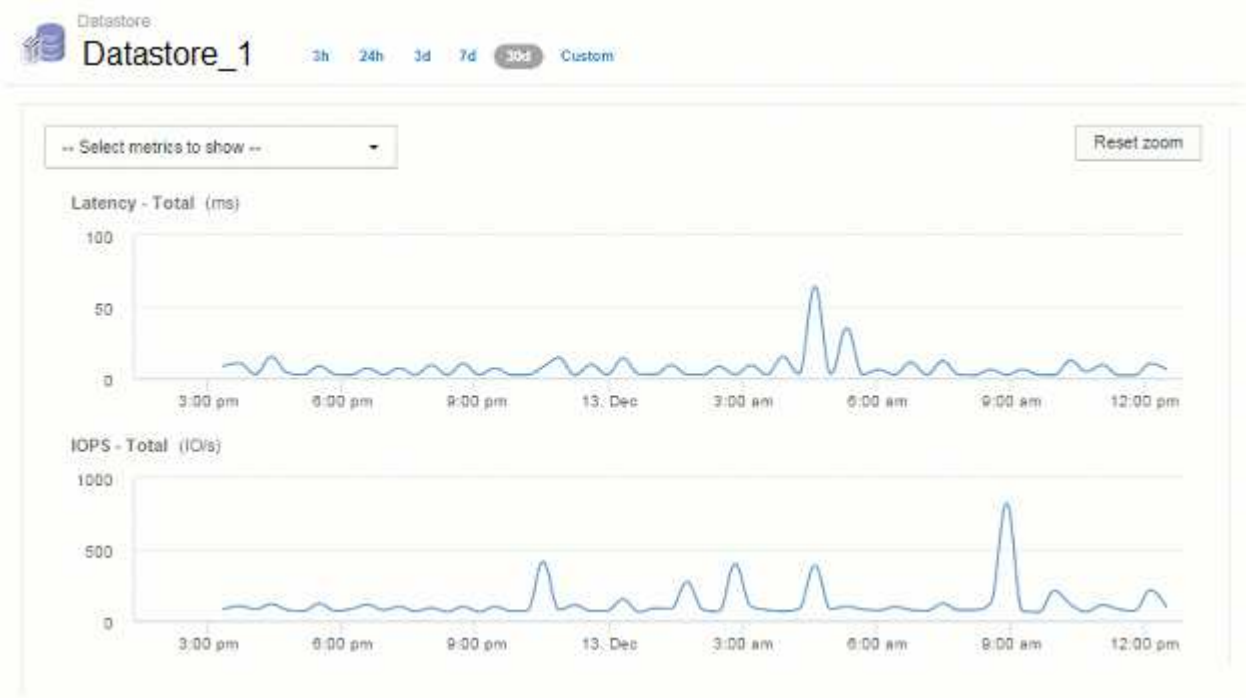
Poiché stiamo scegliendo un intervallo di tempo inferiore a 7 giorni e abbiamo meno di 1,000 punti dati da inserire nel grafico, i dati visualizzati sono dati effettivi. Non si verifica alcun downsampling.



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.

Amministrazione del Data Warehouse

Benvenuto nel data warehouse di OnCommand Insight

Il data warehouse di OnCommand Insight è un repository centralizzato che memorizza i dati provenienti da più server OnCommand Insight e li trasforma in un modello di dati comune e multidimensionale per eseguire query e analisi.

Il data warehouse di OnCommand Insight consente di accedere a un database aperto costituito da diversi data mart che consentono di generare report personalizzati sulla capacità e sulle performance, come report di chargeback, report sui trend con dati storici, analisi dei consumi e report di previsione.

Funzionalità di Data Warehouse

Il data warehouse di OnCommand Insight è un database indipendente composto da diversi data mart.

Data Warehouse include le seguenti funzionalità:

- Dati di configurazione e inventario attuali e storici che consentono di creare report di trend utili per la previsione e la pianificazione
- Diversi data mart storici multidimensionali e un data mart aggiuntivo di inventario solo corrente
- Database ottimizzato per query predefinite o definite dall'utente
- Una piattaforma per l'integrazione con motori di reporting e business intelligence di terze parti, tra cui:
  - Database per la gestione della configurazione
  - Sistemi di contabilità finanziaria
  - Sistemi di gestione delle risorse

Componenti del data warehouse

Data Warehouse contiene diversi componenti.

- Portale Data Warehouse
- Portale di reporting OnCommand Insight
- Strumenti per la creazione di report

Operazioni che è possibile eseguire utilizzando il portale Data Warehouse

Il portale Data Warehouse è un'interfaccia utente basata su Web che consente di configurare le opzioni e impostare pianificazioni fisse per il recupero dei dati. Dal portale del data warehouse, è possibile accedere anche al portale di reporting OnCommand Insight.

Utilizzando il portale Data Warehouse, è possibile effettuare le seguenti operazioni:

- Accedi al portale di reporting di OnCommand Insight per visualizzare report predefiniti o per creare report personalizzati utilizzando strumenti per la creazione di report.

- Consolidare più database OnCommand Insight.
- Gestire le connessioni ai server OnCommand Insight.
- Verificare lo stato dei processi o delle query correnti in esecuzione.
- Pianifica le build del Data Warehouse.
- Modificare il nome del sito.
- Visualizza la versione di Data Warehouse e la cronologia degli aggiornamenti, incluse informazioni specifiche come versioni dei moduli, siti e licenze.
- Importa annotazioni.
- Configurare una build dalla cronologia.
- Visualizza la documentazione di Data Warehouse e lo schema del database.
- Ripristinare il database Data Warehouse.
- Eseguire il backup e il ripristino del database Data Warehouse.
- Risolvere i problemi di Data Warehouse.
- Gestire gli account utente.

Componenti software Data Warehouse

Il data warehouse di OnCommand Insight include diversi componenti software.

- Database MySQL

  Repository back-end per le tabelle data mart

- IBM Cognos

  Il motore di reporting per OnCommand Insight

- Database Apache Derby

  Utilizzato per memorizzare la configurazione e il contenuto di Cognos

- WildFly

  Il server applicativo Java Enterprise che ospita i componenti OnCommand Insight

Processi di Data Warehouse

Data Warehouse esegue diversi tipi di processi.

- **Processo ETL**

  Il processo ETL (Extract Transform and Load) recupera i dati da più database OnCommand Insight, li trasforma e li salva nel data mart. Il processo di creazione del data warehouse è un processo ETL.

- **Lavori**

  Data Warehouse esegue e crea report su processi come: Inventario, dimensioni, capacità, capacità delle porte, capacità delle macchine virtuali, utilizzo del file system, performance, efficienza della capacità,

licenze, creazione della cronologia, Annotazioni dinamiche, rimozione del connettore, creazione ignorata, opzione ASUP e lavori di manutenzione.

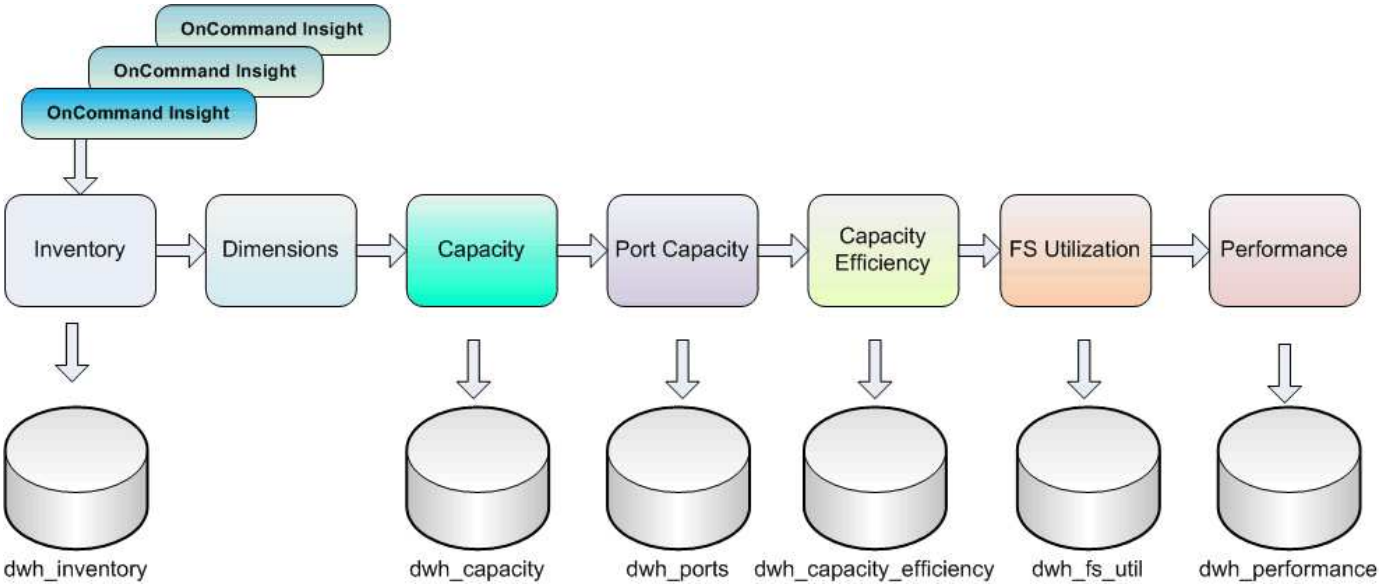
- **Processo di consolidamento**

  Data warehouse supporta il consolidamento di più server OnCommand Insight nello stesso database del data warehouse. In molte configurazioni, potrebbe accadere che lo stesso oggetto venga segnalato da più connettori (ovvero, lo stesso switch esiste in due istanze di OnCommand Insight). In questo caso, Data Warehouse consolida più oggetti in uno (viene scelto un connettore primario e i dati dell'oggetto vengono presi solo da quel connettore).

In che modo Data Warehouse estrae i dati

Il processo di estrazione, trasformazione e caricamento (ETL) recupera i dati da più database OnCommand Insight, li trasforma e li salva nei data mart.

I connettori OnCommand Insight richiamano una serie di job batch per estrarre dati da più database MySQL OnCommand Insight e pubblicare i dati in diversi data mart, come mostrato nel diagramma seguente.



Il processo ETL include i seguenti processi:

- **Estrarre**

  Questo processo preleva i dati da più database OnCommand Insight, li trasforma e li salva nel data mart. Il processo viene eseguito su ogni istanza di OnCommand Insight contemporaneamente. Per garantire l'esecuzione della pulizia e della deduplica dei dati, non è possibile suddividere il processo ETL in più operazioni ETL pianificate.

- **Trasformazione**

  Questo processo applica le regole o le funzioni della logica di business per estrarre i dati dal database OnCommand Insight.

- **Carico**

  Questo processo carica i dati trasformati in data mart pubblici.

Frequenza ETL e dati di data

È necessario eseguire il processo ETL (Extract, Transform, and Load) almeno una volta al giorno; tuttavia, si sceglie di eseguire ETL più volte, se necessario.

Per impostazione predefinita, il motore di reporting Cognos considera tutti i dati relativi a capacità e performance come additivi. Di conseguenza, se il processo ETL viene eseguito più volte al giorno senza i filtri temporali appropriati, sussiste il rischio di raddoppiare i dati di capacità di conteggio.

Due elementi dei dati nella dimensione Date sono correlati al processo ETL giornaliero. La dimensione Date, utilizzata in diversi modelli di dati, include i seguenti elementi di dati che sono interessati dall'ETL:

- **È un rappresentante giornaliero**

  L'elemento di dati "is Day Representative" viene impostato su un valore pari a 1 (true) durante il primo processo ETL eseguito in un determinato giorno. Se il primo processo ETL viene eseguito alle ore 1:00, è il rappresentante del giorno viene impostato su 1 per tutti i dati caricati durante le ore 1:00 Processo ETL. Se viene pianificato un secondo ETL in un secondo momento (ad esempio, alle 13:00), il valore è Day Representative (rappresentante giorno) impostato su 0 (falso) per i dati caricati durante il processo ETL.

- **È l'ultimo**

  Il membro "is latest" viene impostato su un valore pari a 1 (true) al termine di ogni processo ETL. Se il primo processo ETL viene eseguito alle ore 1:00, l'opzione è più recente viene impostata su 1 per tutti i dati caricati durante le ore 1:00 Processo ETL. Se viene pianificato un altro processo ETL in un secondo momento (ad esempio, alle 13:00), l'opzione è più recente viene impostata su 1 per i dati caricati durante le 13:00 Processo ETL. Il processo ETL imposta anche l'1:00 del mattino Il carico ETL è l'ultima voce a 0 (falso).

Come vengono conservati i dati storici nel Data Warehouse

I dati vengono conservati nel Data Warehouse in base a una pianificazione. Man mano che i dati invecchiano, la conservazione dei record di dati viene ridotta.

Data Warehouse conserva i dati storici in base ai data mart e alla granularità dei dati, come mostrato nella tabella seguente.

Data mart	Oggetto misurato	Granularità	Periodo di conservazione
Performance mart	Volumi e volumi interni	Ogni ora	14 giorni
Performance mart	Volumi e volumi interni	Ogni giorno	13 mesi
Performance mart	Applicazione	Ogni ora	13 mesi
Performance mart	Host	Ogni ora	13 mesi
Performance mart	Prestazioni dello switch per la porta	Ogni ora	5 settimane

Performance mart	Prestazioni dello switch per host, storage e nastro	Ogni ora	13 mesi
Performance mart	Nodo storage	Ogni ora	14 giorni
Performance mart	Nodo storage	Ogni giorno	13 mesi
Performance mart	Performance delle macchine virtuali	Ogni ora	14 giorni
Performance mart	Performance delle macchine virtuali	Ogni giorno	13 mesi
Performance mart	Performance dell'hypervisor	Ogni ora	14 giorni
Performance mart	Performance dell'hypervisor	Ogni giorno	13 mesi
Performance mart	Performance VMDK	Ogni ora	14 giorni
Performance mart	Performance VMDK	Ogni giorno	13 mesi
Performance mart	Performance del disco	Ogni ora	14 giorni
Performance mart	Performance del disco	Ogni giorno	13 mesi
Capacità	Tutti (tranne i singoli volumi)	Ogni giorno	13 mesi
Capacità	Tutti (tranne i singoli volumi)	Rappresentante mensile	14 mesi e oltre
Inventario Mart	Singoli volumi	Stato corrente	1 giorno (o fino al prossimo ETL)

Dopo 13 mesi (configurabile), Data Warehouse conserva un solo record al mese invece di un record al giorno per dati su capacità, performance e risorse nelle seguenti tabelle dei fatti:

- Tabella dei fatti di chargeback (dwh_capacity.chargeback_fact)
- Tabella dati sull'utilizzo del file system (dwh_fs_util.fs_util_fact)
- Tabella dati host (dwh_sa.sa_host_Fact)
- Tabella dati capacità volume interna (dwh_capacity.internal_volume_capacity_fact)
- Tabella delle porte (dwh_ports.ports_fact)
- Tabella dati delle capacità del qtree (dwh_Capacity.qtree_Capacity_Fact)

- Tabella dati sulla capacità dello storage e del pool di storage (dwh_Capacity.storage_and_storage_pool_Capacity_Fact)
- Tabella dati sulla capacità del volume (dwh_Capacity.vm_Capacity_Fact)
- Tabelle dei fatti Storage Node Hourly Performance (Storage_Node_Hourly_performance_Fact) e Storage Node Daily Performance (Storage_Node_Daily_performance_Fact)

Conservazione dei dati, ETL e periodi di tempo

Il data warehouse di OnCommand Insight conserva i dati ottenuti dal processo di estrazione, trasformazione e caricamento (ETL) per diversi periodi di tempo in base ai diversi data mart e alla granularità temporale dei dati.

Performance Mart e granularità oraria per volumi e volumi interni

Il data warehouse di OnCommand Insight registra le medie orarie, i massimi orari e i bit di accesso per ogni ora del giorno (24 punti dati) per 14 giorni. Il bit di accesso è un valore booleano true se si accede al volume o false se non si accede al volume durante l'intervallo orario. Tutti i 24 punti dati del giorno precedente vengono ottenuti durante il primo processo ETL della giornata.

Non è necessario eseguire un processo ETL all'ora per raccogliere i punti dati orari. L'esecuzione di processi ETL aggiuntivi durante la giornata non consente di ottenere informazioni sulle performance dai server OnCommand Insight.

Performance Mart e granularità giornaliera per volumi e volumi interni

Ogni giorno in cui viene elaborato l'ETL, le medie giornaliere del giorno precedente vengono calcolate e popolate all'interno del Data Warehouse. La media giornaliera è un riepilogo dei 24 punti dati del giorno precedente. I data mart delle performance conservano riepiloghi giornalieri per volumi e volumi interni per 13 mesi.

Capacità e granularità giornaliera

Le unità di misura della capacità forniscono misurazioni giornaliere di diversi dati relativi alla capacità per un periodo di 13 mesi. I dati relativi alla capacità nel Data Warehouse sono aggiornati all'ultima acquisizione dell'origine dati per il dispositivo prima dell'ETL.

Capacità e granularità mensile

Data Warehouse conserva i dati di capacità giornalieri per 13 mesi. Una volta raggiunta la soglia di 13 mesi, i dati relativi alla capacità vengono riepilogati su base mensile. I dati mensili si basano sui valori riportati dalla data rappresentativa del mese.

La tabella seguente mostra i dati mensili inclusi nel riepilogo mensile:

Data	È il valore rappresentativo del mese	Capacità allocata
1 gennaio	1 (vero)	50 TB
2 gennaio	0 (Falso)	52 TB
…	…	…

Gennaio 31	0 (Falso)	65 TB
1 febbraio	1 (vero)	65 TB

In base alla tabella, un report mensile indicherebbe 50 TB allocati per gennaio e 65 TB allocati per febbraio. Tutti gli altri valori di capacità per gennaio non verranno inclusi nel riepilogo mensile.

Mart. Inventario

Il data mart di inventario non è storico. Ogni volta che viene eseguito un processo ETL, il magazzino viene cancellato e ricostruito. Pertanto, qualsiasi report generato dal magazzino non riflette la configurazione dell'inventario cronologico.

Introduzione a Data Warehouse

Data warehouse di OnCommand Insight consente di configurare le opzioni necessarie prima di generare report che includono i dati. Data Warehouse contiene molte funzionalità; tuttavia, è necessario utilizzarne solo alcune per iniziare. Per configurare Data Warehouse, utilizzare le opzioni nel portale Data Warehouse.

A proposito di questa attività

Per configurare il data warehouse di OnCommand Insight, un amministratore dello storage deve completare le seguenti procedure:

- Accesso al portale Data Warehouse
- Connessione del data warehouse ai server OnCommand Insight
- Creazione del database dalla cronologia
- Impostazione dei processi di backup e ripristino

Inoltre, un amministratore dello storage potrebbe voler completare le seguenti procedure.

- Accesso a MySQL tramite l'interfaccia a riga di comando
- Pianificazione delle build giornaliere
- Impostazione di tenancy multiple nel reporting
- Risoluzione dei problemi di installazione
  - Perché non riesco a vedere le mie annotazioni?
  - Cosa devo fare con i punti di costruzione storici non riusciti?

Se si utilizza il portale Data Warehouse per la prima volta, è necessario configurare Data Warehouse prima di poter visualizzare qualsiasi informazione nella pagina Jobs. È inoltre necessario ripetere questo processo di configurazione dopo aver reimpostato il database Data Warehouse.

Accesso al portale Data Warehouse

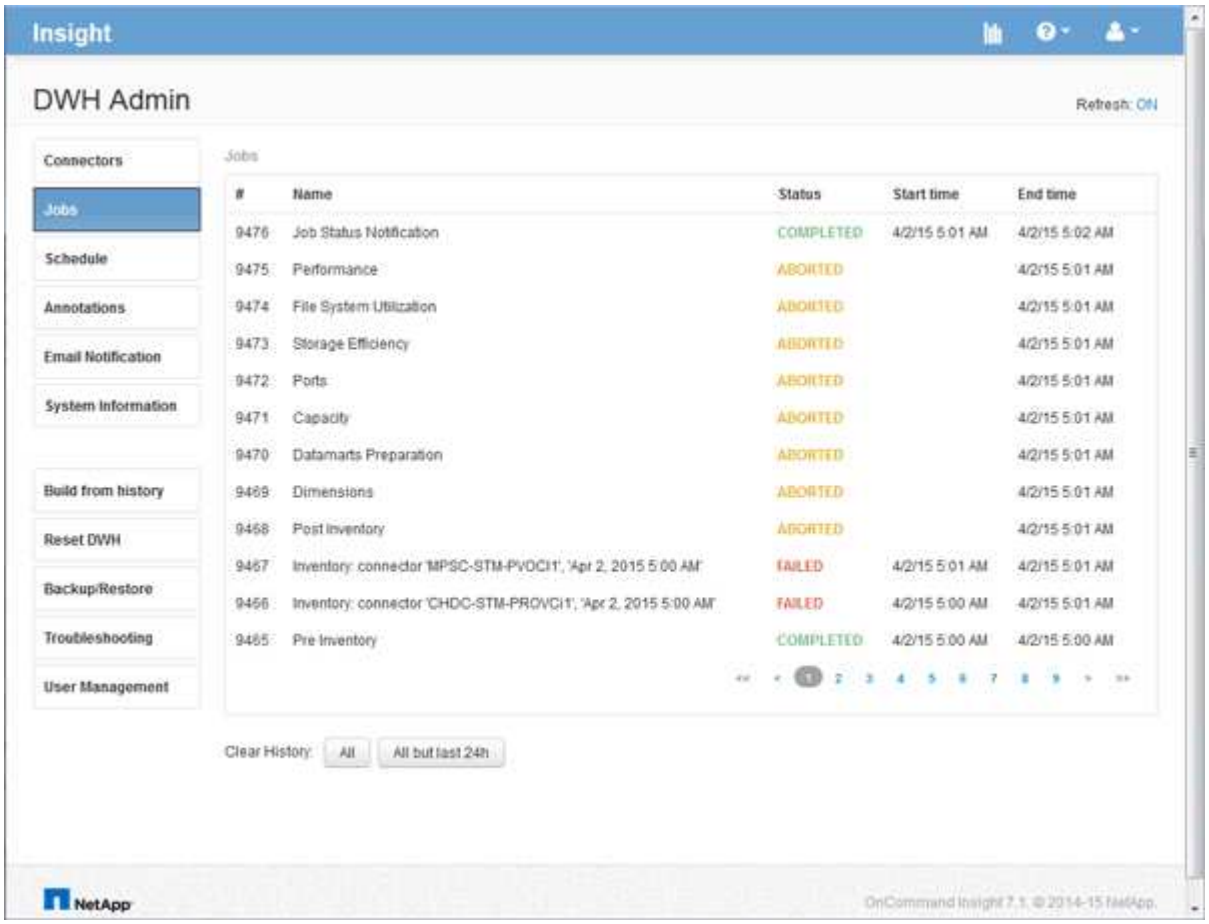
Il portale del data warehouse di OnCommand Insight è un'interfaccia utente basata su web che può essere utilizzata per aggiornare le informazioni del connettore, visualizzare

le code dei processi, pianificare le build giornaliere, selezionare le annotazioni, impostare le notifiche via email, visualizzare le informazioni di sistema, creare il database, ripristinare il data warehouse, eseguire il backup e il ripristino del database, risolvere i problemi, Gestisci gli account utente del portale Data Warehouse e Reporting e accedi alla documentazione e ai diagrammi dello schema.

Fasi

1. Accedere al portale Data Warehouse all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Immettere il nome utente e la password.
3. Fare clic su **Login**.

   Il portale Data Warehouse apre:



Gestione degli account utente Data Warehouse e Reporting

Gli account utente, l'autenticazione utente e l'autorizzazione utente per i tool di reporting OnCommand Insight vengono definiti e gestiti dal data warehouse (DWH). In base a queste configurazioni, utenti e amministratori possono accedere ad alcuni o a tutti i report OnCommand Insight disponibili.

L'accesso alla gestione utenti nel Data Warehouse richiede un account con privilegi di amministratore di

sistema. Ciò include:

- Funzionalità amministrative complete per il data warehouse
- Configurazione e manutenzione di tutti gli account utente
- Accesso in lettura al database
- Possibilità di configurare i connettori nell'ETL, pianificare i processi di Data Warehouse, ripristinare il database, assegnare o modificare i ruoli e aggiungere e rimuovere gli account utente

Accesso al portale Data Warehouse e Reporting

Il portale Data Warehouse consente di accedere alle opzioni di amministrazione. Dal portale Data Warehouse, puoi anche accedere al portale Reporting.

Fasi

1. Accedere come amministratore al portale Data Warehouse all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire il portale Reporting.

Creazione di report sui ruoli utente

A ciascun account utente viene assegnato un ruolo con una serie di autorizzazioni. Il numero di utenti è limitato dal numero di licenze di Reporting associate a ciascun ruolo.

Ciascun ruolo può eseguire le seguenti azioni:

- **Destinatario**

  Visualizza i report del portale di reporting OnCommand Insight e imposta le preferenze personali, ad esempio quelle per le lingue e i fusi orari.

  > I destinatari non possono creare report, eseguire report, pianificare report, esportare report o eseguire attività amministrative.

- **Business Consumer**

  Esegue i report ed esegue tutte le opzioni dei destinatari.

- **Business Author**

  Visualizza report pianificati, esegue report in modo interattivo, crea storie, oltre a eseguire tutte le opzioni Business Consumer.

- **Pro Author**

  Crea report, crea pacchetti e moduli di dati, oltre a eseguire tutte le opzioni di Business Author.

- **Amministratore**

  Esegue attività amministrative di reporting come l'importazione e l'esportazione delle definizioni dei report, la configurazione dei report, la configurazione delle origini dati e l'arresto e il riavvio delle attività di reporting.

La tabella seguente mostra i privilegi e il numero massimo di utenti consentiti per ciascun ruolo:

Funzione	Destinatario	Consumer aziendale	Autore di business	Pro Author	Amministratore
Visualizzare i report nella scheda contenuto team	Sì	Sì	Sì	Sì	Sì
Eseguire i report	No	Sì	Sì	Sì	Sì
Pianifica i report	No	Sì	Sì	Sì	Sì
Caricare file esterni	No	No	Sì	Sì	No
Crea storie	No	No	Sì	Sì	No
Creare report	No	No	Sì	Sì	No
Creare pacchetti e moduli dati	No	No	No	Sì	No
Eseguire attività amministrative	No	No	No	No	Sì
Numero di utenti	Numero di utenti OnCommand Insight	20	2	1	1

Quando si aggiunge un nuovo utente di Data Warehouse e Reporting, se si supera il limite di un ruolo, l'utente viene aggiunto come "deactivated," ed è necessario disattivare o rimuovere un altro utente con tale ruolo per assegnare un nuovo utente.

> Le funzionalità di creazione dei report richiedono la licenza Insight Plan. Puoi aggiungere altri utenti Business Author e Pro Author acquistando IL PACCHETTO ARAP (Additional Report Authoring Package). Per assistenza, contattare il rappresentante OnCommand Insight.

Questi ruoli utente di reporting non influiscono sull'accesso diretto al database. Questi ruoli utente di reporting non influiscono sulla capacità di creare query SQL utilizzando i data mart.

Aggiunta di un utente di Reporting

È necessario aggiungere un nuovo account utente per ogni persona che richiede l'accesso al portale di reporting. La disponibilità di un account utente diverso per ciascuna persona consente di controllare i diritti di accesso, le preferenze individuali e la responsabilità.

Prima di iniziare

Prima di aggiungere un utente di Reporting, è necessario aver assegnato un nome utente univoco, determinato la password da utilizzare e verificato il ruolo o i ruoli utente corretti. Questi ruoli sono specializzati nel portale Reporting.

Fasi

1. Accedere come amministratore 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 **User Management** (Gestione utenti).
3. Nella finestra **User Management**, fare clic su **Add New User** (Aggiungi nuovo utente).
4. Inserire le seguenti informazioni per il nuovo utente di Reporting:
   - **Nome utente**

     Nome utente (alfanumerico, compreso a-z, A-Z e 0-9) per l'account
   - **Indirizzo e-mail**

     Indirizzo e-mail associato all'account utente e richiesto se l'utente si iscrive a qualsiasi report
   - **Password**

     Password per accedere a OnCommand Insight con questo account utente, che in genere viene selezionato dall'utente e confermato nell'interfaccia
   - **Ruolo Insight**

     Ruoli disponibili per l'utente con autorizzazioni appropriate

     > Le opzioni per il ruolo OnCommand Insight vengono visualizzate solo se OnCommand Insight è installato sullo stesso computer delle strutture di reporting, cosa non tipica.
   - **Ruoli di reporting**

     Ruolo di reporting per questo account utente (ad esempio, Pro Author)

     > Il ruolo di amministratore è unico. È possibile aggiungere questo ruolo a qualsiasi utente.
5. Fare clic su **Aggiungi**.

Gestione degli account utente

È possibile configurare account utente, autenticazione utente e autorizzazione utente dal portale Data Warehouse. A ciascun account utente viene assegnato un ruolo con uno dei seguenti livelli di autorizzazione. Il numero di utenti è limitato dal numero di licenze di Reporting associate a ciascun ruolo.

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 **User Management** (Gestione utenti).

User Management

	OnCommand Insight roles			Reporting roles									
Name	Guest	User	Administrator	Recipient	Business Consumer	Business Author	Pro Author	Administrator	E-mail				
guest	X									Edit	Delete	Change password	Deactivate
user	X	X								Edit	Delete	Change password	Deactivate
admin	X	X	X				X	X		Edit		Change password	
oadmin	X	X	X							Edit		Change password	Deactivate

LDAP Configuration | Add New User | Change DWH User password

The following table shows the privileges for each reporting role:

Feature	Recipient	Business Consumer	Business Author	Pro Author	Administrator
View reports (in Public Folder tab, My Folders)	Yes	Yes	Yes	Yes	Yes
Run reports	No	Yes	Yes	Yes	Yes
Schedule Reports	No	Yes	Yes	Yes	Yes
Create reports in Query Studio	No	No	Yes	Yes	No
Create reports in Workspace (Standard)	No	Yes	Yes	Yes	No
Create reports in Workspace (Advanced)	No	No	Yes	Yes	No
Create reports in Report Studio	No	No	No	Yes	No
Perform administrative tasks	No	No	No	No	Yes

3. Effettuare una delle seguenti operazioni:
   - Per modificare un utente esistente, selezionare la riga dell'utente e fare clic su **Edit** (Modifica).
   - Per modificare la password di un utente, selezionare la riga dell'utente e fare clic su **Change password** (Modifica password).
   - Per eliminare un utente, selezionare la riga dell'utente e fare clic su **Delete** (Elimina)
4. Per attivare o disattivare un utente, selezionare la riga corrispondente e fare clic su **Activate** o **Deactivate**.

Configurazione di LDAP per il reporting

Dal portale Data Warehouse, l'amministratore può configurare l'utilizzo LDAP per Data Warehouse e Reporting.

Prima di iniziare

Per eseguire questa attività, è necessario accedere a Insight come amministratore.

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.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema su cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **User Management** (Gestione utenti).
3. Fare clic su **Configurazione LDAP**.
4. Selezionare **Enable LDAP** (attiva LDAP) per avviare il processo di autenticazione e autorizzazione dell'utente LDAP.
5. Apportare le modifiche necessarie per configurare LDAP.

   La maggior parte dei campi contiene valori predefiniti. Le impostazioni predefinite sono valide per Active

Directory.

- **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`.

- **Riferimento**

  Indica se seguire il percorso verso altri domini se nell'azienda sono presenti più domini. Utilizzare sempre l'impostazione predefinita `follow` impostazione.

- **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.

- **Server LDAP**

  Indirizzo IP o nome DNS per identificare il server LDAP. Per identificare una porta specifica, dove `ldap-server-address` È il nome del server LDAP, è possibile utilizzare il seguente formato:

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

  Per utilizzare la porta predefinita, è possibile utilizzare il seguente formato:

  ```
  ldap://ldap-server-address
  ```

```
 When entering multiple LDAP servers in this field,
separate entries with a comma, and ensure that the correct
port number is used in each entry.
+ per importare i certificati LDAP, fare clic su *Importa
certificati* e importare automaticamente o individuare
manualmente i file dei certificati.
```

- **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
```

- **Gruppo Insight server Admins**

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

- **Gruppo di amministratori Insight**

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

- **Gruppo utenti Insight**

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

- **Insight Guest group**

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

- **Gruppo di amministratori dei report**

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

- **Gruppo di autori di Reporting pro**

  Gruppo LDAP per utenti con privilegi di autore Insight Reporting Pro. Il valore predefinito è `insight.report.proauthors`.

- **Gruppo di autori del business di reporting**

  Gruppo LDAP per utenti con privilegi di autori aziendali Insight Reporting. Il valore predefinito è `insight.report.business.authors`.

- **Reporting business consumer group**

  Gruppo LDAP per utenti con privilegi Insight Reporting per i clienti aziendali. Il valore predefinito è

`insight.report.business.consumers`.

- **Gruppo destinatari report**

  Gruppo LDAP per utenti con privilegi di destinatario Insight Reporting. Il valore predefinito è `insight.report.recipients`.

6. Se sono state apportate modifiche, immettere i valori nei campi **Directory lookup user** e **Directory lookup user password**.

   Se non si inseriscono i valori modificati in questi campi, le modifiche non vengono salvate.

7. Digitare nuovamente la password utente per la ricerca nella directory nel campo **Conferma password utente per la ricerca nella directory** e fare clic su **convalida password** per convalidare la password sul server.
8. Fare clic su **Update** (Aggiorna) per salvare le modifiche. Fare clic su **Annulla** per rimuovere le modifiche.

Connessione del data warehouse ai server OnCommand Insight

I connettori stabiliscono le connessioni dal data warehouse OnCommand Insight ai server OnCommand Insight. È possibile collegare il data warehouse a uno o più server OnCommand Insight. È possibile aggiungere o rimuovere connessioni a o da database OnCommand Insight.

A proposito di questa attività

Data Warehouse assegna un ID univoco globale al connettore utilizzato insieme al nome del connettore. Dopo aver aggiunto un connettore, Data Warehouse richiede al database OnCommand Insight il nome e la versione del sito OnCommand Insight.

È possibile scegliere di connettersi a un'origine dati con o senza SSL. La scelta dell'origine dati sicura impone alla connessione di utilizzare SSL durante la comunicazione con il database remoto di OnCommand Insight.

Data warehouse può fornire una vista consolidata dei dati provenienti da più installazioni OnCommand Insight. Questo database consolidato fornisce le seguenti informazioni:

- Identificatori univoci a livello globale

  A ciascun oggetto viene assegnato un ID univoco globale, indipendente dagli ID utilizzati dai singoli siti, per evitare conflitti di ID e consentire il rilevamento dei duplicati. Questi ID sono condivisi tra tutti i data mart. Questo ID è il GUID (Globally Unique ID) nella colonna Comment (Commento) delle tabelle dei data mart di inventario.

- Nessuna duplicazione

  Le entità presenti in più database OnCommand Insight vengono registrate una sola volta nel database consolidato.

- Record corrente

  I dati nel database consolidato (data mart di inventario) sono sempre i più aggiornati possibili.

Quando si aggiunge o si modifica una connessione, è anche possibile testarla. Il test esegue le seguenti

operazioni:

- Verifica l'indirizzo IP dell'host, il nome utente e la password e garantisce che sia possibile stabilire una connessione.

  Le connessioni non valide vengono visualizzate in rosso.

- Confronta la versione di OnCommand Insight con la versione del data warehouse.

  Se le versioni non sono compatibili, viene visualizzato un messaggio di errore.

- Verifica che il database OnCommand Insight non sia stato modificato o ripristinato in un database diverso come visto dall'ultima elaborazione del data warehouse. In caso di modifica, viene visualizzato un messaggio di errore.

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**.

   La tabella Connectors (connettori) appare vuota e mostra le informazioni sul connettore dopo l'aggiunta di un connettore.

3. Fare clic su **New** (nuovo) per aggiungere un nuovo connettore.
4. Immettere quanto segue:

   - **Crittografia**

     Per abilitare le richieste di Data Warehouse da effettuare utilizzando la crittografia SSL, selezionare `Enabled`.

   - **Nome**

     Un nome di connettore che identificherà il connettore nella vista connettori.

   - **Host**

     Host IP address (Indirizzo IP host)

   - **Nome utente**

     "inventory"

     > Utilizzando questo nome utente e la password, è possibile accedere al database remoto di OnCommand Insight ed eseguire query sui dati.

   - **Password**

     "SANscreen"

5. Per specificare la porta da utilizzare per le connessioni TCP all'host, fare clic su **Advanced** (Avanzate) e inserire il numero della porta TCP.

6. Per specificare la porta (diversa da quella predefinita) da utilizzare per le connessioni HTTPS all'host, fare clic su **Avanzate** e immettere il numero di porta.
7. Fare clic su **Test**.

   Data Warehouse verifica la connessione.

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

   Se si inseriscono più connessioni per installazioni multiple, Data Warehouse richiama processi di creazione indipendenti, uno per ogni database da cui estrarre i dati. Ciascun processo di creazione estrae i dati da un database OnCommand Insight e li carica nel database consolidato.

Creazione del database Data Warehouse dalla panoramica della cronologia

È possibile creare il database del data warehouse utilizzando i dati storici nel server OnCommand Insight. Data warehouse estrae i dati dai server OnCommand Insight e crea i data mart del data warehouse in base alla build dalla pianificazione della cronologia.

Questa opzione non richiede una licenza speciale e i dati di inventario sono inclusi nella build. Tuttavia, per creare informazioni sulla capacità, sono necessari il piano OnCommand Insight e le licenze OnCommand Insight Perform.

Se è già stata eseguita una build (dalla cronologia o corrente), la build non può essere eseguita in date precedenti all'ultimo job. Ciò significa che se si esegue una build corrente, non è possibile creare dalla cronologia. In particolare, se hai eseguito build della cronologia terminate il 1° gennaio 2012, non puoi eseguire alcuna build nell'anno 2011.

Se la creazione della cronologia non include uno o due giorni di processi ETL non riusciti, non tentare di creare la cronologia solo per questi giorni. I dati storici si riferiscono a periodi più lunghi e uno o due giorni non cambieranno in modo significativo i trend. Se si desidera ricostruire dalla cronologia, ricostruire l'intera cronologia.

La vista Build from History (Crea dalla cronologia) visualizza tutti i lavori di creazione da tutti i connettori. Ad esempio, la vista potrebbe visualizzare un processo di inventario per ogni connettore, un processo di capacità delle porte per ogni esecuzione di creazione e un processo di annotazioni.

Prima di configurare la build dalla cronologia, è necessario che si verifichi quanto segue:

- I connettori devono essere configurati.
- Le annotazioni devono essere inserite in OnCommand Insight e possono essere aggiornate manualmente utilizzando l'opzione **Imponi aggiornamento delle annotazioni per DWH** nel vecchio portale OnCommand Insight oppure verranno aggiornate automaticamente 15 minuti dopo l'impostazione.

Aggiunta di un job che crea un database Data Warehouse dalla cronologia

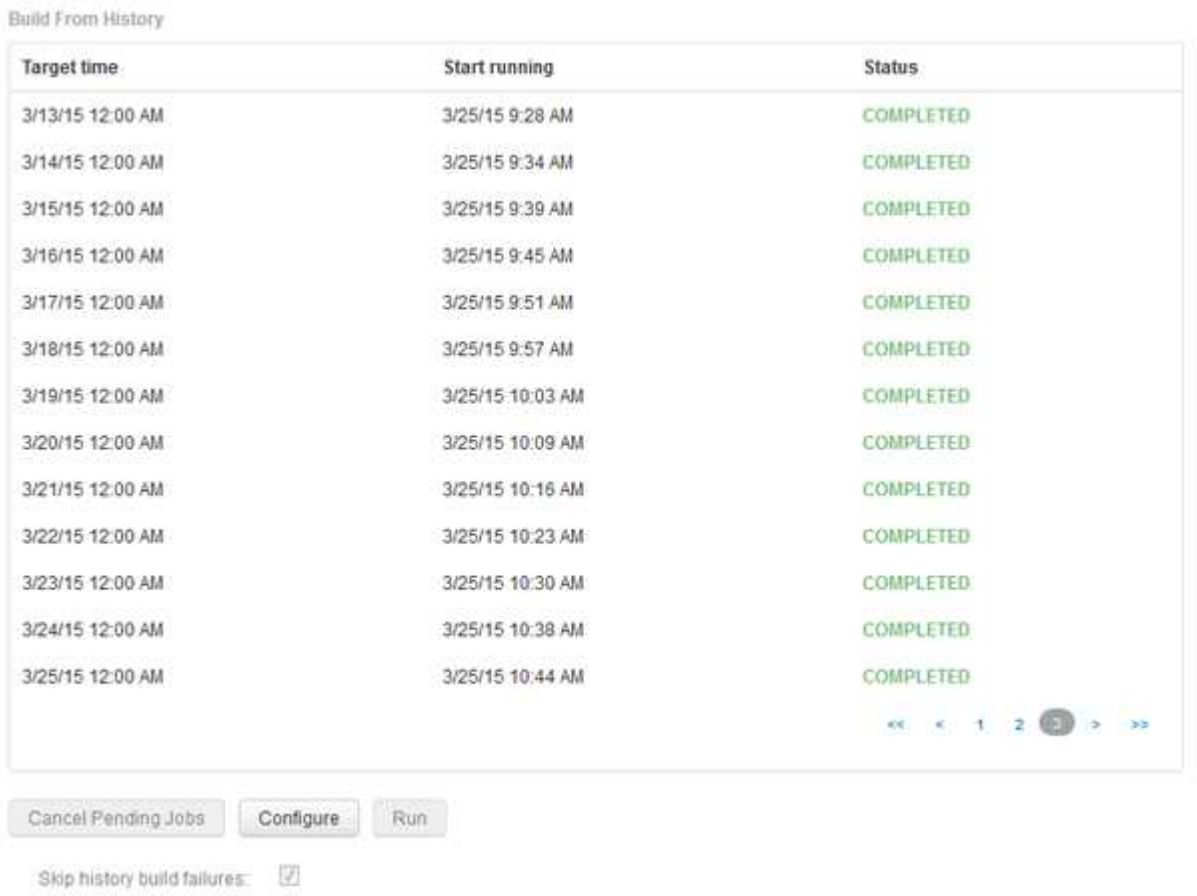
È possibile creare il database del data warehouse utilizzando i dati storici memorizzati nel server OnCommand Insight, che consentono di eseguire report di proiezione.

Prima di iniziare

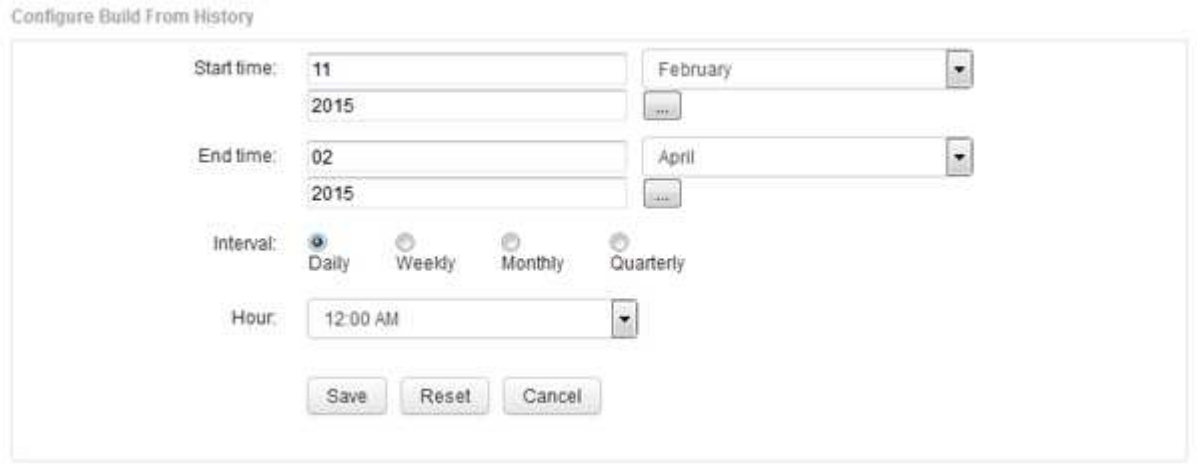
È necessario aggiornare le annotazioni nel server OnCommand Insight e forzare un aggiornamento delle informazioni di annotazione per il data warehouse.

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 **Build from History** (Crea dalla cronologia).



3. Fare clic su **Configura**.



4. Inserire l'ora di inizio e di fine.

   Per visualizzare un calendario dal quale è possibile selezionare queste date, fare clic sulla freccia rivolta verso il basso accanto al nome del mese.

Il formato dell'ora dipende dalle impostazioni internazionali del server Data Warehouse.

Gli orari di inizio e fine devono rientrare nell'intervallo di cronologia contenuto in tutti i server OnCommand Insight a cui è collegato il data warehouse, come impostato nell'opzione connettori del portale del data warehouse. Gli orari di inizio e di fine predefiniti riflettono il periodo massimo valido. Il processo di creazione del Data Warehouse viene eseguito automaticamente all'ora specificata.

> La configurazione di una pianificazione non realistica, ad esempio "Dogni giorno per 4 anni", comporta 1460 cicli di costruzione, che potrebbero richiedere 10 giorni.

5. Scegliere l'intervallo.

   Se si seleziona un intervallo mensile o settimanale, viene visualizzato il campo giorno. Se si seleziona mensile, giorno è una data. Se si seleziona Settimanale, il giorno è da domenica a sabato.

6. Scegliere l'ora in cui verrà eseguita la creazione.
7. In alternativa, per ripristinare le impostazioni predefinite delle opzioni, fare clic su **Reset** (Ripristina).
8. Fare clic su **Save** (Salva).
9. Dalla pagina **Build from History** (Crea dalla cronologia), per eseguire una build al di fuori della build di pianificazione automatica, fare clic su **Run** (Esegui).

   La colonna Target Time (ora di destinazione) visualizza l'ora in cui è stata creata questa voce. La colonna Status (Stato) indica se la creazione è stata completata o meno.

Annullamento di una build da un processo di cronologia

È possibile annullare tutti i lavori pianificati. Lo stato del lavoro diventa "Aborted".

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 **Build from History** (Crea dalla cronologia).
3. Fare clic su **Annulla**.

Backup del database Data Warehouse

È possibile eseguire il backup del database Data Warehouse, che include anche un backup di Cognos, su un file e ripristinarlo successivamente utilizzando il portale Data Warehouse. Un backup di questo tipo consente di migrare a un server Data Warehouse diverso o di eseguire l'aggiornamento a una nuova versione di Data Warehouse.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://fqdn/dwh`.
2. Dal riquadro di navigazione a sinistra, selezionare **Backup/Ripristino**.
3. Fare clic su **Backup** e selezionare la configurazione di backup:

   a. Tutti i Datamart tranne Performance Datamart

b. Tutti i Datamart

Questa operazione può richiedere 30 minuti o più.

+ Data Warehouse crea un file di backup e ne visualizza il nome.

4. Fare clic con il pulsante destro del mouse sul file di backup e salvarlo nella posizione desiderata.

   Potrebbe non essere necessario modificare il nome del file; tuttavia, è necessario memorizzare il file al di fuori del percorso di installazione di Data Warehouse.

   Il file di backup di Data Warehouse include MySQL dell'istanza DWH; schemi personalizzati (MySQL DBS) e tabelle; configurazione LDAP; origini dati che collegano Cognos al database MySQL (non le origini dati che collegano il server Insight ai dispositivi per acquisire dati); importazione ed esportazione di task che importavano o esportavano report; creazione di report su ruoli, gruppi e spazi dei nomi di sicurezza; account utente; Qualsiasi report modificato del portale di reporting e qualsiasi report personalizzato, indipendentemente dalla posizione in cui sono memorizzati, anche nella directory cartelle personali. Non viene eseguito il backup dei parametri di configurazione del sistema di Cognos, ad esempio le impostazioni del server SMTP e della memoria personalizzata di Cognos.

   Gli schemi predefiniti in cui viene eseguito il backup delle tabelle personalizzate includono quanto segue:

dwh_capacity
dwh_capacity_staging
dimensioni_dwh
dwh_fs_util
dwh_inventory
dwh_inventory_staging
dwh_inventory_transitori
gestione_dwh
dwh_performance
dwh_performance_staging
porte_dwh
report_dwh
dwh_sa_staging

Gli schemi in cui le tabelle personalizzate sono escluse dal backup includono quanto segue:

schema_informazioni
acquisizione
cloud_model
host_data
innodb
inventario
inventory_private
tempo_inventario
registri
gestione
mysql
nas
performance
schema_performance
performance_views
SANscreen
scrub
serviceassurance
test
tmp
banco di lavoro

In qualsiasi backup avviato manualmente, un `.zip` viene creato un file contenente i seguenti file:

- Un backup giornaliero `.zip` File, che contiene le definizioni dei report di Cognos
- Un backup dei report `.zip` File, che contiene tutti i report in Cognos, inclusi quelli nella directory cartelle personali
- Un file di backup del database Data Warehouse oltre ai backup manuali, che è possibile eseguire in qualsiasi momento, Cognos crea un backup giornaliero (generato automaticamente ogni giorno in un file chiamato `DailyBackup.zip`) che include le definizioni del report. Il backup giornaliero include le cartelle principali e i pacchetti forniti con il prodotto. La directory cartelle personali e le directory create al di fuori delle cartelle principali del prodotto non sono incluse nel backup di Cognos.

> A causa del modo in cui Insight nomina i file in `.zip` file, alcuni programmi di decompressione mostrano che il file è vuoto all'apertura. Fino a quando `.zip` il file ha una dimensione maggiore di 0 e non termina con a. `.bad` interno, il `.zip` il file è valido. È possibile aprire il file con un altro programma di decompressione come 7-zip o WinZip®.

Backup di report personalizzati e artefatti di report

Se sono stati creati report personalizzati in una versione di Insight precedente alla 7.0 e si desidera eseguire l'aggiornamento alla versione più recente di Insight, è necessario eseguire il backup dei report e segnalare gli artefatti prima dell'installazione dell'aggiornamento e ripristinarli dopo l'installazione dell'aggiornamento. Prestare attenzione anche alle cartelle utilizzate per memorizzare gli artefatti dei report.

A proposito di questa attività

Se sono state apportate modifiche ai report predefiniti, creare le proprie copie di tali report in una cartella separata. In questo modo, quando si aggiornano gli artefatti predefiniti, le modifiche non vengono sovrascritte.

Se si dispone di report nell'area cartelle personali, è necessario copiarli nelle cartelle rapporti personalizzati in modo che non vadano persi.

Ripristino del database Data Warehouse

È possibile ripristinare un database Data Warehouse utilizzando `.zip` File creato al momento del backup del database Data Warehouse.

A proposito di questa attività

Quando si ripristina un database Data Warehouse, è possibile ripristinare anche le informazioni dell'account utente dal backup. Le tabelle di gestione degli utenti vengono utilizzate dal motore di report Data Warehouse in un'installazione solo Data Warehouse.

Fasi

1. Accedere al Data Warehouse Portal all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema su cui è installato il data warehouse di OnCommand Insight.
2. Dal riquadro di navigazione a sinistra, fare clic su **Backup/Restore**.
3. Nella sezione **Restore Database and Reports** (Ripristina database e report), fare clic su **Browse** (Sfoglia)

e individuare `.zip` File che contiene il backup di Data Warehouse.

4. Se si desidera ripristinare i report o i dati dell'account utente, selezionare una o entrambe le seguenti caselle di controllo:

   - **Ripristinare il database**

     Include le impostazioni del Data Warehouse, i data mart, le connessioni e le informazioni sull'account utente.

   - **Ripristina report**

     Include report personalizzati, report predefiniti, modifiche apportate ai report predefiniti e impostazioni di reporting create in Reporting Portal.

     > Se il backup del database contiene un report personalizzato con una barra (/) o una parentesi aperta ([) nel nome (ad esempio, US IT Center Switch Port Boston/July), l'operazione di ripristino rinomina il report, sostituendo la barra o la parentesi aperta con un trattino basso (ad esempio, US IT Center Switch Port Boston_luglio).

5. Fare clic su **Restore** (Ripristina).

   Al termine del processo di ripristino, viene visualizzato un messaggio sotto il pulsante Restore (Ripristina). Se il processo di ripristino ha esito positivo, viene visualizzato il messaggio Success (riuscito). Se il processo di ripristino non riesce, il messaggio riporta l'eccezione specifica che ha causato l'errore. Se si verifica un'eccezione e il processo di ripristino non riesce, il database originale viene ripristinato automaticamente.

Impostazione di tenancy multiple nel reporting

Il data warehouse di OnCommand Insight consente di gestire più tenancy (spesso abbreviata in "multitenancy" o "multiancy") nel reporting, consentendo di associare gli utenti a una o più entità aziendali. Con questa funzione, gli amministratori possono separare dati o report in base agli attributi dell'utente o all'affiliazione dell'utente.

Le entità di business utilizzano una gerarchia ai fini del chargeback della capacità utilizzando i seguenti valori:

- Tenant: Utilizzato principalmente dai service provider per associare le risorse a un cliente, ad esempio NetApp.
- Line of Business (LOB): Una linea di business all'interno di un'azienda, ad esempio "hardware" o "Software".
- Business unit: Business unit tradizionale, ad esempio "Vendite" o "Marketing".
- Project (progetto): Un progetto a cui si desidera assegnare il chargeback della capacità.

Il processo di configurazione di più tenancy prevede i seguenti passaggi principali:

- Configurare un account utente Data Warehouse.
- Creare un gruppo in Reporting Portal.
- Assegnare gli utenti a uno o più gruppi, che rappresentano le entità aziendali.
- Assegnare gli utenti a una o più entità aziendali. Ad esempio, gli utenti associati a "NetApp" ottengono l'accesso a tutte le entità aziendali che hanno "NetApp" come tenant.

- Verificare che gli utenti possano visualizzare solo i report che dovrebbero visualizzare.

I seguenti punti riassumono il modo in cui gli utenti accedono ai dati di reporting:

- Un utente, non assegnato a nessun gruppo, ottiene l'accesso a tutti i dati.
- Un utente, assegnato a qualsiasi gruppo, non potrà accedere ai record senza entità aziendale.

Ad esempio, potrebbe essere necessario disporre dei seguenti reparti e separare i report per gli utenti all'interno di tali reparti.

Utente	Progettazione	Supporto	Finanza	Legale
Utente1	X	X		
Utente2			X	X
Utente3		X		

Configurazione degli account utente

Per configurare gli account utente, è necessario completare diversi passaggi.

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 **User Management** (Gestione utenti).
3. Configurare ciascun account utente.

Assegnazione di utenti a entità aziendali

È necessario completare una serie di passaggi per assegnare gli utenti alle entità aziendali. Data Warehouse consente di gestire più tenancy (spesso abbreviata in "multiancy" o "multitenancy") nel reporting, consentendo di associare gli utenti a una o più entità aziendali. Ciò consente agli amministratori di separare i dati o i report in base agli attributi dell'utente o all'affiliazione dell'utente.

Fasi

1. Accedere al Data Warehouse Portal come amministratore all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire il portale di reporting.
3. Inserire il nome utente e la password e fare clic su **Login**.
4. Dal menu Avvio, selezionare **IBM Cognos Administration**.
5. Fare clic sulla scheda **Security**:
6. Nella directory, selezionare **Cognos**.
7. Creare una nuova sottocartella nella cartella Cognos denominata "BES", per le entità aziendali.

8. Aprire la cartella BES.
9. Fare clic sull'icona **nuovo gruppo** per aggiungere gruppi che corrispondono a diversi livelli di autorizzazione.

   Questi livelli di autorizzazione possono essere il nome completo dell'entità aziendale (ad esempio, NetApp.N/A) o un prefisso (ad esempio, NetApp.N/A.Finance). Entrambi questi formati consentono l'accesso a tutti i progetti all'interno dell'entità aziendale (NetApp.N/A.Finance).

   Viene visualizzata la procedura guidata nuovo gruppo.

10. Completare le pagine della procedura guidata.
11. Selezionare un'entità aziendale e fare clic su **Altro**.
12. Fare clic su **Imposta membri**.
13. Fare clic su **Aggiungi**.
14. Selezionare la directory SANscreen.
15. Dall'elenco degli utenti, selezionare ciascun utente che si desidera includere nell'entità aziendale e aggiungerlo alla casella voci selezionate.
16. Fare clic su **OK**.
17. Ripetere il processo di aggiunta di membri a ciascuno dei gruppi di entità aziendali.

Risoluzione dei problemi di installazione

Esistono diversi problemi comuni relativi a annotazioni, build e report che potrebbero verificarsi durante la configurazione. È possibile risolvere questi problemi seguendo la procedura descritta.

Perché non riesco a vedere le mie annotazioni

Se non è possibile visualizzare le annotazioni in Data Warehouse, potrebbe essere necessario forzare un aggiornamento delle annotazioni e avviare una creazione di Data Warehouse.

Le annotazioni mancanti influiscono sul modo in cui i dati vengono importati in Data Warehouse e visualizzati nei report. Ad esempio, se l'annotazione "Tier" non è disponibile, non sarà possibile raggruppare i sistemi storage per Tier nei report Data Warehouse.

Forzare un aggiornamento delle annotazioni per Data Warehouse

È possibile avviare un aggiornamento delle annotazioni da OnCommand Insight a Data Warehouse.

A proposito di questa attività

È possibile aggiornare le annotazioni utilizzando una delle due opzioni seguenti:

- Inclusi gli oggetti cancellati: Sono inclusi i dati relativi ai dispositivi che non esistono più, ad esempio host, storage array o switch rimossi. Ciò è necessario se si desidera creare dati Data Warehouse con punti dati storici.

- Non includere gli oggetti eliminati: Selezionare questa opzione se si desidera escludere gli oggetti eliminati.

Fasi

1. Accedere al portale OnCommand Insight come amministratore `https://hostname`, dove `hostname` È il nome del sistema in cui è installato OnCommand Insight.
2. Fare clic su **Admin** > **Troubleshooting**. Nella parte inferiore della pagina, fare clic su **risoluzione avanzata dei problemi**.
3. Nella scheda **azioni**, fare clic su **Aggiorna annotazioni DWH (Includi eliminate)**.

Generazione manuale di una build di Data Warehouse

Dopo aver forzato un aggiornamento delle annotazioni (esecuzione di dati transitori) in OnCommand Insight, è necessario avviare una creazione di data warehouse. È possibile attendere fino alla successiva build pianificata o iniziare subito una build.

Fasi

1. Accedere come amministratore 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 **Schedule** (Pianificazione).
3. Fare clic su **Crea ora**.

Importazione di annotazioni definite dall'utente in Data Warehouse

Dopo aver forzato l'aggiornamento di un'annotazione in OnCommand Insight, è necessario selezionare le annotazioni desiderate in Data Warehouse e avviare una creazione di data warehouse. È possibile attendere fino alla successiva build pianificata o iniziare subito una build.

Fasi

1. Accedere come amministratore 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 **Annotazioni**.

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✔
Data_Center	dataCenter	Storage	✔
Data_Center	dataCenter	Switch	✔
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✔
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

L'elenco visualizza una riga per ogni tipo di annotazione e un oggetto di destinazione a cui è possibile assegnare l'annotazione. Un segno di spunta nella colonna pubblicata indica che l'annotazione è già stata selezionata per l'oggetto di destinazione specifico ed è già disponibile attraverso i data mart di Data Warehouse.

3. Fare clic su **Modifica** per modificare la modalità di importazione delle annotazioni da OnCommand Insight.

Edit Annotations

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	☐	☐
Data_Center	dataCenter	Host	☑	☐
Data_Center	dataCenter	Storage	☑	☐
Data_Center	dataCenter	Switch	☑	☐
Note	Note	Switch	☐	☐
Switch_Level	switchLevel	Switch	☑	☐
Tier	Tier	Internal Volume	☐	☐
Tier	Tier	Qtree	☐	☐
Tier	Tier	Storage	☐	☐
Tier	Tier	Storage Pool	☐	☐
Tier	Tier	Volume	☐	☐

Save Cancel

4. Per modificare il processo di annotazione, procedere come segue:
   - Selezionare **pubblicato** per aggiungere le annotazioni recuperate da OnCommand Insight nel database del data warehouse. Fare clic su **tutto** per selezionare tutte le annotazioni su tutti gli oggetti. Fare clic su **None** (Nessuno) per assicurarsi che tutte le opzioni non siano selezionate.

     > Deselezionare questa opzione per rimuovere la colonna di annotazione dalla tabella di inventario dell'oggetto specifico e dai grafici dei dati associati. Se qualsiasi report personalizzato utilizza i dati di annotazione, i report non vengono eseguiti correttamente.

   - Selezionare **Init with current** (Inizializza con corrente) per inizializzare i dati storici nelle tabelle delle

dimensioni del Data Warehouse con il valore di annotazione corrente. Fare clic su **tutto** per selezionare tutte le annotazioni su tutti gli oggetti. Fare clic su **None** (Nessuno) per assicurarsi che tutte le opzioni non siano selezionate. Questa casella di controllo è disattivata dopo la pubblicazione di un'annotazione; la casella di controllo è attivata per le annotazioni non pubblicate. Ad esempio, se un host è annotato con il tipo di annotazione "floor" e ottiene il valore "1" e ci sono 3 righe per quell'host nella tabella host_dimension, selezionando **Init with current** il valore "1" nella colonna "floor" per tutte e 3 le righe nella tabella host_dimension. Se non si seleziona **Init with current** (Inizializzazione con corrente), solo l'ultima riga per quell'host avrà il valore "1" nella colonna del piano.

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

   Viene visualizzato un messaggio di avviso che indica che questo causerà modifiche alla struttura dei dati o perdita di dati, se si rimuovono le annotazioni.

6. Per continuare, fare clic su **Sì**.

   Data Warehouse avvia un lavoro di annotazioni asincrone che applica le modifiche richieste. Il lavoro viene visualizzato nella pagina lavori. È inoltre possibile visualizzare le modifiche nello schema del database Data Warehouse.

Cosa fare con i punti di costruzione storici non riusciti

Puoi creare dalla cronologia, omettendo qualsiasi build non riuscita attivando l'opzione **Ignora errori di generazione della cronologia**.

In questo caso, la build dalla storia continua. Se una build non riesce e questa opzione è attivata, Data Warehouse continua la creazione e ignora le build non riuscite. In questi casi, non esiste alcun punto dati nei dati storici per nessuna build saltata. Se non si attiva questa opzione e la creazione non riesce, tutti i lavori successivi vengono interrotti.

Attività amministrative che è possibile eseguire utilizzando Data Warehouse

Data warehouse di OnCommand Insight è un'interfaccia utente basata su web che consente agli utenti di configurare e risolvere i problemi dei dati nel data warehouse di OnCommand Insight e di impostare le pianificazioni per recuperare i dati da OnCommand Insight.

Utilizzando il portale Data Warehouse, è possibile eseguire le seguenti attività amministrative:

- Verificare lo stato dei processi o delle query correnti in esecuzione
- Gestire le annotazioni
- Configurare le notifiche e-mail
- Accesso e creazione di report personalizzati
- Esaminare la documentazione e lo schema del database di Data Warehouse
- Modificare il nome del sito
- Identificare la versione di Data Warehouse e la cronologia degli aggiornamenti
- Crea i dati del data warehouse dalla cronologia

- Ripristinare il database Data Warehouse
- Eseguire il backup e il ripristino del database Data Warehouse
- Risolvere i problemi relativi al data warehouse e consultare i registri OnCommand Insight
- Gestire gli account utente

Gestione dei lavori

È possibile visualizzare un elenco dei lavori correnti e il relativo stato. Il primo lavoro di un ciclo di costruzione è in grassetto. La build che Data Warehouse esegue per ogni connettore e per ogni data mart è considerata un lavoro.

A proposito di questa attività

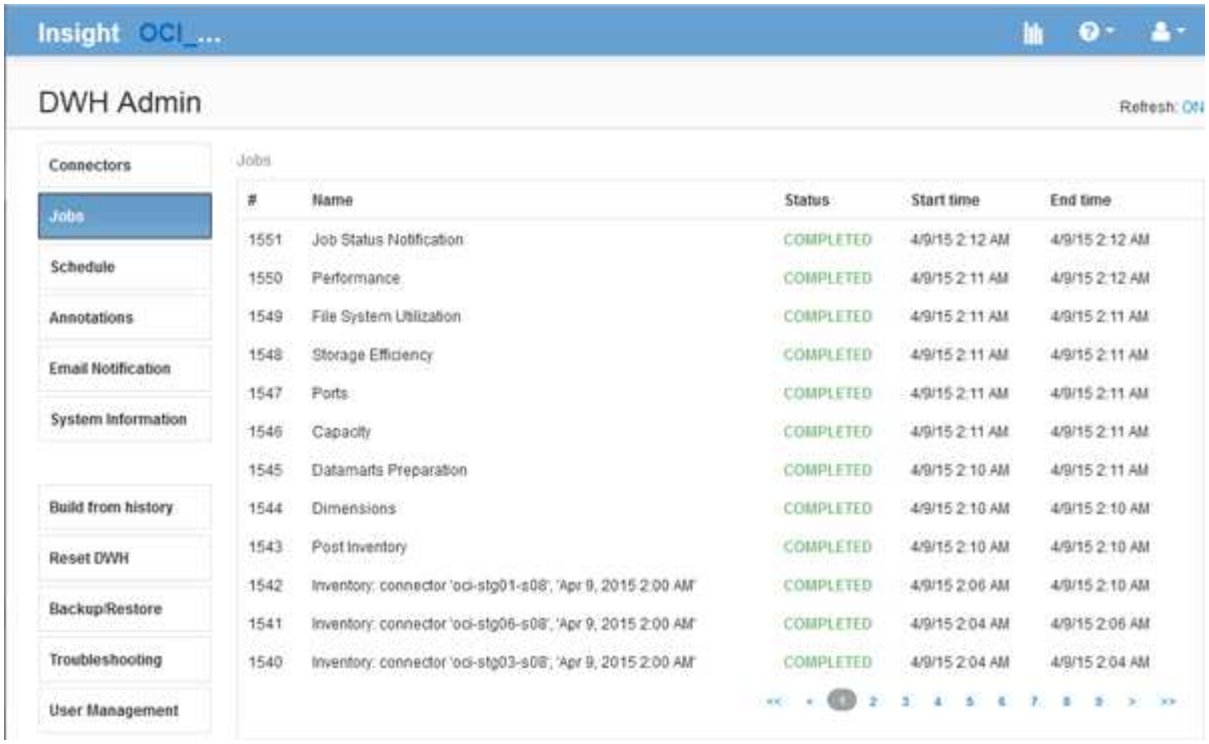
È possibile annullare qualsiasi processo in sospeso pianificato o iniziato. È inoltre possibile cancellare la cronologia dei lavori eseguiti in precedenza. È possibile cancellare la cronologia dei lavori che non sono in sospeso, in esecuzione o in corso di interruzione. È possibile cancellare tutta la cronologia o tutta la cronologia tranne le 24 ore precedenti per rimuovere tutte le voci tranne l'ultimo giorno.

È possibile visualizzare informazioni sui seguenti tipi di job: Licenza, Pre Inventory, Inventory, Post Inventory, Dimensions, Preparazione dei datamarts, capacità, porte, efficienza dello storage, utilizzo del file system, Performance, Job Status Notification, History Build, annotazioni dinamiche, rimozione del connettore, Build, Phone Home e manutenzione ignorati.

Un lavoro di manutenzione viene eseguito settimanalmente e utilizza i tool MySQL per ottimizzare il database.

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 **Jobs**.



Se viene visualizzato uno stato Pending (in sospeso), viene visualizzato il collegamento Cancel (Annulla).

3. Per annullare un processo in sospeso, fare clic su **Annulla**.
4. Per rimuovere la cronologia dei lavori, fare clic su **tutto** o **tutto tranne le ultime 24 ore**.

Monitoraggio dello stato di Data Warehouse

Il Data Warehouse (DWH) include un monitor dello stato di salute che visualizza informazioni sullo stato di DWH. I messaggi di allarme vengono visualizzati nelle pagine **connettori** e **lavori** del DWH, nonché inviati al server Insight connesso, dove vengono visualizzati nella pagina **Admin** > **Health**.

DWH raccoglie le metriche ogni dieci minuti e visualizza un allarme nelle seguenti condizioni:

- La connessione al server Insight non è attiva
- L'utilizzo del disco è superiore al 90%
- Il servizio di reporting (Cognos) non è attivo
- Una query mantiene un blocco su qualsiasi tabella per un periodo di tempo prolungato
- Un ordine di manutenzione è disattivato
- Il backup automatico è disattivato
- Rischio di protezione: Chiavi di crittografia predefinite rilevate

Gli avvisi di monitoraggio dello stato di salute nel Data Warehouse possono essere soppressi per un massimo di 30 giorni.

Quando viene attivata la notifica via email, questi eventi vengono segnalati anche tramite email. Tenere presente che l'e-mail non contiene allegati.

Questi eventi vengono registrati in `dwh_troubleshoot.log` file nelle seguenti posizioni:

- Finestre: `<install dir>\SANscreen\Wildfly\Standalone\Logs`
- Linux: `/var/log/netapp/oci/wildfly/`

Pianificazione delle build giornaliere

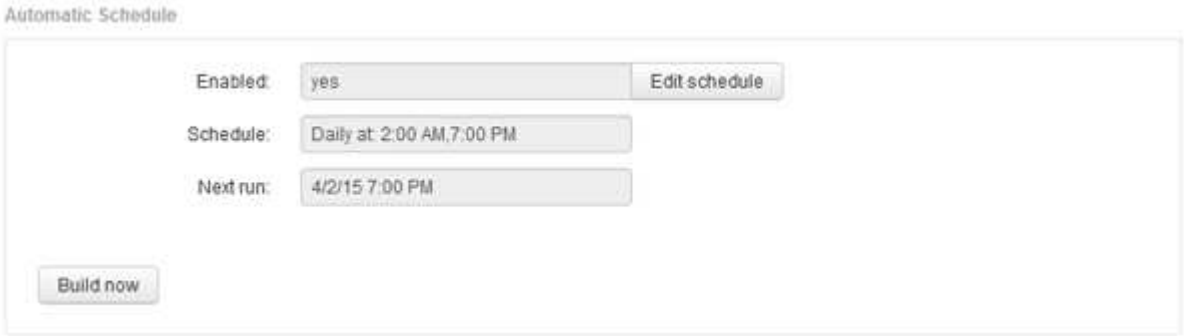
Sebbene sia possibile creare manualmente Data Warehouse utilizzando il controllo build Now in qualsiasi momento, è consigliabile pianificare le build automatiche, definendo quando e con quale frequenza creare il database Data Warehouse. Data Warehouse esegue un processo di creazione per ciascun connettore e per ciascun data mart. Data Warehouse esegue un processo di creazione per ciascun connettore per le licenze e l'inventario e tutti gli altri processi di creazione (ad esempio, la capacità) vengono eseguiti sul database consolidato.

A proposito di questa attività

Ogni volta che il Data Warehouse viene costruito, esegue un processo di inventario per ogni connettore. Una volta completati i job di inventario, Data Warehouse esegue i job per dimensioni, capacità e data mart rimanenti.

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 **Edit Schedule** (Modifica pianificazione).



3. Nella finestra di dialogo **Crea pianificazione**, fare clic su **Modifica** per aggiungere una nuova pianificazione.

4. Scegliere la frequenza - settimanale.
5. Scegliere l'ora del giorno per ogni giorno in cui si desidera eseguire il processo.
6. Scegliere N/D per i giorni in cui non si desidera eseguire la build.
7. Per attivare la pianificazione, selezionare **Enabled** (attivato).

> Se non si seleziona questa opzione, la generazione della pianificazione non viene eseguita.

8. Fare clic su **Save** (Salva).
9. Per creare data warehouse al di fuori della build pianificata automatica, fare clic su **Crea ora**.

Configurazione di una pianificazione settimanale

Sebbene sia possibile creare manualmente Data Warehouse utilizzando il controllo build Now in qualsiasi momento, è consigliabile pianificare le build automatiche, definendo quando e con quale frequenza creare il database Data Warehouse. Data Warehouse esegue un processo di creazione per ciascun connettore e per ciascun data mart. Data Warehouse esegue un processo di creazione per ciascun connettore per le licenze e l'inventario e tutti gli altri processi di creazione (ad esempio, la capacità) vengono eseguiti sul database consolidato. Con una pianificazione settimanale, è possibile specificare l'ora in cui si desidera che la build venga eseguita per ogni giorno della settimana.

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 **Edit Schedule** (Modifica pianificazione).
3. Scegliere la frequenza - settimanale.
4. Scegliere l'ora del giorno per ogni giorno in cui si desidera eseguire il processo.
5. Scegliere N/D per i giorni in cui non si desidera eseguire la build.
6. Per attivare la pianificazione, selezionare **Enabled** (attivato).

> Se non si seleziona questa opzione, la generazione della pianificazione non viene eseguita.

7. Fare clic su **Save** (Salva).
8. Per creare data warehouse al di fuori della build pianificata automatica, fare clic su **Crea ora**.

Pianificazione dei backup giornalieri

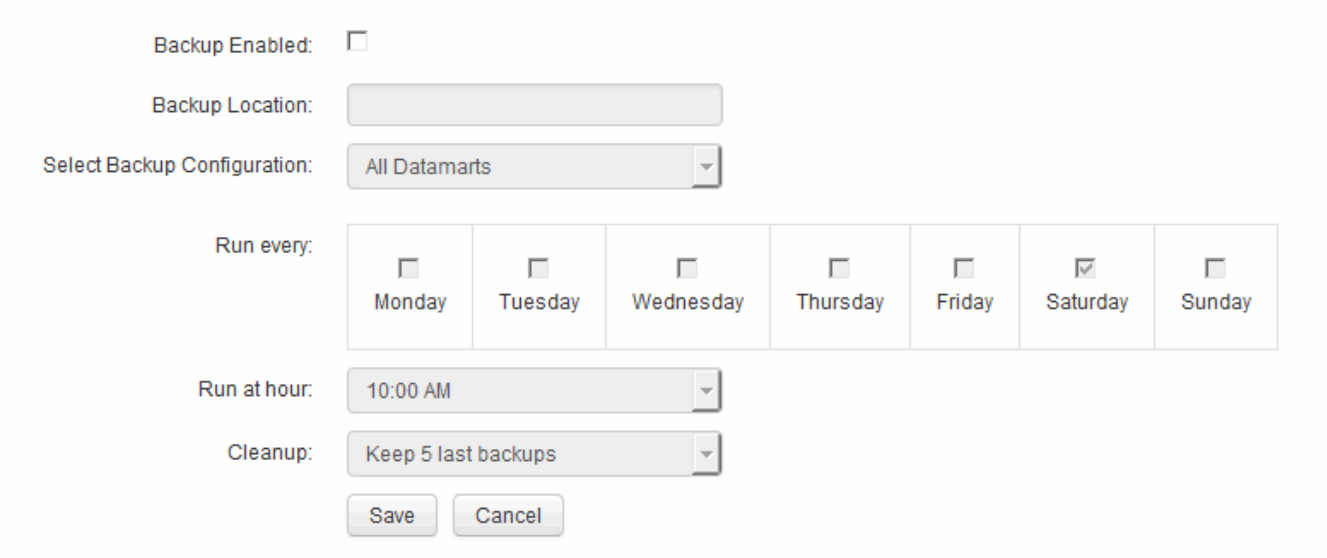
Sebbene sia possibile eseguire manualmente il backup di Data Warehouse utilizzando il controllo Backup/Restore in qualsiasi momento, è consigliabile pianificare backup automatici, definendo quando e con quale frequenza eseguire il backup del database Data Warehouse e dell'archivio di contenuti Cognos. I backup offrono protezione dalla perdita di dati, consentendo di ripristinare il database Data Warehouse, se necessario. È inoltre possibile utilizzare un backup quando si esegue la migrazione a un nuovo server Data Warehouse o quando si esegue l'aggiornamento a una nuova versione di Data Warehouse.

A proposito di questa attività

La pianificazione dei backup nei momenti in cui il server Data Warehouse non è occupato migliora le prestazioni di backup e riduce l'impatto sugli utenti.

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 **Schedule** (Pianificazione).
3. Nella finestra di dialogo **Backup Schedule**, fare clic su **Edit** (Modifica) per aggiungere una nuova pianificazione.



4. Per attivare i backup pianificati, selezionare **Backup enabled**.
5. Specificare la posizione in cui si desidera memorizzare i file di backup.
6. Specificare i dati di cui si desidera eseguire il backup.
7. Specificare il giorno o i giorni in cui si desidera eseguire il backup.

8. Specificare l'ora in cui si desidera avviare il backup.
9. Specificare il numero di copie di backup precedenti che si desidera conservare.
10. Fare clic su **Save** (Salva).

Esecuzione di script personalizzati in Data Warehouse

Data Warehouse consente ai clienti di creare lavori in grado di eseguire script personalizzati per la preparazione di dati personalizzati in Data Warehouse.

Prima di iniziare

Per evitare che lo script personalizzato venga cancellato durante un aggiornamento del data warehouse, non è necessario memorizzarlo nella directory SANscreen.

A proposito di questa attività

Il processo può specificare un solo script. È possibile eseguire più script e comandi da un unico script.

Fasi

1. In Data Warehouse, selezionare **DWH Admin** > **Schedule**.
2. Selezionare la casella di controllo **script attivato**.
3. Inserire il percorso assoluto del nome dello script nella casella di testo **posizione script**.
4. Fare clic su **Save** (Salva).

Risultati

Il motore dei processi Data Warehouse pianifica l'attività per eseguire un processo "Custom scripting". Il processo viene pianificato per essere eseguito dopo un ETL ed evitare altri processi in background in conflitto. Il processo non viene eseguito da un'operazione "build from history".

Operazioni che è possibile eseguire utilizzando le annotazioni

Le annotazioni forniscono un metodo per definire le informazioni relative agli oggetti nell'ambiente e consentono di tenere traccia degli oggetti in base all'annotazione. Ad esempio, è possibile aggiungere annotazioni sui numeri di edificio o di piano ai dispositivi dell'ambiente e creare una query che restituisca tutti i dispositivi al primo piano di un data center.

Inoltre, è possibile esaminare tutti i dispositivi di un data center o di un'entità aziendale specifica e determinare quale entità aziendale utilizza lo storage di livello 1. A tale scopo, assegnare un data center, un'entità aziendale o un'annotazione di livello al dispositivo utilizzando l'interfaccia utente Web di OnCommand Insight. Quindi, puoi portare annotazioni selezionate definite dall'utente da OnCommand Insight nel data warehouse. Questa operazione consente di visualizzare i valori di annotazione assegnati agli oggetti nei report personalizzati.

È possibile specificare quali annotazioni definite dall'utente si propagano al Data Warehouse. Le annotazioni vengono aggiunte come colonne aggiuntive alla tabella degli oggetti nell'inventario e alla tabella delle dimensioni corrispondente nei data mart. Quando si aggiornano le annotazioni sulle risorse utilizzando l'interfaccia utente di OnCommand Insight e si avvia o si attende la successiva generazione di data

warehouse, i risultati vengono visualizzati nelle seguenti tabelle:

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

Assicurarsi che le annotazioni inserite in OnCommand Insight siano incluse nel data warehouse richiede i seguenti processi principali:

- Prima di importare le annotazioni nel data warehouse, è necessario assicurarsi che siano preparate in OnCommand Insight.

  A tale scopo, è possibile eseguire manualmente l'opzione **Troubleshooting** > **Force Update of Annotations for Data Warehouse** (risoluzione dei problemi* > **Force Update of Annotations for Data Warehouse**) o attendere il successivo processo di esecuzione dei dati temporanei pianificato. Quando si forza l'aggiornamento delle annotazioni, si forza il server OnCommand Insight a calcolare e posizionare i dati transitori (come i valori delle annotazioni) nelle tabelle del database in modo che il processo ETL del data warehouse possa leggere i dati. L'aggiornamento dei dati delle annotazioni avviene automaticamente ogni quindici minuti; tuttavia, è possibile forzarne l'esecuzione più frequente.

- È quindi possibile importare le annotazioni in Data Warehouse utilizzando l'opzione **Annotazioni** Data Warehouse.
- Se si desidera includere annotazioni nei report creati utilizzando gli strumenti di creazione dei report del portale di reporting di OnCommand Insight, è necessario aggiornare il modello di metadati dei report di OnCommand Insight.

Quando si aggiorna Data Warehouse, il processo di annotazione viene eseguito automaticamente durante il processo di ripristino del database. Il job di annotazioni viene eseguito automaticamente anche all'avvio di WildFly.

> WildFly è un application server in cui viene eseguito il codice Java OnCommand Insight ed è necessario sia per il server OnCommand Insight che per il data warehouse.

Preparazione delle annotazioni in OnCommand Insight

Le annotazioni devono essere preparate in OnCommand Insight prima di poter essere importate nel data warehouse.

Fasi

1. Accedere al portale OnCommand Insight come amministratore `https://hostname`, dove `hostname` È il nome del sistema in cui è installato OnCommand Insight.
2. Fare clic su **Admin** > **Troubleshooting**. Nella parte inferiore della pagina, fare clic su **risoluzione avanzata dei problemi**.
3. Nella scheda **azioni**, fare clic su **Aggiorna annotazioni DWH (Includi eliminate)**.

Importazione di annotazioni definite dall'utente in Data Warehouse

Dopo aver forzato l'aggiornamento di un'annotazione in OnCommand Insight, è necessario selezionare le annotazioni desiderate in Data Warehouse e avviare una creazione di data warehouse. È possibile attendere fino alla successiva build pianificata o iniziare subito una build.

Fasi

1. Accedere come amministratore 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 **Annotazioni**.

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✔
Data_Center	dataCenter	Storage	✔
Data_Center	dataCenter	Switch	✔
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✔
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

L'elenco visualizza una riga per ogni tipo di annotazione e un oggetto di destinazione a cui è possibile assegnare l'annotazione. Un segno di spunta nella colonna pubblicata indica che l'annotazione è già stata selezionata per l'oggetto di destinazione specifico ed è già disponibile attraverso i data mart di Data Warehouse.

3. Fare clic su **Modifica** per modificare la modalità di importazione delle annotazioni da OnCommand Insight.

Edit Annotations

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	☐	☐
Data_Center	dataCenter	Host	☑	☐
Data_Center	dataCenter	Storage	☑	☐
Data_Center	dataCenter	Switch	☑	☐
Note	Note	Switch	☐	☐
Switch_Level	switchLevel	Switch	☑	☐
Tier	Tier	Internal Volume	☐	☐
Tier	Tier	Qtree	☐	☐
Tier	Tier	Storage	☐	☐
Tier	Tier	Storage Pool	☐	☐
Tier	Tier	Volume	☐	☐

Save Cancel

4. Per modificare il processo di annotazione, procedere come segue:
   - Selezionare **pubblicato** per aggiungere le annotazioni recuperate da OnCommand Insight nel database del data warehouse. Fare clic su **tutto** per selezionare tutte le annotazioni su tutti gli oggetti. Fare clic su **None** (Nessuno) per assicurarsi che tutte le opzioni non siano selezionate.

> Deselezionare questa opzione per rimuovere la colonna di annotazione dalla tabella di inventario dell'oggetto specifico e dai grafici dei dati associati. Se qualsiasi report personalizzato utilizza i dati di annotazione, i report non vengono eseguiti correttamente.

- Selezionare **Init with current** (Inizializza con corrente) per inizializzare i dati storici nelle tabelle delle dimensioni del Data Warehouse con il valore di annotazione corrente. Fare clic su **tutto** per selezionare tutte le annotazioni su tutti gli oggetti. Fare clic su **None** (Nessuno) per assicurarsi che tutte le opzioni non siano selezionate. Questa casella di controllo è disattivata dopo la pubblicazione di un'annotazione; la casella di controllo è attivata per le annotazioni non pubblicate. Ad esempio, se un host è annotato con il tipo di annotazione "floor" e ottiene il valore "1" e ci sono 3 righe per quell'host nella tabella host_dimension, selezionando **Init with current** il valore "1" nella colonna "floor" per tutte e 3 le righe nella tabella host_dimension. Se non si seleziona **Init with current** (Inizializzazione con corrente), solo l'ultima riga per quell'host avrà il valore "1" nella colonna del piano.

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

   Viene visualizzato un messaggio di avviso che indica che questo causerà modifiche alla struttura dei dati o perdita di dati, se si rimuovono le annotazioni.

6. Per continuare, fare clic su **Sì**.

   Data Warehouse avvia un lavoro di annotazioni asincrone che applica le modifiche richieste. Il lavoro viene visualizzato nella pagina lavori. È inoltre possibile visualizzare le modifiche nello schema del database Data Warehouse.

Visualizzazione del lavoro Annotazioni nell'elenco lavori

È possibile visualizzare il job Annotations (Annotazioni) nell'elenco Jobs (lavori) e applicare le modifiche dell'annotazione ai data mart di Data Warehouse.

Fasi

1. Accedere come amministratore 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 **Jobs**.

Visualizzazione delle modifiche delle annotazioni nello schema del database

Lo schema del database riflette le modifiche apportate nella tabella specifica.

A proposito di questa attività

Ad esempio, se si aggiungono annotazioni a un array di storage, queste vengono visualizzate nella tabella dello storage o dello switch nell'inventario o in altri data mart.

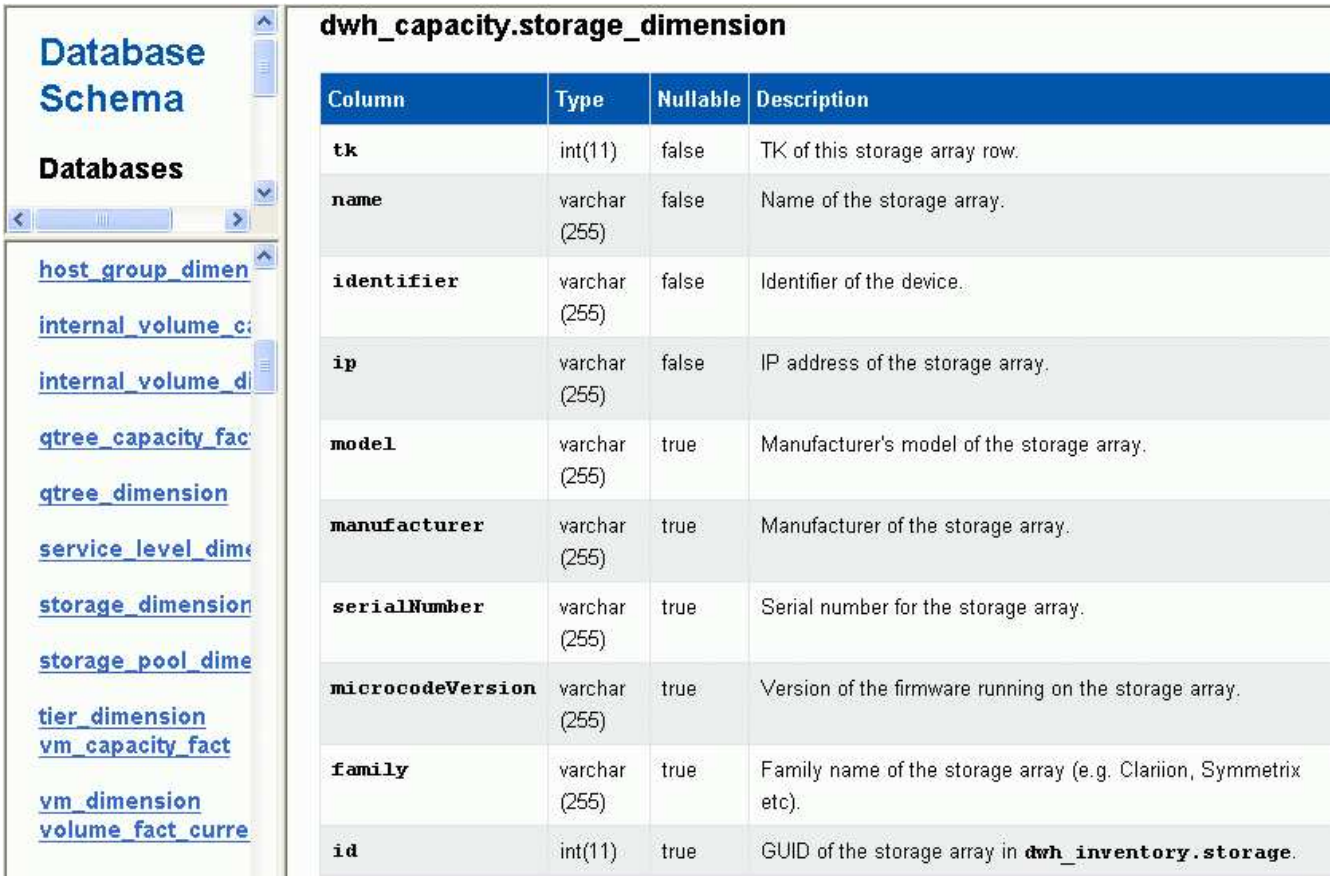
Se si aggiornano le annotazioni sulle risorse utilizzando l'interfaccia utente di OnCommand Insight e si avvia o si attende la successiva generazione del data warehouse, viene visualizzata una nuova colonna aggiunta o rimossa nell'oggetto corrispondente nell'inventario (dwh_Inventory) e anche nella tabella delle dimensioni corrispondente (nel data mart appropriato). I risultati vengono visualizzati nelle seguenti tabelle:

- dwh_inventory.annotation_value
- dwh_inventory.object_to_annotation

Fasi

1. Fare clic su Sulla barra degli strumenti Data Warehouse e selezionare **documentazione**.
2. Selezionare **Schema database**.
3. Nel riquadro **Schema database** a sinistra, scorrere fino alla sezione **DWH_INVENTORY** e fare clic su **switch**.

4. La tabella **dwh_Inventory.switch** riflette le modifiche:



Column	Type	Nullable	Description
tk	int(11)	false	TK of this storage array row.
name	varchar (255)	false	Name of the storage array.
identifier	varchar (255)	false	Identifier of the device.
ip	varchar (255)	false	IP address of the storage array.
model	varchar (255)	true	Manufacturer's model of the storage array.
manufacturer	varchar (255)	true	Manufacturer of the storage array.
serialNumber	varchar (255)	true	Serial number for the storage array.
microcodeVersion	varchar (255)	true	Version of the firmware running on the storage array.
family	varchar (255)	true	Family name of the storage array (e.g. Clariion, Symmetrix etc).
id	int(11)	true	GUID of the storage array in dwh_inventory.storage.

La colonna di annotazione del data center viene visualizzata nella tabella storage_dimensions.

Impostazione delle notifiche e-mail

È possibile fare in modo che Data Warehouse invii un'e-mail a un indirizzo e-mail specifico quando i processi Data Warehouse non vengono completati correttamente.

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 **Email Notification** (notifica e-mail).
3. Immettere quanto segue:
   - Indirizzo del server SMTP

     Specifica il server che funge da server SMTP nell'organizzazione, identificato utilizzando un nome host o un indirizzo IP utilizzando il formato nnn.nnn.nnn.nnn.nnn. Se si specifica un nome host, assicurarsi che il DNS sia in grado di risolverlo.

   - Nome utente e password del server SMTP

     Specifica il nome utente per accedere al server di posta elettronica ed è richiesto solo se il server SMTP richiede l'accesso di un utente al server. Si tratta dello stesso nome utente utilizzato per accedere all'applicazione e all'e-mail.

- Notifiche attivate

  Sì attiva le notifiche; **No** disattiva le notifiche.

- Email del mittente

  Specifica l'indirizzo e-mail utilizzato per inviare le notifiche. Deve essere un indirizzo e-mail valido all'interno dell'organizzazione.

- Email del destinatario

  Specifica l'indirizzo e-mail o gli indirizzi della persona o delle persone che riceveranno sempre l'e-mail. Separare più indirizzi con virgole.

- Oggetto dell'e-mail

  Specifica l'oggetto della notifica.

- Firma e-mail

  Specifica le informazioni visualizzate nella parte inferiore del messaggio di posta elettronica, ad esempio il nome del reparto.

Accesso al portale di reporting

Dal portale Data Warehouse è possibile accedere al portale Reporting, dove è possibile creare report personalizzati utilizzando strumenti di creazione report come Workspace Advanced e Report Studio.

Fasi

1. Nella barra degli strumenti Data Warehouse, fare clic su Per aprire Insight Reporting Portal.
2. Inserire il nome utente e la password e fare clic su **Login**.

Visualizzazione della documentazione relativa allo schema del database Data Warehouse

È possibile rivedere le informazioni sullo schema del database Data Warehouse.

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. Nella barra degli strumenti Data Warehouse, fare clic su E selezionare **Schema**.

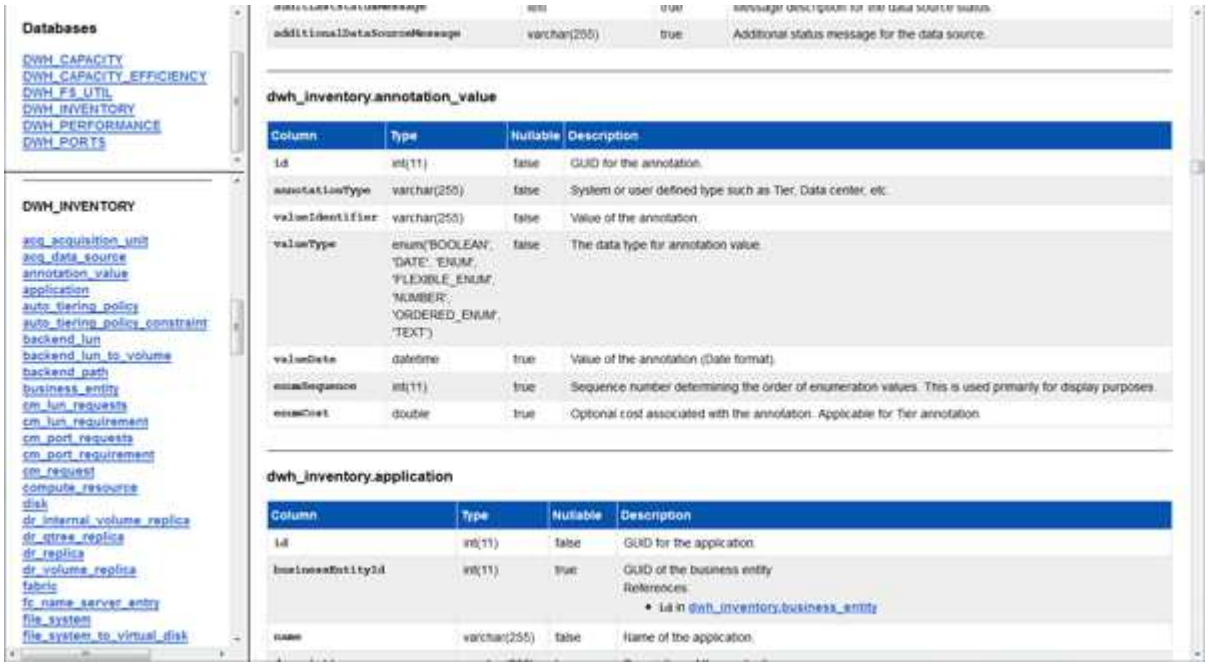
Visualizzazione dello schema del database Data Warehouse

È possibile visualizzare lo schema del database per comprendere come utilizzare i dati in un'altra API o sviluppare query SQL. L'opzione schema elenca tutti i database, le tabelle e le colonne nello schema. È inoltre possibile esaminare i diagrammi dello schema del

database che mostrano le relazioni della tabella.

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. Fare clic su Nella barra degli strumenti Data Warehouse, selezionare **documentazione**.
3. Selezionare **Schema database**.
4. Ad esempio, nel riquadro **Databases**, fare clic su **DWH_INVENTORY**.
5. Nel riquadro **All tables** (tutte le tabelle), scorrere verso il basso fino alla sezione **DWH_INVENTORY** e fare clic sulla tabella **annotation_value**.



Viene visualizzata la tabella dwh_inventory.annotation.

Visualizzazione delle informazioni di sistema

È possibile visualizzare le informazioni di aggiornamento di sistema, modulo, licenza e Data Warehouse.

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 **System Information** (informazioni di sistema).
3. Nella scheda **sistema**, esaminare le informazioni di sistema e modificare il nome del sito, se necessario, effettuando le seguenti operazioni:
   a. Fare clic su **Edit Site Name** (Modifica nome sito)
   b. Inserire il nuovo nome del sito e fare clic su **Save** (Salva).

4. Per visualizzare le informazioni sull'applicazione (nome dell'applicazione, modulo, versione e data di installazione), fare clic sulla scheda **Info applicazione**.
5. Per visualizzare le informazioni sulla licenza (protocollo, codice, data di scadenza e quantità), fare clic sulla scheda **Licenses** (licenze).
6. Per visualizzare le informazioni sull'aggiornamento dell'applicazione (nome dell'applicazione, da data, a data, ora, utente, E dimensione del file), fare clic su **Cronologia aggiornamenti**.

Opzioni avanzate

Data Warehouse include diverse opzioni avanzate.

Saltare le build non riuscite

Dopo la prima generazione, a volte si potrebbe riscontrare una build non riuscita. Per garantire che tutti i lavori dopo una creazione non riuscita siano stati completati correttamente, è possibile attivare l'opzione **Ignora errori di creazione della cronologia**.

A proposito di questa attività

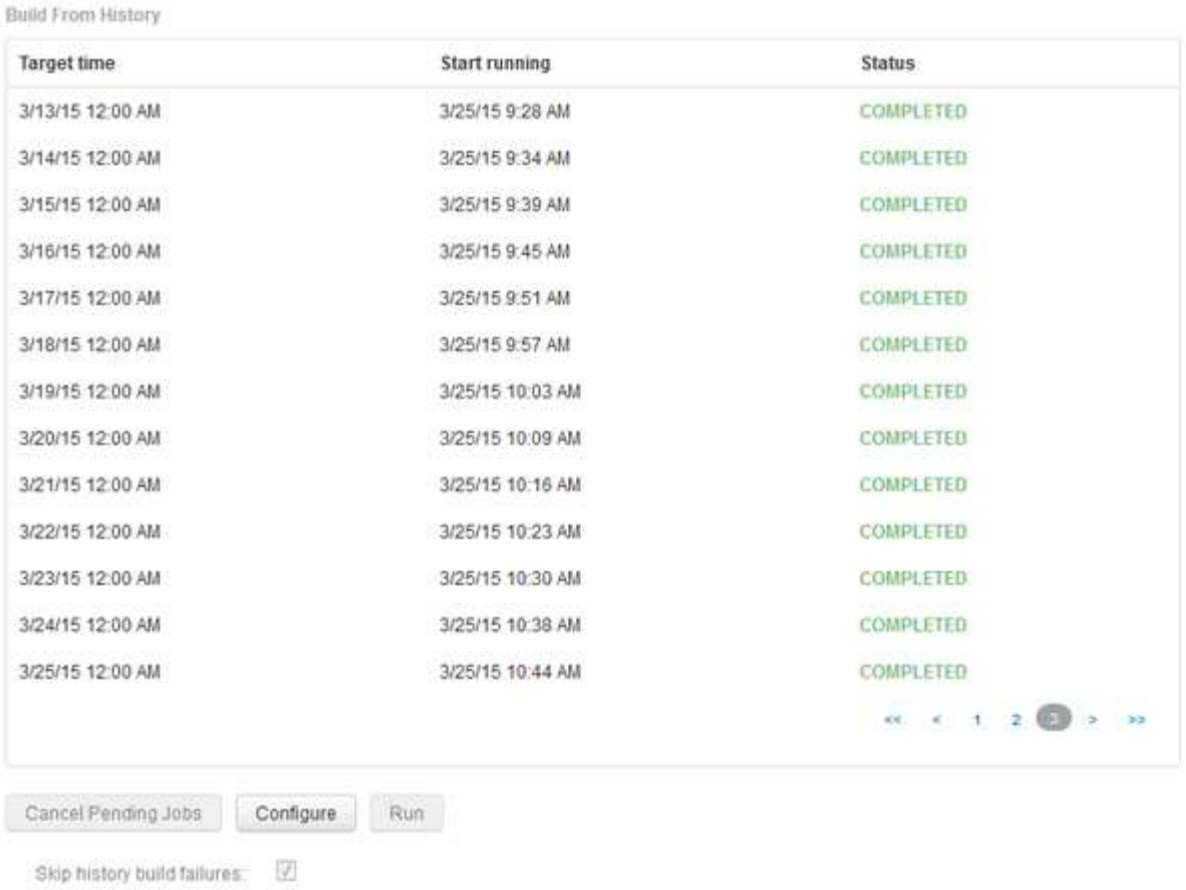
Se una build non riesce e l'opzione **Skip history build failures** è attivata, Data Warehouse continua a costruire e ignora le build guaste. In questo caso, non ci sarà un punto dati nei dati storici per nessuna build saltata.

Utilizzare questa opzione solo se la creazione non riesce.

Se una build non riesce nella generazione dalla cronologia e la casella di controllo **Ignora errori di creazione della cronologia** non è selezionata, tutti i processi successivi vengono interrotti.

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 **build from history** (Crea dalla cronologia).



3. Fare clic su **Configura**.
4. Configurare la build.
5. Fare clic su **Save** (Salva).
6. Per ignorare le build non riuscite, selezionare **Ignora errori di generazione della cronologia**.

   Questa casella di controllo viene visualizzata solo se il pulsante **Esegui** è attivato.

7. Per eseguire una build al di fuori della build pianificata automatica, fare clic su **Esegui**.

Reimpostazione del database Data Warehouse o del server di reporting

È possibile eliminare il contenuto dei data mart di Data Warehouse ed eliminare tutti i connettori configurati. Questa operazione potrebbe essere utile se un'installazione o un aggiornamento non sono stati completati correttamente e il database Data Warehouse è stato lasciato in uno stato intermedio. È inoltre possibile eliminare solo il modello di dati Inventory o il modello di dati Cognos Reporting.

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 **Reset DWH database** (Ripristina database DWH).
3. Fare clic su una delle seguenti opzioni:

- **Ripristinare il database DWH**

  In questo modo si elimina il contenuto di tutti i data mart del Data Warehouse e di tutti i connettori configurati e si posiziona il Data Warehouse nello stato di installazione predefinito senza alcuna configurazione personalizzata. È possibile scegliere questa opzione, ad esempio, se sono stati modificati i server connessi, ma è stato accidentalmente ripristinato un database Data Warehouse diverso sul server e se è necessario tornare allo stato di installazione predefinito. In questo modo non vengono cancellati i report. (I report vengono salvati nell'archivio contenuti di Cognos.)

- **Ripristina solo inventario**

  In questo modo si elimina solo il contenuto del modello di dati di inventario. In questo modo non vengono cancellati i dati storici.

- **Ripristina contenuto report**

  In questo modo viene ripristinato il contenuto del server di reporting. In questo modo vengono eliminati eventuali report personalizzati. Eseguire il backup dei report prima di scegliere questa opzione.

Viene visualizzato un messaggio di avviso.

4. Per continuare, fare clic su **Sì**.

Ripristino e aggiornamento dei report per le versioni precedenti alla 6.3

Se si sta aggiornando una versione di Insight precedente alla 6.3, è necessario ripristinare manualmente gli artefatti di reporting.

Prima di iniziare

Seguire le istruzioni riportate negli argomenti "aggiornamento del data warehouse (DWH)" e "Backup di report personalizzati e artefatti di reporting".

Fasi

1. Per ripristinare gli artefatti di reporting dalle release precedenti alla versione 6.3, copiare il file Export Backup.zip creato e memorizzato nel `<install>\cognos\c10_64\deployment` directory.
2. Aprire un browser e accedere a. `http://<server>:<port>/reporting` per il server e la porta utilizzati durante l'installazione.
3. Inserire il nome utente e la password e fare clic su **Login**.
4. Dal menu **Launch**, selezionare **Insight Reporting Administration**.
5. Fare clic sulla scheda **Configurazione**.

   A causa delle modifiche apportate al modello di dati, i report nei vecchi pacchetti potrebbero non essere eseguiti e devono essere aggiornati.

6. Fare clic su **Content Administration** (Amministrazione contenuti).
7. Fare clic sul pulsante **New Import** (Nuova importazione).
8. Assicurarsi che l'archivio sia stato copiato nella directory di distribuzione (ad esempio, `backup6.0.zip`) E fare clic su **Avanti**.
9. Se è stata immessa una password per proteggere l'archivio, inserire la password e fare clic su **OK**.

10. Modificare il nome `Export...` a. `Import Backup` E fare clic su **Avanti**.
11. Fare clic sull'icona a forma di matita accanto al nome di ciascun pacchetto e, se necessario, inserire un nuovo nome di destinazione. Ad esempio, aggiungere un `_original` suffisso al nome esistente. Quindi fare clic su **OK**.
12. Dopo aver rinominato i nomi dei pacchetti di destinazione per tutti i pacchetti, selezionare tutte le cartelle blu e fare clic su **Avanti** per continuare.
13. Accettare tutti i valori predefiniti.
14. Fare clic su **fine**, quindi selezionare **Esegui**.
15. Verificare i dettagli dell'importazione e fare clic su **OK**.
16. Fare clic su **Refresh** (Aggiorna) per visualizzare lo stato dell'importazione.
17. Fare clic su **Close** (Chiudi) al termine dell'importazione.

Risultati

Nella scheda cartelle pubbliche vengono visualizzati due set di pacchetti. Ad esempio, uno con un `7.0` suffisso (per la versione più recente) e uno con un `_original` (o qualsiasi altro elemento inserito durante la procedura di backup/ripristino) suffisso che contiene i vecchi report. A causa delle modifiche apportate al modello di dati, i report nei vecchi pacchetti potrebbero non essere eseguiti e devono essere aggiornati. Le schede del portale indicano ora la versione corrente delle pagine del portale.

Accesso a MySQL tramite l'interfaccia a riga di comando

Oltre ad accedere agli elementi dei dati di Data Warehouse attraverso i tool di creazione dei report, puoi ottenere l'accesso agli elementi dei dati di Data Warehouse direttamente connettendoti come utente MySQL. È possibile connettersi come utente MySQL per utilizzare gli elementi dati nelle proprie applicazioni.

A proposito di questa attività

Esistono diversi modi per connettersi. I seguenti passaggi mostrano un modo.

Quando si accede a MySQL, connettersi al database MySQL sulla macchina in cui è installato Data Warehouse. La porta MySQL è 3306 per impostazione predefinita; tuttavia, è possibile modificarla durante l'installazione. Il nome utente e la password sono dwhuser/netapp123.

Fasi

1. Sul computer in cui è installato Data Warehouse, aprire una finestra della riga di comando.
2. Accedere alla directory MySQL nella directory OnCommand Insight.
3. Digitare il seguente nome utente e password: `mysql -udwhuser -pnetapp123`

   A seconda di dove è installato Data Warehouse, viene visualizzato quanto segue:

   ```
   c:\Program Files\SANscreen\mysql\bin> mysql -udwhuser -pnetapp123
   ```

```
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 882
Server version: 5.1.28-rc-community MySQL Community Server (GPL)
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

4. Mostra i database del data warehouse: `show databases;`

   Viene visualizzato quanto segue:

```
mysql> show databases;
+-------------------------+
| Database                |
+-------------------------+
| information_schema      |
| dwh_capacity            |
| dwh_capacity_efficiency |
| dwh_fs_util             |
| dwh_inventory           |
| dwh_performance         |
| dwh_ports               |
+-------------------------+
```

Risoluzione dei problemi di Data Warehouse

È possibile eseguire varie attività relative alla risoluzione dei problemi di Data Warehouse.

- Utilizzare OnCommand Insight ASUP.
- Visualizzare i log di OnCommand Insight.
- Risolvere i problemi relativi agli aggiornamenti e alle entità aziendali.
- Risolvere i problemi relativi al consolidamento di più server OnCommand Insight.

È possibile consolidare più server OnCommand Insight nello stesso database del data warehouse. Molte configurazioni possono riportare lo stesso oggetto da più connettori (ovvero, lo stesso switch esiste in due istanze di OnCommand Insight). In questi casi, Data Warehouse consolida più oggetti in uno (viene scelto un connettore primario e i dati dell'oggetto vengono presi solo da quel connettore).

L'amministratore dello storage può utilizzare la pagina risoluzione dei problemi per risolvere i problemi relativi al consolidamento.

Risoluzione dei problemi con ASUP

È possibile inviare i registri ASUP al supporto tecnico per ricevere assistenza nella

risoluzione dei problemi. ASUP for Data Warehouse è configurato per l'esecuzione automatica. In Data Warehouse Portal, è possibile disattivare il processo di invio automatico, scegliere di includere un backup del database Data Warehouse o avviare una trasmissione ad ASUP.

Le informazioni contenute nei registri vengono inoltrate al supporto tecnico utilizzando il protocollo HTTPS. Nessun dato viene inoltrato tramite ASUP, a meno che non venga prima configurato su Insight Server.

Data warehouse invia i log al server OnCommand Insight che è il primo connettore elencato nella pagina connettori del portale del data warehouse. Il processo automatico invia i seguenti file:

- Registri di Data Warehouse, che includono:
  - boot.log (backup inclusi)
  - dwh.log (inclusi backup come dwh.log.1)
  - dhw_troubleshoot.log
  - dwh_upgrade.log (backup inclusi)
  - WildFly.log (backup inclusi)
  - ldap.log (backup inclusi)
  - Dump SQL del database di gestione del Data Warehouse
  - mysql: my.cnf, .err e slow query log
  - stato innodb completo
- I log di Cognos, che includono:
  - cognos-logs.zip

    Contiene i file di log di Cognos di `<install>\cognos\c10_64\logs` directory. Contiene inoltre i log generati da Cognos e il file OnCommand InsightAP.log che contiene tutti i log degli utenti che accedono e disconnettono dal reporting di OnCommand Insight.

  - DailyBackup.zip

    Contiene il backup degli artefatti di reporting nelle cartelle pubbliche. Il contenuto delle cartelle personali non è incluso in questo documento.

  - cognos_`version_site name`_content_store.zip

    Contiene un backup completo dell'archivio contenuti di Cognos.

È possibile generare manualmente un report per la risoluzione dei problemi. Il file .zip del report per la risoluzione dei problemi contiene le seguenti informazioni sul data warehouse:

- boot.log (backup inclusi)
- dwh.log (inclusi backup come dwh.log.1)
- dwh_upgrade.log (backup inclusi)
- wildfly.log (backup inclusi)
- ldap.log (backup inclusi)
- Dump dei file in c: File di programma/SANscreen/wildfly/standalone/log/dwh

- Dump SQL del database di gestione del Data Warehouse
- mysql: my.cnf, .err e slow query log
- stato innodb completo

> ASUP non invia automaticamente al supporto tecnico un backup del database OnCommand Insight.

Disattivazione delle trasmissioni automatiche ASUP

Tutti i prodotti NetApp sono dotati di funzionalità automatizzate per fornire il miglior supporto possibile per la risoluzione dei problemi che si verificano nel tuo ambiente. ASUP invia periodicamente informazioni specifiche predefinite al supporto clienti. Per impostazione predefinita, ASUP è attivato per Data Warehouse; tuttavia, è possibile disattivarlo se non si desidera più inviare le informazioni.

Fasi

1. Dal riquadro di navigazione a sinistra, fare clic su **risoluzione dei problemi**.
2. Fare clic su **Disable** (Disattiva) per impedire ad ASUP di inviare un report giornaliero.

   Viene visualizzato il messaggio ASUP is disabled (ASUP disattivato).

Incluso un backup del database Data Warehouse

Per impostazione predefinita, ASUP invia al supporto tecnico solo i file di log di Data Warehouse per assistenza nella risoluzione dei problemi; tuttavia, è possibile anche scegliere di includere un backup del database Data Warehouse e selezionare il tipo di dati da inviare.

Fasi

1. Accedere al portale Data Warehouse 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 **risoluzione dei problemi**.
3. Per specificare che ASUP deve includere un backup del database Data Warehouse, fare clic sull'elenco **include DWH Database Backup** (Includi backup database DWH) e selezionare una delle seguenti opzioni per il tipo di dati che il backup deve includere:
   - Tutti (incluse le performance)
   - Tutti tranne Performance
   - Solo inventario
4. Fare clic su **Aggiorna**.

Invio dei registri Insight ad ASUP

È possibile inviare i registri ASUP al supporto tecnico per ricevere assistenza nella risoluzione dei problemi. ASUP for Data Warehouse è configurato per l'esecuzione

automatica. Nel portale Data Warehouse, è possibile disattivare il processo di invio automatico, scegliere di includere un backup del database Data Warehouse o avviare una trasmissione ad ASUP. Quando si richiede un report ASUP, la richiesta di report viene visualizzata come job nella pagina Jobs del portale Data Warehouse.

A proposito di questa attività

Il lavoro viene gestito dalla coda dei lavori in modo simile all'elaborazione di altri lavori. Se un lavoro ASUP è già in uno stato in sospeso o in esecuzione, viene visualizzato un messaggio di errore che indica che la richiesta di report ASUP non può essere aggiunta alla richiesta di lavoro, perché la coda contiene richieste in sospeso o in esecuzione.

Fasi

1. Accedere al portale Data Warehouse 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 **risoluzione dei problemi**.
3. Nella sezione **OnCommand Insight ASUP** della pagina **risoluzione dei problemi**, fare clic su **Scarica report di risoluzione dei problemi DWH** per recuperare il report di risoluzione dei problemi.
4. Per inviare il report al server OnCommand Insight elencato come primo connettore nella pagina **connettori** del portale del data warehouse, fare clic su **Invia ora**.

Visualizzazione dei registri OnCommand Insight

In OnCommand Insight è possibile visualizzare diversi log di data warehouse e Cognos.

A proposito di questa attività

È possibile esaminare le informazioni relative alla risoluzione dei problemi e allo stato nei file di log di Cognos e Data Warehouse.

Fasi

1. Accedere al portale Data Warehouse all'indirizzo `https://hostname/dwh`, dove `hostname` È il nome del sistema in cui è installato il data warehouse di OnCommand Insight.
2. Nel riquadro di navigazione a sinistra, fare clic su **risoluzione dei problemi**.
3. Nella sezione **Logs**, fare clic su **Log Files**.

   Vengono visualizzati i seguenti file di log:

dwh.log
Elenca lo stato dei job di Data Warehouse
wildfly.log
Fornisce informazioni sul server applicativo WildFly

registro dwh_upgrade	
Fornisce informazioni sull'aggiornamento su Data Warehouse	
ldap.log	
Registra i messaggi relativi all'autenticazione LDAP	
dwh_troubleshoot.log	
Registra i messaggi che possono aiutare a risolvere i problemi di DWH	
sanscreenap.log	
Fornisce informazioni sulla connessione al server, l'autenticazione e l'accesso al repository Cognos e informazioni su altri processi	
cognosserver.log	
Log di Cognos	

4. Fare clic sul nome del file di log che si desidera visualizzare.

Problemi di consolidamento di più chassis server

È possibile visualizzare i connettori che riportano gli host e gli adattatori, gli switch SAN e gli array di storage. È inoltre possibile visualizzare i vari connettori che riportano un oggetto e identificano il connettore primario, che è il connettore scelto per l'oggetto.

Visualizzazione di problemi di consolidamento di host e adattatori

I dati riportati per gli host e gli adattatori associati sono derivati dal data mart di inventario.

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. Nel riquadro di navigazione a sinistra, fare clic su **risoluzione dei problemi**.
3. Nella sezione **consolidamento chassis**, fare clic su **host e adattatori**.

> La configurazione illustrata in questo esempio non è valida. I connettori principali e disponibili sull'host locale suggeriscono che Insight Server e DWH siano entrambi installati sullo stesso server. Lo scopo di questo esempio è quello di familiarizzare con la tabella di consolidamento.

Hosts and Adapters Consolidation

Filter

Host GUID	Host Name	Host IP	Adapter GUID	Adapter WWN	Principal Connector	Available Connectors	Insight ID	Insight Change Time
288	Agassi	192.1.168.71			localhost (1)	localhost (1)	9927	11/18/10 1:36 PM
			576	40:A0:00:00:00:00:00:84	localhost (1)	localhost (1)	9928	11/18/10 1:36 PM
			577	40:A0:00:00:00:00:00:85	localhost (1)	localhost (1)	9930	11/18/10 1:36 PM
305	AI_Host1	192.1.168.88			localhost (1)	localhost (1)	12254	11/18/10 1:38 PM
			597	40:A0:00:00:00:00:01:05	localhost (1)	localhost (1)	12255	11/18/10 1:38 PM
306	AI_Host2	192.1.168.89			localhost (1)	localhost (1)	12257	11/18/10 1:38 PM
			598	40:A0:00:00:00:00:01:06	localhost (1)	localhost (1)	12258	11/18/10 1:38 PM
307	AI_Host3	192.1.168.90			localhost (1)	localhost (1)	12260	11/18/10 1:38 PM

Per tutti gli host e gli adattatori è presente una riga per ciascun connettore che riporta i relativi dati, oltre al connettore primario da cui vengono presi l'host e l'adattatore. Solo per host e adattatori, un host segnalato da un connettore potrebbe riportare i relativi adattatori da un connettore diverso.

È inoltre possibile visualizzare il tempo di modifica OnCommand Insight di un host/adattatore per ciascun connettore. Utilizzando questo parametro, è possibile scoprire quando si è verificato un aggiornamento in OnCommand Insight per l'host/adattatore e quando lo stesso host/adattatore è stato aggiornato in altri server OnCommand Insight.

4. Facoltativamente, filtrare i dati in questa vista digitando una parte del testo e facendo clic su **Filter** (filtro). Per eliminare il filtro, eliminare il testo nella casella **Filter** e fare clic su **Filter**. È possibile filtrare in base al nome host, all'indirizzo IP host, al numero WWN dell'adattatore o all'ID oggetto OnCommand Insight.

   Il filtro fa distinzione tra maiuscole e minuscole.

5. Esaminare i seguenti dati:
   - **GUID host**

     Global Unique Identifier per questo tipo di dispositivo consolidato (host)

   - **Nome host**

Nome dell'host consolidato così come appare nel data warehouse

- **IP host**

  Indirizzo IP dell'host consolidato

- **GUID adattatore**

  Identificatore univoco globale dell'adattatore host

- **WWN adattatore**

  WWN dell'adattatore host

- **Connettore principale**

  Nome del connettore OnCommand Insight che era l'origine effettiva dei dati

- **Connettori disponibili**

  Tutti i connettori OnCommand Insight in cui risiede l'host/adattatore consolidato

- **Insight ID**

  ID OnCommand Insight dell'host/adattatore consolidato per il relativo connettore di reporting

- **Insight Change Time**

  Quando si è verificato un aggiornamento in OnCommand Insight per l'host/adattatore e quando lo stesso host/adattatore è stato aggiornato in altri server OnCommand Insight

6. Per ottenere informazioni dettagliate sul connettore, fare clic sul connettore.

   Sono disponibili le seguenti informazioni relative al connettore:

   - Nome host
   - L'ultima volta in cui è stato eseguito un processo Data Warehouse su quel connettore
   - L'ultima volta in cui è stata ricevuta una modifica da quel connettore
   - La versione del server OnCommand Insight indicata dal connettore

Visualizzazione dei problemi di consolidamento degli array di storage

I dati riportati per gli array di storage derivano dal data mart di inventario. Per tutti gli array di storage, è presente una riga per ciascun connettore che riporta su di essi, oltre al connettore primario da cui viene prelevato ciascun array.

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 **risoluzione dei problemi**.
3. Nella sezione **chassis Consolidation**, fare clic su **SAN Storage Array**.

4. Se si desidera, per filtrare i dati in questa vista, digitare una parte del testo nella casella Filter (filtro) e fare clic su **Filter** (filtro). Per eliminare il filtro, eliminare il testo nella casella filtro e fare clic su **filtro**. È possibile filtrare in base al nome dello storage, all'IP dello storage, al modello del vendor o all'ID oggetto OnCommand Insight.

   Il filtro fa distinzione tra maiuscole e minuscole.

5. Esaminare i seguenti dati:
   - **GUID**

     Global Unique Identifier per questo tipo di dispositivo consolidato (storage array)

   - **Nome**

     Nome dell'array storage consolidato così come appare nel Data Warehouse

   - **IP**

     Indirizzo IP dello storage array consolidato

   - **Fornitore e modello**

     Nome del vendor che vende lo storage array consolidato e numero di modello del produttore

   - **Connettore principale**

     Nome del connettore OnCommand Insight che era l'origine effettiva dei dati

   - **Connettori disponibili**

     Tutti i connettori OnCommand Insight in cui risiede lo storage array consolidato

   - **Insight ID**

     ID dello storage array consolidato sullo chassis OnCommand Insight in cui risiede il connettore principale

   - **Insight Change Time**

     Quando si è verificato un aggiornamento in OnCommand Insight per lo storage array e quando lo stesso storage array è stato aggiornato in altri server OnCommand Insight

Visualizzazione dei problemi di consolidamento degli switch

I dati riportati per gli switch derivano dal data mart di inventario. Per tutti gli switch, è presente una riga per ciascun connettore che li segnala, oltre al connettore primario da cui ciascuno switch viene prelevato.

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**Troubleshooting** (risoluzione dei problemi).

3. Nella sezione **consolidamento dello chassis**, fare clic su **Switch SAN**.
4. Facoltativamente, filtrare i dati in questa vista digitando una parte del testo e facendo clic su **Filter** (filtro). Per deselezionare il filtro, deselezionare la casella Filter (filtro) e fare clic su **Filter** (filtro). È possibile filtrare in base al nome dello switch, all'IP dello switch, al modello del vendor o all'ID oggetto OnCommand Insight.

   Il filtro fa distinzione tra maiuscole e minuscole.

5. Esaminare i seguenti dati:
   - **GUID**

     Global Unique Identifier per questo tipo di dispositivo consolidato (storage array)

   - **Nome**

     Nome dell'array storage consolidato così come appare nel data warehouse

   - **IP**

     Indirizzo IP dello storage array consolidato

   - **Fornitore e modello**

     Nome del vendor che vende lo storage array consolidato e numero di modello del produttore

   - **WWN**

     WWN per lo switch di consolidamento

   - **Connettore principale**

     Nome del connettore OnCommand Insight che era l'origine effettiva dei dati

   - **Connettori disponibili**

     Tutti i connettori OnCommand Insight in cui risiede lo storage array consolidato

   - **Insight ID**

     ID dello storage array consolidato sullo chassis OnCommand Insight in cui risiede il connettore principale

   - **Insight Change Time**

     Quando si è verificato un aggiornamento in OnCommand Insight per lo storage array e quando lo stesso storage array è stato aggiornato in altri server OnCommand Insight

Risoluzione di problemi di consolidamento delle annotazioni su più server

La vista Annotation Consolidation (consolidamento annotazioni) nella vista Data Warehouse Troubleshooting (risoluzione dei problemi di Data Warehouse) visualizza una tabella contenente tutti i tipi di annotazioni disponibili e i tipi di oggetti a cui è possibile applicarli.

A proposito di questa attività

Il consolidamento dei valori di annotazione si basa sul valore del tipo di annotazione. Un array di storage potrebbe avere due diversi valori di Tier, ciascuno proveniente da un connettore diverso. Pertanto, se in un connettore è presente un livello definito dal nome gold e in un secondo connettore un livello viene definito con il nome goldy, queste informazioni vengono visualizzate in Data Warehouse come due livelli separati.

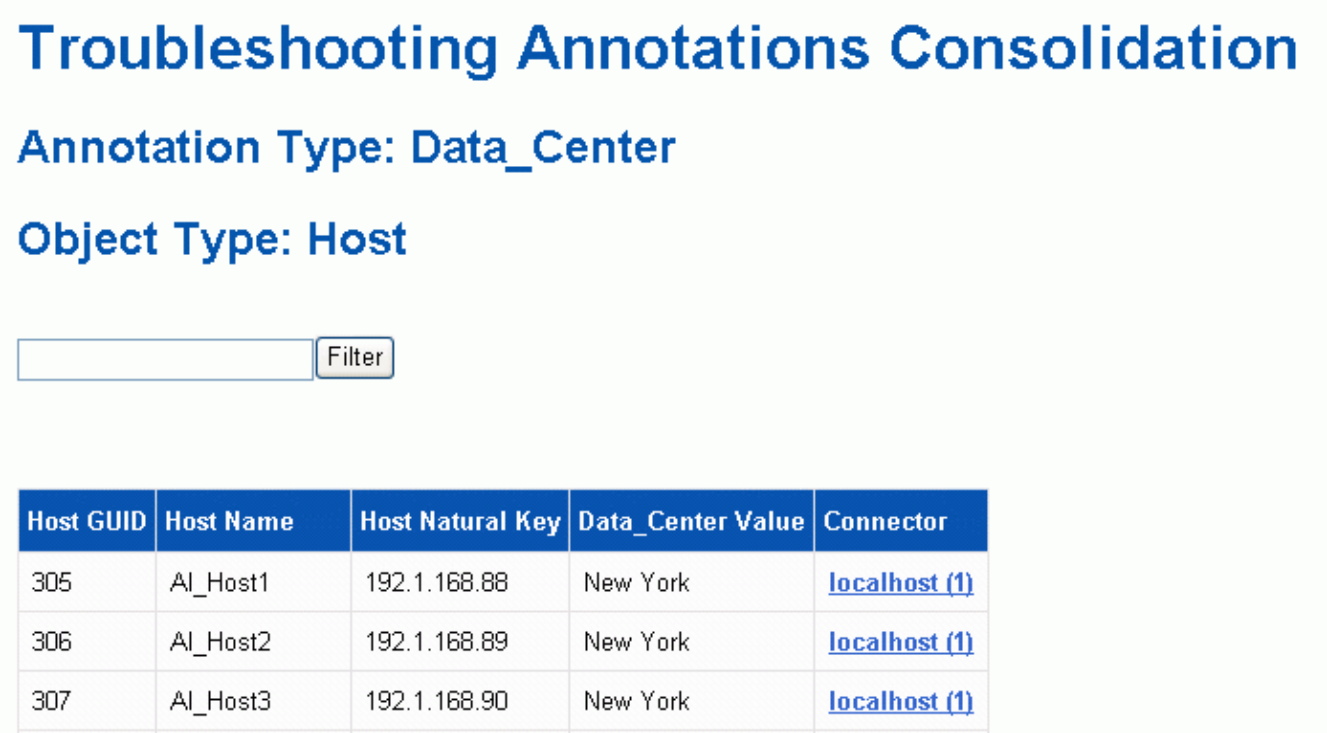
Poiché alcuni tipi di annotazione consentono l'assegnazione di più valori di annotazione allo stesso oggetto, Data Warehouse consente agli oggetti (ad esempio, "host") di assegnare più valori di annotazione (ad esempio, "dATA center 1" e "`dATA center 2" potrebbero essere assegnati allo stesso host).

L'annotazione Tier sui volumi funziona in modo leggermente diverso dalle tabelle di annotazione generali. Potenzialmente, nell'ambiente potrebbe essere presente un numero molto elevato di volumi e la visualizzazione di tutti i volumi nel Data Warehouse potrebbe influire sull'usabilità delle informazioni. Pertanto, la vista Annotations Consolidation (consolidamento annotazioni) visualizza solo i volumi a cui sono stati assegnati più valori di Tier e lo storage che contiene ciascuno di tali volumi.

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 **risoluzione dei problemi**.
3. Nella sezione **Annotation Consolidation**, fare clic su **Show** (Mostra) nella riga dell'oggetto.

   Di seguito viene riportato un esempio di annotazioni per Data_Center:



Host GUID	Host Name	Host Natural Key	Data_Center Value	Connector
305	AI_Host1	192.1.168.88	New York	localhost (1)
306	AI_Host2	192.1.168.89	New York	localhost (1)
307	AI_Host3	192.1.168.90	New York	localhost (1)

Creazione di report

Benvenuti nel reporting OnCommand Insight

OnCommand Insight Reporting è uno strumento di business intelligence che consente di visualizzare report predefiniti o creare report personalizzati. Il reporting OnCommand Insight genera report dai dati del data warehouse (DWH).

Con il reporting OnCommand Insight è possibile eseguire le seguenti attività:

- Eseguire un report predefinito
- Creare un report personalizzato
- Personalizzare il formato del report e il metodo di consegna
- Pianificare l'esecuzione automatica dei report
- Invia report via email
- Utilizzare i colori per rappresentare le soglie sui dati

I report predefiniti sono i report standard di OnCommand Insight. Questa guida descrive i report predefiniti disponibili con tutte le licenze del prodotto.

Accesso al portale di reporting OnCommand Insight

È possibile accedere al portale di reporting OnCommand Insight direttamente da un browser Web, dal data warehouse o dal server Insight . Il portale di reporting consente di accedere a report predefiniti o di creare report personalizzati utilizzando i dati del data warehouse.

Accedere al portale di reporting da un browser Web

Fasi

1. Aprire un browser Web.
2. Immettere il seguente URL: `https://server-name:9300/bi`

   9300 rappresenta la porta predefinita specificata durante l'installazione. Se è stata specificata un'altra porta, è necessario modificarla.

3. Immettere il nome utente e la password, quindi fare clic su **OK**.

Accesso al portale di reporting dal server Insight

Fasi

1. Aprire un browser Web.
2. Immettere il seguente URL per accedere al server Insight: `https://server-name`
3. Immettere il nome utente e la password, quindi fare clic su **OK**.
4. Nella barra degli strumenti Insight, fare clic su .

5. Nella pagina di accesso visualizzata, immettere il nome utente e la password, quindi fare clic su **OK**.

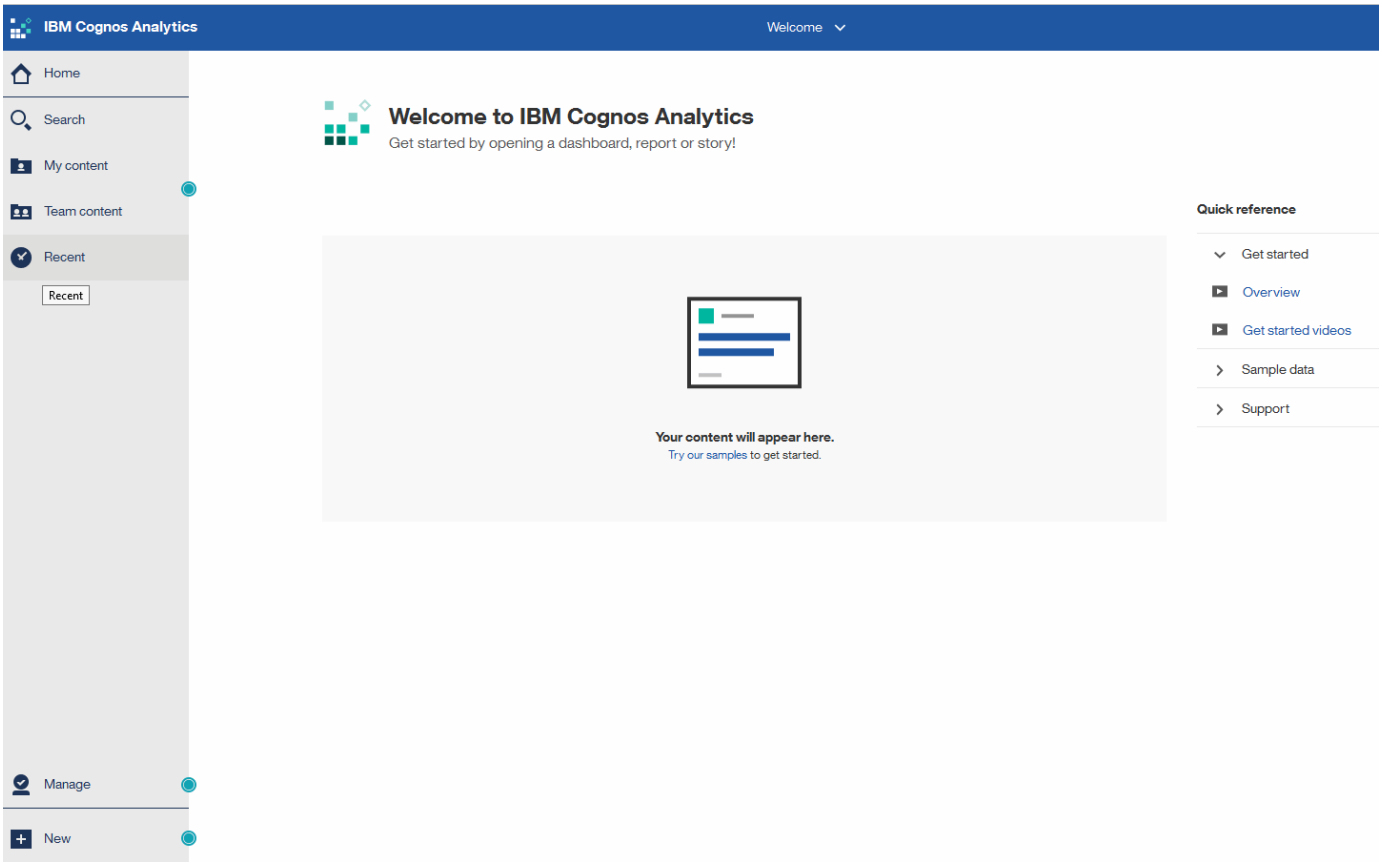
Accesso al portale di reporting dal Data Warehouse

Fasi

1. Aprire un browser Web.
2. Immettere il seguente URL per accedere al Data Warehouse: `https://server-name/dwh`
3. Immettere il nome utente e la password, quindi fare clic su **OK**.
4. Nella barra degli strumenti Data Warehouse, fare clic su .
5. Nella pagina di accesso visualizzata, immettere il nome utente e la password, quindi fare clic su **OK**.

Risultati

Viene visualizzata la pagina di benvenuto di IBM Cognos Analytics. Questa è la landing page predefinita del portale di reporting OnCommand Insight.



Variazioni dovute alle licenze installate

I dati contenuti nei report OnCommand Insight si basano sulle licenze OnCommand Insight acquistate. Ad esempio, senza la licenza Plan, si ottengono dati point-in-time (oggi) nel datamart di inventario per capacità e performance, ma non si ha la possibilità di creare un trend (report su un periodo di tempo) dei dati di capacità o performance per qualsiasi dispositivo.

L'assenza di una licenza Plan elimina la possibilità di creare nuovi report o di modificarli. È possibile che si riscontrino differenze tra i report disponibili nel sistema OnCommand Insight e le illustrazioni della documentazione. Queste variazioni sono dovute alle differenze tra le licenze installate sul sistema e le licenze utilizzate per creare le illustrazioni.

Per ulteriori informazioni sulle licenze, consultare la guida all'installazione di OnCommand Insight.

Creazione di report sui ruoli utente

A ciascun account utente viene assegnato un ruolo con una serie di autorizzazioni. Il numero di utenti è limitato dal numero di licenze di Reporting associate a ciascun ruolo.

Ciascun ruolo può eseguire le seguenti azioni:

- **Destinatario**

  Visualizza i report del portale di reporting OnCommand Insight e imposta le preferenze personali, ad esempio quelle per le lingue e i fusi orari.

  > I destinatari non possono creare report, eseguire report, pianificare report, esportare report o eseguire attività amministrative.

- **Business Consumer**

  Esegue i report ed esegue tutte le opzioni dei destinatari.

- **Business Author**

  Visualizza report pianificati, esegue report in modo interattivo, crea storie, oltre a eseguire tutte le opzioni Business Consumer.

- **Pro Author**

  Crea report, crea pacchetti e moduli di dati, oltre a eseguire tutte le opzioni di Business Author.

- **Amministratore**

  Esegue attività amministrative di reporting come l'importazione e l'esportazione delle definizioni dei report, la configurazione dei report, la configurazione delle origini dati e l'arresto e il riavvio delle attività di reporting.

La tabella seguente mostra i privilegi e il numero massimo di utenti consentiti per ciascun ruolo:

Funzione	Destinatario	Consumer aziendale	Autore di business	Pro Author	Amministratore
Visualizzare i report nella scheda contenuto team	Sì	Sì	Sì	Sì	Sì
Eseguire i report	No	Sì	Sì	Sì	Sì

Pianifica i report	No	Sì	Sì	Sì	Sì
Caricare file esterni	No	No	Sì	Sì	No
Crea storie	No	No	Sì	Sì	No
Creare report	No	No	No	Sì	No
Creare pacchetti e moduli dati	No	No	No	Sì	No
Eseguire attività amministrative	No	No	No	No	Sì
Numero di utenti	Numero di utenti OnCommand Insight	20	2	1	1

Quando si aggiunge un nuovo utente di Data Warehouse e Reporting, se si supera il limite di un ruolo, l'utente viene aggiunto come "deactivated," ed è necessario disattivare o rimuovere un altro utente con tale ruolo per assegnare un nuovo utente.

> Le funzionalità di creazione dei report richiedono la licenza Insight Plan. Puoi aggiungere altri utenti Business Author e Pro Author acquistando IL PACCHETTO ARAP (Additional Report Authoring Package). Per assistenza, contattare il rappresentante OnCommand Insight.

Questi ruoli utente di reporting non influiscono sull'accesso diretto al database. Questi ruoli utente di reporting non influiscono sulla capacità di creare query SQL utilizzando i data mart.

Abilitazione delle intestazioni di sicurezza

Le intestazioni HTTP possono essere configurate per migliorare la sicurezza generale dell'applicazione web Cognos Analytics.

Per aggiungere le intestazioni delle risposte:

- Accedere all'interfaccia utente di Cognos Analytics e selezionare **Gestisci> Configurazione> sistema> Impostazioni avanzate**
- Aggiungere la seguente chiave/valore e applicare:
  - Chiave: `BIHeaderFilter.responseHeaders`
  - Valore: `[{"name":"X-FRAME-OPTIONS","value":"SAMEORIGIN"},{"name":"X-XSS-Protection","value":"1"},{"name":"X-Content-Type-Options","value":"nosniff"}]`
- Aggiornare il browser per attivare le intestazioni.

Creazione di report semplificata

È possibile generare report predefiniti dal portale di reporting OnCommand Insight, inviarli via email ad altri utenti e persino modificarli. Diversi report consentono di filtrare per dispositivo, entità aziendale o Tier. Gli strumenti di reporting utilizzano IBM Cognos come base e offrono numerose opzioni di presentazione dei dati.

- I report predefiniti di OnCommand Insight mostrano l'inventario, la capacità dello storage, il chargeback, le performance, l'efficienza dello storage, e dati sui costi del cloud. È possibile modificare questi report predefiniti e salvare le modifiche.

I dati del report disponibili sono controllati da diversi elementi, tra cui:

- Accesso al portale di reporting OnCommand Insight, definito in base ai ruoli.
- La configurazione del data warehouse di OnCommand InsightData, che memorizza i dati per i report.

È possibile generare report in diversi formati, tra cui HTML, PDF, CSV, XML, Ed Excel.

OnCommand Insight consente di gestire più tenancy nel reporting, consentendo di associare gli utenti alle business unit. Con questa funzione, gli amministratori possono separare i dati o i report in base agli attributi di un utente o della sua affiliazione.

> Con Cognos versione 11.1.2 in poi, gli URL di reporting non sono considerati "stabili" e sono soggetti a modifiche. Se si dispone di URL di reporting con segnalibri, questi segnalibri potrebbero non riuscire. Ulteriori informazioni sono disponibili qui: http://queryvision.com/ibm-analytics-11-x-urls-they-are-a-changing/

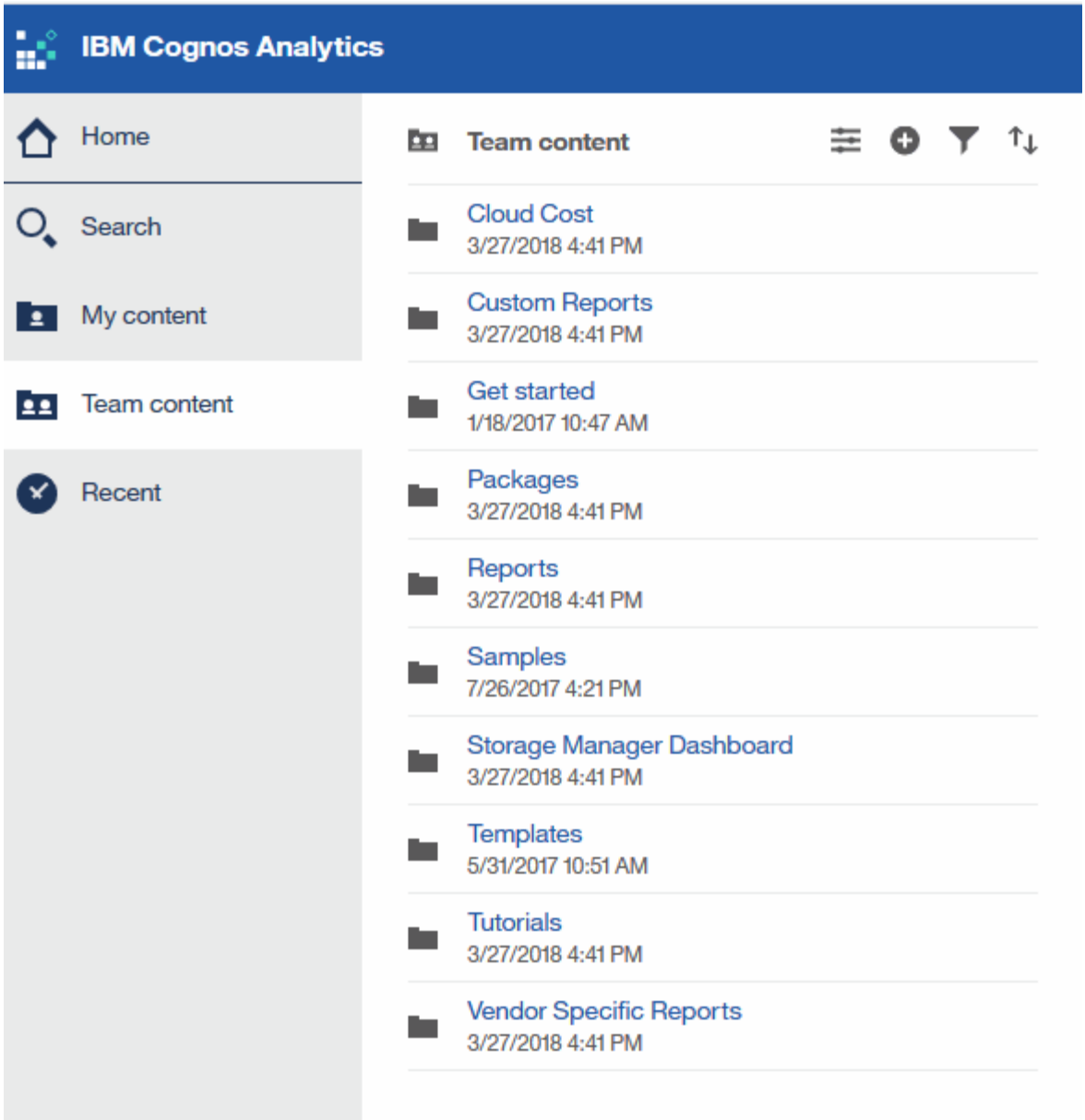
> OnCommand Insight non supporta i dashboard creati utilizzando pacchetti in IBM Cognos, a meno che non si utilizzi la nuova funzione modulo dati.

Navigazione verso report OnCommand Insight predefiniti

Quando si apre il portale di reporting, la cartella del contenuto del team è il punto di partenza per selezionare il tipo di informazioni necessarie nei report di OnCommand Insight.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **contenuto del team** e selezionare la categoria di informazioni che si desidera utilizzare.



2. Fare clic su **Report** per accedere ai report predefiniti.
3. Fare clic su **Get Started**, **Samples** o **Tutorial** per informazioni su come creare i report.

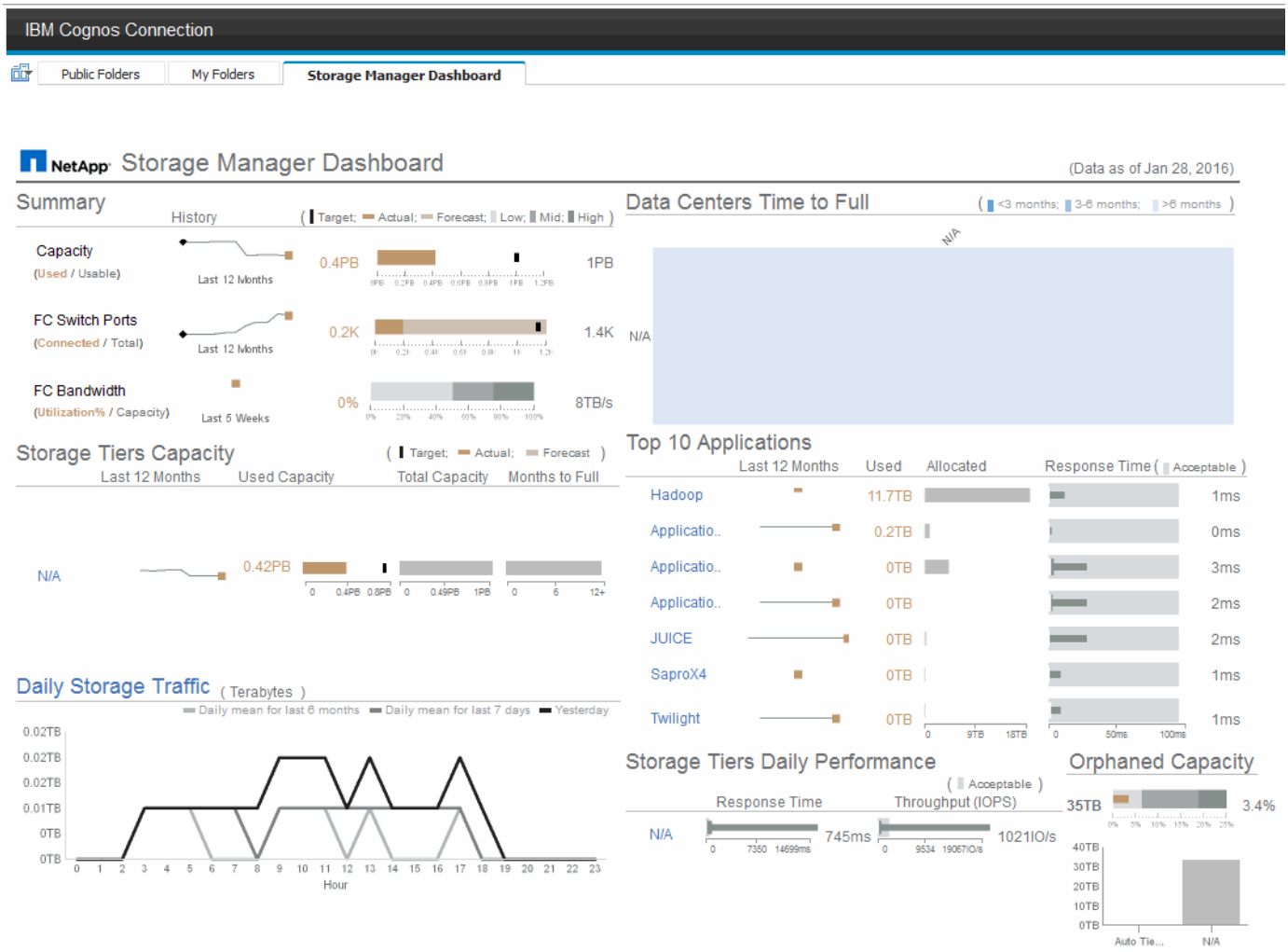
Cosa ti consente di fare Storage Manager Dashboard

È possibile utilizzare Storage Manager Dashboard per la gestione quotidiana dei servizi di storage.

La dashboard di Storage Manager offre una visualizzazione centralizzata che consente di confrontare e confrontare l'utilizzo delle risorse nel tempo con gli intervalli accettabili e i giorni di attività precedenti. Mostrando solo le metriche chiave delle performance per i tuoi servizi storage, puoi prendere decisioni su come gestire i tuoi data center.

La dashboard comprende sette componenti che contengono informazioni contestuali su alcuni aspetti dell'ambiente di storage. È possibile approfondire gli aspetti dei servizi storage per eseguire un'analisi approfondita di una sezione che interessa di più.

Riepilogo



Questo componente mostra la capacità di storage utilizzata rispetto a quella utilizzabile, il numero totale di porte switch rispetto al numero di porte switch connesse e l'utilizzo totale delle porte switch connesse rispetto alla larghezza di banda totale, nonché l'andamento di ciascuna di queste nel tempo. È possibile visualizzare l'utilizzo effettivo rispetto ai range basso, medio e alto, che consente di confrontare e confrontare l'utilizzo tra le proiezioni Insight e gli effettivi desiderati, in base a un target. Per la capacità e le porte dello switch, è possibile configurare questa destinazione. La previsione si basa su un'estrapolazione del tasso di crescita corrente e della data impostata. Quando la capacità utilizzata prevista, che si basa sulla data di proiezione dell'utilizzo futuro, supera la destinazione, viene visualizzato un avviso (cerchio rosso fisso) accanto a Capacity (capacità).

Capacità dei Tier di storage

Questo componente mostra la capacità del Tier utilizzata rispetto alla capacità allocata al Tier, che indica come la capacità utilizzata aumenta o diminuisce in un periodo di 12 mesi e quanti mesi rimangono alla capacità completa. L'utilizzo della capacità viene visualizzato con i valori forniti per l'utilizzo effettivo, le previsioni di utilizzo da parte di Insight e un target per la capacità, che è possibile configurare. Quando la capacità utilizzata prevista, basata sulla data di proiezione dell'utilizzo futuro, supera la capacità di destinazione, viene visualizzato un avviso (cerchio rosso) accanto a un livello.

È possibile fare clic su qualsiasi Tier per visualizzare il report Storage Pools Capacity and Performance Details, che mostra le capacità gratuite rispetto a quelle utilizzate, il numero di giorni da esaurire e i dettagli delle performance (IOPS e tempo di risposta) per tutti i pool del Tier selezionato. È inoltre possibile fare clic su qualsiasi nome di storage o pool di storage in questo report per visualizzare la pagina delle risorse che

riepiloga lo stato corrente di tale risorsa.

Traffico di storage giornaliero

Questo componente mostra le performance dell'ambiente, in caso di crescita elevata, cambiamenti o potenziali problemi rispetto ai sei mesi precedenti. Mostra inoltre il traffico medio rispetto al traffico dei sette giorni precedenti e del giorno precedente. È possibile visualizzare eventuali anomalie nelle prestazioni dell'infrastruttura, in quanto fornisce informazioni che evidenziano variazioni cicliche (sette giorni precedenti) e stagionali (sei mesi precedenti).

È possibile fare clic sul titolo (**Daily Storage Traffic**) per visualizzare il report Storage Traffic Details, che mostra la mappa termica del traffico di storage orario per il giorno precedente per ciascun sistema di storage. Fare clic su un nome di storage qualsiasi in questo report per visualizzare la pagina delle risorse che riepiloga lo stato corrente della risorsa.

Data Center Time to Full (i data center sono in fase di

Questo componente mostra tutti i data center rispetto a tutti i Tier e la capacità residua in ogni data center per ciascun Tier di storage in base ai tassi di crescita previsti da Insight. Il livello di capacità del Tier viene visualizzato in blu; più scuro è il colore, minore è il tempo trascorso dal Tier nella posizione prima che sia pieno.

È possibile fare clic su una sezione di un livello per visualizzare il report Storage Pools Days to Full Details (giorni di archiviazione per dettagli completi), che mostra la capacità totale, la capacità libera e il numero di giorni da esaurire per tutti i pool nel Tier selezionato e nel data center. Fare clic su un nome di storage o pool di storage in questo report per visualizzare la pagina delle risorse che riepiloga lo stato corrente della risorsa.

10 applicazioni principali

Questo componente mostra le prime 10 applicazioni in base alla capacità utilizzata. Indipendentemente dal modo in cui il Tier organizza i dati, quest'area visualizza la capacità corrente utilizzata e la condivisione dell'infrastruttura. È possibile visualizzare la gamma di esperienze utente dei sette giorni precedenti per verificare se i consumatori sperimentano tempi di risposta accettabili (o, cosa più importante, inaccettabili).

Quest'area mostra anche i trend, che indicano se le applicazioni soddisfano gli obiettivi di performance del livello di servizio (SLO). È possibile visualizzare il tempo di risposta minimo della settimana precedente, il primo quartile, il terzo quartile e il tempo di risposta massimo, con una mediana visualizzata rispetto a un SLO accettabile, che è possibile configurare. Quando il tempo di risposta medio di un'applicazione non rientra nell'intervallo SLO accettabile, accanto all'applicazione viene visualizzato un avviso (cerchio rosso fisso). È possibile fare clic su un'applicazione per visualizzare la pagina delle risorse che riepiloga lo stato corrente di tale risorsa.

Performance giornaliere dei Tier di storage

Questo componente mostra un riepilogo delle performance del Tier per i tempi di risposta e gli IOPS per i sette giorni precedenti. Queste performance vengono confrontate con un SLO, che è possibile configurare, per verificare se esiste l'opportunità di consolidare i Tier, riallineare i carichi di lavoro forniti da tali Tier o identificare problemi con determinati Tier. Quando il tempo di risposta mediano o l'IOPS mediano non rientra nell'intervallo SLO accettabile, viene visualizzato un avviso (cerchio rosso pieno) accanto a un livello.

È possibile fare clic sul nome di un Tier per visualizzare il report Storage Pools Capacity and Performance Details, che mostra le capacità gratuite rispetto a quelle utilizzate, il numero di giorni da esaurire e i dettagli delle performance (IOPS e tempo di risposta) per tutti i pool del Tier selezionato. Fare clic su uno storage o pool di storage in questo report per visualizzare la pagina delle risorse che riepiloga lo stato corrente della risorsa.

Capacità orfana

Questa componente mostra la capacità orfana totale e la capacità orfana per Tier, confrontandola con gli intervalli accettabili per la capacità utilizzabile totale e mostrando la capacità effettiva orfana. La capacità orfana è definita dalla configurazione e dalle performance. *Storage orfano per configurazione* descrive una situazione in cui lo storage è allocato a un host. Tuttavia, la configurazione non è stata eseguita correttamente e l'host non può accedere allo storage. *Orfano per performance* è quando lo storage è configurato correttamente per l'accesso da parte di un host. Tuttavia, non c'è stato traffico di storage.

La barra orizzontale sovrapposta mostra gli intervalli accettabili. Più scuro è il grigio, più inaccettabile è la situazione. La situazione effettiva viene mostrata con la stretta barra di bronzo che mostra la capacità effettiva che è orfana.

È possibile fare clic su un Tier per visualizzare il report "Orphaned Storage Details" (Dettagli storage orfani), che mostra tutti i volumi identificati come orfani in base alla configurazione e alle performance per il Tier selezionato. Fare clic su qualsiasi storage, pool di storage o volume in questo report per visualizzare la pagina delle risorse che riepiloga lo stato corrente della risorsa.

Utilizzo di report predefiniti per rispondere a domande comuni

OnCommand Insight include report predefiniti che rispondono a una serie di requisiti di reporting comuni, fornendo informazioni critiche di cui gli stakeholder hanno bisogno per prendere decisioni informate sulla propria infrastruttura di storage.

I seguenti report predefiniti sono disponibili in **contenuto del team** > **Report** o **contenuto del team** > **Report specifici del fornitore**.

Le versioni più recenti dei report potrebbero essere disponibili presso il NetApp Storage Automation Store. È necessario controllare regolarmente l'Automation Store per i report.

- **AWS Cloud Cost Data**

  Il report sui costi del cloud offre una vista consolidata di tutte le risorse, in modo da poter monitorare, analizzare e ottimizzare l'utilizzo e i costi dei servizi basati sul cloud e on-premise in base alla scalabilità dinamica nel tuo ambiente.

  Il report offre una correlazione infrastruttura-costo, fornendo report chiari e pratici per garantire il giusto dimensionamento attraverso una pianificazione della capacità mirata e il rilevamento degli sprechi.

- **Capacità e performance del livello di servizio dell'applicazione**

  Il report Application Service Level Capacity and Performance fornisce una panoramica di alto livello delle applicazioni. È possibile utilizzare queste informazioni per la pianificazione della capacità o per un piano di migrazione.

- **Chargeback**

  Il report Chargeback fornisce informazioni di chargeback della capacità di storage e di responsabilità per host, applicazioni ed entità aziendali e include dati attuali e storici.

  Per evitare il doppio conteggio, non includere server ESX, monitorare solo le macchine virtuali.

  Una versione aggiornata di questo report è disponibile presso il NetApp Storage Automation Store.

- **Origini dati**

  Il report origini dati mostra tutte le origini dati installate nel sito, lo stato dell'origine dati (operazione riuscita/non riuscita) e i messaggi di stato. Il report fornisce informazioni su dove iniziare la risoluzione dei problemi delle origini dati. Le origini dati non riuscite influiscono sull'accuratezza dei report Insight e sull'usabilità generale del prodotto.

- **Prestazioni ESX vs VM**

  Il report sulle performance di ESX e VM offre un confronto tra server e macchine virtuali ESX, mostrando IOPS medi e di picco, throughput, latenza e utilizzo per server e macchine virtuali ESX. Per evitare il doppio conteggio, escludere i server ESX; includere solo le macchine virtuali.

  Una versione aggiornata di questo report è disponibile presso il NetApp Storage Automation Store.

- **Riepilogo fabric**

  Il report Fabric Summary identifica le informazioni relative a switch e switch, inclusi il numero di porte, le versioni del firmware e lo stato della licenza. Il report non include le porte dello switch NPV.

- **HBA host**

  Il report HBA host fornisce una panoramica degli host nell'ambiente e fornisce il vendor, il modello e la versione firmware degli HBA e il livello firmware degli switch a cui sono collegati. Questo report può essere utilizzato per analizzare la compatibilità del firmware quando si pianifica un aggiornamento del firmware per uno switch o un HBA.

- **Capacità e performance del livello di servizio host**

  Il report host Service Level Capacity and Performance fornisce una panoramica dell'utilizzo dello storage per host per applicazioni a blocchi.

- **Riepilogo host**

  Il report host Summary (Riepilogo host) fornisce una panoramica dell'utilizzo dello storage da parte di ciascun host selezionato con informazioni sugli host Fibre Channel e iSCSI. Il report consente di confrontare porte e percorsi, capacità Fibre Channel e ISCSI e conteggi delle violazioni.

- **Dettagli licenza**

  Il report License Details (Dettagli licenza) mostra la quantità autorizzata di risorse per le quali si dispone della licenza in tutti i siti con licenze attive. Il report mostra anche una somma della quantità effettiva in tutti i siti con licenze attive. La somma può includere sovrapposizioni di array di storage gestiti da più server.

- **Volumi mappati ma non mascherati**

  Il report Mapped but Not Masked Volumes (volumi mappati ma non mascherati) elenca i volumi il cui numero di unità logica (LUN) è stato mappato per l'utilizzo da parte di un determinato host, ma non è mascherato da tale host. In alcuni casi questi LUN potrebbero essere dismessi e non mascherati. Qualsiasi host può accedere ai volumi senza maschera, rendendoli vulnerabili alla corruzione dei dati.

- **Capacità e performance NetApp**

  Il report NetApp Capacity and Performance fornisce dati globali per la capacità allocata, utilizzata e impegnata con dati di trend e performance per la capacità NetApp.

- **Scheda di valutazione OCI**

  Il report Scorecard OCI fornisce un riepilogo e lo stato generale di tutte le risorse rilevate da OnCommand Insight. Lo stato è indicato da indicatori verdi, gialli e rossi:

  - Verde indica la condizione normale
  - Il giallo indica un potenziale problema nell'ambiente
  - Il rosso indica un problema che richiede attenzione. Tutti i campi del report sono descritti nel Dizionario dati fornito con il report.

- **Riepilogo dello storage**

  Il report Storage Summary fornisce un riepilogo globale dei dati di capacità utilizzati e inutilizzati per i pool di storage raw, allocati e volumi. Questo report fornisce una panoramica di tutto lo storage rilevato.

  Una versione più recente di questo report è disponibile presso il NetApp Storage Automation Store.

- **Capacità e performance delle macchine virtuali**

  Descrive l'ambiente della macchina virtuale (VM) e il relativo utilizzo della capacità. Gli strumenti delle macchine virtuali devono essere abilitati per visualizzare alcuni dati, ad esempio quando le macchine virtuali sono state spenti.

- **Percorsi delle macchine virtuali**

  Il report sui percorsi delle macchine virtuali fornisce dati sulla capacità dell'archivio dati e metriche delle performance per le quali la macchina virtuale è in esecuzione su quale host, gli host che accedono a quali volumi condivisi, il percorso di accesso attivo e ciò che comprende l'allocazione e l'utilizzo della capacità.

- **Capacità HDS di Thin Pool**

  Il report HDS Capacity by Thin Pool mostra la quantità di capacità utilizzabile in un pool di storage con thin provisioning.

- **Capacità NetApp per aggregato**

  Il report NetApp Capacity by aggregate mostra lo spazio totale, totale, utilizzato, disponibile e impegnato degli aggregati.

- **Symmetrix Capacity by Thick Array**

  Il report Symmetrix Capacity by Thick Array mostra capacità raw, capacità utilizzabile, capacità libera, mappata, mascherata, e capacità libera totale.

- **Symmetrix Capacity by Thin Pool**

  Il report Symmetrix Capacity by Thin Pool mostra capacità raw, capacità utilizzabile, capacità utilizzata, capacità libera, percentuale utilizzata, capacità sottoscritta e tasso di abbonamento.

- **XIV capacità per array**

  Il report XIV Capacity by Array (capacità XIV per array) mostra la capacità utilizzata e inutilizzata per l'array.

- **XIV capacità per pool**

Il report XIV Capacity by Pool mostra la capacità utilizzata e inutilizzata per i pool di storage.

Creazione di un report con Cognos 11

La creazione di report con Cognos 11 è diversa dalle versioni precedenti di Cognos. Utilizzare questa procedura per creare un report utilizzando i report OnCommand Insight predefiniti.

A proposito di questa attività

Per generare un semplice report sulla capacità fisica dei pool di storage e storage in diversi data center, procedere come segue.

Fasi

1. Nella barra degli strumenti, fare clic su +
2. Fare clic su **Report**
3. Fare clic su **modelli** > **vuoto**
4. Fare clic su **Temi** > **Blu** > **OK**

   Vengono visualizzate le schede origine e dati

5. Fare clic su **origine** > +
6. Nella finestra di dialogo Apri file, fare clic su **contenuto del team** > **pacchetti**

   Viene visualizzato un elenco dei pacchetti disponibili.

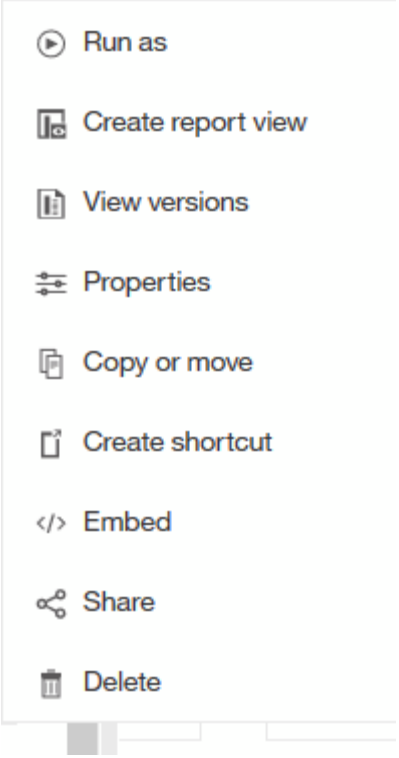
7. Fare clic su **Storage and Storage Pool Capacity** > **Open**
8. Fare clic su +

   Vengono visualizzati gli stili disponibili per il report.

9. Fare clic su **List** (elenco)

   Aggiungere i nomi appropriati per elenco e query

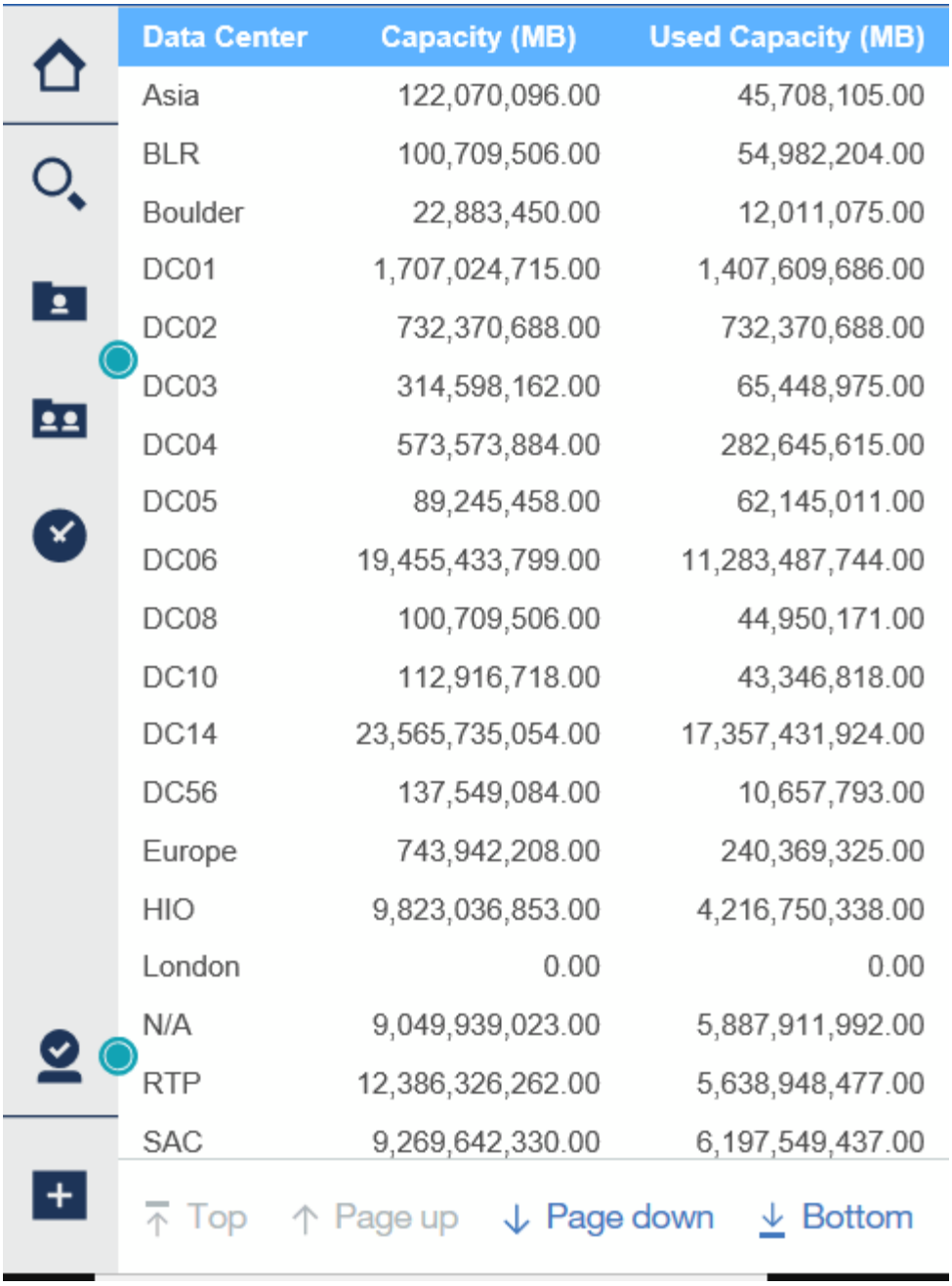
10. Fare clic su **OK**
11. Espandere **capacità fisica**
12. Espandere fino al livello più basso di **Data Center**
13. Trascinare Data Center Al palato dei report.
14. Espandere **capacità (MB)**
15. Trascinare **Capacity (MB)** sul tavolozza dei report.
16. Trascinare **capacità utilizzata (MB)** sul tavolozza dei report.
17.

Eseguire il report facendo clic su 

e selezionando un tipo di output.

Risultati

Viene creato un report simile al seguente:



Data Center	Capacity (MB)	Used Capacity (MB)
Asia	122,070,096.00	45,708,105.00
BLR	100,709,506.00	54,982,204.00
Boulder	22,883,450.00	12,011,075.00
DC01	1,707,024,715.00	1,407,609,686.00
DC02	732,370,688.00	732,370,688.00
DC03	314,598,162.00	65,448,975.00
DC04	573,573,884.00	282,645,615.00
DC05	89,245,458.00	62,145,011.00
DC06	19,455,433,799.00	11,283,487,744.00
DC08	100,709,506.00	44,950,171.00
DC10	112,916,718.00	43,346,818.00
DC14	23,565,735,054.00	17,357,431,924.00
DC56	137,549,084.00	10,657,793.00
Europe	743,942,208.00	240,369,325.00
HIO	9,823,036,853.00	4,216,750,338.00
London	0.00	0.00
N/A	9,049,939,023.00	5,887,911,992.00
RTP	12,386,326,262.00	5,638,948,477.00
SAC	9,269,642,330.00	6,197,549,437.00

Gestione dei report

Per ciascun report, è possibile selezionare il collegamento **More** nella colonna Actions (azioni) e accedere a tutte le operazioni del report, ad esempio l'impostazione delle proprietà del report, la pianificazione dei report o l'invio tramite e-mail dei report. Gli amministratori dispongono di più opzioni di gestione rispetto ad altri utenti.

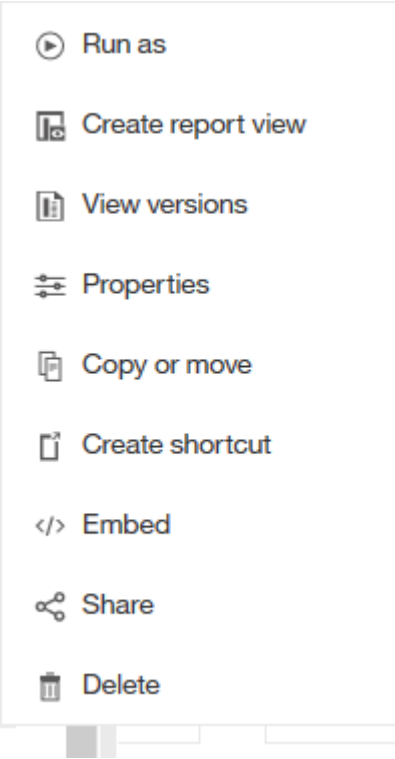
Gli amministratori possono impostare le autorizzazioni per altri utenti di report in base al proprio ruolo OnCommand Insight.

Personalizzazione del formato di output e della consegna di un report

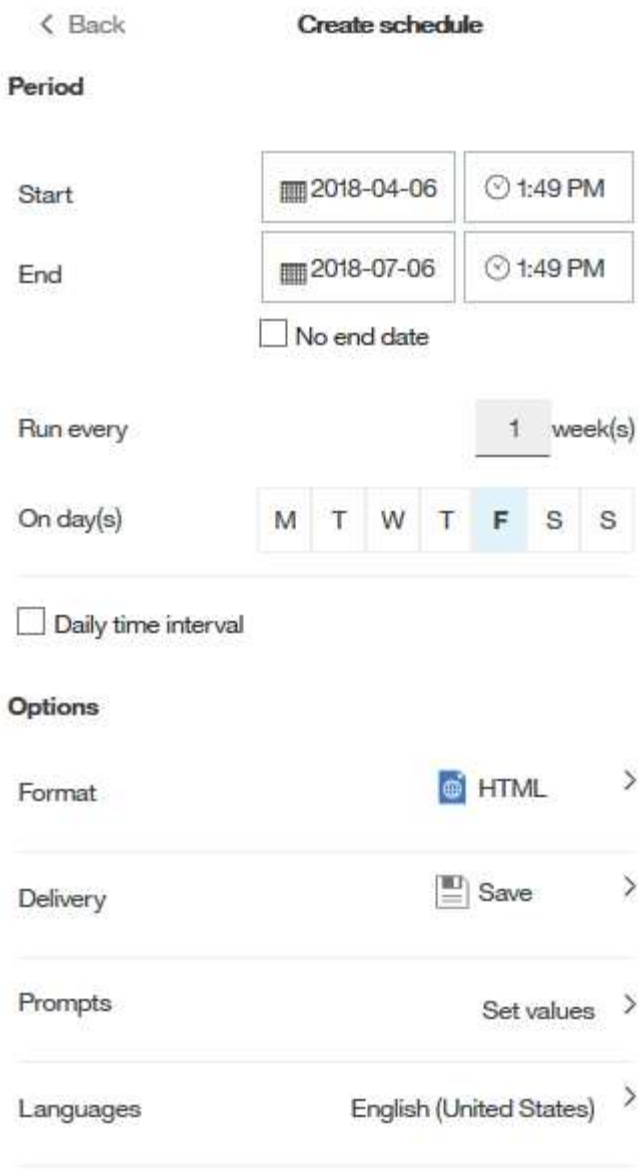
È possibile personalizzare il formato e il metodo di consegna dei report.

Fasi

1. Aprire il portale dei report OnCommand Insight e selezionare il report che si desidera personalizzare, quindi fare clic su **[...]**.



2. Fare clic su **Proprietà** > **Pianificazione**



3. È possibile impostare le seguenti opzioni:
   - **Pianificazione** per l'esecuzione dei report.
   - **Format** l'output del report.
   - **Consegna** stampare, salvare o inviare via email il report.
   - **Lingue** definisce la lingua in cui viene consegnato il report.
4. Fare clic su **Create** (Crea) per produrre il report utilizzando le selezioni effettuate.

Copia di un report negli Appunti

Questa procedura consente di copiare un report negli Appunti.

Fasi

1. Aprire il portale di reporting di Cognos 11: https://server-name:9300/bi/
2. Nella barra degli strumenti, fare clic su 

3. Fare clic su **Report**
4. Fare clic sull'icona *pagine*

   Icona **Report** Report viene visualizzato
5. Fare clic con il pulsante sinistro del mouse sull'icona **Report**

   Vengono visualizzate le opzioni del report.
6. Fare clic su **Copy Report to Clipboard** (Copia report negli Appunti).

Apertura di report (xml) dagli Appunti

È possibile aprire una specifica del report precedentemente copiata negli Appunti.

A proposito di questa attività

Per accedere all'interfaccia utente di Reporting, creare un nuovo report o aprire un report esistente

Fasi

1. Aprire il portale di reporting di Cognos 11: https://server-name:9300/bi/
2. Nella barra degli strumenti, fare clic su
3. Fare clic su **Report**
4. Fare clic sull'icona *pagine*

   Icona **Report** Report viene visualizzato
5. Fare clic con il pulsante sinistro del mouse sull'icona **Report**

   Vengono visualizzate le opzioni del report.
6. Fare clic su **Apri report dagli Appunti**.

Creazione di report personalizzati ad hoc

È possibile utilizzare gli strumenti di creazione dei report per creare report personalizzati. Dopo aver creato i report, è possibile salvarli ed eseguirli in base a una pianificazione regolare. I risultati dei report possono essere inviati automaticamente via email a te e ad altri.

Gli esempi di questa sezione mostrano il seguente processo, che può essere utilizzato per qualsiasi modello di dati OnCommand Insight:

- Identificazione di una domanda a cui rispondere con un report
- Determinazione dei dati necessari per supportare i risultati
- Selezione degli elementi dei dati per il report

Cosa occorre fare prima di progettare il report

Prima di progettare un report personalizzato, è necessario completare alcune attività preliminari. Se non vengono completati, i report potrebbero essere imprecisi o incompleti.

Ad esempio, se non si completa il processo di identificazione del dispositivo, i report relativi alla capacità non saranno accurati. In alternativa, se non si finisce di impostare annotazioni (ad esempio Tier, business unit e data center), i report personalizzati potrebbero non riportare in modo preciso i dati nel dominio e potrebbero mostrare "N/A" per alcuni data point.

Prima di progettare i report, completare le seguenti attività:

- Configurare tutte le origini dati. Per ulteriori informazioni, consultare la *Guida alla configurazione e all'amministrazione di OnCommand Insight*.
- Inserire annotazioni (ad esempio Tier, data center e business unit) sui dispositivi e sulle risorse del proprio ambiente. È vantaggioso che le annotazioni siano stabili prima di generare report, perché il data warehouse di OnCommand Insight raccoglie informazioni storiche.
- Configurare il data warehouse di OnCommand Insight per accettare i dati dal server OnCommand Insight nel processo di estrazione, trasformazione e caricamento (ETL).

Processo di creazione dei report

Il processo di creazione di report ad hoc prevede diverse attività.

- Pianificare i risultati del report.
- Identifica i dati a supporto dei tuoi risultati.
- Selezionare il modello di dati (ad esempio, modello di dati Chargeback, modello di dati di inventario e così via) che contiene i dati.
- Selezionare gli elementi dei dati per il report.
- Facoltativamente, è possibile formattare, ordinare e filtrare i risultati dei report.

Come pianificare i risultati del report personalizzato

Prima di aprire gli strumenti di progettazione dei report, è possibile pianificare i risultati desiderati dal report. Con gli strumenti per la creazione di report, è possibile creare report in modo semplice e senza bisogno di una grande pianificazione; tuttavia, è consigliabile avere un'idea dei requisiti dei report da parte del richiedente.

- Identificare la domanda esatta a cui si desidera rispondere. Ad esempio:
  - Quanta capacità ho ancora a disposizione?
  - Quali sono i costi di chargeback per business unit?
  - Qual è la capacità per Tier per garantire che le business unit siano allineate al livello di storage appropriato?
  - Come posso prevedere i requisiti di alimentazione e raffreddamento? (Aggiungere metadati personalizzati aggiungendo annotazioni alle risorse).
- Identificare gli elementi dei dati necessari per supportare la risposta.
- Identificare le relazioni tra i dati che si desidera visualizzare nella risposta. Non includere relazioni illogiche

nella domanda, ad esempio “desidero visualizzare le porte relative alla capacità”.

- Identificare i calcoli necessari sui dati.
- Determinare i tipi di filtraggio necessari per limitare i risultati.
- Determinare se è necessario utilizzare dati correnti o storici.
- Determinare se è necessario impostare i privilegi di accesso sui report per limitare i dati a un pubblico specifico.
- Identificare la modalità di distribuzione del report. Ad esempio, deve essere inviato tramite e-mail in base a una pianificazione prestabilita o incluso nell’area della cartella dei contenuti del team?
- Determinare chi gestirà il report. Questo potrebbe influire sulla complessità del progetto.
- Creare un modello del report.

Suggerimenti per la progettazione dei report

Durante la progettazione dei report, potrebbero essere utili diversi suggerimenti.

- Determinare se è necessario utilizzare dati correnti o storici.

  La maggior parte dei report deve solo generare report sui dati più recenti disponibili nel Data Warehouse.

- Data Warehouse fornisce informazioni storiche su capacità e performance, ma non sull’inventario.
- Tutti vedono tutti i dati; tuttavia, potrebbe essere necessario limitare i dati a un pubblico specifico.

  Per segmentare le informazioni per diversi utenti, è possibile creare report e impostare autorizzazioni di accesso per tali utenti.

Modello di dati di reporting

La tua azienda può trarre vantaggio dai dati rilevati e memorizzati nel data warehouse di OnCommand Insight. Il data warehouse di OnCommand Insight è un repository centralizzato che memorizza i dati provenienti da più fonti di informazioni e li trasforma in un modello di dati comune e multidimensionale per eseguire query e analisi in modo efficiente.

Da questo repository, è possibile generare report personalizzati come chargeback, analisi dei consumi e report di previsione che rispondono a domande come le seguenti:

- Di quale inventario dispongo?
- Dov’è il mio inventario?
- Chi utilizza le nostre risorse?
- Qual è il chargeback per lo storage allocato per una business unit?
- Quanto spazio di crescita ho sulle porte dello switch?
- Per quanto tempo è necessario acquisire ulteriore capacità di storage?
- Le business unit sono allineate lungo i livelli di storage appropriati?
- Come cambia l’allocazione dello storage in un mese, un quarto o un anno?

Utilizzando il modello di dati fornito con i report di OnCommand Insight, è possibile utilizzare gli strumenti di

creazione dei report per progettare e pianificare i report.

Panoramica del modello di dati

OnCommand Insight fornisce diversi modelli di dati da utilizzare nello sviluppo di report. Ogni modello di dati è un'aggregazione che riepiloga i dati in modo da poterli interrogare e ricercare. Ad esempio, i report sulla pianificazione della capacità utilizzano il modello di dati della capacità.

I modelli di dati di reporting Enterprise di OnCommand Insight forniscono elementi di dati e relazioni interattive tra gli elementi di dati che forniscono viste di business dei dati. Utilizzando gli elementi e le relazioni dei dati, è possibile creare report utilizzando gli strumenti di generazione report di IBM Cognos Analytics consigliati da NetApp.

OnCommand Insight fornisce inoltre data mart che possono essere utilizzati per sviluppare le query SQL. Esiste una distinzione tra questi data mart di query SQL e i modelli di dati utilizzati nel reporting. I singoli modelli di dati di reporting di OnCommand Insight utilizzano lo schema di database OnCommand Insight sottostante fornito nei data mart; tuttavia, i modelli di dati utilizzano tabelle aggiuntive e talvolta nuovi elementi nelle tabelle. Ad esempio, il modello di dati include una tabella dati mensile di capacità nel modello di dati di capacità di storage che si basa sulla tabella dati di capacità dello schema del database e del data mart. Il modello di dati filtra i valori dalla tabella dello schema del database per mostrare solo le informazioni del mese.

Un altro esempio di differenza tra lo schema di database utilizzato nei data mart e il modello di dati è rappresentato dalla tabella delle violazioni e dalla colonna tipo di violazione. Il modello di dati traduce i valori denominati a livello di programmazione nel database in modo che corrispondano al testo visualizzato nell'interfaccia utente Web di OnCommand Insight.

Modelli di dati OnCommand Insight

OnCommand Insight include diversi modelli di dati da cui è possibile selezionare report predefiniti o creare report personalizzati.

Ogni modello di dati contiene un semplice data mart e un data mart avanzato:

- Il data mart semplice offre un rapido accesso agli elementi di dati più comunemente utilizzati e include solo l'ultima snapshot dei dati di Data Warehouse; non include dati storici.
- Il data mart avanzato fornisce tutti i valori e i dettagli disponibili dal data mart semplice e include l'accesso ai valori dei dati storici.
- **Modello dati di capacità**

  Consente di rispondere a domande sulla capacità dello storage, sull'utilizzo del file system, sulla capacità del volume interno, sulla capacità delle porte, sulla capacità del qtree, E capacità delle macchine virtuali (VM). Il modello di dati Capacity è un container per diversi modelli di dati di capacità. È possibile creare report che rispondono a diversi tipi di domande utilizzando questo modello di dati:

  - **Modello di dati sulla capacità dello storage e del pool di storage**

    Consente di rispondere a domande sulla pianificazione delle risorse di capacità dello storage, inclusi i pool di storage e storage, e include dati del pool di storage fisico e virtuale. Questo semplice modello di dati può aiutarti a rispondere alle domande relative alla capacità sul piano e all'utilizzo della capacità dei pool di storage per Tier e data center nel tempo.

    Se non sei ancora al reporting della capacità, devi iniziare con questo modello di dati perché si tratta di

un modello di dati più semplice e mirato. Con questo modello di dati puoi rispondere a domande simili a quelle riportate di seguito:

- Qual è la data prevista per raggiungere la soglia di capacità del 80% dello storage fisico?
- Qual è la capacità dello storage fisico su un array per un determinato Tier?
- Qual è la mia capacità di storage per produttore, famiglia e data center?
- Qual è la tendenza all'utilizzo dello storage su un array per tutti i Tier?
- Quali sono i primi 10 sistemi storage con il massimo utilizzo?
- Qual è la tendenza all'utilizzo dello storage dei pool di storage?
- Quanta capacità è già allocata?
- Quale capacità è disponibile per l'allocazione?

◦ **Modello di dati sull'utilizzo del file system**

Consente di rispondere alle domande sull'utilizzo del file system. Questo modello di dati offre visibilità sull'utilizzo della capacità da parte degli host a livello di file system. Gli amministratori possono determinare la capacità allocata e utilizzata per file system, determinare il tipo di file system e identificare le statistiche di trend in base al tipo di file system. Puoi rispondere alle seguenti domande utilizzando questo modello di dati:

- Quali sono le dimensioni del file system?
- Dove vengono conservati i dati e come si accede, ad esempio, a livello locale o SAN?
- Quali sono le tendenze storiche per la capacità del file system? Quindi, in base a questo, cosa possiamo prevedere per le esigenze future?

◦ **Modello di dati della capacità del volume interno**

Consente di rispondere alle domande relative alla capacità utilizzata per il volume interno, alla capacità allocata e all'utilizzo della capacità nel tempo:

- Quali volumi interni hanno un utilizzo superiore a una soglia predefinita?
- Quali volumi interni rischiano di esaurire la capacità in base a una tendenza?
- Qual è la capacità utilizzata rispetto alla capacità allocata sui nostri volumi interni?

◦ **Modello dati Port Capacity**

Consente di rispondere a domande sulla connettività delle porte dello switch, sullo stato delle porte e sulla velocità delle porte nel tempo. Puoi rispondere a domande simili a quelle riportate di seguito per aiutarti a pianificare l'acquisto di nuovi switch:

- Come si può creare una previsione del consumo delle porte che preveda la disponibilità delle risorse (porte) (in base al data center, al vendor dello switch e alla velocità delle porte)?
- Quali porte potrebbero esaurire la capacità, fornendo velocità dei dati, data center, vendor e numero di porte host e storage?
- Quali sono le tendenze della capacità delle porte dello switch nel tempo?
- Quali sono le velocità delle porte?
- Quale tipo di capacità delle porte è necessaria e quale organizzazione sta per esaurire un determinato tipo di porta o fornitore?
- Qual è il momento migliore per acquistare tale capacità e renderla disponibile?

- **Modello dati Qtree Capacity**

  Consente di trend dell'utilizzo del qtree (con dati come capacità utilizzata e allocata) nel tempo. È possibile visualizzare le informazioni in base a diverse dimensioni, ad esempio per entità aziendale, applicazione, Tier e livello di servizio. Puoi rispondere alle seguenti domande utilizzando questo modello di dati:

  - Qual è la capacità utilizzata per i qtree rispetto ai limiti impostati per applicazione o entità aziendale?
  - Quali sono le tendenze della nostra capacità utilizzata e gratuita, in modo da poter pianificare la capacità?
  - Quali entità aziendali utilizzano la capacità maggiore?
  - Quali applicazioni consumano il maggior numero di capacità?

- **Modello di dati della capacità delle macchine virtuali**

  Consente di creare report sull'ambiente virtuale e sull'utilizzo della capacità. Questo modello di dati consente di creare report sulle modifiche dell'utilizzo della capacità nel tempo per le macchine virtuali e gli archivi di dati. Il modello di dati fornisce anche dati di thin provisioning e chargeback delle macchine virtuali.

  - Come è possibile determinare il chargeback della capacità in base alla capacità fornita a macchine virtuali e archivi dati?
  - Quale capacità non viene utilizzata dalle macchine virtuali e quale porzione di inutilizzato è libera, orfana o di altro tipo?
  - Quali sono i requisiti per l'acquisto in base alle tendenze di consumo?
  - Quali sono i risparmi in termini di efficienza dello storage ottenuti utilizzando le tecnologie di thin provisioning e deduplica dello storage? Le capacità del modello di dati della capacità della macchina virtuale sono prese dai dischi virtuali (VMDK). Ciò significa che la dimensione di provisioning di una macchina virtuale che utilizza il modello di dati della capacità della macchina virtuale corrisponde alla dimensione dei dischi virtuali. Si tratta di una funzione diversa dalla capacità fornita nella vista macchine virtuali di OnCommand Insight, che mostra le dimensioni del provisioning per la macchina virtuale stessa.

- **Modello di dati Volume Capacity**

  Consente di analizzare tutti gli aspetti dei volumi nel proprio ambiente e di organizzare i dati in base a vendor, modello, Tier, livello di servizio e data center. È possibile visualizzare la capacità relativa ai volumi orfani, ai volumi inutilizzati e ai volumi di protezione (utilizzati per la replica). È inoltre possibile visualizzare diverse tecnologie di volume (iSCSI o FC) e confrontare volumi virtuali con volumi non virtuali per problemi di virtualizzazione degli array. Questo modello di dati consente di rispondere a domande simili a quelle riportate di seguito:

  - Quali volumi hanno un utilizzo superiore a una soglia predefinita?
  - Qual è la tendenza del mio data center per quanto riguarda la capacità dei volumi orfani?
  - Quanta capacità del mio data center è virtualizzata o con thin provisioning?
  - Quanta capacità del data center deve essere riservata alla replica?

- **Modello di dati chargeback**

  Consente di rispondere alle domande sulla capacità utilizzata e allocata sulle risorse di storage (volumi, volumi interni e qtree). Questo modello di dati fornisce informazioni di chargeback della capacità dello

storage e di responsabilità per host, applicazioni ed entità aziendali e include dati attuali e storici. I dati dei report possono essere classificati in base al livello di servizio e al livello di storage.

È possibile utilizzare questo modello di dati per generare report di chargeback individuando la quantità di capacità utilizzata da un'entità aziendale. Questo modello di dati consente di creare report unificati di più protocolli (tra cui NAS, SAN, FC e iSCSI).

- Per lo storage senza volumi interni, i report di chargeback mostrano il chargeback in base ai volumi.
- Per lo storage con volumi interni:
  - Se le entità aziendali sono assegnate ai volumi, i report di chargeback mostrano il chargeback per volumi.
  - Se le entità di business non sono assegnate ai volumi ma assegnate ai qtree, i report di chargeback mostrano il chargeback per qtree.
  - Se le entità di business non sono assegnate ai volumi e non alle qtree, i report di chargeback mostrano il volume interno.
  - La decisione se mostrare il chargeback per volume, qtree o volume interno viene presa per ogni volume interno, pertanto è possibile che diversi volumi interni nello stesso pool di storage mostrino il chargeback a diversi livelli. I dati relativi alla capacità vengono eliminati dopo un intervallo di tempo predefinito. Per ulteriori informazioni, vedere processi di data warehouse.

  I report che utilizzano il modello di dati Chargeback potrebbero visualizzare valori diversi rispetto a quelli che utilizzano il modello di dati Storage Capacity.
- Per gli array di storage che non sono sistemi di storage NetApp, i dati di entrambi i modelli di dati sono gli stessi.
- Per i sistemi storage NetApp e Celerra, il modello di dati Chargeback utilizza un singolo layer (di volumi, volumi interni o qtree) per basare le proprie spese, mentre il modello di dati Storage Capacity utilizza più layer (di volumi e volumi interni) per basare le proprie spese.

- **Modello di dati di inventario**

  Consente di rispondere a domande sulle risorse di inventario, tra cui host, sistemi storage, switch, dischi, nastri, qtree, quote, macchine virtuali e server e dispositivi generici. Il modello di dati di inventario include diversi sottomarini che consentono di visualizzare informazioni su repliche, percorsi FC, percorsi iSCSI, percorsi NFS e violazioni. Il modello di dati di inventario non include dati storici. Le domande a cui puoi rispondere con questo data mart potrebbero includere:

  - Quali risorse sono disponibili e dove si trovano?
  - Chi utilizza le risorse?
  - Quali tipi di dispositivi sono disponibili e quali sono i componenti di tali dispositivi?
  - Quanti host per sistema operativo sono disponibili e quante porte esistono su tali host?
  - Quali array di storage per vendor esistono in ogni data center?
  - Quanti switch per vendor ho in ogni data center?
  - Quante porte non sono concesse in licenza?
  - Quali nastri vendor utilizziamo e quante porte esistono su ciascun nastro?
  - Tutti i dispositivi generici vengono identificati prima di iniziare a lavorare sui report?
  - Quali sono i percorsi tra host e volumi o nastri di storage?
  - Quali sono i percorsi tra dispositivi generici e volumi o nastri di storage?

- Quante violazioni di ogni tipo ho per data center?
- Per ciascun volume replicato, quali sono i volumi di origine e di destinazione?
- Sono presenti incompatibilità del firmware o discorrispondenze della velocità delle porte tra HBA host Fibre Channel e switch?

- **Modello di dati delle performance**

  Consente di rispondere a domande sulle performance di volumi, volumi applicativi, volumi interni, switch, applicazioni, VM, VMDK, ESX rispetto a VM, host e nodi applicativi. Utilizzando questo modello di dati, è possibile creare report in grado di rispondere a diversi tipi di domande sulla gestione delle performance:

  - Quali volumi o volumi interni non sono stati utilizzati o a cui non è stato effettuato l'accesso durante un periodo specifico?
  - Possiamo individuare eventuali errori di configurazione dello storage per un'applicazione (non utilizzata)?
  - Qual è stato il modello generale di comportamento di accesso per un'applicazione?
  - I volumi a più livelli sono assegnati in modo appropriato per una data applicazione?
  - Potremmo utilizzare uno storage più conveniente per un'applicazione attualmente in esecuzione senza alcun impatto sulle performance delle applicazioni?
  - Quali sono le applicazioni che producono più accessi allo storage attualmente configurato? Quando si utilizzano le tabelle delle prestazioni dello switch, è possibile ottenere le seguenti informazioni:
  - Il traffico host attraverso le porte connesse è bilanciato?
  - Quali switch o porte presentano un elevato numero di errori?
  - Quali sono gli switch più utilizzati in base alle performance delle porte?
  - Quali sono gli switch sottoutilizzati in base alle performance delle porte?
  - Qual è il throughput di tendenza dell'host in base alle performance delle porte?
  - Qual è l'utilizzo delle performance degli ultimi X giorni per uno specifico host, sistema storage, nastro o switch?
  - Quali dispositivi producono traffico su uno switch specifico (ad esempio, quali dispositivi sono responsabili dell'utilizzo di uno switch altamente utilizzato)?
  - Qual è il throughput per una specifica business unit nel nostro ambiente? Quando si utilizzano le tabelle delle prestazioni dei dischi, è possibile ottenere le seguenti informazioni:
  - Qual è il throughput per un pool di storage specifico in base ai dati sulle performance dei dischi?
  - Qual è il pool di storage più utilizzato?
  - Qual è l'utilizzo medio del disco per uno storage specifico?
  - Qual è la tendenza all'utilizzo di un sistema storage o di un pool di storage in base ai dati sulle performance dei dischi?
  - Qual è l'andamento dell'utilizzo del disco per uno specifico pool di storage? Quando si utilizzano le tabelle delle performance di VM e VMDK, è possibile ottenere le seguenti informazioni:
  - Il mio ambiente virtuale funziona in modo ottimale?
  - Quali VMDK stanno riportando i carichi di lavoro più elevati?
  - Come posso utilizzare le performance riportate dai VMD mappati a diversi datastore per prendere decisioni sul re-tiering. Il modello di dati sulle performance include informazioni che consentono di determinare l'adeguatezza dei Tier, le configurazioni errate dello storage per le applicazioni e gli ultimi

tempi di accesso dei volumi e dei volumi interni. Questo modello di dati fornisce dati quali tempi di risposta, IOPS, throughput, numero di scritture in sospeso e stato di accesso.

- **Modello di dati sull'efficienza dello storage**

  Consente di tenere traccia del potenziale e del punteggio di efficienza dello storage nel tempo. Questo modello di dati memorizza le misurazioni non solo della capacità fornita, ma anche della quantità utilizzata o consumata (la misurazione fisica). Ad esempio, quando il thin provisioning è attivato, OnCommand Insight indica la capacità del dispositivo. È inoltre possibile utilizzare questo modello per determinare l'efficienza quando la deduplica è attivata. Puoi rispondere a diverse domande utilizzando il data mart sull'efficienza dello storage:

  - Quali sono i nostri risparmi in termini di efficienza dello storage derivanti dall'implementazione delle tecnologie di thin provisioning e deduplica?
  - Quali sono i risparmi in termini di storage nei data center?
  - In base alle tendenze storiche della capacità, quando è necessario acquistare storage aggiuntivo?
  - Quale sarebbe il guadagno di capacità se si abilassero tecnologie come il thin provisioning e la deduplica?
  - Per quanto riguarda la capacità dello storage, sono a rischio adesso?

Tabelle di dimensioni e fatti del modello di dati

Ogni modello di dati include tabelle di fatti e dimensioni.

- Tabelle dei fatti: Contengono dati misurati, ad esempio quantità, capacità raw e utilizzabile. Contiene chiavi esterne per dimensionare le tabelle.
- Dimension tables (tabelle delle dimensioni): Contiene informazioni descrittive su fatti, ad esempio, data center e business unit. Una dimensione è una struttura, spesso composta da gerarchie, che classifica i dati. Gli attributi dimensionali aiutano a descrivere i valori dimensionali.

Utilizzando attributi di dimensione diversi o multipli (visti come colonne nei report), si creano report che accedono ai dati per ogni dimensione descritta nel modello di dati.

Per una spiegazione di tutti gli elementi dei dati utilizzati per la creazione dei report, consultare il Data Glossary (Glossario dei dati).

Colori utilizzati negli elementi del modello di dati

I colori sugli elementi del modello di dati hanno indicazioni diverse.

- Risorse gialle: Rappresentano le misurazioni.
- Risorse non gialle: Rappresentano gli attributi. Questi valori non vengono aggregati.

Utilizzo di più modelli di dati in un unico report

In genere, si utilizza un modello di dati per ogni report. Tuttavia, è possibile scrivere un report che combina i dati di più modelli di dati.

Per scrivere un report che combina dati provenienti da più modelli di dati, scegliere uno dei modelli di dati da utilizzare come base, quindi scrivere query SQL per accedere ai dati dai data mart aggiuntivi. È possibile utilizzare la funzionalità di Unione SQL per combinare i dati delle diverse query in una singola query che è possibile utilizzare per scrivere il report.

Ad esempio, supponiamo di voler utilizzare la capacità corrente per ciascun array di storage e di voler acquisire annotazioni personalizzate sugli array. È possibile creare il report utilizzando il modello di dati Storage Capacity. È possibile utilizzare gli elementi delle tabelle capacità e dimensioni correnti e aggiungere una query SQL separata per accedere alle informazioni sulle annotazioni nel modello di dati di inventario. Infine, è possibile combinare i dati collegando i dati dello storage di inventario alla tabella Storage Dimension utilizzando il nome dello storage e i criteri di Unione.

FAQ

Domande generali

Questa domanda frequente risponde alle domande generali più comuni su OnCommand Insight.

Quando è stato introdotto OnCommand Insight (OCI)?

OCI è uno dei prodotti per il monitoraggio dell'infrastruttura più maturi del settore, con oltre un decennio di sviluppo attivo. Precedentemente noto come Onaro o SANscreen, il nome SANscreen è stato modificato quando si è Unito alla suite di prodotti del portfolio OnCommand ed è ora indicato come OnCommand Insight, o più comunemente Insight o OCI.

Quanto tempo sarà necessario per l'implementazione di OCI nel mio ambiente?

OCI è semplicemente un download di software. Il software viene installato su due server fisici o virtuali dedicati. Le installazioni tipiche possono essere eseguite in sole 2 ore e i dati di inventario, capacità e performance inizieranno a essere forniti quasi immediatamente. Eventuali criteri aggiuntivi relativi a performance e Best practice, annotazioni dell'utente e setup di consapevolezza dei costi richiederanno ulteriori discussioni sulla pianificazione.

OCI richiede agenti, collettori o sonde?

OCI è al 100% senza agente e non richiede l'uso di agenti, prese o sonde. Il rilevamento di tutte le periferiche viene eseguito in sola lettura, fuori banda e su IP.

In che modo OCI rileva e si connette ai dispositivi?

L'installazione di OCI sfrutta le API e i protocolli nativi spesso già presenti nell'ambiente del data center, senza la necessità di agenti o sonde. SSH, HTTP, SMIS e CLI sono solo alcuni esempi. Laddove esistano già gestori di elementi di dispositivo (ad esempio, l'Unisphere di EMC), OCI comunicherà ai gestori di elementi per acquisire i dati ambientali esistenti. La maggior parte dei rilevamenti delle periferiche richiede solo un indirizzo IP e un nome utente e una password di sola lettura. Questi rilevamenti dei dispositivi possono essere "uno a molti", ad esempio con l'origine dati VMware di OCI. Scoprendo VMware vCenter, OCI scopre a sua volta tutti gli host ESXi e le macchine virtuali associate, tutti con un singolo indirizzo IP e una singola credenziale.

OCI richiede servizi professionali? È disponibile e cosa offrono?

Per ambienti di medie dimensioni, consigliamo Professional Services per implementazione, configurazione e integrazioni, oltre a un'ampia gamma di possibilità personalizzate di reporting e convalida dei dati. Una breve discussione con il team OCI e l'account Engagement Manager può aiutarti a determinare quali servizi ti trarranno maggior beneficio.

Con quale frequenza OCI rilascia aggiornamenti per nuove funzionalità e miglioramenti?

Gli aggiornamenti dei prodotti e i Service Pack sono disponibili per più versioni di OCI. Le release principali o minori vengono in genere fornite ogni pochi mesi, con service pack che includono il supporto per i nuovi dispositivi e il rilascio del firmware con maggiore frequenza. Entrambi sono disponibili sul sito di download support.netapp.com. Alcuni aggiornamenti, ad esempio i nuovi modelli di dischi che provengono più

frequentemente dai produttori, vengono inviati automaticamente al software OCI. Inoltre, la raccolta di dispositivi di origine dati OCI può essere patchata on-site subito dopo una correzione o un aggiornamento dello sviluppo.

In che modo il team di gestione OCI assegna la priorità alle richieste di nuove origini dati?

Il team di gestione dei prodotti di OCI tiene traccia attivamente di tutte le richieste di miglioramento dei clienti e delle funzionalità di interoperabilità (IFR). Ogni richiesta viene dettagliata, valutata per la fattibilità e assegnata una priorità in base alla domanda del cliente e all'impatto strategico generale del business. Una volta accettate, le richieste vengono dimensionate in base al livello di impegno e pianificate per lo sviluppo futuro. La natura agile del processo di sviluppo OCI consente regolarmente di rendere disponibili nuove origini dati al di fuori dei normali cicli di rilascio pianificati. I rappresentanti degli account NetApp possono fornire assistenza nelle richieste dei clienti e nell'invio di nuove richieste per conto dell'utente. Le origini dati possono essere aggiornate on-site, senza la necessità di aggiornare OCI.

La mia azienda funziona completamente su Linux. OCI funzionerà su Linux?

Sì, OCI supporta diverse versioni di Linux e Windows. Tenere presente che Cognos (lo strumento di reporting di IBM utilizzato da OCI in combinazione con Data Warehouse) è supportato solo su Windows, quindi se si utilizza OCI per la creazione di report, sarà necessario eseguire lo strumento di reporting su un server Windows. La Guida all'installazione di OCI elenca i requisiti del server e i sistemi operativi supportati per ciascun componente OCI.

OCI è adatto per ambienti sicuri senza accesso a Internet?

Sì, OCI è utilizzato dalle 10 principali aziende Fortune 500 e dalle principali agenzie bancarie, sanitarie, di ricerca e governative di tutto il mondo. OCI fornisce supporto per le CAC (Military Common Access Card) degli Stati Uniti e offre soluzioni per ambienti geograficamente dispersi o con pareti di fuoco elevate.

Continuo a sapere che OnCommand Unified Manager (OCUM) è la soluzione di gestione per cDOT. Puoi aiutarmi a capire perché userei anche OCI?

Il gestore unificato di OnCommand opera nel layer di storage array "evice management `d`", fornendo un'analisi approfondita degli eventi e degli incidenti degli array Clustered Data ONTAP (cDOT) e delle relative interconnessioni cluster. OCI offre una vista olistica degli ambienti on-premise e distribuiti a livello globale, che comprendono 7-mode, Clustered Data ONTAP e altri array di terze parti. La sua visibilità end-to-end, dalle macchine virtuali al fuso, consente di eseguire trend storici e previsioni di capacità, performance e modellazione dei costi che promuovono un approccio proattivo alla qualità del servizio per la gestione del data center.

Qual è l'ETL secondario OnCommand Insight menzionato nello storefront di automazione?

Il requisito "ETL secondario" a cui si fa riferimento in alcuni download di report di OnCommand Insight Automation Storefront si riferisce a un'implementazione di servizi professionali sviluppata utilizzata per richiamare l'estrazione, la trasformazione e il carico (ETL) aggiuntivi dei dati acquisiti per la popolazione nel data warehouse OnCommand Insight.

Lo scopo principale del processo ETL secondario consiste nel precaricare i dati "batch", consentendo la generazione più rapida di report più complessi o la pianificazione dell'esecuzione giornaliera.

Questo ETL secondario è in aggiunta all'ETL consigliato "una volta al giorno" descritto nella guida

all’amministrazione del data warehouse di OnCommand Insight.

I servizi professionali NetApp sono qualificati per configurare lo scripting ETL secondario per evitare l’impatto sulle pianificazioni dei report OnCommand Insight esistenti, sui backup automatizzati, sulla scalabilità o su altre attività di performance del sistema. Per ulteriori informazioni sulle esigenze di scripting ETL o di convalida dei dati, contatta il tuo rappresentante commerciale NetApp e spiega come i servizi professionali NetApp possono aiutarti.

Licenze OnCommand Insight

Risposte alle domande più frequenti sulle licenze OnCommand Insight.

Panoramica sulle licenze OCI

OCI viene concesso in licenza in base alla capacità. I clienti devono acquistare una licenza per ogni modulo che desiderano abilitare:

Discover è un prerequisito per assicurare, eseguire e pianificare e non viene offerto da solo. Discover è concesso in licenza da TB di capacità gestita.

ASSure è concesso in licenza da TB di capacità gestita (come singola unità di costo per tutte le infrastrutture di storage: FC, NAS, iSCSI, FCoE).

Perform è concesso in licenza da TB di capacità gestita.

Plan è concesso in licenza da TB di capacità gestita.

Per “mcapacità anaged” si intende la capacità raw dei dischi fisici, dei dischi virtuali e dei nastri prima della formattazione. Questo è applicabile a tutto lo storage rilevato da Insight, sia on-premise che nel cloud.

La maggior parte delle origini dati sta considerando la capacità raw di base 2 su disco. Non viene preso in considerazione il ruolo del disco, ad esempio un disco spare, un disco non assegnato o un disco RAID.

Sono disponibili due tipi di licenze Insight: **Perpetual** e **Subscription**.

Le licenze perpetue consentono di utilizzare a tempo indeterminato la versione/release specifica del software ottenuto, in base ai termini di licenza applicabili. Se hai acquistato un Software Support Plan (SSP), NetApp fornisce l’accesso agli aggiornamenti software disponibili in commercio tramite il sito NetApp Support quando e se gli aggiornamenti sono disponibili in conformità ai termini dei servizi di supporto. NetApp fornisce inoltre l’accesso a patch speciali come stabilito dal NetApp Technical Support Center.

L’abbonamento è una licenza a termine del software che concede il diritto di:

- Utilizzare il software on-premise solo per un periodo limitato (generalmente 12 mesi), in base ai termini di licenza applicabili
- Ricevere il supporto software (precedentemente indicato come SSP) per il periodo di validità
- In effetti, il Licenziatario può utilizzare la versione, la release o l’aggiornamento più recenti disponibili in commercio, qualora siano disponibili e riceva supporto per il software

Al termine di ciascun periodo fisso (generalmente 12 mesi), la licenza può essere rinnovata per un ulteriore periodo fisso (generalmente 12 mesi). Se la licenza non viene rinnovata, il Licenziatario non avrà più i diritti di utilizzo del software, non avrà più diritto ai benefici di SSP e dovrà distruggere tutte le copie del software.

Ulteriori informazioni sui moduli di licenza OCI

OCI dispone di 4 moduli di licenza core per soddisfare le esigenze odierne dell'ambiente dei data center. Questi moduli sono **Discover, Perform, Assure e Plan**. Discover è il modulo base ed è necessario per tutti gli altri moduli acquistati.

Il modulo **Discover** consente a OCI di individuare le risorse nel data center e mappare dinamicamente i percorsi di servizio del dispositivo. Vengono fornite informazioni quali capacità, informazioni sul fornitore, modello, firmware e numeri di serie.

Perform è il modulo di raccolta delle performance di OCI. Esegue l'acquisizione di IOPS, throughput, latenza e informazioni su CPU e memoria, oltre a fornire altre analisi.

Assure si colloca in ambienti Fibre Channel e tecnologie per l'efficienza. Aiuta a identificare e gestire i rischi in ambienti Fibre Channel e iSCSI. Assicurare aiuta anche a fornire informazioni su identificazione, mappatura e avvisi di mascheramento, mappatura e suddivisione in zone dei percorsi di servizio e policy di Best practice per l'efficienza, come ridondanza del fabric, switch hop, rapporti fan-out e thin provisioning.

Plan consente di identificare e prevedere le tendenze di calcolo, fabric e vari tipi di storage (cDOT, 7-mode, terze parti) in ambienti ibridi on-premise e di data center distribuiti a livello globale. Consente tempi di conservazione più lunghi. Il Data Warehouse è costituito da un'intelligence integrata che consente l'authoring dei report ed evita il doppio conteggio delle metriche negli ambienti storage condivisi aziendali. È in grado di generare e pianificare un insieme di report prodotti "out of the box" o creare report personalizzati utilizzando i tool di creazione dei report integrati `" drag and drop`".

Configurazione e dispositivi supportati

Questa domanda frequente risponde alle domande più frequenti sulla configurazione OnCommand Insight e sui dispositivi supportati.

OCI apporta modifiche al mio ambiente?

No OCI è uno strumento di sola lettura che raccoglie informazioni sull'ambiente. OCI non apporta alcuna modifica alle risorse o alle configurazioni.

Quale accesso a livello di autorizzazione richiede OCI ai miei dispositivi?

Nella maggior parte dei casi in cui il dispositivo lo supporta, è necessario un accesso di sola lettura. Alcune soluzioni non consentono l'accesso in sola lettura e richiedono pertanto le autorizzazioni elevate appropriate.

Con quale frequenza OCI raccoglie informazioni?

In genere, OCI raccoglie i dati delle performance ogni 5 minuti e scopre costrutti logici e fisici ogni ½ ora OCI imposta gli intervalli di polling predefiniti in base alle Best practice e alla scalabilità suggerite, ma consente all'utente di avere il controllo completo su questi intervalli.

Qual è l'impatto di OCI sul mio ambiente?

Le comunicazioni IP senza agenti, out-of-band e passive di OCI contribuiscono a ridurre al minimo l'installazione, la manutenzione e l'impatto sull'ecosistema del data center. Il team di sviluppo delle performance di OCI adotta misure eccezionali per ridurre al minimo l'impatto sulle performance del data center nelle attività di monitoraggio delle performance stesse. L'impatto è considerato trascurabile nei normali ambienti operativi e può essere rilassato o inasprito nelle piattaforme tecnologiche altamente utilizzate o con

performance inferiori. Per ulteriori informazioni, consultare la Guida all'installazione di OnCommand Insight.

Come posso elencare tutti gli host/VM in OCI?

I widget e le possibilità di elenco delle query di OCI possono essere utilizzati per fornire elenchi di stili di inventario per le risorse del data center. È possibile rendere disponibili elenchi di macchine virtuali fino agli spindle e numerosi costrutti per query, widget, dashboard e report di data warehouse e accedere tramite l'API RESTful.

OCI offre lo stesso tipo di supporto per gli host non hypervisor correlati (ad esempio server fisici)?

Gli hypervisor come VMware forniscono informazioni dettagliate sugli host ESXI e sulle macchine virtuali associate (VM). Per i server fisici, OCI raccoglie le metriche fino all'HBA host. OCI utilizza un metodo unico in cui rileva i server fisici utilizzando una tecnologia in attesa di brevetto. Una volta rilevato lo storage e/o gli switch, i nomi host dei server fisici sono contenuti nelle informazioni alias del fabric. OCI seleziona questi nomi host, li confronta in DNS e porta automaticamente gli host in OCI. Questa tecnica riduce notevolmente la necessità di aggiornamenti manuali dell'immissione e manutenzione dell'inventario degli strumenti.

OCI fornisce la stessa profondità metrica del dispositivo (parità) in ambienti eterogenei?

Esistono diversi livelli di standardizzazione, compatibilità e nomenclatura per le piattaforme di terze parti e le tecnologie dei vendor. OCI tenta di normalizzare le informazioni su capacità e performance in un framework coerente. Alcune metriche di capacità e performance sono fornite in modo nativo dai contatori del dispositivo, come gli IOPS, la latenza e la capacità raw. Quando i contatori non sono forniti, OCI può tentare di riepilogare i valori (ad esempio, totalizzando gli IOPS o le capacità dei volumi sottostanti) e, nei casi in cui non sono disponibili, OCI tenterà di derivare i valori metrici attraverso vari algoritmi di calcolo. OCI offre una funzionalità di integrazione SNMP generica per incorporare metriche aggiuntive non attualmente raccolte da OCI.

OCI supporta gli switch Fibre Channel?

Sì, oltre alla raccolta dei dati dalle risorse di storage, OCI acquisisce anche i dati di inventario e performance dagli switch Cisco, Brocade e QLogic del tuo ambiente.

Sono disponibili viste topopologie dell'intera infrastruttura? OCI mostra "visibilità end-to-end"?

Sì, OCI rileva e mappa dinamicamente i costrutti logici e fisici, fornendo una vista topologia end-to-end interattiva di calcolo, fabric, virtualizzatori e storage back-end. Le icone della topologia consentono di accedere rapidamente alle risorse interessate e di identificare i carichi di lavoro e le violazioni negli ambienti di storage condivisi.

Scalabilità e facilità d'uso

Questa FAQ risponde alle domande più frequenti sulla scalabilità e la facilità d'uso di OnCommand Insight.

In che modo OCI è in grado di scalare?

OCI è leader in termini di interoperabilità e numero di risorse che può acquisire con un impatto minimo. In primo luogo, OCI richiede 2 server virtuali o fisici: Uno per il server operativo che rileva tutte le risorse del data

center e uno per il data warehouse consolidato per il reporting storico a lungo termine. La copertura Enterprise di OCI supporta centinaia di array, decine di migliaia di macchine virtuali, 100,000 percorsi Fibre Channel e oltre 10,000 porte Fibre Channel, il tutto in una singola istanza del server.

Quante persone sono necessarie per gestire l'applicazione OCI?

OCI può essere gestito da una singola persona. Tuttavia, OCI dispone di funzionalità che possono essere utilizzate da più persone all'interno dell'ambiente di business, ciascuna con ruoli diversi, ciascuno con esigenze di reporting, troubleshooting o analytics diverse. Tutti gli sforzi sono fatti per ridurre al minimo la manutenzione degli strumenti, dai menu di stato e notifica che visualizzano i problemi di configurazione al rilevamento automatico degli host fisici collegati a un fabric. Le annotazioni flessibili portano il contesto di business nei dati dell'ecosistema per tutti i tipi di utenti. Dagli amministratori dello storage, del fabric e della virtualizzazione agli addetti alla pianificazione delle capacità, agli analisti aziendali e ai dirigenti, OCI riunisce in un unico pannello di controllo la condivisione delle informazioni tra silos di business e tecnologie.

OCI supporta il reporting personalizzato?

Sì. OCI fornisce il reporting tramite lo strumento di business intelligence IBM Cognos, che consente di creare report completamente personalizzati dai dati raccolti nel Data Warehouse di OCI.

È facile creare report personalizzati?

Il reporting OCI offre funzionalità sia per utenti principianti che avanzati. OCI offre una serie di funzionalità per la creazione di report, tra cui la creazione di report "dRAG and Drop" e la creazione di report basati su query SQL per un impegno più avanzato da parte di utenti o servizi professionali. La soluzione di business intelligence integrata di OCI (IBM Cognos) evita errori comuni come la capacità di doppio conteggio. Con un complemento di report pronti all'uso, widget, query e dashboard, sono disponibili offerte adatte ai requisiti di reporting di chiunque.

I clienti possono anche trovare modelli di reporting scaricabili dal community store OCI.

OCI è in grado di mostrare performance e disponibilità con la semplicità del "semaforo"?

Sì. OCI Data Warehouse e Reporting consentono di creare report con miglioramenti dei colori, ad esempio "condizionale" di valori rosso/giallo/verde. La generazione di un font colorato o di uno sfondo in un report può essere implementata sia dagli utenti finali che dai servizi professionali. Le librerie di widget OCI consentono di visualizzare metriche di performance specifiche per l'azienda in dashboard.

Risoluzione dei problemi relativi alle performance

Questa domanda frequente risponde alle domande più frequenti sulla risoluzione dei problemi relativi alle performance di OnCommand Insight.

Come posso creare un elenco di tutte le risorse più utili del mio ambiente?

Gli analytics di correlazione di OCI aiutano a identificare le risorse avide e degradate per un percorso di servizio specifico. L'analisi generata dalla funzione di correlazione viene eseguita in tempo reale durante la visualizzazione di ciascun oggetto. L'analisi fornita riduce notevolmente il tempo necessario per la risoluzione dei problemi di performance e l'identificazione della causa principale. L'esplorazione delle violazioni generate delle policy di performance definite è un punto di partenza per scoprire risorse avide o degradate. Widget e dashboard che utilizzano le più recenti funzionalità di query consentono di filtrare, ordinare e visualizzare le

risorse con IOPS (avidi), utilizzo o latenza superiori al previsto.

OCI può fornire un unico posto per diagnosticare i problemi di performance?

Sì. Il troubleshooting delle performance in OCI può essere affrontato in diversi modi. OCI offre diversi metodi di avviso. SNMP, Syslog e Avvisi inviati via e-mail vengono utilizzati comunemente. Gli avvisi inviati tramite e-mail consentono agli utenti di fare clic e avviare rapidamente le risorse interessate all'interno di OCI. Una finestra di ricerca globale consente agli amministratori di digitare semplicemente il nome di una risorsa per iniziare ad analizzare la situazione.

La dashboard delle violazioni di OCI consente agli utenti di assegnare priorità alle attività in base al numero di eventi, alla durata e all'ora del giorno. Un esempio di diversi tipi di avviso potrebbe essere latenza, IOPS, utilizzo, severità, business unit o persino applicazione associata.

L'analisi della correlazione di OCI aiuta gli amministratori a confrontare gli oggetti associati alla risorsa interessata e a determinarne l'impatto su IOPS, latenza, utilizzo, CPU e crediti BB.

La tecnologia Query di OCI e le dashboard dei widget consentono di individuare le specifiche in viste organizzate che riguardano le aree problematiche all'interno del data center.

OCI può aiutarti con le migrazioni da 7-mode a cDOT?

Sì, OCI offre una comprensione inestimabile per la domanda di workload esistente e le validazioni successive alla migrazione. Il ruolo di OCI nella modernizzazione del data center di oggi consente simulazioni di gestione delle modifiche, pianificazione dell'ottimizzazione pre-migrazione e definizione del giusto Tier of service. OCI raccoglie e correla senza problemi l'impatto del business su migliaia di condivisioni NFS e percorsi Fibre Channel in ambienti multi-vendor con pochi clic. Dalla migrazione agli aggiornamenti tecnologici, OCI sta fornendo un percorso verso migrazioni affidabili e dimensionate correttamente e mitigando le interruzioni non pianificate del servizio.

Quanto "al time `re`" è il monitoraggio delle performance di OCI?

OCI è considerato **quasi in tempo reale** per la gestione del data center del cloud ibrido e on-premise. Sebbene il polling delle origini dati possa essere configurato in modo che avvenga più spesso, la maggior parte degli utenti non ottiene significativi benefici analitici grazie a un intervallo di raccolta delle performance per la maggior parte dei dispositivi inferiore a 5 minuti. Una raccolta più frequente può gravare sugli oggetti in gestione e sulle analisi eseguite. Naturalmente, in alcuni casi potrebbe essere necessaria una raccolta più granulare e, fortunatamente, OCI offre una flessibilità completa, tra cui l'inventario configurabile dei dispositivi e gli intervalli di polling delle performance per soddisfare le specifiche esigenze dell'ambiente del data center.

Perché il mio "totale" è diverso dal mio "lettura" più "scrittura"?

In alcuni casi, è possibile notare che il *Total* per un contatore non è uguale alla somma di *letture* più *scritture* per quel contatore. Ci sono alcuni casi in cui questo potrebbe accadere.

IOPS: Oltre alle operazioni di lettura e scrittura, un array di storage o un'altra risorsa elaborerà operazioni interne non correlate al flusso di dati del carico di lavoro. Queste operazioni sono talvolta denominate "sSystem", "metadata" o semplicemente "altre" e possono essere attribuite a processi interni come snapshot, deduplica o riallocazione dello spazio. In questi casi, per individuare la quantità di operazioni di sistema per una data risorsa, sottrarre la somma di IOPS *Read* e *Write* dagli IOPS *Total*. La somma degli IOPS di lettura e scrittura è l'IOPS totale direttamente correlato al flusso di dati.

Latenza: Il tempo di risposta totale (latenza) per un'operazione può talvolta essere riportato come *meno del* tempo di risposta in scrittura, perché il tempo di risposta totale è una media ponderata nel tempo. I carichi di

lavoro di i/o sono spesso costituiti da più operazioni di lettura che di scrittura, con le scritture che in genere osservano latenze maggiori. Ad esempio, se un carico di lavoro ha eseguito 10 operazioni di lettura con una latenza media di 5 ms e 5 operazioni di scrittura con una latenza media di 10 ms, la latenza media pesata totale verrà calcolata come il numero di letture volte la latenza media di lettura, più il numero di scritture volte la latenza media di scrittura, diviso per il numero totale di operazioni i/o, ad esempio (10 * 5 + 5 * 10) / (10 + 5) = 6,33 ms.

Perché OCI e OCUM mostrano valori diversi per lo spazio in eccesso?

La nozione di spazio "provisioning" di OnCommand Unified Manager (OCUM) può includere limiti di crescita automatica a cui possono crescere FlexVol (volumi interni di OnCommand Insight). La "capacità" dell'OCI non riflette questi limiti di crescita automatica. Pertanto, in un ambiente in cui esistono Flexvols di crescita automatica, il totale della capacità fornita da OCUM supererà il livello di storage OCI totale "over-commit Capacity" - il delta sarà la differenza tra la capacità di Flexvols e la relativa capacità di crescita automatica.

Gestione dell'ambiente

Questa domanda frequente risponde alle domande più frequenti sulla gestione degli ambienti OnCommand Insight.

È possibile consentire l'accesso a OCI a un utente specifico, limitando la visualizzazione solo a determinate risorse (ad es. SVM e relativi volumi, macchine virtuali, server)?

OCI offre accesso in base al ruolo. Ad esempio, l'accesso al reporting viene controllato attraverso il reporting del data warehouse di OCI. I report possono essere pianificati, inviati via email come PDF, HTML o CSV, oppure a una condivisione di file o persino a un URL che richiede all'utente di autenticarsi prima della visualizzazione. L'accesso basato sull'utente viene concesso sotto forma di amministratori, utenti e ospiti. È disponibile anche il supporto Active directory/ldap.

Integrazione di Insight con altri strumenti

Questa FAQ risponde alle domande più frequenti sull'integrazione di OnCommand Insight con altri strumenti.

OCI può integrarsi con altri strumenti e quali punti di integrazione sono disponibili?

Sì, OCI è una soluzione estensibile (ampiamente aperta) che consente integrazioni con sistemi di orchestrazione, gestione aziendale, controllo delle modifiche e ticketing di terze parti e integrazioni CMDB personalizzate. I principali punti di integrazione dell'API RESTful e del database MySQL aperto di OCI consentono uno spostamento semplice ed efficace dei dati e consentono agli utenti di ottenere un accesso perfetto ai propri dati.

La documentazione API di Insight basata su Swagger si trova nel prodotto sotto **(?) Guida > documentazione API REST**.

Che cos'è Insight BMC Connector?

OnCommand Insight Connector per BMC integra il data warehouse di OnCommand Insight e il database di gestione della configurazione di BMC Atrium (CMDB). Insight Connector per BMC mappa i dati memorizzati

fisici e logici dei sistemi di storage di rete (ad esempio, unità di storage, servizi di storage host, VS Storage Service e VM Storage Service) e le loro relazioni con i dispositivi (host, switch storage, E nastri) e li importa in BMC CMDB come elementi di configurazione e relazioni. Ulteriori informazioni su OnCommand Insight Connector per BMC sono disponibili sul sito del supporto NetApp.

OCI funziona con SCOM o VROP?

Sì, OCI integra numerose soluzioni di gestione del business ed è considerata una fonte autorevole di informazioni su storage, calcolo, hypervisor e fabric per il data center. I clienti di OCI sfruttano l'API RESTful di OCI e il database MySQL Extensible per migliorare numerose applicazioni come BMC Remedy, ServiceNow, SCOM, Vrops e Splunk, per citarne alcuni. OCI estende le integrazioni importando informazioni da quasi tutte le fonti di record e/o inviando le metriche ambientali acquisite ai più diffusi sistemi di monitoraggio, ticketing, fatturazione e orchestrazione CMDB di terze parti.

OCI può lavorare con i servizi cloud che già utilizzo o che sto considerando di utilizzare?

Sì, la gestione degli ambienti di cloud ibrido sia on-premise che agile di OCI offre visibilità quando si determina la piattaforma migliore e più conveniente per le esigenze del tuo servizio di business. OCI può essere sfruttato per l'analisi pre e post-migrazione, contribuendo a identificare i carichi di lavoro adatti al cloud. Per selezionare il servizio cloud appropriato, sono necessari trend storici della capacità, performance e costi. I service design Workshop che sfruttano la densità i/o di OCI e altre metriche possono anche aiutarti a rispondere a domande come se hai ottimizzato il tuo ambiente e se il cloud ha senso. OCI continua a espandere la propria copertura con il supporto per NetApp Private Storage, Cloud ONTAP, Amazon S3 e OpenStack KVM. OCI continua a svolgere un ruolo fondamentale nella campagna di gestione del cloud di NetApp, in particolare nelle aree in cui la visibilità su Capacity Planning, Performance, Service Quality e Chargeback è importante.

OCI può aprire incidenti nella nostra soluzione per la gestione degli incidenti?

Sì, gli eventi di violazione OCI possono essere attivati e inviati via SNMP come trap o tramite Syslog a un server, mentre alcuni tramite l'API RESTful. I dettagli contenuti negli eventi forniti possono essere interpretati da molte soluzioni di gestione degli incidenti e di ticketing di terze parti.

È possibile allocare risorse a una o più business unit?

Sì, OCI incorpora un metodo di tagging dei metadati denominato Annotations. Le business unit, le linee di business, i tenant e i progetti possono essere assegnati alle risorse del data center per un contesto di business più ricco in termini di risorse, pianificazione della capacità, troubleshooting e reporting.

OCI funziona con Work Flow Automator (Wfa)?

Le funzionalità di integrazione di OCI con le tecnologie CMDB, Billing e Orchestration di terze parti sono un valore chiave per il suo successo e WFA non fa eccezione. I Professional Services di NetApp hanno eseguito numerose integrazioni di successo che esistono oggi con i workflow WFA e OCI . È disponibile un connettore WFA per il download per OCI su NetApp Automation Storefront.

Quanto durano i tempi di conservazione OCI per i dati delle performance?

Il server OCI offre 90 giorni di performance quasi in tempo reale e l'inventario corrente (point in time) (costrutti logici e fisici).

Gli intervalli di polling delle performance OCI sono configurabili dall'utente. Le performance dello storage vengono generalmente configurate ogni 5 minuti per la maggior parte dei vendor. Ogni giorno, i dati di

performance/inventario vengono inviati al data warehouse OCI (DWH) per la creazione di report cronologici e previsionali a lungo termine. DWH trasforma questi dati in dati riepilogati (dati di rollup orari, giornalieri e mensili). La nostra capacità di tenere traccia delle “modifiche”, ad esempio la cronologia ambientale monitorata per la configurazione/mappatura di storage/calcolo/fabric, non ha attualmente alcun limite definito.

Data Warehouse conserva i dati storici in base ai data mart e alla granularità dei dati.

Esistono report di pianificazione delle performance?

Sì, sono disponibili diversi report con OCI e molti altri nel nostro catalogo Professional Services, in base al caso di utilizzo. Il modulo Data Warehouse viene fornito anche con una suite di tool per la creazione di report Cognos che consentono agli utenti di creare report personalizzati. È inoltre disponibile una serie di modelli di reporting generati dalla community e altri download dal NetApp Automation Storefront.

IOPS dello storage Data ONTAP

Questa domanda frequente risponde alle domande più frequenti su come i numeri IOPS derivano dai sistemi storage Data ONTAP.

Come vengono derivati gli IOPS dello storage dai sistemi storage Data ONTAP

- Gli IOPS a livello di array di storage vengono aggregati dagli IOPS dei volumi interni
- Gli IOPS a livello di nodo di storage includono OPS meta-dati
- Gli IOPS a livello di pool di storage escludono gli OPS dei meta-dati; misura solo i dischi
- Gli IOPS interni a livello di volume includono OPS di lettura e scrittura (operazioni) + altri OPS

Domanda - in che modo gli IOPS aggregati possono essere a volte superiori agli IOPS del nodo?

Prima di CDOT 8.3.1, gli IOPS dei nodi sono costituiti da IOPS del protocollo. In CDOT 8.3.1. e in seguito, sono costituiti da metriche dei componenti del sistema. Includono richieste 'solo' di dati, richieste che arrivano dalla porta d’ingresso, ma non includono attività di back-end come snapmirrors, deduplica e così via. D’altra parte, queste attività producono IOPS su disco, quindi aggregano IOPS. Di conseguenza, è possibile che gli IOPS aggregati siano superiori agli IOPS del nodo.

Domanda - come vengono calcolati i metadati o altri OPS

Altri OPS = totale - (lettura + scrittura)

Guide pratiche

Introduzione a Insight

Una volta installato e concesso in licenza OnCommand Insight, è necessario iniziare a preparare l'ambiente per la presentazione dei dati importanti.

Alcune delle attività eseguite in un ambiente tipico includono:

1. **Annotando le risorse** per prepararle alle query e ai report. Le annotazioni iniziali utili includono in genere data center, Tier e livello di servizio.
2. **Creazione di query** per mostrare dati importanti e aiutare la risoluzione dei problemi
3. **Assegnazione di applicazioni** e **entità aziendali** alle risorse
4. **Creazione di policy sulle performance** e **avvisi** per violazioni di tali policy
5. **Creazione di dashboard personalizzate** per evidenziare i dati in base alle esigenze o al ruolo dell'utente

Impostazione delle notifiche

È possibile configurare Insight in modo che invii notifiche su eventi di attivazione come policy di performance, percorsi globali o violazioni della capacità tramite e-mail, SNMP o Syslog. È inoltre possibile configurare Insight in modo che invii notifiche e-mail su eventi a livello di sistema come errori di origine dati o guasti dell'unità di acquisizione.

Queste sono istruzioni di base. Per ulteriori informazioni sulle notifiche, vedere Configurazione e amministrazione > Configurazione e amministrazione di Insight > Configurazione di Insight.

Impostazione dell'e-mail per le notifiche

Insight può inviare notifiche e-mail sugli eventi di attivazione, ad esempio le violazioni delle policy sulle performance.

A proposito di questa attività

Per configurare le notifiche e-mail, attenersi alla seguente procedura di base:

Fasi

1. Fare clic su **Admin** > **Notifiche** e passare alla sezione **e-mail**.
2. Nella casella **Server**, immettere il nome del server SMTP. È possibile immettere un nome di dominio completo o un indirizzo IP.
3. Inserire il nome utente SMTP e la password (se richiesta dal server SMTP).
4. Nella casella **email mittente**, inserisci l'account email del mittente che verrà identificato come mittente nelle notifiche.

   Questo account deve essere un account e-mail valido all'interno dell'organizzazione.

5. Nella casella **Firma email**, immettere il testo che si desidera inserire in ogni messaggio inviato.

6. Nella casella **destinatari**, fare clic su ➕Per inserire un indirizzo e-mail, quindi fare clic su **OK**.
7. Fare clic su **Save** (Salva).

   Per modificare o rimuovere un indirizzo e-mail o per inviare un'e-mail di prova, selezionare l'indirizzo e fare clic sul pulsante appropriato visualizzato.

   Nota: È possibile configurare Insight in modo che invii notifiche e-mail per violazioni specifiche dei criteri di performance a singoli individui o gruppi. Ad esempio, è possibile inviare violazioni delle risorse cloud a un gruppo e gli eventi dell'host fisico a un altro. Accedere a **Manage** > **Performance policy** per configurare le notifiche delle singole policy.

Impostazione di Syslog per la registrazione

Insight può inviare eventi syslog per violazioni di capacità o percorso e avvisi sulle performance.

A proposito di questa attività

Per configurare la notifica syslog in Insight, attenersi alla seguente procedura di base:

Fasi

1. Fare clic su **Admin** > **Notifications** e passare alla sezione **Syslog**.
2. Selezionare la casella di controllo **Syslog enabled**.
3. Nel campo **Server**, immettere l'indirizzo IP del server di log.
4. Nel campo **Facility**, selezionare il livello di struttura corrispondente al tipo di programma che sta registrando il messaggio.
5. Fare clic su **Save** (Salva).

Impostazione di SNMP per le notifiche

Insight può inviare notifiche SNMP su eventi di attivazione, ad esempio violazioni o quando vengono superate le soglie dell'origine dati.

A proposito di questa attività

Per configurare SNMP in Insight, attenersi alla seguente procedura di base:

Fasi

1. Fare clic su **Admin** > **Notifications** e passare alla sezione **SNMP**.
2. Fare clic su **azioni** e selezionare **Aggiungi origine trap**.
3. Nella finestra di dialogo **Aggiungi destinatari trap SNMP**, immettere l'indirizzo **IP** e **porta** a cui si desidera inviare i messaggi trap SNMP. Per **Community String**, utilizzare "public" per i messaggi trap SNMP.
4. Fare clic su **Save** (Salva).

Preparazione delle risorse: Annotazione

L'annotazione consente di associare tag o etichette specifiche alle risorse scelte,

agevolando la gestione e il reporting di tali risorse.

Creazione di annotazioni per la tua azienda

Questa guida descrive come creare e personalizzare le annotazioni per il proprio ambiente da utilizzare per eseguire query, filtrare, inviare notifiche di avviso e creare report.

Un'annotazione è una nota o un tag che si associa a risorse specifiche nel proprio ambiente. OnCommand Insight offre diverse annotazioni che è possibile configurare per le risorse in base alle necessità oppure creare annotazioni personalizzate in base alle esigenze aziendali.

Gli esempi che seguono sono quelli generalmente configurati per primi nei nuovi ambienti dei clienti, per fungere da riferimento per ulteriori azioni. Le tue esigenze di annotazione possono variare, ma i passaggi descritti nel presente documento possono essere utilizzati come guida per la configurazione di eventuali annotazioni necessarie sulle risorse che desideri.

Questa guida si basa sui seguenti presupposti:

- Il server OnCommand Insight è installato e concesso in licenza.
- Vuoi esplorare le Best practice, non tutte le opzioni disponibili.
- Comprendete che questi sono solo esempi e che le vostre esigenze specifiche possono variare.

Questa guida illustra la modifica delle annotazioni esistenti e la creazione di annotazioni personalizzate

Nel nostro ambiente di esempio, desideriamo essere in grado di elencare le risorse in base a data center, Tier, livello di servizio e ambiente.

Configurazione delle annotazioni del data center

L'annotazione del data center viene in genere utilizzata per associare un array di storage, uno switch o una risorsa host fisica a una posizione del data center. È possibile associare l'annotazione del data center anche ad altre risorse del proprio ambiente.

Fasi:

- Accedere a Insight come utente con autorizzazioni amministrative.
- Selezionare **Gestisci** > **Annotazioni**.
- Scegliere l'annotazione **Data Center** e fare clic sull'icona **Edit**.
- Fare clic su **+Aggiungi** e aggiungere il nome e la descrizione del primo data center all'elenco delle annotazioni.
- Fai lo stesso per gli altri data center.
- Al termine, fare clic su **Save** (Salva).

Esempi di annotazioni del data center:

Nome	Descrizione
DC1_SVL	Bldg di Sunnyvale 1

DC2_SVLb3	SVL Bldg3 ITA
DC3_NY	New York
DC4_Londra	Londra
…	

Insight è dotato di diversi tipi di annotazione pronti all'uso che consentono agli utenti di definire o modificare i valori in base alle proprie esigenze. Questi tipi di annotazione predefiniti saranno sempre disponibili per l'interfaccia utente Web Insight e per il reporting. Le annotazioni personalizzate appena create sono visibili nell'interfaccia utente Web di Insight, ma richiedono misure aggiuntive per renderle disponibili per il reporting. Per informazioni sull'inclusione di annotazioni personalizzate nei report. Contatta il tuo rappresentante del supporto clienti NetApp.

> Alcuni utenti potrebbero essere inclini a utilizzare l'annotazione Paese per impostare le posizioni delle risorse, invece che in combinazione con l'annotazione del data center. Tuttavia, tenere presente che l'annotazione Country viene trattata come un tipo di annotazione personalizzato nel data warehouse Insight e pertanto potrebbe non essere visualizzata nei report con la stessa granularità del data center.

Configurare le annotazioni Tier

L'annotazione Tier viene utilizzata per associare le risorse ai rispettivi Tier, ad esempio per la contabilità dei costi. Insight viene fornito con una serie di annotazioni Tier predefinite; è possibile modificarle in base alle convenzioni di denominazione dei tiering o creare livelli personalizzati in base alle esigenze.

Quando si impostano le annotazioni Tier, tenere presente quanto segue:

- Il costo è per gigabyte.
- I Tier 1, 2, 3 sono Tier predefiniti configurati a livello di storage array, in base al tipo di disco. Tuttavia, molti clienti avranno diversi tipi di dischi all'interno di un array o tra array dello stesso tipo.
- La Best practice consiste nel creare annotazioni Tier in base al tipo di disco e/o alla velocità del disco. Si tratta di una tipica metodologia Tier; le tue esigenze potrebbero variare.

Fasi:

- Scegliere l'annotazione **Tier** e fare clic sull'icona **Edit**.
- Se lo si desidera, fare clic su **+Aggiungi** e aggiungere il nome e la descrizione del primo livello all'elenco delle annotazioni.
- Fai lo stesso per gli altri livelli.
- Al termine, fare clic su **Save** (Salva).

Annotazioni Tier di esempio:

Nome	Descrizione	Costo per GB

Tier automatico	Tier di storage automatico	0.5
SSD di livello 1	All Flash Array	0.5
SAS di livello 2	SAS	0.25
SATA Tier 3	SATA	0.1
…		

Configurare le annotazioni del livello di servizio

L'annotazione del livello di servizio viene utilizzata per associare le risorse ai rispettivi livelli di servizio.

Le annotazioni dei livelli di servizio sono generalmente impostate solo negli ambienti dei clienti che utilizzano il tiering automatico. Nel data warehouse Insight, è preferibile il Tier. Tuttavia, la Best practice consiste nell'utilizzare il livello di servizio quando si desidera descrivere in dettaglio i costi di provisioning rispetto a. Costo del cliente. Quando entrambi sono presenti nel Data Warehouse, il livello di servizio sostituirà il livello.

Fasi:

- Scegliere l'annotazione **livello di servizio** e fare clic sull'icona **Modifica**.
- Fare clic su **+Aggiungi** e aggiungere il nome e la descrizione del primo livello di servizio all'elenco delle annotazioni.
- Fare lo stesso per gli altri livelli di servizio.
- Al termine, fare clic su **Save** (Salva).

Esempio di annotazioni sul livello di servizio:

Nome	Descrizione	Costo per GB
Livello di servizio 1	Controller FAS con FC o SAS, mirror locale e remoto e nastro	0.93
Livello di servizio 2	Controller FAS con FC o SAS, mirror locali e remoti	0.85
Livello di servizio 3	Controller FAS con SATA e mirror locale	0.48
…		

Configurare le annotazioni dell'ambiente personalizzate

L'annotazione Environment è un'annotazione personalizzata per associare le risorse con la rispettiva posizione ambientale o utilizzo, ad esempio Lab, R&D, produzione, ecc.

Creando l'annotazione Environment e impostandola su queste risorse, è possibile trovare, filtrare e creare report sulle risorse di laboratorio separatamente dalle risorse di produzione, ad esempio.

Fasi:

- Selezionare **Gestisci** > **Annotazioni**.
- Fare clic sul pulsante **+Aggiungi** nella parte superiore della pagina.
- Per **Nome**, immettere '**ambiente**'.
- Per **Description**, immettere '**Asset environment type**'.
- Per **tipo**, selezionare **elenco**. Vengono visualizzati nuovi campi per la creazione dell'elenco.
- Per il momento, lasciare deselezionato **Aggiungi nuove risorse in tempo reale**. Selezionare questa opzione se si desidera aggiungere nuovi ambienti all'elenco di opzioni contemporaneamente all'associazione con le risorse.
- Immettere il nome e la descrizione del primo ambiente.
- Fare clic su **+Aggiungi** e fare lo stesso per gli altri ambienti.
- Al termine, fare clic su **Save** (Salva).

Esempi di annotazioni di ambiente:

Nome	Descrizione
Laboratorio	Laboratorio
Sviluppo	Sviluppo
PRD	Produzione
…	

Ricerca delle risorse: Query

È possibile trovare e visualizzare facilmente le risorse nel proprio ambiente utilizzando potenti query.

Utilizzo delle query per annotare le risorse

Ora che hai creato le tue annotazioni iniziali, diamo un'occhiata a come associarle a risorse specifiche.

Negli esempi che seguono, applicheremo queste annotazioni a risorse specifiche. Ad esempio, creeremo una query per elencare tutti gli array di storage che risiedono in un data center specifico e contrassegneremo quelli con l'annotazione appropriata. Quindi, faremo lo stesso per le risorse appartenenti a un livello e a un livello di servizio specifici.

Query e annotazione dei data center

Le query vengono utilizzate per associare le annotazioni alle risorse appropriate nel proprio ambiente. In questo esempio, verranno associate le annotazioni del data center alle risorse selezionate.

Durante l'acquisizione della fonte di dati, Insight raccoglie (tra le altre informazioni) i nomi di ogni risorsa che rileva. In questo esempio, si presuppone che tutti gli array di storage siano stati denominati in base al data center in cui risiedono, ad esempio "SVL_NN_<label>" per gli array residenti in Sunnyvale. Le query Insight semplificano l'annotazione di queste risorse.

- Accedere a Insight come utente con autorizzazioni amministrative
- Selezionare **Query** > **+Nuova query**
- Selezionare il campo **Cerca…** e scegliere **Storage**. Viene visualizzato un elenco di tutti gli array di storage.
- Nel campo del filtro **Nome**, digitare "SVL" e fare clic su (O premere Invio). L'elenco dei risultati della query viene ora aggiornato per mostrare solo gli array che contengono la stringa "SVL".
- Durante il filtraggio, è possibile utilizzare uno qualsiasi dei seguenti caratteri da solo o combinati per perfezionare la ricerca in qualsiasi casella di testo della pagina Query:
  - Un asterisco consente di cercare tutto. Ad esempio, "vol*rhel" visualizza le risorse che iniziano con "vol" e terminano con "rhel".
  - Il punto interrogativo consente di cercare un numero specifico di caratteri. Ad esempio, il filtraggio per "SVL-PRD??-S12" visualizza SVL-PRD12-S12, SVL-PRD13-S12 e così via.
  - L'operatore OR consente di specificare più entità. Ad esempio, "FAS2240, CX600 O FAS3270" trova più modelli di storage.
- Selezionare gli array di storage che si desidera associare al data center. Una volta selezionati tutti gli array desiderati, fare clic sul pulsante **Actions** (azioni) e selezionare **Edit annotation** (Modifica annotazione).
- Nella finestra di dialogo **Add Annotation** (Aggiungi annotazione), selezionare l'annotazione **Data Center**.
- Scegliere il **valore** desiderato, ad esempio "DC1_SVL".
- Fare clic su **Save** (Salva).
- Se la colonna Data Center non è visibile nella pagina risultati query, selezionarla facendo clic sul pulsante **colonne** e scegliendo **Data Center**.
- Se lo si desidera, è possibile salvare la query per un utilizzo futuro facendo clic sul pulsante **Save** (Salva) nell'angolo superiore destro della pagina Query e assegnando un nome univoco ed esplicito. Ad esempio, "Storage Arrays - SVL data center".

Se si desidera associare l'annotazione "SVL" ad altre risorse, creare una nuova query e seguire questa procedura per ciascun tipo di risorsa desiderato.

Ripetere questi passaggi per le risorse di ciascun data center.

Query e annotazione dei livelli

Le query vengono utilizzate per associare le annotazioni alle risorse appropriate nel proprio ambiente. In questo caso, verranno associati tali livelli alle risorse appropriate.

In precedenza, abbiamo impostato le annotazioni per i tuoi livelli. In questo esempio, verranno associati i Tier ai pool di storage e si presuppone che le annotazioni dei Tier siano configurate come segue:

Valore	Descrizione	Costo per GB
SSD di livello 1	All Flash Array	0.5
SAS di livello 2	SAS	0.25
SATA Tier 3	SATA	0.1

Cerchiamo tutti i dischi SSD nel tuo ambiente e associiamo l'annotazione "SSD Tier 1".

- Accedere a Insight come utente con autorizzazioni amministrative
- Selezionare **Query** > **+Nuova query**
- Selezionare il campo **Cerca…** e scegliere **Pool di storage**. Viene visualizzato un elenco di tutti i pool di storage.
- Il campo **Nome** potrebbe non essere utile questa volta, quindi usiamo un altro campo. Fare clic sull'elenco a discesa **More** (Altro) e selezionare "Least Performing Disk type" (tipo di disco meno performante).

  Questo campo elenca i tipi di dischi a cui siamo interessati. Immettere "SSD" nel campo e fare clic su pulsante. L'elenco dei risultati della query mostra solo i pool di storage SSD.
- È possibile filtrare ulteriormente facendo clic sull'elenco a discesa **More** (Altro) e selezionando altri campi.
- Selezionare i pool di storage che si desidera associare a questo livello. Una volta selezionati tutti i pool di storage desiderati, fare clic sul pulsante **azioni** e selezionare **Modifica annotazione**.
- Nella finestra di dialogo **Add Annotation** (Aggiungi annotazione), selezionare l'annotazione **Tier**.
- Scegliere il **valore** desiderato dall'elenco. Per questo esempio, scegliere "SSD Tier 1".
- Fare clic su **Save** (Salva).
- Se la colonna Tier non è visibile nella pagina Query Results, selezionarla facendo clic sul pulsante **Columns** e scegliendo **Tier**. Dovrebbe essere visualizzata l'annotazione appropriata associata alle risorse.
- Salvare la query facendo clic sul pulsante **Save** nell'angolo in alto a destra della pagina Query e assegnando un nome univoco ed esplicito. Ad esempio, "Storage Pools - Tier 1 SSD".

Se si desidera associare l'annotazione "SSD Tier 1" ad altre risorse, creare una nuova query e seguire questi passaggi per ciascun tipo di risorsa desiderato.

Ripetere questi passaggi per le risorse in ciascuno dei livelli rimanenti.

Annotazioni sul livello di servizio e sull'ambiente

Aggiungi annotazioni sul livello di servizio e sull'ambiente alle risorse appropriate utilizzando i passaggi e i concetti appresi.

Per aggiungere annotazioni sul livello di servizio e sull'ambiente alle risorse appropriate nel proprio ambiente, seguire i passaggi indicati in precedenza, scegliendo le risorse desiderate e le annotazioni appropriate sul livello di servizio o sull'ambiente. È possibile associare più annotazioni alle stesse risorse e, di fatto, questa pratica consente una maggiore flessibilità nella gestione dell'ambiente attraverso Insight.

Dopo aver creato delle query per annotare le risorse, è possibile utilizzare queste annotazioni in diversi modi, ad esempio:

- Policy sulle performance per avvisare l’utente quando si verificano eventi sulle risorse desiderate
- Dashboard e widget personalizzati per monitorare l’attività
- Creazione di report

Struttura aziendale: Creazione di entità aziendali e applicazioni

La comprensione degli elementi della struttura aziendale consente di tenere traccia dell’utilizzo delle risorse e di generare report sui costi.

Configurazione delle entità di business per la tua azienda

La comprensione degli elementi di business della tua struttura aziendale ti aiuta a tenere traccia dell’utilizzo delle risorse e a generare report sui costi. Qui configureremo le tue entità aziendali.

A proposito di questa attività

OnCommand Insight consente di definire le entità di business in una gerarchia che include fino a quattro livelli di granularità.

- **Tenant**

  Utilizzato principalmente dai service provider per associare le risorse a un cliente. Il livello di tenant è necessario se l’azienda è un ISP e si desidera tenere traccia dell’utilizzo delle risorse da parte dei clienti.

- **Line of Business (LOB)**

  Una linea di business o di prodotto all’interno di un’azienda, ad esempio Data Storage. La linea di business è necessaria nella gerarchia se è necessario tenere traccia dei dati delle diverse linee di prodotti.

- **Business Unit**

  Rappresenta una business unit tradizionale, ad esempio legale o di marketing. La 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.

- **Progetto**

  Spesso utilizzato per identificare un progetto specifico all’interno di una business unit per cui si desidera un chargeback della capacità. Ad esempio, “Patents” potrebbe essere un nome di progetto per l’unità aziendale legale e “Sales Events” potrebbe essere un nome di progetto per l’unità aziendale marketing. I nomi dei livelli possono includere spazi.

Un esempio di gerarchia di entità di business potrebbe essere:

```
NetApp
└ Data Storage
    ├ Legal
    │   └ Patents
    └ Marketing
        └ Sales Events
N/A
└ N/A
    └ Safety and Security
        └ N/A
…
```

Best practice: Creare una tabella con ciascuna riga che mostri un'entità aziendale completa nella gerarchia:

Tenant	Linea di business	Unità aziendale	Progetto
NetApp Inc	Storage dei dati	Legale	Brevetti
NetApp Inc	Storage dei dati	Marketing	Eventi commerciali
N/A.	N/A.	Sicurezza	N/A.
…			

Non è necessario utilizzare tutti i livelli nella progettazione della gerarchia aziendale. Puoi scegliere "N/A" per i livelli che non utilizzi.

Per creare una gerarchia di entità di business in Insight:

Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative.
2. Selezionare **Gestisci** > **entità aziendali**.
3. Fare clic sul pulsante **+Aggiungi**
4. Fare clic sulla casella **tenant** e digitare il nome del tenant.

   Se sono già stati inseriti tenant per il proprio ambiente, viene visualizzato un elenco di tenant esistenti tra cui scegliere. È inoltre possibile scegliere N/A se il tenant non si applica a questa entità aziendale.

5. Ripetere l'operazione per **Line of Business**, **Business Unit** e **Project**.
6. Fare clic su **Save** (Salva)

Al termine

Best practice:

- Mappare la gerarchia di business in una tabella e verificare che i nomi nella gerarchia siano esplicativi nelle viste Insight e nei report.
- Crea le tue entità di business in Insight prima di creare applicazioni.
- Identificare ed elencare tutte le applicazioni che saranno associate a ciascuna entità aziendale.

Configurazione delle applicazioni per la tua azienda

La comprensione delle applicazioni utilizzate nell'ambiente aziendale consente di tenere traccia dell'utilizzo delle risorse e di generare report sui costi. Qui configureremo le applicazioni della tua azienda e le assoceremo alle risorse appropriate.

A proposito di questa attività

Nella sezione *Configurazione delle entità di business per la tua azienda*, abbiamo creato alcune entità di business e ti consigliamo di elencare tutte le applicazioni associate a ciascuna entità di business. OnCommand Insight ci consente di tenere traccia dei dati associati a tali applicazioni per attività come l'utilizzo o il reporting dei costi.

Prima di tenere traccia dei dati associati alle applicazioni in esecuzione nel proprio ambiente, è necessario definire tali applicazioni e associarle alle risorse appropriate. È possibile associare le applicazioni alle seguenti risorse: Host, macchine virtuali, volumi, volumi interni, qtree, condivisioni e hypervisor.

In questa procedura dettagliata, desideriamo tenere traccia dell'utilizzo delle macchine virtuali utilizzato dal team di marketing per la posta elettronica Exchange. Ricorderai la seguente tabella creata durante la definizione delle nostre entità di business. Aggiungiamo una colonna a questo foglio di lavoro che elenca le applicazioni utilizzate da ciascuna entità aziendale. (Questa tabella è solo un esempio di foglio di lavoro. Non verrà visualizzata la colonna "Applications" nella tabella delle entità di business in Insight).

Tenant	Linea di business	Unità aziendale	Progetto	Applicazioni
NetApp	Storage dei dati	Legale	Brevetti	Oracle Identity Manager, Oracle on Demand, PatentWiz
NetApp	Storage dei dati	Marketing	Eventi commerciali	Exchange, Oracle Shared Database, BlastOff Event Planner
N/A.	N/A.	Sicurezza	N/A.	N/A.
…				

Creazione di applicazioni in Insight:

Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative.
2. Selezionare **Gestisci** > **applicazioni**
3. Fare clic sul pulsante **+Aggiungi**

4. Immettere il nome dell'applicazione (ad esempio, immettere "Exchange")
5. Selezionare una priorità per l'applicazione
6. Se si desidera associare l'applicazione a un'entità aziendale, selezionarne una dall'elenco a discesa **entità aziendale**. In caso contrario, puoi lasciare l'opzione "None".
7. Se si desidera garantire che ciascun host abbia accesso agli stessi volumi in un cluster, assicurarsi che la casella **convalida condivisione volume** sia selezionata. 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. Se non si utilizza la condivisione del volume, deselezionare la casella **Validate volume sharing** (convalida condivisione volume). Ciò richiede la licenza di assicurazione.
8. Fare clic su Salva.
9. Ripetere l'operazione per tutte le altre applicazioni dell'ambiente.

Al termine

Vediamo che il team di marketing utilizza l'applicazione Exchange. Vogliamo vedere l'utilizzo delle macchine virtuali per Exchange, per prevedere quando sarà necessario aggiungere ulteriore storage. Associiamo l'applicazione Exchange a tutte le macchine virtuali del marketing. Il modo più semplice per farlo è tramite una query.

Seguendo questa procedura, è possibile associare ciascuna applicazione alle risorse appropriate.

Associazione delle applicazioni alle risorse:

Ora che hai creato le tue applicazioni (e le hai legate alle entità aziendali, come desiderato), possiamo associare tali applicazioni alle risorse del tuo ambiente. In questo esempio, l'applicazione Exchange verrà associata a diverse macchine virtuali della tua azienda. Il modo più semplice per eseguire questa operazione è la query.

1. Selezionare **Query** > **+Nuova query**.
2. Nell'elenco a discesa **Select Resource Type** (Seleziona tipo di risorsa), scegliere *Virtual Machine*
3. Supponiamo che il team di marketing nomina le proprie risorse con la stringa "_mktg_". Nella casella del filtro Nome, immettere "`*mktg* `" (senza virgolette) e fare clic sul pulsante Applica (segno di spunta).
4. Viene visualizzato l'elenco di tutte le macchine virtuali con la stringa "`*mktg* `".
5. Se lo si desidera, fare clic sull'elenco a discesa **More** (Altro) e aggiungere altri filtri.
6. Selezionare le macchine virtuali utilizzate per Exchange facendo clic sulla casella di controllo accanto al nome di ciascuna macchina virtuale desiderata oppure selezionare tutte le macchine virtuali facendo clic sulla casella di controllo nella parte superiore della colonna.
7. Una volta selezionate le macchine virtuali desiderate, fare clic sul pulsante **azioni** e scegliere **Aggiungi applicazione**.
8. Nella finestra di dialogo Assegna applicazione, fare clic sull'elenco a discesa **applicazione** e selezionare "Exchange".
9. Fare clic su **Save** (Salva).
10. Ripetere l'operazione secondo necessità per associare l'applicazione Exchange ad altre risorse (host, volumi, ecc.)

Creazione di policy sulle performance per gli avvisi

Le policy sulle performance consentono di monitorare e inviare avvisi quando vengono soddisfatte condizioni specifiche.

A proposito di questa attività

Ora che abbiamo annotato le nostre risorse, creiamo una policy sulle performance che possiamo utilizzare per avvisarci quando la latenza è superiore a 2 ms in qualsiasi array di storage nel nostro data center Sunnyvale (DC1_SVL). Quando si verificano queste condizioni, invieremo un'e-mail ai destinatari selezionati.

Fasi

1. Selezionare **Gestisci** > **Criteri di performance**.

   Viene visualizzata la pagina Performance policy. Sono già state impostate diverse policy predefinite che è possibile modificare in base alle proprie esigenze. Tuttavia, creeremo una nuova politica.

2. Fare clic sul pulsante **+Aggiungi**.

   Viene visualizzata la finestra di dialogo **Aggiungi policy**.

3. Nel campo **Nome policy**, immettere "SVL Data Center Latency 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 di "latenza" per un volume interno e di un altro criterio di "latenza" per un volume diverso. La procedura consigliata consiste nell'utilizzare sempre un nome univoco per qualsiasi policy, indipendentemente dal tipo di oggetto.

4. Per **Apply to objects of type** (Applica a oggetti di tipo), selezionare **Storage** (archiviazione).
5. Nel campo **con annotazione**, selezionare **il data center** è "C1_SVL `D`" (oppure scegliere il nome del data center desiderato).
6. Applicare dopo una finestra di **prima occorrenza** .

   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.

7. Dall'elenco **con severità**, selezionare **Avviso**.
8. Nella sezione **destinatari email**, fare clic per ignorare l'elenco globale dei destinatari. Fare clic su**+**per aggiungere l'indirizzo e-mail del primo destinatario di avviso desiderato, quindi fare clic su **OK**. Ripetere l'operazione per tutti i destinatari di posta elettronica desiderati.
9. Lasciare l'opzione predefinita Create alert (Crea avviso) se si verifica una delle seguenti condizioni. In questo modo viene inviato un avviso se viene soddisfatta una qualsiasi delle soglie impostate. È inoltre possibile scegliere di inviare un avviso solo se vengono soddisfatte le soglie impostate per **tutte**.
10. Per impostare la prima soglia, selezionare **Latency - Total** (latenza - totale) nell'elenco a discesa e impostarla su un valore superiore a 2 ms.
11. Se lo si desidera, aggiungere ulteriori soglie per l'avviso facendo clic sul pulsante **Add threshold** (Aggiungi soglia). Una volta personalizzato il criterio come desiderato, fare clic su **Save** (Salva).
12. È inoltre possibile scegliere di **interrompere l'elaborazione di ulteriori policy se viene generato un**

avviso. In questo modo, gli avvisi aggiuntivi relativi ai criteri verranno interrotte se le condizioni di questo criterio vengono soddisfatte.

13. È possibile aggiungere tutte le nuove policy desiderate, impostando avvisi per altri destinatari in base alle diverse condizioni, in base alle esigenze aziendali. Qualsiasi policy configurata senza destinatari specifici invierà avvisi all'elenco globale dei destinatari impostato nella pagina **Admin** > **Notifiche**

Al termine

Ogni nuova policy viene attivata automaticamente al momento del salvataggio e i destinatari iniziano a ricevere avvisi quando le condizioni della policy vengono soddisfatte (nota come *violazione*). È inoltre possibile monitorare queste violazioni nella dashboard * > * dashboard violazioni*.

Evidenziazione dei dati tramite dashboard

Ora che hai annotato le tue risorse e configurato le policy sulle performance per avvisare in caso di violazioni, puoi creare dashboard per evidenziare i dati specifici che desideri indirizzare.

A proposito di questa attività

In questo esempio forniremo una vista di alto livello della creazione di dashboard creando una dashboard con un singolo widget che evidenzia i dati delle performance delle macchine virtuali. È possibile aggiungere tutti i widget necessari in una singola dashboard e creare tutte le dashboard necessarie. I widget possono essere ridimensionati e spostati come desiderato.

Ulteriori informazioni su dashboard e widget sono disponibili nella documentazione di OnCommand Insight.

Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative.
2. Dal menu **Dashboard**, selezionare **+nuovo dashboard**.

   Viene visualizzata la pagina nuovo dashboard.

3. Best practice: Assegna un nome e salva la dashboard non appena la crei. Fare clic sul pulsante **Save** (Salva) e immettere un nome univoco per la dashboard nel campo **Name** (Nome). Ad esempio "VM Performance Dashboard". Fare clic su **Save** (Salva).
4. Se necessario, spostare l'interruttore **Edit** su "on" per attivare la modalità di modifica. In questo modo è possibile iniziare ad aggiungere widget alla dashboard.
5. Fare clic sul pulsante **+widget** e selezionare **Tabella** per aggiungere un nuovo widget tabella alla dashboard.

   Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget).

6. Nel campo Nome, eliminare "Widget 1" e immettere "Virtual Machine Performance Table".
7. Fare clic sull'elenco a discesa tipo di risorsa e modificare **Storage** in **Virtual Machine**.

   I dati della tabella vengono modificati per mostrare tutte le macchine virtuali nell'ambiente.

8. Per aggiungere ulteriori colonne alla tabella, fare clic su *colonne* E selezionare le colonne desiderate, ad esempio*Data Center*, *Storage name* e *Tier*. È possibile ordinare la tabella in base a una di

queste colonne.

9. È possibile impostare i filtri in base alle necessità per evidenziare i dati importanti per questa dashboard, ad esempio, è possibile scegliere di visualizzare solo le macchine virtuali con l'annotazione "Tier 1 - SSD". Fare clic sul pulsante"` + `"accanto a **Filtra per** e selezionare*Tier*. Fare clic su **Any** e immettere "Tier 1 - SSD". Fare clic su per salvare il filtro.

   La tabella ora mostra solo le macchine virtuali nel Tier "SSD".

10. È possibile raggruppare i risultati facendo clic sul pulsante"` + `" accanto a **Raggruppa per** e selezionando un campo per cui raggruppare, ad esempio il data center. Il raggruppamento viene applicato automaticamente alla tabella.
11. Una volta personalizzato il widget in base alle proprie esigenze, fare clic sul pulsante **Save** (Salva).

    Il widget della tabella viene salvato nella dashboard.

12. Puoi ridimensionare il widget sulla dashboard trascinando l'angolo in basso a destra.
13. Per aggiungere altri widget, fare clic sul pulsante **+widget**. Ogni widget viene aggiunto alla dashboard quando viene salvato.
14. Una volta apportate tutte le modifiche desiderate, fare clic su **Save** (Salva) per salvare la dashboard.
15. È possibile creare dashboard aggiuntivi per evidenziare dati diversi.

Creazione di dashboard personalizzati

OnCommand Insight 7.3 include funzionalità avanzate di dashboard personalizzato per offrire agli utenti una vista operativa dei dati importanti per loro e fornire una vista unificata di tali dati.

OnCommand Insight offre agli utenti la flessibilità necessaria per creare dati dell'infrastruttura con viste operative su piattaforme IT, consentendo di creare dashboard personalizzate con una vasta gamma di widget, ciascuno dei quali offre una flessibilità estesa nella visualizzazione e nella creazione di grafici dei dati. In questa procedura verrà creata una dashboard di esempio per evidenziare le performance delle macchine virtuali.

Questa procedura dovrebbe servire solo come esempio e non copre tutti gli scenari possibili. I concetti e le procedure qui descritti possono essere utilizzati per creare dashboard personalizzati per evidenziare i dati specifici per le esigenze specifiche.

Panoramica

È possibile creare una dashboard personalizzata utilizzando uno dei seguenti metodi:

- **Dashboard** > **+Nuova dashboard**
- **Dashboard** > **Mostra tutte le dashboard** e fai clic su **+Aggiungi**

La schermata New Dashboard (Nuova dashboard) dispone di diversi comandi:

- **Time selector**: Consente di visualizzare i dati della dashboard per un intervallo di tempo compreso tra 3 ore e 90 giorni utilizzando il selettore di intervalli di date personalizzato. È possibile scegliere di ignorare questo intervallo di tempo globale nei singoli widget.
- Pulsante **Modifica**: Selezionando "on" si attiva la modalità Modifica, che consente di apportare modifiche

alla dashboard. Per impostazione predefinita, vengono aperti nuovi dashboard in modalità di modifica.

- Pulsante **Salva**: Consente di salvare, rinominare o eliminare la dashboard.
- Pulsante **variabile**: È possibile aggiungere variabili ai dashboard. La modifica della variabile consente di aggiornare tutti i widget contemporaneamente. Per ulteriori informazioni sulle variabili, vedere "Concetti della dashboard personalizzata"
- **Widget**, che consente di aggiungere un numero qualsiasi di tabelle, grafici o altri widget alla dashboard.

I widget possono essere ridimensionati e ricollocati in diverse posizioni all'interno della dashboard, per offrire la migliore visualizzazione dei dati in base alle esigenze attuali.

Tipi di widget

È possibile scegliere tra i seguenti tipi di widget:

Widget **Table**: Una tabella che visualizza i dati in base ai filtri e alle colonne scelti. I dati delle tabelle possono essere combinati in gruppi che possono essere compressi ed espansi.

Grafici di linee, spline, area, area impilata: Sono widget grafici di serie temporali su cui è possibile visualizzare le performance e altri dati nel tempo.

Widget **valore singolo**: Widget che consente di visualizzare un singolo valore che può essere derivato direttamente da un contatore o calcolato utilizzando una query o un'espressione. Ad esempio, è possibile visualizzare la somma degli IOPS totali per tutto lo storage nell'ambiente come singolo valore nella parte superiore della dashboard.

Grafico **Bar**: Un grafico per visualizzare 5, 10, 20 o 50 valori in alto o in basso.

Grafico **Box Plot**: Un grafico del minimo, massimo, mediano e dell'intervallo tra il quartile inferiore e quello superiore dei dati in un singolo grafico.

Grafico **Scatter Plot**: Traccia i dati correlati come punti, ad esempio IOPS e latenza. In questo esempio, si vedranno rapidamente le risorse con latenza elevata e IOPS bassi.

Inoltre, è possibile scegliere tra diversi widget legacy. Nell'elenco a discesa **Widget**, selezionare **Mostra altri…** per visualizzare questi widget.

Concetti della dashboard personalizzata

Dashboard e widget personalizzati consentono una grande flessibilità nella visualizzazione dei dati. Ecco alcuni concetti che ti aiuteranno a ottenere il massimo dalle dashboard personalizzate. Ogni concetto viene spiegato in maggiore dettaglio nelle sezioni seguenti.

Variabili

Le variabili consentono di modificare i dati visualizzati in alcuni o tutti i widget di una dashboard contemporaneamente. Impostando ciascun widget in modo che utilizzi una variabile comune, le modifiche apportate in un'unica posizione causano l'aggiornamento automatico dei dati visualizzati in ciascun widget.

Query e/o espressioni multiple

Ogni widget Time Series (grafici a linee, spline, area o area sovrapposta) può avere fino a cinque query e/o espressioni per determinare quali dati visualizzare, consentendo di confrontare diversi set di dati su un singolo

grafico. Ad esempio, è possibile disporre di un grafico a linee che mostri gli IOPS per storage e macchine virtuali o di un singolo grafico che confronta throughput e latenza per tutti i pool di storage.

Rollup e raggruppamento

I dati visualizzati in ciascun widget vengono arrotolati dai punti dati raccolti. È possibile scegliere di eseguire il rolloup di questi dati in uno dei seguenti modi:

- AVG: Consente di eseguire il rollup dei dati come media dei dati sottostanti
- Max: Consente di eseguire il rollup dei dati al massimo dei dati sottostanti
- Min: Consente di eseguire il rollup dei dati al minimo dei dati sottostanti
- Somma: Consente di eseguire il roling dei dati come somma dei dati sottostanti

Per impostazione predefinita, tutti i dati sottostanti vengono inseriti in una singola voce (tutti) nel grafico o nella tabella. È possibile scegliere di eseguire il rolloup dei dati per un attributo specifico, ad esempio un data center o un Tier, per distribuire i dati sottostanti nei gruppi desiderati. Il widget visualizza i dati solo per gli attributi selezionati.

È possibile raggruppare i dati in un widget tabella in base all'attributo scelto. Ad esempio, è possibile scegliere di raggruppare la tavola in base al data center. I gruppi possono essere espansi o compressi a volontà. I dati relativi alle performance di una tabella vengono arrotolati nell'intestazione del gruppo in base al metodo di rollup impostato nel widget (Average, max, min o SUM).

I widget delle tabelle possono essere ordinati in base a qualsiasi colonna e le colonne possono essere spostate o ridimensionate in base alle esigenze.

Superiore/inferiore

Utilizzare questa opzione per limitare il set di risultati nei widget grafico, per selezionare se visualizzare i risultati N superiori nel widget o i risultati N inferiori. È possibile scegliere questa opzione quando i dati non vengono arrotolati o vengono arrotolati da un attributo specifico.

Sostituire l'ora del dashboard

Per impostazione predefinita, la maggior parte dei widget aggiunti a una dashboard mostra i dati in base all'impostazione dell'intervallo di tempo della dashboard (3h, 24h, 3d, 7d, 30d o intervallo personalizzato). Tuttavia, è possibile ignorare questa impostazione di tempo nei singoli widget per costringerli a mostrare i dati in un contesto temporale specifico, indipendentemente dall'impostazione dell'ora del dashboard.

Questi concetti sono spiegati in maggiore dettaglio nella sezione seguente.

Variabili della dashboard

Le variabili della dashboard consentono di filtrare i dati in più widget su una dashboard in modo rapido e semplice.

Prima di iniziare

Questo esempio richiede l'impostazione dell'annotazione **Città** (chiamata anche attributo Città) su più risorse di storage.

Per ottenere i migliori risultati, imposta diverse città su diversi storage.

A proposito di questa attività

Le variabili offrono un metodo semplice e rapido per filtrare i dati visualizzati in alcuni o in tutti i widget di una dashboard personalizzata. I seguenti passaggi ti guideranno alla creazione di widget che utilizzano variabili e ti mostreranno come utilizzarli nella dashboard.

Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative
2. Fare clic su **Dashboard** > **+New Dashboard**.
3. Prima di aggiungere widget, è necessario definire le variabili da utilizzare per filtrare i dati della dashboard. Fare clic sul pulsante **Variable** (variabile).

   Viene visualizzato l'elenco degli attributi.

4. Supponiamo di voler impostare la dashboard in modo che filtri in base alla città. Selezionare l'attributo **City** dall'elenco.

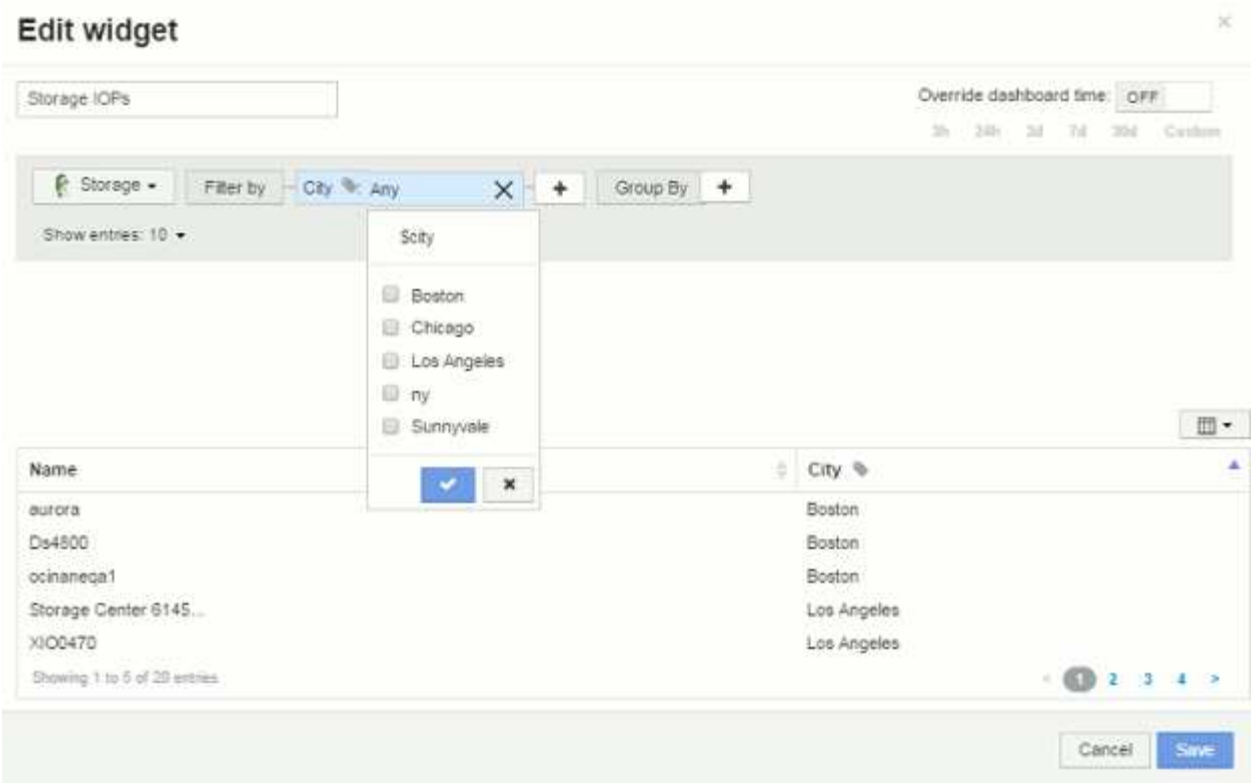
   Il campo della variabile città viene creato e aggiunto alla dashboard.

5. Quindi, dobbiamo dire ai nostri widget di utilizzare questa variabile. Il modo più semplice per illustrare questo aspetto consiste nell'aggiungere un widget di tabella che mostra la colonna Città. Fare clic sul pulsante **Widget** e selezionare il widget **Table**.
6. Per prima cosa, aggiungere il campo Città alla tavola selezionandolo dal selettore di colonne pulsante.

   City è un attributo list-type, quindi contiene un elenco di scelte precedentemente definite. Puoi anche scegliere gli attributi text, boolean o date-type.

7. Quindi, fai clic sul pulsante **Filtra per +** e scegli **Città**.
8. Fare clic su **Any** per visualizzare le possibili opzioni di filtro per Città. Si noti che l'elenco include ora "`City" nella parte superiore, oltre alle opzioni disponibili in precedenza. Selezionare "` City" per utilizzare questa variabile della dashboard.

   La scelta "`` città" viene visualizzata solo se precedentemente definita nella pagina principale del dashboard. Se la variabile non è stata definita in precedenza, verranno visualizzate solo le scelte esistenti per il filtro. Solo le variabili applicabili al tipo di attributo selezionato verranno visualizzate nell'elenco a discesa del filtro.



9. **Salvare** il widget.
10. Nella pagina del dashboard, fare clic su **Any** accanto alla variabile City e selezionare la città o le città che si desidera visualizzare.

    Il widget della tabella viene aggiornato per visualizzare solo le città selezionate. È possibile modificare i valori della variabile città in base alle proprie esigenze e tutti i widget della dashboard impostati per l'utilizzo della variabile città verranno aggiornati automaticamente in modo da visualizzare solo i dati relativi ai valori selezionati.

11. Assicurarsi di **salvare** la dashboard una volta configurata come desiderato.

Ulteriori informazioni sulle variabili della dashboard

Le variabili della dashboard sono disponibili in diversi tipi, possono essere utilizzate in diversi campi e devono seguire le regole per la denominazione. Questi concetti sono spiegati qui.

Tipi di variabili

Una variabile può essere di uno dei seguenti tipi:

Testo: Stringa alfanumerica. Questo è il tipo di variabile predefinito.

Numerico: Un numero o un intervallo di numeri.

Booleano: Utilizzare per i campi con valori True/False, Yes/No, 0/1, ecc. Per la variabile booleana, le scelte sono *Yes*, *No*, *None*, *Any*.

Data: Una data o un intervallo di date.

Variabili “Generic”

È possibile impostare una variabile generica o universale facendo clic sul pulsante **variabile** e selezionando uno dei tipi elencati sopra. Questi tipi vengono sempre visualizzati nella parte superiore dell’elenco a discesa. Alla variabile viene assegnato un nome predefinito, ad esempio "`` var1", e non è legato a un’annotazione o attributo specifico.

La configurazione di una variabile generica consente di utilizzare tale variabile nei widget per filtrare i campi *any* di quel tipo. Ad esempio, se si dispone di un widget di tabella che mostra *Name*, *Alias* e *Vendor* (che sono tutti attributi di tipo testo) e "`` var1" è una variabile di tipo testo, è possibile impostare i filtri per ciascuno di questi campi nel widget per utilizzare la variabile €var1. È possibile impostare altri widget in modo che utilizzino il valore di €var1 per questi o per qualsiasi campo di testo.

Nella pagina della dashboard, impostando il valore di` var1 (ad esempio "`NetApp") si filtreranno *tutti* i campi in *tutti* widget impostati per utilizzare tale variabile. In questo modo, puoi aggiornare più widget contemporaneamente per evidenziare i dati della dashboard scelti a tuo ritmo.

Poiché è possibile utilizzare variabili generiche per qualsiasi campo di quel tipo, è possibile modificare il nome di una variabile generica senza modificarne la funzionalità.

> Tutte le variabili vengono trattate come variabili "generiche", anche quelle create per un attributo specifico, perché tutte le variabili configurate di un tipo vengono visualizzate quando si imposta un filtro per qualsiasi attributo o annotazione di quel tipo. Tuttavia, la procedura consigliata consiste nel creare una variabile generica quando la si utilizzerà per filtrare un valore in più campi, come nell’esempio *Name/Alias/Vendor* riportato sopra.

Naming variabile

Nomi delle variabili:

- Il prefisso deve essere sempre "``". Questa opzione viene aggiunta automaticamente quando si configura una variabile.
- Non può contenere caratteri speciali; sono consentite solo le lettere a-z e le cifre 0-9.
- Non può contenere più di 20 caratteri, incluso il simbolo "``".
- Non sono sensibili al maiuscolo/minuscolo: Il nome della città e il nome della città sono la stessa variabile.
- Non può essere uguale al nome di una variabile esistente.
- Non può essere solo il simbolo "``".

Widget che utilizzano variabili

Le variabili possono essere utilizzate con i seguenti widget:

- Grafico ad area
- Grafico a barre
- Grafico a caselle
- Grafico a linee
- Grafico a dispersione
- Widget a valore singolo
- Grafico Spline

- Grafico ad area sovrapposta
- Widget tabella

Visualizzazione delle legende dei widget

I widget nelle dashboard possono essere visualizzati con o senza legende.

Le legende nei widget possono essere attivate o disattivate su una dashboard in due modi:

1. Quando si crea o si modifica il widget, selezionare la casella di controllo Legends (legende) e salvare il widget.
2. Con la dashboard in modalità Edit (Modifica), fare clic sul pulsante Options (Opzioni) sul widget e selezionare la casella di controllo Legends (legende) nel menu.

Durante la modifica e la modifica dei dati visualizzati nel widget, la legenda del widget viene aggiornata dinamicamente.

Quando vengono visualizzate le legende, se è possibile accedere alla pagina di destinazione della risorsa indicata dalla legenda, la legenda viene visualizzata come collegamento alla pagina della risorsa.

Query e filtri dei widget della dashboard

Il widget Query in a Dashboard è un potente strumento per gestire la visualizzazione dei dati. Di seguito sono riportate alcune informazioni da tenere presenti sulle query dei widget.

Alcuni widget possono avere fino a cinque query. Ogni query traccia il proprio set di righe o grafici nel widget. L'impostazione di rollup, raggruppamento, risultati top/bottom, ecc. su una query non influisce su altre query per il widget.

È possibile fare clic sull'icona occhio per nascondere temporaneamente una query. La visualizzazione del widget si aggiorna automaticamente quando si nasconde o si visualizza una query. Ciò consente di controllare i dati visualizzati per le singole query durante la creazione del widget.

I seguenti tipi di widget possono avere più query:

- Grafico ad area
- Grafico ad area sovrapposta
- Grafico a linee
- Grafico di spline
- Widget a valore singolo

I restanti tipi di widget possono avere una sola query:

- Tabella
- Grafico a barre
- Grafico a caselle
- Grafico a dispersione

Filtraggio nelle query della dashboard

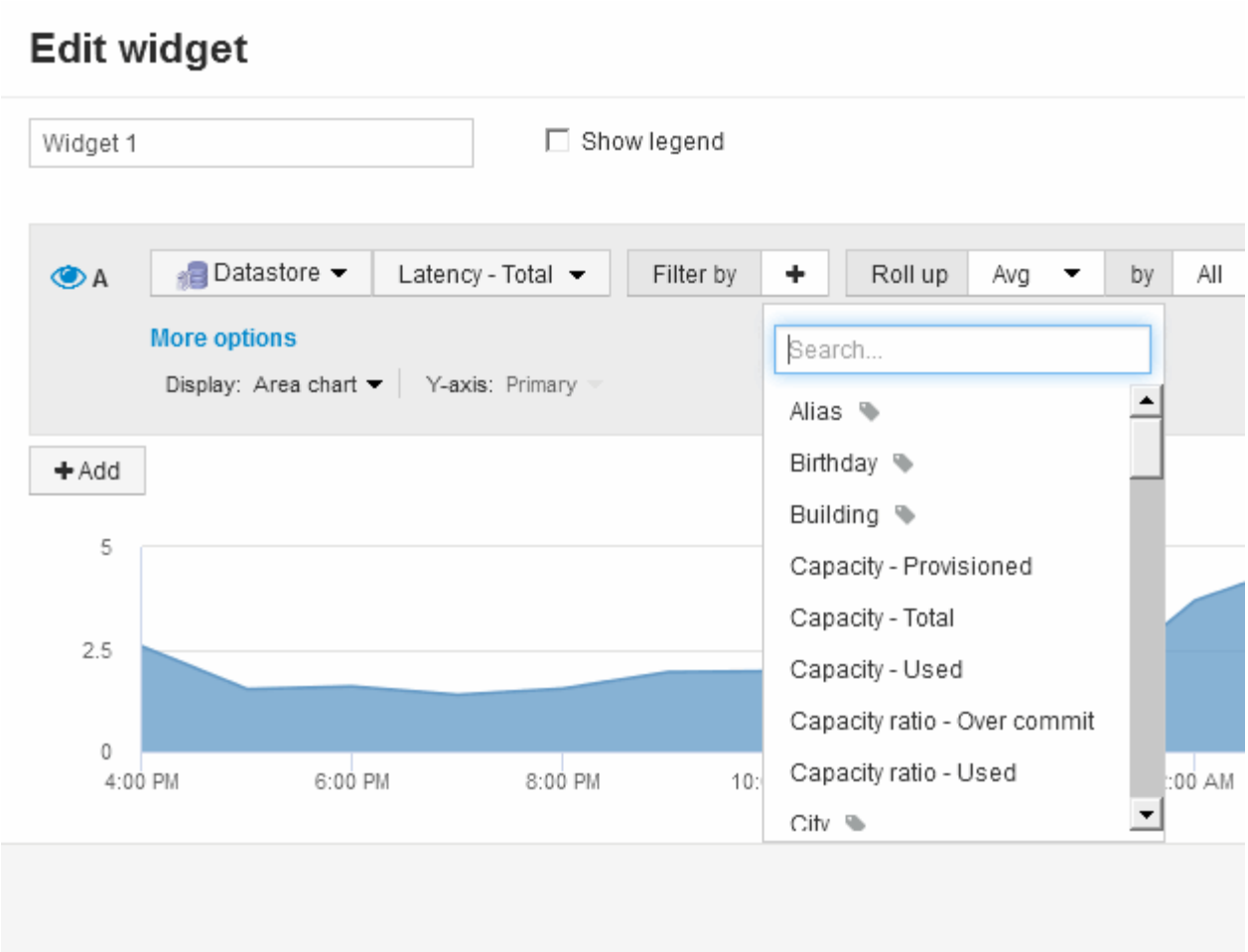
È possibile filtrare utilizzando una delle seguenti opzioni per perfezionare la ricerca in qualsiasi campo di testo* della query:

- 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 contengono valori nulli.

Se racchiudi una stringa di filtro tra virgolette doppie, Insight tratta tutto ciò che va dalla prima all’ultima quotazione come una corrispondenza esatta. Tutti i caratteri speciali o gli operatori all’interno delle virgolette saranno trattati come valori letterali. Ad esempio, il filtraggio per “*” restituisce risultati che sono un asterisco letterale; in questo caso, l’asterisco non verrà trattato come carattere jolly. Gli operatori E, O e NON verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

Identificazione degli oggetti restituiti da query e filtri

Gli oggetti restituiti dalle query e dai filtri sono simili a quelli mostrati nella seguente illustrazione. Gli oggetti con 'tag' assegnati sono annotazioni, mentre gli oggetti senza tag sono contatori delle prestazioni o attributi degli oggetti.



Roll-up e aggregazione

I dati visualizzati nei widget della dashboard vengono arrotolati dai punti dati acquisiti, consentendo flessibilità e concisione nelle dashboard.

I dati visualizzati in ciascun widget vengono arrotolati dai punti dati sottostanti raccolti durante l'acquisizione. Ad esempio, se nel tempo si dispone di un widget grafico a linee che mostra gli IOPS dello storage, potrebbe essere necessario visualizzare una riga separata per ciascuno dei data center, per un rapido confronto. È possibile scegliere di eseguire il rolloup di questi dati in uno dei seguenti modi:

- **Media**: Visualizza ciascuna riga come *media* dei dati sottostanti.
- **Max**: Visualizza ogni riga come *massimo* dei dati sottostanti.
- **Min**: Visualizza ogni riga come *minimo* dei dati sottostanti.
- **SUM**: Visualizza ogni riga come *somma* dei dati sottostanti.

Per farlo, nella query del widget, scegli prima un tipo di risorsa (ad esempio, *Storage*) e una metrica (ad esempio *IOPS - Total*). Per **Roll up**, scegliere un metodo di rollup (ad esempio *Avg*) e selezionare un attributo o un'annotazione in base alla quale eseguire il rollup dei dati (ad esempio, *Data Center*). Il widget si aggiorna automaticamente e mostra una riga per ciascun data center.

Puoi anche scegliere di eseguire il rollup di *tutti* i dati sottostanti nel grafico o nella tabella. In questo caso, otterrai una singola riga per ogni query nel widget, che mostrerà la media, il minimo, il massimo o la somma della metrica scelta per tutte le risorse sottostanti.

Se è stato impostato un filtro per la query, i dati di cui viene eseguito il rollup si basano sui dati filtrati.

Nota: Quando scegli di eseguire il rollup di un widget per qualsiasi campo (ad esempio, *Model*), dovrai comunque **Filtra per** quel campo per visualizzare correttamente i dati di quel campo sul grafico o sulla tabella.

Aggregando i dati: è possibile allineare ulteriormente i grafici delle serie temporali (linee, aree, ecc.) aggregando i punti dati in bucket di minuti, ore o giorni prima che i dati vengano successivamente arrotolati per attributo (se scelto). È possibile scegliere di aggregare i punti dati in base al valore medio, massimo, minimo o somma oppure in base all'ultimo punto dati raccolto durante l'intervallo selezionato. Per scegliere un metodo di aggregazione, fare clic su **altre opzioni** nella sezione delle query del widget.

L'intervallo minimo consentito è di dieci minuti. Un piccolo intervallo combinato con un lungo intervallo di tempo può determinare un "intervallo di aggregazione che ha determinato un numero eccessivo di punti dati". attenzione. Questo potrebbe essere visualizzato se si dispone di un intervallo limitato e si aumenta l'intervallo di tempo del dashboard a 7 giorni. In questo caso, Insight aumenterà temporaneamente l'intervallo di aggregazione a 1 ora fino a quando non si seleziona un intervallo di tempo inferiore.

Puoi anche aggregare i dati nel widget per grafici a barre e nel widget a valore singolo.

Per impostazione predefinita, la maggior parte dei contatori delle risorse viene aggregata a *Avg*. Per impostazione predefinita, alcuni contatori vengono aggregati a *Max*, *min* o *SUM*. Ad esempio, per impostazione predefinita, gli errori di porta si aggregano a *SUM*, dove gli IOPS dello storage si aggregano a *Avg*.

Visualizzazione dei risultati in alto/in basso nei widget della dashboard

In un widget grafico su una dashboard personalizzata, è possibile visualizzare i risultati superiori o inferiori per i dati arrotolati e scegliere il numero di risultati visualizzati. In un widget tabella, è possibile selezionare il numero di righe visualizzate e ordinare in base a qualsiasi colonna.

Widget grafico in alto/in basso

In un widget grafico, quando si sceglie di eseguire il rollup dei dati in base a un attributo specifico, è possibile visualizzare i risultati in alto N o in basso N. Nota: Non è possibile scegliere i risultati superiori o inferiori quando si sceglie di eseguire il rollup in base agli attributi *all*.

È possibile scegliere i risultati da visualizzare scegliendo **Top** o **Bottom** nel campo **Show** della query e selezionando un valore dall'elenco fornito.

Il widget tabella mostra le voci

In un widget tabella, è possibile selezionare il numero di risultati visualizzati nella tabella dei risultati. È possibile scegliere tra 5, 10, 20 o 50 risultati. Non è possibile scegliere i risultati superiori o inferiori, in quanto la tabella consente di ordinare in ordine crescente o decrescente in base a qualsiasi colonna su richiesta.

È possibile scegliere il numero di risultati da visualizzare nella tabella della dashboard selezionando un valore dal campo **Mostra voci** della query.

Si noti che più risultati si sceglie di visualizzare, più alto sarà il widget quando lo si salva nella dashboard. Non sarà possibile ridimensionare il widget più piccolo del numero di righe visualizzate.

Raggruppamento in widget tabella

I dati in un widget tabella possono essere raggruppati in base a qualsiasi attributo disponibile, consentendo di visualizzare una panoramica dei dati e di approfonirne i dettagli. Le metriche nella tabella vengono inserite per una facile visualizzazione in ogni riga compressa.

I widget tabella consentono di raggruppare i dati in base agli attributi impostati. Ad esempio, è possibile che la tabella mostri gli IOPS di storage totali raggruppati in base ai data center in cui risiedono tali storage. In alternativa, è possibile visualizzare una tabella di macchine virtuali raggruppate in base all'hypervisor che le ospita. Dall'elenco, è possibile espandere ciascun gruppo per visualizzare le risorse di quel gruppo.

Il raggruppamento è disponibile solo nel tipo di widget **Table**.

Rolloup dei dati sulle performance

Se si include una colonna per i dati delle performance (ad esempio, *IOPS - Total*) in un widget di tabella, quando si sceglie di raggruppare i dati è possibile scegliere un metodo di rolloup per tale colonna. Il metodo di rolloup predefinito consiste nella visualizzazione della *media* dei dati sottostanti nella riga del gruppo. l'unità organizzativa può anche scegliere di visualizzare i dati *sum*, *minimum* o *maximum*.

Esempio di raggruppamento (con spiegazione del rollup)

I widget delle tabelle consentono di raggruppare i dati per una visualizzazione più semplice.

A proposito di questa attività

In questo esempio, creeremo un widget di tabella che mostra tutte le macchine virtuali raggruppate per data center.

Fasi

1. Creare o aprire una dashboard e aggiungere un widget **Table**.
2. Selezionare **Virtual Machine** come tipo di risorsa per questo widget.
3. Fare clic su Column Selector (selettore colonna) E scegliere *Hypervisor name* e *IOPS - Total*.

   Tali colonne vengono ora visualizzate nella tabella.

4. Ignoriamo qualsiasi macchina virtuale senza IOPS e includiamo solo macchine virtuali con IOPS totali superiori a 1. Fare clic sul pulsante **Filtra per +** e selezionare **IOPS - totale**. Fare clic su **qualsiasi** e nel campo **da** digitare 1. Lasciare vuoto il campo **to**. Fare clic sul pulsante di selezione per applicare il filtro.

   La tabella mostra ora tutte le macchine virtuali con IOPS totali maggiori o uguali a 1. Si noti che non esiste alcun raggruppamento nella tabella. Vengono visualizzate tutte le macchine virtuali.

5. Selezionare il pulsante **Raggruppa per +**.

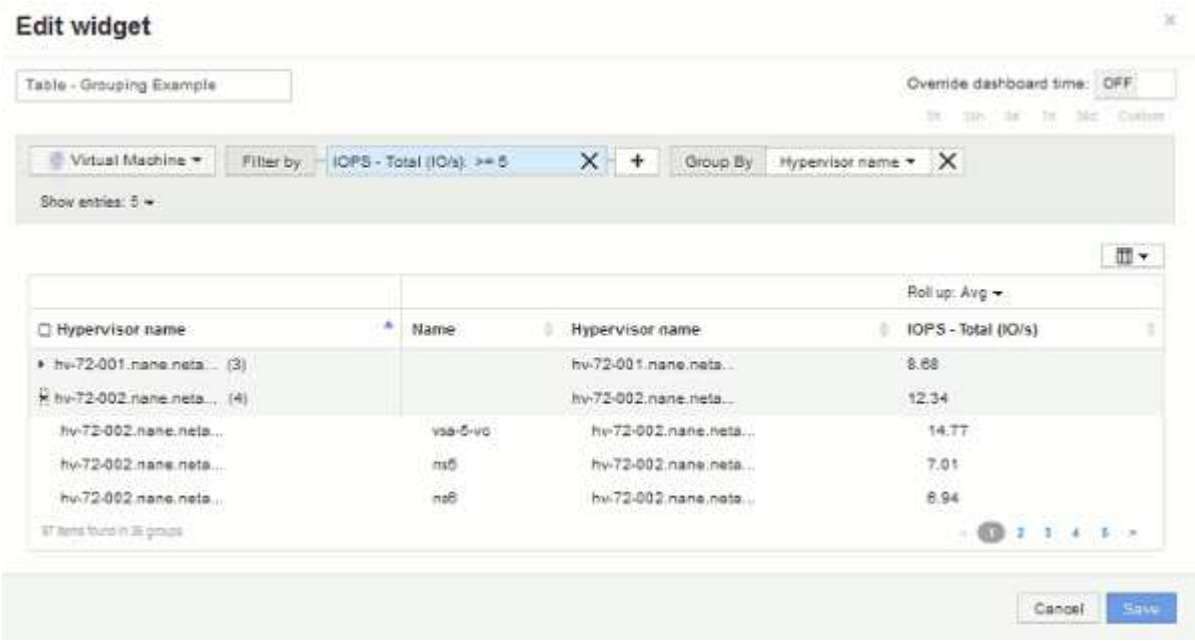
   Poiché l'opzione **all** è selezionata come metodo di raggruppamento per impostazione predefinita, tutte le macchine virtuali vengono spostate in un singolo gruppo denominato "all".

6. Sopra la colonna *IOPS - Total* è ora disponibile l'opzione **Roll-up**. Il metodo di rolloup predefinito è *Avg*.

Ciò significa che il numero visualizzato per il gruppo corrisponde alla media di tutti gli IOPS totali riportati per ciascuna macchina virtuale all'interno del gruppo. Puoi scegliere di far scorrere questa colonna verso l'alto per *Avg*, *SUM*, *min* o *Max*. È possibile eseguire il rollup singolo di ogni colonna visualizzata contenente metriche delle performance.

7. Fare clic su **tutto** e selezionare **Nome hypervisor**.

   L'elenco delle macchine virtuali è ora raggruppato in base all'hypervisor. È possibile espandere ciascun hypervisor per visualizzare le macchine virtuali ospitate dall'IT.



8. Fare clic su **Save** (Salva) per salvare la tabella nella dashboard. È possibile ridimensionare il widget.
9. Fare clic su **Save** (Salva) per salvare la dashboard.

Ignorare il tempo della dashboard per i singoli widget

È possibile ignorare l'impostazione del time frame della dashboard principale nei singoli widget. Questi widget visualizzano i dati in base al periodo di tempo impostato, non al periodo di tempo della dashboard.

Per eseguire l'override dell'ora del dashboard e forzare un widget a utilizzare un proprio intervallo di tempo, nella modalità di modifica del widget impostare **Ignora ora ora ora dashboard** su **on** e selezionare un intervallo di tempo per il widget. **Salva** il widget nella dashboard.

Il widget visualizza i dati in base all'intervallo di tempo impostato, indipendentemente dall'intervallo di tempo selezionato sulla dashboard stessa.

L'intervallo di tempo impostato per un widget non influisce sugli altri widget della dashboard.

Spiegazione degli assi primario e secondario

L'asse secondario semplifica la visualizzazione dei dati da due diversi set di valori che utilizzano unità di misura diverse.

A proposito di questa attività

Metriche diverse utilizzano unità di misura diverse per i dati che riportano in un grafico. Ad esempio, quando si guardano gli IOPS, l'unità di misura è il numero di operazioni di i/o al secondo di tempo (io/s), mentre la latenza è puramente una misura di tempo (millisecondi, microsecondi, secondi, ecc.). Quando si inseriscono entrambe le metriche in un singolo grafico utilizzando un singolo set di valori a per l'asse Y, i numeri di latenza (in genere una manciata di millisecondi) vengono inseriti nella stessa scala con gli IOPS (in genere numerati in migliaia) e la riga di latenza viene persa in quella scala.

Tuttavia, è possibile inserire entrambi i set di dati in un singolo grafico significativo, impostando un'unità di misura sull'asse Y primario (lato sinistro) e l'altra unità di misura sull'asse Y secondario (lato destro). Ogni metrica viene tracciata in base alla propria scala.

Fasi

1. Creare o aprire una dashboard. Aggiungere un widget **grafico a linee**, **grafico a spline**, **grafico a aree** o **grafico a aree impilate** alla dashboard.
2. Selezionare un tipo di risorsa (ad esempio **Storage**) e scegliere **IOPS - Total** per la prima metrica. Impostare i filtri desiderati e scegliere un metodo di roll-up, se desiderato.

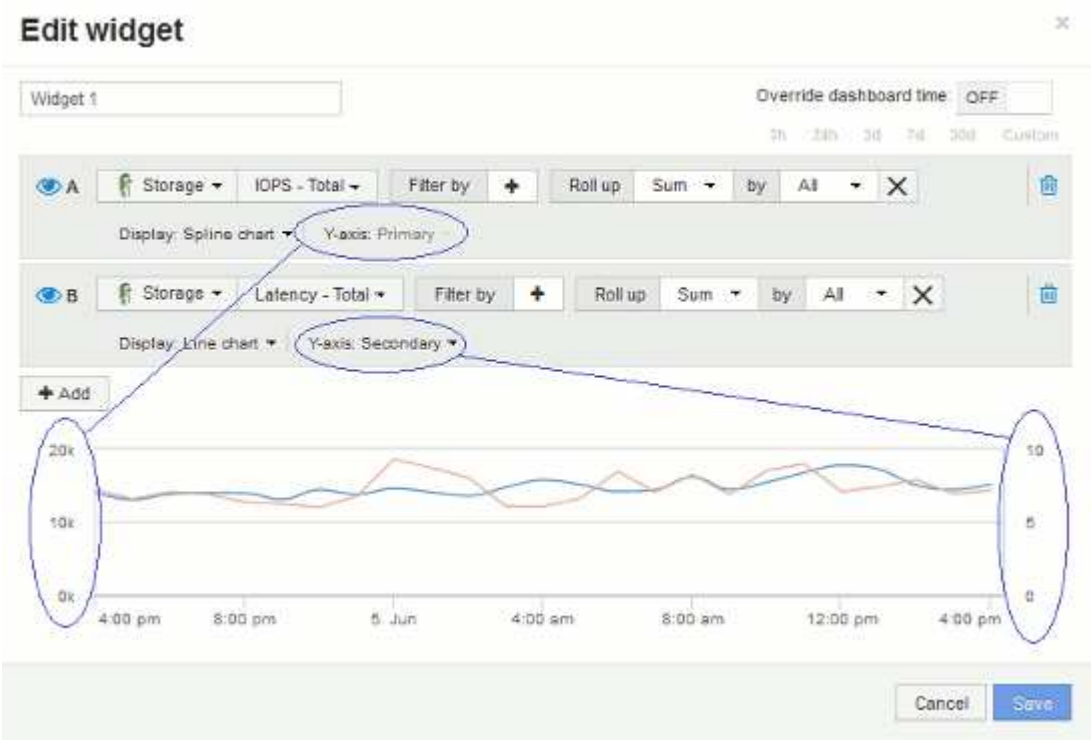
   La riga IOPS viene visualizzata sul grafico, con la relativa scala a sinistra.

3. Fare clic su **+Aggiungi** per aggiungere una seconda riga al grafico. Per questa riga, scegliere **latenza - totale** per la metrica.

   Notare che la riga viene visualizzata piatta nella parte inferiore del grafico. Questo perché viene tracciato alla stessa scala della linea IOPS.

4. Nella query di latenza, selezionare **asse Y: Secondario**.

   La linea di latenza viene ora tracciata in base alla propria scala, che viene visualizzata sul lato destro del grafico.



Espressioni nei widget della dashboard

Le espressioni nei widget Time Series consentono di visualizzare i dati in base ai calcoli con metriche di propria scelta.

In una dashboard, qualsiasi widget Time Series (linea, spline, area, area sovrapposta) consente di creare espressioni a partire dalle metriche scelte e mostrare il risultato di tali espressioni in un singolo grafico. Gli esempi seguenti utilizzano espressioni per risolvere problemi specifici. Nel primo esempio, vogliamo mostrare gli IOPS in lettura come percentuale degli IOPS totali per tutte le risorse di storage nel nostro ambiente. Il secondo esempio ci dà visibilità sugli IOPS "di sistema" o "overhead" che si verificano nel nostro ambiente - quegli IOPS che non sono dalla lettura o dalla scrittura dei dati.

Esempio di espressioni: Percentuale IOPS di lettura

Utilizzando le espressioni, è possibile visualizzare le metriche in modi alternativi, ad esempio in percentuale del totale.

A proposito di questa attività

In questo esempio si desidera visualizzare gli IOPS in lettura come percentuale degli IOPS totali. Si può pensare a questo come alla seguente formula:

- Percentuale di lettura = (IOPS di lettura/IOPS totali) x 100

Questi dati possono essere visualizzati in un grafico a linee sulla dashboard. A tale scopo, attenersi alla seguente procedura:

Fasi

1. Creare una nuova dashboard o aprirne una esistente in **modalità di modifica**.
2. Aggiungere un widget alla dashboard. Scegliere **Area chart**.

   Il widget si apre in modalità di modifica. Per impostazione predefinita, viene visualizzata una query che mostra **IOPS - Total** per le risorse **Storage**. Se lo si desidera, selezionare un tipo di risorsa diverso.

3. Fare clic sul pulsante **Converti in espressione**.

   La query corrente viene convertita in modalità espressione. Non è possibile modificare il tipo di risorsa in modalità espressione. In modalità espressione, il pulsante cambia in **Ripristina query**. Fare clic su questa opzione per tornare alla modalità Query in qualsiasi momento. Tenere presente che il passaggio da una modalità all'altra ripristinerà i valori predefiniti dei campi.

   Per il momento, rimanere in modalità **Expression**.

4. La metrica **IOPS - Total** si trova ora nel campo della variabile alfabetica "a". Nel campo della variabile "b", fai clic su **Seleziona** e scegli **IOPS - lettura**.

   È possibile aggiungere fino a un totale di cinque variabili alfabetiche per l'espressione facendo clic sul pulsante**+**che segue i campi delle variabili. Per il nostro esempio di percentuale di lettura, abbiamo bisogno solo di IOPS totali ("a") e IOPS di lettura ("b").

5. Nel campo **espressione**, utilizzare le lettere corrispondenti a ciascuna variabile per creare l'espressione. Sappiamo che *percentuale di lettura = (IOPS di lettura / IOPS totali) x 100*, quindi scriveremmo questa espressione come: `(b / a) * 100`

6. Il campo **Label** identifica l'espressione. Modificare l'etichetta in "Read percent" (percentuale di lettura) o in qualcosa di altrettanto significativo per l'utente.
7. Modificare il campo **unità** in "%" o "Percent".

   Il grafico mostra la percentuale di lettura IOPS nel tempo per i dispositivi di storage selezionati. Se lo si desidera, è possibile impostare un filtro o scegliere un metodo di rollup diverso. Tenere presente che se si seleziona **Sum** come metodo di rollup, tutti i valori percentuali vengono sommati, che potrebbero superare il 100%.

8. Fare clic su **Save** (Salva) per salvare il grafico nella dashboard.

   È inoltre possibile utilizzare le espressioni nei widget **Line Chart**, **Spline Chart** o **Stacked Area Chart**.

Esempio di espressioni: I/o "di sistema"

Le espressioni ti offrono la libertà di inserire dati che possono essere calcolati da altre metriche.

A proposito di questa attività

Esempio 2: OnCommand Insight acquisisce molte metriche da origini dati. Tra questi vi sono IOPS totali, di lettura e scrittura. Tuttavia, il numero totale di IOPS riportati dall'acquisizione talvolta include IOPS "di sistema", che sono operazioni io che non fanno parte diretta della lettura o scrittura dei dati. Questo i/o di sistema può anche essere considerato come un i/o "overhead", necessario per il corretto funzionamento del sistema ma non direttamente correlato alle operazioni sui dati.

Per visualizzare questi i/o di sistema, è possibile sottrarre gli IOPS di lettura e scrittura dai IOPS totali riportati dall'acquisizione. La formula potrebbe essere simile alla seguente:

- IOPS di sistema = IOPS totali - (IOPS di lettura + IOPS di scrittura)

Questi dati possono quindi essere visualizzati in un grafico a linee sulla dashboard. A tale scopo, attenersi alla seguente procedura:

Fasi

1. Creare una nuova dashboard o aprirne una esistente in **modalità di modifica**.
2. Aggiungere un widget alla dashboard. Scegliere **Line chart**.

   Il widget si apre in modalità di modifica. Per impostazione predefinita, viene visualizzata una query che mostra **IOPS - Total** per le risorse **Storage**. Se lo si desidera, selezionare un tipo di risorsa diverso.

3. Fare clic sul pulsante per creare una copia della query.

   Un duplicato della query viene aggiunto sotto l'originale.

4. Nella seconda query, fare clic sul pulsante **Converti in espressione**.

   La query corrente viene convertita in modalità espressione. Fare clic su **Ripristina query** se si desidera tornare alla modalità Query in qualsiasi momento. Tenere presente che il passaggio da una modalità all'altra ripristinerà i valori predefiniti dei campi.

   Per il momento, rimanere in modalità **Expression**.

5. La metrica **IOPS - Total** si trova ora nel campo della variabile alfabetica “a”. Fare clic su **IOPS - Total** (IOPS - totale) e impostarlo su **IOPS - Read** (IOPS - lettura). .
6. Nel campo della variabile “b”, fai clic su **Select** e scegli **IOPS - Write**.
7. Nel campo **espressione**, utilizzare le lettere corrispondenti a ciascuna variabile per creare l’espressione. Scriveremmo la nostra espressione semplicemente come: `a + b`. Nella sezione **Display**, selezionare**grafico area** per questa espressione.
8. Il campo **Label** identifica l’espressione. Cambia l’etichetta in “SSystem IOPS”, o qualcosa di altrettanto significativo per te.

   Il grafico mostra gli IOPS totali come grafico a linee, con un grafico a aree che mostra la combinazione di IOPS di lettura e scrittura sottostante. Il divario tra i due indica gli IOPS che non sono direttamente correlati alle operazioni di lettura o scrittura dei dati.

9. Fare clic su **Save** (Salva) per salvare il grafico nella dashboard.

Dashboard personalizzato: Performance delle macchine virtuali

I dashboard e i widget personalizzati di OnCommand Insight offrono viste operative sui trend di inventario e performance.

A proposito di questa attività

Le operazioni IT devono affrontare molte sfide. Agli amministratori viene chiesto di fare di più con meno risorse e avere una visibilità completa nei data center dinamici è un must. In questo esempio, ti mostreremo come creare una dashboard personalizzata con widget che ti forniranno informazioni operative sulle performance delle macchine virtuali nel tuo ambiente. Seguendo questo esempio e creando widget per soddisfare le tue esigenze specifiche, potrai visualizzare le performance dello storage back-end rispetto alle performance delle macchine virtuali front-end o visualizzare la latenza delle macchine virtuali rispetto alla domanda di i/O.

I dashboard personalizzati consentono di assegnare priorità agli sforzi e identificare la disponibilità delle risorse. Puoi rispondere al flusso e al flusso di workload e ridurre al minimo il tempo necessario per rilevare e risolvere i problemi emergenti. Le dashboard personalizzate ti consentono di creare viste con priorità nell’infrastruttura business-critical e sono utili per identificare la disponibilità delle performance nelle tecnologie multi-vendor.

In questa sezione verrà creata una dashboard per le performance delle macchine virtuali contenente quanto segue:

- Una tabella che elenca i nomi delle macchine virtuali e i dati relativi alle performance
- Un grafico che confronta la latenza delle macchine virtuali con la latenza dello storage
- Un grafico che mostra gli IOPS totali, di lettura e scrittura per le macchine virtuali
- Un grafico che mostra il throughput massimo per le macchine virtuali

Questo è solo un esempio di base. Puoi personalizzare la dashboard per evidenziare e confrontare i dati sulle performance che scegli di indirizzare alle tue Best practice operative.

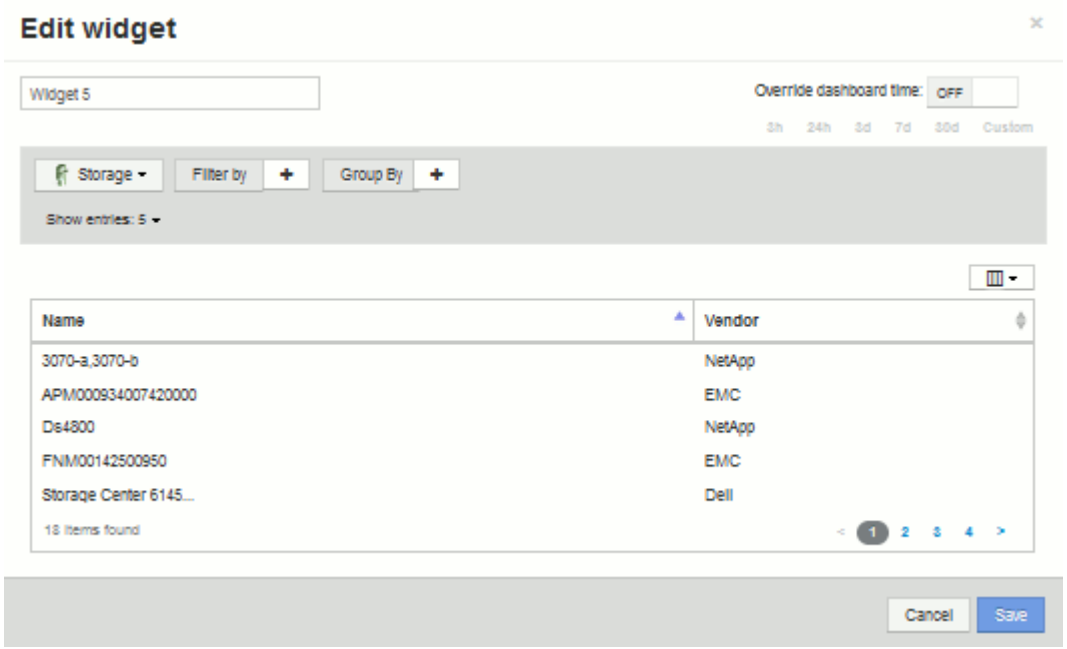
Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative.
2. Dal menu **Dashboard**, selezionare **+nuovo dashboard**.

Viene visualizzata la pagina nuovo dashboard.

3. Diamo un nome significativo alla nostra dashboard. Fare clic su **Save** (Salva). Nel campo **Nome**, immettere un nome univoco per la dashboard, ad esempio “VM Performance by Application”.
4. Fare clic su **Save** (Salva) per salvare la dashboard con il nuovo nome.
5. Iniziamo ad aggiungere i nostri widget. Se necessario, spostare l’interruttore **Edit** su “on” per attivare la modalità di modifica.
6. Fare clic sul pulsante **widget** e selezionare **widget tabella** per aggiungere un nuovo widget tabella alla dashboard.

   Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Il nome predefinito è “Widget 1” e i dati predefiniti visualizzati sono relativi a tutti gli storage dell’ambiente.



7. Possiamo personalizzare questo widget. Nel campo Nome, eliminare “Widget 1” e immettere “Virtual Machine Performance Table”.
8. Fare clic sull’elenco a discesa tipo di risorsa e modificare **Storage** in **Virtual Machine**.

   I dati della tabella vengono modificati per mostrare tutte le macchine virtuali nell’ambiente. Per ora, la tabella mostra solo i nomi delle macchine virtuali. Aggiungiamo alcune colonne alla tabella.

9. Fare clic su *colonne* E selezionare *Data Center*, *Storage name* e *IOPS - Total*. Puoi anche provare a digitare il nome nella ricerca per visualizzare rapidamente i campi desiderati.

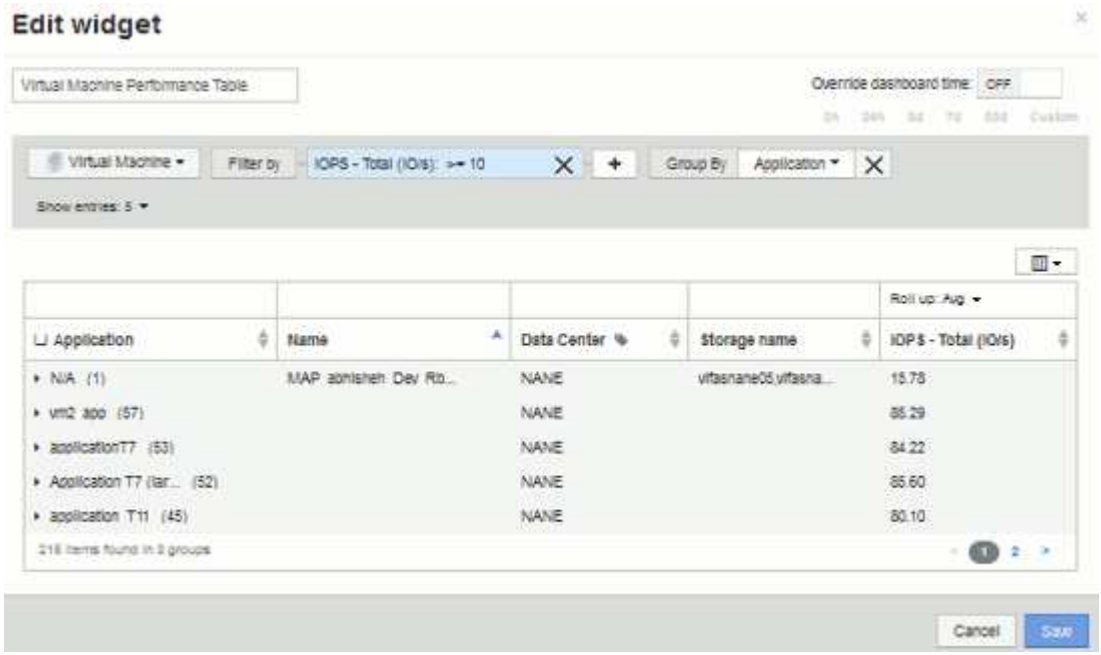
   Queste colonne vengono ora visualizzate nella tabella. È possibile ordinare la tabella in base a una di queste colonne. Le colonne vengono visualizzate nell’ordine in cui sono state aggiunte al widget.

10. Per questo esercizio escludiamo le macchine virtuali che non sono attivamente in uso, quindi filtriamo qualsiasi elemento con meno di 10 IOPS totali. Fare clic sul pulsante"` + `"accanto a **Filtra per** e selezionare*IOPS - Total (io/s)*. Fare clic su **qualsiasi** e digitare “10” nel campo **da**. Lasciare vuoto il campo **to**. Fare clic su per salvare il filtro.

    La tabella ora mostra solo le macchine virtuali con 10 o più IOPS totali.

11. È possibile comprimere ulteriormente la tabella raggruppando i risultati. Fare clic sul pulsante"` + `" accanto a **Raggruppa per** e selezionare un campo per cui raggruppare, ad esempio applicazione o cluster. Il raggruppamento viene applicato automaticamente.

    Le righe della tabella vengono ora raggruppate in base alle impostazioni. È possibile espandere e comprimere i gruppi in base alle esigenze. Le righe raggruppate mostrano i dati arrotolati per ciascuna colonna. Alcune colonne consentono di scegliere il metodo di rolloup per tale colonna.



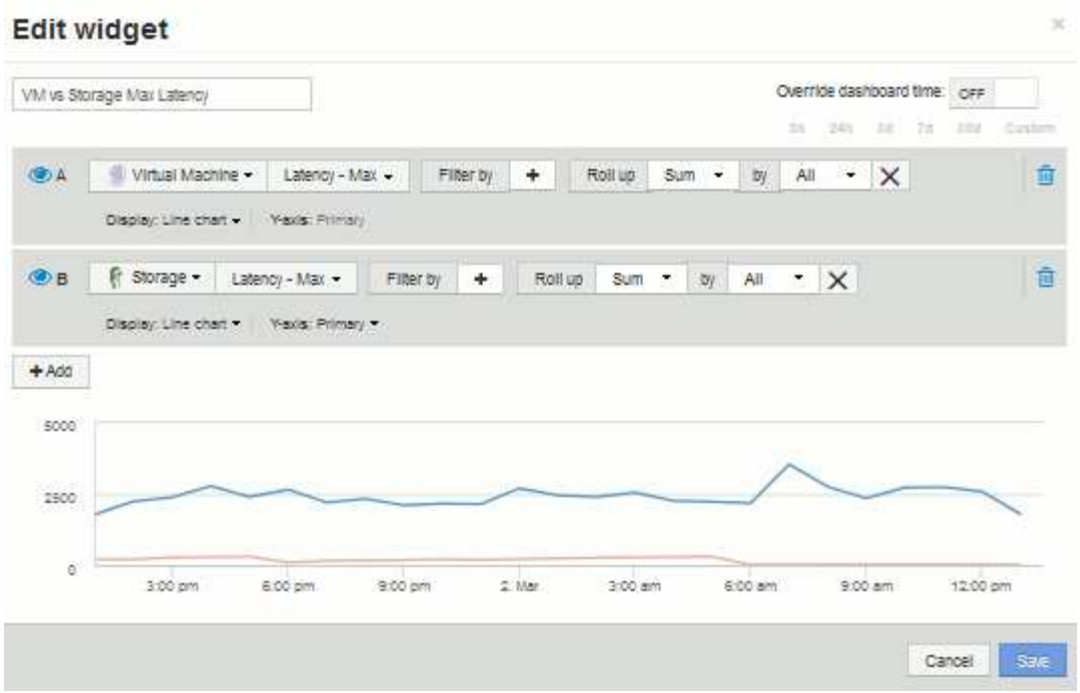
12. Una volta personalizzato il widget della tabella in base alle proprie esigenze, fare clic sul pulsante **Save** (Salva).

    Il widget della tabella viene salvato nella dashboard.

13. Puoi ridimensionare il widget sulla dashboard trascinando l'angolo in basso a destra. Allarga il widget per mostrare tutte le colonne in modo chiaro. Fare clic su **Save** (Salva) per salvare la dashboard corrente.
14. Successivamente aggiungeremo alcuni grafici per mostrare le nostre performance delle macchine virtuali. Creiamo un grafico a linee che confronta la latenza delle macchine virtuali con la latenza dello storage.
15. Se necessario, spostare l'interruttore **Edit** su "on" per attivare la modalità di modifica.
16. Fare clic sul pulsante **Widget** e selezionare **Line Chart** per aggiungere un nuovo widget grafico a linee alla dashboard.

    Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Fare clic sul campo **Nome** e assegnare un nome al widget "VM vs Storage Max Latency"

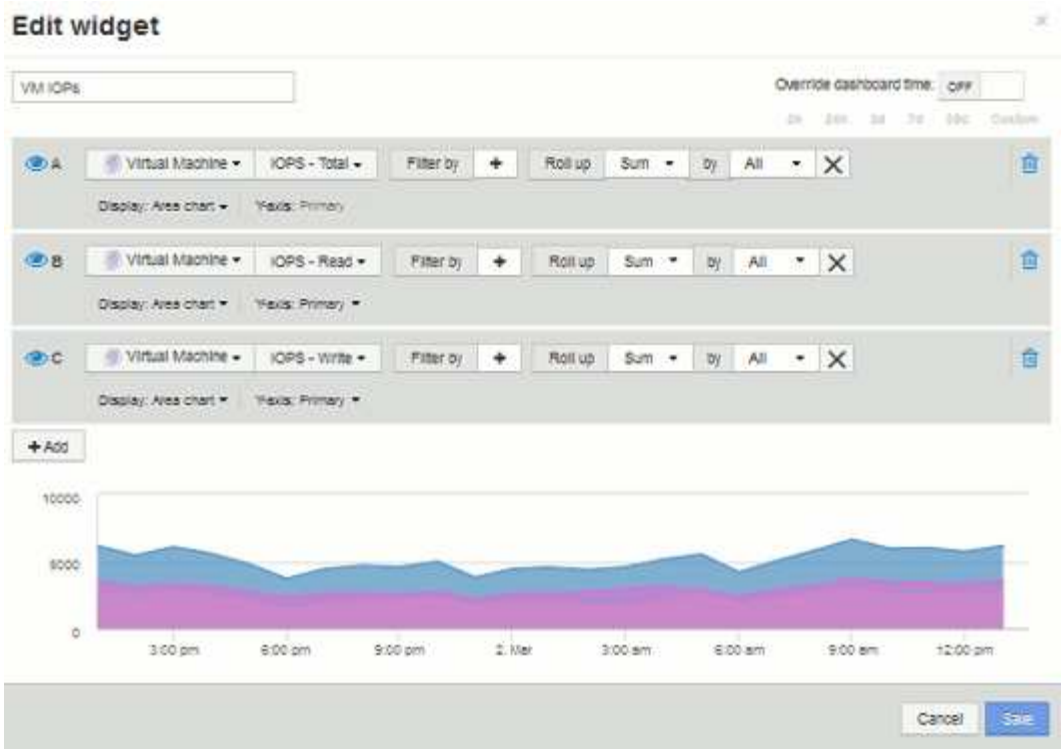
17. Selezionare **Virtual Machine** e scegliere **Latency - Max**. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere "Sum" da "all". Visualizzare questi dati come * Line Chart** e lasciare l'asse Y come **primario**.
18. Fare clic sul pulsante **+Aggiungi** per aggiungere una seconda riga di dati. Per questa riga, selezionare **Storage** e **Latency - Max**. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere "Sum" da "all". Visualizzare questi dati come * Line Chart** e lasciare l'asse Y come **primario**.



19. Fare clic su **Save** (Salva) per aggiungere questo widget alla dashboard.
20. Successivamente, aggiungeremo un grafico che mostra gli IOPS totali, di lettura e scrittura delle macchine virtuali in un singolo grafico.
21. Fare clic sul pulsante **Widget** e selezionare **Area Chart** per aggiungere un nuovo widget di area chart alla dashboard.

    Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Fare clic sul campo **Nome** e assegnare un nome al widget “VM IOPS”

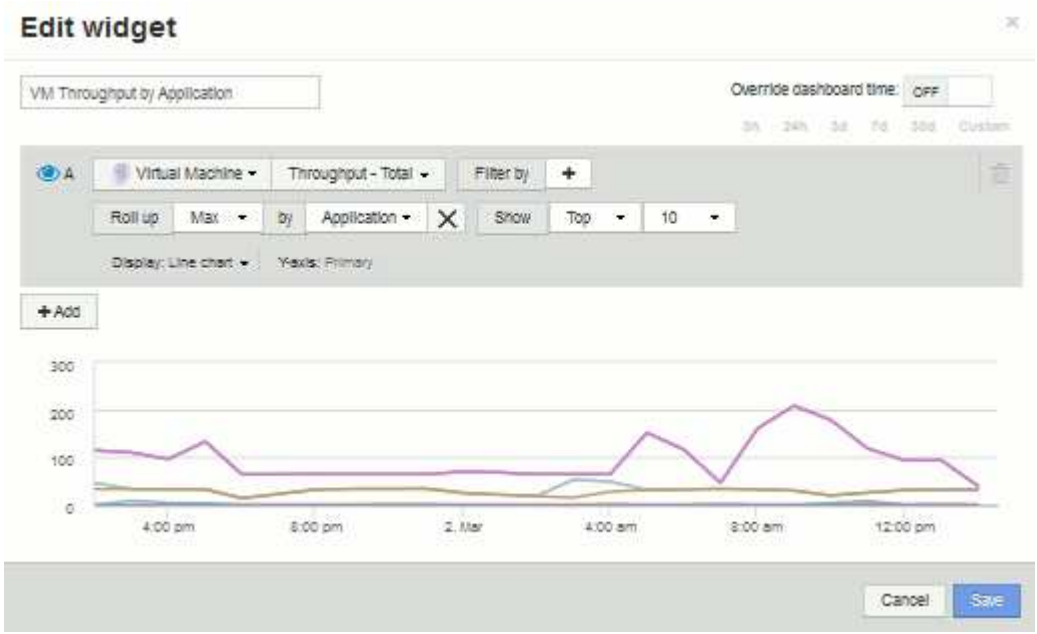
22. Selezionare **Virtual Machine** e scegliere **IOPS - Total**. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere “Sum” da “all”. Visualizzare questi dati come * grafico area** e lasciare l’asse Y come **primario**.
23. Fare clic sul pulsante +Add (Aggiungi) per aggiungere una seconda riga di dati. Per questa riga, selezionare **Virtual Machine** e scegliere **IOPS - Read**. Lasciare l’asse Y come **primario**.
24. Fare clic sul pulsante +Add (Aggiungi) per aggiungere una terza riga di dati. Per questa riga, selezionare **Virtual Machine** e scegliere **IOPS - Write**. Lasciare l’asse Y come **primario**.



25. Fare clic su **Save** (Salva) per aggiungere questo widget alla dashboard.
26. Quindi, aggiungeremo un grafico che mostra il throughput delle macchine virtuali per ciascuna applicazione associata alla macchina virtuale. A tale scopo, verrà utilizzata la funzione di rollio.
27. Fare clic sul pulsante **Widget** e selezionare **Line Chart** per aggiungere un nuovo widget grafico a linee alla dashboard.

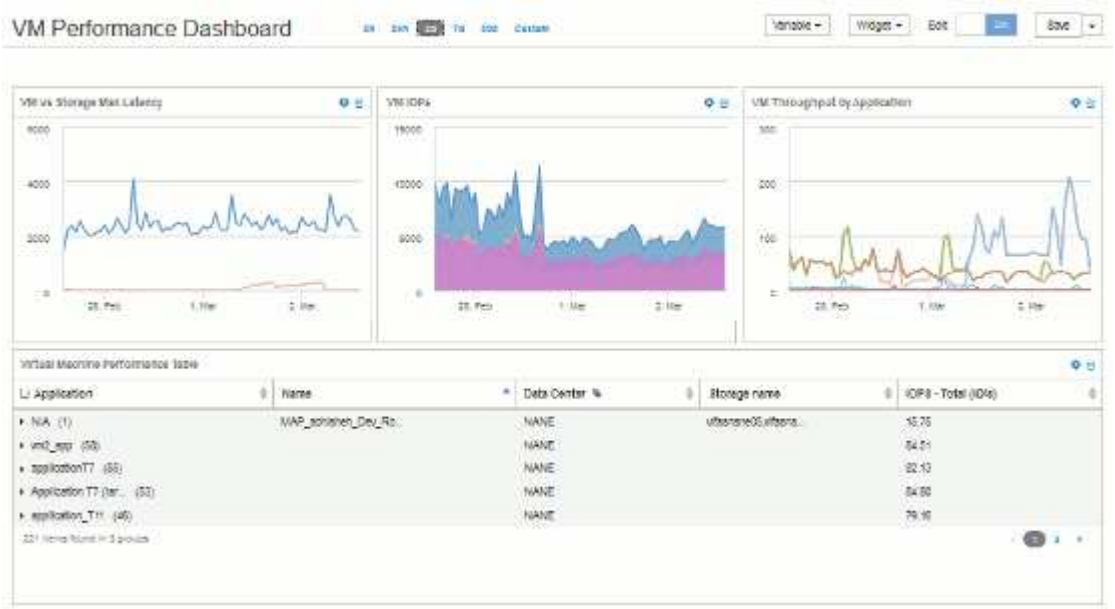
    Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Fare clic sul campo **Nome** e assegnare un nome a questo widget “VM throughput by Application”

28. Selezionare **Virtual Machine** e scegliere **throughput - Total**. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegli “MAX” e seleziona “Application” o “Name”. Mostra le applicazioni **Top 10**. Visualizzare questi dati come * Line Chart** e lasciare l’asse Y come **primario**.



29. Fare clic su **Save** (Salva) per aggiungere questo widget alla dashboard.
30. Puoi spostare i widget tenendo premuto il pulsante del mouse in un punto qualsiasi nella parte superiore del widget e trascinandoli in una nuova posizione. Puoi ridimensionare i widget trascinando l'angolo in basso a destra. Assicurarsi di **salvare** la dashboard dopo aver apportato le modifiche.

    La tua dashboard finale sulle performance delle macchine virtuali avrà un aspetto simile al seguente:



Esempio di dashboard di utilizzo del nodo di storage con variabili

Creare una dashboard personalizzata per l'analisi dello storage con variabili per storage, pool di storage, nodo, Tier, utilizzo e latenza.

Prima di iniziare

La familiarità con i dashboard di Insight è consigliata, ma non necessaria.

A proposito di questa attività

La seguente procedura consente di creare una dashboard panoramica di analisi dello storage personalizzata che utilizza le variabili per lo storage, il pool di storage, il nodo, il Tier, l'utilizzo e la latenza. Le variabili nell'esempio riportato di seguito verranno utilizzate per filtrare le risorse o le metriche visualizzate in uno o più widget disponibili nella dashboard. I widget che utilizzano queste variabili come filtri verranno aggiornati con contenuti filtrati on-demand in base ai valori immessi nei campi variabili della dashboard, consentendo di filtrare rapidamente più grafici e grafici per eseguire il drill-down di una specifica area di interesse.

Seguendo la procedura descritta in questo esempio, si crea una dashboard come quella riportata di seguito. È possibile modificare questi widget o aggiungere un numero qualsiasi di widget aggiuntivi per evidenziare i dati scelti.

Fasi

1. Creare una nuova dashboard e assegnarle il nome “Analysis: Storage Overview” (analisi: Panoramica dello storage), o qualcosa di altrettanto descrittivo.
2. Fare clic sull’elenco a discesa **Variable** (variabile) e selezionare **Text** variable type (tipo variabile **testo**). Per impostazione predefinita, la variabile è denominata *€var1*. Fare clic su _ var1_ per modificare il nome e impostarlo su _ storage_, quindi fare clic sul segno di spunta per salvare la variabile. Ripetere la procedura per creare variabili di testo per _ nodo_, _ pool_ e _ volume_.
3. Ripetere il processo sopra descritto per creare variabili di tipo **Number** denominate _ utilizzo_ e _ latenza_.
4. Fare clic sull’elenco a discesa **Variable** (variabile) e cercare l’annotazione *Tier*. Selezionare questa opzione per creare una variabile denominata _ Tier_.

   È possibile aggiungere variabili in qualsiasi momento, tuttavia è più semplice crearle in anticipo e renderle

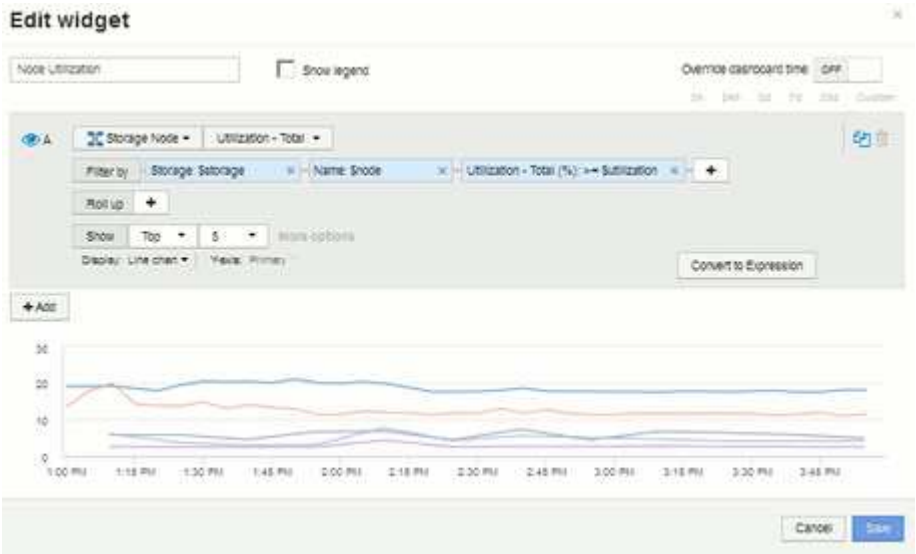
quindi disponibili a tutti i widget durante la creazione.

5. Aggiungere un widget facendo clic sull'elenco a discesa **Widget** e selezionando un widget **line chart**o **area chart**. Assegnare un nome al widget "Node Utilization". Fare clic sul tipo di risorsa **Storage** e modificarlo in **Storage Node**. Selezionare **Utilization - Total** (utilizzo - totale) per i dati del grafico.
6. Fare clic sul pulsante **Filtra per +** per aggiungere un filtro. Cercare e selezionare **Storage**, quindi fare clic su **Any** e selezionare la variabile _ storage_.
7. Fare clic sul pulsante**+**per aggiungere un altro filtro per **Nome**. Impostare la variabile su _ nodo_.

   È possibile assegnare variabili diverse al filtro dei nomi delle annotazioni. Utilizzare la coppia nome/variabile al livello più basso a seconda dell'oggetto nel widget. Ad esempio:

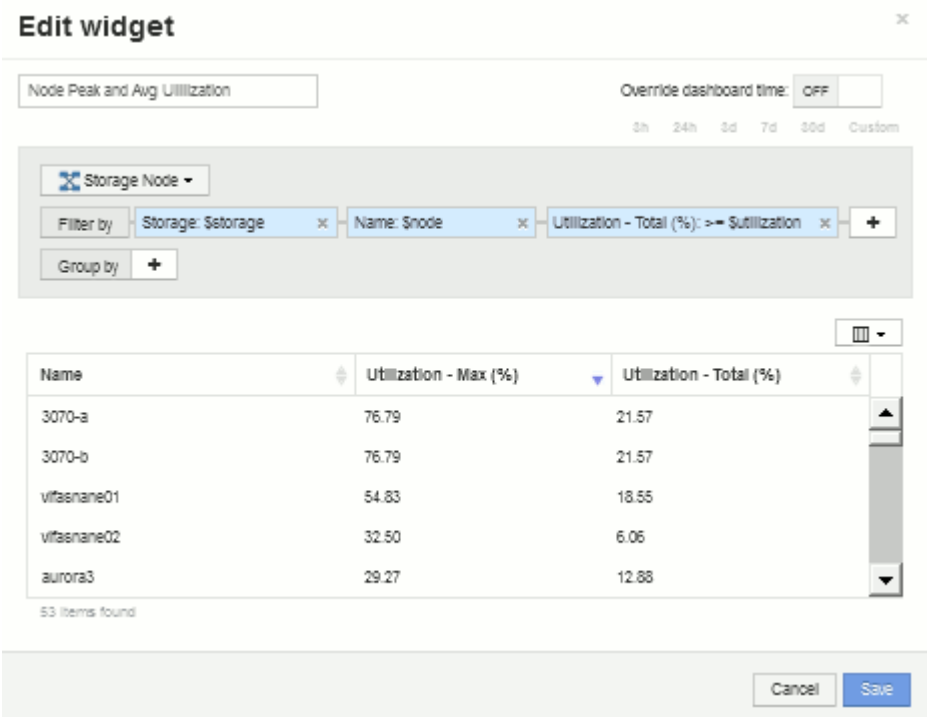
   - È possibile assegnare la variabile _ nodo_ al filtro **Nome** per un widget incentrato sul nodo.
   - È possibile assegnare la variabile _ pool_ al filtro **Name** per un widget Pool-Focused.
8. Fare clic sul pulsante**+**per aggiungere un altro filtro per **Utilization - Total (%)**. Impostare la variabile su >= *utilizzo* dollari.
9. Fare clic su **X** dopo il campo**Roll-up** per comprimere il campo.
10. Selezionare **Mostra i primi 5** e fare clic su **Salva** per salvare il widget e tornare alla dashboard.

    Il widget dovrebbe avere un aspetto simile al seguente:



11. Aggiungi un altro widget grafico a linee o aree alla dashboard. Selezionare **Storage Node** come tipo di risorsa e **Latency - Total** come metrica da inserire nel grafico.
12. Fare clic sul pulsante **Filtra per +** per aggiungere i filtri per **Storage: €storage** e **Name: €node**.
13. Aggiungi un filtro per **latenza - totale** e seleziona la variabile * latenza*.
14. Assegnare un nome al widget "Node Latency" e salvarlo.
15. È possibile aggiungere tabelle di supporto per visualizzare ulteriori dettagli per i grafici creati, ad esempio, utilizzo massimo o medio dei nodi. Aggiungere un widget **Table** alla dashboard e selezionare **Storage Node** come tipo di risorsa, quindi creare filtri per **Storage: Storage in dollari**, **Name: Nodo in dollari** e **Utilization - Total: Utilizzo in dollari**.
16. Aggiungere colonne alla tabella per **Utilization - Max**, **Utilization - Total** o qualsiasi altra colonna desiderata.

17. Assegnare un nome al widget “Node Peak and Avg Utilization” e salvarlo.

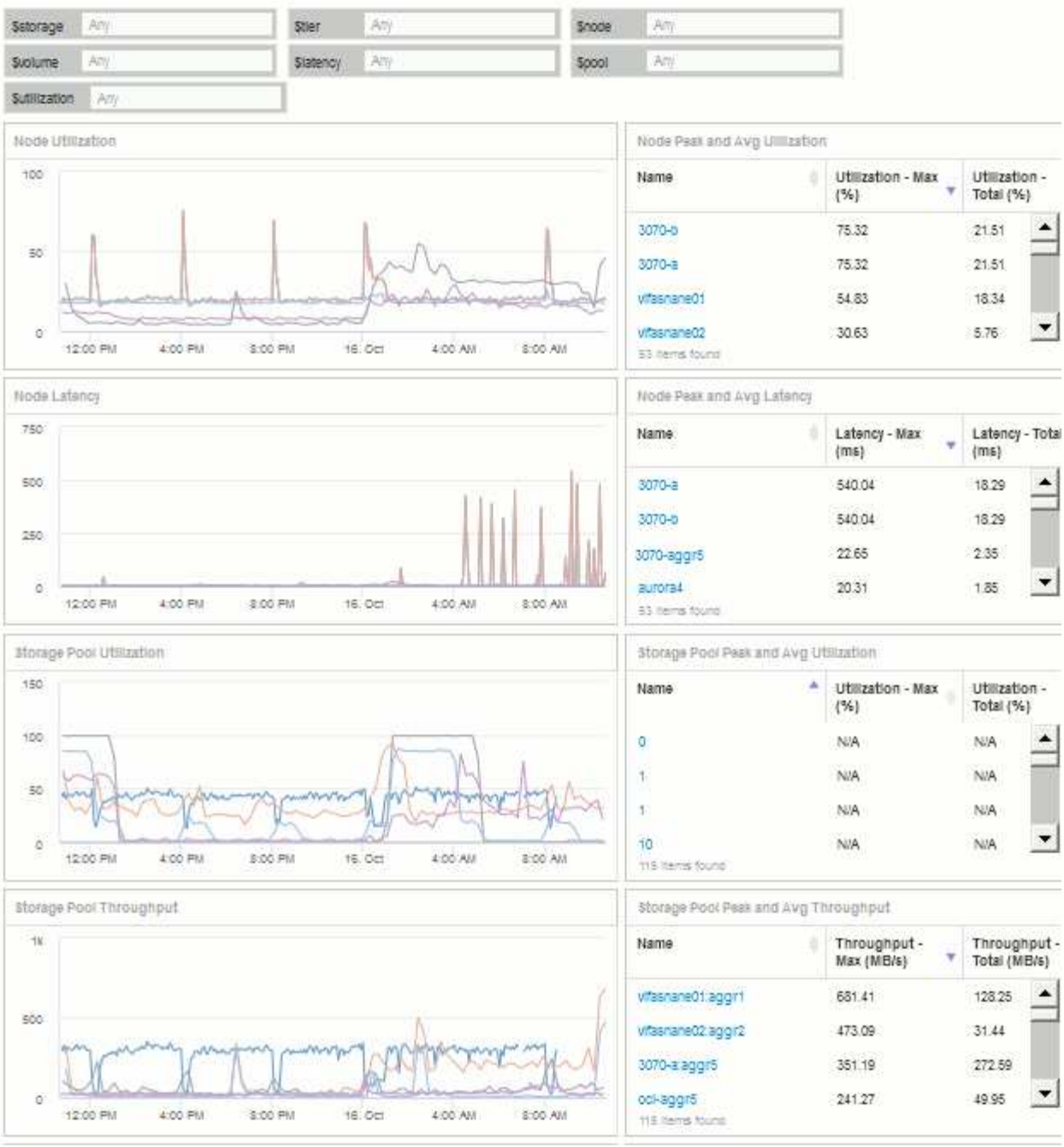


18. Ripetere i passaggi per creare una tabella per la latenza del nodo, che mostra **latenza - Max**, **latenza - totale** o altre colonne come desiderato.
19. Per completare la dashboard, è possibile aggiungere ulteriori widget di tabella e grafico per alcuni o tutti i seguenti elementi:

Grafico	Tabella
Utilizzo del pool di storage	Utilizzo medio e massimo del pool di storage
Throughput del pool di storage	Throughput medio e picco del pool di storage
Latenza del volume	Volume Peak e latenza media
IOPS del volume	Volume Peak (picco volume) e AVG IOPS (IOPS medio

1. Puoi spostare e ridimensionare i widget in qualsiasi posizione sulla dashboard. Al termine, assicurarsi di **salvare** la dashboard.

   La tua dashboard finale avrà un aspetto simile al seguente:



2. È possibile utilizzare le variabili per concentrarsi su risorse specifiche nella dashboard. Quando si immettono valori nei campi variabili, i widget vengono aggiornati automaticamente per riflettere tali variabili. Ad esempio, inserendo “15” nel campo della variabile di utilizzo dei dollari, i widget che utilizzano tale variabile vengono aggiornati per visualizzare solo le risorse con un utilizzo totale >= 15%.

   Widget di utilizzo del nodo che mostra i primi 5 di tutti i nodi:

Widget di utilizzo dei nodi che mostra i nodi con un utilizzo pari o superiore al 15%:

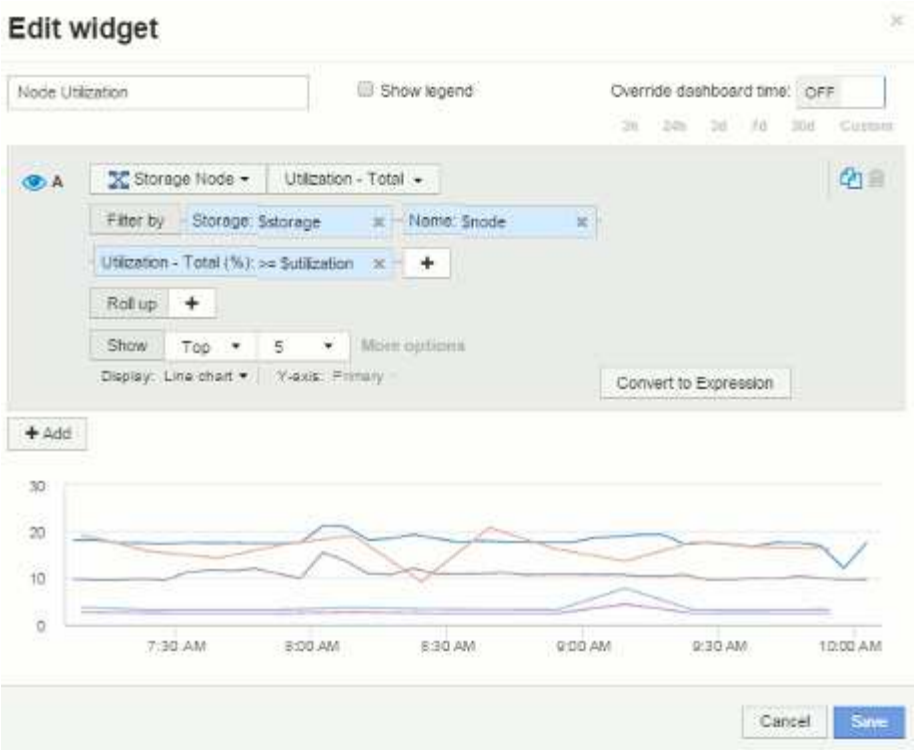
3. Durante la creazione dei widget, tenere presente quanto segue:
   - La variabile del Tier di dollari avrà un impatto solo sulle risorse annotate con l'annotazione **Tier**.
   - Non tutti i filtri influiscono su tutti i widget, a seconda che il widget sia progettato per accettare le variabili specificate.
   - Le variabili numeriche vengono applicate come "maggiore o uguale a" il valore specificato. Si noti che qualsiasi variabile può essere utilizzata come filtro su qualsiasi widget a qualsiasi livello di una gerarchia di storage, purché la variabile sia valida per la risorsa in base alla quale il widget è in esecuzione. Man mano che si passa da un livello di nodo a un pool di storage a un widget di volume, sono presenti più variabili da assegnare come filtri. Ad esempio, in un widget a livello di nodo di storage, le variabili *Storage* e *Name* possono essere assegnate come filtri. A livello di Storage Pool, sono disponibili *Storage*, *Node*, *Storage Pool* e *Name*. Assegnare le variabili in base alle esigenze e utilizzare la variabile del nome del dollaro al livello più basso dello stack. In questo modo, la variabile del tuo nome sarà in grado di filtrare il nome effettivo della risorsa in base alla quale il widget è in esecuzione.

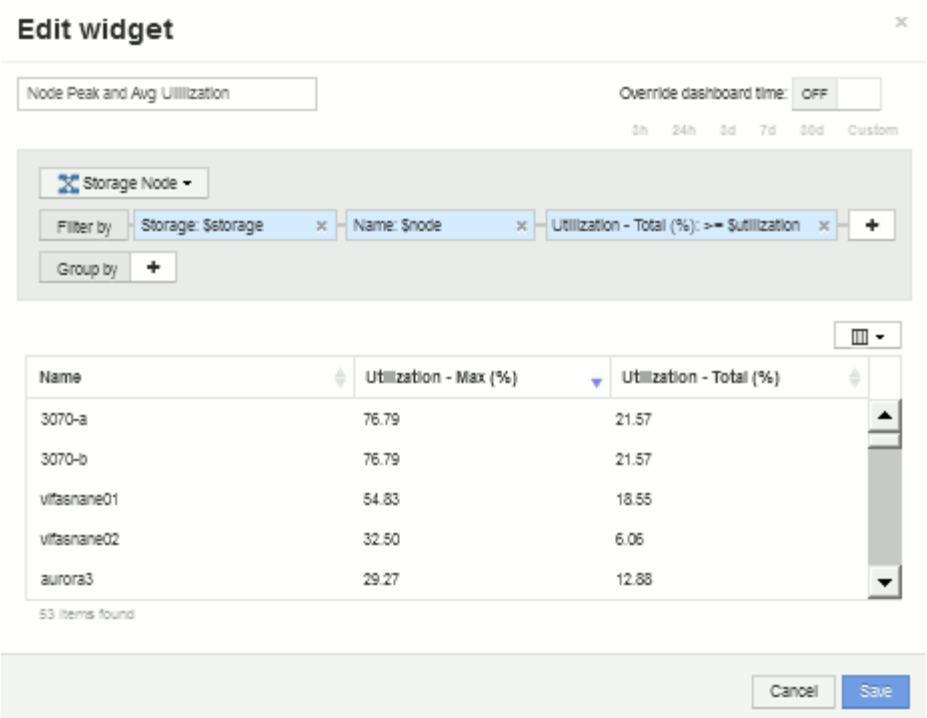
Esempio di dashboard del nodo impostazioni widget

Esempio di impostazioni widget per la dashboard dei nodi con variabili.

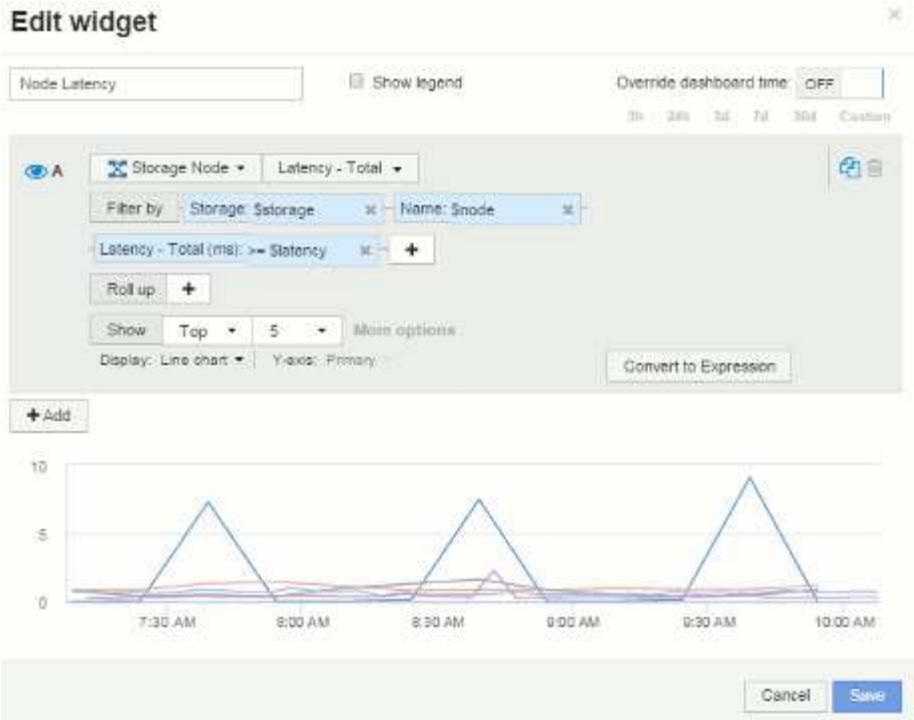
Di seguito sono riportate le impostazioni per ciascuno dei widget nell'esempio della dashboard del nodo di storage.

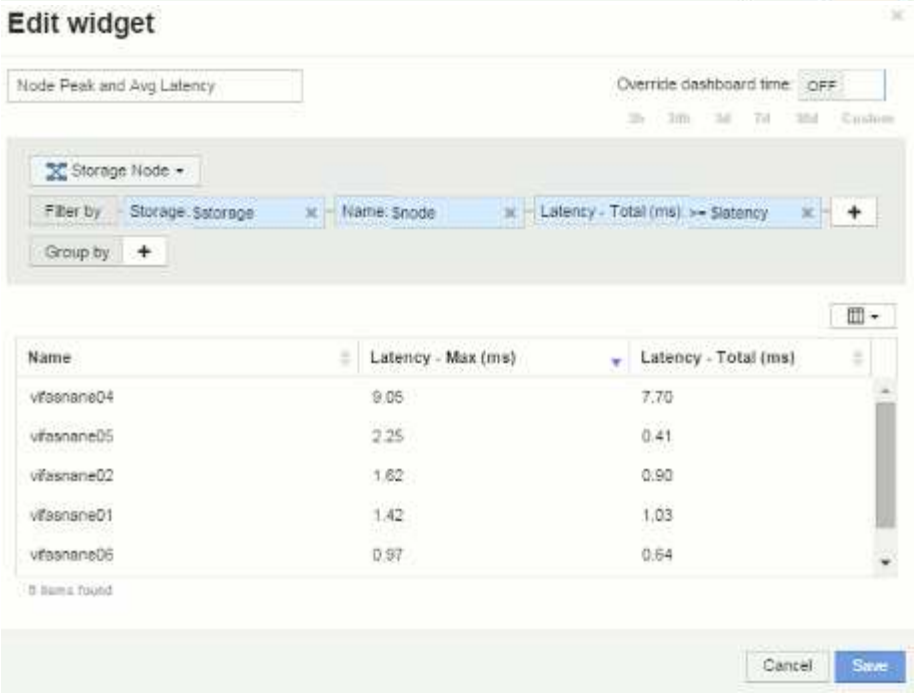
Utilizzo del nodo:



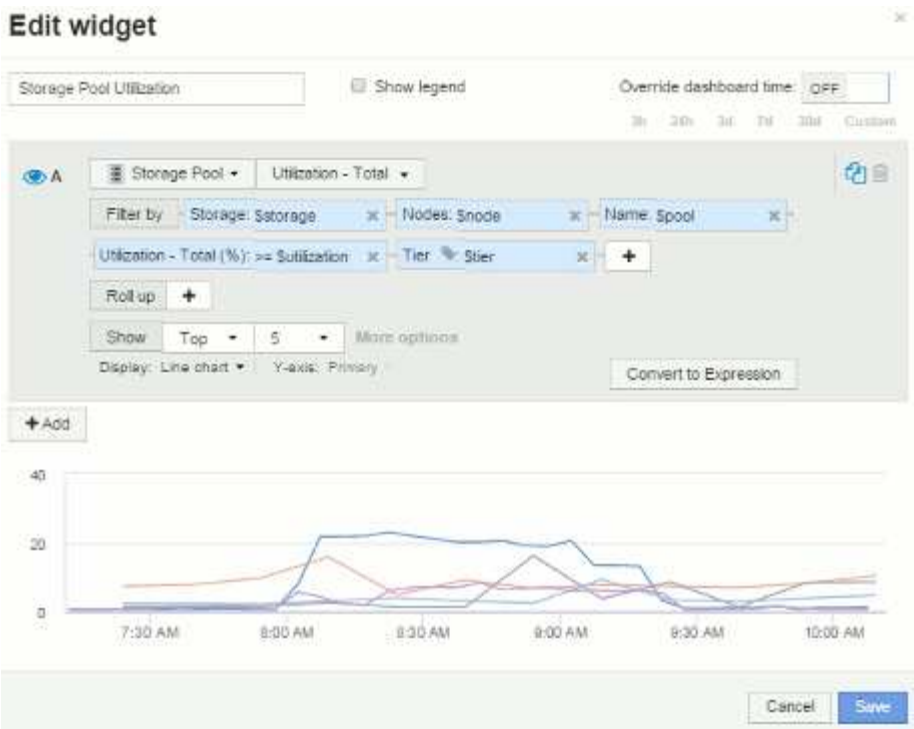


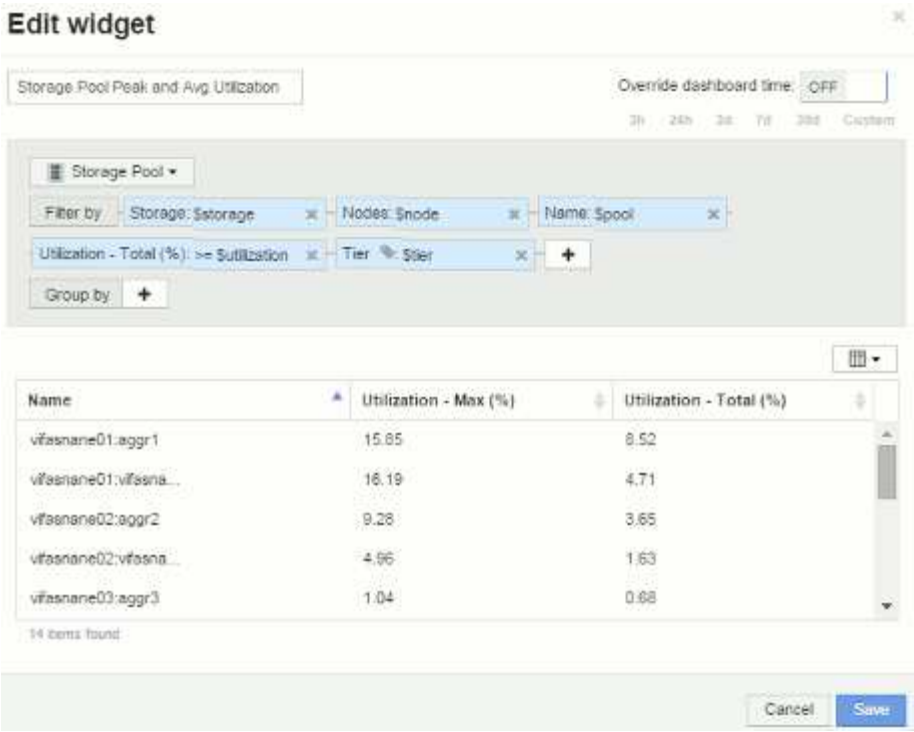
Latenza del nodo:



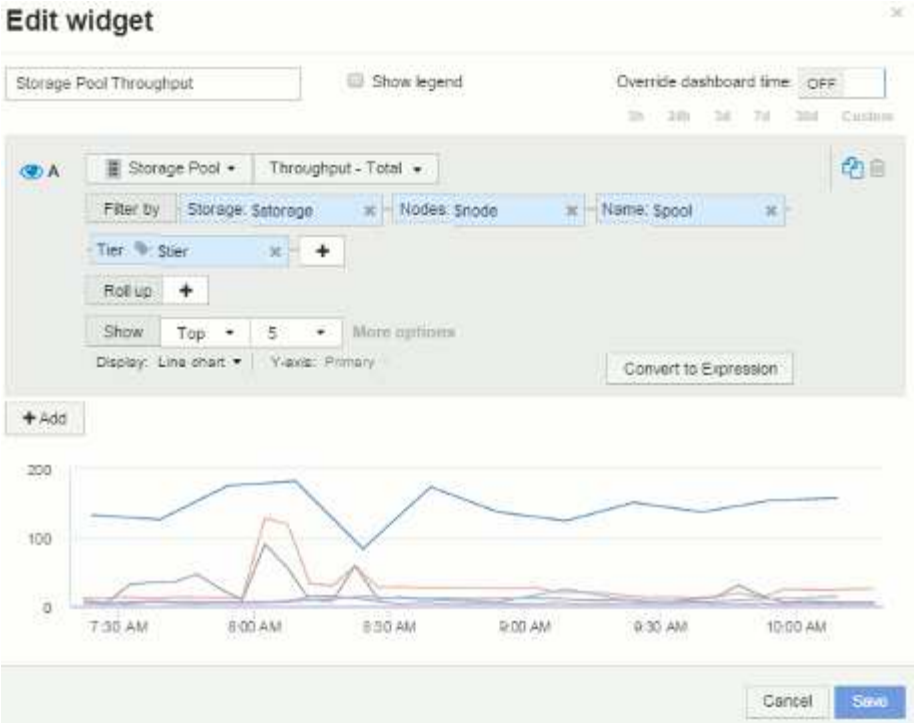


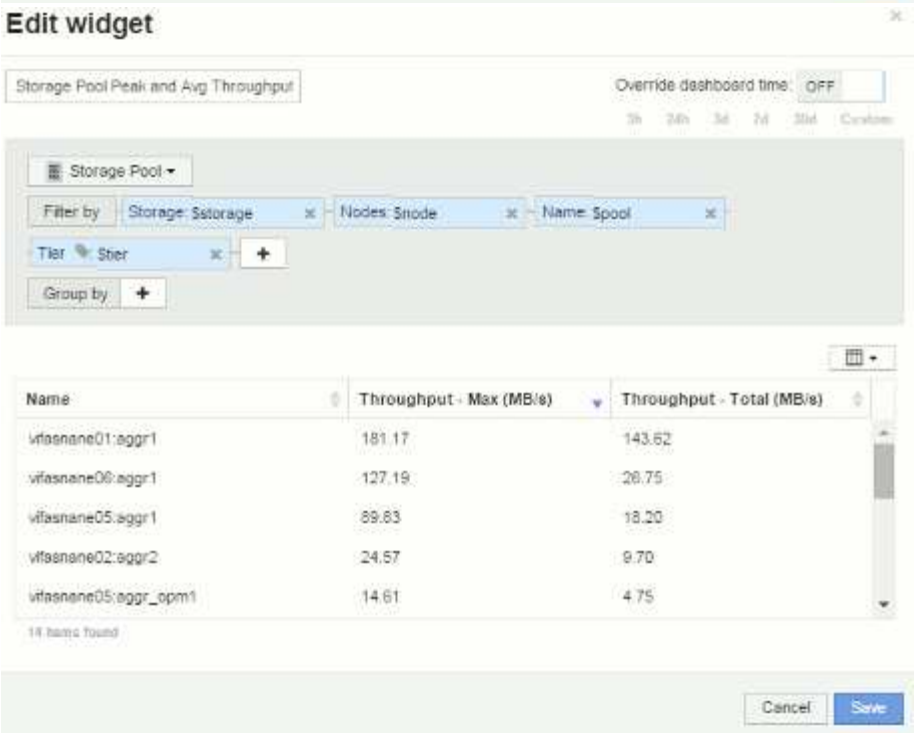
Utilizzo del pool di storage:



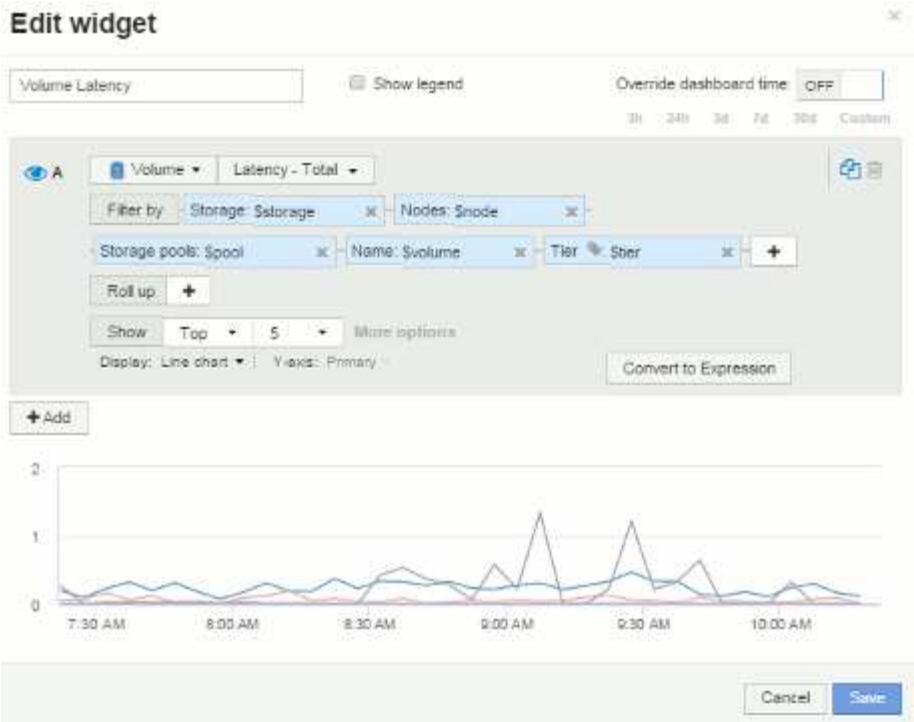


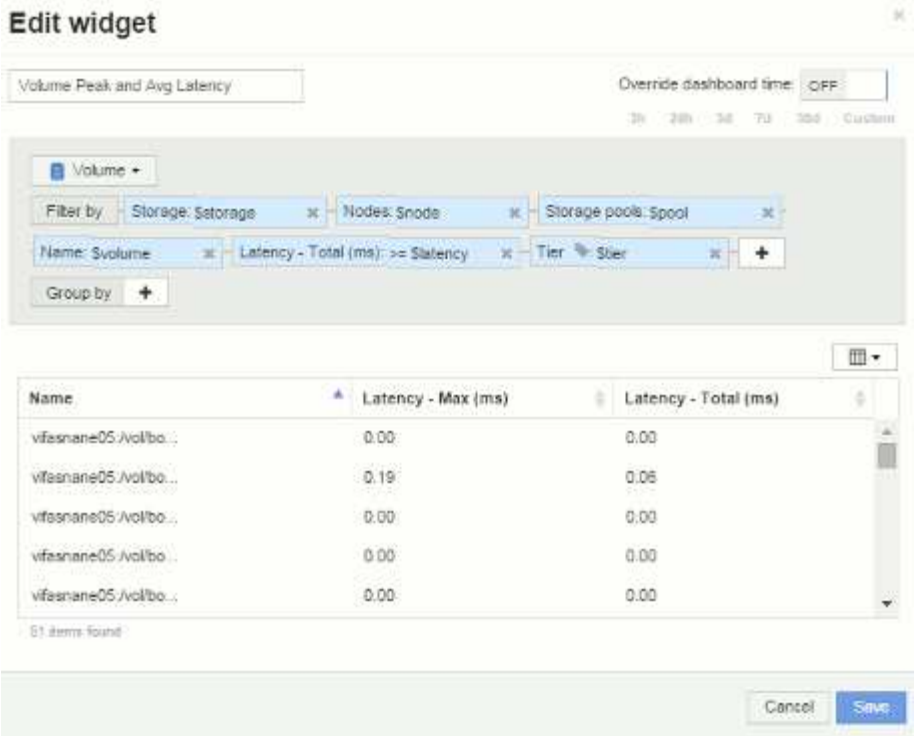
Throughput del pool di storage:



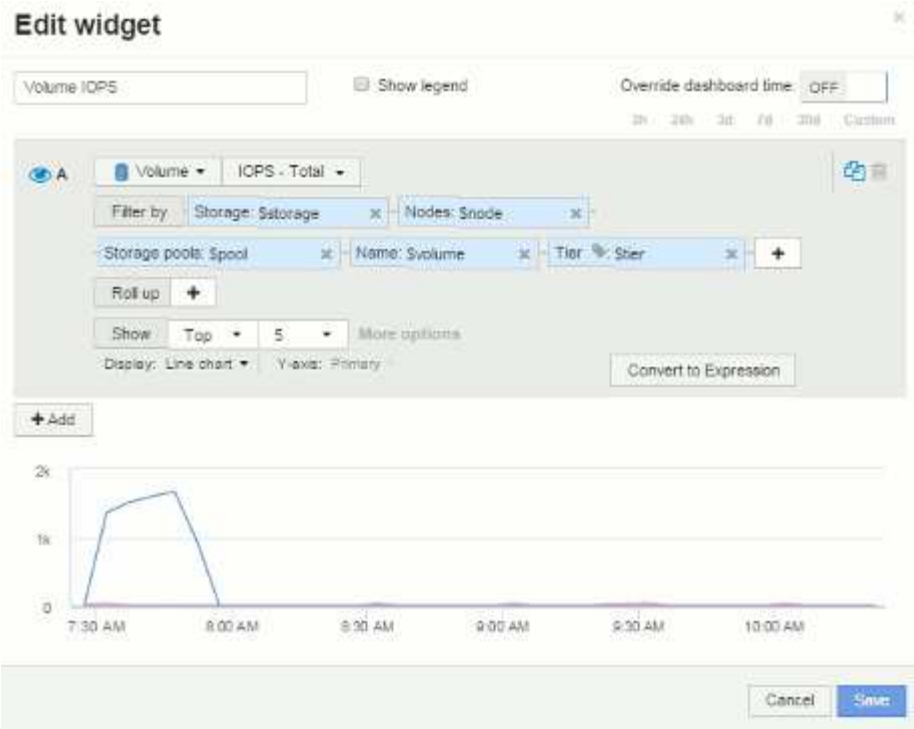


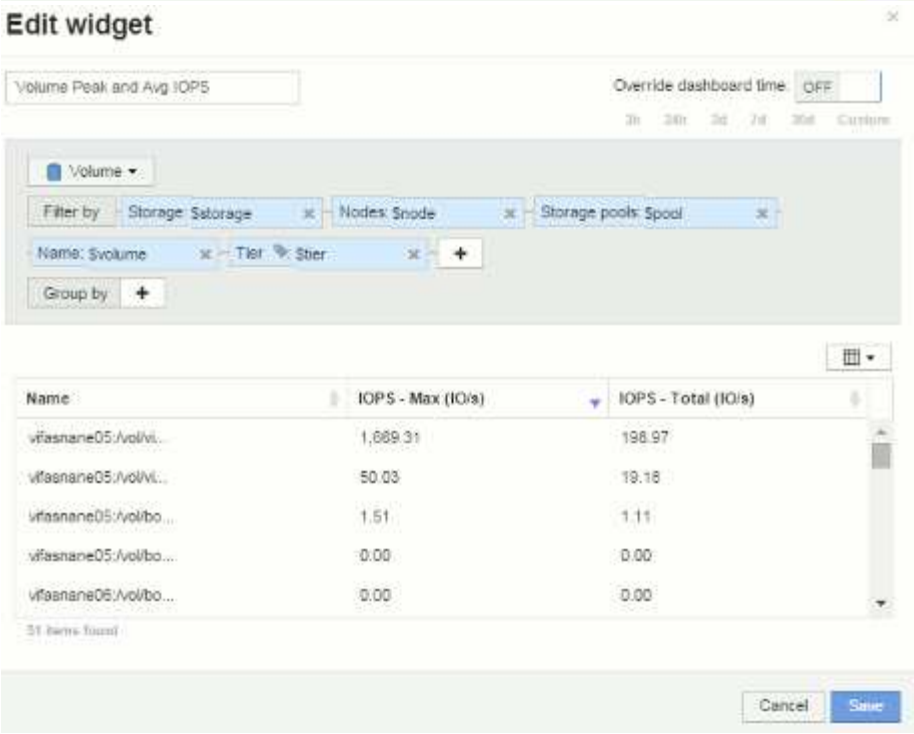
Latenza del volume:





IOPS del volume:





Best practice per dashboard e widget

Suggerimenti e trucchi per ottenere il massimo dalle potenti funzionalità di dashboard e widget.

Best practice: Trovare la metrica giusta

OnCommand Insight acquisisce contatori e metriche utilizzando nomi che a volte differiscono dall'origine dei dati all'origine dei dati.

Quando si cerca la metrica o il contatore corretto per il widget dashboard, tenere presente che la metrica desiderata potrebbe essere sotto un nome diverso da quello a cui si sta pensando. Anche se gli elenchi a discesa in OnCommand Insight sono generalmente in ordine alfabetico, a volte un termine potrebbe non essere visualizzato nell'elenco in cui si ritiene opportuno. Ad esempio, termini come "capacità raw" e "capacità utilizzata" non vengono visualizzati insieme nella maggior parte degli elenchi.

Procedura consigliata: Utilizzare la funzione di ricerca in campi come **Filtra per** o posizioni come il selettore di colonna per trovare ciò che stai cercando. Ad esempio, la ricerca di "CAP" mostrerà tutte le metriche con "capacità" nei loro nomi, indipendentemente da dove si verifica. È quindi possibile selezionare facilmente le metriche desiderate dall'elenco breve.

Ecco alcune frasi alternative che puoi provare quando cerchi le metriche:

Quando si desidera trovare:	Prova anche a cercare:
CPU	Del processore
Capacità	Capacità utilizzata capacità raw Capacità fornita Capacità dei pool di storage capacità <other asset type> Capacità scritta
Velocità del disco	Velocità minima del disco tipo di disco con prestazioni inferiori
Host	HypervisorHost
Hypervisor	Hypervisor ostis
Microcodice	Firmware
Nome	Nome AliasHypervisor Nome dello storage nome <other asset type> Nome semplice Nome della risorsa Alias fabric

Lettura/scrittura	Scritture R/WPending parziali IOPS - scrittura Capacità scritta Latenza - lettura Utilizzo della cache - lettura
Macchina virtuale	VMIS virtuale

Non si tratta di un elenco completo. Questi sono solo esempi di possibili termini di ricerca.

Best practice: Trovare le risorse giuste

Le risorse Insight a cui puoi fare riferimento nei filtri e nelle ricerche dei widget variano a seconda del tipo di risorsa.

Nei dashboard, il tipo di risorsa intorno al quale si sta creando il widget determina gli altri contatori dei tipi di risorsa per i quali è possibile filtrare o aggiungere una colonna. Quando si crea il widget, tenere presente quanto segue:

Questo tipo di risorsa/contatore:	Può essere filtrato per sotto queste risorse:
Macchina virtuale	VMDK
Datastore	VolumeVMDK interno Macchina virtuale Volume
Hypervisor	Macchina virtuale
È un hypervisor	Host
Host	Volume volumeinterno
Cluster	Macchina virtuale host
Fabric	Porta

Non si tratta di un elenco completo.

Procedura consigliata: Se si esegue il filtraggio per un determinato tipo di risorsa che non compare nell'elenco, provare a creare la query intorno a un tipo di risorsa alternativo.

Esempio di diagramma di dispersione: Conoscere l'asse

La modifica dell'ordine dei contatori in un widget di scatterplot modifica gli assi su cui vengono visualizzati i dati.

A proposito di questa attività

In questo esempio viene creato un grafico di dispersione che consente di visualizzare macchine virtuali con performance inferiori e latenza elevata rispetto a IOPS bassi.

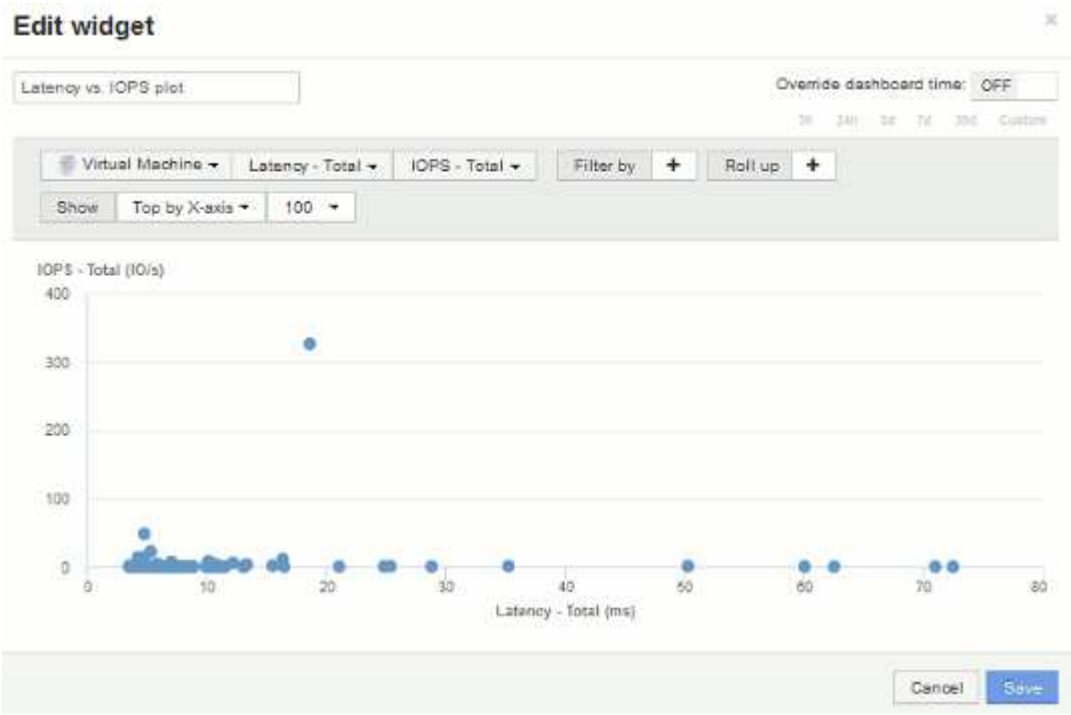
Fasi

1. Creare o aprire una dashboard in modalità di modifica e aggiungere un widget **grafico a dispersione**.
2. Selezionare un tipo di risorsa, ad esempio **Virtual Machine**.
3. Selezionare il primo contatore che si desidera tracciare. Per questo esempio, selezionare **latenza - totale**.

   Latenza - totale viene indicato lungo l'asse X del grafico.

4. Selezionare il secondo contatore che si desidera tracciare. Per questo esempio, selezionare **IOPS - Total**.

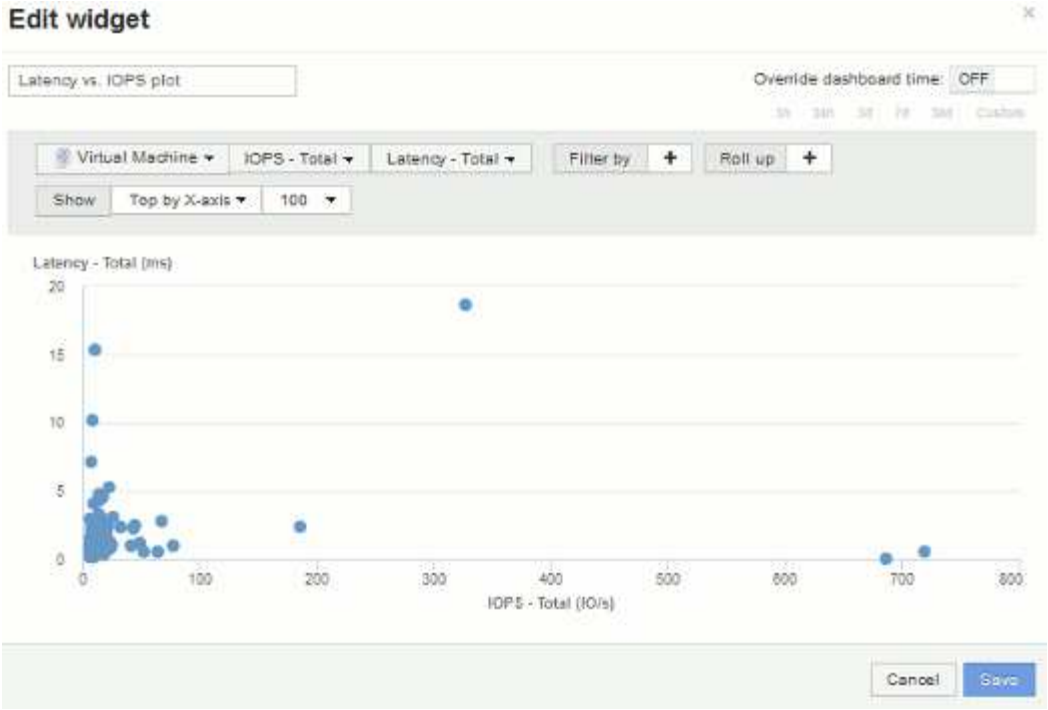
   IOPS - Total viene indicato lungo l'asse Y nel grafico. Le macchine virtuali con latenza superiore vengono visualizzate sul lato destro del grafico. Vengono visualizzate solo le prime 100 macchine virtuali con la latenza più elevata, poiché l'impostazione **inizio per asse X** è corrente.



5. Invertire l'ordine dei contatori impostando il primo contatore su **IOPS - Total** e il secondo su **Latency - Total**.

   latency- Total viene ora tracciato lungo l'asse Y nel grafico e*IOPS - Tota*l lungo l'asse X. Le macchine virtuali con IOPS superiori vengono ora visualizzate sul lato destro del grafico.

   Nota: Poiché non abbiamo modificato l'impostazione **Top by X-axis**, il widget ora visualizza le prime 100 macchine virtuali IOPS più alte, poiché questo è ciò che viene attualmente tracciato lungo l'asse X.



6. È possibile scegliere se visualizzare il grafico in alto N per asse X, in alto N per asse Y, in basso N per asse X o in basso N per asse Y. Nell'esempio finale, il grafico mostra le prime 100 macchine virtuali con il massimo *IOPS totale*. Se la si modifica in Top by Y-axis, il grafico visualizza nuovamente le prime 100 macchine virtuali con la massima *latenza totale*.

   Si noti che in un grafico a dispersione, è possibile fare clic su un punto per aprire la pagina delle risorse per tale risorsa.

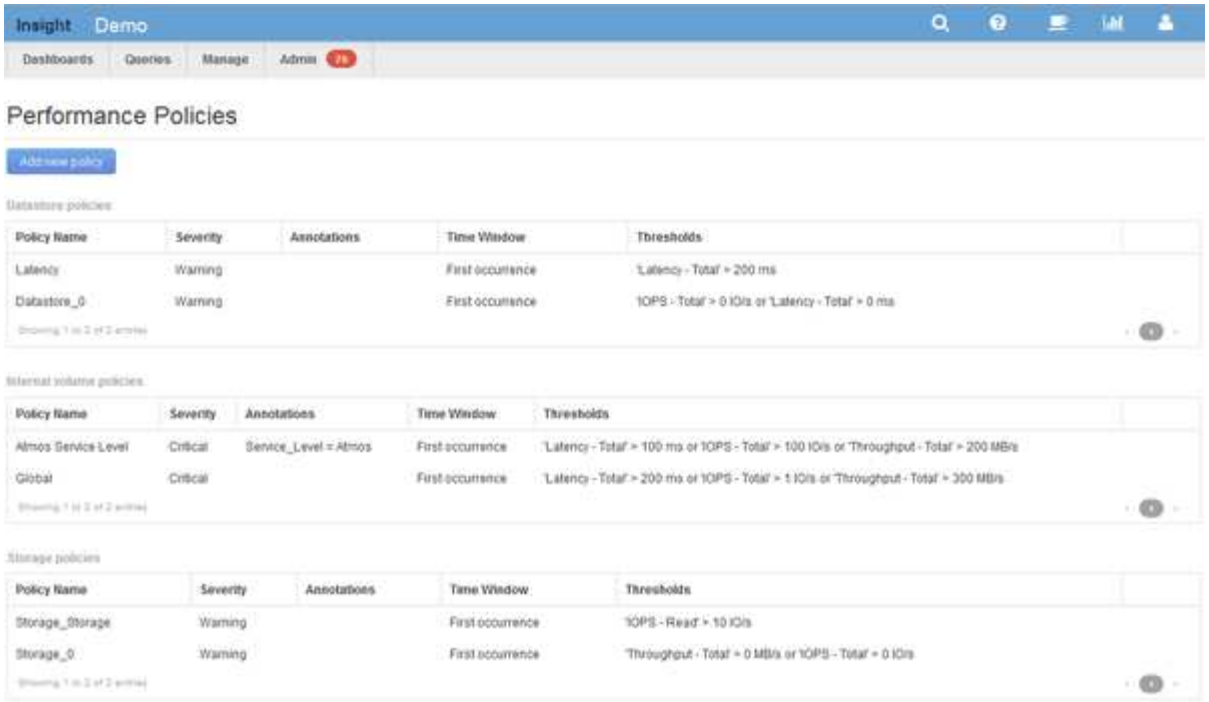
Creazione di policy sulle performance

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.

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).

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.

Risoluzione dei problemi relativi agli errori di credito BB Fibre Channel 0

Fibre Channel utilizza crediti da buffer a buffer (crediti BB) per controllare il flusso di trasmissione. Il valore del credito viene decrementato quando un frame viene inviato da una porta e il valore del credito viene reintegro quando la porta riceve una risposta. Se i crediti BB nella porta non vengono riforniti, il flusso di trasmissione potrebbe risentire. Le porte necessitano di memoria o buffer per memorizzare temporaneamente i frame fino a quando non vengono assemblati in sequenza e consegnati. Il numero di buffer è il numero di frame che una porta può memorizzare ed è chiamato credito buffer.

Poiché i crediti disponibili per una data porta si avvicinano a zero, un errore avverte che la porta interromperà la ricezione delle trasmissioni quando viene raggiunto lo zero e non riprenderà fino a quando i crediti BB non saranno riforniti.

Le policy sulle performance di Insight consentono di impostare le soglie sulle seguenti metriche delle porte.

Credito BB zero - Rx
Numero di volte in cui il conteggio del credito buffer-to-buffer di ricezione è passato a zero durante il periodo di campionamento
Credito BB zero - Tx
Numero di volte in cui il conteggio del credito buffer-to-buffer di trasmissione è passato a zero durante il periodo di campionamento

Credito BB zero - totale	
Numero di volte in cui questa porta ha dovuto interrompere la trasmissione perché la porta collegata non aveva crediti da fornire	
Durata zero credito BB - Tx	
Tempo in millisecondi durante il quale il credito Tx BB è stato pari a zero durante l'intervallo di campionamento	

Gli errori di credito BB potrebbero essere causati da alcuni dei seguenti scenari:

- Se una data implementazione ha una percentuale elevata di frame FC di dimensioni significativamente inferiori alla dimensione massima, potrebbe essere necessario un numero maggiore di BB_Credits.
- Modifiche dei carichi di lavoro nell'ambiente che potrebbero influire sulle porte o sui dispositivi connessi, ad esempio i nodi di storage.

È possibile utilizzare le pagine delle risorse relative a fabric, switch e porte per monitorare l'ambiente Fibre Channel. Le pagine delle risorse delle porte contengono informazioni riepilogative sulla risorsa, sulla sua topologia (il dispositivo e le sue connessioni), sui grafici delle performance e sulle tabelle delle risorse associate. Durante la risoluzione dei problemi relativi a Fibre Channel, il grafico delle performance per ogni risorsa porta è utile perché mostra il traffico per la porta principale contributore selezionata. Le pagine delle risorse delle porte mostrano anche le metriche di credito buffer-to-buffer e gli errori delle porte in questo grafico, con Insight che visualizza un grafico delle performance separato per ciascuna metrica.

Creazione di policy e soglie di performance per le porte

È possibile creare policy sulle performance con soglie per le metriche associate a una porta. Per impostazione predefinita, i criteri relativi alle performance si applicano a tutti i dispositivi del tipo specificato quando vengono creati. È possibile creare un'annotazione per includere solo un dispositivo specifico o una serie di dispositivi nella policy delle performance. Per semplicità, in questa procedura non viene utilizzata un'annotazione.

Prima di iniziare

Se si desidera utilizzare un'annotazione con questo criterio di performance, è necessario creare l'annotazione prima di creare il criterio di performance.

Fasi

1. Dalla barra degli strumenti di Insight, fare clic su **Gestisci** > **Criteri di performance**

   Vengono visualizzati i criteri esistenti. Se esiste un criterio per le porte dello switch, è possibile modificare il criterio esistente, aggiungendo nuovi criteri e soglie.

2. Modificare un criterio di porta esistente o creare un nuovo criterio di porta

   - Fare clic sull'icona a forma di matita all'estrema destra della policy esistente. Aggiungere le soglie descritte nei passaggi "d" e "e".
   - Fare clic su **+Aggiungi** per aggiungere una nuova policy

i. Aggiungere un “Policy Name”: Slow drain device
ii. Selezionare porta come tipo di oggetto
iii. Inserire la prima occorrenza per “Apply after window” di
iv. Inserire la soglia: BB credit zero - Rx > 1,000,000
v. Inserire la soglia: BB credit zero - Tx > 1,000,000
vi. Fare clic su “Stop processing further policies if alert is generated” (top elaborazione di ulteriori policy
vii. Fai clic su “Save”

Il criterio creato monitora le soglie impostate in un periodo di 24 ore. Se la soglia viene superata, viene segnalata una violazione.

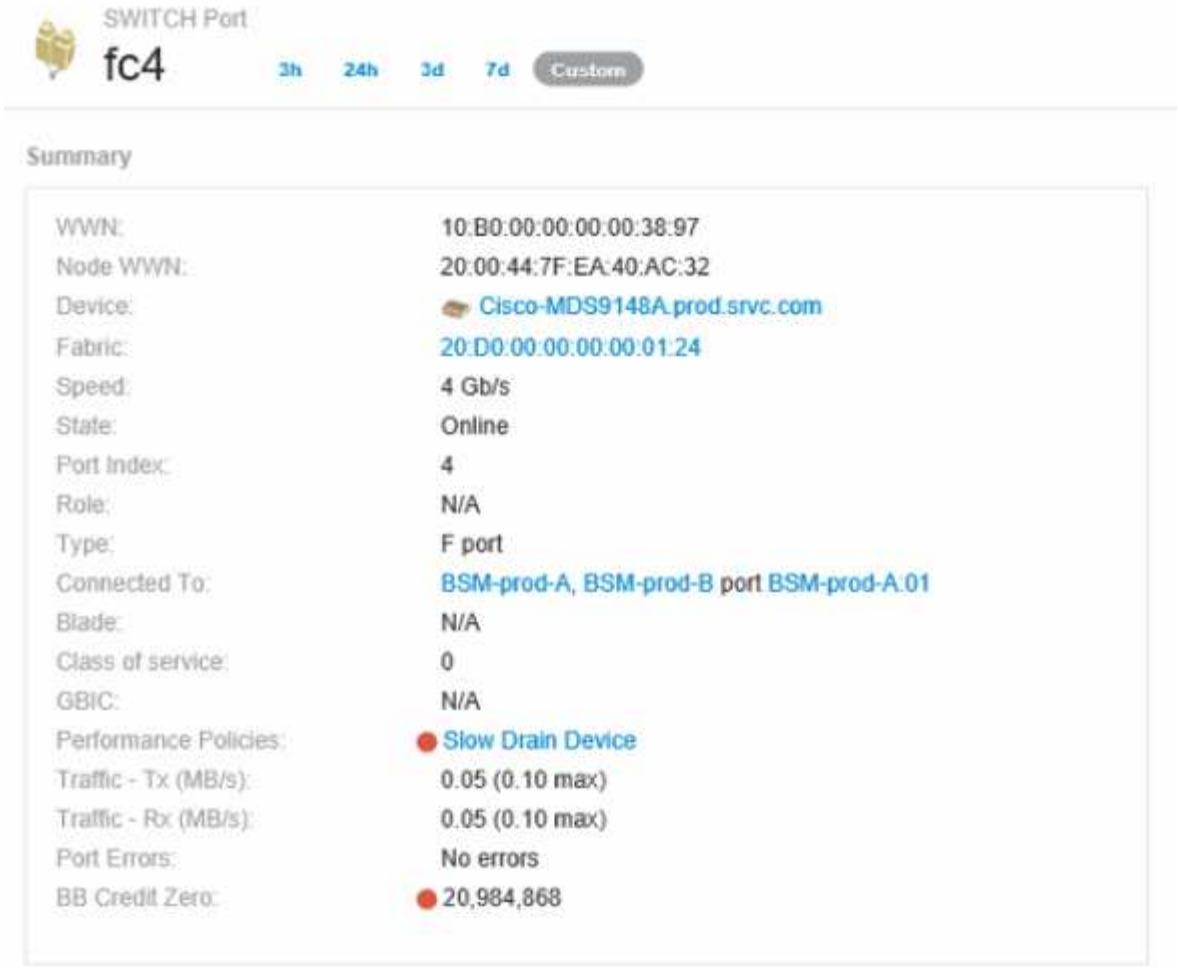
3. Fare clic su **Dashboard** > **dashboard violazioni**

   Il sistema visualizza tutte le violazioni che si sono verificate nel sistema. Cercare o ordinare le violazioni per visualizzare le violazioni “Slow drain device”. La dashboard delle violazioni mostra tutte le porte che hanno riscontrato errori di credito BB 0 che superano le soglie impostate nella policy sulle performance. Ciascuna porta dello switch identificata nella dashboard violazioni è un link evidenziato alla pagina iniziale della porta.

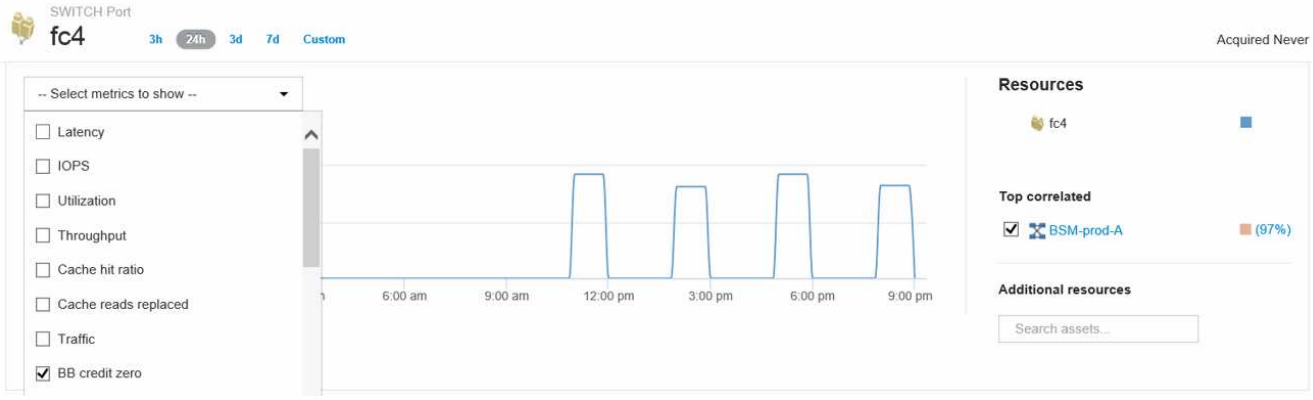
4. Fare clic su un collegamento di porta evidenziato per visualizzare la pagina di destinazione della porta.

   Viene visualizzata la landing page della porta che include informazioni utili per la risoluzione dei problemi relativi al credito BB 0:

   - Dispositivi a cui è collegata la porta
   - Identificazione della porta che segnala la violazione, che è una porta Fibre Channel Switch.
   - La velocità della porta
   - Il nodo e il nome della porta associati



5. Scorrere verso il basso per visualizzare le metriche delle porte. Fare clic su **Select metrics to show** > **BB credit zero** (Seleziona metriche da visualizzare) per visualizzare il grafico del credito BB.



6. Fare clic su **Top Correlated**

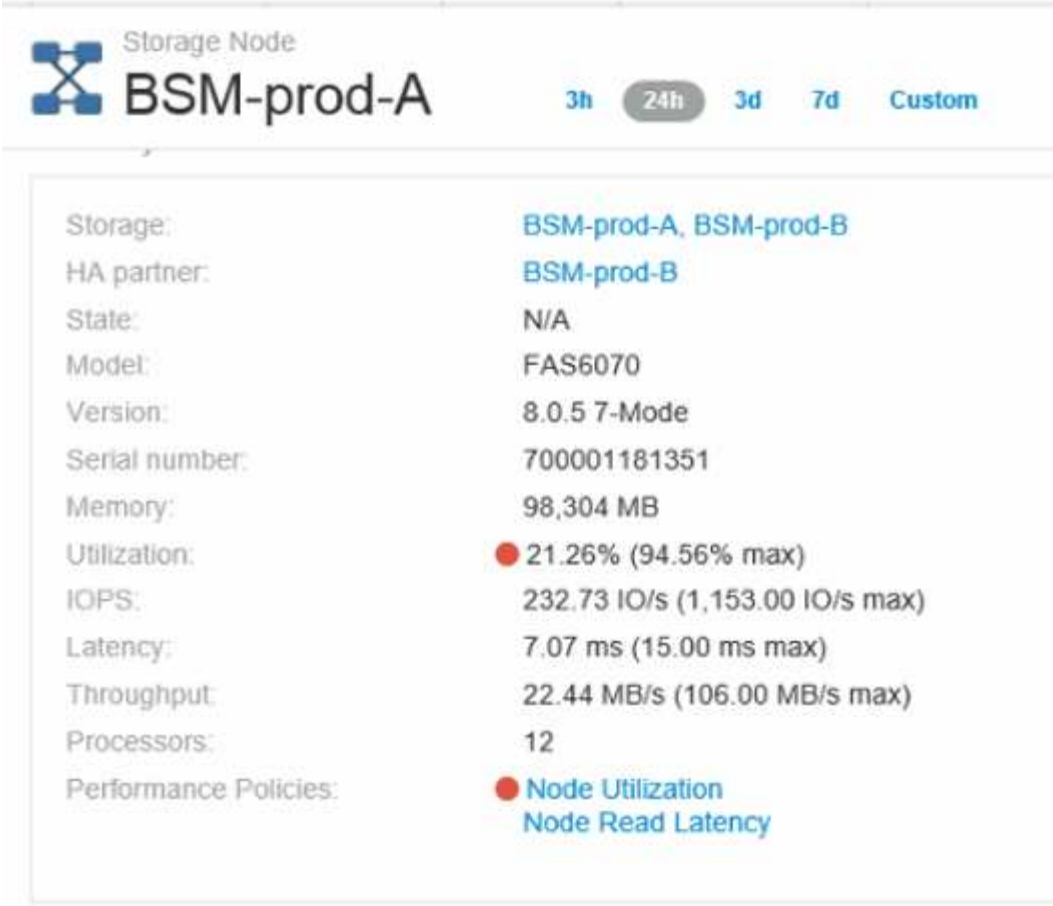
   L'analisi delle risorse correlate in alto mostra il nodo del controller connesso che la porta sta servendo come risorsa più correlata alle performance. Questa fase confronta le metriche IOPS dell'attività della porta con l'attività complessiva del nodo. Il display mostra le metriche di azzeramento del credito Tx e Rx BB e gli IOPS del nodo del controller. Sul display viene visualizzato quanto segue:

   - I controller iOS sono altamente correlati al traffico delle porte

- La policy sulle performance viene violata quando la porta trasmette i/o al server.
- Dato che la nostra violazione delle performance delle porte si verifica in concomitanza con un carico IOPS elevato sul controller dello storage, è probabile che la violazione sia dovuta al carico di lavoro sul nodo dello
storage.

7. Tornare alla pagina di destinazione della porta e accedere alla pagina di destinazione del nodo dello storage controller per analizzare le metriche del carico di lavoro.

   Il nodo mostra una violazione di utilizzo e le metriche mostrano elevati valori di "cache replaced" correlati agli stati di credito zero buffer-to-buffer.



8. Dalla landing page del nodo, è possibile confrontare gli zero del credito BB selezionando la porta dall'elenco delle risorse correlate e selezionando i dati di utilizzo, inclusi i dati di utilizzo della cache, per il nodo dal menu delle metriche.

Questi dati rendono chiaro che il rapporto di hit della cache è inversamente correlato alle altre metriche. Invece di poter rispondere al carico del server dalla cache, il nodo di storage sta riscontrando elevati valori di lettura della cache. È probabile che la necessità di recuperare la maggior parte dei dati dal disco piuttosto che dalla cache causi il ritardo nella trasmissione dei dati della porta al server. La causa del problema di performance sembra essere una modifica del comportamento io generata dal carico di lavoro e la causa è la cache del nodo e la sua configurazione. Il problema potrebbe essere risolto aumentando le dimensioni della cache del nodo o modificando il comportamento dell'algoritmo di caching.

Analisi dell'infrastruttura

Le procedure descritte in questo argomento sono quelle che è possibile utilizzare per eseguire un'analisi di parti dell'infrastruttura nel proprio ambiente. I passaggi, le viste e i dati raccolti in questo esercizio utilizzano oggetti di calcolo virtuale come esempio. L'analisi di altre risorse nel tuo ambiente seguirà passaggi simili utilizzando contatori pertinenti per ogni risorsa specifica. Lo scopo di questo esercizio è quello di familiarizzare con la varietà di opzioni offerte da Insight per monitorare e comprendere le caratteristiche delle risorse nel data center.

A proposito di questa attività

Alcune delle azioni che è possibile intraprendere per analizzare lo stato dell'infrastruttura potrebbero includere quanto segue:

- Osservare il comportamento di un oggetto nel tempo
- Confronta le metriche di un oggetto con le metriche dei primi 10 oggetti simili
- Confronta i numeri per gli oggetti
- Confronta i primi 10 oggetti con la media
- Confronta le metriche A con B per molti oggetti per mostrare categorie e anomalie
- Confronta un intervallo di oggetti con altri oggetti
- Utilizzare un'espressione per visualizzare le metriche non disponibili nell'interfaccia utente Web

È possibile creare tutte queste viste degli oggetti nell'infrastruttura in una dashboard utilizzando i widget per ogni analisi eseguita. I dashboard possono essere salvati per fornire un rapido accesso ai dati correnti sulla tua infrastruttura.

Osservare il comportamento di un oggetto nel tempo

È possibile osservare il comportamento di un singolo oggetto per determinare se l'oggetto funziona entro i livelli operativi previsti.

Fasi

1. Utilizzare una query per identificare la macchina virtuale oggetto dell'analisi: **Query** > **+ Nuova query** > **macchina virtuale** > **"nome"**

   Lasciando vuoto il campo del nome, vengono restituite tutte le macchine virtuali. Selezionare la macchina virtuale che si desidera utilizzare in questo esercizio. È possibile selezionarla scorrendo l'elenco delle macchine virtuali.

2. Creare una nuova dashboard per le informazioni che si desidera raccogliere. Dalla barra degli strumenti, fare clic su **Dashboard** > **+Nuova dashboard**.
3. Nella nuova dashboard, selezionare **variabile** > **testo**.

   a. Aggiungere il nome della macchina virtuale dalla query come`$var1` valore.

   b. Fare clic sulla casella di controllo.

   La variabile viene utilizzata per alternare facilmente diversi set di oggetti che si desidera analizzare. In altre fasi dell'analisi, è possibile riutilizzare questa variabile per un'analisi aggiuntiva rispetto alla singola macchina virtuale inizialmente scelta. Le variabili diventano più utili quando si identificano più oggetti.

4. Aggiungi un widget per il grafico a linee alla nuova dashboard: **Widget** > **grafico a linee**.

   a. Modificare il tipo di risorsa predefinito in macchina virtuale: Fare clic su **macchina virtuale** > **latenza-totale**.

   b. Fare clic su **Filtra per** > **Nome** > * var1*.

   c. Modificare il periodo di tempo sul dashboard: **Ignora ora ora dashboard** > **on** > **7 giorni**.

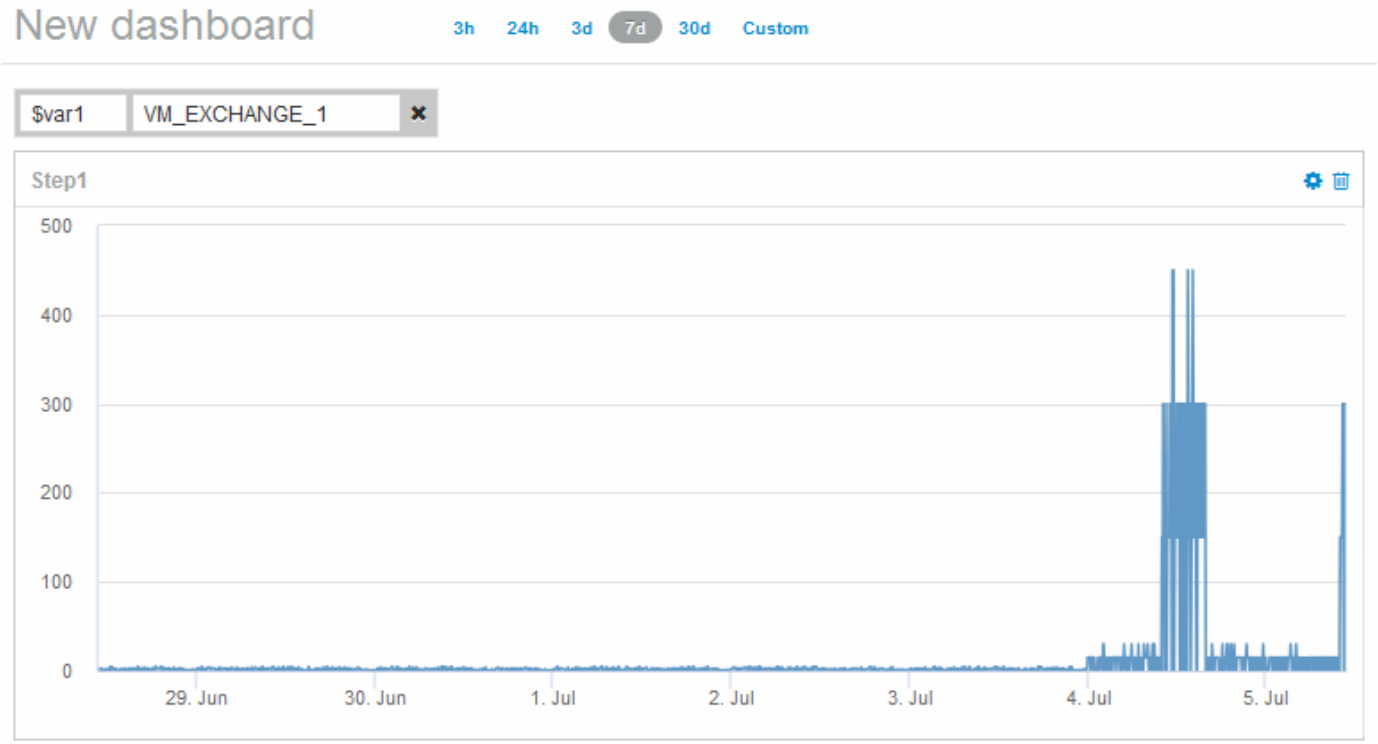
      È possibile modificare la durata della visualizzazione utilizzando una delle selezioni predefinite o specificando un intervallo di tempo personalizzato.

   + il dashboard visualizza il **IOPS-Total** della macchina virtuale per il periodo di tempo specificato.

5. Assegnare un nome al widget e salvarlo.

Risultati

Il widget deve contenere dati simili ai seguenti:



La VM mostra un periodo di latenza eccessivamente elevata per un breve periodo di tempo nei 7 giorni visualizzati.

Confronta gli oggetti con la latenza totale massima di 10 latenza con la latenza media per tutti gli oggetti simili

Si consiglia di confrontare le macchine virtuali con la latenza totale massima di 10 latenza rispetto alla latenza media totale per identificare quelle che sono estremamente fuori dall'intervallo medio. Queste informazioni potrebbero aiutare nelle decisioni di bilanciamento dei carichi di lavoro sulle macchine virtuali.

Fasi

1. Aggiungere un widget con un grafico ad area sovrapposta alla nuova dashboard: **Widget** > **grafico ad area sovrapposta**

   a. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **latenza totale**

      Il widget visualizza il totale di latenza, per tutte le macchine virtuali, per 24 ore in un grafico ad area sovrapposta.

   b. Creare una seconda visualizzazione in questo widget che mostri la latenza totale media per tutte le macchine virtuali: **Widget** > **grafico a linee**

   c. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **macchina virtuale** > **latenza-totale**

      Il widget visualizza la latenza totale per il periodo di tempo predefinito di 24 ore utilizzando un grafico a linee.

   d. Fare clic su **X** nella barra **Roll-up** e selezionare **Show** > **Top** > **10**

   Il sistema visualizza le prime 10 macchine virtuali in base alla latenza totale.

2. Per confrontare la latenza media totale per tutte le macchine virtuali con il totale dei primi 10 IOPS, attenersi alla seguente procedura:

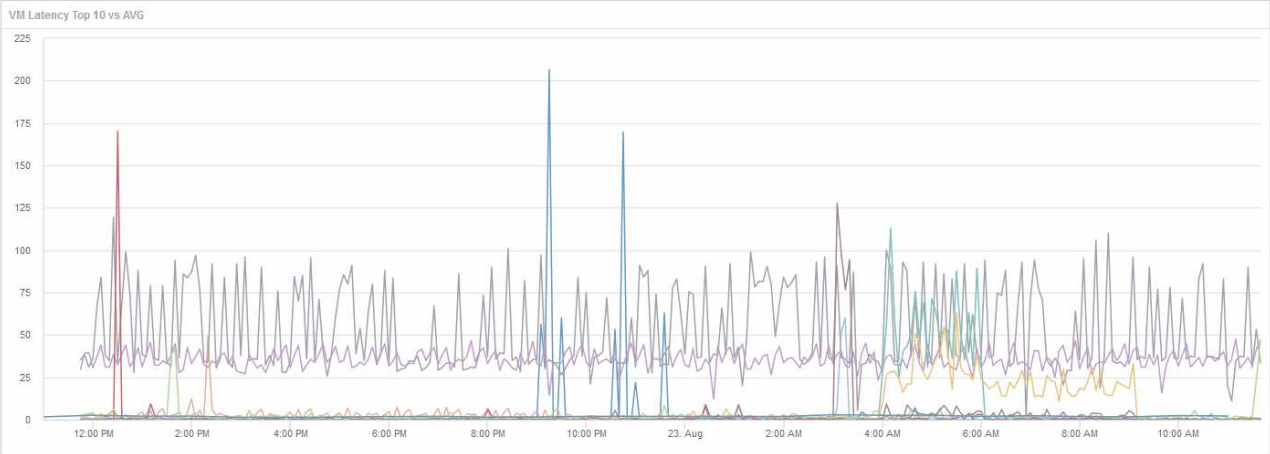
   a. Fare clic su **+Aggiungi**

   b. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **IOPS Total**

   c. Fare clic su **X** nella barra **Roll-up** e selezionare **Show** > **Top** > **10**

      Il sistema visualizza i 10 oggetti con latenza elevata e la latenza media in un grafico a linee.

      +



+ la latenza media è di 1.6 ms, mentre nelle prime dieci macchine virtuali la latenza è superiore a 200 ms.

Confronta il totale di latenza di un oggetto con il totale di latenza dei primi 10 oggetti

I seguenti passaggi mettono a confronto il totale di latenza di una singola macchina virtuale con le macchine virtuali che riportano il totale di latenza Top 10 nell'intera infrastruttura virtuale.

Fasi

1. Aggiungere un widget con un grafico a linee alla nuova dashboard: **Widget** > **grafico a linee**

   a. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **Latency-total**

      Il widget visualizza la latenza totale, per tutte le macchine virtuali, per le 24 ore predefinite in un grafico ad area.

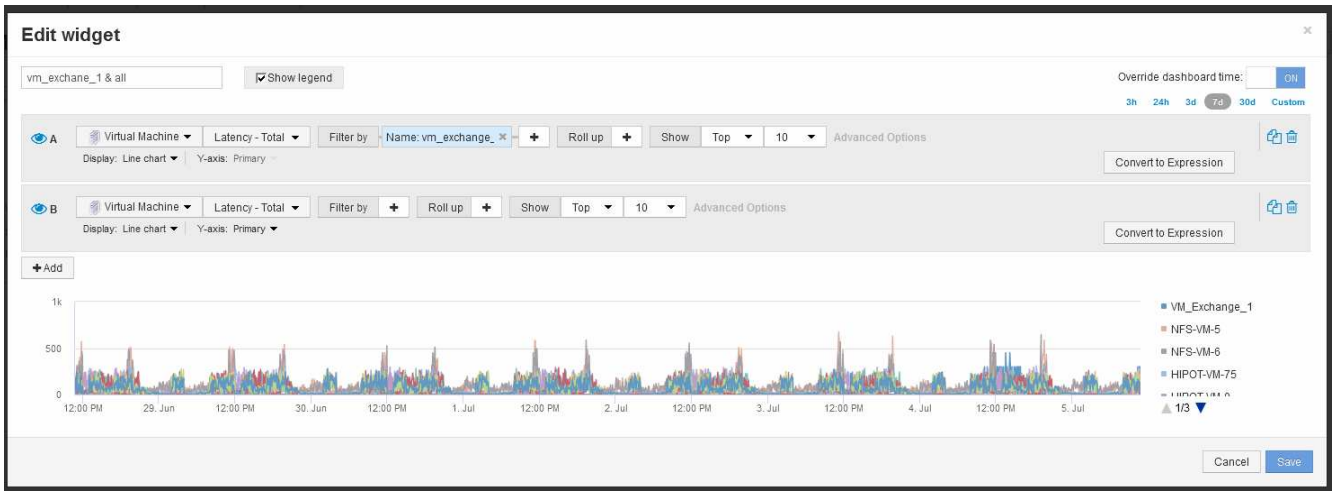
   b. Creare una seconda visualizzazione in questo widget che mostri la latenza totale media per tutte le macchine virtuali: **Widget** > **grafico a linee**

   c. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **Latency-Total**

      Il widget visualizza il totale di latenza per il periodo di tempo predefinito di 24 ore utilizzando un grafico a linee.

   d. Fare clic su **X** nella barra **Roll-up** e selezionare **Show** > **Top** > **10**

   Il sistema visualizza le prime 10 macchine virtuali in base alla latenza - totale.



2. Aggiungere la macchina virtuale che si desidera confrontare con la Top 10:
   a. Fare clic su **+Aggiungi**
   b. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **latenza totale**
   c. Fare clic su **Filtra per** > **Nome** > * var1*
3. Fare clic su **Mostra legenda**

Risultati

Una legenda identifica ciascuna delle macchine virtuali in analisi. È possibile identificare facilmente VM_Exchange_1 e determinare se presenta una latenza simile alle prime dieci macchine virtuali dell'ambiente.

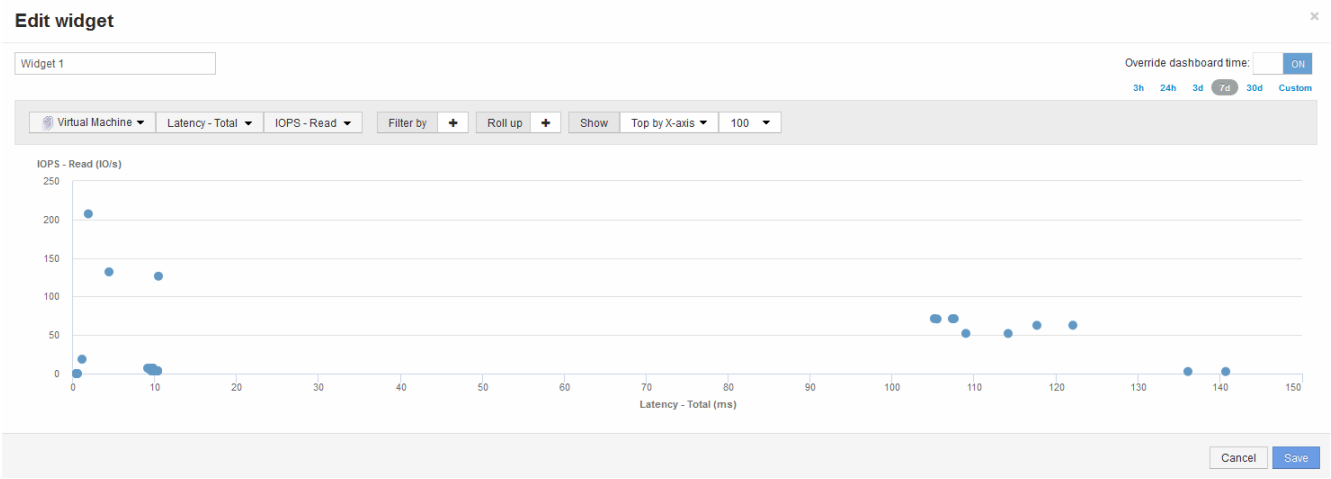
Confronta le metriche A con quelle B per mostrare le categorie e le anomalie

È possibile utilizzare un grafico a dispersione per visualizzare due set di dati per ciascun oggetto. Ad esempio, è possibile specificare IOPS Read (lettura IOPS) e Latency Total (totale latenza) da visualizzare per ciascun oggetto. Utilizzando questo grafico è possibile identificare l'oggetto che si considera problematico in base agli IOPS e alla latenza combinata.

Fasi

1. Aggiungere un widget con un grafico a dispersione alla nuova dashboard: **Widget** > **grafico a dispersione**
2. Impostare il dispositivo predefinito su macchina virtuale: Fare clic su **Storage** > **Virtual Machine** > **latenza totale** > **IOPS Read**

   Il sistema visualizza un grafico a dispersione simile a quanto segue:



Utilizzare un’espressione per identificare metriche alternative

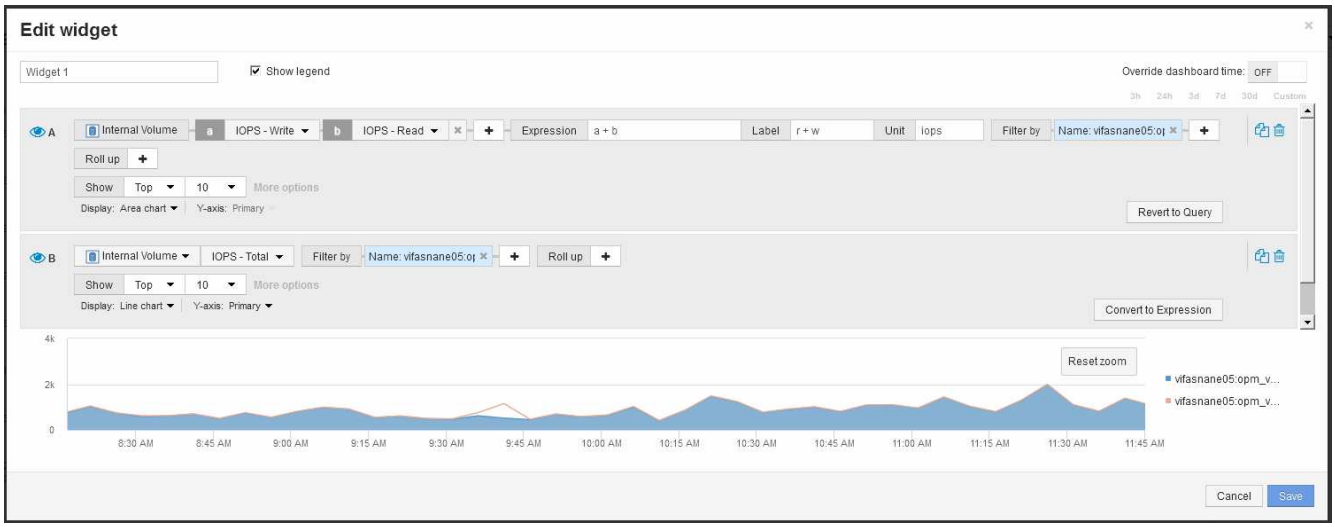
È possibile utilizzare le espressioni per visualizzare le metriche non fornite dall’interfaccia utente Web, ad esempio gli IOPS generati dall’overhead di sistema.

A proposito di questa attività

È possibile utilizzare un’espressione per visualizzare gli IOPS totali generati da operazioni non di lettura o non di scrittura, ad esempio operazioni di overhead per un volume interno.

Fasi

1. Aggiungere un widget alla dashboard. Scegliere **Area chart**.
2. Impostare il dispositivo predefinito su Volume interno: Fare clic su **Storage** > **Internal volume** > **IOPS Write**
3. Fare clic sul pulsante **Converti in espressione**.
4. La metrica **IOPS - Write** si trova ora nel campo della variabile alfabetica “**a**”.
5. Nel campo della variabile “**b**”, fare clic su **Select** e scegliere **IOPS - Read**.
6. Nel campo **espressione**, digitare **a + b**. Nella sezione **Display**, selezionare**Area chart** per l’espressione.
7. Nel campo **Filtra per**, immettere il nome del volume interno che si sta analizzando.
8. Il campo **Label** identifica l’espressione. Modificare l’etichetta con un valore significativo come “R + W IOPS”.
9. Fare clic su **+Add**per aggiungere una riga per gli IOPS totali al widget.
10. Impostare il dispositivo predefinito su Volume interno: Fare clic su **Storage** > **Internal volume** > **IOPS Total**
11. Nel campo **Filtra per**, immettere il nome del volume interno analizzato.



Il grafico mostra gli IOPS totali come una riga, mentre il grafico mostra la combinazione di IOPS di lettura e scrittura in blu. Il divario tra 9:30 e 9:45 mostra operazioni io (overhead) non in lettura e non in scrittura.

Introduzione alla riduzione dei rischi nel thin provisioning

Negli odierni data center IT ibridi, gli amministratori sono costretti a estendere l'utilizzo delle risorse oltre i limiti fisici, utilizzando tecnologie per l'efficienza della capacità, come il thin provisioning, per controllare l'allocazione e sfruttare le capacità un tempo non disponibili.

OnCommand Insight fornisce informazioni sull'utilizzo e sull'utilizzo della capacità quasi in tempo reale in diversi layer con thin provisioning all'interno dello stack di servizi IT. La mancata gestione corretta del rischio di oversubscription potrebbe causare un downtime inopportuno per l'azienda.

Monitoraggio del pool di storage

Ogni landing page del pool di storage fornisce rapporti di oversubscription, identifica le risorse correlate, l'utilizzo di LUN e dischi, nonché violazioni e violazioni delle policy che si sono verificate con il pool di storage.

Utilizza la landing page del pool di storage per identificare eventuali problemi con le risorse fisiche che supportano l'infrastruttura virtuale. È possibile tenere traccia dei trend dei rapporti di capacità e capacità per 30 giorni o utilizzare un intervallo di tempo personalizzato. Prestare attenzione ai dati nelle sezioni seguenti per monitorare lo stato del pool di storage.

- **Riepilogo**

  Utilizzare questa sezione per comprendere:

  - Informazioni sulla capacità del pool di storage, tra cui la capacità fisica e la capacità di overcommit.
  - Se l'aggregato è sovrascruto e in base alla quantità.
  - Eventuali violazioni delle policy che si sono verificate.
- **Risorse di storage e dischi**

La sezione delle risorse di storage mostra l'utilizzo del LUN.

La sezione dischi mostra i singoli dischi che compongono il pool di storage.

- **Risorse**

  Utilizzare questa sezione per comprendere la correlazione tra VMDK e LUN e il percorso dell'applicazione da storage a macchina virtuale.

- **Sezione violazioni**

  La sezione violazioni identifica eventuali violazioni alle policy di performance impostate per il pool di storage.

Monitoraggio dei datastore

La landing page di Datastore identifica i rapporti di oversubscription, l'utilizzo di LUN e dischi, le risorse correlate e mostra i casi di violazione delle policy che si sono verificati con il Datastore.

Utilizzare questa landing page per identificare i problemi relativi all'infrastruttura virtuale. Puoi tenere traccia dei trend di capacità e rapporto di capacità per anticipare i cambiamenti nella tua capacità.

- **Riepilogo**

  Utilizzare questa sezione per comprendere:

  - Informazioni sulla capacità del datastore, tra cui la capacità fisica e la capacità di overcommit.
  - La percentuale di capacità in eccesso.
  - Metriche per latenza, IOPS e throughput.

- **VMDK**

  La sezione VMDK mostra la capacità e le performance dei dischi virtuali.

- **Risorse di storage**

  Questa sezione mostra la capacità utilizzata e le metriche delle performance per il volume interno correlato al datastore.

- **Risorse**

  Utilizzare questa sezione per comprendere la correlazione tra VMDK e LUN e il percorso dell'applicazione da storage a macchina virtuale.

- **Sezione violazioni**

  La sezione violazioni identifica eventuali violazioni alle policy di performance impostate per il datastore.

Creare dashboard per monitorare gli ambienti con thin provisioning

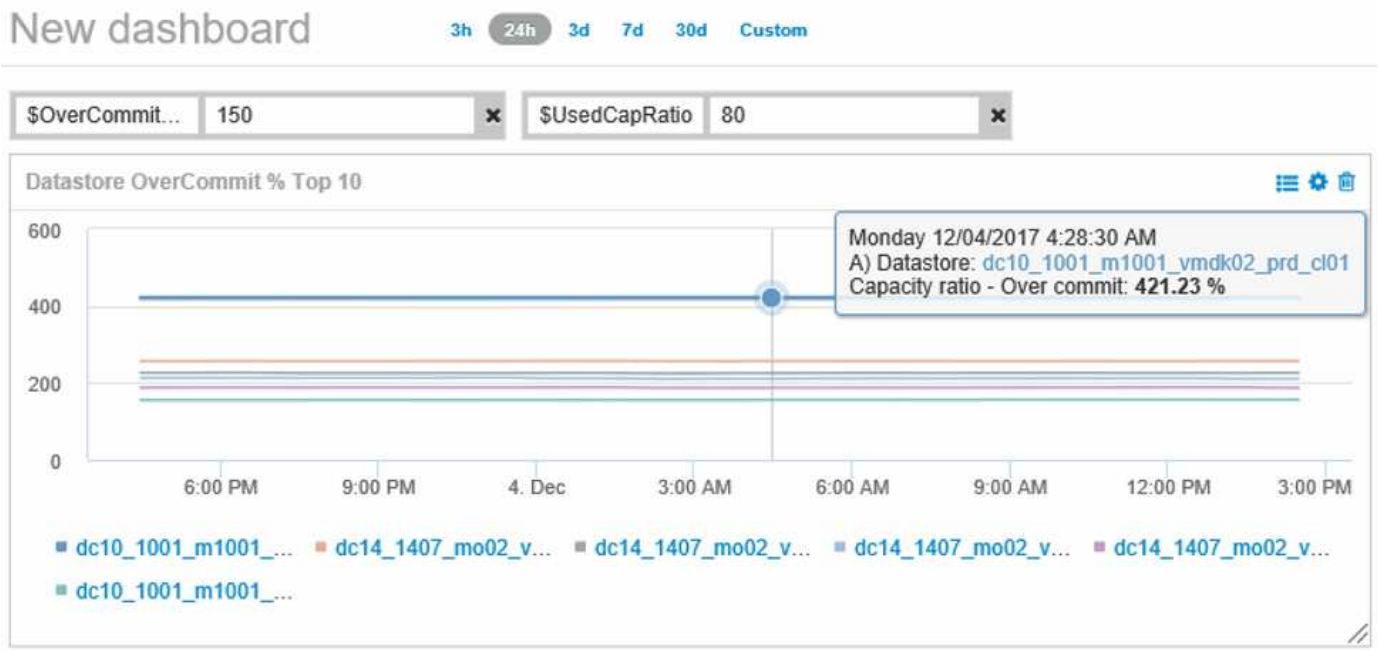
Le opzioni flessibili di progettazione e visualizzazione dei widget della dashboard di OnCommand Insight consentono un'analisi approfondita dell'utilizzo e dell'utilizzo della

capacità, informazioni strategiche per ridurre al minimo i rischi nelle infrastrutture dei data center con thin provisioning.

È possibile creare dashboard che forniscono l'accesso alle informazioni del datastore e del pool di storage che si desidera monitorare.

Utilizzo di dashboard per accedere alle informazioni del datastore

È possibile creare dashboard che consentono di accedere rapidamente ai dati che si desidera monitorare nell'infrastruttura virtuale. Una dashboard potrebbe includere widget simili ai seguenti per identificare i primi 10 datastore in base alla percentuale di overcommit e un widget che mostra i dati di capacità per i datastore. Le dashboard utilizzano variabili per evidenziare i datastore che sono overcommit di oltre il 150% e i datastore che hanno superato oltre il 80% della capacità utilizzata.



Overcommit Subscription %

Name	Capacity - Total (GB)	Capacity - Used (GB)	Capacity - Provisioned (GB)	Capacity ratio - Over commit (%)	Capacity ratio - Used (%)
dc14_1407_...1_prd_cl03	5,008.00	4,091.04	12,876.38	257.12	81.69
dc14_1407_...2_prd_cl03	6,936.69	5,872.31	14,633.80	210.96	84.66
dc14_1407_...3_prd_cl03	9,437.03	7,951.36	17,639.86	186.92	84.26
dc14_1407_...4_prd_cl03	7,911.09	6,627.00	17,891.24	226.15	83.77

4 items found

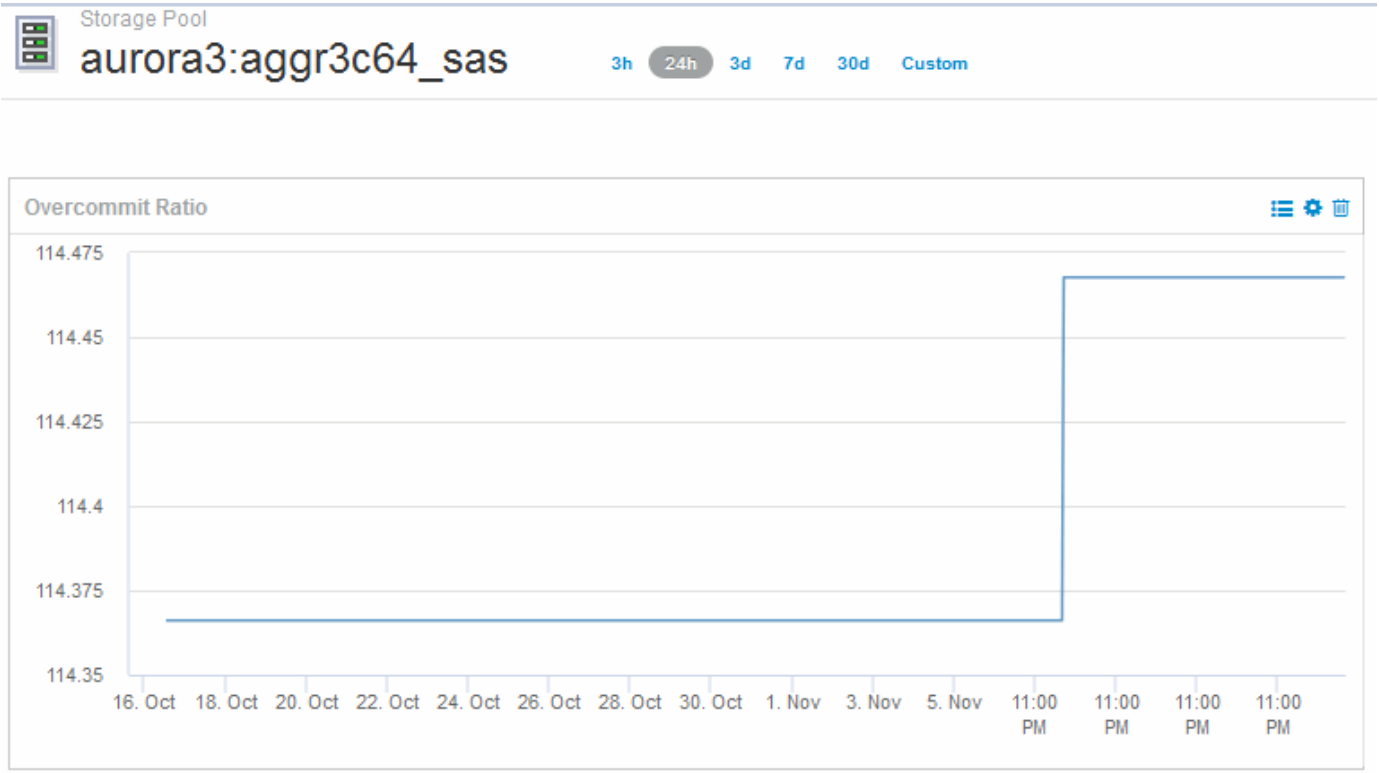
I widget aggiuntivi che potrebbero essere utilizzati per monitorare l'ambiente con thin provisioning potrebbero includere alcune delle seguenti informazioni:

- Capacità VMDK correlate ai datastore

- Capacità delle macchine virtuali
- La capacità del data store ha utilizzato i trend

Utilizzo di dashboard per accedere alle informazioni del pool di storage

Una dashboard potrebbe includere widget simili ai seguenti, identificando la quantità di capacità di storage fisica utilizzata o identificando la capacità di overcommit per un pool di storage.



Utilizzo di policy sulle performance per ridurre i rischi nel thin provisioning

È necessario creare policy sulle performance per generare avvisi in caso di violazione delle soglie dell'infrastruttura virtuale. Gli avvisi consentono di rispondere alle modifiche dell'ambiente prima che causino interruzioni o interruzioni delle operazioni.

Le policy che aiutano a monitorare l'infrastruttura virtuale includono:

- **Datastore**

  È possibile utilizzare i seguenti criteri nel datastore:

  - Rapporto di capacità - assegnazione in eccesso
  - Rapporto di capacità - utilizzato
  - Capacità - utilizzata
  - Capacità - totale
- **Pool di storage**

  Le seguenti policy possono proteggere da interruzioni di capacità legate allo storage in ambienti con thin provisioning:

- Provisioning della capacità
- Capacità utilizzata
- Rapporto di capacità - assegnazione in eccesso
- Rapporto di capacità - utilizzato

È possibile espandere queste policy per monitorare la capacità dell'infrastruttura virtuale, tra cui:

- Volumi interni
- LUN
- Dischi
- VMDK
- Macchine virtuali

È possibile configurare le policy utilizzando le annotazioni. Assegnare la stessa annotazione alle risorse specifiche che supportano un'applicazione. Ad esempio, è possibile assegnare annotazioni agli archivi dati e ai pool di storage di un'applicazione con thin provisioning. Le annotazioni potrebbero essere denominate produzione per l'ambiente di produzione, sviluppo per l'ambiente di sviluppo e così via. È possibile modificare le soglie e la criticità degli avvisi in base al tipo di applicazione supportata dalle risorse. Ad esempio, una violazione di una soglia per il datastore di un'applicazione di produzione potrebbe generare un *avviso critico*, mentre la stessa violazione per un ambiente di sviluppo potrebbe solo generare un *avviso*. L'integrazione di annotazioni all'interno di policy definite può contribuire a ridurre ulteriormente il rumore di avviso indesiderato per le risorse non critiche.

Creazione di policy sulle performance per i pool di storage

È possibile creare policy sulle performance che attivino avvisi per notificare il superamento delle soglie per le risorse dello Storage Pool.

Prima di iniziare

Questa procedura presuppone che sia stato eseguito il thin provisioning del pool di storage.

A proposito di questa attività

Si desidera creare policy che monitorino e segnalino le modifiche in un pool di storage che potrebbero contribuire alle interruzioni. Per il pool di storage fisico con thin provisioning, si desidera monitorare la capacità fisica e il rapporto di overcommit.

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. Se le notifiche sono attivate (**Admin** > **Notifiche**), puoi configurare Insight per l'invio di e-mail in caso di violazione delle policy di performance.

3. Fare clic su **+Add**per creare una nuova policy.

4. In **Policy Name** (Nome policy), immettere un nome di policy per il pool di storage.
5. In **Applica a oggetti di tipo** selezionare Storage Pool.
6. In **Apply after window of** inserire la prima occorrenza.
7. In **con severità** inserire critico
8. Configurare i destinatari e-mail a cui si desidera inviare una notifica in caso di superamento delle soglie.

   Per impostazione predefinita, gli avvisi e-mail sulle violazioni dei criteri vengono 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 questa policy verranno inviati a tutti i destinatari dell'elenco.

9. In **Create alert (Crea avviso), se uno dei seguenti valori è vero**, immettere Capacity Ratio - used > 85%

Risultati

Questa configurazione comporta l'invio di un messaggio di avviso critico quando si utilizza più del 85% della capacità fisica del pool di storage. L'utilizzo del 100% della memoria fisica causerà un errore dell'applicazione.

Creare policy aggiuntive per il pool di storage

A proposito di questa attività

Creare un ulteriore criterio "Capacity Ratio - used" che genera un messaggio di avviso quando la capacità dello Storage Pool utilizzata supera il 75%. Se le notifiche sono attivate (**Admin** > **Notifiche**), puoi configurare Insight per l'invio di e-mail in caso di violazione delle policy di performance.

Creazione di policy sulle performance per gli archivi dati

È possibile creare policy sulle performance con soglie per le metriche associate agli archivi dati che si riferiscono ai pool di storage che si stanno monitorando. Per impostazione predefinita, i criteri relativi alle performance si applicano a tutti i dispositivi del tipo specificato quando vengono creati. È possibile creare un'annotazione per includere solo un dispositivo specifico o una serie di dispositivi nella policy delle performance.

Prima di iniziare

Quando si utilizza un'annotazione in una policy di performance, l'annotazione deve esistere prima della creazione della policy.

A proposito di questa attività

Si crea un criterio di performance che fornisce una notifica quando uno o più datastore monitorati superano una soglia impostata. Il sistema potrebbe già contenere una policy globale che soddisfa le tue esigenze oppure una policy che utilizza le annotazioni potrebbe funzionare anche se annoti tuoi datastore.

Fasi

1. Dalla barra degli strumenti di Insight, selezionare **Gestisci** > **Criteri di performance**

Viene visualizzata la pagina delle policy di performance. Esaminare le policy di performance esistenti per identificare le policy esistenti che affrontano le metriche delle soglie che si desidera monitorare.

2. Fare clic su **+Aggiungi** per aggiungere una nuova policy
3. Aggiungi un “Policy Name”

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

4. Selezionare "datastore" come tipo di oggetto
5. Fare clic su “First ricorrenza”

   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.

6. Fare clic su “Warning”
7. Per “Create alert”, selezionare **Capacity ratio - over commit** e impostare il valore su **> 150**

   È possibile creare avvisi aggiuntivi relativi alla capacità, ad esempio **capacità totale**e **capacità utilizzata**.

Raccolta dei dati di utilizzo del file system host e VM

L’origine dati dei file system host e VM, combinata con la licenza di utilizzo degli host, consente la creazione di report e il chargeback a livello di file system per host e macchine virtuali noti.

OnCommand Insight raccoglie i dati dai dispositivi di storage, la maggior parte dei quali riporta i propri volumi come dispositivi a blocchi. Ciò consente a Insight di creare report sull’utilizzo a livello di storage, ma non a livello di file system. Gli array di storage in genere sanno quali blocchi sono stati scritti, ma non quali sono stati liberati.

Gli host client e le macchine virtuali implementano file system (ntfs, ext*…) in cima a questi dispositivi a blocchi. La maggior parte dei file system conserva un sommario contenente metadati di directory e file. Quando i file vengono cancellati, le relative voci vengono semplicemente rimosse dal sommario. I blocchi consumati da questi file sono ora idonei per il riutilizzo da parte del file system, ma lo storage array non lo sa. Affinché Insight possa generare report sull’utilizzo del file system, deve essere raccolto dal punto di vista dell’host client o della macchina virtuale per un chargeback accurato.

Insight consente questo livello di raccolta dei dati di utilizzo del file system attraverso l’origine dati **NetApp host and VM file System**, in combinazione con la licenza **host Utilization**. Le macchine virtuali devono essere annotate con il nome **Compute Resource Group** appropriato e gli storage array associati devono essere annotati con le annotazioni **Tier** appropriate con i costi appropriati per un reporting dei costi accurato.

> La licenza di utilizzo host è basata sulle risorse, invece che sulla capacità come altre licenze Insight.

Configurare Insight per la raccolta del file system

Per configurare Insight per la raccolta dei dati di utilizzo del file system, è necessario installare la licenza host Utilization Pack e configurare l'origine dati dei file system VM e host di NetApp.

Prima di iniziare

Se non lo si è già fatto, installare la licenza host Utilization Pack. È possibile verificare la licenza nella pagina **Admin** > **Setup**, nella scheda **Licenses**.

L'origine dati dei file system host e VM riporta solo l'utilizzo del file system e i metadati del file system per le risorse di calcolo note (host e macchine virtuali) attualmente raccolte o scoperte in Insight:

- Le macchine virtuali vengono raccolte da origini dati hypervisor come Hyper-V e VMware.
- Gli host vengono rilevati tramite la risoluzione del dispositivo.

Le annotazioni Tier appropriate devono essere presenti sulle risorse di storage appropriate.

Sono supportati i seguenti dispositivi di storage a blocchi collegati:

- CDOT (NetApp Clustered Data ONTAP)
- NetApp 7-Mode
- CLARiiON
- Windows: Dischi virtuali VMware (VMDK) per FC, iSCSI
- Linux: VMDK VMware (iSCSI e FC non supportati)

Un **Compute Resource Group** è un'annotazione che consente il raggruppamento di host e/o macchine virtuali che condividono una credenziale amministrativa comune.

Fasi

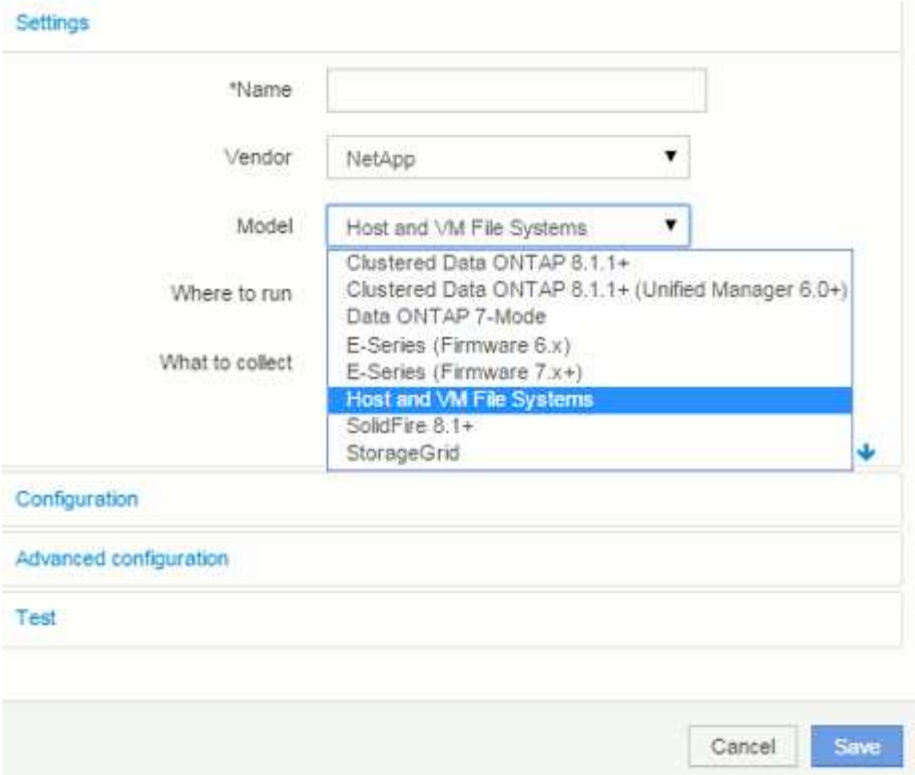
1. Per prima cosa, annotare gli host e/o le macchine virtuali da includere nel proprio **Compute Resource Group**. Vai a **Query** > **+Nuova query** e cerca le risorse di *Virtual Machine*.

   È necessario ripetere questi passaggi per le risorse *host*.

2. Fare clic sul selettore di colonna a destra della tabella e selezionare la colonna **Compute Resource Group** per visualizzarla nella tabella dei risultati della query.
3. Selezionare le macchine virtuali che si desidera aggiungere al gruppo di risorse di calcolo desiderato. È possibile utilizzare un filtro per cercare risorse specifiche.
4. Fare clic sul pulsante **azioni** e scegliere **Modifica annotazione**.
5. Selezionare l'annotazione *Compute Resource Group*, quindi scegliere il nome del gruppo di risorse desiderato nel campo *value*.

   L'annotazione del gruppo di risorse viene aggiunta alle macchine virtuali selezionate. Il nome del gruppo di risorse deve corrispondere al nome che verrà configurato in seguito nell'origine dati dei file system host e VM.

6. Per configurare l'origine dati dei file system host e VM per un gruppo di risorse di calcolo, fare clic su **Admin** > **origini dati** e **Aggiungi** l'origine dati *NetApp host and VM file Systems*.



7. Nella sezione **Configurazione**, immettere **Nome utente** e **Password** per un utente del sistema operativo con i diritti appropriati per recuperare i dati del file system. Per gli utenti del sistema operativo Windows, questo deve includere il prefisso di dominio se utilizzato dall'ambiente Windows.

   Si noti che un'unità di acquisizione Insight (AU) installata su Linux può generare report sulle risorse di calcolo Linux, mentre un'unità AU installata su Windows può comunicare con risorse di calcolo Linux o Windows.

8. Immettere il nome del gruppo di risorse di calcolo* per le risorse da cui si desidera raccogliere i dati di utilizzo del file system. Questo nome deve corrispondere al nome del gruppo di risorse utilizzato per annotare le risorse di cui sopra.

   Se si lascia vuoto il campo Compute Resource Group, l'origine dati raccoglierà i dati per gli host o le macchine virtuali che non dispongono di annotazione Compute Resource Group.

9. Nella sezione **Advanced Configuration**, inserire l'intervallo di polling desiderato per questa origine dati. Il valore predefinito di 6 ore è generalmente adeguato.
10. Si consiglia di **testare** la connessione all'origine dati prima di salvarla. Il risultato di una connessione riuscita mostra anche il numero di destinazioni delle risorse di calcolo contenute nel gruppo.
11. Fare clic su **Save** (Salva). L'origine dati dei file system host e VM inizierà a raccogliere i dati al prossimo sondaggio.
12. Una volta raccolti i dati del file system, è possibile visualizzarli nella pagina delle risorse dell'host o della macchina virtuale, nel widget file system:

File Systems

Name	Capacity (Used / Total GB)	Type	Storage Resource
/	9.15% (11.0 / 120.0)	xfs	vifasnane:...:vm_oci_
/boot	23.79% (0.1 / 0.5)	xfs	vifasnane:...:vm_oci_
/dev/dm-1	7.8	swap	vifasnane:...:vm_oci_

Showing 1 to 3 of 3 entries

13. Ripetere questi passaggi per ciascun gruppo di risorse di calcolo. Ciascun gruppo di risorse di calcolo deve essere associato alla propria origine dati dei file system host e VM.

    Si noti che le informazioni sul file system verranno raccolte per host e macchine virtuali già acquisiti da qualsiasi origine dati VMware o Hyper-V tradizionale nel proprio ambiente.

Chargeback e reporting del file system

Il chargeback per i file system viene sempre eseguito dal punto di vista dello storage. Gli array di storage associati alle macchine virtuali annotati per un particolare gruppo di risorse di calcolo verranno inclusi nei report di chargeback per quel gruppo di risorse.

Prima di iniziare

Tutte le macchine virtuali che si desidera includere nel chargeback di utilizzo del file system devono essere annotate con il nome appropriato del gruppo di risorse di calcolo. Gli array di storage associati a tali macchine virtuali devono essere annotati con le annotazioni Tier appropriate. L'ETL al data warehouse deve essere avvenuto dopo che queste annotazioni sono state inserite.

Fasi

1. Aprire un browser nel server di reporting, in genere `https://<host or IP>:9300/p2pd``http://<host or IP\>:9300/bi (7.3.3 or later)` ed effettuare l'accesso.
2. Scegliere il pacchetto **file System Utilization** e creare un nuovo report.

3. Trascinare gli elementi dal data mart per creare il report.

    L'esempio seguente è un report molto semplice. È possibile creare report complessi basati sulle esigenze specifiche del business.

Name	Type	Allocated Capacity GB	Used Capacity GB	Tier Name	Cost	Storage Name
/	xfs	119.96	9.96	N/A		vifasnane05,vifasnane06
/	xfs	5,492.53	799.63	Tier 1	100	vifasnane
/boot	xfs	0.48	0.17	N/A		vifasnane05,vifasnane06
/boot	xfs	8.72	2.41	Tier 1	100	vifasnane
/dev/dm-1	swap	7.81	0.00	N/A		vifasnane05,vifasnane06
/dev/dm-1	swap	140.61	0.78	Tier 1	100	vifasnane
C:\	NTFS	948.27	331.98	Tier 1	100	vifasnane
PHYSICALDRIVE0: System Reserved	NTFS	1.70	1.41	Tier 1	100	vifasnane

Configurazione del sistema per il report dei dati di chargeback

I report di chargeback forniscono informazioni di chargeback della capacità di storage e di responsabilità per host, applicazioni ed entità aziendali e includono dati attuali e storici.

Questa guida descrive come configurare Insight per generare un report di chargeback che fornisce la responsabilità per i costi del livello di servizio e di utilizzo dello storage. Lo scopo della guida è quello di fornire i passaggi necessari per creare un semplice report di chargeback e familiarizzare gli utenti Insight con le opzioni disponibili durante la configurazione del chargeback nel proprio ambiente specifico.

Per ciascuna applicazione, il report di esempio identifica le risorse fornite e il costo delle risorse. L'output del report viene creato definendo i seguenti dati in Insight

- Tier di storage
- Costo associato a ciascun Tier di storage
- Capacità di storage fornita
- Livelli di servizio
- Costo per livello di servizio

Le sezioni seguenti descrivono i passaggi necessari per configurare questi dati in modo che possano essere accessibili da Insight Reporting.

Definizione delle annotazioni da utilizzare con il chargeback

Quando si personalizza OnCommand Insight per tenere traccia dei dati in base ai requisiti aziendali, è possibile definire annotazioni specializzate necessarie per fornire un quadro completo dei dati: Ad esempio, un'annotazione può definire la fine del ciclo di vita di una risorsa, il data center in cui risiede la risorsa o un Tier di storage che definisce il costo per GB dello storage.

A proposito di questa attività

L'esempio di report di chargeback in questa guida fornisce i dati per il livello di servizio e per il livello di livello.

È necessario creare annotazioni per ogni livello di servizio e livello e quindi definire i costi per i livelli di servizio e livello.

Fasi

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

   Viene visualizzata la pagina delle annotazioni.

3. Posizionare il cursore sul livello di servizio o sull'annotazione Tier e fare clic su .

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

4. Fare clic su **ADD** per aggiungere nuovi livelli e costi.

   Nell'esempio del report, i nomi dei livelli di servizio e di livello utilizzano l'analogia con il metallo prezioso Gold, Sliver e Bronze. È possibile utilizzare qualsiasi convenzione di denominazione scelta dall'organizzazione, ad esempio Tier 1, Level 2, Supreme.

5. Immettere i valori per i livelli Gold-Fast, Gold, Silver e Bronze e i costi associati a ciascuno di essi.

   I valori immessi definiscono il costo per GB per lo storage utilizzato dalle applicazioni. Il costo del livello di servizio può essere il costo della fornitura del servizio o il prezzo effettivo per il servizio al consumatore. Questi costi verranno riportati nel report Chargeback.

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

Definizione delle applicazioni da utilizzare con il chargeback

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

Prima di iniziare

Se si desidera associare l'applicazione a un'entità aziendale, è necessario aver già creato l'entità aziendale.

> Questo esempio non associa alcuna applicazione alle entità aziendali.

Fasi

1. Accedere all'interfaccia utente Web di OnCommand Insight.
2. Fare clic su **Gestisci** > **applicazione**

   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. Inserire le applicazioni identificate nel report: African Tours, APAC Commercial Sales e così via.

5. Fare clic su **priorità** e selezionare la priorità (critica, alta, media o bassa) per l'applicazione nell'ambiente in uso.
6. Se si prevede di utilizzare questa applicazione con un'entità aziendale, fare clic su **entità aziendale** e selezionare l'entità dall'elenco.
7. Non si utilizzerà la condivisione del volume. Fare clic per deselezionare la casella di condivisione del volume **convalida**.
8. Fare clic su **Save** (Salva).

   Le applicazioni vengono visualizzate nella pagina applicazioni. Facendo clic sul nome dell'applicazione, Insight visualizza la pagina delle risorse dell'applicazione. 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, è necessario associarle a risorse specifiche. È possibile utilizzare un semplice metodo ad hoc per applicare un'applicazione a una risorsa. Gli utenti che desiderano applicare le applicazioni in blocco devono utilizzare un metodo di query per identificare le risorse da assegnare a un'applicazione.

Assegnazione di applicazioni alle risorse utilizzando un metodo ad hoc

È possibile assegnare un'applicazione a una risorsa in modo da identificare le risorse della risorsa utilizzata dall'applicazione. Se un asset ha un costo assegnato all'IT, è possibile identificare il costo sostenuto dall'applicazione e, se la risorsa è misurata in base alla dimensione, è possibile determinare se la risorsa deve essere rifornita.

A proposito di questa attività

Utilizzare il seguente metodo per assegnare le applicazioni 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:

Opzione	Descrizione
Accedere all'elenco delle risorse	Fare clic su **Dashboard** > **Assets Dashboard** e selezionare la risorsa.
Cercare la 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 a un 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.

Assegnazione di applicazioni a una risorsa mediante una query

È possibile assegnare un'applicazione a una risorsa in modo da identificare le risorse della risorsa utilizzata dall'applicazione. Se un asset ha un costo assegnato all'IT, è possibile identificare il costo sostenuto dall'applicazione e, se la risorsa è misurata in base alla dimensione, è possibile determinare se la risorsa deve essere rifornita.

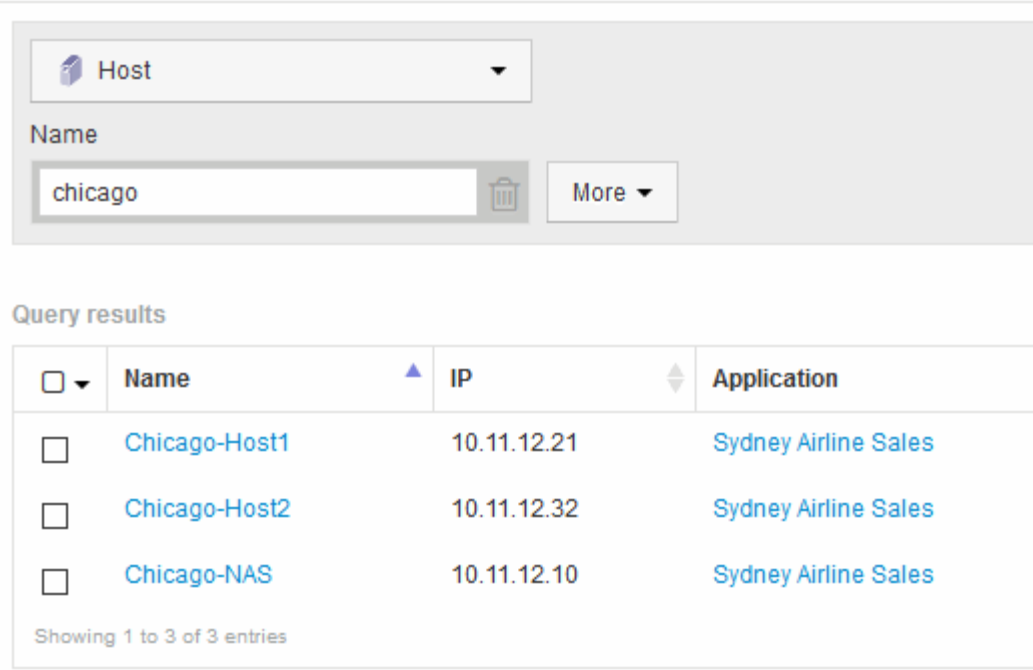
A proposito di questa attività

È possibile semplificare l'attività di assegnazione di più risorse a un'applicazione utilizzando una query.

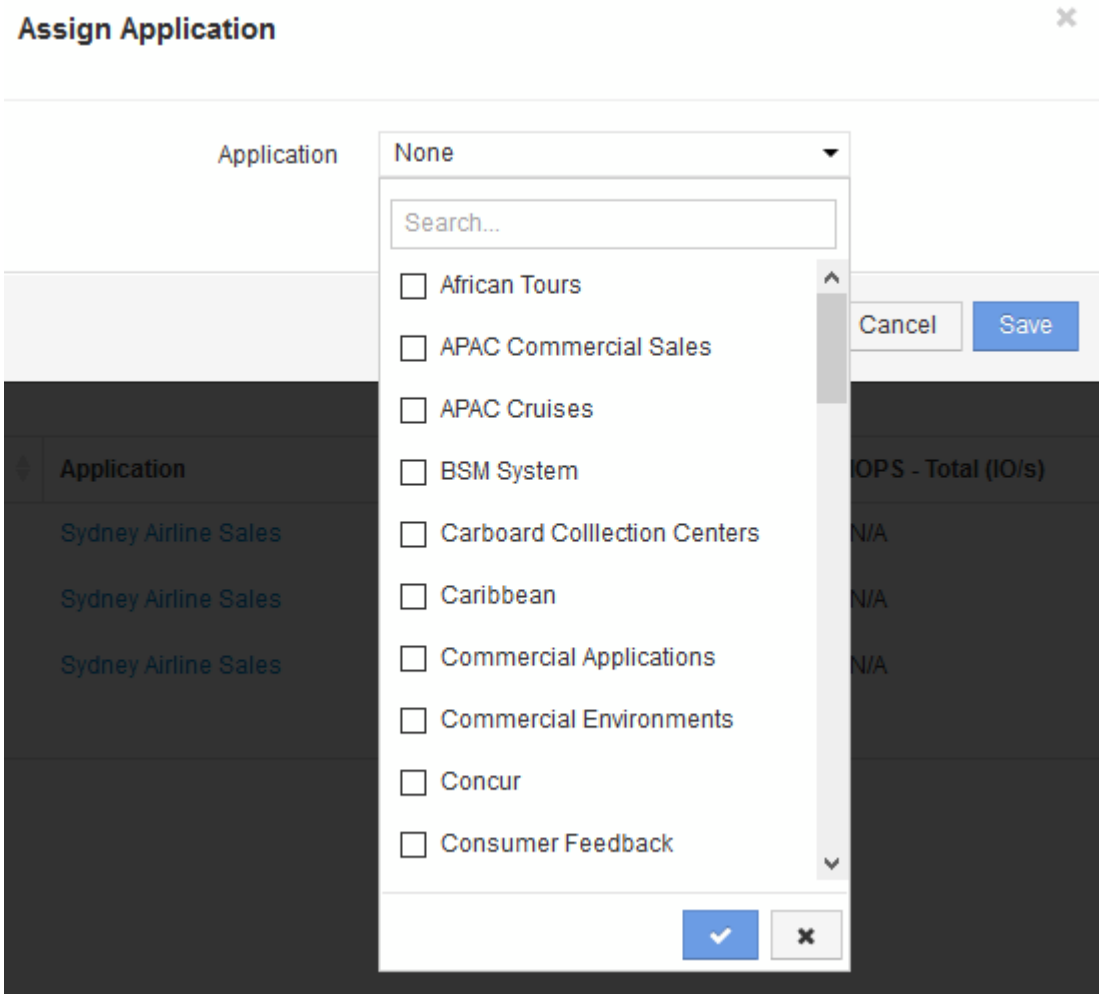
Fasi

1. Creare una nuova query per identificare le risorse a cui si desidera assegnare un'applicazione. Ad esempio, se si desidera assegnarlo a un host con un nome specifico relativo a una posizione geografica, fare clic su **Query** > **+Nuova query**
2. Fare clic su **host**
3. Nel campo **Nome**, immettere `Chicago`

   Il sistema visualizza tutti gli host con `Chicago` come parte se il loro nome.



4. Selezionare uno o più host identificati dalla query.
5. Fare clic su **azioni** > **Aggiungi applicazione**



Viene visualizzata la finestra di dialogo Assegna applicazione.

6. Selezionare l'applicazione che si desidera assegnare all'host e fare clic su 
7. Fare clic su **Save** (Salva)

   Il nome dell'applicazione viene visualizzato nella sezione User Data (dati utente).

Creazione di un semplice report di chargeback

I report di chargeback consentono ad amministratori e manager di valutare l'utilizzo della capacità per applicazione, entità aziendale, livello di servizio e Tier. I report di chargeback includono la responsabilità della capacità, la responsabilità storica della capacità e i dati di tendenza. I dati per questi report vengono creati e pianificati dal data warehouse di OnCommand Insight.

Prima di iniziare

Per creare il report di esempio, il sistema deve essere configurato in modo da riportare i costi per i Tier di storage. È necessario completare le seguenti attività:

- Definire le annotazioni per i livelli.
- Assegnare i costi alle annotazioni.
- Definire le applicazioni per le quali si desidera tenere traccia dei dati.
- Assegnare le applicazioni alle risorse.

A proposito di questa attività

In questo esempio viene utilizzato lo strumento di reporting avanzato di Cognos Workspace per creare il report Chargeback. Con Workspace Advanced, è possibile creare report trascinando e rilasciando gli elementi dei dati in un pallet di report.

Fasi

1. Nell'interfaccia utente Web di OnCommand Insight, fare clic sull'icona di reporting.
2. Accedere al portale di reporting.
3. Nella barra degli strumenti di IBM Cognos Connection, fare clic su **Launch** > **Cognos Worksapce Advanced**

   Viene visualizzata la schermata del pacchetto Workspace Advanced.

4. Fare clic su **pacchetti** > **Chargeback**

   Viene visualizzata la schermata IBM Workspace Advanace.

5. Fare clic su **nuovo**
6. Nella finestra di dialogo **New** report (nuovo report), fare clic su **List** (elenco) per specificare un report a elenco.

   Viene visualizzata la tavolozza dei report e i messaggi "Simple data mart" e "Advanced data mart" vengono

visualizzati sotto l’intestazione Source (origine).

7. Fare clic sulle frecce accanto a ciascun data mart per espanderlo.

   Viene visualizzato il contenuto completo dei data mart.

8. Trascinare “Application” da "`Simple Data Mart `" nella colonna più a sinistra della tavolozza dei report.

   Quando si trascina un elemento nella tavolozza, la colonna si restringe ed è evidenziata. Se si rilasciano i dati dell’applicazione nelle colonne evidenziate, tutte le applicazioni vengono elencate correttamente nella colonna.

9. Trascinare “Tier” da "`Simple Data Mart `" nella colonna successiva della tavolozza dei report.

   Il livello di storage associato a ciascuna applicazione viene aggiunto alla tavolozza.

10. Trascinare “Tier Cost” da "`Simple Data Mart `" nella colonna successiva della tavolozza dei report.
11. Trascinare “Provised Capacity” da "`Simple Data Mart `" nella colonna successiva della tavolozza dei report.
12. Tenere premuto il tasto **Ctrl** e selezionare le colonne “Tier cost” e “provisioning Capacity” nel pallet.
13. Fare clic con il pulsante destro del mouse in una delle colonne selezionate.
14. Fare clic su **Calculate** > **Tier cost * Provised Capacity DB**

    Una nuova colonna viene aggiunta al pallet con il titolo "Tier Cost * Provision Capacity GB".

15. Fare clic con il pulsante destro del mouse sulla colonna **Tier Cost * Provision Capacity GB**.
16. Fare clic su **Style** > **Data Type** (tipo di dati)
17. Fare clic su **tipo formato** > **valuta**
18. Fare clic su **OK**

    I dati della colonna sono ora formattati come valuta statunitense.

19. Fare clic con il pulsante destro del mouse su “Tier Cost * Provision Capacity GB” e selezionare **Edit Data Item Label**
20. Sostituire il campo Nome con “Provised Capacity Cost”
21. Per eseguire il report, fare clic su **Esegui** > **Esegui report - HTML**

    Viene visualizzato un report simile al seguente.

Application	Service Level	Service Level Cost	Tier	Tier Cost	Provisioned Capacity GB	Provisioned Capacity Cost
APAC Commercial Sales	Gold-Fast	12	Gold-Fast	12	674.04	$8,088.42
APAC Commercial Sales	Silver	10	Silver	7	1,903.83	$13,326.82
APAC Cruises	Gold-Fast	12	Gold-Fast	12	730.20	$8,762.44
African Tours	Gold	12	Gold	10	4,856.12	$48,561.16
African Tours	Silver	10	Silver	7	1,480.85	$10,365.93
CRM	Bronze	3	Bronze	3	5,689.08	$17,067.23
Caribbean	Gold	12	Gold	10	4,590.41	$45,904.08
Commercial Applications	Bronze	3	Bronze	3	14,312.88	$42,938.64
Commercial Applications	Gold-Fast	12	Gold-Fast	12	40,308.42	$483,701.05
Commercial Environments	Bronze	3	Bronze	3	16,812.27	$50,436.81
Commercial Environments	Gold	12	Gold	10	9,313.51	$93,135.13
Commercial Environments	Silver	10	Silver	7	1,480.79	$10,365.54
Concur	Gold	12	Gold	10	247.39	$2,473.91
Concur	Gold-Fast	12	Gold-Fast	12	575.17	$6,902.09
Consumer Feedback	Gold	12	Gold	10	1,335.89	$13,358.94

Garantire che i report sulla densità io descrivano solo i volumi di dati interni

Nei sistemi storage NetApp, l'aggregato root contiene il volume root. Il volume root contiene directory speciali e file di configurazione per la gestione e il controllo del sistema storage. Le operazioni di gestione e controllo potrebbero causare una grande quantità di attività nell'aggregato root. Quando interroga il sistema Insight per i primi 10 volumi interni con la densità io più elevata, i risultati potrebbero includere gli aggregati root di NetApp come membri dei primi 10 volumi.

Durante il monitoraggio dell'ambiente, è più importante determinare quali volumi di dati interni producono numeri di densità i/o elevati. Per identificare con precisione solo i volumi di dati, è necessario isolare i volumi interni di NetApp dalle query utilizzate per monitorare la densità di i/O.

Questa guida descrive come identificare facilmente gli aggregati root di NetApp, isolarli dai risultati delle query di volume interne e creare regole che escludono eventuali nuovi aggregati root di NetApp man mano che vengono aggiunti al sistema. Le seguenti funzionalità Insight vengono utilizzate per garantire che i report di densità i/o derivino da volumi di dati interni.

- Viene creata una query per identificare tutti gli aggregati root NetApp monitorati da Insight.
- A ciascuno degli aggregati root di NetApp viene assegnata un'annotazione.
- Viene creata una regola di annotazione per escludere gli aggregati NetApp

Creazione di una query per identificare gli aggregati root di NetApp nel tuo ambiente

Le query forniscono ricerche a un livello granulare, in base ai criteri selezionati dall'utente. L'utilizzo di una query consente di cercare volumi interni nell'ambiente che contengono l'aggregato root NetApp.

Fasi

1. Nell'interfaccia utente Web di OnCommand Insight, creare una query per identificare gli aggregati root NetApp nell'ambiente: **Query** > **Nuova query** > **Seleziona tipo di risorsa**
2. Fare clic su **Storage Pool**
3. Immettere il nome dell'aggregato root

   In questo esempio viene utilizzato "aggr0" come nome. Quando si crea un aggregato, è necessario rispettare solo i seguenti requisiti per il nome:

   - Deve iniziare con una lettera o un carattere di sottolineatura (_).
   - Può contenere solo lettere, cifre e caratteri di sottolineatura.
   - Può contenere fino a 250 caratteri. Nella maggior parte dei casi l'aggregato è il nome aggr0, aggr_0 o qualcosa di simile. Potrebbe essere necessario un processo iterativo per identificare tutti gli aggregati root NetApp nel tuo ambiente.
4. Fare clic su **Save** (Salva) e immettere un nome per la nuova query.

   Come accennato in precedenza, questo potrebbe essere un processo iterativo e richiedere più query per identificare tutti gli aggregati root di NetApp.

Creare un'annotazione per i volumi root restituiti dalle query

Le annotazioni sono note specializzate assegnate alle risorse, che consentono di filtrare le risorse in base alle annotazioni. L'annotazione creata verrà utilizzata per identificare gli aggregati root di NetApp nel tuo ambiente e garantire che non siano inclusi in un report specifico.

Prima di iniziare

È necessario aver identificato tutti gli aggregati root che si desidera escludere dal report "High i/o Density".

Fasi

1. Creare un'annotazione per associare tutti gli aggregati root NetApp identificati con le query: **Gestisci** > **Annotazioni**
2. Fare clic su **Aggiungi**
   a. Inserire il nome dell'annotazione: **RootAgg**
   b. Inserire una descrizione dell'annotazione: **Rimuovere l'aggregato root dal report "High i/o Density"**
   c. Inserire il tipo di annotazione: **Booleano**
3. Fare clic su **Save** (Salva)

Creare una regola di annotazione per automatizzare l'esclusione di aggregati specifici dal report di densità i/O.

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 regole di annotazione si basano sulle query create e, quando vengono

eseguite sul sistema, aggiungono nuove risorse a set di risorse esistenti. Quando questi set di asset sono esclusi da un report, anche i nuovi asset vengono automaticamente esclusi.

Prima di iniziare

È necessario aver creato e salvato una query che identifichi gli aggregati root NetApp identificati nel proprio ambiente.

Fasi

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

   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: "RootAggrExclude"
   b. Fare clic su Query e selezionare la query che Insight deve utilizzare per applicare la regola di annotazione a:"` Aggregate0`"
   c. Fare clic su Annotation (Annotazione) e selezionare "Root Agg Exclude" (Escludi agg
   d. Fare clic su valore e immettere True

Raccolta dei dati di integrazione

È possibile importare i dati di integrazione nel sistema OnCommand Insight. I dati possono essere importati utilizzando collectd, software open source che viene eseguito come daemon per raccogliere i dati sulle performance, oppure utilizzando l'origine dati SNMP di integrazione che consente di raccogliere dati SNMP generici.

Flusso di dati per i dati di integrazione

Quanto segue si applica alla quantità totale di dati di integrazione che è possibile presentare al server OnCommand Insight:

- Viene mantenuta una coda di 100 chiamate.

  Quando un client attende nella coda per più di un minuto, si verifica un errore di timeout.

- Il tasso di acquisizione consigliato per i dati di integrazione è una volta al minuto, per client.
- È consentito un limite di 300 tipi di oggetti di integrazione.

Accesso al software e alla documentazione collectd

È possibile accedere al software del plugin di output writer e alla documentazione da collectd sul sito GitHub di NetApp: https://github.com/NetApp/OCI_collectd

Backup e ripristino dei dati di integrazione

Il backup e il ripristino dei dati di integrazione vengono modellati in base alle policy di backup e ripristino dei dati delle performance di OnCommand Insight. Quando un backup viene configurato per i dati delle performance, anche i dati di integrazione vengono inclusi nel backup. Come per il backup delle performance, i sette giorni più recenti di dati di integrazione sono inclusi nel backup. Tutti i dati di integrazione presenti in un backup vengono ripristinati durante un'operazione di ripristino.

Licenze

Per la segnalazione dei dati di integrazione è necessaria una licenza Perform. Se non è presente una licenza Perform, viene visualizzato il messaggio "Perform License required to report Integration data" (eseguire la licenza richiesta per i dati di integrazione).

Raccolta dei dati di integrazione SNMP

L'origine dati SNMP di integrazione consente di raccogliere dati SNMP generici in OnCommand Insight.

Pacchetti di integrazione

L'origine dati di integrazione SNMP utilizza un "Integration Pack" per definire i valori di integrazione raccolti e gli oggetti SNMP che forniscono tali valori.

Un pacchetto di integrazione è costituito da:

- Un file di configurazione JSON (Integration.json) che definisce il contenuto del payload di integrazione in termini di oggetti SNMP di un tipo di dispositivo specifico (switch, router e così via).
- Un elenco di file MIB da cui dipende il pacchetto di integrazione.

Un pacchetto di integrazione può definire diversi tipi di dati. Ad esempio, quando si integra un host RHEL, è possibile definire un tipo di dati per le informazioni generali del sistema, come l'uptime, il numero di utenti e il numero di processi in esecuzione, è possibile definire un secondo tipo di dati per i dati sulla memoria e sull'utilizzo del file system. In generale, ogni tipo di dati deve essere "flat" e non può contenere dati nidificati.

Un singolo pacchetto di integrazione non deve definire più di 24 tipi di dati. Insight limita la quantità di dati di integrazione raccolti. Se si tenta di acquisire più di 24 report in un periodo di un minuto, si verifica un errore di velocità.

I nomi dei tipi di integrazione devono rispettare le seguenti regole:

- Il nome non può iniziare con i seguenti caratteri: _, -, o,+
- Il nome non può contenere i seguenti caratteri: N., /, *, ?, ", <, >, |, ' , `,
- Non può superare i 100 byte codificati UTF-8
- Non può essere nominato . oppure ..

Formato del file di integrazione

Un pacchetto di integrazione è un file ZIP che contiene un file di configurazione JSON (Integration.json) che definisce il contenuto del payload di integrazione in termini di oggetti SNMP. Contiene anche una cartella MIBS che contiene tutti i file MIB e le relative dipendenze MIB.

Il `integration.json` Il file deve esistere al livello superiore del file ZIP e i file MIB devono esistere nella sottodirectory "resources/mib" all'interno del file ZIP. Il file ZIP può anche contenere file, ad esempio "readme.txt", se necessario. Un esempio di struttura ZIP di integrazione è:

```
.
├── integration.json
└── resources
    └── mibs
        ├── IANAifType-MIB.txt
        ├── IF-MIB.txt
        ├── INET-ADDRESS-MIB.txt
        ├── IP-MIB.txt
        ├── RFC1155-SMI.txt
        ├── RFC-1212.txt
        ├── RFC1213-MIB.txt
        ├── SNMPv2-CONF.txt
        ├── SNMPv2-MIB.txt
        ├── SNMPv2-SMI.txt
        ├── SNMPv2-TC.txt
        └── TCP-MIB.txt
```

Importazione di pacchetti di integrazione SNMP

I pacchetti di integrazione SNMP vengono importati in OnCommand Insight utilizzando l'interfaccia utente Web. I pacchetti di integrazione sono identificati dal valore "IntegrationPackName" definito in `integration.json` File di configurazione contenuto nel file ZIP.

Prima di iniziare

È necessario aver creato un file ZIP formattato correttamente che contenga il pacchetto di integrazione che si desidera importare nel server OnCommand Insight.

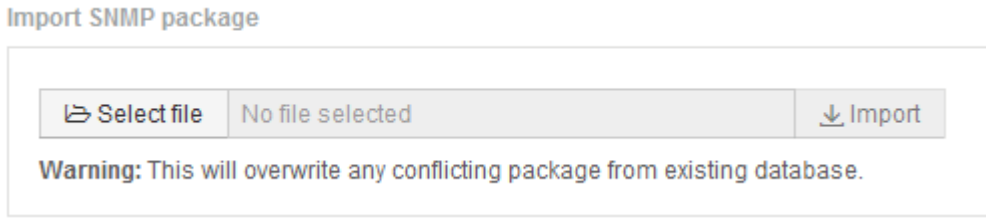
A proposito di questa attività

Per importare i pacchetti di integrazione SNMP nel server Insight, procedere come segue.

Fasi

1. Fare clic su **Admin** > **Setup** > **SNMP Integration**

   Viene visualizzata la schermata Import SNMP package (Importa pacchetto SNMP):

2. Fare clic su **Select file** (Seleziona file) per selezionare il file locale contenente il pacchetto SNMP.

Il file selezionato viene visualizzato nella casella file.

> Qualsiasi pacchetto di integrazione esistente con lo stesso nome viene sovrascritto.

3. Fare clic su **Importa**

   Il file viene importato nel server Insight.

Creazione di un'origine dati di integrazione SNMP

L'origine dati SNMP di integrazione fornisce proprietà di configurazione SNMP comuni simili ad altre origini dati basate su SNMP incluse con le origini dati OnCommand Insight per Brocade e Cisco.

Prima di iniziare

Per utilizzare correttamente l'origine dati SNMP di integrazione per la raccolta, devono essere vere le seguenti condizioni:

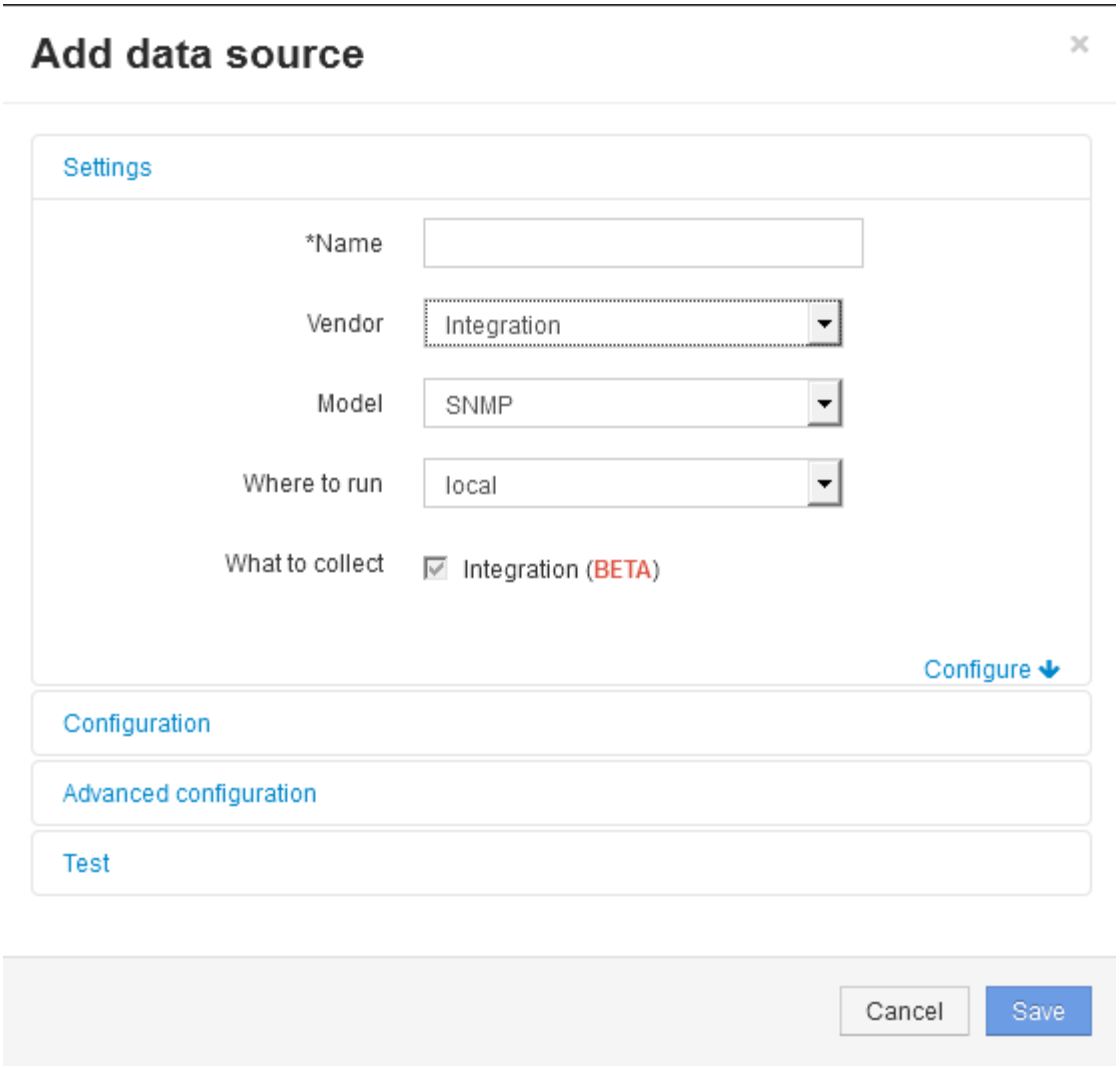
- È necessario aver già importato un pacchetto di integrazione da utilizzare per questa origine dati SNMP.
- Tutti i dispositivi di destinazione condividono le stesse credenziali.
- Tutti i dispositivi di destinazione implementano gli oggetti SNMP a cui fa riferimento il pacchetto di integrazione configurato.

A proposito di questa attività

Per creare un'origine dati di integrazione SNMP, scegliere il vendor "Integration" (integrazione) e il modello "SNMP" nella creazione guidata dell'origine dati.

Fasi

1. Nell'interfaccia utente Web di OnCommand Insight, fare clic su **Amministratore** > **origini dati**
2. Fare clic su **+Aggiungi**
3. Immettere un nome per l'origine dati
4. Per Vendor (fornitore), selezionare **Integration** (integrazione)
5. Per modello, selezionare **SNMP**



6. Per cosa raccogliere, selezionare **integrazione**

   Questo è l'unico pacchetto su questa origine dati ed è selezionato per impostazione predefinita:

7. Fare clic su **Configuration** (Configurazione)
8. Inserire gli indirizzi IP dei sistemi da cui si desidera raccogliere i dati SNMP
9. Selezionare un SNMP Integration Pack importato
10. Impostare l'intervallo di polling dell'integrazione
11. Selezionare la versione SNMP
12. Immettere la stringa di comunità SNMP

    Per SNMP V1 e V2.

13. Aggiungere il nome utente e la password per i sistemi da cui verranno raccolti i dati.

    Per SNMP V3.

14. Fare clic su **Advanced Configuration** (Configurazione avanzata)

    Vengono visualizzate le impostazioni predefinite della configurazione avanzata. Apportare le modifiche necessarie a queste impostazioni.

Informazioni sul file Integration.json

Il file Integration.json identifica il payload .

La seguente illustrazione fornisce una rappresentazione codificata a colori di un semplice file Integration.json. La tabella allegata identifica la funzione degli oggetti nel file.

```
{
 "integrationPackName": "WindowsSnmp",
 "description": "Generic integration for mibs supported by the default
SNMP  Agent for Windows 2012, including HOST-RESOURCES",
 "acquisitionType": "SNMP",
 "integrationTypes": [
  {
   "integrationType":      "snmp_win2012_host",
   "name": {
    "mibModuleName":     "RFC1213-MIB",
    "objectName":       "sysName"
   },
   "identifiers": {
    "hostname": {
     "mibModuleName":     "RFC1213-MIB",
    }
   },
   "attributes": {
    "description": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":       "sysDescr"
    },
    "snmp_sys_obj_id": {
     "mibModuleName":     "RFC1213-MIB",
     "objectName":       "sysObjectID"
    }
   },
   "dataPoints": {
    "uptime": {
     "num": {
      "mibModuleName":   "RFC1213-MIB",
      "objectName":      "sysUpTime"
     }
    }
   }
  }]}
```

Blue	Reserved
Red	User customizable strings and IDs
Green	MIB names
Purple	MIB object
Black	JSON structure

Informazioni sui file Integration.json

Ciascun campo presenta le seguenti caratteristiche:

- La sezione "identificatori" forma una chiave composta univoca per creare un nuovo "oggetto" in Insight
- Gli "attributi" forniscono metadati di supporto relativi all'oggetto.

In entrambi i casi, viene conservato solo il valore dell'ultimo report per l'oggetto (identificato dagli identificatori).

- I "datapoint" sono dati di serie temporali e devono essere valori numerici. Insight mantiene ogni valore riportato qui per 90 giorni (per impostazione predefinita) e li collega all'oggetto identificato.

Espressioni numeriche

Per impostazione predefinita, tutte le espressioni di valore vengono riportate come stringhe nel payload di integrazione. gli "identificatori" e gli "attributi" possono definire solo valori di stringa. I "datapoint" possono definire valori numerici o di stringa. I valori numerici vengono definiti utilizzando uno dei seguenti tasti modificatori:

- num - numero totale di byte ricevuti dall'ultima inizializzazione del contatore
- delta - il numero di byte ricevuti durante l'intervallo di polling
- rate (tasso) - la velocità di ricezione media durante l'intervallo di polling in byte al secondo

  È possibile ottenere una velocità di ricezione media in megabyte al secondo durante l'intervallo di polling utilizzando una combinazione di velocità e operazioni matematiche

Operazioni matematiche

Il `integration.json` il file supporta le seguenti operazioni matematiche: aggiungere, sottrarre, moltiplicare, dividere. Nell'esempio seguente vengono illustrate le operazioni di moltiplicazione, divisione e somma in un file JSON.

```
"network_utilization":
{
  "mult": [
    {
      "div": [
        {
          "sum": [
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCOutOctets",
              "comment":        "bytes per second out"
            },
            "rate": {
              "mibModuleName":  "IF-MIB",
              "objectName":     "ifHCInOctets",
              "comment":        "bytes per second in"
            }
          ]
        },
        {
          "num": {
            "mibModuleName":  "IF-MIB",
            "objectName":     "ifSpeed",
            "comment":        "1,000,000 bits per second"
          }
        }
      ]
    },
    {
      "const":                0.0008,
      "comment":        "normalize to ratio of bits and convert to percent:
                        8 * 100 / 1,000,000 = 0.0008"
    }
  ]
}
```

Parole chiave

Una parola chiave del pacchetto di integrazione, string, viene implementata per forzare le stringhe DI OTTETTI o i tipi proprietari derivati da UNA STRINGA DI OTTETTI che normalmente sarebbe rappresentata in formato esadecimale per essere invece rappresentata come caratteri ASCII.

Spesso le stringhe DI OTTETTI contengono dati binari, ad esempio indirizzi MAC e WWN:

```
        "interface_mac": {
                  "mibModuleName":      "IF-MIB",
                  "objectName":         "ifPhysAddress"
                 }
```

IfPhysAddress è di tipo PhysAddress, che è solo una STRINGA DI OTTETTI:

```
  PhysAddress ::= TEXTUAL-CONVENTION
                DISPLAY-HINT "1x:"
                STATUS       current
                DESCRIPTION
                               "Represents media- or physical-level
addresses."
                SYNTAX       OCTET STRING
```

Quando ifPhysAddress viene visualizzato come esadecimale per impostazione predefinita, il risultato è:

```
"interface_mac": "00:50:56:A2:07:E7"
```

Tuttavia, se si dispone di UNA STRINGA DI OTTETTI o di un tipo proprietario derivato dalla STRINGA DI OTTETTI che si desidera interpretare come ASCII, è possibile utilizzare la parola chiave "string":

```
        "string_test_1": {
          "string": {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
          }
        },

        "string_test_2": {
          "string": [
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            },
            {
              "const": "JSD"
            },
            {
              "mibModuleName":      "IF-MIB",
              "objectName":         "ifPhysAddress"
            }
          ]
        }
```

La parola chiave segue le regole di concatenazione delle stringhe esistenti, inserendo un singolo spazio tra i termini nel seguente esempio:

```
      "string_test_1": "PV¢ç",
              "string_test_2": "PV¢ç JSD PV¢ç"
```

La parola chiave "string" agisce su un singolo termine o su un elenco di termini, ma non su espressioni nidificate. Le espressioni nidificate sono supportate solo per le espressioni datapoint. Se si tenta di utilizzare un'espressione "stringa" in un'espressione datapoint, si verificherà un errore simile al seguente:

_java.lang.IllegalArgumentException: Integration pack 'GenericSwitch32' index 'nmp_generic_interface_32' sezione chiave 'daPoints' 'string_test_3' espressione numerica JSON '{"string":{"mibModuleName":"IF-MIB","objectName":"ifPhysAddress"}}'

Alcuni tipi di STRINGA DI OTTETTI derivati, come DisplayString, SnmpAdminString, hanno la precedenza hard-coded sulla parola chiave "string". Questo perché SnmpAdminString è specificamente codificato in UTF-8 e vogliamo gestirlo correttamente, mentre la parola chiave "string" forza la rappresentazione della stringa predefinita restituita da snmp_Framework, che presuppone punti di codice ascii a byte singolo per carattere.

Analisi di un problema di performance applicativa

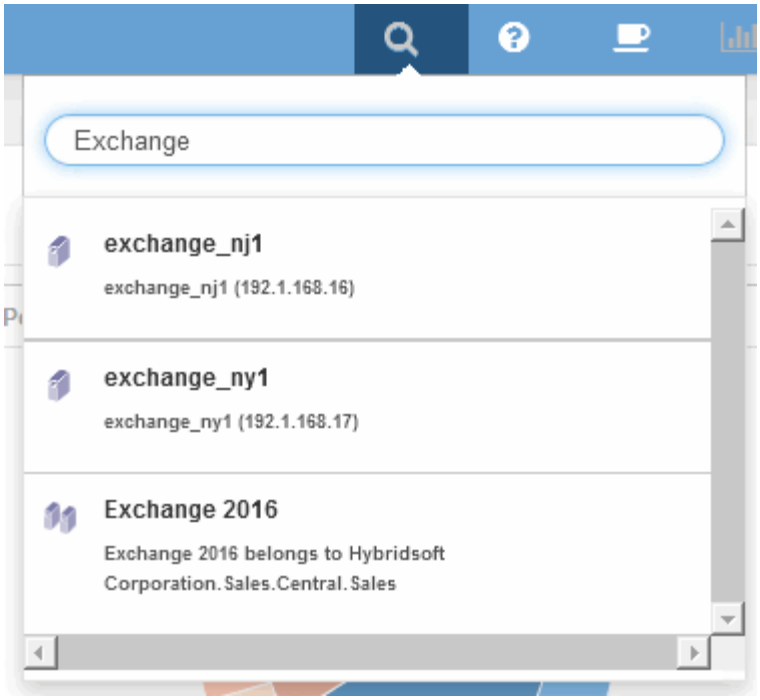
Questo documento descrive le operazioni che è possibile eseguire per risolvere i report relativi a problemi di performance di un'applicazione che hanno un impatto su utenti o amministratori. Ad esempio, gli utenti si lamentano del fatto che l'applicazione Exchange sta attraversando periodi di lentezza durante la giornata.

A proposito di questa attività

In OnCommand Insight, un'applicazione è un'entità configurata. Si assegnano un nome e un'entità aziendale all'applicazione e si assegnano risorse di calcolo e storage all'applicazione. Ciò consente una migliore visione end-to-end dello stato dell'infrastruttura e una gestione più proattiva della gestione delle risorse dell'infrastruttura.

Fasi

1. Per iniziare a esaminare il problema, utilizzare la barra degli strumenti Insight per eseguire una ricerca globale dell'applicazione Exchange.



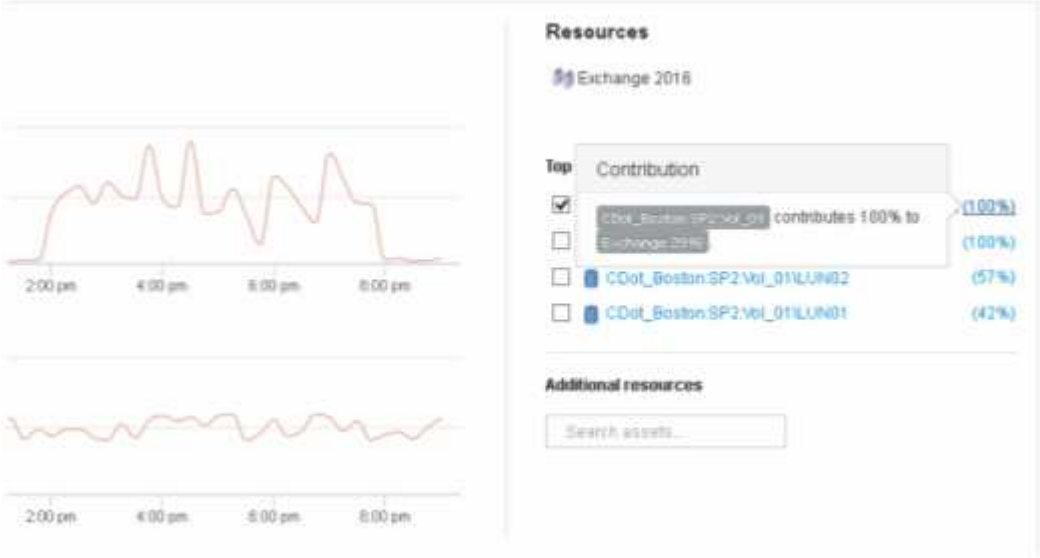
Quando si esegue una ricerca, è possibile aggiungere un descrittore di oggetti prima del nome dell'oggetto per perfezionare i risultati della ricerca.

2. Quando si seleziona "Exchange 2016" dai risultati della ricerca, viene visualizzata la pagina di destinazione dell'applicazione.

Nella landing page dell'applicazione sono disponibili le seguenti informazioni:

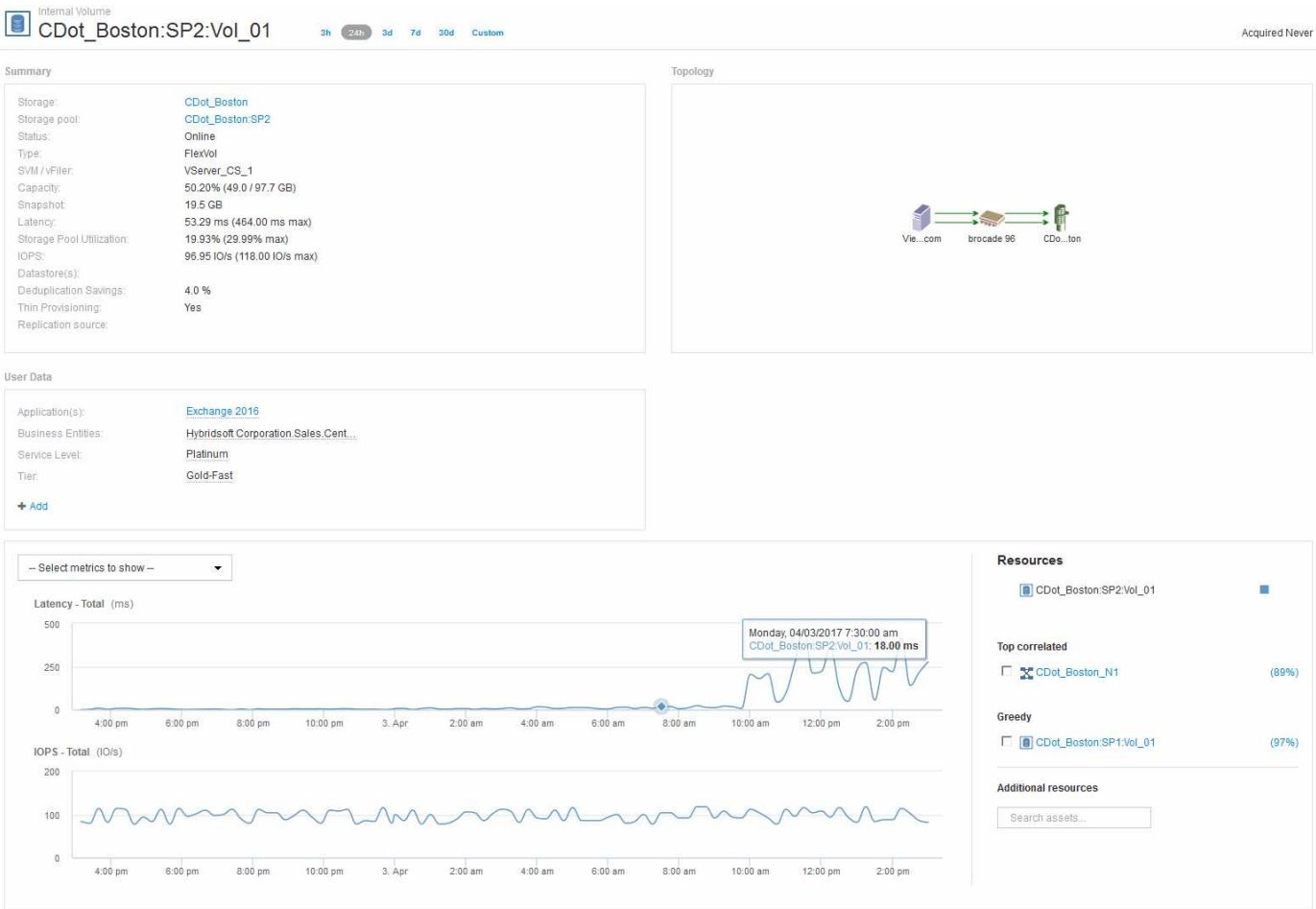
- Nel periodo di tempo di 24 ore selezionato, un aumento della latenza viene mostrato a destra del grafico della latenza.

- Durante il periodo di maggiore latenza non si verificano cambiamenti significativi nel livello di IOPS. Sembra che l'aumento della latenza non sia causato da un utilizzo più pesante delle applicazioni. Non stiamo riscontrando un'elevata domanda di IOPS sullo storage che potrebbe rappresentare il picco di latenza. L'aumento della latenza potrebbe essere dovuto a un fattore esterno.
- A destra dei grafici nella sezione Top Contributors (collaboratori principali), fare clic sul 100% per il volume interno selezionato (CDot_Boston:SP2:Vol_01). Il sistema mostra che questa risorsa contribuisce al 100% all'applicazione Exchange 2016.



- Fare clic sul collegamento di navigazione per questo volume interno (CDot_Boston:SP2:Vol_01) per accedere alla landing page del volume interno. L'analisi del volume interno potrebbe fornire informazioni relative al picco di latenza.

Esame del volume interno



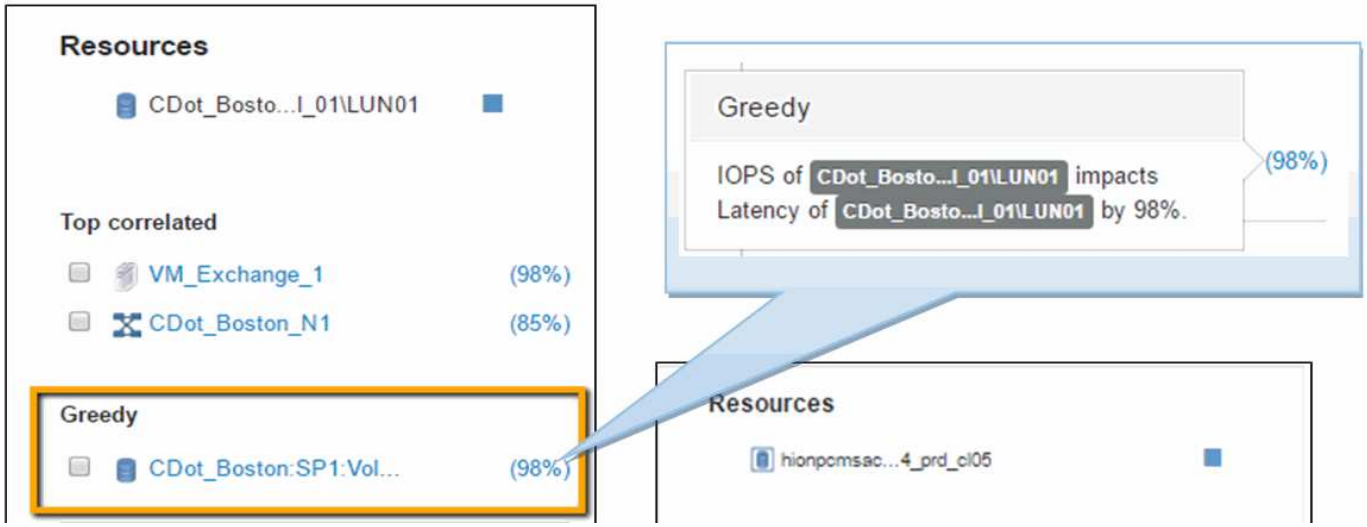
Nella landing page del volume interno, viene visualizzato:

- I grafici delle performance per il volume interno corrispondono a quanto osservato in precedenza per le performance applicative sia per la latenza che per gli IOPS.
- Nella sezione Resources (risorse), dove vengono visualizzate le risorse correlate, viene identificata una risorsa “greedy” (CDot_Boston:SP1:Vol_01).

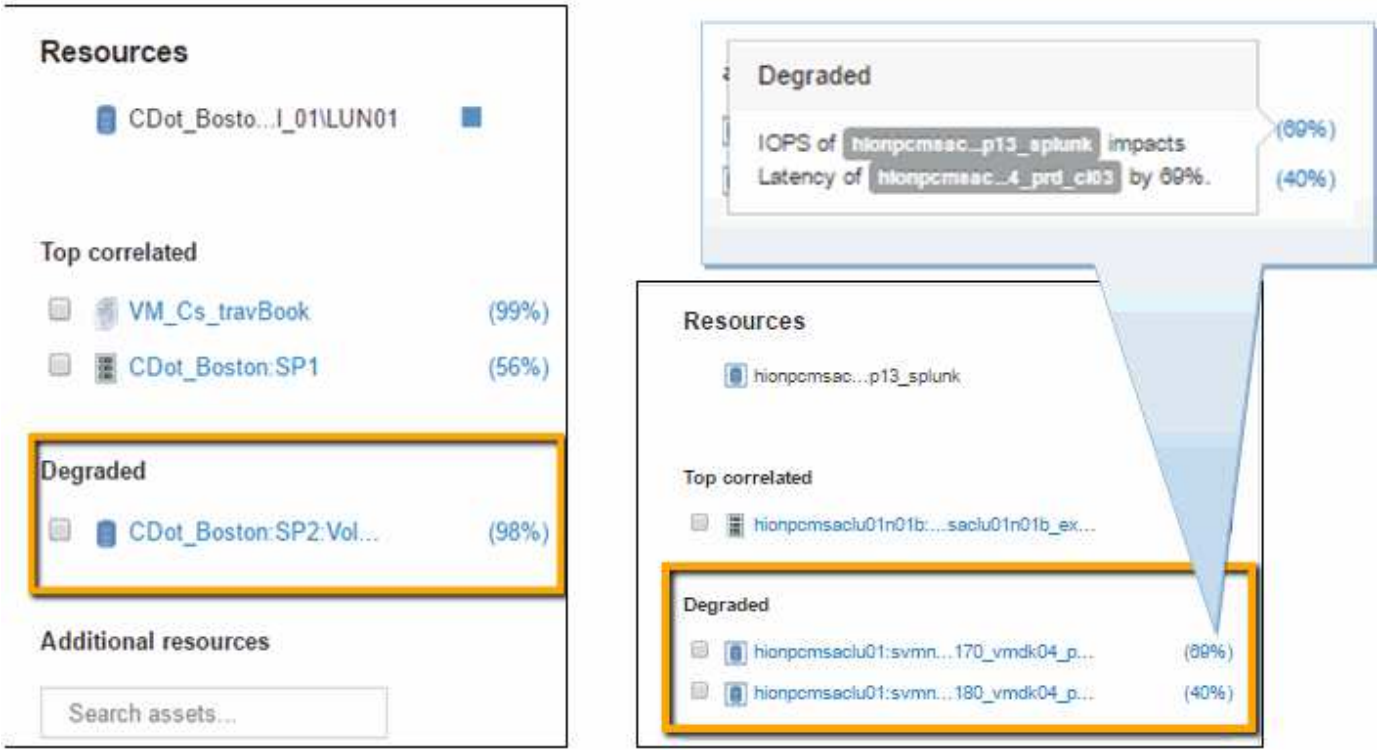
Una risorsa avida è identificata da analytics di correlazione di Insight. Le risorse avide/degradate sono “peer” che utilizzano la stessa risorsa condivisa. La risorsa avida ha IOPS o tassi di utilizzo che influiscono negativamente sugli IOPS o sulla latenza della risorsa degradata.

Le risorse greedy e degradate possono essere identificate nelle landing page di macchine virtuali, volumi e volumi interni. Su ciascuna landing page verranno visualizzate al massimo due risorse utili.

La selezione della classifica di correlazione (%) fornisce i risultati più avidi dell’analisi delle risorse. Ad esempio, facendo clic su un valore percentuale di riferimento si identifica l’operazione su una risorsa che influisce sull’operazione sulla risorsa degradata, in modo simile a quanto illustrato nell’esempio seguente.



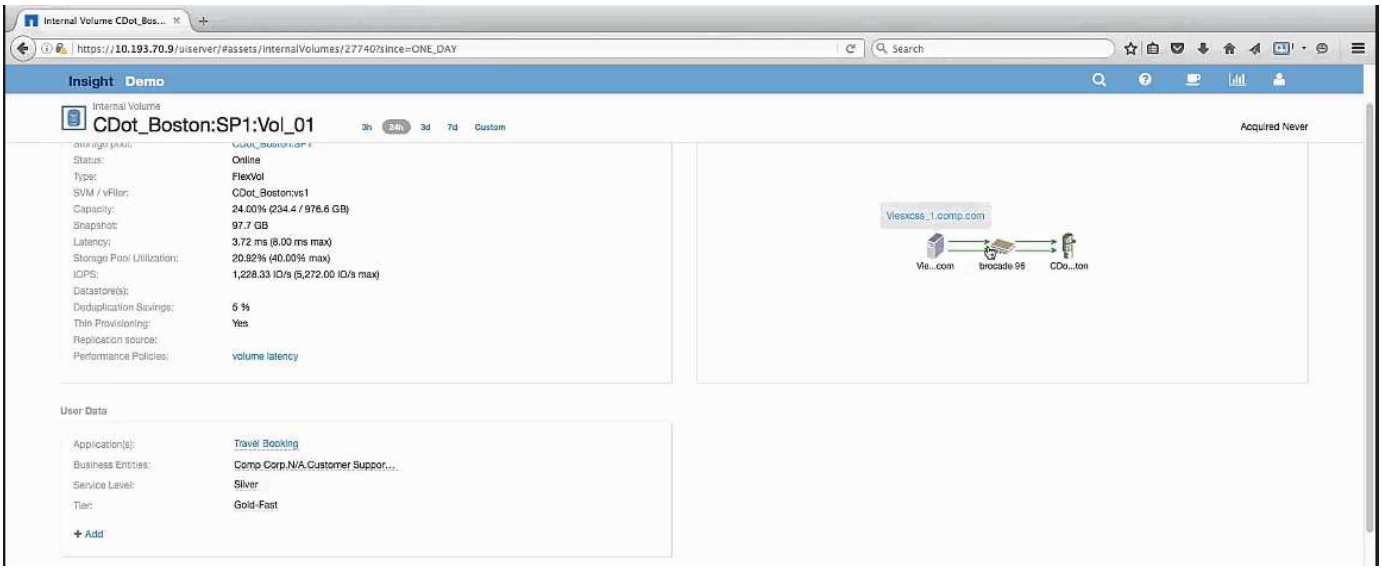
Quando viene identificata una risorsa degradata, è possibile selezionare il punteggio degradata (%) per identificare l'operazione e la risorsa che ha un impatto sulla risorsa degradata.



Esaminare la risorsa avida

Facendo clic sul volume interno identificato come risorsa avida si apre la landing page del volume CDot_Boston:SP1:Vol_01.

Nota nei dettagli riepilogativi, questo volume interno è una risorsa per un'applicazione diversa (Travel Booking) e, sebbene contenuto in un pool di storage diverso, si trova sullo stesso nodo del volume interno per Exchange 2016 (CDot_Boston_N1)



La landing page mostra:

- Volume interno associato a un'applicazione Travel Booking.
- Un nuovo pool di storage viene identificato nelle risorse correlate.
- Il volume interno originale che si stava esaminando (CDot_Boston:SP2:Vol_01) è identificato come "Degraded".
- Nel grafico delle performance, l'applicazione ha un profilo di latenza costante e presenta un picco IOPS all'incirca nello stesso momento in cui vediamo il picco di latenza sull'applicazione Exchange.

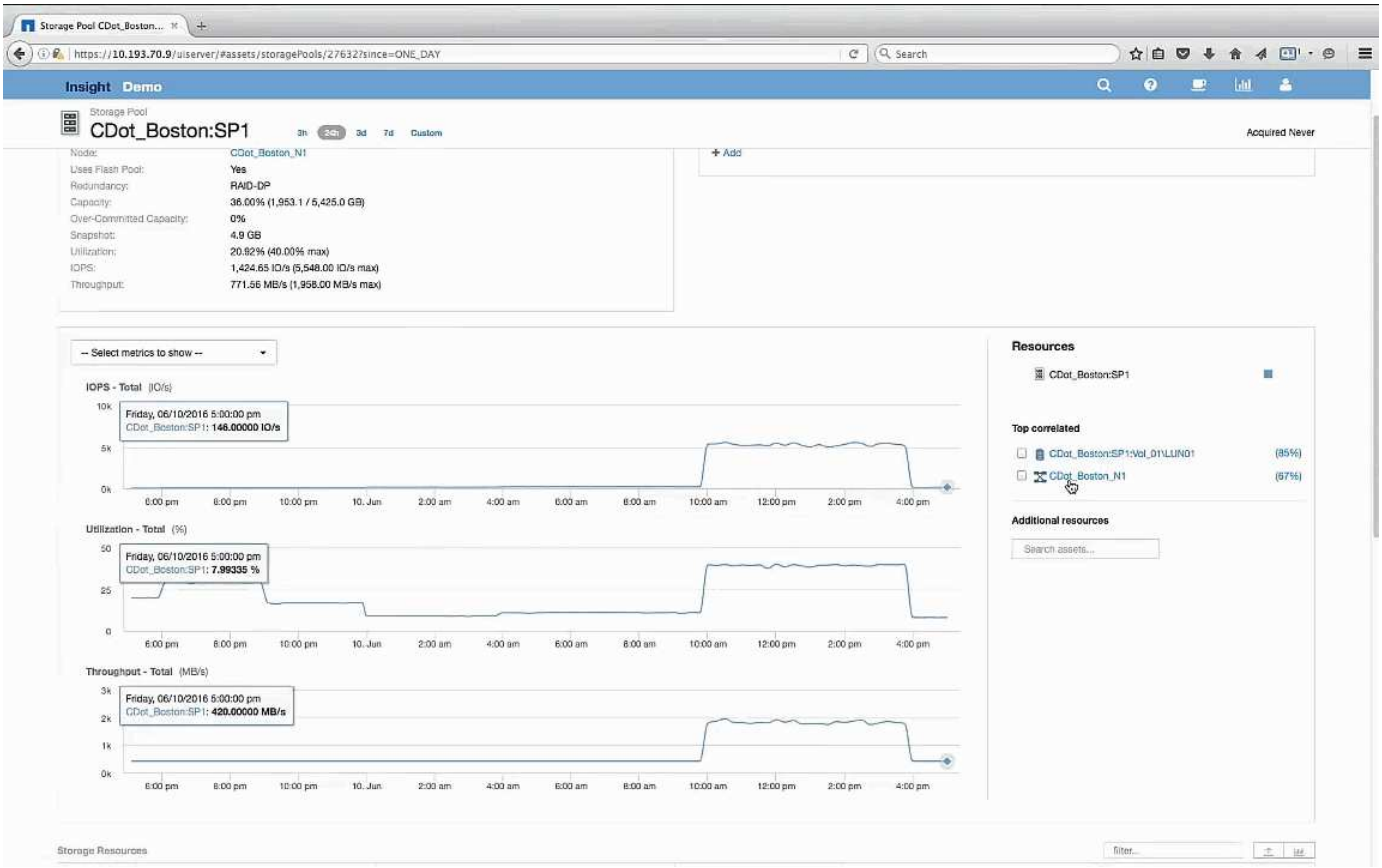
  Questo potrebbe indicare che il picco di latenza nell'applicazione Exchange è probabilmente causato dal picco IOPS su questo volume.

A destra dei grafici nella sezione Resource, notare la risorsa degradata correlata, ovvero il volume interno di Exchange 2016 (CDot_Boston:SP2:Vol_01). Fare clic sulla casella di controllo per includere il volume interno degradato nel nei grafici delle prestazioni. L'allineamento dei due grafici delle performance mostra che i picchi di latenza e IOPS si verificano quasi esattamente allo stesso tempo. Questo ci dice che vogliamo avere una migliore comprensione dell'applicazione Travel Booking. Dobbiamo capire perché l'applicazione sta riscontrando un picco di IOPS così prolungato.

L'esame del pool di storage associato all'applicazione Travel Booking potrebbe identificare il motivo per cui l'applicazione sta riscontrando il picco IOPS. Fare clic su CDot_Boston:SP1 per visualizzare la landing page dello Storage Pool.

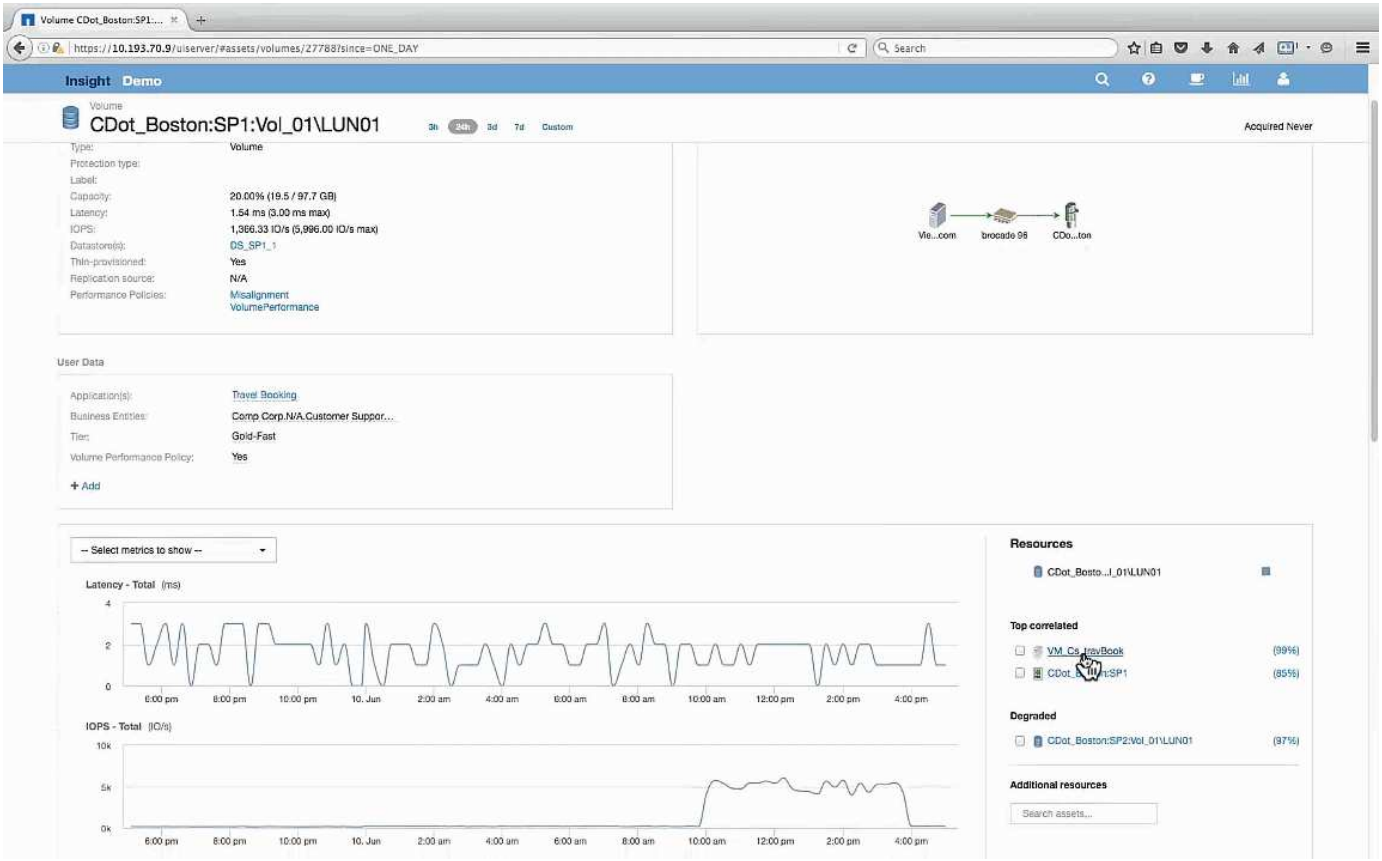
Esaminare il pool di storage

L'esame della landing page del pool di storage mostra lo stesso picco IOPS riscontrato nelle risorse correlate. Nella sezione risorse è possibile vedere che questa landing page del pool di storage si collega al volume dell'applicazione di viaggio. Fare clic sul volume per aprire la landing page del volume.



Esame del volume

La landing page del volume mostra lo stesso picco IOPS familiare riscontrato nelle risorse correlate.



Nella sezione delle risorse viene identificata la VM per l'applicazione Travel Booking. Fare clic sul collegamento VM per visualizzare la landing page delle macchine virtuali.

Esame della macchina virtuale

Nella landing page delle macchine virtuali, selezionare le metriche aggiuntive da visualizzare e includere l'utilizzo della CPU e della memoria. I grafici relativi all'utilizzo della CPU e della memoria mostrano che entrambi operano a quasi il 100% della capacità. Questo ci indica che il problema del server Exchange non è un problema di storage, ma è il risultato dell'elevato utilizzo della CPU e della memoria delle macchine virtuali e del conseguente scambio di memoria tra i/o e disco.

Per risolvere questo problema, è possibile cercare ulteriori risorse simili. Immettere “Node” nella finestra di dialogo di immissione delle risorse aggiuntive per visualizzare le metriche relative alle risorse simili alla VM Exchange. Il confronto può aiutare a identificare un nodo che potrebbe essere più adatto per ospitare il carico di lavoro in caso di necessità di una modifica.

Raccolta e reporting dei dati di fatturazione AWS

L’origine dati dei costi Amazon AWS Cloud importa i dati di fatturazione generati da Amazon in Insight come dati di integrazione, rendendolo disponibile per il data

warehouse per il reporting.

I dati di fatturazione del cloud sono disponibili per Insight in tre parti:

Verifica delle informazioni dell'account AWS.

Configurazione dell'origine dati dei costi AWS Cloud in Insight per la raccolta dei dati.

Invio dei dati al Data Warehouse tramite ETL per l'utilizzo nei report.

Preparazione di AWS per la raccolta di dati Insight

L'account AWS deve essere configurato correttamente per consentire a Insight di raccogliere dati sui costi del cloud.

A proposito di questa attività

I seguenti passaggi vengono eseguiti tramite l'account AWS. Per ulteriori informazioni, consulta la documentazione di Amazon: "http://docs.aws.amazon.com". Se non conosci la configurazione di un account cloud AWS, contatta il tuo cloud provider per ricevere assistenza.

> Questi passaggi sono forniti qui a titolo di cortesia e sono ritenuti corretti al momento della pubblicazione. NetApp non garantisce la correttezza di questi passaggi. Per informazioni o assistenza sulla configurazione dell'account AWS, contattare il provider cloud o il titolare dell'account AWS.

Best practice: Insight consiglia di creare un utente IAM primario sullo stesso account proprietario del bucket S3 in cui vengono caricati i report di fatturazione e di utilizzarlo per configurare e raccogliere i dati di fatturazione AWS.

Per configurare l'account AWS in modo da consentire a Insight di raccogliere dati, attenersi alla seguente procedura:

Fasi

1. Accedere al proprio account AWS come utente IAM (Identity Access Management). Per ottenere una raccolta corretta, accedere all'account IAM principale, invece di un account IAM di gruppo.
2. Vai su **Amazon S3** per creare il tuo bucket. Immettere un nome bucket univoco e verificare la regione corretta.
3. Attiva Amazon Cost and Usage Report. Vedere https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html per informazioni.
   a. Vai alla sezione AWS **Billing and Cost Management Dashboard**e scegli **Report**.
   b. Fare clic su **Create report** (Crea report) e immettere il nome del report. Per **unità di tempo**, scegliere giornaliera. Selezionare la casella per includere **ID risorsa**, quindi fare clic su **Avanti**.
   c. Fare clic sul collegamento **Sample Policy** nella pagina Select delivery options. Copiare il testo della policy di esempio nella casella negli Appunti. Fare clic su **Chiudi**.
   d. Tornare al bucket S3 creato, fare clic sulla scheda **Permissions** e selezionare il pulsante **Bucket Policy**.
   e. Incollare il testo dalla policy di esempio e sostituirlo `<bucketname>` con il nome effettivo del bucket in ogni riga che contiene quanto segue: `"Resource": "arn:aws:s3:: <bucketname>"`. **Salvare** la

policy.

f. Tornare alla schermata Create Report (Crea report), inserire il bucket S3 e fare clic sul pulsante **Verify** (verifica). Fare clic su **Avanti**.

g. Verificare le informazioni e fare clic su **Rivedi e completa**.

4. Per consentire a Insight di raccogliere i dati da AWS, è necessario concedere le autorizzazioni. Il seguente collegamento fornisce informazioni dettagliate su come concedere le autorizzazioni a **Elenca tutti i bucket** (fase 4.1) e impostare le autorizzazioni sugli oggetti nella cartella (fase 5.2): https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html.
5. Nella console IAM, selezionare **Policy** e fare clic su **Create policy**.
6. Immettere un nome nel campo **Policy Name** (Nome policy) e fare clic su **Create policy** (Crea policy) in basso.
7. Nella console di IAM, selezionare l'utente, quindi selezionare **Add Inline Policy** (Aggiungi policy in linea) nella parte inferiore della schermata.
8. Fare clic su **Scegli un servizio** e selezionare S3.
9. Selezionare la scheda **JSON**. Copiare il testo di esempio JSON dal punto 5.1.2.g della procedura dettagliata AWS nella casella JSON.
10. Sostituire i campi *companybucket* e *Development* in JSON con le informazioni S3.
11. Fare clic su **Review Policy** (esamina policy) per rivedere le impostazioni dei criteri.

Configurazione dell'origine dati dei costi di AWS Cloud

Configuri l'origine dati dei costi di AWS Cloud come per qualsiasi origine dati Insight.

Prima di iniziare

Devi avere il tuo account Amazon AWS già configurato e preparato per la raccolta dati Insight e avere a portata di mano le seguenti informazioni.

- Nome report
- Nome bucket S3
- Regione AWS in cui risiede il bucket S3.
- Prefisso del percorso del report

A proposito di questa attività

Una volta che l'account AWS è pronto e sono state impostate le autorizzazioni appropriate, è possibile configurare OnCommand Insight per la raccolta dei dati dei report di fatturazione.

> Sarà necessario aggiungere un'origine dati dei costi AWS Cloud separata per ciascun utente/account fatturabile da cui si desidera recuperare i dati di fatturazione.

Fasi

1. Accedere a OnCommand Insight come amministratore.
2. Fare clic su **Admin** > **Data Sources** per aprire la pagina Insight Data Source.
3. Fare clic su **+Aggiungi** per aggiungere una nuova origine dati. Scegliere **Amazon** e selezionare **AWS Cloud Cost**.

4. Nella sezione **Configurazione**, compilare i campi *Nome report*, *Nome bucket S3*, *Regione S3* (deve essere la regione in cui si trova il bucket S3), *prefisso percorso report*, *ID chiave di accesso IAM AWS* e *chiave di accesso segreta IAM AWS*. In caso di dubbi, rivolgersi al proprio provider di servizi cloud o al titolare dell'account AWS.
5. Fare clic sulla casella di controllo per verificare che AWS fatturare le richieste API e i trasferimenti di dati effettuati dall'origine dati Insight.
6. In **Advanced Configuration** (Configurazione avanzata), inserire la connessione HTTP e il timeout socket. L'impostazione predefinita è 300 secondi.
7. Fare clic su **Save** (Salva).

Elaborazione dei dati dei costi di AWS Cloud in Insight

Insight raccoglie i dati dal report di fatturazione AWS una volta al mese per il mese precedente e riflette il costo del cloud finalizzato per quel mese.

Dopo aver configurato le origini dati dei costi di AWS Cloud, se sono già stati generati report di fatturazione su S3, si otterranno fino a tre mesi di dati passati subito dopo il primo sondaggio dell'origine dati.

Insight raccoglie i dati "final" di AWS una volta al mese. Questa raccolta avviene alcuni giorni dopo la chiusura del mese precedente, consentendo ad AWS di finalizzare i dati effettivi.

I dati di fatturazione AWS vengono inviati al Data Warehouse di Insight per essere utilizzati nel reporting.

Tenere presente che ogni origine dati deve essere configurata per un singolo account/utente fatturabile.

Reporting sui dati dei costi del cloud in Insight

I dati mensili sui costi del cloud raccolti in Insight vengono inviati al data warehouse ed è disponibile nel datamart dei costi del cloud per l'utilizzo nei report.

Prima di iniziare

È necessario che le origini dati siano configurate per raccogliere i dati sui costi del cloud da AWS. Ogni utente/account fatturabile deve disporre di un'origine dati separata.

Consentire a Insight di iniziare la raccolta dei dati per almeno 36 ore.

Consentire l'esecuzione di ETL almeno una volta dopo tale periodo, per inviare i dati al data warehouse.

A proposito di questa attività

Una volta raccolti e inviati i dati al data warehouse, è possibile visualizzarli in uno dei diversi report preconfigurati o creare report personalizzati. Insight memorizza i dati nel proprio datamart Cloud Cost.

Per visualizzare i dati sui costi del cloud in uno dei report preconfigurati:

Fasi

1. Aprire Insight Reporting con uno dei seguenti metodi:
    - Fare clic sull'icona del portale di reporting Nell'interfaccia utente Web di Insight Server o nell'interfaccia utente di Data Warehouse.

- Avviare il reporting direttamente immettendo il seguente URL: `https://<dwh_server_name\>:9300/p2pd/servlet/dispatch` oppure `https://<dwh_server_name\>:9300/bi` (7.3.3 and later)

2. Una volta effettuato l'accesso a Reporting, fare clic su **cartelle pubbliche** e selezionare **costo cloud**.
3. È possibile visualizzare i dati di fatturazione di AWS nei report disponibili nella cartella **Cloud Cost** oppure creare un report personalizzato utilizzando il datamart * Cloud Cost disponibile nella cartella **Packages**.

Integrazione con ServiceNow

OnCommand Insight si integra con il software di gestione ServiceNow per offrire un valore maggiore rispetto ai prodotti separatamente.

Utilizzando uno script Python, Insight può integrare i dati con ServiceNow, sincronizzando le seguenti informazioni:

- Dati delle risorse di storage per i server ServiceNow
- URL host e VM per server ServiceNow
- Relazioni tra host/VM e storage

Preparazione e prerequisiti per l'integrazione di Service Now

Prima dell'integrazione, è necessario soddisfare i requisiti e i prerequisiti necessari per ServiceNow, Insight e il connettore middleware Python.

Workflow consigliato

Quando si integra ServiceNow con Insight, si consiglia vivamente di utilizzare il seguente flusso di lavoro:

1. Implementare prima il connettore middleware Python nell'istanza di sviluppo.
2. Una volta che tutti i guasti sono stati identificati e corretti nell'istanza di sviluppo, implementare il connettore nell'istanza di test/fase.
3. Una volta confermato il corretto funzionamento nell'istanza di staging, distribuire il connettore nell'istanza di produzione.

Se durante una di queste fasi vengono rilevati problemi, seguire la procedura di rollback e disattivare il connettore, quindi risolvere il problema e ridistribuire.

Prerequisiti generali:

- Per ospitare il connettore middleware python, è possibile utilizzare un host standalone o una macchina virtuale (scelta consigliata) o l'host/macchina virtuale del server Insight.
- Si consiglia vivamente di eseguire il backup del server Insight di produzione e di implementarlo in un'istanza di sviluppo.
- ServiceNow deve rilevare con precisione i server nel CMDB.
- Insight deve essere in grado di rilevare con precisione i tuoi ambienti di storage e calcolo.
- Porta 443 e 80 per Insight Server e ServiceNow Instance.

Prerequisiti di ServiceNow:

- Si consiglia vivamente di utilizzare un'istanza di sviluppo/test.
- Autorizzazione per caricare i set di aggiornamento ServiceNow.
- Permesso di creare utenti.
- ServiceNow versione Jakarta o successiva

Prerequisiti di Insight:

- Si consiglia vivamente di utilizzare un'istanza di sviluppo/test.
- Autorizzazione alla creazione di utenti (autorizzazioni di amministratore).
- Insight versione 7.3.1 o successiva è supportato, ma per ottenere il massimo da Insight, utilizza la versione più recente.

Prerequisiti del connettore middleware Python:

- Python versione 3.6 o superiore installato.
- Durante l'installazione di Python, selezionare la casella per abilitare tutti gli utenti. Questo imposta Python per le posizioni di installazione standard delle applicazioni.
- Durante l'installazione di Python, selezionare la casella per consentire al programma di installazione di aggiornare il percorso. In caso contrario, sarà necessario aggiornare il percorso manualmente.
- Scarica le librerie Python **pysnow** e **Requests**.

Download del connettore Python ServiceNow

È necessario scaricare l'integrazione di Python Connector for ServiceNow ed estrarla in una posizione a propria scelta.

Fasi

1. Scaricare il connettore di integrazione * ServiceNow dal "NetApp Storefront".
2. Ad esempio, estrarre il file .zip in una cartella `c:\OCI2SNOW`.

   Lo script del connettore di integrazione viene denominato `oci_snow_sync.pyz`.

Configurazione di ServiceNow per l'integrazione

L'integrazione di ServiceNow con Insight richiede diverse attività di configurazione.

A proposito di questa attività

Quando si integra ServiceNow con Insight, è necessario eseguire le seguenti attività:

Sul lato ServiceNow:

- Elevare il ruolo
- Installare i set di aggiornamenti
- Configurare gli utenti

Dal punto di vista della Insight:

- Aggiungere l'utente ServiceNow

Sul lato del connettore Python:

- Installare Python
- Installare librerie aggiuntive
- Inizializzare il connettore
- Modificare il file config.ini
- Verificare il connettore
- Sincronizzare il connettore
- Pianificare l'esecuzione quotidiana delle attività

Ciascuno di questi elementi viene spiegato in maggiore dettaglio nelle sezioni seguenti.

Elevare il ruolo

Devi elevare il tuo ruolo ServiceNow a Security_admin prima di poter integrare con Insight.

Fasi

1. Accedere all'istanza di ServiceNow con le autorizzazioni di amministratore.
2. Nell'elenco a discesa **System Administrator** (Amministratore di sistema), selezionare **Elevate Roles** (Eleva ruoli) e elevare il proprio ruolo a Security_admin. Fare clic su OK.

Installare il set di aggiornamenti

Nell'ambito dell'integrazione tra ServiceNow e OnCommand Insight, è necessario installare un set di aggiornamenti, che carica i dati preconfigurati in ServiceNow per fornire al connettore campi e tabelle specifici per l'estrazione e il caricamento dei dati.

Fasi

1. Accedere alla tabella dei set di aggiornamenti remoti in ServiceNow cercando "set di aggiornamenti recuperati".
2. Fare clic su **Importa set di aggiornamenti da XML**.
3. Il set di aggiornamenti si trova nel file .zip di Python Connector precedentemente scaricato sul disco locale (nel nostro esempio, il `C:\OCI2SNOW`) in `\update_sets` sotto-cartella. Fare clic su **Choose file** (Scegli file) e selezionare il file .xml in questa cartella. Fare clic su **carica**.
4. Una volta caricato il set di aggiornamenti, aprirlo e fare clic su **Preview Update Set** (Anteprima set di aggiornamenti).

   Se vengono rilevati errori, è necessario correggerli prima di poter eseguire il commit del set di aggiornamenti.

5. Se non si verificano errori, fare clic su **Commit Update Set** (Esegui commit Update Set).

Una volta eseguito il commit, il set di aggiornamenti viene visualizzato nella pagina **System Update Sets** > **Update Sources**.

Integrazione di ServiceNow - impostazione dell'utente

Per consentire a Insight di connettersi e sincronizzare i dati, è necessario configurare un utente ServiceNow.

A proposito di questa attività

Fasi

1. Creare un account di servizi in ServiceNow. Accedere a ServiceNow e accedere a **sicurezza del sistema** > **utenti e gruppi** > **utenti**. Fare clic su **nuovo**.
2. Immettere un nome utente. In questo esempio, useremo "OCI2SNOW" come utente dell'integrazione. Immettere una password per questo utente.

> In questa procedura viene utilizzato un account utente dei servizi denominato "OCI2SNOW"`" nella documentazione. È possibile utilizzare un account di servizi diverso, ma assicurarsi che sia coerente con l'ambiente in uso.

3. Fare clic con il pulsante destro del mouse sulla barra dei menu e fare clic su **Save** (Salva). In questo modo, sarà possibile rimanere su questo utente per aggiungere ruoli.
4. Fare clic su **Edit** (Modifica) e aggiungere i seguenti ruoli a questo utente:
   - risorsa
   - importa_trasformatore
   - servizio_rest
5. Fare clic su **Save** (Salva).
6. Questo stesso utente deve essere aggiunto a OnCommand Insight. Accedere a Insight come utente con autorizzazioni di amministratore.
7. Accedere a **Admin** > **Setup** e fare clic sulla scheda **Users**.
8. Fare clic sul pulsante **azioni** e selezionare **Aggiungi utente**.
9. Per il nome, immettere "OCI2SNOW". Se si utilizza un nome utente diverso, immetterlo qui. Inserire la stessa password utilizzata per l'utente ServiceNow. È possibile lasciare vuoto il campo e-mail.
10. Assegnare a questo utente il ruolo **utente**. Fare clic su **Save** (Salva).

Installare Python e le librerie

Python può essere installato sul server Insight o su un host o una macchina virtuale standalone.

Fasi

1. Sulla macchina virtuale o sull'host, scaricare Python 3.6 o versione successiva.
2. Scegliere l'installazione personalizzata e scegliere le seguenti opzioni. Questi sono necessari per il corretto funzionamento dello script del connettore o sono altamente consigliati.
   - Installare il programma di avvio per tutti gli utenti

- Aggiungi Python al PERCORSO
- Installare pip (che consente a Python di installare altri pacchetti)
- Installare tk/tcl e IDLE
- Installare la suite di test Python
- Installare py launcher per tutti gli utenti
- Associare i file a Python
- Creare collegamenti per le applicazioni installate
- Aggiungere python alle variabili di ambiente
- Precompilare la libreria standard

3. Dopo aver installato Python, installa le librerie Python “requests” e “psnow”. Eseguire il seguente comando: `python -m pip install requests pysnow`

   NOTA: questo comando potrebbe non riuscire quando si opera in un ambiente proxy. Per risolvere questo problema, è necessario scaricare manualmente ciascuna delle librerie Python ed eseguire le richieste di installazione una alla volta e nell’ordine corretto.

   Il comando installerà diversi file.

4. Verificare che le librerie Python siano installate correttamente. Avviare Python utilizzando uno dei seguenti metodi:
   - Aprire un prompt cmd e digitare `python`
   - In Windows, aprire **Start** e scegliere **Python** > **python-<version>.exe**
5. Al prompt di Python, digitare `modules`

   Python ti chiederà di aspettare un attimo mentre raccoglie un elenco di moduli, che verrà visualizzato.

Installazione del middleware Python

Ora che Python e le librerie necessarie sono installate, è possibile configurare il connettore middleware per comunicare con OnCommand Insight e ServiceNow.

Fasi

1. Sull’host o sulla macchina virtuale in cui è stato scaricato il software Connector, aprire una finestra cmd come amministratore e passare a. `\OCI2SNOW\` cartella.
2. È necessario inizializzare lo script per generare un file **config.ini** vuoto. Eseguire il seguente comando: `oci_snow_sync.pyz init`
3. Aprire **config.ini**file in un editor di testo ed apportare le seguenti modifiche nella sezione [OCI]:
   - Impostare url su <code><a href="https://<name.domain&gt" class="bare">https://<name.domain&gt;</code> oppure <code><a href="https://<ip" class="bare">https://<ip address></code> Per l’istanza Insight.
   - Impostare **user** e **password** sull’utente Insight creato, ad esempio OCI2SNOW.
   - Impostare **include_off_vm** su **false**
4. Nella sezione [SNOW], apportare le seguenti modifiche:

- Impostare **Instance** sull'FQDN o sull'indirizzo ip dell'istanza di ServiceNow
- Impostare **User** e **Password** sull'utente dell'account di servizio ServiceNow, ad esempio OCI2SNOW.
- In **field for the OCI URL** (campo **URL** OCI), impostare il campo **url** su "u_oci_url". Questo campo viene creato come parte del set di aggiornamenti OCI del connettore. È possibile modificarlo nell'ambiente del cliente, ma in tal caso è necessario modificarlo qui e in ServiceNow. La Best practice consiste nell'abbandonare questo campo così com'è.
- Impostare il campo **filter_status** su "Installed, in Stock". Se si dispone di uno stato diverso, è necessario impostare questo stato qui per ottenere la corrispondenza di tutti i record con i record Insight prima di caricare nuovi record. Nella maggior parte dei casi, questo campo deve rimanere invariato.
- Impostare **stale_status**su "ritirata".

5. La sezione [Proxy] è necessaria solo se si utilizza un server proxy. Se è necessario utilizzare questa sezione, verificare le seguenti impostazioni:
   - ;https = http://<host>:<port>
   - ;http = http://<host>:<port>
   - ;Include_oci = vero
   - ;Include_snow = vero
6. Modificare la sezione [Log] solo se sono necessarie informazioni di debug più dettagliate.
7. Per verificare il connettore, aprire un prompt dei comandi come amministratore e passare alla cartella OCI2SNOW. Eseguire il seguente comando: `oci_snow_sync.pyz test`

   I dettagli sono disponibili nella `logs\` cartella.

Sincronizzazione del connettore

Una volta configurati correttamente ServiceNow, Insight e il connettore, è possibile sincronizzare il connettore.

Fasi

1. Aprire un prompt dei comandi e passare alla cartella OCI2SNOW.
2. Eseguire due volte il seguente comando. La prima sincronizzazione aggiorna gli elementi, la seconda aggiorna le relazioni: `oci_snow_sync.pyz sync`
3. Verificare che la tabella Storage Server nell'istanza di ServiceNow sia popolata. Aprire un server di storage e verificare che siano elencate le risorse correlate a tale storage.

Pianificazione della sincronizzazione giornaliera

È possibile utilizzare il Task Scheduler di Windows per sincronizzare automaticamente il connettore ServiceNow.

A proposito di questa attività

La sincronizzazione automatica garantisce che i dati Insight vengano regolarmente spostati in ServiceNow. È possibile utilizzare qualsiasi metodo per la pianificazione. La seguente procedura utilizza Task Scheduler di Windows per eseguire la sincronizzazione automatica.

Fasi

1. Nella schermata di Windows, fare clic su **Start** e digitare **Esegui** > **Task Scheduler**.
2. Fare clic su **Crea attività di base…**
3. Immettere un nome significativo, ad esempio “OCI2SNOW Connector Sync”. Inserire una descrizione dell’attività. Fare clic su **Avanti**.
4. Selezionare per eseguire l’attività **Daily**. Fare clic su **Avanti**.
5. Scegliere un’ora del giorno in cui eseguire l’attività. Fare clic su **Avanti**.
6. Per azione, selezionare **Avvia un programma**. Fare clic su **Avanti**.
7. Nel campo **Program/script**, immettere `C:\OCI2SNOW\oci_snow_sync_pyz`. Nel campo **argomenti**, immettere `sync`. Nel campo **Start in**, immettere `C:\OCI2SNOW`. Fare clic su **NEXT** (Avanti).
8. Esaminare i dettagli del riepilogo e fare clic su **fine**.

   La sincronizzazione è ora pianificata per essere eseguita quotidianamente.

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

http://www.netapp.com/us/legal/copyright.aspx

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

http://www.netapp.com/us/legal/netapptmlist.aspx

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/us/media/patents-page.pdf

Direttiva sulla privacy

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Avviso

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per OnCommand Insight 7.3.15"

"Avviso per OnCommand Insight 7.3.14"

"Avviso per OnCommand Insight 7.3.13"