Documentazione Cloud Insights

Cloud Insights

NetApp
April 16, 2024

Sommario

Documentazione Cloud Insights

NetApp Cloud Insights è uno strumento di monitoraggio dell'infrastruttura cloud che offre visibilità sull'intera infrastruttura. Con Cloud Insights, puoi monitorare, risolvere i problemi e ottimizzare tutte le risorse, inclusi i cloud pubblici e i data center privati.

Cosa può fare Cloud Insights per me?

Cloud Insights offre il monitoraggio multicloud ibrido, offrendo l'osservabilità completa dell'infrastruttura e dei carichi di lavoro.

- Raccolta di dati per infrastrutture e carichi di lavoro eterogenei, tra cui Kubernetes
- Aprire Telegraf Collector e aprire le API per una facile integrazione
- Avvisi e notifiche completi
- Apprendimento automatico per informazioni intelligenti
- Ottimizzare l'utilizzo delle risorse
- Dashboard integrate o personalizzabili con filtri avanzati per ridurre al minimo il rumore dello schermo per rispondere alle domande
- Scopri lo stato delle tue operazioni di storage ONTAP
- Proteggi la tua risorsa di business più preziosa, i dati, dagli attacchi ransomware o di distruzione dei dati

---

Per iniziare

- Come fare **"per iniziare"** Con Cloud Insights?
- Mi sono iscritto. Cosa devo fare?"Acquisizione dei dati"
  "Configurazione degli utenti"
- Fantastico! Quali sono le prossime novità?"Preparazione delle risorse: Annotazione"
  "Trovare le risorse desiderate: Eseguire query"
  "Visualizzazione dei dati desiderati: Dashboard"
  "Monitoraggio e avvisi"
  "Protezione dei dati"
- È un'ottima cosa! Sono pronto **"iscriviti"**.

Novità di Cloud Insights

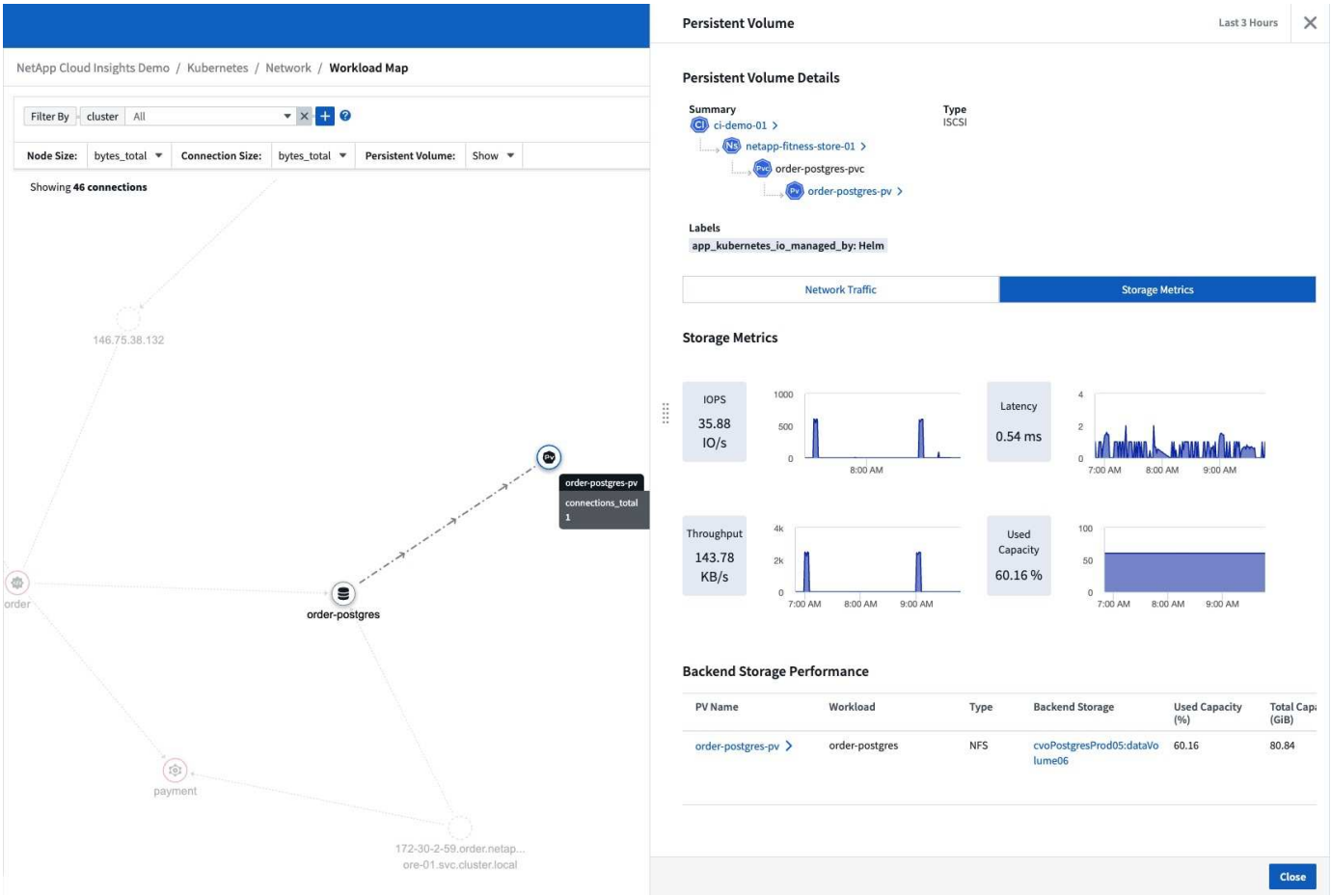
NetApp continua a migliorare e migliorare i propri prodotti e servizi. Di seguito sono riportate alcune delle funzionalità più recenti disponibili nelle edizioni commerciali di Cloud Insights.

> Alcune di queste funzionalità potrebbero non essere disponibili nell'edizione federale di Cloud Insights o potrebbero essere disponibili con funzionalità ridotte. Laddove possibile, queste differenze sono annotate nella documentazione.

Aprile 2024

Supporto SAN iSCSI per Kubernetes Network Map

Identifica le dipendenze dello storage sottostante di Kubernetes per NFS e ora iSCSI.
Accelera la risoluzione dei problemi ottenendo informazioni approfondite sull'attività della rete di storage dell'applicazione Kubernetes e sulle metriche di storage non definite. Scopri come l'applicazione Kubernetes utilizza l'infrastruttura storage per chargeback e reporting di showback.



Supporto del sistema operativo

Oltre a questi, le unità di acquisizione Cloud Insights supportano i seguenti sistemi operativi "già supportato":

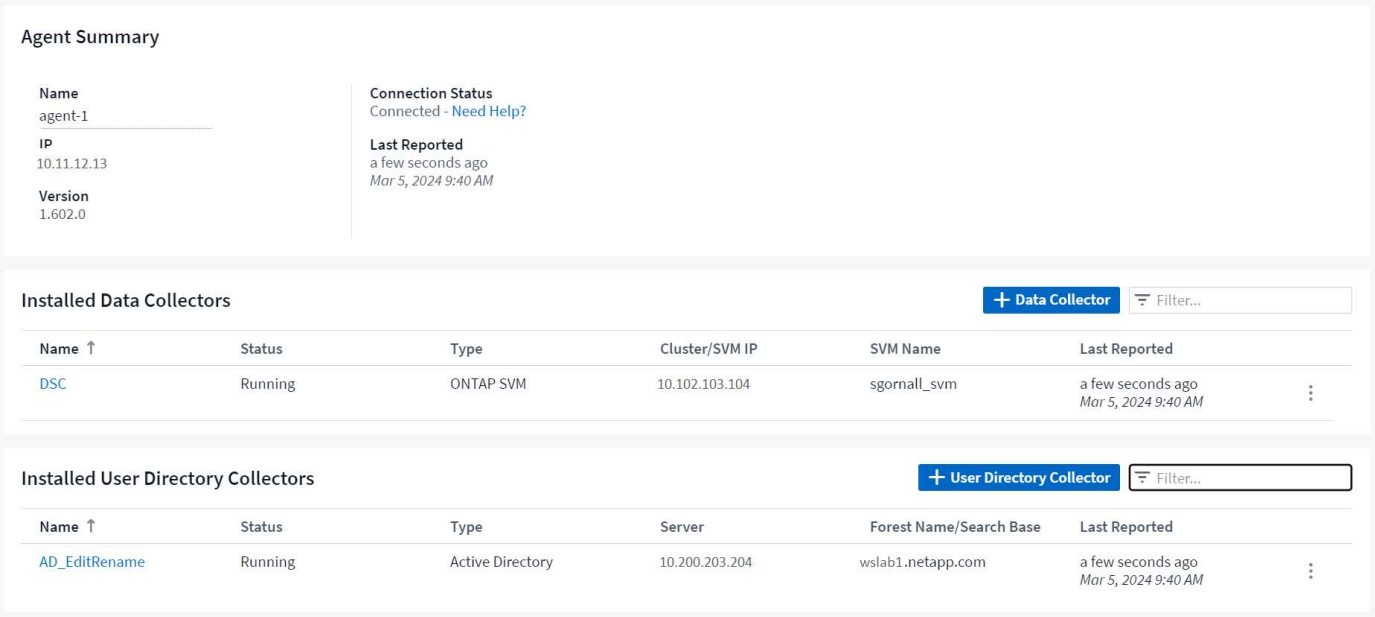
- Oracle Enterprise Linux 8,8

- Red Hat Enterprise Linux 8,8
- Rocky 9,3
- OpenSUSE Leap da 15,1 a 15,5
- SUSE Enterprise Linux Server 15, da 15 SP2 a 15 SP5

Marzo 2024

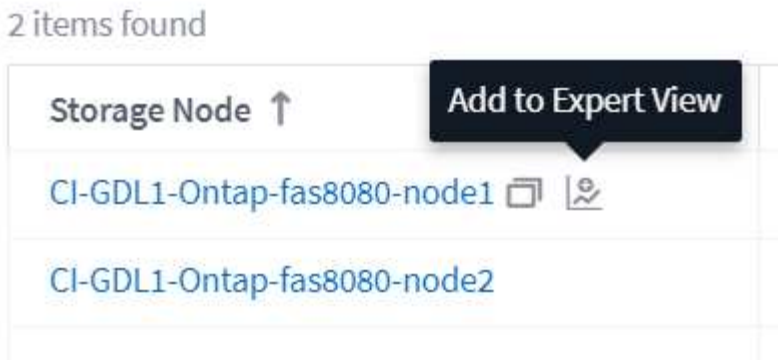
Dettagli agente di sicurezza del carico di lavoro

Ogni agente di sicurezza del carico di lavoro dispone di una propria pagina di destinazione, in cui è possibile visualizzare facilmente le informazioni di riepilogo relative all'agente, nonché i Data Collector installati e i User Directory Collector associati a tale agente.

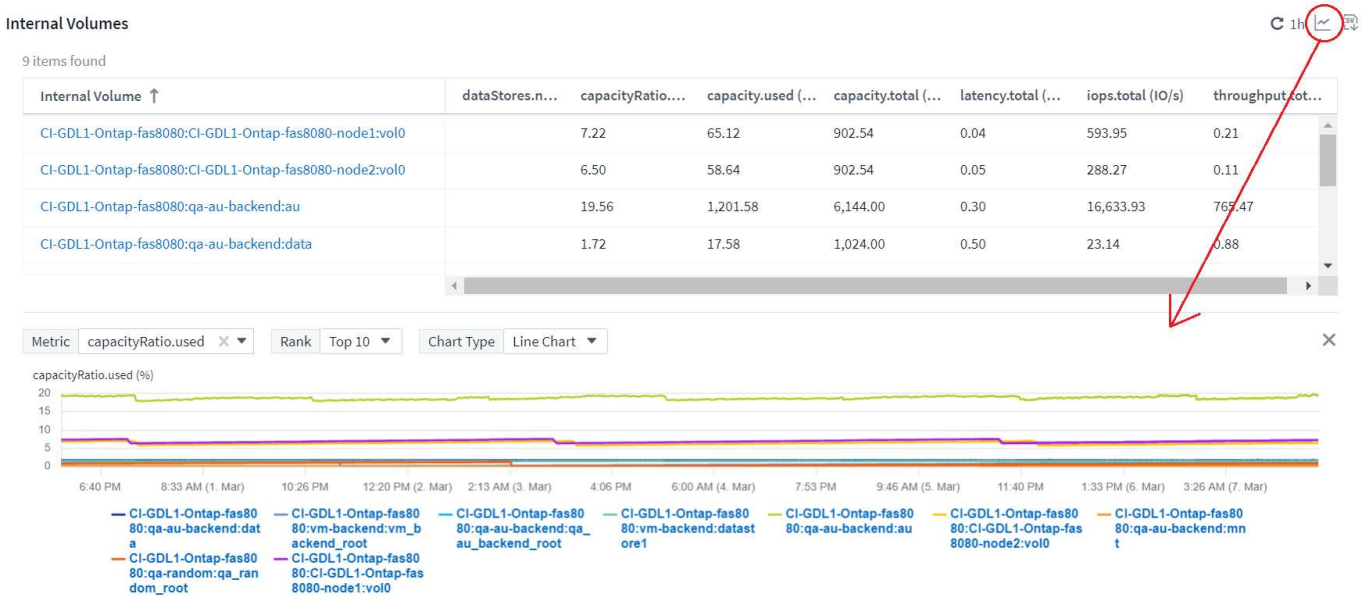


Creare più dati con una maggiore rapidità

Quando si analizzano i dati nella landing page di una risorsa, l'aggiunta di dati aggiuntivi ai grafici Expert View è un'operazione immediata. Per ogni tabella nella pagina di destinazione, se un tipo di oggetto contiene dati pertinenti, passare il mouse sull'oggetto per visualizzare l'icona "Aggiungi alla visualizzazione esperto". Selezionando questa icona si aggiunge l'oggetto alle risorse aggiuntive e lo si visualizza nei grafici Vista Esperti.



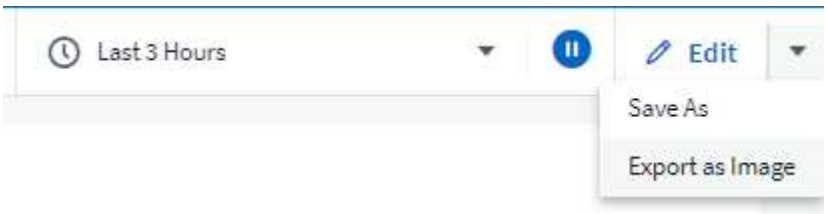
O forse vuoi vedere i dati di una tabella di una pagina di destinazione nel proprio grafico. È sufficiente selezionare l'icona *Mostra grafico* per aprire il grafico sotto la tabella:



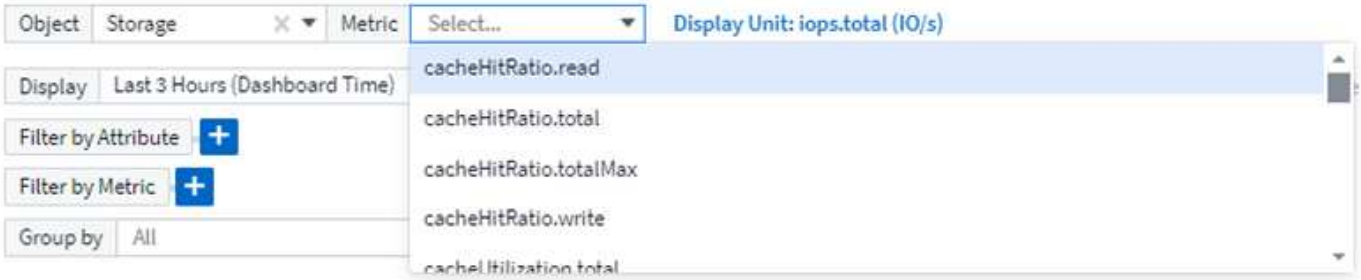
Febbraio 2024

Miglioramenti di usabilità

Salvare un'istantanea **istantanea** del dashboard corrente selezionando *Esporta come immagine* dall'elenco a discesa nell'angolo destro. Cloud Insights crea un file .PNG degli stati del widget corrente.



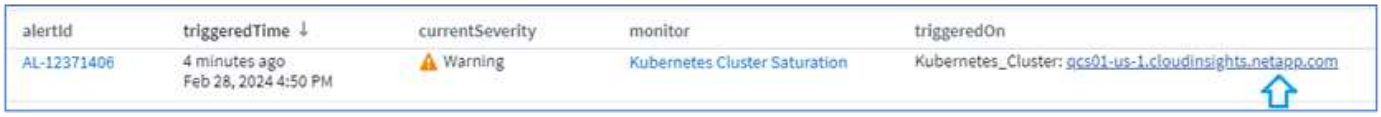
La selezione di oggetti e metriche è più facile che mai per widget, monitor, ecc. Scegliere il tipo di oggetto desiderato, quindi selezionare una metrica relativa all'oggetto nell'elenco a discesa separato.



Esportare gli elenchi Data Collector and Acquisition Unit in .CSV selezionando l'icona nella parte superiore delle pagine.

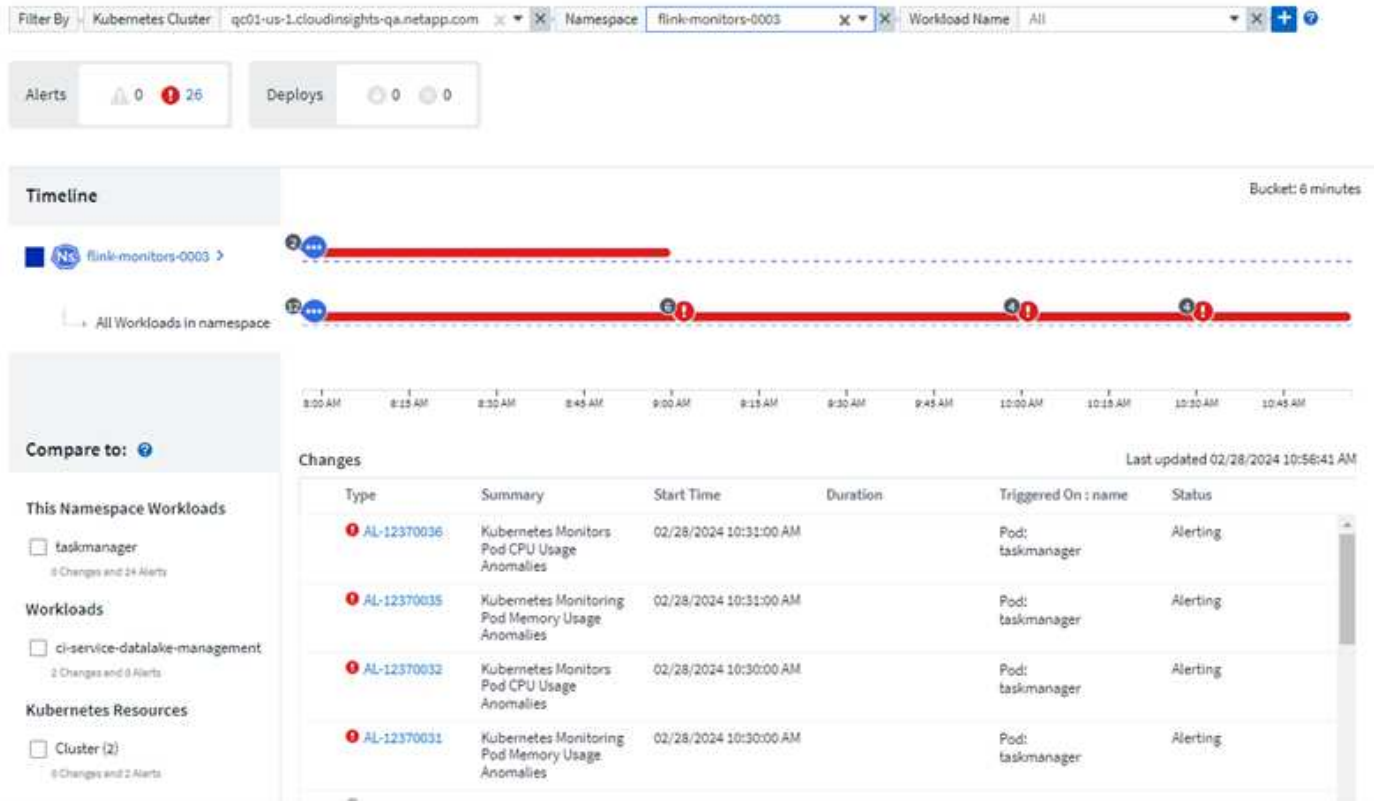
Abbiamo **riorganizzato la pagina Guida > supporto** in modo che sia più facile trovare ciò che si sta cercando e, poiché è stato richiesto, abbiamo aggiunto collegamenti diretti in questa pagina a **API Swagger** e alla documentazione per l'utente.

Collegamenti nella colonna "triggeredOn" della pagina dell'elenco Avvisi, si accede alla pagina di destinazione appropriata, se è disponibile una pagina di destinazione per quell'oggetto.



Visualizza tutte le modifiche nello spazio dei nomi

L'analisi del cambiamento in Kubernetes ti consente ora di vedere una timeline delle modifiche quando si seleziona il cluster e il namespace. In precedenza, è necessario aver selezionato anche il carico di lavoro. Quando si filtrano su cluster e namespace, la timeline di tutte le modifiche del carico di lavoro in tale spazio dei nomi viene visualizzata su un'unica riga.



Registri correlati per gli avvisi

Quando viene visualizzato un avviso di registro, le voci di registro correlate vengono visualizzate in una nuova tabella. Una voce di registro è correlata se si verifica nella stessa origine e nello stesso intervallo di tempo dell'avviso ed è soggetta alle stesse condizioni. Selezionare "analizza registri" per ulteriori informazioni.

Raccogliere i dati degli switch ONTAP

Cloud Insights è in grado di raccogliere dati dagli switch back-end del sistema ONTAP; è sufficiente abilitare la raccolta nella sezione *Configurazione avanzata* del data Collector e verificare che il sistema ONTAP sia configurato per fornire "informazioni sull'interruttore" e ha l'appropriato "permessi" impostare.

API Data Collector di sicurezza del workload

Negli ambienti di grandi dimensioni, è possibile automatizzare la creazione di Collector di sicurezza dei workload utilizzando la nuova API di Data Collector. Accedere a **Admin > API Access > API Documentation** e selezionare il tipo di API *workload Security* per ulteriori informazioni.

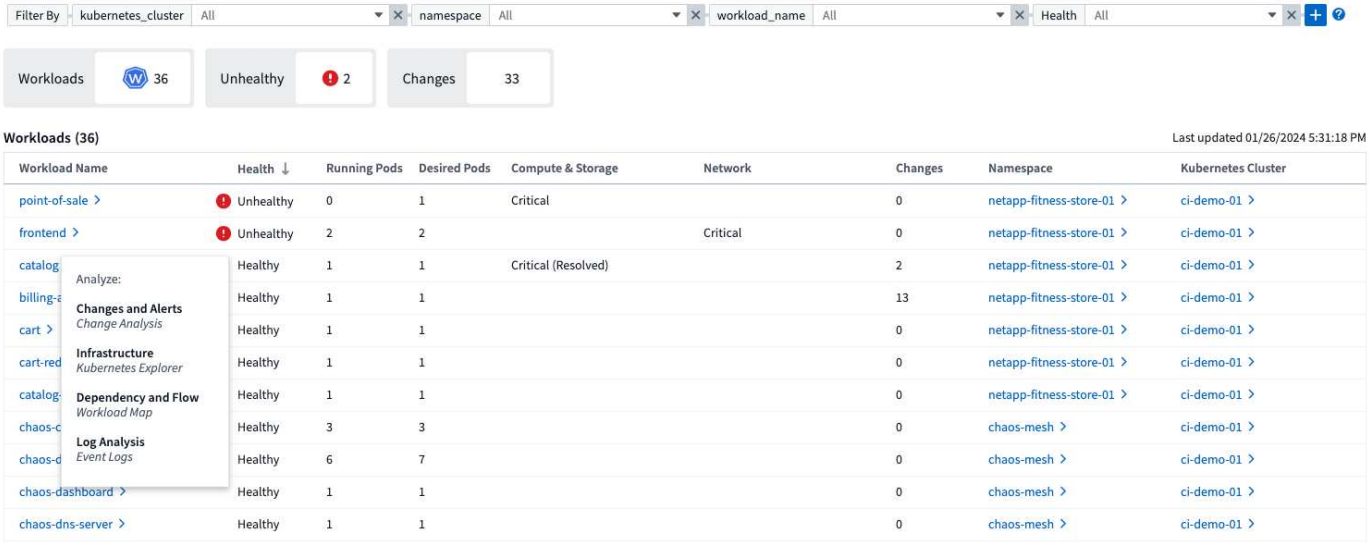
Gennaio 2024

Prova le funzionalità di Cloud Insights che non hai ancora utilizzato

Oltre alla versione di prova iniziale di Cloud Insights, è possibile usufruire di "Versioni di prova dei moduli". Ad esempio, se sei abbonato a Cloud Insights e hai monitorato lo storage e le macchine virtuali, quando Aggiungi Kubernetes al tuo ambiente, entrerai automaticamente in una prova di 30 giorni di Kubernetes Observability. L'utilizzo delle unità gestite da Kubernetes Observability non verrà conteggiato in base al tuo diritto sottoscritto fino alla fine del periodo di prova.

Quanto salutano i miei carichi di lavoro?

Lo stato dei workload è disponibile con una semplice occhiata alla pagina **Kubernetes > Esplora > workload**, in modo da poter vedere rapidamente quali carichi di lavoro funzionano correttamente e quali potrebbero richiedere assistenza. Identifica con facilità se il problema di salute è correlato a modifiche all'infrastruttura, alla rete o alla configurazione e analizza la causa principale.



Aggiornamenti di Data Collector

Identificazione del dominio dati

Il Data Domain Collector è stato migliorato per identificare meglio i sistemi ha per la durata negli eventi di failover. Questa modifica causerà una * una volta* riidentificazione delle appliance Data Domain nei sistemi ha, il che causerà la rimozione delle annotazioni su tali risorse (poiché questi array verranno riidentificati). Sarà necessario ricollegare le annotazioni agli oggetti Data Domain.

Algoritmo ML di rilevamento ransomware avanzato

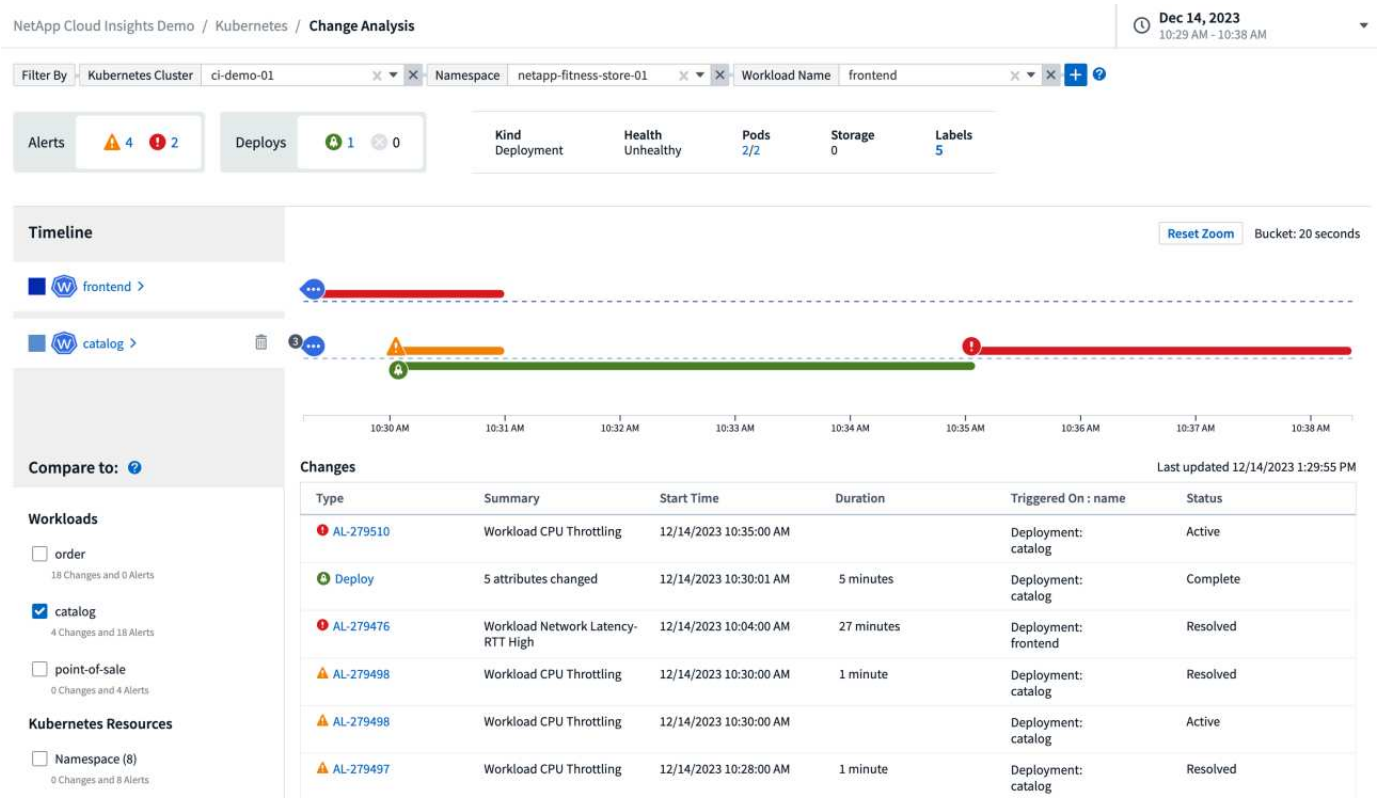
Workload Security include un nuovo algoritmo ML di rilevamento ransomware di 2nd generazione per rilevare in modo più rapido e preciso gli attacchi più sofisticati.

"Stagionalità" dei comportamenti: Il comportamento del fine settimana può seguire diversi modelli dal giorno della settimana, o il comportamento del mattino dal pomeriggio. Gli algoritmi di sicurezza del carico di lavoro tengono conto di questa stagionalità.

Dicembre 2023

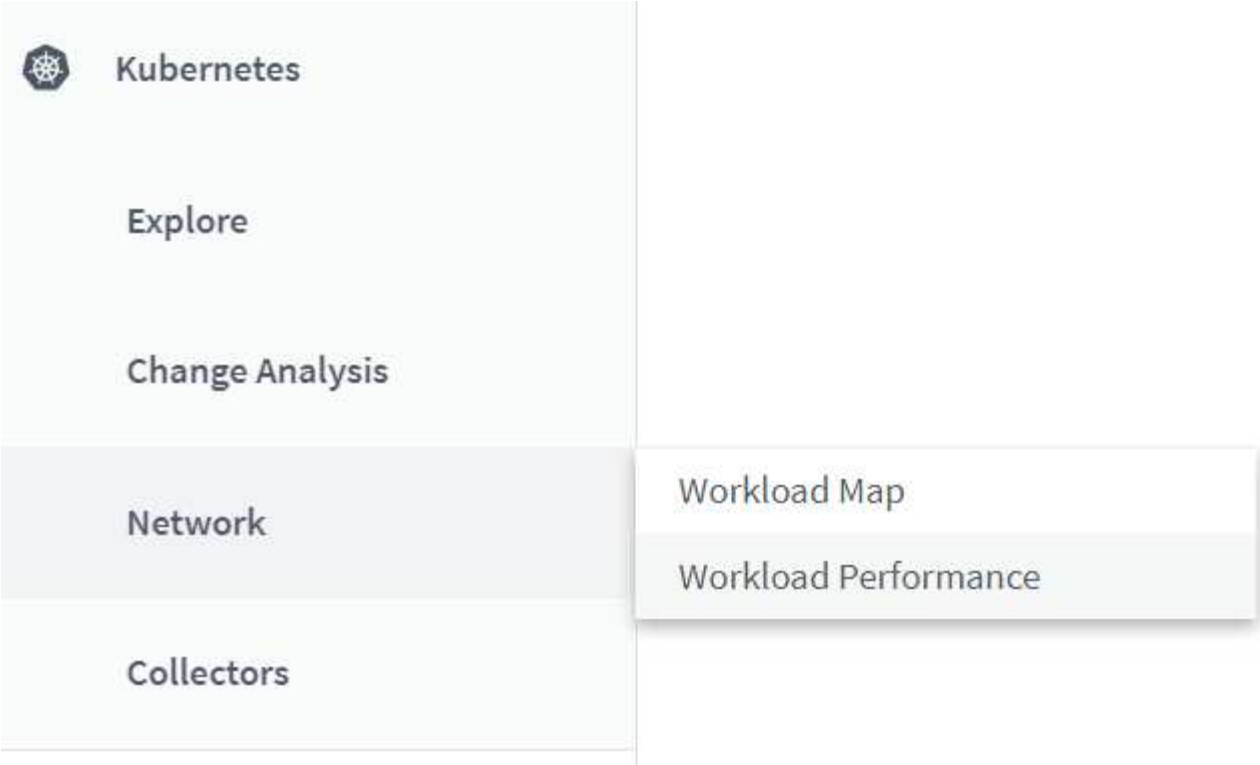
Cambia l’analisi in un colpo d’occhio

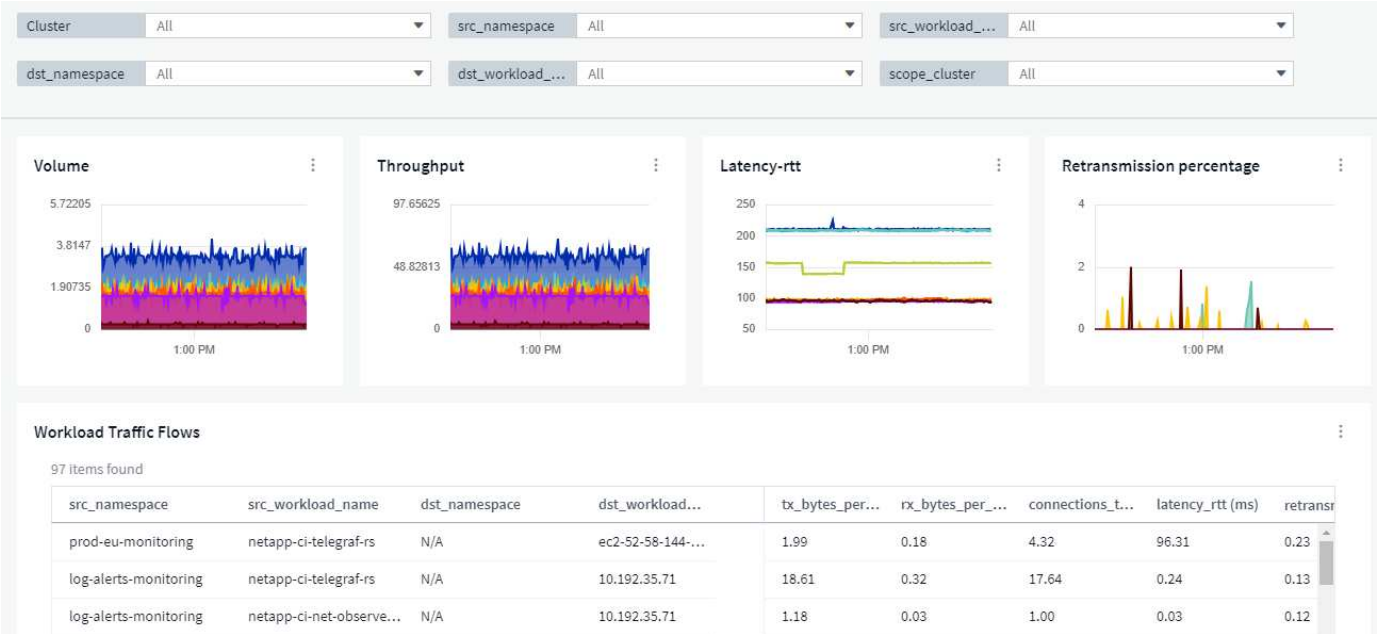
Kubernetes "Cambia analisi" Fornire una vista completa delle recenti modifiche all’ambiente Kubernetes. Gli avvisi e lo stato dell’implementazione sono a portata di mano. Con Change Analytics, puoi monitorare ogni modifica di implementazione e configurazione e correlarla con lo stato e le performance dei servizi, dell’infrastruttura e dei cluster K8s.



Dashboard delle performance del carico di lavoro di Kubernetes

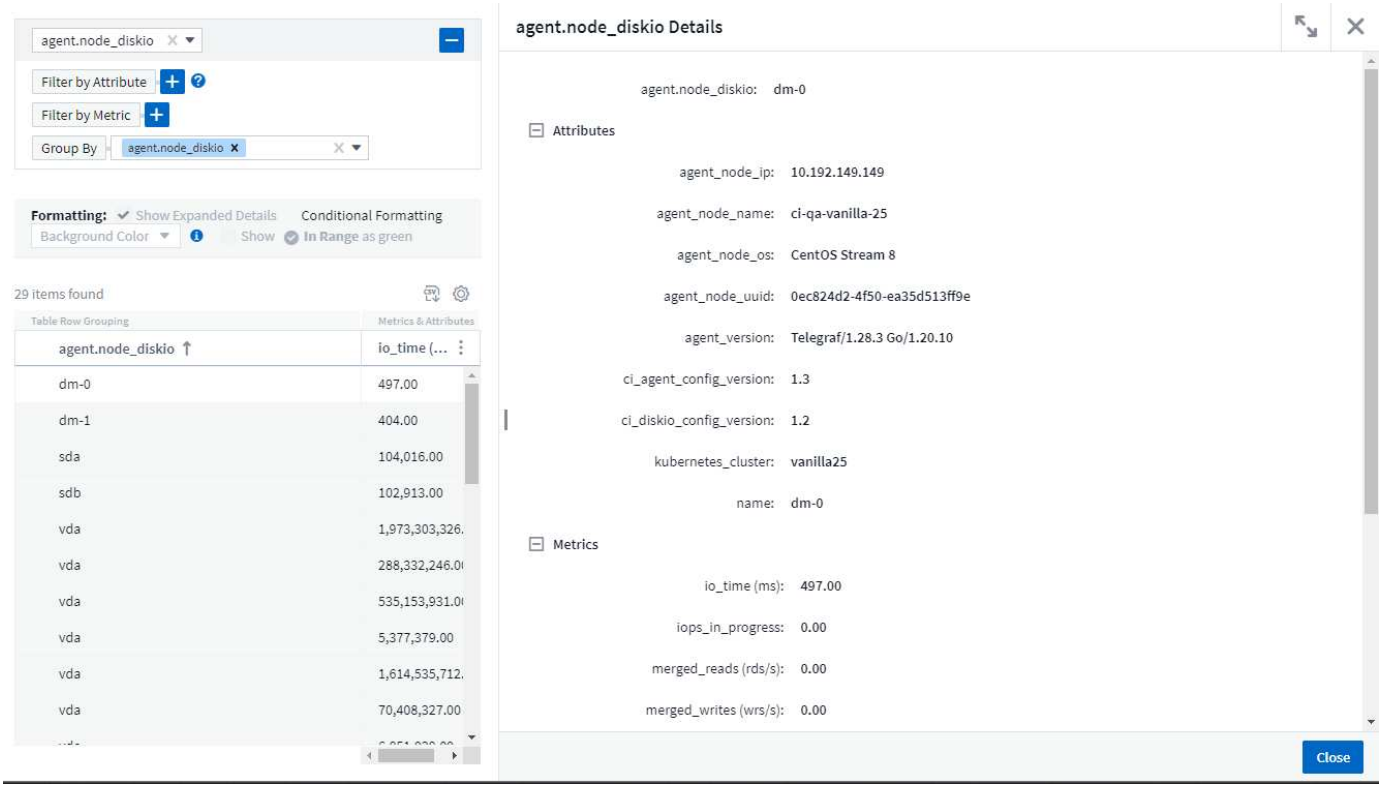
Le performance dei workload sono disponibili in breve nella dashboard completa delle performance dei workload di Kubernetes. È possibile visualizzare rapidamente i grafici dei trend di volume, throughput, latenza e ritrasmissione, nonché una tabella del traffico del carico di lavoro per ogni spazio dei nomi nell’ambiente. I filtri consentono una facile messa a fuoco delle aree di interesse.





Dettagli query su un’unica schermata

In una query, selezionando una riga si apre un pannello laterale che mostra attributi, annotazioni e dettagli metrici per la riga selezionata, fornendo informazioni utili senza dover eseguire il drill-down nella pagina di destinazione dell’oggetto. I collegamenti nella fila o nel pannello laterale consentono una facile navigazione.



Aggiornamenti di Data Collector:

- **Brocade FOS REST**: Questo raccoglitore viene spostato da "Preview" ed è ora generalmente disponibile. Alcune cose da notare:
  - FOS ha introdotto la propria API REST con FOS 8,2. Tuttavia, alcune funzioni come l'instradamento hanno ricevuto solo funzionalità di API REST con 9,0.
  - Se si dispone di un fabric costituito da risorse FOS miste 8,2 volte superiori, oltre a circa < 8,2, il REST Collector Cloud Insights FOS non sarà in grado di rilevare tali risorse precedenti. È possibile modificare il collettore REST FOS e creare un elenco delimitato da virgole dell'indirizzo IPv4 di tali dispositivi per l'esclusione da tale collettore.
- **SELinux**: Cloud Insights include miglioramenti all'installazione iniziale dell'unità di acquisizione Linux per garantire la robustezza del funzionamento in ambienti Linux con l'applicazione SELinux abilitata. Questi miglioramenti hanno un impatto solo sulle distribuzioni *new* AU; in caso di problemi di SELinux relativi agli aggiornamenti AU, contattare il supporto NetApp per risolvere la configurazione di SELinux.

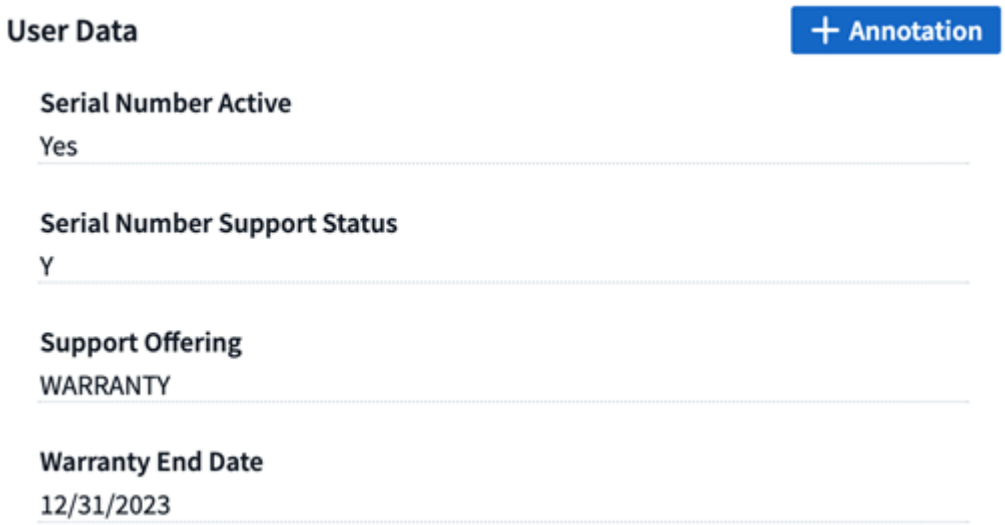
Novembre 2023

Sicurezza del carico di lavoro: Pausa/ripresa di un servizio di raccolta

In sicurezza del carico di lavoro, è possibile sospendere un Data Collector se il collettore è in stato *running*. Aprire il menu "tre punti" per il raccoglitore e selezionare PAUSA. Mentre il raccoglitore è in pausa, non vengono raccolti dati da ONTAP e non vengono inviati dati dal raccoglitore a ONTAP. Selezionare Riprendi per iniziare nuovamente la raccolta.

Informazioni di supporto del nodo di storage

Nella landing page di un nodo storage, la sezione *dati utente* fornisce informazioni immediate sulla tua offerta di supporto, sullo stato corrente, sullo stato del supporto e sulla data di fine della garanzia. Si noti che attualmente Cloud Insights pubblica automaticamente queste informazioni solo per i dispositivi NetApp. Si noti inoltre che questi campi di supporto sono annotazioni, quindi possono essere utilizzati in query e dashboard.



Associare i tag VMware alle annotazioni Cloud Insights

Il "VMware" Data Collector consente di popolare annotazioni di testo Cloud Insights con tag con lo stesso nome configurati su VMware.

Brocade CLI Collector Reliability Enhancements per FOS 9,1.1c e versioni successive del firmware

Su alcuni switch Brocade Fibre Channel che eseguono il firmware 9,1.1c, l'output di alcuni comandi CLI potrebbe essere preceduto dal testo del banner di accesso "motd" o dagli avvisi per gli utenti di modificare le password predefinite. Il collettore CLI Brocade è stato migliorato per ignorare questi due tipi di testo estraneo.

Prima di questo miglioramento, solo gli switch FOS 9,1.1c senza Virtual Fabrics presenti erano probabilmente rilevabili con questo tipo di collettore.

Ottobre 2023

Maggiore sicurezza dei carichi di lavoro

La sicurezza del carico di lavoro è stata migliorata con quanto segue:

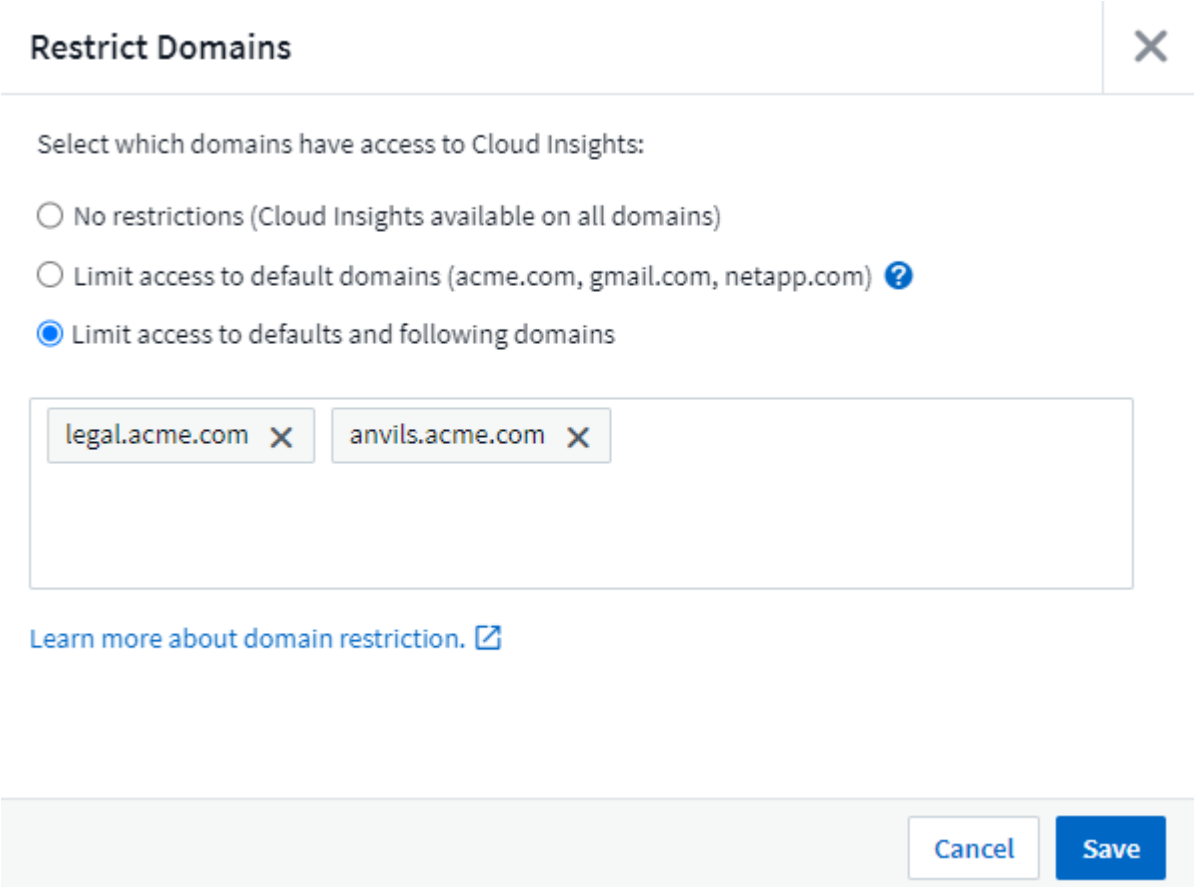
- **Accesso negato**: Workload Security si integra con ONTAP per ricevere "Eventi "accesso negato"" e fornire un livello aggiuntivo di analisi e risposte automatiche.
- **Tipi di file consentiti**: Se viene rilevato un attacco ransomware per un'estensione di file nota, tale estensione può essere aggiunta a un "tipi di file consentiti" per evitare avvisi non necessari.

Versioni di prova dei moduli

Oltre alla versione di prova iniziale di Cloud Insights, è possibile usufruire di "Versioni di prova dei moduli". Ad esempio, se sei già abbonato all'opzione Infrastructure Observability ma stai aggiungendo Kubernetes al tuo ambiente, potrai entrare automaticamente in una prova di 30 giorni di Kubernetes Observability. Ti verrà addebitato solo l'utilizzo delle unità gestite da Kubernetes Observability al termine del periodo di prova.

Limitare l'accesso a domini specifici

Gli amministratori e i proprietari di account ora hanno la possibilità di farlo "Limitare l'accesso Cloud Insights" per inviare e-mail ai domini specificati. Andare su **Admin > User Management** e selezionare il pulsante *Restringi domini*.



Aggiornamenti di Data Collector

Sono state apportate le seguenti modifiche al Data Collector/Acquisition Unit:

- **Isilon / PowerScale REST**: Sono stati aggiunti vari nuovi attributi e metriche alle funzionalità analitiche avanzate di Cloud Insights con il nome *emc_isilon.node_pool.**. Questi contatori e attributi consentiranno agli utenti di creare dashboard e monitor per il consumo di capacità *node_pool*; gli utenti con cluster Isilon costruiti da modelli di nodi hardware diversi avranno pool di nodi multipli e la comprensione del consumo di capacità totale/HDD/SSD a livello di pool di nodi è utile sia per il monitoraggio che per la pianificazione.
- **Supporto dell'autenticazione Rubrik** "account di servizio": Il collettore Rubrik di Cloud Insights ora supporta sia l'autenticazione di base HTTP tradizionale (nome utente e password) sia l'approccio dell'account di servizio di Rubrik, che richiede un nome utente + segreto + ID organizzazione.

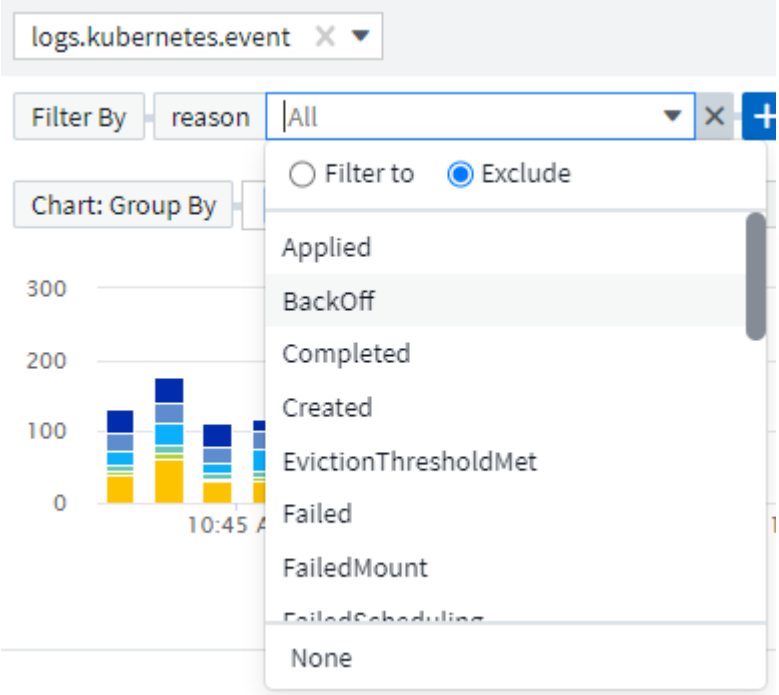
Settembre 2023

Trova facilmente ciò che vuoi nei registri

Query registro (**osservabilità > query registro > +Nuova query registro**) include un numero di "miglioramenti" per rendere l'esplorazione dei log più semplice e più informativa.

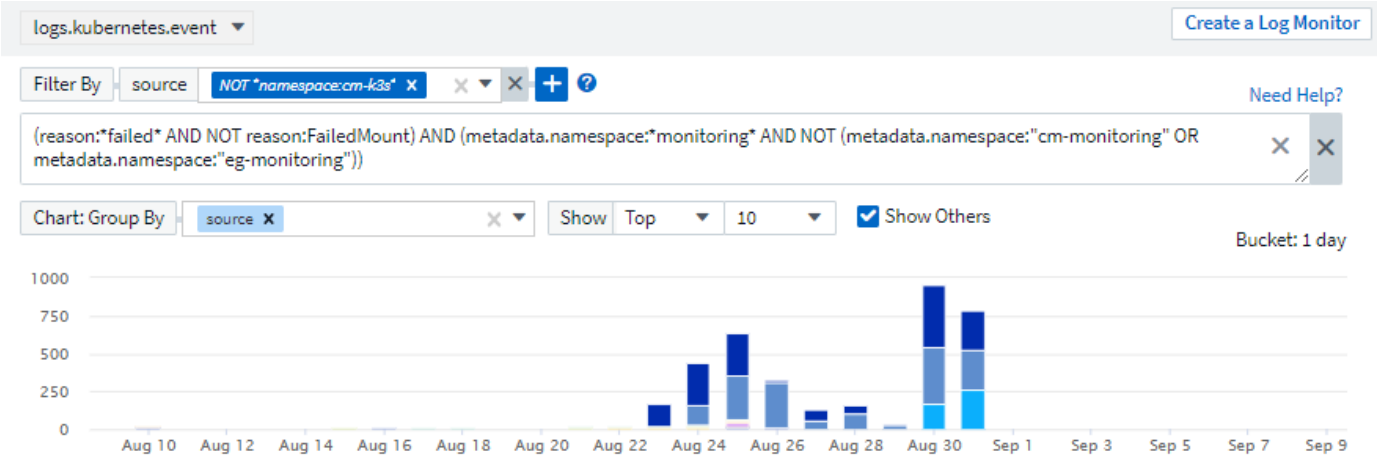
Includi/Escludi

Quando si filtra un valore, è possibile scegliere facilmente se includere i risultati **includere** o **escludere** corrispondenti al filtro. Selezionando "Escludi" si crea un filtro "NON <value>". È possibile combinare i valori Includi ed Escludi in un singolo filtro.



Query avanzata

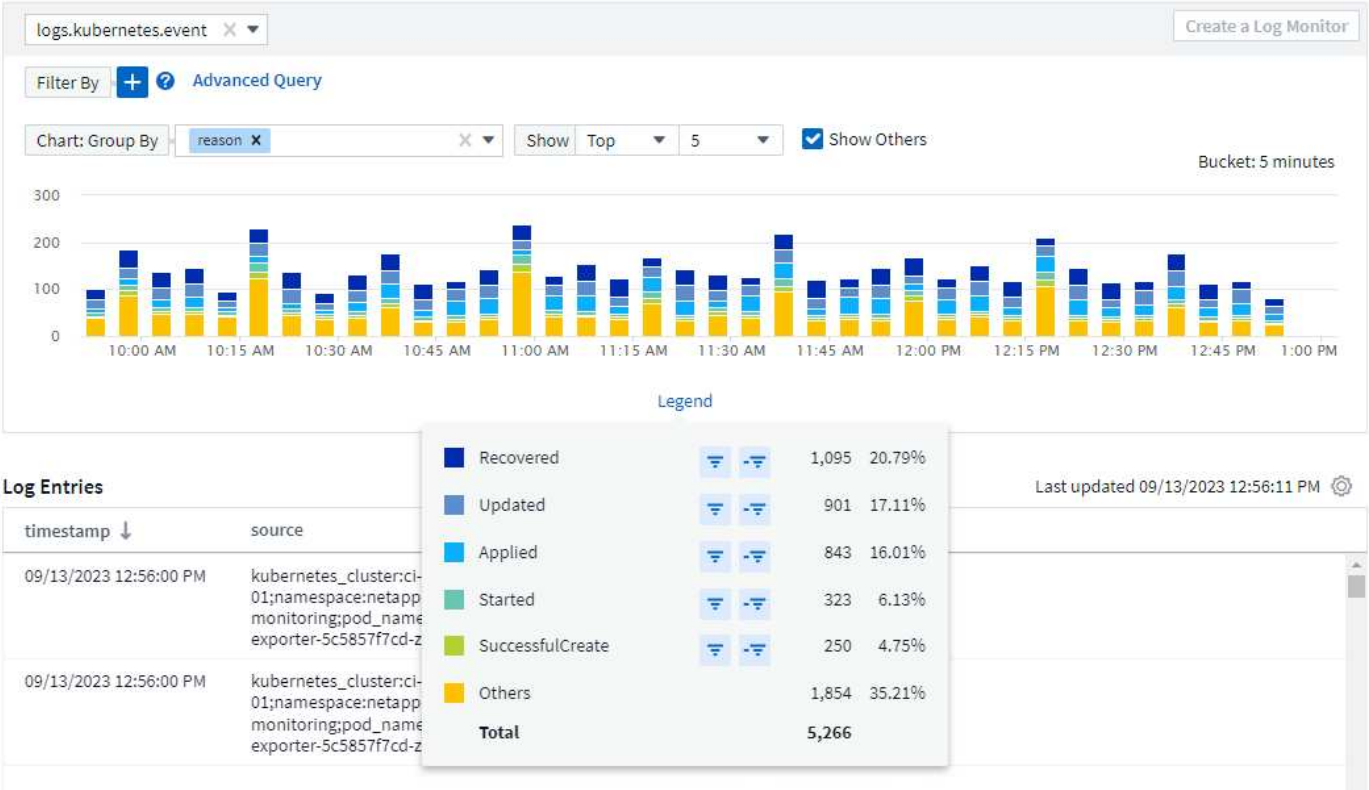
L'interrogazione avanzata offre la possibilità di creare filtri in "formato libero", combinando o escludendo i valori utilizzando E, NON, O, caratteri jolly, ecc.



"Filter by" (Filtra per) e Advanced Query (Query avanzata) vengono "E" insieme per formare una singola query. I risultati vengono visualizzati nell'elenco dei risultati e nel grafico.

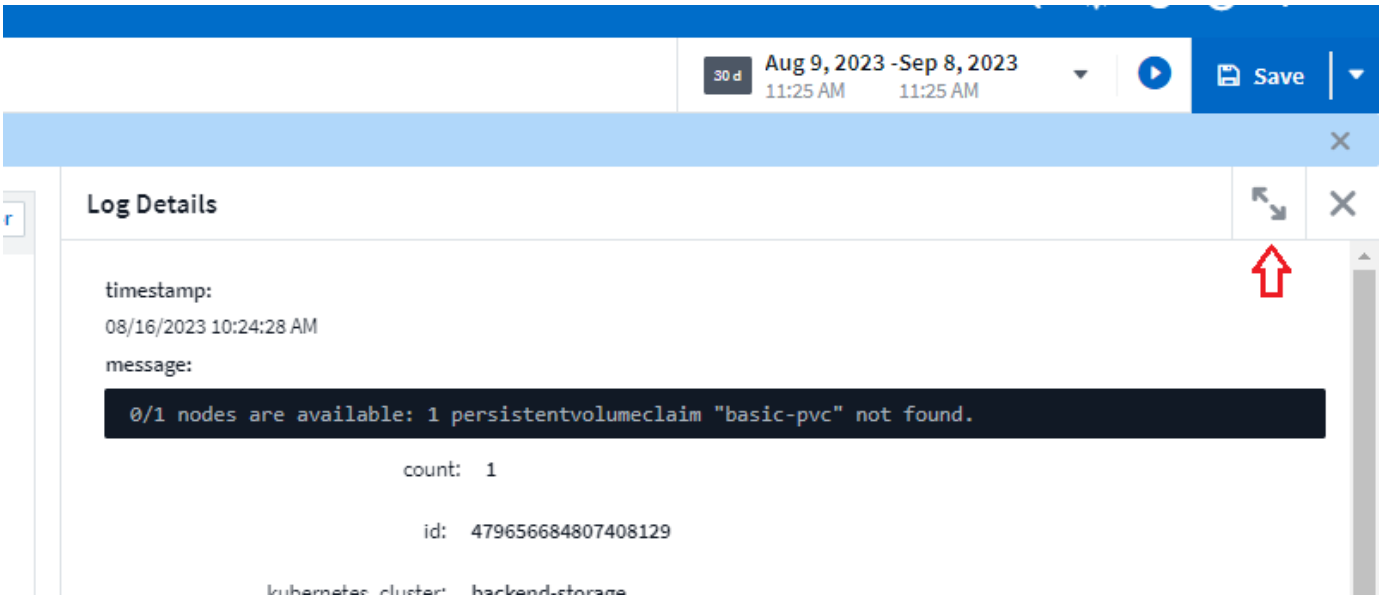
Raggruppamento nel grafico

Quando si seleziona un attributo di registro in **Raggruppa per**, l'elenco e il grafico mostrano i risultati del filtro corrente. Nel grafico, le colonne sono raggruppate in colori. Passando con il mouse sopra una colonna del grafico vengono visualizzati i dettagli relativi alle voci specifiche, in modo simile alle informazioni generali visualizzate quando si espande la legenda del grafico. Nella legenda è inoltre possibile scegliere di impostare un filtro Includi o Escludi per un raggruppamento specifico.



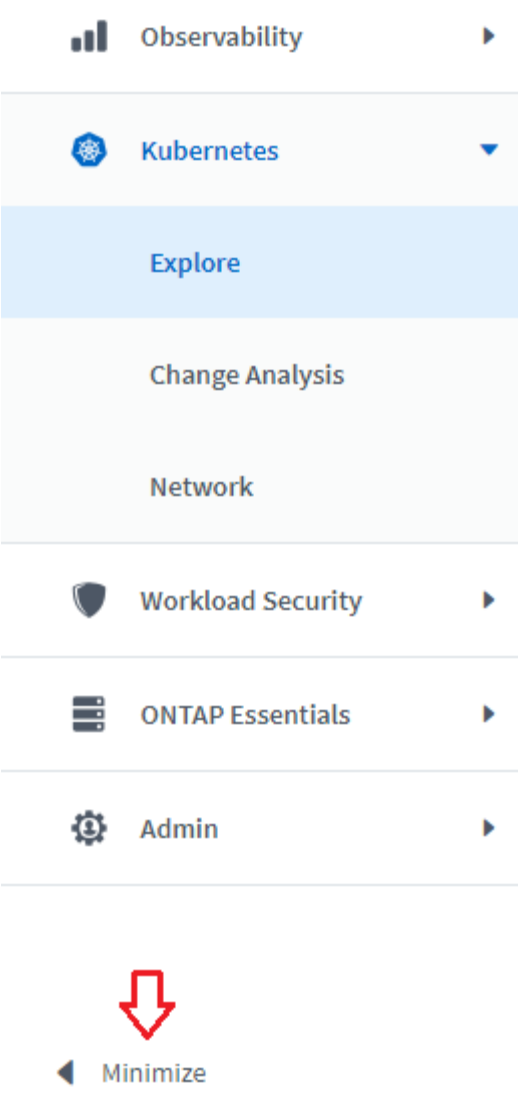
Pannello Dettagli registro "mobile"

Quando si esplorano i registri utilizzando la query del registro, selezionando una voce nell'elenco si apre un pannello dei dettagli per tale voce. A questo punto potete scegliere di visualizzare il pannello scorrevole "fluttuante" (cioè visualizzato sul resto dello schermo) o "nella pagina" (cioè visualizzato come proprio fotogramma all'interno della pagina). Per passare da una vista all'altra, seleziona il pulsante "in Page / Floating" nell'angolo in alto a destra del pannello.



Chiudere il menu

È possibile comprimere il menu di navigazione Cloud Insights sul lato sinistro selezionando il pulsante "Riduci a icona" sotto il menu. Mentre il menu è ridotto a icona, passare il mouse su un'icona per vedere quale sezione si apre; selezionando l'icona si apre il menu e si accede direttamente a quella sezione.



Miglioramenti a Data Collector

Cloud Insights ha semplificato la visualizzazione e la ricerca delle informazioni di raccolta dati:

- **L'elaborazione degli elenchi di raccolta dati** è più efficiente, il che significa che il tempo necessario per visualizzare e navigare in questi elenchi è notevolmente ridotto. Se si dispone di un ambiente di grandi dimensioni con molti raccoglitori di dati, si noterà un miglioramento significativo quando si elencano i raccoglitori di dati.
- La **Data Collector Support Matrix** è stata spostata da un file .PDF a una pagina basata su .HTML, in modo più rapido e facile da gestire. Consulta la nuova tabella qui: https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html

Agosto 2023

Raccolta dei registri Isilon/PowerScale e dei dati di analisi avanzata

I collettori A RIPOSO Isilon e PowerScale contengono i seguenti miglioramenti:

- Gli eventi del registro Isilon sono disponibili per l'utilizzo in query e avvisi
- Gli attributi Isilon Advanced Analytic sono disponibili per l'uso in query, dashboard e avvisi:
  - cluster emc_isilon
  - emc_isilon.node
  - emc_isilon.node_disk
  - emc_isilon.net_iface

Queste sono abilitate per impostazione predefinita per gli utenti dei collettori REST Isilon e/o PowerScale. NetApp consiglia vivamente agli utenti del collettore basato su CLI di Isilon di migrare al nuovo collettore basato su API REST per ricevere miglioramenti come quelli sopra descritti.

Mappa dei carichi di lavoro migliorata

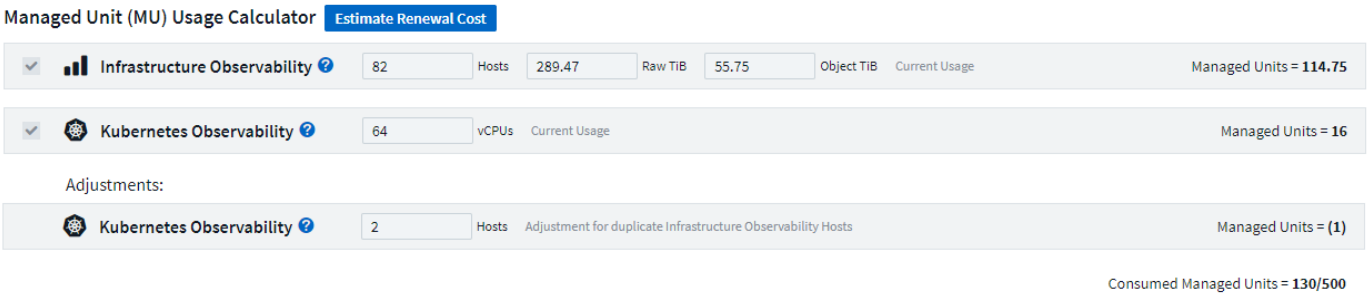
La mappa dei carichi di lavoro è più utilizzabile e meno rumorosa; raggruppa tutti i servizi esterni simili in un unico nodo se comunicano con gli stessi carichi di lavoro, riducendo la complessità del grafico e semplificando la comprensione delle modalità di interconnessione dei servizi.

Scegliendo un nodo raggruppato verrà visualizzata una tabella dettagliata con le metriche di traffico di rete per ogni servizio esterno relativo a quel nodo.

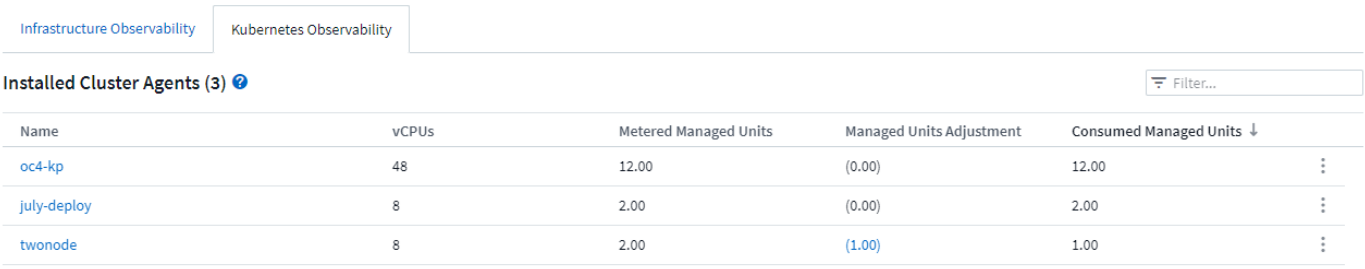
Regolazione dell'utilizzo delle unità gestite Kubernetes

Nel caso in cui una risorsa di calcolo nel tuo ambiente cluster Kubernetes venga conteggiata sia dall'operatore di monitoring NetApp Kubernetes che da un raccoglitore di dati dell'infrastruttura sottostante (per esempio, VMware), il tuo utilizzo di queste risorse sarà regolato per garantire il conteggio più efficiente delle unità gestite. È possibile visualizzare le regolazioni delle UM di Kubernetes nella pagina Admin > Subscription (Amministrazione > abbonamento), nelle schede Summary (Riepilogo) e Usage (utilizzo).

Scheda Summary (Riepilogo):



Scheda utilizzo:



Modifiche di acquisizione/raccolta:

Sono state apportate le seguenti modifiche al Data Collector/Acquisition Unit:

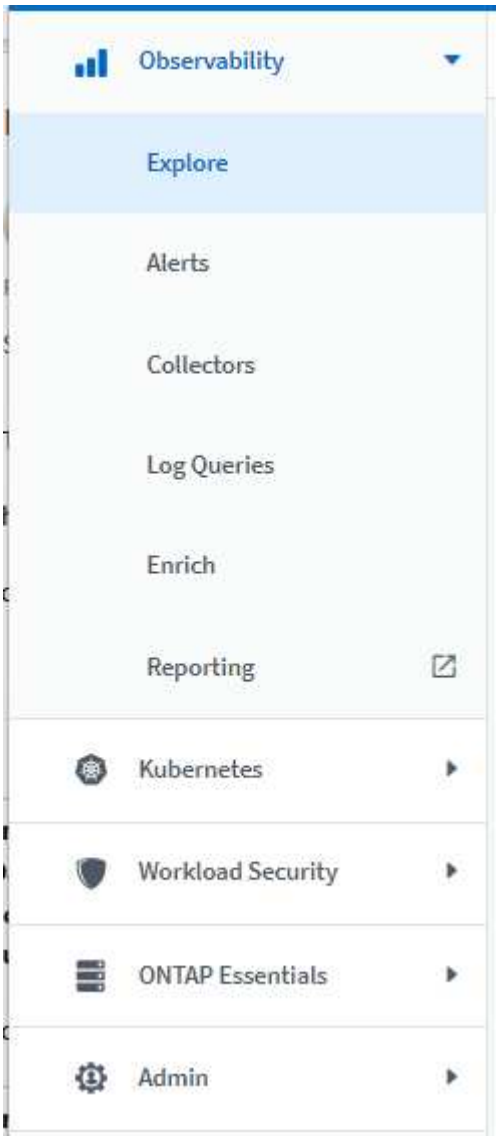
- Le unità di acquisizione supportano ora RHEL 8,7.

Menu migliorati

Abbiamo aggiornato il menu di navigazione a sinistra per supportare meglio i flussi di lavoro dei nostri clienti. I nuovi elementi di livello superiore come *Kubernetes* forniscono un accesso accelerato a ciò di cui il cliente ha bisogno, mentre una console di amministratori consolidata supporta il ruolo di proprietario del tenant.

Ecco alcuni esempi aggiuntivi delle modifiche:

- Il menu *Observability* di primo livello mostra il rilevamento dei dati, gli avvisi e le query di registro
- La funzionalità "accesso API" per l'osservabilità e la sicurezza del carico di lavoro si trova in un unico menu
- Allo stesso modo per la funzionalità 'Notifiche' di osservabilità e sicurezza del carico di lavoro, ora anche in un unico menu



Di seguito è riportato un breve elenco delle funzioni disponibili in ogni menu:

Osservabilità:

- Esplora (dashboard, query metriche, approfondimenti sull’infrastruttura)
- Avvisi (monitor e avvisi)
- Collettori (Data Collector e unità di acquisizione)
- Eseguire il log delle query
- Arricchimento (Annotazioni e regole di annotazione, applicazioni, risoluzione del dispositivo)
- Creazione di report

Kubernetes:

- Esplorazione cluster e mappa della rete

Sicurezza del carico di lavoro:

- Avvisi
- Analisi
- Collezionisti
- Policy

Informazioni di base su ONTAP:

- Protezione dei dati
- Sicurezza
- Avvisi
- Infrastruttura
- Networking
- Carichi di lavoro
  *VMware

Amministratore:

- Accesso API
- Controllo
- Notifiche
- Informazioni sulla sottoscrizione
- Gestione utenti

Luglio 2023

Mostra modifiche recenti

Le landing page di Data Collector ora includono un elenco di modifiche recenti. Fai clic sul pulsante "Recent Changes" (modifiche recenti) nella parte inferiore della landing page del data collector per visualizzare le modifiche recenti del data collector.

Changes Reported by This Data Collector (1)

Time ↓	Change
07/06/2023 6:39:12 PM	Storage CI-GDL1-Ontap-fas8080 **configuration changed** Property **Display IP** is changed from "**10.192.122.10**" to "**10.192.122.12**" Property **Manage URL** is changed from "**HTTPS://10.192.122.10:443**" to "**HTTPS://10.192.122.12:443**"

Hide Recent Changes

Miglioramenti per l'operatore

Sono stati apportati i seguenti miglioramenti "Operatore Kubernetes" implementazione:

- Opzione per ignorare la raccolta di metriche docker
- Possibilità di aggiungere e personalizzare le tolleranze ai set di demoni e repliche di telegraf

Insight: Recuperare lo storage a freddo

Il "Recuperare le informazioni sullo storage a freddo di ONTAP" Ora supporta FlexGroups ed è ora disponibile per tutti i clienti.

Firma immagine operatore

Per i clienti che utilizzano un repository privato per il proprio operatore di monitoraggio Kubernetes NetApp, è ora possibile copiare la chiave pubblica della firma immagine durante l'installazione dell'operatore, consentendo di confermare l'autenticità del software scaricato. Selezionare il pulsante *Copy Image Signature Public Key* durante la fase opzionale per *caricare l'immagine dell'operatore nel repository privato*.

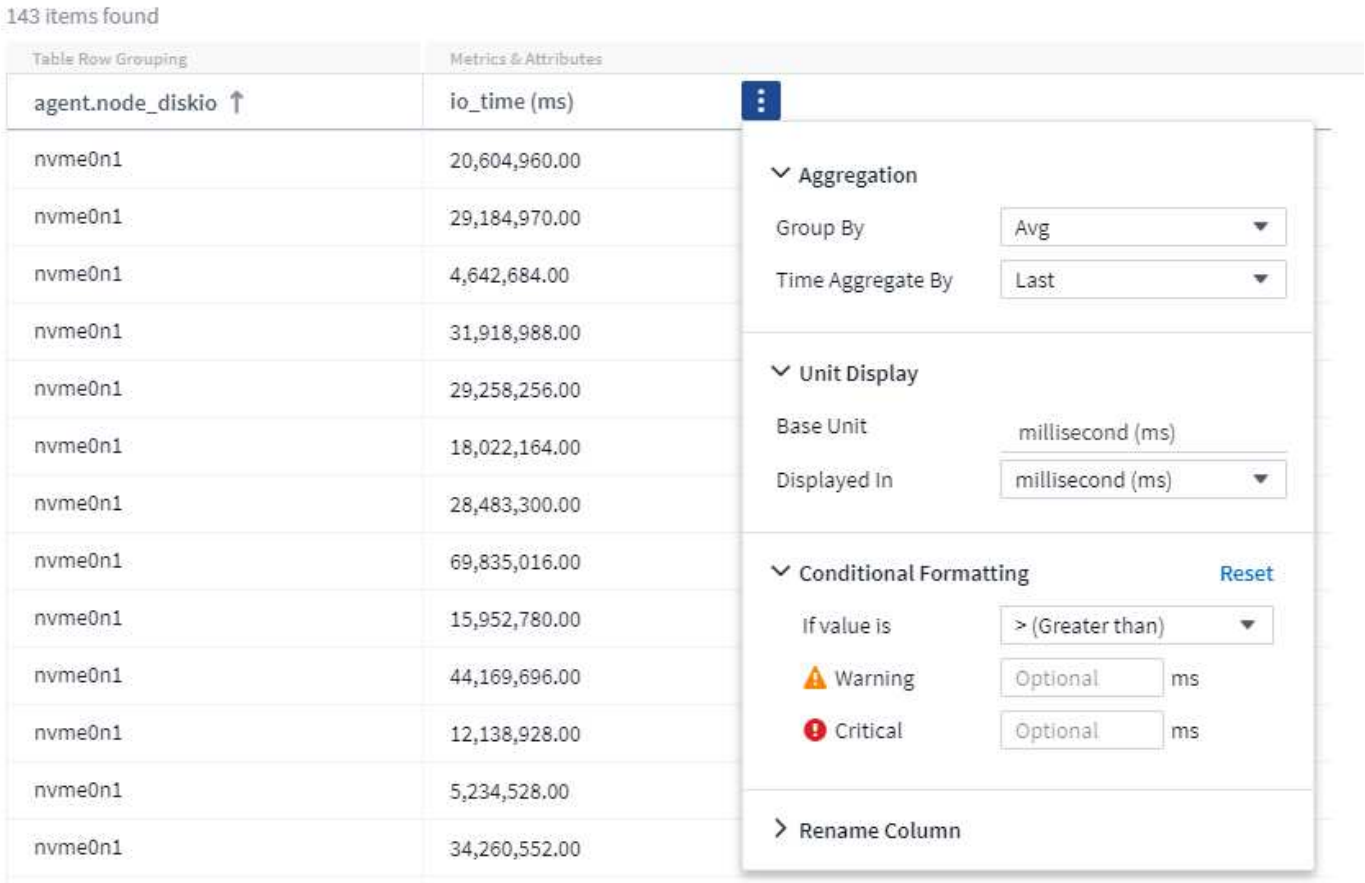
Copy Image Signature Public Key

Reveal Image Signature Public Key


```
-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAoA/Iww7C/1DfDrwYKwPL
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiY1di23TL16p+M7y2y
JjgBSYJdEEOLlopj+X6W/N0OB4kHMDlV8VXzJOlk3zcT2NHiySzB/IYicTfhelpI
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiY1di23TL16p+M7y2y
NiX7KwYpG6K8YSIW89MvTwbgAr7S76liw8Um6VsnsXF655h3dd769UhahiQqv6Z5
```


Aggregazione, formattazione condizionale e altro ancora per le query

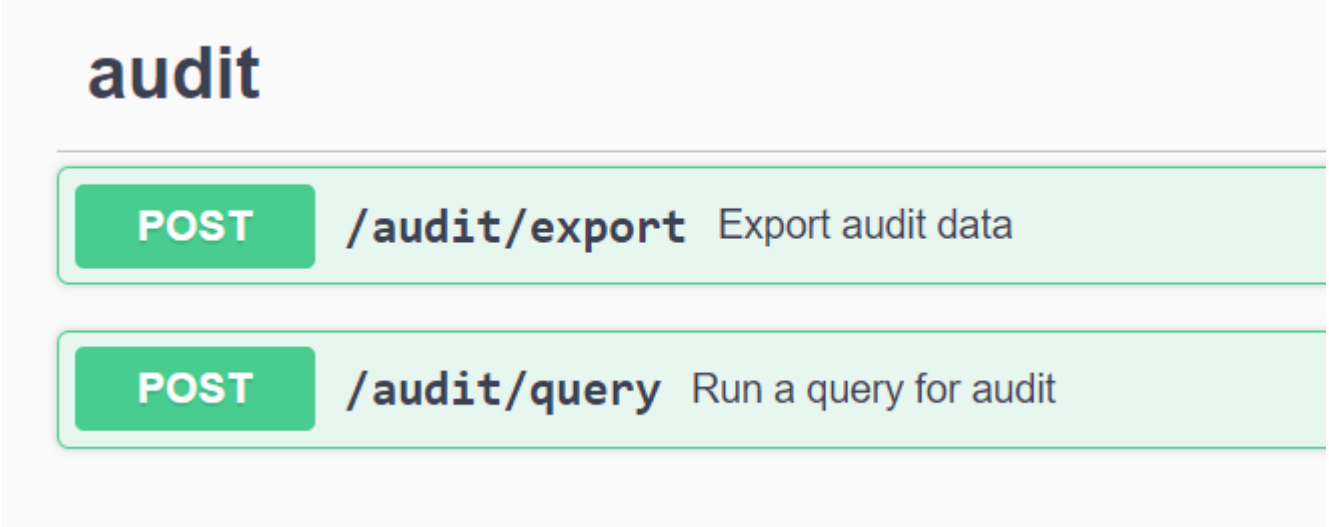
Aggregazione, selezione dell'unità, formattazione condizionale e ridenominazione delle colonne sono tra le funzionalità più utili di un widget della tabella della dashboard e ora sono disponibili le stesse funzionalità per "Query".



Queste funzionalità sono ora disponibili per i dati di tipo integrato (Kubernetes, metriche avanzate ONTAP, ecc.) e saranno presto disponibili per gli oggetti infrastruttura (storage, volume, switch, ecc.).

API per l'audit

È ora possibile utilizzare un'API per eseguire query o esportare eventi controllati. Accedere a Admin > API Access (Amministrazione > accesso API) e selezionare il collegamento *API Documentation* (documentazione API) per informazioni.



Data Collector: Trident Economy

Cloud Insights ora supporta il driver economico Trident, ottenendo questi vantaggi:

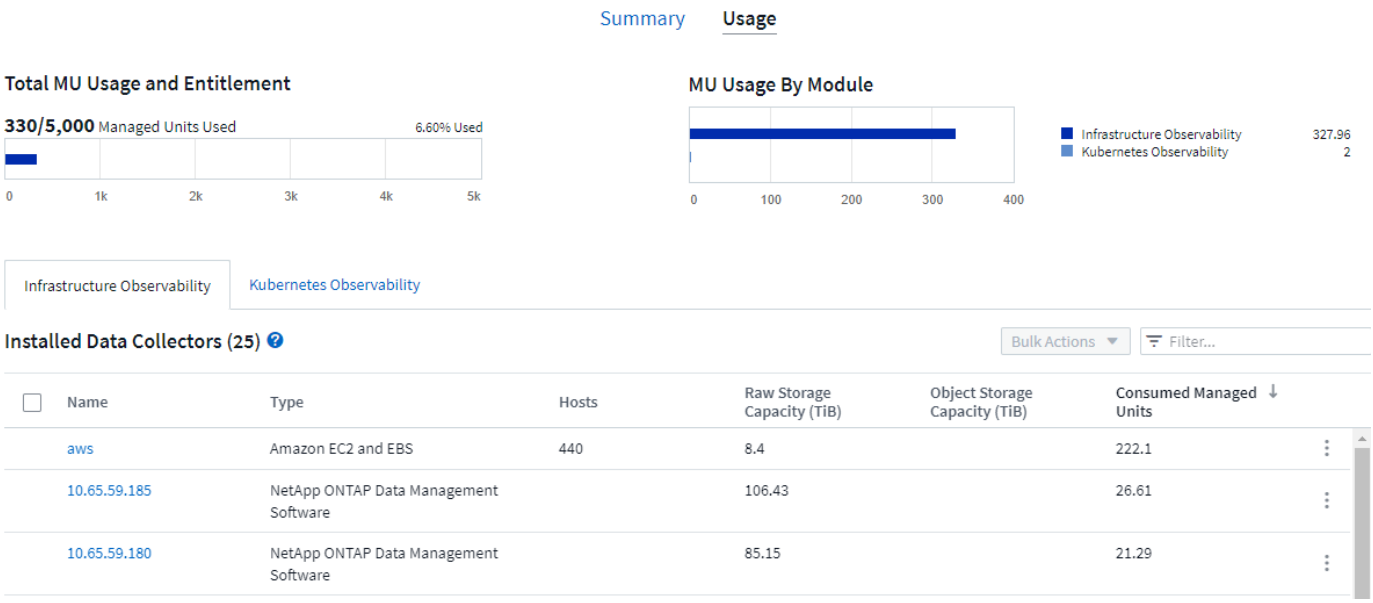
- Ottieni visibilità sulla mappatura del Qtree pod-to-ONTAP e sulle metriche delle performance.
- Risoluzione dei problemi perfetta e facile navigazione dai pod Kubernetes allo storage back-end
- Rilevamento proattivo dei problemi di performance back-end con i monitor

---

Giugno 2023

Verifica l'utilizzo

A partire da giugno 2023, Cloud Insights fornisce un'analisi dettagliata dell'utilizzo delle unità gestite in base al set di funzionalità. Ora è possibile visualizzare e monitorare rapidamente l'utilizzo delle unità gestite (MU) per l'infrastruttura e l'utilizzo delle UM legate a Kubernetes.



Kubernetes Network Monitoring and Map è disponibile per tutti

Il "*Kubernetes Network Performance and Map*" Semplifica il troubleshooting mappando le dipendenze tra i carichi di lavoro Kubernetes, fornendo visibilità in tempo reale sulle latenze e sulle anomalie delle performance di rete di Kubernetes per identificare i problemi di performance prima che influiscano sugli utenti. Molti clienti lo hanno trovato utile durante l'anteprima e ora è disponibile per tutti.

Modifiche di acquisizione/raccolta:

Sono state apportate le seguenti modifiche al Data Collector/Acquisition Unit:

- Le UM di Data Domain e Cohesity vengono dosate a 40 TIB: 1 MU.
- Le unità di acquisizione supportano ora RHEL e Rocky 9.0 e 9.1.

Nuove dashboard di ONTAP Essentials

Le seguenti dashboard di ONTAP Essentials sono disponibili negli ambienti di anteprima e ora sono disponibili per tutti:

- Dashboard di sicurezza
- Data Protection Dashboard (include panoramiche sulla protezione locale e remota)

Monitor di sistema aggiuntivi

Cloud Insights include i seguenti monitor di sistema:

- Servizio FCP Storage VM non disponibile
- Servizio iSCSI Storage VM non disponibile

Maggio 2023

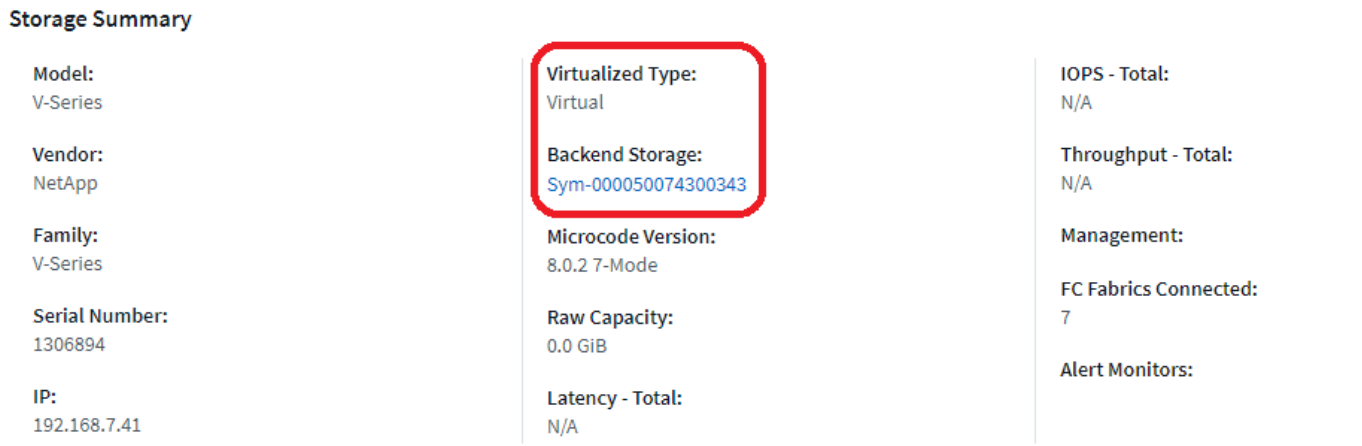
Installazione migliorata dell'operatore di monitoraggio Kubernetes

Installazione e configurazione di "NetApp Kubernetes Monitoring Operator" è più semplice che mai grazie ai seguenti miglioramenti:

- Ambiente "impostazioni di configurazione" sono contenuti in un singolo file di configurazione autodotarato.
- Istruzioni dettagliate per caricare le immagini dell'operatore di monitoraggio Kubernetes nel repository privato.
- Semplice da aggiornare con un singolo comando per aggiornare il monitoraggio Kubernetes mantenendo le configurazioni personalizzate.
- Più sicuro: Le chiavi API gestiscono in modo sicuro i segreti.
- Facile da integrare e implementare con i tool di automazione ci/CD.

Virtualizzazione dello storage

Cloud Insights è in grado di distinguere tra un array di storage con storage locale o virtualizzazione di altri array di storage. In questo modo è possibile correlare i costi e distinguere le performance dal front-end fino al back-end dell'infrastruttura.



Nuovi parametri Webhook

Quando si crea un "Webhook" notifica, ora puoi includere questi parametri nella definizione di webhook:

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%

Creazione di report sui dati Kubernetes

I dati Kubernetes raccolti da Cloud Insights, inclusi volumi persistenti (PV), PVC, carichi di lavoro, cluster e namespace, sono ora disponibili per l'utilizzo in Reporting, che consente chargeback, trend, previsioni, calcoli TTF, E altri report aziendali sulle metriche per Kubernetes.

Monitor di sistema ONTAP predefiniti abilitati per i nuovi clienti

Molti monitor di sistema ONTAP sono abilitati (ad esempio *ripresa*) per impostazione predefinita nei nuovi ambienti Cloud Insights. In precedenza, la maggior parte dei monitor era in stato di default *Paused*. Poiché le esigenze di business variano da azienda a azienda, consigliamo sempre di dare un'occhiata a "monitor di sistema" nel tuo ambiente e mettere in pausa o riprendere ciascuno in base alle tue esigenze di avviso.

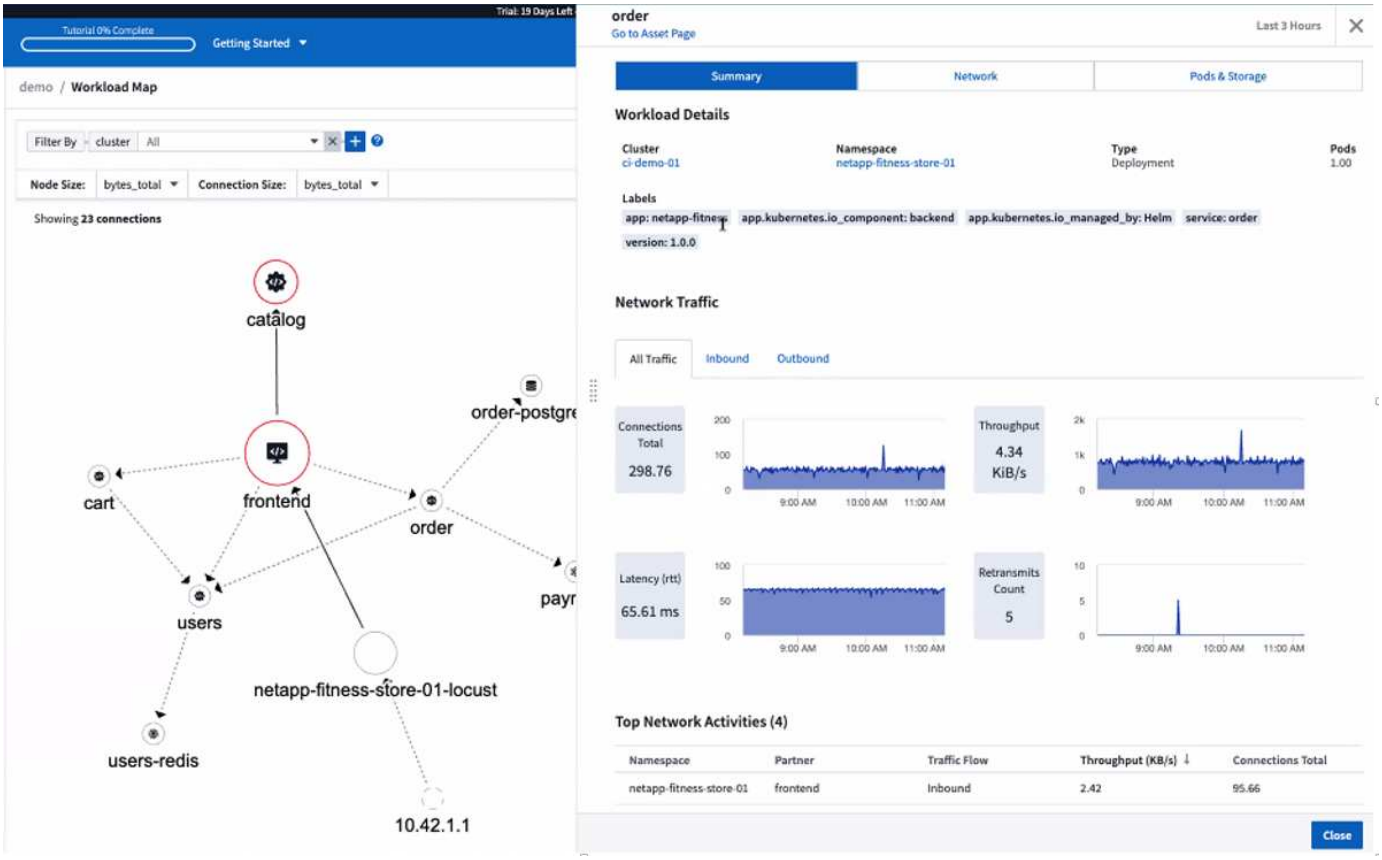
Aprile 2023

Kubernetes Performance Monitoring and Map (monitoraggio e mappa delle performance di Kubernetes)

Il "*Kubernetes Network Performance and Map*" Semplifica la risoluzione dei problemi mappando le dipendenze tra i carichi di lavoro di Kubernetes. Fornisce visibilità in tempo reale sulle latenze e sulle anomalie delle performance di rete di Kubernetes per identificare i problemi di performance prima che influiscano sugli utenti. Questa funzionalità aiuta le organizzazioni a ridurre i costi complessivi analizzando e revisionando i flussi di traffico Kubernetes.

Caratteristiche principali: • La mappa del carico di lavoro presenta le dipendenze e i flussi dei carichi di lavoro di Kubernetes e evidenzia i problemi di rete e di performance. • Monitora il traffico di rete tra pod, carichi di lavoro e nodi Kubernetes; identifica l'origine dei problemi di traffico e latenza. • Riduci i costi complessivi analizzando il traffico di rete in entrata, in uscita, cross-region e cross-zone.

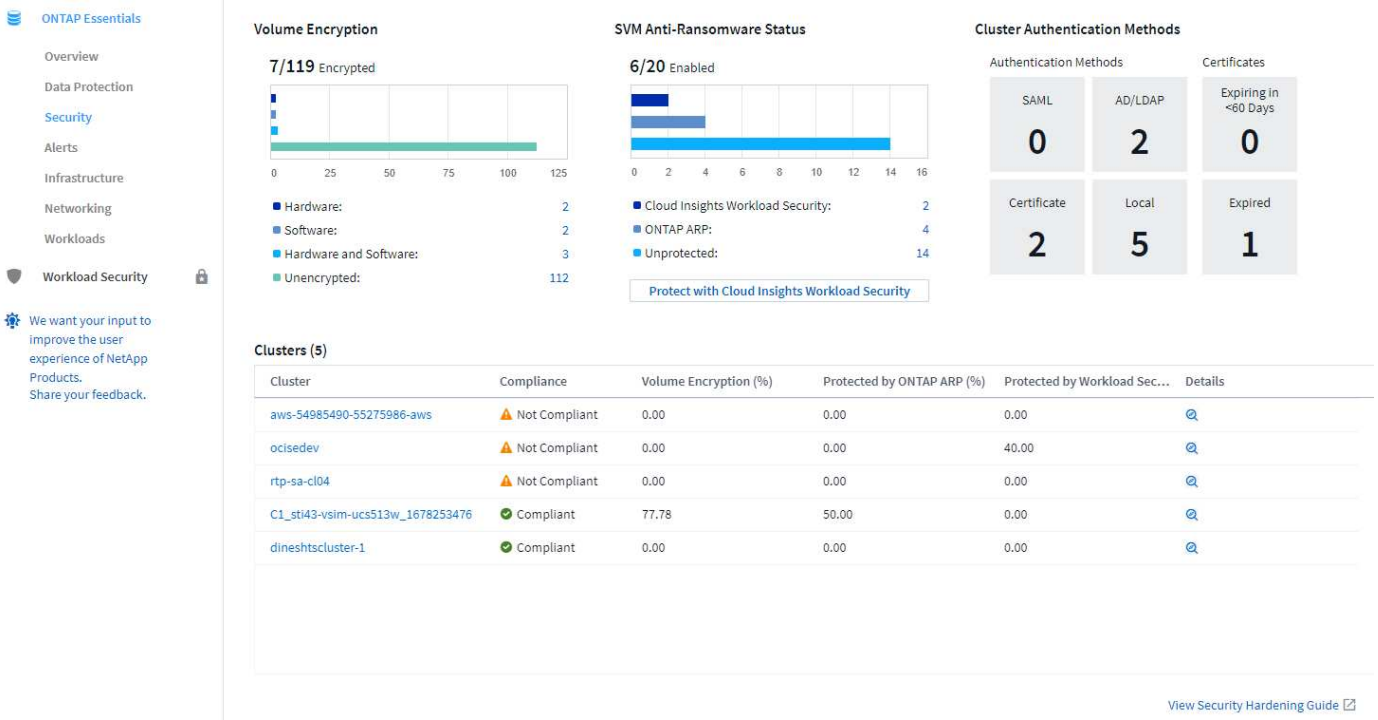
Mappa del carico di lavoro che mostra i dettagli "Slideout":



Kubernetes Performance Monitoring and Map è disponibile come "Anteprima" funzione.

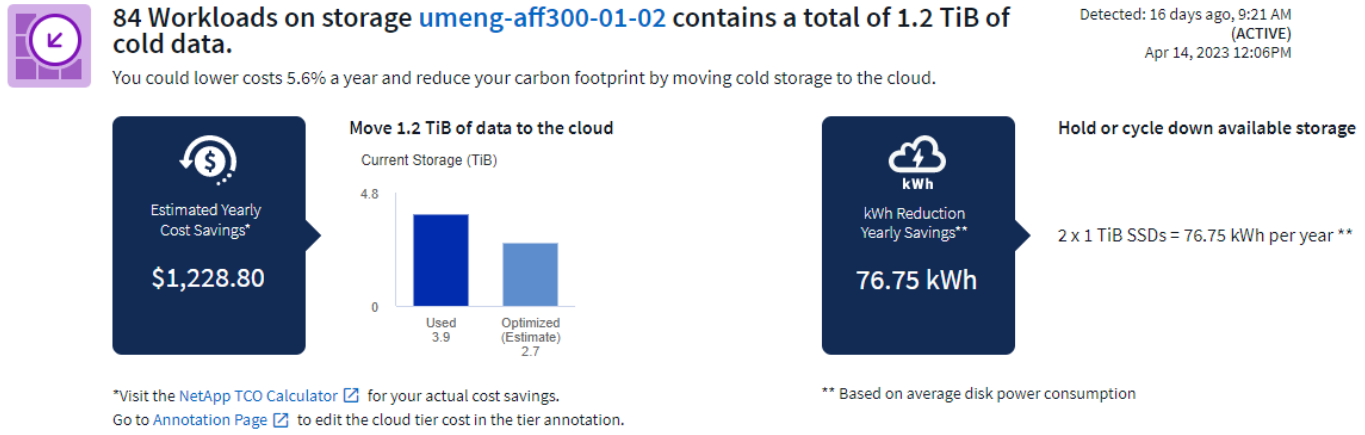
Dashboard di sicurezza di ONTAP Essentials

Il "Dashboard di sicurezza" fornisce una vista istantanea della situazione di sicurezza corrente, mostrando grafici per la crittografia dei volumi hardware e software, lo stato anti-ransomware e i metodi di autenticazione del cluster. Il dashboard di sicurezza è disponibile come "Anteprima" funzione.



Recuperare lo storage a freddo ONTAP

L'analisi di *recupero dello storage a freddo ONTAP* fornisce dati sulla capacità a freddo, sui potenziali risparmi di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP.



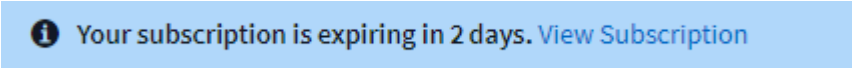
Con questa Insight, puoi rispondere a domande come:

- Quale quantità di dati cold in un cluster di storage si trova su (a) dischi SSD ad alto costo, (b) dischi HDD e (c) dischi virtuali?
- Quali carichi di lavoro contribuiscono maggiormente allo storage non ottimizzato?
- Qual è la durata (in giorni) in cui i dati sono stati cold su un determinato carico di lavoro?

Recuperare lo storage a freddo ONTAP è considerato un "*Anteprima*" ed è pertanto soggetto a modifiche.

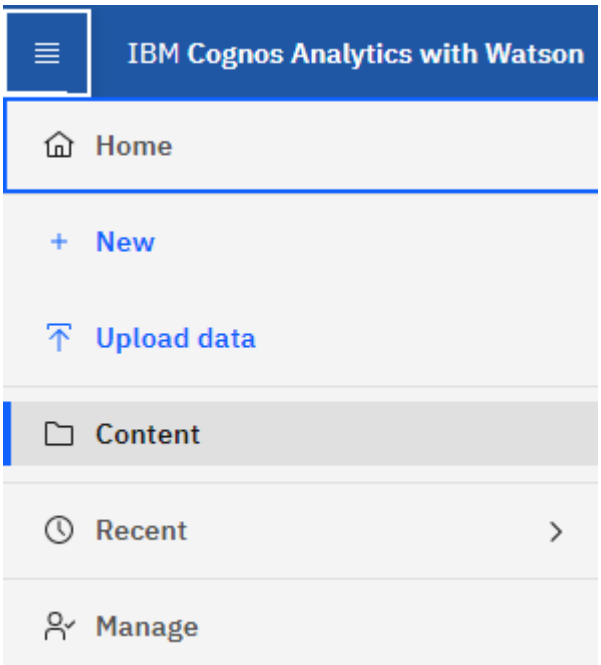
Subscription Notification controlla anche i messaggi banner

L'impostazione dei destinatari per le notifiche di abbonamento (Admin > Notifiche) ora controlla anche chi vedrà le notifiche di banner in-product relative all'abbonamento.



Il reporting ha un nuovo look

Si noterà che le schermate dei report di Cloud Insights hanno un nuovo aspetto e che alcune delle opzioni di navigazione del menu sono state modificate. Queste schermate e le modifiche di navigazione sono state aggiornate nella versione corrente "Documentazione di reporting".



Monitor in pausa per impostazione predefinita

Per i nuovi ambienti Cloud Insights, tenere presente questo "monitor definiti dal sistema" non inviare notifiche di avviso per impostazione predefinita. È necessario attivare le notifiche per qualsiasi monitor che si desidera venga avvisato, aggiungendo uno o più metodi di erogazione per il monitor. Per gli ambienti Cloud Insights esistenti, l'elenco predefinito dei destinatari delle notifiche *globali* è stato rimosso per tutti i monitor definiti dal sistema attualmente in stato di *pausa*. Le notifiche definite dall'utente rimangono invariate, così come le impostazioni di notifica per i monitor definiti dal sistema attualmente attivi.

Stai cercando la scheda API Metering (misurazione API)?

API Metering è stato spostato dalla pagina Subscription (abbonamento) alla pagina **Admin > API Access** (Amministratore > accesso API).

Marzo 2023

Connessione cloud per ONTAP 9.9+ obsoleta

La connessione cloud per il data collector ONTAP 9.9+ è obsoleta. A partire dal 4 aprile 2023, i data collutori di Cloud Connection nel tuo ambiente non raccoglieranno più dati e presenteranno invece un errore durante il polling. Il data collector connessione cloud verrà rimosso completamente da Cloud Insights in un aggiornamento successivo.

Prima del 4 aprile 2023, è obbligatorio configurare un nuovo data collector per il software di gestione dei dati NetApp ONTAP per tutti i sistemi ONTAP attualmente raccolti da Cloud Connection. "Scopri di più".

Gennaio 2023

Nuovi monitor di log

Abbiamo aggiunto quasi due dozzine "monitor di sistema aggiuntivi" per avvisare in caso di collegamenti di interconnessione interrotti, problemi heartbeat e altro ancora. Inoltre, sono stati aggiunti tre nuovi monitor di log per la protezione dei dati, per avvisare sulle modifiche apportate a SnapMirror: Risincronizzazione automatica, mirroring MetroCluster e risincronizzazione FabricPool.

Alcuni di questi monitor saranno *abilitati* per impostazione predefinita; è necessario *mettere in pausa* se non si desidera ricevere avvisi. Si noti inoltre che questi monitor non sono configurati per inviare notifiche; è necessario configurare i destinatari delle notifiche su questi monitor se si desidera inviare avvisi via email o webhook.

Esportazione .CSV per tutti i widget della tabella Dashboard

Garantire l'accessibilità ai tuoi dati è essenziale, per cui abbiamo effettuato l'esportazione in formato .CSV [icona di esportazione .csv] disponibile per tutte le query metriche, i widget della tabella della dashboard e le landing page degli oggetti, indipendentemente dal tipo di dati (risorsa o integrazione) che si sta interrogando.

Le personalizzazioni dei dati, come la selezione delle colonne, la ridenominazione delle colonne e le conversioni delle unità, sono ora incluse nella nuova funzionalità di esportazione.

Dicembre 2022

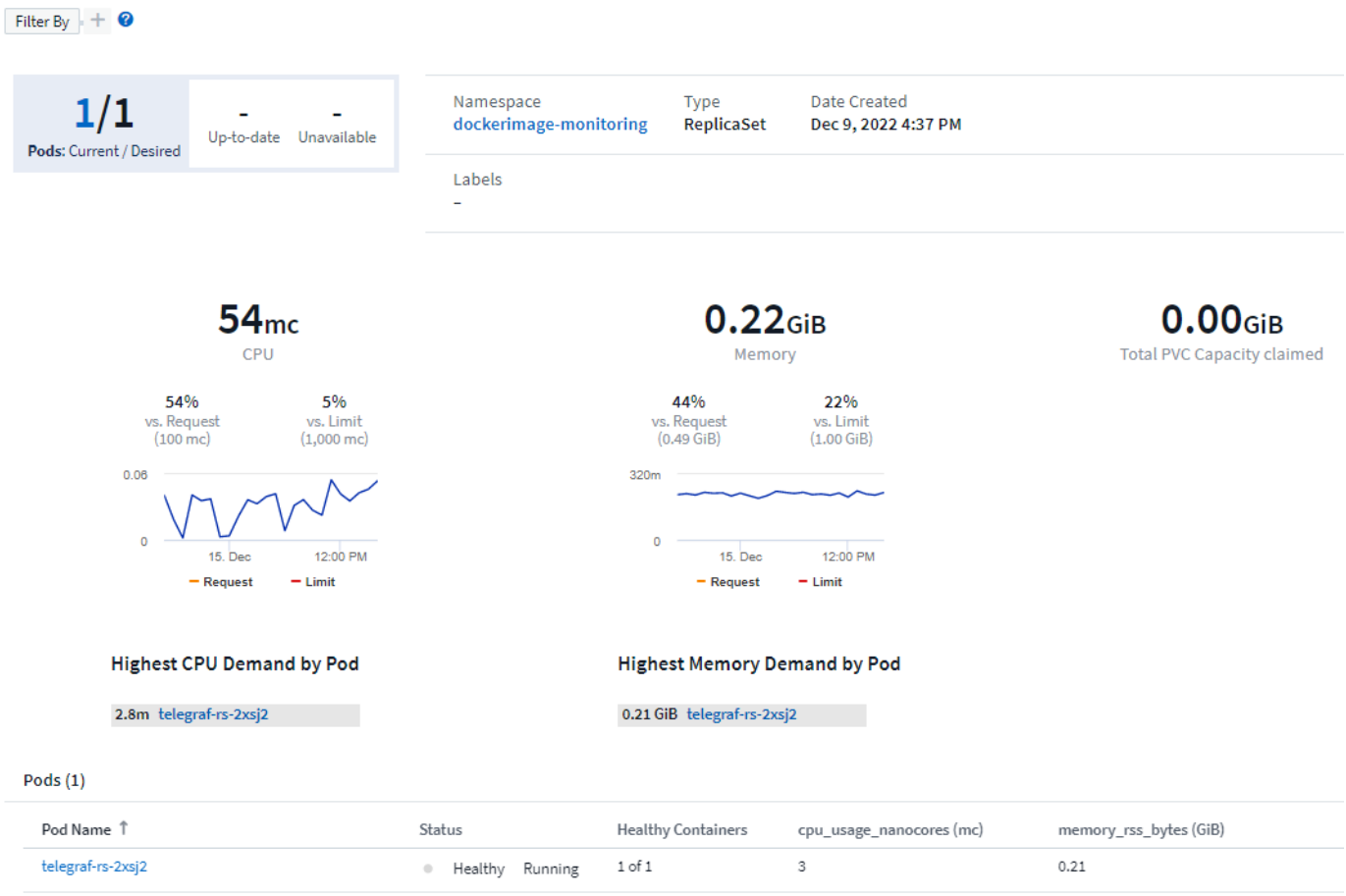
Esplora la protezione ransomware e altre funzionalità di sicurezza durante la versione di prova di Cloud Insights

A partire da oggi, iscrivendoti alla nuova versione di prova di Cloud Insights potrai esplorare le funzionalità di sicurezza come il rilevamento ransomware e la policy di risposta automatica per il blocco degli utenti. Se non ti sei iscritto alla versione di prova, puoi farlo oggi stesso!

I carichi di lavoro di Kubernetes dispongono di una landing page personalizzata

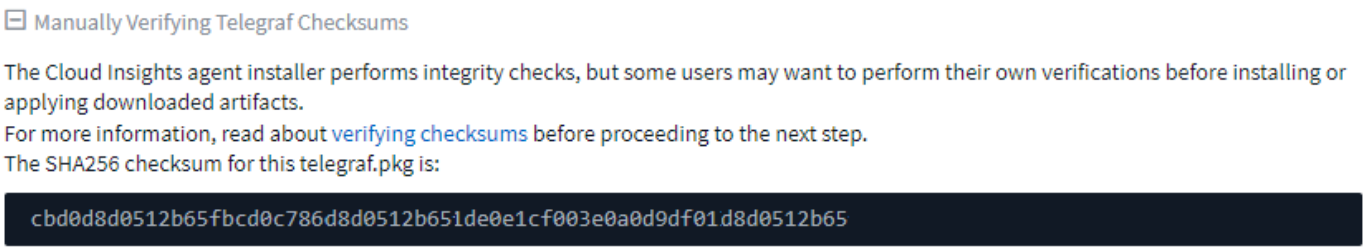
I carichi di lavoro sono una parte chiave del tuo ambiente Kubernetes, quindi Cloud Insights ora fornisce le landing page per questi carichi di lavoro. Da qui puoi visualizzare, esplorare e risolvere i problemi che

influiscono sui carichi di lavoro Kubernetes.



Controlla i checksum

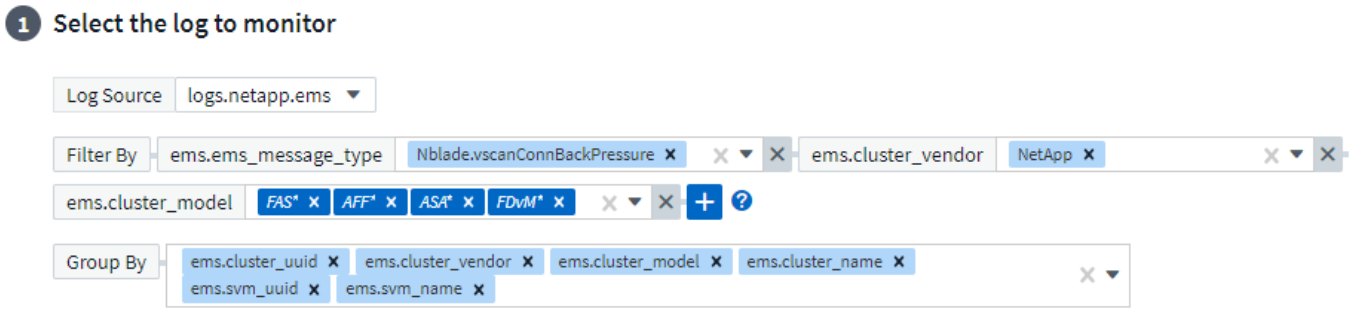
Ci hai chiesto di fornirti i valori checksum durante l'installazione dell'agente per Windows e Linux e pensiamo che sia un'ottima idea. Ecco quindi:



Miglioramenti di Log Alerting

Raggruppa per

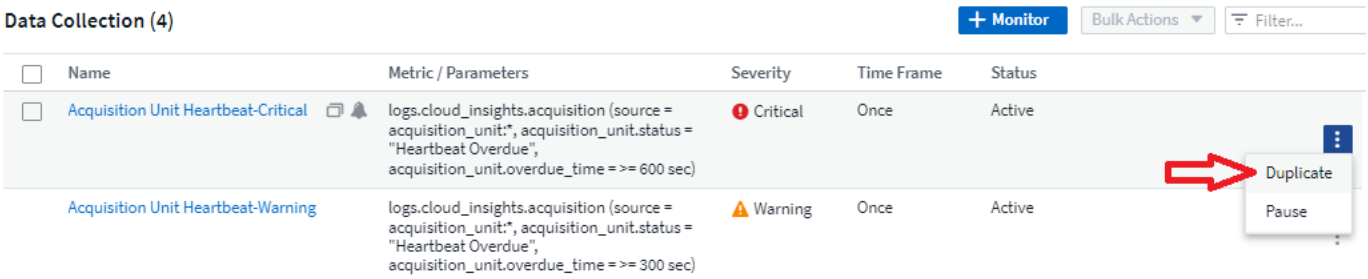
Quando si crea o si modifica un Log Monitor, è ora possibile impostare gli attributi "Group by" (Raggruppa per) per consentire avvisi più mirati. Cercare gli attributi "Group by" (Raggruppa per) sotto le impostazioni "Filter" (filtro) nella definizione del monitor.



Questa modifica consente ai monitor metrici e ai monitor di log di ottenere la parità delle funzioni normalizzando l'aspetto "Group by" (Raggruppa per) delle definizioni dei monitor. Questa parità consentirà ai clienti di clonare/duplicare **tutti** i monitor predefiniti definiti dal sistema per un'ulteriore personalizzazione.

Duplicazione

È ora possibile clonare (duplicare) i monitor Change Log, Kubernetes Log e Data Collector Log. In questo modo viene creato un nuovo monitor di log personalizzato che è possibile modificare in base alle definizioni specifiche.



11 nuovi monitor ONTAP predefiniti che coprono SnapMirror per la business continuity

Abbiamo aggiunto quasi una dozzina di novità "monitor di sistema" Per SnapMirror for Business Continuity (SMBC), che avvisa in caso di modifiche ai certificati SMBC e ai mediatori ONTAP.

Novembre 2022

Più di 40 nuovi monitor di sicurezza, raccolta dati e CVO!

Abbiamo aggiunto decine di nuovi monitor definiti dal sistema per avvisarti di potenziali problemi con Cloud Volumes, sicurezza e protezione dei dati. Scopri di più su questi monitor "qui".

Ottobre 2022

Rilevamento ransomware migliore e più accurato con l'integrazione della protezione ransomware autonoma di ONTAP

Cloud Secure migliora il rilevamento ransomware attraverso l'integrazione con ONTAP "Protezione ransomware autonoma" (ARP).

Cloud Secure riceve gli eventi ARP di ONTAP sulla potenziale attività di crittografia dei file di volume, e.

- Correla gli eventi di crittografia dei volumi con l'attività dell'utente per identificare chi causa il danno,
- Implementa policy di risposta automatica per bloccare l'attacco,
- Identifica i file interessati, contribuendo a ripristinarli più rapidamente e a condurre indagini sulle violazioni dei dati.

Settembre 2022

Monitor disponibili nell'edizione di base

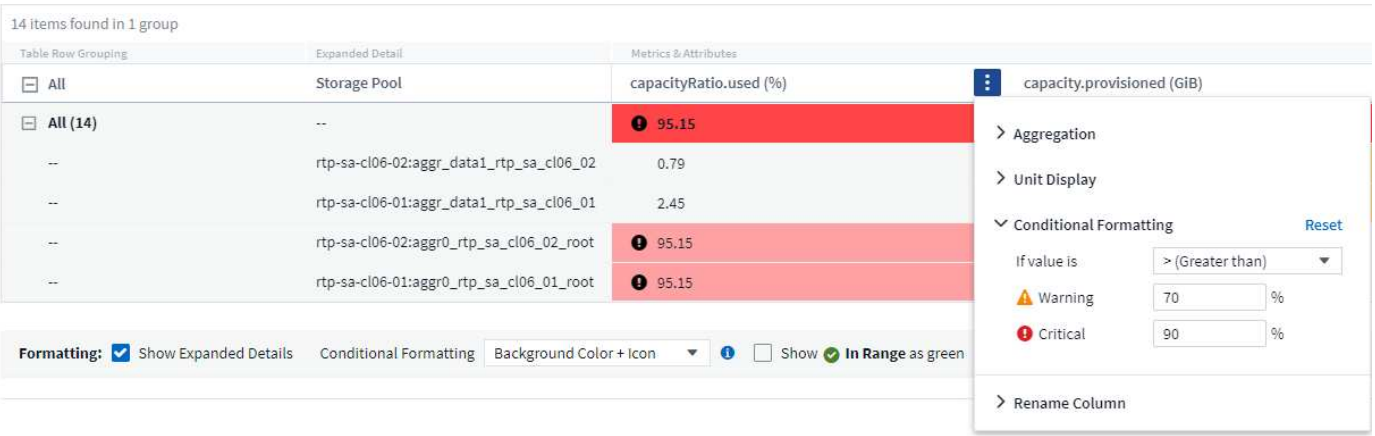
ONTAP "Monitor predefiniti" Ora disponibile per l'utilizzo nell'edizione di base di Cloud Insights. Questo include oltre 70 monitor dell'infrastruttura e 30 esempi di workload.

Dashboard di alimentazione e StorageGRID di ONTAP

La galleria del dashboard include una nuova dashboard per l'alimentazione e la temperatura ONTAP e quattro dashboard per StorageGRID. Se il tuo ambiente sta raccogliendo metriche di alimentazione ONTAP e/o dati StorageGRID, importa queste dashboard selezionando **+dalla galleria**.

Visibilità della soglia immediata nelle tabelle

La formattazione condizionale consente di impostare ed evidenziare le soglie di livello di avviso e critico nei widget delle tabelle, offrendo visibilità istantanea agli outlier e ai punti dati eccezionali.

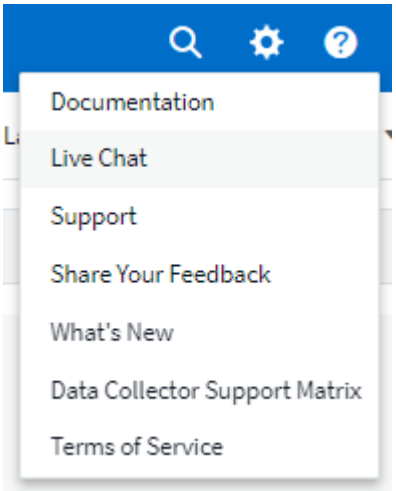


Security Monitor

Cloud Insights può avvisare l'utente quando rileva che la modalità FIPS è disattivata sul sistema ONTAP. Scopri di più "Monitor di sistema"E guarda questo spazio per altri Security Monitor, presto disponibili!

Chat ovunque

Chatta con uno specialista del supporto NetApp da qualsiasi schermata Cloud Insights selezionando il nuovo collegamento **Guida > Chat live**. La guida è disponibile nella sezione "?" nella parte superiore destra dello schermo.



Approfondimenti più visibili

Se l'ambiente in uso sta riscontrando un "Insight" Ad esempio *risorse condivise sotto stress* o *Kubernetes Namespace che stanno esaurendo lo spazio*, le landing page delle risorse interessate ora includono collegamenti alla Insight stessa, che consentono un'esplorazione e un troubleshooting più rapidi.

Nuovi Data Collector

- Amazon S3 (disponibile in anteprima)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0

Altri aggiornamenti di Data Collector

Tutte le origini dati sono ora ottimizzate per riprendere il polling delle performance dopo gli aggiornamenti e/o le patch dell'unità di acquisizione.

Supporto del sistema operativo

Oltre a questi, le unità di acquisizione Cloud Insights supportano i seguenti sistemi operativi "già supportato":

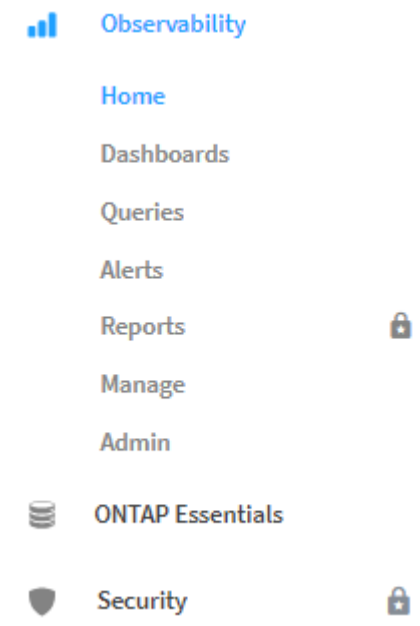
- Red Hat Enterprise Linux 8.5, 8.6

Agosto 2022

Cloud Insights ha un nuovo look!

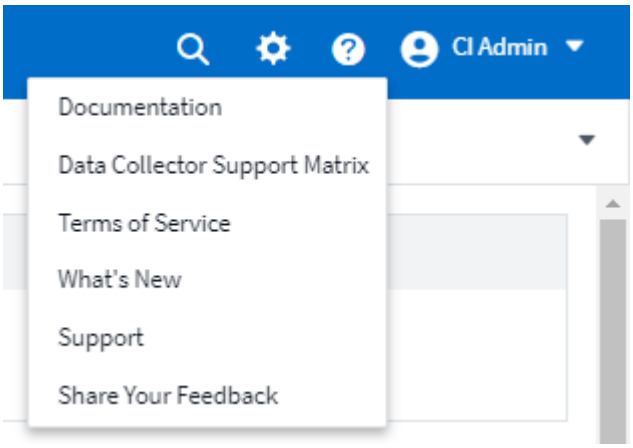
A partire da questo mese, "Monitor and Optimize" è stato rinominato **Observability**. Qui troverai tutte le tue funzionalità preferite, come dashboard, query, avvisi e report. Inoltre, cercare Cloud Secure nel nuovo menu

sicurezza. Si noti che solo i menu sono stati modificati; la funzionalità delle funzioni rimane invariata.



Cerchi il menu **Help**?

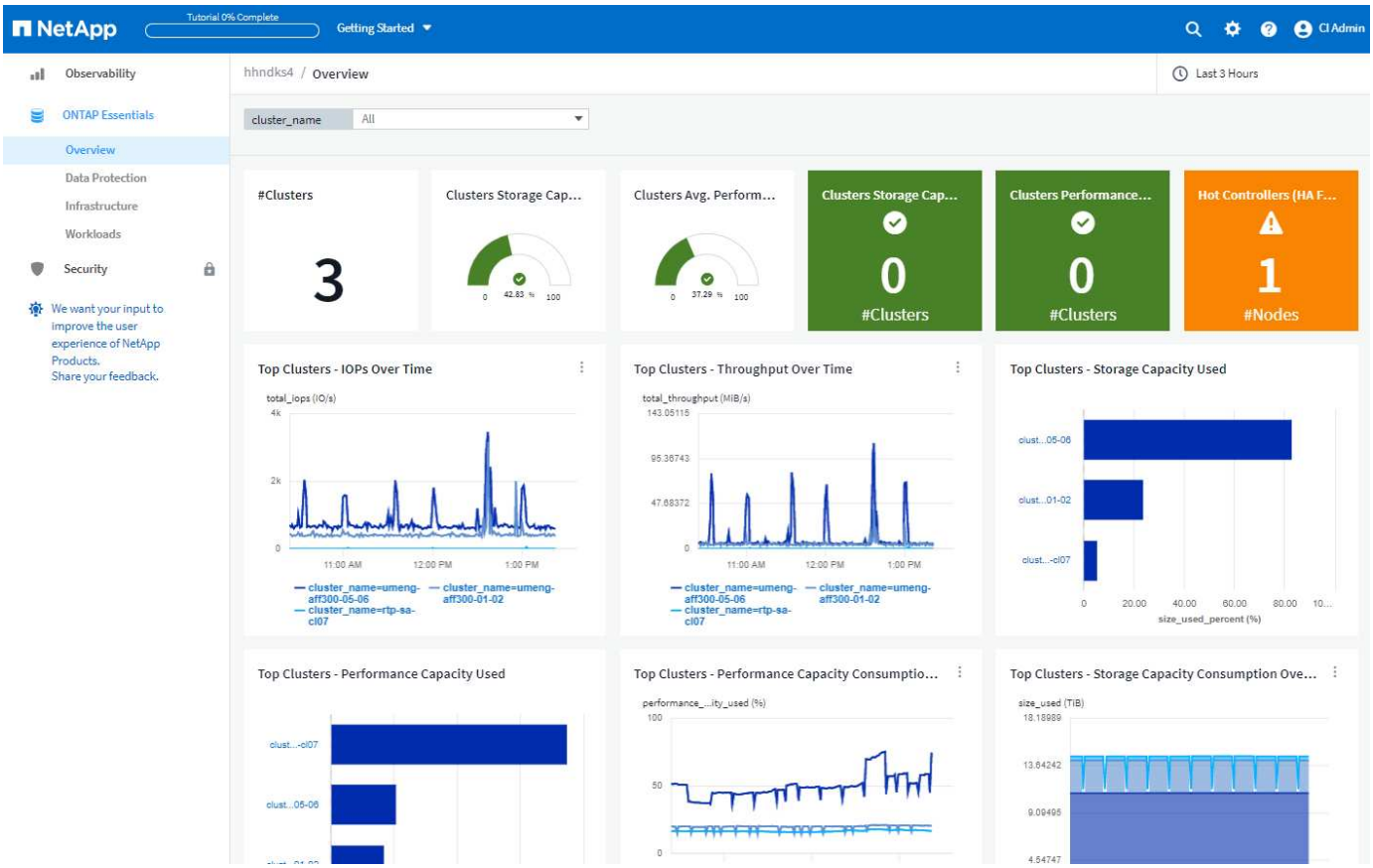
La guida ora si trova nella parte superiore destra dello schermo.



Non sai da dove iniziare? Scopri gli elementi essenziali di ONTAP!

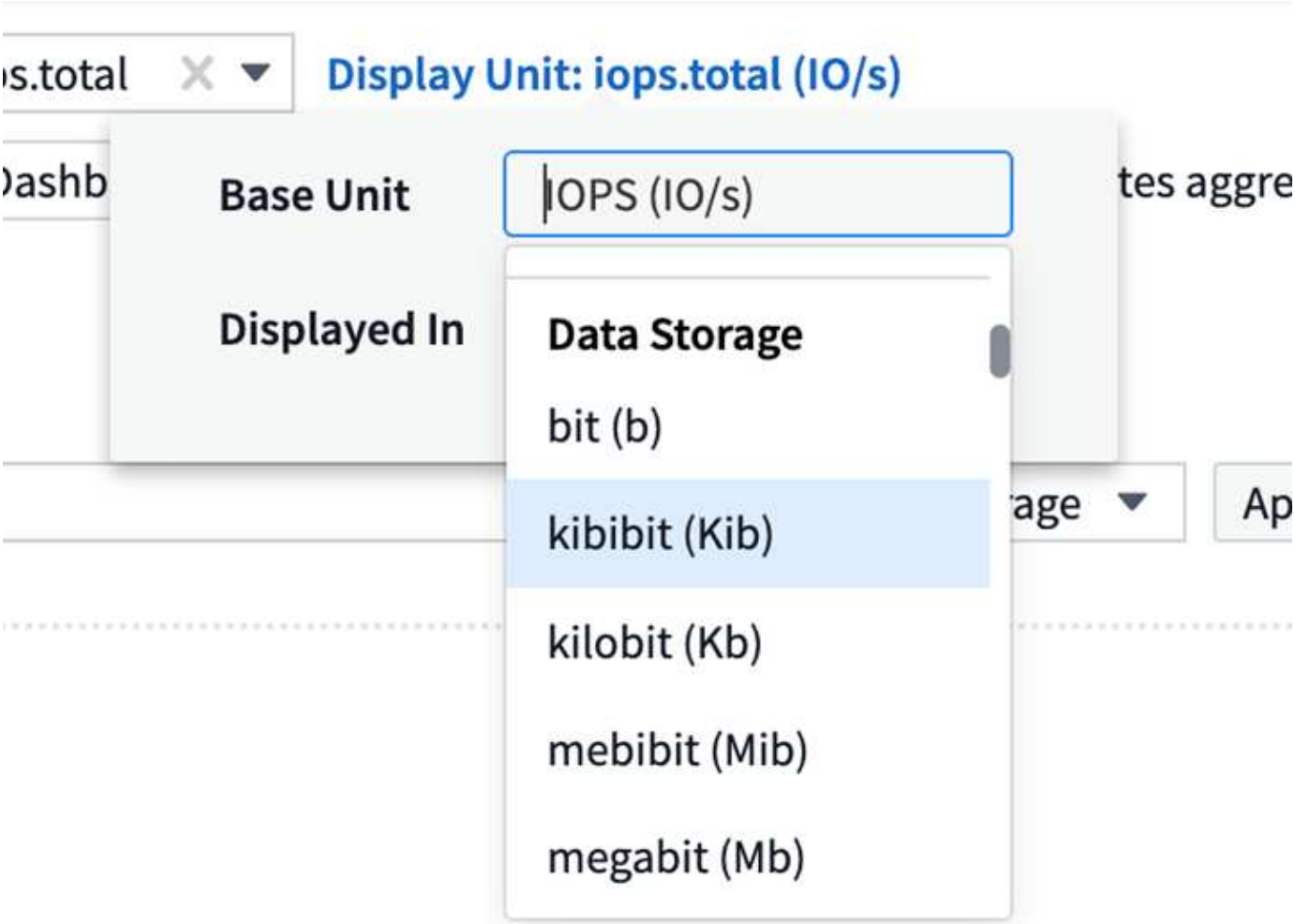
"Elementi essenziali di ONTAP" È un insieme di dashboard e flussi di lavoro che offre viste dettagliate degli inventari, dei carichi di lavoro e della protezione dei dati di NetApp ONTAP, incluse previsioni da giorni a completi per capacità e performance dello storage. Puoi anche vedere se alcuni controller sono in esecuzione con un utilizzo elevato. ONTAP Essentials è il posto ideale per tutte le tue esigenze di monitoraggio di NetApp ONTAP.

ONTAP Essentials, disponibile in tutte le edizioni, è progettato per essere intuitivo per gli operatori e gli amministratori ONTAP esistenti, semplificando la transizione da ActiveIQ Unified Manager a tool di gestione basati sui servizi.



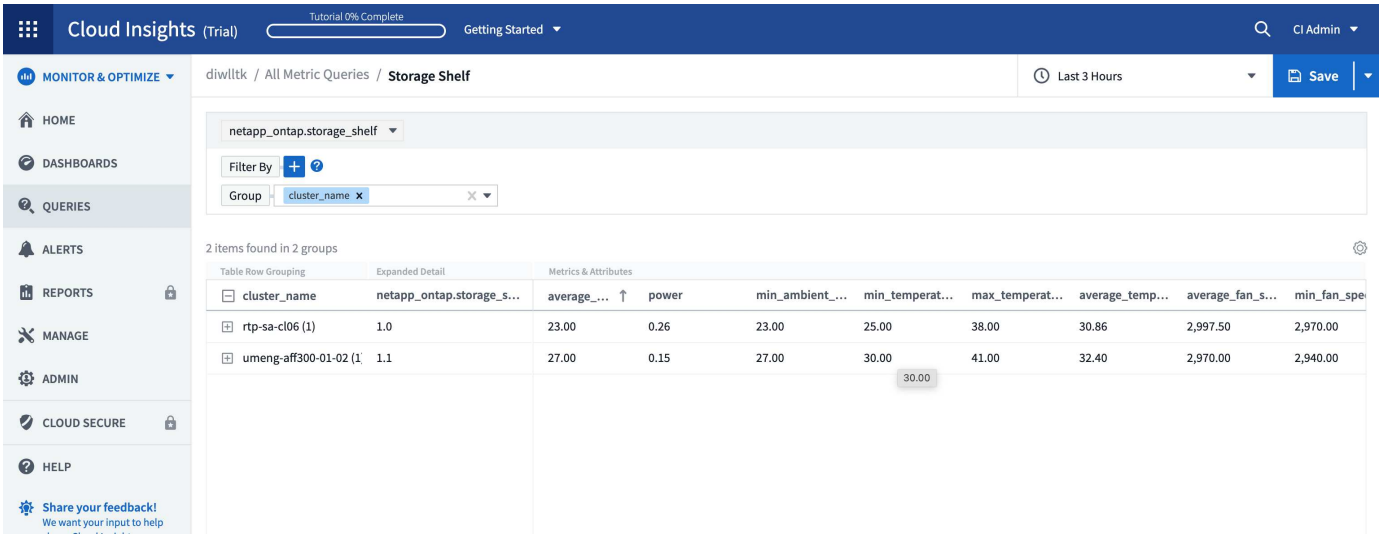
Le famiglie di dati di storage vengono unite

Hai chiesto e ora CE l'hai. Le unità dati di base 2 e 10 di storage sono ora combinate in un'unica famiglia, da bit e byte a tebbit e terabyte, semplificando la visualizzazione dei dati nelle dashboard. I data rate sono ora anche una grande famiglia di prodotti.



Quanta energia utilizza lo storage?

Visualizza e monitora il tuo shelf di storage ONTAP e il consumo energetico del nodo, la temperatura e la velocità della ventola utilizzando le metriche netapp_ontap.storage_shelf, netapp_ontap.system_node e netapp_ontap.cluster (solo consumo di energia).



Funzionalità graduate da Preview

Le seguenti funzionalità sono state spostate da Anteprima e sono ora disponibili per tutti i clienti:

Funzione	Descrizione
Kubernetes Namespace che esauriscono lo spazio	L'Insight *Kubernetes Namespace running of Space* ti offre una vista dei carichi di lavoro degli spazi dei nomi Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si esaurisca."Scopri di più"
Risorsa condivisa sotto stress	L'Insight di *Shared Resource Under stress* utilizza ai/ML per identificare automaticamente dove il conflitto di risorse sta causando il degrado delle performance nel tuo ambiente, evidenzia i carichi di lavoro interessati dall'IT e fornisce le azioni consigliate per risolvere i problemi di performance più rapidamente."Scopri di più"
Cloud Secure: Blocca l'accesso degli utenti in caso di attacco	Maggiore protezione dei dati business-critical con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatizzate o manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Scopri di più"

Qual è lo stato di salute della raccolta dati?

Cloud Insights offre due nuovi monitor heartbeat per le unità di acquisizione, oltre a due monitor per avvisare in caso di guasti del data collector. Questi possono essere utilizzati per avvisare rapidamente i clienti in caso di problemi di raccolta dei dati.

I seguenti monitor sono ora disponibili nel gruppo di monitor *Data Collection*:

- Unità di acquisizione: Heartbeat-critical
- Heartbeat unità di acquisizione - Avviso
- Collector non riuscito
- Avviso di raccolta

Si noti che questi monitor sono in stato *Paused* per impostazione predefinita. Attivarli per essere avvisati in caso di problemi di raccolta dei dati.

Rinnovo automatico dei token API

È ora possibile impostare i token di accesso API per il rinnovo automatico. Attivando questa funzione, i token di accesso API nuovi/aggiornati verranno generati automaticamente per i token in scadenza. Gli agenti Cloud Insights che utilizzano un token in scadenza verranno aggiornati automaticamente per utilizzare il corrispondente token di accesso API nuovo/aggiornato, consentendo loro di continuare a funzionare senza problemi. Quando crei il token, seleziona la casella "Rinnova automaticamente il token". Questa funzione è attualmente supportata dagli agenti Cloud Insights in esecuzione sulla piattaforma Kubernetes con l'ultimo operatore di monitoraggio di NetApp Kubernetes.

Basic Edition offre molto di più

La versione di prova è terminata, ma non sei ancora sicuro se un abbonamento è adatto a te? L'edizione di base ti ha sempre dato la possibilità di continuare a utilizzare Cloud Insights con il tuo attuale data collector ONTAP, ma ora puoi continuare a catturare anche la versione, la topologia e i dati IOPS/throughput/latenza di VMware. I clienti NetApp con supporto Premium sui propri sistemi storage avranno diritto al supporto per Cloud Insights.

Sei pronto per saperne di più?

Consulta la sezione **Learning Center** della pagina Guida > supporto per i link alle offerte dei corsi NetApp University Cloud Insights.

Supporto del sistema operativo

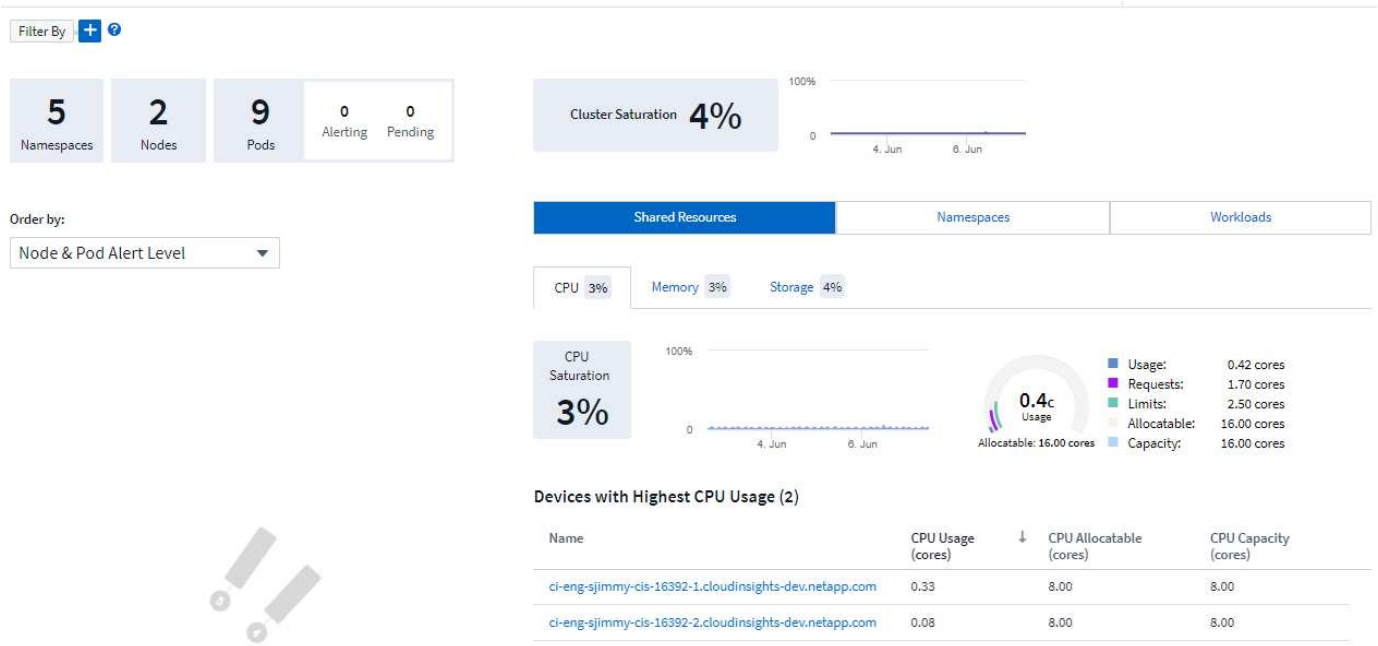
Oltre a questi, le unità di acquisizione Cloud Insights supportano anche il seguente sistema operativo "già supportato":

- Windows 11

Giugno 2022

Kubernetes saturazione del cluster e altri dettagli

Cloud Insights semplifica l'esplorazione dell'ambiente Kubernetes con una pagina dei dettagli del cluster migliorata che fornisce dettagli sulla saturazione e una vista più pulita degli spazi dei nomi e dei carichi di lavoro.



La pagina dell'elenco dei cluster offre inoltre una rapida visualizzazione della saturazione, oltre ai conteggi di nodi, Pod, namespace e workload:

Filter By

Clusters (2)

Name	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

Quanti anni ha il tuo cluster Kubernetes?

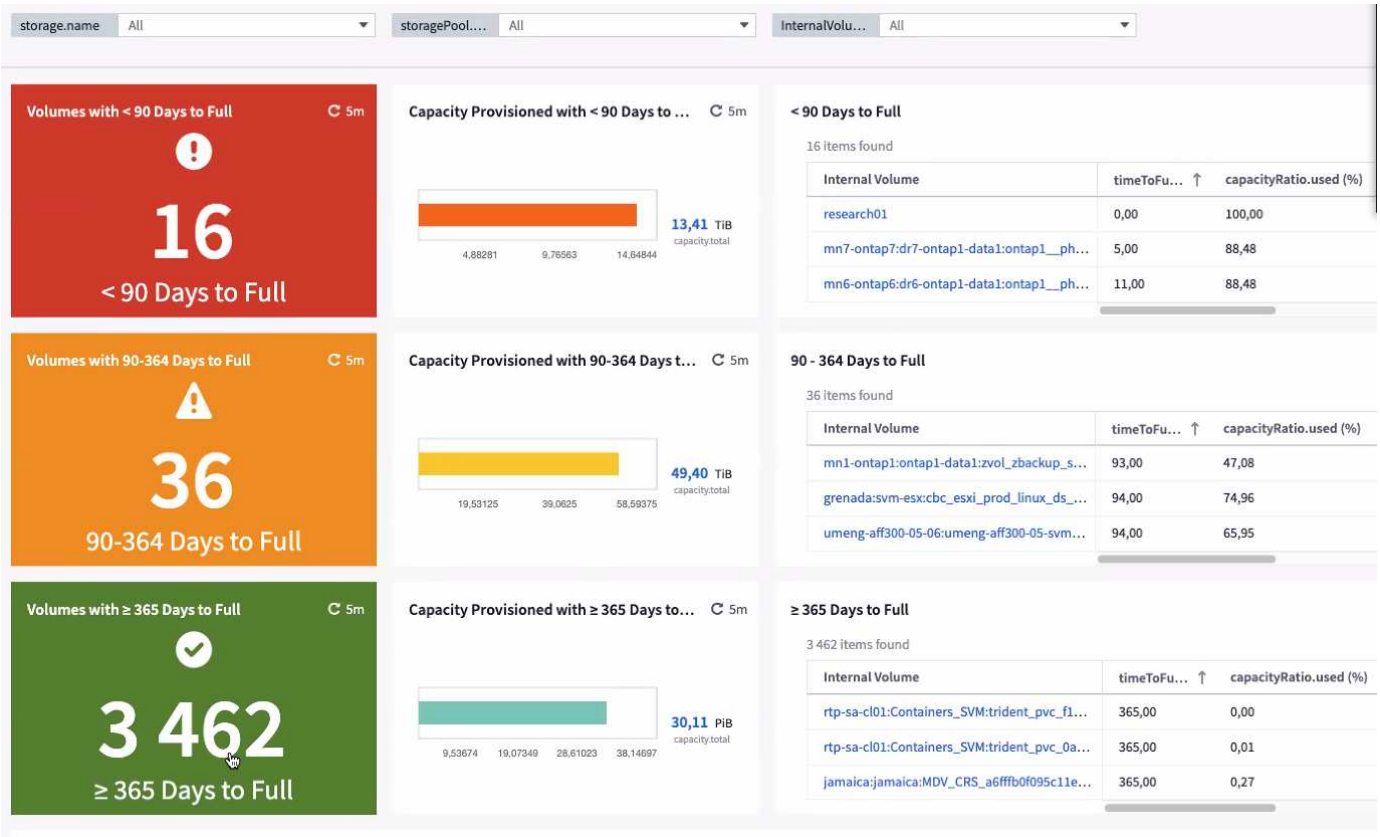
Il tuo cluster sta iniziando solo nel mondo o ha vissuto una lunga vita digitale? *Age* è stato aggiunto come metrica temporale raccolta per i nodi Kubernetes.

2 items found in 2 groups

Table Row Grouping		Expanded Detail	Metrics & Attributes
node_name	kubernetes_cluster	kubernetes.node	age (day)
ci-aumonitors-1 (1)	aumonitors	ci-aumonitors-1	10.82
ci-aumonitors-2 (1)	aumonitors	ci-aumonitors-2	10.82

Previsione del time-to-full della capacità

Cloud Insights fornisce un dashboard per prevedere il numero di giorni fino allo scadere della capacità per ogni volume interno monitorato. Questi valori possono contribuire a ridurre significativamente il rischio di un'interruzione.



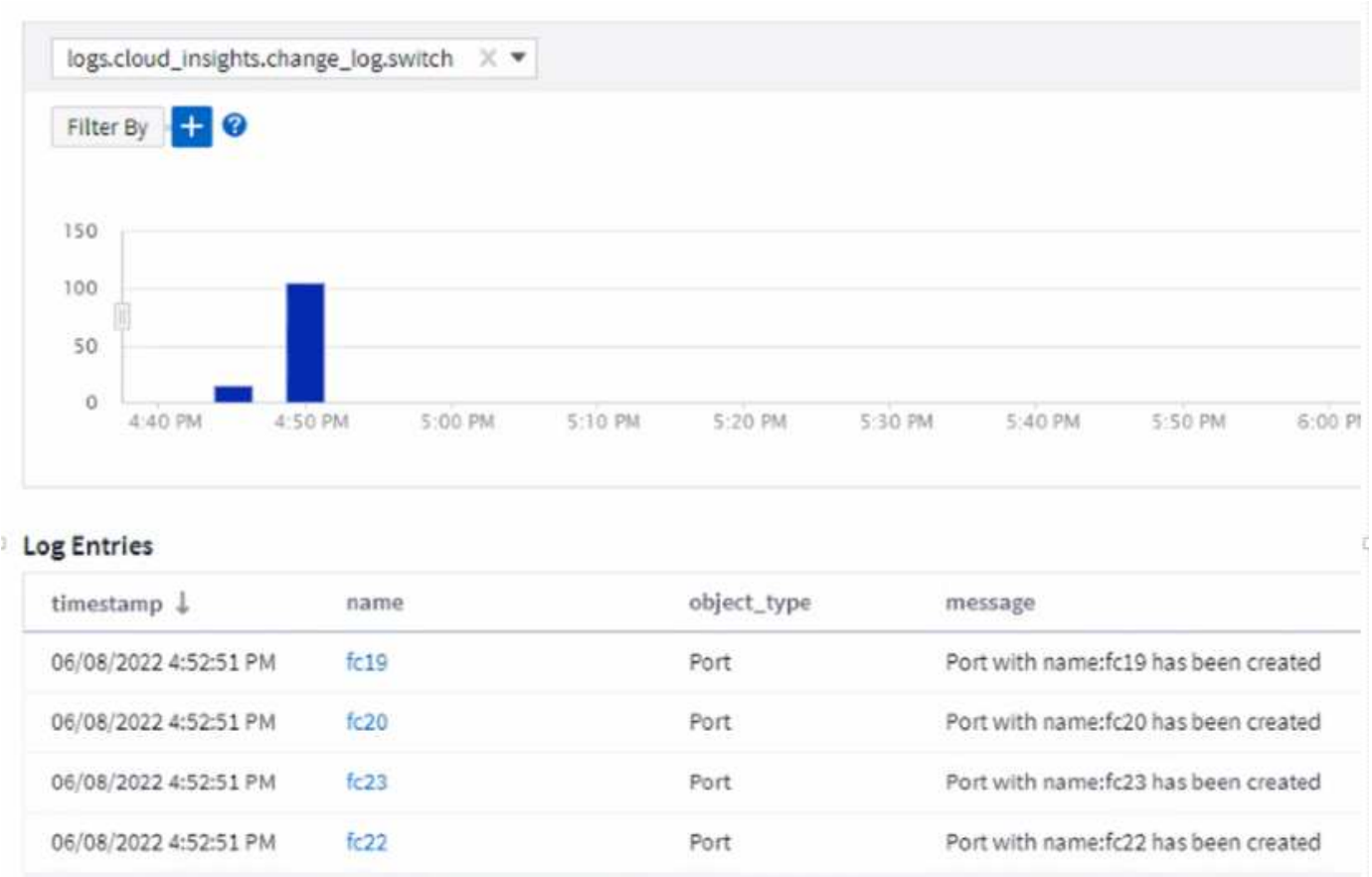
I contatori TTF sono disponibili anche per Storage, Storage Pool e Volume. Continua a guardare questo spazio

per ulteriori dashboard per questi oggetti.

Si noti che le previsioni Time-to-Full stanno per uscire da *Preview* e verranno implementate a tutti i clienti.

Cosa è cambiato nel mio ambiente?

Le voci del registro delle modifiche ONTAP possono essere visualizzate in esplora log.



Supporto del sistema operativo

Oltre a questi, le unità di acquisizione Cloud Insights supportano i seguenti sistemi operativi "già supportato":

- CentOS Stream 9
- Windows 2022

Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato alla versione **1.22.3**, con miglioramenti in termini di performance e sicurezza. Gli utenti che desiderano eseguire l'aggiornamento possono fare riferimento alla sezione relativa all'aggiornamento appropriata di "Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza richiedere alcuna azione da parte dell'utente.

Funzioni di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se si desidera visualizzare l'anteprima di una o più di queste funzioni, contattare il "Team di vendita NetApp" per ulteriori

informazioni.

Funzione	Descrizione
Kubernetes Namespace che esauriscono lo spazio	L'Insight *Kubernetes Namespace running of Space* ti offre una vista dei carichi di lavoro degli spazi dei nomi Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si esaurisca."Scopri di più"
Cloud Secure: Blocca l'accesso degli utenti in caso di attacco	Maggiore protezione dei dati business-critical con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatica o manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Scopri di più"
Risorsa condivisa sotto stress	L'Insight di *Shared Resource Under stress* utilizza ai/ML per identificare automaticamente dove il conflitto di risorse sta causando il degrado delle performance nel tuo ambiente, evidenzia i carichi di lavoro interessati dall'IT e fornisce le azioni consigliate per risolvere i problemi di performance più rapidamente."Scopri di più"

Maggio 2022

Chat live con il supporto NetApp

Ora puoi chattare in diretta con il personale del supporto NetApp! Nella pagina Help > Support (Guida > supporto tecnico), fare clic sull'icona Chat o fare clic su *Chat* nella sezione "Contact US" (Contattaci) per avviare una sessione di chat. Il supporto via chat è disponibile nei giorni feriali USA per gli utenti Standard e Premium Edition.

Operatore Kubernetes

Abbiamo reso più semplice l'installazione e l'esecuzione con il monitoraggio avanzato di Kubernetes e cluster explorer di Cloud Insights.

Il "NetApp Kubernetes Monitoring Operator" (NKMO) è il metodo preferito per l'installazione di Kubernetes per Cloud Insights Insights, per una configurazione più flessibile del monitoraggio in meno passaggi, oltre a maggiori opportunità per il monitoraggio di altri software in esecuzione nel cluster K8s.

Fare clic sul collegamento riportato sopra per ulteriori informazioni e prerequisiti

Gestisci utenti e inviti con API

Ora puoi gestire utenti e inviti utilizzando la potente API di Cloud Insights. Per ulteriori informazioni, consultare "Documentazione API Swagger".

Avvisi di raccolta dati

Non lasciarti sfuggire le metriche critiche a causa di un collector guasto.

Tenere traccia dei dati raccolti è più facile che mai con il nuovo "avvisi" per guasti dell'unità di acquisizione e del data collector. Tenere presente che questi monitor sono *in pausa* per impostazione predefinita. Per attivarla, accedere alla pagina dei monitor e individuare e riprendere "Acquisition Unit Shutdown" (arresto unità di acquisizione) e "Collector Failed" (collettore non riuscito)

Avviso sulle modifiche dello storage ONTAP

Non lasciare che modifiche dello storage impreviste portino a interruzioni!

È ora possibile configurare Cloud Insights in modo che avvisi quando vengono rilevate modifiche o rimozione di FlexVol, nodi e SVM sui sistemi ONTAP.

Funzioni di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se si desidera visualizzare l'anteprima di una o più di queste funzioni, contattare il "Team di vendita NetApp" per ulteriori informazioni.

Funzione	Descrizione
Kubernetes Namespace che esauriscono lo spazio	L'Insight *Kubernetes Namespace running of Space* ti offre una vista dei carichi di lavoro degli spazi dei nomi Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si esaurisca."Scopri di più"
Previsione del time-to-full del volume interno e della capacità del volume	Cloud Insights è in grado di programmare il numero di giorni fino allo scadere della capacità per ogni volume interno e volume monitorato. Questo valore può contribuire a ridurre significativamente il rischio di un'interruzione.
Cloud Secure: Blocca l'accesso degli utenti in caso di attacco	Maggiore protezione dei dati business-critical con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatica o manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Scopri di più"
Risorsa condivisa sotto stress	L'Insight di *Shared Resource Under stress* utilizza ai/ML per identificare automaticamente dove il conflitto di risorse sta causando il degrado delle performance nel tuo ambiente, evidenzia i carichi di lavoro interessati dall'IT e fornisce le azioni consigliate per risolvere i problemi di performance più rapidamente."Scopri di più"

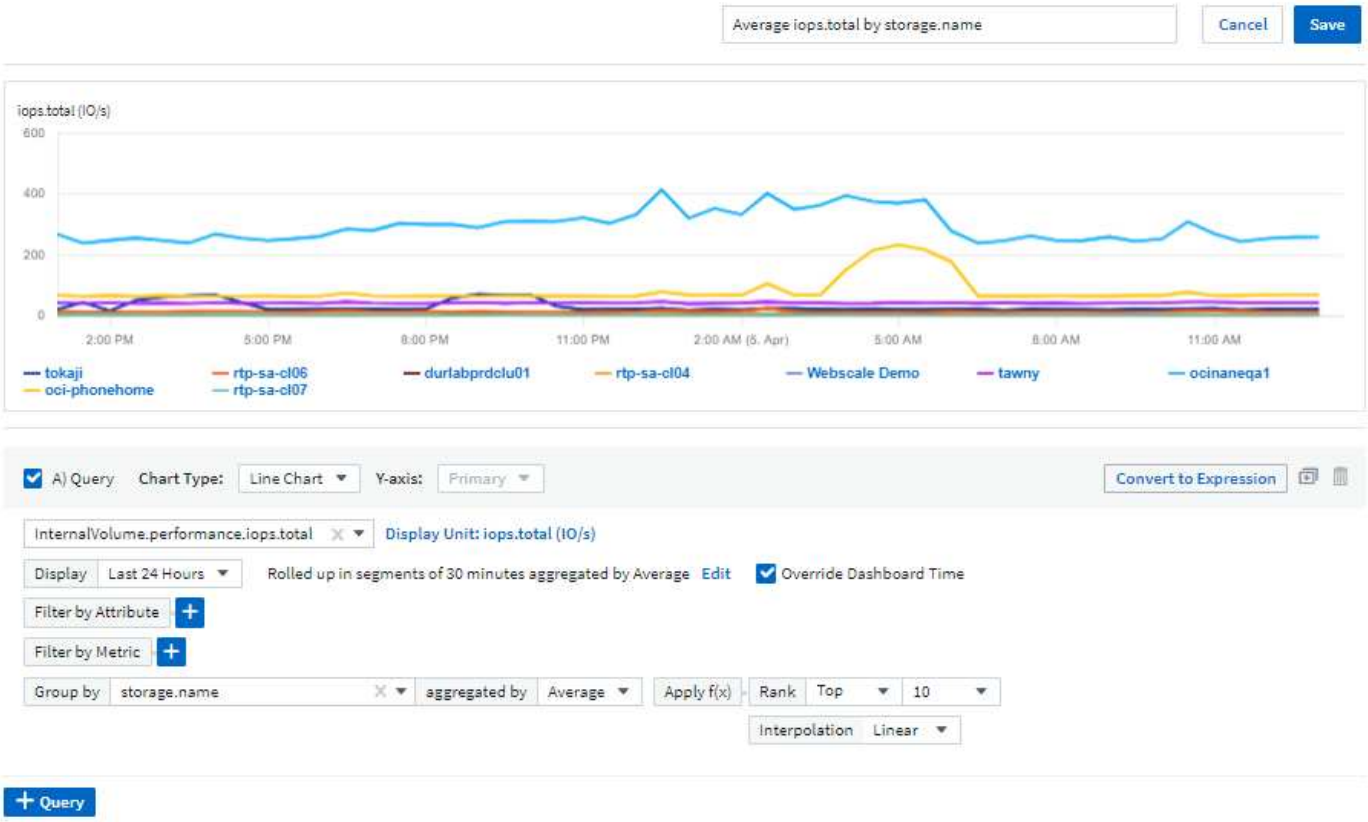
Aprile 2022

Condividi il tuo feedback!

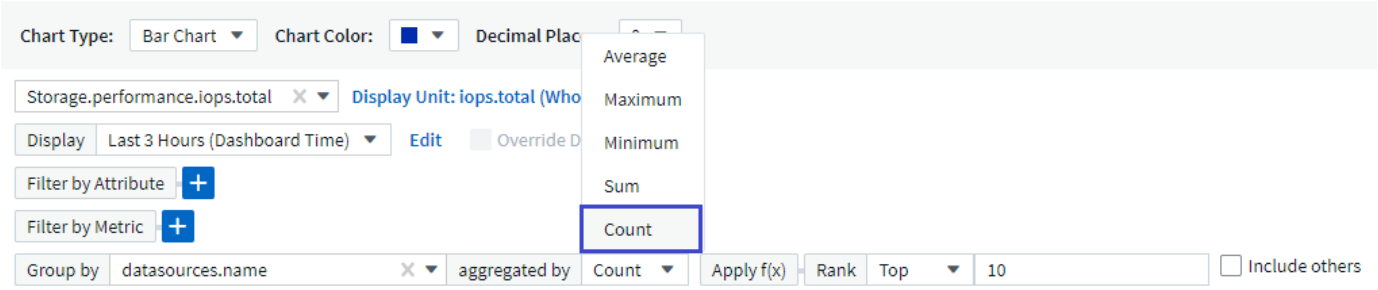
Vogliamo che il tuo contributo contribuiscano a dare forma a Cloud Insights. Guadagna punti e premi partecipando al programma **Insights to Action** di NetApp. "**Iscriviti subito**"!

Aggiornato Dashboard Editor

Abbiamo rivisto i nostri strumenti di creazione della dashboard per semplificare la visualizzazione dei dati in modo ancora più rapido. Accedere alla pagina "Dashboard" di Cloud Insights per modificare una dashboard esistente, aggiungerne una dalla galleria o crearne una nuova per visualizzarla.



È stato inoltre introdotto un nuovo metodo di aggregazione dei conteggi. Quando si raggruppano i dati in un grafico a barre, un grafico a colonne e un grafico a torta, è possibile visualizzare in modo rapido e semplice il numero di oggetti rilevanti per la metrica selezionata.



Inoltre, i grafici a linee consentono ora di selezionare una delle tre opzioni "interpolazione" metodi:

- Nessuno - non viene eseguita alcuna interpolazione
- Lineare - interpola un punto dati tra i punti esistenti
- Scala - utilizza il punto dati precedente come punto dati interpolato

Monitoraggio avanzato per l'infrastruttura Kubernetes

Cloud Insights ti tiene al corrente delle modifiche apportate all'ambiente Kubernetes avvisandoti quando vengono creati o rimossi pod, demonset e replicaset, nonché quando vengono create nuove implementazioni. Kubernetes controlla lo stato di default di *paused*, quindi dovresti abilitare solo quelli specifici di cui hai bisogno.

Funzioni di anteprima

Cloud Insights evidenzia regolarmente una serie di nuove interessanti funzionalità di anteprima. Se si desidera visualizzare l'anteprima di una o più di queste funzioni, contattare il "Team di vendita NetApp" per ulteriori informazioni.

Funzione	Descrizione
Previsione del time-to-full del volume interno e della capacità del volume	Cloud Insights è in grado di programmare il numero di giorni fino allo scadere della capacità per ogni volume interno e volume monitorato. Questo valore può contribuire a ridurre significativamente il rischio di un'interruzione.
Cloud Secure: Blocca l'accesso degli utenti in caso di attacco	Maggiore protezione dei dati business-critical con la possibilità di bloccare l'accesso degli utenti quando viene rilevato un attacco. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatica o manualmente dalle pagine degli avvisi o dei dettagli dell'utente."Scopri di più"
Risorsa condivisa sotto stress	La funzionalità Shared Resource Under stress Insight utilizza ai/ML per identificare automaticamente dove il conflitto di risorse sta causando il degrado delle performance nel tuo ambiente, evidenzia i carichi di lavoro interessati dall'IT e fornisce le azioni consigliate per risolvere i problemi di performance più rapidamente."Scopri di più"

Nuovo Data Collector

- **Cohesity SmartFiles** - questo collector basato su API REST acquisirà un cluster Cohesity, scoprendo le "viste" (come ci Internal Volumes), i vari nodi e raccogliendo le metriche delle performance.

Altri aggiornamenti di Data Collector

La raccolta e la visualizzazione dei dati sulle performance sono state migliorate nei seguenti data collection:

- CLI Brocade
- Dell/EMC VPlex, PowerStore, Isilon/PowerScale, VNX Block/CLARiiON CLI, XtremIO, Unity/VNXe
- Pure FlashArray

Questi miglioramenti delle performance sono già disponibili in tutti i data collezioner NetApp, VMware e Cisco e verranno implementati in tutti gli altri data collezioner nei prossimi mesi.

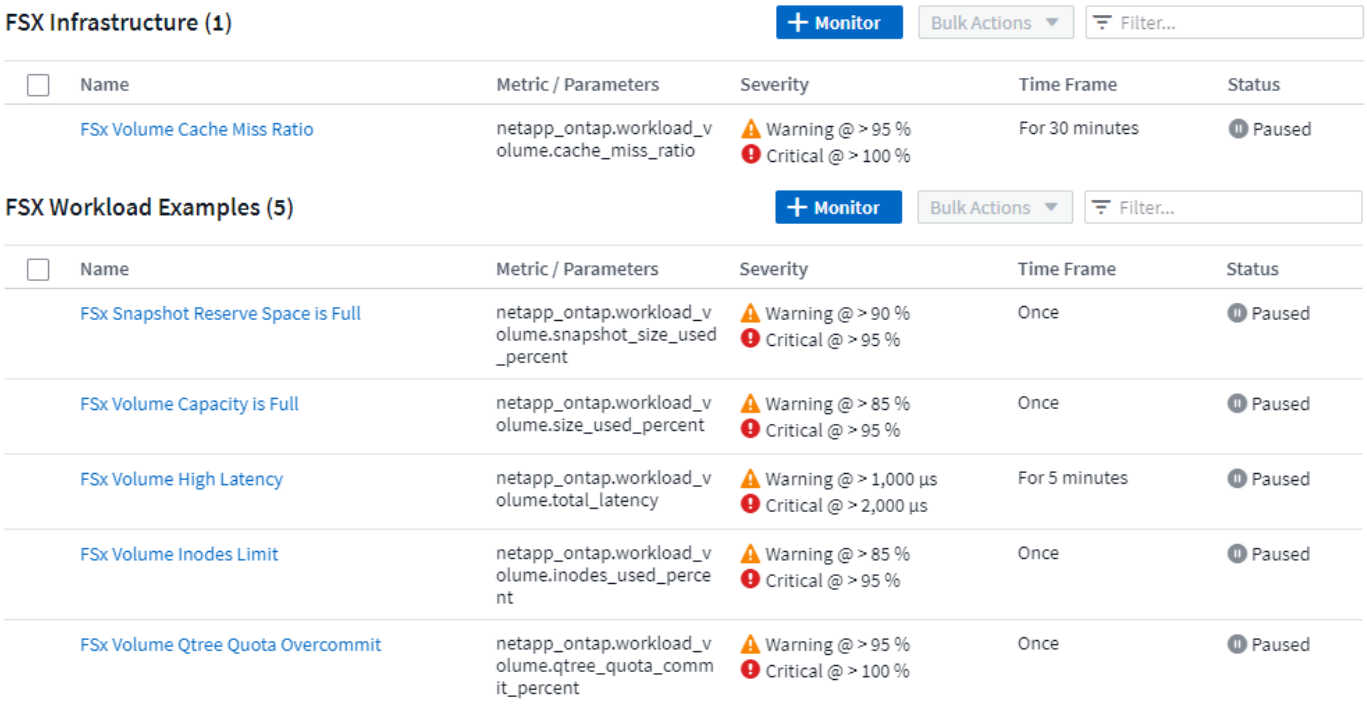
Marzo 2022

Connessione cloud per ONTAP 9.9+

Il "Connessione cloud NetApp per ONTAP 9.9+" data collector elimina la necessità di installare un'unità di acquisizione esterna, semplificando così la risoluzione dei problemi, la manutenzione e l'implementazione iniziale.

Nuovo FSX per i monitor ONTAP NetApp

Il monitoraggio dell'ambiente FSX per NetApp ONTAP è semplice con il nuovo "monitor definiti dal sistema" sia per l'infrastruttura (metriche) che per i carichi di lavoro (log).



FSX Infrastructure (1)

+ Monitor | Bulk Actions | Filter...

Name	Metric / Parameters	Severity	Time Frame	Status
FSx Volume Cache Miss Ratio	netapp_ontap.workload_volume.cache_miss_ratio	Warning @ > 95 % Critical @ > 100 %	For 30 minutes	Paused

FSX Workload Examples (5)

+ Monitor | Bulk Actions | Filter...

Name	Metric / Parameters	Severity	Time Frame	Status
FSx Snapshot Reserve Space is Full	netapp_ontap.workload_volume.snapshot_size_used_percent	Warning @ > 90 % Critical @ > 95 %	Once	Paused
FSx Volume Capacity is Full	netapp_ontap.workload_volume.size_used_percent	Warning @ > 85 % Critical @ > 95 %	Once	Paused
FSx Volume High Latency	netapp_ontap.workload_volume.total_latency	Warning @ > 1,000 µs Critical @ > 2,000 µs	For 5 minutes	Paused
FSx Volume Inodes Limit	netapp_ontap.workload_volume.inodes_used_percent	Warning @ > 85 % Critical @ > 95 %	Once	Paused
FSx Volume Qtree Quota Overcommit	netapp_ontap.workload_volume.qtree_quota_commit_percent	Warning @ > 95 % Critical @ > 100 %	Once	Paused

Nuove funzionalità Cloud Secure disponibili per tutti

Il tuo ambiente è più sicuro che mai grazie alle seguenti funzionalità di Cloud Secure ora disponibili:

Funzione	Descrizione
Distruzione dei dati: Rilevamento degli attacchi di eliminazione dei file	Rileva attività anomale di eliminazione dei file su larga scala, blocca l'accesso ai file dannosi da parte di utenti malintenzionati e effettua snapshot automatiche con policy di risposta automatica.
Separare le notifiche per Avvertenze e Avvisi	Le notifiche di avviso e avviso possono essere inviate a destinatari separati, in modo che il team giusto possa rimanere informato

Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato alla versione **1.21.2**, con miglioramenti in termini di performance e sicurezza. Gli utenti che desiderano eseguire l'aggiornamento possono fare riferimento alla sezione relativa all'aggiornamento appropriata di "Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza richiedere alcuna azione da parte dell'utente.

Aggiornamenti di Data Collector

- Il data collector degli switch Fibre Channel Broadcom è stato ottimizzato per ridurre il numero di comandi CLI emessi con ciascun sondaggio di inventario.

Febbraio 2022

Cloud Insights risolve le vulnerabilità di Apache Log4j

La sicurezza dei clienti è una priorità assoluta per NetApp. Cloud Insights include aggiornamenti alle librerie software per risolvere le recenti vulnerabilità di Apache Log4j.

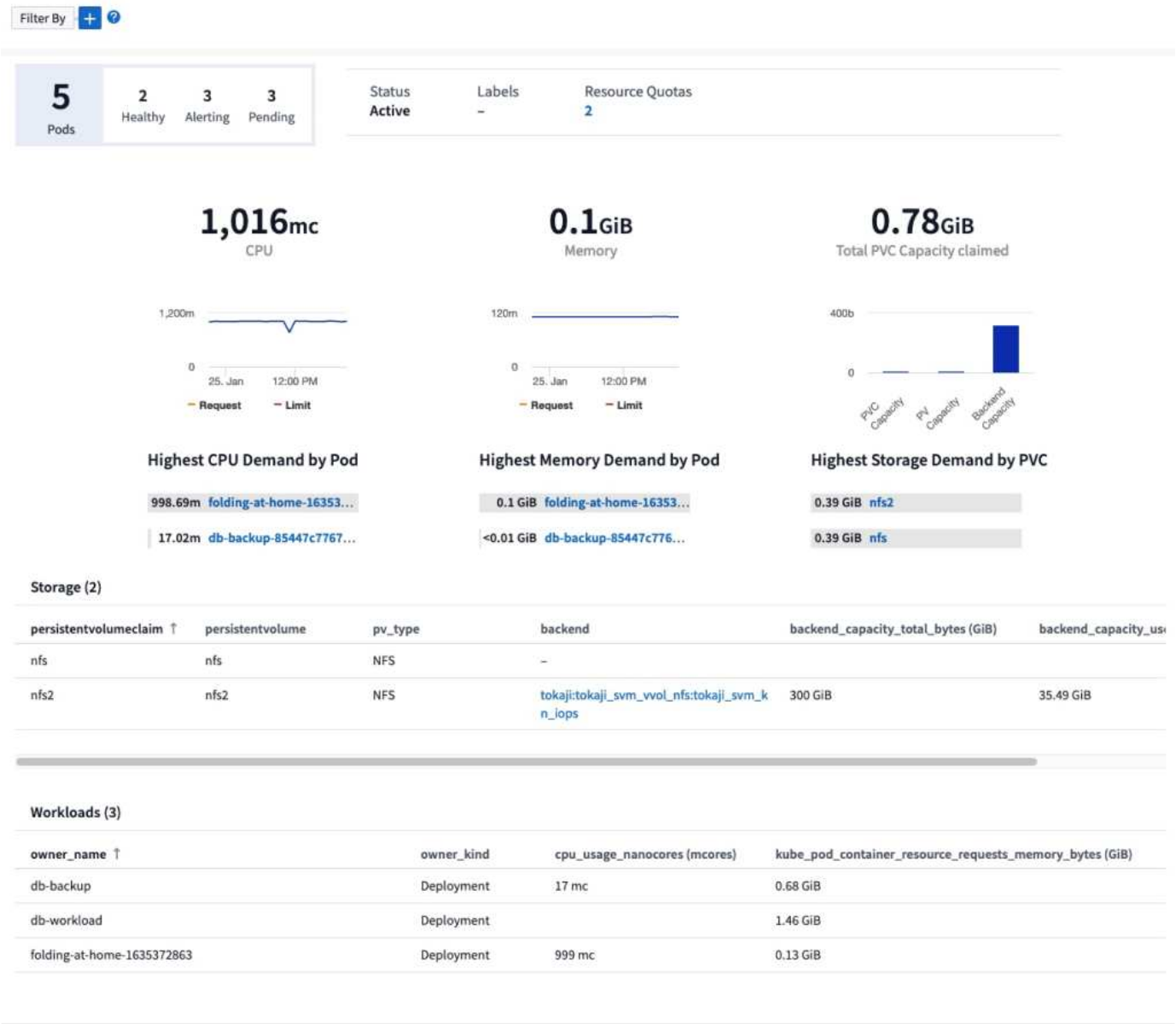
Fare riferimento a quanto segue sul sito Web Product Security Advisory di NetApp:

"CVE-2021-44228"
"CVE-2021-45046"
"CVE-2021-45105"

Per ulteriori informazioni su queste vulnerabilità e sulla risposta di NetApp, visitare il sito "Newsroom di NetApp".

Pagina dei dettagli dello spazio dei nomi Kubernetes

L'esplorazione dell'ambiente Kubernetes è ora migliore che mai, con pagine di dettagli informative per gli spazi dei nomi del cluster. La pagina dei dettagli dello spazio dei nomi fornisce un riepilogo di tutte le risorse utilizzate da uno spazio dei nomi, incluse tutte le risorse di storage back-end e i relativi utilizzi della capacità.



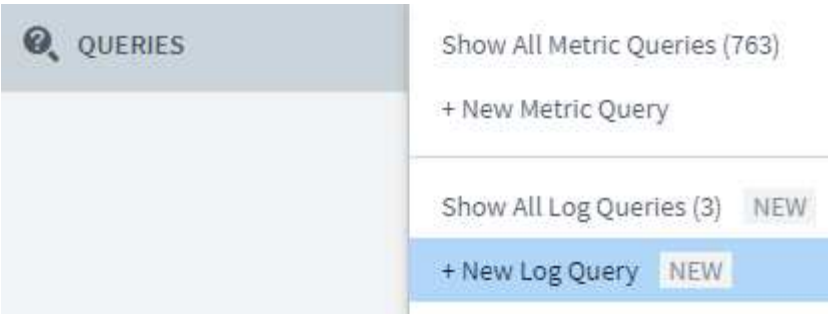
Dicembre 2021

Integrazione più profonda per i sistemi ONTAP

Semplifica gli avvisi per guasti hardware ONTAP e molto altro ancora grazie alla nuova integrazione con il sistema di gestione degli eventi NetApp."Esplora e allerta" Sui messaggi ONTAP di basso livello in Cloud Insights per informare e migliorare i flussi di lavoro di troubleshooting e ridurre ulteriormente la dipendenza dagli strumenti di gestione degli elementi ONTAP.

Query dei registri

Per i sistemi ONTAP, le query Cloud Insights includono un potente "Esplora log", Che consente di analizzare e risolvere facilmente i problemi relativi alle voci di registro EMS.



Notifiche a livello di Data Collector.

Oltre ai monitor personalizzati e definiti dal sistema per gli avvisi, è possibile impostare le notifiche di avviso per i data collector ONTAP, consentendo di specificare i destinatari degli avvisi a livello di raccolta, indipendentemente dagli altri avvisi di monitoraggio.

Maggiore flessibilità dei ruoli Cloud Secure

Gli utenti possono accedere alle funzionalità di Cloud Secure in base a. "ruoli" impostato da un amministratore:

Ruolo	Accesso a Cloud Secure
Amministratore	È in grado di eseguire tutte le funzioni Cloud Secure, incluse quelle per avvisi, analisi, raccolta dati, policy di risposta automatizzate e API per Cloud Secure. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli Cloud Secure.
Utente	Consente di visualizzare e gestire gli avvisi e visualizzare le analisi. Il ruolo dell'utente può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente e bloccare l'accesso dell'utente.
Ospite	Consente di visualizzare avvisi e analisi. Il ruolo ospite non può modificare lo stato degli avvisi, aggiungere una nota, acquisire snapshot manualmente o bloccare l'accesso dell'utente.

Supporto del sistema operativo

Il supporto di CentOS 8.x viene sostituito con il supporto di **CentOS 8 Stream**. CentOS 8.x arriverà al termine del ciclo di vita il 31 dicembre 2021.

Aggiornamenti di Data Collector

Sono stati aggiunti diversi nomi di data collector Cloud Insights per riflettere le modifiche dei vendor:

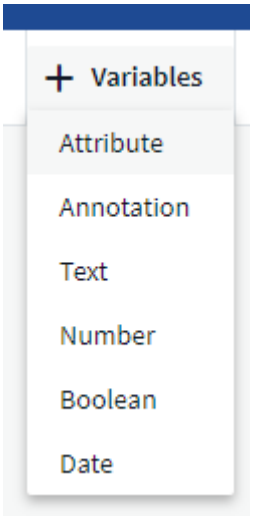
Vendor/modello	Nome precedente
Dell EMC PowerScale	Isilon
HPE Alletra 9000/Primera	3PAR
HPE Alletra 6000	Agile

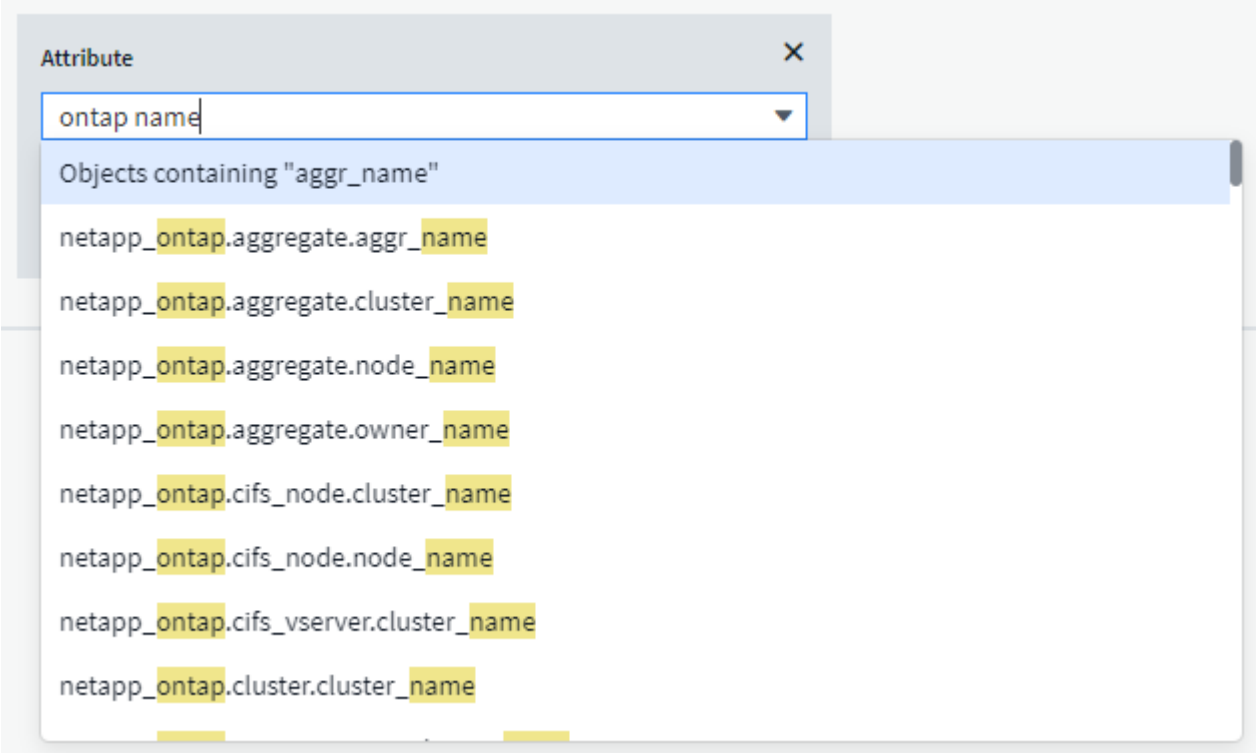
Novembre 2021

Dashboard adattivi

Nuove variabili per gli attributi e la possibilità di utilizzare le variabili nei widget.

Le dashboard sono ora più potenti e flessibili che mai. Crea dashboard adattivi con variabili di attributo per filtrare rapidamente le dashboard in tempo reale. Utilizzando questi e altri pre-esistenti "variabili" ora puoi creare una dashboard di alto livello per visualizzare le metriche per l'intero ambiente e filtrare senza problemi in base a nome, tipo, posizione e altro ancora. Utilizza le variabili numeriche nei widget per associare le metriche raw ai costi, ad esempio il costo per GB per lo storage come servizio.





Accedere al database dei report tramite API

Funzionalità avanzate per l'integrazione con strumenti di reporting, ITSM e automazione di terze parti: Il potente Cloud Insights "API" Consente agli utenti di eseguire query direttamente nel database dei report di

Cloud Insights, senza utilizzare l'ambiente di reporting di Cognos.

Tabelle Pod sulla pagina di destinazione delle macchine virtuali

Navigazione perfetta tra le macchine virtuali e i Kubernetes Pod che li utilizzano: Per una migliore risoluzione dei problemi e una gestione più ampia delle performance, una tabella dei Kubernetes Pod associati verrà ora visualizzata sulle landing page delle macchine virtuali.

Kubernetes Pods

15 items found

pod_name	kubernetes_cluster	namespace	owner_kind	owner_name
calico-kube-controllers-649b7b795b-ktp2n	ci-rancher	kube-system	ReplicaSet	calico-kube-controllers-649b7b795b
canal-mpvhx	ci-rancher	kube-system	DaemonSet	canal
cattle-cluster-agent-74c7797cc5-b9jhz	ci-rancher	cattle-system	ReplicaSet	cattle-cluster-agent-74c7797cc5
cattle-node-agent-bn225	ci-rancher	cattle-system	DaemonSet	cattle-node-agent
coredns-autoscaler-79599b9dc6-dtwpj	ci-rancher	kube-system	ReplicaSet	coredns-autoscaler-79599b9dc6

Aggiornamenti di Data Collector

- ECS ora riporta il firmware per lo storage e il nodo
- Isilon ha migliorato il rilevamento dei prompt
- Azure NetApp Files raccoglie i dati sulle performance più rapidamente
- StorageGRID ora supporta SSO (Single Sign-on)
- Brocade CLI riporta correttamente il modello per X&-4

Sistemi operativi aggiuntivi supportati

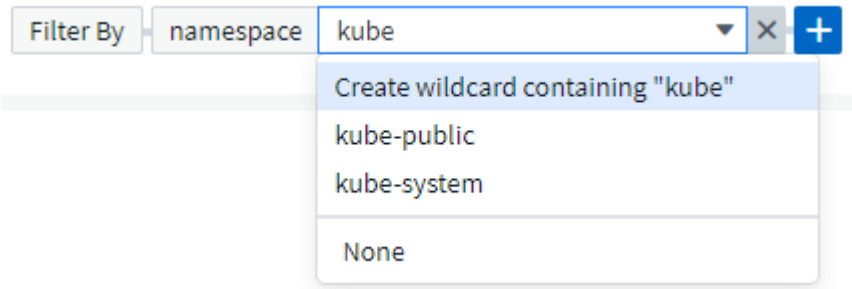
L'unità di acquisizione Cloud Insights supporta i seguenti sistemi operativi, oltre a quelli già supportati:

- CentOS (64 bit) 8.4
- Oracle Enterprise Linux (64 bit) 8.4
- Red Hat Enterprise Linux (64 bit) 8.4

Ottobre 2021

Filtri sulle pagine Explorer di K8S

"Kubernetes Explorer" I filtri di pagina ti offrono un controllo mirato dei dati visualizzati per l'esplorazione di cluster, nodi e pod Kubernetes.



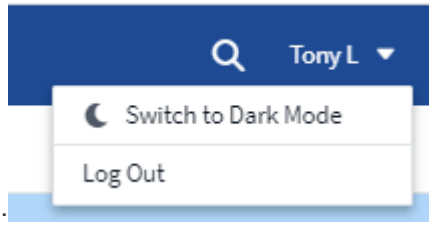
Dati K8s per il reporting

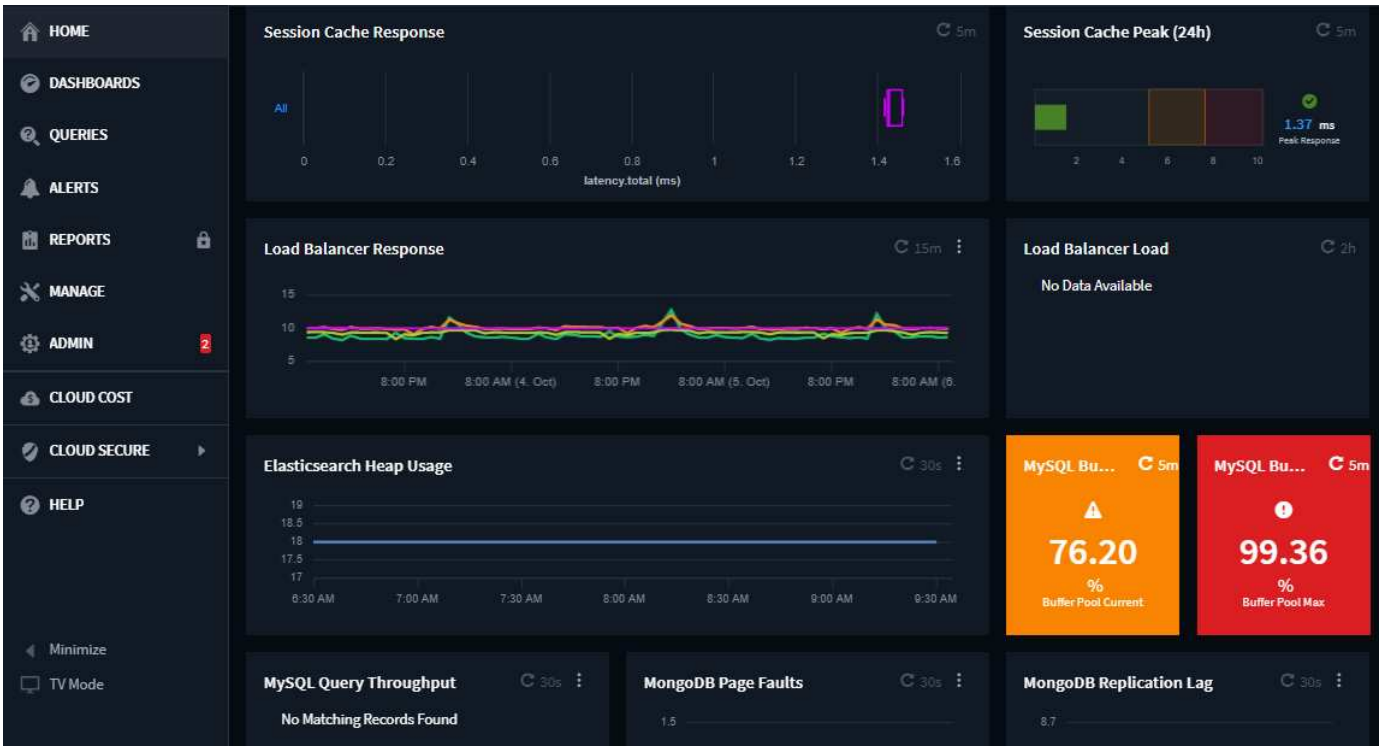
I dati Kubernetes sono ora disponibili per l'utilizzo in Reporting, consentendo di creare chargeback o altri report. Per passare i dati di chargeback di Kubernetes a Reporting, è necessario disporre di una connessione attiva e Cloud Insights deve ricevere dati dal cluster Kubernetes e dal relativo storage back-end. Se non vengono ricevuti dati dallo storage back-end, Cloud Insights non può inviare i dati dell'oggetto Kubernetes a Reporting.

K8s Cluster	Tier	K8s Namespace	Backend Resource	Backend Storage	Provisioned (GB)	Monthly Provisioned Cost
K8S-ETL	Tier 1	k8testns	qacvo:svm_qacvo:volume1	qacvo	10	$204.80
	Tier 1 - Total				**10**	**$204.80**
	Tier 2	demo	tawny:tawny_svm_oci_dev:vm_flexVol_dev01	tawny	4,096	$33,554.43
	Tier 2 - Total				**4,096**	**$33,554.43**
K8S-ETL - Total					**4,106**	**$33,759.23**
Overall - Total					**4,106**	**$33,759.23**

Dark Theme è arrivato

Molti di voi hanno chiesto un tema scuro e Cloud Insights ha risposto. Per passare dal tema chiaro a quello scuro e viceversa, fare clic sull'elenco a discesa accanto al nome utente.





Supporto Data Collector

Abbiamo apportato alcuni miglioramenti ai Data Collector di Cloud Insights. Ecco alcuni punti salienti:

- Nuovo collector per Amazon FSX per ONTAP

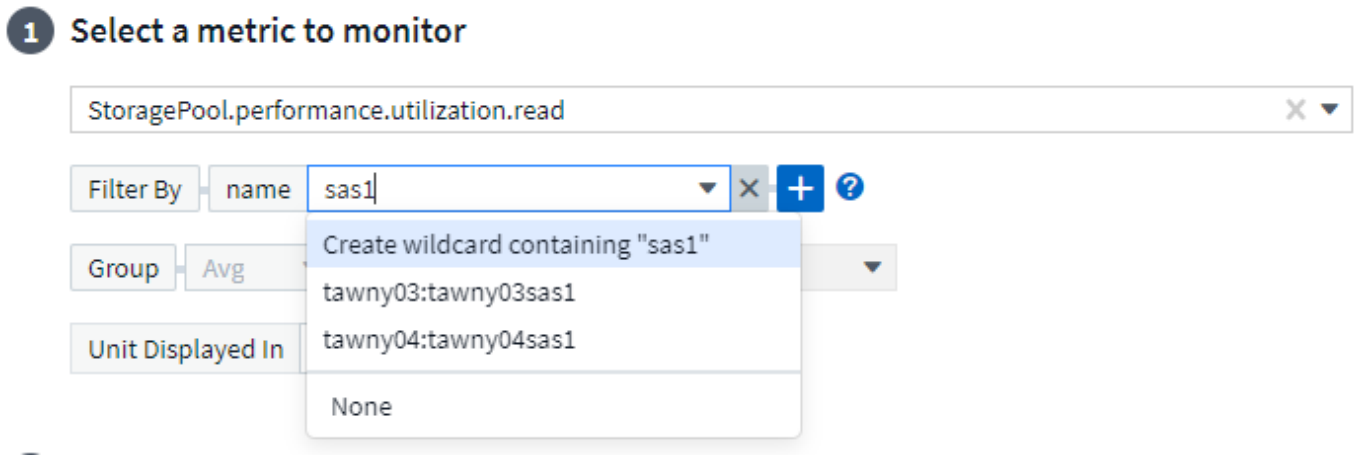
Settembre 2021

Le policy sulle performance sono ora monitorate

I monitor e gli avvisi hanno soppiantato le policy di performance e le violazioni in Cloud Insights. "Avvisi con i monitor" offre maggiore flessibilità e informazioni su potenziali problemi o tendenze nel tuo ambiente.

Suggerimenti di completamento automatico, caratteri jolly ed espressioni in Monitor

Quando si crea un monitor per gli avvisi, la digitazione di un filtro è ora predittiva, consentendo di cercare e trovare facilmente le metriche o gli attributi del monitor. Inoltre, è possibile creare un filtro con caratteri jolly in base al testo digitato.



Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato alla versione **1.19.3**, con miglioramenti in termini di performance e sicurezza. Gli utenti che desiderano eseguire l'aggiornamento possono fare riferimento alla sezione relativa all'aggiornamento appropriata di "Installazione dell'agente" documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza richiedere alcuna azione da parte dell'utente.

Supporto Data Collector

Abbiamo apportato alcuni miglioramenti ai Data Collector di Cloud Insights. Ecco alcuni punti salienti:

- Microsoft Hyper-V Collector ora utilizza PowerShell invece di WMI
- Azure VM e VHD Collector sono ora fino a 10 volte più veloci grazie alle chiamate parallele
- HPE Nimble ora supporta configurazioni federate e iSCSI

E poiché stiamo sempre migliorando la raccolta di dati, ecco alcuni altri cambiamenti recenti:

- Nuovo collector per EMC Powerstore
- Nuovo collector per Hitachi Ops Center
- Nuovo collector per Hitachi Content Platform
- ONTAP Collector migliorato per il report dei pool di fabric
- ANF migliorato con le performance di Storage Pool e Volume
- EMC ECS migliorato con nodi di storage e performance di storage, nonché il numero di oggetti nei bucket
- EMC Isilon migliorato con metriche di Storage Node e Qtree
- EMC Symetrix ottimizzato con metriche dei limiti DI QOS dei volumi
- IBM SVC ed EMC PowerStore migliorati con numero di serie principale dei nodi di storage

---

Agosto 2021

Nuova interfaccia utente della pagina di audit

Il "Pagina di audit" Fornisce un'interfaccia più pulita e ora consente l'esportazione di eventi di audit in file .CSV.

Gestione avanzata dei ruoli utente

Cloud Insights offre ora una libertà ancora maggiore per l'assegnazione dei ruoli utente e dei controlli degli accessi. È ora possibile assegnare agli utenti autorizzazioni granulari per il monitoraggio, la creazione di report e Cloud Secure separatamente.

Ciò significa che puoi consentire a un maggior numero di utenti l'accesso amministrativo alle funzioni di monitoraggio, ottimizzazione e reporting, limitando al contempo l'accesso ai dati sensibili di attività e audit di Cloud Secure solo a quelli che ne hanno bisogno.

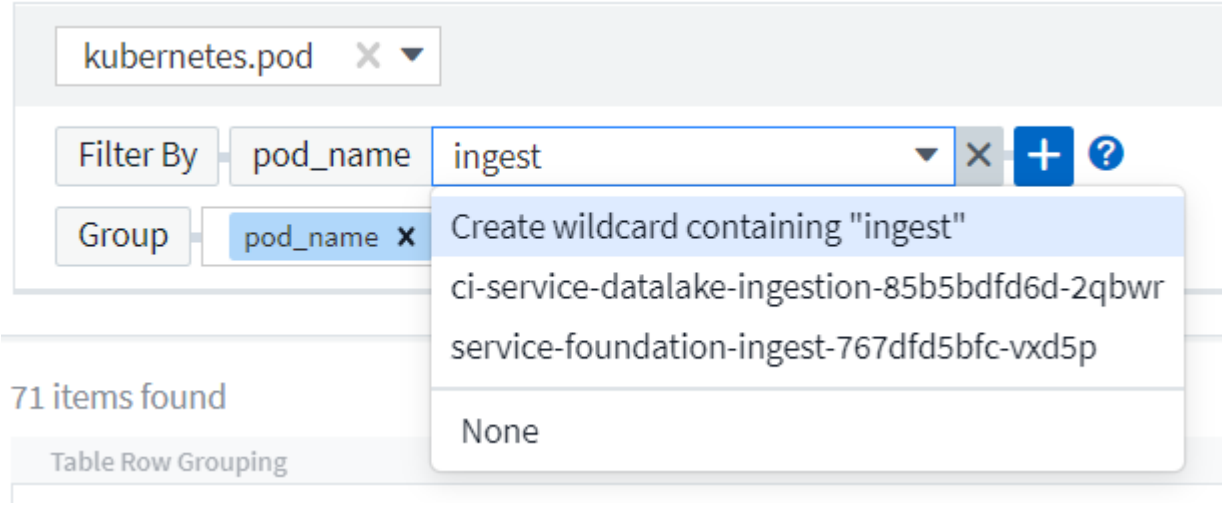
"Scopri di più" Informazioni sui diversi livelli di accesso nella documentazione di Cloud Insights.

Giugno 2021

Suggerimenti di completamento automatico, caratteri jolly ed espressioni in filtri

Con questa versione di Cloud Insights, non è più necessario conoscere tutti i nomi e i valori possibili su cui filtrare in una query o in un widget. Durante il filtraggio, puoi semplicemente iniziare a digitare e Cloud Insights suggerirà i valori in base al testo. Non dovrai più cercare in anticipo i nomi delle applicazioni o gli attributi Kubernetes per trovare quelli che vuoi mostrare nel widget.

Durante la digitazione di un filtro, il filtro visualizza un elenco intelligente di risultati da cui è possibile scegliere, nonché l'opzione per creare un filtro * con caratteri jolly* in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione con caratteri jolly. Naturalmente, è anche possibile selezionare più valori singoli che si desidera aggiungere al filtro.



Inoltre, è possibile creare **espressioni** in un filtro utilizzando NOT o OPPURE OPPURE selezionare l'opzione "None" (Nessuno) per filtrare i valori nulli nel campo.

Scopri di più "opzioni di filtraggio" in query e widget.

API disponibili per edizione

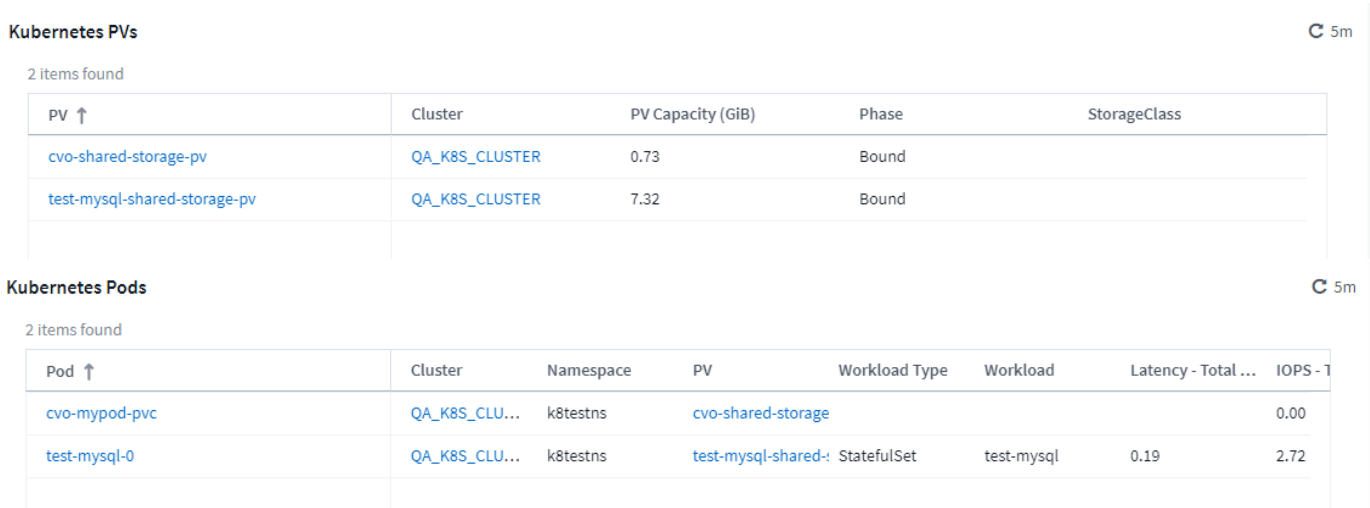
Le potenti API di Cloud Insights sono più accessibili che mai, con le API Alert ora disponibili nelle edizioni Standard e Premium. Per ciascuna edizione sono disponibili le seguenti API:

Categoria API	Di base	Standard	Premium
Unità di acquisizione	✔	✔	✔
Raccolta di dati	✔	✔	✔
Avvisi		✔	✔
Risorse		✔	✔
Acquisizione dei dati		✔	✔

Kubernetes visibilità PV e Pod

Cloud Insights offre visibilità sullo storage back-end per gli ambienti Kubernetes, fornendo informazioni dettagliate sui pod Kubernetes e sui volumi persistenti (PVS). È ora possibile tenere traccia dei contatori FV come IOPS, latenza e throughput dall'utilizzo di un singolo Pod attraverso un contatore FV a un FV e fino al dispositivo di storage back-end.

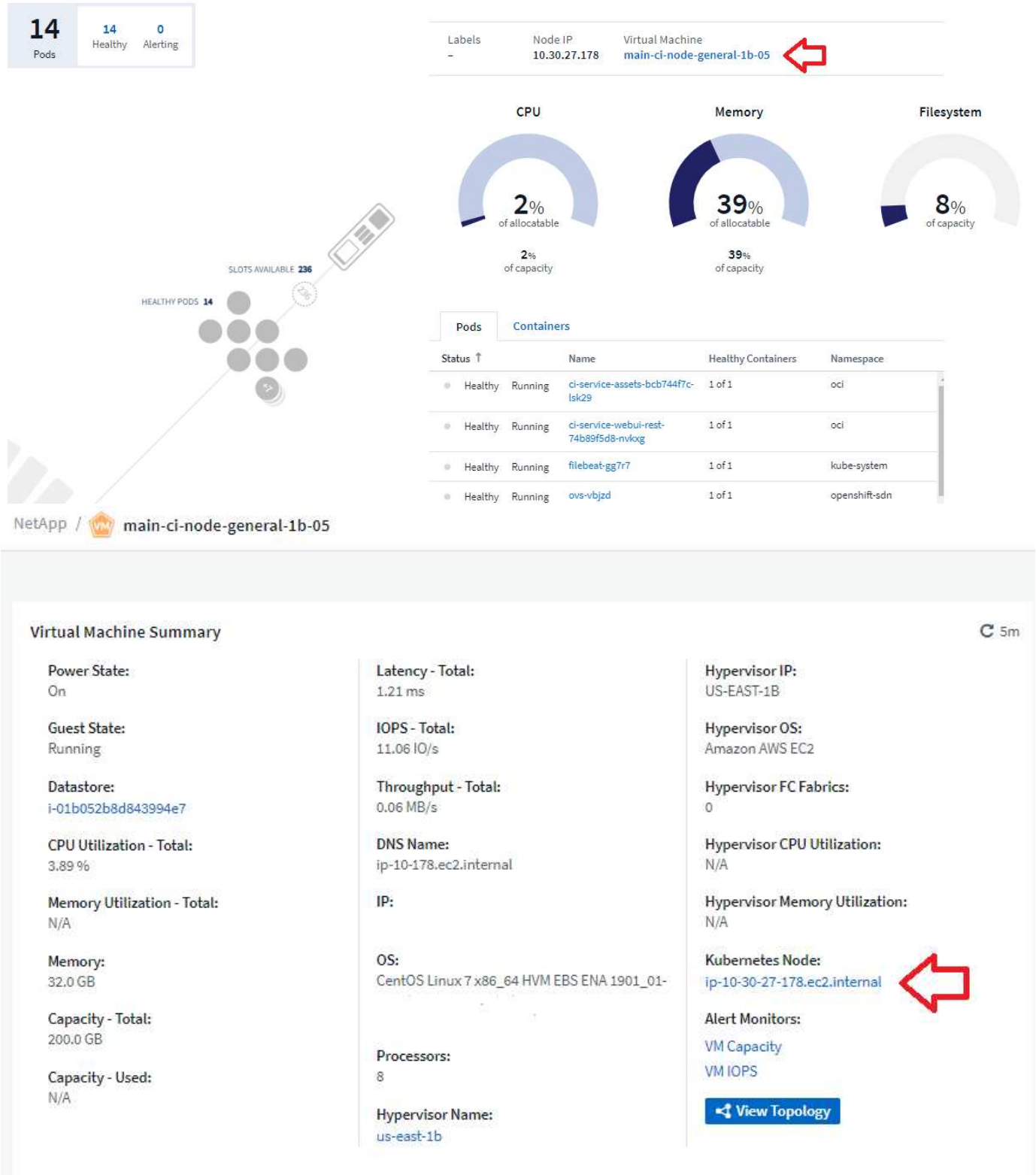
In una landing page del volume o del volume interno, vengono visualizzate due nuove tabelle:



Si noti che per sfruttare queste nuove tabelle, si consiglia di disinstallare l'agente Kubernetes corrente e installarlo di nuovo. È inoltre necessario installare Kube-state-Metrics versione 2.1.0 o successiva.

Collegamenti tra nodo e VM di Kubernetes

In una pagina Kubernetes Node, è ora possibile fare clic per aprire la pagina della macchina virtuale del nodo. La pagina VM include anche un collegamento al nodo stesso.



Alert Monitor sostituisce le policy di performance

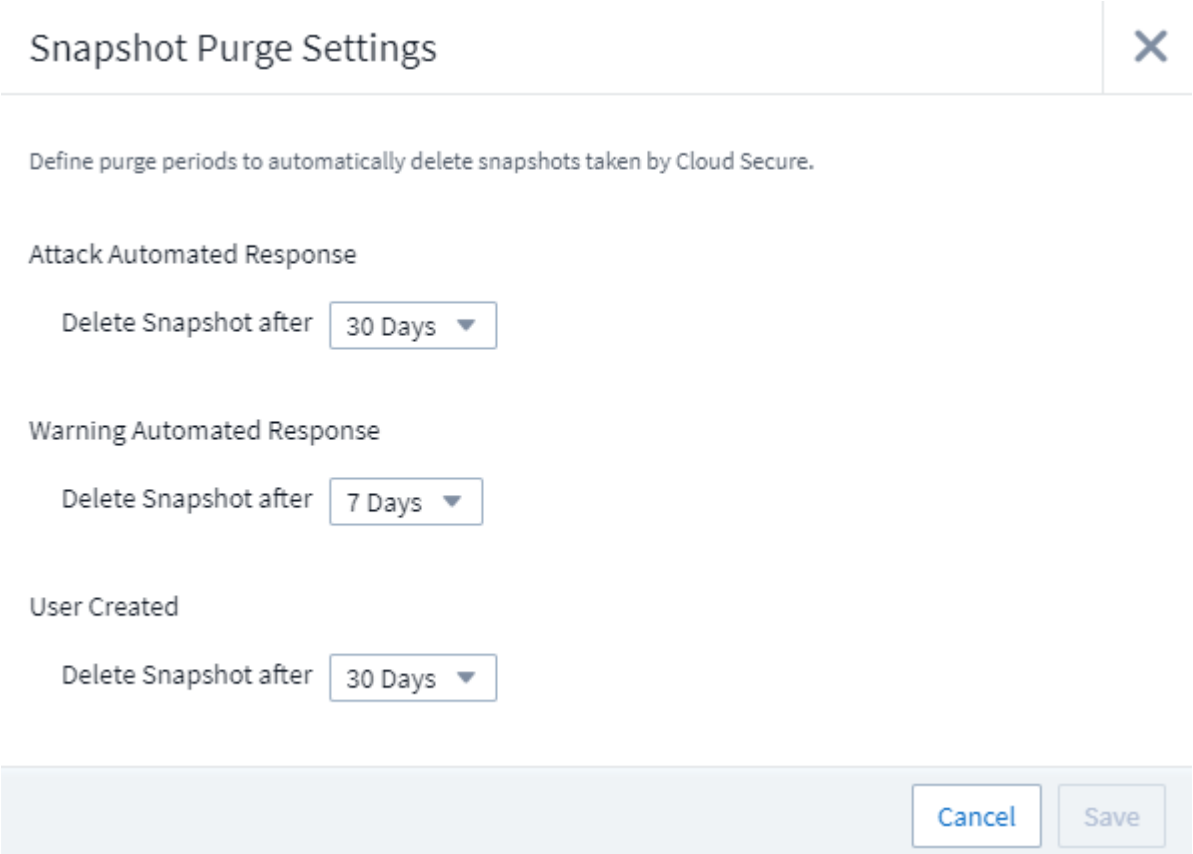
Per consentire i vantaggi aggiuntivi di soglie multiple, invio di avvisi tramite webhook e email, avvisi su tutte le metriche utilizzando una singola interfaccia e altro ancora, Cloud Insights convertirà i clienti delle edizioni standard e premium da **policy sulle performance** a **monitor** durante i mesi di luglio e agosto 2021. Scopri di più "Avvisi e monitor"e restate sintonizzati per questo cambiamento entusiasmante.

Cloud Secure supporta NFS

Cloud Secure ora supporta la raccolta dati NFS per ONTAP. Monitorate l'accesso degli utenti SMB e NFS per proteggere i vostri dati da attacchi ransomware. Inoltre, Cloud Secure supporta le directory utente Active-Directory e LDAP per la raccolta degli attributi degli utenti NFS.

Eliminazione dello snapshot Cloud Secure

Cloud Secure elimina automaticamente gli snapshot in base alle impostazioni di eliminazione degli snapshot, per risparmiare spazio di storage e ridurre la necessità di eliminare manualmente gli snapshot.



Velocità di raccolta dei dati Cloud Secure

Un singolo sistema di agenti di data collector è ora in grado di inviare fino a 20,000 eventi al secondo a Cloud Secure.

Maggio 2021

Ecco alcuni dei cambiamenti che abbiamo apportato ad aprile:

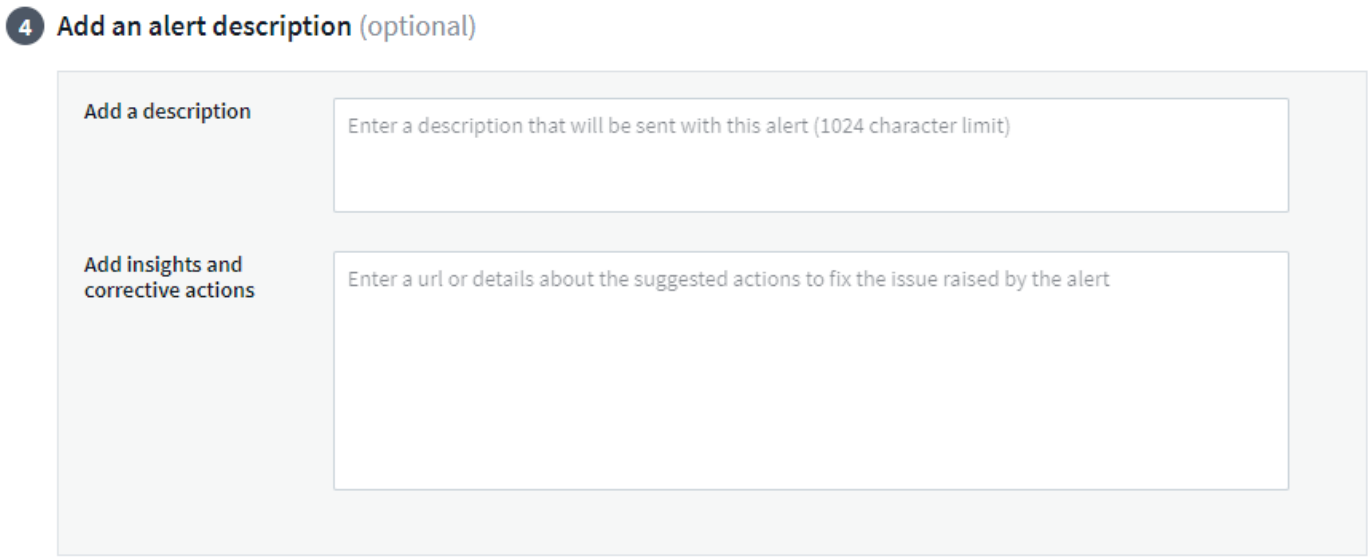
Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato alla versione 1.17.3, con miglioramenti in termini di performance e sicurezza. Gli utenti che desiderano eseguire l'aggiornamento possono fare riferimento alla sezione relativa all'aggiornamento appropriata di "Installazione dell'agente"

documentazione. Le versioni precedenti dell'agente continueranno a funzionare senza richiedere alcuna azione da parte dell'utente.

Aggiungere azioni correttive a un avviso

È ora possibile aggiungere una descrizione opzionale e ulteriori informazioni e/o azioni correttive durante la creazione o la modifica di un monitor compilando la sezione **Aggiungi una descrizione dell'avviso**. La descrizione verrà inviata con l'avviso. Il campo *approfondimenti e azioni correttive* può fornire istruzioni dettagliate per la gestione degli avvisi e verrà visualizzato nella sezione riepilogativa della landing page degli avvisi.



API Cloud Insights per tutte le edizioni

L'accesso API è ora disponibile in tutte le edizioni di Cloud Insights. Gli utenti di Basic Edition possono ora automatizzare le azioni per le unità di acquisizione e i Data Collector, mentre gli utenti di Standard Edition possono eseguire query sulle metriche e acquisire metriche personalizzate. Premium Edition continua a consentire l'utilizzo completo di tutte le categorie API.

Categoria API	Di base	Standard	Premium
Unità di acquisizione	✔	✔	✔
Raccolta di dati	✔	✔	✔
Risorse		✔	✔
Acquisizione dei dati		✔	✔
Data Warehouse			✔

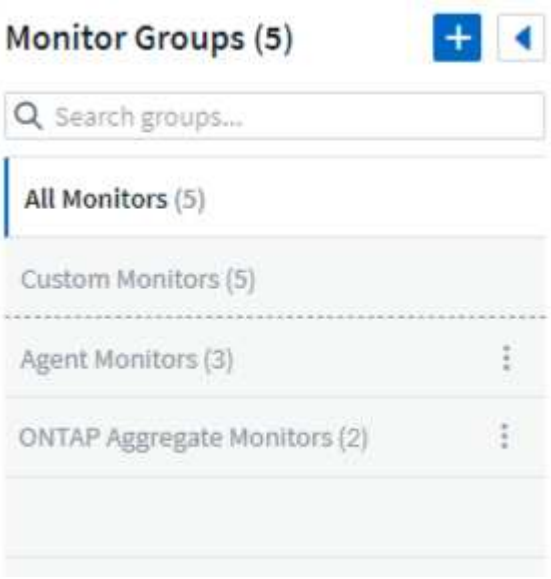
Per ulteriori informazioni sull'utilizzo delle API, fare riferimento a. "Documentazione API".

Aprile 2021

Gestione semplificata dei monitor

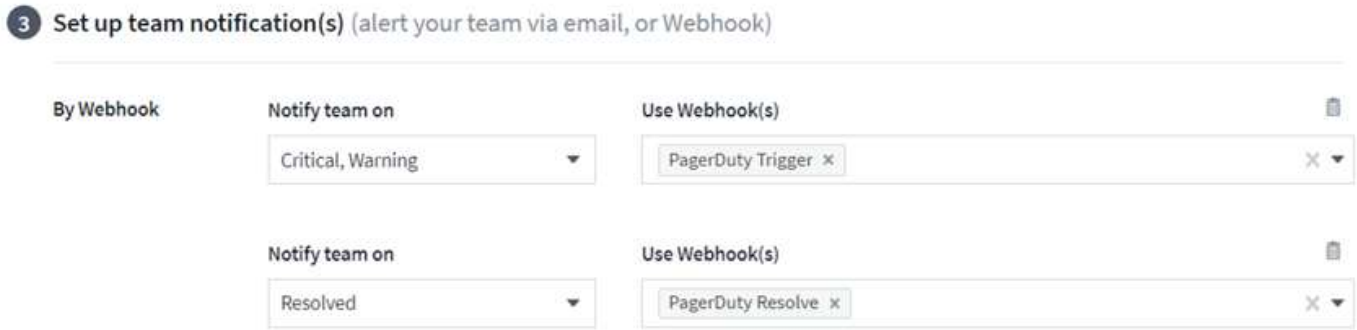
"Raggruppamento dei monitor" semplifica la gestione dei monitor nel tuo ambiente. È ora possibile raggruppare più monitor e mettere in pausa come un unico monitor. Ad esempio, se si verifica un aggiornamento su uno stack di infrastruttura, è possibile sospendere gli avvisi da tutti i dispositivi con un solo clic.

I gruppi di monitor sono la prima parte di una nuova ed entusiasmante funzionalità che consente di migliorare la gestione dei dispositivi ONTAP in Cloud Insights.



Opzioni avanzate di avviso con webhook

Supporto di molte applicazioni commerciali "Webhook" come interfaccia di input standard. Cloud Insights ora supporta molti di questi canali di delivery, fornendo modelli predefiniti per slack, PagerDuty, team e discordia, oltre a fornire webhook generici personalizzabili per supportare molte altre applicazioni.



Identificazione dei dispositivi migliorata

Per migliorare il monitoraggio e la risoluzione dei problemi, oltre a fornire report accurati, è utile comprendere i nomi dei dispositivi piuttosto che i loro indirizzi IP o altri identificatori. Cloud Insights incorpora ora un metodo automatico per identificare i nomi dei dispositivi di storage e host fisici nell'ambiente, utilizzando un approccio basato su regole chiamato **"Risoluzione del dispositivo"**, Disponibile nel menu **Gestisci**.

Hai chiesto di più!

I clienti hanno chiesto più opzioni predefinite per la visualizzazione della gamma di dati, quindi abbiamo aggiunto le cinque nuove opzioni seguenti, ora disponibili per l'intero servizio tramite il selettore dell'intervallo di tempo:

- Ultimi 30 minuti
- Ultime 2 ore
- Ultime 6 ore
- Ultime 12 ore
- Ultimi 2 giorni

Abbonamenti multipli in un ambiente Cloud Insights

A partire dal 2 aprile, Cloud Insights supporta più sottoscrizioni dello stesso tipo di edizione per un cliente in una singola istanza di Cloud Insights. Ciò consente ai clienti di co-term parti del proprio abbonamento Cloud Insights con acquisti di infrastrutture. Contatta il reparto vendite NetApp per assistenza con più abbonamenti.

Scegli il tuo percorso

Durante la configurazione di Cloud Insights, è ora possibile scegliere se iniziare con monitoraggio e avvisi o ransomware e rilevamento delle minacce interne. Cloud Insights configurerà l'ambiente di partenza in base al percorso scelto. È possibile configurare l'altro percorso in qualsiasi momento.

Inserimento Cloud Secure più semplice

Inoltre, è più facile che mai iniziare a utilizzare Cloud Secure, con una nuova checklist per la configurazione passo-passo.

Come sempre, ci piace ascoltare i tuoi suggerimenti! Inviali a ng-cloudinsights-customerfeedback@netapp.com.

Febbraio 2021

Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato alla versione 1.17.0, che include correzioni di vulnerabilità e bug.

Cloud Cost Analyzer

Scopri la potenza di Spot by NetApp con Cloud Cost, che offre un dettaglio "analisi dei costi" della spesa passata, presente e stimata, fornendo visibilità sull'utilizzo del cloud nel tuo ambiente. La dashboard Cloud Cost offre una visione chiara delle spese cloud e un'analisi dettagliata dei singoli carichi di lavoro, account e servizi.

Il costo del cloud può aiutare a risolvere queste sfide principali:

- Monitoraggio e monitoraggio delle spese cloud
- Identificazione degli sprechi e delle potenziali aree di ottimizzazione
- Fornire elementi di azione eseguibili

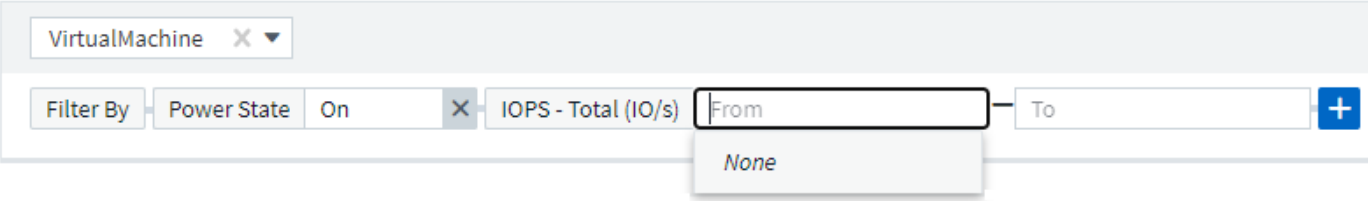
Il costo del cloud è incentrato sul monitoraggio. Effettua l'upgrade all'account Spot by NetApp completo per consentire il risparmio automatico dei costi e l'ottimizzazione dell'ambiente.

Esecuzione di query per oggetti con valori nulli utilizzando filtri

Cloud Insights consente ora di cercare attributi e metriche con valori nulli/nulli attraverso l'utilizzo di filtri. È possibile eseguire questo filtraggio su qualsiasi attributo/metrica nei seguenti punti:

- Nella pagina Query
- Nei widget Dashboard e nelle variabili di pagina
- Nella pagina dell'elenco Avvisi
- Durante la creazione di monitor

Per filtrare i valori null/none, è sufficiente selezionare l'opzione *None* quando viene visualizzata nell'elenco a discesa del filtro appropriato.



Supporto multi-regione

A partire da oggi offriamo il servizio Cloud Insights in diverse aree geografiche in tutto il mondo, che facilita le performance e aumenta la sicurezza per i clienti al di fuori degli Stati Uniti. Cloud Insights/Cloud Secure memorizza le informazioni in base alla regione in cui viene creato l'ambiente.

Fare clic su "qui" per ulteriori informazioni.

Gennaio 2021

Metriche ONTAP aggiuntive rinominate

Nell'ambito del nostro costante impegno per migliorare l'efficienza della raccolta dei dati dai sistemi ONTAP, le seguenti metriche ONTAP sono state rinominate.

Se si dispone di widget dashboard o query che utilizzano una qualsiasi di queste metriche, sarà necessario modificarli o ricrearli per utilizzare i nuovi nomi delle metriche.

Nome metrica precedente	Nuovo nome metrico
netapp_ontap.disk_costituente.total_transfers	netapp_ontap.disk_costituente.total_iops
netapp_ontap.disk.total_transfers	netapp_ontap.disk.total_iops
netapp_ontap.fcp_lif.read_data	netapp_ontap.fcp_lif.read_throughput
netapp_ontap.fcp_lif.write_data	netapp_ontap.fcp_lif.write_throughput

---

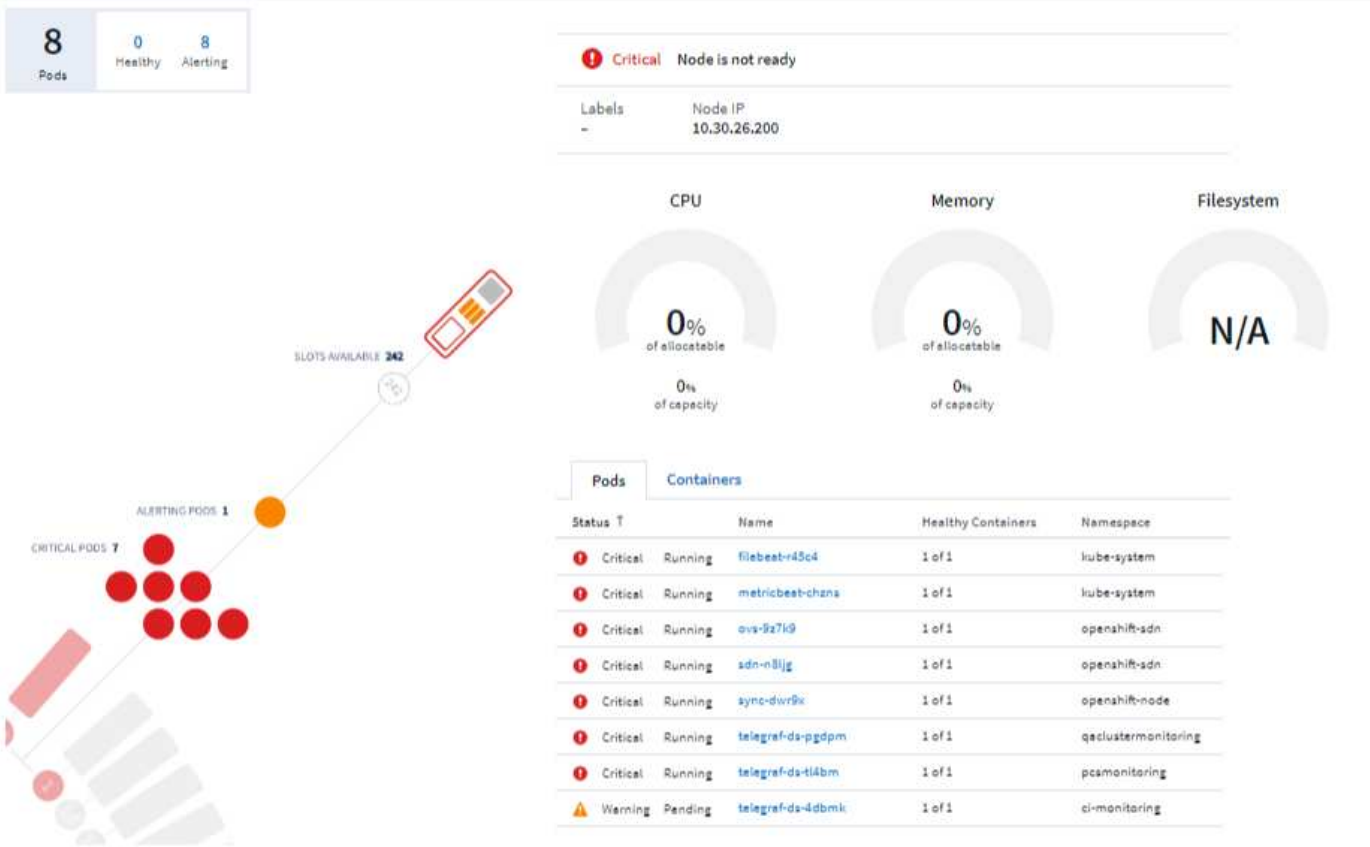
Nome metrica precedente	Nuovo nome metrico
netapp_ontap.iscsi_lif.read_data	netapp_ontap.iscsi_lif.read_throughput
netapp_ontap.iscsi_lif.write_data	netapp_ontap.iscsi_lif.write_throughput
netapp_ontap.lif.recv_data	netapp_ontap.lif.recv_throughput
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
netapp_ontap.lun.read_data	netapp_ontap.lun.read_throughput
netapp_ontap.lun.write_data	netapp_ontap.lun.write_throughput
netapp_ontap.nic_common.rx_bytes	netapp_ontap.nic_common.rx_throughput
netapp_ontap.nic_common.tx_bytes	netapp_ontap.nic_common.tx_throughput
netapp_ontap.path.read_data	netapp_ontap.path.read_throughput
netapp_ontap.path.write_data	netapp_ontap.path.write_throughput
netapp_ontap.path.total_data	netapp_ontap.path.total_throughput
netapp_ontap.policy_group.read_data	netapp_ontap.policy_group.read_throughput
netapp_ontap.policy_group.write_data	netapp_ontap.policy_group.write_throughput
netapp_ontap.policy_group.other_data	netapp_ontap.policy_group.other_throughput
netapp_ontap.policy_group.total_data	netapp_ontap.policy_group.total_throughput
netapp_ontap.system_node.disk_data_read	netapp_ontap.system_node.disk_throughput_read
netapp_ontap.system_node.disk_data_written	netapp_ontap.system_node.disk_throughput_written
netapp_ontap.system_node.hdd_data_read	netapp_ontap.system_node.hdd_throughput_read
netapp_ontap.system_node.hdd_data_written	netapp_ontap.system_node.hdd_throughput_written
netapp_ontap.system_node.ssd_data_read	netapp_ontap.system_node.ssd_throughput_read
netapp_ontap.system_node.ssd_data_written	netapp_ontap.system_node.ssd_throughput_written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
netapp_ontap.system_node.fcp_data_recv	netapp_ontap.system_node.fcp_throughput_recv
netapp_ontap.system_node.fcp_data_sent	netapp_ontap.system_node.fcp_throughput_sent
netapp_ontap.volume_node.cifs_read_data	netapp_ontap.volume_node.cifs_read_throughput
netapp_ontap.volume_node.cifs_write_data	netapp_ontap.volume_node.cifs_write_throughput
netapp_ontap.volume_node.nfs_read_data	netapp_ontap.volume_node.nfs_read_throughput
netapp_ontap.volume_node.nfs_write_data	netapp_ontap.volume_node.nfs_write_throughput
netapp_ontap.volume_node.iscsi_read_data	netapp_ontap.volume_node.iscsi_read_throughput
netapp_ontap.volume_node.iscsi_write_data	netapp_ontap.volume_node.iscsi_write_throughput
netapp_ontap.volume_node.fcp_read_data	netapp_ontap.volume_node.fcp_read_throughput
netapp_ontap.volume_node.fcp_write_data	netapp_ontap.volume_node.fcp_write_throughput

Nome metrica precedente	Nuovo nome metrico
netapp_ontap.volume.read_data	netapp_ontap.volume.read_throughput
netapp_ontap.volume.write_data	netapp_ontap.volume.write_throughput
netapp_ontap.workload.read_data	netapp_ontap.workload.read_throughput
netapp_ontap.workload.write_data	netapp_ontap.workload.write_throughput
netapp_ontap.workload_volume.read_data	netapp_ontap.workload_volume.read_throughput
netapp_ontap.workload_volume.write_data	netapp_ontap.workload_volume.write_throughput

Nuovo Kubernetes Explorer

Il "Kubernetes Explorer" Fornisce una semplice vista della topologia di Kubernetes Clusters, consentendo anche ai non esperti di identificare rapidamente problemi e dipendenze, dal livello del cluster fino al container e allo storage.

È possibile esplorare un'ampia gamma di informazioni utilizzando i dettagli dettagliati di Kubernetes Explorer relativi allo stato, all'utilizzo e allo stato di Clusters, Node, Pods, Containers e Storage nell'ambiente Kubernetes.



Dicembre 2020

Installazione più semplice di Kubernetes

L'installazione di Kubernetes Agent è stata semplificata per richiedere meno interazioni con gli utenti. "Installazione di Kubernetes Agent" Ora include la raccolta di dati Kubernetes.

Novembre 2020

Dashboard aggiuntivi

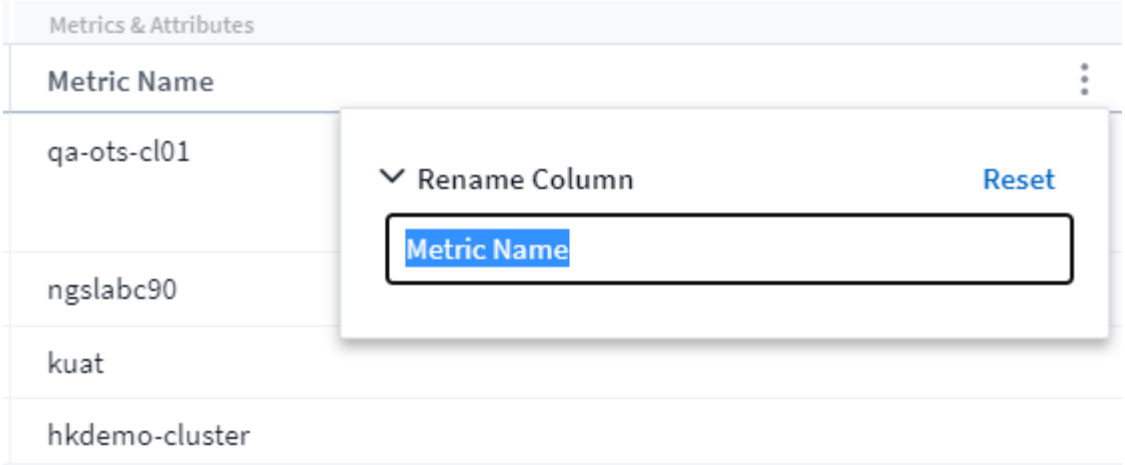
Sono state aggiunte alla galleria le seguenti dashboard incentrate su ONTAP e sono disponibili per l'importazione:

- ONTAP: Capacità e performance aggregate
- ONTAP FAS/AFF - utilizzo della capacità
- ONTAP FAS/AFF - capacità del cluster
- ONTAP FAS/AFF - efficienza
- ONTAP FAS/AFF - prestazioni FlexVol
- ONTAP FAS/AFF - punti operativi/ottimali nodo
- ONTAP FAS/AFF - efficienza della capacità pre-post
- ONTAP: Attività della porta di rete
- ONTAP: Prestazioni dei protocolli dei nodi
- ONTAP: Performance del carico di lavoro del nodo (front-end)
- ONTAP: Processore
- ONTAP: Performance del carico di lavoro SVM (front-end)
- ONTAP: Performance dei volumi di lavoro (front-end)

Rinomina colonna nei widget tabella

Puoi rinominare le colonne nella sezione *metriche e attributi* di un widget tabella aprendo il widget in modalità Modifica e facendo clic sul menu nella parte superiore della colonna. Immettere il nuovo nome e fare clic su *Save* (Salva) oppure fare clic su *Reset* (Ripristina) per riportare la colonna al nome originale.

Si noti che questo influisce solo sul nome visualizzato della colonna nel widget della tabella; il nome della metrica/attributo non cambia nei dati sottostanti stessi.



Ottobre 2020

Espansione predefinita dei dati di integrazione

Il raggruppamento dei widget tabella ora consente espansioni predefinite di Kubernetes, dati avanzati ONTAP e metriche dei nodi agente. Ad esempio, se si raggruppano Kubernetes *Nodes* per *Cluster*, viene visualizzata una riga nella tabella per ciascun cluster. È quindi possibile espandere ogni riga del cluster per visualizzare un elenco degli oggetti Node.

Supporto tecnico Basic Edition

Il supporto tecnico è ora disponibile per gli abbonati all'edizione di base di Cloud Insights oltre alle edizioni standard e Premium. Inoltre, Cloud Insights ha semplificato il flusso di lavoro per la creazione di un ticket di supporto NetApp.

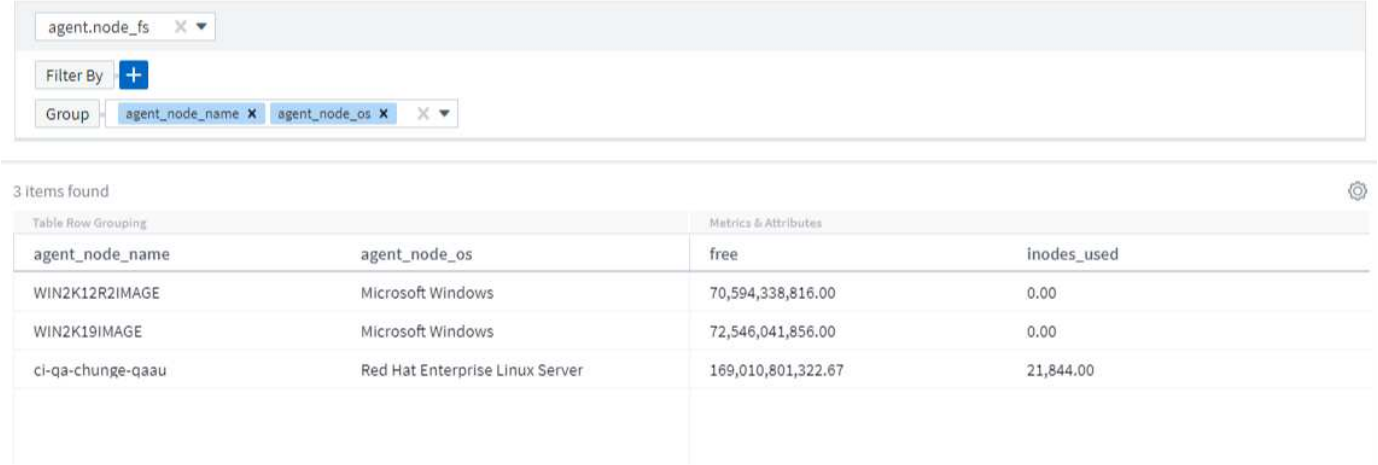
API pubblica Cloud Secure

Supporto di Cloud Secure "API REST" Per accedere alle informazioni sulle attività e sugli avvisi. Ciò avviene mediante l'utilizzo di token di accesso API, creati tramite l'interfaccia utente amministrativa di Cloud Secure, che vengono quindi utilizzati per accedere alle API REST. La documentazione di swagger per queste API REST è integrata con Cloud Secure.

Settembre 2020

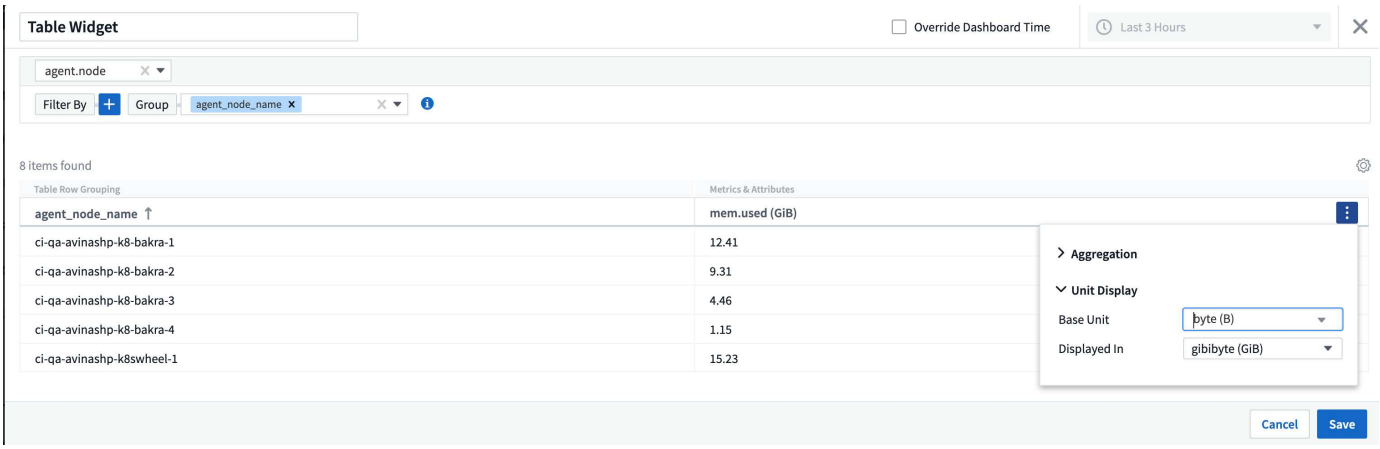
Pagina di query con dati di integrazione

La pagina delle query Cloud Insights supporta i dati di integrazione (ad esempio da Kubernetes, metriche avanzate ONTAP, ecc.). Quando si lavora con i dati di integrazione, la tabella dei risultati della query visualizza una vista "Split-Screen", con l'oggetto/raggruppamento a sinistra e i dati dell'oggetto (attributi/metriche) a destra. È inoltre possibile scegliere più attributi per raggruppare i dati di integrazione.



Formattazione visualizzazione unità nel widget Tabella

La formattazione della visualizzazione delle unità è ora disponibile nei widget Tabella per le colonne che visualizzano i dati delle metriche/contatori (ad esempio, gigabyte, MB/secondo, ecc.). Per modificare l'unità di visualizzazione di una metrica, fare clic sul menu "tre punti" nell'intestazione della colonna e selezionare "visualizzazione unità". È possibile scegliere una delle unità disponibili. Le unità disponibili variano in base al tipo di dati metrici nella colonna di visualizzazione.



Pagina dei dettagli dell'unità di acquisizione

Le unità di acquisizione dispongono ora di una landing page specifica, che fornisce informazioni utili per ogni AU e informazioni utili per la risoluzione dei problemi. Il "Pagina dettagli AU" Fornisce collegamenti ai data collettori dell'AU e informazioni utili sullo stato.

Dipendenza di Cloud Secure Docker rimossa

La dipendenza di Cloud Secure da Docker è stata rimossa. Docker non è più necessario per l'installazione dell'agente Cloud Secure.

Ruoli utente di reporting

Se si dispone di Cloud Insights Premium Edition con Reporting, ogni utente di Cloud Insights nel proprio ambiente dispone anche di un accesso Single Sign-on (SSO) all'applicazione di reporting (ad esempio, Cognos); facendo clic sul collegamento **Report** nel menu, verrà automaticamente eseguito l'accesso a

Reporting.

Il ruolo dell'utente in Cloud Insights ne determina il ruolo "Ruolo utente di reporting":

Ruolo di Cloud Insights	Ruolo di reporting	Autorizzazioni di reporting
Ospite	Consumatore	Consente di visualizzare, pianificare ed eseguire report e di impostare preferenze personali, ad esempio per lingue e fusi orari. Gli utenti non possono creare report o eseguire attività amministrative.
Utente	Autore	Può eseguire tutte le funzioni Consumer, nonché creare e gestire report e dashboard.
Amministratore	Amministratore	Può eseguire tutte le funzioni autore, nonché tutte le attività amministrative, come la configurazione dei report e l'arresto e il riavvio delle attività di reporting.

I report Cloud Insights sono disponibili per ambienti con almeno 500 MU.

Se sei un cliente di Premium Edition e desideri conservare i tuoi report, leggi questa sezione "nota importante per i clienti esistenti".

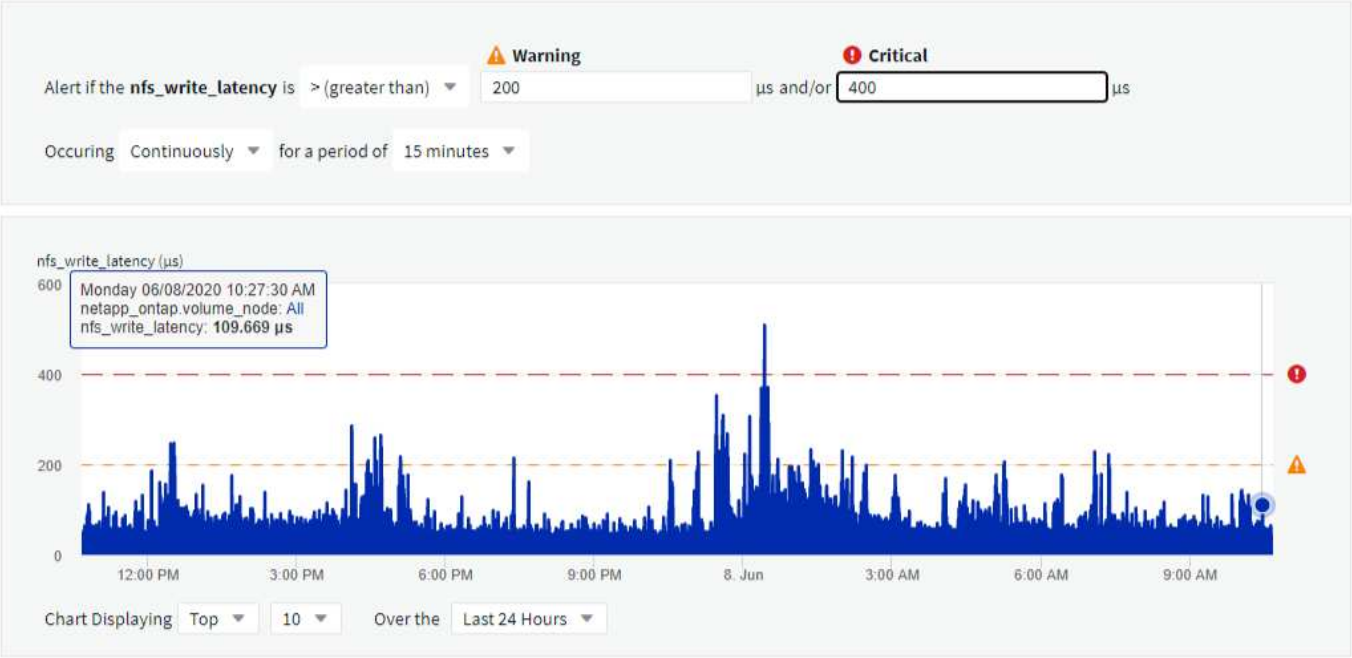
Nuova categoria API per l'acquisizione dei dati

Cloud Insights ha aggiunto una categoria di API **acquisizione dati**, che offre un maggiore controllo su agenti e dati personalizzati. La documentazione dettagliata per questa e altre categorie API è disponibile in Cloud Insights selezionando **Amministratore > accesso API** e facendo clic sul collegamento *documentazione API*. È inoltre possibile allegare un commento all'AU nel campo Note (Nota), visualizzato nella pagina dei dettagli dell'AU e nella pagina dell'elenco dell'AU.

Agosto 2020

Monitoraggio e avvisi

Oltre alla capacità attuale di impostare policy di performance per oggetti storage, macchine virtuali, EC2 e porte, Cloud Insights Standard Edition ora include la possibilità di "configurare i monitor" Per soglie sui dati di integrazione per Kubernetes, metriche avanzate di ONTAP e plug-in Telegraf. È sufficiente creare un monitor per ogni metrica oggetto che si desidera attivare gli avvisi, impostare le condizioni per le soglie del livello di avviso o critico e specificare i destinatari e-mail desiderati per ciascun livello. A questo punto è possibile "visualizzare e gestire gli avvisi" per tenere traccia delle tendenze o risolvere i problemi.



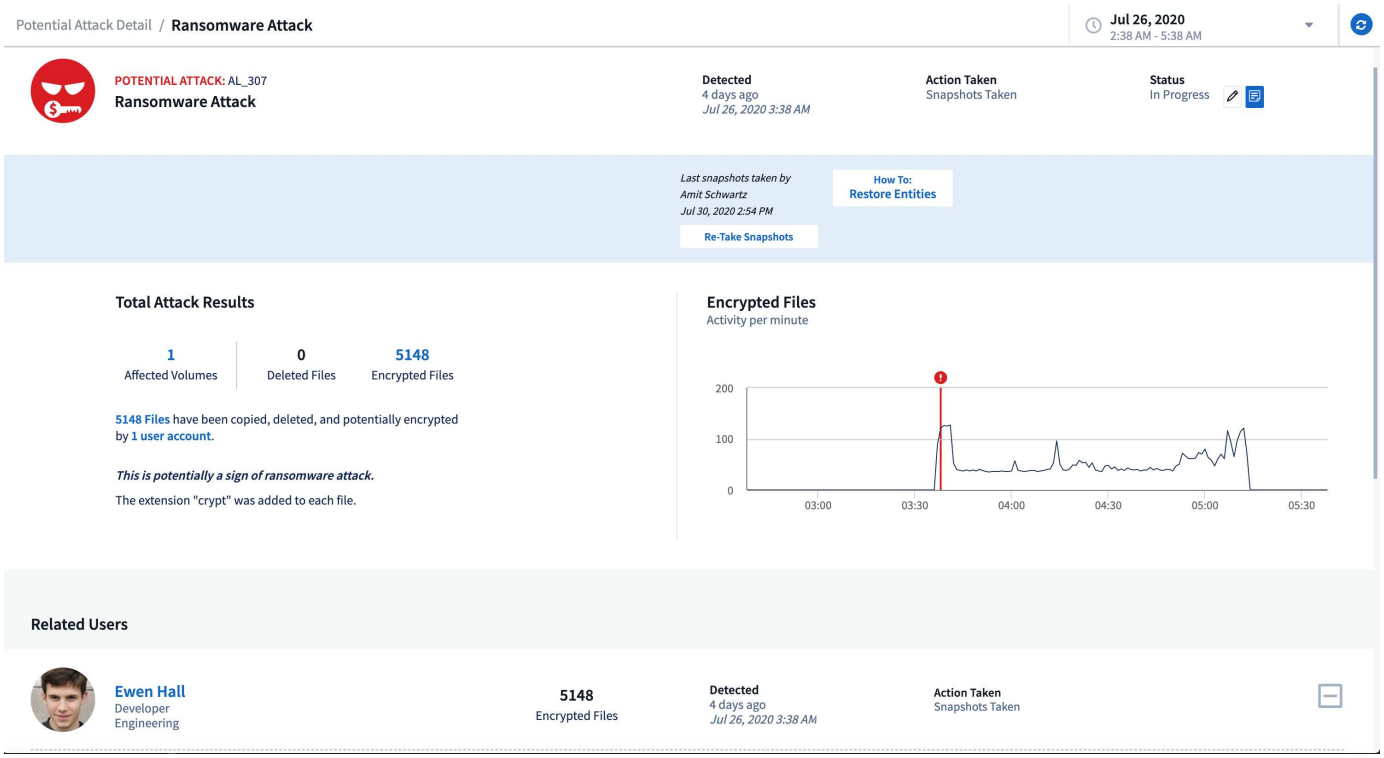
Luglio 2020

Cloud Secure *fare un'istantanea* azione

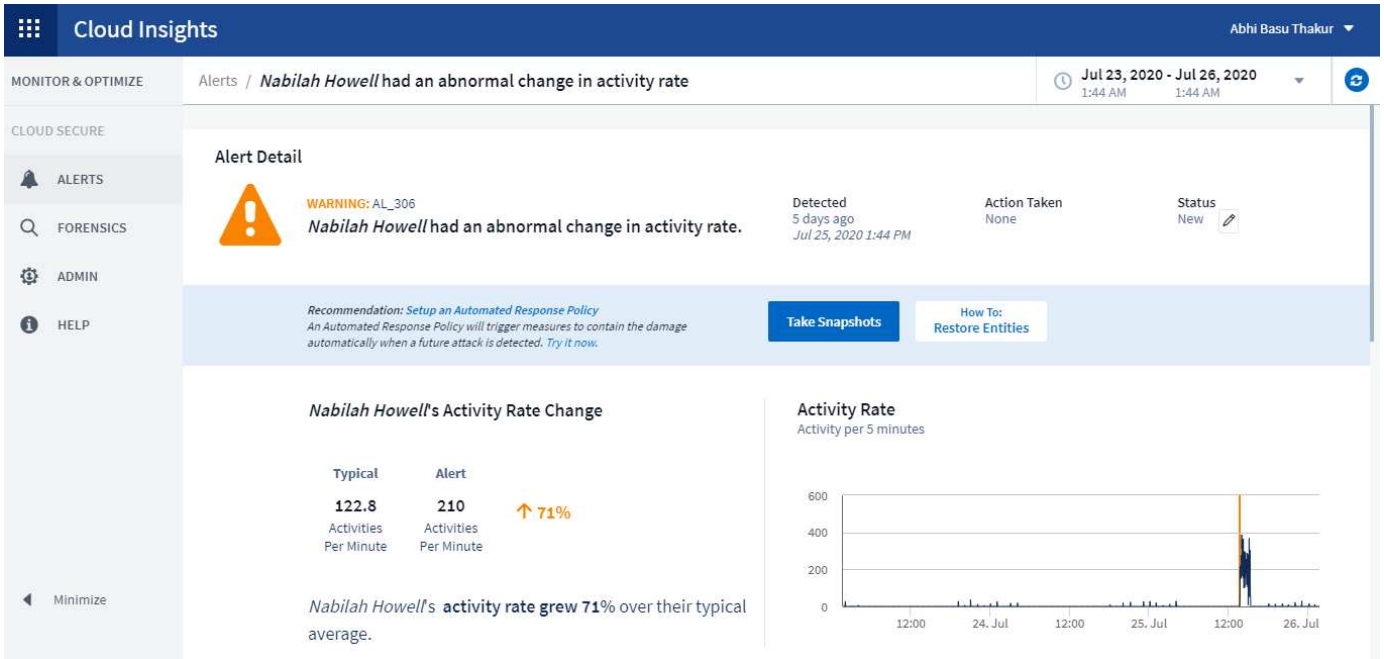
Cloud Secure protegge i dati eseguendo automaticamente un'istantanea quando viene rilevata un'attività dannosa, garantendo un backup sicuro dei dati.

È possibile definire policy di risposta automatizzate che richiedono un'istantanea quando viene rilevato un attacco ransomware o un'altra attività utente anomala. È anche possibile acquisire un'istantanea manualmente dalla pagina di avviso.

Snapshot
automatica:



Snapshot manuale:



Aggiornamenti metriche/contatori

I seguenti contatori di capacità sono disponibili per l'utilizzo nell'interfaccia utente Cloud Insights e nell'API REST. In precedenza, questi contatori erano disponibili solo per Data Warehouse/Reporting.

Tipo di oggetto	Contatore
Storage	Capacità - capacità raw di riserva - raw non riuscito

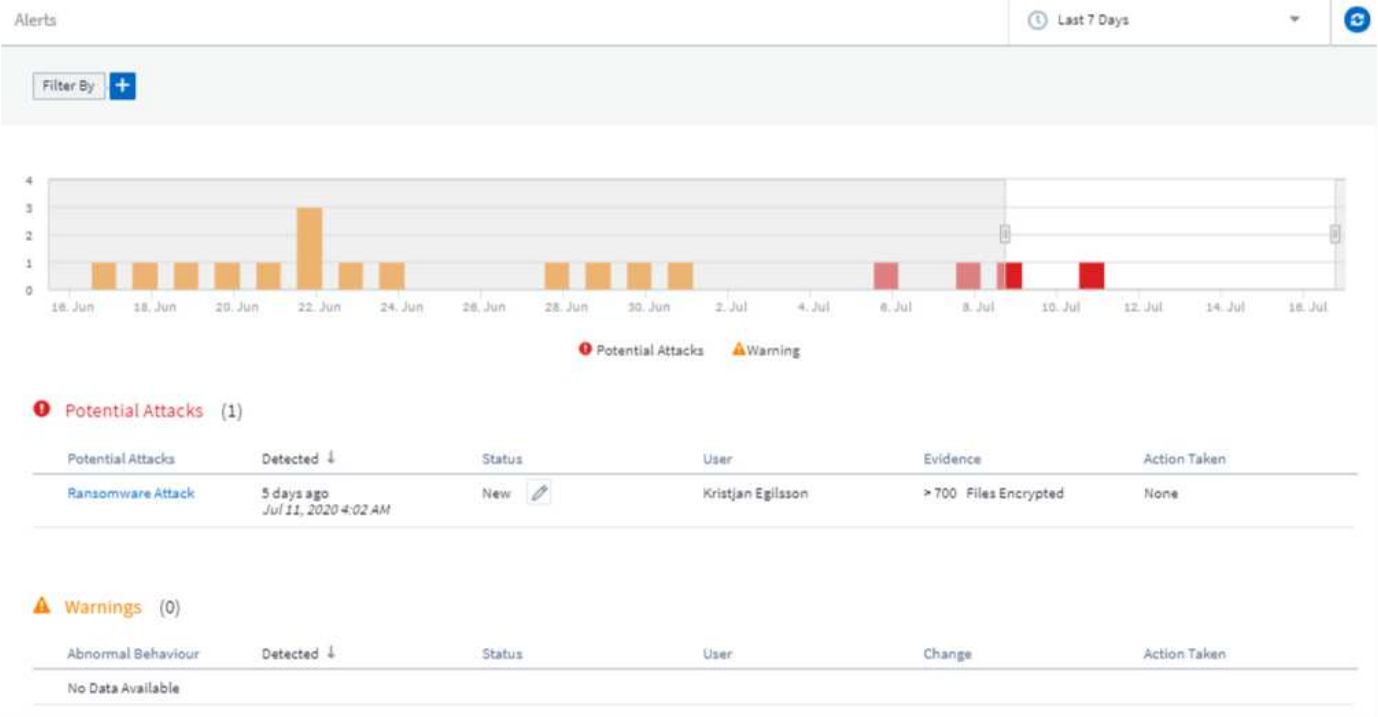
Tipo di oggetto	Contatore
Pool di storage	Capacità dei dati - capacità dei dati utilizzati - capacità totale altra - capacità usata altra - capacità totale - capacità raw - limite progressivo
Volume interno	Capacità dei dati - capacità dei dati utilizzati - capacità totale altra - capacità usata altra - capacità totale salvata del clone - totale

Rilevamento di potenziali attacchi Cloud Secure

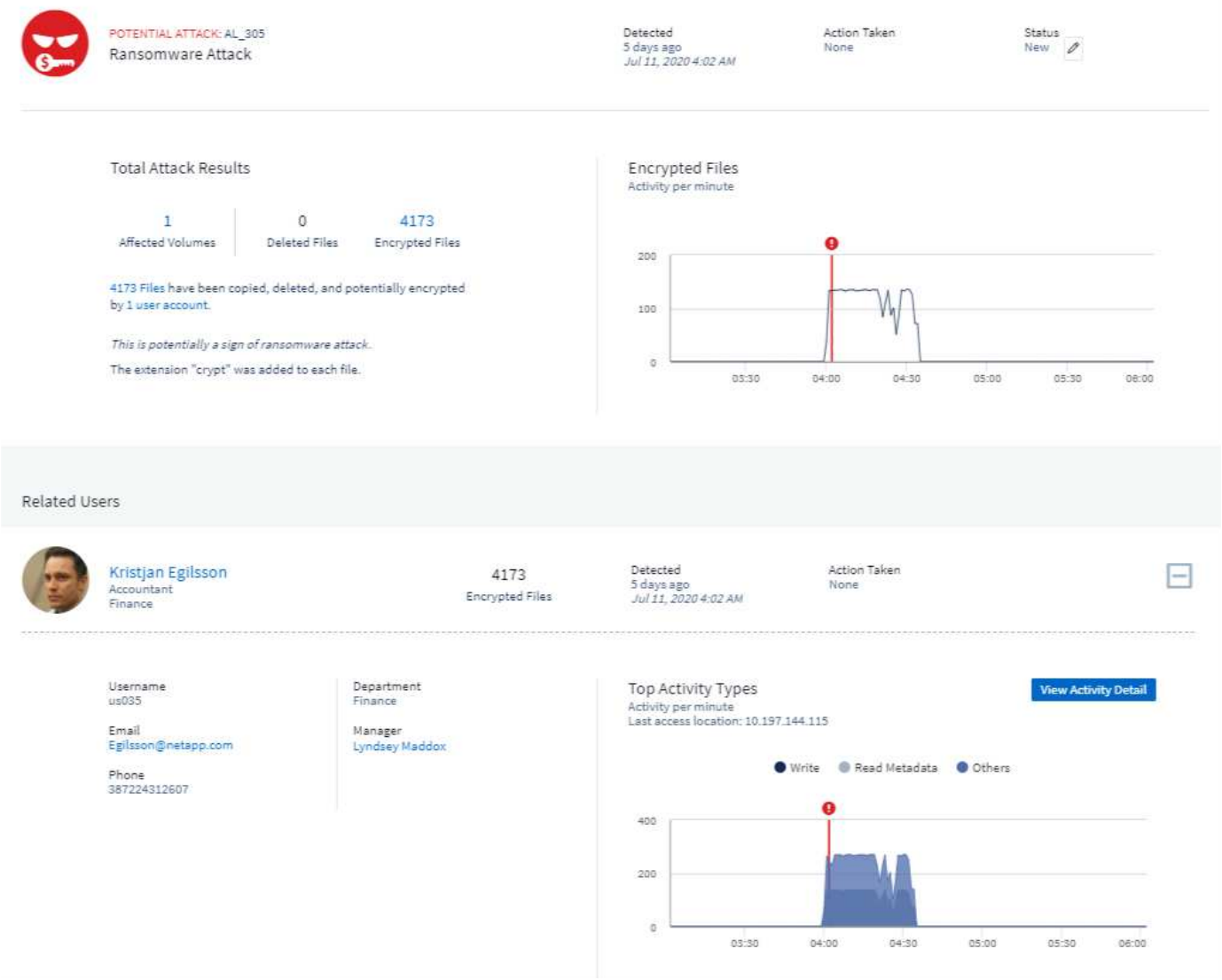
Cloud Secure ora rileva potenziali attacchi come ransomware. Fare clic su un avviso nella pagina dell'elenco degli avvisi per aprire una pagina dei dettagli che mostra quanto segue:

- Tempo di attacco
- Attività associata a utente e file
- Azione intrapresa
- Ulteriori informazioni per aiutare a tenere traccia di eventuali violazioni della sicurezza

Pagina degli avvisi che mostra un potenziale attacco ransomware:



Pagina dei dettagli per un potenziale attacco ransomware:



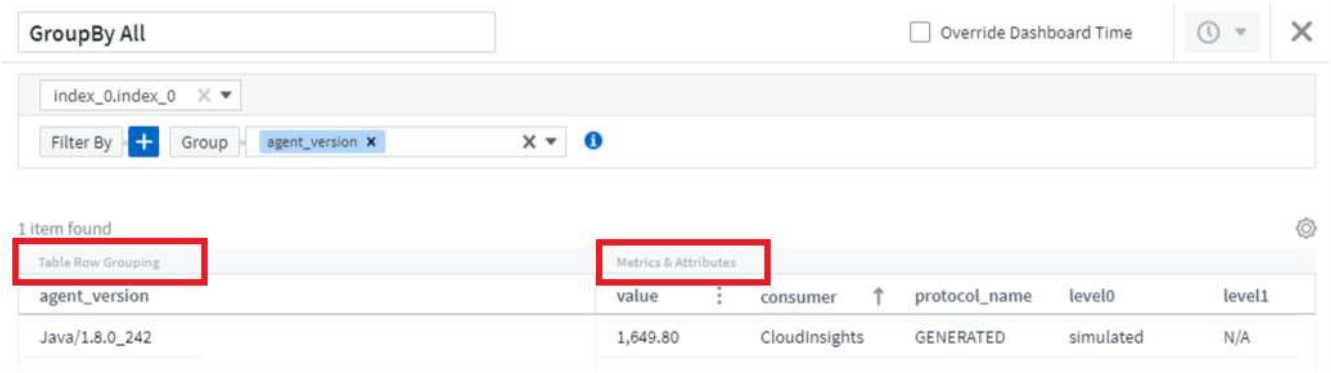
Iscriviti alla Premium Edition tramite AWS

Durante la versione di prova di Cloud Insights, è possibile "iscriviti in autonomia" Tramite il marketplace AWS per Cloud Insights Standard Edition o Premium Edition. In precedenza, era possibile effettuare l'autoscrittura solo tramite AWS Marketplace per la Standard Edition.

Widget tabella avanzato

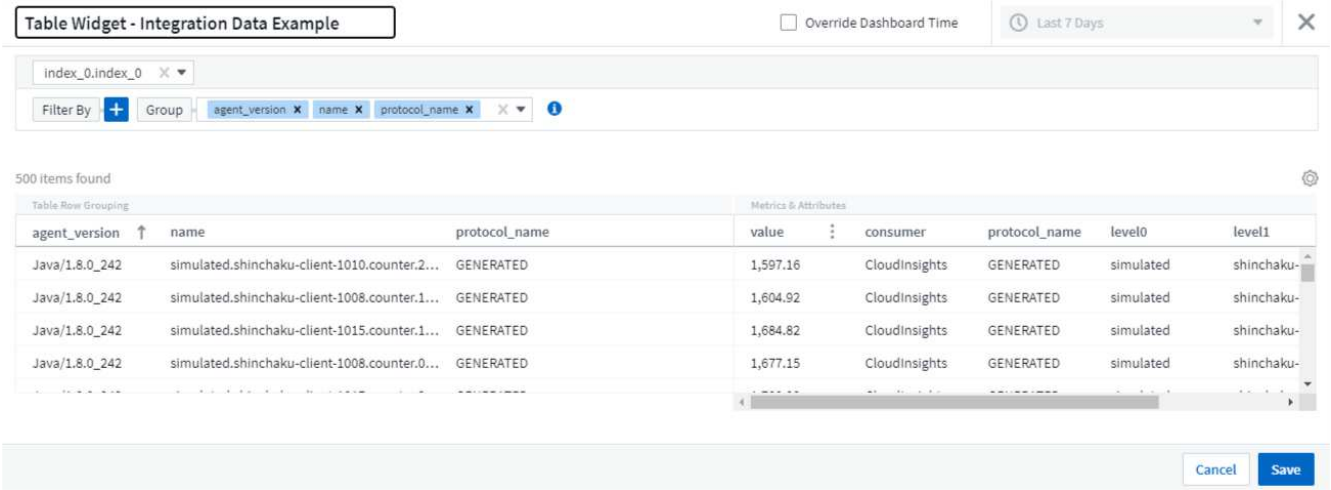
Il widget Tabella dashboard/pagina risorse include i seguenti miglioramenti:

- Vista "split-screen": I widget della tabella visualizzano l'oggetto/raggruppamento a sinistra e i dati dell'oggetto (attributi/metriche) a destra.



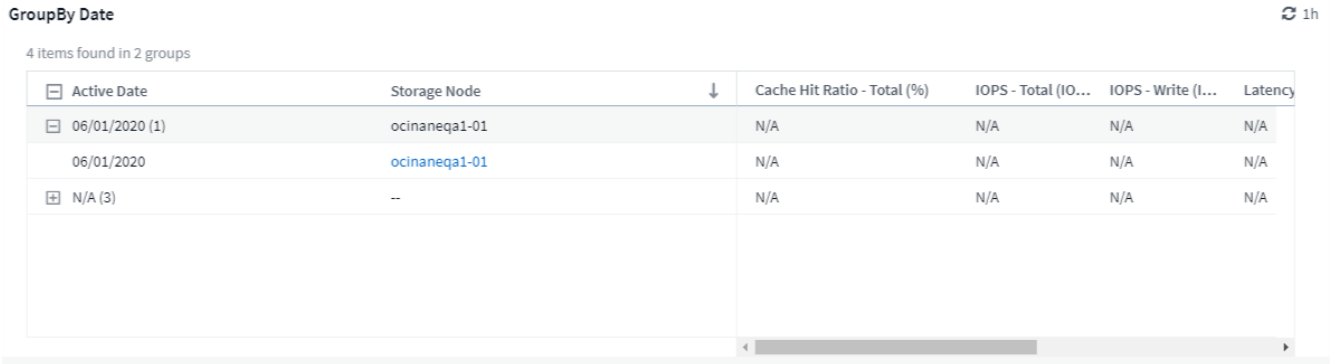
- Raggruppamento di più attributi: Per i dati di integrazione (Kubernetes, metriche avanzate di ONTAP, Docker, ecc.), è possibile scegliere più attributi per il raggruppamento. I dati vengono visualizzati in base agli attributi di raggruppamento scelti.

  Raggruppamento con dati di integrazione (visualizzato in modalità di modifica):



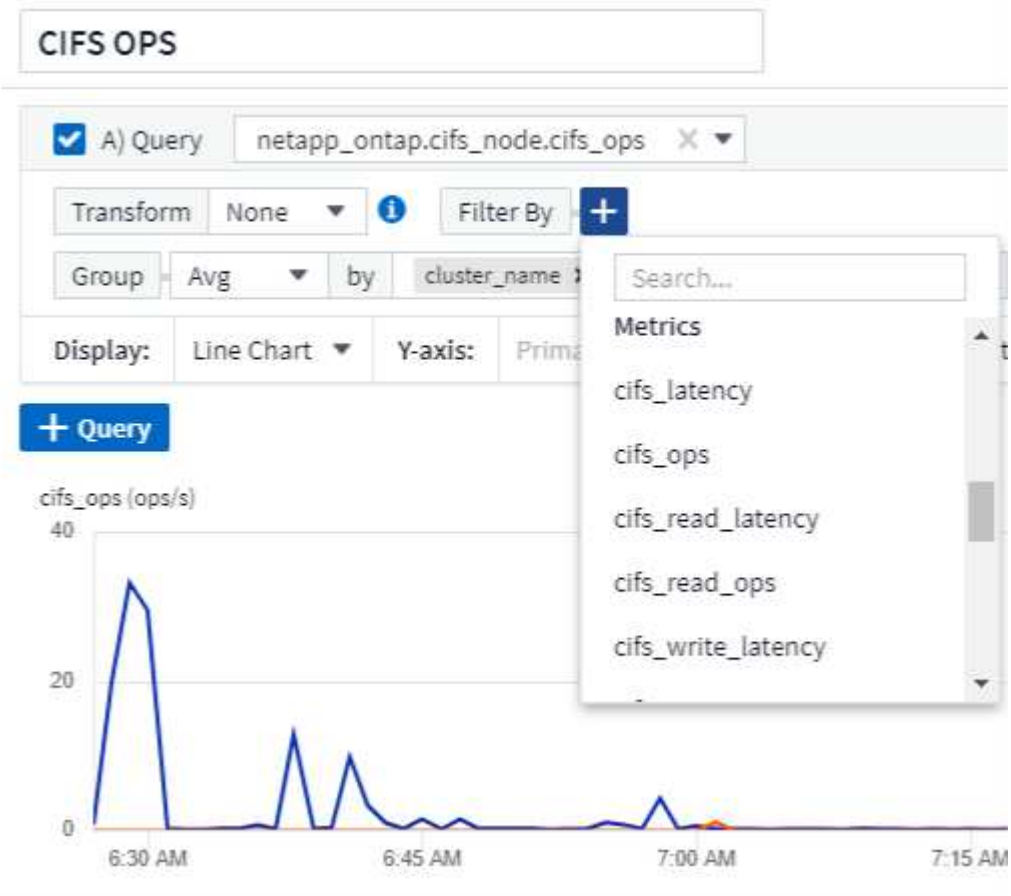
- Il raggruppamento dei dati dell'infrastruttura (storage, EC2, VM, porte, ecc.) avviene mediante un singolo attributo come in precedenza. Durante il raggruppamento in base a un attributo che non è l'oggetto, la tabella consente di espandere la riga di gruppo per visualizzare tutti gli oggetti all'interno del gruppo.

  Raggruppamento con i dati dell'infrastruttura (visualizzati in modalità di visualizzazione):

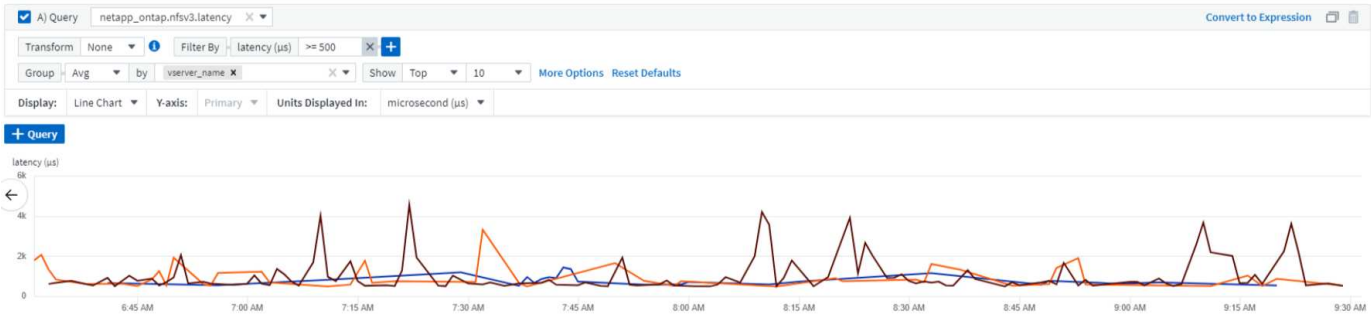


Filtraggio delle metriche

Oltre a filtrare gli attributi di un oggetto in un widget, è possibile filtrare anche le metriche.



Quando si lavora con i dati di integrazione (Kubernetes, dati avanzati ONTAP, ecc.), il filtraggio metrico rimuove i singoli punti dati/non corrispondenti dalla serie di dati plottati, a differenza dei dati dell'infrastruttura (storage, VM, porte, ecc.) in cui i filtri funzionano sul valore aggregato della serie di dati e potenzialmente rimuovono l'intero oggetto dal grafico.

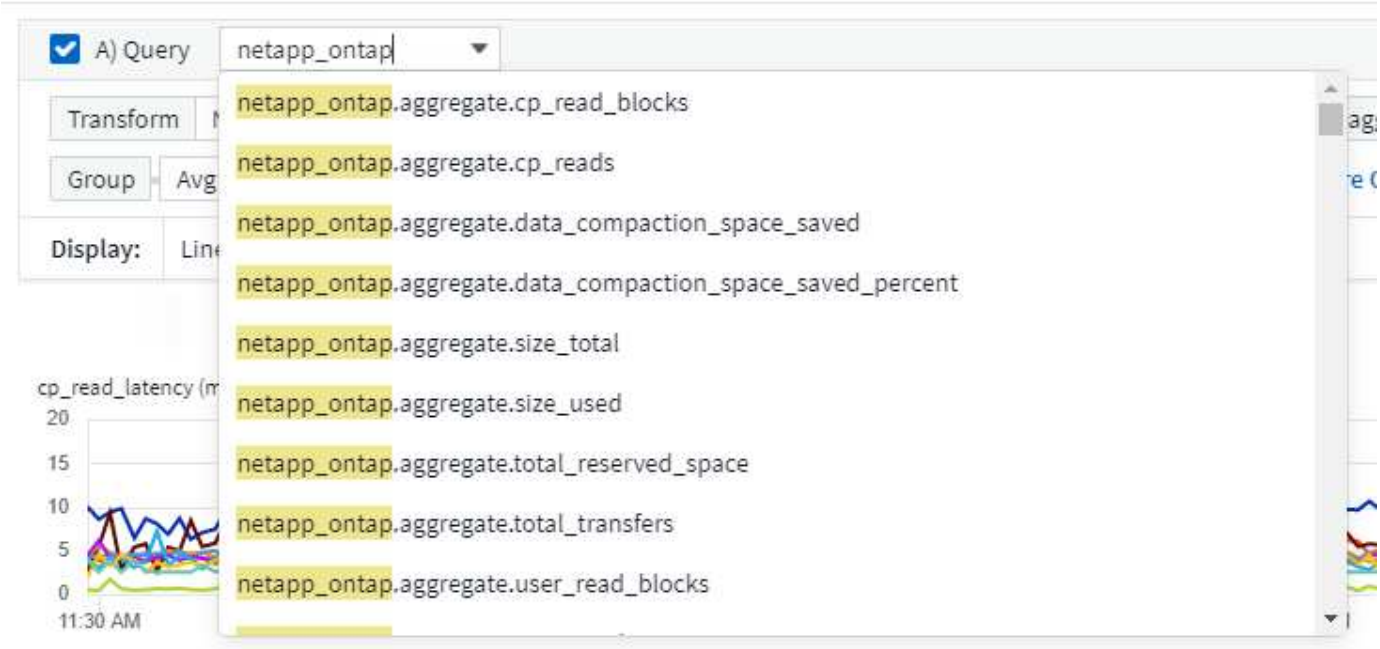


Dati avanzati del contatore ONTAP

Cloud Insights sfrutta i **dati avanzati dei contatori** specifici di ONTAP di NetApp, che forniscono una serie di contatori e metriche raccolti dai dispositivi ONTAP. I dati avanzati del contatore ONTAP sono disponibili per tutti i clienti NetApp ONTAP. Queste metriche consentono una visualizzazione personalizzata e ad ampio raggio in widget e dashboard Cloud Insights.

I contatori avanzati di ONTAP si trovano cercando "netapp_ontap" nella query del widget e selezionando uno

dei contatori.



È possibile perfezionare la ricerca digitando parti aggiuntive del nome del contatore. Ad esempio:

- *lif*
- *aggregato*
- *offbox_vscan_server*
- e molto altro ancora

Tenere presente quanto segue:

- Per impostazione predefinita, la raccolta dati avanzata viene attivata per i nuovi data collection ONTAP. Per abilitare la raccolta avanzata dei dati per i data collector ONTAP esistenti, modificare il data collector ed espandere la sezione *Configurazione avanzata*.
- La raccolta dati avanzata non è disponibile per ONTAP 7-mode.

Dashboard contatori avanzati

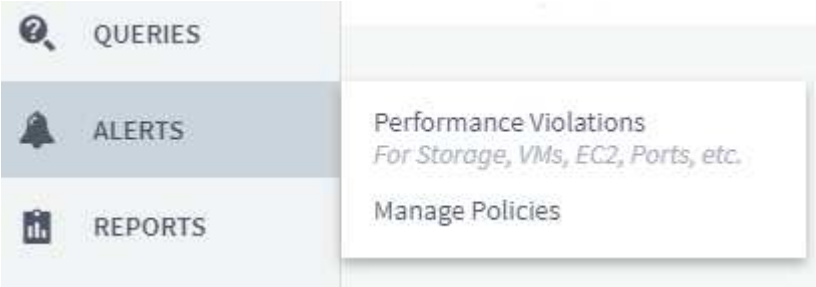
Cloud Insights è dotato di una serie di dashboard pre-progettate per aiutarti a visualizzare i contatori avanzati di ONTAP per argomenti come *prestazioni aggregate*, *carico di lavoro dei volumi*, *attività del processore* e molto altro ancora. Se hai configurato almeno un data collector ONTAP, questi possono essere importati dalla galleria dashboard in qualsiasi pagina di elenco dashboard.

Scopri di più

Ulteriori informazioni sui dati avanzati di ONTAP sono disponibili ai seguenti xref:./*
https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest (Nota: È necessario accedere al supporto NetApp)
* https://nabox.org/faq/

Menu politiche e violazioni

Policy sulle performance e violazioni sono ora disponibili nel menu **Alerts**. Le funzionalità di policy e violazione non sono modificate.



Aggiornato Telegraf Agent

L'agente per l'acquisizione dei dati di integrazione di telegraf è stato aggiornato a. "versione 1.14", che include correzioni di bug, correzioni di sicurezza e nuovi plug-in.

Nota: Durante la configurazione di un data collector Kubernetes sulla piattaforma Kubernetes, potrebbe essere visualizzato un errore "HTTP status 403 Forbidden" nel log, a causa di autorizzazioni insufficienti nell'attributo "clusterrole".

Per risolvere questo problema, aggiungere le seguenti righe evidenziate alla sezione *rules:* del ruolo del cluster di accesso all'endpoint, quindi riavviare i pod Telegraf.

```
rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
  attributeRestrictions: null
  resources:
  - nodes/metrics
  - nodes/proxy     <== Add this line
  - nodes/stats
  - pods            <== Add this line
  verbs:
  - get
  - list            <== Add this line
```

Giugno 2020

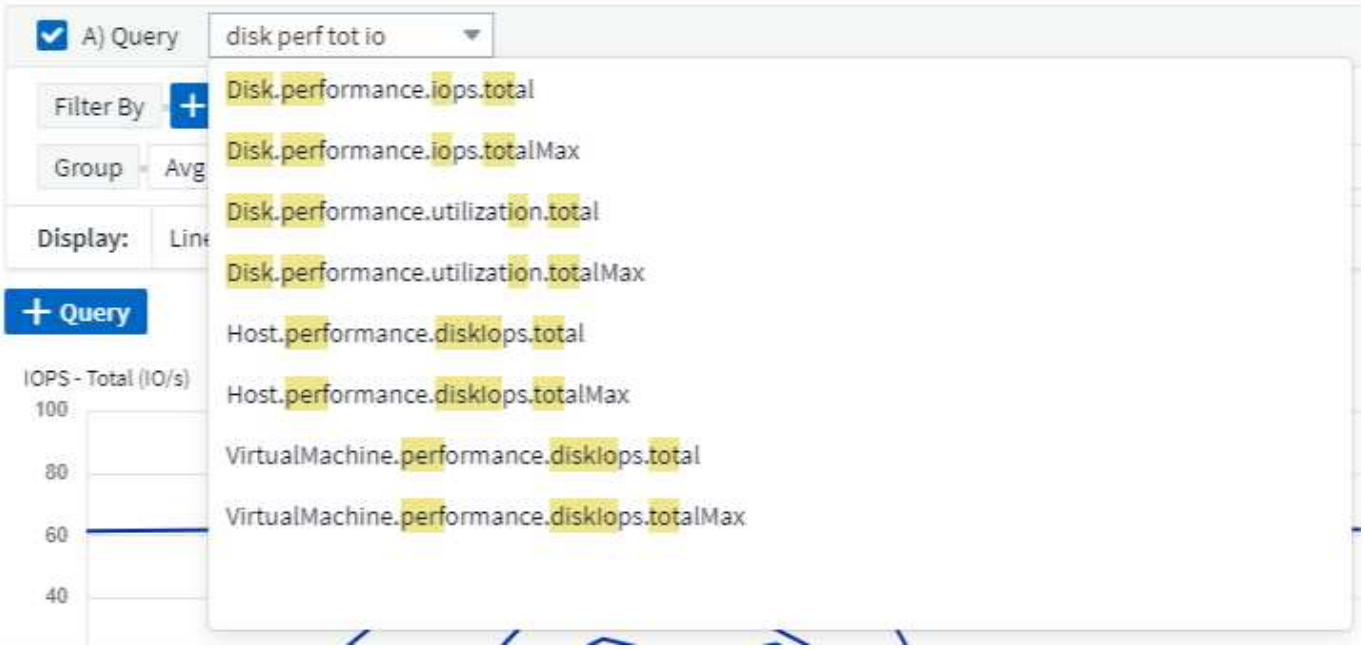
Report degli errori di Data Collector semplificato

La segnalazione di un errore di data collector è più semplice con il pulsante *Send Error Report* (Invia report errori) nella pagina di data collector. Fare clic sul pulsante per inviare a NetApp le informazioni di base sull'errore e richiedere l'analisi del problema. Una volta premuto, Cloud Insights riconosce che NetApp è stata notificata e il pulsante Report errori viene disattivato per indicare che è stato inviato un report degli errori per quel data collector. Il pulsante rimane disattivato fino a quando la pagina del browser non viene aggiornata.

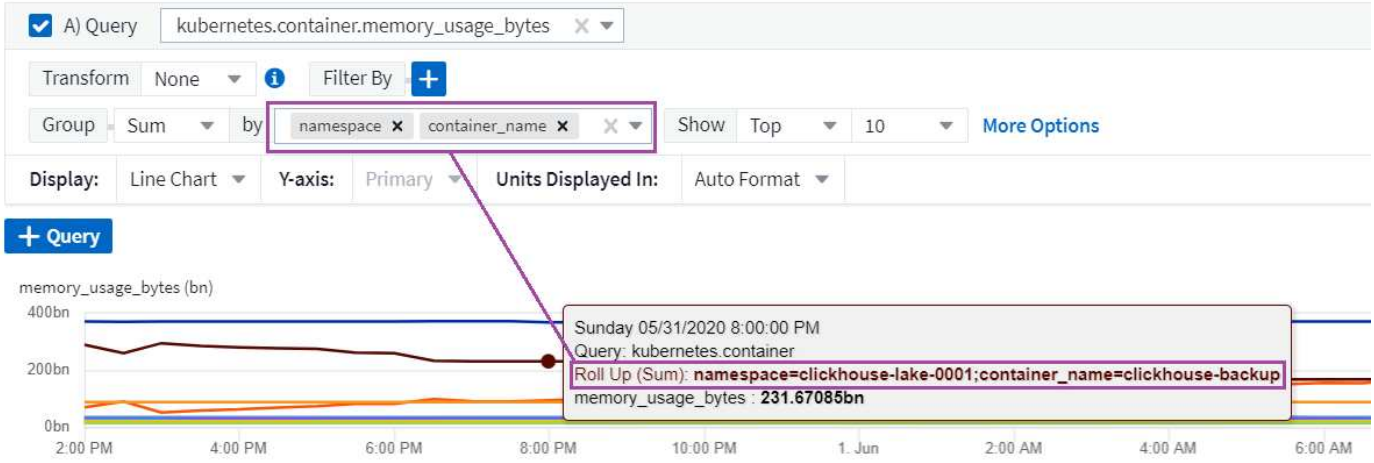
Miglioramenti dei widget

I seguenti miglioramenti sono stati apportati ai widget della dashboard. Questi miglioramenti sono considerati funzionalità di anteprima e potrebbero non essere disponibili per tutti gli ambienti Cloud Insights.

- Nuovo strumento di scelta di oggetti/metriche: Gli oggetti (storage, disco, porte, nodi, ecc.) e le relative metriche (IOPS, latenza, numero di CPU, ecc.) sono ora disponibili nei widget in un unico menu a discesa completo con una potente funzione di ricerca. È possibile inserire più termini parziali nell'elenco a discesa e Cloud Insights elenca tutte le metriche degli oggetti che soddisfano tali termini.



- Raggruppamento di tag multipli: Quando si lavora con i dati di integrazione (Kubernetes, ecc.), è possibile raggruppare i dati in base a tag/attributi multipli. Ad esempio, somma dell'utilizzo della memoria da parte dello spazio dei nomi Kubernetes e del nome del container.



Maggio 2020

Ruoli utente di reporting

Sono stati aggiunti i seguenti ruoli per il reporting:

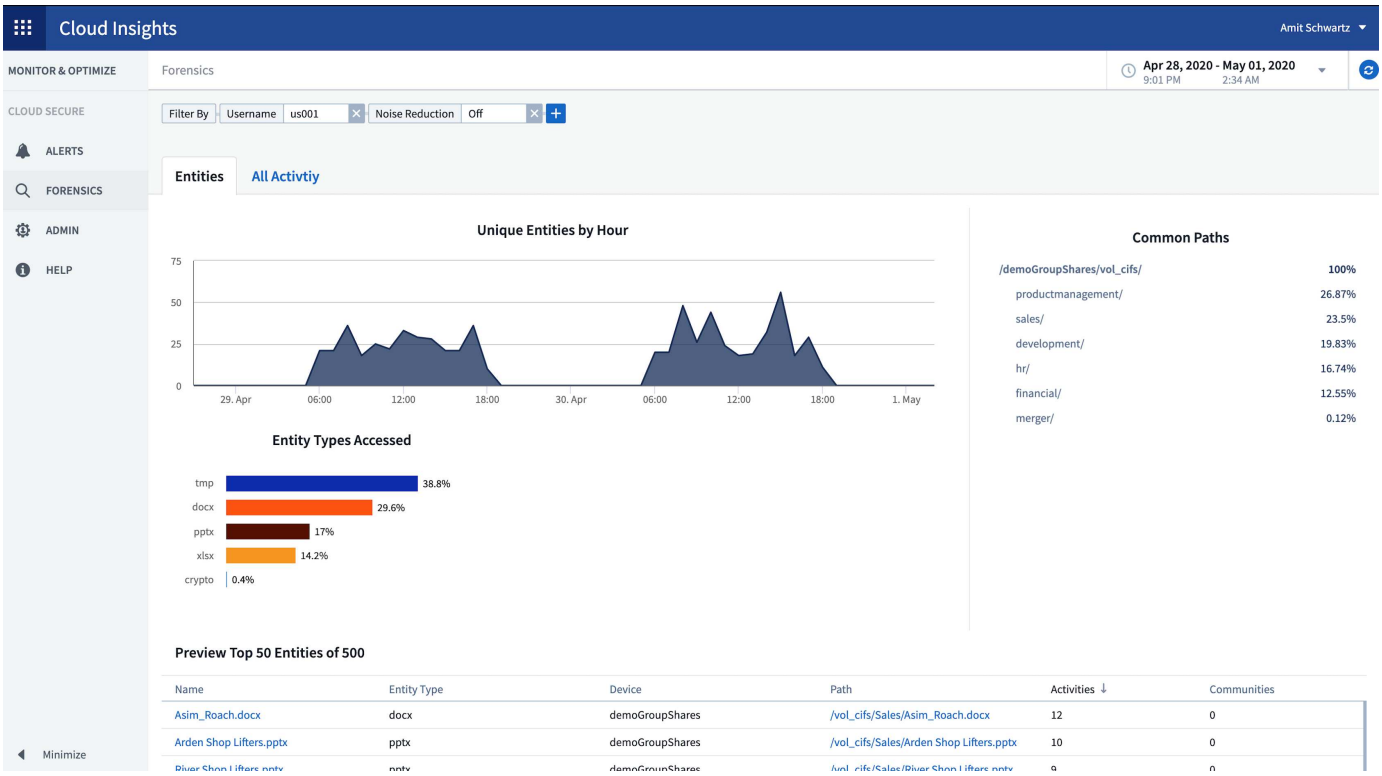
- Utenti Cloud Insights: Possono eseguire e visualizzare report
- Autori Cloud Insights: Possono eseguire le funzioni del cliente e creare e gestire report e dashboard
- Amministratori di Cloud Insights: Possono eseguire le funzioni autore e tutte le attività amministrative

Aggiornamenti Cloud Secure

Cloud Insights include le seguenti recenti modifiche Cloud Secure.

Nella pagina Forensics > Activity Forensics, sono disponibili due viste per analizzare e analizzare le attività degli utenti:

- Vista delle attività, incentrata sull'attività dell'utente (quale operazione? Dove sono state eseguite?)
- Vista delle entità, incentrata sui file a cui l'utente ha effettuato l'accesso.

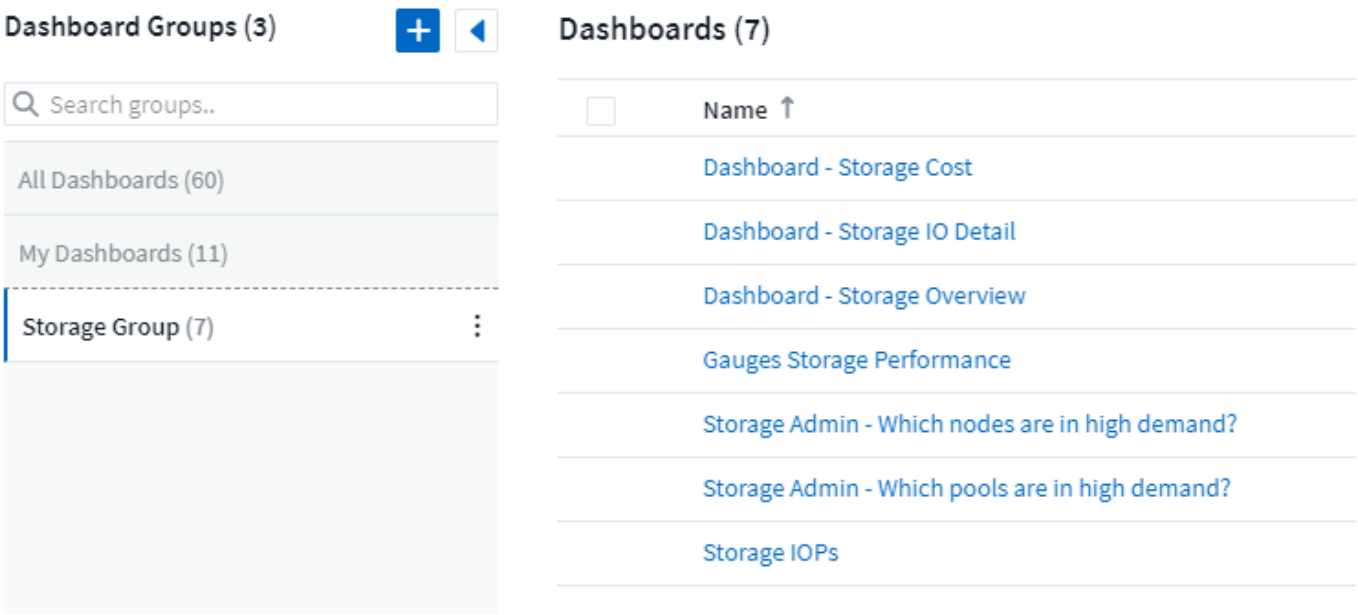


Inoltre, la notifica e-mail di avviso ora contiene un collegamento diretto alla pagina di avviso.

Raggruppamento dashboard

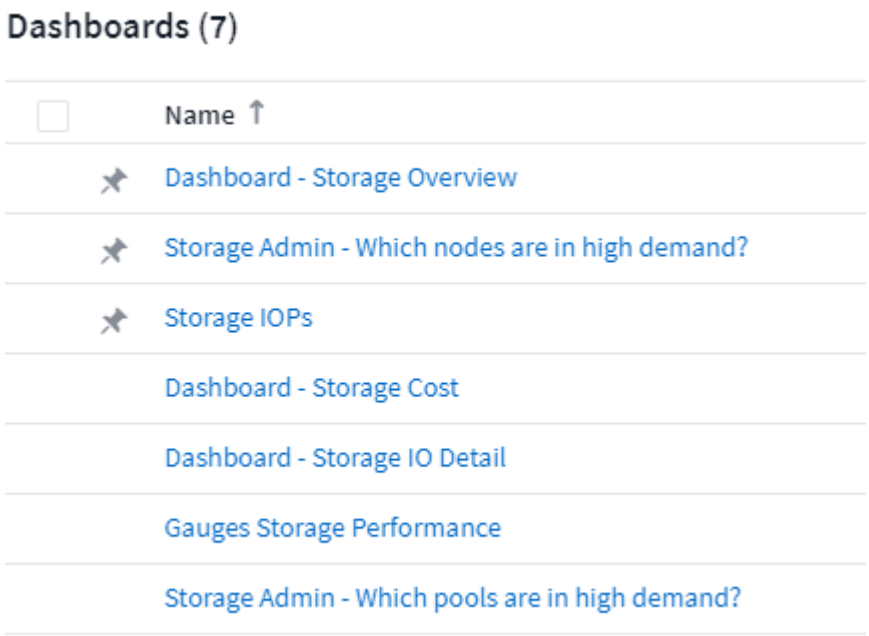
Il raggruppamento delle dashboard consente di migliorare "gestione delle dashboard" che sono importanti per te. È possibile aggiungere dashboard correlati a un gruppo per la gestione "one-stop", ad esempio, dello storage o delle macchine virtuali.

I gruppi sono personalizzati per utente, in modo che i gruppi di una persona possano essere diversi da quelli di un'altra persona. Puoi avere tutti i gruppi di cui hai bisogno, con il numero di dashboard in ogni gruppo che preferisci.



Pinning della dashboard

Puoi inserire i dashboard in modo che i preferiti siano sempre visualizzati all'inizio dell'elenco.



Modalità TV e aggiornamento automatico

"Modalità TV e aggiornamento automatico" consentire la visualizzazione quasi in tempo reale dei dati su una dashboard o una pagina di risorse:

- **La modalità TV** offre un display ordinato; il menu di navigazione è nascosto, offrendo più spazio per la visualizzazione dei dati.
- Dati nei widget su dashboard e pagine di destinazione risorse **aggiornamento automatico** in base a un intervallo di refresh (minimo ogni 10 secondi) determinato dall'intervallo di tempo del dashboard

selezionato (o intervallo di tempo del widget, se impostato per sostituire l'ora del dashboard).

La combinazione di modalità TV e aggiornamento automatico offre una visualizzazione live dei dati Cloud Insights, perfetta per dimostrazioni senza problemi o monitoring in-house.

Aprile 2020

Nuove scelte di intervallo temporale del dashboard

Le scelte di intervallo di tempo per dashboard e altre pagine Cloud Insights ora includono *ultima 1 ora* e *ultimi 15 minuti*.

Aggiornamenti Cloud Secure

Cloud Insights include le seguenti recenti modifiche Cloud Secure.

- Migliore riconoscimento dei metadati di file e cartelle per rilevare se l'utente ha modificato Permission, Owner o Group Ownership.
- Esporta report attività utente in CSV.

Cloud Secure monitora e controlla tutte le operazioni di accesso degli utenti su file e cartelle. Il controllo delle attività consente di rispettare le policy di sicurezza interne, soddisfare i requisiti di conformità esterni come PCI, GDPR e HIPAA e condurre indagini su violazioni dei dati e incidenti di sicurezza.

Ora dashboard predefinita

L'intervallo di tempo predefinito per le dashboard è ora di 3 ore invece di 24 ore.

Tempi di aggregazione ottimizzati

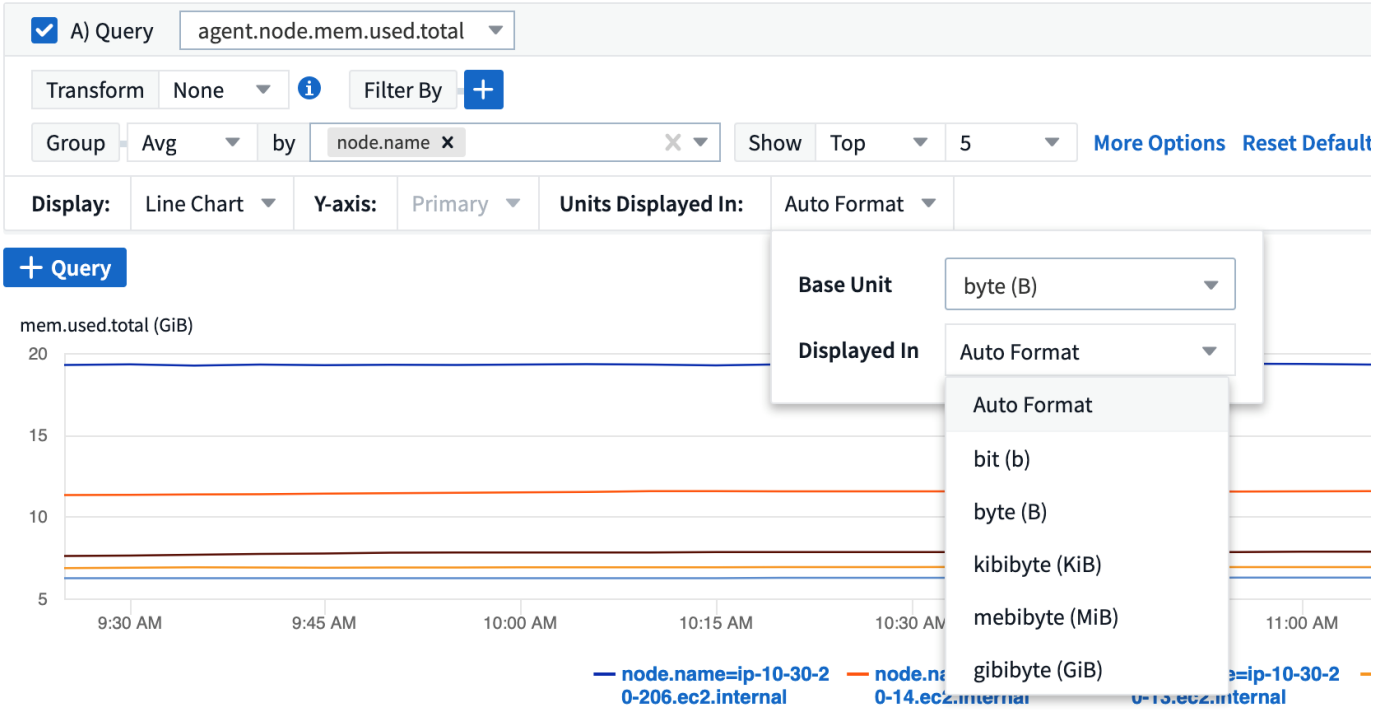
Ottimizzato "aggregazione del tempo" Gli intervalli nei widget Time-Series (grafici Line, Spline, Area e Stacked Area) sono più frequenti per intervalli di tempo di 3 ore e 24 ore per dashboard/widget, consentendo una più rapida registrazione dei dati.

- l'intervallo di tempo di 3 ore consente di ottimizzare l'intervallo di aggregazione di 1 minuto. In precedenza era di 5 minuti.
- l'intervallo di tempo di 24 ore consente di ottimizzare un intervallo di aggregazione di 30 minuti. In precedenza era di 1 ora.

È comunque possibile eseguire l'override dell'aggregazione ottimizzata impostando un intervallo personalizzato.

Formattazione automatica unità di visualizzazione

Nella maggior parte dei widget, Cloud Insights conosce l'unità base in cui visualizzare i valori, ad esempio *Megabyte*, *migliaia*, *percentuale*, *millisecondi (ms)*, ecc., e ora "formatta automaticamente" il widget per l'unità più leggibile. Ad esempio, un valore dei dati di 1,234,567,890 byte viene automaticamente formattato in 1.23 gibibyte. In molti casi, Cloud Insights conosce il formato migliore per i dati acquisiti. Nei casi in cui non si conosce il formato migliore o nei widget in cui si desidera eseguire l'override della formattazione automatica, è possibile scegliere il formato desiderato.

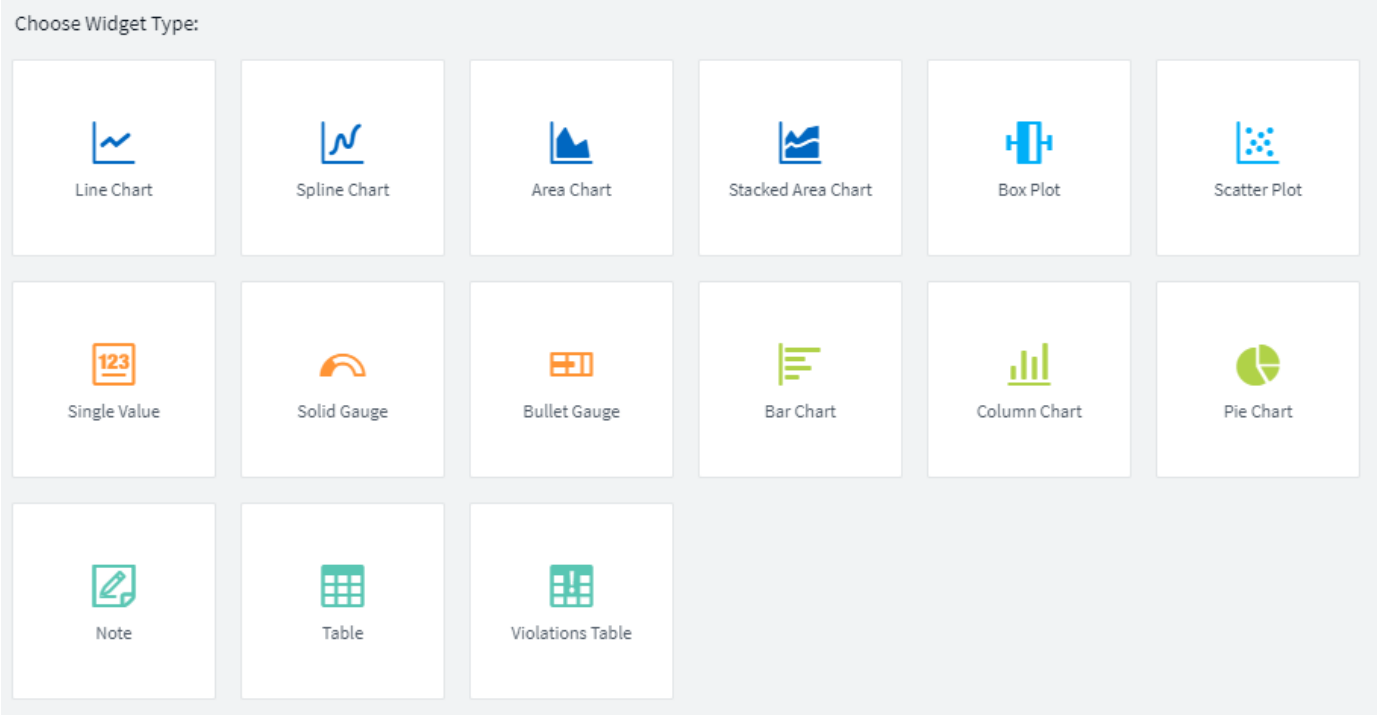


Importa annotazioni usando API

Con la potente API di Cloud Insights Premium Edition, ora puoi farlo "importa annotazioni" E assegnarli agli oggetti utilizzando un file .CSV. È inoltre possibile importare le applicazioni e assegnare le entità di business nello stesso modo.

Strumento di selezione dei widget più semplice

L'aggiunta di widget a dashboard e pagine di destinazione delle risorse è più semplice grazie a un nuovo selettore di widget che mostra tutti i tipi di widget in una singola vista all-at-one, in modo che l'utente non debba più scorrere un elenco di tipi di widget per trovare quello che desidera aggiungere. I widget correlati sono coordinati in base al colore e raggruppati in base alla prossimità nel nuovo selettore.



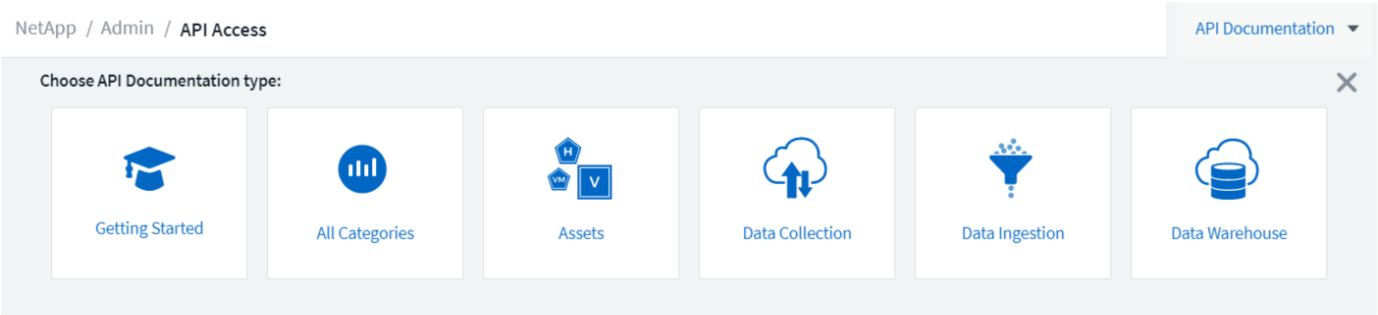
Febbraio 2020

API con Premium Edition

L'edizione Premium di Cloud Insights include un "API potente" Che può essere utilizzato per integrare Cloud Insights con altre applicazioni, come CMDB o altri sistemi di ticketing.

Informazioni dettagliate e basate su Swagger sono disponibili in **Admin > API Acccess**, sotto il link **API Documentation**. Swagger fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provare ogni API nel proprio ambiente.

L'API Cloud Insights utilizza i token di accesso per fornire l'accesso basato sulle autorizzazioni a categorie di API, come AD esempio LE RISORSE o LA RACCOLTA.



Polling iniziale dopo l'aggiunta Di un Data Collector

In precedenza, dopo aver configurato un nuovo data collector, Cloud Insights eseguirebbe il polling immediato del data collector per raccogliere i dati *inventory*, ma attendeva fino all'intervallo di polling delle prestazioni configurato (in genere 15 minuti) per raccogliere i dati iniziali di *performance*. Quindi, prima di iniziare il

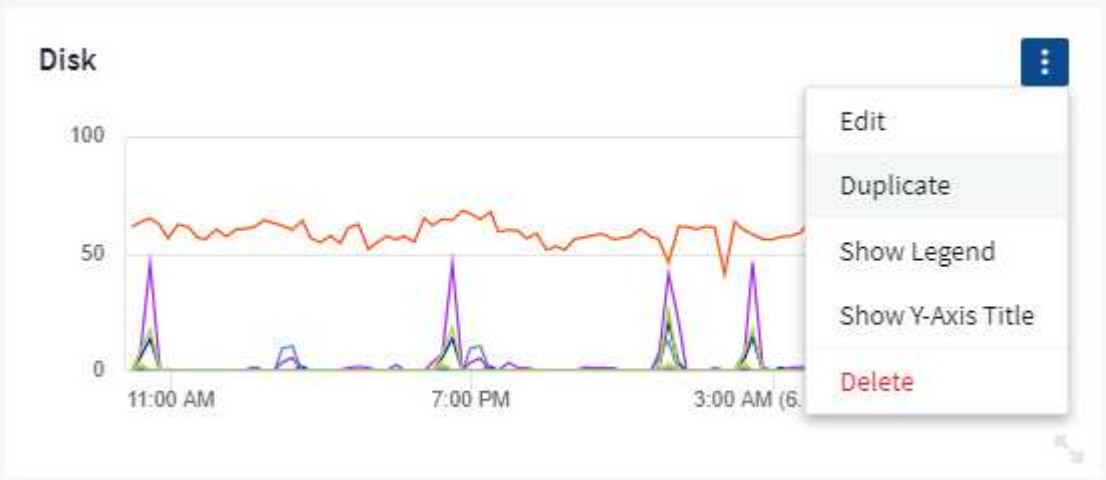
secondo sondaggio sulle performance, il sistema attenderebbe un altro intervallo, il che significa che sarebbero necessari fino a *30 minuti* prima che i dati significativi fossero acquisiti da un nuovo data collector.

Data collector "polling" è stato notevolmente migliorato, in modo che il sondaggio iniziale sulle performance si verifichi immediatamente dopo il sondaggio sull'inventario, con il secondo sondaggio sulle performance che si verifica entro pochi secondi dal completamento del primo sondaggio sulle performance. Ciò consente a Cloud Insights di iniziare a mostrare dati utili su dashboard e grafici in un tempo molto breve.

Questo comportamento di polling si verifica anche dopo la modifica della configurazione di un data collector esistente.

Duplicazione dei widget più semplice

Creare una copia di un widget su una dashboard o una landing page è più semplice che mai. In modalità Dashboard Edit (Modifica dashboard), fare clic sul menu del widget e selezionare **Duplicate** (Duplica). Viene avviato l'editor dei widget, compilato con la configurazione originale del widget e con il suffisso "copy" nel nome del widget. È possibile apportare facilmente le modifiche necessarie e salvare il nuovo widget. Il widget viene posizionato nella parte inferiore della dashboard ed è possibile posizionarlo in base alle esigenze. Ricordarsi di salvare la dashboard una volta completate tutte le modifiche.



Single Sign-on (SSO)

Con l'edizione Premium di Cloud Insights, gli amministratori possono abilitare **"Single Sign-on (accesso singolo)"** (SSO) accesso a Cloud Insights per tutti gli utenti del proprio dominio aziendale, senza doverli invitare singolarmente. Con SSO attivato, qualsiasi utente con lo stesso indirizzo e-mail di dominio può accedere a Cloud Insights utilizzando le proprie credenziali aziendali.

> SSO è disponibile solo in Cloud Insights Premium Edition e deve essere configurato prima di poter essere abilitato per Cloud Insights. La configurazione SSO include "Federazione delle identità" Tramite NetApp Cloud Central. La federazione consente agli utenti single sign-on di accedere ai tuoi account NetApp Cloud Central utilizzando le credenziali della tua directory aziendale.

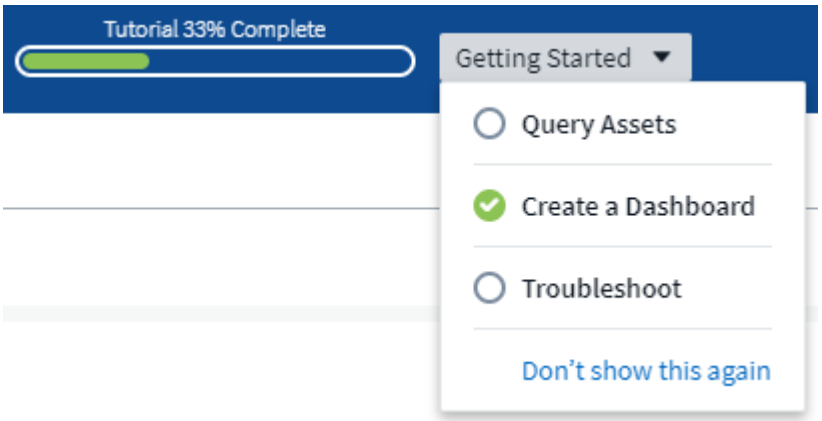
Gennaio 2020

Documentazione di swagger per API REST

Swagger spiega ogni API REST disponibile in Cloud Insights, il suo utilizzo e la sua sintassi. Le informazioni sulle API Cloud Insights sono disponibili in "documentazione".

Barra di avanzamento dei tutorial delle funzioni

L'elenco di controllo dei tutorial sulle funzionalità è stato spostato sul banner superiore e ora presenta un indicatore di avanzamento. I tutorial sono disponibili per ciascun utente fino a quando non vengono dismessi e sono sempre disponibili in Cloud Insights "documentazione".



Modifiche dell'unità di acquisizione

Quando si installa un'unità di acquisizione (AU) su un host o una macchina virtuale con lo stesso nome di un AU già installato, Cloud Insights garantisce un nome univoco aggiungendo il nome dell'AU con "_1", "_2", ecc. Questo avviene anche quando si disinstalla e reinstalla un AU dalla stessa macchina virtuale senza prima rimuoverlo da Cloud Insights. Vuoi un nome AU diverso? Nessun problema; gli AU possono essere rinominati dopo l'installazione.

Aggregazione di tempo ottimizzata nei widget

Nei widget, è possibile scegliere tra un intervallo di aggregazione del tempo *ottimizzato* o un intervallo *personalizzato* impostato. Optimized aggregation seleziona automaticamente l'intervallo di tempo corretto in base all'intervallo di tempo del dashboard selezionato (o intervallo di tempo del widget, se si sovrascriverà l'ora del dashboard). L'intervallo cambia dinamicamente quando viene modificato l'intervallo di tempo del dashboard o del widget.

Processo semplificato "Getting Started with Cloud Insights"

Il processo per iniziare a utilizzare Cloud Insights è stato semplificato per semplificare e semplificare la prima installazione. È sufficiente selezionare un data collector iniziale e seguire le istruzioni. Cloud Insights guida l'utente nella configurazione del data collector e di qualsiasi agente o unità di acquisizione richiesta. Nella maggior parte dei casi, l'IT importa anche una o più dashboard iniziali in modo da poter iniziare a ottenere rapidamente informazioni sull'ambiente (ma attendere fino a 30 minuti per consentire a Cloud Insights di raccogliere dati significativi).

Ulteriori miglioramenti:

- L'installazione dell'unità di acquisizione è più semplice e veloce.

- Le opzioni di raccolta dati alfabetici semplificano la ricerca di quello desiderato.
- Le istruzioni di configurazione di Data Collector migliorate sono più semplici da seguire.
- Gli utenti esperti possono saltare il processo di guida introduttiva con un semplice clic.
- Una nuova barra di avanzamento mostra la posizione in cui ci si trova nel processo.

Dicembre 2019

L'entità aziendale può essere utilizzata nei filtri

Le annotazioni dell'entità aziendale possono essere utilizzate nei filtri per query, widget, policy di performance e landing page.

Drill-down disponibile per i widget Single-Value e Gauge e per tutti i widget inseriti da "All"

Facendo clic sul valore in un widget a valore singolo o gauge si apre una pagina di query che mostra i risultati della prima query utilizzata nel widget. Inoltre, facendo clic sulla legenda per qualsiasi widget i cui dati vengono arrotolati da "tutti", viene visualizzata anche una pagina di query che mostra i risultati della prima query utilizzata nel widget.

Periodo di prova esteso

I nuovi utenti che si iscrivono per una versione di prova gratuita di Cloud Insights hanno ora 30 giorni per valutare il prodotto. Si tratta di un aumento rispetto al periodo di prova precedente di 14 giorni.

Calcolo dell'unità gestita

Il calcolo delle unità gestite (MU) in Cloud Insights è stato modificato come segue:

- 1 unità gestita = 2 host (qualsiasi macchina virtuale o fisica)
- 1 unità gestita = 4 TB di capacità non formattata di dischi fisici o virtuali

Questa modifica raddoppia effettivamente la capacità dell'ambiente che è possibile monitorare utilizzando l'abbonamento Cloud Insights esistente.

Novembre 2019

Tabella di confronto delle funzionalità delle edizioni

Pagina **Admin > Subscription** "tabella di confronto" È stato aggiornato per elencare i set di funzionalità

disponibili nelle edizioni di base, standard e Premium di Cloud Insights. NetApp sta costantemente migliorando i suoi servizi cloud, quindi consulta spesso questa pagina per trovare l'edizione più adatta alle tue esigenze di business in continua evoluzione.

Ottobre 2019

Creazione di report

"Report Cloud Insights" è uno strumento di business intelligence che consente di visualizzare report predefiniti o di creare report personalizzati. Con Reporting 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 Cloud Insights possono generare report personalizzati per aree come chargeback, analisi dei consumi e previsioni e possono aiutare a rispondere a domande come:

- 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?
- 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?

I report sono disponibili con Cloud Insights **Premium Edition**.

Miglioramenti di Active IQ

"Rischi Active IQ" sono ora disponibili come oggetti che possono essere interrogati e utilizzati nei widget della tabella della dashboard. Sono inclusi i seguenti attributi degli oggetti rischi: * Categoria * Categoria di mitigazione * potenziale impatto * dettaglio del rischio * severità * origine * Storage * Storage Node * Categoria UI

Settembre 2019

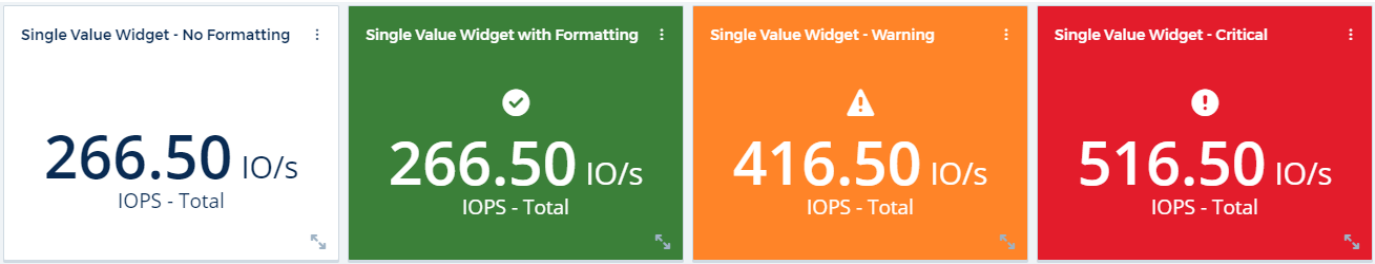
Nuovi widget Gauge

Sono disponibili due nuovi widget per visualizzare i dati a valore singolo sui dashboard in colori accattivanti in base alle soglie specificate. È possibile visualizzare i valori utilizzando un **indicatore solido** o **indicatore**

elenco. I valori che rientrano nell'intervallo di avviso sono visualizzati in arancione. I valori nell'intervallo critico vengono visualizzati in rosso. I valori al di sotto della soglia di avviso vengono visualizzati in verde.

Formattazione del colore condizionale per il widget a valore singolo

È ora possibile visualizzare il widget valore singolo con uno sfondo colorato in base alle soglie impostate.



Invita utenti durante l'inserimento

In qualsiasi momento durante il processo di assunzione, puoi fare clic su Amministrazione > Gestione utenti > +utente per invitare altri utenti nel tuo ambiente Cloud Insights. Tenere presente che gli utenti con ruoli *Guest* o *User* otterranno maggiori benefici una volta completata l'assunzione e raccolti i dati.

Miglioramento della pagina dei dettagli di Data Collector

La pagina dei dettagli del data collector è stata migliorata per visualizzare gli errori in un formato più leggibile. Gli errori vengono ora visualizzati in una tabella separata della pagina, con ciascun errore visualizzato su una riga separata in caso di errori multipli per il data collector.

Agosto 2019

Tutti contro Data Collector disponibili

Quando si aggiungono dati di raccolta al proprio ambiente, è possibile impostare un filtro per visualizzare solo i dati di raccolta disponibili in base al livello di abbonamento o a tutti i dati di raccolta.

Integrazione ActiveIQ

Cloud Insights raccoglie i dati da NetApp ActiveIQ, che fornisce una serie di visualizzazioni, analytics e altri servizi correlati al supporto ai clienti NetApp e ai loro sistemi hardware/software. Cloud Insights si integra con i sistemi di gestione dei dati ONTAP. Vedere "Active IQ" per ulteriori informazioni.

Luglio 2019

Miglioramenti della dashboard

Dashboard e widget sono stati migliorati con le seguenti modifiche:

- Oltre a somma, min, Max e Avg, **Count** è ora un'opzione per il rolloup nei widget a valore singolo. Quando si esegue il rollup per "Conteggio", Cloud Insights verifica se un oggetto è attivo o meno e aggiunge solo quelli attivi al conteggio. Il numero risultante è soggetto a aggregazione e filtri.
- Nel widget valore singolo, è possibile visualizzare il numero risultante con 0, 1, 2, 3 o 4 cifre decimali.
- I grafici a linee mostrano un'etichetta e le unità dell'asse quando viene tracciato un singolo contatore.
- L'opzione **Transform** è ora disponibile per i dati di integrazione dei servizi in tutti i widget Time-Series per tutte le metriche. Per qualsiasi contatore o metrica di integrazione dei servizi (Telegraf) nei widget Time-Series (linea, Spline, Area, Stacked Area), è possibile scegliere la modalità desiderata "Trasformare i valori". Nessuno (valore visualizzato così com'è), somma, Delta, cumulativo, ecc.

Downgrade a Basic Edition

Il downgrade a Basic Edition non riesce e viene visualizzato un messaggio di errore se non è stato configurato alcun dispositivo NetApp disponibile che abbia completato correttamente un sondaggio negli ultimi 7 giorni.

Raccolta delle metriche dello stato del Kube

Il "Kubernetes Data Collector" Ora raccoglie oggetti e contatori dal plugin kube-state-metrics, espandendo notevolmente il numero e l'ambito delle metriche disponibili per il monitoraggio in Cloud Insights.

Giugno 2019

Edizioni Cloud Insights

Cloud Insights è disponibile in diverse edizioni per soddisfare le tue esigenze di budget e di business. Gli attuali clienti NetApp con un account di supporto NetApp attivo possono usufruire di 7 giorni di conservazione dei dati e di accesso ai data collezioner NetApp con la * Basic Edition* gratuita, oppure ottenere una maggiore

conservazione dei dati, l'accesso a tutti i data collezioner supportati, il supporto tecnico esperto e molto altro ancora con **Standard Edition**. Per ulteriori informazioni sulle funzionalità disponibili, consulta la sezione di NetApp "Cloud Insights" sito.

Nuovo Data Collector per l'infrastruttura: NetApp HCI

- "Centro virtuale NetApp HCI" È stato aggiunto come data collector dell'infrastruttura. Il data collector del centro virtuale HCI raccoglie le informazioni dell'host NetApp HCI e richiede privilegi di sola lettura per tutti gli oggetti all'interno del centro virtuale.

Nota: Il data collector HCI acquisisce solo dal centro virtuale HCI. Per raccogliere i dati dal sistema storage, è necessario configurare anche NetApp "SolidFire" data collector.

Maggio 2019

Nuovo Service Data Collector: Kapacitor

- "Kapacitor" è stato aggiunto come data collector per i servizi.

Integrazione con i servizi via Telegraf

Oltre all'acquisizione di dati da dispositivi infrastrutturali come switch e storage, Cloud Insights ora raccoglie dati da una varietà di sistemi operativi e servizi, utilizzando "Telegraf come suo agente" per la raccolta di dati di integrazione. Telegraf è un agente basato su plug-in che può essere utilizzato per raccogliere e segnalare le metriche. I plug-in di input vengono utilizzati per raccogliere le informazioni desiderate nell'agente accedendo direttamente al sistema/sistema operativo, chiamando API di terze parti o ascoltando flussi configurati.

La documentazione per le integrazioni attualmente supportate è disponibile nel menu a sinistra sotto **riferimento e supporto**.

Risorse di macchine virtuali per lo storage

- Le macchine virtuali per lo storage (SVM) sono disponibili come risorse in Cloud Insights. Le SVM dispongono di una propria pagina di destinazione delle risorse e possono essere visualizzate e utilizzate in ricerche, query e filtri. Le SVM possono essere utilizzate anche nei widget della dashboard e associate alle annotazioni.

Requisiti di sistema dell'unità di acquisizione ridotti

- I requisiti di CPU e memoria del sistema per il software dell'unità di acquisizione (AU) sono stati ridotti. I nuovi requisiti sono:

Componente	Requisito precedente	Nuovo requisito
Core della CPU	4	2
Memoria	16 GB	8 GB

Piattaforme aggiuntive supportate

- Le seguenti piattaforme sono state aggiunte a quelle attualmente "Supportato per Cloud Insights":

Linux	Windows
CentOS 7.3 64-bit CentOS 7.4 64-bit CentOS 7.6 64-bit Debian 9 64-bit Red Hat Enterprise Linux 7.3 64-bit Red Hat Enterprise Linux 7.4 64-bit Red Hat Enterprise Linux 7.6 64-bit Ubuntu Server 18.04 LTS	Microsoft Windows 10 64-bit Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019

Aprile 2019

Filtra macchine virtuali per tag

Quando si configurano i seguenti data collection, è possibile filtrare per includere o escludere macchine virtuali dalla raccolta dati in base ai tag o alle etichette.

- "Amazon EC2"
- "Azure"
- "Piattaforma Google Cloud"

Marzo 2019

Notifiche e-mail per eventi correlati all'abbonamento

- È possibile selezionare i destinatari per l'e-mail "notifiche" quando si verificano eventi correlati all'abbonamento, come la prossima scadenza della prova o le modifiche dell'account sottoscritto. È possibile scegliere tra i seguenti destinatari per queste notifiche:
  - Tutti i proprietari di account
  - Tutti gli amministratori
  - Indirizzi e-mail aggiuntivi specificati dall'utente

Dashboard aggiuntivi

- Il seguente nuovo AWS-Focused "dashboard" sono stati aggiunti alla galleria e sono disponibili per l'importazione:
  - AWS Admin - quali EC2 sono in forte richiesta?
  - Performance istanza AWS EC2 per regione

Febbraio 2019

Raccolta da account secondari AWS

- Supporto di Cloud Insights "Raccolta dagli account secondari AWS" in un singolo data collector. L'ambiente AWS deve essere configurato in modo da consentire a Cloud Insights di eseguire la raccolta dagli account

secondari.

Nome del Data Collector

- I nomi dei Data Collector possono ora includere punti (.), trattini (-) e spazi ( ) oltre a lettere, numeri e caratteri di sottolineatura. I nomi non possono iniziare o terminare con uno spazio, un punto o un trattino.

Unità di acquisizione per Windows

- È possibile configurare un'unità di acquisizione Cloud Insights su un server/macchina virtuale Windows. Esaminare le finestre "prerequisiti" prima di installare "Software dell'unità di acquisizione".

Gennaio 2019

Il campo "Owner" è più leggibile

- Negli elenchi Dashboard e Query, i dati per il campo "Owner" (Proprietario) erano in precedenza una stringa di ID autorizzazione, invece di un nome utente intuitivo. Il campo "Owner" (Proprietario) ora mostra un nome proprietario più semplice e leggibile.

Analisi delle unità gestite sulla pagina di abbonamento

- Per ciascun data collector elencato nella pagina **Admin > Subscription**, è ora possibile visualizzare un'analisi dei conteggi delle unità gestite (MU) per host e storage, oltre al totale.

Dicembre 2018

Miglioramento del tempo di caricamento dell'interfaccia utente

- Il tempo di caricamento iniziale per l'interfaccia utente (UI) di Cloud Insights è stato notevolmente migliorato. Il tempo di refresh per l'interfaccia utente beneficia anche di questo miglioramento nelle circostanze in cui vengono caricati i metadati.

Raccolta di dati di modifica in blocco

- È possibile modificare le informazioni per più data collezionisti contemporaneamente. Nella pagina **osservabilità > Collector**, selezionare i data collector da modificare selezionando la casella a sinistra di ciascuno di essi e fare clic sul pulsante **azioni in blocco**. Scegliere **Modifica** e modificare i campi necessari.

  I data raccoglitori selezionati devono essere dello stesso fornitore e modello e risiedere nella stessa unità di acquisizione.

Le pagine di supporto e abbonamento sono disponibili durante l'inserimento

- Durante il flusso di lavoro di assunzione, è possibile accedere alle pagine **Help > Support** (Guida > supporto) e **Admin > Subscription** (Amministratore > abbonamento). Tornando da queste pagine si torna

al workflow di assunzione, a condizione che non sia stata chiusa la scheda del browser.

Novembre 2018

Iscriviti tramite NetApp Sales o AWS Marketplace

- L'abbonamento e la fatturazione a Cloud Insights sono ora disponibili direttamente tramite NetApp. Questo si aggiunge all'abbonamento self-service disponibile tramite AWS Marketplace. Nella pagina **Admin > Subscription** viene visualizzato un nuovo collegamento **Contact Sales**. Per i clienti i cui ambienti prevedono o prevedono di disporre di 1,000 o più unità gestite (MU), si consiglia di contattare NetApp Sales tramite il link Contact Sales.

Collegamenti ipertestuali per le annotazioni di testo

- Le annotazioni di tipo testo possono ora includere collegamenti ipertestuali.

Presentazione dell'assunzione

- Cloud Insights offre ora una procedura dettagliata per il primo utente (amministratore o proprietario dell'account) a effettuare l'accesso a un nuovo ambiente. La procedura dettagliata consente di installare un'unità di acquisizione, configurare un data collector iniziale e selezionare una o più dashboard utili.

Importa dashboard dalla Gallery

- Oltre a selezionare le dashboard durante l'inserimento, puoi importare le dashboard tramite **Dashboard > Show All Dashboard** e facendo clic su **+da Gallery**.

Duplicazione di dashboard

- La possibilità di duplicare una dashboard è stata aggiunta alla pagina dell'elenco della dashboard come scelta nel menu delle opzioni per ogni dashboard e nella pagina principale di una dashboard stessa dal menu *Save*.

Menu dei prodotti Cloud Central

- Il menu che consente di passare ad altri prodotti NetApp Cloud Central è stato spostato nell'angolo superiore destro dello schermo.

Assunzione di Cloud Insights

Prima di iniziare a lavorare con Cloud Insights, è necessario registrarsi sul portale **NetApp BlueXP**. Se hai già un accesso BlueXP, puoi avviare una prova gratuita di Cloud Insights con pochi e rapidi passaggi.

Creazione dell'account NetApp BlueXP

Per iniziare a utilizzare i servizi cloud di NetApp, visitare il sito Web all'indirizzo **"NetApp BlueXP"** E fare clic su **inizia**.

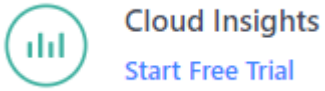
- Se non hai ancora effettuato la registrazione, seleziona **Registrati**
- Immettere un indirizzo e-mail aziendale valido e scegliere una password.
- Immettere il nome della società e il nome completo.
- Accettare i termini e le condizioni e selezionare **continua**.
- BlueXP ti guiderà nella guida introduttiva.

Cosa succede se dispongo già di un accesso a NetApp BlueXP?

Una volta ottenuto un account NetApp BlueXP, è sufficiente selezionare **Accedi** sul **"NetApp BlueXPI"** pagina del portale.

Inserire l'indirizzo e-mail e la password. Verrà visualizzata la pagina delle offerte cloud di NetApp.

Selezionare Cloud Insights.



Avvio della versione di prova gratuita di Cloud Insights

Se è la prima volta che accedi a Cloud Insights, sotto l'offerta Cloud Insights, fai clic su **Avvia prova gratuita**. Cloud Insights ti guiderà nella creazione dell'ambiente della tua azienda.

Una volta completata la creazione del tuo ambiente, puoi utilizzare le tue credenziali BlueXP per accedere e iniziare la prova gratuita di 30 giorni di Cloud Insights. Durante questa versione di prova potrai esplorare le funzionalità offerte da Cloud Insights.

Durante la prova gratuita, è possibile "avvia l'abbonamento" A Cloud Insights in qualsiasi momento. Una volta effettuato l'abbonamento, è possibile utilizzare le funzioni di Cloud Insights in base all'abbonamento in uso.

Accedi e vai

Una volta creato l'ambiente, sarà possibile accedere in qualsiasi momento al portale NetApp BlueXP e fare clic su **Vai a Cloud Insights**. Sarete portati direttamente al vostro ambiente Cloud Insights.

È anche possibile aprire un browser direttamente sull'URL dell'ambiente Cloud Insights, ad esempio:

```
 https://<environment-prefix>.c01.cloudinsights.netapp.com/
L'URL verrà inoltre incluso nell'e-mail di invito di ciascun utente per un
accesso semplice e per la creazione di segnalibri. Se l'utente non ha già
effettuato l'accesso a BlueXP, verrà richiesto di effettuare l'accesso.
```

> I nuovi utenti devono comunque registrarsi per l'accesso a BlueXP prima che possano accedere all'URL del loro ambiente.

La prima volta che si accede a un nuovo ambiente, viene guidata la configurazione di **"iniziare a raccogliere i dati"**.

Disconnessione

Per disconnettersi da Cloud Insights, fare clic su **Nome utente** e selezionare **Disconnetti**. Verrai riportato al "Accedi a BlueXP" schermo.

> La disconnessione da Cloud Insights consente di uscire da BlueXP. Inoltre, verrai disconnesso dagli altri servizi cloud di NetApp che utilizzano l'accesso BlueXP.

Timeout di inattività

Per impostazione predefinita, BlueXP effettua il log out di un utente in assenza di attività per sei ore (360 minuti). Indipendentemente dall'attività, gli utenti verranno disconnessi dopo sette giorni.

Sicurezza

Sicurezza Cloud Insights

La sicurezza dei dati di prodotti e clienti è di estrema importanza per NetApp. Cloud Insights segue le Best practice di sicurezza durante l'intero ciclo di vita del rilascio per garantire che le informazioni e i dati dei clienti siano protetti nel modo migliore possibile.

Panoramica sulla sicurezza

Sicurezza fisica

L'infrastruttura di produzione Cloud Insights è ospitata in Amazon Web Services (AWS). I controlli fisici e ambientali relativi alla sicurezza per i server di produzione Cloud Insights, che includono edifici e serrature o chiavi utilizzate sulle porte, sono gestiti da AWS. Come da AWS: "L'accesso fisico è controllato sia sul perimetro che nei punti di ingresso dell'edificio da personale di sicurezza professionale che utilizza videosorveglianza, sistemi di rilevamento delle intrusioni e altri mezzi elettronici. Il personale autorizzato utilizza meccanismi di autenticazione a più fattori per accedere ai data center".

Cloud Insights segue le Best practice di "Modello di responsabilità condivisa" Descritto da AWS.

Sicurezza del prodotto

Cloud Insights segue un ciclo di vita dello sviluppo in linea con i principi Agile, consentendoci così di affrontare più rapidamente qualsiasi difetto software orientato alla sicurezza, rispetto alle metodologie di sviluppo del ciclo di rilascio più lungo. Grazie a metodologie di integrazione continua, siamo in grado di rispondere rapidamente alle modifiche funzionali e di sicurezza. Le procedure e le policy di gestione delle modifiche definiscono quando e come si verificano le modifiche e contribuiscono a mantenere la stabilità dell'ambiente di produzione. Qualsiasi modifica di impatto viene formalmente comunicata, coordinata, correttamente esaminata e approvata prima del rilascio nell'ambiente di produzione.

Sicurezza di rete

L'accesso di rete alle risorse nell'ambiente Cloud Insights è controllato da firewall basati su host. Ogni risorsa (ad esempio un'istanza di bilanciamento del carico o di macchina virtuale) dispone di un firewall basato su host che limita il traffico in entrata solo alle porte necessarie per eseguire la funzione di tale risorsa.

Cloud Insights utilizza diversi meccanismi, tra cui i servizi di rilevamento delle intrusioni, per monitorare l'ambiente di produzione per rilevare eventuali anomalie di sicurezza.

Valutazione dei rischi

Il team Cloud Insights segue un processo formalizzato di valutazione dei rischi per fornire un metodo sistematico e ripetibile per identificare e valutare i rischi in modo che possano essere gestiti in modo appropriato attraverso un piano di trattamento dei rischi.

Protezione dei dati

L'ambiente di produzione Cloud Insights è configurato in un'infrastruttura altamente ridondante che utilizza più zone di disponibilità per tutti i servizi e i componenti. Oltre all'utilizzo di un'infrastruttura di calcolo ridondante e altamente disponibile, viene eseguito il backup dei dati critici a intervalli regolari e i ripristini vengono periodicamente testati. Le policy e le procedure di backup formali riducono al minimo l'impatto delle interruzioni

delle attività di business e proteggono i processi di business dagli effetti dei guasti dei sistemi informativi o dei disastri e ne garantiscono una ripresa tempestiva e adeguata.

Autenticazione e gestione degli accessi

Tutto l'accesso del cliente a Cloud Insights avviene tramite interazioni dell'interfaccia utente del browser su https. L'autenticazione viene eseguita tramite il servizio di terze parti Auth0. NetApp si è centralizzata su questo come livello di autenticazione per tutti i servizi dati cloud.

Cloud Insights segue le Best practice del settore, tra cui "privilegio minimo" e "controllo degli accessi basato sui ruoli", in merito all'accesso logico all'ambiente di produzione Cloud Insights. L'accesso è controllato in base a esigenze rigorose e viene concesso solo a personale autorizzato selezionato che utilizza meccanismi di autenticazione a più fattori.

Raccolta e protezione dei dati dei clienti

Tutti i dati dei clienti vengono crittografati in transito attraverso reti pubbliche e a riposo. Cloud Insights utilizza la crittografia in vari punti del sistema per proteggere i dati dei clienti utilizzando tecnologie che includono TLS (Transport Layer Security) e l'algoritmo AES-256 standard di settore.

Deprovisioning del cliente

Le notifiche e-mail vengono inviate a vari intervalli per informare il cliente che l'abbonamento sta per scadere. Una volta scaduto l'abbonamento, l'interfaccia utente viene limitata e inizia un periodo di tolleranza per la raccolta dei dati. Il cliente viene quindi avvisato tramite e-mail. Gli abbonamenti in prova hanno un periodo di tolleranza di 14 giorni e gli account di abbonamento a pagamento hanno un periodo di tolleranza di 28 giorni. Una volta scaduto il periodo di tolleranza, il cliente riceve una notifica via e-mail che l'account verrà cancellato tra 2 giorni. Un cliente a pagamento può anche richiedere direttamente di non usufruire del servizio.

I tenant scaduti e tutti i dati dei clienti associati vengono cancellati dal team delle operazioni Cloud Insights (SRE) al termine del periodo di tolleranza o alla conferma della richiesta di chiusura del conto da parte di un cliente. In entrambi i casi, il team SRE esegue una chiamata API per eliminare l'account. La chiamata API elimina l'istanza del tenant e tutti i dati del cliente. L'eliminazione del cliente viene verificata chiamando la stessa API e verificando che lo stato del tenant del cliente sia "CANCELLATO".

Gestione degli incidenti di sicurezza

Cloud Insights è integrato con il processo del team di risposta agli incidenti per la sicurezza dei prodotti (PSIRT) di NetApp per individuare, valutare e risolvere le vulnerabilità note. PSIRT prende informazioni sulle vulnerabilità da più canali, tra cui report sui clienti, engineering interno e fonti ampiamente riconosciute come il database CVE.

Se il team tecnico di Cloud Insights rileva un problema, il team avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

È inoltre possibile che un cliente o un ricercatore Cloud Insights identifichi un problema di sicurezza con il prodotto Cloud Insights e lo riferisca al supporto tecnico o direttamente al team di risposta agli incidenti di NetApp. In questi casi, il team Cloud Insights avvierà il processo PSIRT, valuterà e potenzialmente risolverà il problema.

Test di vulnerabilità e penetrazione

Cloud Insights segue le Best practice del settore ed esegue regolarmente test di vulnerabilità e penetrazione utilizzando aziende e professionisti della sicurezza interni ed esterni.

Training sulla consapevolezza della sicurezza

Tutto il personale di Cloud Insights viene sottoposto a un training sulla sicurezza, sviluppato per ruoli individuali, per garantire che ciascun dipendente sia in grado di gestire le sfide specifiche legate alla sicurezza dei propri ruoli.

Conformità

Cloud Insights esegue audit e convalide indipendenti di terze parti da parte di una società CPA con licenza esterna in relazione alla sicurezza, ai processi e ai servizi, incluso il completamento dell'audit SOC 2.

Avvisi di sicurezza NetApp

Puoi visualizzare gli avvisi sulla sicurezza disponibili di NetApp "qui".

Informazioni e Regione

NetApp prende molto sul serio la sicurezza delle informazioni dei clienti. Ecco come e dove Cloud Insights memorizza le tue informazioni.

Quali informazioni memorizza Cloud Insights?

Cloud Insights memorizza le seguenti informazioni:

- Dati sulle performance

  I dati sulle performance sono dati Time-Series che forniscono informazioni sulle performance del dispositivo/origine monitorato. Ad esempio, il numero di iOS forniti da un sistema di storage, il throughput di una porta FibreChannel, il numero di pagine inviate da un server Web, il tempo di risposta di un database e molto altro ancora.

- Dati di inventario

  I dati di inventario sono costituiti da metadati che descrivono il dispositivo/origine monitorato e il modo in cui sono configurati. Ad esempio, le versioni hardware e software installate, i dischi e le LUN in un sistema di storage, i core della CPU, la RAM e i dischi di una macchina virtuale, gli spazi delle tabelle di un database, il numero e il tipo di porte su uno switch SAN, i nomi di directory/file (se la protezione del carico di lavoro dello storage è attivata) e così via

- Dati di configurazione

  In questo modo vengono riepilogati i dati di configurazione forniti dal cliente utilizzati per gestire l'inventario e le operazioni del cliente, ad esempio nomi host o indirizzi IP dei dispositivi monitorati, intervalli di polling, valori di timeout, ecc.

- Segreti

  I segreti sono costituiti dalle credenziali utilizzate dall'unità di acquisizione Cloud Insights per accedere ai dispositivi e ai servizi del cliente. Queste credenziali vengono crittografate utilizzando una crittografia asimmetrica avanzata e le chiavi private vengono memorizzate solo sulle unità di acquisizione e non escono mai dall'ambiente del cliente. Anche gli SRE Cloud Insights con privilegi non sono in grado di accedere ai segreti dei clienti in formato testo semplice a causa di questo design.

- Dati funzionali

Si tratta di dati generati in seguito alla fornitura da parte di NetApp del Cloud Data Service, che informa NetApp sullo sviluppo, l'implementazione, le operazioni, la manutenzione e la protezione del Cloud Data Service. I dati funzionali non contengono informazioni sul cliente o informazioni personali.

- Dati di accesso dell'utente

  Informazioni di autenticazione e accesso che consentono a NetApp Cloud Central di comunicare con i siti Cloud Insights regionali, inclusi i dati relativi all'autorizzazione dell'utente.

- Storage workload Security User Directory Data

  Nei casi in cui la funzionalità workload Security è attivata E il cliente sceglie di attivare User Directory Collector, il sistema memorizza i nomi degli utenti, gli indirizzi e-mail aziendali e altre informazioni raccolte da Active Directory.

> I dati della directory utente si riferiscono alle informazioni della directory utente raccolte dal data collector della directory utente di workload Security, non ai dati relativi agli utenti di Cloud Insights/workload Security stessi.

Nessun dato personale esplicito viene raccolto dalle risorse dell'infrastruttura e dei servizi. Le informazioni raccolte comprendono solo metriche delle performance, informazioni di configurazione e metadati dell'infrastruttura, come molti case telefoniche dei vendor, tra cui il supporto automatico di NetApp e ActiveIQ. Tuttavia, a seconda delle convenzioni di denominazione di un cliente, i dati per condivisioni, volumi, macchine virtuali, qtree, le applicazioni, ecc. possono contenere informazioni di identificazione personale.

Se la sicurezza del carico di lavoro è attivata, il sistema esamina inoltre i nomi di file e directory su SMB o altre condivisioni, che potrebbero contenere informazioni di identificazione personale. Quando i clienti abilitano il modulo di raccolta directory utente per la sicurezza del carico di lavoro (che essenzialmente associa i SID di Windows ai nomi utente tramite Active Directory), il nome visualizzato, l'indirizzo di posta elettronica aziendale e gli eventuali attributi aggiuntivi selezionati verranno raccolti e memorizzati da Cloud Insights.

Inoltre, i registri di accesso a Cloud Insights vengono mantenuti e contengono gli indirizzi IP e di posta elettronica degli utenti utilizzati per accedere al servizio.

Dove sono memorizzate le mie informazioni?

Cloud Insights memorizza le informazioni in base alla regione in cui viene creato l'ambiente.

Nella regione host vengono memorizzate le seguenti informazioni:

- Telemetria e informazioni su asset/oggetti, inclusi contatori e metriche delle performance
- Informazioni sull'unità di acquisizione
- Dati funzionali
- Informazioni di audit sulle attività degli utenti all'interno di Cloud Insights
- Sicurezza del carico di lavoro informazioni su Active Directory
- Informazioni sulla verifica della sicurezza del carico di lavoro

Le seguenti informazioni risiedono negli Stati Uniti, indipendentemente dalla regione in cui risiede l'ambiente Cloud Insights:

- Informazioni sul sito dell'ambiente (talvolta chiamate "tenant"), come il proprietario del sito o dell'account.

- Informazioni che consentono a NetApp Cloud Central di comunicare con i siti Cloud Insights regionali, incluso qualsiasi cosa relativa all'autorizzazione dell'utente.
- Informazioni relative alla relazione tra l'utente Cloud Insights e il tenant.

Regioni host

Le regioni host includono:

- USA: US-est-1
- EMEA: eu-Central-1
- APAC: ap-sud-est-2

Ulteriori informazioni

Per ulteriori informazioni sulla privacy e la sicurezza di NetApp, consultare i seguenti xref:./* "Trust Center"
* "Trasferimenti di dati transfrontalieri"
* "Regole aziendali vincolanti"
* "Risposta a richieste di dati di terze parti"
* "Principi di privacy di NetApp"

Strumento securityadmin

Cloud Insights include funzionalità di sicurezza che consentono al tuo ambiente di operare con una maggiore sicurezza. Le funzionalità includono miglioramenti alla crittografia, all'hashing delle password e alla possibilità di modificare le password utente interne, nonché coppie di chiavi che crittografano e decrittare le password.

Per proteggere i dati sensibili, NetApp consiglia di modificare le chiavi predefinite e la password utente *Acquisition* dopo un'installazione o un aggiornamento.

Le password crittografate dell'origine dati vengono memorizzate in Cloud Insights, che utilizza una chiave pubblica per crittografare le password quando un utente le inserisce in una pagina di configurazione del data collector. Cloud Insights non dispone delle chiavi private necessarie per decrittare le password del data collector; solo le unità di acquisizione (aus) dispongono della chiave privata del data collector necessaria per decrittare le password del data collector.

Considerazioni sull'aggiornamento e l'installazione

Se il sistema Insight contiene configurazioni di sicurezza non predefinite (ad esempio, password ridigettate), 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 della sicurezza sull'unità di acquisizione

Lo strumento securityadmin consente di gestire le opzioni di sicurezza per Cloud Insights e viene eseguito sul sistema dell'unità di acquisizione. 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

- Per installare il software dell'unità di acquisizione (che include lo strumento securityadmin), è necessario disporre dei privilegi di amministratore sul sistema AU.
- Se in seguito si dispone di utenti non amministratori che dovranno accedere allo strumento securityadmin, questi devono essere aggiunti al gruppo *cisys*. Il gruppo *cisys* viene creato durante l'installazione dell'AU.

Dopo l'installazione di AU, lo strumento securityadmin si trova nel sistema dell'unità di acquisizione in una delle seguenti posizioni:

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

Utilizzando lo strumento securityadmin

Avviare lo strumento securityadmin in modalità interattiva (-i).

> Si consiglia di utilizzare lo strumento securityadmin in modalità interattiva, per evitare di trasmettere segreti sulla riga di comando, che possono essere acquisiti nei registri.

Vengono visualizzate le seguenti opzioni:

```
[root@ci-qa-xitij-cis2-28594linau bin]# ./securityadmin -i
Select Action:

1 - Backup

2 - Restore

3 - Register / Update External Key Retrieval Script

4 - Rotate Encryption Keys

5 - Reset to Default Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Collector Password

9 - Exit

Enter your choice:
```

1. **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:

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

Si consiglia di mantenere al sicuro i backup del vault, poiché includono informazioni riservate.

2. **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 utilizzando i seguenti passaggi: 1) modificare le chiavi di crittografia sull'AU. 2) creare un backup del vault. 3) ripristinare il backup del vault in ciascuna delle aus.

3. **Registra / Aggiorna script di recupero chiave esterna**

   Utilizzare uno script esterno per registrare o 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.

   Nota questa opzione è disponibile solo su Linux.

   Quando si utilizza il proprio script di recupero delle chiavi con lo strumento securityadmin, tenere presente quanto segue:

   - L'algoritmo attualmente supportato è RSA con un minimo di 2048 bit.
   - Lo script deve restituire le chiavi private e pubbliche in testo normale. Lo script non deve restituire chiavi private e pubbliche crittografate.
   - Lo script deve restituire contenuti codificati raw (solo formato PEM).
   - Lo script esterno deve disporre delle autorizzazioni *execute*.

4. **Ruota chiavi di crittografia**

   Ruotare le chiavi di crittografia (Annulla la registrazione delle chiavi correnti e registra le nuove chiavi). Per utilizzare una chiave di un sistema di gestione delle chiavi esterno, è necessario specificare l'id della chiave pubblica e l'ID della chiave privata.

5. **Ripristina chiavi 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.

6. **Modifica password Truststore**

   Modificare la password del truststore.

7. **Modifica password keystore**

   Modificare la password del keystore.

8. **Encrypt Collector Password**

   Crittografare la password del data collector.

9. **Esci**

   Uscire dallo strumento securityadmin.

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

Specificare un utente per eseguire lo strumento

Se ci si trova in un ambiente controllato e consapevole della sicurezza, è possibile che non si disponga del gruppo *cisys*, ma che si desideri comunque che utenti specifici eseguano lo strumento securityadmin.

Per ottenere questo risultato, installare manualmente il software AU e specificare l'utente/gruppo a cui si desidera accedere.

- Utilizzando l'API, scaricare il programma di installazione ci nel sistema AU e decomprimerlo.
  - È necessario un token di autorizzazione una tantum. Consultare la documentazione API Swagger (*Admin > API Access* e selezionare il link *API Documentation*) e individuare la sezione *GET /au/oneTimeToken* API.
  - Una volta ottenuto il token, utilizzare l'API *GET /au/installers/{platform}/{version}* per scaricare il file di installazione. È necessario fornire la versione della piattaforma (Linux o Windows) e dell'installatore.
- Copiare il file di installazione scaricato nel sistema AU e decomprimerlo.
- Accedere alla cartella contenente i file ed eseguire il programma di installazione come root, specificando l'utente e il gruppo:

```
./cloudinsights-install.sh <User> <Group>
```

Se l'utente e/o il gruppo specificati non esistono, verranno creati. L'utente avrà accesso allo strumento securityadmin.

Aggiornamento o rimozione del proxy

Lo strumento securityadmin può essere utilizzato per impostare o rimuovere le informazioni proxy per l'unità di acquisizione eseguendo lo strumento con il parametro *-pr*:

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>

The purpose of this tool is to enable reconfiguration of security aspects
of the Acquisition Unit such as encryption keys, and proxy configuration,
etc. For more information about this tool, please check the Cloud Insights
Documentation.

-ap,--add-proxy <arg>       add a proxy server.  Arguments: ip=ip
                             port=port user=user password=password
                             domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
-h,--help
-rp,--remove-proxy          remove proxy server
-upr,--update-proxy <arg>   update a proxy.  Arguments: ip=ip port=port
                             user=user password=password domain=domain
                             (Note: Always use double quote(") or single
                             quote(') around user and password to escape
                             any special characters, e.g., <, >, ~, `, ^,
                             !
                             For example: user="test" password="t'!<@1"
                             Note: domain is required if the proxy auth
                             scheme is NTLM.)
```

Ad esempio, per rimuovere il proxy, eseguire il seguente comando:

```
 [root@ci-eng-linau bin]# ./securityadmin -pr -rp
Dopo aver eseguito il comando, riavviare l'unità di acquisizione.
```

Per aggiornare un proxy, il comando è

```
./securityadmin -pr -upr <arg>
```

Recupero della chiave esterna

Se si fornisce uno script di shell UNIX, può essere eseguito dall'unità di acquisizione per recuperare la **chiave privata** e la **chiave pubblica** dal sistema di gestione delle chiavi.

Per recuperare la chiave, Cloud Insights eseguirà lo script, passando due parametri: *Key id* e *key type*. *Key id* può essere utilizzato per identificare la chiave nel sistema di gestione delle chiavi. *Key type* è "public" o "private". Quando il tipo di chiave è "public", lo script deve restituire la chiave pubblica. Quando il tipo di chiave è "privata", la chiave privata deve essere restituita.

Per inviare nuovamente il tasto all'unità di acquisizione, lo script deve stampare il tasto sull'output standard. Lo script deve stampare *solo* la chiave per l'output standard; nessun altro testo deve essere stampato su output standard. Una volta che la chiave richiesta viene stampata nell'output standard, lo script deve uscire con un codice di uscita di 0; qualsiasi altro codice di ritorno viene considerato un errore.

Lo script deve essere registrato con l'unità di acquisizione utilizzando lo strumento securityadmin, che eseguirà lo script insieme all'unità di acquisizione. Lo script deve avere l'autorizzazione *Read* e *execute* per l'utente root e "cisys". Se lo script della shell viene modificato dopo la registrazione, lo script della shell modificato deve essere nuovamente registrato con l'unità di acquisizione.

parametro di input: id chiave	Identificatore chiave utilizzato per identificare la chiave nel sistema di gestione delle chiavi del cliente.
parametro di immissione: tipo di chiave	pubblico o privato.
uscita	La chiave richiesta deve essere stampata sull'output standard. La chiave RSA a 2048 bit è attualmente supportata. Le chiavi devono essere codificate e stampate nel seguente formato: Formato chiave privata - PEM, DER-encoded PKCS8 PrivateKeyInfo RFC 5958 Formato chiave pubblica - PEM, DER-encoded X,509 SubjectPublicKeyInfo RFC 5280
codice di uscita	Codice di uscita zero per successo. Tutti gli altri valori di uscita sono considerati falliti.
autorizzazioni script	Lo script deve disporre dell'autorizzazione di lettura ed esecuzione per l'utente root e "cisys".
registri	Vengono registrate le esecuzioni degli script. I registri si trovano in - /var/log/netapp/cloudinsights/securityadmin/securityadmin.log /var/log/netapp/cloudinsigies/acq/acq.log

Crittografia di una password per l'utilizzo in API

L'opzione 8 consente di crittografare una password, che è quindi possibile passare a un agente di raccolta dati tramite API.

Avviare lo strumento securityadmin in modalità interattiva e selezionare l'opzione 8: *Encrypt Password*.

```
 securityadmin.sh -i
Viene richiesto di immettere la password che si desidera crittografare. I
caratteri digitati non vengono visualizzati sullo schermo.  Inserire
nuovamente la password quando richiesto.
```

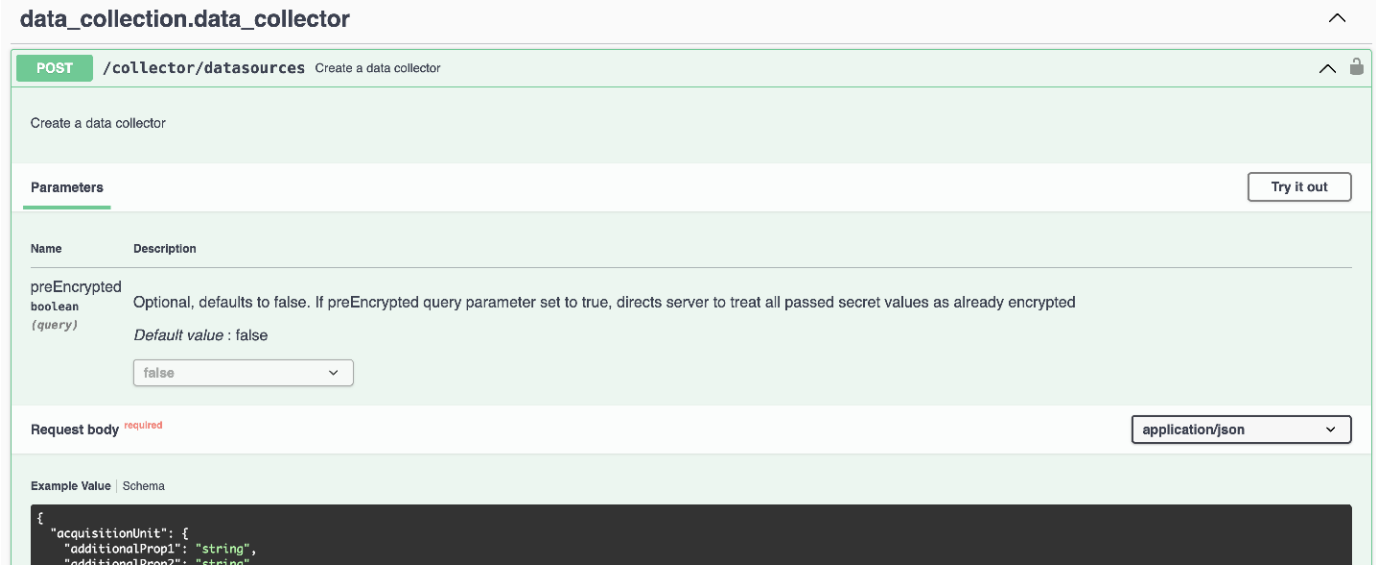
In alternativa, se si utilizza il comando in uno script, sulla riga di comando utilizzare *securityadmin.sh* con il parametro "-enc", passando la password non crittografata:

```
 securityadmin -enc mypassword
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["Esempio CLI"]
```

La password crittografata viene visualizzata sullo schermo. Copiare l'intera stringa, inclusi i simboli iniziali o finali.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i
Select Action:

1 - Backup

2 - Restore

3 - Change Encryption Keys

4 - Reset to Default Keys

5 - Check for Default Encryption Keys

6 - Change Truststore Password

7 - Change Keystore Password

8 - Encrypt Password

9 - Exit

Enter your choice: 8
Please enter your password to encrypt:
Please confirm your password to encrypt:

Your Encrypted Password below

ciYJAMpdEncBsLQwF2gobbiERl4Jrwb7tLWOfYhu0dERGZZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2klBd8gqJiQ+tS/lZkmJ6XKgTDcf3LGn8UqzQy
RnOv5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpjuOG5UmeZzlKGCT0aBTggri/JIYyyr4w2ZLnGOw21
LGm59vor7OGUOiKZYabLd+7LpsdCCBi1eF86BCj2RkxXOof891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

Per inviare la password crittografata a un data collector, è possibile utilizzare l'API di raccolta dati. Lo swagger per questa API si trova in **Admin > API Access** e fare clic sul collegamento "API Documentation". Selezionare il tipo di API "raccolta dati". Sotto l'intestazione *data_collection.data_collector*, scegliere l'API */collector/datasources* POST per questo esempio.



Se si imposta l'opzione *preEncrypted* su *True*, qualsiasi password passata attraverso il comando API verrà considerata come **già crittografata**; l'API non crittograferà nuovamente le password. Quando si crea l'API, è sufficiente incollare la password precedentemente crittografata nella posizione appropriata.

https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true


```
{
"name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
"J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnlBVsAWyLmORxFAw
vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHfTvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
+nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlmM9QAyPoyw/JT0nXHDuf683uE
K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

Per iniziare

Tutorial sulle funzioni

Cloud Insights è dotato di utili funzionalità che consentono di trovare rapidamente e facilmente i dati, risolvere i problemi e fornire informazioni dettagliate sull'ambiente aziendale. Trova facilmente i dati con potenti query, visualizza i dati in dashboard e invia avvisi e-mail per le soglie dei dati impostate.

Cloud Insights include una serie di tutorial video per aiutarti a comprendere queste funzionalità e implementare meglio le tue strategie di business Insight. Tutti gli utenti che hanno accesso al tuo ambiente Cloud Insights possono trarre vantaggio da queste esercitazioni.

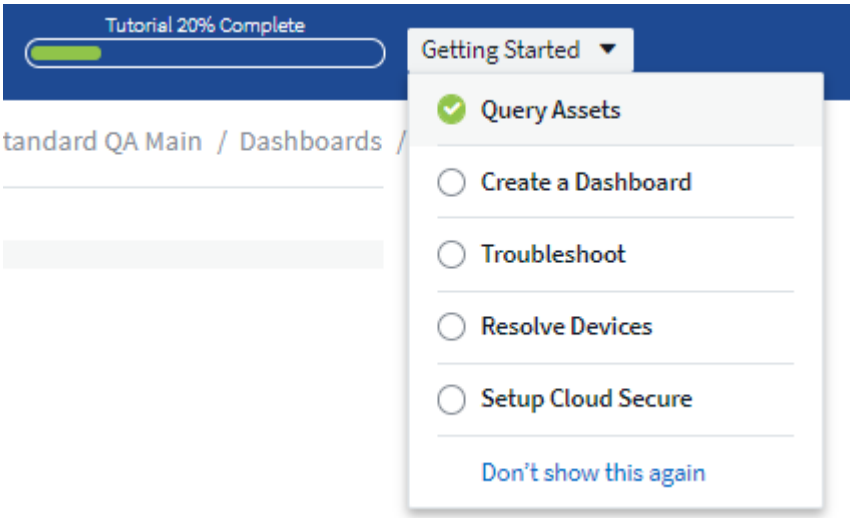
Introduzione

Guarda un breve tutorial che spiega come funziona Cloud Insights.

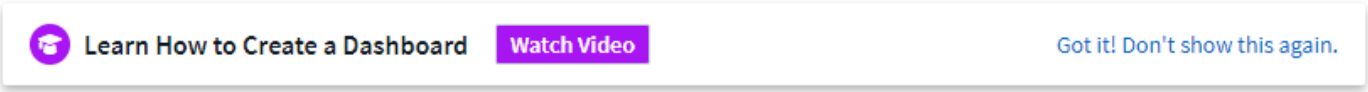
► https://docs.netapp.com/it-it/cloudinsights//media/howTo.mp4 *(video)*

Checklist e video tutorial

La **Lista di controllo per l'avvio** visualizzata sul sito Cloud Insights contiene un elenco di diversi concetti e attività utili. Selezionando un elemento nell'elenco di controllo si accede alla pagina Cloud Insights appropriata per quel concetto. Ad esempio, facendo clic sulla voce *Crea dashboard* viene aperta la pagina Cloud Insights **Dashboard**.



Nella parte superiore della pagina è presente un link a un tutorial video che mostra come creare una dashboard. È possibile visualizzare il video tutte le volte che si desidera fino a quando non si fa clic sul pulsante _got it! Non mostrare più questo link per quel video. Il video è disponibile ogni volta che si accede alla pagina Dashboards, fino a quando non viene visualizzato.



Dopo aver guardato il video almeno una volta, la voce *Create a Dashboard* nella lista di controllo è selezionata, a indicare che il tutorial è stato completato. Quindi passare al tutorial successivo.

> È possibile visualizzare i tutorial in qualsiasi ordine, tutte le volte che si desidera, fino a quando non vengono scartati.

Disperdere l'elenco di controllo

L'elenco di controllo per l'avvio viene visualizzato sul sito fino a quando non si fa clic sul collegamento *Do't Show Again* (non mostrare più questo) nella parte inferiore dell'elenco di controllo. Anche dopo aver disattivato l'elenco di controllo, i tutorial sono ancora disponibili su ogni pagina Cloud Insights appropriata fino a quando non si chiude ogni pagina dalla barra di intestazione del messaggio.

Visualizzare i tutorial

Esecuzione di query sui dati

► https://docs.netapp.com/it-it/cloudinsights//media/Queries.mp4 *(video)*

Creazione di una dashboard

► https://docs.netapp.com/it-it/cloudinsights//media/Dashboards.mp4 *(video)*

Risoluzione dei problemi

► https://docs.netapp.com/it-it/cloudinsights//media/Troubleshooting.mp4 *(video)*

Risolvere i dispositivi

► https://docs.netapp.com/it-it/cloudinsights//media/AHR_small.mp4 *(video)*

Raccolta dei dati

Per iniziare a raccogliere i dati

Dopo aver effettuato la registrazione a Cloud Insights e aver effettuato l'accesso all'ambiente per la prima volta, verrà illustrata la procedura seguente per iniziare a raccogliere e gestire i dati.

I raccoglitori di dati rilevano le informazioni provenienti dalle origini dati, ad esempio dispositivi di storage, switch di rete e macchine virtuali. Le informazioni raccolte vengono utilizzate per l'analisi, la convalida, il monitoraggio e la risoluzione dei problemi.

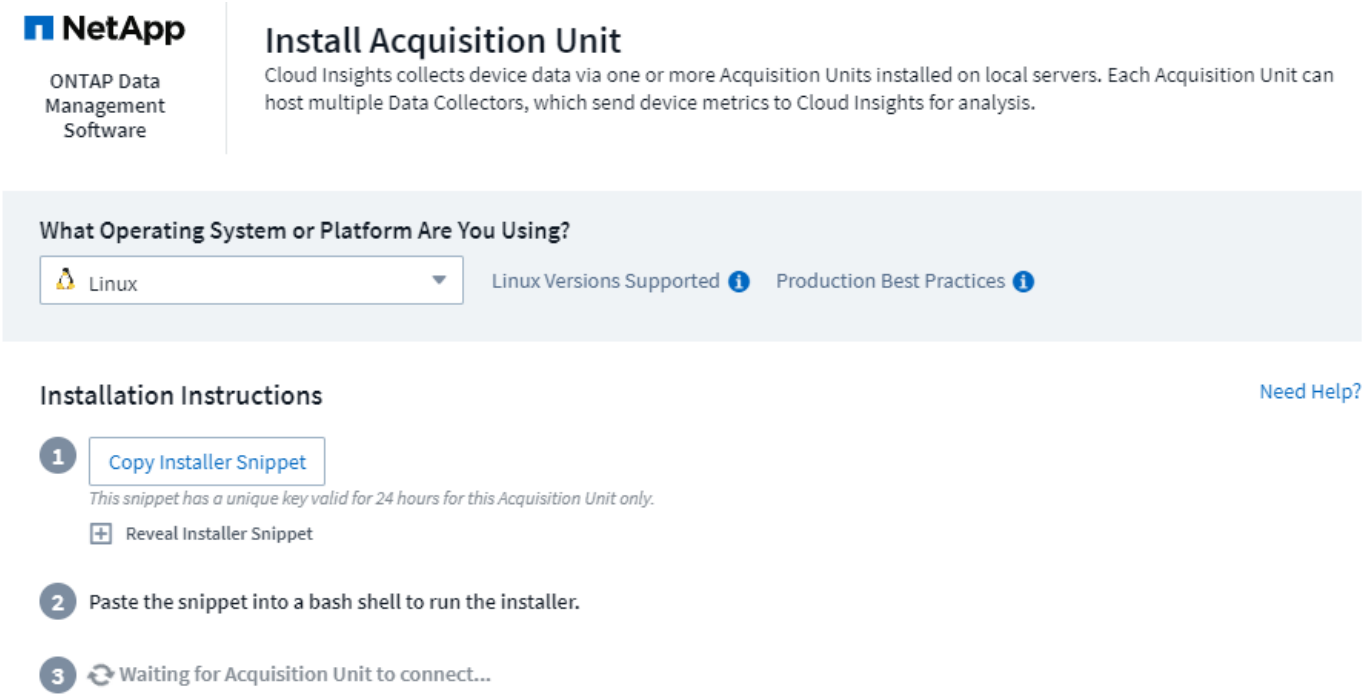
Cloud Insights ha a disposizione tre tipi di raccolta dati:

- Infrastruttura (dispositivi storage, switch di rete, infrastruttura di calcolo)
- Sistemi operativi (ad esempio VMware o Windows)
- Servizi (come Kafka)

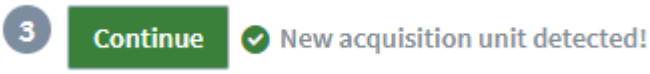
Seleziona il tuo primo data collector tra i vendor e i modelli supportati disponibili. È possibile aggiungere facilmente altri data collezioner in un secondo momento.

Installare un'unità di acquisizione

Se è stato selezionato un data collector *infrastruttura*, è necessaria un'unità di acquisizione per inserire i dati in Cloud Insights. È necessario scaricare e installare il software dell'unità di acquisizione su un server o una macchina virtuale nel data center da cui si desidera effettuare la raccolta. È possibile utilizzare una singola unità di acquisizione per più data colleziones.



- Seguire la "istruzioni" Visualizzato per installare l'unità di acquisizione. Una volta installato il software dell'unità di acquisizione, viene visualizzato il pulsante continua ed è possibile passare alla fase successiva.



Se necessario, è possibile configurare ulteriori unità di acquisizione in un secondo momento. Ad esempio, potrebbero essere necessarie diverse unità di acquisizione che raccolgono informazioni dai data center di diverse regioni.

Configurare l'infrastruttura Data Collector

Per i data collector di *infrastruttura*, ti verrà richiesto di compilare i campi di data collector presentati:

- Assegnare al data collector un nome univoco e significativo.
- Immettere le credenziali (nome utente e password) per connettersi alla periferica, a seconda dei casi.
- Compilare tutti gli altri campi obbligatori nelle sezioni *Configurazione* e *Configurazione avanzata*.
- Fare clic su **Add Collector** per salvare il data collector.

Sarà possibile configurare altri data collezioner in un secondo momento.

Configurare Data Collector - sistemi operativi e servizi

Sistema operativo:

Per i data raccoglitori di sistemi operativi, scegliere una piattaforma (Linux, Windows) per installare un agente Cloud Insights. Per raccogliere i dati dai servizi, è necessario disporre di almeno un agente. L'agente raccoglie anche i dati dall'host stesso, per l'utilizzo in Cloud Insights. Questi dati sono classificati come dati "nodo" nei widget, ecc.

- Aprire un terminale o una finestra di comando sull'host dell'agente o sulla macchina virtuale e incollare il comando visualizzato per installare l'agente.
- Al termine dell'installazione, fare clic su **complete Setup** (completa installazione).

Servizi:

Per i data raccoglitori *Service*, fare clic su un riquadro per aprire la pagina delle istruzioni per il servizio.

- Scegliere una piattaforma e un Agent Access Key.
- Se non si dispone di un agente installato su tale piattaforma, seguire le istruzioni per installare l'agente.
- Fare clic su **Continue** (continua) per aprire la pagina delle istruzioni di data collector.
- Seguire le istruzioni per configurare il data collector.
- Una volta completata la configurazione, fare clic su **complete Setup** (completa installazione).

Aggiungere dashboard

A seconda del tipo di data collector iniziale selezionato per la configurazione (storage, switch, ecc.), verranno importati uno o più dashboard pertinenti. Ad esempio, se è stato configurato un data collector per lo storage, verrà importato un set di dashboard relativi allo storage e ne verrà impostata una come home page di Cloud Insights. È possibile modificare la home page dall'elenco **Dashboards > Show All Dashboards** (Dashboard > Mostra tutti i dashboard).

È possibile importare ulteriori dashboard in un secondo momento oppure "crea il tuo".

Questo è tutto ciò che c'è da fare

Una volta completato il processo di configurazione iniziale, l'ambiente inizierà a raccogliere i dati.

Se il processo di configurazione iniziale viene interrotto (ad esempio, se si chiude la finestra del browser), seguire la procedura manualmente:

- Scegliere un Data Collector
- Installare un agente o un'unità di acquisizione, se richiesto
- Configurare Data Collector

Definizioni utili

Le seguenti definizioni possono essere utili quando si parla di raccolta di dati Cloud Insights o di funzionalità:

- Ciclo di vita del raccoglitore: Un raccoglitore appartiene a uno dei seguenti stati nel suo ciclo di vita:
  - **Anteprima**: Disponibile con capacità limitata o per un pubblico limitato. "Funzioni di anteprima" E i data collezionisti dovrebbero diventare GA dopo il periodo di anteprima. I periodi di anteprima variano in

base al pubblico o alla funzionalità.

  - **GA**: Una funzionalità o un data collector generalmente disponibile per tutti i clienti, in base all'edizione o al set di funzionalità.
  - **Deprecated**: Si applica ai data collezions che non sono o sono previsti per diventare più sostenibili dal punto di vista funzionale. I data collezioner deprecati vengono spesso sostituiti con data collezioner più recenti e aggiornati dal punto di vista funzionale.
  - **Deleted**: Un data collector rimosso e non più disponibile.

- Unità di acquisizione: Un computer dedicato all'hosting dei data collezioner, in genere una macchina virtuale. Questo computer si trova generalmente nello stesso data center/VPC degli elementi monitorati.
- Origine dati: Modulo per la comunicazione con uno stack hardware o software. È costituito da una configurazione e da un codice che vengono eseguiti sul computer AU per comunicare con il dispositivo.

Requisiti dell'unità di acquisizione

È necessario installare un'unità di acquisizione (AU) per acquisire informazioni dai data collettori dell'infrastruttura (storage, VM, porta, EC2, ecc.). Prima di installare l'unità di acquisizione, assicurarsi che l'ambiente soddisfi i requisiti di sistema operativo, CPU, memoria e spazio su disco.

Requisiti

Componente	Requisiti Linux	Requisiti Windows

Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti componenti: * CentOS (64 bit): Da 7,2 a 7,9, da 8,1 a 8,4, Stream 8, Stream 9 * Debian (64 bit): 9 e 10 * OpenSUSE Leap dal 15,1 al 15,5 * Oracle Enterprise Linux (64 bit): Da 7,5 a 7,9, da 8,1 a 8,8 * Red Hat Enterprise Linux (64 bit): Da 7,2 a 7,9, da 8,1 a 8,8, 9,1, 9,2 * Rocky 9,0, 9,1, 9,3 * SUSE Enterprise Linux Server 15, dal 15 SP2 al 15 SP5 * Ubuntu Server: 18,04, 20,04, 22,04 LTS * SELinux sulle piattaforme precedenti Questo computer non deve eseguire alcun altro software a livello di applicazione. Si consiglia di utilizzare un server dedicato. Se si utilizza SELinux, si consiglia di eseguire i seguenti comandi sul sistema dell'unità di acquisizione: sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/.*)?" Sudo restorecon -R /opt/netapp/cloudinsights	Un computer che esegue una versione con licenza di uno dei seguenti componenti: * Microsoft Windows 10 64-bit * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 questo computer non deve eseguire altri software a livello di applicazione. Si consiglia di utilizzare un server dedicato.
CPU	2 core CPU	Stesso
Memoria	8 GB DI RAM	Stesso
Spazio su disco disponibile	50 GB (100 GB consigliati) Per Linux, lo spazio su disco deve essere allocato in questo modo: /Opt/netapp 10 GB (20 GB per ambienti di grandi dimensioni) /Var/log/netapp 40 GB (80 GB per ambienti di grandi dimensioni) /Tmp almeno 1 GB disponibili durante l'installazione	50 GB

Rete	Sono richiesti un collegamento Ethernet a 100 Mbps/1 Gbps, un indirizzo IP statico e una connettività della porta 80 o 443 dall'unità di acquisizione a *.cloudinsights.netapp.com o l'ambiente Cloud Insights (ad es. \Https://<environment_id>.c01.cloudinsights.netapp.com). Per i requisiti tra l'unità di acquisizione e ciascun Data Collector, fare riferimento alle istruzioni del "Data Collector". Se l'organizzazione richiede l'utilizzo del proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy dell'organizzazione e cercare alcune eccezioni per il funzionamento di Cloud Insights. Ad esempio, l'organizzazione blocca l'accesso per impostazione predefinita e consente l'accesso a siti/domini Web specifici solo in base all'eccezione? In tal caso, sarà necessario aggiungere il seguente dominio all'elenco delle eccezioni: *.cloudinsights.netapp.com Per ulteriori informazioni, consultare informazioni sui proxy "Qui (Linux)" oppure "Qui (Windows)".	Stesso
Permessi	Sudo permissions on the Acquisition Unit server (sudo permessi sul server dell'unità /tmp deve essere montato con funzionalità exec.	Autorizzazioni di amministratore sul server dell'unità di acquisizione
Virus Scan (scansione virus)		Durante l'installazione, è necessario disattivare completamente tutti i virus scanner. Dopo l'installazione, i percorsi utilizzati dal software dell'unità di acquisizione devono essere esclusi dalla scansione dei virus.

Consigli aggiuntivi

- Per un controllo accurato e la creazione di report dei dati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'unità di acquisizione utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Per quanto riguarda il dimensionamento

È possibile iniziare con un'unità di acquisizione Cloud Insights con soli 8 GB di memoria e 50 GB di spazio su disco, tuttavia, per gli ambienti più grandi, è necessario porsi le seguenti domande:

Prevedete di:

- Scopri più di 2500 macchine virtuali o 10 cluster ONTAP di grandi dimensioni (> 2 nodi), array Symmetrix o array VSP/XP HDS/HPE su questa unità di acquisizione?
- Implementare 75 o più data raccoglitori totali su questa unità di acquisizione?

Per ogni risposta "Sì" sopra, si consiglia di aggiungere 8 GB di memoria e 50 GB di spazio su disco all'AU. Ad esempio, se hai risposto "Sì" a entrambi, devi implementare un sistema di memoria da 24 GB con almeno 150 GB di spazio su disco. Su Linux, lo spazio su disco da aggiungere alla posizione del log.

Per ulteriori domande sul dimensionamento, contatta il supporto NetApp.

Requisito aggiuntivo della Federal Edition

- Per le installazioni delle unità di acquisizione nei cluster Cloud Insights Edizione Federale, il sistema operativo sottostante deve avere una buona fonte di entropia. Sui sistemi Linux, questo viene generalmente eseguito installando *rng-tools* o utilizzando la generazione di numeri casuali (RNG) dell'hardware. È responsabilità del cliente assicurarsi che questo requisito sia soddisfatto sulla macchina dell'unità di acquisizione.

Configurazione delle unità di acquisizione

Cloud Insights raccoglie i dati dei dispositivi utilizzando una o più unità di acquisizione installate sui server locali. Ogni unità di acquisizione può ospitare più Data Collector, che inviano le metriche del dispositivo a Cloud Insights per l'analisi.

In questo argomento viene descritto come aggiungere unità di acquisizione e vengono descritte le procedure aggiuntive necessarie quando l'ambiente utilizza un proxy.

> Per un controllo accurato e la creazione di report dei dati, si consiglia vivamente di sincronizzare l'ora sulla macchina dell'unità di acquisizione utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

Informazioni sulla sicurezza di Cloud Insights "qui".

Aggiunta di un'unità di acquisizione Linux

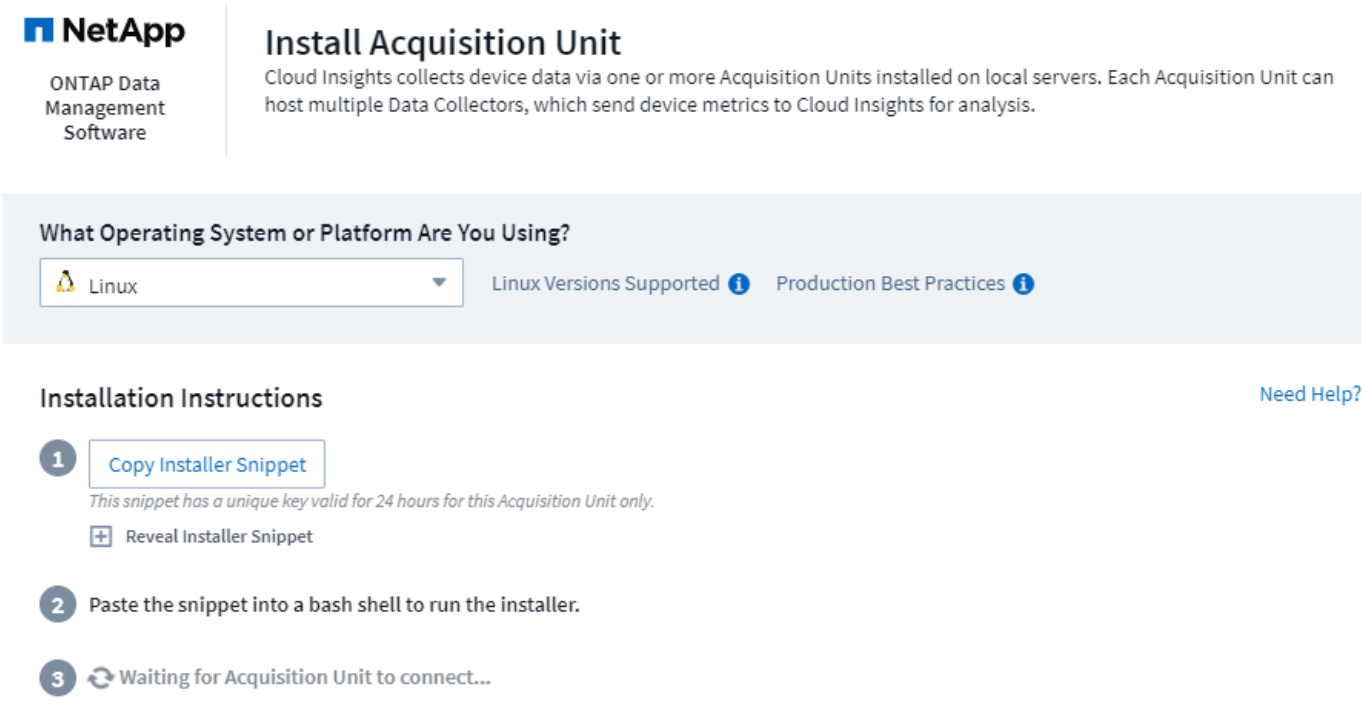
Prima di iniziare

- Se il sistema utilizza un proxy, è necessario impostare le variabili di ambiente proxy prima di installare l'unità di acquisizione. Per ulteriori informazioni, vedere Impostazione delle variabili di ambiente proxy.

Procedura per l'installazione dell'unità di acquisizione Linux

1. Accedere come amministratore o come proprietario dell'account all'ambiente Cloud Insights.
2. Fare clic su **osservabilità > Collector > unità di acquisizione > +unità di acquisizione**

   Viene visualizzata la finestra di dialogo *Install Acquisition Unit* (Installa unità di acquisizione). Scegli Linux.



1. Verificare che il server o la macchina virtuale che ospita l'unità di acquisizione soddisfi i requisiti di sistema consigliati.
2. Verificare che sul server sia in esecuzione una versione supportata di Linux. Fare clic su *versioni del sistema operativo supportate (i)* per un elenco delle versioni supportate.
3. Copiare il frammento del comando di installazione nella finestra di dialogo in una finestra terminale sul server o sulla macchina virtuale che ospiterà l'unità di acquisizione.
4. Incollare ed eseguire il comando nella shell di Bash.

Al termine

- Fare clic su **osservabilità > Collector > unità di acquisizione** per controllare lo stato delle unità di acquisizione.
- È possibile accedere ai registri delle unità di acquisizione all'indirizzo /var/log/netapp/cloudsights/acq/acq.log
- Utilizzare il seguente script per controllare l'unità di acquisizione:
  - cloudinsights-service.sh (arrestare, avviare, riavviare, controllare lo stato)
- Utilizzare il seguente script per disinstallare l'unità di acquisizione:
  - cloudinsights-uninstall.sh

Impostazione delle variabili di ambiente proxy

Per gli ambienti che utilizzano un proxy, è necessario impostare le variabili di ambiente proxy prima di aggiungere l'unità di acquisizione. Le istruzioni per la configurazione del proxy sono disponibili nella finestra di dialogo *Add Acquisition Unit* (Aggiungi unità di acquisizione).

1. Fare clic su + in *have a Proxy Server?*
2. Copiare i comandi in un editor di testo e impostare le variabili proxy in base alle necessità.

   Nota: Prestare attenzione alle restrizioni relative ai caratteri speciali nei campi del nome utente e della password del proxy: '%' e '!' sono consentiti nel campo nome utente. ':', '%' e '!' sono consentiti nel campo password.

3. Eseguire il comando modificato in un terminale utilizzando la shell Bash.
4. Installare il software dell'unità di acquisizione.

Configurazione del proxy

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Cloud Insights. Il certificato client deve essere passato al server Cloud Insights per essere autenticato. A tale scopo, il proxy deve essere impostato per inoltrare la richiesta https al server Cloud Insights senza decifrare i dati.

Il modo più semplice per farlo è specificare la configurazione con caratteri jolly nel proxy/firewall per comunicare con Cloud Insights, ad esempio:

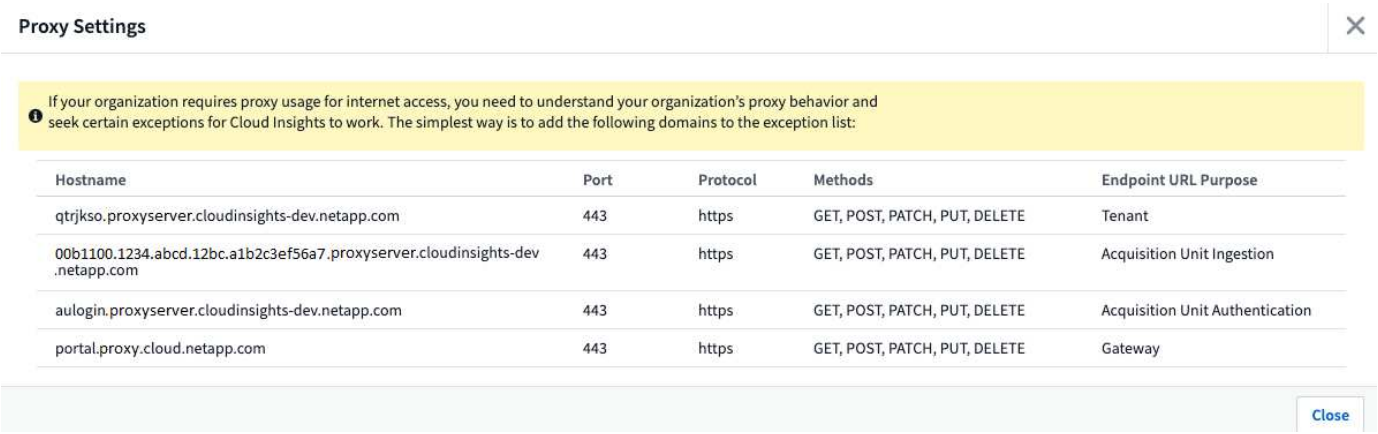
```
*.cloudinsights.netapp.com
```

> L'uso di un asterisco (*) per i caratteri jolly è comune, ma la configurazione del proxy/firewall potrebbe utilizzare un formato diverso. Consultare la documentazione del proxy per verificare la correttezza delle specifiche dei caratteri jolly nell'ambiente in uso.

Ulteriori informazioni sulla configurazione del proxy sono disponibili in NetApp "Knowledge base".

Visualizzazione degli URL proxy

È possibile visualizzare gli URL degli endpoint proxy facendo clic sul collegamento **Proxy Settings** (Impostazioni proxy) quando si sceglie un data collector durante l'acquisizione oppure sul collegamento *Proxy Settings* (Impostazioni proxy) nella pagina **Help > Support** (Guida > supporto). Viene visualizzata una tabella simile alla seguente.



Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev .netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

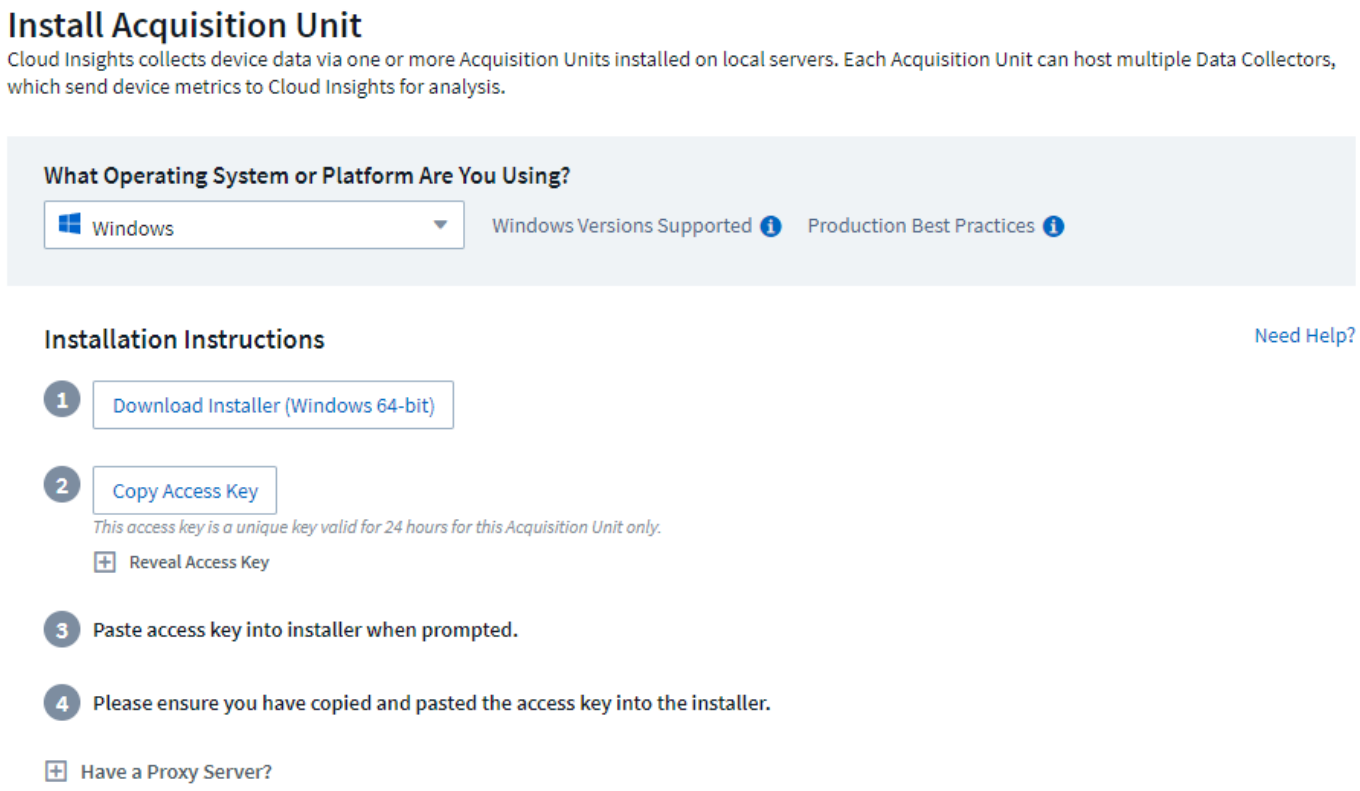
Se nel proprio ambiente si dispone di workload Security, in questo elenco vengono visualizzati anche gli URL degli endpoint configurati.

Aggiunta di un'unità di acquisizione Windows

Procedura per l'installazione dell'unità di acquisizione Windows

1. Accedere al server/VM dell'unità di acquisizione come utente con autorizzazioni di amministratore.
2. Su tale server, aprire una finestra del browser e accedere all'ambiente Cloud Insights come Amministratore o Proprietario dell'account.
3. Fare clic su **osservabilità > Collettori > unità di acquisizione > +unità di acquisizione** .

   Viene visualizzata la finestra di dialogo *Install Acquisition Unit* (Installa unità di acquisizione). Scegliere Windows.



1. Verificare che il server o la macchina virtuale che ospita l'unità di acquisizione soddisfi i requisiti di sistema consigliati.
2. Verificare che sul server sia in esecuzione una versione supportata di Windows. Fare clic su *versioni del sistema operativo supportate (i)* per un elenco delle versioni supportate.
3. Fare clic sul pulsante **Download Installer (Windows 64-bit)**.
4. Copiare la chiave di accesso. Ciò sarà necessario durante l'installazione.
5. Sul server/VM dell'unità di acquisizione, eseguire il programma di installazione scaricato.
6. Quando richiesto, incollare la chiave di accesso nella procedura guidata di installazione.
7. Durante l'installazione, verrà visualizzata l'opportunità di fornire le impostazioni del server proxy.

Al termine

- Fare clic su * > osservabilità > Collector > unità di acquisizione* per controllare lo stato delle unità di acquisizione.
- È possibile accedere al log dell'unità di acquisizione in <install dir>/informazioni sul cloud/unità di acquisizione/log acq.log

- Utilizzare il seguente script per arrestare, avviare, riavviare o controllare lo stato dell'unità di acquisizione:

```
cloudinsights-service.sh
```

Configurazione del proxy

L'unità di acquisizione utilizza l'autenticazione reciproca/bidirezionale per connettersi al server Cloud Insights. Il certificato client deve essere passato al server Cloud Insights per essere autenticato. A tale scopo, il proxy deve essere impostato per inoltrare la richiesta https al server Cloud Insights senza decifrare i dati.

Il modo più semplice per farlo è specificare la configurazione con caratteri jolly nel proxy/firewall per comunicare con Cloud Insights, ad esempio:

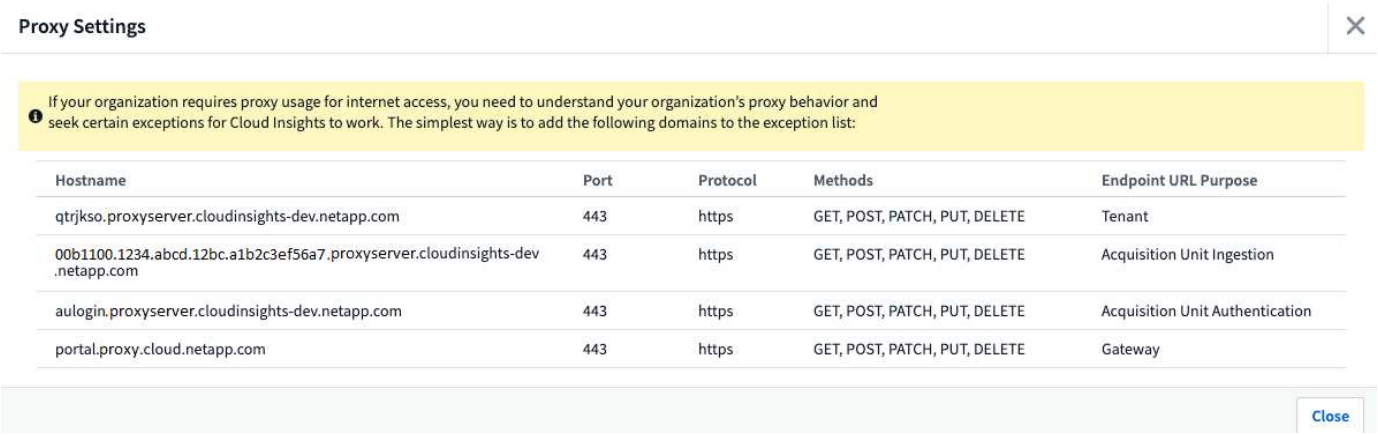
```
*.cloudinsights.netapp.com
```

> L'uso di un asterisco (*) per i caratteri jolly è comune, ma la configurazione del proxy/firewall potrebbe utilizzare un formato diverso. Consultare la documentazione del proxy per verificare la correttezza delle specifiche dei caratteri jolly nell'ambiente in uso.

Ulteriori informazioni sulla configurazione del proxy sono disponibili in NetApp "Knowledge base".

Visualizzazione degli URL proxy

È possibile visualizzare gli URL degli endpoint proxy facendo clic sul collegamento **Proxy Settings** (Impostazioni proxy) quando si sceglie un data collector durante l'acquisizione oppure sul collegamento *Proxy Settings* (Impostazioni proxy) nella pagina **Help > Support** (Guida > supporto). Viene visualizzata una tabella simile alla seguente.



Se nel proprio ambiente si dispone di workload Security, in questo elenco vengono visualizzati anche gli URL degli endpoint configurati.

Disinstallazione di un'unità di acquisizione

Per disinstallare il software dell'unità di acquisizione, procedere come indicato di seguito:

Windows:

Se si disinstalla un'unità di acquisizione **Windows**:

1. Sul server/VM dell'unità di acquisizione, aprire il pannello di controllo e scegliere **Disinstalla un programma**. Selezionare il programma dell'unità di acquisizione Cloud Insights da rimuovere.
2. Fare clic su Disinstalla e seguire le istruzioni.

Linux:

Se si disinstalla un'unità di acquisizione **Linux**:

1. Sul server/VM dell'unità di acquisizione, eseguire il seguente comando:

```
 sudo cloudinsights-uninstall.sh -p
. Per assistenza con la disinstallazione, eseguire:
```

```
sudo cloudinsights-uninstall.sh --help
```

Windows e Linux:

Dopo disinstallazione dell'AU:

1. In Cloud Insights, andare su **osservabilità > Collector e selezionare la scheda *unità di acquisizione**.
2. Fare clic sul pulsante Options (Opzioni) a destra dell'unità di acquisizione che si desidera disinstallare e selezionare *Delete* (Elimina). È possibile eliminare un'unità di acquisizione solo se non vi sono raccoglitori di dati assegnati.

> Non è possibile eliminare un'unità di acquisizione (AU) a cui sono collegati i collettori di dati. Spostare tutti i raccoglitori di dati dell'unità AU in un'altra unità AU (modificare il raccoglitore e selezionare semplicemente un'altra unità AU) prima di eliminare l'unità AU originale.

Per la risoluzione del dispositivo viene utilizzata un'unità di acquisizione con una stella accanto. Prima di rimuovere questa AU, è necessario selezionare un'altra AU da utilizzare per la risoluzione del dispositivo. Passare il mouse su un'AU diversa e aprire il menu "tre punti" per selezionare "Usa per la risoluzione del dispositivo".

Reinstallazione di un'unità di acquisizione

Per reinstallare un'unità di acquisizione sullo stesso server/macchina virtuale, attenersi alla seguente procedura:

Prima di iniziare

Prima di reinstallare un'unità di acquisizione, è necessario configurare un'unità di acquisizione temporanea su un server/macchina virtuale separato.

Fasi

1. Accedere al server/VM dell'unità di acquisizione e disinstallare il software AU.
2. Accedere all'ambiente Cloud Insights e andare a **osservabilità > Collector**.
3. Per ciascun data collector, fare clic sul menu Options (Opzioni) a destra e selezionare *Edit* (Modifica). Assegnare il data collector all'unità di acquisizione temporanea e fare clic su **Save** (Salva).

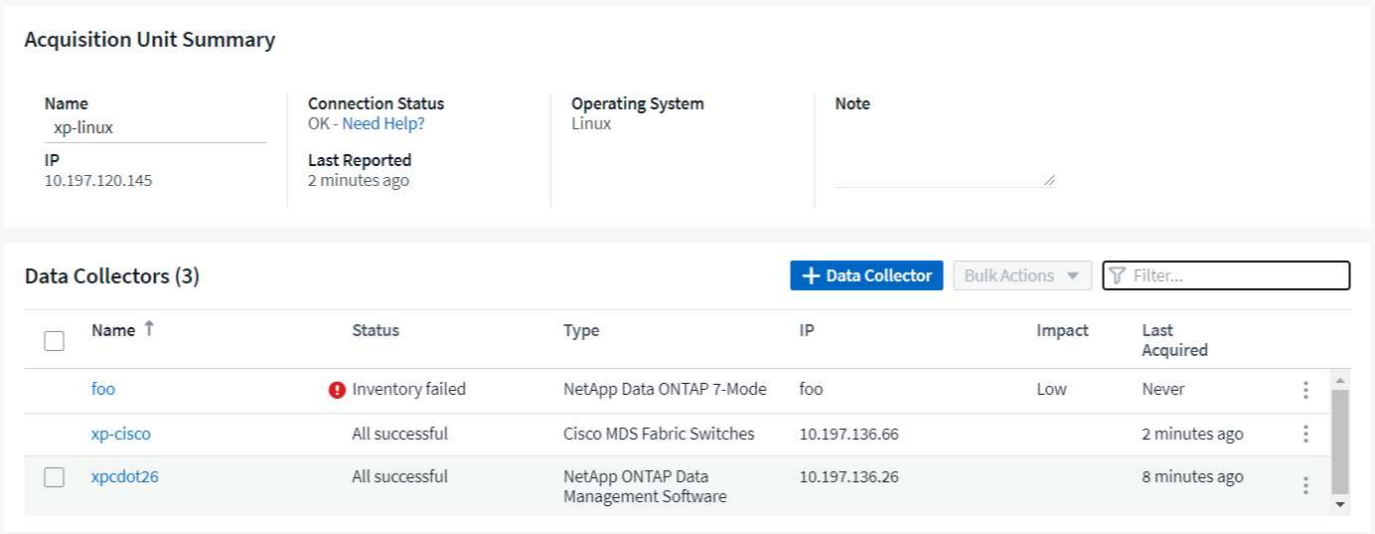
   È inoltre possibile selezionare più raccoglitori di dati dello stesso tipo e fare clic sul pulsante **azioni in blocco**. Scegliere *Edit* e assegnare i data collezioner all'unità di acquisizione temporanea.

4. Dopo aver spostato tutti i raccoglitori di dati nell'unità di acquisizione temporanea, andare su **osservabilità > Collector** e selezionare la scheda **unità di acquisizione**.
5. Fare clic sul pulsante Options (Opzioni) a destra dell'unità di acquisizione che si desidera reinstallare e selezionare *Delete* (Elimina). È possibile eliminare un'unità di acquisizione solo se non vi sono raccoglitori di dati assegnati.
6. È ora possibile reinstallare il software dell'unità di acquisizione sul server/VM originale. Fare clic su **+Acquisition Unit** (unità di acquisizione) e seguire le istruzioni riportate sopra per installare l'unità di acquisizione.
7. Una volta reinstallata l'unità di acquisizione, riassegnare i dati raccolti all'unità di acquisizione.

Visualizzazione dei dettagli AU

La pagina dei dettagli dell'unità di acquisizione (AU) fornisce dettagli utili per un AU e informazioni utili per la risoluzione dei problemi. La pagina dei dettagli AU contiene le seguenti sezioni:

- Una sezione **riepilogativa** che mostra quanto segue:
  - **Nome** e **IP** dell'unità di acquisizione
  - Connessione corrente **Stato** dell'AU
  - **Ultimo report** tempo di polling riuscito del data collector
  - Il **sistema operativo** della macchina AU
  - Qualsiasi **Nota** corrente per l'AU. Utilizzare questo campo per inserire un commento per l'AU. Il campo visualizza la nota aggiunta più di recente.
- Una tabella dei **Data Collector** dell'AU che mostra, per ciascun data collector:
  - **Nome** - fare clic su questo collegamento per accedere alla pagina dei dettagli del data collector con ulteriori informazioni
  - **Status** - informazioni sull'errore o sul successo
  - **Tipo** - fornitore/modello
  - Indirizzo **IP** del data collector
  - Livello di **impatto** corrente
  - Ora **ultima acquisizione** - l'ultima volta in cui il data collector è stato eseguito correttamente



Per ciascun data collector, è possibile fare clic sul menu "Three dots" (tre punti) per clonare, modificare, polling o eliminare il data collector. In questo elenco è inoltre possibile selezionare più data raccoglitori per eseguire azioni in blocco su di essi.

Per riavviare l'unità di acquisizione, fare clic sul pulsante **Restart** (Riavvia) nella parte superiore della pagina. Selezionare questo pulsante per tentare di **ripristinare la connessione** all'AU in caso di problemi di connessione.

Configurazione di un agente per la raccolta dei dati (Windows/Linux)

Cloud Insights utilizza "Telefono" come agente per la raccolta di dati di integrazione. Telegraf è un agente server basato su plug-in che può essere utilizzato per raccogliere e generare report su metriche, eventi e registri. I plug-in di input vengono utilizzati per raccogliere le informazioni desiderate nell'agente accedendo direttamente al sistema/sistema operativo, chiamando API di terze parti o ascoltando flussi configurati (ad esempio Kafka, statsD, ecc.). I plug-in di output vengono utilizzati per inviare metriche, eventi e registri raccolti dall'agente a Cloud Insights.

La versione corrente di Telegraf per Cloud Insights è **1.24.0**.

Per informazioni sull'installazione su Kubernetes, consulta la "NetApp Kubernetes Monitoring Operator" pagina.

> Per un audit e un reporting dei dati accurati, si consiglia di sincronizzare l'ora sul computer dell'agente utilizzando **Network Time Protocol (NTP)** o **Simple Network Time Protocol (SNTP)**.

> Se si desidera verificare i file di installazione prima di installare Agent, consultare la sezione seguente a. Verifica dei checksum.

Installazione di un agente

Se si sta installando un servizio di raccolta dati e non si è ancora configurato un agente, viene richiesto di installare prima un agente per il sistema operativo appropriato. In questo argomento vengono fornite istruzioni per l'installazione di Telegraf Agent sui seguenti sistemi operativi:

- Windows
- RHEL e CentOS
- Ubuntu e Debian

Per installare un agente, indipendentemente dalla piattaforma in uso, è necessario prima effettuare le seguenti operazioni:

1. Accedere all'host da utilizzare per l'agente.
2. Accedere all'ambiente Cloud Insights e accedere a **osservabilità > Collector**.
3. Fare clic su **+Data Collector** e scegliere un data collector da installare.
4. Scegli la piattaforma appropriata per il tuo host (Windows, Linux)
5. Seguire i passaggi rimanenti per ciascuna piattaforma.

Una volta installato un agente su un host, non è necessario installare nuovamente un agente su tale host.

Una volta installato un agente su un server/macchina virtuale, Cloud Insights raccoglie le metriche da quel sistema oltre a raccogliere dati da qualsiasi raccolta di dati configurata. Queste metriche vengono raccolte come "Metriche "nodo"".

Se si utilizza un proxy, leggere le istruzioni per il proxy della piattaforma prima di installare l'agente Telegraf.

Posizioni dei log

I messaggi di log di Telegraf vengono reindirizzati da stdout ai seguenti file di log.

- RHEL/CentOS: /Var/log/telegraf/telegraf.log
- Ubuntu/Debian: /Var/log/telegraf/telegraf.log
- Windows: C: File di programma telegraf.log

Windows

Prerequisiti:

- PowerShell deve essere installato
- Se si utilizza un proxy, seguire le istruzioni nella sezione **Configurazione del supporto proxy per Windows**.

Configurazione del supporto proxy per Windows

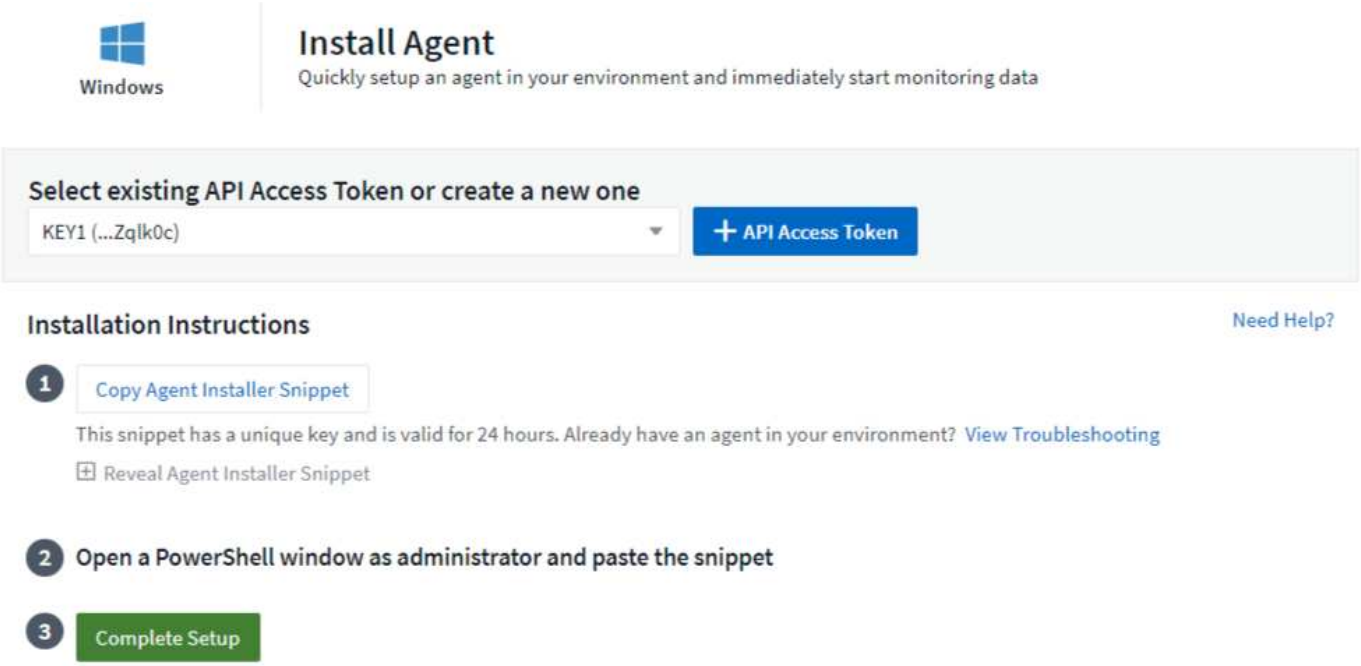
Se l'ambiente in uso utilizza un proxy, leggere questa sezione prima di procedere con l'installazione.

I passaggi riportati di seguito illustrano le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

Per i sistemi che risiedono dietro un proxy, eseguire le seguenti operazioni per impostare le variabili di ambiente *https_proxy* e/o *http_proxy* **PRIMA** dell'installazione dell'agente Telegrafe:

```
[System.Environment]::SetEnvironmentVariable("https_proxy",
"<proxy_server>:<proxy_port>",
[System.EnvironmentVariableTarget]::Machine)
```

Installazione dell'agente



Procedura per l'installazione dell'agente su Windows:

1. Scegliere un tasto di accesso dell'agente.
2. Copiare il blocco di comandi dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli Appunti per copiare rapidamente il comando negli Appunti.
3. Aprire una finestra PowerShell
4. Incollare il comando nella finestra PowerShell e premere Invio.
5. Il comando scarica il programma di installazione dell'agente appropriato, lo installa e imposta una configurazione predefinita. Al termine, il servizio dell'agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **fine** o **continua**

Una volta installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

```
Start-Service telegraf
Stop-Service telegraf
```

Disinstallazione dell'agente

Per disinstallare l'agente su Windows, eseguire le seguenti operazioni in una finestra PowerShell:

1. Interrompere ed eliminare il servizio Telegraf:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Rimuovere il certificato dal trustore:

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. Eliminare la cartella *C:/Program Files/telegraf* per rimuovere i file binari, i log e i file di configurazione
4. Rimuovere la chiave *SYSTEM/CurrentControlSet/Services/EventLog/Application/telegraf* dal Registro di sistema

Aggiornamento dell'Agent

Per aggiornare telegraf Agent, procedere come segue:

1. Interrompere ed eliminare il servizio telegraf:

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. Eliminare la chiave *SYSTEM/CurrentControlSet/Services/EventLog/Application/telegraf* dal Registro di sistema
3. Delete *C:/Program Files/telegraf.conf*
4. Delete *C:/Program Files/telegraf/telegraf.exe*
5. "Installare il nuovo agente".

RHEL e CentOS

Prerequisiti:

- Devono essere disponibili i seguenti comandi: Curl, sudo, ping, sha256sum, openssl, e dmidecode
- Se si utilizza un proxy, seguire le istruzioni nella sezione **Configurazione del supporto proxy per RHEL/CentOS**.

Configurazione del supporto proxy per RHEL/CentOS

> Se l'ambiente in uso utilizza un proxy, leggere questa sezione prima di procedere con l'installazione.

> I passaggi riportati di seguito illustrano le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

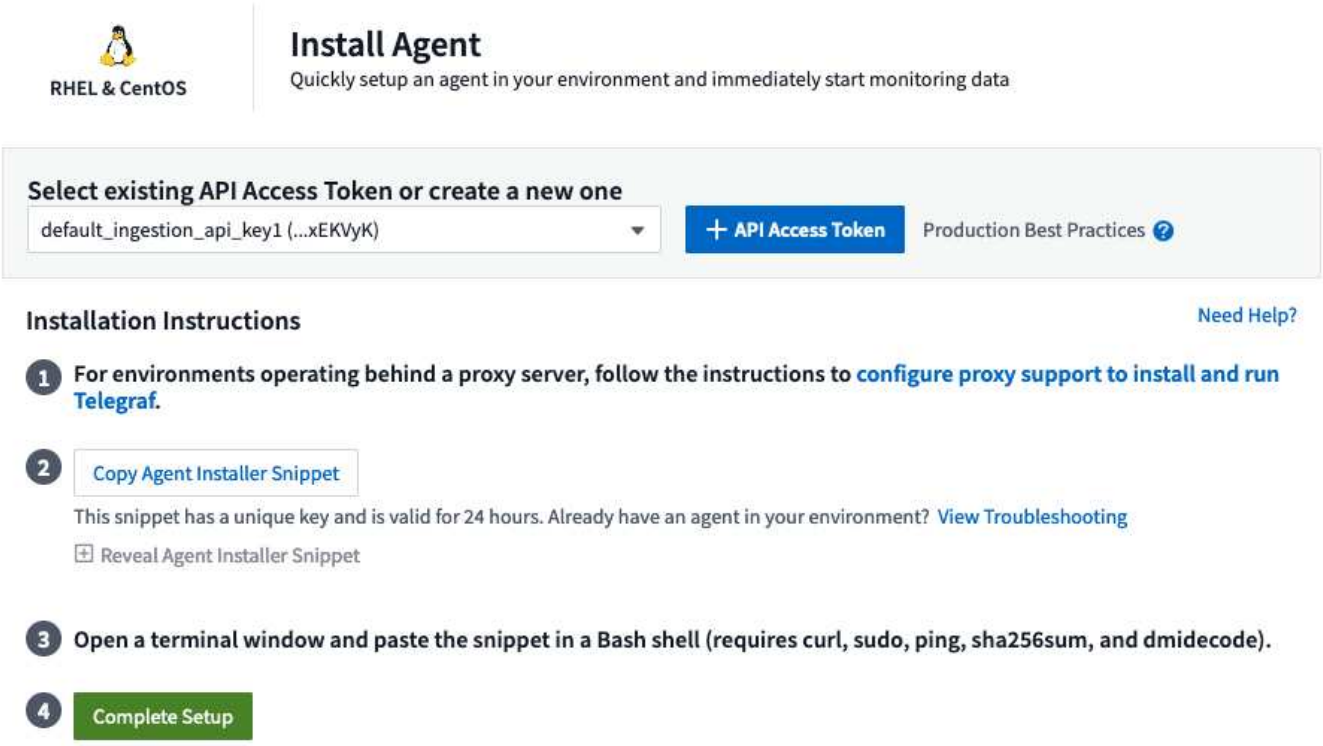
Per i sistemi che risiedono dietro un proxy, eseguire i seguenti passaggi **PRIMA** dell'installazione dell'agente Telegraf:

1. Impostare le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Creare _/etc/default/telegraf_ e inserire le definizioni per le
variabili _https_proxy_ e/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installazione dell'agente



Procedura per l'installazione dell'agente su RHEL/CentOS:

1. Scegliere un tasto di accesso dell'agente.
2. Copiare il blocco di comandi dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli Appunti per copiare rapidamente il comando negli Appunti.
3. Aprire una finestra Bash
4. Incollare il comando nella finestra Bash e premere Invio.

5. Il comando scarica il programma di installazione dell'agente appropriato, lo installa e imposta una configurazione predefinita. Al termine, il servizio dell'agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **fine** o **continua**

Una volta installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

Se il sistema operativo utilizza systemd (CentOS 7+ e RHEL 7+):

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Se il sistema operativo in uso non utilizza systemd (CentOS 7+ e RHEL 7+):

```
sudo service telegraf start
sudo service telegraf stop
```

Disinstallazione dell'agente

Per disinstallare l'agente su RHEL/CentOS, in un terminale Bash, procedere come segue:

1. Interrompere il servizio Telegraf:

   ```
   systemctl stop telegraf (If your operating system is using systemd
   (CentOS 7+ and RHEL 7+)
   /etc/init.d/telegraf stop (for systems without systemd support)
   ```

2. Rimuovere l'agente Telegraf:

   ```
    yum remove telegraf
   . Rimuovere eventuali file di configurazione o log che potrebbero essere
   lasciati indietro:
   ```

   ```
   rm -rf /etc/telegraf*
   rm -rf /var/log/telegraf*
   ```

Aggiornamento dell'Agent

Per aggiornare telegraf Agent, procedere come segue:

1. Interrompere il servizio telegraf:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere l'agente telegrafo precedente:

```
 yum remove telegraf
. xref:{relative_path}#rhel-and-centos["Installare il nuovo agente"].
```

Ubuntu e Debian

Prerequisiti:

- Devono essere disponibili i seguenti comandi: Curl, sudo, ping, sha256sum, openssl, e dmidecode
- Se si utilizza un proxy, seguire le istruzioni nella sezione **Configurazione del supporto proxy per Ubuntu/Debian**.

Configurazione del supporto proxy per Ubuntu/Debian

> Se l'ambiente in uso utilizza un proxy, leggere questa sezione prima di procedere con l'installazione.

> I passaggi riportati di seguito illustrano le azioni necessarie per impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

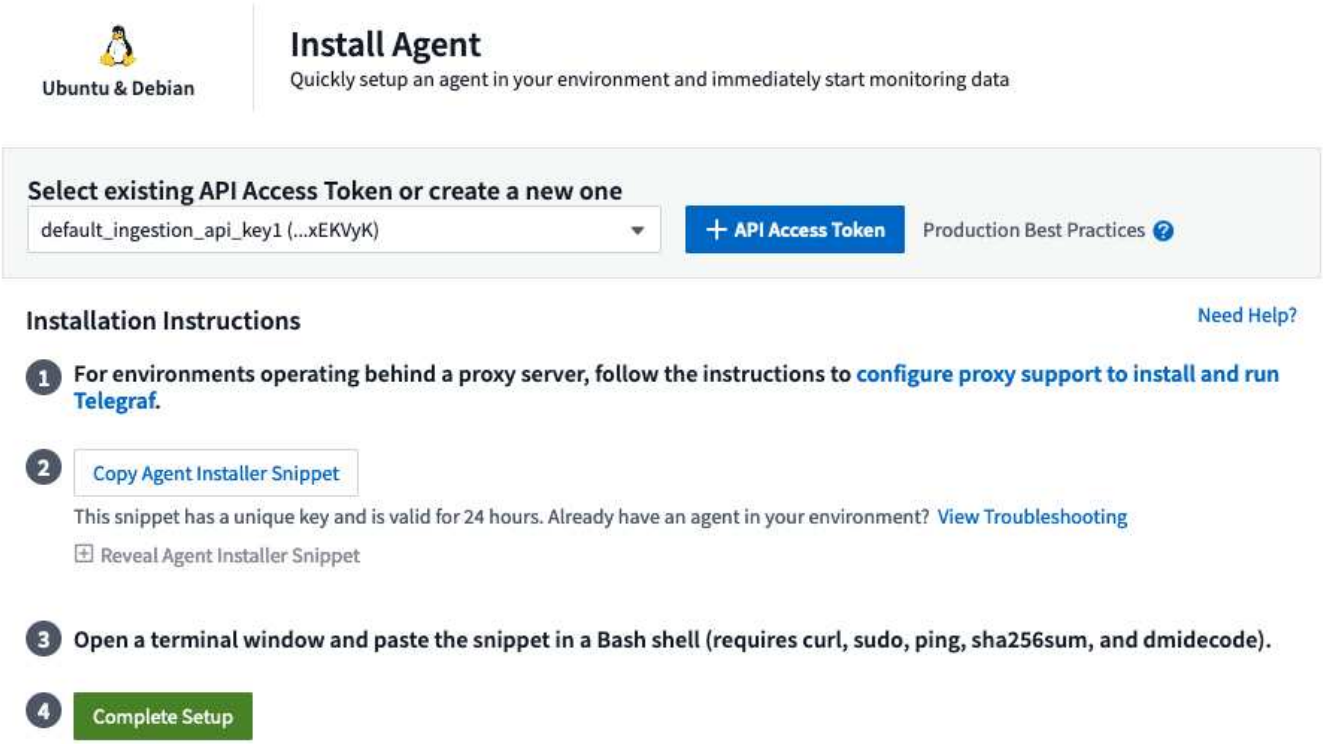
Per i sistemi che risiedono dietro un proxy, eseguire i seguenti passaggi **PRIMA** dell'installazione dell'agente Telegraf:

1. Impostare le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:

```
 export https_proxy=<proxy_server>:<proxy_port>
. Creare /etc/default/telegraf e inserire le definizioni per le
variabili _https_proxy_ e/o _http_proxy_:
```

```
https_proxy=<proxy_server>:<proxy_port>
```

Installazione dell'agente



Procedura per installare Agent su Debian o Ubuntu:

1. Scegliere un tasto di accesso dell'agente.
2. Copiare il blocco di comandi dalla finestra di dialogo di installazione dell'agente. È possibile fare clic sull'icona degli Appunti per copiare rapidamente il comando negli Appunti.
3. Aprire una finestra Bash
4. Incollare il comando nella finestra Bash e premere Invio.
5. Il comando scarica il programma di installazione dell'agente appropriato, lo installa e imposta una configurazione predefinita. Al termine, il servizio dell'agente verrà riavviato. Il comando ha una chiave univoca ed è valido per 24 ore.
6. Fare clic su **fine** o **continua**

Una volta installato l'agente, è possibile utilizzare i seguenti comandi per avviare/arrestare il servizio:

Se il sistema operativo in uso utilizza systemd:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

Se il sistema operativo non utilizza systemd:

```
sudo service telegraf start
sudo service telegraf stop
```

Disinstallazione dell'agente

Per disinstallare l'agente su Ubuntu/Debian, in un terminale Bash, eseguire quanto segue:

1. Interrompere il servizio Telegraf:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere l'agente Telegraf:

```
 dpkg -r telegraf
. Rimuovere eventuali file di configurazione o log che potrebbero essere
lasciati indietro:
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

Aggiornamento dell'Agent

Per aggiornare telegraf Agent, procedere come segue:

1. Interrompere il servizio telegraf:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Rimuovere l'agente telegrafo precedente:

```
 dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["Installare il nuovo agente"].
```

Verifica dei checksum

Il programma di installazione dell'agente Cloud Insights esegue controlli di integrità, ma alcuni utenti potrebbero voler eseguire le proprie verifiche prima di installare o applicare gli artefatti scaricati. Questo può essere fatto scaricando il programma di installazione e generando un checksum per il pacchetto scaricato, quindi confrontando il checksum con il valore mostrato nelle istruzioni di installazione.

Scaricare il pacchetto di installazione senza eseguire l'installazione

Per eseguire un'operazione di solo download (invece del download e dell'installazione predefiniti), gli utenti possono modificare il comando di installazione dell'agente ottenuto dall'interfaccia utente e rimuovere l'opzione finale di "installazione".

Attenersi alla seguente procedura:

1. Copiare il frammento del programma di installazione dell'agente come indicato.
2. Invece di incollare il frammento in una finestra di comando, incollarlo in un editor di testo.
3. Rimuovere "--install" (Linux) o "-install" (Windows) dal comando.
4. Copiare l'intero comando dall'editor di testo.
5. Incollarlo nella finestra di comando (in una directory di lavoro) ed eseguirlo.

Non Windows (questi esempi sono per Kubernetes; i nomi degli script effettivi possono variare):

- Download e installazione (impostazione predefinita):

```
 installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download --install
* Solo download:
```

```
installerName=cloudinsights-kubernetes.sh … && sudo -E -H
./$installerName --download
```

Finestre:

- Download e installazione (impostazione predefinita):

```
 !$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download -install)
* Solo download:
```

```
!$($installerName=".\cloudinsights-windows.ps1") … -and
$(&$installerName -download)
```

Il comando di solo download scaricherà tutti gli artefatti richiesti da Cloud Insights nella directory di lavoro. Gli artefatti includono, ma non possono essere limitati a:

- uno script di installazione
- un file di ambiente
- File YAML
- un file checksum (che termina con sha256.signed o sha256.ps1)

Lo script di installazione, il file di ambiente e i file YAML possono essere verificati utilizzando l'ispezione visiva.

Generare un valore di checksum

Per generare il valore del checksum, eseguire il seguente comando per la piattaforma appropriata:

- RHEL/Ubuntu:

```
 sha256sum <package_name>
* Finestre:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

Verificare il checksum

Estrarre il checksum previsto dal file checksum

- Non Windows:

```
 openssl smime -verify -in telegraf*.sha256.signed -CAfile
netapp_cert.pem -purpose any -nosigs -noverify
* Finestre:
```

```
(Get-Content telegraf.zip.sha256.ps1 -First 1).toUpper()
```

Installare il pacchetto scaricato

Una volta verificati correttamente tutti gli artefatti, l'installazione dell'agente può essere avviata eseguendo:

Non Windows:

```
 sudo -E -H ./<installation_script_name> --install
Finestre:
```

```
.\cloudinsights-windows.ps1 -install
```

Risoluzione dei problemi

Alcuni suggerimenti da provare in caso di problemi durante la configurazione di un agente:

Problema:	Prova:
Dopo aver configurato un nuovo plug-in e aver riavviato Telegraf, Telegraf non si avvia. I log indicano un errore simile al seguente: "[telegrafo] errore durante l'esecuzione dell'agente: Errore durante il caricamento del file di configurazione /etc/telegrafo/telegrafo.d/cloudindsightsees-default.conf: Plugin outputs.http: Riga <linenumber>: La configurazione ha specificato i campi ["use_system_proxy"], ma non sono stati utilizzati"	La versione installata di Telegraf è obsoleta. Seguire la procedura riportata in questa pagina per **aggiornare l'Agent** per la piattaforma appropriata.
Ho eseguito lo script del programma di installazione su una vecchia installazione e ora l'agente non invia dati	Disinstallare telegraf Agent ed eseguire nuovamente lo script di installazione. Seguire la procedura **Upgrade the Agent** riportata in questa pagina per la piattaforma appropriata.
È già stato installato un agente utilizzando Cloud Insights	Se un agente è già stato installato sull'host/VM, non è necessario installarlo di nuovo. In questo caso, è sufficiente scegliere la piattaforma e la chiave appropriate nella schermata Installazione agente e fare clic su **continua** o **fine**.
Un agente è già installato, ma non tramite il programma di installazione di Cloud Insights	Rimuovere l'agente precedente ed eseguire l'installazione dell'agente Cloud Insights per verificare che le impostazioni predefinite del file di configurazione siano corrette. Al termine, fare clic su **continua** o **fine**.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione di Data Collector

I Data Collector vengono configurati nell'ambiente Cloud Insights per la raccolta dei dati dai dispositivi del data center.

Prima di iniziare

- È necessario aver configurato un'unità di acquisizione prima di iniziare la raccolta dei dati.
- Sono necessarie le credenziali per i dispositivi da cui si stanno raccogliendo i dati.
- Per tutti i dispositivi da cui si stanno raccogliendo i dati sono necessari indirizzi di rete, informazioni sull'account e password.

Fasi

1. Dal menu Cloud Insights, fare clic su **osservabilità > Collector**

   Il sistema visualizza i Data Collector disponibili organizzati in base al vendor.

2. Fare clic su **+ Collector** e selezionare il data collector da configurare.

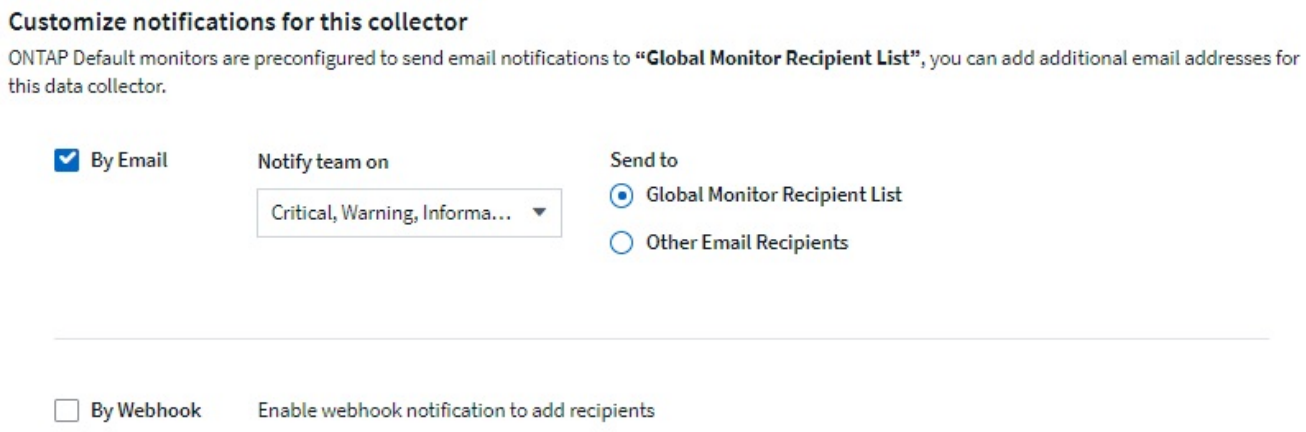
   Nella finestra di dialogo è possibile configurare il data collector e aggiungere un'unità di acquisizione.

3. Inserire un nome per il data collector.

   I nomi possono contenere lettere (a-z), numeri (0-9), trattini (-), caratteri di sottolineatura (_), apostrofi ('), e

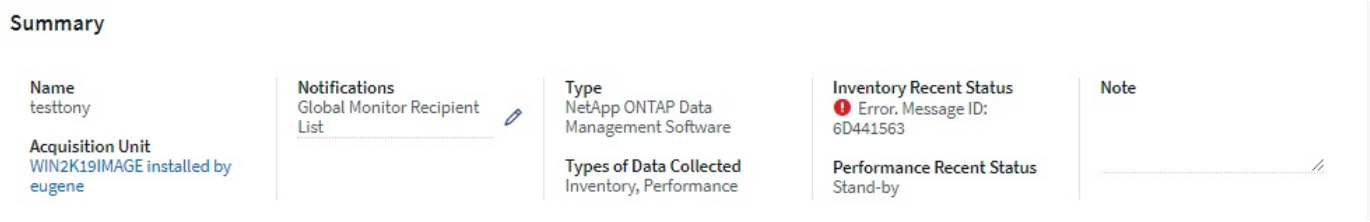
punti (.).

4. Inserire l'unità di acquisizione da associare a questo data collector.
5. Inserire i campi obbligatori nella schermata Configuration (Configurazione).
6. Quando viene richiesto di configurare le notifiche, scegliere di inviare avvisi tramite e-mail, Webhook o entrambi e scegliere i tipi di avvisi in base ai quali inviare la notifica (critico, Avviso, informativo e/o risolto). È possibile scegliere di inviare una notifica all'elenco dei destinatari di Global Monitor (configurato in **Admin > Notifiche**) o specificare altri destinatari. Quando si desidera continuare, fare clic su **complete Setup** (completa installazione).



Quando si visualizza una landing page di **ONTAP data collector**, è possibile modificare le notifiche facendo clic sull'icona a forma di matita nel campo "Notifiche" della sezione di riepilogo del data collector.

> Le notifiche del Data Collector di ONTAP hanno la precedenza su qualsiasi notifica specifica del Monitor rilevante per il cluster/data collector. L'elenco dei destinatari impostato per Data Collector riceverà gli avvisi di data collector. Se non sono presenti avvisi di data collector attivi, gli avvisi generati dal monitor verranno inviati a destinatari specifici del monitor.



1. Fare clic su **Advanced Configuration** (Configurazione avanzata) per aggiungere ulteriori campi di configurazione. (Non tutti i data collettori richiedono una configurazione avanzata).
2. Fare clic su **Test Configuration** per verificare che il data collector sia configurato correttamente.
3. Fare clic su **Aggiungi modulo di raccolta** per salvare la configurazione e aggiungere il modulo di raccolta dati al tenant Cloud Insights.

Dopo aver aggiunto un nuovo data collector, Cloud Insights avvia tre sondaggi:

- primo sondaggio di inventario: immediatamente
- 1° sondaggio sui dati delle performance per stabilire un riferimento: immediatamente dopo il sondaggio dell'inventario
- secondo sondaggio sulle performance: entro 15 secondi dal completamento del primo sondaggio sulle

performance

Il polling procede quindi in base agli intervalli di polling delle performance e dell'inventario configurati.

Determinazione dello stato di acquisizione del data collector

Poiché i data collezioner sono la principale fonte di informazioni per Cloud Insights, è fondamentale assicurarsi che rimangano in uno stato di esecuzione.

Lo stato del data collector viene visualizzato nell'angolo in alto a destra di qualsiasi pagina asset come messaggio "Acquisited N minutes ago" (acquisito N minuti fa), dove N indica il tempo di acquisizione più recente del data collector dell'asset. Viene visualizzata anche la data e l'ora di acquisizione.

Facendo clic sul messaggio viene visualizzata una tabella con il nome del data collector, lo stato e l'ultimo tempo di acquisizione riuscito. Se si effettua l'accesso come amministratore, facendo clic sul collegamento relativo al nome del data collector nella tabella si accede alla pagina dei dettagli del data collector.

Gestione dei data collettori configurati

La pagina dei Data Collector installati consente di accedere ai data collector configurati per Cloud Insights. È possibile utilizzare questa pagina per modificare i data collettori esistenti.

Fasi

1. Nel menu Cloud Insights, fare clic su **osservabilità > Collector**

   Viene visualizzata la schermata Available Data Collector (raccolta dati disponibili).

2. Fare clic su **Installed Data Collector** (raccolta dati installati)

   Viene visualizzato un elenco di tutti i Data Collector installati. L'elenco fornisce il nome del collector, lo stato, l'indirizzo IP a cui il collector accede e l'ultima volta che i dati sono stati acquisiti da un dispositivo. Le azioni che è possibile eseguire in questa schermata includono:

   - Polling del controllo
   - Modificare le credenziali del data collector
   - Clonare i data collettori

Controllo del polling di Data Collector

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

Fasi

1. Nel menu Cloud Insights, fare clic su **osservabilità > Collector**
2. Fare clic su **Installed Data Collector** (raccolta dati installati)
3. Selezionare la casella di controllo a sinistra del Data Collector che si desidera modificare
4. Fare clic su **azioni in blocco** e selezionare l'azione di polling che si desidera eseguire.

   Le azioni bulk possono essere eseguite simultaneamente su più Data Collector. Selezionare i data

collettori e scegliere l'azione da eseguire dal menu **azione in blocco**.

Modifica delle informazioni di data collector

È possibile modificare le informazioni di configurazione del data collector esistente.

Per modificare un singolo data collector:

1. Nel menu Cloud Insights, fare clic su **osservabilità > Collector** per aprire l'elenco dei Data Collector installati.
2. Nel menu delle opzioni a destra del data collector che si desidera modificare, fare clic su **Edit** (Modifica).

   Viene visualizzata la finestra di dialogo Edit Collector (Modifica modulo di raccolta).

3. Inserire le modifiche e fare clic su **Test Configuration** (verifica configurazione) per verificare la nuova configurazione oppure fare clic su **Save** (Salva) per salvare la configurazione.

È inoltre possibile modificare più data raccoglitori:

1. Selezionare la casella di controllo a sinistra di ciascun data collector che si desidera modificare.
2. Fare clic sul pulsante **azioni in blocco** e scegliere **Modifica** per aprire la finestra di dialogo Modifica raccolta dati.
3. Modificare i campi come indicato sopra.

   > I data raccoglitori selezionati devono essere dello stesso fornitore e modello e risiedere nella stessa unità di acquisizione.

   Quando si modificano più data collector, il campo Data Collector Name (Nome Data Collector) mostra "Mixed" (misto) e non può essere modificato. Altri campi, come nome utente e password, mostrano "Mixed" e possono essere modificati. I campi che condividono lo stesso valore tra i data collettori selezionati mostrano i valori correnti e possono essere modificati.

   Quando si modificano più data colleziones, il pulsante **Test Configuration** non è disponibile.

Cloning data raccoglitori

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. Nel menu Cloud Insights, fare clic su **osservabilità > Collector**.
2. Fare clic su **Installed Data Collector** (raccolta dati installati).
3. Fare clic sulla casella di controllo a sinistra del data collector che si desidera copiare.
4. Nel menu delle opzioni a destra del data collector selezionato, fare clic su **Clone**.

   Viene visualizzata la finestra di dialogo Clone Data Collector.

5. Inserire nuove informazioni nei campi obbligatori.
6. Fare clic su **Save** (Salva).

Al termine

L'operazione di clonazione copia tutti gli altri attributi e impostazioni per creare il nuovo data collector.

Esecuzione di azioni in blocco sui data collettori

È possibile modificare contemporaneamente alcune informazioni per più data collezions. Questa funzione consente di avviare un polling, posticipare il polling e riprendere il polling su più data raccoglitori. Inoltre, è possibile eliminare più data raccoglitori.

Fasi

1. Nel menu Cloud Insights, fare clic su **osservabilità > Collector**
2. Fare clic su **Installed Data Collector** (raccolta dati installati)
3. Fare clic sulla casella di controllo a sinistra dei raccoglitori di dati che si desidera modificare.
4. Nel menu delle opzioni a destra, fare clic sull'opzione che si desidera eseguire.

Al termine

L'operazione selezionata viene eseguita sui data colleziones. Quando si sceglie di eliminare i data colleziones, viene visualizzata una finestra di dialogo che richiede di conformare l'azione.

Ricerca di un data collector guasto

Se un data collector presenta un messaggio di errore e un impatto alto o medio, è necessario ricercare il problema utilizzando la pagina di riepilogo del data collector con le relative informazioni collegate.

Attenersi alla seguente procedura per determinare la causa dei dati non riusciti. I messaggi di errore di Data Collector vengono visualizzati nel menu **Admin** e nella pagina **Installed Data Collector**.

Fasi

1. Fare clic su **Admin** > **Data Collector** > **Installed Data Collector**.
2. Fare clic sul Linked Name (Nome collegato) del data collector in errore per aprire la pagina Summary (Riepilogo).
3. Nella pagina Summary (Riepilogo), consultare l'area Comments (commenti) per leggere eventuali note lasciate da un altro tecnico che potrebbe anche esaminare questo guasto.
4. Annotare eventuali messaggi relativi alle prestazioni.
5. Spostare il puntatore del mouse sui segmenti del grafico della cronologia degli eventi per visualizzare ulteriori informazioni.
6. Selezionare un messaggio di errore per un dispositivo e visualizzato sotto la cronologia degli eventi, 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 dispositivi segnalati da questo Data Collector, è possibile filtrare l'elenco in modo da visualizzare solo i dispositivi di interesse ed è possibile fare clic sul collegamento **Nome** di un dispositivo per visualizzare la pagina delle risorse per tale dispositivo.
8. Quando si torna alla pagina di riepilogo del data collector, controllare l'area **Show Recent Changes** (Mostra modifiche recenti) nella parte inferiore della pagina per verificare se le modifiche recenti potrebbero aver causato il problema.

Importazione dalla galleria Dashboard

Cloud Insights offre una serie di dashboard consigliati per fornire informazioni aziendali sui dati. Ogni dashboard contiene widget progettati per rispondere a una particolare domanda o risolvere un particolare problema relativo ai dati attualmente raccolti nell'ambiente.

Per importare una dashboard dalla galleria, procedere come segue:

1. Selezionare **Dashboard > Dashboard**
2. Fare clic su **+da Gallery**

   Viene visualizzato un elenco di **Dashboard raccomandati**. Ogni dashboard viene chiamata con una domanda specifica che la dashboard può aiutarti a risolvere. Sono disponibili dashboard per rispondere a domande relative a diversi tipi di oggetti, tra cui AWS, NetApp, Storage, VMware, e altri

3. Selezionare una o più dashboard dall'elenco e fare clic su **Aggiungi dashboard**. Queste dashboard vengono ora visualizzate nell'elenco della dashboard.

Oltre ai dashboard consigliati, è anche possibile scegliere di importare **Dashboard aggiuntivi** che non sono rilevanti per i dati correnti. Ad esempio, se non si dispone di data raccoglitori di storage attualmente installati ma si prevede di configurarne alcuni in futuro, è comunque possibile scegliere di importare i dashboard relativi allo storage. Queste dashboard saranno disponibili per la visualizzazione ma potrebbero non mostrare alcun dato rilevante fino a quando non viene configurato almeno un data collector per lo storage.

L'importazione dalla galleria del dashboard è disponibile per gli utenti con ruolo di amministratore o di proprietario dell'account.

Account utente e ruoli

Cloud Insights offre fino a quattro ruoli di account utente: Proprietario dell'account, amministratore, utente e ospite. A ciascun account vengono assegnati livelli di autorizzazione specifici, come indicato nella tabella seguente. Gli utenti lo sono "invitato" A Cloud Insights e assegnato un ruolo specifico, oppure può accedere tramite "Autorizzazione Single Sign-on (SSO)" con un ruolo predefinito. L'autorizzazione SSO è disponibile come funzione nell'edizione Premium di Cloud Insights.

> Gli accessi utente nell'edizione federale di Cloud Insights sono limitati ai provider di identità configurati (con i rispettivi domini di posta elettronica specificati). Quando un nuovo utente viene invitato a un ambiente federale Cloud Insights, il relativo indirizzo e-mail deve corrispondere al dominio configurato per tale ambiente.

Livelli di autorizzazione

Per creare o modificare gli account utente, si utilizza un account con privilegi di amministratore. A ciascun account utente viene assegnato un ruolo per ciascuna funzione di Cloud Insights a partire dai seguenti livelli di autorizzazione.

Ruolo	Osservabilità	Sicurezza del carico di lavoro	Creazione di report
Proprietario dell'account	Può modificare le sottoscrizioni, visualizzare le informazioni di fatturazione e utilizzo ed eseguire tutte le funzioni di amministratore per Observability, Security e Reporting. I proprietari possono anche invitare e gestire gli utenti, oltre a gestire le impostazioni di autenticazione SSO e federazione di identità. Il primo account Owner viene creato quando ti registri a Cloud Insights. Si consiglia vivamente di avere almeno due account Owner per ogni ambiente Cloud Insights.		
Amministratore	Può eseguire tutte le funzioni di osservazione, tutte le funzioni dell'utente, nonché la gestione dei data raccoglitori, dei token API di osservazione e delle notifiche. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di osservabilità.	È in grado di eseguire tutte le funzioni di sicurezza, incluse quelle per Avvisi, analisi, raccolta dati, policy di risposta automatizzate e token API per la sicurezza. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza.	Può eseguire tutte le funzioni utente/autore, inclusa la gestione dei token API di reporting, nonché tutte le attività amministrative, come la configurazione dei report, l'arresto e il riavvio delle attività di reporting. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di reporting.
Utente	Può visualizzare e modificare dashboard, query, avvisi, annotazioni, regole di annotazione, e le applicazioni, oltre a gestire la risoluzione dei dispositivi.	Consente di visualizzare e gestire gli avvisi e visualizzare le analisi. Il ruolo dell'utente può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente e gestire la limitazione dell'accesso degli utenti.	Può eseguire tutte le funzioni Guest/Consumer, nonché creare e gestire report e dashboard.
Ospite	Dispone di accesso in sola lettura a pagine di risorse, dashboard, avvisi e può visualizzare ed eseguire query.	Consente di visualizzare avvisi e analisi. Il ruolo ospite non può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente o limitare l'accesso dell'utente.	Consente di visualizzare, pianificare ed eseguire report e di impostare preferenze personali, ad esempio per lingue e fusi orari. Gli utenti guest/consumer non possono creare report o eseguire attività amministrative.

La procedura consigliata consiste nel limitare il numero di utenti con autorizzazioni di amministratore. Il maggior numero di account deve essere costituito da account utente o guest.

Autorizzazioni Cloud Insights per ruolo utente

La tabella seguente mostra le autorizzazioni Cloud Insights concesse a ciascun ruolo utente.

Funzione	Amministratore/Proprietario dell'account	Utente	Ospite

Unità di acquisizione: Aggiungi/Modifica/Elimina	Y	N	N
Avvisi*: Creazione/modifica/eliminazione	Y	Y	N
Avvisi*: Visualizzazione	Y	Y	Y
Regole di annotazione: Crea/Esegui/Modifica/Elimina	Y	Y	N
Annotazioni: Crea/Modifica/Assegna/Visualizza/Rimuovi/Elimina	Y	Y	N
Accesso API*: Creazione/ridenominazione/disattivazione/revoca	Y	N	N
Applicazioni: Creare/visualizzare/modificare/eliminare	Y	Y	N
Pagine di risorse: Modifica	Y	Y	N
Pagine di risorse: Visualizza	Y	Y	Y
Audit: Vista	Y	N	N
Costo del cloud	Y	N	N
Sicurezza	Y	N	N
Dashboard: Creare/modificare/eliminare	Y	Y	N
Dashboard: Vista	Y	Y	Y
Data Collector: Add/Modify/poll/Delete (Aggiungi/Modifica/polling/Elimina)	Y	N	N
Notifiche: Visualizzazione	Y	Y	Y
Notifiche: Modifica	Y	N	N
Query: Crea/Modifica/Elimina	Y	Y	N
Query: Visualizza/Esegui	Y	Y	Y
Risoluzione del dispositivo	Y	Y	N
Report*: Visualizza/Esegui	Y	Y	Y

Report*: Crea/Modifica/Elimina/Pianifica	Y	Y	N
Iscrizione: Visualizza/Modifica	Y	N	N
User Management (Gestione utenti): Invita/Aggiungi/Modifica/Disattiva	Y	N	N

*Richiede Premium Edition

Creazione di account invitando gli utenti

La creazione di un nuovo account utente avviene tramite Cloud Central. Un utente può rispondere all'invito inviato tramite e-mail, ma se non dispone di un account con Cloud Central, deve iscriversi a Cloud Central per poter accettare l'invito.

Prima di iniziare

- Il nome utente è l'indirizzo e-mail dell'invito.
- Comprendere i ruoli utente che verranno assegnati.
- Le password vengono definite dall'utente durante il processo di registrazione.

Fasi

1. Accedere a Cloud Insights
2. Nel menu, fare clic su **Admin > User Management**

   Viene visualizzata la schermata User Management (Gestione utenti). La schermata contiene un elenco di tutti gli account del sistema.

3. Fare clic su **+ User**

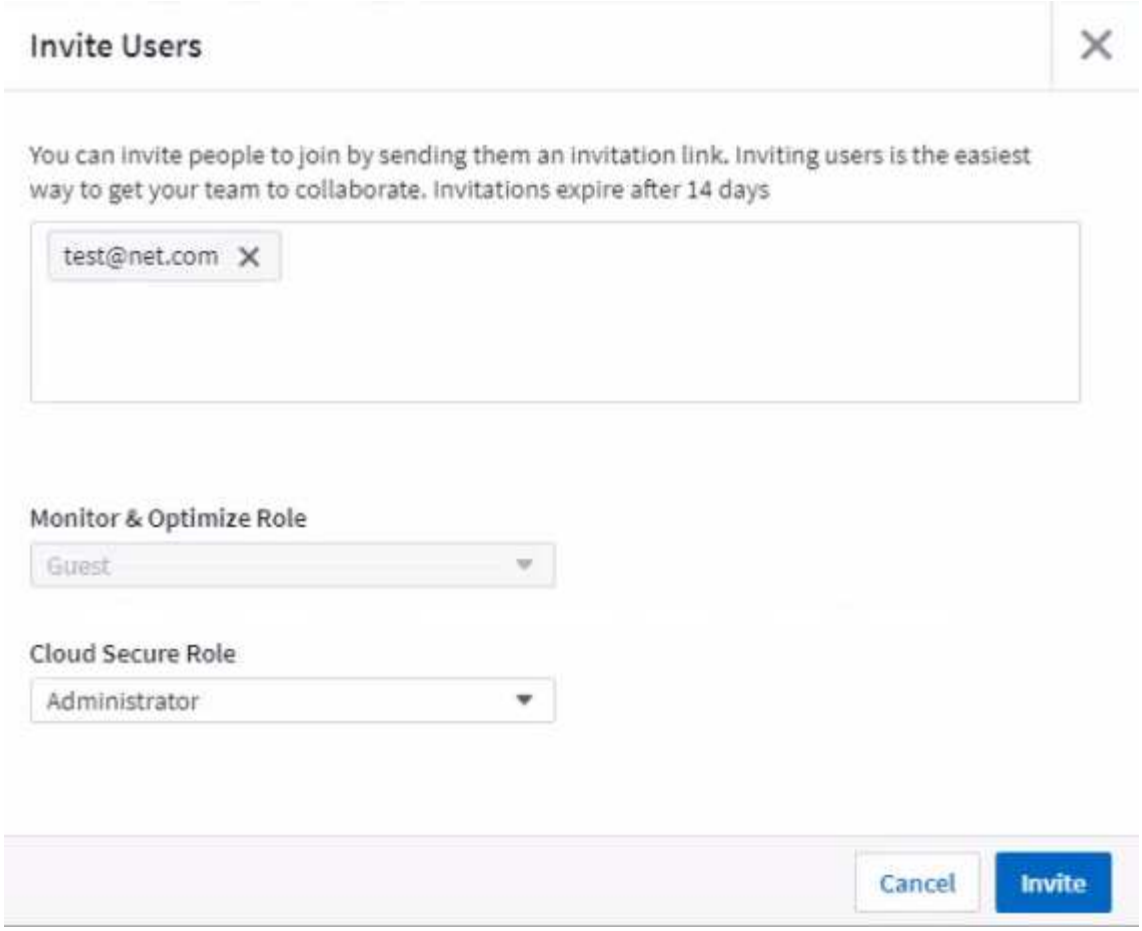
   Viene visualizzata la schermata **invita utente**.

4. Inserire un indirizzo e-mail o più indirizzi per gli inviti.

   Nota: quando inserisci più indirizzi, questi vengono tutti creati con lo stesso ruolo. È possibile impostare solo più utenti sullo stesso ruolo.

5. Selezionare il ruolo dell'utente per ciascuna funzione di Cloud Insights.

   Le funzionalità e i ruoli tra cui scegliere dipendono dalle funzioni a cui si ha accesso nel proprio ruolo di amministratore. Ad esempio, se si dispone del ruolo di amministratore solo per Reporting, sarà possibile assegnare gli utenti a qualsiasi ruolo in Reporting, ma non sarà possibile assegnare ruoli per Observability o Security.



6. Fare clic su **invita**

   L'invito viene inviato all'utente. Gli utenti avranno a disposizione 14 giorni per accettare l'invito. Una volta accettato l'invito, l'utente viene portato al NetApp Cloud Portal, dove si iscriva utilizzando l'indirizzo e-mail dell'invito. Se dispone di un account per tale indirizzo e-mail, può semplicemente accedere e accedere al proprio ambiente Cloud Insights.

Modifica del ruolo di un utente esistente

Per modificare il ruolo di un utente esistente, incluso l'aggiunta come **proprietario di un account secondario**, attenersi alla seguente procedura.

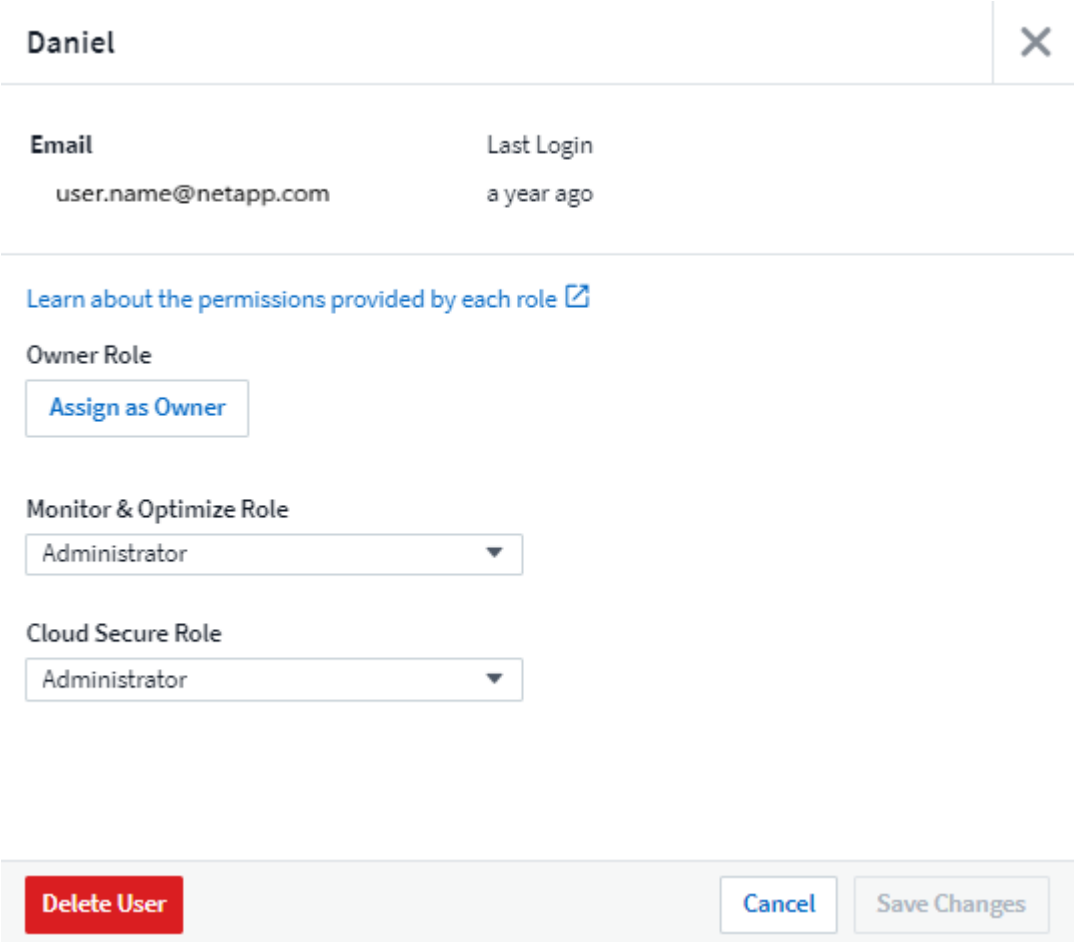
1. Fare clic su **Admin > User Management** (Amministrazione > Gestione utenti). Viene visualizzato un elenco di tutti gli account del sistema.
2. Fare clic sul nome utente dell'account che si desidera modificare.
3. Modificare il ruolo dell'utente in ogni set di funzionalità Cloud Insights in base alle necessità.
4. Fare clic su *Save Changes* (Salva modifiche).

Per assegnare un account Owner secondario

Per poter assegnare il ruolo di proprietario dell'account a un altro utente, devi essere connesso come proprietario dell'account per l'osservabilità.

1. Fare clic su **Admin > User Management** (Amministrazione > Gestione utenti).

2. Fare clic sul nome utente dell'account che si desidera modificare.
3. Nella finestra di dialogo User (utente), fare clic su **Assign as Owner** (Assegna come proprietario).
4. Salvare le modifiche.



Puoi avere tutti i proprietari di account che desideri, ma la Best practice consiste nel limitare il ruolo del proprietario solo a selezionare le persone.

Eliminazione di utenti

Un utente con il ruolo di amministratore può eliminare un utente (ad esempio, qualcuno che non è più presente nella società) facendo clic sul nome dell'utente e facendo clic su *Delete User* (Elimina utente) nella finestra di dialogo. L'utente verrà rimosso dall'ambiente Cloud Insights.

Tenere presente che eventuali dashboard, query e così via creati dall'utente rimarranno disponibili nell'ambiente Cloud Insights anche dopo la rimozione dell'utente.

Single Sign-on (SSO) e Identity Federation

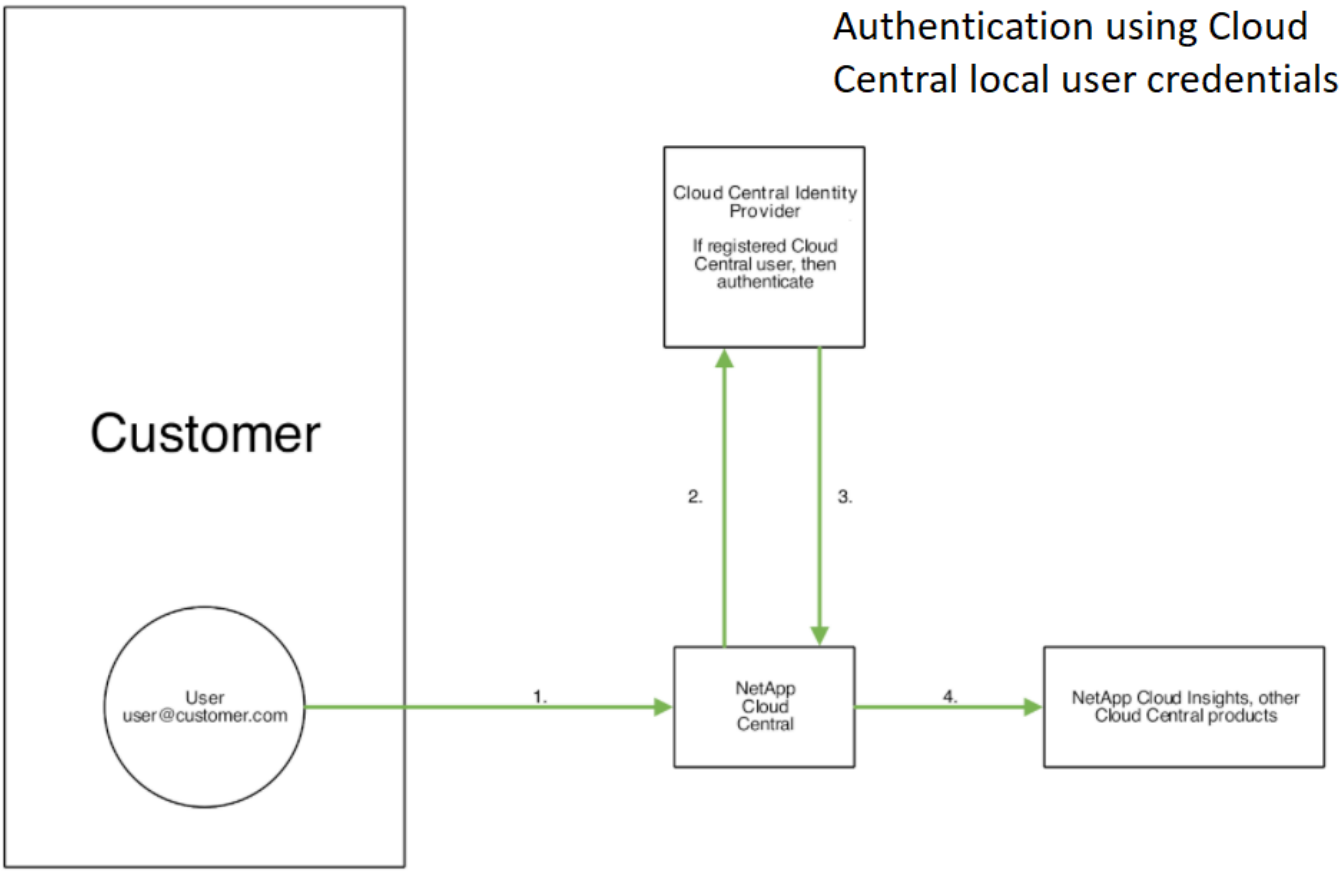
Abilitazione della federazione di identità per SSO in Cloud Insights

Con Identity Federation:

- L'autenticazione viene delegata al sistema di gestione delle identità del cliente, utilizzando le credenziali del cliente dalla directory aziendale e le policy di automazione come l'autenticazione multifattore (MFA).

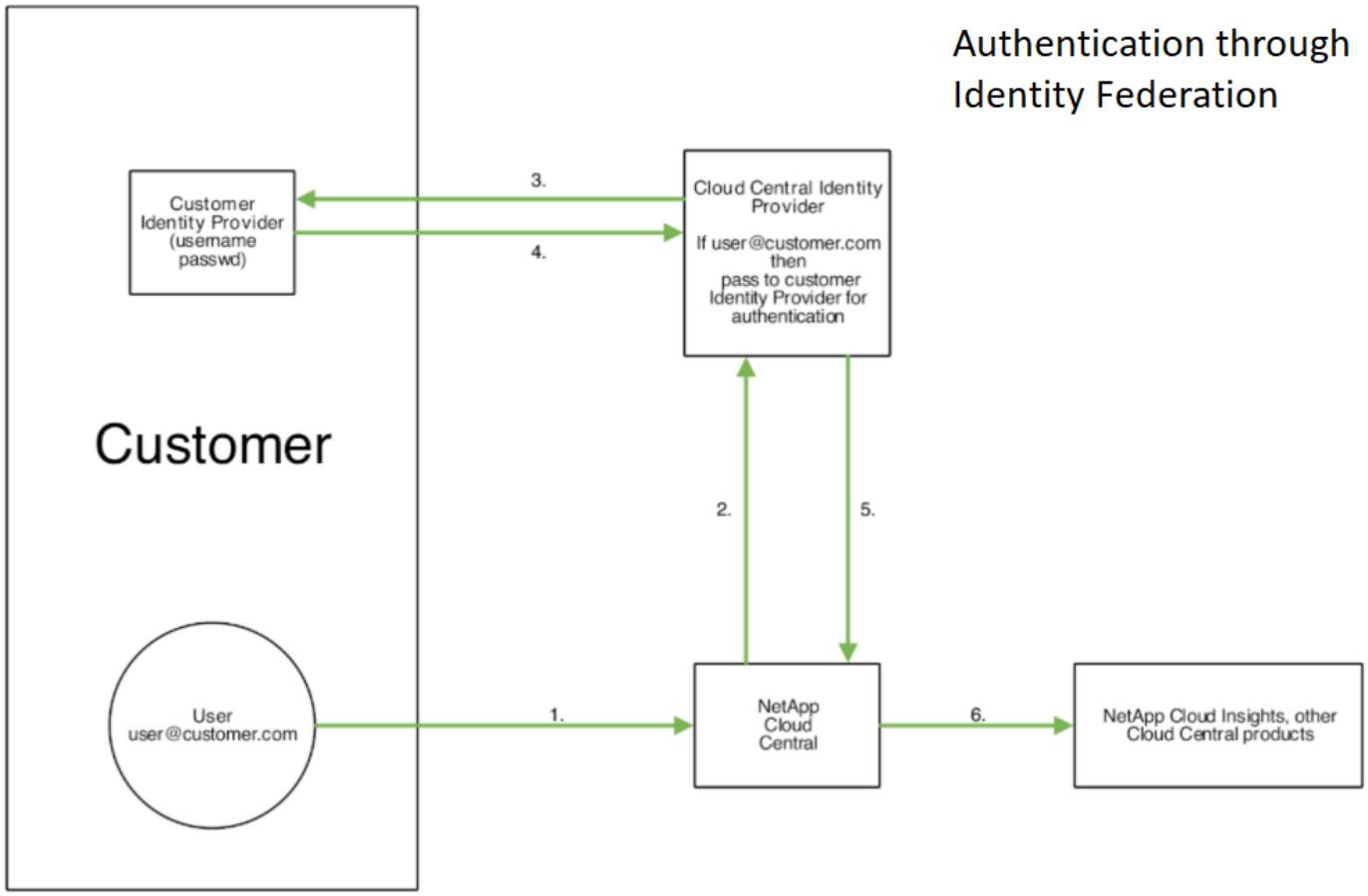
- Gli utenti accedono una volta a tutti i servizi cloud di NetApp (Single Sign-on).

Gli account utente sono gestiti in NetApp Cloud Central per tutti i servizi cloud. Per impostazione predefinita, l'autenticazione viene eseguita utilizzando il profilo utente locale di Cloud Central. Di seguito è riportata una panoramica semplificata di tale processo:



Tuttavia, alcuni clienti desiderano utilizzare il proprio provider di identità per autenticare i propri utenti per Cloud Insights e gli altri servizi NetApp Cloud Central. Con Identity Federation, gli account NetApp Cloud Central vengono autenticati utilizzando le credenziali della directory aziendale.

Di seguito viene riportato un esempio semplificato di tale processo:



Nel diagramma precedente, quando un utente accede a Cloud Insights, tale utente viene indirizzato al sistema di gestione delle identità del cliente per l'autenticazione. Una volta autenticato l'account, l'utente viene indirizzato all'URL del tenant Cloud Insights.

Cloud Central utilizza Auth0 per implementare Identity Federation e integrarsi con servizi come Active Directory Federation Services (ADFS) e Microsoft Azure Active Directory (ad). Per ulteriori informazioni sull'installazione e la configurazione di Identity Federation, consultare la documentazione di Cloud Central all'indirizzo "Federazione delle identità".

È importante comprendere che la modifica della federazione delle identità in Cloud Central si applicherà non solo a Cloud Insights, ma a tutti i servizi cloud NetApp. Il cliente deve discutere di questo cambiamento con il team NetApp di ciascun prodotto Cloud Central di sua proprietà per assicurarsi che la configurazione che sta utilizzando funzioni con Identity Federation o se è necessario apportare modifiche a qualsiasi account. Il cliente dovrà coinvolgere anche il proprio team SSO interno nella modifica alla federazione delle identità.

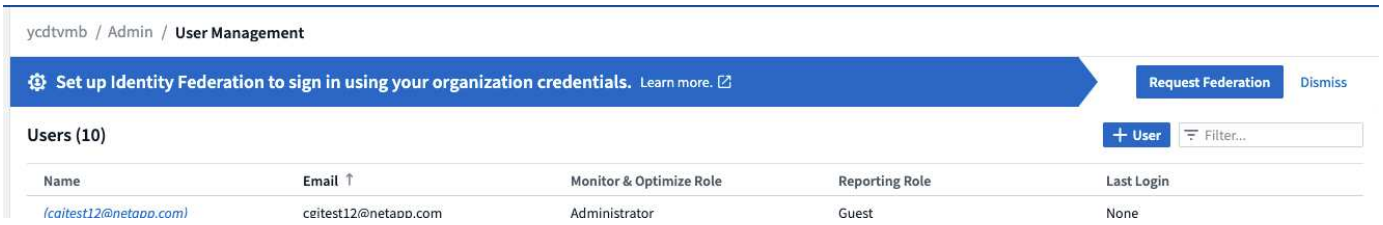
È inoltre importante comprendere che, una volta attivata la federazione delle identità, qualsiasi modifica apportata al provider di identità dell'azienda (ad esempio, il passaggio da SAML a Microsoft ad) richiederà probabilmente risoluzione dei problemi, modifiche e attenzione in Cloud Central per aggiornare i profili degli utenti.

Provisioning automatico utente Single Sign-on (SSO)

Oltre a invitare gli utenti, gli amministratori possono abilitare l'accesso a Cloud Insights per l'accesso a **Single Sign-on (SSO) User Auto-Provisioning** per tutti gli utenti del proprio dominio aziendale, senza doverli invitare singolarmente. Con SSO attivato, qualsiasi utente con lo stesso indirizzo e-mail di dominio può accedere a Cloud Insights utilizzando le proprie credenziali aziendali.

Provisioning automatico utente SSO è disponibile in Cloud Insights Premium Edition e deve essere configurato prima di poter essere abilitato per Cloud Insights. La configurazione di Auto-Provisining utente SSO include "Federazione delle identità" Tramite NetApp Cloud Central come descritto nella sezione precedente. Federation consente agli utenti single sign-on di accedere ai tuoi account NetApp Cloud Central utilizzando le credenziali della tua directory aziendale, utilizzando standard aperti come Security Assertion Markup Language 2.0 (SAML) e OpenID Connect (OIDC).

Per configurare *SSO User Auto-Provisioning*, nella pagina **Admin > User Management**, fare clic sul pulsante **Request Federation**. Una volta configurato, gli amministratori possono abilitare l'accesso utente SSO. Quando un amministratore abilita *SSO User Auto-Provisioning*, sceglie un ruolo predefinito per tutti gli utenti SSO (come Guest o User). Gli utenti che accedono tramite SSO avranno questo ruolo predefinito.



A volte, un amministratore desidera promuovere un singolo utente al di fuori del ruolo SSO predefinito (ad esempio, per renderlo un amministratore). Per eseguire questa operazione, fare clic sul menu a destra della pagina **Admin > User Management** e selezionare *Assign role*. Gli utenti a cui viene assegnato un ruolo esplicito in questo modo continuano ad avere accesso a Cloud Insights anche se il provisioning automatico dell'utente SSO viene successivamente disattivato.

Se l'utente non richiede più il ruolo di livello elevato, fare clic sul menu per *Remove User* (Rimuovi utente). L'utente verrà rimosso dall'elenco. Se l'opzione *provisioning automatico utente SSO* è attivata, l'utente può continuare l'accesso a Cloud Insights tramite SSO, con il ruolo predefinito.

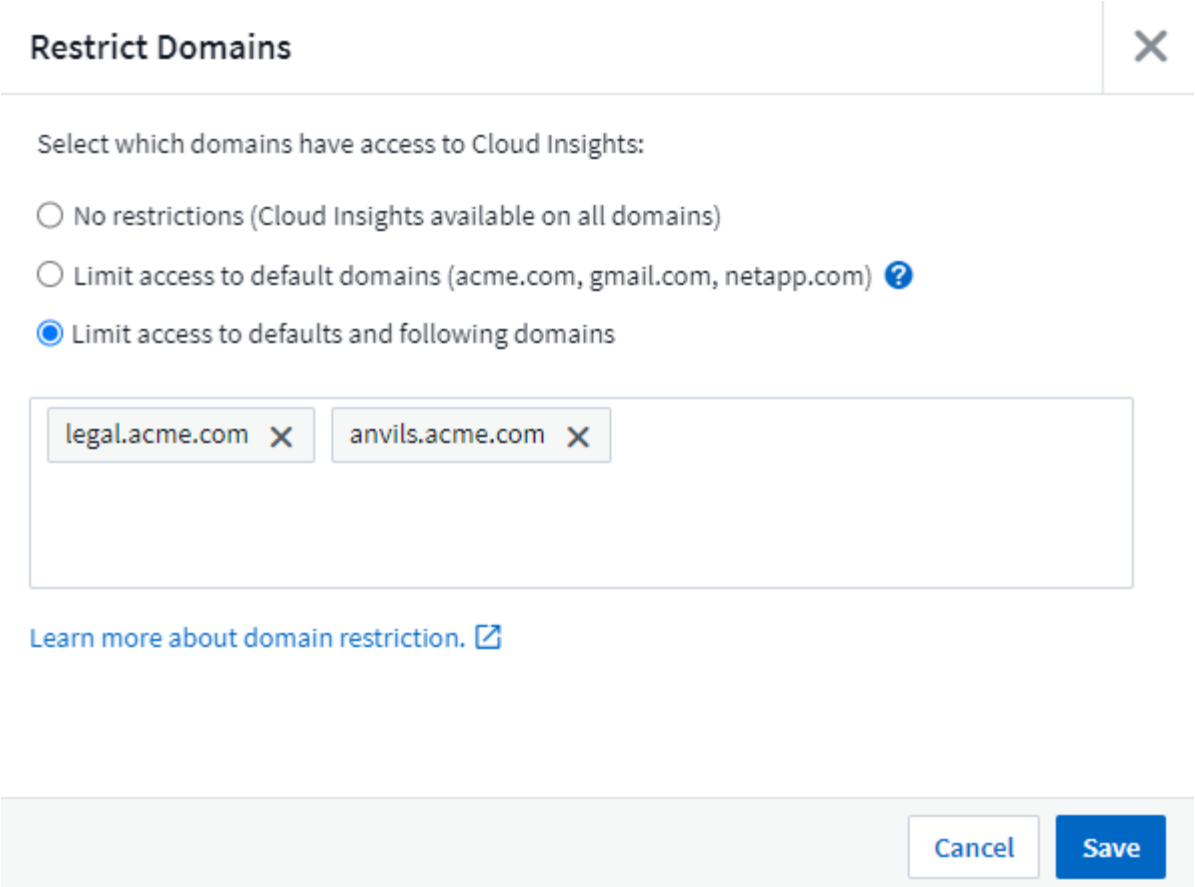
È possibile scegliere di nascondere gli utenti SSO deselezionando la casella di controllo **Show SSO Users** (Mostra utenti SSO).

Tuttavia, non attivare *SSO User Auto-Provisioning* se una delle seguenti condizioni è vera:

- La tua organizzazione dispone di più tenant Cloud Insights
- L'organizzazione non desidera che tutti gli utenti del dominio federato dispongano di un certo livello di accesso automatico al tenant Cloud Insights. *A questo punto, non abbiamo la possibilità di utilizzare i gruppi per controllare l'accesso ai ruoli con questa opzione*.

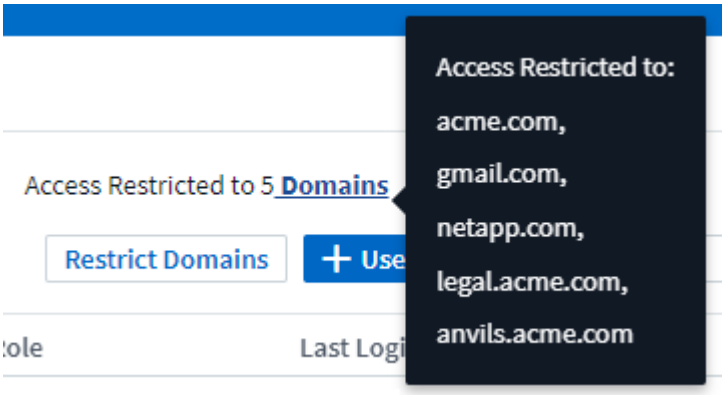
Limitazione dell'accesso per dominio

Cloud Insights può limitare l'accesso degli utenti solo ai domini specificati. Nella pagina **Amministrazione > Gestione utenti**, selezionare "limita domini".



Vengono visualizzate le seguenti opzioni:

- Nessuna restrizione: Cloud Insights resta accessibile agli utenti indipendentemente dal loro dominio.
- Limita accesso ai domini predefiniti: I domini predefiniti sono quelli utilizzati dai proprietari degli account dell'ambiente Cloud Insights. Questi domini sono sempre accessibili.
- Limitare l'accesso ai valori predefiniti e ai domini specificati. Elencare tutti i domini ai quali si desidera accedere all'ambiente Cloud Insights, oltre ai domini predefiniti.



Elenco di data collector Cloud Insights

Cloud Insights supporta una vasta gamma di data collector di molti vendor e servizi.

I Data Collector sono classificati in base ai seguenti tipi:

- Infrastruttura: Acquisita da dispositivi vendor come storage array, switch, hypervisor o dispositivi di backup.
- Servizio: Acquistato da servizi come Kubernetes o Docker. Chiamato anche *integrazione*.

Elenco alfabetico dei Data Collector supportati da Cloud Insights:

Data Collector	Tipo
"Amazon EC2 ed EBS"	Infrastruttura
"AWS S3 come storage"	Infrastruttura
"Amazon FSX per NetApp ONTAP"	Infrastruttura
"Apache"	Servizio
"Azure NetApp Files"	Infrastruttura
"Macchine virtuali Azure e VHD"	Infrastruttura
"Brocade Network Advisor (BNA)"	Infrastruttura
"Switch Fibre Channel Brocade"	Infrastruttura
"Brocade FOS REST "	Infrastruttura
"Switch Cisco MDS Fabric"	Infrastruttura
"Console"	Servizio
"Couchbase"	Servizio
"Database dei CouchDB"	Servizio
"SmartFiles di Cohesity"	Infrastruttura
"Dominio dati Dell EMC"	Infrastruttura
"ECS Dell EMC"	Infrastruttura
"Dell EMC PowerScale (in precedenza Isilon)"	Infrastruttura
"Dell EMC Isilon/PowerScale REST"	Infrastruttura
"Dell EMC PowerStore"	Infrastruttura
"Recoverpoint Dell EMC"	Infrastruttura
"Dell EMC ScaleIO/PowerFlex "	Infrastruttura
"Dell EMC Unity"	Infrastruttura
"Dell EMC Unisphere REST (RIPOSO unisfer"	Infrastruttura
"Famiglia di dispositivi Dell EMC VMAX/PowerMax"	Infrastruttura
"Storage a blocchi Dell EMC VNX"	Infrastruttura

Data Collector	Tipo
"File VNX Dell EMC"	Infrastruttura
"Dell EMC VNX Unified"	Infrastruttura
"Dell EMC VPLEX"	Infrastruttura
"Dell EMC XtremIO"	Infrastruttura
"Dell serie XC"	Infrastruttura
"Docker"	Servizio
"Elasticsearch"	Servizio
"Flink"	Servizio
"Fujitsu ETERNUS DX"	Infrastruttura
"Calcolo e storage Google"	Infrastruttura
"Hadoop"	Servizio
"HAProxy"	Servizio
"Hitachi Content Platform (HCP)"	Infrastruttura
"Suite di comandi Hitachi Vantara"	Infrastruttura
"Piattaforma NAS Hitachi Vantara"	Infrastruttura
"Hitachi Ops Center"	Infrastruttura
"Storage HP Enterprise Alletra 6000 (precedentemente agile)"	Infrastruttura
"Storage HP Enterprise Alletra 9000 / Primera (in precedenza 3PAR)"	Infrastruttura
"HP Enterprise Command View"	Infrastruttura
"Dispositivi Huawei OceanStor e Dorado"	Infrastruttura
"IBM Cleversafe"	Infrastruttura
"IBM CS Series"	Infrastruttura
"IBM PowerVM"	Infrastruttura
"IBM SAN Volume Controller (SVC)"	Infrastruttura
"IBM System Storage serie DS8000"	Infrastruttura
"IBM XIV e A9000 Storages"	Infrastruttura
"Infinidat InfiniBox"	Infrastruttura
"Java"	Servizio
"Kafka"	Servizio
"Kapacitor"	Servizio
"Kibana"	Servizio
"Kubernetes"	Servizio

Data Collector	Tipo
"Lenovo serie HX"	Infrastruttura
"Memcached"	Servizio
"Microsoft Azure NetApp Files"	Infrastruttura
"Microsoft Hyper-V."	Infrastruttura
"MongoDB"	Servizio
"MySQL"	Servizio
"NetApp Cloud Volumes ONTAP"	Infrastruttura
"NetApp Cloud Volumes Services per AWS"	Infrastruttura
"Connessione cloud NetApp per ONTAP 9.9+"	Infrastruttura
"NetApp Data ONTAP 7-Mode"	Infrastruttura
"NetApp e-Series"	Infrastruttura
"Amazon FSX per NetApp ONTAP"	Infrastruttura
"Centro virtuale NetApp HCI"	Infrastruttura
"Software per la gestione dei dati NetApp ONTAP"	Infrastruttura
"NetApp ONTAP Select"	Infrastruttura
"Array all-flash NetApp SolidFire"	Infrastruttura
"NetApp StorageGRID"	Infrastruttura
"Netstat"	Servizio
"Nginx"	Servizio
"Nodo"	Servizio
"Nutanix serie NX"	Infrastruttura
"OpenStack"	Infrastruttura
"OpenZFS"	Servizio
"Appliance di storage Oracle ZFS"	Infrastruttura
"PostgreSQL"	Servizio
"Agente di puppet"	Servizio
"Pure Storage FlashArray"	Infrastruttura
"Virtualizzazione Red Hat"	Infrastruttura
"Redis"	Servizio
"RethinkDB"	Servizio
"RHEL CentOS"	Servizio
"Storage CDM Rubrik"	Infrastruttura
"Ubuntu Debian"	Servizio

Data Collector	Tipo
"VMware vSphere"	Infrastruttura
"Windows"	Servizio
"Zoosekeeper"	Servizio

Iscrizione a Cloud Insights

Per iniziare con Cloud Insights è sufficiente seguire tre semplici passaggi:

- Iscriviti per un account su **"NetApp BlueXP"** Per accedere a tutte le offerte cloud di NetApp.
- Registratevi per un **"prova gratuita"** Di Cloud Insights per esplorare le funzionalità disponibili.
- **Iscriviti** a Cloud Insights per un accesso continuo e ininterrotto ai tuoi dati tramite "Vendite NetApp" diretto o. "Mercato AWS".

Durante il processo di registrazione, è possibile scegliere la regione globale in cui ospitare l'ambiente Cloud Insights. Per ulteriori informazioni, leggi informazioni su Cloud Insights "Informazioni e Regione".

> Se non diversamente specificato, le informazioni contenute in questa pagina si applicano generalmente alle edizioni commerciali di Cloud Insights. L'edizione federale di Cloud Insights potrebbe non contenere alcune delle funzionalità descritte in questa pagina.

Per un confronto completo delle funzionalità disponibili nelle edizioni Cloud Insights di base e Premium, vedere "Prezzi Cloud Insights" pagina.

> Gli ambienti inattivi dell'edizione di base di Cloud Insights vengono cancellati e le relative risorse vengono recuperate. Un ambiente viene considerato inattivo se non vi sono attività dell'utente per 30 giorni consecutivi, o se non vi sono dati acquisiti per 7 giorni consecutivi. Cloud Insights invierà una notifica e fornirà un periodo di tolleranza di quattro giorni prima dell'eliminazione di un ambiente.

Quando si utilizza Cloud Insights, se viene visualizzata un'icona a forma di lucchetto , Significa che la funzione non è disponibile nell'edizione corrente o è disponibile in una forma limitata. Effettua l'aggiornamento per accedere completamente alla funzionalità.

Versione di prova

Quando ti iscrivi a Cloud Insights e il tuo ambiente è attivo, potrai accedere a una versione di prova gratuita di 30 giorni di Cloud Insights. Durante questa versione di prova potrai esplorare le funzionalità offerte da Cloud Insights nel tuo ambiente.

Puoi iscriverti a Cloud Insights in qualsiasi momento durante il periodo di prova. L'iscrizione a Cloud Insights garantisce un accesso ininterrotto ai tuoi dati e un'estensione **"supporto del prodotto"** opzioni.

Cloud Insights visualizza un banner quando la versione di prova gratuita è prossima alla fine All'interno di questo banner è presente un link *View Subscription*, che apre la pagina **Admin** → **Subscription**. Gli utenti non amministratori vedranno il banner ma non potranno accedere alla pagina di abbonamento.

> Se hai bisogno di ulteriore tempo per valutare Cloud Insights e la tua prova è impostata per scadere tra 4 giorni o meno, puoi estendere la prova per altri 30 giorni. Puoi estendere la prova una sola volta. Non è possibile prolungare la validità se la versione di prova è scaduta.

Prova con AWS Marketplace

Puoi anche iscriverti per una prova gratuita tramite AWS Marketplace. La versione di prova gratuita di AWS Marketplace ti offre l'accesso a Cloud Insights per un periodo di prova di 33 giorni e consente fino a 499 Unità

gestite (Mus).

Nota: Se si configurano più di 499 MU, si entra nello stato "violato". Mentre la versione di prova è in stato violato, l'accesso ad alcune funzionalità di Cloud Insights viene perso fino a quando la violazione non viene risolta, riducendo il numero di MU configurate o sottoscrivendo Cloud Insights.

La versione di prova gratuita di AWS Marketplace non può essere estesa. In qualsiasi momento durante la prova, puoi eseguire il downgrade a un abbonamento Cloud Insights edizione base o passare a un abbonamento Cloud Insights a pagamento visitando la pagina **Amministratore** → **abbonamento**.

Cosa fare se la versione di prova è scaduta?

Se la versione di prova gratuita è scaduta e non si è ancora abbonati a Cloud Insights, le funzionalità saranno limitate fino a quando non si effettua l'iscrizione.

Versioni di prova dei moduli

Presto disponibile!

> La versione di prova del modulo è considerata una funzionalità di anteprima ed è pertanto soggetta a modifiche.

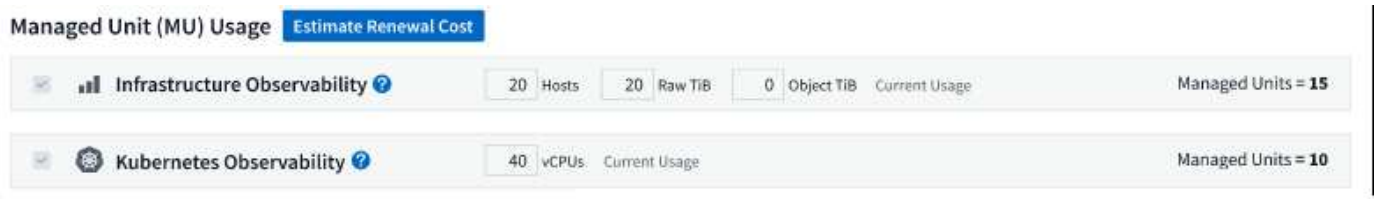
Oltre alla versione di prova iniziale di Cloud Insights, è possibile usufruire anche di **versioni di prova dei moduli**. Ad esempio, se sei già abbonato all'osservabilità dell'infrastruttura ma stai aggiungendo Kubernetes al tuo ambiente, potrai entrare automaticamente in una prova di 30 giorni dell'osservabilità Kubernetes, a partire da quando installi l'operatore di monitoring NetApp Kubernetes. Ti verrà addebitato solo l'utilizzo delle unità gestite da Kubernetes Observability al termine del periodo di prova.

> Tenere presente che dopo il periodo di prova verrà addebitato l'utilizzo di nuove unità gestite (MU), quindi assicurarsi di pianificare di conseguenza. Al termine del periodo di prova del modulo, verrà visualizzato un messaggio di notifica se sarà necessario aggiungere altre MU per evitare l'interruzione del servizio.

È possibile monitorare l'utilizzo dell'unità gestita nella pagina **Admin > Subscription** della scheda **Usage**.

Generatore di stime

Durante una prova del modulo, non viene modificato l'utilizzo delle UM per le risorse consumate per il modulo, ma potete aprire il **Tool** (nella scheda *Summary*) per vedere come le MU saranno addebitate dopo la prova, così come giocare con gli scenari "What if" con il numero di MU che potreste avere bisogno in futuro. Azzerare i numeri uscendo dal calcolatore.



Selezionare la casella di controllo accanto a un modulo per aggiungere o rimuovere le UM dell'intero modulo dal costo stimato.

Lo strumento di stima consente inoltre di vedere in che modo i numeri si accumulano per un Add on (Aggiungi), in cui si mantiene il periodo di abbonamento corrente e si aumenta il numero di unità gestite concesse in licenza, o per un'opzione Renew (Rinnova) per un abbonamento di rinnovo che si desidera acquistare al momento dell'abbonamento corrente termine terminato.

Si noti che i clienti hanno diritto a una versione di prova del modulo una sola volta per abbonamento.

Opzioni di abbonamento

Per iscriverti, vai a **Admin** → **Subscription**. Oltre ai pulsanti **Subscribe**, potrai visualizzare i data collezioner installati e calcolare i prezzi stimati. Per un ambiente tipico, fare clic sul pulsante self-service AWS Marketplace. Se il tuo ambiente include o prevede di includere 1,000 o più unità gestite, sei idoneo per il Volume Pricing.

Prezzi

Il prezzo di Cloud Insights è pari a **unità gestita**. L'utilizzo delle unità gestite viene calcolato in base al numero di **host o macchine virtuali** e alla quantità di **capacità non formattata** gestita nell'ambiente dell'infrastruttura.

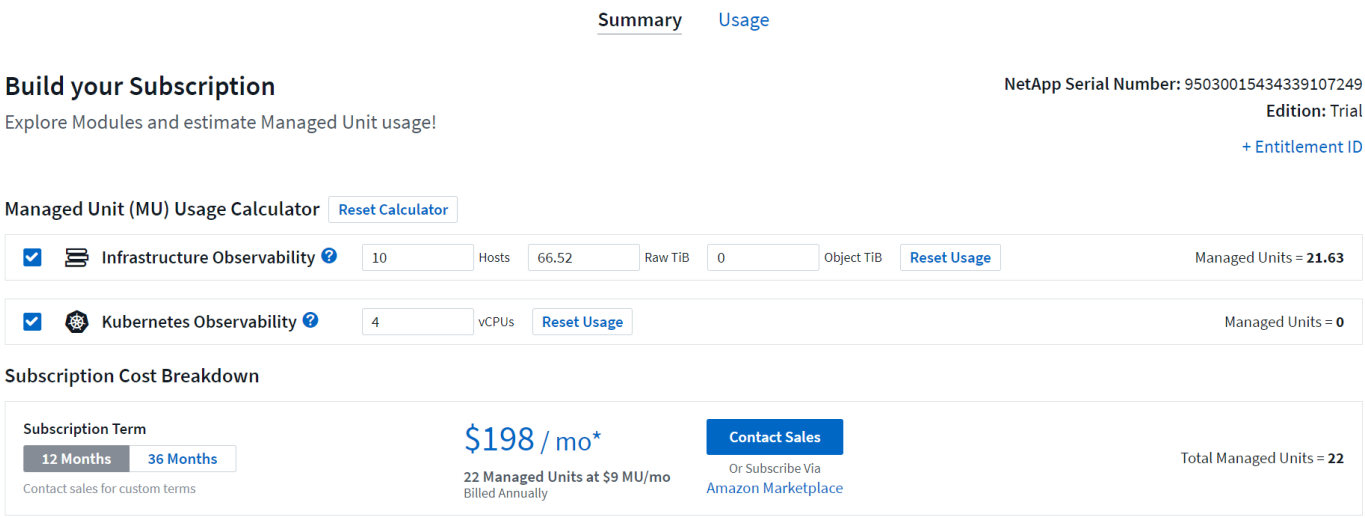
- 1 unità gestita = 2 host (qualsiasi macchina virtuale o fisica)
- 1 unità gestita = 4 TIB di capacità non formattata di dischi fisici o virtuali
- 1 unità gestita = 40 TiB di capacità non formattata dello storage secondario selezionato: AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik.
- 1 unità gestita = 4 vCPU di Kuberentes

Se il tuo ambiente include o prevede di includere 1,000 o più unità gestite, sei idoneo per **Volume Pricing** e ti verrà richiesto di contattare NetApp Sales per iscriverti. Vedere di seguito per ulteriori dettagli.

Stima del costo dell'abbonamento

I calcolatori degli abbonamenti consentono di stimare il costo dell'abbonamento a Cloud Insights in base al numero di unità gestite necessarie. I valori correnti sono precompilati e puoi modificarli per aiutarti nella pianificazione della crescita futura stimata. È possibile regolare i valori per Infrastructure (infrastruttura), Kubernetes (Kubernetes) o entrambi.

Il costo di listino stimato cambierà in base alla durata dell'abbonamento.
NOTA: I calcolatori sono solo a scopo di stima. Il tuo prezzo esatto verrà impostato al momento dell'iscrizione.



Come posso iscrivermi?

Se il numero di unità gestite è inferiore a 1,000, puoi iscriverti tramite NetApp Sales, o. iscriviti in autonomia Tramite AWS Marketplace.

Iscriviti tramite NetApp Sales Direct

Se il numero di unità gestite previsto è 1,000 o superiore, fare clic su **"Contattare il reparto vendite"** Per iscriversi al NetApp Sales Team.

Devi fornire il tuo Cloud Insights **numero di serie** al tuo commerciale NetApp per poter applicare l'abbonamento a pagamento al tuo ambiente Cloud Insights. Il numero di serie identifica in modo univoco l'ambiente di prova di Cloud Insights e si trova nella pagina **Amministratore > abbonamento**.

Self-Subscribe through AWS Marketplace

> Per poter applicare un abbonamento AWS Marketplace all'account di prova Cloud Insights esistente, devi essere un proprietario o un amministratore dell'account. Inoltre, devi disporre di un account Amazon Web Services (AWS).

Facendo clic sul link Amazon Marketplace si apre AWS "Cloud Insights" pagina di iscrizione, in cui puoi completare l'abbonamento. Nota: I valori immessi nel calcolatore non vengono inseriti nella pagina di abbonamento AWS; in questa pagina sarà necessario immettere il numero totale di unità gestite.

Dopo aver inserito il numero totale di unità gestite e aver scelto un periodo di abbonamento di 12 mesi o 36 mesi, fare clic su **Configura account** per completare il processo di abbonamento.

Una volta completato il processo di abbonamento AWS, si torna all'ambiente Cloud Insights. In alternativa, se l'ambiente non è più attivo (ad esempio, l'utente si è disconnesso), verrà visualizzata la pagina di accesso a NetApp BlueXP. Quando accedi nuovamente a Cloud Insights, l'abbonamento sarà attivo.

Dopo aver fatto clic su **Configura il tuo account** nella pagina di AWS Marketplace, devi completare la procedura di abbonamento AWS entro un'ora. Se non viene completata entro un'ora, fare nuovamente clic su **Configura account** per completare il processo.

Se si verifica un problema e il processo di abbonamento non viene completato correttamente, il banner "versione di prova" verrà visualizzato quando si accede all'ambiente. In questo caso, è possibile accedere a **Admin > Subscription** e ripetere la procedura di abbonamento.

Visualizzare lo stato dell'abbonamento

Una volta attivato l'abbonamento, puoi visualizzare lo stato dell'abbonamento e l'utilizzo dell'unità gestita dalla pagina **Admin > Subscription**.

La scheda Subscription Summary (Riepilogo abbonamento) visualizza quanto segue:

- Edizione corrente
- Numero di serie dell'abbonamento
- Utilizzo corrente delle UM e "cosa succederebbe se?" stimatori dei costi
- Link per modificare l'abbonamento
- Viste dell'utilizzo dell'unità gestita

Visualizza la gestione dell'utilizzo

La scheda Usage Management (Gestione utilizzo) mostra una panoramica dell'utilizzo delle unità gestite e schede che suddividono il consumo delle unità gestite per collettore o cluster Kubernetes.

Il numero di unità gestite con capacità non formattate riflette la somma della capacità raw totale nell'ambiente e viene arrotondato all'unità gestita più vicina.

La somma delle unità gestite potrebbe differire leggermente dal conteggio dei Data Collector nella sezione di riepilogo. Questo perché i conteggi delle unità gestite vengono arrotondati all'unità gestita più vicina. La somma di questi numeri nell'elenco Data Collector (raccolta dati) potrebbe essere leggermente superiore a quella delle unità gestite totali nella sezione Status (Stato). La sezione riepilogativa indica il numero effettivo di unità gestite per l'abbonamento.

Nel caso in cui l'utilizzo sia quasi o superi l'importo sottoscritto, è possibile ridurre l'utilizzo eliminando i data collezioner o interrompendo il monitoraggio di Kubernetes Clusters. Eliminare una voce dall'elenco facendo clic sul menu "tre punti" e selezionando *Elimina*.

Cosa succede se si supera il proprio utilizzo?

Gli avvisi vengono visualizzati quando l'utilizzo dell'unità gestita supera il 80%, il 90% e il 100% dell'importo totale sottoscritto:

Quando l'utilizzo supera:	Questo accade / azione consigliata:
80%	Viene visualizzato un banner informativo. Non è necessaria alcuna azione.

90%	Viene visualizzato un banner di avviso. È possibile aumentare il numero di unità gestite sottoscritte.
100%	Viene visualizzato un banner di errore e le funzionalità saranno limitate fino a quando non si esegue una delle seguenti operazioni: * Rimuovi Data Collector in modo che l'utilizzo della tua unità gestita sia pari o inferiore all'importo sottoscritto * Modificare l'abbonamento per aumentare il numero di unità gestite sottoscritte

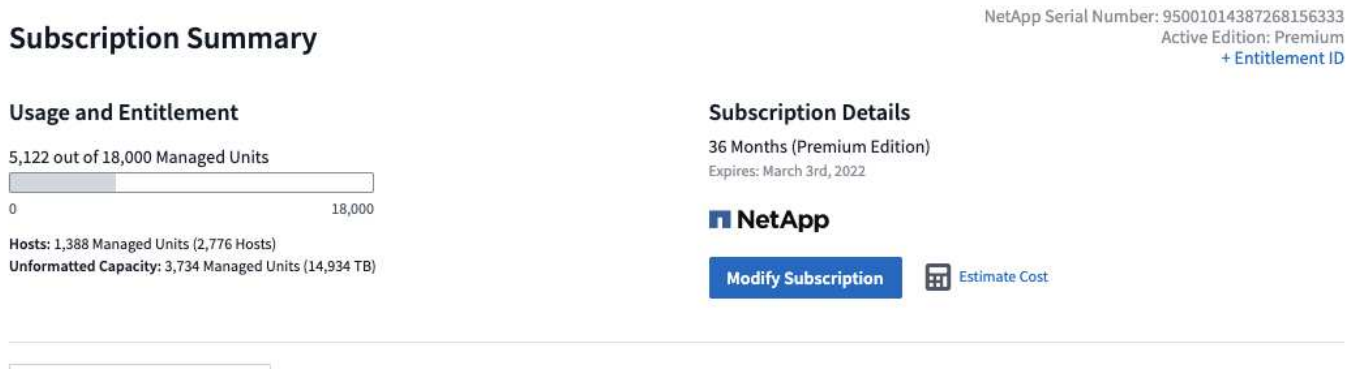
Iscriviti direttamente e ignora la versione di prova

Puoi anche iscriverti a Cloud Insights direttamente da "Mercato AWS", senza prima creare un ambiente di prova. Una volta completato l'abbonamento e configurato l'ambiente, l'utente verrà immediatamente iscritto.

Aggiunta di un ID licenza

Se possiedi un prodotto NetApp valido in bundle con Cloud Insights, puoi aggiungere il numero di serie del prodotto all'abbonamento Cloud Insights esistente. Ad esempio, se si è acquistato il centro di controllo Astra, è possibile utilizzare il numero di serie della licenza per identificare l'abbonamento in Cloud Insights. Cloud Insights fa riferimento a questo documento come *ID licenza*.

Per aggiungere un ID diritto all'abbonamento Cloud Insights, nella pagina **Amministratore > abbonamento**, fare clic su *+ID diritto*.



Risoluzione automatica del dispositivo

Panoramica automatica della risoluzione dei dispositivi

È necessario identificare tutti i dispositivi che si desidera monitorare con Cloud Insights. L'identificazione è necessaria per tenere traccia con precisione delle performance e dell'inventario nel tuo ambiente. In genere, la maggior parte dei dispositivi rilevati nell'ambiente viene identificata tramite *Automatic Device Resolution*.

Dopo aver configurato i data raccoglitori, 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 tipo data collector, 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

I dispositivi che rimangono 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 Cloud Insights.

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:

- **Fibre Channel 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 Address 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.
- **Regole di risoluzione automatica** contiene l'elenco di regole eseguite durante l'esecuzione della risoluzione del dispositivo Fibre Channel. Si tratta di regole create per risolvere i dispositivi Fibre Channel non identificati.

- **Preferenze** fornisce le opzioni di configurazione utilizzate per personalizzare la risoluzione del dispositivo per l'ambiente in uso.

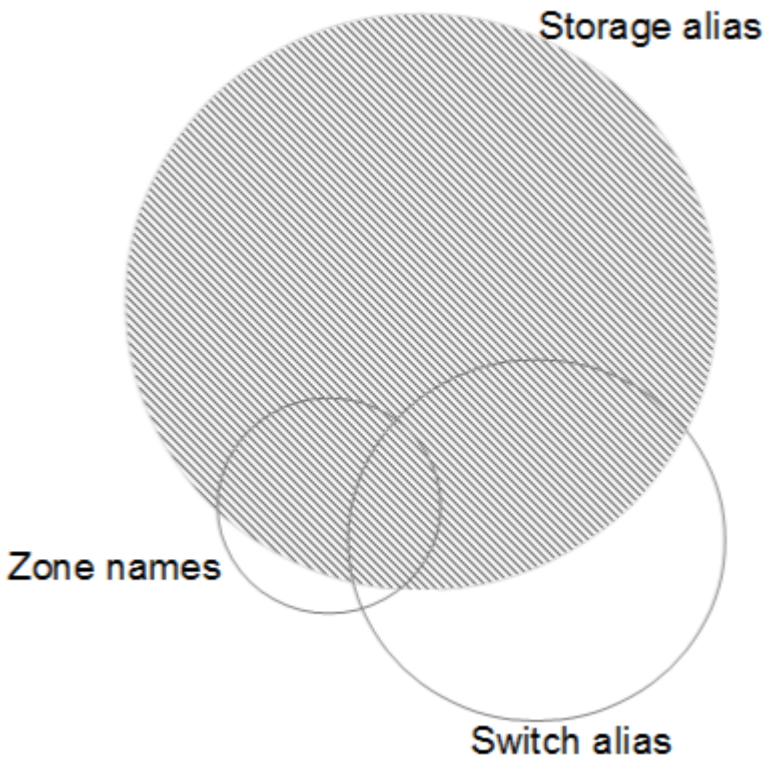
Prima di iniziare

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?
- 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 l'identificazione dei dispositivi

In genere, per identificare i dispositivi nell'ambiente in uso, si utilizza un workflow simile a quello riportato di seguito. L'identificazione è un processo iterativo e potrebbe richiedere più fasi di pianificazione e definizione delle regole.

- Ambiente di ricerca
- Regole del piano
- Creare/rivedere le regole
- Esaminare i risultati
- Creare regole aggiuntive o identificare manualmente i dispositivi
- Fatto

> Se nell'ambiente sono presenti dispositivi non identificati (noti anche come dispositivi 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.

Correlato:"Creazione di regole di risoluzione dei dispositivi"
"Risoluzione del dispositivo Fibre Channel"
"Risoluzione del dispositivo IP"
"Impostazione delle preferenze di risoluzione del dispositivo"

Regole di risoluzione dei dispositivi

Vengono create regole di risoluzione dei dispositivi per identificare host, storage e nastri che non vengono identificati automaticamente da Cloud Insights. Le regole create consentono di identificare i dispositivi attualmente presenti nell'ambiente e i dispositivi simili man mano che vengono aggiunti all'ambiente.

Creazione di regole di risoluzione dei dispositivi

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 host * alias storage contenente un nome host o nastro incorporato * alias 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) * Delimiters * 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.

Procedura

1. Fare clic su **Gestisci > risoluzione periferica**

2. Nella scheda **regole di risoluzione automatica**, fare clic su **+ regola host** o **+ regola nastro**.

   Viene visualizzata la schermata **Resolution Rule** (regola di risoluzione).

   > Fare clic sul collegamento *View Matching Criteria* per ottenere assistenza 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.

   A seconda dell'origine scelta, Cloud Insights visualizza la seguente risposta:

   a. **Zones** elenca le zone e il WWN che devono essere identificati da Cloud Insights.
   b. **SRM** elenca gli alias non identificati che devono essere identificati da Cloud Insights
   c. **Alias dello storage** elenca gli alias dello storage e il WWN che devono essere identificati da Cloud Insights
   d. **Switch alias** elenca gli alias dello switch che devono essere identificati da Cloud Insights

5. Nell'elenco **Method** (metodo), selezionare il metodo da utilizzare per identificare l'host.

Origine	Metodo
SRM	Così come sono, i Delimiters, le espressioni regolari
Alias storage	Delimitatori, espressioni regolari
Cambiare alias	Delimitatori, espressioni regolari
Zone	Delimitatori, espressioni regolari

   - Le regole che utilizzano i delimitatori richiedono i delimitatori e la lunghezza minima del nome host. La lunghezza minima del nome host è il numero di caratteri che Cloud Insights deve utilizzare per identificare un host. Cloud Insights 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 un input squing di *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 espressioni regolari richiedono un'espressione regolare, il formato e la selezione della distinzione tra maiuscole e minuscole.
6. Fare clic su **Esegui AR** per eseguire tutte le regole oppure fare clic sulla freccia in basso nel pulsante per eseguire la regola creata (e qualsiasi altra regola creata dall'ultima esecuzione completa di AR).

   I risultati dell'esecuzione della regola vengono visualizzati nella scheda **FC Identify**.

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.

Procedura

1. Accedere all'interfaccia utente Web di Cloud Insights.
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 basata su 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.

Prima di iniziare

Sono presenti diversi dispositivi non identificati e più regole che consentono di identificare correttamente altri dispositivi.

> 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.

Procedura

1. Accedere all'interfaccia utente Web di Cloud Insights.
2. Fare clic su **Gestisci > risoluzione periferica**
3. Fare clic sulla scheda **Fibre Channel Identify**.

   Il sistema visualizza i dispositivi insieme al relativo stato di risoluzione.

4. Selezionare più dispositivi non identificati.
5. Fare clic su **azioni in blocco** e selezionare **set host resolution** (Imposta risoluzione host) o **set tape resolution** (Imposta risoluzione nastro).

   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.

Cloud Insights 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).

Correlato:"Risoluzione del dispositivo Fibre Channel"
"Risoluzione del dispositivo IP"
"Impostazione delle preferenze di risoluzione del dispositivo"

Risoluzione del dispositivo Fibre Channel

La schermata Fibre Channel Identify (identificazione Fibre Channel) visualizza il WWN e il WWPN dei dispositivi Fibre Channel i cui host non sono stati identificati dalla risoluzione automatica dei dispositivi. 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. I dispositivi mancanti hanno uno stato di *Unidentified*. I dispositivi specificamente esclusi dall'identificazione hanno lo stato *excluded*. La copertura totale per l'identificazione dei dispositivi è riportata in questa pagina.

È possibile eseguire operazioni in blocco selezionando più periferiche sul lato sinistro della schermata Fibre Channel Identify (identificazione Fibre Channel). È possibile eseguire azioni su un singolo dispositivo passando il mouse su un dispositivo e selezionando i pulsanti *Identify* o *UnIdentify* all'estrema destra dell'elenco.

Il collegamento *Total Coverage* 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 Cloud Insights utilizzando la funzione *aggiunta manuale* disponibile nella scheda identificazione Fibre Channel per la risoluzione del 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.

Procedura

1. Accedere all'interfaccia utente Web di Cloud Insights
2. Fare clic su **Gestisci > risoluzione periferica**
3. Fare clic sulla scheda **Fibre Channel Identify**.
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.

   Il dispositivo inserito viene aggiunto all'elenco dei dispositivi nella scheda Fibre Channel Identify (identificazione Fibre Channel). 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 risoluzione del dispositivo Cloud Insights utilizzando un elenco di dispositivi in un file .CSV.

1. Prima di iniziare

È necessario disporre di un file .CSV formattato correttamente per importare gli identificatori dei dispositivi direttamente nella risoluzione dei dispositivi. Il file .CSV per le periferiche Fibre Channel richiede le seguenti informazioni:

WWN	IP	Nome	Tipo

I campi dati devono essere racchiusi tra virgolette, come mostrato nell'esempio seguente.

```
"WWN","IP","Name","Type"
"WWN:2693","ADDRESS2693|IP2693","NAME-2693","HOST"
"WWN:997","ADDRESS997|IP997","NAME-997","HOST"
"WWN:1860","ADDRESS1860|IP1860","NAME-1860","HOST"
```

> Come procedura consigliata, si consiglia di esportare prima le informazioni di identificazione Fibre Channel in un file .CSV, apportare le modifiche desiderate in tale file e quindi importarlo nuovamente in Fibre Channel Identify. In questo modo, le colonne previste sono presenti e nell'ordine corretto.

Per importare le informazioni di identificazione Fibre Channel:

1. Accedere all'interfaccia utente Web di Cloud Insights.
2. Fare clic su **Gestisci > risoluzione periferica**
3. Selezionare la scheda **Fibre Channel Identify**.

4. Fare clic sul pulsante **identifica > identifica dal file**.
5. 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 Fibre Channel Identify (identificazione Fibre Channel). 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 Cloud Insights. È possibile esportare un identificativo del dispositivo in modo da poterlo modificare e quindi importarlo nuovamente in Cloud Insights, 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 l'identificazione di un dispositivo Fibre Channel in un file .CSV, il file contiene le seguenti informazioni nell'ordine indicato:

WWN	IP	Nome	Tipo

Procedura

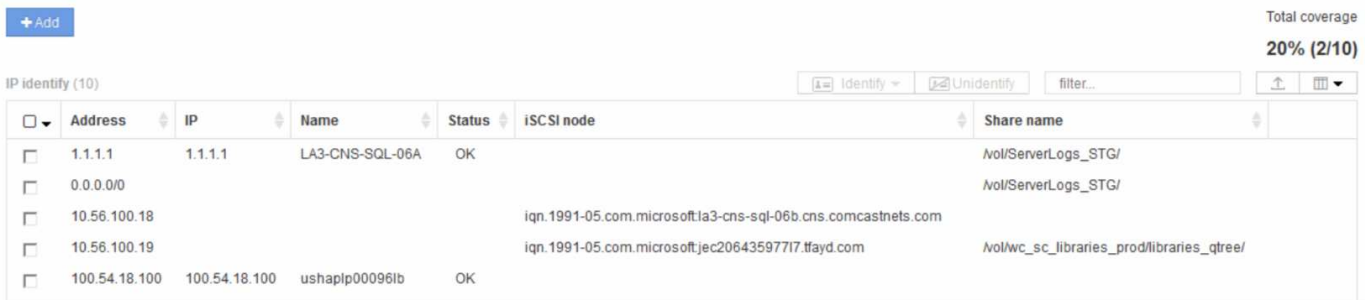
1. Accedere all'interfaccia utente Web di Cloud Insights.
2. Fare clic su **Gestisci > risoluzione periferica**
3. Selezionare la scheda **Fibre Channel Identify**.
4. Selezionare il dispositivo Fibre Channel o i dispositivi di cui si desidera esportare l'identificativo.
5. Fare clic su **Export** (Esporta) pulsante.

   Selezionare se aprire il file .CSV o salvarlo.

Correlato:"Risoluzione del dispositivo IP"
"Creazione di regole di risoluzione dei dispositivi"
"Impostazione delle preferenze di risoluzione del dispositivo"

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 Cloud Insights utilizzando la funzione di aggiunta manuale disponibile nella schermata di identificazione IP.

Procedura

1. Accedere all'interfaccia utente Web di Cloud Insights.
2. Fare clic su **Gestisci > risoluzione del dispositivo**
3. Fare clic sulla scheda **IP Address Identify** (identificazione indirizzo 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.

Risultato

Il dispositivo inserito viene aggiunto all'elenco dei dispositivi nella scheda IP Address Identify (identificazione indirizzo 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.

1. 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 i dispositivi IP richiede le seguenti informazioni:

Indirizzo	IP	Nome

I campi dati devono essere racchiusi tra virgolette, come mostrato nell'esempio seguente.

```
"Address","IP","Name"
"ADDRESS6447","IP6447","NAME-6447"
"ADDRESS3211","IP3211","NAME-3211"
"ADDRESS593","IP593","NAME-593"
```

> Come procedura consigliata, si consiglia di esportare prima le informazioni di identificazione dell'indirizzo IP in un file .CSV, apportare le modifiche desiderate in tale file, quindi importare nuovamente il file in IP Address Identify (identificazione indirizzo IP). In questo modo, le colonne previste sono presenti e nell'ordine corretto.

Esportazione dell'identificazione del dispositivo IP in un file .CSV

È possibile esportare gli identificativi dei dispositivi IP esistenti in un file .CSV dalla funzione di risoluzione dei dispositivi Cloud Insights. È possibile esportare un identificativo del dispositivo in modo da poterlo modificare e quindi importarlo nuovamente in Cloud Insights, dove viene utilizzato per identificare i dispositivi simili a quelli che corrispondono originariamente all'identificativo esportato.

A proposito di questa attività

1. 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 identificativo del dispositivo IP in un file .CSV, il file contiene le seguenti informazioni nell'ordine indicato:

Indirizzo	IP	Nome

Procedura

1. Accedere all'interfaccia utente Web di Cloud Insights.
2. Fare clic su **Gestisci > risoluzione periferica**
3. Selezionare la scheda **IP Address Identify** (identificazione indirizzo IP).
4. Selezionare il dispositivo IP o i dispositivi di cui si desidera esportare l'identificativo.
5. Fare clic su **Export** (Esporta) pulsante.

   Selezionare se aprire il file .CSV o salvarlo.

Correlato:"Risoluzione del dispositivo Fibre Channel"
"Creazione di regole di risoluzione dei dispositivi"
"Impostazione delle preferenze di risoluzione del dispositivo"

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 *manually*, 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 IPs (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 i nastri funzionano solo per i WWN in cui il fornitore per quel WWN è impostato su *incluso come solo nastro* nelle preferenze del vendor.

Vedere anche: "Esempi di espressioni regolari"

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 Cloud Insights.

Formattazione delle espressioni regolari

Quando si creano espressioni regolari per la risoluzione automatica di Cloud Insights, è possibile configurare il formato di output immettendo i valori in un campo denominato *FORMAT*.

L'impostazione predefinita è 1, il che significa che 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 campo DEL FORMATO.

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 sono presenti tre gruppi di parentesi, le variabili 1, 2 e 3
vengono popolate.
```

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.

Esempi

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]*)_.*
La variabile conterrà solo _myComputerName123_ dopo essere stata valutata
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: Nome computer

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 simbolo ^ (circonflesso o accento circonflesso) **all'interno delle parentesi quadre** nega l'espressione, ad esempio [^FF] indica qualsiasi cosa tranne F maiuscola o minuscola, mentre [^a-z] indica tutto tranne a-z minuscola e, nel caso precedente, qualsiasi cosa tranne _. 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 Cloud Insights:[^_] ()_([^_]).*formato in Cloud Insights

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.

Storage Alias: host/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: -(.*-).*

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-

Creazione di dashboard

Panoramica delle dashboard

Cloud Insights offre agli utenti la flessibilità di creare viste operative dei dati dell'infrastruttura, consentendo di creare dashboard personalizzati con una vasta gamma di widget, ciascuno dei quali offre una flessibilità estesa nella visualizzazione e nella creazione di grafici dei dati.

> Gli esempi in queste sezioni hanno solo scopo esplicativo e non coprono tutti gli scenari possibili. I concetti e le fasi qui descritti possono essere utilizzati per creare dashboard personalizzati per evidenziare i dati specifici per le esigenze specifiche.

Creazione di una dashboard

È possibile creare una nuova dashboard in due posizioni:

- **Dashboard > [+Nuova dashboard]**
- **Dashboard > Mostra tutti i dashboard >** fare clic sul pulsante **[+Dashboard]**

Comandi della dashboard

La schermata Dashboard dispone di diversi comandi:

- **Time selector**: Consente di visualizzare i dati della dashboard per un intervallo di tempo compreso tra gli ultimi 15 minuti e gli ultimi 30 giorni o un intervallo di tempo personalizzato fino a 31 giorni. È possibile scegliere di ignorare questo intervallo di tempo globale nei singoli widget.
- Pulsante **Edit** (Modifica): Selezionando questa opzione si attiva la modalità Edit (Modifica), che consente di apportare modifiche alla dashboard. Per impostazione predefinita, vengono aperti nuovi dashboard in modalità di modifica.
- Pulsante **Save** (Salva): Consente di salvare o eliminare la dashboard.

  È possibile rinominare la dashboard corrente digitando un nuovo nome prima di fare clic su **Salva**.

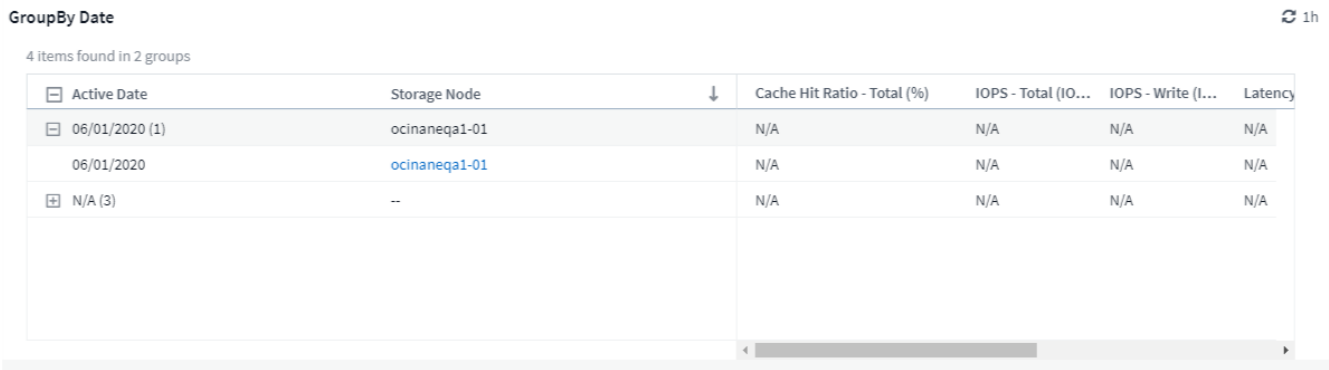
- **Aggiungi widget**, che consente di aggiungere un numero qualsiasi di tabelle, grafici o altri widget alla dashboard.

  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.

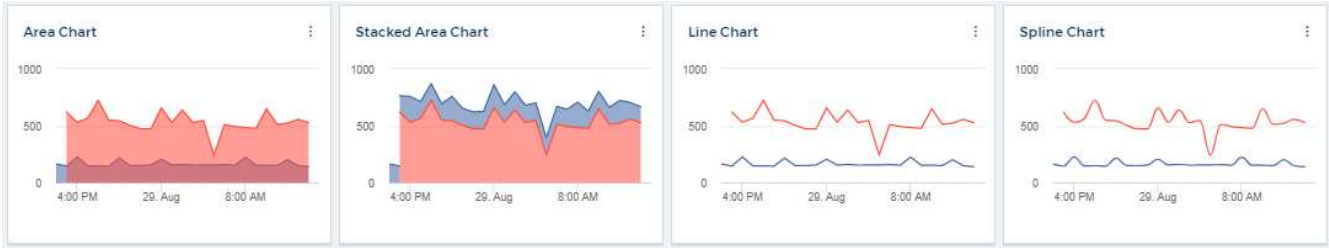
Tipi di widget

È possibile scegliere tra i seguenti tipi di widget:

- **Widget tabella**: 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.

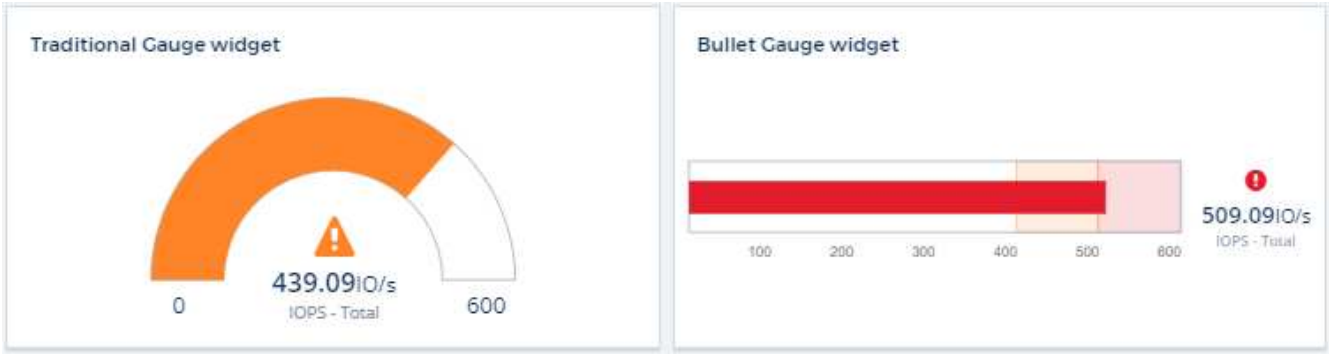


- **Grafici di linee, spline, area, area sovrapposte**: Sono widget grafici di serie temporali su cui è possibile visualizzare le performance e altri dati nel tempo.



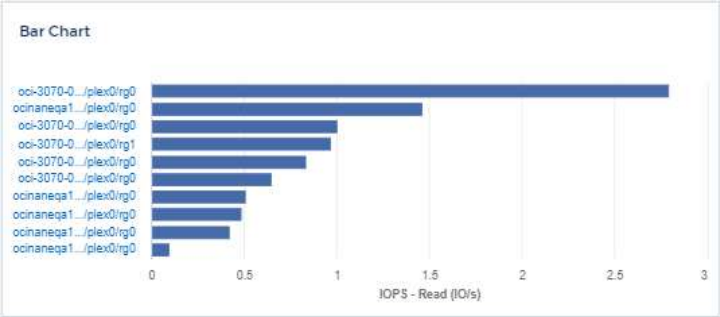
- **Widget a valore singolo**: Widget che consente di visualizzare un singolo valore che può essere derivato direttamente da un contatore o calcolato utilizzando una query o un'espressione. È possibile definire le soglie di formattazione del colore per indicare se il valore rientra nell'intervallo previsto, di avviso o critico.

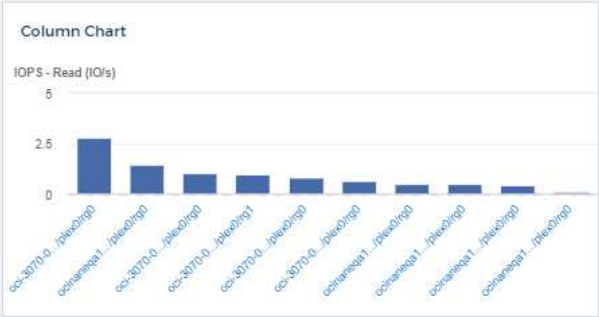
- Widget **Gauge**: Visualizza i dati a valore singolo in un indicatore tradizionale (a tinta unita) o in un indicatore a tinta unita, con colori basati sui valori "Avvertenza" o "critici" "personalizzare".



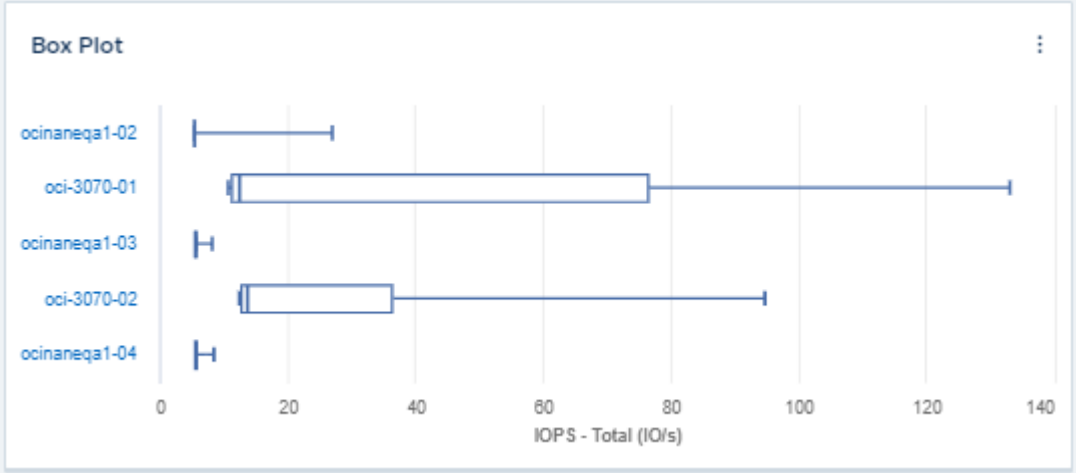
- **Barra, grafici a colonne**: Visualizza i valori N superiori o inferiori, ad esempio i primi 10 storage in base

alla capacità o i 5 volumi inferiori in base agli IOPS.

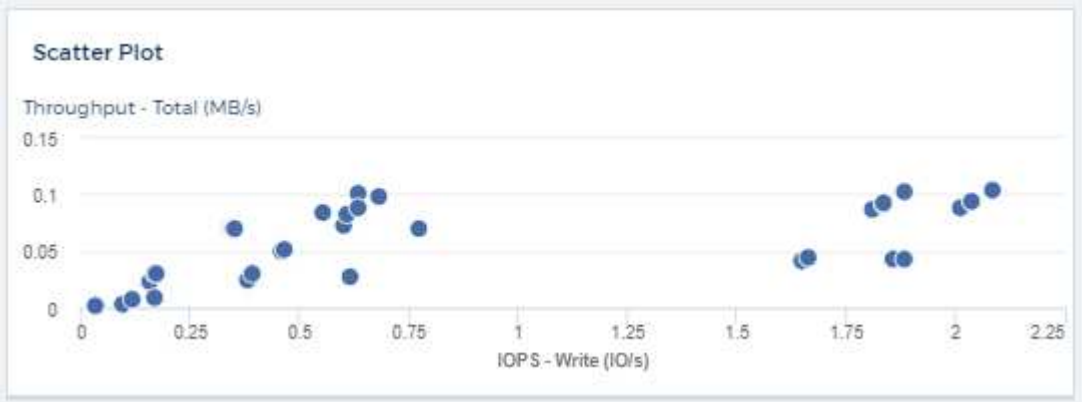




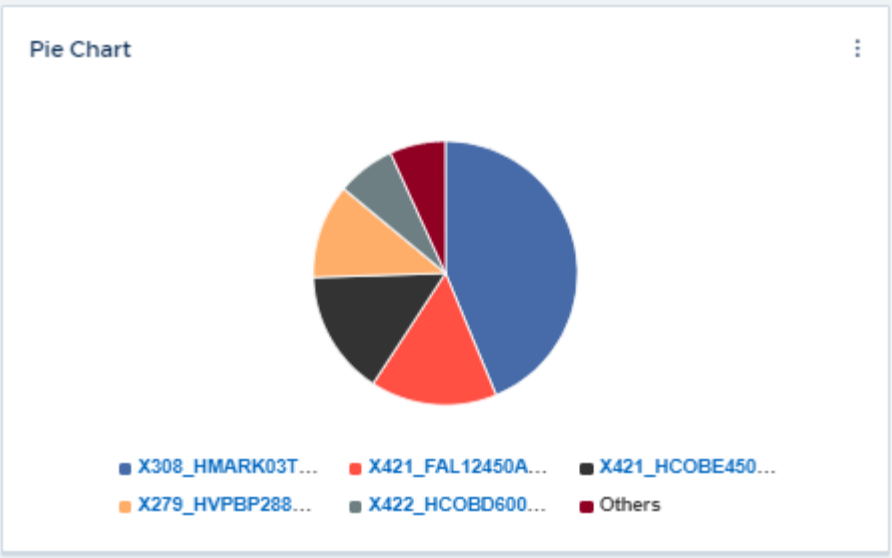
- **Box Plot Chart**: Un grafico del minimo, massimo, mediano e dell'intervallo tra il quartile inferiore e quello superiore dei dati in un singolo grafico.



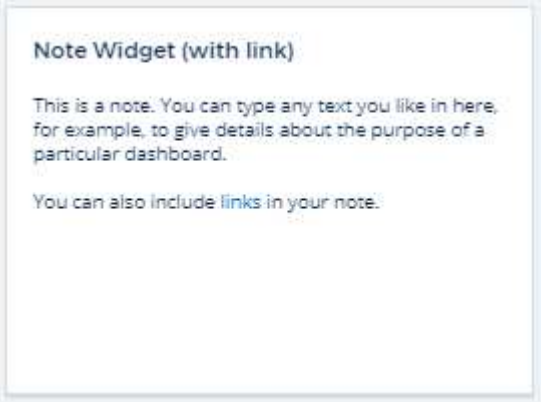
- **Grafico di dispersione**: Traccia i dati correlati come punti, ad esempio IOPS e latenza. In questo esempio, è possibile individuare rapidamente le risorse con throughput elevato e IOPS ridotti.



- **Grafico a torta**: Un grafico a torta tradizionale per visualizzare i dati come parte del totale.



- **Widget Nota**: Fino a 1000 caratteri di testo libero.



- **Alerts Table**: Visualizza fino agli ultimi 1,000 avvisi.

Per una spiegazione più dettagliata di queste e altre funzionalità della dashboard, "fare clic qui".

Impostazione di una dashboard come home page

È possibile scegliere quale dashboard impostare come **home page** dell'ambiente utilizzando uno dei seguenti metodi:

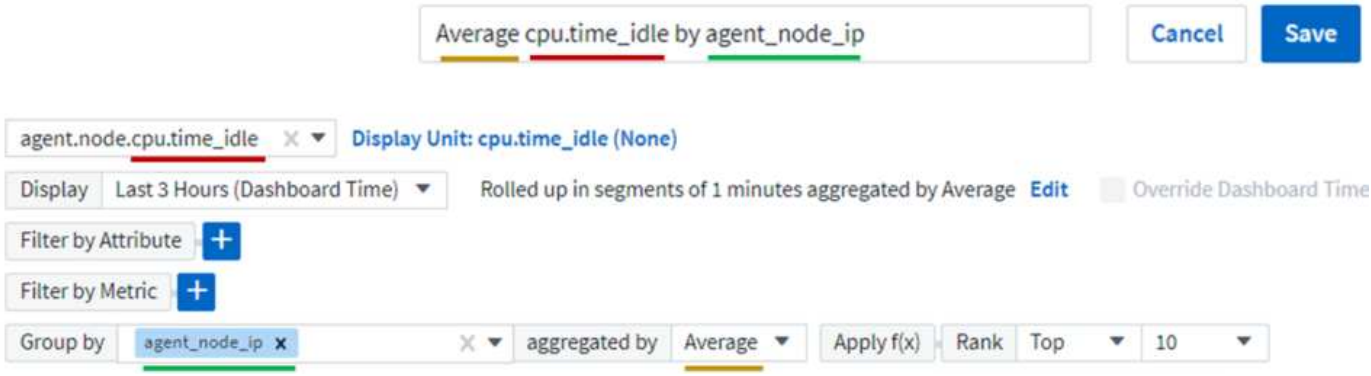
- Accedere a **Dashboard > Show All Dashboard** (Mostra tutti i dashboard) per visualizzare l'elenco dei dashboard nell'ambiente. Fare clic sul menu delle opzioni a destra della dashboard desiderata e selezionare **Imposta come home page**.
- Fare clic su una dashboard dall'elenco per aprire la dashboard. Fare clic sul menu a discesa nell'angolo superiore e selezionare **Imposta come home page**.

Caratteristiche della dashboard

Dashboard e widget consentono una grande flessibilità nella visualizzazione dei dati. Ecco alcuni concetti che ti aiuteranno a ottenere il massimo dalle dashboard personalizzate.

Nome widget

I widget vengono denominati automaticamente in base all'oggetto, alla metrica o all'attributo selezionato per la prima query del widget. Se si sceglie anche un raggruppamento per il widget, gli attributi "Raggruppa per" vengono inclusi nella naming automatica (metodo di aggregazione e metrica).



La selezione di un nuovo oggetto o attributo di raggruppamento aggiorna il nome automatico.

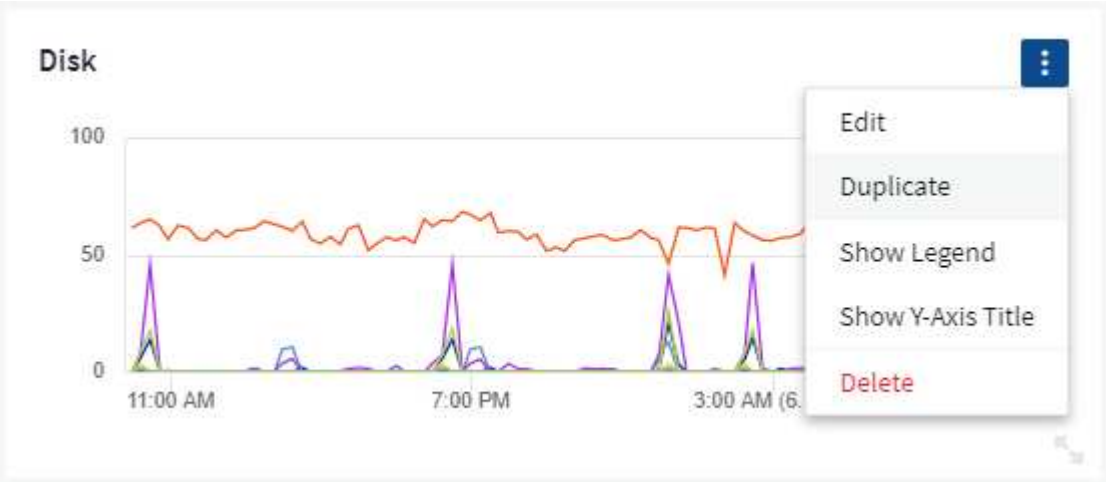
Se non si desidera utilizzare il nome automatico del widget, è sufficiente digitare un nuovo nome.

Posizionamento e dimensioni widget

Tutti i widget della dashboard possono essere posizionati e dimensionati in base alle esigenze di ogni dashboard.

Duplicazione di un widget

In modalità Dashboard Edit (Modifica dashboard), fare clic sul menu del widget e selezionare **Duplicate** (Duplica). Viene avviato l'editor dei widget, compilato con la configurazione originale del widget e con il suffisso "copy" nel nome del widget. È possibile apportare facilmente le modifiche necessarie e salvare il nuovo widget. Il widget viene posizionato nella parte inferiore della dashboard ed è possibile posizionarlo in base alle esigenze. Ricordarsi di salvare la dashboard una volta completate tutte le modifiche.



Visualizzazione delle legende dei widget

La maggior parte dei widget sui dashboard può essere visualizzata con o senza legende. Le legende nei widget possono essere attivate o disattivate su una dashboard in uno dei seguenti modi:

- Quando viene visualizzata la dashboard, fare clic sul pulsante **Opzioni** sul widget e selezionare **Mostra legende** nel menu.

Man mano che i dati visualizzati nel widget cambiano, 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. Se la legenda visualizza "tutti", facendo clic sul collegamento viene visualizzata una pagina di query corrispondente alla prima query nel widget.

Trasformazione delle metriche

Cloud Insights offre diverse opzioni **transform** per determinate metriche nei widget (in particolare, quelle metriche chiamate "personalizzate" o metriche di integrazione, come Kubernetes, dati avanzati ONTAP, plug-in Telegraf, ecc.), consentendo di visualizzare i dati in diversi modi. Quando si aggiungono metriche trasformabili a un widget, viene visualizzato un menu a discesa che offre le seguenti scelte di trasformazione:

Nessuno
: I dati vengono visualizzati così come sono, senza alcuna manipolazione.

Tasso
: Valore corrente diviso per l'intervallo di tempo dall'osservazione precedente.

Cumulativo
: L'accumulo della somma dei valori precedenti e del valore corrente.

Delta
: La differenza tra il valore di osservazione precedente e il valore corrente.

Delta rate (tasso delta)
: Valore delta diviso per l'intervallo di tempo dall'osservazione precedente.

Tasso cumulativo
: Valore cumulativo diviso per l'intervallo di tempo dall'osservazione precedente.

Si noti che la trasformazione delle metriche non modifica i dati sottostanti, ma solo il modo in cui vengono visualizzati.

Query e filtri dei widget della dashboard

Query

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 dei widget della dashboard

Ecco alcune cose che puoi fare per ottenere il massimo dai tuoi filtri.

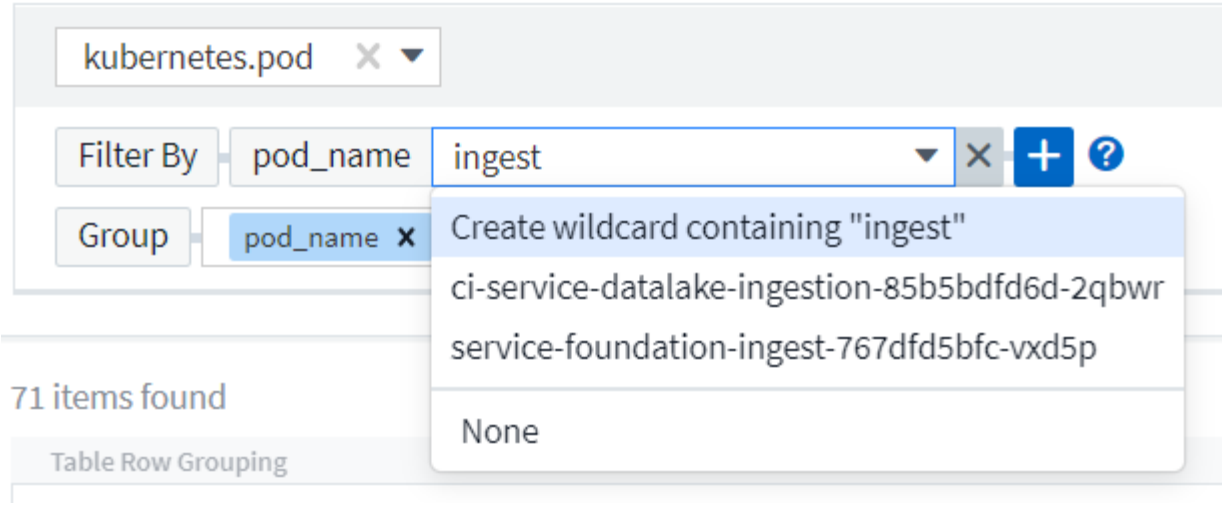
Filtro Exact Match

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 "*" restituirà 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.

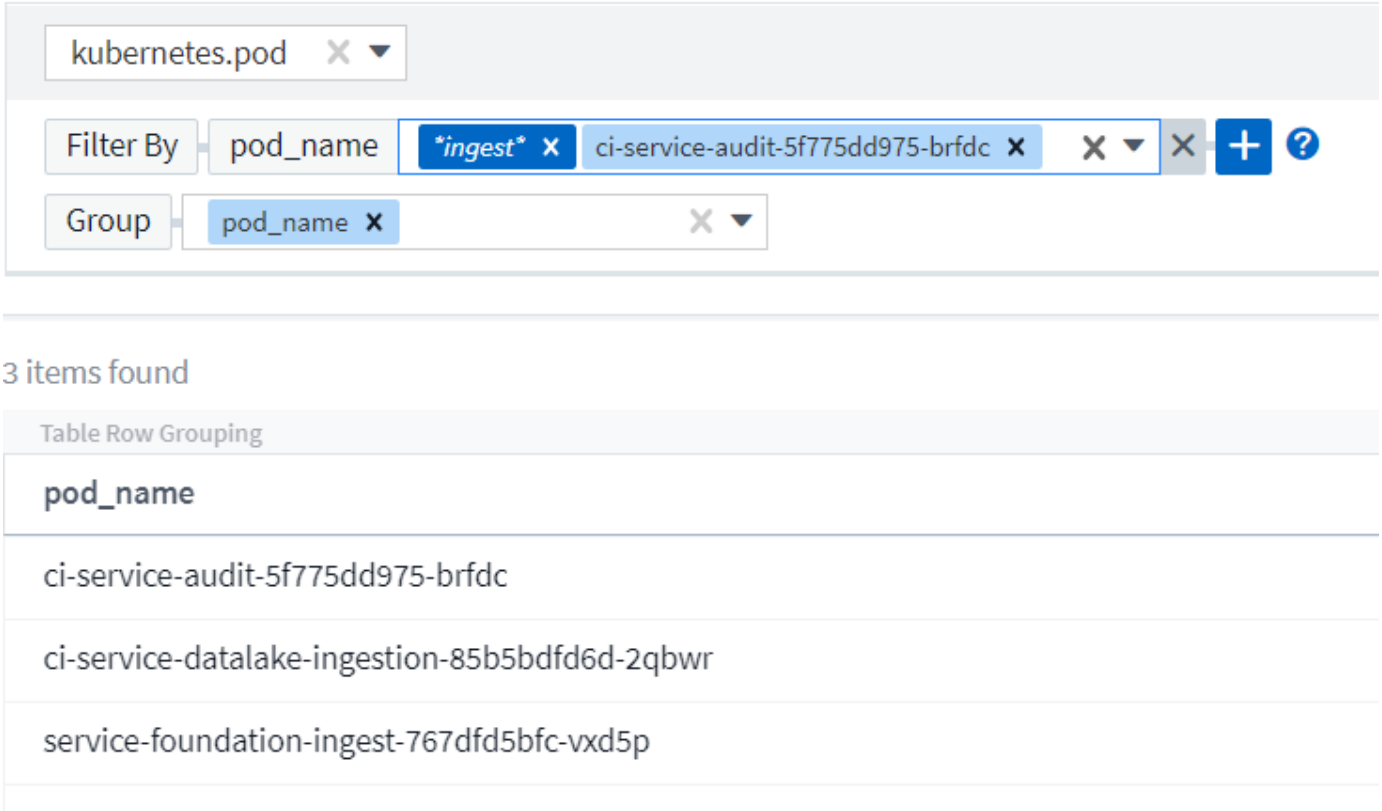
È possibile utilizzare filtri di corrispondenza precisi per trovare risorse specifiche, ad esempio il nome host. Se si desidera trovare solo il nome host 'marketing' ma si escludono 'marketing01', 'markketing-boston', ecc., è sufficiente racchiudere il nome "marketing" tra virgolette doppie.

Caratteri jolly ed espressioni

Quando si filtrano valori di testo o di elenco nelle query o nei widget della dashboard, quando si inizia a digitare viene visualizzata l'opzione per creare un filtro * con caratteri jolly* in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione con caratteri jolly. È inoltre possibile creare **espressioni** utilizzando NOR o OPPURE, oppure selezionare l'opzione "None" (Nessuno) per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio, NO, O "None", ecc.) vengono visualizzati in blu scuro nel campo del filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in blu chiaro.



Si noti che i caratteri jolly e il filtraggio delle espressioni funzionano con testo o elenchi, ma non con valori numerici, date o booleani.

Advanced Text Filtering con suggerimenti contestuali di tipo avanzato

Il filtraggio nelle query widget è *contestuale*; quando si seleziona uno o più valori di un filtro per un campo, gli altri filtri per tale query mostreranno i valori relativi a tale filtro. Ad esempio, quando si imposta un filtro per un oggetto *Name* specifico, il campo da filtrare per *Model* mostrerà solo i valori relativi a tale nome oggetto.

Il filtraggio contestuale si applica anche alle variabili della pagina della dashboard (solo attributi di testo o

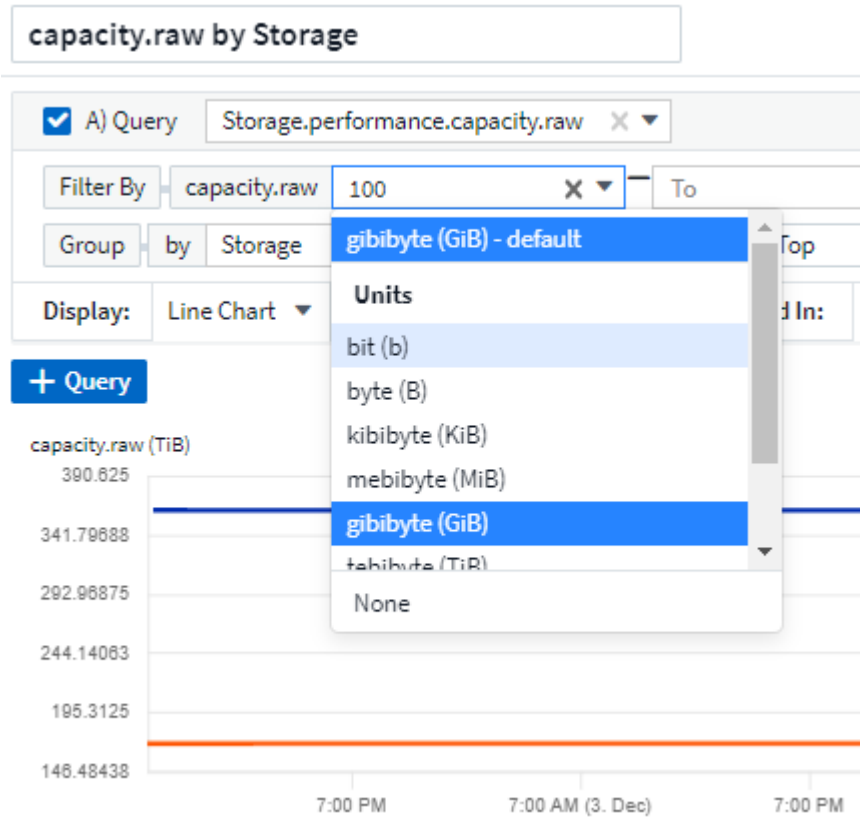
annotazioni). Quando si seleziona un valore filer per una variabile, qualsiasi altra variabile che utilizza oggetti correlati mostrerà solo i possibili valori di filtro in base al contesto di tali variabili correlate.

Nota: Solo i filtri di testo mostrano suggerimenti contestuali di tipo anticipato. Date (Data), Enum (elenco), ecc. non mostrano suggerimenti di tipo anticipato. Detto questo, è possibile _impostare un filtro su un campo Enum (ad esempio elenco) e fare in modo che altri campi di testo siano filtrati nel contesto. Ad esempio, selezionando un valore in un campo Enum come Data Center, gli altri filtri mostreranno solo i modelli/nomi in quel data center), ma non viceversa.

L'intervallo di tempo selezionato fornirà anche il contesto per i dati mostrati nei filtri.

Scelta delle unità di filtraggio

Mentre si digita un valore in un campo di filtro, è possibile selezionare le unità in cui visualizzare i valori nel grafico. Ad esempio, è possibile filtrare la capacità raw e scegliere di visualizzarla nel GIB di default oppure selezionare un altro formato, ad esempio TIB. Ciò è utile se si dispone di una serie di grafici sulla dashboard che mostrano i valori in TIB e si desidera che tutti i grafici mostrino valori coerenti.



Ulteriori miglioramenti del filtraggio

Per perfezionare ulteriormente i filtri, è possibile utilizzare quanto segue.

- 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*
```

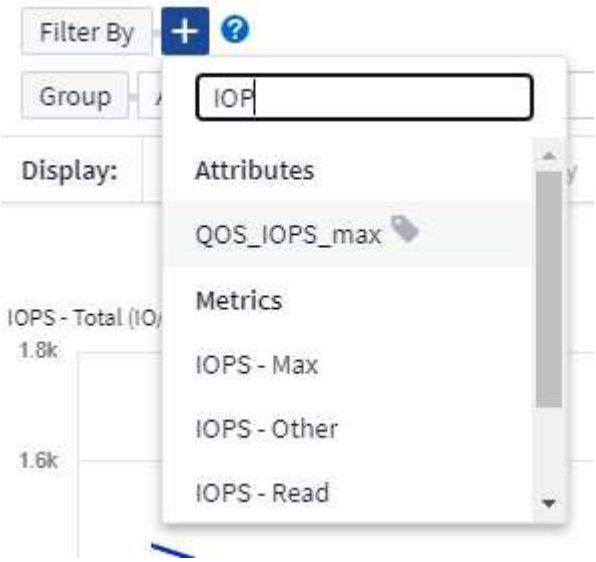
  Trova tutto ciò che non inizia con "EMC". È possibile utilizzare

```
NOT *
```

  per visualizzare i campi che non contengono valori.

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.



Raggruppamento e aggregazione

Raggruppamento (rollio)

I dati visualizzati in un widget vengono raggruppati (talvolta chiamati arrotolati) a partire 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 raggruppare questi dati in uno dei seguenti modi:

- **Average** (Media): Visualizza ciascuna riga come *media* dei dati sottostanti.
- **Massimo**: Visualizza ogni riga come *massimo* dei dati sottostanti.
- **Minimum** (minimo): Visualizza ciascuna riga come *Minimum* dei dati sottostanti.
- **SUM**: Visualizza ogni riga come *somma* dei dati sottostanti.
- **Count**: Visualizza un *count* di oggetti che hanno riportato dati entro il periodo di tempo specificato. È possibile scegliere l' *intera finestra temporale* in base all'intervallo di tempo della dashboard (o l'intervallo di tempo del widget, se impostato per ignorare l'ora della dashboard) o una *finestra temporale personalizzata* selezionata.

Fasi

Per impostare il metodo di raggruppamento, procedere come segue.

1. Nella query del widget, scegli un tipo di risorsa e una metrica (ad esempio, *Storage*) e una metrica (ad esempio *Performance IOPS Total*).
2. Per **Group**, scegliere un metodo di rolloup (ad esempio *Average*) e selezionare gli attributi o le metriche in base ai quali eseguire il rolloup dei dati (ad esempio, *Data Center*).

   Il widget si aggiorna automaticamente e mostra i dati per ciascun data center.

Puoi anche scegliere di raggruppare *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, la somma o il conteggio della metrica o delle metriche scelte per tutte le risorse sottostanti.

Facendo clic sulla legenda per qualsiasi widget i cui dati sono raggruppati per "tutti", viene aperta una pagina di query che mostra i risultati della prima query utilizzata nel widget.

Se è stato impostato un filtro per la query, i dati vengono raggruppati in base ai dati filtrati.

Nota: Quando scegli di raggruppare un widget in un campo qualsiasi (ad esempio, *Model*), dovrai comunque filtrare in base a quel campo per visualizzare correttamente i dati di quel campo nel grafico o nella tabella.

Aggregare i dati

È possibile allineare ulteriormente i grafici delle serie temporali (linea, area, ecc.) aggregando i punti dati in bucket di minuti, ore o giorni prima che i dati vengano successivamente arrotolati in base all'attributo (se scelto). Puoi scegliere di aggregare i punti dati in base ai rispettivi *Average, Maximum, Minimum, Sum* o *Count*.

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 fino a quando non si seleziona un intervallo di tempo inferiore.

Puoi anche aggregare i dati nel widget del grafico a barre e nel widget a valore singolo.

Per impostazione predefinita, la maggior parte dei contatori delle risorse viene aggregata alla *media*. 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 *Average*.

Visualizzazione dei risultati in alto/in basso

In un widget grafico, è possibile visualizzare i risultati **Top** o **Bottom** per i dati di cui è stato eseguito il rollup e scegliere il numero di risultati dall'elenco a discesa fornito. In un widget tabella, è possibile 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. 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.

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 Tabella.

Esempio di raggruppamento (con spiegazione del rollup)

I widget delle tabelle consentono di raggruppare i dati per una visualizzazione più semplice.

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 sul selettore di colonna e scegliere *Nome hypervisor* e *IOPS - totale*.

   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 - Total*. Fare clic su *any* e nel campo **from** digitare **1**. Lasciare vuoto il campo **to**. Premere Invio e fare clic sul campo del filtro 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. Fare clic sul pulsante **Raggruppa per [+]**.

   È possibile raggruppare in base a qualsiasi attributo o annotazione visualizzata. Scegliere *all* per visualizzare tutte le macchine virtuali in un singolo gruppo.

   Qualsiasi intestazione di colonna per una metrica delle performance visualizza un menu a tre punti contenente un'opzione **Roll-up**. Il metodo di rolloup predefinito è *Average*. 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 eseguire il rollup di questa colonna per *Average, Sum, Minimum* o *Maximum*. È possibile eseguire il rollup singolo di qualsiasi colonna visualizzata contenente metriche delle performance.

6. Fare clic su *All* e selezionare *Hypervisor name*.

   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.

7. Fare clic su **Save** (Salva) per salvare la tabella nella dashboard. È possibile ridimensionare o spostare il widget come desiderato.
8. Fare clic su **Save** (Salva) per salvare la dashboard.

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 (*AVG*) dei dati sottostanti nella riga del gruppo. È inoltre possibile scegliere di visualizzare la somma, il minimo o il massimo dei dati.

Selettore intervallo di tempo della dashboard

È possibile selezionare l'intervallo di tempo per i dati della dashboard. Solo i dati relativi all'intervallo di tempo selezionato verranno visualizzati nei widget della dashboard. È possibile scegliere tra i seguenti intervalli di tempo:

- Ultimi 15 minuti
- Ultimi 30 minuti
- Ultimi 60 minuti
- Ultime 2 ore
- Ultime 3 ore (impostazione predefinita)
- Ultime 6 ore
- Ultime 12 ore
- Ultime 24 ore
- Ultimi 2 giorni
- Ultimi 3 giorni
- Ultimi 7 giorni
- Ultimi 30 giorni
- Intervallo di tempo personalizzato

  L'intervallo di tempo personalizzato consente di selezionare fino a 31 giorni consecutivi. È inoltre possibile impostare l'ora di inizio e l'ora di fine del giorno per questo intervallo. L'ora di inizio predefinita è 12:00 AM nel primo giorno selezionato e l'ora di fine predefinita è 11:59 PM nell'ultimo giorno selezionato. Fare clic su **Apply** (Applica) per applicare l'intervallo di tempo personalizzato alla dashboard.

Ignorare l'ora del dashboard nei singoli widget

È possibile ignorare l'impostazione dell'intervallo di tempo 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 ignorare l'ora del dashboard e forzare un widget a utilizzare il proprio intervallo di tempo, nella modalità di modifica del widget impostare **Ignora ora ora ora dashboard** su **on** (selezionare la casella) 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.

Asse primario e secondario

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

Questo esempio illustra il concetto di assi primari e secondari in un widget grafico.

1. Creare o aprire una dashboard. Aggiungi un grafico a linee, un grafico a spline, un grafico ad area o un widget grafico ad area sovrapposta 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.

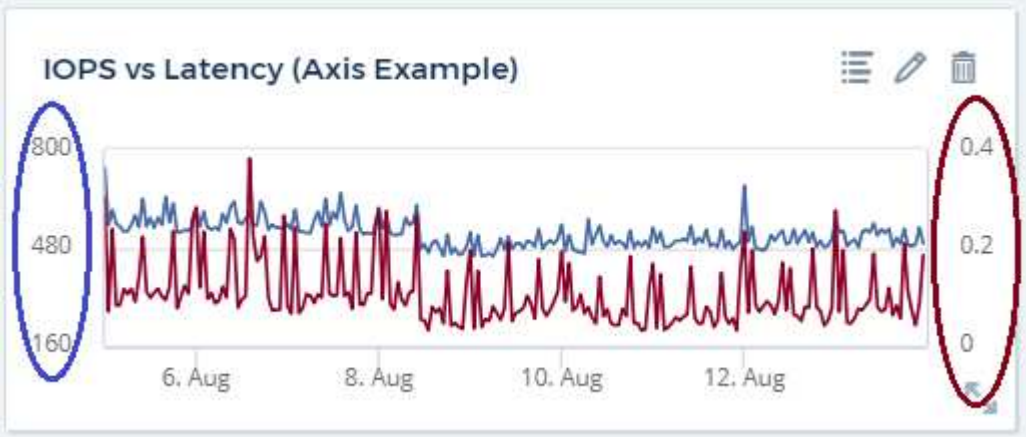
   La riga IOPS viene visualizzata sul grafico, con la relativa scala a sinistra.

3. Fare clic su **[+Query]** 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 disegnato *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

In un dashboard, qualsiasi widget di serie temporali (linea, spline, area, area impilata), grafico a barre, grafico a colonne, grafico a torta o widget di tabella consente di creare espressioni dalle metriche scelte e di visualizzare il risultato di tali espressioni in un singolo grafico (o colonna nel caso di widget di tabella). 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 fornisce visibilità sugli IOPS "di sistema" o "overhead" che si verificano nel tuo ambiente, ovvero gli IOPS che non sono direttamente derivanti dalla lettura o dalla scrittura dei dati.

È possibile utilizzare le variabili nelle espressioni (ad esempio, *€var1 * 100*)

Esempio di espressioni: Percentuale IOPS di lettura

In questo esempio, vogliamo mostrare gli IOPS in lettura come percentuale degli IOPS totali. Si può pensare a questo come alla seguente formula:

```
 Read Percentage = (Read IOPS / Total IOPS) 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 aprirla 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 collegamento **Converti in espressione** a destra.

   La query corrente viene convertita in modalità espressione. Non è possibile modificare il tipo di risorsa in modalità espressione. In modalità espressione, il collegamento diventa **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**", fare clic su **Select** e scegliere **IOPS - Read**.

   È possibile aggiungere fino a un totale di cinque variabili alfabetiche per l'espressione facendo clic sul pulsante + dopo 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
   . Il campo *Label* identifica l'espressione. Modificare l'etichetta in
   "percentuale di lettura", o qualcosa di altrettanto significativo per
   te.
   . Impostare il campo *unità* su "%" o "percentuale".
   ```

   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 potenzialmente possono superare il 100%.

6. Fare clic su **Save** (Salva) per salvare il grafico nella dashboard.

Esempio di espressioni: I/o "di sistema"

Esempio 2: Tra le metriche raccolte dalle origini dati vi sono IOPS totali, di lettura, scrittura e. Tuttavia, il numero totale di IOPS segnalati da un'origine dati a volte include IOPS "di sistema", che sono operazioni io che non sono 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:

```
 System IOPS = Total IOPS - (Read IOPS + Write IOPS)
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 aprirla 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. Nel campo **Roll Up**, selezionare *SUM* per *All*.

   Il grafico visualizza una riga che mostra la somma degli IOPS totali.

4. Fare clic sull'icona *Duplica questa query* per creare una copia della query.

   Un duplicato della query viene aggiunto sotto l'originale.

5. 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.

6. La metrica *IOPS - Total* si trova ora nel campo della variabile alfabetica "**a**". Fare clic su *IOPS - Total* e modificarlo in *IOPS - Read*.
7. Nel campo della variabile "**b**", fare clic su **Select** e scegliere *IOPS - Write*.
8. 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 (visualizzazione), selezionare **Area chart** per questa espressione.

9. Il campo **Label** identifica l'espressione. Modificare l'etichetta in "System IOPS" (IOPS di sistema) o in qualcosa di altrettanto significativo per l'utente.

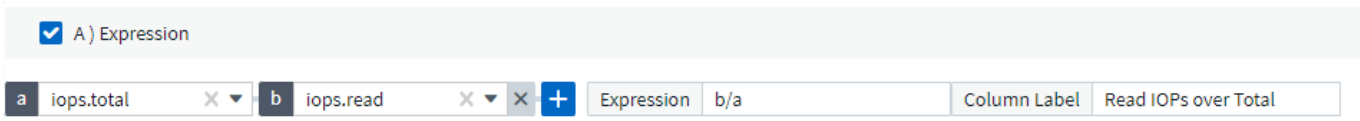
   Il grafico mostra gli IOPS totali come grafico a linee, con un grafico a aree che mostra la combinazione di IOPS di lettura e scrittura sottostante. Il divario tra i due indica gli IOPS che non sono direttamente correlati alle operazioni di lettura o scrittura dei dati. Questi sono i tuoi IOPS di "sistema".

10. Fare clic su **Save** (Salva) per salvare il grafico nella dashboard.

Per utilizzare una variabile in un'espressione, è sufficiente digitare il nome della variabile, ad esempio *€var1 * 100*. Nelle espressioni possono essere utilizzate solo variabili numeriche.

Espressioni in un widget di tabella

I widget della tavola gestiscono le espressioni in modo leggermente diverso. È possibile includere fino a cinque espressioni in un singolo widget di tabella, ciascuna delle quali viene aggiunta come nuova colonna alla tabella. Ogni espressione può includere fino a cinque valori su cui eseguire il calcolo. È possibile assegnare un nome alla colonna in modo semplice e significativo.



Variabili

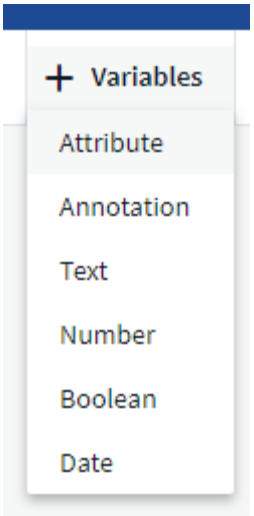
Le variabili consentono di modificare i dati visualizzati in alcuni o tutti i widget di una dashboard contemporaneamente. Impostando uno o più widget per l'utilizzo di una variabile comune, le modifiche apportate in un unico punto causano l'aggiornamento automatico dei dati visualizzati in ciascun widget.

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

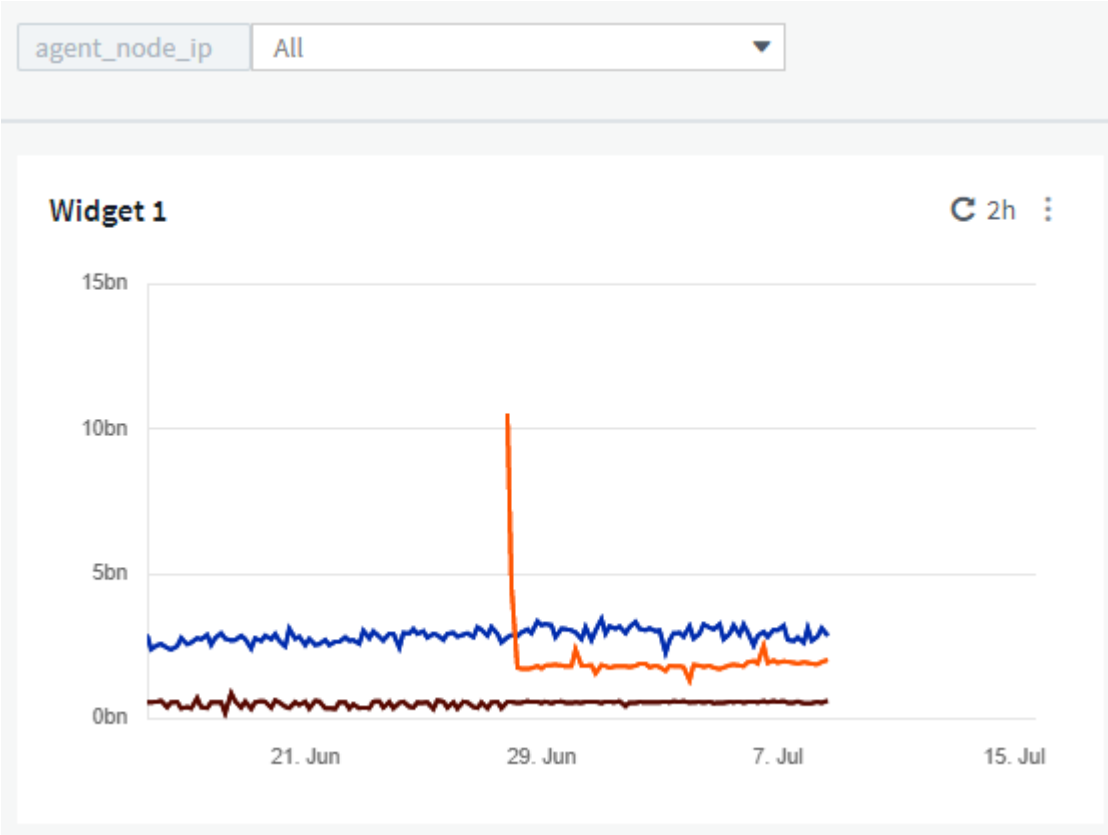
Una variabile può essere di uno dei seguenti tipi:

- **Attribute**: Utilizza gli attributi o le metriche di un oggetto per filtrare
- **Annotation** (Annotazione): Utilizzare un predefinito "Annotazione" per filtrare i dati del widget.
- **Text**: Stringa alfanumerica.
- **Numerico**: Un valore numerico. Utilizzare da solo o come valore "da" o "a", a seconda del campo del widget.
- **Booleano**: Utilizzare per i campi con valori vero/Falso, Sì/No, ecc. Per la variabile booleana, le opzioni sono Yes (Sì), No, None (Nessuno), Any (qualsiasi).
- **Data**: Un valore di data. Utilizzare come valore "da" o "a", a seconda della configurazione del widget.

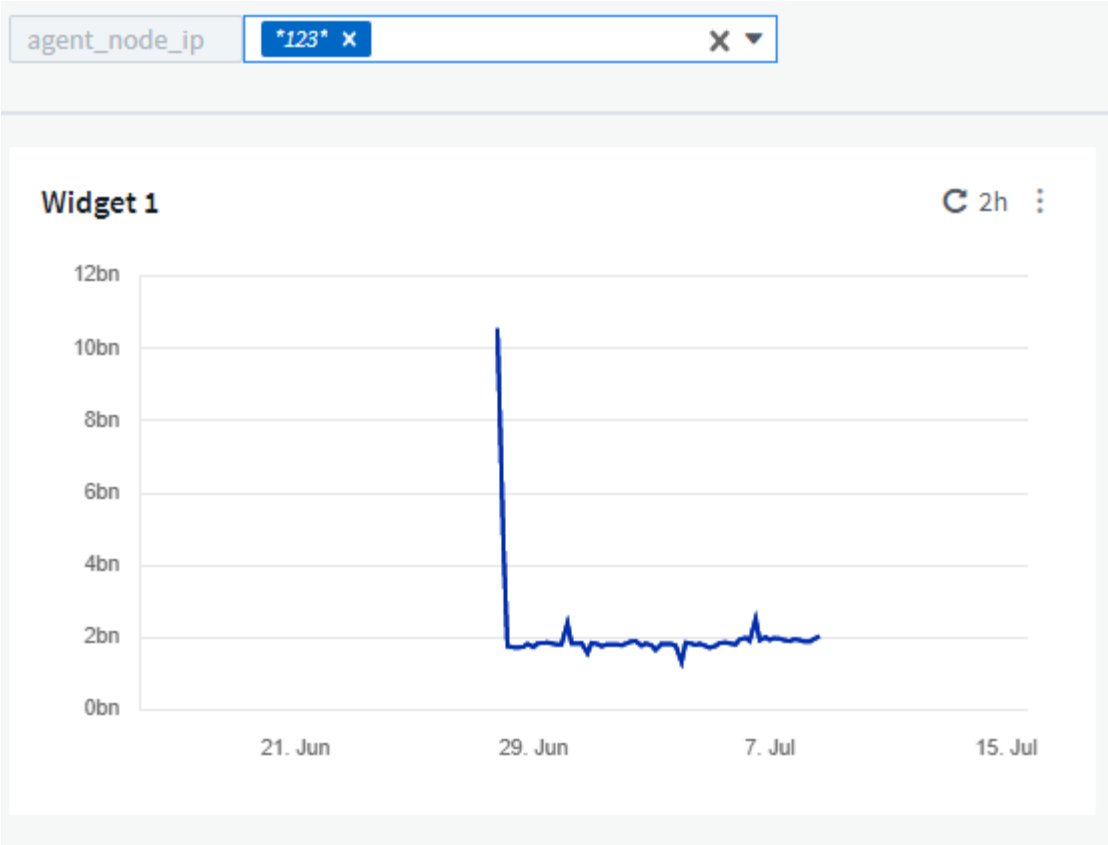


Variabili di attributo

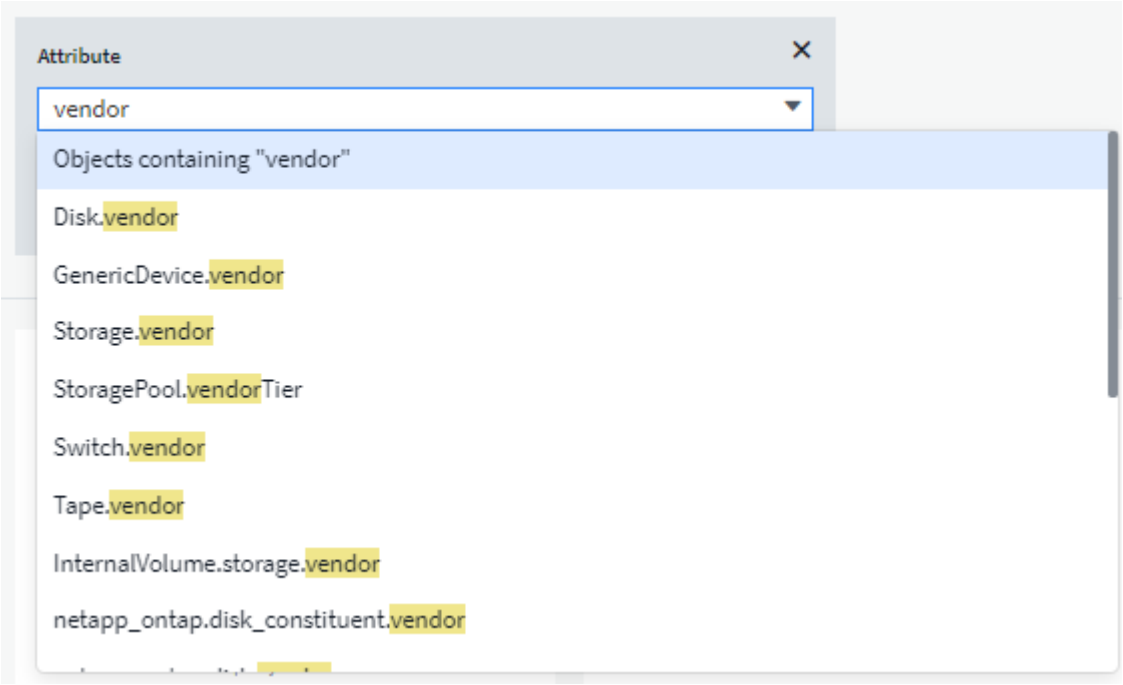
La selezione di una variabile di tipo di attributo consente di filtrare i dati widget contenenti il valore o i valori di attributo specificati. L'esempio riportato di seguito mostra un widget di riga che mostra i trend della memoria libera per i nodi dell'agente. È stata creata una variabile per gli IP del nodo dell'agente, attualmente impostata per visualizzare tutti gli IP:



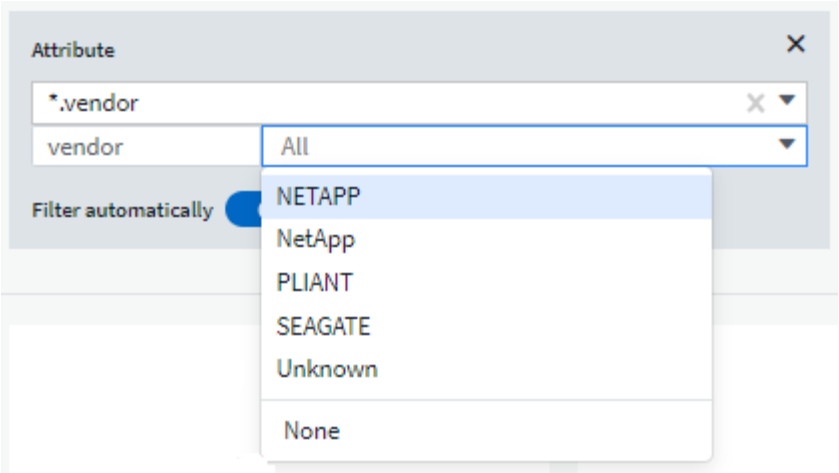
Tuttavia, se si desidera visualizzare temporaneamente solo i nodi nelle singole subnet dell'ambiente, è possibile impostare o modificare la variabile in un IP o IP del nodo agente specifico. Qui vengono visualizzati solo i nodi sulla subnet "123":



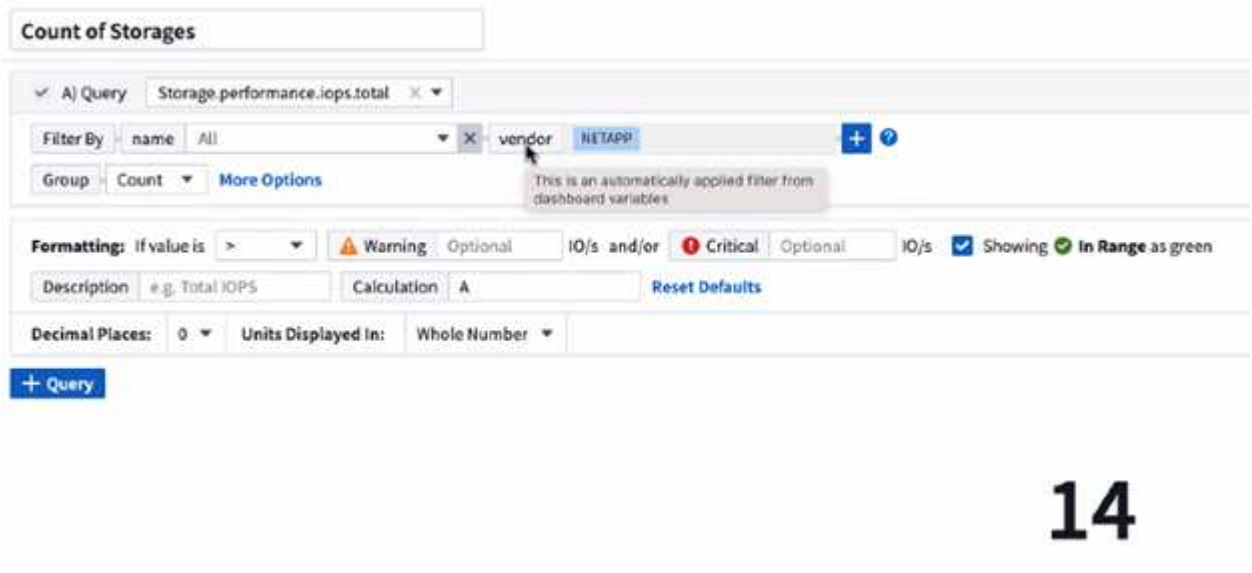
È inoltre possibile impostare una variabile per filtrare gli oggetti *all* con un attributo particolare indipendentemente dal tipo di oggetto, ad esempio gli oggetti con un attributo di "vendor", specificando **.vendor* nel campo della variabile. Non è necessario digitare "*."; se si seleziona l'opzione con il carattere jolly, Cloud Insights lo fornirà.



Quando si seleziona l'elenco a discesa delle scelte per il valore della variabile, i risultati vengono filtrati in modo da visualizzare solo i vendor disponibili in base agli oggetti presenti nella dashboard.



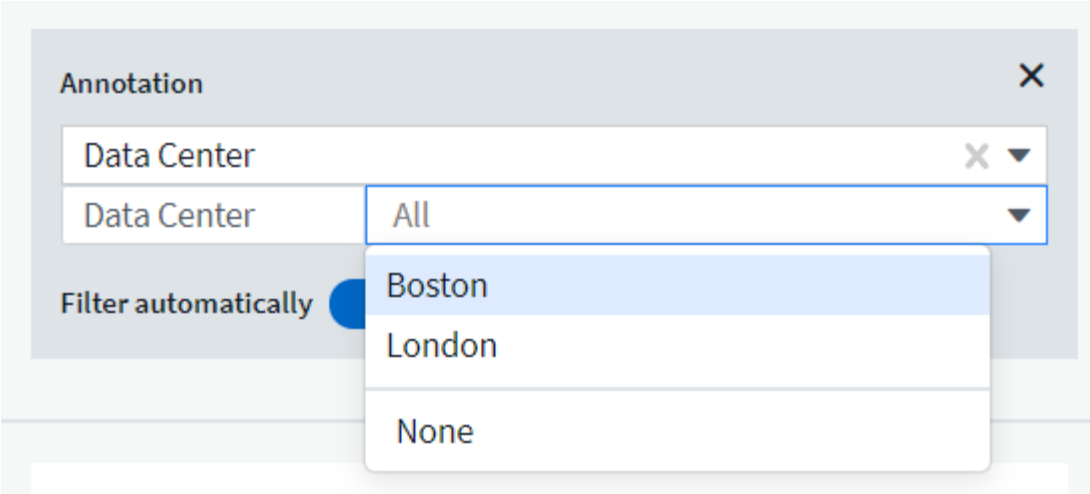
Se modifichi un widget sulla dashboard in cui il filtro degli attributi è rilevante (ovvero, gli oggetti del widget contengono un attributo **.vendor*), il filtro degli attributi viene applicato automaticamente.



L'applicazione delle variabili è semplice quanto la modifica dei dati degli attributi scelti.

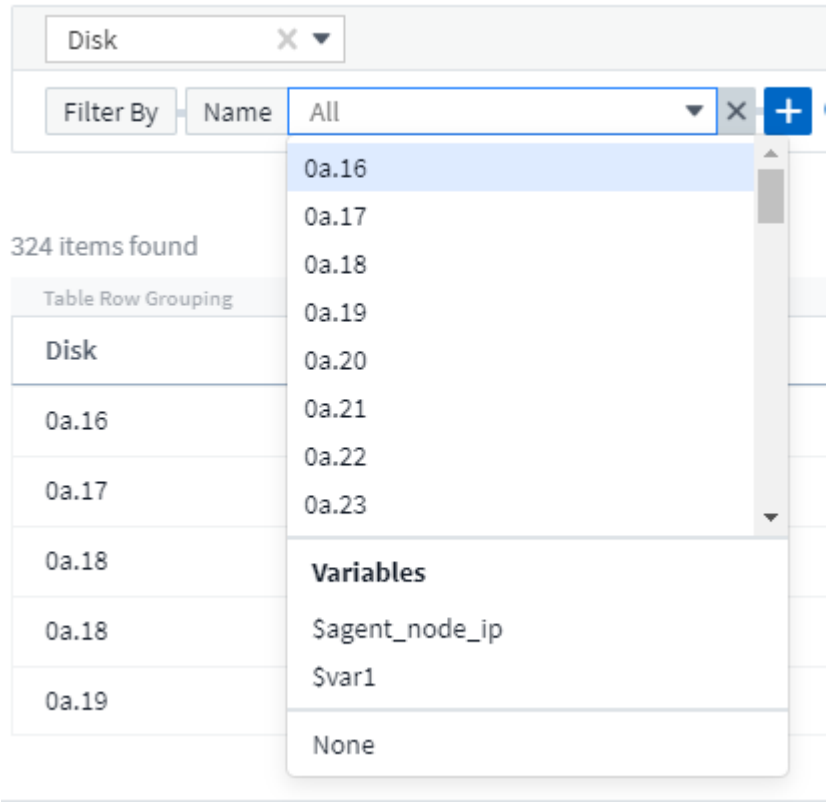
Variabili di annotazione

La scelta di una variabile di annotazione consente di filtrare gli oggetti associati a tale annotazione, ad esempio quelli appartenenti allo stesso data center.



Text, Number, Date o Boolean Variable

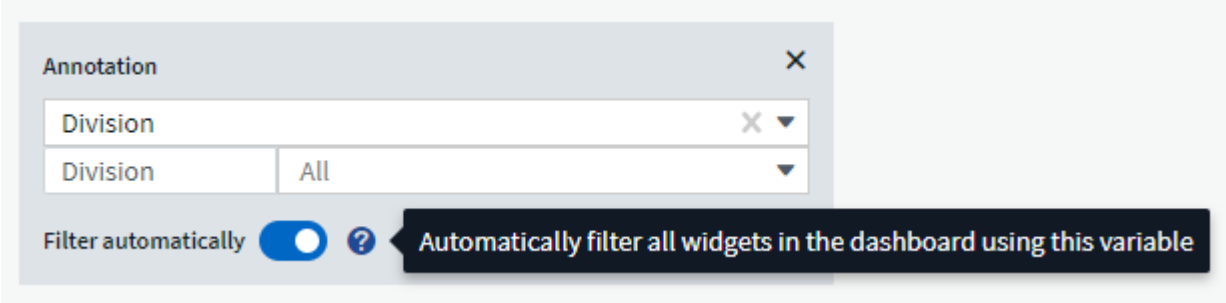
È possibile creare variabili generiche non associate a un particolare attributo selezionando un tipo di variabile *Text*, *Number*, *Boolean* o *Date*. Una volta creata la variabile, è possibile selezionarla in un campo di filtro widget. Quando si imposta un filtro in un widget, oltre ai valori specifici che è possibile selezionare per il filtro, tutte le variabili create per la dashboard vengono visualizzate nell'elenco, raggruppate nella sezione "variabili" dell'elenco a discesa e hanno nomi che iniziano con "". La scelta di una variabile in questo filtro consente di cercare i valori immessi nel campo delle variabili della dashboard stessa. Tutti i widget che utilizzano tale variabile in un filtro verranno aggiornati dinamicamente.



Ambito del filtro variabile

Quando si aggiunge una variabile Annotation o Attribute alla dashboard, la variabile può essere applicata a *tutti* i widget della dashboard, il che significa che tutti i widget della dashboard visualizzano i risultati filtrati in

base al valore impostato nella variabile.



Si noti che solo le variabili di attributo e annotazione possono essere filtrate automaticamente in questo modo. Le variabili non-Annotation o -attribute non possono essere filtrate automaticamente. Ciascun widget deve essere configurato per utilizzare variabili di questi tipi.

Per disattivare il filtraggio automatico in modo che la variabile si applichi solo ai widget in cui è stata impostata, fare clic sul dispositivo di scorrimento "Filter automatically" (filtro automatico) per disattivarla.

Per impostare una variabile in un singolo widget, aprire il widget in modalità di modifica e selezionare l'annotazione o l'attributo specifico nel campo *Filtra per*. Con una variabile Annotation, è possibile selezionare uno o più valori specifici o il nome della variabile (indicato dal simbolo "" iniziale) per consentire la digitazione della variabile a livello di dashboard. Lo stesso vale per le variabili di attributo. Solo i widget per i quali si imposta la variabile mostreranno i risultati filtrati.

Il filtraggio delle variabili è *contestuale*; quando si seleziona un valore di filtro o valori per una variabile, le altre variabili nella pagina mostreranno solo i valori relativi a tale filtro. Ad esempio, quando si imposta un filtro variabile su uno storage specifico *Model*, qualsiasi variabile impostata per filtrare lo storage *Name* mostrerà solo i valori relativi a quel modello.

Per utilizzare una variabile in un'espressione, è sufficiente digitare il nome della variabile come parte dell'espressione, ad esempio *€var1 * 100*. Nelle espressioni possono essere utilizzate solo variabili numeriche. Non è possibile utilizzare annotazioni numeriche o variabili di attributo nelle espressioni.

Il filtraggio delle variabili è *contestuale*; quando si seleziona un valore di filtro o valori per una variabile, le altre variabili nella pagina mostreranno solo i valori relativi a tale filtro. Ad esempio, quando si imposta un filtro variabile su uno storage specifico *Model*, qualsiasi variabile impostata per filtrare lo storage *Name* mostrerà solo i valori relativi a quel modello.

Naming variabile

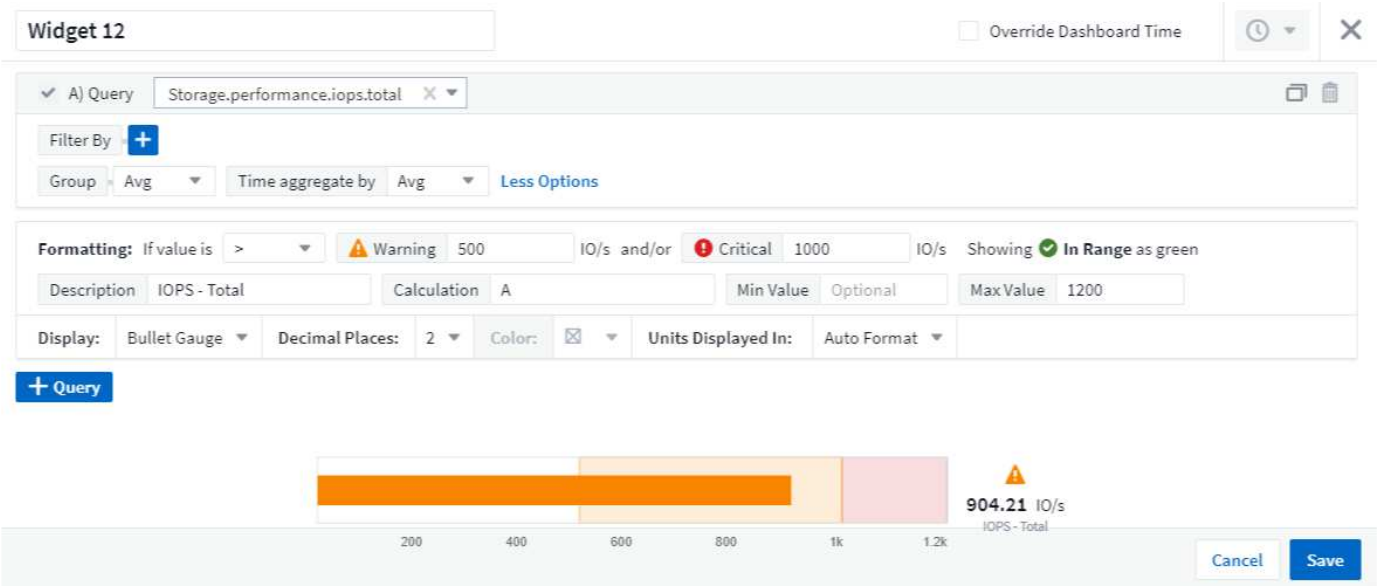
Nomi delle variabili:

- Deve includere solo le lettere a-z, le cifre da 0 a 9, il punto (.), il carattere di sottolineatura (_) e lo spazio ( ).
- Non può contenere più di 20 caratteri.
- Sono sensibili al maiuscolo/minuscolo: Il nome della città e il nome della città sono variabili diverse.
- Non può essere uguale al nome di una variabile esistente.
- Non può essere vuoto.

Formattazione dei widget Gauge

I widget Solid e Bullet Gauge consentono di impostare le soglie per i livelli *Warning* e/o *critical*, fornendo una

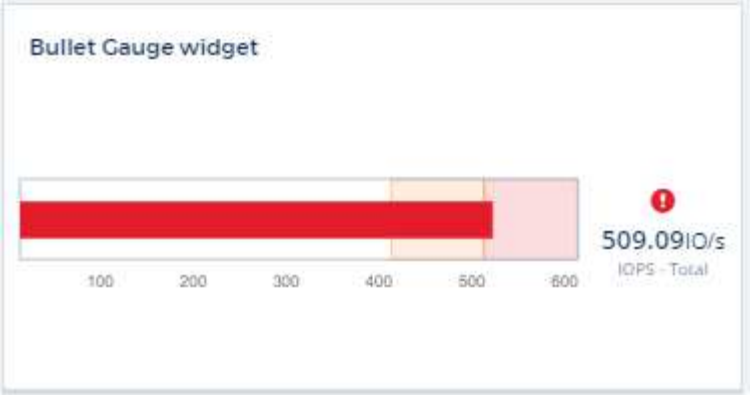
chiara rappresentazione dei dati specificati.



Per impostare la formattazione per questi widget, attenersi alla seguente procedura:

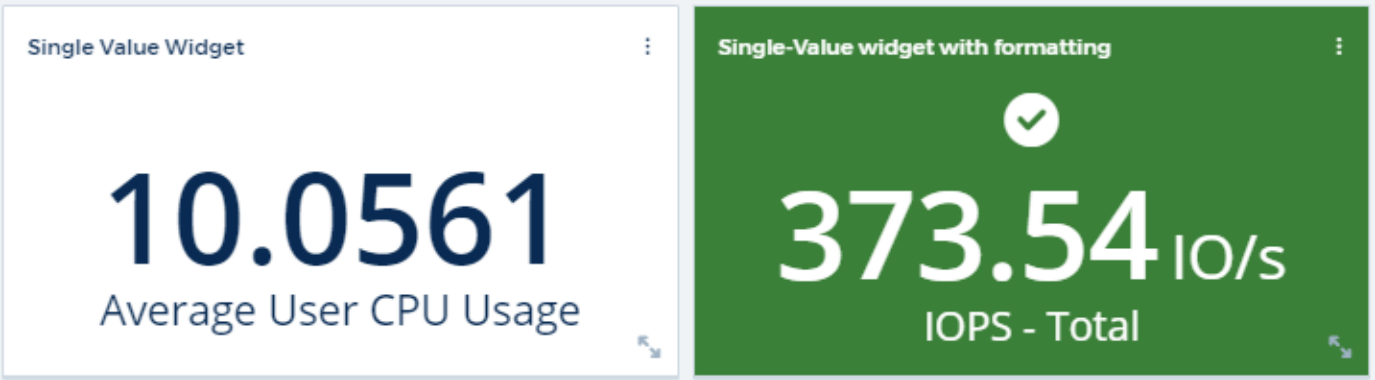
1. Scegliere se si desidera evidenziare valori superiori a (>) o inferiori a (<) soglie. In questo esempio, evidenzieremo valori superiori a (>) i livelli di soglia.
2. Scegliere un valore per la soglia "Avviso". Quando il widget visualizza valori superiori a questo livello, l'indicatore viene visualizzato in arancione.
3. Scegliere un valore per la soglia "critica". Valori superiori a questo livello indicheranno la visualizzazione dell'indicatore in rosso.

È possibile scegliere un valore minimo e massimo per l'indicatore. I valori inferiori al minimo non visualizzano l'indicatore. I valori superiori al valore massimo visualizzano un indicatore completo. Se non si scelgono i valori minimi o massimi, il widget seleziona i valori minimi e massimi ottimali in base al valore del widget.



Formattazione del widget a valore singolo

Nel widget valore singolo, oltre all'impostazione delle soglie di avviso (arancione) e critico (rosso), è possibile scegliere di visualizzare i valori "in Range" (sotto il livello di avviso) con sfondo verde o bianco.



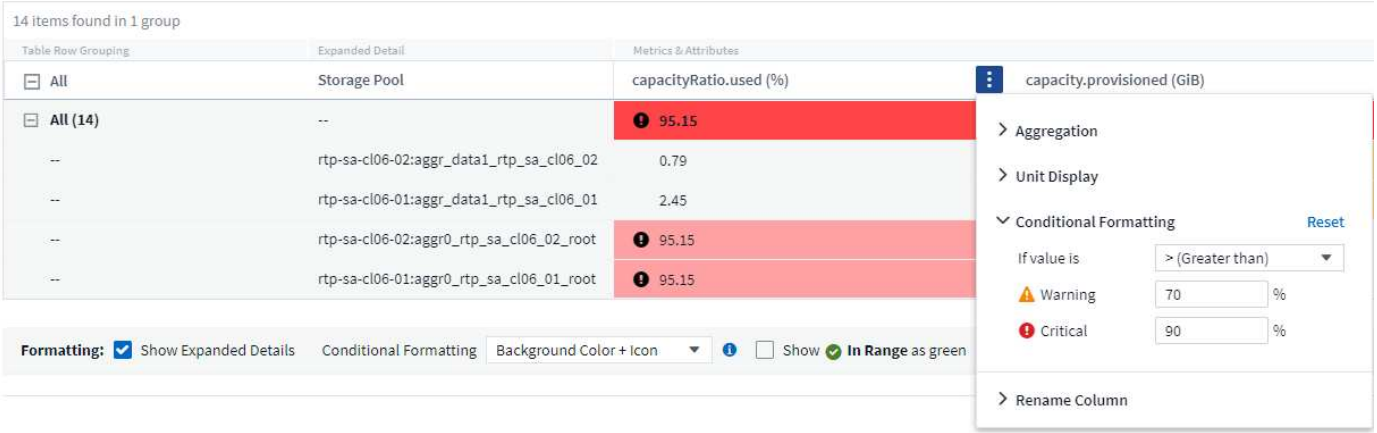
Facendo clic sul collegamento in un widget a valore singolo o in un widget indicatore viene visualizzata una pagina di query corrispondente alla prima query nel widget.

Formattazione dei widget della tabella

Come per i widget a valore singolo e per gli indicatori, è possibile impostare la formattazione condizionale nei widget delle tabelle, consentendo di evidenziare i dati con colori e/o icone speciali.

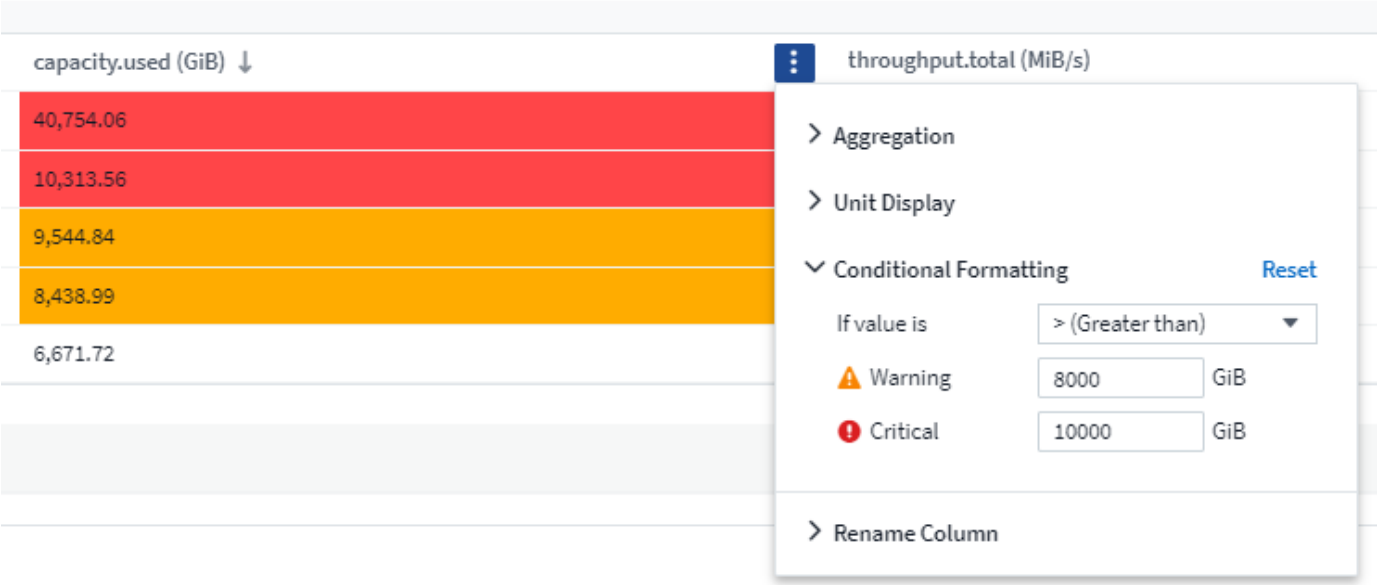
> La formattazione condizionale non è attualmente disponibile nell'edizione federale di Cloud Insights.

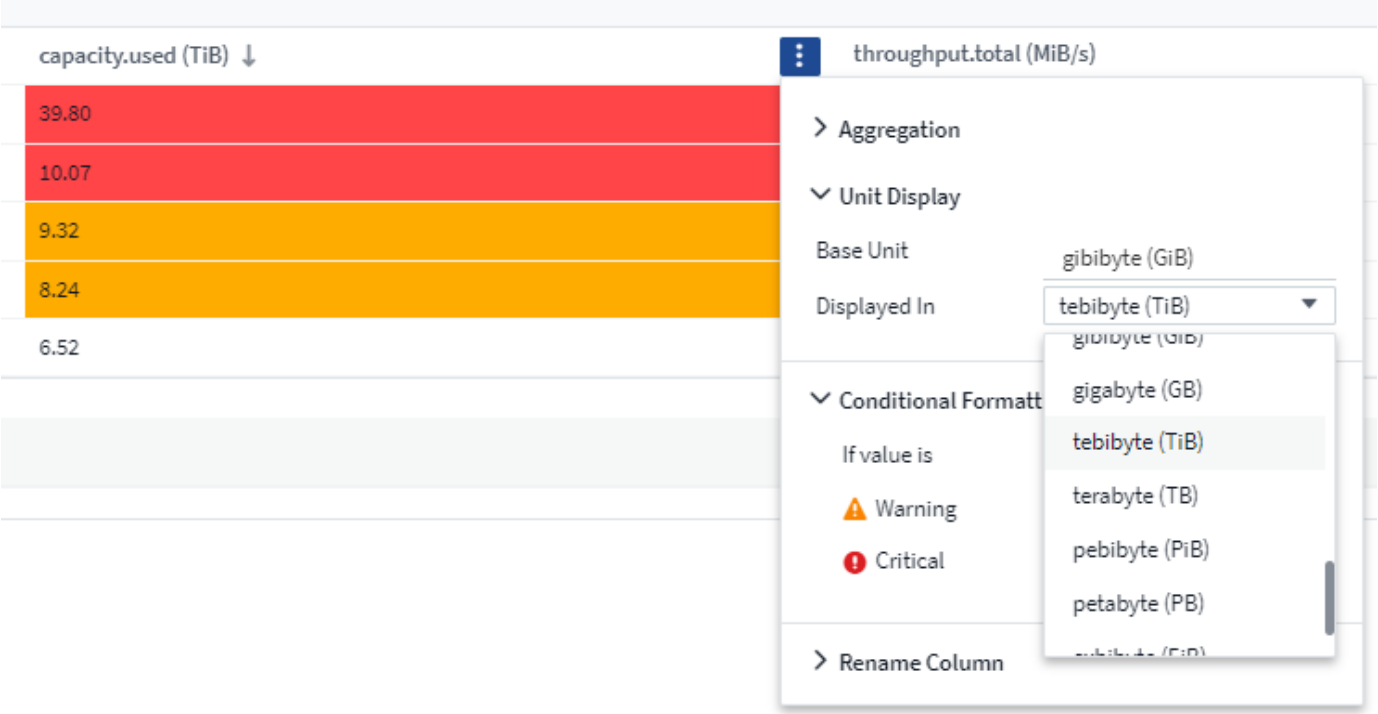
La formattazione condizionale consente di impostare ed evidenziare le soglie di livello di avviso e critico nei widget delle tabelle, offrendo visibilità istantanea agli outlier e ai punti dati eccezionali.



La formattazione condizionale viene impostata separatamente per ogni colonna di una tabella. Ad esempio, è possibile scegliere un set di soglie per una colonna di capacità e un altro set per una colonna di throughput.

Se si modifica la visualizzazione unità per una colonna, la formattazione condizionale rimane e riflette la modifica dei valori. Le immagini riportate di seguito mostrano la stessa formattazione condizionale anche se il display è diverso.



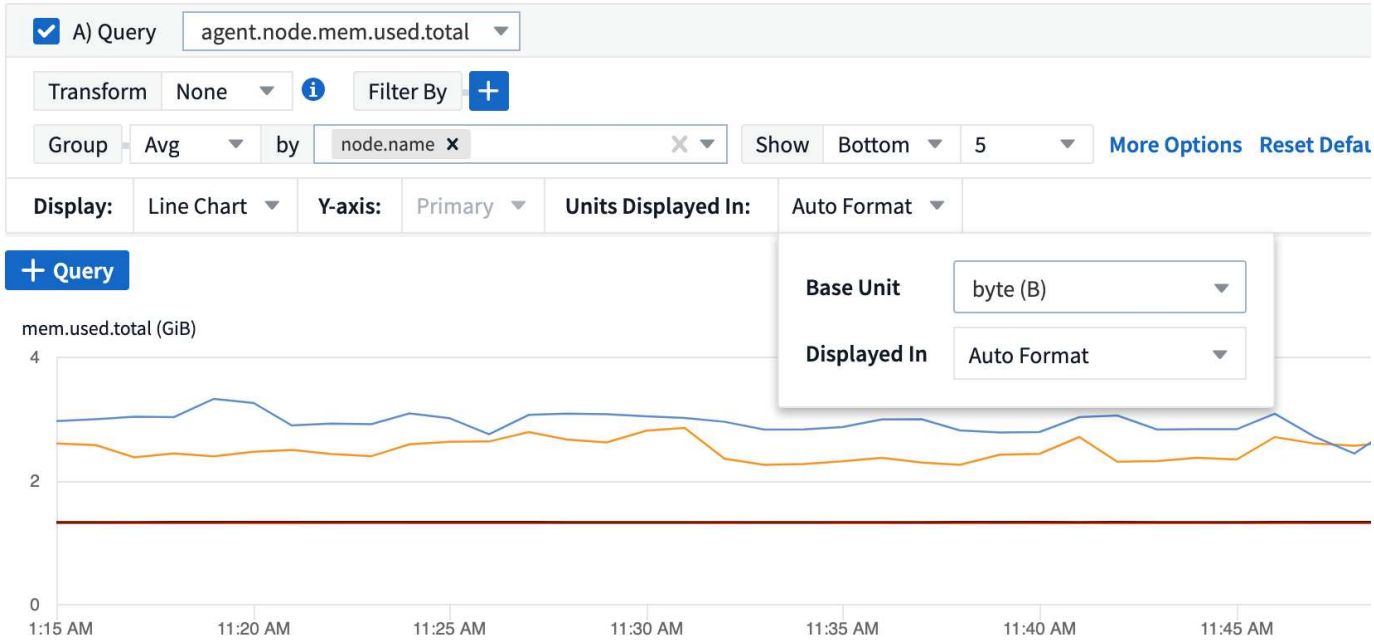


È possibile scegliere se visualizzare la formattazione delle condizioni come colore, icone o entrambi.

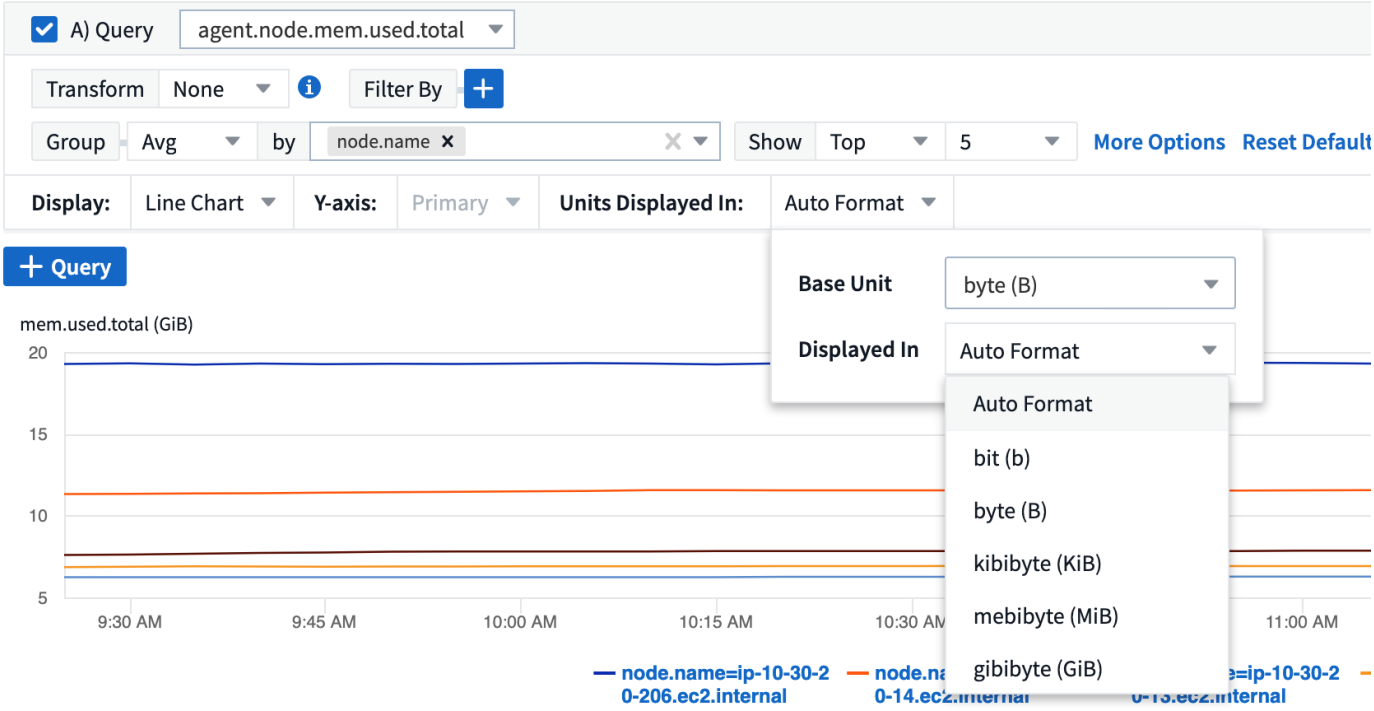
Scelta dell'unità per la visualizzazione dei dati

La maggior parte dei widget di una dashboard consente di specificare le unità in cui visualizzare i valori, ad esempio *Megabyte*, *migliaia*, *percentuale*, *millisecondi (ms)*, ecc. In molti casi, Cloud Insights conosce il formato migliore per i dati acquisiti. Nei casi in cui non si conosce il formato migliore, è possibile impostare il formato desiderato.

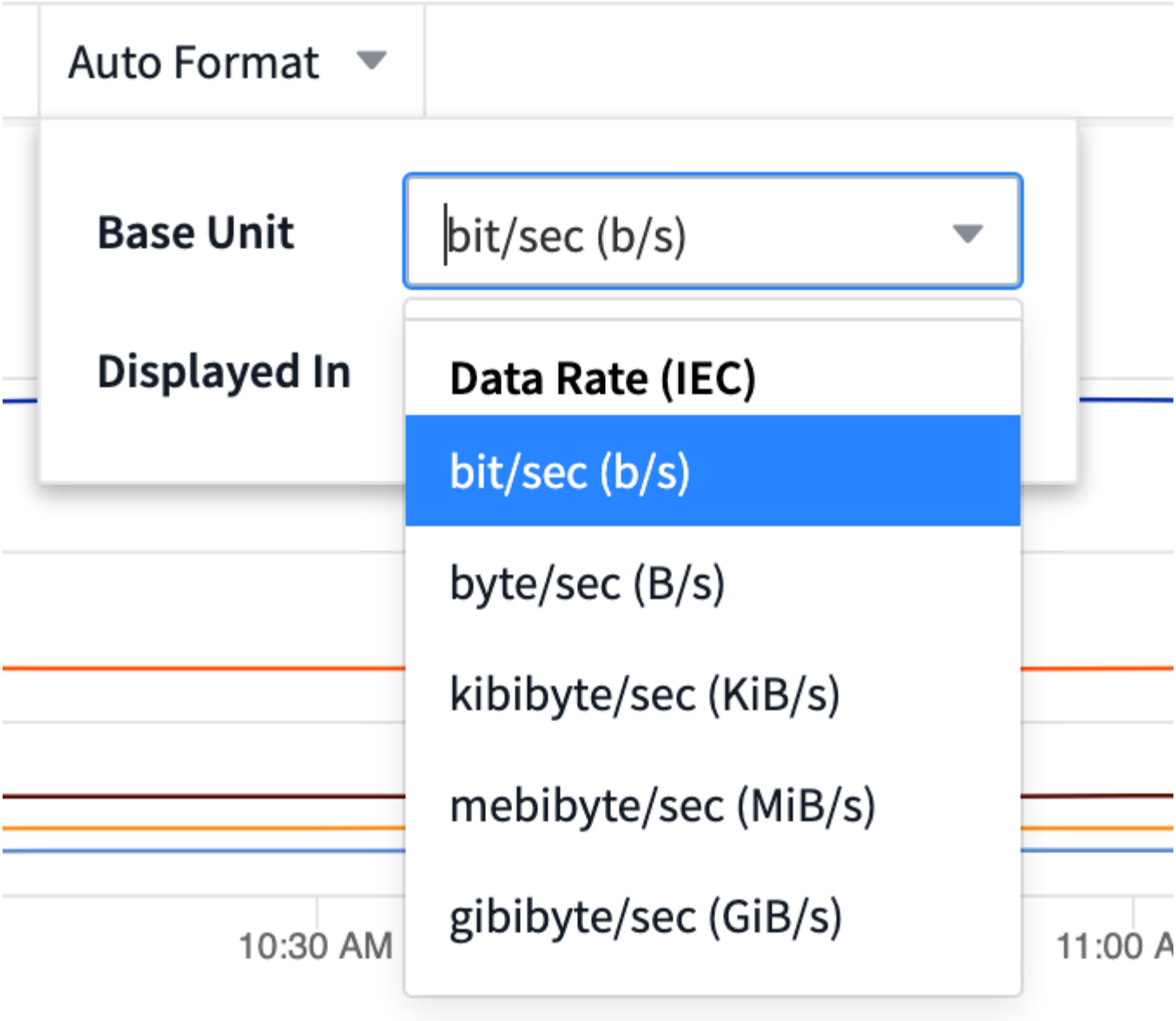
Nell'esempio riportato di seguito, i dati selezionati per il widget sono in *byte* (l'unità dati IEC di base: Vedere la tabella seguente), quindi l'unità base viene selezionata automaticamente come 'byte (B)'. Tuttavia, i valori dei dati sono abbastanza grandi da essere presentati come gibytes (GiB), quindi Cloud Insights per impostazione predefinita formatta automaticamente i valori come GiB. L'asse Y del grafico mostra "GiB" come unità di visualizzazione e tutti i valori sono visualizzati in termini di unità.



Se si desidera visualizzare il grafico in un'unità diversa, è possibile scegliere un altro formato in cui visualizzare i valori. Poiché l'unità di base in questo esempio è *byte*, è possibile scegliere tra i formati supportati "byte-based": Bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibyte (GiB). L'etichetta e i valori dell'asse Y cambiano in base al formato scelto.



Nei casi in cui l'unità base non sia nota, è possibile assegnare un'unità tra "unità disponibili"oppure digitare il proprio. Una volta assegnata un'unità base, è possibile scegliere di visualizzare i dati in uno dei formati supportati appropriati.



Per cancellare le impostazioni e ricominciare, fare clic su **Reset Defaults** (Ripristina impostazioni predefinite).

Una parola su Auto-Format

La maggior parte delle metriche viene riportata dai data collezionisti nell'unità più piccola, ad esempio come un numero intero, ad esempio 1,234,567,890 byte. Per impostazione predefinita, Cloud Insights formatterà automaticamente il valore per la visualizzazione più leggibile. Ad esempio, un valore dei dati di 1,234,567,890 byte viene automaticamente formattato in 1.23 *Gibibytes*. È possibile scegliere di visualizzarlo in un altro formato, ad esempio *Mebibytes*. Il valore viene visualizzato di conseguenza.

> Cloud Insights utilizza gli standard di denominazione dei numeri in inglese americano. Il "miliardo" americano equivale a "migliaia di milioni".

Widget con query multiple

Se si dispone di un widget Time-series (ad esempio linea, spline, area, area sovrapposta) che ha due query in cui entrambe sono tracciate l'asse Y primario, l'unità base non viene visualizzata nella parte superiore dell'asse Y. Tuttavia, se il widget dispone di una query sull'asse Y primario e di una query sull'asse Y

secondario, vengono visualizzate le unità di base per ciascuno di essi.

Se il widget dispone di tre o più query, le unità di base non vengono visualizzate sull'asse Y.

Unità disponibili

La seguente tabella mostra tutte le unità disponibili per categoria.

Categoria	Unità
Valuta	dollaro centesimo
Dati (IEC)	bit byte kibibyte mebibyte gibibyte tebibyte pebibyte exbibyte
Data arate (IEC)	bit/sec byte/sec kibibyte/sec mebibyte/sec gibibyte/sec tebibyte/sec pebibyte/sec
Dati (metrico)	kilobyte megabyte gigabyte terabyte petabyte exabyte
Datarato (metrico)	kilobyte/sec megabyte/sec gigabyte/sec terabyte/sec petabyte/sec exabyte/sec
IEC	kibi mebi tebi pebi exbi
Decimale	migliaia di miliardi di miliardi di miliardi
Percentuale	percentuale
Ora	nanocondo microsecondo millisecondo minuto ora
Temperatura	celsius fahrenheit
Frequenza	hertz kilohertz megahertz gigahertz
CPU	nanocores microcore millicores core kilocores megacores gigacores teracores petacores exacores
Throughput	I/o Ops/sec Ops/sec Requests/sec Requests/sec Reads/sec Scritture/sec Ops/min Reads/min Scritture/min

Modalità TV e aggiornamento automatico

I dati nei widget su Dashboard e Asset Landing Pages si aggiornano automaticamente in base a un intervallo di refresh determinato dal Dashboard Time Range selezionato (o intervallo di tempo widget, se impostato per sostituire l'ora del dashboard). L'intervallo di refresh si basa sul fatto che il widget sia costituito da serie temporali (linea, spline, area, grafico a aree sovrapposte) o da serie non temporali (tutti gli altri grafici).

Intervallo di tempo della dashboard	Intervallo di aggiornamento Time-Series	Intervallo di aggiornamento non Time-Series
Ultimi 15 minuti	10 secondi	1 minuto
Ultimi 30 minuti	15 secondi	1 minuto
Ultimi 60 minuti	15 secondi	1 minuto
Ultime 2 ore	30 secondi	5 minuti
Ultime 3 ore	30 secondi	5 minuti
Ultime 6 ore	1 minuto	5 minuti
Ultime 12 ore	5 minuti	10 minuti
Ultime 24 ore	5 minuti	10 minuti
Ultimi 2 giorni	10 minuti	10 minuti
Ultimi 3 giorni	15 minuti	15 minuti
Ultimi 7 giorni	1 ora	1 ora
Ultimi 30 giorni	2 ore	2 ore

Ciascun widget visualizza l'intervallo di aggiornamento automatico nell'angolo superiore destro del widget.

L'aggiornamento automatico non è disponibile per l'intervallo di tempo della dashboard personalizzata.

Se combinato con la modalità **TV**, l'aggiornamento automatico consente la visualizzazione quasi in tempo reale dei dati su una dashboard o una pagina di risorse. La modalità TV offre una visualizzazione semplice; il menu di navigazione è nascosto, offrendo una maggiore capacità di visualizzazione dei dati, così come il pulsante Edit. La modalità TV ignora i timeout Cloud Insights tipici, lasciando il display attivo fino a quando non viene disconnesso manualmente o automaticamente dai protocolli di sicurezza autorizzati.

> Poiché NetApp Cloud Central ha un timeout di accesso utente di 7 giorni, Cloud Insights deve disconnettersi anche con quell'evento. Puoi semplicemente effettuare nuovamente l'accesso e la dashboard continuerà a essere visualizzata.

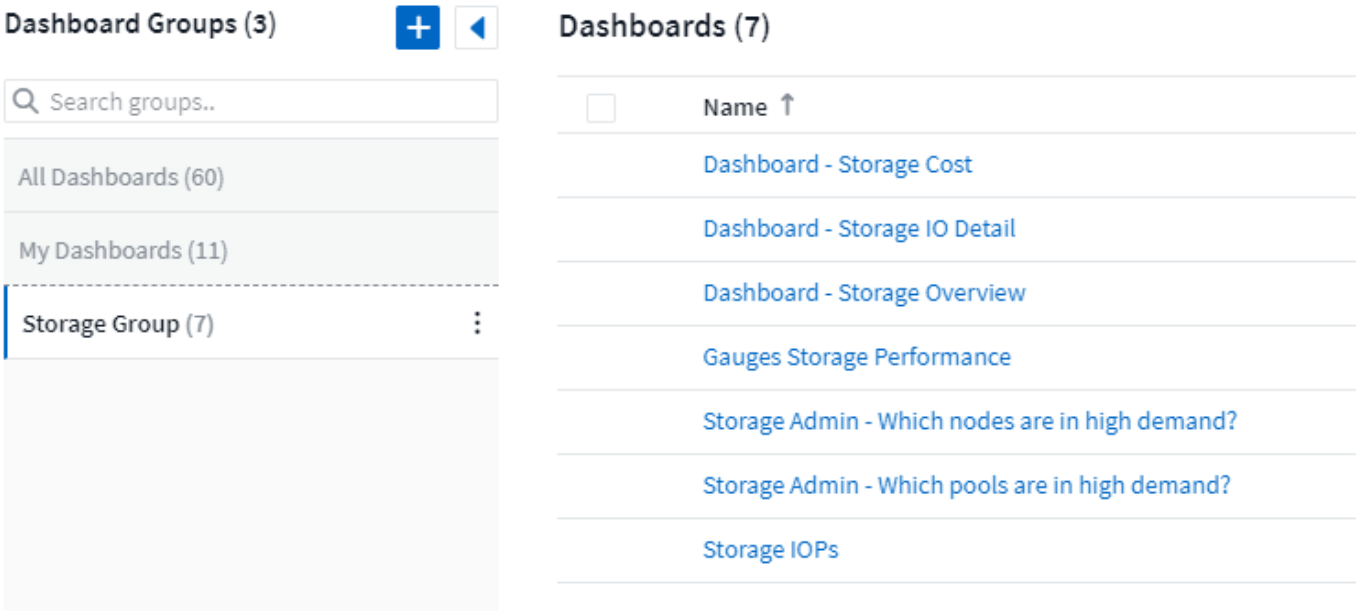
- Per attivare la modalità TV, fare clic su 

pulsante.
- Per disattivare la modalità TV, fare clic sul pulsante **Exit** in alto a sinistra sullo schermo. 

È possibile sospendere temporaneamente l'aggiornamento automatico facendo clic sul pulsante Pause (Pausa) nell'angolo in alto a destra. Durante la pausa, il campo intervallo di tempo della dashboard visualizza l'intervallo di tempo attivo dei dati in pausa. I dati sono ancora in fase di acquisizione e aggiornamento mentre l'aggiornamento automatico è in pausa. Fare clic sul pulsante Riprendi per continuare l'aggiornamento automatico dei dati.

Gruppi di dashboard

Il raggruppamento consente di visualizzare e gestire dashboard correlati. Ad esempio, è possibile disporre di un gruppo di dashboard dedicato allo storage nel proprio ambiente. I gruppi di dashboard sono gestiti nella pagina **Dashboard > Mostra tutti i dashboard**.



Per impostazione predefinita, vengono visualizzati due gruppi:

- **Tutti i dashboard** elenca tutti i dashboard creati, indipendentemente dal proprietario.
- **My Dashboard** elenca solo i dashboard creati dall'utente corrente.

Il numero di dashboard contenuti in ciascun gruppo viene visualizzato accanto al nome del gruppo.

Per creare un nuovo gruppo, fare clic sul pulsante **"+" Create New Dashboard Group** (Crea nuovo gruppo dashboard). Immettere un nome per il gruppo e fare clic su **Create Group** (Crea gruppo). Viene creato un gruppo vuoto con tale nome.

Per aggiungere dashboard al gruppo, fare clic sul gruppo *All Dashboards* per visualizzare tutti i dashboard dell'ambiente, quindi fare clic su *My Dashboards* se si desidera visualizzare solo i dashboard in uso ed eseguire una delle seguenti operazioni:

- Per aggiungere una singola dashboard, fare clic sul menu a destra della dashboard e selezionare *Aggiungi al gruppo*.
- Per aggiungere più dashboard a un gruppo, selezionarle facendo clic sulla casella di controllo accanto a ciascuna dashboard, quindi fare clic sul pulsante **azioni in blocco** e selezionare *Aggiungi al gruppo*.

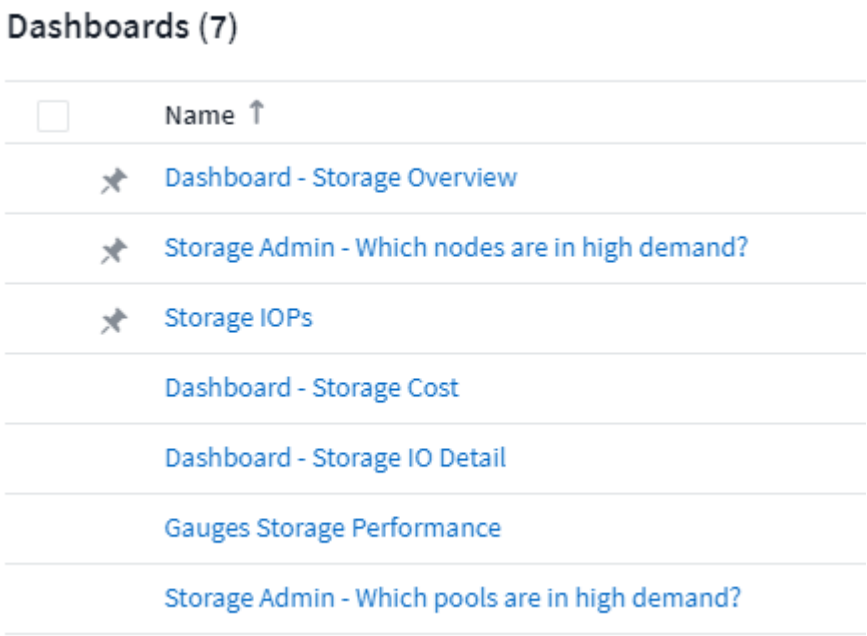
Rimuovere i dashboard dal gruppo corrente nello stesso modo selezionando *Remove from Group*. Non è possibile rimuovere i dashboard dal gruppo *tutti i dashboard* o *i miei dashboard*.

> La rimozione di una dashboard da un gruppo non elimina la dashboard da Cloud Insights. Per rimuovere completamente una dashboard, selezionarla e fare clic su *Delete*. In questo modo viene rimosso da tutti i gruppi a cui apparteneva e non è più disponibile per nessun utente.

Fissa i tuoi dashboard preferiti

È possibile gestire ulteriormente le dashboard inserendo quelle preferite nella parte superiore dell'elenco della dashboard. Per fissare una dashboard, fare clic sul pulsante di identificazione visualizzato quando si passa il puntatore del mouse su una dashboard in un elenco qualsiasi.

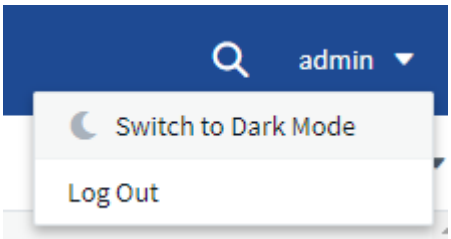
Pin/unpin della dashboard è una preferenza utente individuale e indipendente dal gruppo (o dai gruppi) a cui appartiene la dashboard.



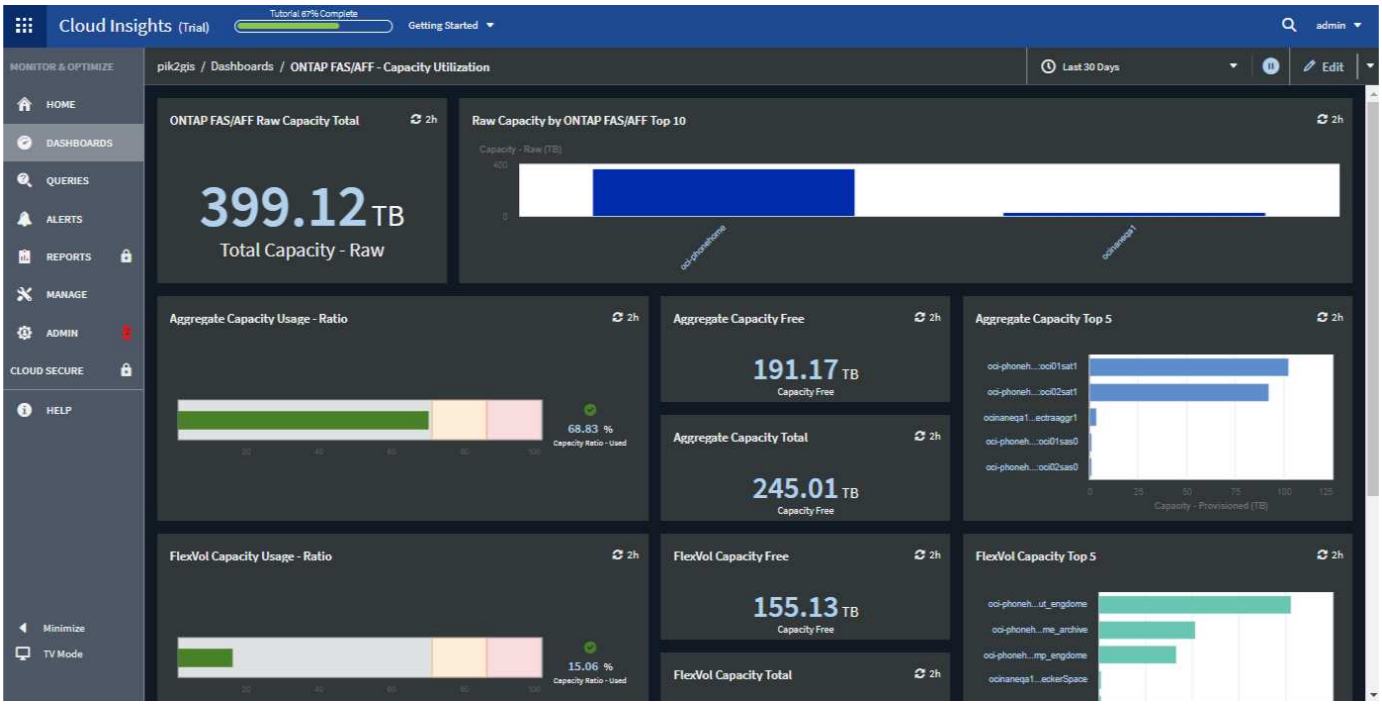
Tema scuro

È possibile scegliere di visualizzare Cloud Insights utilizzando un tema chiaro (impostazione predefinita), che visualizza la maggior parte delle schermate utilizzando uno sfondo chiaro con testo scuro, o un tema scuro che visualizza la maggior parte delle schermate utilizzando uno sfondo scuro con testo chiaro.

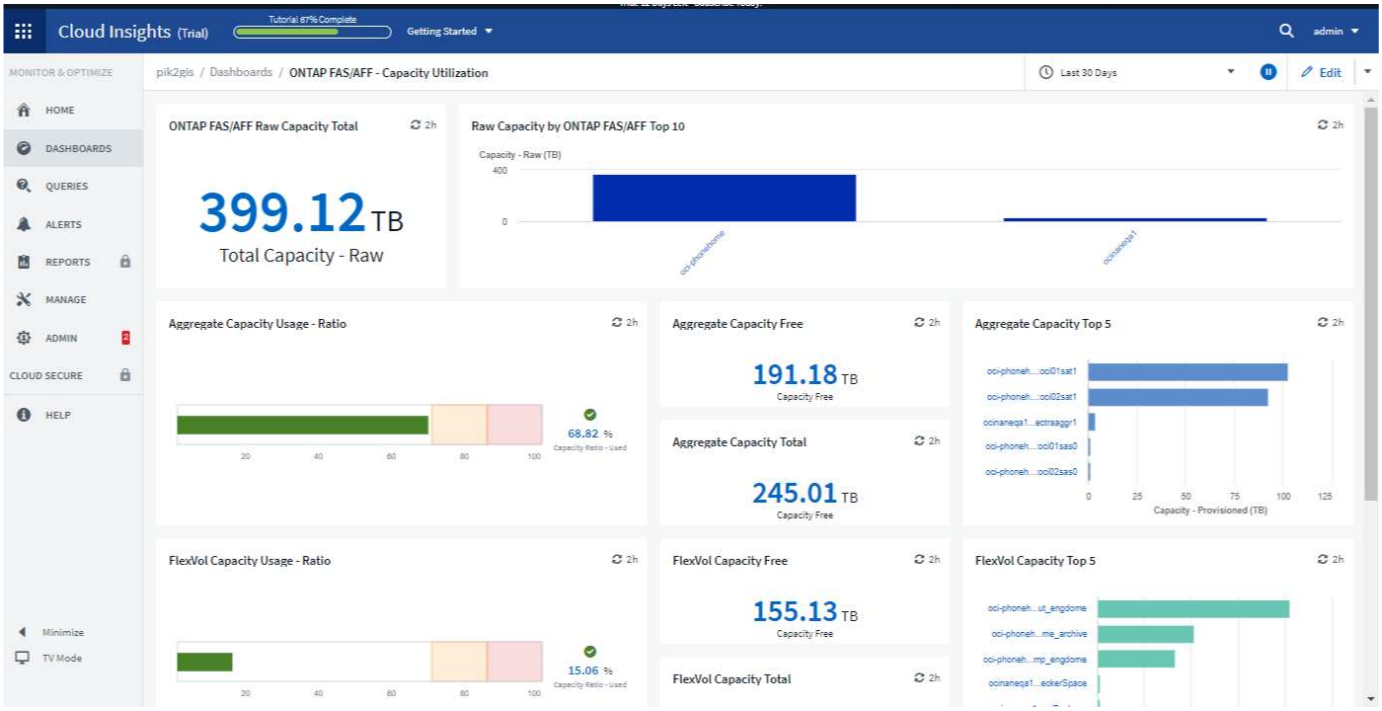
Per passare da un tema chiaro a uno scuro e viceversa, fare clic sul pulsante Username (Nome utente) nell'angolo superiore destro dello schermo e scegliere il tema desiderato.



Vista Dashboard tema scuro:



Vista dashboard tema
luce:



Alcune aree dello schermo, ad esempio alcuni grafici di widget, continuano a mostrare sfondi chiari anche quando vengono visualizzati in un tema scuro.

Interpolazione del grafico a linee

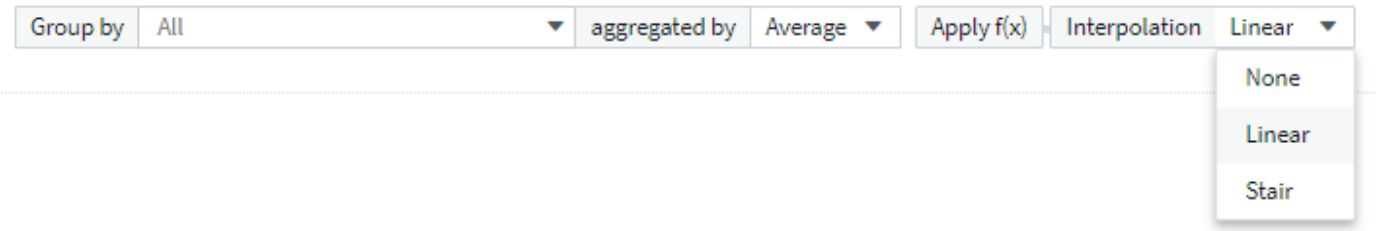
I diversi data raccoglitori spesso eseguono il polling dei dati a intervalli diversi. Ad esempio, il data collector A può eseguire il polling ogni 15 minuti, mentre il data collector B esegue il polling ogni cinque minuti. Quando un widget di un grafico a linee (anche diagrammi di spline, area e area sovrapposta) aggrega questi dati da più raccolte di dati in una singola riga (ad esempio, quando il widget raggruppa per "tutti"), Inoltre, aggiornando la

linea ogni cinque minuti, i dati del raccoglitore B possono essere mostrati con precisione mentre i dati del raccoglitore A possono presentare lacune, influenzando così l'aggregato fino a quando il raccoglitore A esegue di nuovo il polling.

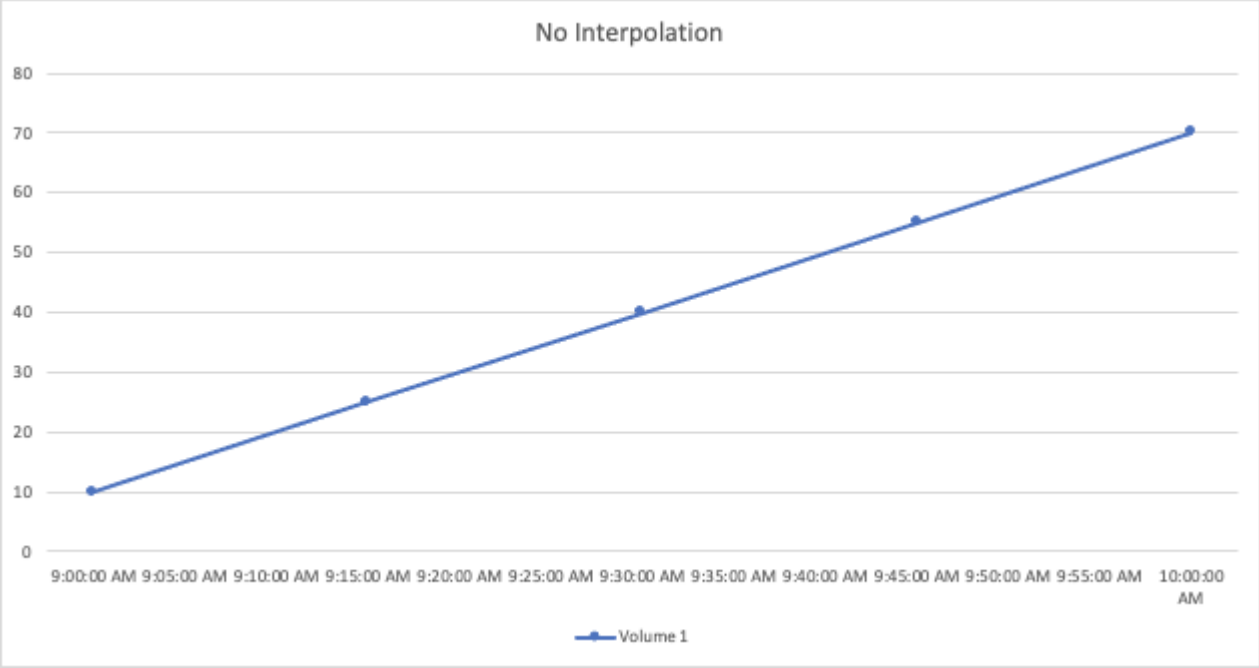
Per ridurre questo problema, Cloud Insights interpola i dati durante l'aggregazione, utilizzando i punti dati circostanti per fare una "ipotesi migliore" sui dati fino a quando i data collezioner non eseguono nuovamente il polling. Puoi sempre visualizzare i dati degli oggetti di ciascun data collector individualmente regolando il raggruppamento del widget.

Metodi di interpolazione

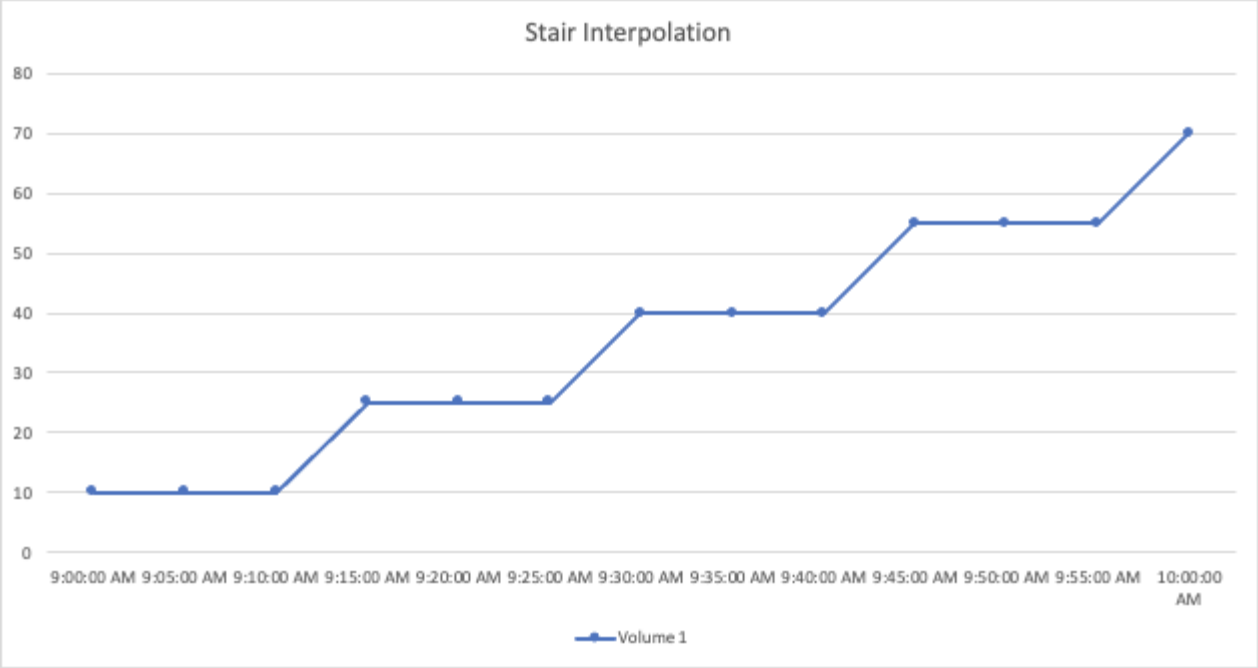
Quando si crea o si modifica un grafico a linee (o un grafico a spline, area o area sovrapposta), è possibile impostare il metodo di interpolazione su uno dei tre tipi. Nella sezione "Raggruppa per", scegliere l'interpolazione desiderata.



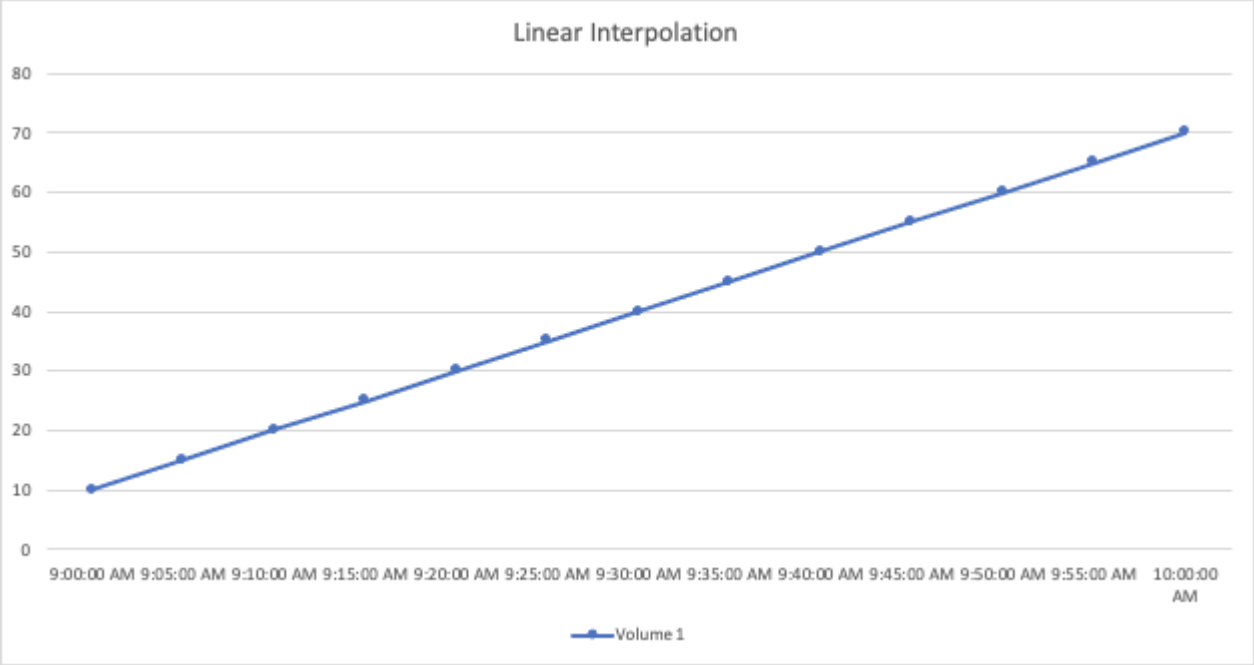
- **Nessuno**: Non fare nulla, ad esempio non generare punti intermedi.



- **Stair**: Viene generato un punto dal valore del punto precedente. In linea retta, questo viene visualizzato come un tipico layout "scala".



- **Lineare**: Viene generato un punto come valore tra due punti di connessione. Genera una linea che assomiglia alla linea che collega i due punti, ma con punti dati aggiuntivi (interpolati).



Dashboard di esempio

Esempio di dashboard: Performance delle macchine virtuali

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 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, puoi fare cose come la visualizzazione delle performance dello storage back-end rispetto alle performance delle macchine virtuali front-end o la visualizzazione della latenza delle macchine virtuali rispetto alla domanda di i/O.

A proposito di questa attività

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 qualsiasi dato di performance scelto, in modo da puntare alle tue Best practice operative.

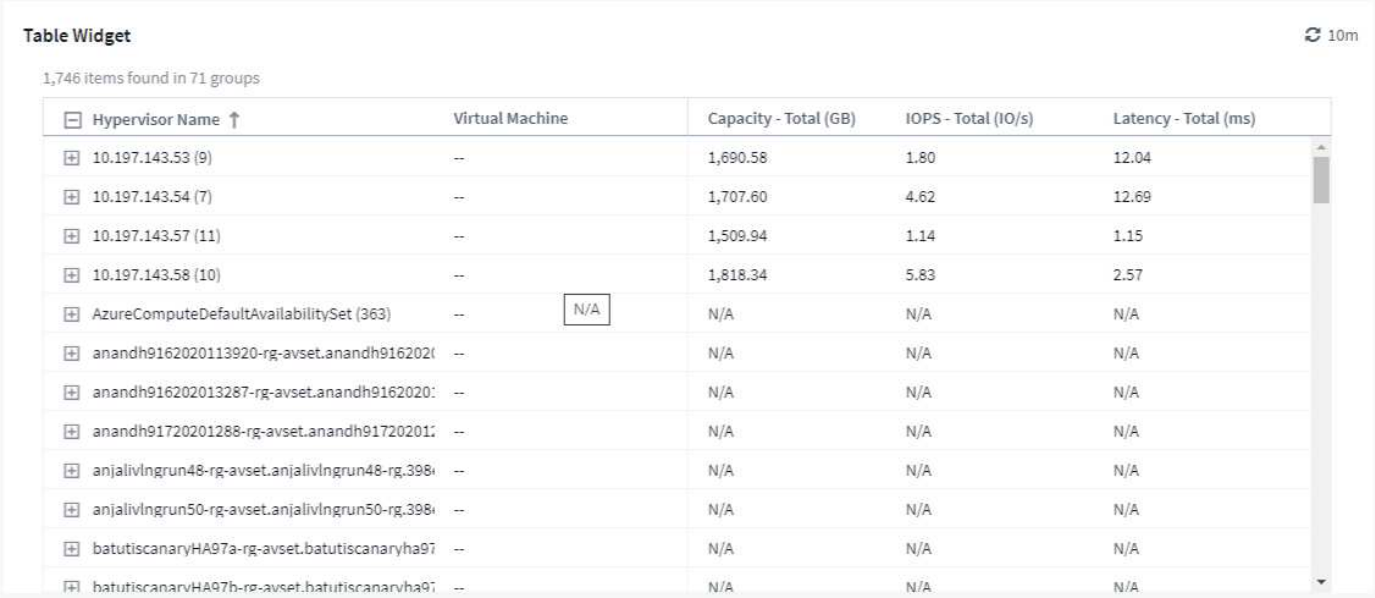
Fasi

1. Accedere a Insight come utente con autorizzazioni amministrative.
2. Dal menu **Dashboard**, selezionare **[+nuovo dashboard]**.

   Viene visualizzata la pagina **nuovo dashboard**.

3. Nella parte superiore della pagina, immettere un nome univoco per la dashboard, ad esempio "VM Performance by Application" (prestazioni VM per applicazione).
4. Fare clic su **Save** (Salva) per salvare la dashboard con il nuovo nome.
5. Iniziamo ad aggiungere i nostri widget. Se necessario, fare clic sull'icona **Edit** (Modifica) per attivare la modalità Edit (Modifica).
6. Fare clic sull'icona **Aggiungi widget** e selezionare **Tabella** per aggiungere un nuovo widget tabella alla dashboard.

   Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). I dati predefiniti visualizzati sono relativi a tutti gli storage dell'ambiente in uso.



1. Possiamo personalizzare questo widget. Nel campo Name (Nome) in alto, eliminare "Widget 1" e immettere "Virtual Machine Performance table" (Tabella delle prestazioni della macchina virtuale).
2. 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.

3. Aggiungiamo alcune colonne alla tabella. Fare clic sull'icona ingranaggio a destra e selezionare *Hypervisor name*, *IOPS - Total* e *Latency - Total*. Puoi anche provare a digitare il nome nella ricerca per visualizzare rapidamente il campo desiderato.

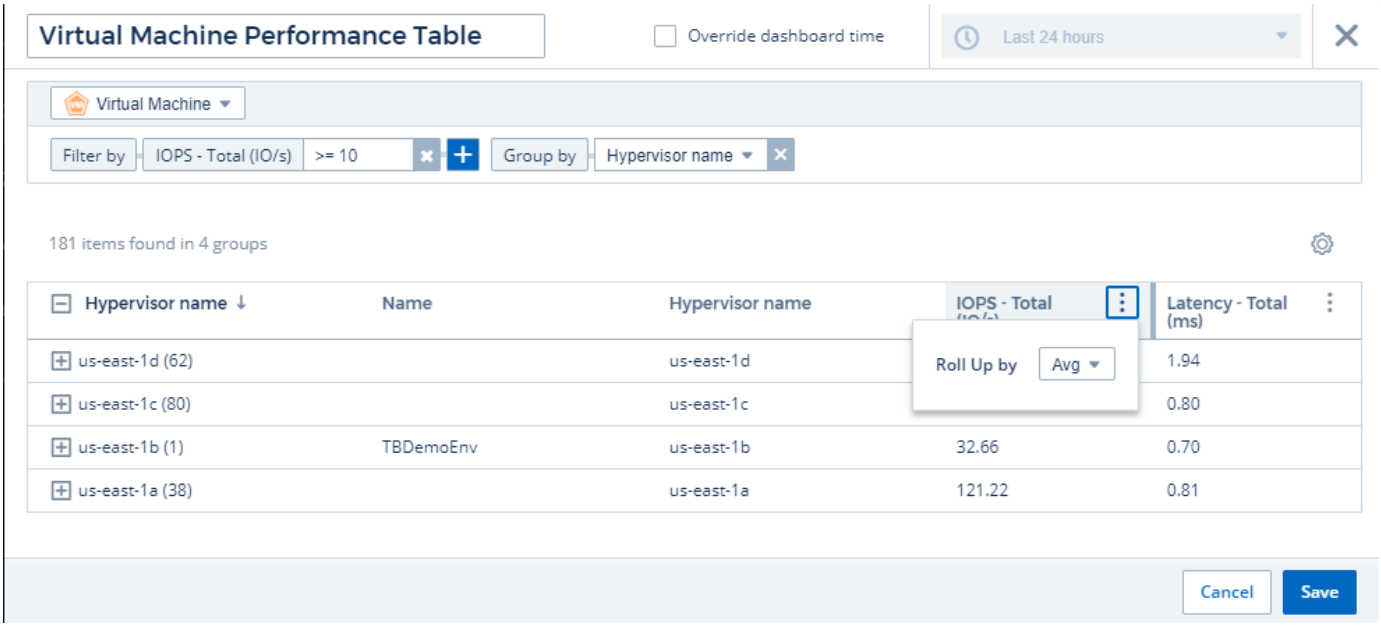
   Queste colonne vengono ora visualizzate nella tabella. È possibile ordinare la tabella in base a una di queste colonne. Le colonne vengono visualizzate nell'ordine in cui sono state aggiunte al widget.

4. 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*. Fare clic su **qualsiasi** e digitare "10" nel campo **da**. Lasciare vuoto il campo **to**. Fare clic su outsude the filter field (fuori dal campo del filtro) o premere Invio per impostare il filtro.

   La tabella ora mostra solo le macchine virtuali con 10 o più IOPS totali.

5. 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 *nome hypervisor*. 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.



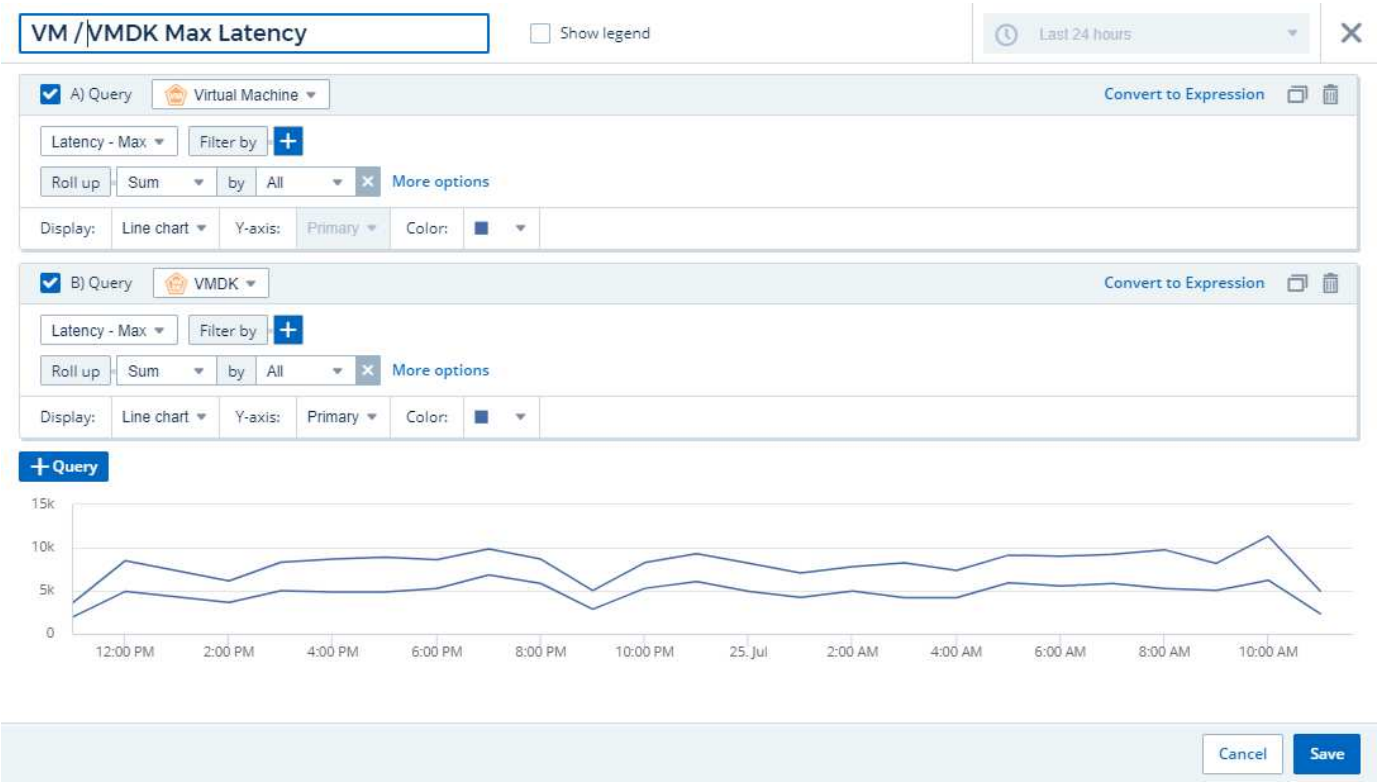
1. Una volta personalizzato il widget della tabella in base alle proprie esigenze, fare clic sul pulsante **[Salva]**.

   Il widget della tabella viene salvato nella dashboard.

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.

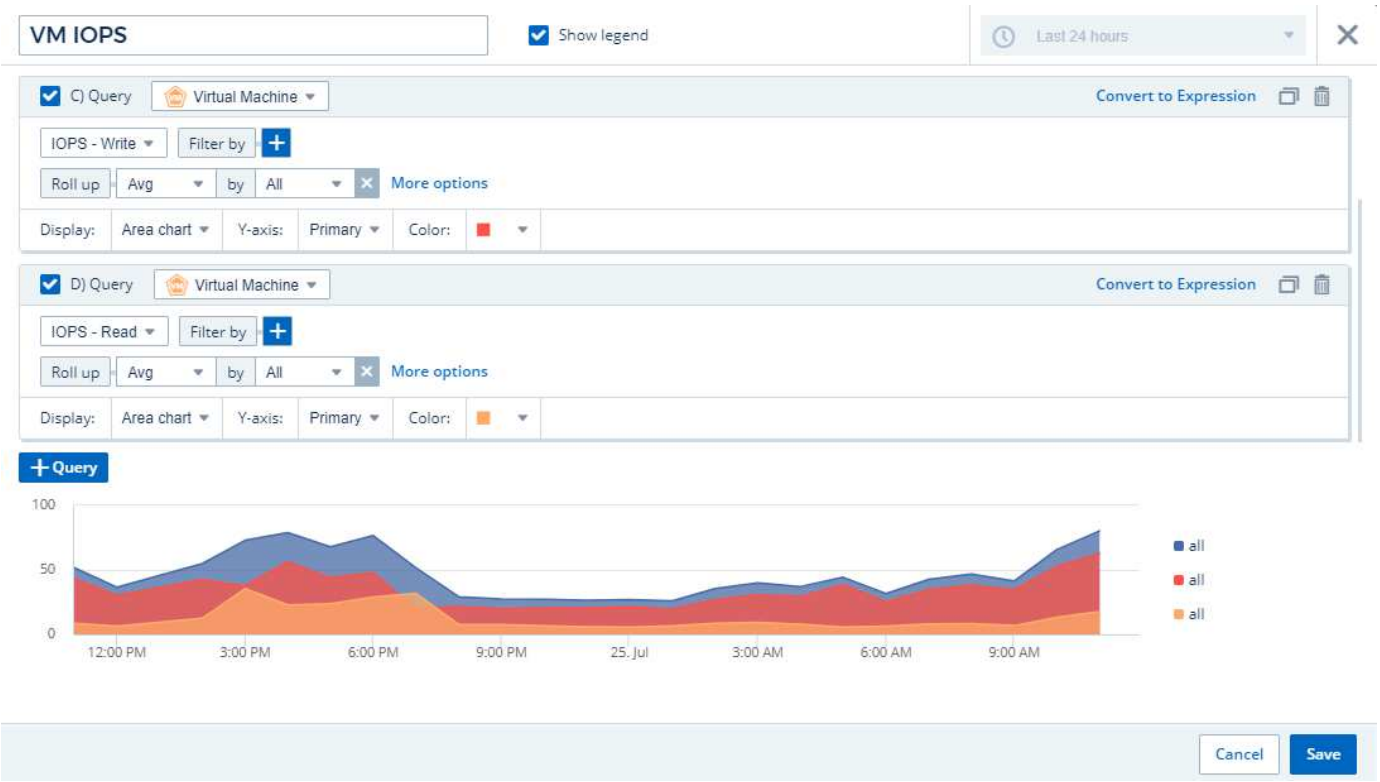
Successivamente aggiungeremo alcuni grafici per mostrare le nostre performance delle macchine virtuali. Creiamo un grafico a linee che confronta la latenza delle macchine virtuali con la latenza VMDK.

1. Se necessario, fare clic sull'icona **Edit** (Modifica) sulla dashboard per attivare la modalità Edit (Modifica).
2. Fare clic sull'icona **[Add widget]** e selezionare *Line Chart* per aggiungere un nuovo widget line chart alla dashboard.
3. Viene visualizzata la finestra di dialogo **Edit Widget** (Modifica widget). Assegnare un nome a questo widget "VM / VMDK Max Latency"
4. Selezionare **Virtual Machine** e scegliere *Latency - Max*. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere *sum* per *all*. Visualizzare questi dati come *grafico a linee* e lasciare *asse Y* come *primario*.
5. Fare clic sul pulsante **[+Query]** per aggiungere una seconda riga di dati. Per questa riga, selezionare *VMDK* e *latenza - Max*. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere *sum* per *all*. Visualizzare questi dati come *grafico a linee* e lasciare *asse Y* come *primario*.
6. Fare clic su **[Save]** per aggiungere questo widget alla dashboard.



Successivamente, aggiungeremo un grafico che mostra gli IOPS totali, di lettura e scrittura delle macchine virtuali in un singolo grafico.

1. Fare clic sull'icona **[Aggiungi widget]** e selezionare *Area Chart* per aggiungere un nuovo widget per area chart alla dashboard.
2. Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Assegna un nome a questo widget "VM IOPS"
3. Selezionare **Virtual Machine** e scegliere *IOPS - Total*. Impostare i filtri desiderati oppure lasciare vuoto il campo **Filtra per**. Per **Roll up**, scegliere *sum* per *all*. Visualizzare questi dati come *Area Chart* e lasciare *asse Y* come *primario*.
4. Fare clic sul pulsante **[+Query]** per aggiungere una seconda riga di dati. Per questa riga, selezionare **Virtual Machine** e scegliere *IOPS - Read*.
5. Fare clic sul pulsante **[+Query]** per aggiungere una terza riga di dati. Per questa riga, selezionare **Virtual Machine** e scegliere *IOPS - Write*.
6. Fare clic su **Mostra legenda** per visualizzare una legenda per questo widget nella dashboard.



1. Fare clic su **[Save]** per aggiungere questo widget alla dashboard.

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.

1. Fare clic sull'icona **[Add widget]** e selezionare *Line Chart* per aggiungere un nuovo widget line chart alla dashboard.
2. Viene visualizzata la finestra di dialogo Edit Widget (Modifica widget). Assegnare a questo widget il nome "throughput VM per applicazione"
3. Selezionare Virtual Machine (macchina virtuale) e scegliere throughput - Total (throughput - totale). Impostare i filtri desiderati o lasciare vuoto Filter by (Filtra per). Per Roll-up, scegli "Max" e seleziona "Application" o "Name". Mostra le prime 10 applicazioni. Visualizzare questi dati come grafico a linee e lasciare l'asse Y come primario.
4. Fare clic su **[Save]** per aggiungere questo widget alla dashboard.

È possibile spostare i widget nella dashboard tenendo premuto il pulsante del mouse in un punto qualsiasi nella parte superiore del widget e trascinandolo in una nuova posizione.

Puoi ridimensionare i widget trascinando l'angolo in basso a destra.

Assicurati di **[Salva]** la dashboard dopo aver apportato le modifiche.

La tua dashboard finale sulle performance delle macchine virtuali avrà un aspetto simile al seguente:

Best practice per dashboard e widget

Suggerimenti e trucchi per ottenere il massimo dalle potenti funzionalità di dashboard e widget.

Trovare la metrica giusta

Cloud Insights acquisisce contatori e metriche utilizzando nomi che a volte differiscono da data collector a data collector.

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 Cloud Insights 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.

Best Practice: Utilizza 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 trovano nell'elenco. È quindi possibile selezionare facilmente le metriche desiderate da un elenco più 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 con meno prestazioni
Host	Host hypervisor

Hypervisor	L'host è un hypervisor
Microcodice	Firmware
Nome	Alias Nome hypervisor Nome archivio Nome <other asset type> Nome semplice Nome risorsa fabric Alias
Lettura/scrittura	IOPS di scrittura parziale R/W in attesa - latenza della capacità di scrittura - utilizzo della cache di lettura - lettura
Macchina virtuale	La VM è virtuale

Non si tratta di un elenco completo. Questi sono solo esempi di possibili termini di ricerca.

Trovare le risorse giuste

Le risorse a cui puoi fare riferimento nei filtri e nelle ricerche dei widget variano a seconda del tipo di risorsa.

Nelle dashboard e nelle pagine delle risorse, 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	Volume interno VMDK Virtual Machine Volume
Hypervisor	Virtual Machine è l'host dell'hypervisor
Host	Macchina virtuale host Volume Cluster interna
Fabric	Porta

Non si tratta di un elenco completo.

Best practice: Se si esegue il filtraggio per un tipo di risorsa particolare che non compare nell'elenco, provare a creare la query intorno a un tipo di risorsa alternativo.

Esempio di grafico a dispersione: Conoscere l'asse

La modifica dell'ordine dei contatori in un widget del grafico a dispersione 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.

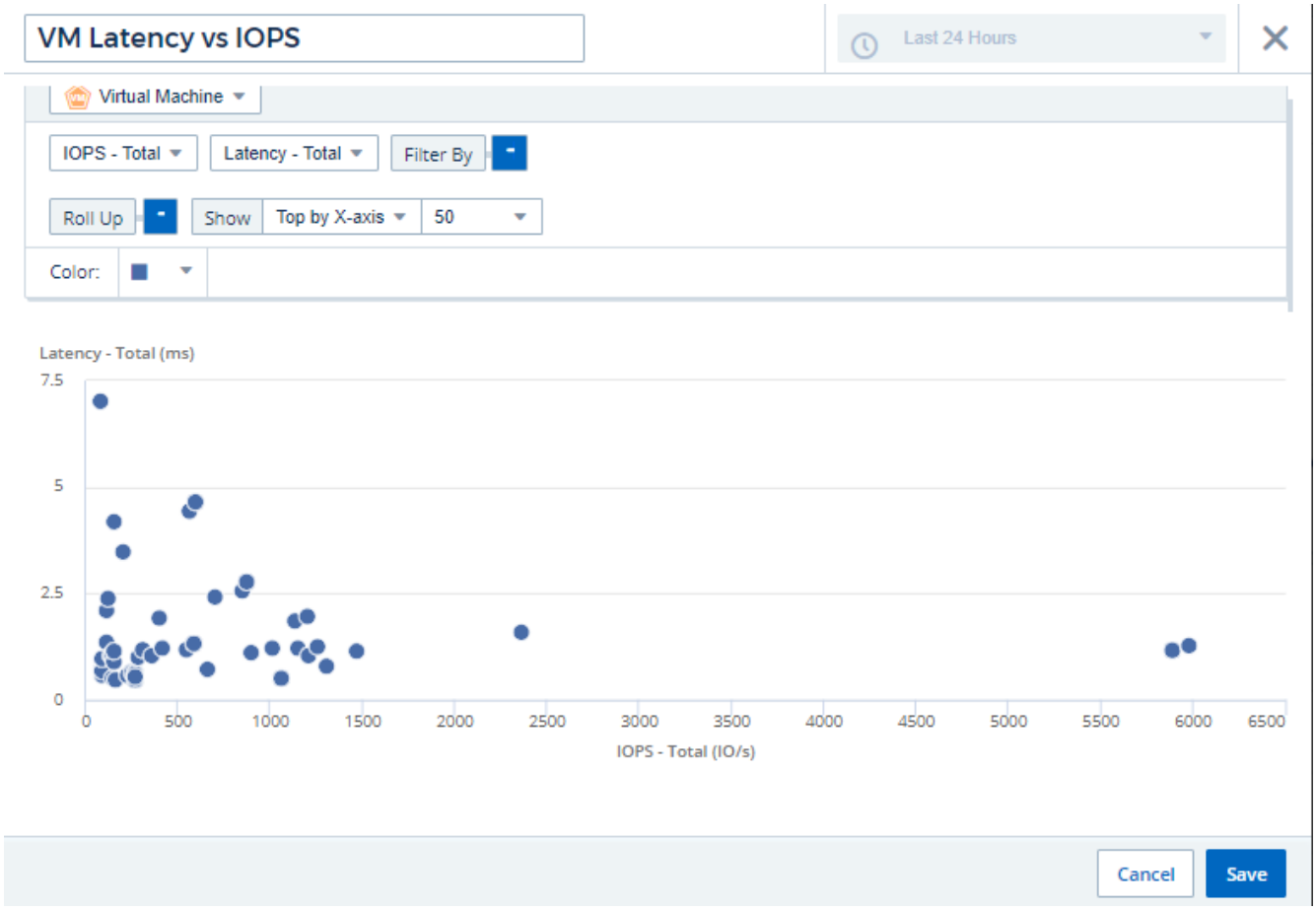
4. Selezionare il secondo contatore che si desidera tracciare. Per questo esempio, selezionare *IOPS - Total*.

   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*.

   Latenza- totale viene ora indicato lungo l'asse Y nel grafico e *IOPS - totale* 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.



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 IOPS totali più elevati. Se lo si modifica in **Top by Y-axis**, il grafico mostrerà nuovamente le prime 100 macchine virtuali con la latenza totale più elevata.

Si noti che in un grafico a dispersione, è possibile fare clic su un punto per visualizzare la pagina delle risorse per tale risorsa.

Kubernetes

Panoramica del cluster Kubernetes

Cloud Insights Kubernetes Explorer è un potente strumento per visualizzare lo stato generale e l'utilizzo dei cluster Kubernetes e consente di analizzare facilmente le aree di ricerca.

Facendo clic su **Dashboards > Kubernetes Explorer** si apre la pagina Kubernetes Cluster. Questa pagina di panoramica contiene la tabella dei cluster Kubernetes nel tuo ambiente.

Name	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

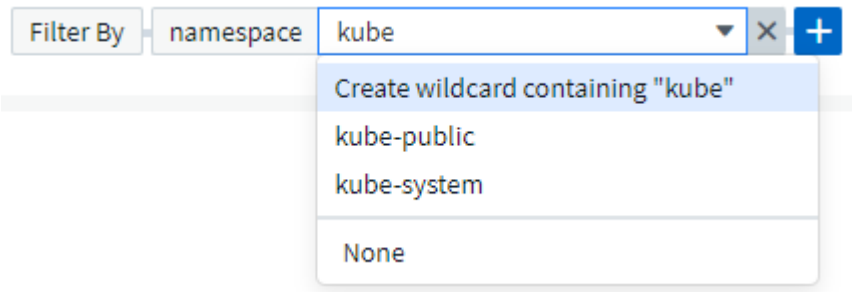
Elenco dei cluster

L'elenco dei cluster visualizza le seguenti informazioni per ciascun cluster dell'ambiente:

- Cluster **Nome**. Facendo clic sul nome di un cluster, viene aperto il **"pagina dei dettagli"** per quel cluster.
- Percentuali di **saturazione**. La saturazione complessiva è la più alta tra CPU, memoria o saturazione dello storage.
- Numero di **nodi** nel cluster. Facendo clic su questo numero si apre la pagina Node list (elenco nodi).
- Numero di **pod** nel cluster. Facendo clic su questo numero si apre la pagina dell'elenco dei pod.
- Numero di **namespace** nel cluster. Facendo clic su questo numero si apre la pagina dell'elenco dei namespace.
- Numero di **carichi di lavoro** nel cluster. Facendo clic su questo numero si apre la pagina elenco workload.

Rifinitura del filtro

Quando si esegue il filtraggio, quando si inizia a digitare viene visualizzata l'opzione per creare un **filtro con caratteri jolly** in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione con caratteri jolly. È inoltre possibile creare **espressioni** utilizzando NOR o E, oppure selezionare l'opzione "None" (Nessuno) per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio, NOD, AND, "None", ecc.) vengono visualizzati in blu

scuro nel campo del filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in blu chiaro.

I filtri Kubernetes sono contestuali, il che significa ad esempio che se ci si trova in una pagina di nodo specifica, il filtro pod_name elenca solo i pod correlati a quel nodo. Inoltre, se si applica un filtro per uno spazio dei nomi specifico, il filtro pod_name elencherà solo i pod su quel nodo *e* in tale spazio dei nomi.

Si noti che i caratteri jolly e il filtraggio delle espressioni funzionano con testo o elenchi, ma non con valori numerici, date o booleani.

Prima di installare o aggiornare l'operatore di monitoraggio NetApp Kubernetes

Leggere queste informazioni prima di installare o aggiornare l'operatore di monitoraggio NetApp Kubernetes

Prerequisiti:

- Se si utilizza un repository di docker privato o personalizzato, seguire le istruzioni nella sezione utilizzo di un repository di docker privato o personalizzato
- L'installazione di NetApp Kubernetes Monitoring Operator è supportata con Kubernetes versione 1.20 o successiva.
- Quando Cloud Insights sta monitorando lo storage back-end e Kubernetes viene utilizzato con il runtime del container Docker, Cloud Insights può visualizzare le mappature e le metriche pod-to-PV-to-storage per NFS e iSCSI; altre runtime mostrano solo NFS.
- A partire da agosto 2022, NetApp Kubernetes Monitoring Operator include il supporto per Pod Security Policy (PSP). Se il tuo ambiente utilizza PSP, devi eseguire l'aggiornamento all'ultimo NetApp Kubernetes Monitoring Operator.
- Se si utilizza OpenShift 4.6 o versione successiva, è necessario seguire le istruzioni di OpenShift riportate di seguito oltre a garantire che questi prerequisiti siano soddisfatti.
- Il monitoraggio viene installato solo sui nodi Linux Cloud Insights supporta il monitoraggio dei nodi Kubernetes che eseguono Linux, specificando un selettore di nodi Kubernetes che cerca le seguenti etichette Kubernetes su queste piattaforme:

Piattaforma	Etichetta
Kubernetes v1.20 e versioni successive	Kubernetes.io/os = linux
Rancher + Cattle.io come piattaforma di orchestrazione/Kubernetes	cattle.io/os = linux

- NetApp Kubernetes Monitoring Operator e le relative dipendenze (telegraf, kube-state-metrics, fluentbit, ecc.) non sono supportate sui nodi che eseguono l'architettura Arm64.
- Devono essere disponibili i seguenti comandi: Curl, kubectl. Il comando docker è necessario per una fase di installazione opzionale. Per ottenere risultati ottimali, aggiungere questi comandi al PERCORSO. Si noti che kubectl deve essere configurato con accesso minimo ai seguenti oggetti kubernetes: Agenti, clusterrolebinding, customresourcedefinizioni, implementazioni, namespace, ruoli, associazioni di ruoli, segreti, serviceaccounts, e servizi. Vedere qui per un file .yaml di esempio con questi privilegi minimi di

ruolo del clusterrole.

- L'host da utilizzare per l'installazione dell'operatore di monitoraggio Kubernetes di NetApp deve avere kubectl configurato per comunicare con il cluster K8s di destinazione e disporre di connettività Internet all'ambiente Cloud Insights.
- Se si utilizza un proxy durante l'installazione o quando si utilizza il cluster K8s da monitorare, seguire le istruzioni nella sezione Configurazione del supporto proxy.
- NetApp Kubernetes Monitoring Operator installa le proprie metriche di stato kube per evitare conflitti con altre istanze. Per un controllo accurato e la creazione di report dei dati, si consiglia di sincronizzare l'ora sul computer dell'agente utilizzando il protocollo NTP (Network Time Protocol) o SNTP (Simple Network Time Protocol).
- Se si sta ridistribuendo l'operatore (ovvero si sta aggiornando o sostituendo), non è necessario creare un token API *new*; è possibile riutilizzare il token precedente.
- Si noti inoltre che se si dispone di un recente NetApp Kubernetes Monitoring Operator installato e si utilizza un token di accesso API rinnovabile, i token in scadenza verranno sostituiti automaticamente da token di accesso API nuovi/aggiornati.
- Monitoraggio della rete:
  - Richiede il kernel Linux versione 4.18.0 e superiore
  - Il sistema operativo Photon non è supportato.

Configurazione dell'operatore

Nelle versioni più recenti dell'operatore, le impostazioni modificate più comunemente possono essere configurate nella risorsa personalizzata *AgentConfiguration*. È possibile modificare questa risorsa prima di implementare l'operatore modificando il file *operator-config.yaml*. Questo file include esempi commentati di alcune impostazioni. Vedere l'elenco di "impostazioni disponibili" per la versione più recente dell'operatore.

È inoltre possibile modificare questa risorsa dopo che l'operatore è stato distribuito utilizzando il seguente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Per determinare se la versione implementata dell'operatore supporta
AgentConfiguration, eseguire il seguente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Error from server (notfound)" (errore
dal server (non trovato)), l'operatore deve essere aggiornato prima di
poter utilizzare AgentConfiguration.
```

Cose importanti da notare prima di iniziare

Se si utilizza un proxy, hanno un repository personalizzato, o stanno utilizzando OpenShift, leggere attentamente le seguenti sezioni.

Leggi anche di Permessi.

Se si sta eseguendo l'aggiornamento da un'installazione precedente, leggere la Aggiornamento in corso

informazioni.

Configurazione del supporto proxy

Per installare NetApp Kubernetes Monitoring Operator, è possibile utilizzare un proxy nel proprio ambiente in due punti. Questi possono essere sistemi proxy identici o separati:

- Proxy necessario durante l'esecuzione del frammento di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito il frammento all'ambiente Cloud Insights
- Proxy necessario dal cluster Kubernetes di destinazione per comunicare con l'ambiente Cloud Insights

Se si utilizza un proxy per uno o entrambi questi, per installare il monitor operativo Kubernetes di NetApp è necessario prima assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Cloud Insights. Ad esempio, dai server/VM da cui si desidera installare l'operatore, è necessario poter accedere a Cloud Insights e scaricare i file binari da Cloud Insights.

Per il proxy utilizzato per installare NetApp Kubernetes Operating Monitor, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

Per impostare le variabili, eseguire le seguenti operazioni sul sistema **prima** dell'installazione di NetApp Kubernetes Monitoring Operator:

1. Impostare le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:
   a. Se il proxy da configurare non dispone dell'autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone dell'autenticazione (nome
utente/password), eseguire questo comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Per il proxy utilizzato per la comunicazione del cluster Kubernetes con l'ambiente Cloud Insights, installare l'operatore di monitoraggio Kubernetes dopo aver letto tutte le istruzioni.

Configurare la sezione proxy di AgentConfiguration in operator-config.yaml prima di implementare NetApp Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utilizzando un repository di docker personalizzato o privato

Per impostazione predefinita, l'operatore di monitoraggio di NetApp Kubernetes estrarrà le immagini container dal repository Cloud Insights. Se si utilizza un cluster Kubernetes come destinazione per il monitoraggio e tale cluster è configurato in modo da estrarre solo immagini container da un repository Docker personalizzato o privato o da un registro container, è necessario configurare l'accesso ai container richiesti dall'operatore di monitoraggio NetApp Kubernetes.

Eseguire il frammento Image Pull dalla sezione di installazione di NetApp Monitoring Operator. Questo comando effettua l'accesso al repository Cloud Insights, inserisce tutte le dipendenze dell'immagine per l'operatore e si disconnette dal repository Cloud Insights. Quando richiesto, inserire la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, incluse le funzioni opzionali. Vedere di seguito per quali funzioni vengono utilizzate queste immagini.

Funzionalità principale dell'operatore e monitoraggio Kubernetes

- monitoraggio netapp
- kube-rbac-proxy
- kube-state-metrics
- telefono
- distroless-root-user

Registro eventi

- fluente
- kubernetes-event-exportent

Mappa e performance di rete

- ci-net-osservatore

Trasferire l'immagine del gestore nel repository del supporto privato/locale/aziendale in base alle policy aziendali. Assicurarsi che i tag delle immagini e i percorsi delle directory per queste immagini nel repository siano coerenti con quelli nel repository Cloud Insights.

Modificare l'implementazione dell'operatore di monitoraggio in operator-deployment.yaml e modificare tutti i riferimenti alle immagini per utilizzare il repository Docker privato.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modificare la configurazione dell'agente in operator-config.yaml in modo che rifletta la nuova posizione del responsabile del docker. Crea un nuovo imagePullSecret per il tuo repository privato; per ulteriori dettagli, consulta *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Istruzioni per OpenShift

Se si utilizza OpenShift 4.6 o versione successiva, è necessario modificare la configurazione dell'agente in *operator-config.yaml* per attivare l'impostazione *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift potrebbe implementare un ulteriore livello di sicurezza che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Permessi

Se il cluster che si sta monitorando contiene risorse personalizzate che non hanno un ClusterRole che "aggregati da visualizzare", Sarà necessario concedere manualmente all'operatore l'accesso a queste risorse

per monitorarle con i registri eventi.

1. Modificare *operator-additional-permissions.yaml* prima dell'installazione o dopo l'installazione modificare la risorsa *ClusterRole/<namespace>-additional-permissions*
2. Creare una nuova regola per gli apartGroup e le risorse desiderati con i verbi ["Get", "Watch", "list"]. Vedere https://kubernetes.io/docs/reference/access-authn-authz/rbac/
3. Applicare le modifiche al cluster

Tolerazioni e contamini

I DaemonSet *netapp-ci-telegraf-ds*, *netapp-ci-fluent-bit-ds* e *netapp-ci-net-observer-L4-ds* devono pianificare un pod su ogni nodo del cluster per raccogliere correttamente i dati su tutti i nodi. L'operatore è stato configurato in modo da tollerare alcuni **segni** noti. Se sono stati configurati dei tipi di contamini personalizzati sui nodi, impedendo l'esecuzione dei pod su ogni nodo, è possibile creare una **tolleranza** per tali tipi di contamini "In *AgentConfiguration*". Se sono stati applicati dei tipi di manutenzione personalizzati a tutti i nodi del cluster, è necessario aggiungere anche le tolleranze necessarie all'implementazione dell'operatore per consentire la pianificazione e l'esecuzione del pod operatore.

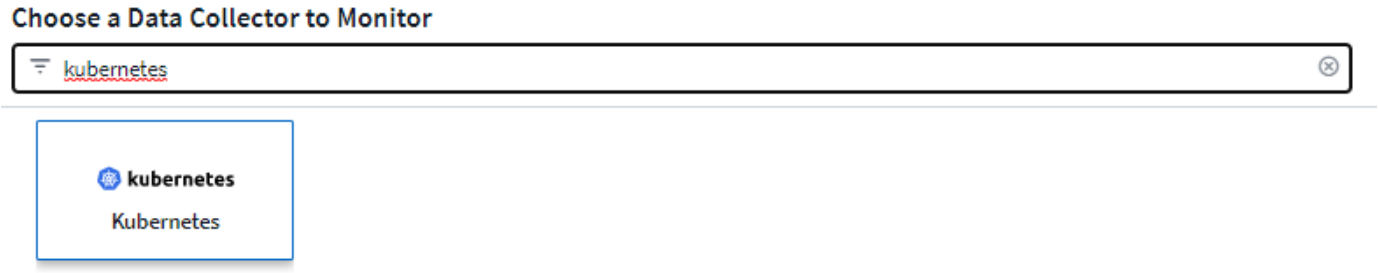
Scopri di più su Kubernetes "Contamini e pedaggi".

Tornare al **"Pagina Installazione dell'operatore di monitoraggio NetApp Kubernetes"**

Installazione e configurazione dell'operatore di monitoraggio Kubernetes

Cloud Insights offre la raccolta * NetApp Kubernetes Monitoring Operator* (NKMO) per Kubernetes. Quando si aggiunge un data collector, è sufficiente selezionare la sezione Kubernetes.

> Se si dispone dell'edizione federale di Cloud Insights, le istruzioni di installazione e configurazione potrebbero essere diverse da quelle riportate su questa pagina. Seguire le istruzioni in Cloud Insights per installare l'operatore di monitoraggio NetApp Kubernetes.

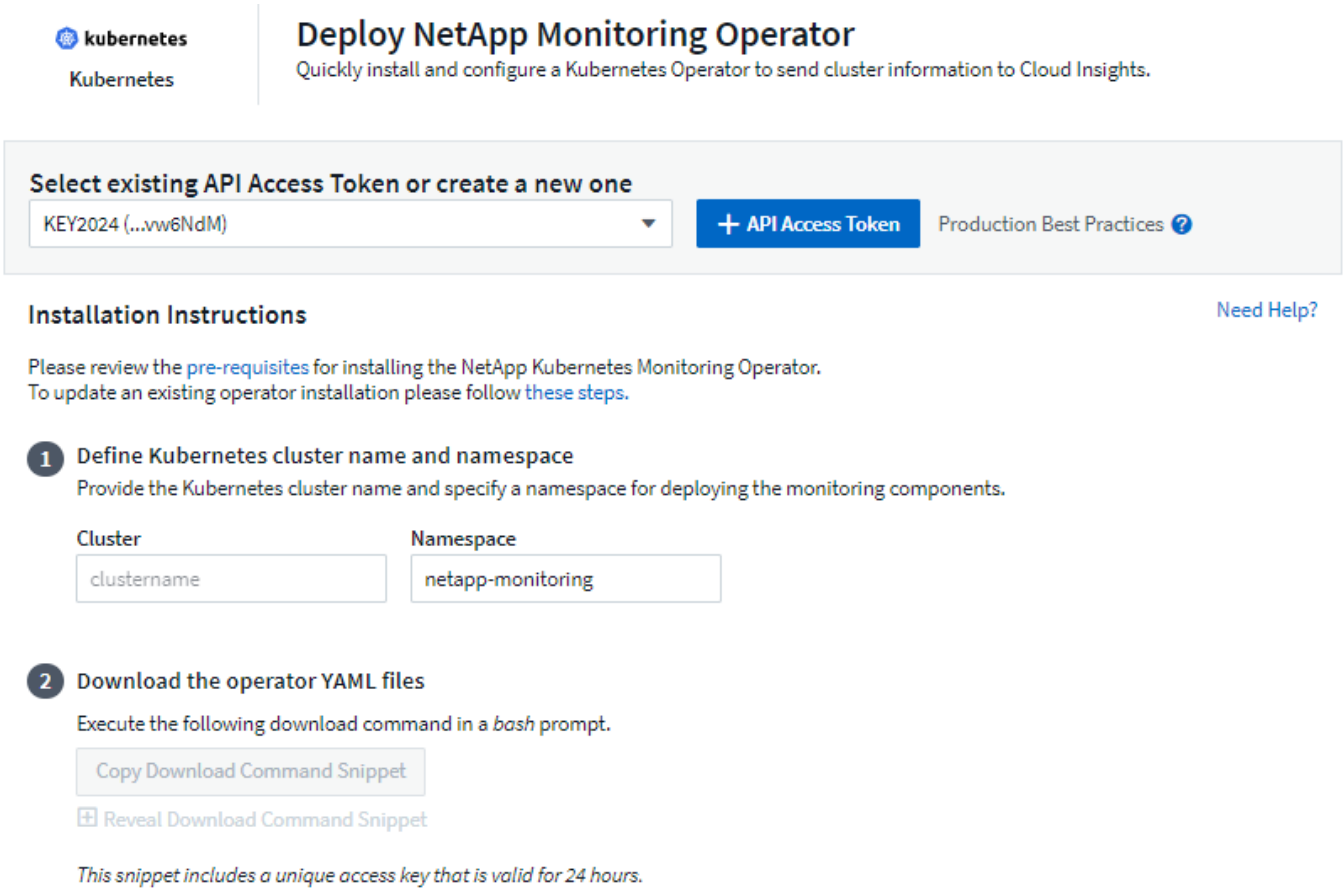


L'operatore Kubernetes e i data collector vengono scaricati dal Registro di Docker di Cloud Insights. Una volta installato, l'operatore gestisce quindi tutti i collettori compatibili con l'operatore implementati nei nodi del cluster Kubernetes per acquisire i dati, inclusa la gestione del ciclo di vita di tali collettori. In seguito a questa catena, i dati vengono acquisiti dai collettori e inviati a Cloud Insights.

Prima di installare NetApp Kubernetes Monitoring Operator

Leggere il **"Prima dell'installazione o dell'aggiornamento"** Documentazione pre-requisiti prima di installare o aggiornare l'operatore di monitoraggio Kubernetes NetApp.

Installazione di NetApp Kubernetes Monitoring Operator



3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure.
Finally, update the image paths in operator-deployment.yaml and the docker repository settings in operator-config.yaml.
For more information review the documentation.

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

This password is valid for 24 hours.

4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the instructions and available options.

5 Deploy the operator (create new or upgrade existing)

Execute the *kubectl* snippet to apply the following operator YAML files.

- operator-setup.yaml - Create the operator's dependencies.
- operator-secrets.yaml - Create secrets holding your API key.
- operator-deployment.yaml, operator-cr.yaml - Deploy the NetApp Kubernetes Monitoring Operator.
- operator-config.yaml - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store operator-secrets.yaml.**

6 Next

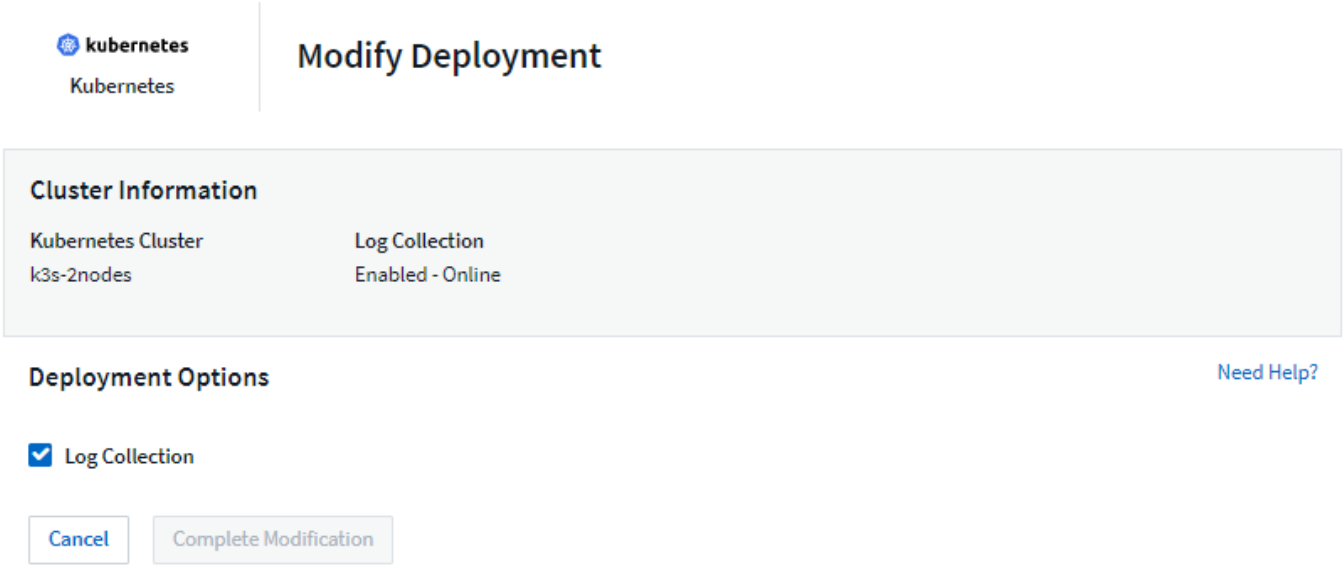
Procedura per installare NetApp Kubernetes Monitoring Operator Agent su Kubernetes:

1. Immettere un nome cluster e uno spazio dei nomi univoci. Se lo sei aggiornamento in corso Da un operatore Kubernetes precedente, utilizzare lo stesso nome del cluster e lo stesso namespace.
2. Una volta immessi, è possibile copiare il frammento Download Command negli Appunti.
3. Incollare il frammento in una finestra *bash* ed eseguirlo. I file di installazione dell'operatore verranno scaricati. Tenere presente che il frammento ha una chiave univoca ed è valido per 24 ore.
4. Se si dispone di un repository personalizzato o privato, copiare il frammento Image Pull opzionale, incollarlo in una shell *bash* ed eseguirlo. Una volta estratte le immagini, copiarle nel repository privato. Assicurarsi di mantenere gli stessi tag e la stessa struttura di cartelle. Aggiornare i percorsi in *operator-deployment.yaml* e le impostazioni del repository di docker in *operator-config.yaml*.
5. Se lo si desidera, esaminare le opzioni di configurazione disponibili, ad esempio le impostazioni del proxy o del repository privato. Ulteriori informazioni su "opzioni di configurazione".
6. Quando sei pronto, implementa l'operatore copiando il frammento kubectl apply, scaricandolo ed eseguendolo.
7. L'installazione procede automaticamente. Una volta completata l'operazione, fare clic sul pulsante *Avanti*.
8. Al termine dell'installazione, fare clic sul pulsante *Next*. Assicurarsi inoltre di eliminare o memorizzare in modo sicuro il file *operator-secrets.yaml*.

Scopri di più configurazione del proxy.

Scopri di più utilizzando un repository di docker personalizzato/privato.

La raccolta dei log EMS di Kubernetes è attivata per impostazione predefinita quando si installa NetApp Kubernetes Monitoring Operator. Per disattivare questa raccolta dopo l'installazione, fare clic sul pulsante **Modify Deployment** (Modifica distribuzione) nella parte superiore della pagina dei dettagli del cluster Kubernetes e deselezionare "Log collection" (raccolta log).



Questa schermata mostra anche lo stato corrente della raccolta dei log. Di seguito sono riportati i possibili stati:

- Disattivato
- Attivato
- Enabled (attivato) - Installazione in corso
- Abilitato - non in linea
- Abilitato - Online
- Errore - le autorizzazioni della chiave API non sono sufficienti

Aggiornamento in corso

Aggiornamento all'ultimo NetApp Kubernetes Monitoring Operator

Determinare se esiste una configurazione Agentcon l'operatore esistente (se lo spazio dei nomi non è il *monitoraggio netapp* predefinito, sostituire lo spazio dei nomi appropriato):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-
configuration
Se esiste una configurazione AgentConfiguration:
```

- Installare L'operatore più recente rispetto all'operatore esistente.
  - Assicurati di sì estrarre le immagini container più recenti se si utilizza un repository personalizzato.

Se AgentConfiguration non esiste:

- Prendere nota del nome del cluster riconosciuto da Cloud Insights (se lo spazio dei nomi non è il monitoraggio netapp predefinito, sostituire lo spazio dei nomi appropriato):

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* Creare un backup dell'operatore esistente (se lo spazio dei nomi non è
il monitoraggio netapp predefinito, sostituire lo spazio dei nomi
appropriato):
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-netapp-kubernetes-monitoring-operator,Disinstallare>>
L'operatore esistente.
* <<installing-the-netapp-kubernetes-monitoring-operator,Installare>>
L'operatore più recente.
```

  - Utilizzare lo stesso nome del cluster.
  - Dopo aver scaricato i file YAML dell'operatore più recenti, portare le personalizzazioni trovate in Agent_backup.yaml nell'operator-config.yaml scaricato prima di eseguire la distribuzione.
  - Assicurati di sì estrarre le immagini container più recenti se si utilizza un repository personalizzato.

Arresto e avvio di NetApp Kubernetes Monitoring Operator

Per arrestare NetApp Kubernetes Monitoring Operator:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Per avviare NetApp Kubernetes Monitoring Operator:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

Disinstallazione in corso

Per rimuovere NetApp Kubernetes Monitoring Operator

Si noti che lo spazio dei nomi predefinito per NetApp Kubernetes Monitoring Operator è "netapp-monitoring". Se è stato impostato uno spazio dei nomi personalizzato, sostituire tale spazio dei nomi in questi e in tutti i comandi e file successivi.

Le versioni più recenti dell'operatore di monitoraggio possono essere disinstallate con i seguenti comandi:

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

Se l'operatore di monitoraggio è stato distribuito nel proprio spazio dei nomi dedicato, eliminare lo spazio dei nomi:

```
 kubectl delete ns <NAMESPACE>
Se il primo comando restituisce "Nessuna risorsa trovata", attenersi alle
istruzioni riportate di seguito per disinstallare le versioni precedenti
dell'operatore di monitoraggio.
```

Eseguire ciascuno dei seguenti comandi nell'ordine indicato. A seconda dell'installazione corrente, alcuni di questi comandi potrebbero restituire i messaggi 'oggetto non trovato'. Questi messaggi possono essere ignorati in modo sicuro.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

Se in precedenza è stato creato un vincolo del contesto di protezione:

```
kubectl delete scc telegraf-hostaccess
```

A proposito di Kube-state-metrics

NetApp Kubernetes Monitoring Operator installa automaticamente le metriche dello stato kube, senza richiedere alcuna interazione da parte dell'utente.

Contatori di metriche di stato kube

Utilizzare i seguenti collegamenti per accedere alle informazioni relative ai contatori delle metriche di stato del kube:

1. "Metriche di ConfigMap"
2. "Metriche DemonSet"
3. "Metriche di implementazione"
4. "Metriche di ingresso"
5. "Metriche dello spazio dei nomi"
6. "Metriche del nodo"
7. "Metriche di volume persistenti"
8. "Metriche delle richieste di rimborso per volumi persistenti"
9. "Metriche pod"
10. "Metriche ReplicaSet"
11. "Metriche segrete"
12. "Metriche del servizio"
13. "Metriche StatefulSet"

```
 == Configuring the Operator
Nelle versioni più recenti dell'operatore, le impostazioni modificate più
comunemente possono essere configurate nella risorsa personalizzata
_AgentConfiguration_. È possibile modificare questa risorsa prima di
implementare l'operatore modificando il file _operator-config.yaml_.
Questo file include esempi commentati di alcune impostazioni. Vedere
l'elenco di
xref:{relative_path}telegraf_agent_k8s_config_options.html["impostazioni
disponibili"] per la versione più recente dell'operatore.
```

È inoltre possibile modificare questa risorsa dopo che l'operatore è stato distribuito utilizzando il seguente comando:

```
 kubectl -n netapp-monitoring edit AgentConfiguration
Per determinare se la versione implementata dell'operatore supporta
AgentConfiguration, eseguire il seguente comando:
```

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
Se viene visualizzato il messaggio "Error from server (notfound)" (errore
dal server (non trovato)), l'operatore deve essere aggiornato prima di
poter utilizzare AgentConfiguration.
```

Configurazione del supporto proxy

Per installare NetApp Kubernetes Monitoring Operator, è possibile utilizzare un proxy nel proprio ambiente in

due punti. Questi possono essere sistemi proxy identici o separati:

- Proxy necessario durante l'esecuzione del frammento di codice di installazione (utilizzando "curl") per connettere il sistema in cui viene eseguito il frammento all'ambiente Cloud Insights
- Proxy necessario dal cluster Kubernetes di destinazione per comunicare con l'ambiente Cloud Insights

Se si utilizza un proxy per uno o entrambi questi, per installare il monitor operativo di NetApp Kubernetes è necessario prima assicurarsi che il proxy sia configurato per consentire una buona comunicazione con l'ambiente Cloud Insights. Se si dispone di un proxy e si può accedere a Cloud Insights dal server/VM da cui si desidera installare l'operatore, è probabile che il proxy sia configurato correttamente.

Per il proxy utilizzato per installare NetApp Kubernetes Operating Monitor, prima di installare l'operatore, impostare le variabili di ambiente *http_proxy/https_proxy*. Per alcuni ambienti proxy, potrebbe essere necessario impostare la variabile *no_proxy environment*.

Per impostare le variabili, eseguire le seguenti operazioni sul sistema **prima** dell'installazione di NetApp Kubernetes Monitoring Operator:

1. Impostare le variabili di ambiente *https_proxy* e/o *http_proxy* per l'utente corrente:
   a. Se il proxy da configurare non dispone dell'autenticazione (nome utente/password), eseguire il seguente comando:

```
 export https_proxy=<proxy_server>:<proxy_port>
.. Se il proxy da configurare dispone dell'autenticazione (nome
utente/password), eseguire questo comando:
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Per il proxy utilizzato per la comunicazione del cluster Kubernetes con l'ambiente Cloud Insights, installare l'operatore di monitoraggio Kubernetes dopo aver letto tutte le istruzioni.

Configurare la sezione proxy di AgentConfiguration in operator-config.yaml prima di implementare NetApp Kubernetes Monitoring Operator.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
...
```

Utilizzando un repository di docker personalizzato o privato

Per impostazione predefinita, l'operatore di monitoraggio di NetApp Kubernetes estrarrà le immagini container dal repository Cloud Insights. Se si utilizza un cluster Kubernetes come destinazione per il monitoraggio e tale cluster è configurato in modo da estrarre solo immagini container da un repository Docker personalizzato o privato o da un registro container, è necessario configurare l'accesso ai container richiesti dall'operatore di monitoraggio NetApp Kubernetes.

Eseguire il frammento Image Pull dalla sezione di installazione di NetApp Monitoring Operator. Questo comando effettua l'accesso al repository Cloud Insights, inserisce tutte le dipendenze dell'immagine per l'operatore e si disconnette dal repository Cloud Insights. Quando richiesto, inserire la password temporanea del repository fornita. Questo comando scarica tutte le immagini utilizzate dall'operatore, incluse le funzioni opzionali. Vedere di seguito per quali funzioni vengono utilizzate queste immagini.

Funzionalità principale dell'operatore e monitoraggio Kubernetes

- monitoraggio netapp
- ci-kube-rbac-proxy
- ci-ksm
- ci-telegraf
- distroless-root-user

Registro eventi

- ci-fluent-bit
- ci-kukasub-esportatore-di-eventi

Mappa e performance di rete

- ci-net-osservatore

Trasferire l'immagine del gestore nel repository del supporto privato/locale/aziendale in base alle policy aziendali. Assicurarsi che i tag delle immagini e i percorsi delle directory per queste immagini nel repository siano coerenti con quelli nel repository Cloud Insights.

Modificare l'implementazione dell'operatore di monitoraggio in operator-deployment.yaml e modificare tutti i riferimenti alle immagini per utilizzare il repository Docker privato.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

Modificare la configurazione dell'agente in operator-config.yaml in modo che rifletta la nuova posizione del responsabile del docker. Crea un nuovo imagePullSecret per il tuo repository privato; per ulteriori dettagli, consulta *https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/*

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
from as compared to CI's docker registry
  # Please see documentation link here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
private docker registry
  dockerImagePullSecret: docker-secret-name
```

Istruzioni per OpenShift

Se si utilizza OpenShift 4.6 o versione successiva, è necessario modificare la configurazione dell'agente in *operator-config.yaml* per attivare l'impostazione *runPrivileged*:

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift potrebbe implementare un ulteriore livello di sicurezza che potrebbe bloccare l'accesso ad alcuni componenti di Kubernetes.

Una nota sui segreti

Per rimuovere l'autorizzazione per l'operatore di monitoraggio Kubernetes NetApp per visualizzare segreti a livello del cluster, eliminare le seguenti risorse dal file *operatore-setup.yaml* prima di eseguire l'installazione:

```
 ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

Se si tratta di un aggiornamento, eliminare anche le risorse dal cluster:

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

Se l'analisi delle modifiche è attivata, modificare *AgentConfiguration* o *operator-config.yaml* per annullare il commento alla sezione di gestione delle modifiche e includere *kindsToIgnoreFromWatch: '"secrets"'* nella sezione di gestione delle modifiche. Notare la presenza e la posizione di virgolette singole e doppie in questa riga.

```
# change-management:
  ...
  # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
  # # Each kind will have to be prefixed by its apigroup
  # # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
  kindsToIgnoreFromWatch: '"secrets"'
  ...
```

Verifica dei checksum di Kubernetes

Il programma di installazione dell'agente Cloud Insights esegue controlli di integrità, ma alcuni utenti potrebbero voler eseguire le proprie verifiche prima di installare o applicare gli artefatti scaricati. Per eseguire un'operazione di solo download (invece del download e dell'installazione predefiniti), questi utenti possono modificare il comando di installazione dell'agente ottenuto dall'interfaccia utente e rimuovere l'opzione finale di "installazione".

Attenersi alla seguente procedura:

1. Copiare il frammento del programma di installazione dell'agente come indicato.
2. Invece di incollare il frammento in una finestra di comando, incollarlo in un editor di testo.
3. Rimuovere il file "--install" finale dal comando.
4. Copiare l'intero comando dall'editor di testo.
5. Incollarlo nella finestra di comando (in una directory di lavoro) ed eseguirlo.
    - Download e installazione (impostazione predefinita):

```
 installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download --install
** Solo download:
```

```
installerName=cloudinsights-rhel_centos.sh … && sudo -E -H
./$installerName --download
```

Il comando di solo download scaricherà tutti gli artefatti richiesti da Cloud Insights nella directory di lavoro. Gli artefatti includono, ma non possono essere limitati a:

- uno script di installazione
- un file di ambiente
- File YAML
- un file checksum firmato (sha256.signed)
- Un file PEM (netapp_cert.pem) per la verifica della firma

Lo script di installazione, il file di ambiente e i file YAML possono essere verificati utilizzando l'ispezione visiva.

Il file PEM può essere verificato confermando che l'impronta digitale è la seguente:

```
 1A918038E8E127BB5C87A202DF173B97A05B4996
In particolare,
```

```
 openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
Il file checksum firmato può essere verificato utilizzando il file PEM:
```

```
 openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
Una volta verificati correttamente tutti gli artefatti, l'installazione
dell'agente può essere avviata eseguendo:
```

```
sudo -E -H ./<installation_script_name> --install
```

Risoluzione dei problemi

Alcune cose da provare in caso di problemi durante la configurazione dell'operatore di monitoraggio di NetApp Kubernetes:

Problema:	Prova:
Non viene visualizzato un collegamento ipertestuale/connessione tra il volume persistente Kubernetes e il dispositivo di storage back-end corrispondente. Il volume persistente Kubernetes viene configurato utilizzando il nome host del server di storage.	Seguire la procedura per disinstallare l'agente Telegraf esistente, quindi reinstallare l'agente Telegraf più recente. È necessario utilizzare Telegraf versione 2.0 o successiva e lo storage del cluster Kubernetes deve essere monitorato attivamente da Cloud Insights.

Problema:	Prova:
Nei registri vengono visualizzati messaggi simili a quelli riportati di seguito: E0901 15:21:39,962145 1 Reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.MutatingWebhookConfigurazione: Il server non ha trovato la risorsa richiesta E0901 15:21:43,168161 1 Reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: Impossibile elencare *v1.Lease: Il server non ha trovato la risorsa richiesta (get leases.Coordination.k8s.io) ecc.	Questi messaggi possono verificarsi se si utilizza kube-state-metrics versione 2.0.0 o superiore con versioni di Kubernetes inferiori alla 1.20. Per ottenere la versione di Kubernetes: *kubectl version* Per ottenere la versione kube-state-metrics: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* Per evitare che questi messaggi si verifichino, gli utenti possono modificare la distribuzione delle metriche dello stato-kube per disabilitare i seguenti leasing: *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* In particolare, possono utilizzare il seguente argomento CLI: resources=certificatesigningrequires,configmaps,cronjob,daemonset, deployments,endpoints,horizontalpodautoscalers,ingresses,job,limitrange, namespace,networkpolicy,node,persistentvolumeclaims L'elenco delle risorse predefinito è: "certificatesigningrequests,configmaps,cronjob,daemonsets,deployments, endpoint,horizontalpodautoscalers,ingresses,job,leases,limitrange, mutatingwebhookconfigurations,namespaces,network policy,nodi, persistentvolumeclaimes,durentvolumetsets,poddisruptionbudgets,pods,replicasets, replicationstoricasets,replicationfors,storeforcsets,servizi,storeforcsets,storeforcsets convalidatingwebhookconfigurations,volumeattachments"

Problema:	Prova:
Vengono visualizzati messaggi di errore di Telegraf simili ai seguenti, ma Telegraf si avvia ed esegue: Oct 11 14:23:41:00 ip-172-31-39-47 systemd[1]: Avviato l'agente server basato su plugin per la generazione di rapporti sulle metriche in InfluxDB. Ottobre 11 14:23:41 ip-172-31-39-47 telegraf[1827]: Time="2021-10-11T14:23:41Z" level=error msg="Impossibile creare la directory della cache. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: permesso negato. Ignorato\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Ott 11 14:23:41:00 ip-172-31-39-47 telegraf[1827]: Time="2021-10-11T14:23:41Z" level=error msg="Impossibile aprire. Ignorato. aprire /etc/telegraf/.cache/snowflake/ocsp_response_cache.j son: no File o directory\n" func="gosnowflake.(*defaultLogger).Errorf" file="log.go:120" Oct:23:41:ip-172-31-39-47:11 14 telegraf[1827]: 2021-10-11T14:23:41Z i! Avvio di Telegraf 1.19.3	Si tratta di un problema noto. Fare riferimento a. "Questo articolo di GitHub" per ulteriori dettagli. Finché Telegraf è in funzione, gli utenti possono ignorare questi messaggi di errore.
In Kubernetes, i pod Telegraf riportano il seguente errore: "Errore durante l'elaborazione delle informazioni sui mount stats: Impossibile aprire il file mountstats: /Hostfs/proc/1/mountstats, errore: Open /hostfs/proc/1/mountstats: Permesso negato"	Se SELinux è abilitato e abilitato, probabilmente impedisce ai pod Telegraf di accedere al file /proc/1/mountstats sul nodo Kubernetes. Per superare questa restrizione, modificare la configurazione dell'agente e attivare l'impostazione runPrivileged. Per ulteriori informazioni, fare riferimento a: https://docs.netapp.com/us-en/cloudinsights/task_config_telegraf_agent_k8s.html#openshift-instructions.
In Kubernetes, il pod Telegraf ReplicaSet riporta il seguente errore: [inputs.prometheus] errore nel plugin: Impossibile caricare keypair /etc/kuowski/pki/etcd/server.crt:/etc/kuowski/pki/etcd/s erver.key: Aprire /etc/kuowski/pki/etcd/server.crt: Nessun file o directory di questo tipo	Il pod ReplicaSet di Telegraf è destinato all'esecuzione su un nodo designato come master o etcd. Se il pod ReplicaSet non è in esecuzione su uno di questi nodi, si otterranno questi errori. Verificare se i nodi master/etcd presentano delle contaminazioni. In tal caso, aggiungere le tolleranze necessarie a Telegraf ReplicaSet, telegraf-rs. Ad esempio, modificare ReplicaSet… kubectl edit rs telegraf-rs …e aggiungere le tolleranze appropriate alle specifiche. Quindi, riavviare il pod ReplicaSet.

Problema:	Prova:
Ho un ambiente PSP/PSA. Questo influisce sul mio operatore di monitoraggio?	Se il cluster Kubernetes è in esecuzione con Pod Security Policy (PSP) o Pod Security Admission (PSA), è necessario eseguire l'aggiornamento all'ultimo NetApp Kubernetes Monitoring Operator. Per eseguire l'aggiornamento all'NKMO corrente con il supporto per PSP/PSA, procedere come segue: 1. Disinstallare l'operatore di monitoraggio precedente: kubectl delete agent-monitoring-netapp -n monitoring kubectl elimina ns monitoraggio netapp kubectl cancella crd agents.monitoring.netapp.com kubectl elimina agente-manager-ruolo-agente-proxy-ruolo-agente-metrica-lettore kubectl elimina agente di associazione-manager-agente di legame-proxy-agente di legame-cluster-admin-rolebinding 2. Installare la versione più recente dell'operatore di monitoraggio.
Ho riscontrato problemi nel tentativo di implementare NKMO e ho utilizzato PSP/PSA.	1. Modificare l'agente utilizzando il seguente comando: kubectl -n <name-space> edit agent 2. Contrassegnare 'sicurezza-policy-enabled' come 'false'. In questo modo verranno disabilitati i criteri di sicurezza Pod e l'ammissione alla sicurezza Pod e verrà consentito l'implementazione di NKMO. Confermare utilizzando i seguenti comandi: Kubectl Prendi psp (dovrebbe mostrare la politica di sicurezza del Pod rimossa) kubectl get all -n <namespace>
grep -i psp (dovrebbe mostrare che non si trova nulla)	Errori "ImagePullBackoff" rilevati
Questi errori possono essere rilevati se si dispone di un repository di docker personalizzato o privato e non si è ancora configurato NetApp Kubernetes Monitoring Operator per riconoscerlo correttamente. Scopri di più informazioni sulla configurazione per repo personalizzato/privato.	Si verifica un problema con l'implementazione dell'operatore di monitoraggio e la documentazione corrente non mi aiuta a risolverlo.

Problema:	Prova:

Acquisire o annotare in altro modo l'output dei seguenti comandi e contattare il team di supporto tecnico.
 	
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	I pod Net-Observer (Workload Map) nello spazio dei nomi NKMO si trovano in CrashLoopBackOff

Questi pod corrispondono al data collector Workload Map per l'osservabilità della rete. Provare a effettuare le seguenti operazioni: • Controllare i log di uno dei pod per confermare la versione minima del kernel. Ad esempio: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"failed in validation. Motivo: La versione del kernel 3.10.0 è inferiore alla versione minima del kernel 4.18.0","Time":"2022-11-09T08:23:08Z"} ---- • I pod Net-observer richiedono che la versione del kernel Linux sia almeno 4.18.0. Controllare la versione del kernel usando il comando "uname -r" e assicurarsi che siano >= 4.18.0	I pod vengono eseguiti nello spazio dei nomi NKMO (impostazione predefinita: monitoraggio netapp), ma non vengono visualizzati dati nell'interfaccia utente per la mappa del carico di lavoro o le metriche Kubernetes nelle query
Controllare l'impostazione dell'ora sui nodi del cluster K8S. Per un controllo accurato e la creazione di report dei dati, si consiglia di sincronizzare l'ora sul computer dell'agente utilizzando il protocollo NTP (Network Time Protocol) o SNTP (Simple Network Time Protocol).	Alcuni dei pod net-osservatore nello spazio dei nomi NKMO sono in stato Pending

Problema:	Prova:
NET-osservatore è un DemonSet che esegue un pod in ogni nodo del cluster k8s. • Notare il pod che si trova nello stato in sospeso e controllare se si verifica un problema di risorse per la CPU o la memoria. Assicurarsi che la memoria e la CPU richieste siano disponibili nel nodo.	Vedo quanto segue nei miei log subito dopo l'installazione dell'operatore di monitoraggio NetApp Kubernetes: [inputs.prometheus] errore nel plugin: Errore durante la richiesta HTTP a. http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: Ottieni http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics: dial tcp: lookube-state-metrics.<namespace>.svc.cluster.local: no tale host
Questo messaggio viene visualizzato in genere solo quando viene installato un nuovo operatore e il pod *telegraf-rs* è attivo prima che il pod *ksm* sia attivo. Questi messaggi dovrebbero interrompersi una volta che tutti i pod sono in esecuzione.	Non vedo alcuna metrica raccolta per Kubernetes Cronjobs che esiste nel mio cluster.
Verificare la versione di Kubernetes (ad es `kubectl version`). Se è v1.20.x o inferiore, si tratta di un limite previsto. La release di metriche dello stato kube implementata con l'operatore di monitoraggio Kubernetes di NetApp supporta solo v1.cronjob. Con Kubernetes 1.20.x e versioni precedenti, la risorsa cronjob è v1beta.cronjob. Di conseguenza, le metriche dello stato del kube non riescono a trovare la risorsa di crono-job.	Dopo aver installato l'operatore, i pod telegraf-ds entrano in CrashLoopBackOff e i registri del pod indicano "su: Authentication failure" (su: Errore di autenticazione).

Problema:	Prova:
Modificare la sezione telegraf in *AgentConfiguration* e impostare *dockerMetricCollectionEnabled* su false. Per ulteriori dettagli, fare riferimento al manuale dell'operatore "opzioni di configurazione". NOTA: se si utilizza l'Edizione Federale di Cloud Insights, gli utenti con restrizioni sull'uso di *su* non potranno raccogliere metriche di docker perché l'accesso al socket di docker richiede l'esecuzione del contenitore di telegraf come root o l'utilizzo di *su* per aggiungere l'utente di telegraf al gruppo di docker. La raccolta di metriche Docker e l'utilizzo di *su* sono attivati per impostazione predefinita; per disabilitare entrambi, rimuovere la voce *telegraf.docker* nel file *AgentConfiguration*: … specifiche: … telegraf: … - nome: docker modalità di esecuzione: - DaemonSet sostituzioni: CHIAVE: DOCKER_UNIX_SOCK_PLACEHOLDER valore: unix://run/docker.sock … …	Nei registri di Telegraf vengono visualizzati messaggi di errore ricorrenti simili a quelli riportati di seguito: E! [Agent] Error writing to outputs.http: Post "<a href="https://<tenant_url>/rest/v1/lake/ingest/influxdb":" class="bare">https://<tenant_url>/rest/v1/lake/ingest/influxdb": Scadenza contesto superata (timeout client superato in attesa di intestazioni)
Modificare la sezione telegraf in *AgentConfiguration* e impostare *dockerMetricCollectionEnabled* su false. Per ulteriori dettagli, fare riferimento al manuale dell'operatore "opzioni di configurazione".	Mancano i dati *involvedobject* per alcuni registri eventi.
Assicurarsi di aver seguito i passaggi descritti in "Permessi" sezione precedente.	Perché vedo due pod operatore di monitoring in esecuzione, uno denominato netapp-ci-monitoring-operator-<pod> e l'altro denominato monitoring-operator-<pod>?
A partire dal 12 ottobre 2023, Cloud Insights ha ridefinito l'operatore per servire meglio i nostri utenti; affinché tali modifiche siano completamente adottate, è necessario rimuovere il vecchio operatore e. installare il nuovo.	I miei eventi kuowski hanno inaspettatamente smesso di segnalare a Cloud Insights.
Recuperare il nome del pod dell'esportatore di eventi: `kubectl -n netapp-monitoring get pods	grep event-exporter

Problema:	Prova:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` Deve essere "netapp-ci-event-exportant" o "event-exportant". Quindi, modificare l'agente di monitoraggio `kubectl -n netapp-monitoring edit agent`, E impostare il valore per LOG_FILE in modo che rifletta il nome del pod dell'esportatore di eventi appropriato trovato nel passaggio precedente. In particolare, LOG_FILE deve essere impostato su "/var/log/containers/netapp-ci-event-exportant.log" o "/var/log/containers/event-exportant*.log" …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. In alternativa, si può anche disinstallazione e. reinstallare l'agente.
Sto vedendo i pod implementati dal crash dell'operatore di monitoring NetApp Kubernetes a causa di risorse insufficienti.	Fare riferimento all'operatore di monitoraggio Kubernetes NetApp "opzioni di configurazione" Per aumentare i limiti di CPU e/o memoria in base alle esigenze.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Opzioni di configurazione dell'operatore di monitoraggio NetApp Kubernetes

Il "NetApp Kubernetes Monitoring Operator" è possibile personalizzare l'installazione e la configurazione.

La tabella seguente elenca le possibili opzioni per il file AgentConfiguration:

Componente	Opzione	Descrizione
agente		Opzioni di configurazione comuni a tutti i componenti che l'operatore può installare. Queste opzioni possono essere considerate "globali".
	DockerRepo	Un override dockerRepo per estrarre le immagini dai repos del docker privato dei clienti rispetto a Cloud Insights docker repo. Il valore predefinito è Cloud Insights docker repo
	DockerImagePullSecret	Facoltativo: Un segreto per i clienti privati

Componente	Opzione	Descrizione
	Nome cluster	Campo di testo libero che identifica in modo univoco un cluster in tutti i cluster dei clienti. Questo dovrebbe essere unico in un tenant Cloud Insights. Il valore predefinito è quello che il cliente inserisce nell'interfaccia utente per il campo "Cluster Name" (Nome cluster)
	proxy Formato: proxy: server: porta: nome utente: password: NoProxy: IsTelegrafProxyEnabled: IsAuxyEnabled: IsFluentbitProxyEnabled: IsCollectorProxyEnabled:	Opzionale per impostare proxy. Si tratta in genere del proxy aziendale del cliente.
telefono		Opzioni di configurazione che consentono di personalizzare l'installazione di telegraf dell'operatore
	CollectionInterval	Intervallo di raccolta delle metriche, in secondi (max=60s)
	DsCpuLimit	Limite CPU per telegraf ds
	DsMemLimit	Limite di memoria per telegraf ds
	DsCpuRequest	Richiesta CPU per telegraf ds
	DsMemRequest	Richiesta di memoria per telegraf ds
	RsCpuLimit	Limite CPU per telegraf rs
	RsMemLimit	Limite di memoria per telegraf rs
	RsCpuRequest	Richiesta CPU per telegraf rs
	RsMemRequest	Richiesta di memoria per telegraf rs
	DockerMountPoint	Un override per il percorso dockerMountPoint. Questo vale per le installazioni di docker non standard su piattaforme k8s come la fonderia cloud
	DockerUnixSocket	Un override per il percorso dockerUnixSocket. Questo vale per le installazioni di docker non standard su piattaforme k8s come la fonderia cloud.
	CrioSockPath	Un override per il percorso di crioSockPath. Questo vale per le installazioni di docker non standard su piattaforme k8s come la fonderia cloud.

Componente	Opzione	Descrizione
	RunPriveged	Eseguire il container telegraf in modalità privilegiata. Impostare questa opzione su true se SELinux è attivato sui nodi k8s
	Batch Size (dimensione batch)	Vedere "Documentazione sulla configurazione di Telegraf"
	BufferLimit	Vedere "Documentazione sulla configurazione di Telegraf"
	RoundInterval	Vedere "Documentazione sulla configurazione di Telegraf"
	CollectionJitter	Vedere "Documentazione sulla configurazione di Telegraf"
	precisione	Vedere "Documentazione sulla configurazione di Telegraf"
	FlushInterval	Vedere "Documentazione sulla configurazione di Telegraf"
	FlushJitter	Vedere "Documentazione sulla configurazione di Telegraf"
	OutputTimeout	Vedere "Documentazione sulla configurazione di Telegraf"
	DockerMetricCollectionEnabled	Raccogli le metriche di Docker. Per impostazione predefinita, questa opzione è impostata su true e le metriche del docker verranno raccolte per le implementazioni k8s on-premise e basate su docker. Per disattivare la raccolta di metriche docker, impostarla su false.
	DsTolerazioni	teletegraf-ds tollerazioni aggiuntive.
	RsTolerazioni	tollerazioni aggiuntive di telegraf-rs.
kube-state-metrics		Opzioni di configurazione che possono personalizzare l'installazione delle metriche di stato kube dell'operatore
	CpuLimit	Limite di CPU per l'implementazione delle metriche di stato kube
	MemLimit	Limite MEM per l'implementazione delle metriche dello stato del kube
	CpuRequest	Richiesta di CPU per l'implementazione delle metriche di stato del kube
	MemRequest	Richiesta MEM per l'implementazione delle metriche di stato del kube

Componente	Opzione	Descrizione
	risorse	un elenco separato da virgole di risorse da acquisire. esempio: cronjobs,demonset,implementazioni,inserimenti,job,namespaces,nodi,persistentvolumeclaims, persistentvolumes,pod,replicasets,resourcequotas,servizi,statefulsets
	tollerazioni	tolleranze aggiuntive delle metriche dello stato del kube.
	etichette	un elenco separato da virgole di risorse che kube-state-metrics dovrebbe acquisire esempio: cronjobs=[*],demonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namespaces=[*],nodes=[*], persistentvolumeclaims=[*],persistentvolumes=[*],pods=[*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]
registri		Opzioni di configurazione che consentono di personalizzare la raccolta e l'installazione dei log dell'operatore
	ReadFromHead	vero/falso, dovrebbe leggere fluentemente il log dalla testa
	timeout	timeout, in sec.
	DnsMode	TCP/UDP, modalità per DNS
	tolleranza ai bit fluente	tolleranza aggiuntiva ai bit fluenti.
	tolleranza-evento-esportatore	tolleranza aggiuntiva per gli esportatori di eventi.
mappa del carico di lavoro		Opzioni di configurazione che consentono di personalizzare la raccolta e l'installazione della mappa del carico di lavoro dell'operatore
	CpuLimit	Limite CPU per i server di osservazione della rete
	MemLimit	limite mem per gli osservatori netti
	CpuRequest	Richiesta CPU per net osservatore ds
	MemRequest	richiesta mem per net osservatore ds
	MetricAggregationInterval	intervallo di aggregazione metrico, in secondi
	BpfPollInterval	Intervallo di polling BPF, in secondi
	EnableDNSLookup	Vero/falso, attiva ricerca DNS
	l4-tollerazioni	tolleranza aggiuntiva net-observer-l4-ds.
	RunPriveged	Vero/falso - impostare runPrivileged su true se SELinux è abilitato sui tuoi nodi Kubernetes.

Componente	Opzione	Descrizione
change-management		Opzioni di configurazione per l'analisi e la gestione delle modifiche di Kubernetes
	CpuLimit	Limite CPU per change-observer-watch-rs
	MemLimit	Limite MEM per change-observer-watch-rs
	CpuRequest	Richiesta CPU per change-observer-watch-rs
	MemRequest	richiesta mem per change-observer-watch-rs
	FailureDeclarationIntervalMins	Intervallo in minuti dopo il quale un'implementazione non riuscita di un carico di lavoro viene contrassegnata come non riuscita
	DeployAggrIntervalSeconds	Frequenza con cui vengono inviati gli eventi di distribuzione del carico di lavoro in corso
	NonWorkloadAggrIntervalSeconds	Frequenza di combinazione e invio delle implementazioni non a carico di lavoro
	TermsToRedact	Insieme di espressioni regolari utilizzate nei nomi env e nelle mappe di dati il cui valore verrà rivisto Termini di esempio:"pwd", "password", "token", "apikey", "api-key", "jwt"
	AdditionalKindsToWatch	Un elenco separato da virgole di tipi aggiuntivi da guardare dal set di tipi predefinito guardato dal raccoglitore
	KindsToIgnoreFromWatch	Un elenco di tipi separati da virgole da ignorare dall'insieme predefinito di tipi controllati dal raccoglitore
	LogRecordAggrIntervalSeconds	Frequenza con cui i record di registro vengono inviati al ci dal raccoglitore
	tolleranza di controllo	modifica-osservatore-guarda-ds tolleranze aggiuntive. Solo formato abbreviato a riga singola. Esempio: '{key: taint1, operator: Exists, Effect: NoSchedule},{key: taint2, operator: Exists, Effect: NoExecute}'

Esempio di file AgentConfiguration

Di seguito è riportato un esempio di file AgentConfiguration.

```
apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-monitoring-configuration
  namespace: "NAMESPACE_PLACEHOLDER"
  labels:
    installed-by: nkmo-NAMESPACE_PLACEHOLDER
```

```
spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
reference
  # #   To update them, uncomment the line, change the value, and apply
the updated AgentConfiguration.
  agent:
    # # [Required Field] A uniquely identifiable user-friendly
clustername.
    # # clusterName must be unique across all clusters in your Cloud
Insights environment.
    clusterName: "CLUSTERNAME_PLACEHOLDER"

    # # Proxy settings. The proxy that the operator should use to send
metrics to Cloud Insights.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
    # proxy:
    #   server:
    #   port:
    #   noproxy:
    #   username:
    #   password:
    #   isTelegrafProxyEnabled:
    #   isFluentbitProxyEnabled:
    #   isCollectorsProxyEnabled:

    # # [Required Field] By default, the operator uses the CI repository.
    # # To use a private repository, change this field to your repository
name.
    # # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
    dockerRepo: 'DOCKER_REPO_PLACEHOLDER'
    # # [Required Field] The name of the imagePullSecret for dockerRepo.
    # # If you are using a private repository, change this field from
'docker' to the name of your secret.
    {{ if not (contains .Values.config.cloudType "aws") }}# {{ end -}}
    dockerImagePullSecret: 'docker'

    # # Allow the operator to automatically rotate its ApiKey before
expiration.
    # tokenRotationEnabled: '{{
.Values.telegraf_installer.kubernetes.rs.shim_token_rotation  }}'
    # # Number of days before expiration that the ApiKey should be
```

```
rotated. This must be less than the total ApiKey duration.
    # tokenRotationThresholdDays: '{{
.Values.telegraf_installer.kubernetes.rs.shim_token_rotation_threshold_day
s  }}'

  telegraf:
    # # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
    # # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#a
gent

    # # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
    # collectionInterval: '{{
.Values.telegraf_installer.agent_resources.collection_interval }}'
    # # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
    # batchSize: '{{
.Values.telegraf_installer.agent_resources.metric_batch_size }}'
    # # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
    # bufferLimit: '{{
.Values.telegraf_installer.agent_resources.metric_buffer_limit }}'
    # # Collect metrics on multiples of interval (round_interval).
    # roundInterval: '{{
.Values.telegraf_installer.agent_resources.round_interval }}'
    # # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
    # collectionJitter: '{{
.Values.telegraf_installer.agent_resources.collection_jitter }}'
    # # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
    # precision: '{{ .Values.telegraf_installer.agent_resources.precision
}}'
    # # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
    # flushInterval: '{{
.Values.telegraf_installer.agent_resources.flush_interval }}'
    # # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
    # flushJitter: '{{
.Values.telegraf_installer.agent_resources.flush_jitter }}'
```

```
    # # Timeout for writing to outputs (timeout).
    # outputTimeout: '{{
.Values.telegraf_installer.http_output_plugin.timeout }}'

    # # telegraf-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    dsCpuLimit: '{{
.Values.telegraf_installer.telegraf_resources.ds_cpu_limits  }}'
    dsMemLimit: '{{
.Values.telegraf_installer.telegraf_resources.ds_mem_limits  }}'
    dsCpuRequest: '{{
.Values.telegraf_installer.telegraf_resources.ds_cpu_request  }}'
    dsMemRequest: '{{
.Values.telegraf_installer.telegraf_resources.ds_mem_request  }}'

    # # telegraf-rs CPU/Mem limits and requests.
    rsCpuLimit: '{{
.Values.telegraf_installer.telegraf_resources.rs_cpu_limits  }}'
    rsMemLimit: '{{
.Values.telegraf_installer.telegraf_resources.rs_mem_limits  }}'
    rsCpuRequest: '{{
.Values.telegraf_installer.telegraf_resources.rs_cpu_request  }}'
    rsMemRequest: '{{
.Values.telegraf_installer.telegraf_resources.rs_mem_request  }}'

    # # telegraf additional tolerations. Use the following abbreviated
single line format only.
    # # Inspect telegraf-rs/-ds to view tolerations which are always
present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # dsTolerations: ''
    # rsTolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # runPrivileged: 'false'

    # # Collect NFS IO metrics.
    # dsNfsIOEnabled: '{{
.Values.telegraf_installer.kubernetes.ds.shim_nfs_io_processing }}'

    # # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher).  Set this to true if you want collect these
```

```
metrics.
    # managedK8sSystemMetricCollectionEnabled: '{{
.Values.telegraf_installer.kubernetes.shim_managed_k8s_system_metric_colle
ction }}'

    # # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
    # podVolumeMetricCollectionEnabled: '{{
.Values.telegraf_installer.kubernetes.shim_pod_volume_metric_collection
}}'

    # # Declare Rancher cluster as managed.  Set this to true if your
Rancher cluster is managed as opposed to on-premise.
    # isManagedRancher: '{{
.Values.telegraf_installer.kubernetes.is_managed_rancher }}'

  # kube-state-metrics:
    # # kube-state-metrics CPU/Mem limits and requests. By default, when
unset, kube-state-metrics has no CPU/Mem limits nor request.
    # cpuLimit:
    # memLimit:
    # cpuRequest:
    # memRequest:

    # # Comma-separated list of metrics to enable.
    # # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
    # resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespaces,nodes,persisten
tvolumeclaims,persistentvolumes,pods,replicasets,resourcequotas,services,s
tatefulsets'

    # # Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
    # # See metric-labels-allowlist in https://github.com/kubernetes/kube-
state-metrics/blob/main/docs/cli-arguments.md
    # labels:
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'

    # # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
    # # No tolerations are applied by default
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
```

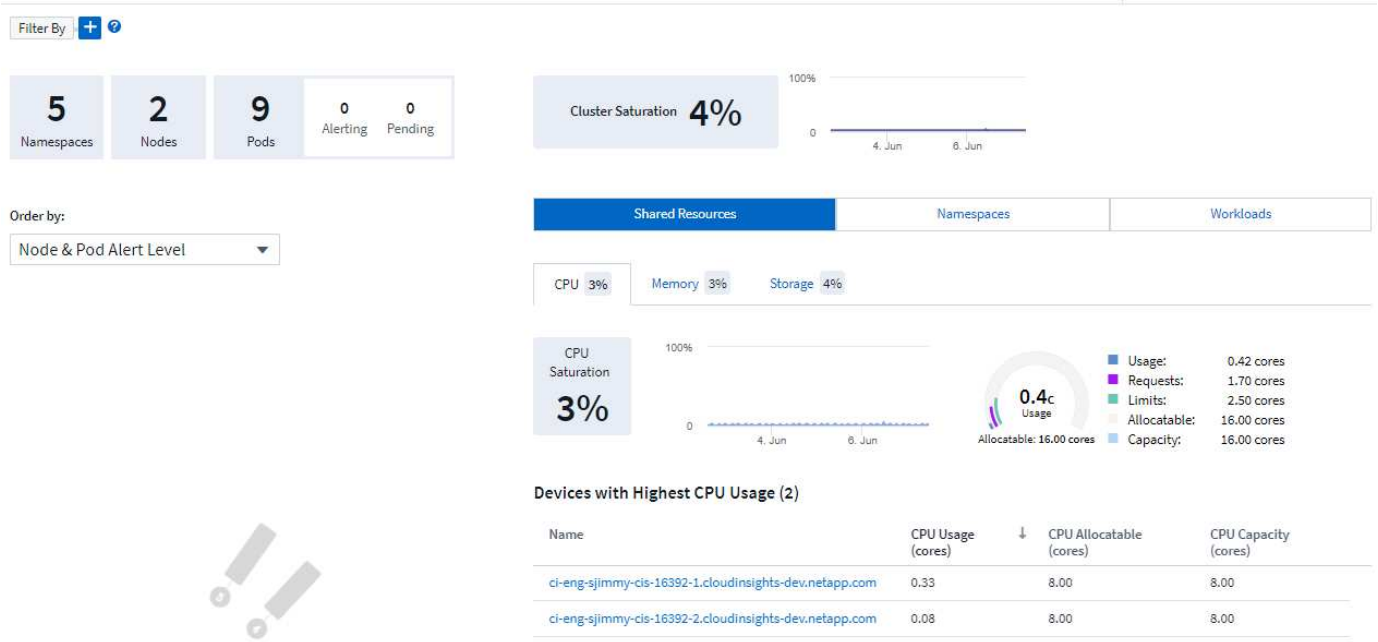
```
    # tolerations: ''

  # # Settings for the Events Log feature.
  # logs:
    # # If Fluent Bit should read new files from the head, not tail.
    # # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
    # readFromHead: "true"

    # # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
    # dnsMode: "UDP"

    # # Logs additional tolerations. Use the following abbreviated single
line format only.
    # # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # fluent-bit-tolerations: ''
    # event-exporter-tolerations: ''

  # # Settings for the Network Performance and Map feature.
  # workload-map:
    # # net-observer-l4-ds CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Metric aggregation interval in seconds. Min=30, Max=120
    # metricAggregationInterval: '60'

    # # Interval for bpf polling. Min=3, Max=15
    # bpfPollInterval: '8'

    # # Enable performing reverse DNS lookups on observed IPs.
    # enableDNSLookup: 'true'

    # # net-observer-l4-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect net-observer-l4-ds to view tolerations which are always
present.
    # # Example: '{key: taint1, operator: Exists, effect:
```

```
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # l4-tolerations: ''

    # # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
    # # Note: In OpenShift environments, this is set to true
automatically.
    # runPrivileged: 'false'

  # change-management:
    # # change-observer-watch-rs CPU/Mem limits and requests.
    # # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
    # cpuLimit: '500m'
    # memLimit: '500Mi'
    # cpuRequest: '100m'
    # memRequest: '500Mi'

    # # Interval in minutes after which a non-successful deployment of a
workload will be marked as failed
    # failureDeclarationIntervalMins: '30'

    # # Frequency at which workload deployment in-progress events are sent
    # deployAggrIntervalSeconds: '300'

    # # Frequency at which non-workload deployments are combined and sent
    # nonWorkloadAggrIntervalSeconds: '15'

    # # A set of regular expressions used in env names and data maps whose
value will be redacted
    # termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"jwt"'

    # # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: 'authorization.k8s.io.subjectaccessreviews'
    # additionalKindsToWatch: ''

    # # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
    # # Each kind will have to be prefixed by its apigroup
    # # Example: 'networking.k8s.io.networkpolicies,batch.jobs'
    # kindsToIgnoreFromWatch: ''

    # # Frequency with which log records are sent to CI from the collector
```

```
    # logRecordAggrIntervalSeconds: '20'

    # # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
    # # Inspect change-observer-watch-ds to view tolerations which are
always present.
    # # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
    # watch-tolerations: ''----
```

Pagina dei dettagli del cluster Kubernetes

La pagina dei dettagli del cluster Kubernetes visualizza una panoramica dettagliata del cluster Kubernetes.



Namespace, Node e Pod Counts

I conteggi nella parte superiore della pagina mostrano il numero totale di spazi dei nomi, nodi e pod nel cluster, nonché il numero di pop-of che sono attualmente in stato di avviso e in sospeso.

Risorse condivise e saturazione

Nella parte superiore destra della pagina dei dettagli si trova la saturazione del cluster come percentuale corrente e un grafico che mostra la tendenza recente nel tempo. La saturazione del cluster è la più alta tra CPU, memoria o saturazione dello storage in ogni punto del tempo.

Di seguito, la pagina mostra per impostazione predefinita l'utilizzo di **risorse condivise**, con schede per CPU, memoria e storage. Ogni scheda mostra la percentuale di saturazione e l'andamento nel tempo, con ulteriori dettagli sull'utilizzo. Per lo storage, il valore mostrato è maggiore tra il backend e la saturazione del file system, che vengono calcolati in modo indipendente.

I dispositivi con il massimo utilizzo sono mostrati in una tabella nella parte inferiore. Fare clic su un collegamento qualsiasi per esplorare questi dispositivi.

Spazi dei nomi

La scheda Namespaces visualizza un elenco di tutti gli spazi dei nomi nell'ambiente Kubernetes, mostrando l'utilizzo di CPU e memoria e il numero di carichi di lavoro in ogni spazio dei nomi. Fare clic sui link Name (Nome) per esplorare ciascun namespace.

Shared Resources | **Namespaces** | Workloads

Namespaces (5)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
netapp-monitoring	0.25	0.38	4
kube-system	0.01	0.03	3
kube-public	0.00	0.00	0
kube-node-lease	0.00	0.00	0
default	0.00	<0.01	1

Carichi di lavoro

Allo stesso modo, la scheda workload visualizza un elenco dei carichi di lavoro in ogni namespace, mostrando nuovamente l'utilizzo di CPU e memoria. Facendo clic sullo spazio dei nomi, è possibile accedere a ciascuno di essi.

Shared Resources | Namespaces | **Workloads**

Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

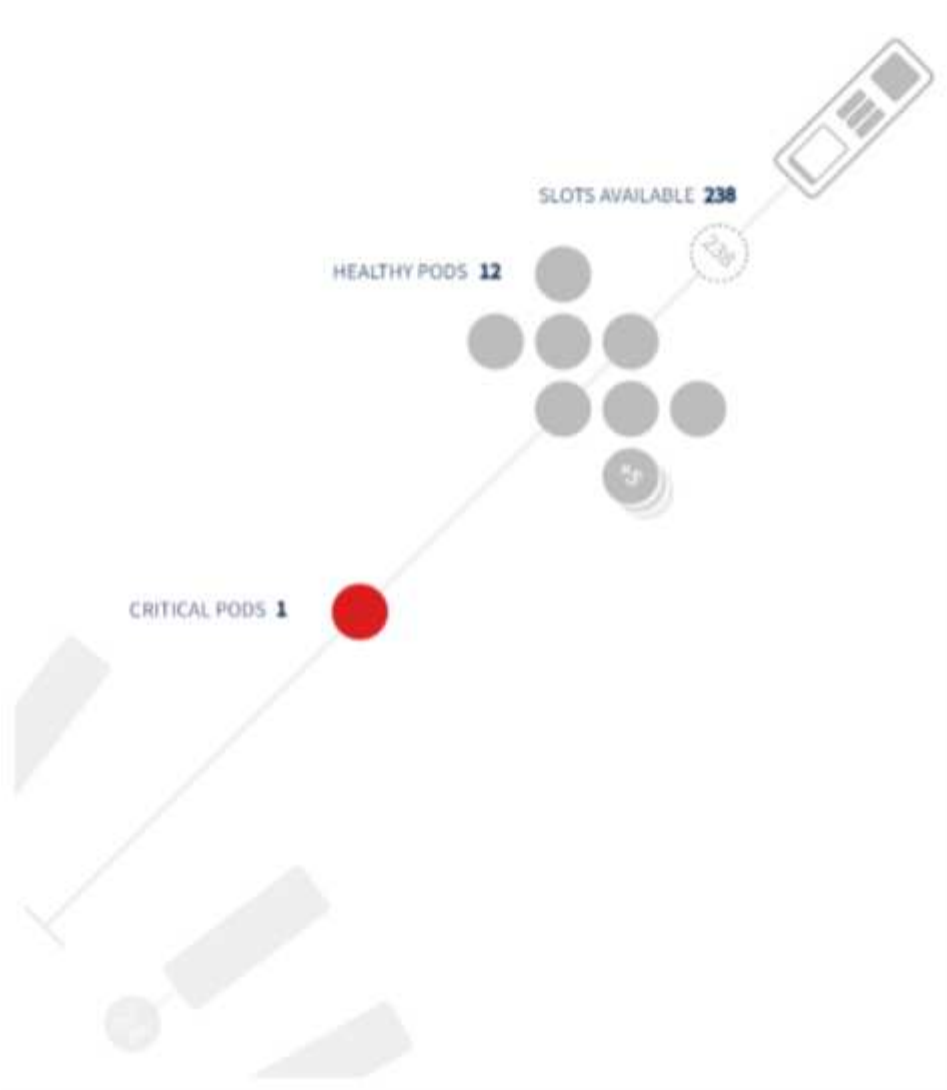
La "ruota" del cluster

La sezione "ruota" del cluster fornisce informazioni sullo stato dei nodi e dei pod, che è possibile analizzare per ulteriori informazioni. Se il cluster contiene più nodi di quelli visualizzabili in quest'area della pagina, sarà possibile ruotare la manopola utilizzando i pulsanti disponibili.

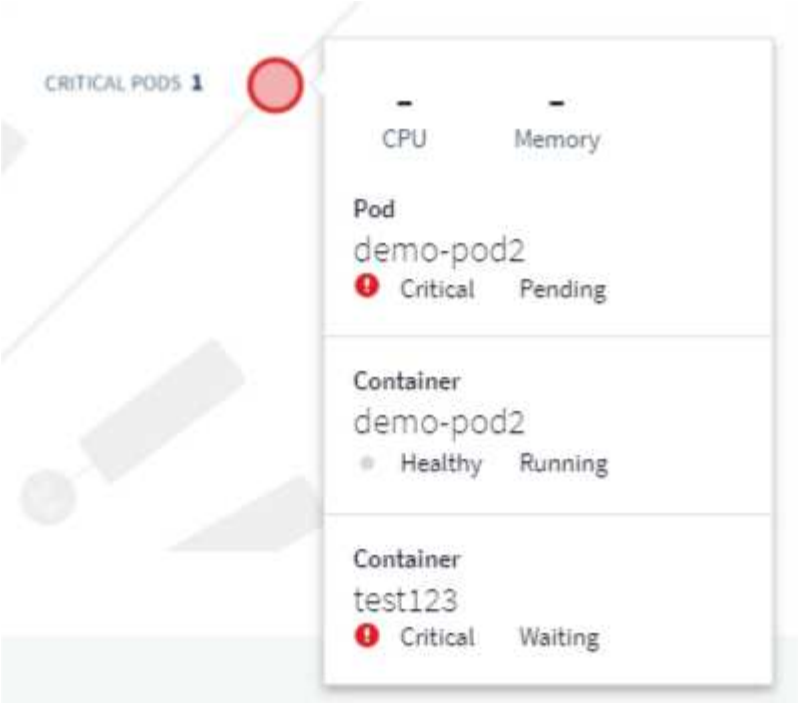
I pod o i nodi di avviso vengono visualizzati in rosso. Le aree di "avvertenza" sono visualizzate in arancione. I pod non pianificati (ovvero non collegati) vengono visualizzati nell'angolo inferiore della "ruota" del cluster.

Passando il mouse su un pod (cerchio) o su un nodo (barra) si estende la vista del nodo.

Facendo clic sul pod o sul nodo in tale vista, viene eseguito lo zoom avanti nella vista Expanded Node (nodo espanso).



Da qui, è possibile passare il mouse su un elemento per visualizzare i dettagli relativi a tale elemento. Ad esempio, passando il mouse sul pod critico in questo esempio vengono visualizzati i dettagli relativi a tale pod.



È possibile visualizzare le informazioni relative a filesystem, memoria e CPU passando il mouse sugli elementi Node.

Una nota sugli indicatori

Gli indicatori della memoria e della CPU mostrano tre colori, in quanto indicano *used* in relazione alla *capacità allocabile* e alla *capacità totale*.

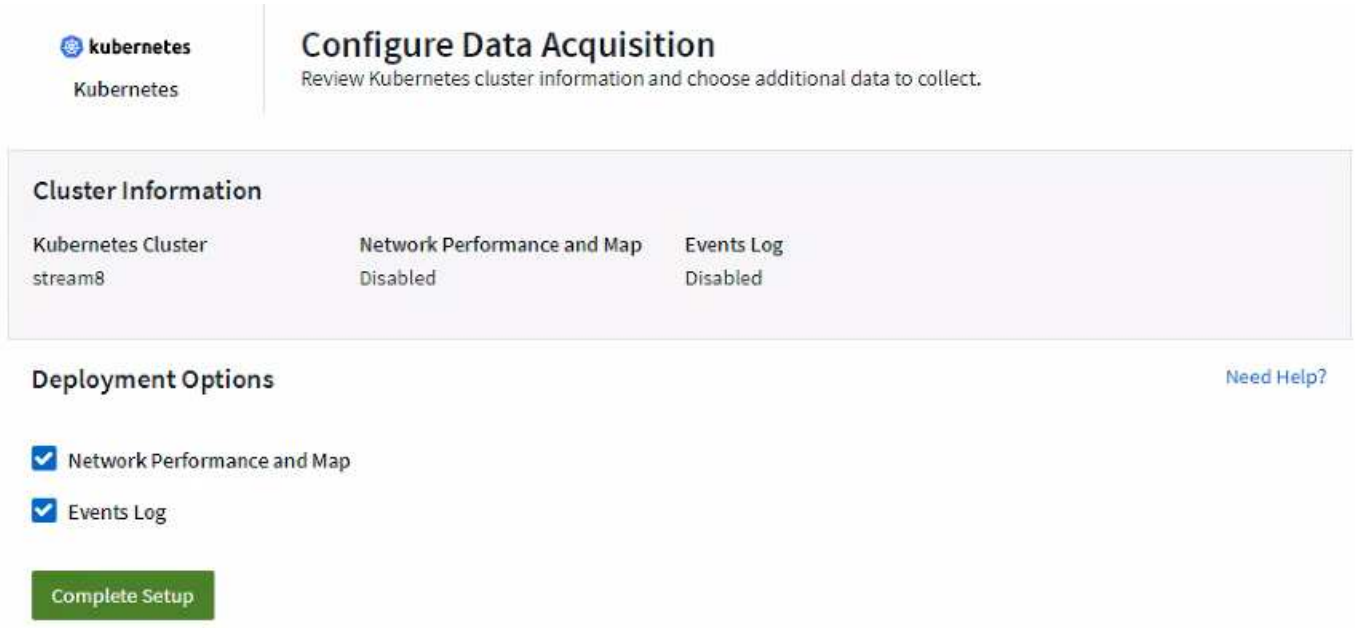
Kubernetes Network Performance Monitoring and Map

Le funzionalità MAP e di Kubernetes Network Performance Monitoring semplificano il troubleshooting mappando le dipendenze tra i servizi (anche denominati workload) e offrono visibilità real-time sulle latenze delle performance di rete e sulle anomalie per identificare i problemi di performance prima che incidano sugli utenti.
Questa funzionalità aiuta le organizzazioni a ridurre i costi complessivi analizzando e revisionando i flussi di traffico Kubernetes.

Caratteristiche principali: • La mappa del carico di lavoro presenta le dipendenze e i flussi dei carichi di lavoro di Kubernetes e evidenzia i problemi di rete e di performance. • Monitora il traffico di rete tra pod, carichi di lavoro e nodi Kubernetes; identifica l'origine dei problemi di traffico e latenza. • Riduci i costi complessivi analizzando il traffico di rete in entrata, in uscita, cross-region e cross-zone.

Prerequisiti

Prima di poter utilizzare Kubernetes Network Performance Monitoring and Map, è necessario aver configurato "NetApp Kubernetes Monitoring Operator" per attivare questa opzione. Durante l'implementazione dell'operatore, selezionare la casella di controllo "Network Performance and Map" (prestazioni di rete e mappa) per attivarla. È inoltre possibile attivare questa opzione accedendo a una landing page di Kubernetes e selezionando "Modify Deployment" (Modifica distribuzione).



Monitor

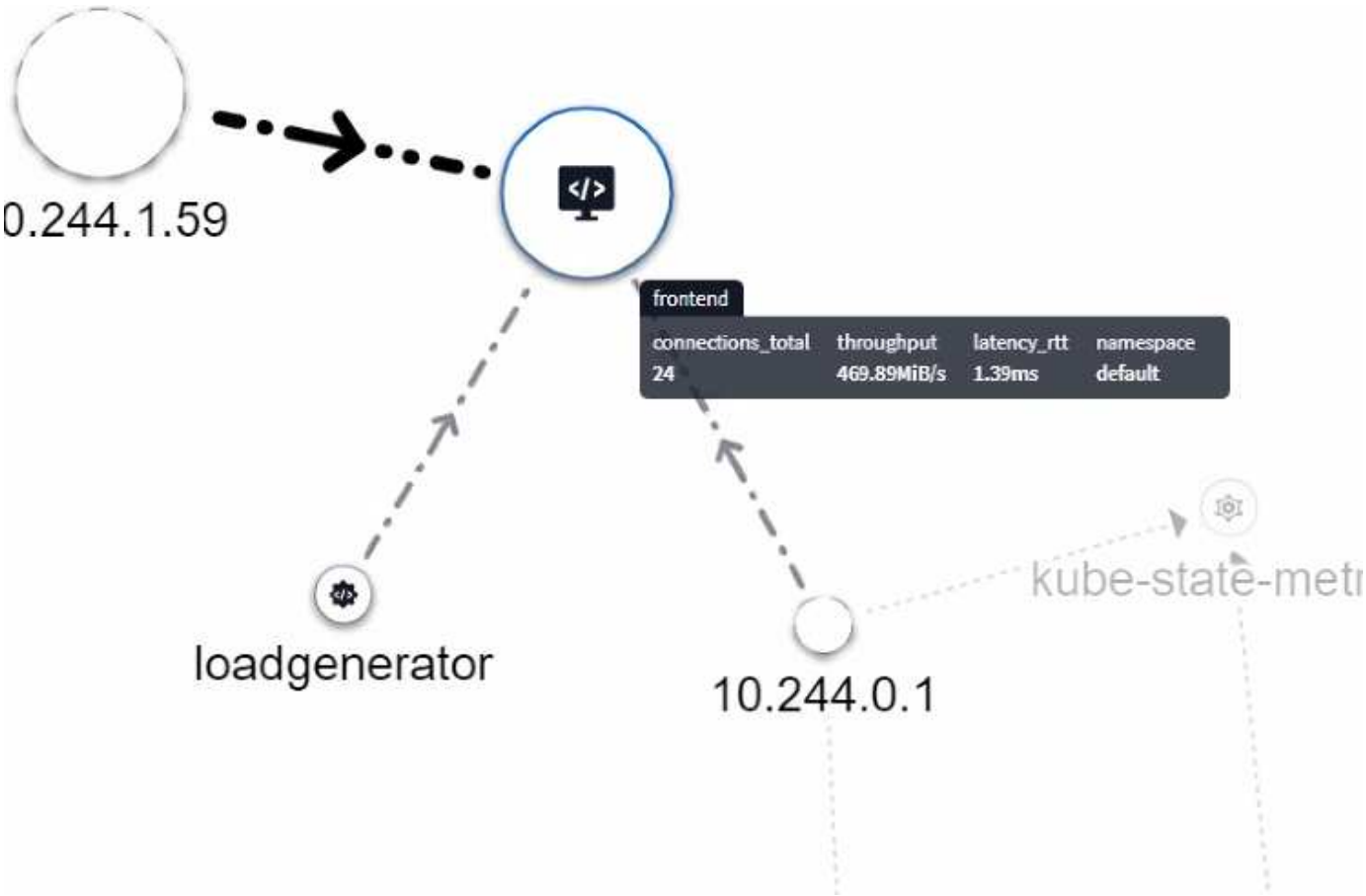
La mappa del carico di lavoro utilizza "monitor" per ricavare informazioni. Cloud Insights fornisce una serie di monitor Kubernetes predefiniti (si noti che per impostazione predefinita potrebbero essere *in pausa*). È possibile *riprendere* (ad esempio attivare) i monitor desiderati) oppure creare monitor personalizzati per gli oggetti Kubernetes, che verranno utilizzati anche dalla mappa del carico di lavoro.

È possibile creare avvisi Cloud Insights metric su uno qualsiasi dei tipi di oggetto riportati di seguito. Assicurarsi che i dati siano raggruppati in base al tipo di oggetto predefinito.

- kubernetes.workload
- kubernetes.demonset
- kubernetes.deployment
- kubernetes.cronjob
- kubernetes.job
- kubernetes.replicaset
- kubernetes.statefulset
- kubernetes.pod
- kubernetes.network_traffic_l4

La mappa

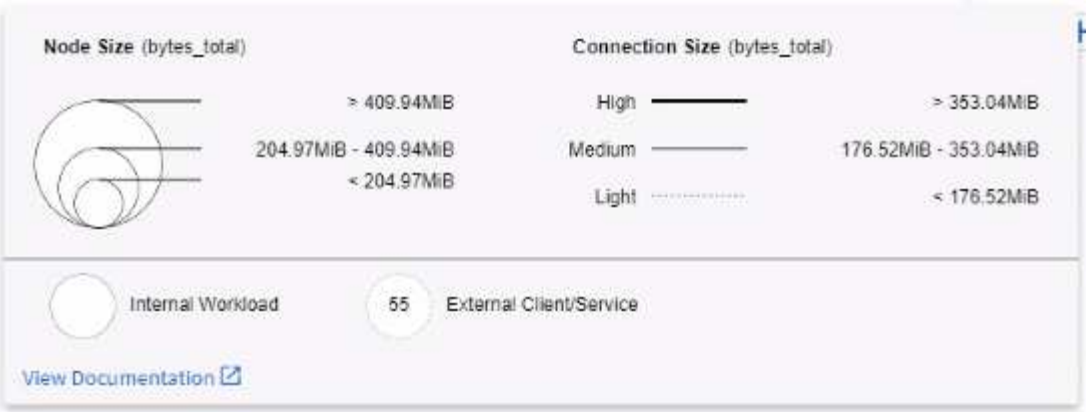
La mappa mostra i servizi/carichi di lavoro e le loro relazioni tra loro. Le frecce indicano le direzioni del traffico. Passando il mouse su un carico di lavoro vengono visualizzate informazioni riepilogative per tale carico di lavoro, come si può vedere in questo esempio:



Le icone all'interno dei cerchi rappresentano diversi tipi di servizio. Si noti che le icone sono visibili solo se sono presenti gli oggetti sottostanti etichette.

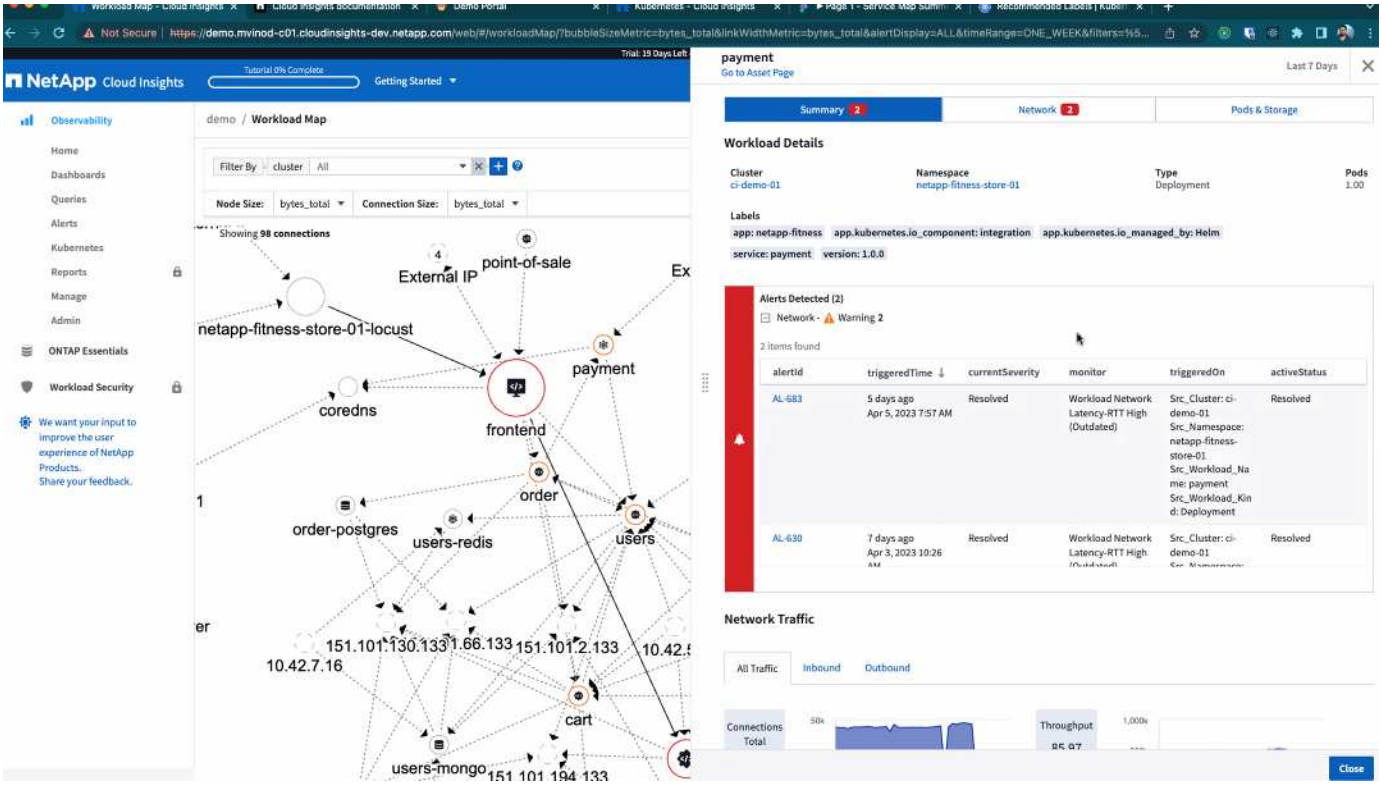
La dimensione di ciascun cerchio indica la dimensione del nodo. Si noti che queste dimensioni sono relative, il livello di zoom del browser o le dimensioni dello schermo potrebbero influire sulle dimensioni effettive dei cerchi. Allo stesso modo, lo stile della linea di traffico offre una vista a colpo d'occhio delle dimensioni della connessione; le linee solide in grassetto sono un traffico elevato, mentre le linee tratteggiate sono un traffico minore.

I numeri all'interno dei cerchi sono il numero di connessioni esterne attualmente elaborate dal servizio.



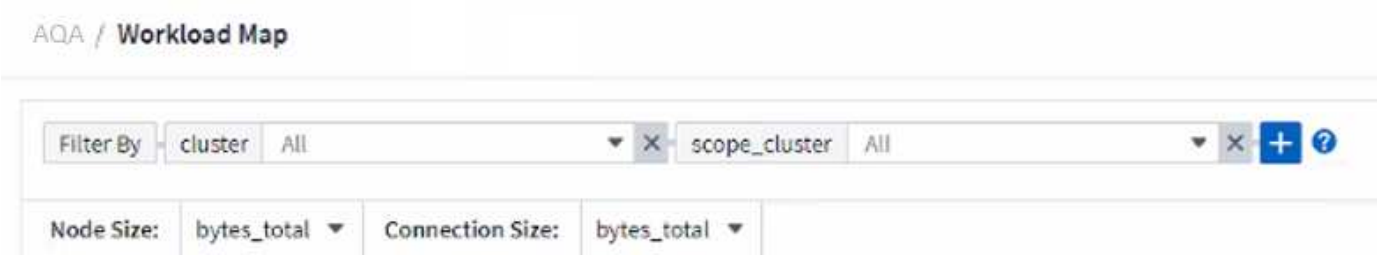
Avvisi e dettagli sul carico di lavoro

I cerchi visualizzati a colori indicano un avviso o un avviso di livello critico per il carico di lavoro. Passare il puntatore del mouse sul cerchio per visualizzare un riepilogo del problema oppure fare clic sul cerchio per aprire un pannello a scorrimento con maggiori dettagli.

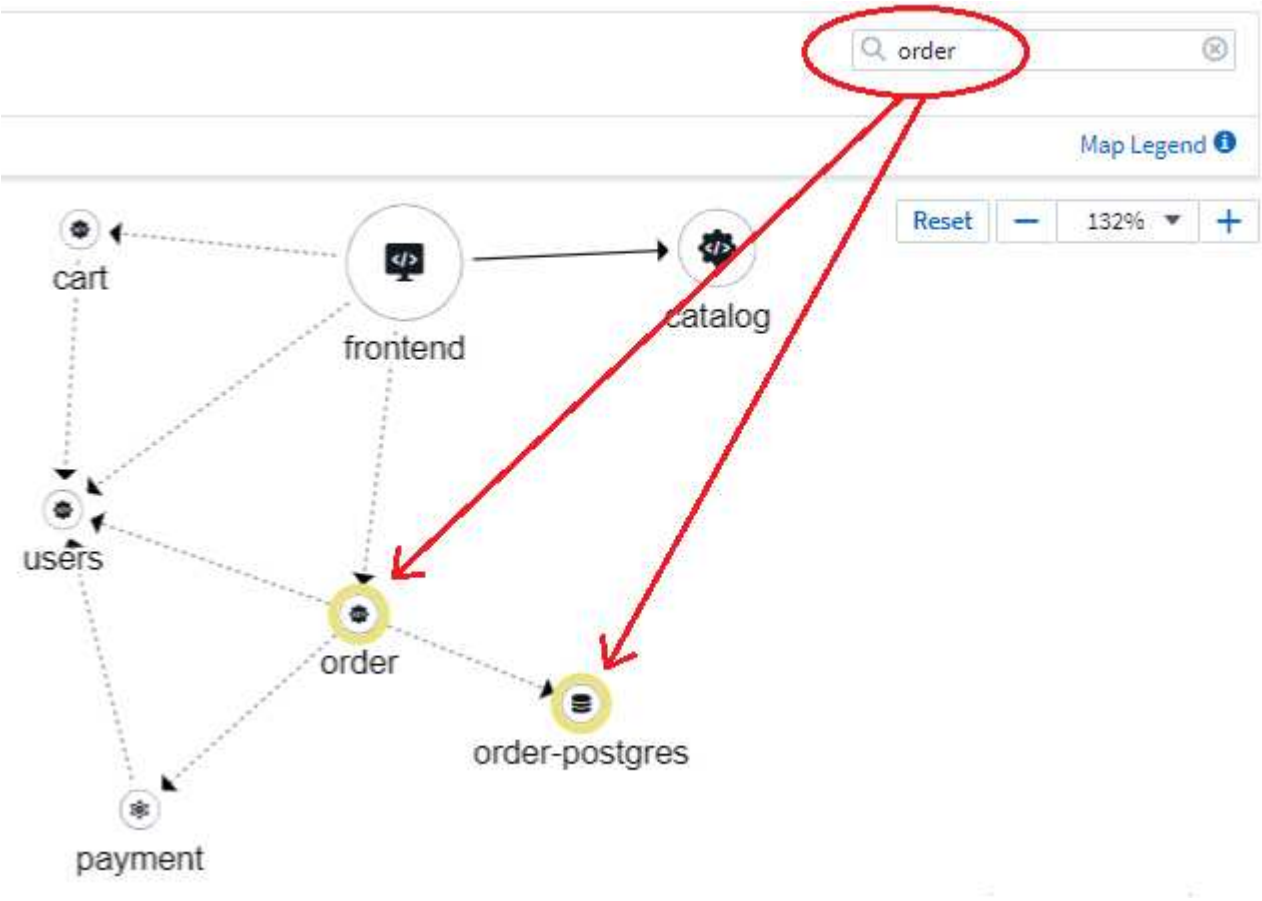


Ricerca e filtraggio

Come per le altre funzionalità di Cloud Insights, è possibile impostare facilmente i filtri in modo che si concentrino sugli oggetti o sugli attributi dei carichi di lavoro specifici desiderati.



Allo stesso modo, digitando una stringa nel campo *Find* si evidenzieranno i carichi di lavoro corrispondenti.



Etichette dei carichi di lavoro

Le etichette dei carichi di lavoro sono necessarie se si desidera che la mappa identifichi i tipi di carichi di lavoro visualizzati (ad esempio, le icone dei cerchi). Le etichette sono derivate come segue:

- Nome del servizio/applicazione in esecuzione in termini generici
- Se l'origine è un pod:
  - L'etichetta deriva dall'etichetta del carico di lavoro del pod
  - Etichetta prevista sul carico di lavoro: App.kubernetes.io/component
  - Riferimento nome etichetta: https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/
  - Etichette consigliate:
    - frontend

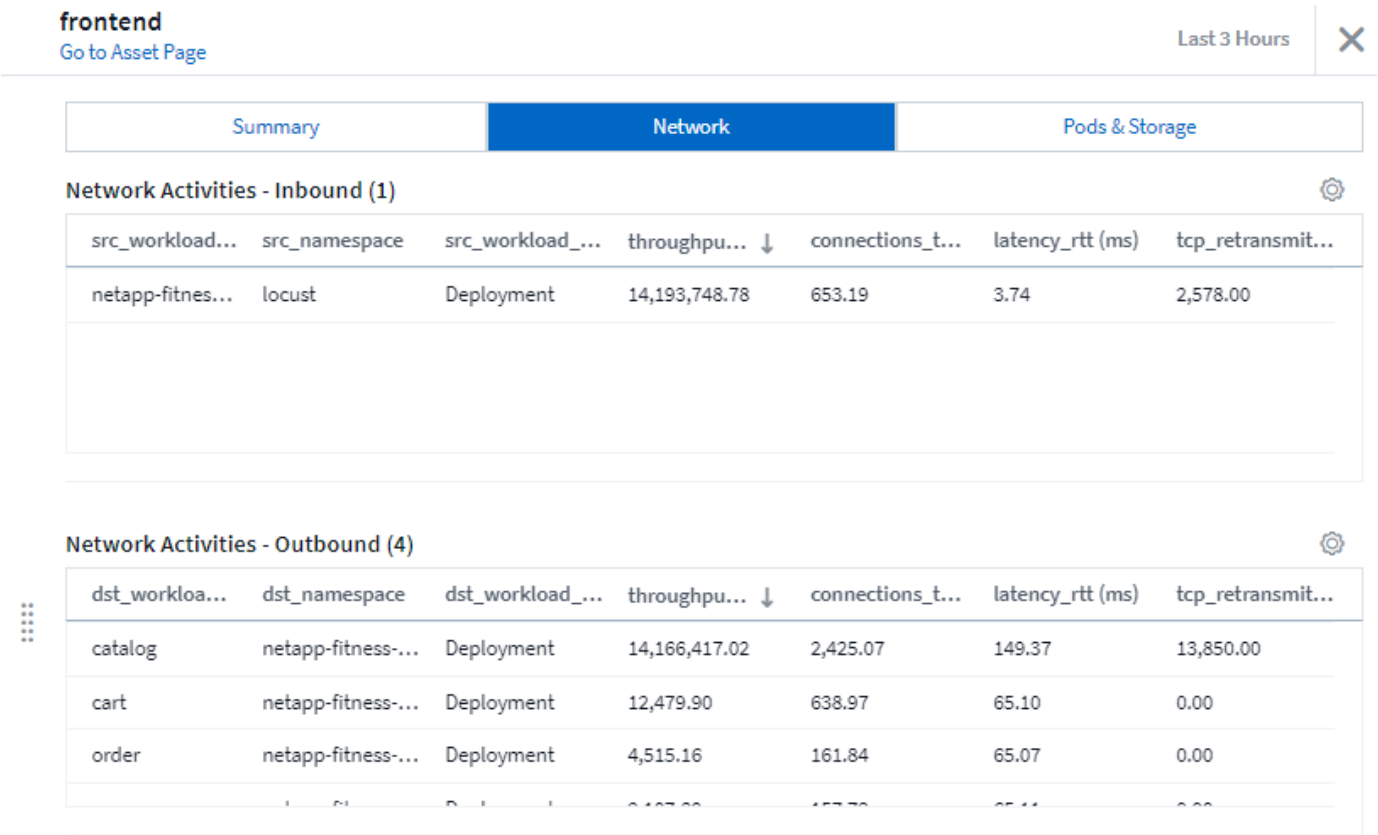
    - back-end
    - database
    - cache
    - coda
    - kafka
- Se l'origine è esterna al cluster kubernetes:
  - Cloud Insights tenterà di analizzare il nome DNS risolto per estrarre il tipo di servizio.

    Ad esempio, con un nome DNS risolto pari a *s3.eu-north-1.amazonaws.com*, il nome risolto viene analizzato per ottenere *s3* come tipo di servizio.

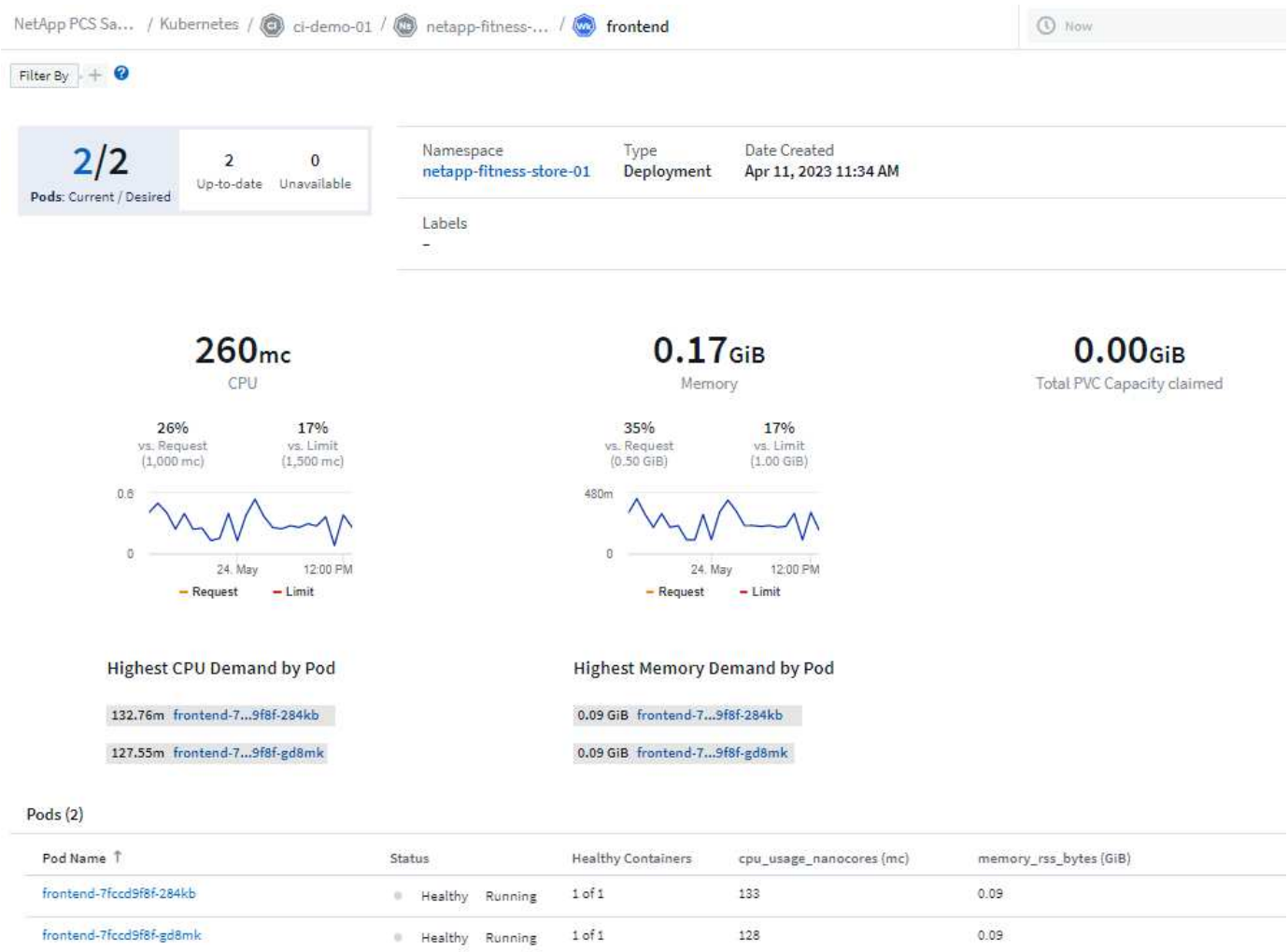
Tuffati in profondità

Facendo clic con il pulsante destro del mouse su un carico di lavoro, è possibile visualizzare ulteriori opzioni. Ad esempio, da qui è possibile ingrandire per visualizzare le connessioni per quel carico di lavoro.

In alternativa, puoi aprire il pannello a scorrimento dei dettagli per visualizzare direttamente la scheda *Summary*, *Network* o *Pod & Storage*.



Infine, selezionando *Go to Asset Page* si apre la landing page dettagliata delle risorse per il carico di lavoro.



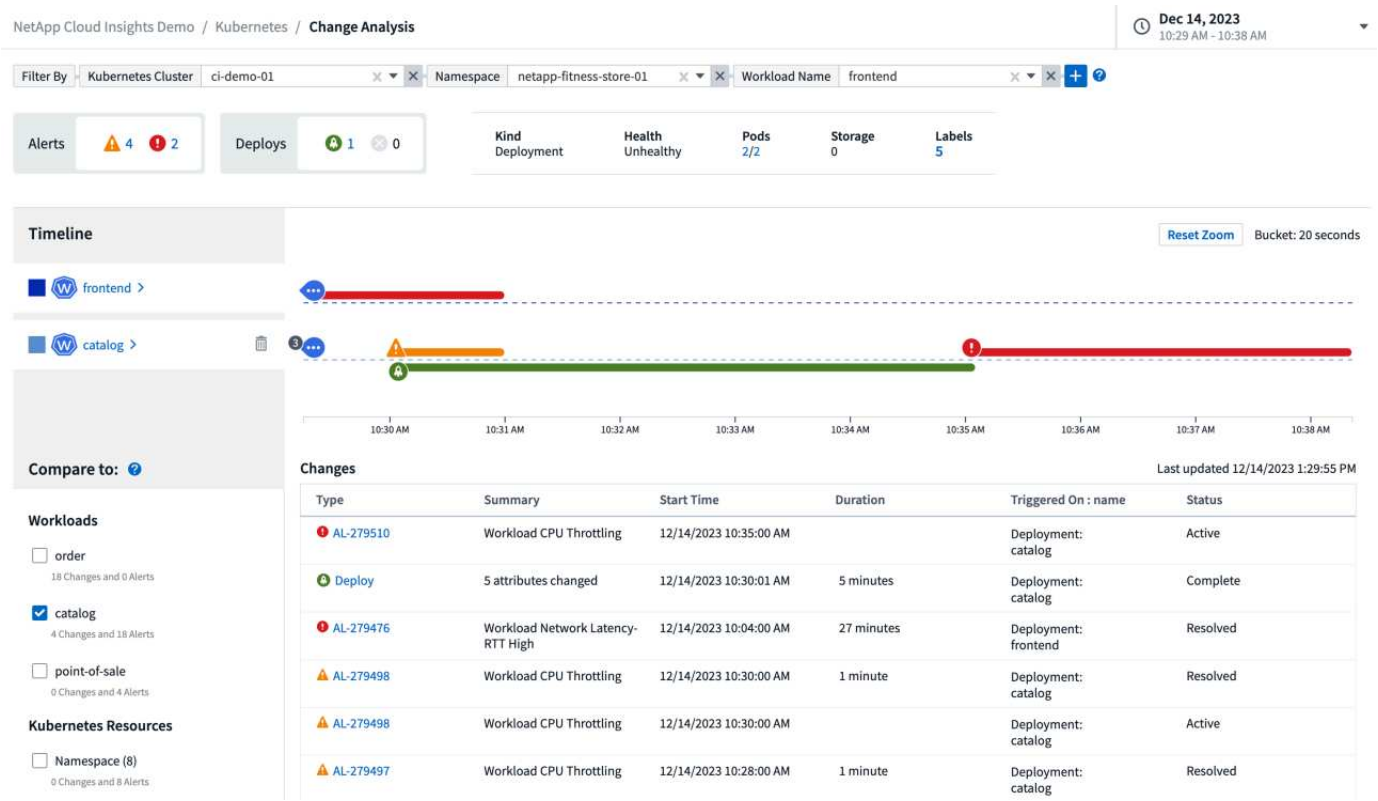
Analytics delle modifiche di Kubernetes

Kubernetes Change Analytics offre una vista completa delle recenti modifiche all'ambiente K8s. Gli avvisi e lo stato dell'implementazione sono a portata di mano. Con Change Analytics, puoi monitorare ogni modifica di implementazione e configurazione e correlarla con lo stato e le performance dei servizi, dell'infrastruttura e dei cluster K8s.

Tenere presente quanto segue:

- Negli ambienti multi-tenant, è possibile che si verifichino interruzioni a causa di modifiche non configurate correttamente. In ambienti molto dinamici, l'analisi delle modifiche Cloud Insights potrebbe non essere in grado di tenere traccia correttamente di tutte le modifiche.
- Change Analytics offre un singolo riquadro per visualizzare e correlare lo stato dei carichi di lavoro e le modifiche alla configurazione. Questo può essere utile nella risoluzione dei problemi degli ambienti dinamici.

Per visualizzare Kubernetes Change Analytics, accedere a **Kubernetes > Change Analysis**.



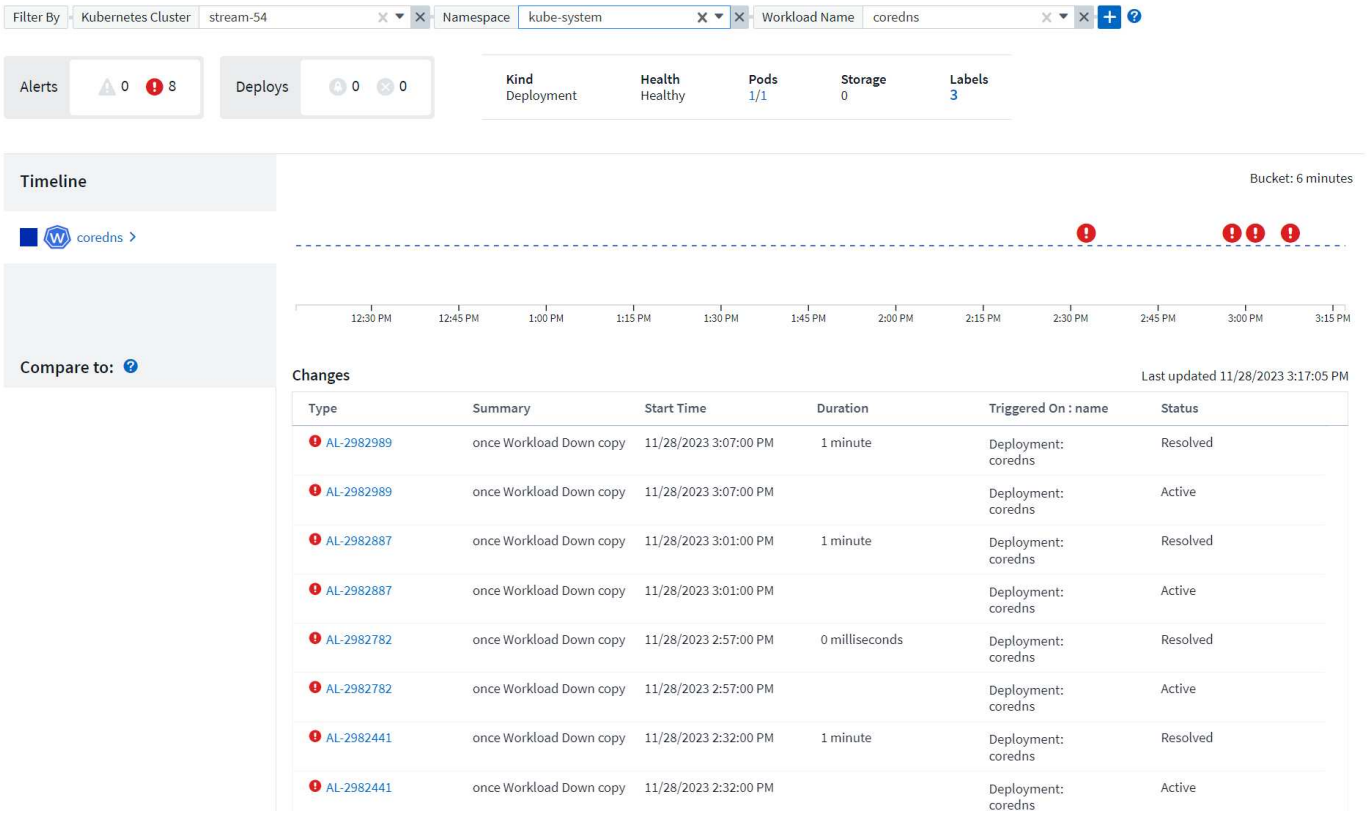
.

La pagina viene aggiornata automaticamente in base all'intervallo di tempo Cloud Insights attualmente selezionato. Intervalli di tempo più piccoli significano un aggiornamento dello schermo più frequente.

Filtraggio

Come per tutte le funzionalità di Cloud Insights, filtrare l'elenco di modifiche è intuitivo: Nella parte superiore della pagina, immettere o selezionare i valori per il cluster Kubernetes, lo spazio dei nomi o il workload oppure aggiungere i propri filtri selezionando il pulsante {+].

Quando si applica un filtro a un cluster, uno spazio dei nomi e un carico di lavoro specifici (insieme agli altri filtri impostati), viene visualizzata una timeline di distribuzione e avvisi per il carico di lavoro nello spazio dei nomi in quel cluster. Ingrandire ulteriormente facendo clic e trascinando il grafico per concentrarsi su un intervallo di tempo più specifico.

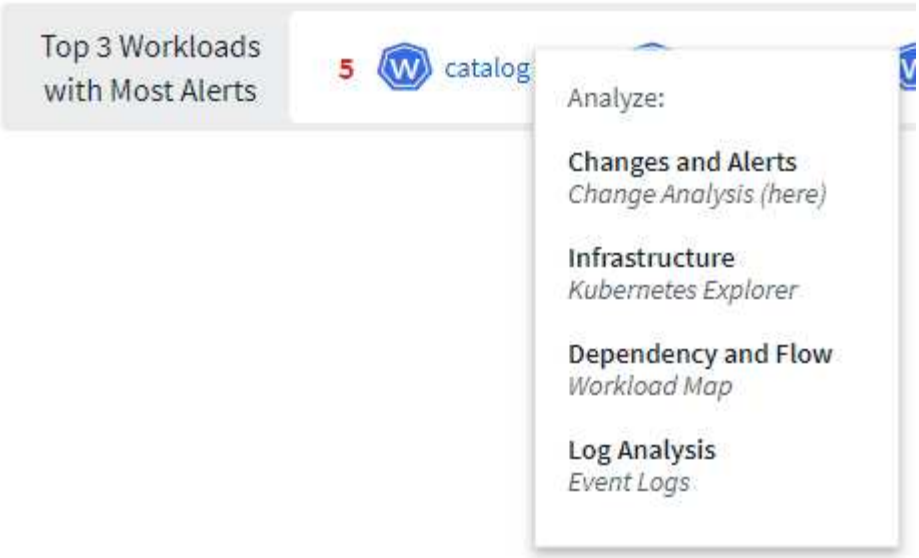


Stato rapido

Al di sotto dell'area di filtraggio sono presenti diversi indicatori di livello alto. A sinistra si trova il numero di avvisi (attenzione e critico). Questo numero include gli avvisi *Active* e *Resolved*. Per visualizzare solo gli avvisi *attivi*, imposta un filtro per "Stato" e scegli "attivo".

Qui viene visualizzato anche lo stato di distribuzione. Anche in questo caso, l'impostazione predefinita è quella di mostrare il numero di implementazioni *started*, *complete* e *Failed*. Per visualizzare solo le distribuzioni *non riuscite*, impostare un filtro per "Stato" e selezionare "non riuscito".

I primi 3 carichi di lavoro con un maggior numero di avvisi sono i prossimi. Il numero in rosso accanto a ciascun carico di lavoro indica il numero di avvisi relativi a tale carico di lavoro. Fare clic sul collegamento del carico di lavoro per esplorare tramite l'infrastruttura (Kubernetes Explorer), le dipendenze (Mappa del carico di lavoro) o l'analisi del registro (registri eventi).



Pannello Dettagli

Selezionando una modifica nell'elenco si apre un pannello che descrive la modifica in modo più dettagliato. Ad esempio, la selezione di una distribuzione non riuscita mostra un riepilogo della distribuzione, con i tempi di inizio e fine, la durata e il punto in cui è stata attivata la distribuzione, con i collegamenti per esplorare tali risorse. Visualizza inoltre il motivo dell'errore, le eventuali modifiche correlate e gli eventi associati.

Deploy Failed

Summary

Start Time
10/18/2023 2:40:01 PM

End Time
10/18/2023 2:50:02 PM

Duration
10 minutes

Triggered On
ci-demo-01 >
netapp-fitness-store-01 >
billing-accounts >

Triggered On : kind
Deployment

Failure Detail

Reason For Failure
ProgressDeadlineExceeded - ReplicaSet "billing-accounts-6ddc7df546" has timed out progressing.

Message
Failed deploy

Changes (2)

Attribute Name	Previous	New
spec.template.spec.containers[0].image	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.0	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.09
metadata.annotations.deployment.kubernetes.io/revision	2964	2965

All Changes Diff

Associated Events

Event Logs

Close

La selezione di un avviso fornisce dettagli sull'avviso, compreso il monitor che ha attivato l'avviso, nonché un grafico che mostra una timeline visiva per l'avviso.

Approfondimenti

Approfondimenti

Le informazioni ti consentono di esaminare aspetti come l'utilizzo delle risorse e il modo in cui questo influisce sulle altre risorse o sulle analisi time-to-full.

Sono disponibili numerose informazioni. Vai a **Dashboard > Insights** per iniziare a fare immersioni. È possibile visualizzare le informazioni attive (informazioni attualmente in corso) nella scheda principale o quelle inattive nella scheda *informazioni inattive*. Le informazioni inattive sono quelle che erano precedentemente attive ma non si verificano più.

Tipi di Insight

Risorse condivise sotto stress

I carichi di lavoro ad alto impatto possono ridurre le performance di altri carichi di lavoro in una risorsa condivisa. In questo modo, la risorsa condivisa viene sottoposta a stress. Cloud Insights fornisce strumenti per analizzare la saturazione delle risorse e l'impatto nell'ambiente. "Scopri di più"

Kubernetes Namespace che esauriscono lo spazio

Kubernetes Namespaces running out of Space Insight offre una vista dei carichi di lavoro degli spazi dei nomi Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni spazio si esaurisca. "Scopri di più"

Recuperare lo storage a freddo ONTAP

L'analisi di *recupero dello storage a freddo ONTAP* fornisce dati sulla capacità a freddo, sui potenziali risparmi in termini di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP. "Scopri di più"

> Si tratta di una funzione *Preview* che può cambiare nel tempo man mano che vengono apportati dei miglioramenti. "Scopri di più" Informazioni sulle funzioni di anteprima di Cloud Insights.

Approfondimenti: Risorse condivise sotto stress

I carichi di lavoro ad alto impatto possono ridurre le performance di altri carichi di lavoro in una risorsa condivisa. In questo modo, la risorsa condivisa viene sottoposta a stress. Cloud Insights fornisce strumenti per analizzare la saturazione delle risorse e l'impatto nell'ambiente.

Terminologia

Quando si parla di impatto sul carico di lavoro o sulle risorse, sono utili le seguenti definizioni.

Un **carico di lavoro impegnativo** è un carico di lavoro attualmente identificato come un impatto sulle altre risorse nel pool di storage condiviso. Questi carichi di lavoro consentono IOPS più elevati (ad esempio), riducendo gli IOPS nei carichi di lavoro interessati. I carichi di lavoro esigenti vengono talvolta chiamati *carichi di lavoro ad alto consumo*.

Un carico di lavoro * con impatto è un carico di lavoro che viene influenzato da un carico di lavoro molto elevato nel pool di storage condiviso. Questi carichi di lavoro stanno sperimentando IOPS ridotti e/o latenza superiore, causati dai carichi di lavoro esigenti.

Si noti che se Cloud Insights non ha rilevato il carico di lavoro di calcolo principale, il volume o il volume interno stesso verrà riconosciuto come carico di lavoro. Questo vale per carichi di lavoro esigenti e interessati.

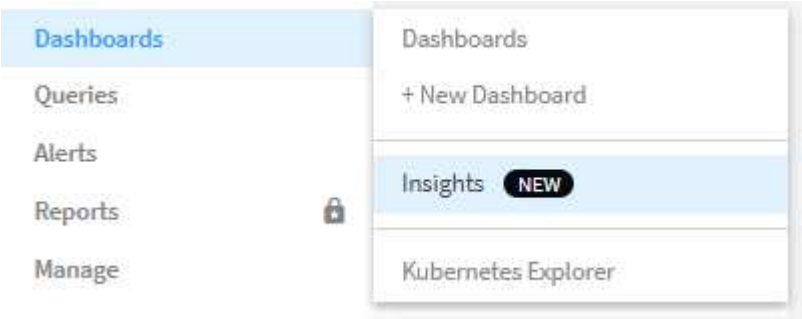
La saturazione delle risorse condivise è il rapporto tra IOPS e *baseline*.

Baseline è definito come il punto dati massimo riportato per ciascun carico di lavoro nell'ora immediatamente precedente la saturazione rilevata.

Si verifica un **conflitto** o **saturazione** quando gli IOPS influiscono su altre risorse o carichi di lavoro nel pool di storage condiviso.

Carichi di lavoro impegnativi

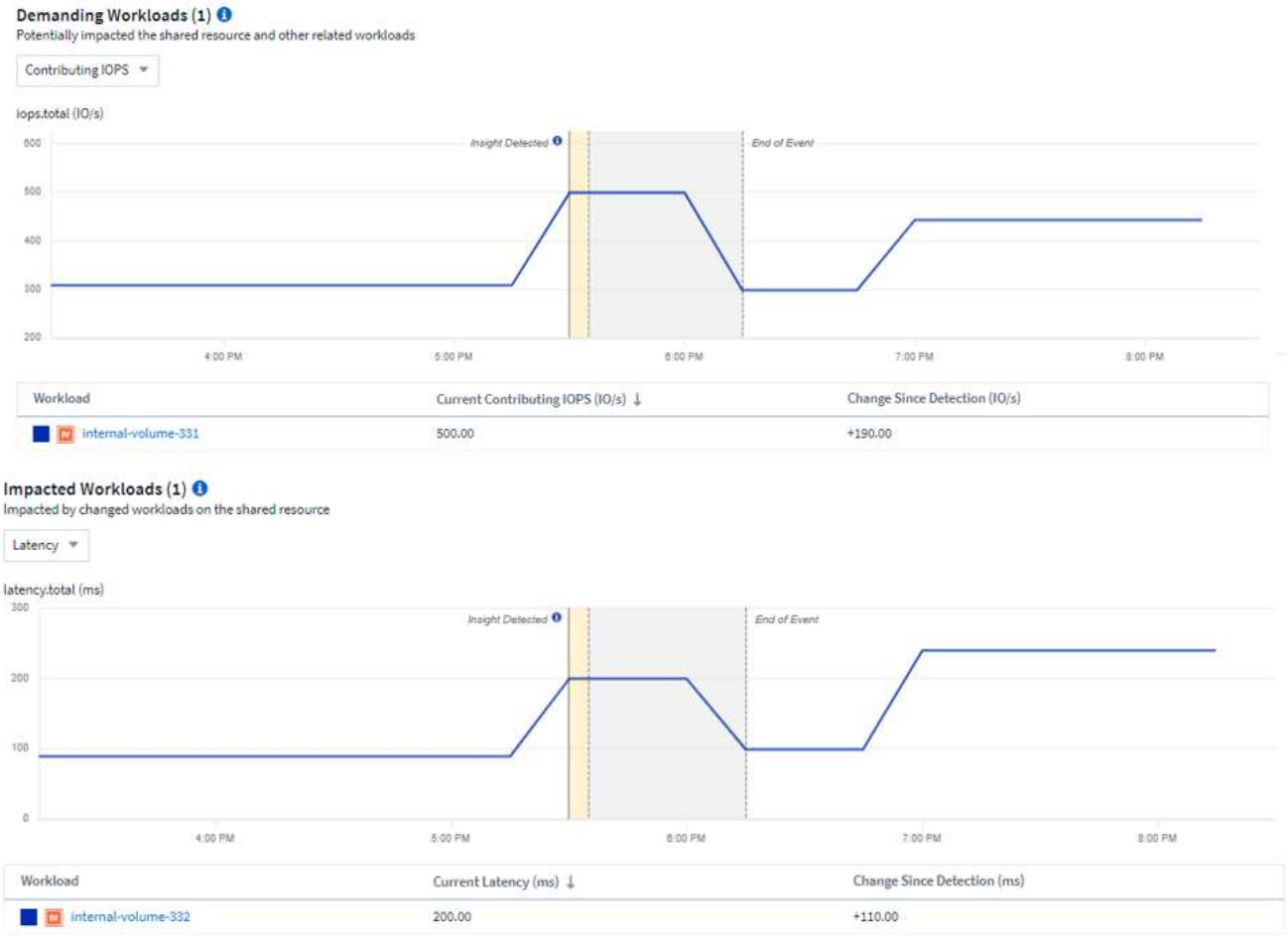
Per iniziare a esaminare i carichi di lavoro impegnativi e influenzati nelle risorse condivise, fare clic su **Dashboard > Insights** e selezionare l'Insight * risorse condivise sotto stress*.



Cloud Insights visualizza un elenco dei carichi di lavoro in cui è stata rilevata una saturazione. Si noti che Cloud Insights mostrerà i carichi di lavoro in cui è stata rilevata almeno una *risorsa impegnativa* **o** *risorsa interessata*.

Fare clic su un carico di lavoro per visualizzare la relativa pagina dei dettagli. Il grafico in alto mostra l'attività sulla risorsa condivisa (ad esempio, un pool di storage) in cui si verifica il conflitto/saturazione.

Di seguito sono riportati due grafici che mostrano i carichi di lavoro *esigenti* e i carichi di lavoro *interessati* da quelli esigenti.



Sotto ogni tabella è riportato un elenco dei carichi di lavoro e/o delle risorse che influiscono o sono interessate dal conflitto. Facendo clic su una risorsa (ad esempio, una macchina virtuale) si apre una pagina dei dettagli relativa a tale risorsa. Facendo clic su un workload si apre una pagina di query che mostra i pod coinvolti. Si noti che se il collegamento apre una query vuota, il pod interessato potrebbe non essere più parte del conflitto attivo. È possibile modificare l'intervallo di tempo della query per visualizzare l'elenco di pod in un intervallo di tempo maggiore o più mirato.

Cosa devo fare per risolvere la saturazione?

È possibile adottare una serie di misure per ridurre o eliminare la possibilità di saturazione nell'ambiente. Per visualizzare tali suggerimenti, espandere il link **+Mostra consigli** nella pagina. Ecco alcune cose che puoi provare.

- Sposta i consumatori con IOPS elevati

  Sposta i carichi di lavoro "avidi" in pool di storage meno saturi. Si consiglia di valutare il Tier e la capacità di questi pool prima di spostare i carichi di lavoro, per evitare costi non necessari o ulteriori vincoli.

- Implementare una policy di qualità del servizio (QoS)

  L'implementazione di una policy di QoS per ogni workload per garantire una quantità sufficiente di risorse disponibili riduce la saturazione dello storage Pool. Si tratta di una soluzione a lungo termine.

- Aggiungere risorse aggiuntive

  Se la risorsa condivisa (ad esempio, lo Storage Pool) ha raggiunto il punto di saturazione IOPS, l'aggiunta

di più dischi o più veloci al pool garantisce risorse disponibili sufficienti per ridurre la saturazione.

Infine, è possibile fare clic su **Copy Insight link** per copiare l'URL della pagina negli Appunti e condividerlo più facilmente con i colleghi.

Approfondimenti: Kubernetes Namespace che esauriscono lo spazio

Esaurire lo spazio nel tuo ambiente non è mai una buona situazione. Cloud Insights ti aiuta a prevedere il tempo che hai prima che i volumi persistenti di Kubernetes diventino pieni.

L'Insight *Kubernetes Namespace running of Space* ti offre una vista dei carichi di lavoro degli spazi dei nomi Kubernetes che rischiano di esaurire lo spazio, con una stima del numero di giorni rimanenti prima che ogni volume persistente si esaurisca.

Per visualizzare questa Insight, accedere a **Dashboard > Insights**.

Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
1 workload at risk on es	35	1	2 days ago
1 workload at risk on manager	24	1	2 days ago
2 workloads at risk on cloudinsights	1	2	2 days ago

Fare clic su un carico di lavoro per aprire una pagina dei dettagli per Insight. In questa pagina viene visualizzato un grafico che mostra le tendenze della capacità del carico di lavoro e una tabella che mostra quanto segue:

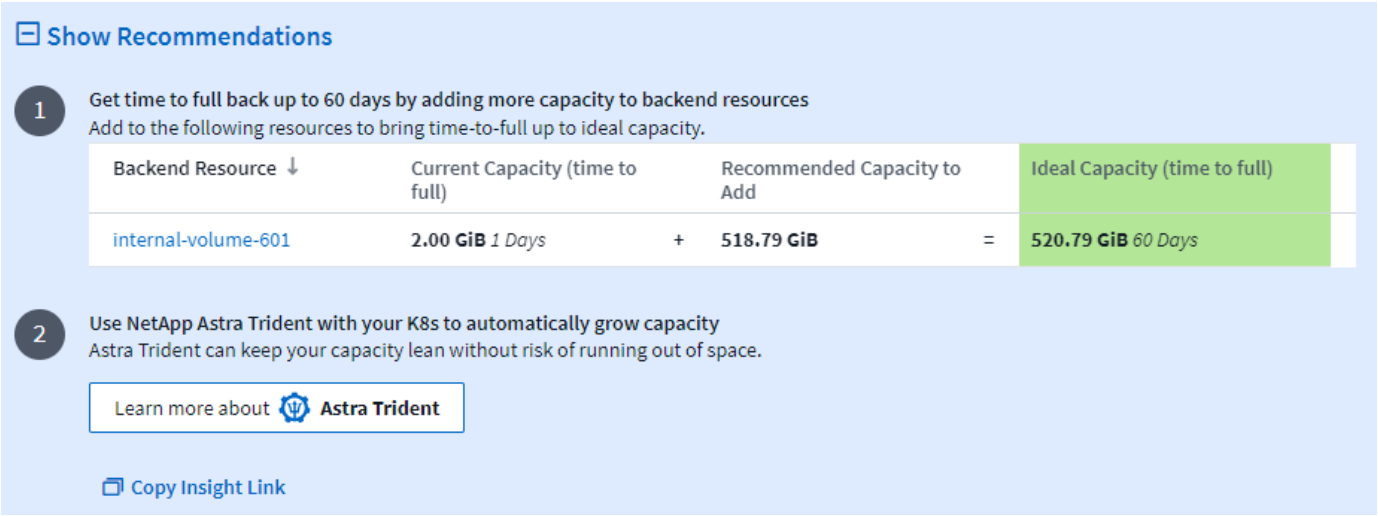
- Nome del carico di lavoro
- Volume persistente interessato
- Tempo previsto per il pieno in giorni
- Capacità del volume persistente
- Risorse di storage back-end interessate, con capacità corrente utilizzata fuori dalla capacità totale. Facendo clic su questo collegamento viene visualizzata la landing page dettagliata del volume di back-end.

Workloads at risk (2)

⊟ Workloads	Persistant Volume (pvClaim)	Time to Full (Days) ↓	Persistant Volume Capacity (GiB)	Backend Storage Resource (Capacity Used)	
⊞ multi (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)
⊞ taskmanager (1)	pv1 (pvc1)	1	4.00	internal-volume-601	60.00% (3.00/5.00 GiB)

Cosa posso fare se lo spazio è esaurito?

Nella pagina Insight, fare clic su **+Mostra consigli** per visualizzare le possibili soluzioni. L'opzione più semplice quando si esaurisce lo spazio consiste nell'aggiungere sempre più capacità e Cloud Insights mostra la capacità ottimale da aggiungere per aumentare il tempo di riempimento a una previsione di 60 giorni. Vengono inoltre mostrati altri consigli.



È anche possibile copiare un comodo link a questa Insight, per aggiungere ai preferiti la pagina o per condividerla facilmente con il tuo team.

Approfondimenti: Recuperare lo storage a freddo ONTAP

L'analisi di *recupero dello storage a freddo ONTAP* fornisce dati sulla capacità a freddo, sui potenziali risparmi in termini di costi/energia e sulle azioni consigliate per i volumi sui sistemi ONTAP.

Per visualizzare queste informazioni, accedere a **Dashboard > informazioni** e dare un'occhiata alle *informazioni sullo storage a freddo ONTAP*. Tenere presente che questa analisi elencherà solo le memorie interessate se Cloud Insights ha rilevato il cold storage, altrimenti verrà visualizzato un messaggio "tutto chiaro".

Tenere presente che i dati cold meno di 30 giorni non vengono visualizzati.

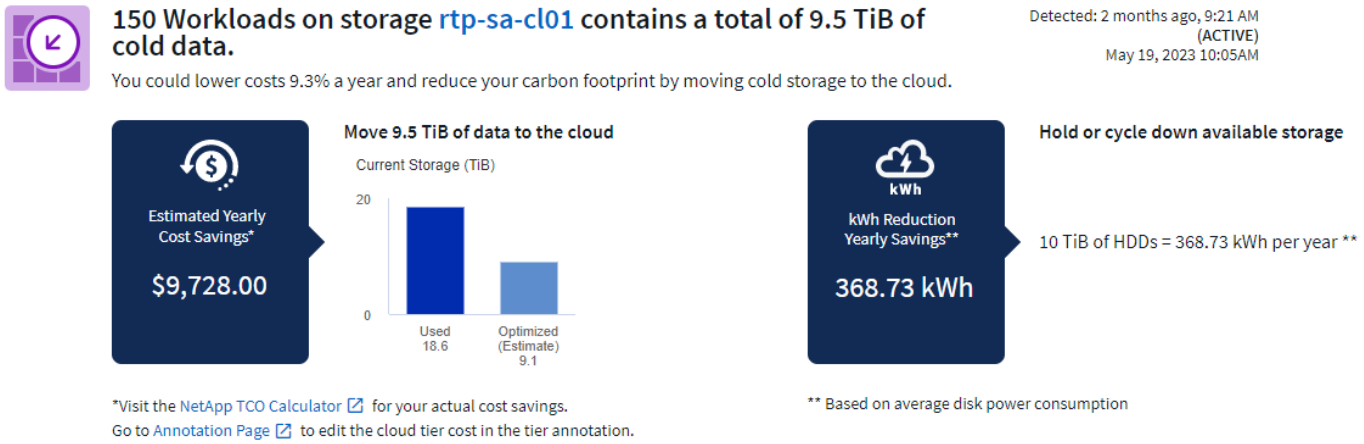
Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected
0.30 TiB of cold data on storage rtp-sa-cl04	0.30	45	an hour ago
1.22 TiB of cold data on storage umeng-aff300-01-02	1.22	84	16 days ago
11.62 TiB of cold data on storage rtp-sa-cl01	11.62	171	16 days ago

La descrizione di Insight fornisce un'indicazione rapida della quantità di dati rilevati come "freddi" e dello storage su cui risiedono i dati. La tabella fornisce anche un numero di workload con dati cold.

Selezionando una Insight dall'elenco, si apre una pagina che mostra ulteriori dettagli, tra cui consigli per spostare i dati nel cloud o per eseguire il ciclo di inattività dei dischi unizzati, oltre a risparmi stimati di costi ed

energia che potrebbero essere possibili implementando tali raccomandazioni. La pagina fornisce anche un pratico link a. "Calcolatore del TCO di NetApp" così puoi sperimentare i numeri.



Raccomandazioni

Nella pagina Insight, espandere **Recommendations** per esplorare le seguenti opzioni:

- Spostare i carichi di lavoro inutilizzati (zombie) su un livello di storage (HDD) a basso costo

  Utilizzando la bandiera zombie, il cold storage e il numero di giorni, è possibile trovare la quantità di dati più fredda e più grande e spostare il carico di lavoro su un livello di storage a costo inferiore (ad esempio un pool di storage che utilizza lo storage su disco rigido). Un carico di lavoro è considerato uno "zombie" quando non riceve richieste di i/o significative per 30 giorni o più.

- Eliminare i carichi di lavoro inutilizzati

  Verificare quali carichi di lavoro non sono in uso e prendere in considerazione la possibilità di archiviarli o rimuoverli dal sistema storage.

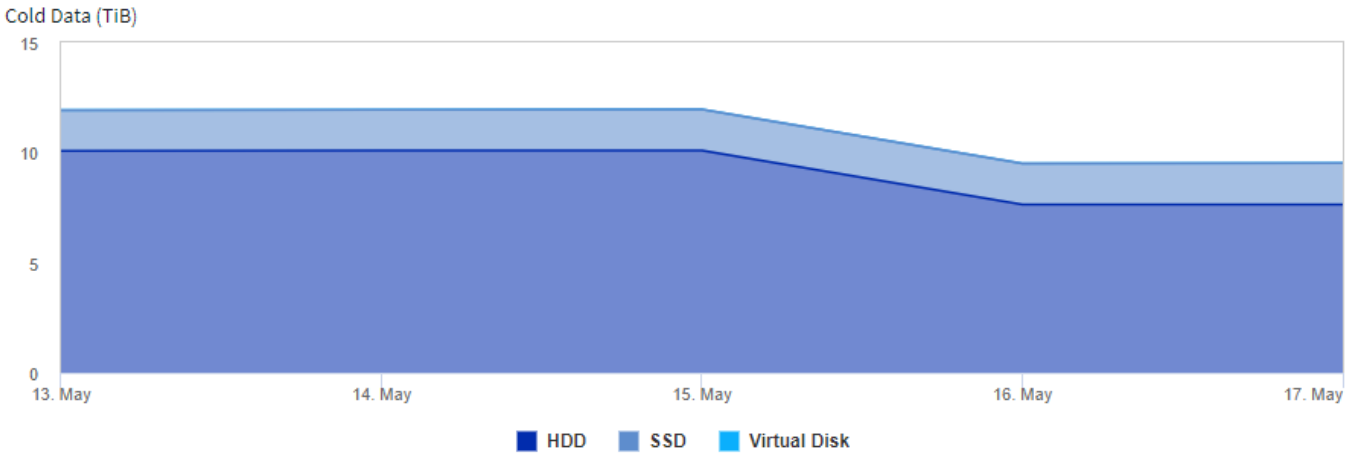
- Prendiamo in considerazione la soluzione Fabric Pool di NetApp

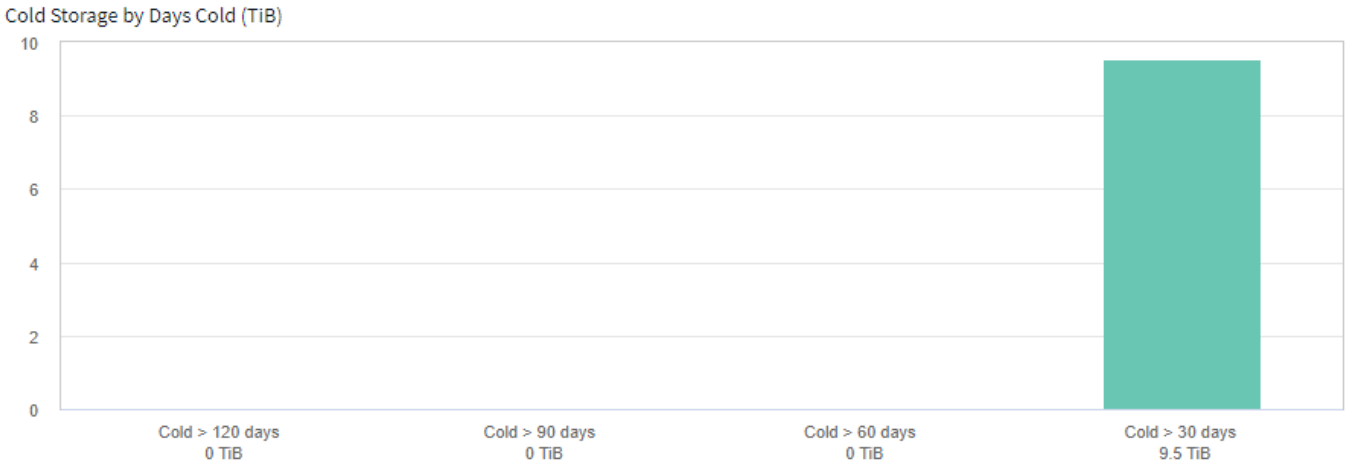
  Di NetApp "Soluzione Fabric Pool" esegue automaticamente il tier dei dati cold su cloud storage a basso costo, aumentando così l'efficienza del tuo tier di performance e fornendo protezione dei dati remota.

Visualizzare ed esplorare

I grafici e la tabella forniscono ulteriori informazioni sui trend e consentono di analizzare i singoli carichi di lavoro.

Cluster Cold Storage Trend Show Details





Workloads with cold data (150) View all workloads

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

Elementi di base di ONTAP

Gli elementi di base di ONTAP sono una serie di dashboard e flussi di lavoro che offrono panoramiche dettagliate degli inventari e dei carichi di lavoro di ONTAP. Quando si lavora con ONTAP Essentials, potrebbero essere utilizzati i seguenti termini:

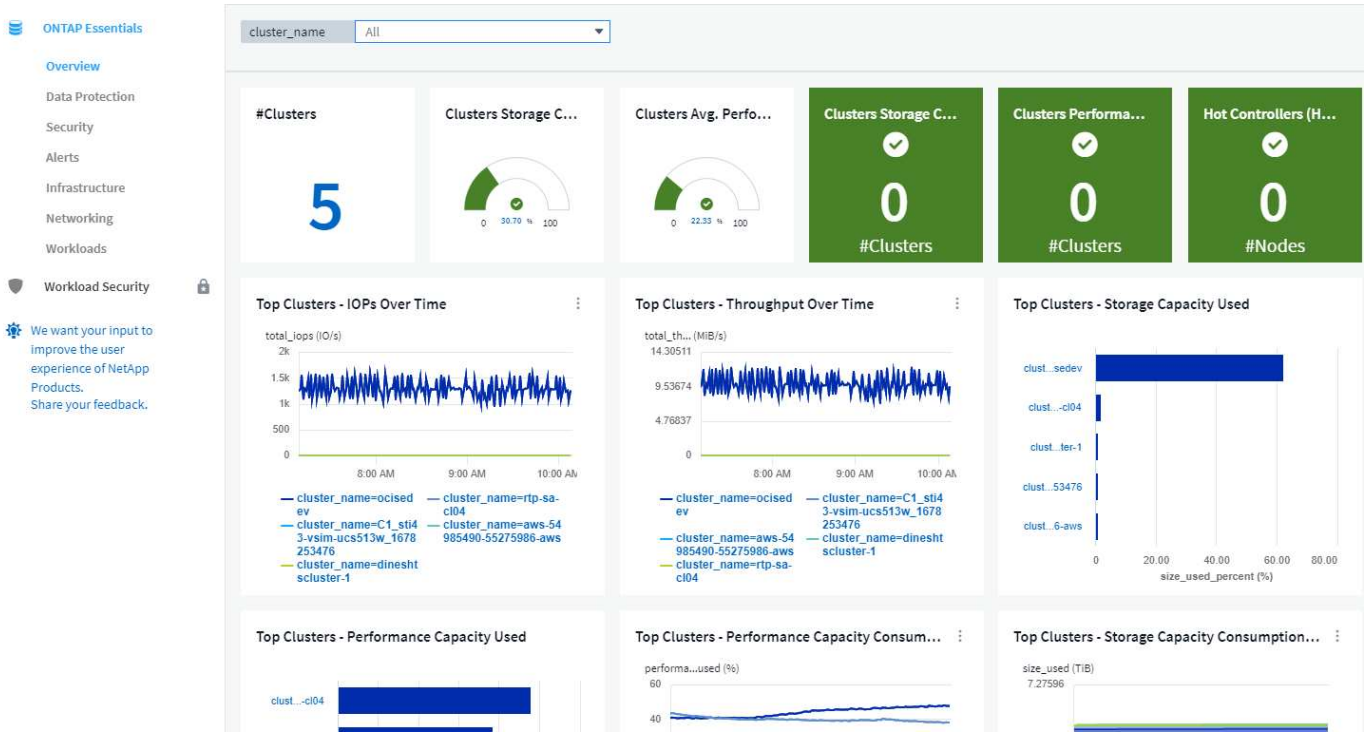
- Infrastructure/Inventory (infrastruttura/inventario): Oggetti che forniscono servizi di storage/rete ai dati dell'utente
- Workload: Oggetti che forniscono agli utenti un'interfaccia per la lettura/scrittura dei dati.
- Protezione dei dati: Oggetti che possono essere protetti utilizzando le tecnologie di protezione dei dati di NetApp

Per ulteriori termini e definizioni relativi a ONTAP, vedere "Servizio di raccolta dati ONTAP" documentazione.

ONTAP Essentials richiede almeno un data collector ONTAP funzionante con i dati raccolti negli ultimi sette giorni.

Panoramica

Per iniziare l'esplorazione, selezionare **elementi essenziali di ONTAP** dal menu principale di Cloud Insights.



La dashboard **Overview** visualizza informazioni utili come il numero di cluster nell'ambiente con le relative percentuali di capacità e performance complessive. Verranno inoltre visualizzati dati predittivi relativi al numero di giorni previsti fino a quando la capacità dello storage o la capacità delle performance non esauriscono lo spazio. Inoltre, se alcuni controller dell'infrastruttura sono in esecuzione con la CPU a oltre il 65% - potenzialmente mettendo il cluster a rischio in caso di failover - ONTAP Essentials li mostra come controller "hot".

I grafici informativi consentono di analizzare le performance nel tempo e i guasti dell'utilizzo della capacità.

Ciascuno di questi grafici o punti dati può essere utilizzato come punto di partenza per l'esplorazione o l'analisi.

Nota: Un numero "giorni per il pieno" di "0" (zero) indica che i giorni per il pieno sono stimati a più di 90 giorni. In altre parole, i tuoi sistemi non rischiano di esaurire lo spazio a breve.

Protezione dei dati

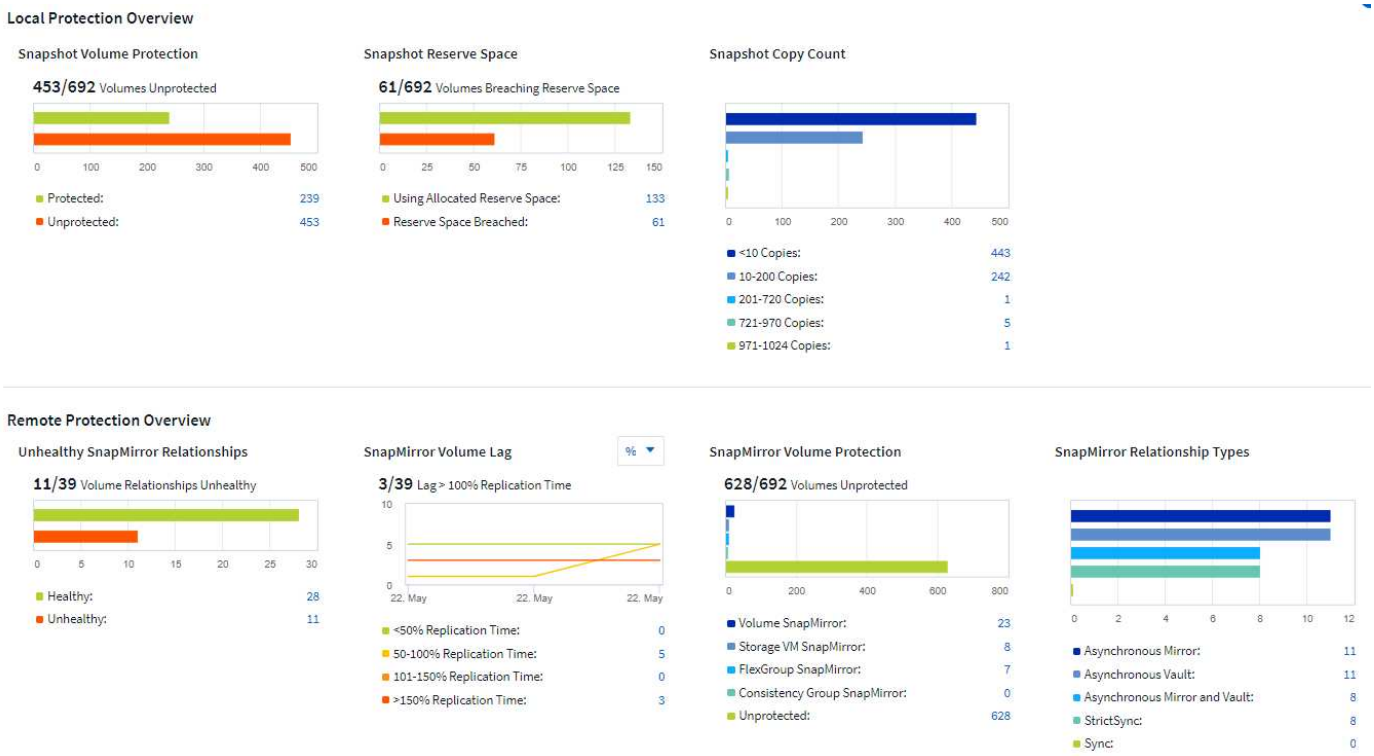
La pagina **Data Protection** mostra lo stato dei volumi protetti da **Snapshot Copies** o **SnapMirror policy**.

Nella sezione *Local Protection Overview*, i grafici forniscono le seguenti informazioni per i volumi protetti dalle copie Snapshot:

- Il numero di volumi protetti da copie Snapshot e non protetti.
- Il numero di volumi che utilizzano o superano lo spazio riservato per le copie Snapshot.
- Il numero di volumi in intervalli specifici del numero di copie Snapshot (ad esempio, meno di 10 copie, da 10 a 200, ecc.).

Nella sezione *Panoramica sulla protezione remota*, i grafici forniscono informazioni relative ai volumi protetti dalle policy di SnapMirror:

- Il numero di relazioni SnapMirror sane e non funzionanti.
- Il numero di relazioni SnapMirror che hanno riscontrato un ritardo RPO (Recovery Point Objective) in base allo stato di ritardo.
- Il numero di relazioni protette dai tipi di protezione dei volumi SnapMirror, ad esempio le relazioni di Volume SnapMirror, le relazioni di SVMDR, le relazioni di FlexGroup SnapMirror, le relazioni di gruppo di coerenza di continuità aziendale (SMBC) di SnapMirror e i volumi non protetti.
- Il numero di relazioni protette dai tipi di relazione SnapMirror come Asynchronous Mirror, Asynchronous Vault, Asynchronous MirrorVault, StrictSync e Sync.



La griglia *Clusters* nella parte inferiore della pagina fornisce i dettagli relativi a quanto segue:

- Volumi non protetti da snapshot.
- Volumi che violano lo spazio di riserva snapshot.
- I volumi non protetti dalle policy di snapmirror e le relazioni di snapmirror subiscono ritardi.
- Relazioni SnapMirror non integre.

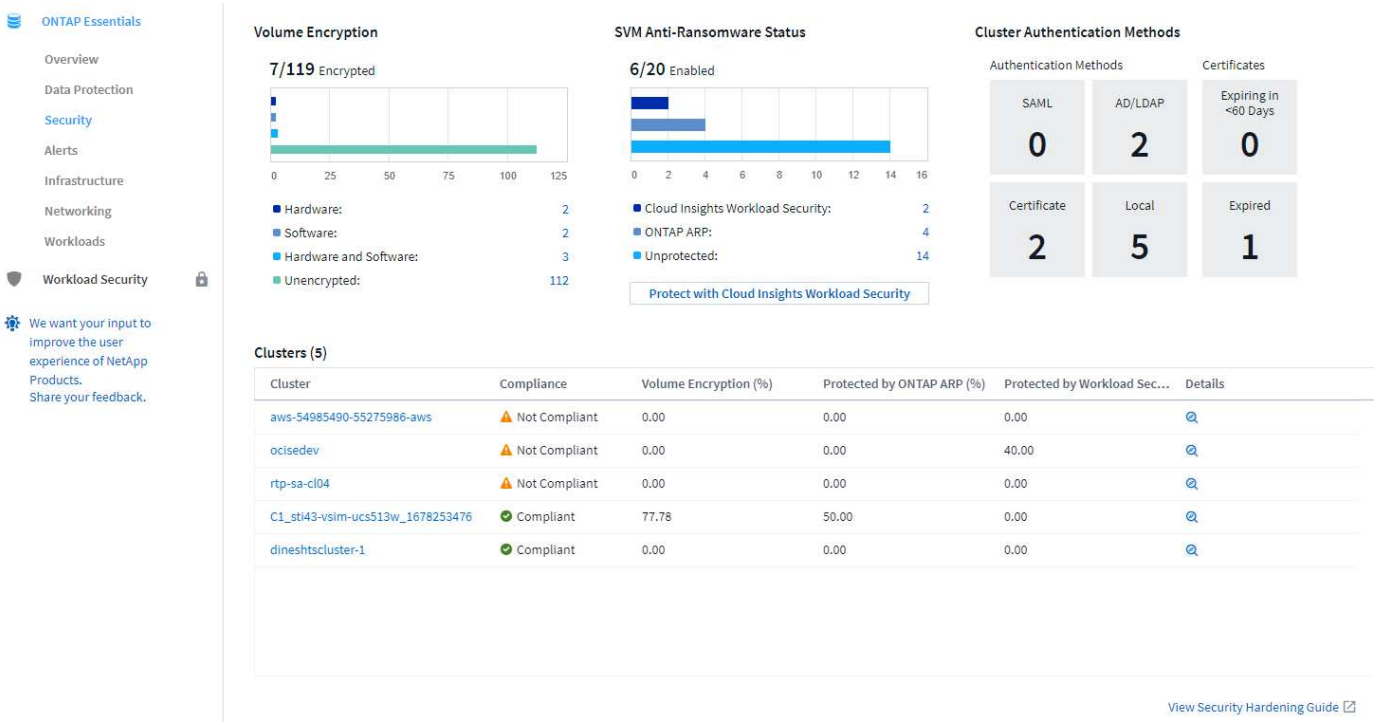
Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsim12	7	4	7	0	3
C1_sti11-vsim-ucs574m_168327	0	0	0	0	0
C1_sti43-vsim-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

Sicurezza

La dashboard di sicurezza offre una vista istantanea della situazione di sicurezza corrente, mostrando grafici per la crittografia dei volumi hardware e software, lo stato anti-ransomware e i metodi di autenticazione del cluster. I criteri di sicurezza vengono valutati in base ai consigli definiti in **"Guida al rafforzamento della sicurezza di NetApp per ONTAP 9"**.

Selezionare uno dei conteggi di crittografia o anti-ransomware da inserire nell'ambiente.



La dashboard di sicurezza di base di ONTAP monitora il tuo ambiente per determinare lo stato di conformità del cluster. Fare riferimento a. "Categorie di conformità del cluster" per saperne di più. ONTAP Essentials utilizza i seguenti monitor per determinare la conformità:

Nome monitor	Nome attributo (visualizzato in Cluster Details)	Valore conforme all'attributo
Modalità FIPS disattivata	Modalità FIPS	Attivato
Crittografia non sicura del cluster per SSH	Impostazioni SSH sicure	Sì
Protocollo Telnet attivato	Telnet	Disattivato
Shell remota attivata	Shell remota	Disattivato
Default Local Admin User Enabled (utente amministratore locale predefinito attivato	Admin User predefinito	Disattivato
Password hash MD5	MD5 in uso	No
Comunicazione peer cluster non crittografata	Peering dei cluster	Crittografato/Nessuna peer
Trasporto HTTPS AutoSupport disattivato	AutoSupport con HTTPS	Sì
Nessun server NTP configurato	Network Time Protocol	Configurato
Il numero di server NTP è basso	Network Time Protocol	Configurato
Banner di accesso cluster disattivato	Banner di accesso	Attivato
Inoltro log non crittografato	Inoltro log crittografato	Sì

Si noti che se un monitor di cui sopra è disattivato, i dettagli del cluster mostreranno il valore come 'non selezionato' per l'attributo di conformità di sicurezza corrispondente.

Cluster	Compliance
aws-54985490-55275986-aws	Not Compliant
ocisedev	Not Compliant
rtp-sa-cl04	Not Compliant
C1_sti43-vsim-ucs513w_1678253476	Compliant
dineshtscluster-1	Compliant

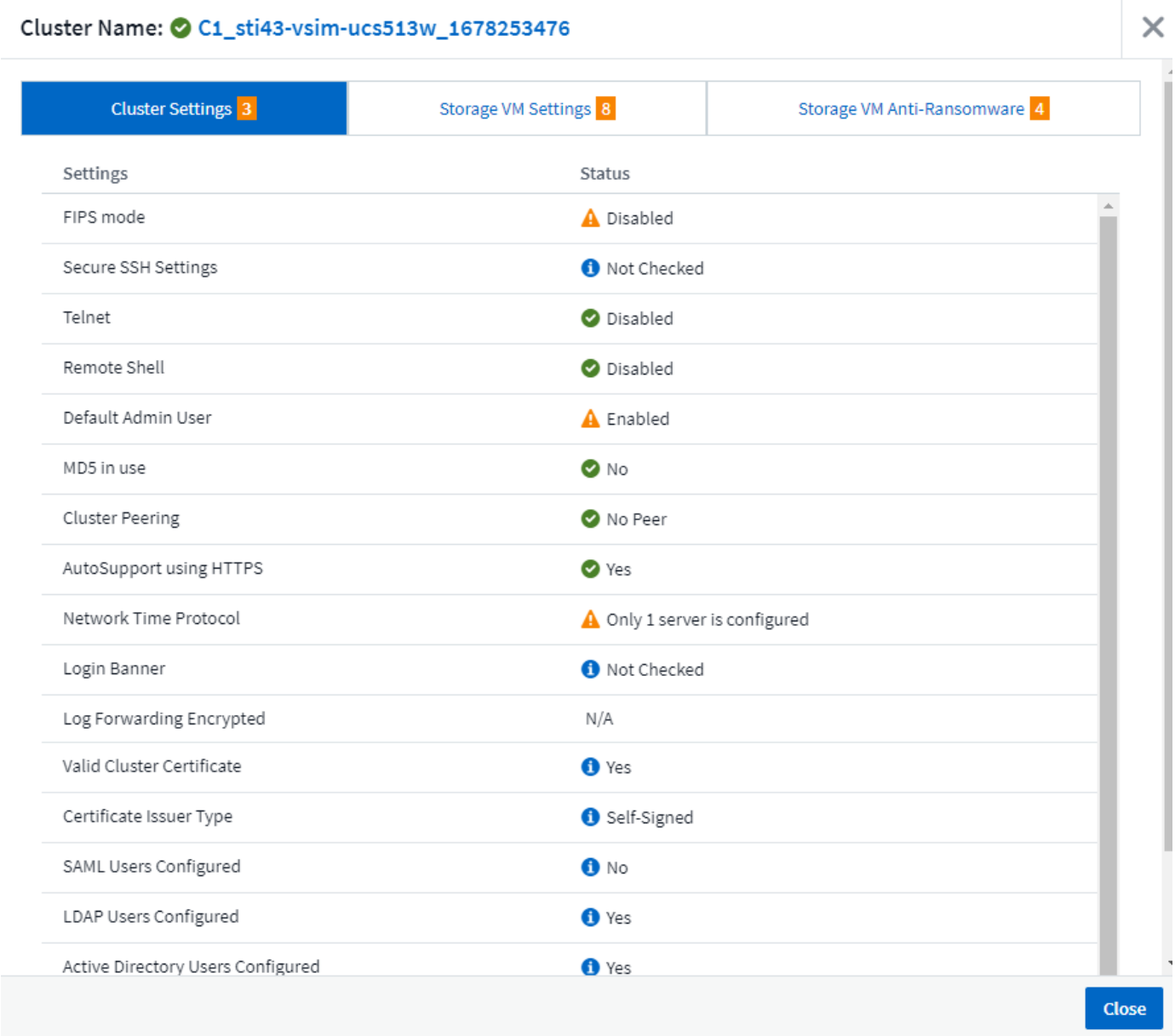
Per le SVM, la dashboard di sicurezza esamina i seguenti monitor:

Nome monitor	Nome attributo (visualizzato in Storage VM Settings)	Valore conforme all'attributo
Crittografia non sicura delle VM di storage per SSH	Impostazioni SSH sicure	Sì

Nome monitor	Nome attributo (visualizzato in Storage VM Settings)	Valore conforme all'attributo
Banner di login Storage VM disattivato	Banner di accesso	Attivato
Log di audit delle VM di storage disattivato	Log di audit	Attivato

Nell'elenco dei cluster, selezionare *View Details* (Visualizza dettagli) per ciascun cluster per aprire un pannello a scorrimento che mostra le impostazioni correnti di *Cluster, Storage VM* o *Anti-ransomware*.

I dettagli del cluster includono stato della connessione, informazioni sul certificato e molto altro ancora:



I dettagli delle VM di storage mostrano le informazioni di audit e SSH:

Cluster Name: rtp-sa-cl04

Cluster Settings 2 | Storage VM Settings 7 | Storage VM Anti-Ransomware 8

Storage VM	Login Banner	Audit Log	Secure SSH Settings
mattsvm07_04	Disabled	N/A	Yes
sf-svmdr1	Disabled	N/A	Yes
ss_balajicifs	Disabled	N/A	Yes
ss_balajicifs_1_encrypted	Disabled	N/A	Yes
test1	Enabled	Disabled	Yes
test2	Disabled	N/A	Yes
test3	Disabled	N/A	Yes
cl04_data_svm1	Enabled	Enabled	Yes

I dettagli anti-ransomware mostrano se una VM di storage è protetta dalla protezione anti-ransomware di ONTAP o dalla sicurezza del carico di lavoro Cloud Insights. La colonna ARP ONTAP visualizza lo stato corrente della protezione anti-ransomware integrata di ONTAP, configurata sul sistema ONTAP. La sicurezza del carico di lavoro Cloud Insights può essere attivata selezionando "Proteggi" nella colonna.

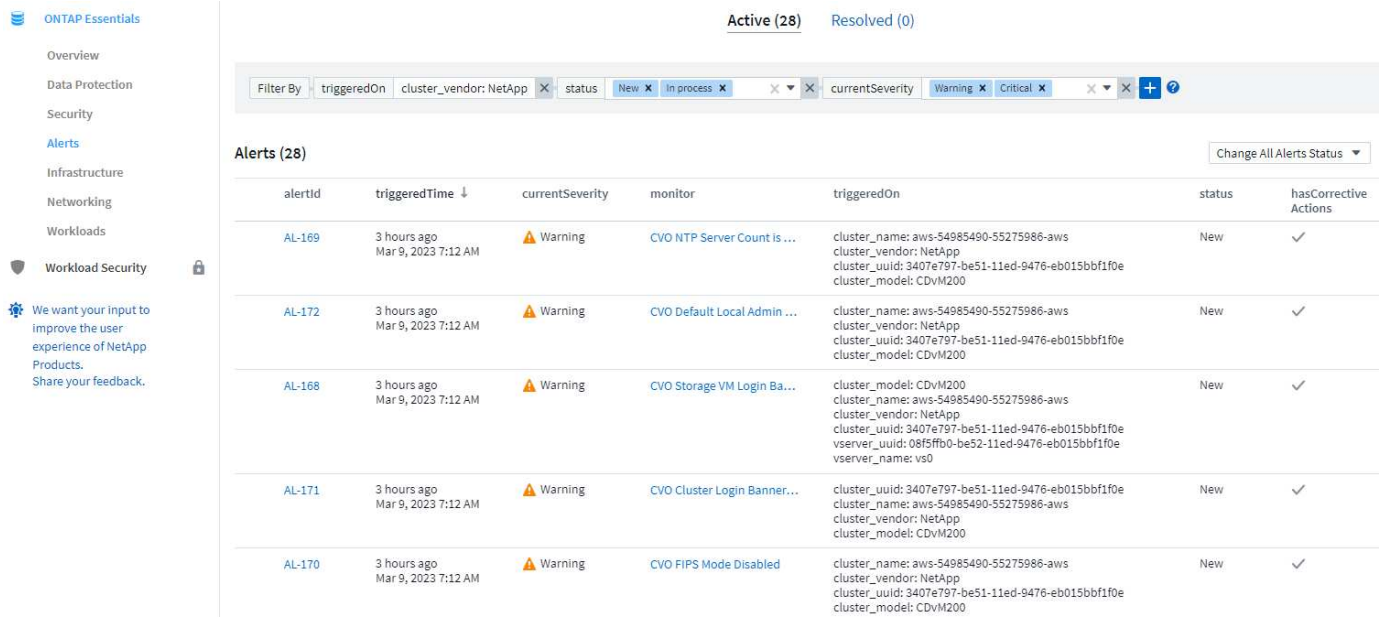
Cluster Name: ocisedev

Cluster Settings 7 | Storage VM Settings 5 | Storage VM Anti-Ransomware 3

Storage VM	Protected by Workload Security	Protected by ONTAP ARP
CloudComplianceSVM	Protect	N/A
t1appSVM01	Protect	N/A
tawny_mirror	Protect	N/A
demoGroupShares	Protected	N/A
demoGroupShares2	Protected	N/A

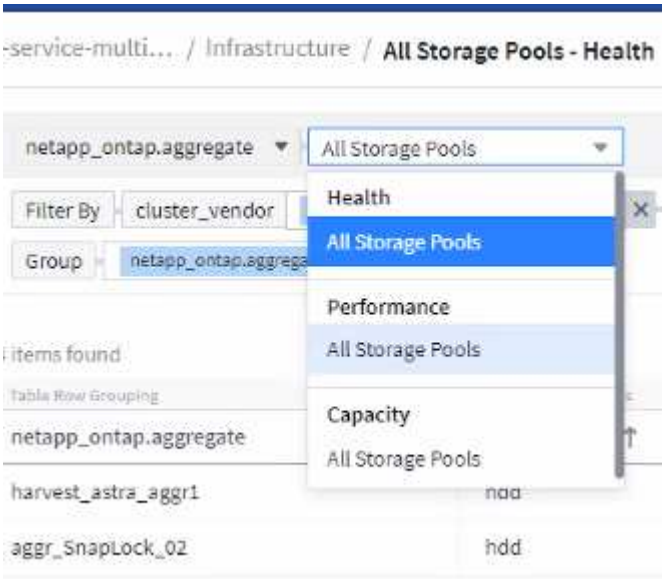
Avvisi

Qui è possibile visualizzare gli avvisi attivi nel proprio ambiente e analizzare rapidamente i potenziali problemi. Selezionare la scheda *Resolved* per visualizzare gli avvisi risolti.

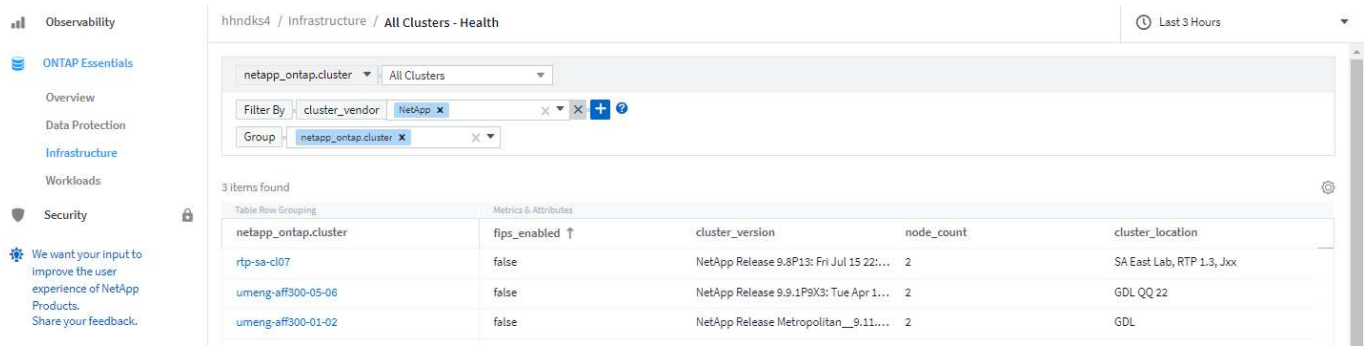


Infrastruttura

La pagina ONTAP Essentials **infrastruttura** offre una panoramica dello stato e delle performance del cluster, utilizzando query predefinite (ancora ulteriormente personalizzabili) su tutti gli oggetti ONTAP di base. Selezionare il tipo di oggetto che si desidera esplorare (cluster, pool di storage, ecc.) e scegliere se visualizzare le informazioni sullo stato o sulle performance. Imposta i filtri per approfondire i singoli sistemi.

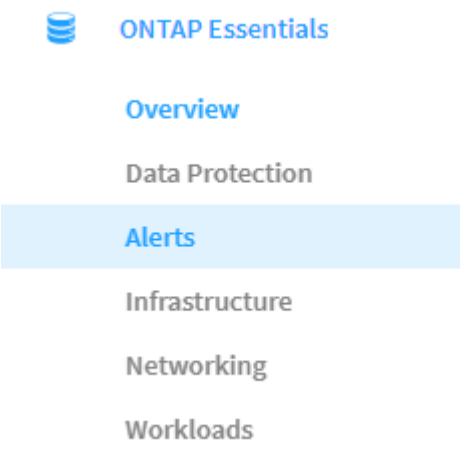


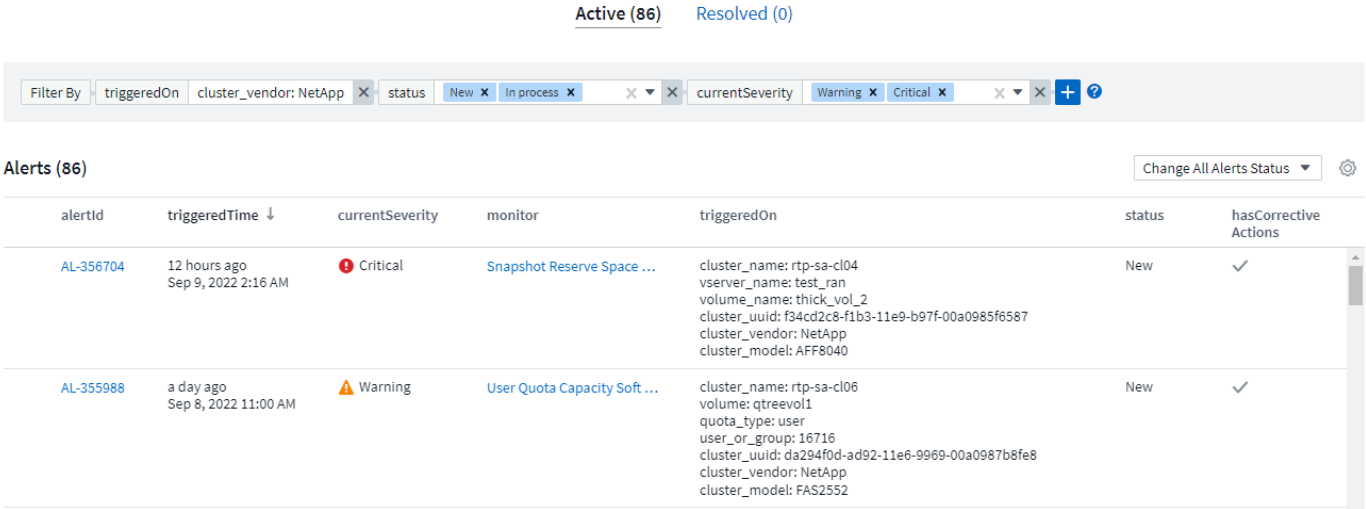
Pagina dell'infrastruttura che mostra lo stato del cluster:



Networking

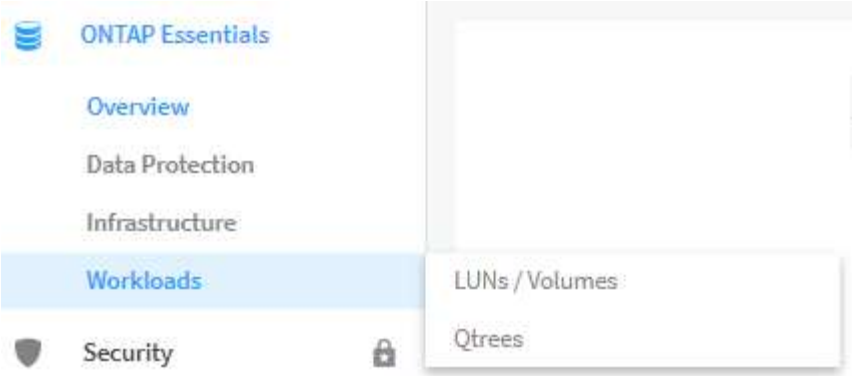
Il networking di base di ONTAP ti offre una panoramica dell'infrastruttura FC, FC NVME, Ethernet e iSCSI. In queste pagine è possibile esplorare le porte dei cluster e dei relativi nodi.

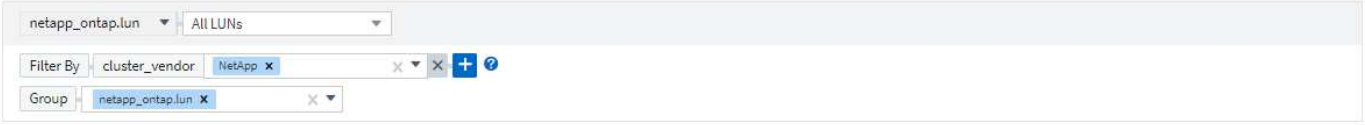




Carichi di lavoro

Visualizza ed esplora i carichi di lavoro su LUN/volumi, condivisioni NFS o SMB o Qtree nel tuo ambiente.





13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late... ↑	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840....	0.00	ste	vs_test	umeng_aff300...	u
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376....	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	u
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	u
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	u
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368....	0.00	kubebug1	vs_test	umeng_aff300...	u
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	u
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	u
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun_...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	u
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	u

Lavorare con le query

Risorse utilizzate nelle query

Le query consentono di monitorare e risolvere i problemi della rete ricercando le risorse e le metriche dell'ambiente a un livello granulare in base a criteri selezionati dall'utente (ad esempio, annotazioni).

Si noti che le regole di annotazione, che assegnano automaticamente le annotazioni alle risorse, *richiedono* una query.

È possibile eseguire query sulle risorse di inventario fisiche o virtuali (e sulle relative metriche) nel proprio ambiente o sulle metriche fornite con l'integrazione, ad esempio Kubernetes o dati avanzati di ONTAP.

Risorse di inventario

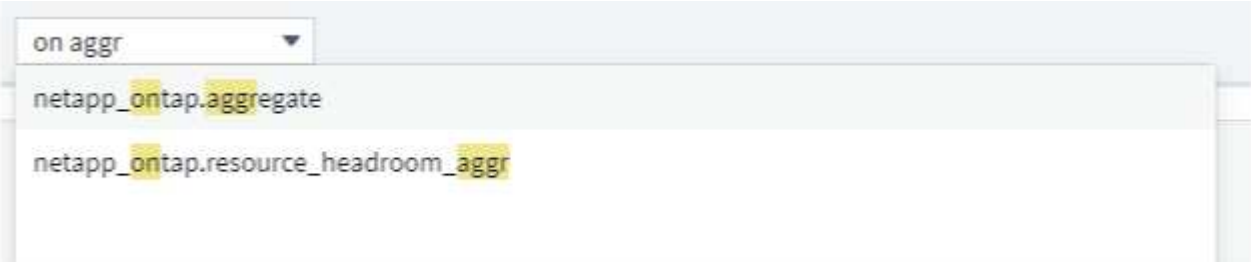
I seguenti tipi di risorse possono essere utilizzati nelle query, nei widget della dashboard e nelle landing page personalizzate delle risorse. I campi e i contatori disponibili per i filtri, le espressioni e la visualizzazione variano in base al tipo di risorsa. Non tutte le risorse possono essere utilizzate 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
- SVM (Storage Virtual Machine)
- Switch
- Nastro
- VMDK
- Macchina virtuale

- Volume
- Zona
- Membro di zona

Metriche di integrazione

Oltre a eseguire query per le risorse di inventario e le relative metriche di performance, è possibile eseguire query anche per le metriche **dati di integrazione**, come quelle generate da Kubernetes o Docker, o fornite con metriche avanzate di ONTAP.



Creazione di query

Le query consentono di cercare le risorse nell'ambiente a un livello granulare, consentendo di filtrare i dati desiderati e di ordinare i risultati in base alle proprie esigenze.

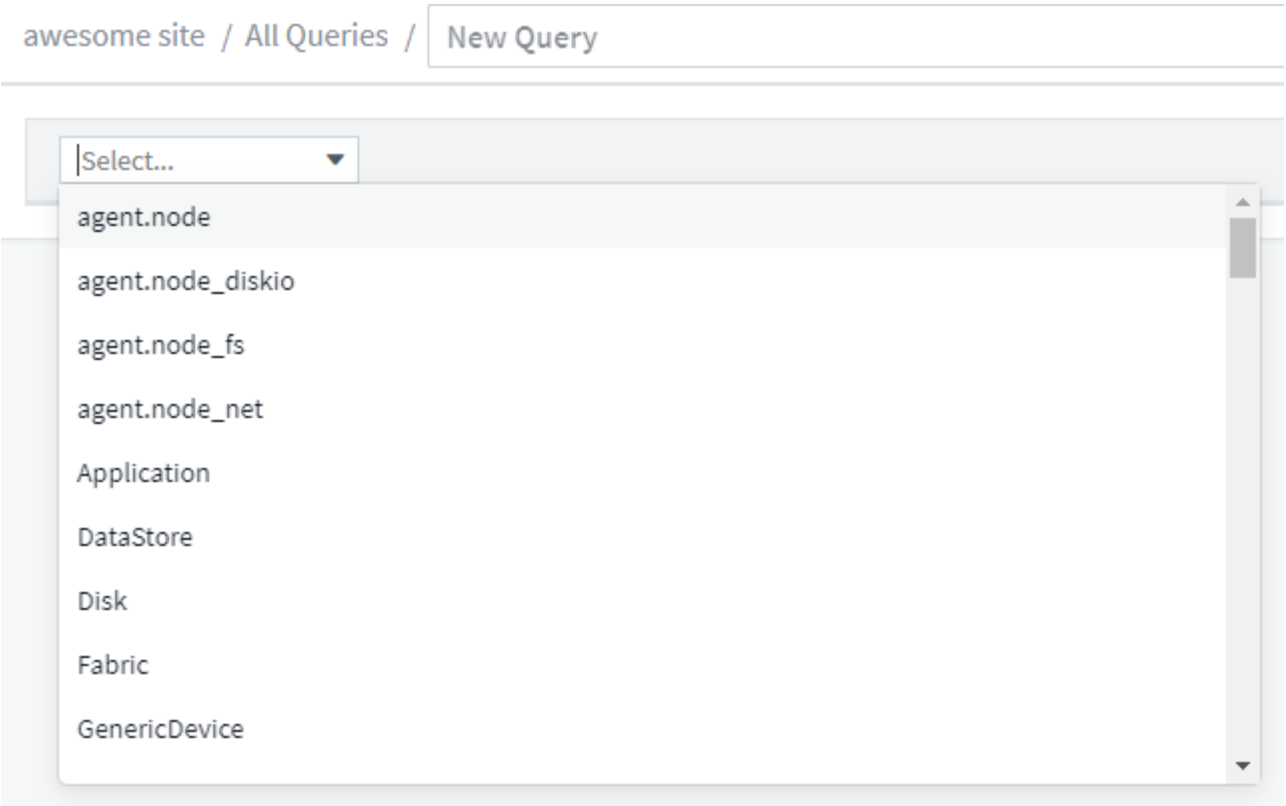
Ad esempio, è possibile creare una query per *volumi*, aggiungere un filtro per trovare *storage* specifici associati ai volumi selezionati, aggiungere un altro filtro per trovare una particolare *annotazione*, ad esempio "Tier 1" sugli storage selezionati, Infine, Aggiungi un altro filtro per trovare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

Nota: Quando viene aggiunto un nuovo data collector che acquisisce le risorse o vengono effettuate annotazioni o assegnazioni di applicazioni, è possibile eseguire query per le nuove risorse, annotazioni o applicazioni solo dopo che le query sono state indicizzate. L'indicizzazione viene eseguita a intervalli regolari pianificati o durante determinati eventi, ad esempio l'esecuzione di regole di annotazione.

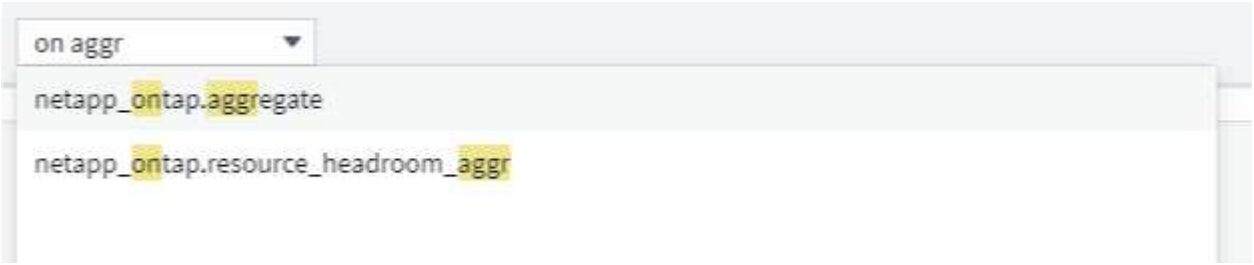
Creare una query è molto semplice:

1. Selezionare **Query > *+Nuova query**.
2. Dalla schermata "Select…" (Seleziona) selezionare il tipo di oggetto per il quale si desidera eseguire la query. È possibile scorrere l'elenco o iniziare a digitare per trovare più rapidamente ciò che si sta cercando.

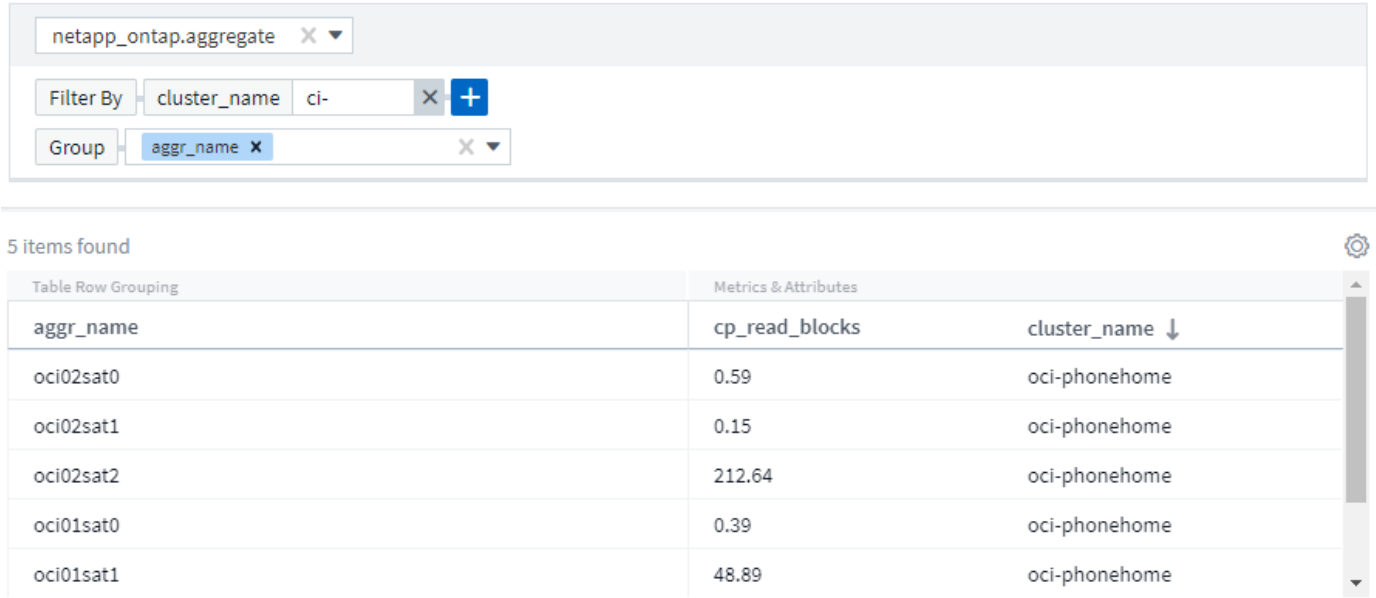
Elenco a scorrimento:



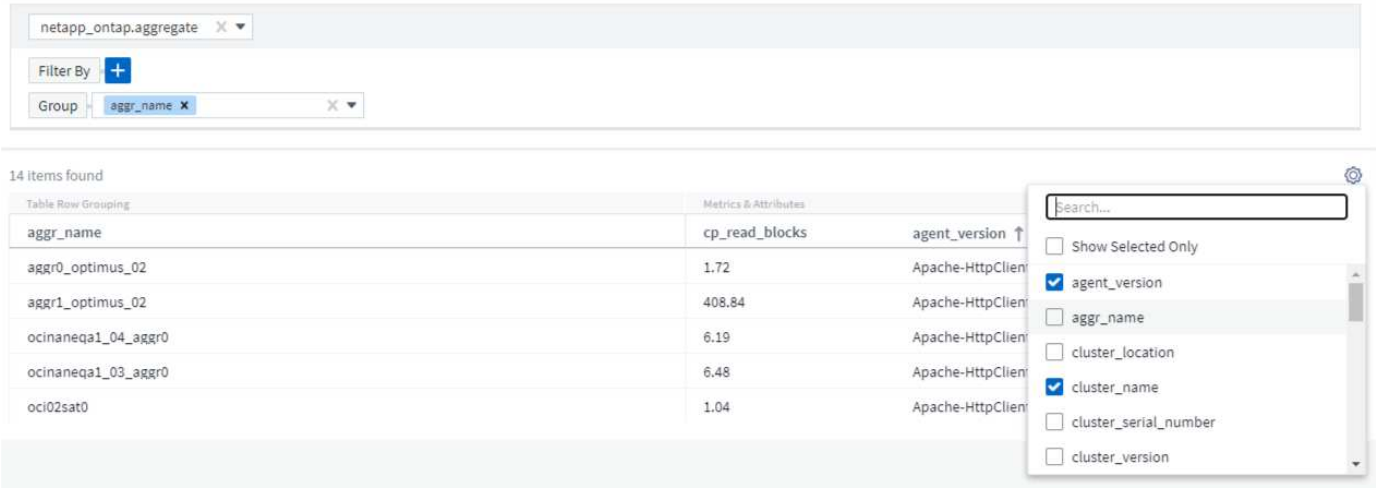
Tipo di ricerca:



È possibile aggiungere filtri per restringere ulteriormente la query facendo clic sul pulsante **+** nel campo **Filtra per**. Raggruppare le righe per oggetto o attributo. Quando si lavora con i dati di integrazione (Kubernetes, metriche avanzate di ONTAP, ecc.), è possibile raggruppare in base a più attributi, se necessario.



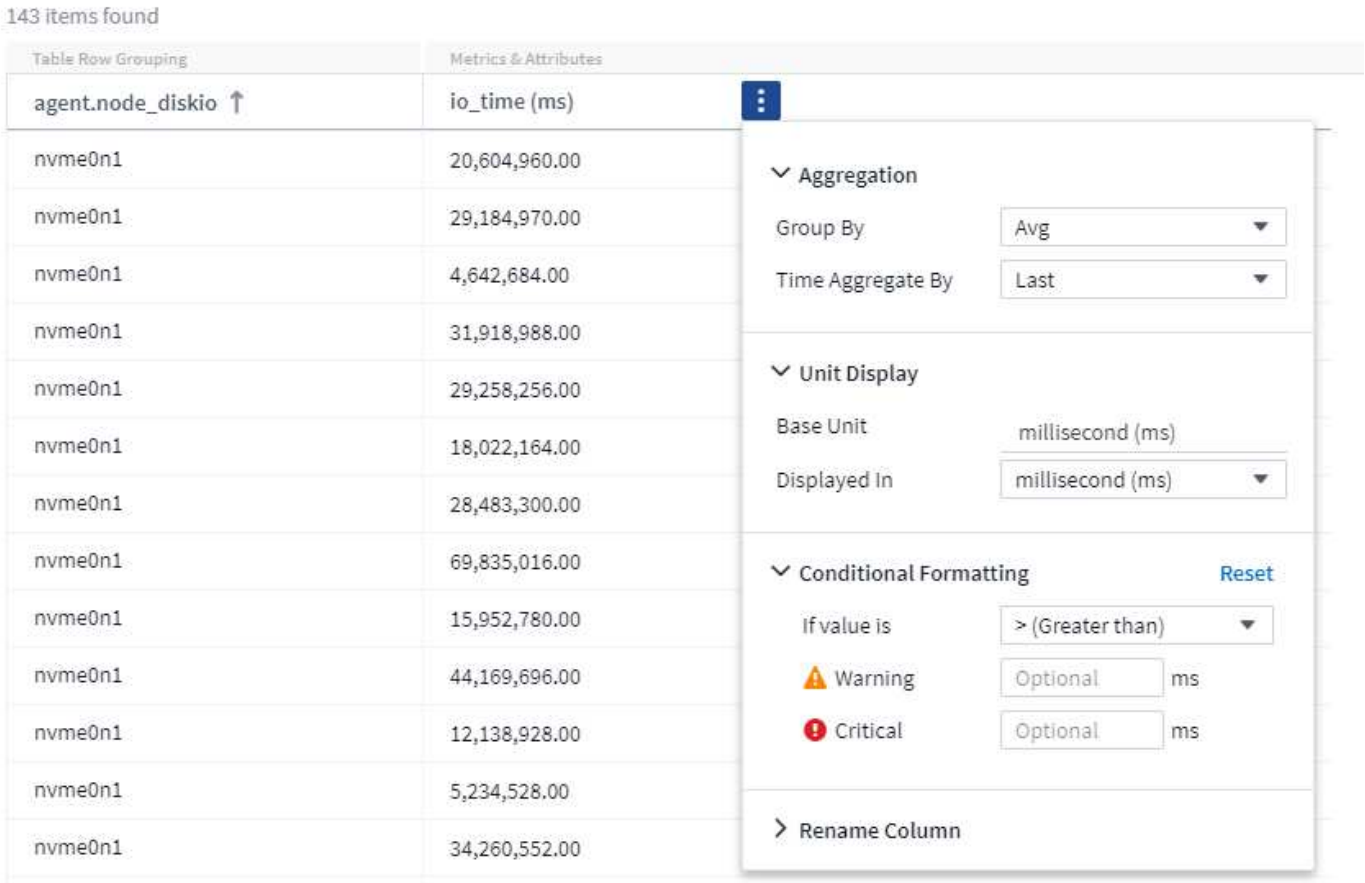
L'elenco dei risultati della query mostra una serie di colonne predefinite, a seconda del tipo di oggetto ricercato. Per aggiungere, rimuovere o modificare le colonne, fare clic sull'icona a forma di ingranaggio a destra della tabella. Le colonne disponibili sono diverse in base al tipo di risorsa/metrica.



Scegliere aggregazione, unità, Formattazione condizionale

Aggregazione e unità

Per le colonne "valore", è possibile perfezionare ulteriormente i risultati della query scegliendo la modalità di aggregazione dei valori visualizzati e selezionando le unità in cui tali valori vengono visualizzati. Queste opzioni si trovano selezionando il menu "tre punti" nell'angolo superiore di una colonna.



Unità

È possibile selezionare le unità in cui visualizzare i valori. Ad esempio, se la colonna selezionata mostra la capacità raw e i valori sono visualizzati in GiB, ma si preferisce visualizzarli come TIB, selezionare TIB dall'elenco a discesa Unit Display (visualizzazione unità).

Aggregazione

Con lo stesso token, se i valori mostrati sono aggregati dai dati sottostanti come "medi", Tuttavia, si preferisce visualizzare la somma di tutti i valori, selezionare "somma" dal menu a discesa *Raggruppa per* (se si desidera che i valori raggruppati mostrino le somme) o dal menu a discesa *aggregato di tempo per* (se si desidera che i valori delle righe mostrino le somme dei dati sottostanti).

Puoi scegliere di aggregare i punti dati raggruppati per *Avg, Max, min o Sum*.

È possibile aggregare i dati delle singole righe in base a *Average, Last data point Acquired, Maximum, Minimum o Sum*.

Formattazione condizionale

La formattazione condizionale consente di evidenziare le soglie a livello di avviso e critico nell'elenco dei risultati della query, offrendo visibilità istantanea agli outlier e ai punti dati eccezionali.

La formattazione condizionale viene impostata separatamente per ciascuna colonna. Ad esempio, è possibile scegliere un set di soglie per una colonna di capacità e un altro set per una colonna di throughput.

Rinominare la colonna

La ridenominazione di una colonna modifica il nome visualizzato nell'elenco risultati query. Il nome della nuova colonna viene visualizzato anche nel file risultante se si esporta l'elenco di query in formato .CSV.

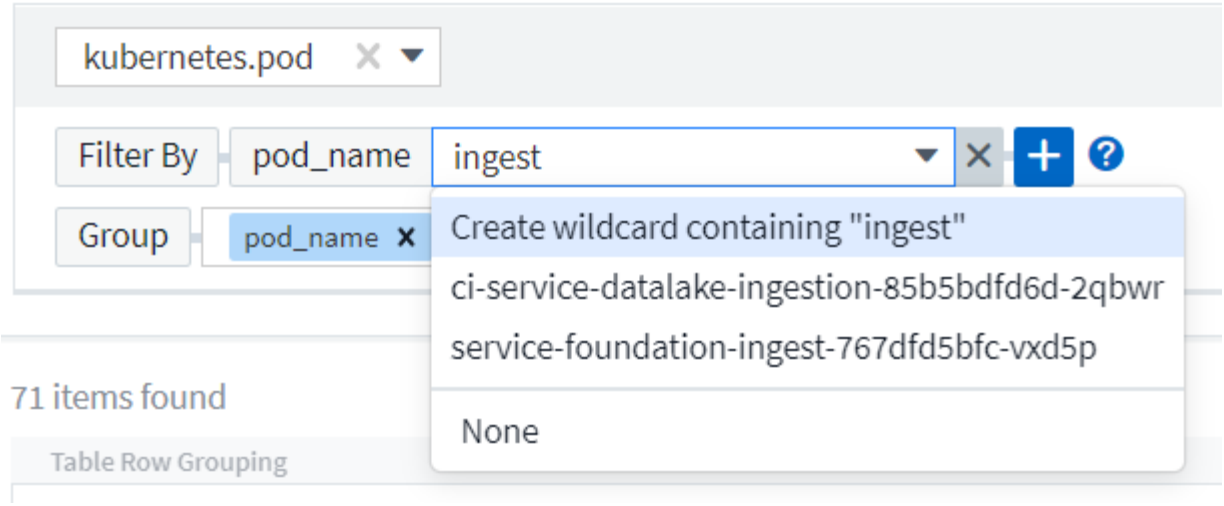
Salva

Dopo aver configurato la query per visualizzare i risultati desiderati, fare clic sul pulsante **Save** (Salva) per salvare la query per un utilizzo futuro. Assegna un nome significativo e unico.

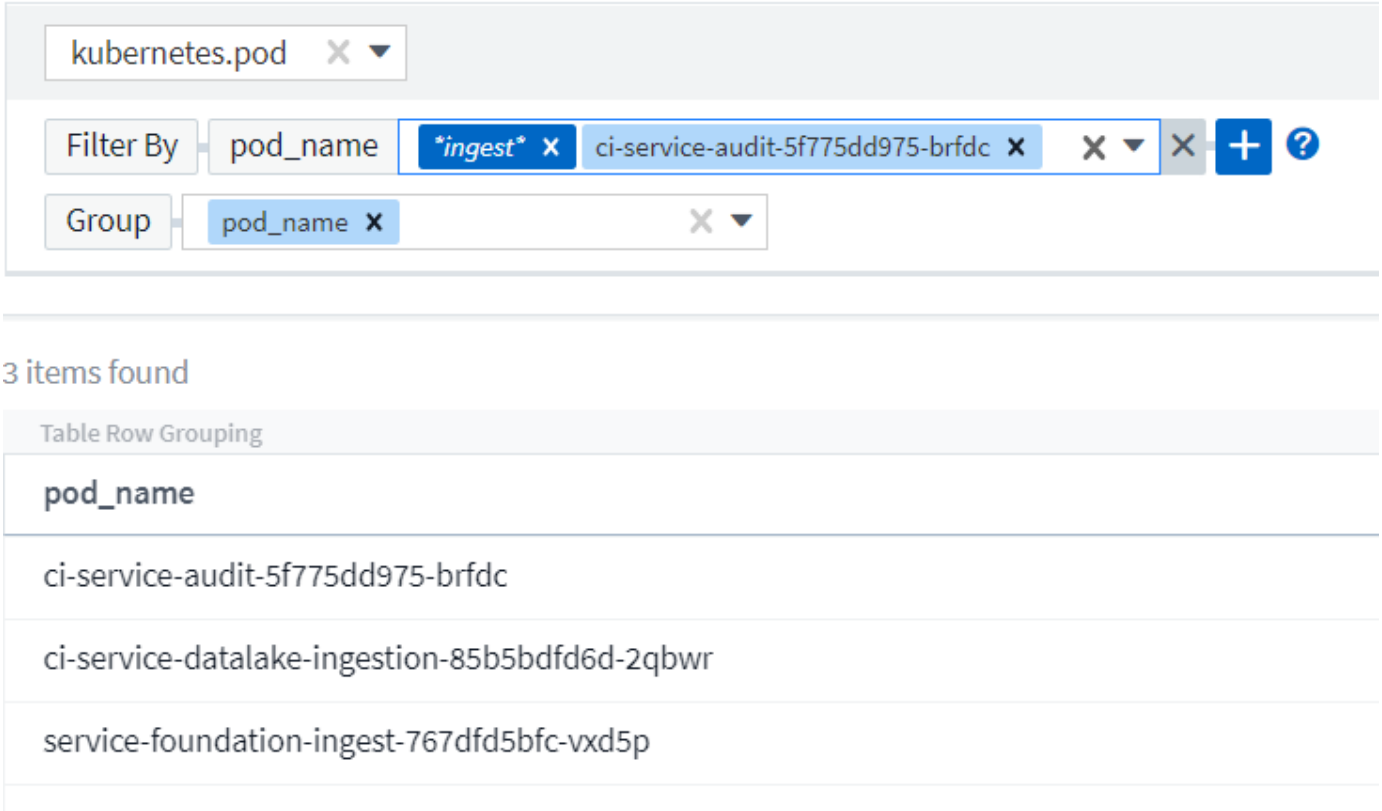
Ulteriori informazioni sul filtraggio

Caratteri jolly ed espressioni

Quando si filtrano valori di testo o di elenco nelle query o nei widget della dashboard, quando si inizia a digitare viene visualizzata l'opzione per creare un filtro * con caratteri jolly* in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione con caratteri jolly. È inoltre possibile creare **espressioni** utilizzando NOR o OPPURE, oppure selezionare l'opzione "None" (Nessuno) per filtrare i valori nulli nel campo.



I filtri basati su caratteri jolly o espressioni (ad esempio, NO, O "None", ecc.) vengono visualizzati in blu scuro nel campo del filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in blu chiaro.



Si noti che i caratteri jolly e il filtraggio delle espressioni funzionano con testo o elenchi, ma non con valori numerici, date o booleani.

Raffinazione dei filtri

Per perfezionare il filtro, utilizzare quanto segue:

Filtro	Che cosa fa	Esempio	Risultato

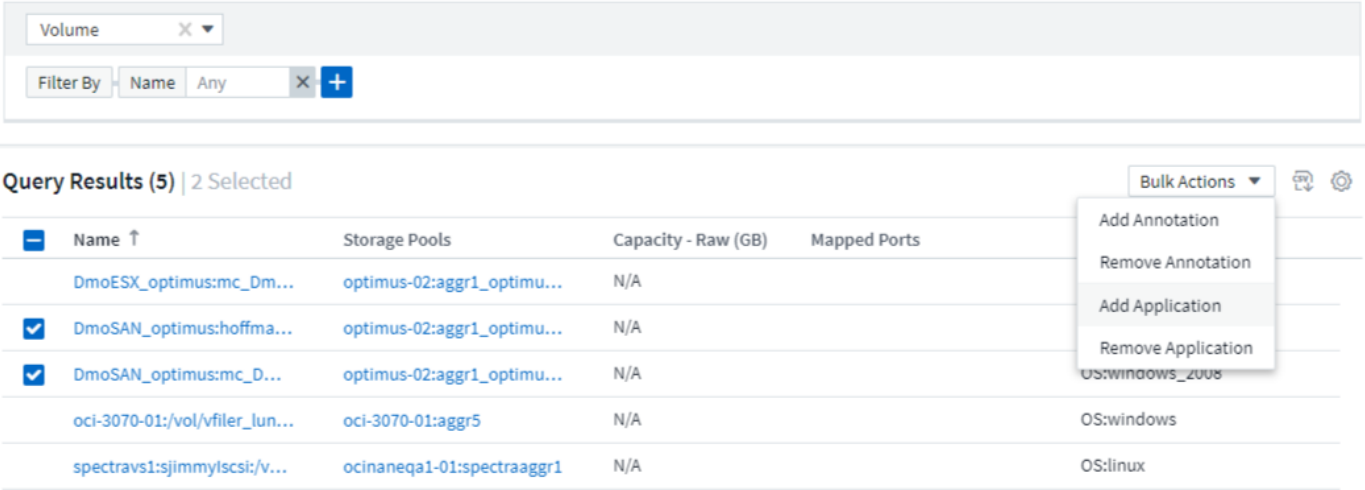
* (Asterisco)	consente di cercare tutto	vol*rhel	restituisce tutte le risorse che iniziano con "vol" e terminano con "rhel"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	BOS-PRD??-S12	Restituisce BOS-PRD***12*** -S12, BOS-PRD***23***-S12 e così via
OPPURE	consente di specificare più entità	FAS2240, CX600 O FAS3270	Restituisce FAS2440, CX600 o FAS3270
NO	consente di escludere il testo dai risultati della ricerca	NON EMC*	Restituisce tutto ciò che non inizia con "EMC"
Nessuno	Ricerca i valori NULL in tutti i campi	*Nessuno*	restituisce risultati in cui il campo di destinazione è vuoto
Non *	Cerca i valori NULL nei campi *text-only*	Non *	restituisce risultati in cui il campo di destinazione è vuoto

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 "*" restituirà risultati che sono un asterisco letterale; in questo caso, l'asterisco non verrà trattato come carattere jolly. Gli operatori O e NON verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

Cosa fare ora che si ottengono i risultati delle query?

La funzione di query consente di aggiungere annotazioni o assegnare applicazioni alle risorse in modo semplice. Nota: È possibile assegnare solo applicazioni o annotazioni alle risorse di inventario (disco, storage, ecc.). Le metriche di integrazione non possono assumere le assegnazioni di annotazioni o applicazioni.

Per assegnare un'annotazione o un'applicazione alle risorse risultanti dalla query, selezionare le risorse utilizzando la colonna della casella di controllo a sinistra della tabella dei risultati, quindi fare clic sul pulsante **azioni in blocco** a destra. Scegliere l'azione desiderata da applicare alle risorse selezionate.



Le regole di annotazione richiedono una query

Se si sta configurando "Regole di annotazione", ogni regola deve disporre di una query sottostante per funzionare. Tuttavia, come hai visto in precedenza, le query possono essere estese o ristrette in base alle tue esigenze.

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 al tenant Cloud Insights.
2. Fare clic su **Query** e selezionare **Mostra tutte le query**. È possibile modificare la modalità di visualizzazione delle query effettuando una delle seguenti operazioni:
3. È possibile inserire del testo nella casella di filtro per cercare e visualizzare query specifiche.
4. 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.
5. 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.
6. 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 Cloud Insights esegue automaticamente il polling dei data collettori. 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 qualsiasi query in un file .CSV, che consente di analizzare i dati o importarli in un'altra applicazione.

Fasi

1. Accedere a Cloud Insights.
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 file .CSV.

> L'esportazione in .CSV è disponibile anche nel menu "Three dots" (tre punti) nei widget della tabella della dashboard e nella maggior parte delle tabelle delle landing page.

I dati esportati rifletteranno il filtro corrente, le colonne e i nomi delle colonne visualizzati.

Nota: 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 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:

1. Aprire un nuovo foglio in Excel.
2. Nella scheda "dati", scegliere "da testo".
3. Individuare il file .CSV desiderato e fare clic su "Import" (Importa).
4. Nella procedura guidata di importazione, scegliere "delimitato" e fare clic su Avanti.
5. Scegliere "virgola" per il delimitatore e fare clic su Avanti.
6. Selezionare le colonne desiderate e scegliere "testo" per il formato dei dati della colonna.
7. Fare clic su fine.

   Gli oggetti devono essere visualizzati in Excel nel formato corretto.

Modifica o eliminazione di una 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.

Modifica di una query

Fasi

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

   Viene visualizzata la pagina Query.

2. Fare clic sul nome della query
3. Per aggiungere un criterio alla query, fare clic su e selezionare un criterio dall'elenco.
4. Per rimuovere un filtro dalla query, fare clic sulla * X* accanto al filtro da rimuovere.

Una volta apportate tutte le modifiche necessarie, effettuare una delle seguenti operazioni:

- Fare clic sul pulsante **Save** (Salva) per salvare la query con il nome utilizzato inizialmente.
- Fare clic sul menu a discesa accanto al pulsante **Save** (Salva) e selezionare **Save As** (Salva con nome) per salvare la query con un altro nome. Questa operazione non sovrascrive la query originale.
- Fare clic sul menu a discesa accanto al pulsante **Save** (Salva) e selezionare **Rename** (Rinomina) per modificare il nome della query utilizzato inizialmente. Questa operazione sovrascrive la query originale.
- Fare clic sul menu a discesa accanto al pulsante **Save** (Salva) e selezionare **Discard changes** (Annulla modifiche) per ripristinare le ultime modifiche salvate.

Eliminazione di una query

Per eliminare una query, fare clic su **Query** e selezionare **Mostra tutte le query**, quindi eseguire una delle seguenti operazioni:

1. Fare clic sul menu a tre punti a destra della query e fare clic su **Delete** (Elimina).
2. Fare clic sul nome della query e selezionare **Delete** (Elimina) dal menu a discesa **Save** (Salva).

Assegnazione di più applicazioni o rimozione di più applicazioni dalle risorse

È possibile assegnare più "applicazioni" per o rimuovere più applicazioni dalle risorse utilizzando una query invece di doverle assegnare o rimuovere manualmente.

> È possibile utilizzare questa procedura per aggiungere o rimuovere "annotazioni" allo stesso modo.

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 sulla casella di controllo in alto per selezionare tutto.

   Il Bulk Actions viene visualizzato il pulsante.

4. Per aggiungere un'applicazione alle risorse selezionate, fare clic su Bulk Actions E selezionare **Aggiungi applicazione**.
5. Selezionare una o più applicazioni.

   È possibile selezionare più applicazioni per host, volumi interni, qtree e macchine virtuali; tuttavia, è possibile selezionare una sola applicazione per un volume o una condivisione.

6. Fare clic su **Save** (Salva).
7. Per rimuovere un'applicazione assegnata alle risorse, fare clic su Bulk Actions E selezionare **Rimuovi applicazione**.
8. Selezionare l'applicazione o le applicazioni che si desidera rimuovere.
9. 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.

Dopo aver fatto clic su *Salva* in un'aggiunta in blocco o su *Rimuovi* in un'azione di eliminazione in blocco,

Cloud Insights informa che l'azione richiederà del tempo. È possibile ignorare questo messaggio; l'azione continuerà in background.

> Per gli ambienti con grandi quantità di risorse correlate, l'ereditarietà delle assegnazioni delle applicazioni a tali risorse potrebbe richiedere diversi minuti. Attendere più tempo per l'ereditarietà se si dispone di molte risorse correlate.

Copia dei valori della tabella

È possibile copiare i valori nelle tabelle negli Appunti 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 negli Appunti.

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, passare il mouse sul campo e fare clic sull'icona degli Appunti a quanto pare. Il valore viene copiato negli Appunti per essere utilizzato nei campi di ricerca o in altre applicazioni.

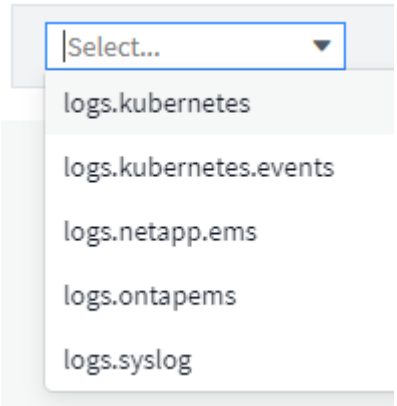
   Questo metodo consente di copiare solo i valori che sono collegamenti alle risorse. Solo i campi che includono valori singoli (ad esempio non elenchi) hanno l'icona di copia.

Esplora log

Esplora log di Cloud Insights è un potente strumento per eseguire query sui log di sistema. Oltre a fornire assistenza per le analisi, è possibile salvare una query di log in un monitor per fornire avvisi quando vengono attivati i trigger di log specifici.

Per iniziare a esplorare i registri, fare clic su **Log queries > +New Log Query**.

Selezionare un registro disponibile dall'elenco.

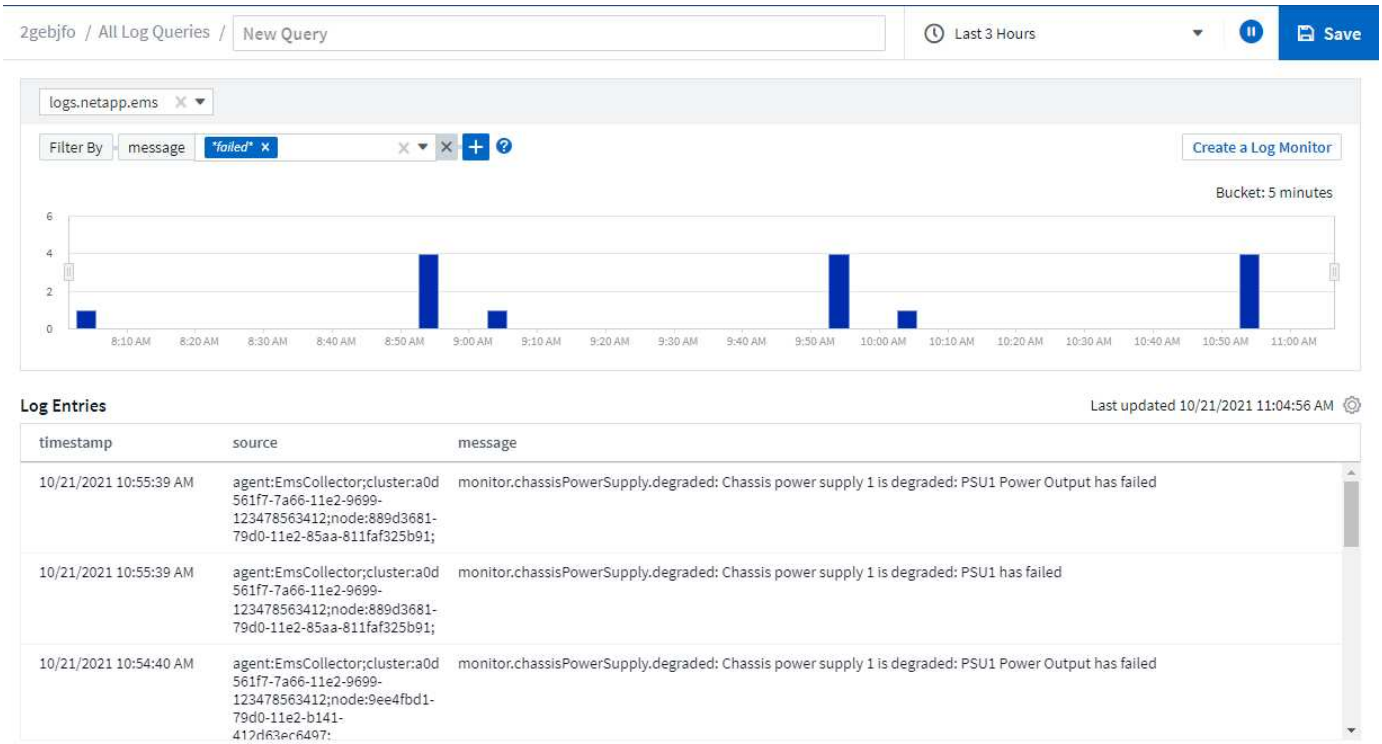


I tipi di log disponibili per le query possono variare a seconda dell'ambiente in uso. È possibile aggiungere altri tipi di log nel tempo.

È possibile impostare filtri per perfezionare ulteriormente i risultati della query. Ad esempio, per trovare tutti i messaggi di registro che mostrano un errore, impostare un filtro per *messaggi* contenente la parola "non riuscito".

È possibile iniziare a digitare il testo desiderato nel campo del filtro; Cloud Insights richiederà di creare una ricerca con caratteri jolly contenente la stringa durante la digitazione.

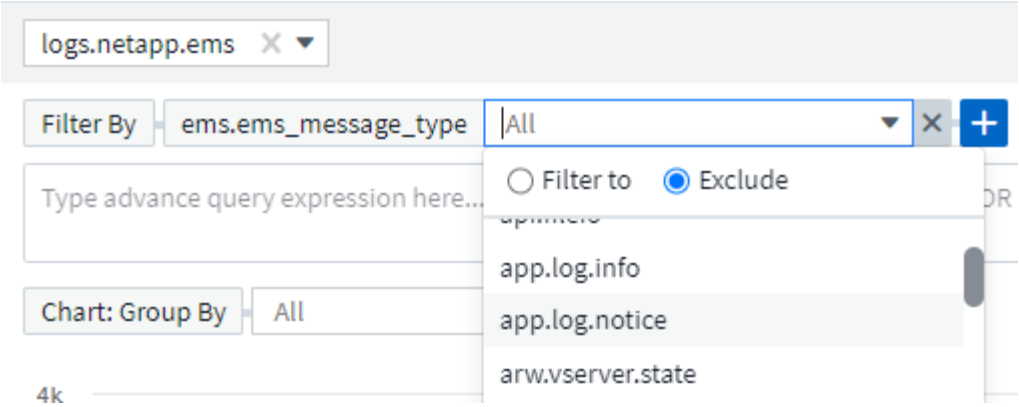
I risultati vengono visualizzati in un grafico che mostra il numero di istanze di log in ciascun periodo di tempo visualizzato. Sotto il grafico sono riportati i modelli di voci di log. Il grafico e le voci si aggiornano automaticamente in base all'intervallo di tempo selezionato.



Filtraggio

Includi/Escludi

Quando si filtrano i log, è possibile scegliere di **includere** (ad esempio "filtro a") o **escludere** le stringhe digitate. Le stringhe escluse vengono visualizzate nel filtro completato come "NON <string>".



I filtri basati su caratteri jolly o espressioni (ad esempio, NO, O "None", ecc.) vengono visualizzati in blu scuro nel campo del filtro. Gli elementi selezionati direttamente dall'elenco vengono visualizzati in blu chiaro.

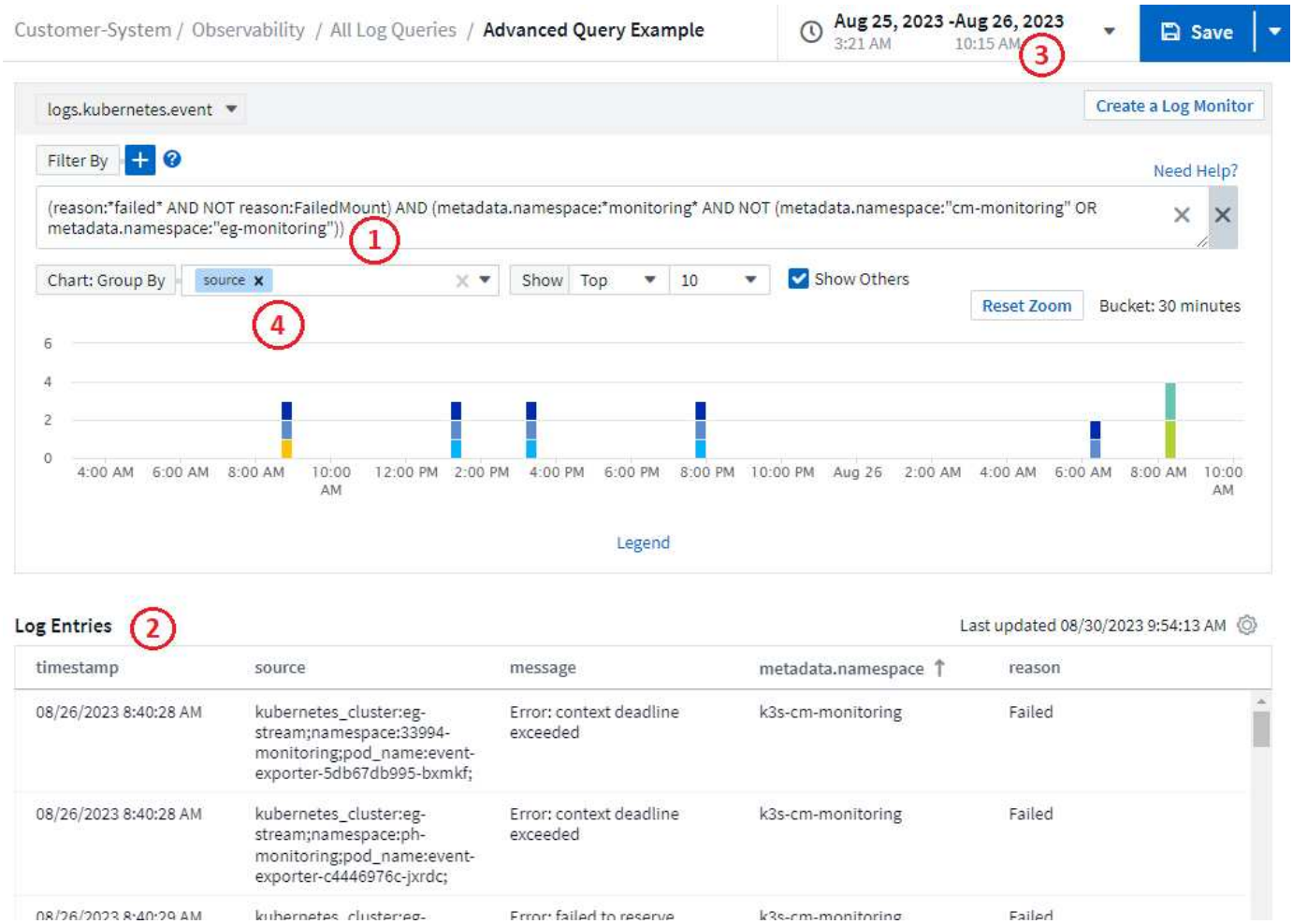
> In qualsiasi momento, è possibile fare clic su *Create a Log Monitor* per creare un nuovo monitor in base al filtro corrente.

Filtraggio avanzato

Quando si filtrano valori di testo o di elenco nelle query o nei widget della dashboard, quando si inizia a digitare viene visualizzata l'opzione per creare un filtro * con caratteri jolly* in base al testo corrente. Selezionando questa opzione verranno restituiti tutti i risultati che corrispondono all'espressione con caratteri jolly. È inoltre possibile creare espressioni utilizzando NON, E, o o, oppure selezionare l'opzione "Nessuno" per filtrare i valori nulli.

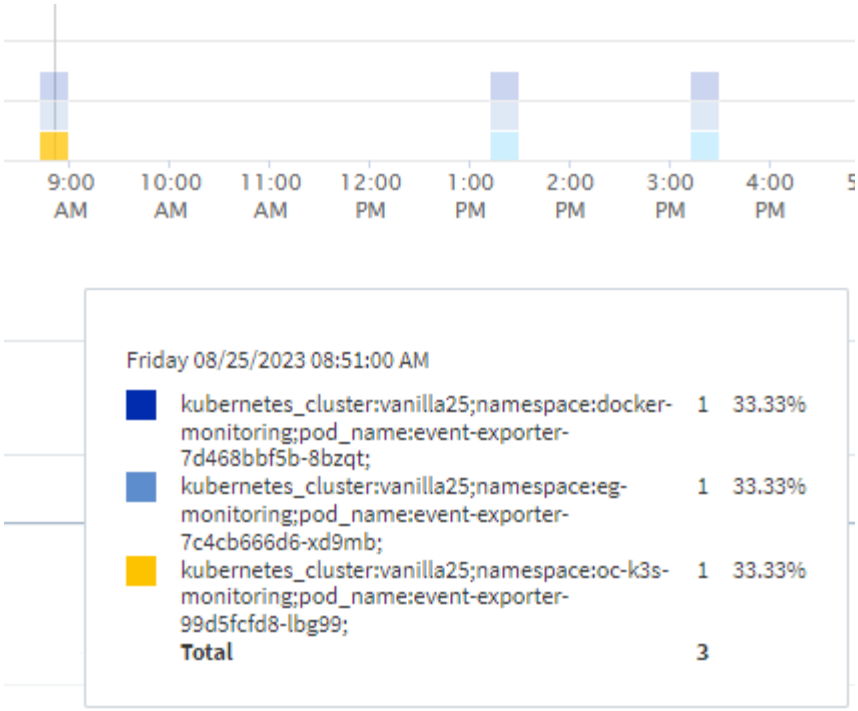
> Assicurarsi di salvare la query in anticipo e spesso durante la creazione del filtro. L'interrogazione avanzata è una voce di stringa "free-form" e gli errori di analisi possono verificarsi durante la compilazione.

Date un'occhiata a questa immagine della schermata che mostra i risultati filtrati per una query avanzata del log *logs.kuPQ.event*. C'è molto in corso in questa pagina, che è spiegato sotto l'immagine:



1. Questa stringa di query avanzata filtra per quanto segue:
   - Filtro per le voci di registro con *reason* che include la parola "FAILED", ma non qualsiasi cosa con il motivo specifico di "FailedMount".
   - Includere una qualsiasi di quelle voci che includono anche un *metadata.namespace* compresa la parola "monitoraggio", ma escludere gli spazi dei nomi specifici di "monitoraggio cm" o "monitoraggio es.".

     Si noti che nel caso precedente, poiché sia "cm-monitoring" che "eg-monitoring" contengono un trattino ("-"), le stringhe devono essere incluse tra virgolette doppie o verrà visualizzato un errore di analisi. Le stringhe che non includono trattini, spazi, ecc. non devono essere racchiuse tra virgolette. In caso di dubbi, provare a inserire la stringa tra virgolette.
2. I risultati del filtro corrente, compresi i valori "Filtra per" E il filtro query avanzate, vengono visualizzati nell'elenco dei risultati. L'elenco può essere ordinato in base alle colonne visualizzate. Per visualizzare colonne aggiuntive, selezionare l'icona "marcia".
3. Il grafico è stato ingrandito per visualizzare solo i risultati del registro che si sono verificati in un intervallo di tempo specifico. L'intervallo di tempo mostrato qui riflette il livello di zoom corrente. Selezionare il pulsante *Reimposta zoom* per riportare il livello di zoom all'intervallo temporale Cloud Insights corrente.
4. I risultati del grafico sono stati raggruppati in base al campo *source*. Il grafico mostra i risultati in ogni colonna raggruppati in colori. Passando con il mouse sopra una colonna del grafico vengono visualizzati alcuni dettagli relativi alle voci specifiche.



Raffinazione dei filtri

Per perfezionare il filtro, utilizzare quanto segue:

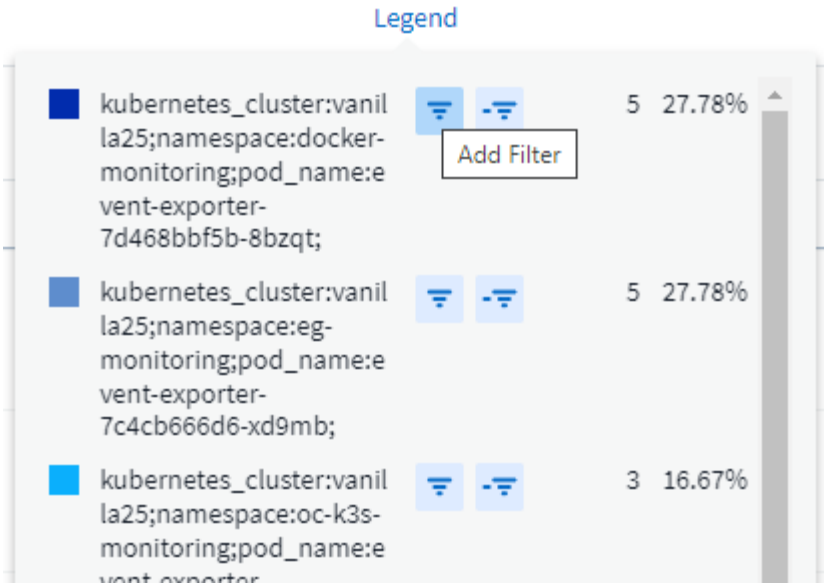
Filtro	Che cosa fa
* (Asterisco)	consente di cercare tutto
? (punto interrogativo)	consente di cercare un numero specifico di caratteri
OPPURE	consente di specificare più entità
NO	consente di escludere il testo dai risultati della ricerca
Nessuno	Ricerca i valori NULL in tutti i campi
Non *	Cerca i valori NULL nei campi *text-only*

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 "*" restituirà risultati che sono un asterisco letterale; in questo caso, l'asterisco non verrà trattato come carattere jolly. Gli operatori O e NON verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

È possibile combinare un filtro semplice con un filtro query avanzato; il filtro risultante è un "AND" dei due.

La legenda del grafico

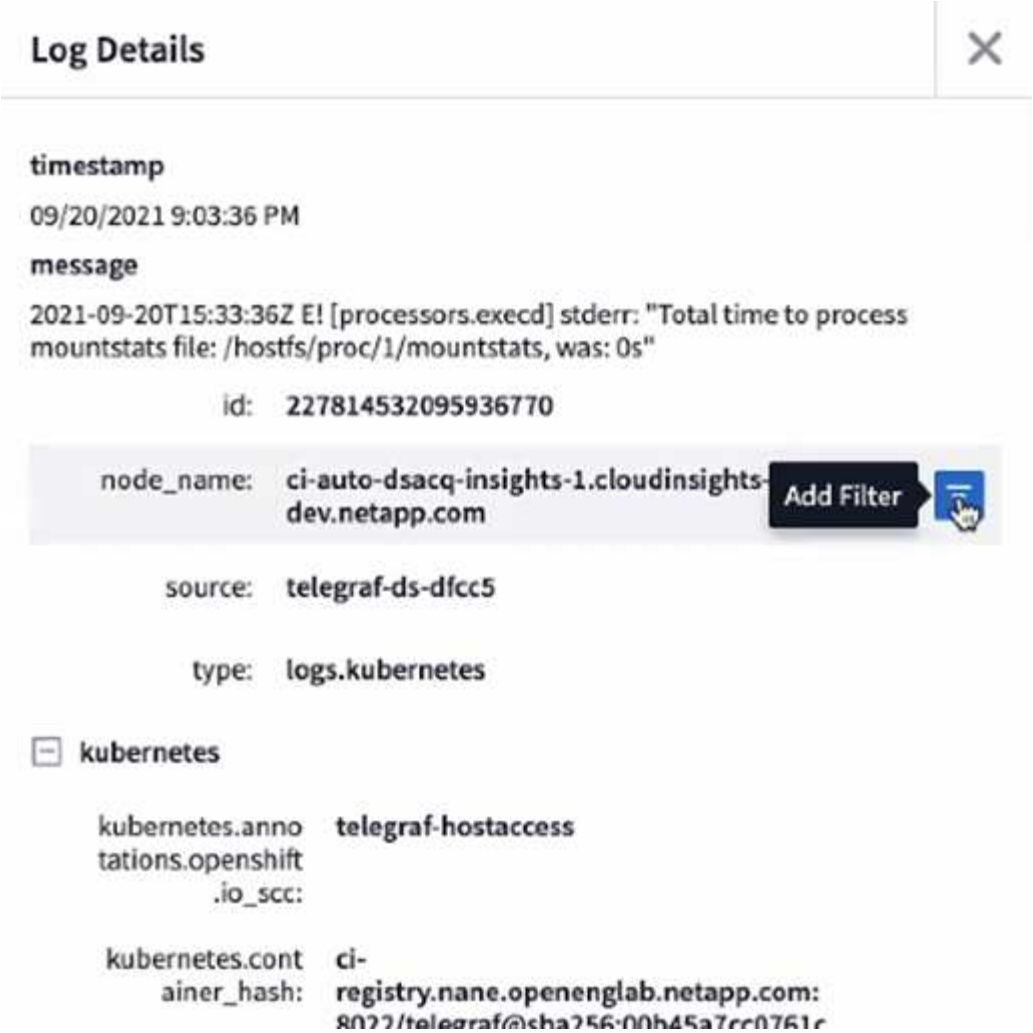
Anche la *Legend* sotto il grafico presenta alcune sorprese. Per ciascun risultato (in base al filtro corrente) visualizzato nella legenda, è possibile visualizzare solo i risultati per tale riga (Aggiungi filtro) o i risultati NON per quella riga (Aggiungi filtro esclusione). Il grafico e l'elenco voci registro vengono aggiornati per visualizzare i risultati in base alla selezione effettuata. Per rimuovere questo filtro, aprire nuovamente la legenda e selezionare [X] per cancellare il filtro basato su legenda.



Dettagli registro

Facendo clic in un punto qualsiasi di una voce di registro nell'elenco, viene aperto un riquadro dei dettagli per tale voce. Qui puoi esplorare ulteriori informazioni sull'evento.

Fare clic su "Add Filter" (Aggiungi filtro) per aggiungere il campo selezionato al filtro corrente. L'elenco delle voci di registro viene aggiornato in base al nuovo filtro.



Risoluzione dei problemi

Qui troverai suggerimenti per la risoluzione dei problemi relativi alle query di log.

Problema:	Provare questo:
Non vengono visualizzati messaggi di "debug" nella query del log	La messaggistica del registro di debug non viene raccolta. Per acquisire i messaggi desiderati, impostare la gravità del messaggio su *informativo, errore, avviso, emergenza o livello _avviso*.

Utilizzo delle annotazioni

Definizione delle annotazioni

Quando si personalizza Cloud Insights per tenere traccia dei dati in base ai requisiti aziendali, è possibile definire note specializzate, denominate annotazioni, e assegnarle alle risorse.

È possibile assegnare annotazioni alle risorse con informazioni quali 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.
- Filtrare le risorse in base alle annotazioni.

Tipi di annotazione predefiniti

Cloud Insights fornisce alcuni tipi di annotazione predefiniti. Queste annotazioni possono essere utilizzate per filtrare o raggruppare i 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 seguente tabella elenca i tipi di annotazione forniti da Cloud Insights.

Tipi di annotazione	Descrizione	Tipo
Alias	Nome intuitivo per una risorsa	Testo
Gruppo di risorse di calcolo	Assegnazione del gruppo utilizzata dal data collector host e VM Filesystems	Elenco
Data center	Ubicazione fisica	Elenco
Caldo	Dispositivi che utilizzano in modo intensivo su base regolare o alla soglia di capacità	Booleano
Nota	Commenti associati a una risorsa	Test

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
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	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. 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, Switch Level (livello switch), Tier (livello) e Violation Severity (gravità violazione) sono annotazioni a livello di sistema che non è possibile eliminare o rinominare; è possibile modificare solo i valori assegnati.

Creazione di annotazioni personalizzate

Utilizzando le annotazioni, è possibile aggiungere dati personalizzati specifici del business che corrispondano alle esigenze del business alle risorse. Sebbene Cloud Insights 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 produttore dello storage, volumi numerici e statistiche delle performance. I dati aggiunti utilizzando le annotazioni non vengono rilevati da Cloud Insights.

Fasi

1. Nel menu Cloud Insights, fare clic su **Gestisci > Annotazioni**.

   La pagina Annotazioni visualizza l'elenco delle annotazioni.

2. Fare clic su **+Aggiungi**
3. Inserire **Nome** e **Descrizione** dell'annotazione.

   È possibile inserire fino a 255 caratteri in questi campi.

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

Tipi di annotazione

Booleano

Crea un elenco a discesa con le opzioni Sì e No Ad esempio, l'annotazione "Direct 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

Crea 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 Add new values on the fly (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

Crea un campo in cui l'utente che assegna l'annotazione può inserire un numero. Ad esempio, se il tipo di annotazione è "Floor" (piano), l'utente può selezionare il tipo di valore "Number" (numero) e inserire il numero di piano.

Testo

Crea un campo che consente il testo in formato libero. Ad esempio, è possibile inserire "Lingua" come tipo di annotazione, selezionare "testo" 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.

1. 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 una descrizione nei campi **valore** e **Descrizione**.
   c. Fare clic su **Aggiungi** per aggiungere altri valori.
   d. Fare clic sull'icona Cestino per eliminare un valore.
2. Fare clic su **Save** (Salva)

Le annotazioni vengono visualizzate nell'elenco della pagina Annotazioni.

Al termine

Nell'interfaccia utente, l'annotazione è immediatamente disponibile per l'utilizzo.

Utilizzo delle annotazioni

È possibile creare annotazioni e assegnarle alle risorse monitorate. Le annotazioni sono note che forniscono informazioni su una risorsa, ad esempio posizione fisica, fine del ciclo di vita, Tier di storage o livelli di servizio del volume.

Definizione delle annotazioni

Utilizzando le annotazioni, è possibile aggiungere dati personalizzati specifici del business che corrispondano alle esigenze del business alle risorse. Sebbene Cloud Insights fornisca una serie di annotazioni predefinite, 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, 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 Cloud Insights.

Prima di iniziare

- Elencare qualsiasi terminologia del settore a cui devono essere associati i dati dell'ambiente.
- Elencare la terminologia aziendale a cui devono essere associati i dati dell'ambiente.
- Identificare i tipi di annotazione predefiniti che potrebbero essere utilizzabili.
- Identificare le annotazioni personalizzate da creare. È necessario creare l'annotazione prima di assegnarla a una risorsa.

Per creare un'annotazione, procedere come segue.

Fasi

1. Nel menu Cloud Insights, fare clic su **Gestisci > Annotazioni**
2. Fare clic su **+ Annotation** per creare una nuova annotazione.
3. Immettere un Nome, una Descrizione e un tipo per la nuova annotazione.

   Ad esempio, immettere quanto segue per creare un'annotazione di testo che definisca la posizione fisica di una risorsa nel Data Center 4:

   - Inserire un nome per l'annotazione, ad esempio "Location" (posizione)
   - Inserire una descrizione dell'annotazione, ad esempio "la posizione fisica è data center 4"
   - Inserire il "tipo" di annotazione, ad esempio "testo".

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'ambiente Cloud Insights.
2. Individuare la risorsa a cui si desidera applicare l'annotazione.
    - È possibile individuare le risorse eseguendo query, scegliendo da un widget dashoard o effettuando una ricerca. Una volta individuata la risorsa desiderata, fare clic sul collegamento per aprire la landing page della risorsa.
3. Nella pagina delle risorse, nella sezione User Data (dati utente), fare clic su **+ Annotation (Annotazione)**.
4. Viene visualizzata la finestra di dialogo Add Annotation (Aggiungi annotazione).
5. Selezionare un'annotazione dall'elenco.
6. Fare clic su Value (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.
7. Fare clic su **Save** (Salva).

Se si desidera modificare il valore dell'annotazione dopo averlo assegnato, fare clic sul campo dell'annotazione e selezionare un valore diverso. Se l'annotazione è di tipo elenco per cui è selezionata l'opzione *Add new values on the fly*, è possibile digitare un nuovo valore oltre alla selezione di un valore esistente.

Assegnazione di annotazioni utilizzando le regole di annotazione

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

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. Fare clic su **Gestisci > regole annotazione**

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

2. Fare clic su **+ Aggiungi**.
3. 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 utilizzata 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.

   e. Fare clic su **Save** (Salva)
   f. 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.

Creazione di regole di annotazione

È possibile utilizzare le regole di annotazione per applicare automaticamente le annotazioni a più risorse in base ai criteri definiti dall'utente. Cloud Insights assegna le annotazioni alle risorse in base a queste regole. Le annotazioni impostate manualmente su una singola pagina di risorse hanno la precedenza sulle annotazioni basate su regole quando Cloud Insight valuta le regole di annotazione.

Prima di iniziare

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

Fasi

1. Nel menu Cloud Insights, fare clic su **Gestisci > regole annotazione**.
2. Fare clic su **+ Rule** per aggiungere una nuova regola di annotazione.

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

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

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

   b. Fare clic su **Query** e selezionare la query utilizzata da Cloud Insights per identificare le risorse a cui si applica l'annotazione.
   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.

   e. Fare clic su **Save** (Salva)
   f. 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.

In un ambiente Cloud Insights di grandi dimensioni, l'esecuzione delle regole di annotazione sembra richiedere qualche istante. Questo perché l'indicizzatore viene eseguito per primo e deve essere completato prima di eseguire le regole. L'indicizzatore consente a Cloud Insights di cercare o filtrare oggetti e contatori nuovi o aggiornati nei dati. Prima di applicare le regole, il motore delle regole attende che l'indicizzatore completi l'aggiornamento.

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. Nel menu Cloud Insights, fare clic su **Gestisci > regole annotazione**.

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

2. Individuare la regola di annotazione che si desidera modificare.

   È possibile filtrare le regole di annotazione immettendo un valore nella casella di filtro o facendo clic su un numero di pagina per sfogliare le regole di annotazione per pagina.

3. Fare clic sull'icona del menu corrispondente alla regola che si desidera modificare.
4. Fare clic su **Edit** (Modifica)

   Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola).

5. Modificare il nome, l'annotazione, il valore o la query della regola di annotazione.

Modifica dell'ordine delle regole

Le regole di annotazione vengono elaborate dall'inizio dell'elenco delle regole alla fine. Per modificare l'ordine di elaborazione di una regola, procedere come segue:

Fasi

1. Fare clic sull'icona del menu corrispondente alla regola che si desidera spostare.
2. Fare clic su **Sposta in alto** o **Sposta in basso** fino a visualizzare la regola nella posizione desiderata.

Quando si eseguono più regole che aggiornano la stessa annotazione su una risorsa, la prima regola (eseguita dall'alto verso il basso) applica l'annotazione e aggiorna la risorsa, quindi la seconda regola si applica senza modificare alcuna annotazione già impostata dalla regola precedente.

Eliminazione delle regole di annotazione

Si consiglia di eliminare le regole di annotazione non più utilizzate.

Fasi

1. Nel menu Cloud Insights, fare clic su **Gestisci > regole annotazione**.

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

2. Individuare la regola di annotazione che si desidera eliminare.

   È possibile filtrare le regole di annotazione immettendo un valore nella casella di filtro o facendo clic su un numero di pagina per sfogliare le regole di annotazione per pagina.

3. Fare clic sull'icona del menu corrispondente alla regola che si desidera eliminare.
4. Fare clic su **Delete** (Elimina)

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

5. Fare clic su **OK**

Importazione delle annotazioni

Cloud Insights include un'API per importare annotazioni o applicazioni da un file CSV e assegnarle agli oggetti specificati.

L'API Cloud Insights è disponibile in **Cloud Insights Premium Edition**.

Importazione in corso

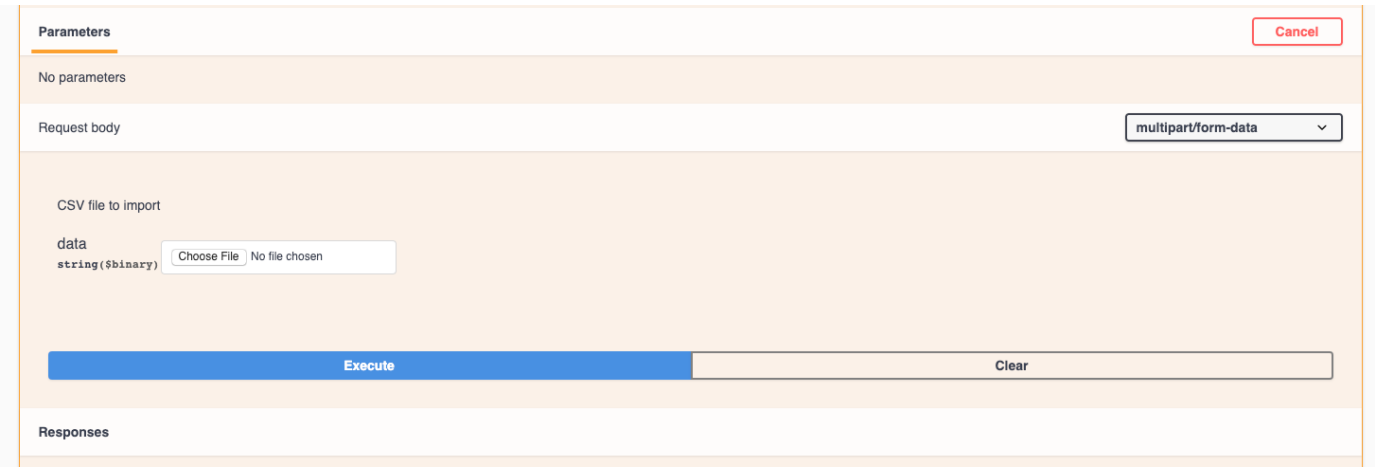
I collegamenti **Admin > API Access** contengono "documentazione" Per l'API **Assets/Import**. La presente documentazione contiene informazioni sul formato file .CSV.

Formato file .CSV

Il formato generale del file CSV è il seguente. La prima riga del file definisce i campi di importazione e specifica l'ordine dei campi. Segue righe separate per ogni annotazione o applicazione. Non è necessario definire tutti i campi. Tuttavia, le righe di annotazione successive devono seguire lo stesso ordine della riga di definizione.

```
 [Object Type] , [Object Name or ID] , Annotation Type [, Annotation
Type,  ...] [, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]
Consultare la documentazione API per esempi di file .CSV.
```

È possibile importare e assegnare annotazioni da un file .CSV all'interno dello swagger API stesso. Basta scegliere il file da utilizzare e fare clic sul pulsante *Execute*:



Comportamento di importazione

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

- Aggiunge un'annotazione o un'applicazione se non esiste alcuna annotazione con lo stesso nome nel sistema di destinazione.
- 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.

  Nota: 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.

- Se un valore di annotazione è vuoto, l'annotazione viene rimossa dall'oggetto. Le annotazioni ereditate non vengono influenzate.
- I valori di annotazione del tipo di data devono essere passati come tempo unix in millisecondi.
- Quando si annotano volumi o volumi interni, il nome dell'oggetto è una combinazione di nome dello storage e nome del volume che utilizza il separatore "→". Ad esempio: *<Storage Name>→<Volume Name>*
- Se il nome di un oggetto contiene una virgola, l'intero nome deve essere tra virgolette doppie. Ad esempio: *"NetApp1,NetApp2"→023F*
- Quando si allegano annotazioni a storage, switch e porte, la colonna "applicazione" viene ignorata.
- Tenant, Line_of_Business, Business_Unit e/o Project crea un'entità aziendale. Come per tutte le entità aziendali, i valori possono essere vuoti.

È possibile annotare i seguenti tipi di oggetti.

TIPO DI OGGETTO	NOME O CHIAVE
Host	id→<id> o <Name> o <IP>
MACCHINA VIRTUALE	id→<id> o <Name>

StoragePool	id→<id> o <Storage Name>→<Storage Pool Name>
Volume interno	id→<id> o <Storage Name>→<Internal Volume Name>
Volume	id→<id> o <Storage Name>→<Volume Name>
Storage	id→<id> o <Name> o <IP>
Switch	id→<id> o <Name> o <IP>
Porta	id→<id> o <WWN>
Qtree	id→<id> o <Storage Name>→<Internal Volume Name>→<Qtree Name>
Condividere	id→<id> o <Storage Name>→<Internal Volume Name>→<Share Name>→<Protocol>[→<Qtree Name (optional in case of default Qtree)>]

Utilizzo delle applicazioni

Monitoraggio dell’utilizzo delle risorse per applicazione

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 questo argomento viene fornito un esempio di monitoraggio dell’utilizzo delle macchine virtuali che il team di marketing utilizza per la posta elettronica Exchange.

È possibile creare una tabella simile a quella riportata di seguito per identificare le applicazioni utilizzate nel proprio ambiente e prendere nota del gruppo o della business unit che utilizza ciascuna applicazione.

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

La tabella mostra che il team di marketing utilizza l’applicazione Exchange. Vogliamo tenere traccia dell’utilizzo delle macchine virtuali per Exchange, in modo da poter prevedere quando sarà necessario aggiungere ulteriore storage. Possiamo associare l’applicazione Exchange a tutte le macchine virtuali di Marketing:

1. Creare un’applicazione denominata *Exchange*
2. Accedere a **Query > +Nuova query** per creare una nuova query per le macchine virtuali (oppure selezionare una query VM esistente, se applicabile).

   Supponendo che tutte le macchine virtuali del team di marketing abbiano un nome contenente la stringa "**mkt**", creare la query per filtrare il nome della macchina virtuale per "mkt".

3. Selezionare le macchine virtuali.
4. Associare le macchine virtuali all’applicazione *Exchange* utilizzando **azioni in blocco > Aggiungi applicazioni**.
5. Selezionare l’applicazione desiderata e fare clic su **Save** (Salva).
6. Al termine, **salvare** la query.

Creazione di applicazioni

Per tenere traccia dei dati associati a specifiche applicazioni in esecuzione nel proprio ambiente, è possibile definire le applicazioni in Cloud Insights.

Prima di iniziare

Se si desidera associare l’applicazione a un’entità aziendale, è necessario creare l’entità aziendale prima di definire l’applicazione.

A proposito di questa attività

Cloud Insights consente di tenere traccia dei dati delle risorse associate alle applicazioni per attività come l'utilizzo o il reporting dei costi.

Fasi

1. Nel menu Cloud Insights, fare clic su **Gestisci > applicazioni**.

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

2. Immettere un nome univoco per l'applicazione.
3. Selezionare una priorità per l'applicazione.
4. Fare clic su **Save** (Salva).

Dopo aver definito un'applicazione, è possibile assegnarla alle risorse.

Assegnazione di applicazioni alle risorse

Questa procedura assegna l'applicazione a un host come esempio. È possibile assegnare a un'applicazione host, macchine virtuali, volumi o volumi interni.

Fasi

1. Individuare la risorsa a cui si desidera assegnare l'applicazione:
2. Fare clic su **Query > +Nuova query** e cercare host.
3. Fare clic sulla casella di controllo a sinistra dell'host che si desidera associare all'applicazione.
4. Fare clic su **azioni in blocco > Aggiungi applicazione**.
5. Selezionare l'applicazione a cui si desidera assegnare la risorsa.

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.

> Per gli ambienti con grandi quantità di risorse correlate, l'ereditarietà delle assegnazioni delle applicazioni a tali risorse potrebbe richiedere diversi minuti. Attendere più tempo per l'ereditarietà se si dispone di molte risorse correlate.

Al termine

Dopo aver assegnato l'host all'applicazione, è possibile assegnare le risorse rimanenti all'applicazione. Per accedere alla landing page dell'applicazione, fare clic su **Manage > Application** (Gestisci > applicazione) e selezionare l'applicazione creata.

Monitor e avvisi

Avvisi con i monitor

È possibile creare monitor per impostare soglie che attivino avvisi per segnalare problemi relativi alle risorse della rete. Ad esempio, è possibile creare un monitor per avvisare della *latenza di scrittura del nodo* per una moltitudine di protocolli.

> Monitor e avvisi sono disponibili in tutte le edizioni Cloud Insights, tuttavia, l'edizione di base è soggetta a quanto segue: * È possibile che siano attivi solo cinque monitor personalizzati alla volta. Tutti i monitor oltre i cinque verranno creati o spostati nello stato *Paused*. * I monitor VMDK, Virtual Machine, host e datastore non sono supportati. Se sono stati creati dei monitor per queste metriche, questi verranno messi in pausa e non potranno essere ripristinati durante il downgrade a Basic Edition.

I monitor consentono di impostare soglie sulle metriche generate da oggetti "infrastruttura" come storage, VM, EC2 e porte, nonché per i dati di "integrazione" come quelli raccolti per Kubernetes, metriche avanzate di ONTAP e plug-in Telegraf. Questi *metric* monitors avvisano l'utente quando vengono superate le soglie del livello di avviso o critico.

È inoltre possibile creare monitor per attivare avvisi a livello di avviso, critico o informativo quando vengono rilevati *eventi di log* specificati.

Cloud Insights fornisce una serie di "Monitor definiti dal sistema" inoltre, in base al tuo ambiente.

Best practice per la sicurezza

Gli avvisi Cloud Insights sono progettati per evidenziare i punti dati e le tendenze nell'ambiente in uso e Cloud Insights consente di inserire qualsiasi indirizzo e-mail valido come destinatario dell'avviso. Se si lavora in un ambiente sicuro, prestare particolare attenzione a chi riceve la notifica o a chi ha accesso all'avviso.

Metriche o Log Monitor?

1. Dal menu Cloud Insights, fare clic su **Avvisi > Gestisci monitor**

   Viene visualizzata la pagina dell'elenco Monitor, che mostra i monitor attualmente configurati.

2. Per modificare un monitor esistente, fare clic sul nome del monitor nell'elenco.
3. Per aggiungere un monitor, fare clic su **+ Monitor**.

Quando si aggiunge un nuovo monitor, viene richiesto di creare un monitor metrico o un monitor di registro.

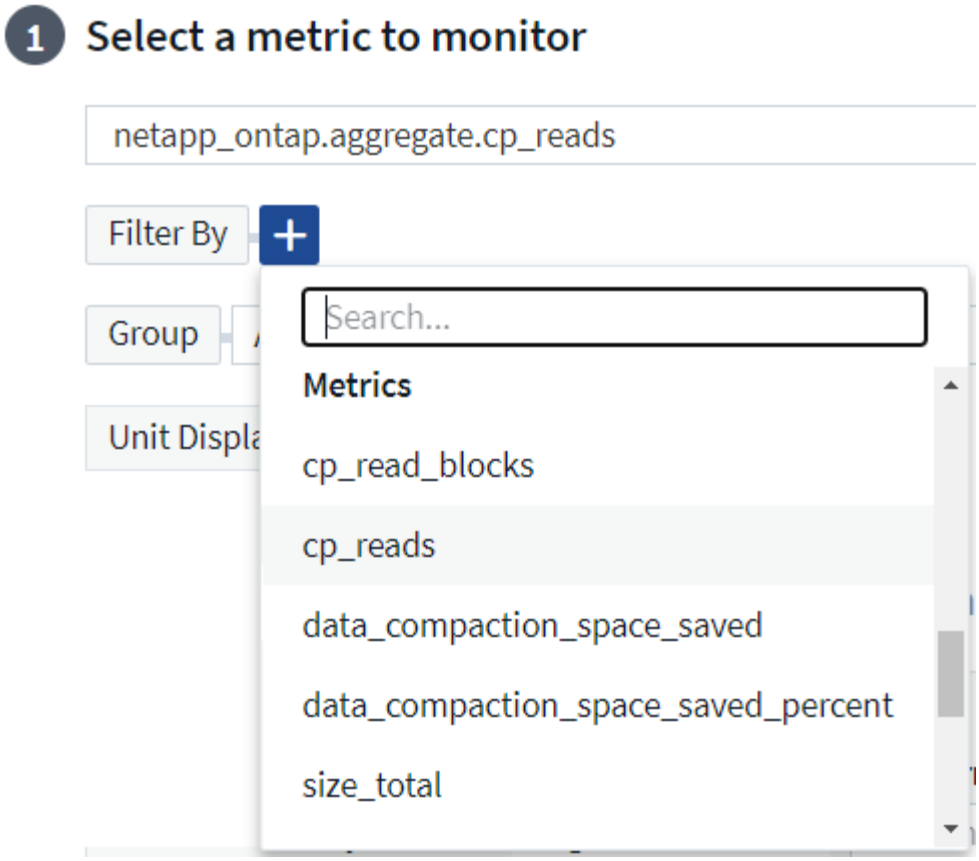
- *Metric* monitora gli avvisi sui trigger relativi all'infrastruttura o alle performance
- *Log* monitora gli avvisi sulle attività correlate al log

Dopo aver scelto il tipo di monitor, viene visualizzata la finestra di dialogo Configurazione monitor. La configurazione varia a seconda del tipo di monitor che si sta creando.

Monitor metrico

1. Nell'elenco a discesa, cercare e scegliere un tipo di oggetto e una metrica da monitorare.

È possibile impostare i filtri per limitare gli attributi o le metriche degli oggetti da monitorare.



Quando si lavora con i dati di integrazione (Kubernetes, dati avanzati ONTAP, ecc.), il filtraggio metrico rimuove i singoli punti dati/non corrispondenti dalla serie di dati plottati, a differenza dei dati dell'infrastruttura (storage, VM, porte, ecc.) in cui i filtri funzionano sul valore aggregato della serie di dati e potenzialmente rimuovono l'intero oggetto dal grafico.

> Per creare un monitor multi-condizione (ad esempio, IOPS > X e latenza > Y), definire la prima condizione come soglia e la seconda condizione come filtro.

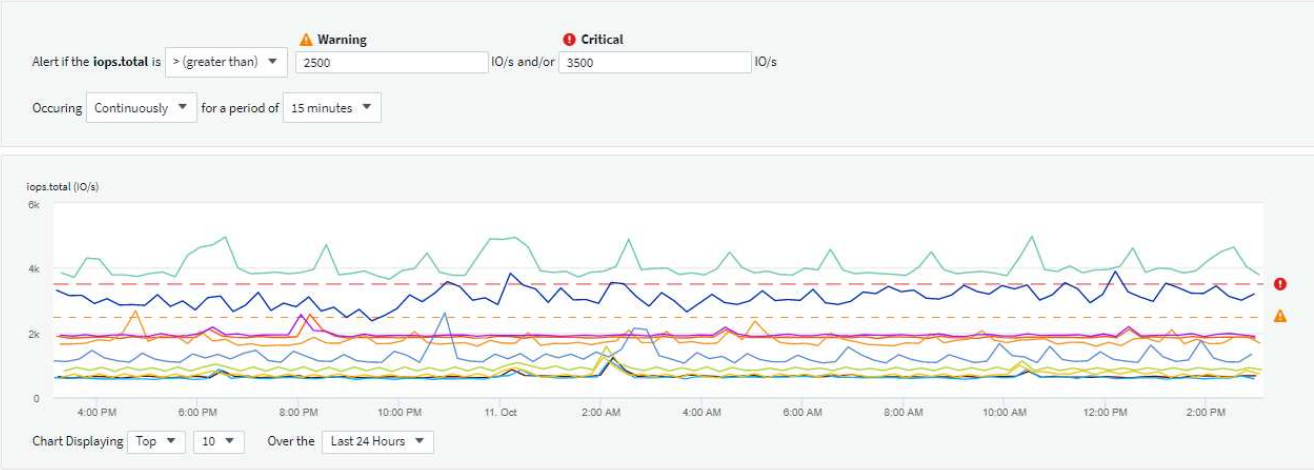
Definire le condizioni del monitor.

1. Dopo aver scelto l'oggetto e la metrica da monitorare, impostare le soglie del livello di avviso e/o critico.
2. Per il livello *Warning*, immettere 200 come esempio. La linea tratteggiata che indica questo livello di avviso viene visualizzata nel grafico di esempio.
3. Per il livello *critico*, immettere 400. La linea tratteggiata che indica questo livello critico viene visualizzata nel grafico di esempio.

   Il grafico mostra i dati storici. Le righe di avviso e livello critico sul grafico rappresentano una rappresentazione visiva del monitor, in modo da poter vedere facilmente quando il monitor potrebbe attivare un avviso in ogni caso.

4. Per l'intervallo di ricorrenza, scegliere *Continuously* per un periodo di *15 minuti*.

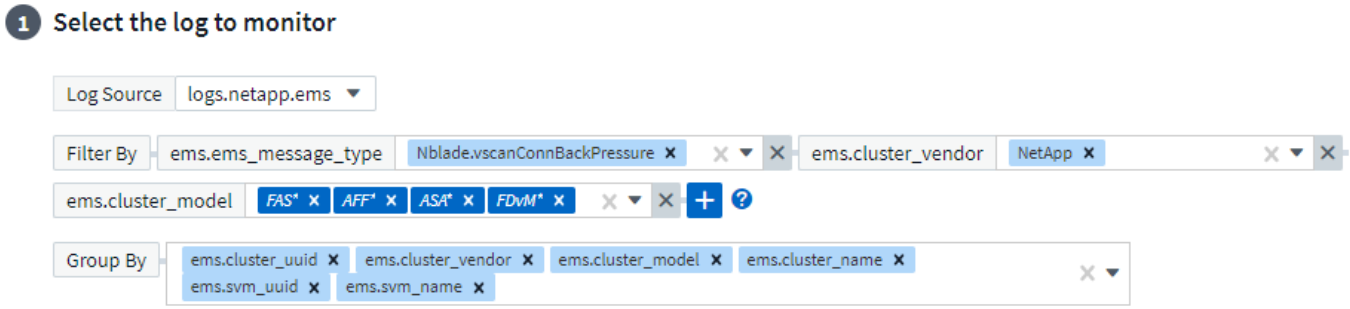
   Puoi scegliere di attivare un avviso quando una soglia viene violata o di attendere che la soglia si trovi in una violazione continua per un certo periodo di tempo. Nel nostro esempio, non vogliamo essere avvisati ogni volta che gli IOPS totali superano il livello di avviso o critico, ma solo quando un oggetto monitorato supera continuamente uno di questi livelli per almeno 15 minuti.



Log Monitor

Quando si crea un monitor **Log**, scegliere innanzitutto quale registro monitorare dall'elenco Available log (registri disponibili). È quindi possibile filtrare in base agli attributi disponibili, come descritto sopra. Puoi anche scegliere uno o più attributi "Raggruppa per".

> Il filtro Log Monitor non può essere vuoto.



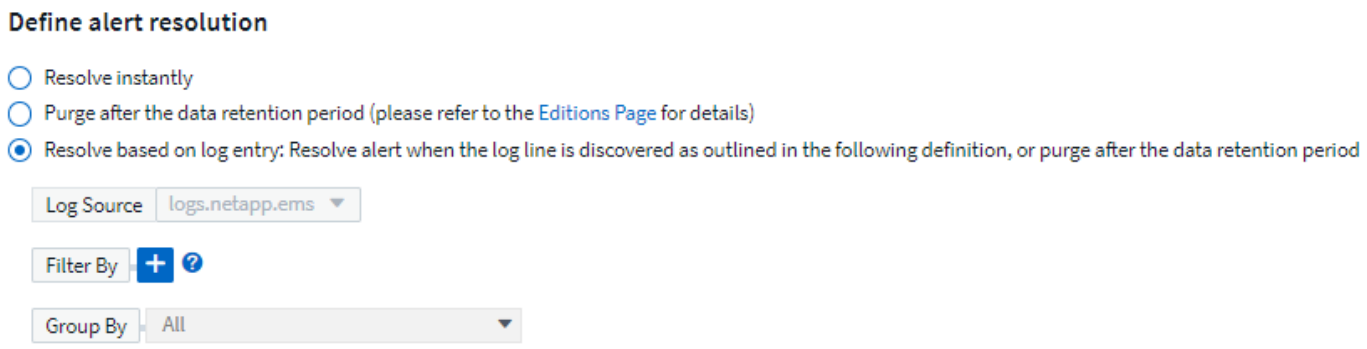
Definire il comportamento degli avvisi

È possibile creare un monitor per avvisare con un livello di gravità di *critico*, *Avviso* o *informativo*, quando le condizioni sopra definite si verificano una sola volta (cioè immediatamente), oppure attendere che le condizioni si verifichino 2 o più volte.

Definire il comportamento di risoluzione degli avvisi

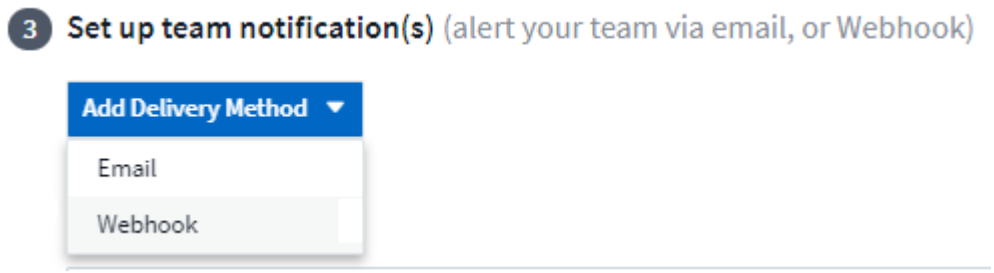
È possibile scegliere la modalità di risoluzione di un avviso di log monitor. Sono disponibili tre opzioni:

- Risolvere immediatamente
- Rimuovi dopo il periodo di conservazione dei dati (per ulteriori informazioni, fare riferimento alla pagina delle edizioni). Tenere presente che il monitor non dispone di alcuna condizione di risoluzione per definizione, pertanto un avviso rimane *attivo* e elimina tutti gli avvisi successivi con la corrispondenza *group_by* generata dal monitor, fino al termine del periodo di conservazione dei dati.
- Resolve Based on log entry (Risolvi in base alla voce del registro): Consente di risolvere l'avviso quando la riga del registro viene rilevata come indicato nella seguente definizione o di eliminare i dati dopo il periodo di conservazione.



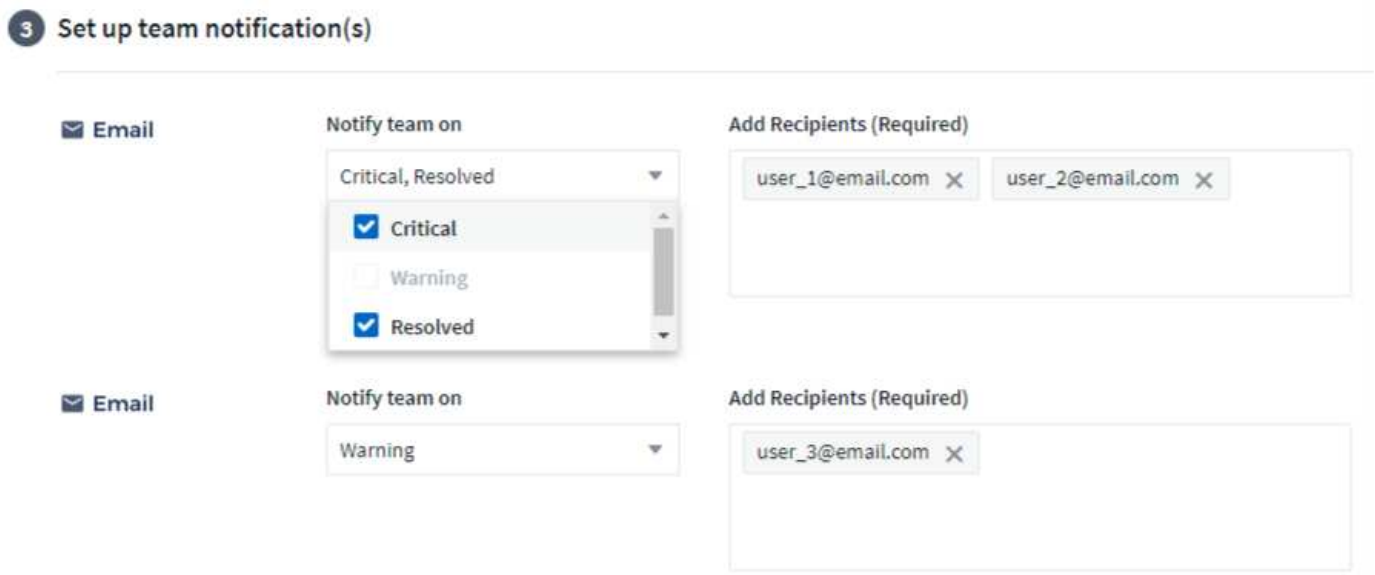
Selezionare il tipo di notifica e i destinatari

Nella sezione *impostare le notifiche del team*, puoi scegliere se avvisare il tuo team tramite e-mail o Webhook.



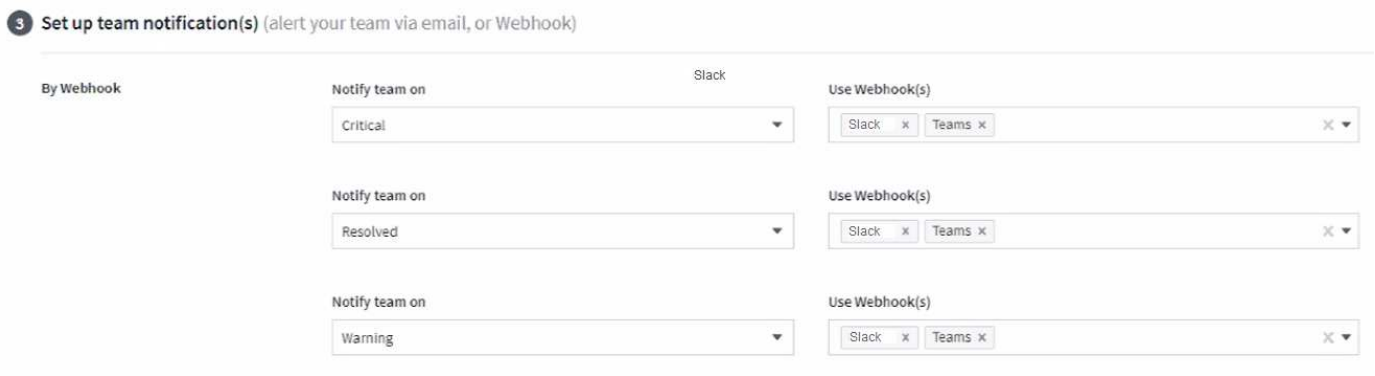
Avvisi via email:

Specificare i destinatari dell'e-mail per le notifiche degli avvisi. Se lo si desidera, è possibile scegliere diversi destinatari per gli avvisi di avviso o critici.



Avvisi via Webhook:

Specificare i webhook per le notifiche degli avvisi. Se lo si desidera, è possibile scegliere diversi webhook per gli avvisi critici o di avviso.

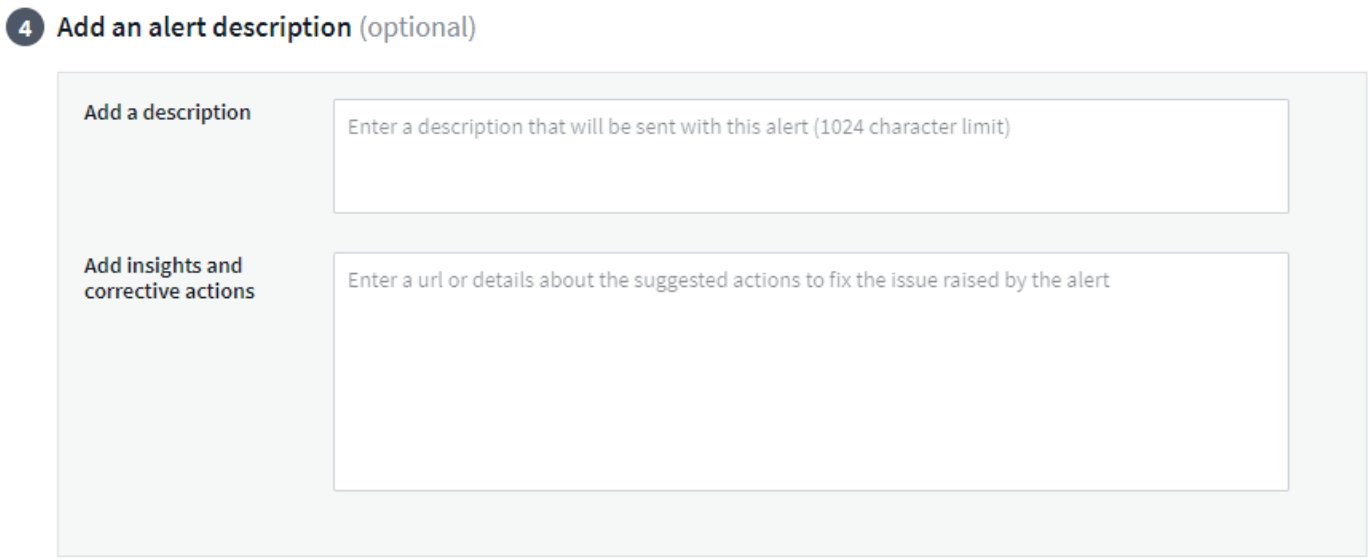


Le notifiche del Data Collector di ONTAP hanno la precedenza su qualsiasi notifica specifica del Monitor rilevante per il cluster/data collector. L'elenco dei destinatari impostato per Data Collector riceverà gli avvisi di data collector. Se non sono presenti avvisi di data collector attivi, gli avvisi generati dal monitor verranno inviati a destinatari specifici del monitor.

Impostazione di azioni correttive o informazioni aggiuntive

È possibile aggiungere una descrizione opzionale, informazioni aggiuntive e/o azioni correttive compilando la sezione **Aggiungi una descrizione dell'avviso**. La descrizione può contenere fino a 1024 caratteri e verrà inviata con l'avviso. Il campo Insight/azione correttiva può contenere fino a 67,000 caratteri e verrà visualizzato nella sezione riepilogativa della landing page degli avvisi.

In questi campi è possibile fornire note, collegamenti o procedure per correggere o risolvere in altro modo l'avviso.



Salvare il monitor

1. Se lo si desidera, è possibile aggiungere una descrizione del monitor.
2. Assegnare un nome significativo al monitor e fare clic su **Save** (Salva).

   Il nuovo monitor viene aggiunto all'elenco dei monitor attivi.

Elenco monitor

La pagina Monitor elenca i monitor attualmente configurati, mostrando quanto segue:

- Nome monitor
- Stato
- Oggetto/metrica monitorati
- Condizioni del monitor

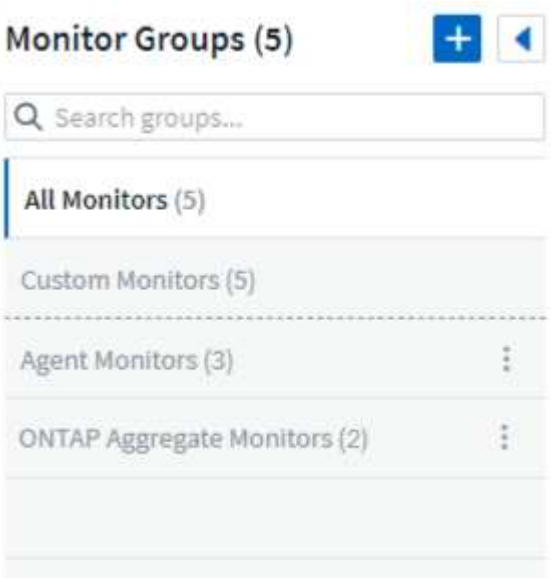
È possibile scegliere di sospendere temporaneamente il monitoraggio di un tipo di oggetto facendo clic sul menu a destra del monitor e selezionando **Pause** (Pausa). Quando si è pronti per riprendere il monitoraggio, fare clic su **Riprendi**.

È possibile copiare un monitor selezionando **Duplica** dal menu. È quindi possibile modificare il nuovo monitor e modificare oggetto/metrica, filtro, condizioni, destinatari e-mail, ecc.

Se un monitor non è più necessario, è possibile eliminarlo selezionando **Delete** (Elimina) dal menu.

Gruppi di monitor

Il raggruppamento consente di visualizzare e gestire i monitor correlati. Ad esempio, è possibile disporre di un gruppo di monitor dedicato allo storage nell'ambiente o di monitoraggi relativi a un determinato elenco di destinatari.



Vengono visualizzati i seguenti gruppi di monitor. Il numero di monitor contenuti in un gruppo viene visualizzato accanto al nome del gruppo.

- **Tutti i monitor** elenca tutti i monitor.
- **Custom Monitor** elenca tutti i monitor creati dall'utente.
- **I monitor sospesi** elencano tutti i monitor di sistema sospesi da Cloud Insights.
- Cloud Insights visualizza inoltre una serie di **gruppi di monitor di sistema**, che elenranno uno o più gruppi di "monitor definiti dal sistema", Inclusi i monitor per l'infrastruttura e il carico di lavoro ONTAP.

I monitor personalizzati possono essere messi in pausa, ripristinati, cancellati o spostati in un altro gruppo. I monitor definiti dal sistema possono essere messi in pausa e ripristinati, ma non possono essere cancellati o spostati.

Monitor sospesi

Questo gruppo viene visualizzato solo se Cloud Insights ha sospeso uno o più monitor. Un monitor potrebbe essere sospeso se genera avvisi eccessivi o continui. Se si tratta di un monitor personalizzato, modificare le condizioni per evitare l'invio di avvisi continui, quindi riprendere il monitor. Il monitor viene rimosso dal gruppo di monitor sospesi quando il problema che causa la sospensione viene risolto.

Monitor definiti dal sistema

Questi gruppi mostrano i monitor forniti da Cloud Insights, a condizione che l'ambiente contenga i dispositivi e/o la disponibilità dei log richiesti dai monitor.

I monitor definiti dal sistema non possono essere modificati, spostati in un altro gruppo o cancellati. Tuttavia, è possibile duplicare un monitor di sistema e modificare o spostare il duplicato.

I monitor di sistema possono includere monitor per l'infrastruttura ONTAP (storage, volume, ecc.) o carichi di lavoro (ad esempio, monitor di log) o altri gruppi. NetApp sta valutando costantemente le esigenze dei clienti e le funzionalità dei prodotti e aggiornerà o aggiungerà i monitor e i gruppi di sistema in base alle esigenze.

Gruppi di monitor personalizzati

È possibile creare gruppi personalizzati per contenere i monitor in base alle proprie esigenze. Ad esempio, potrebbe essere necessario un gruppo per tutti i monitor relativi allo storage.

Per creare un nuovo gruppo di monitor personalizzato, fare clic sul pulsante **"+" Create New Monitor Group** (Crea nuovo gruppo di monitor). Immettere un nome per il gruppo e fare clic su **Create Group** (Crea gruppo). Viene creato un gruppo vuoto con tale nome.

Per aggiungere monitor al gruppo, passare al gruppo *All Monitors* (consigliato) ed eseguire una delle seguenti operazioni:

- Per aggiungere un singolo monitor, fare clic sul menu a destra del monitor e selezionare *Add to Group* (Aggiungi al gruppo). Scegliere il gruppo a cui aggiungere il monitor.
- Fare clic sul nome del monitor per aprire la vista di modifica del monitor e selezionare un gruppo nella sezione *Associa a un gruppo di monitor*.

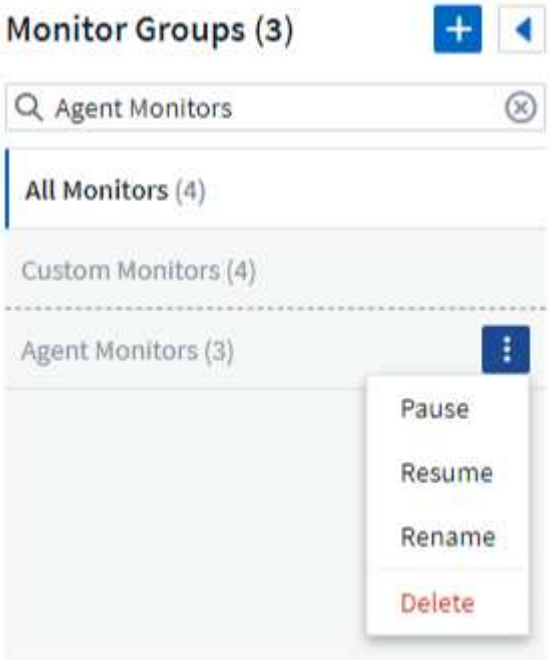
Rimuovere i monitor facendo clic su un gruppo e selezionando *Remove from Group* dal menu. Non è possibile rimuovere i monitor dal gruppo *All Monitors* o *Custom Monitors*. Per eliminare un monitor da questi gruppi, è necessario eliminarlo.

La rimozione di un monitor da un gruppo non elimina il monitor da Cloud Insights. Per rimuovere completamente un monitor, selezionarlo e fare clic su *Delete*. In questo modo viene rimosso anche dal gruppo a cui apparteneva e non è più disponibile per nessun utente.

È anche possibile spostare un monitor in un gruppo diverso nello stesso modo, selezionando *Move to Group* (Sposta in gruppo).

Per mettere in pausa o riprendere contemporaneamente tutti i monitor di un gruppo, selezionare il menu del gruppo e fare clic su *Pause* o *Resume*.

Utilizzare lo stesso menu per rinominare o eliminare un gruppo. L'eliminazione di un gruppo non elimina i monitor da Cloud Insights, ma sono ancora disponibili in *tutti i monitor*.



Monitor definiti dal sistema

Cloud Insights include una serie di monitor definiti dal sistema per metriche e registri. I monitor di sistema disponibili dipendono dai data collezions presenti nell'ambiente. Per questo motivo, i monitor disponibili in Cloud Insights potrebbero cambiare in base all'aggiunta di data collezions o alla modifica delle configurazioni.

Visualizzare il "Monitor definiti dal sistema" Per le descrizioni dei monitor inclusi in Cloud Insights.

Ulteriori informazioni

- "Visualizzazione e disattivazione degli avvisi"

Visualizzazione e gestione degli avvisi dai monitor

Cloud Insights visualizza gli avvisi quando "soglie monitorate" vengono superati.

Monitor e avvisi sono disponibili in Cloud Insights Standard Edition e versioni successive.

Visualizzazione e gestione degli avvisi

Per visualizzare e gestire gli avvisi, procedere come segue.

1. Accedere alla pagina **Avvisi > tutti gli avvisi**.
2. Viene visualizzato un elenco dei 1,000 avvisi più recenti. È possibile ordinare questo elenco in qualsiasi campo facendo clic sull'intestazione della colonna corrispondente al campo. L'elenco visualizza le seguenti informazioni. Nota: Non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare facendo clic sull'icona "ingranaggio" :
   - **ID avviso**: ID avviso univoco generato dal sistema
   - **Triggered time** (tempo di attivazione): L'ora in cui il monitor interessato ha attivato l'avviso
   - **Severità corrente** (scheda Avvisi attivi): La severità corrente dell'avviso attivo
   - **Severità massima** (scheda Avvisi risolti); la severità massima dell'avviso prima che sia stato risolto
   - **Monitor**: Il monitor configurato per attivare l'avviso
   - **Triggered on**: L'oggetto in cui è stata violata la soglia monitorata
   - **Status**: Stato corrente degli avvisi, *New* o *in process*
   - **Stato attivo**: *Attivo* o *risolto*
   - **Condizione**: Condizione di soglia che ha attivato l'avviso
   - **Metrico**: La metrica dell'oggetto su cui è stata violata la soglia monitorata
   - **Monitor Status** (Stato monitor): Stato corrente del monitor che ha attivato l'allarme
   - **Ha un'azione correttiva**: L'avviso ha suggerito delle azioni correttive. Aprire la pagina degli avvisi per visualizzarli.

È possibile gestire un avviso facendo clic sul menu a destra dell'avviso e scegliendo una delle seguenti opzioni:

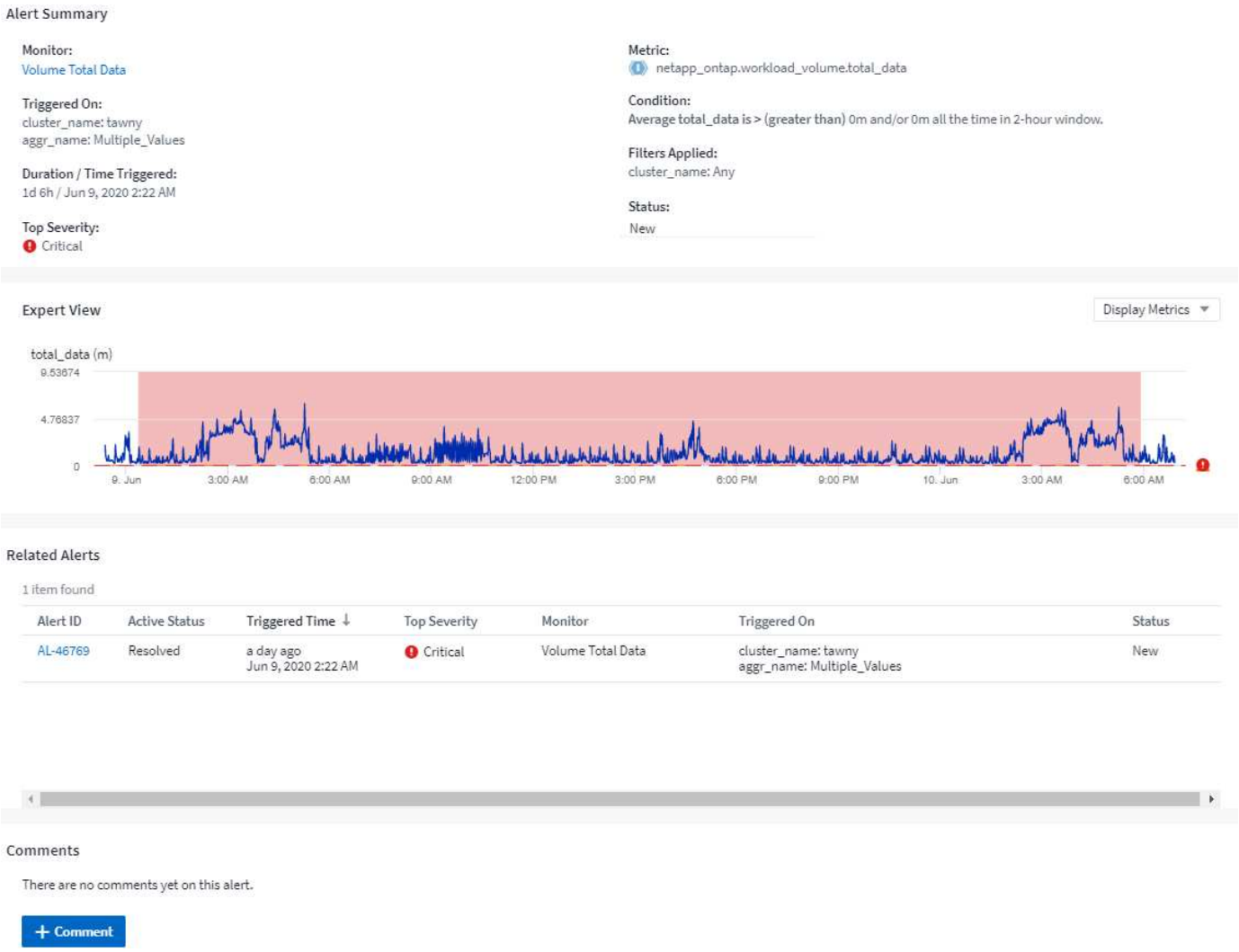
- **In corso** per indicare che l'avviso è in fase di analisi o deve essere mantenuto aperto
- **Chiudi** per rimuovere l'avviso dall'elenco degli avvisi attivi.

È possibile gestire più avvisi selezionando la casella di controllo a sinistra di ciascun avviso e facendo clic su *Change Selected Alerts Status*.

Facendo clic su un ID avviso, viene visualizzata la pagina Dettagli avviso.

Pagina dei dettagli degli avvisi

La pagina dei dettagli degli avvisi fornisce ulteriori dettagli sull'avviso, tra cui un *Riepilogo*, una *visualizzazione avanzata* che mostra i grafici relativi ai dati dell'oggetto, le *risorse correlate* e i *commenti* inseriti dagli investigatori degli avvisi.



Avvisa quando mancano dati

In un sistema in tempo reale come Cloud Insights, per avviare l'analisi di un monitor per decidere se generare un avviso, ci affidiamo a una delle due cose seguenti:

- il prossimo datapoint per arrivare
- un timer da attivare quando non c'è data apoint e hai atteso abbastanza a lungo

Come nel caso di un arrivo lento dei dati, o di un mancato arrivo dei dati, il meccanismo del timer deve assumere il controllo poiché la velocità di arrivo dei dati è insufficiente per attivare gli avvisi in "tempo reale". Quindi, la domanda in genere diventa: "Quanto tempo devo aspettare prima di chiudere la finestra di analisi e guardare quello che ho?" Se si attende troppo a lungo, gli avvisi non vengono generati abbastanza rapidamente da risultare utili.

Se si dispone di un monitor con una finestra di 30 minuti che rileva che una condizione viene violata dall'ultimo data point prima di una perdita di dati a lungo termine, Viene generato un avviso perché il monitor non ha ricevuto altre informazioni da utilizzare per confermare un ripristino della metrica o per notare che la condizione è rimasta.

Avvisi "permanentemente attivi"

È possibile configurare un monitor in modo che la condizione sia **sempre** sull'oggetto monitorato, ad esempio

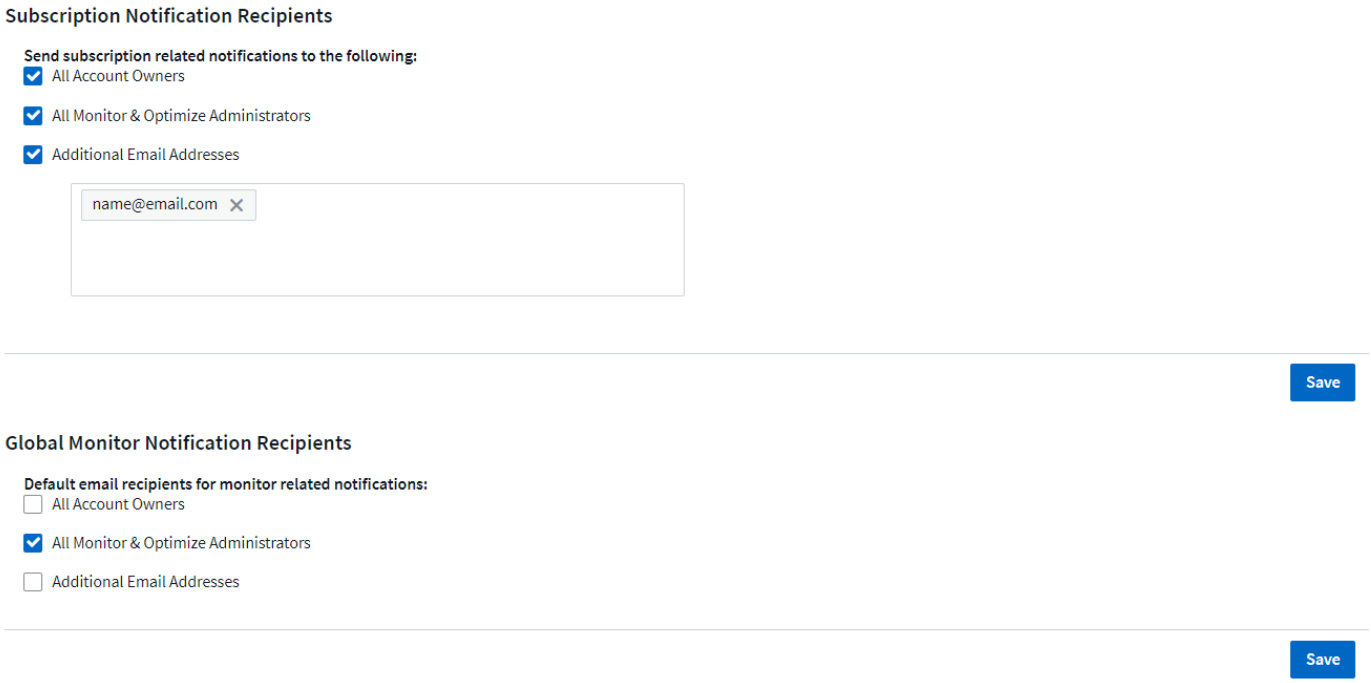
IOPS > 1 o latenza > 0. Questi vengono spesso creati come monitor di "test" e poi dimenticati. Tali monitor creano avvisi che rimangono costantemente aperti sugli oggetti costitutivi, causando problemi di stress e stabilità del sistema nel tempo.

Per evitare questo problema, Cloud Insights chiuderà automaticamente qualsiasi avviso "permanentemente attivo" dopo 7 giorni. Tenere presente che le condizioni di monitoraggio sottostanti potrebbero (probabilmente continueranno) sussistere, causando l'emissione quasi immediata di un nuovo avviso, ma questa chiusura degli avvisi "sempre attivi" riduce alcune delle sollecitazioni del sistema che altrimenti potrebbero verificarsi.

Configurazione delle notifiche e-mail

È possibile configurare un elenco e-mail per le notifiche relative all'abbonamento e un elenco e-mail globale di destinatari per la notifica delle violazioni delle soglie dei criteri di performance.

Per configurare le impostazioni del destinatario della notifica via email, accedere alla pagina **Admin > Notifiche** e selezionare la scheda *Email*.



Destinatari della notifica di abbonamento

Per configurare i destinatari delle notifiche degli eventi relative all'abbonamento, passare alla sezione "destinatari delle notifiche di abbonamento". È possibile scegliere di inviare notifiche via email per gli eventi relativi all'abbonamento a uno o a tutti i seguenti destinatari:

- Tutti i proprietari di account
- Tutti gli amministratori di *monitoraggio e ottimizzazione*
- Indirizzi e-mail aggiuntivi specificati dall'utente

Di seguito sono riportati alcuni esempi dei tipi di notifiche che è possibile inviare e delle azioni dell'utente che è possibile eseguire.

Notifica:	Azione utente:
La versione di prova o l'abbonamento sono stati aggiornati	Consultare i dettagli dell'abbonamento sul "Iscrizione" pagina
L'abbonamento scadrà tra 90 giorni. L'abbonamento scadrà tra 30 giorni	Se l'opzione "rinnovo automatico" è attivata, non è necessaria alcuna azione "Vendite NetApp" per rinnovare l'abbonamento
La prova termina in 2 giorni	Rinnovare la versione di prova di "Iscrizione" pagina. Puoi rinnovare una prova una volta sola. Contatto "Vendite NetApp" per acquistare un abbonamento
La prova o l'abbonamento sono scaduti. L'account interrompe la raccolta dei dati in 48 ore. L'account verrà cancellato dopo 48 ore	Contatto "Vendite NetApp" per acquistare un abbonamento

Elenco globale destinatari per gli avvisi

Le notifiche e-mail degli avvisi vengono inviate all'elenco dei destinatari degli avvisi per ogni azione dell'avviso. È possibile scegliere di inviare notifiche di avviso a un elenco globale di destinatari.

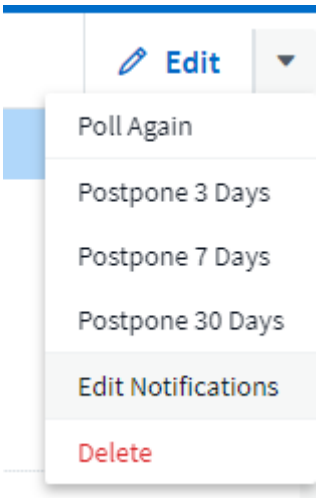
Per configurare i destinatari degli avvisi globali, selezionare i destinatari desiderati nella sezione **destinatari delle notifiche globali di monitoraggio**.

Durante la creazione o la modifica del monitor, è sempre possibile ignorare l'elenco globale dei destinatari di un singolo monitor.

> Le notifiche del Data Collector di ONTAP hanno la precedenza su qualsiasi notifica specifica del Monitor rilevante per il cluster/data collector. L'elenco dei destinatari impostato per Data Collector riceverà gli avvisi di data collector. Se non sono presenti avvisi di data collector attivi, gli avvisi generati dal monitor verranno inviati a destinatari specifici del monitor.

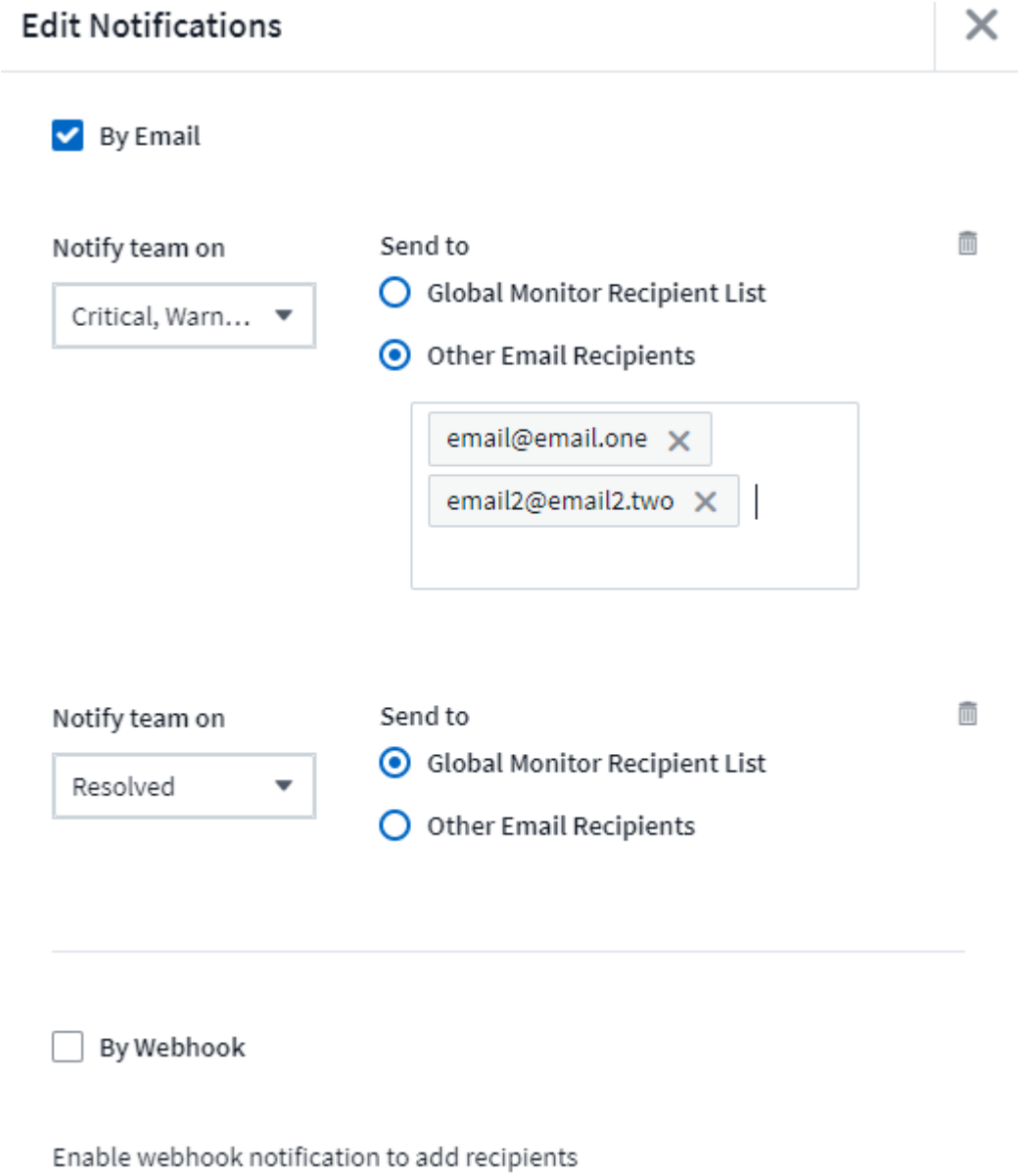
Modifica delle notifiche per ONTAP

Puoi modificare le notifiche per i cluster ONTAP selezionando *Modifica notifiche* dall'elenco a discesa in alto a destra in una landing page dello storage.



Da qui è possibile impostare le notifiche per gli avvisi critici, di avviso, informativi e/o risolti. Ogni scenario può

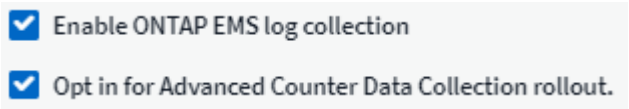
inviare una notifica all'elenco Global Recipient (destinatari globali) o ad altri destinatari scelti.



Monitor di sistema

Cloud Insights include una serie di monitor definiti dal sistema per metriche e registri. I monitor di sistema disponibili dipendono dai data collezions presenti nell'ambiente. Per questo motivo, i monitor disponibili in Cloud Insights potrebbero cambiare in base all'aggiunta di data collezions o alla modifica delle configurazioni.

Per impostazione predefinita, molti monitor di sistema sono in stato di *pausa*. È possibile attivare un monitor di sistema selezionando l'opzione *Riprendi* per il monitor. Assicurarsi che *raccolta dati contatore avanzata* e *attiva raccolta log EMS ONTAP* siano attivati in Data Collector. Queste opzioni sono disponibili nel Data Collector di ONTAP in *Configurazione avanzata*:



Descrizioni dei monitor

I monitor definiti dal sistema comprendono metriche e condizioni predefinite, nonché descrizioni predefinite e azioni correttive, che non possono essere modificate. È possibile modificare l'elenco dei destinatari delle notifiche per i monitor definiti dal sistema. Per visualizzare metriche, condizioni, descrizione e azioni correttive o per modificare l'elenco dei destinatari, aprire un gruppo di monitor definito dal sistema e fare clic sul nome del monitor nell'elenco.

I gruppi di monitor definiti dal sistema non possono essere modificati o rimossi.

I seguenti monitor definiti dal sistema sono disponibili, nei gruppi indicati.

- **L'infrastruttura ONTAP** include i monitor per i problemi relativi all'infrastruttura nei cluster ONTAP.
- **ONTAP workload Examples** include monitor per problemi relativi al carico di lavoro.
- Per impostazione predefinita, i monitor di entrambi i gruppi passano allo stato *Paused*.

Di seguito sono riportati i monitor di sistema attualmente inclusi in Cloud Insights:

Monitor metrici

Nome monitor	Severità	Descrizione del monitor	Azione correttiva

Utilizzo elevato delle porte Fibre Channel	CRITICO	Le porte del protocollo Fibre Channel vengono utilizzate per ricevere e trasferire il traffico SAN tra il sistema host del cliente e i LUN ONTAP. Se l'utilizzo della porta è elevato, In questo modo si trasformerà in un collo di bottiglia che, in ultima analisi, influirà sulle performance dei carichi di lavoro sensibili del protocollo Fibre Channel.…Un avviso indica che è necessario intraprendere un'azione pianificata per bilanciare il traffico di rete.…Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per bilanciare la rete traffico per garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sposta i carichi di lavoro su un'altra porta FCP meno utilizzata. 2. Limitare il traffico di alcune LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP.… In caso di superamento della soglia di avviso, pianificare le seguenti azioni: 1. Configurare più porte FCP per gestire il traffico dati in modo che l'utilizzo delle porte venga distribuito tra più porte. 2. Spostare i carichi di lavoro su un'altra porta FCP meno utilizzata. 3. Limitare il traffico di alcune LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP.

Latenza LUN alta	CRITICO	I LUN sono oggetti che servono il traffico i/o spesso determinato da applicazioni sensibili alle performance, come i database. Un'elevata latenze delle LUN significa che le applicazioni stesse potrebbero subire problemi e non essere in grado di svolgere le proprie attività.…Un avviso indica che è necessario intraprendere un'azione pianificata per spostare la LUN nel nodo o nell'aggregato appropriato.…Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza garantire la continuità del servizio. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi, SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi	In caso di superamento della soglia critica, prendere in considerazione le seguenti azioni per ridurre al minimo l'interruzione del servizio: Se il LUN o il suo volume dispone di una policy di QoS associata, valutare i limiti di soglia e verificare se il carico di lavoro del LUN viene rallentato.… In caso di superamento della soglia di avviso, pianificare le seguenti azioni: 1. Se anche l'aggregato presenta un elevato utilizzo, spostare il LUN in un altro aggregato. 2. Se anche il nodo presenta un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se al LUN o al volume associato è associato un criterio QoS, valutarne i limiti di soglia e verificare se il carico di lavoro del LUN viene rallentato.

Utilizzo della porta di rete elevato	CRITICO	Le porte di rete vengono utilizzate per ricevere e trasferire il traffico dei protocolli NFS, CIFS e iSCSI tra i sistemi host del cliente e i volumi ONTAP. Se l'utilizzo delle porte è elevato, diventa un collo di bottiglia e in ultima analisi influirà sulle prestazioni di NFS, Carichi di lavoro CIFS e iSCSI.…Un avviso indica che è necessario intraprendere un'azione pianificata per bilanciare il traffico di rete.…Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per bilanciare il traffico di rete e garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Limitare il traffico di determinati volumi solo al lavoro essenziale, tramite policy QoS in ONTAP o analisi lato host per ridurre l'utilizzo delle porte di rete. 2. Configurare uno o più volumi per utilizzare un'altra porta di rete meno utilizzata.… In caso di superamento della soglia di avviso, prendere in considerazione le seguenti azioni immediate: 1. Configurare più porte di rete per gestire il traffico dati in modo che l'utilizzo delle porte venga distribuito tra più porte. 2. Configurare uno o più volumi per utilizzare un'altra porta di rete meno utilizzata.

Latenza dello spazio dei nomi NVMe alta	CRITICO	I NVMe Namespace sono oggetti che servono il traffico i/o gestito da applicazioni sensibili alle performance, come i database. Un'elevata latenza NVMe Namespaces significa che le applicazioni stesse potrebbero subire problemi e non essere in grado di svolgere le proprie attività.…Un avviso indica che è necessario intraprendere un'azione pianificata per spostare il LUN nel nodo o nell'aggregato appropriato.…Un avviso critico indica che l'interruzione del servizio è imminente e che devono essere adottate misure di emergenza per garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: Se lo spazio dei nomi NVMe o il suo volume ha assegnato una policy di QoS, valutare le proprie soglie limite nel caso in cui il carico di lavoro dello spazio dei nomi NVMe venga rallentato.… In caso di superamento della soglia di avviso, prendere in considerazione le seguenti azioni: 1. Se anche l'aggregato presenta un elevato utilizzo, spostare il LUN in un altro aggregato. 2. Se anche il nodo presenta un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se lo spazio dei nomi NVMe o il suo volume dispone di un criterio QoS assegnato, valutarne le soglie limite nel caso in cui il carico di lavoro dello spazio dei nomi NVMe venga rallentato.

Capacità qtree piena	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory root all'interno di un volume. Ogni qtree dispone di una quota di spazio predefinita o di una quota definita da una policy di quota per limitare la quantità di dati memorizzati nella struttura all'interno della capacità del volume.…Un avviso indica che è necessario intraprendere un'azione pianificata per aumentare lo spazio.…Un avviso critico indica che l'interruzione del servizio è imminente e è necessario adottare misure di emergenza per liberare spazio e garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del qtree per adattarlo alla crescita. 2. Elimina i dati indesiderati per liberare spazio.… In caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare lo spazio del qtree per adattarlo alla crescita. 2. Eliminare i dati indesiderati per liberare spazio.
Limite massimo capacità qtree	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory root all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che viene utilizzata per memorizzare i dati al fine di controllare la crescita dei dati utente nel volume e non superare la capacità totale.…Un qtree mantiene una quota di capacità di storage soft che fornisce un avviso proattivo all'utente prima di raggiungere il totale limite di quota di capacità nel qtree e impossibilità di memorizzare più i dati. Il monitoraggio della quantità di dati memorizzati all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota di spazio dell'albero per adattarla alla crescita 2. Chiedere all'utente di eliminare i dati indesiderati nell'albero per liberare spazio

Limite soft capacità qtree	ATTENZIONE	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory root all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che può utilizzare per memorizzare i dati al fine di controllare la crescita dei dati utente nel volume e non superare la capacità totale.…Un qtree mantiene una quota di capacità di storage soft che fornisce un avviso proattivo all'utente prima di raggiungere il limite di quota della capacità totale nel qtree e impossibilità di memorizzare più i dati. Il monitoraggio della quantità di dati memorizzati all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di superamento della soglia di avviso, prendere in considerazione le seguenti azioni immediate: 1. Aumentare la quota di spazio dell'albero per adattarla alla crescita. 2. Chiedere all'utente di eliminare i dati indesiderati nell'albero per liberare spazio.
Limite massimo dei file qtree	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory root all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione del file system gestibile all'interno del volume.…Un qtree mantiene una quota del numero di file rigidi oltre la quale i nuovi file nell'albero vengono rifiutati. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota del numero di file per il qtree. 2. Eliminare i file indesiderati dal file system qtree.

Limite di software dei file qtree	ATTENZIONE	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory root all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione del file system gestibile all'interno del volume.…Un qtree mantiene una quota del numero di file soft per fornire un avviso proattivo all'utente prima di raggiungere il limite di file nel qtree e. impossibile memorizzare altri file. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare la quota del numero di file per il qtree. 2. Eliminare i file indesiderati dal file system qtree.

Spazio riserva Snapshot pieno	CRITICO	La capacità di storage di un volume è necessaria per memorizzare i dati delle applicazioni e dei clienti. Una parte di tale spazio, denominata spazio riservato di snapshot, viene utilizzata per memorizzare le snapshot che consentono la protezione dei dati localmente. Maggiore è il numero di dati nuovi e aggiornati memorizzati nel volume ONTAP, maggiore sarà la capacità di snapshot utilizzata e minore sarà la capacità di storage di snapshot disponibile per i dati nuovi o aggiornati in futuro. Se la capacità dei dati di snapshot all'interno di un volume raggiunge lo spazio totale di riserva di snapshot, il cliente potrebbe non essere in grado di memorizzare nuovi dati di snapshot e ridurre il livello di protezione dei dati nel volume. Il monitoraggio della capacità di snapshot del volume utilizzato garantisce la continuità dei servizi dati.	In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare le snapshot in modo che utilizzino lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Eliminare alcune istantanee indesiderate meno recenti per liberare spazio.… In caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare lo spazio di riserva snapshot all'interno del volume per adattarlo alla crescita. 2. Configurare le snapshot in modo che utilizzino lo spazio dati nel volume quando la riserva di snapshot è piena.

Limite di capacità dello storage	CRITICO	Quando un pool di storage (aggregato) si sta riempiendo, le operazioni di i/o rallentano e finiscono per cessare, causando incidenti di disservizio dello storage. Un avviso indica che è necessario intraprendere presto un'azione pianificata per ripristinare lo spazio libero minimo. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per liberare spazio e garantire la continuità del servizio.	In caso di violazione della soglia critica, considerare immediatamente le seguenti azioni per ridurre al minimo l'interruzione del servizio: 1. Eliminare le istantanee su volumi non critici. 2. Eliminare i volumi o le LUN che sono carichi di lavoro non essenziali e che possono essere ripristinati dalle copie fuori dallo storage.……se la soglia di avviso viene violata, pianificare le seguenti azioni immediate: 1. Spostare uno o più volumi in una posizione di storage diversa. 2. Aggiungere ulteriore capacità di storage. 3. Modifica le impostazioni di efficienza dello storage o i dati inattivi di Tier nello storage cloud.

Limite di performance dello storage	CRITICO	Quando un sistema storage raggiunge il limite di performance, le operazioni rallentano, aumenta la latenza e i carichi di lavoro e le applicazioni potrebbero iniziare a guastarsi. ONTAP valuta l'utilizzo del pool di storage per i carichi di lavoro e stima la percentuale di performance consumata.…Un avviso indica che è necessario intraprendere un'azione pianificata per ridurre il carico del pool di storage per garantire che le performance del pool di storage siano sufficienti per gestire i picchi dei carichi di lavoro.…Un avviso critico indica che è imminente una ricerca delle performance e devono essere adottate misure di emergenza per ridurre il carico del pool di storage e garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate, ad esempio le snapshot o la replica di SnapMirror. 2. Carichi di lavoro non essenziali inattivi.… In caso di superamento della soglia di avviso, eseguire immediatamente le seguenti operazioni: 1. Spostare uno o più carichi di lavoro in un'altra posizione di storage. 2. Aggiungere altri nodi storage (AFF) o shelf di dischi (FAS) e ridistribuire i carichi di lavoro 3. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, caching dell'applicazione).

Limite massimo capacità quota utente	CRITICO	ONTAP riconosce gli utenti di sistemi Unix o Windows che dispongono dei diritti di accesso a volumi, file o directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di storage per i propri utenti o gruppi di utenti dei sistemi Linux o Windows. La quota della policy di gruppo o dell'utente limita la quantità di spazio che l'utente può utilizzare per i propri dati.…Un limite massimo di questa quota consente di notificare all'utente quando la quantità di capacità utilizzata all'interno del volume è corretta prima di raggiungere la quota di capacità totale. Il monitoraggio della quantità di dati memorizzati all'interno di una quota utente o di gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio della quota di utenti o gruppi per adattarsi alla crescita. 2. Chiedere all'utente o al gruppo di eliminare i dati indesiderati per liberare spazio.

Limite soft capacità quota utente	ATTENZIONE	ONTAP riconosce gli utenti di sistemi Unix o Windows che dispongono dei diritti di accesso a volumi, file o directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di storage per i propri utenti o gruppi di utenti dei sistemi Linux o Windows. La quota della policy di gruppo o dell'utente limita la quantità di spazio che l'utente può utilizzare per i propri dati.…Un limite minimo di questa quota consente una notifica proattiva all'utente quando la quantità di capacità utilizzata all'interno del volume raggiunge la quota di capacità totale. Il monitoraggio della quantità di dati memorizzati all'interno di una quota utente o di gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare lo spazio della quota di utenti o gruppi per adattarsi alla crescita. 2. Eliminare i dati indesiderati per liberare spazio.

Capacità del volume piena	CRITICO	La capacità di storage di un volume è necessaria per memorizzare i dati delle applicazioni e dei clienti. Maggiore è il numero di dati memorizzati nel volume ONTAP, minore sarà la disponibilità dello storage per i dati futuri. Se la capacità di storage dei dati all'interno di un volume raggiunge la capacità di storage totale, il cliente potrebbe non essere in grado di memorizzare i dati a causa della mancanza di capacità di storage. Il monitoraggio della capacità di storage utilizzata per il volume garantisce la continuità dei servizi dati.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume per adattarlo alla crescita. 2. Eliminare i dati indesiderati per liberare spazio. 3. Se le copie Snapshot occupano più spazio della riserva di snapshot, eliminare le snapshot precedenti o attivare l'eliminazione automatica di Volume Snapshot.…se la soglia di avviso viene superata, pianificare le seguenti azioni immediate: 1. Aumentare lo spazio del volume per adattarlo alla crescita 2. Se le copie Snapshot occupano più spazio rispetto alla riserva di snapshot, eliminare le istantanee precedenti o attivare l'eliminazione automatica di Volume Snapshot.……

Volume Inode Limit (limite nodi volume	CRITICO	I volumi che memorizzano i file utilizzano i nodi indice (inode) per memorizzare i metadati dei file. Quando un volume esaurisce la propria allocazione inode, Non è possibile aggiungere altri file.…Un avviso indica che è necessario intraprendere un'azione pianificata per aumentare il numero di inode disponibili.…Un avviso critico indica che l'esaurimento del limite di file è imminente e che è necessario adottare misure di emergenza per liberare inode per garantire la continuità del servizio.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare il valore degli inode per il volume. Se il valore inode è già al valore massimo, suddividere il volume in due o più volumi perché il file system è cresciuto oltre le dimensioni massime. 2. Utilizza FlexGroup per supportare file system di grandi dimensioni.… In caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, suddividere il volume in due o più volumi perché il file system è cresciuto oltre le dimensioni massime. 2. Utilizza FlexGroup per supportare file system di grandi dimensioni

Latenza del volume elevata	CRITICO	I volumi sono oggetti che servono il traffico i/o spesso determinato da applicazioni sensibili alle performance, tra cui applicazioni DevOps, home directory e database. L'elevata latenze dei volumi implica che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Il monitoraggio delle latenze dei volumi è fondamentale per mantenere performance coerenti con le applicazioni. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	In caso di violazione della soglia critica, prendere in considerazione le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: Se al volume è stata assegnata una policy di QoS, valutare le soglie limite nel caso in cui il carico di lavoro del volume venga rallentato.… In caso di superamento della soglia di avviso, prendere in considerazione le seguenti azioni immediate: 1. Se anche l'aggregato presenta un elevato utilizzo, spostare il volume su un altro aggregato. 2. Se al volume è stato assegnato un criterio QoS, valutarne le soglie limite nel caso in cui il carico di lavoro del volume venga rallentato. 3. Se anche il nodo presenta un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.
Nome monitor	Severità	Descrizione del monitor	Azione correttiva

Nodo a latenza elevata	ATTENZIONE / CRITICO	La latenza del nodo ha raggiunto i livelli in cui potrebbe influire sulle prestazioni delle applicazioni sul nodo. Una latenza dei nodi inferiore garantisce performance costanti delle applicazioni. Le latenze previste in base al tipo di supporto sono: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	In caso di violazione della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate, le snapshot o la replica di SnapMirror 2. Ridurre la domanda di carichi di lavoro con priorità inferiore attraverso i limiti di QoS 3. Inattivare i carichi di lavoro non essenziali considerare azioni immediate in caso di superamento della soglia di avviso: 1. Spostamento di uno o più carichi di lavoro in un'altra posizione di storage 2. Ridurre la domanda di carichi di lavoro con priorità inferiore attraverso i limiti di QoS 3. Aggiungi altri nodi di storage (AFF) o shelf di dischi (FAS) e ridistribuisci i carichi di lavoro 4. Modifica delle caratteristiche del carico di lavoro (dimensioni del blocco, caching delle applicazioni, ecc.)

Limite di performance del nodo	ATTENZIONE / CRITICO	L'utilizzo delle performance dei nodi ha raggiunto i livelli in cui potrebbe influire sulle performance di iOS e delle applicazioni supportate dal nodo. Un basso utilizzo delle performance dei nodi garantisce performance costanti delle applicazioni.	In caso di superamento della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate, le snapshot o la replica di SnapMirror 2. Ridurre la domanda di carichi di lavoro con priorità inferiore attraverso i limiti di QoS 3. Disattivare i carichi di lavoro non essenziali considerare le seguenti azioni in caso di superamento della soglia di avviso: 1. Spostamento di uno o più carichi di lavoro in un'altra posizione di storage 2. Ridurre la domanda di carichi di lavoro con priorità inferiore attraverso i limiti di QoS 3. Aggiungi altri nodi storage (AFF) o shelf di dischi (FAS) e ridistribuisci i carichi di lavoro 4. Modifica delle caratteristiche del carico di lavoro (dimensioni del blocco, caching delle applicazioni, ecc.)

Storage VM elevata latenza	ATTENZIONE / CRITICO	La latenza delle macchine virtuali dello storage (SVM) ha raggiunto i livelli in cui potrebbe influire sulle prestazioni delle applicazioni sulla macchina virtuale dello storage. La minore latenza delle macchine virtuali dello storage garantisce performance costanti delle applicazioni. Le latenze previste in base al tipo di supporto sono: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	In caso di violazione della soglia critica, valutare immediatamente i limiti di soglia per i volumi della VM di storage con un criterio QoS assegnato, per verificare se i carichi di lavoro del volume vengono rallentati, prendere in considerazione la possibilità di seguire azioni immediate in caso di violazione della soglia di avviso: 1. Se anche l'aggregato presenta un elevato utilizzo, spostare alcuni volumi della VM di storage in un altro aggregato. 2. Per i volumi della VM di storage con una policy di QoS assegnata, valutare i limiti di soglia se causano la riduzione dei carichi di lavoro del volume 3. Se il nodo presenta un utilizzo elevato, spostare alcuni volumi della VM di storage in un altro nodo o ridurre il carico di lavoro totale del nodo
Limite massimo dei file di quota utente	CRITICO	Il numero di file creati all'interno del volume ha raggiunto il limite critico e non è possibile creare altri file. Il monitoraggio del numero di file memorizzati garantisce che l'utente riceva un servizio dati ininterrotto.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica….prendere in considerazione le seguenti azioni: 1. Aumentare la quota del numero di file per l'utente specifico 2. Eliminare i file indesiderati per ridurre la pressione sulla quota dei file per l'utente specifico

Limite minimo file quota utente	ATTENZIONE	Il numero di file creati all'interno del volume ha raggiunto il limite di soglia della quota ed è prossimo al limite critico. Non è possibile creare file aggiuntivi se la quota raggiunge il limite critico. Il monitoraggio del numero di file memorizzati da un utente garantisce che l'utente riceva un servizio dati ininterrotto.	Prendere in considerazione azioni immediate in caso di superamento della soglia di avviso: 1. Aumentare la quota del numero di file per la quota utente specifica 2. Eliminare i file indesiderati per ridurre la pressione sulla quota dei file per l'utente specifico

Rapporto errori cache volume	ATTENZIONE / CRITICO	Volume cache Miss ratio (rapporto errori cache volume) è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco invece di essere restituite dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	In caso di violazione della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro fuori dal nodo del volume per ridurre il carico di i/o 2. Se non si trova già nel nodo del volume, aumentare la cache WAFL acquistando e aggiungendo una Flash cache 3. Ridurre la richiesta di carichi di lavoro con priorità inferiore sullo stesso nodo tramite i limiti di QoS considerare azioni immediate in caso di superamento della soglia di avviso: 1. Spostare alcuni carichi di lavoro fuori dal nodo del volume per ridurre il carico di i/o 2. Se non si trova già nel nodo del volume, aumentare la cache WAFL acquistando e aggiungendo una Flash cache 3. Ridurre la domanda di carichi di lavoro con priorità inferiore sullo stesso nodo tramite i limiti di QoS 4. Modifica delle caratteristiche del carico di lavoro (dimensioni del blocco, caching delle applicazioni, ecc.)

Overcommit quota Qtree volume	ATTENZIONE / CRITICO	Volume Qtree quota Overcommit specifica la percentuale in cui un volume viene considerato overcommit dalle quote del qtree. La soglia impostata per la quota qtree viene raggiunta per il volume. Il monitoraggio dell'overcommit della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di violazione della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume 2. Eliminare i dati indesiderati in caso di superamento della soglia di avviso, quindi considerare l'aumento dello spazio del volume.

Torna all'inizio

Log Monitor

Nome monitor	Severità	Descrizione	Azione correttiva
Credenziali AWS non inizializzate	INFO	Questo evento si verifica quando un modulo tenta di accedere alle credenziali Amazon Web Services (AWS) Identity and Access Management (IAM) basate sul ruolo dal thread delle credenziali cloud prima che vengano inizializzate.	Attendere che il thread delle credenziali cloud e il sistema completino l'inizializzazione.

Livello cloud non raggiungibile	CRITICO	Un nodo storage non può connettersi all'API dell'archivio di oggetti Cloud Tier. Alcuni dati non saranno accessibili.	Se si utilizzano prodotti on-premise, eseguire le seguenti azioni correttive: …Verificare che la LIF dell'intercluster sia in linea e funzionante utilizzando il comando "network interface show"….verificare la connettività di rete con il server dell'archivio oggetti utilizzando il comando "ping" sul LIF dell'intercluster del nodo di destinazione.…verificare quanto segue:…la configurazione dell'archivio oggetti non è stata modificata.…le informazioni di accesso e connettività sono disponibili Ancora valido.…se il problema persiste, contattare il supporto tecnico NetApp. Se si utilizza Cloud Volumes ONTAP, eseguire le seguenti azioni correttive: …Assicurarsi che la configurazione dell'archivio di oggetti non sia stata modificata.… Assicurarsi che le informazioni di accesso e di connettività siano ancora valide.…se il problema persiste, contattare il supporto tecnico NetApp.
Disco fuori servizio	INFO	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come non riuscito, viene sanificato o è entrato nel Centro di manutenzione.	Nessuno.

FlexGroup costituente completo	CRITICO	Un componente all'interno di un volume FlexGroup è pieno, il che potrebbe causare un'interruzione del servizio. È comunque possibile creare o espandere i file sul volume FlexGroup. Tuttavia, nessuno dei file memorizzati nel costituente può essere modificato. Di conseguenza, quando si tenta di eseguire operazioni di scrittura sul volume FlexGroup, potrebbero verificarsi errori casuali di spazio insufficiente.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -Files +X"….in alternativa, eliminare i file dal volume FlexGroup. Tuttavia, è difficile determinare quali archivi sono stati depositati sul costituente.
Costituente FlexGroup quasi pieno	ATTENZIONE	Un componente all'interno di un volume FlexGroup è quasi esaurito, il che potrebbe causare una potenziale interruzione del servizio. I file possono essere creati ed espansi. Tuttavia, se il costituente esaurisce lo spazio, potrebbe non essere possibile aggiungere o modificare i file sul costituente.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -Files +X"….in alternativa, eliminare i file dal volume FlexGroup. Tuttavia, è difficile determinare quali archivi sono stati depositati sul costituente.
Costituente FlexGroup quasi fuori dagli nodi	ATTENZIONE	Un componente all'interno di un volume FlexGroup è quasi fuori dagli inode, il che potrebbe causare una potenziale interruzione del servizio. Il costituente riceve richieste di creazione inferiori alla media. Ciò potrebbe influire sulle prestazioni complessive del volume FlexGroup, in quanto le richieste vengono instradate ai componenti con più inode.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -Files +X"….in alternativa, eliminare i file dal volume FlexGroup. Tuttavia, è difficile determinare quali archivi sono stati depositati sul costituente.

Costituente FlexGroup fuori dagli nodi	CRITICO	Un componente di un volume FlexGroup ha esaurito gli inode, il che potrebbe causare una potenziale interruzione del servizio. Non è possibile creare nuovi file su questo costituente. Questo potrebbe portare a una distribuzione generale del contenuto sbilanciata nel volume FlexGroup.	Si consiglia di aggiungere capacità al volume FlexGroup utilizzando il comando "volume modify -Files +X".…in alternativa, eliminare i file dal volume FlexGroup. Tuttavia, è difficile determinare quali archivi sono stati depositati sul costituente.
LUN non in linea	INFO	Questo evento si verifica quando un LUN viene portato offline manualmente.	Riportare il LUN in linea.
Ventola dell'unità principale non riuscita	ATTENZIONE	Una o più ventole dell'unità principale si sono guaste. Il sistema rimane operativo.…tuttavia, se la condizione persiste per troppo tempo, la sovratemperatura potrebbe attivare un arresto automatico.	Riposizionare le ventole guaste. Se l'errore persiste, sostituirli.
Ventola dell'unità principale in stato di avviso	INFO	Questo evento si verifica quando una o più ventole dell'unità principale sono in stato di avviso.	Sostituire le ventole indicate per evitare il surriscaldamento.

Batteria NVRAM scarica	ATTENZIONE	La capacità della batteria NVRAM è molto bassa. Potrebbe verificarsi una potenziale perdita di dati se la batteria si esaurisce.…il sistema genera e trasmette un messaggio AutoSupport o "call home" al supporto tecnico NetApp e alle destinazioni configurate, se configurate. La corretta consegna di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Eseguire le seguenti azioni correttive:…visualizzare lo stato corrente, la capacità e lo stato di carica della batteria utilizzando il comando "System node environment sensors show" (Mostra sensori ambiente nodo sistema).…se la batteria è stata sostituita di recente o il sistema non è stato operativo per un periodo di tempo prolungato, Monitorare la batteria per verificare che si stia caricando correttamente.…contattare il supporto tecnico NetApp se il runtime della batteria continua a scendere al di sotto dei livelli critici e il sistema di storage si spegne automaticamente.

Service Processor non configurato	ATTENZIONE	Questo evento si verifica ogni settimana, per ricordare di configurare il Service Processor (SP). SP è un dispositivo fisico incorporato nel sistema per fornire accesso remoto e funzionalità di gestione remota. È necessario configurare l'SP in modo che utilizzi tutte le funzionalità.	Eseguire le seguenti azioni correttive:…configurare l'SP utilizzando il comando "modifica rete del processore di servizio del sistema".…facoltativamente, Ottenere l'indirizzo MAC dell'SP utilizzando il comando "system service processor network show" (visualizzazione rete del processore di servizio del sistema).…verificare la configurazione della rete SP utilizzando il comando "system service-processor network show" (visualizzazione rete del processore di servizio del sistema).…verificare che l'SP possa inviare un'e-mail AutoSupport utilizzando il comando "system service-processor AutoSupport invoke". NOTA: Gli host e i destinatari di posta elettronica AutoSupport devono essere configurati in ONTAP prima di eseguire questo comando.
Service Processor offline	CRITICO	ONTAP non riceve più heartbeat dal Service Processor (SP), anche se sono state eseguite tutte le azioni di ripristino SP. ONTAP non è in grado di monitorare lo stato dell'hardware senza SP.…il sistema si spegne per evitare danni all'hardware e perdita di dati. Impostare un avviso critico per ricevere una notifica immediata se l'SP passa offline.	Spegnere e riaccendere il sistema eseguendo le seguenti operazioni:…estrarre il controller dal telaio.…reinserire il controller.…riaccendere il controller.…se il problema persiste, sostituire il modulo controller.

Ventole dello shelf non riuscite	CRITICO	Si è verificato un guasto nella ventola di raffreddamento indicata o nel modulo della ventola dello shelf. I dischi nello shelf potrebbero non ricevere un flusso d'aria di raffreddamento sufficiente, il che potrebbe causare un guasto al disco.	Eseguire le seguenti azioni correttive:…verificare che il modulo della ventola sia inserito e fissato correttamente. NOTA: La ventola è integrata nel modulo di alimentazione in alcuni shelf di dischi.…se il problema persiste, sostituire il modulo della ventola.…se il problema persiste, contattare il supporto tecnico NetApp per assistenza.
Il sistema non funziona a causa di un guasto alla ventola dell'unità principale	CRITICO	Una o più ventole dell'unità principale si sono guastate, interrompendo il funzionamento del sistema. Ciò potrebbe causare una potenziale perdita di dati.	Sostituire le ventole guaste.
Dischi non assegnati	INFO	Il sistema dispone di dischi non assegnati: La capacità viene sprecata e il sistema potrebbe presentare modifiche di configurazione errate o parziali.	Eseguire le seguenti azioni correttive:…determinare quali dischi non sono assegnati utilizzando il comando "disk show -n".…assegnare i dischi a un sistema utilizzando il comando "disk assign".
Server antivirus occupato	ATTENZIONE	Il server antivirus è troppo occupato per accettare nuove richieste di scansione.	Se questo messaggio viene visualizzato frequentemente, assicurarsi che siano presenti server antivirus sufficienti per gestire il carico di scansione del virus generato dalla SVM.

Credenziali AWS per il ruolo IAM scadute	CRITICO	Cloud Volume ONTAP è diventato inaccessibile. Le credenziali basate sul ruolo di Identity and Access Management (IAM) sono scadute. Le credenziali vengono acquisite dal server di metadati AWS (Amazon Web Services) utilizzando il ruolo IAM e vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3).	Eseguire le seguenti operazioni:…accedere alla console di gestione di AWS EC2.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e controllarne l'integrità.…verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.
Credenziali AWS per il ruolo IAM non trovate	CRITICO	Il thread delle credenziali cloud non può acquisire le credenziali Amazon Web Services (AWS) Identity and Access Management (IAM) basate sul ruolo dal server di metadati AWS. Le credenziali vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.…	Eseguire le seguenti operazioni:…accedere alla console di gestione di AWS EC2.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e controllarne l'integrità.…verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.
Credenziali AWS per il ruolo IAM non valide	CRITICO	Le credenziali basate sul ruolo di Identity and Access Management (IAM) non sono valide. Le credenziali vengono acquisite dal server di metadati AWS (Amazon Web Services) utilizzando il ruolo IAM e vengono utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…accedere alla console di gestione di AWS EC2.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e controllarne l'integrità.…verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.

Ruolo AWS IAM non trovato	CRITICO	Il thread dei ruoli di Identity and Access Management (IAM) non riesce a trovare un ruolo IAM Amazon Web Services (AWS) sul server di metadati AWS. Il ruolo IAM è necessario per acquisire le credenziali basate sul ruolo utilizzate per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.…	Eseguire le seguenti operazioni:…accedere alla console di gestione di AWS EC2.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e controllarne lo stato.…verificare che il ruolo di AWS IAM associato all'istanza sia valido.
Ruolo AWS IAM non valido	CRITICO	Il ruolo Amazon Web Services (AWS) Identity and Access Management (IAM) sul server di metadati AWS non è valido. Il Cloud Volume ONTAP è diventato inaccessibile.…	Eseguire le seguenti operazioni:…accedere alla console di gestione di AWS EC2.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e controllarne l'integrità.…verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.
Connessione server metadati AWS non riuscita	CRITICO	Il thread dei ruoli IAM (Identity and Access Management) non può stabilire un collegamento di comunicazione con il server di metadati AWS (Amazon Web Services). È necessario stabilire una comunicazione per acquisire le credenziali AWS IAM in base al ruolo necessarie per firmare le richieste API ad Amazon Simple Storage Service (Amazon S3). Cloud Volume ONTAP è diventato inaccessibile.…	Eseguire le seguenti operazioni:…accedere alla console di gestione EC2 di AWS.…accedere alla pagina delle istanze.…individuare l'istanza per l'implementazione di Cloud Volumes ONTAP e verificarne lo stato.…

Limite di utilizzo dello spazio FabricPool quasi raggiunto	ATTENZIONE	L'utilizzo totale dello spazio FabricPool a livello di cluster degli archivi di oggetti da parte di provider con licenza di capacità ha quasi raggiunto il limite concesso in licenza.	Eseguire le seguenti azioni correttive:…controllare la percentuale della capacità concessa in licenza utilizzata da ciascun livello di storage FabricPool utilizzando il comando "storage aggregate object-store show-space".…eliminare le copie Snapshot dai volumi con la policy di tiering "snapshot" o "backup" utilizzando il comando "volume snapshot delete" per liberare spazio.…installare una nuova licenza sul cluster per aumentare la capacità concessa in licenza.
Limite di utilizzo dello spazio FabricPool raggiunto	CRITICO	L'utilizzo totale dello spazio FabricPool a livello di cluster degli archivi di oggetti dei provider con licenza di capacità ha raggiunto il limite di licenza.	Eseguire le seguenti azioni correttive:…controllare la percentuale della capacità concessa in licenza utilizzata da ciascun livello di storage FabricPool utilizzando il comando "storage aggregate object-store show-space".…eliminare le copie Snapshot dai volumi con la policy di tiering "snapshot" o "backup" utilizzando il comando "volume snapshot delete" per liberare spazio.…installare una nuova licenza sul cluster per aumentare la capacità concessa in licenza.

Giveback dell’aggregato non riuscito	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover dello storage (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive:…verificare che la LIF dell’intercluster sia online e funzionante utilizzando il comando "network interface show"….verificare la connettività di rete al server dell’archivio oggetti utilizzando il comando"'ping" sul LIF dell’intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio di oggetti non sia stata modificata e che le informazioni di accesso e connettività siano ancora accurate utilizzando il comando "aggregate object-store config show"….in alternativa, È possibile ignorare l’errore specificando false per il parametro "richiede-partner-in attesa" del comando giveback.…contattare il supporto tecnico NetApp per ulteriori informazioni o assistenza.

Interconnessione HA non disponibile	ATTENZIONE	L’interconnessione ad alta disponibilità (ha) non è disponibile. Rischio di interruzione del servizio quando il failover non è disponibile.	Le azioni correttive dipendono dal numero e dal tipo di collegamenti di interconnessione ha supportati dalla piattaforma, nonché dal motivo per cui l’interconnessione è inattiva. …Se i collegamenti non sono attivi:…verificare che entrambi i controller della coppia ha siano funzionanti.…per i collegamenti esterni, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i Small Form-Factor pluggable (SFP), se presenti, siano posizionati correttamente su entrambi i controller.…per i collegamenti interni, disattivare e riattivare i collegamenti, uno dopo l’altro, utilizzando i comandi "ic link off" (collegamento ic disattivato) e "ic link on" (collegamento ic attivato). …Se i collegamenti sono disattivati, abilitarlo usando il comando "ic link on". …Se un peer non è connesso, disattivare e riattivare i collegamenti, uno dopo l’altro, utilizzando i comandi "ic link Off" (collegamento ic disattivato) e "ic link on" (collegamento ic attivato).…se il problema persiste, contattare il supporto tecnico NetApp.

Numero massimo di sessioni per utente superato	ATTENZIONE	È stato superato il numero massimo di sessioni consentite per utente su una connessione TCP. Qualsiasi richiesta di stabilire una sessione verrà rifiutata fino al rilascio di alcune sessioni. …	Eseguire le seguenti azioni correttive: …Esaminare tutte le applicazioni eseguite sul client e terminare quelle che non funzionano correttamente.…riavviare il client.…controllare se il problema è causato da un'applicazione nuova o esistente:…se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opes-same -file-per-tree". In alcuni casi, i client funzionano come previsto, ma richiedono una soglia più alta. È necessario disporre di privilegi avanzati per impostare una soglia più alta per il client. …Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.

Numero massimo di volte di apertura per file superato	ATTENZIONE	È stato superato il numero massimo di volte in cui è possibile aprire il file tramite una connessione TCP. Qualsiasi richiesta di apertura del file verrà rifiutata fino alla chiusura di alcune istanze aperte del file. Questo indica in genere un comportamento anomalo dell'applicazione.…	Eseguire le seguenti azioni correttive:…ispezionare le applicazioni in esecuzione sul client utilizzando questa connessione TCP. Il client potrebbe non funzionare correttamente a causa dell'applicazione in esecuzione.…riavviare il client.…controllare se il problema è causato da un'applicazione nuova o esistente:…se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opes-same -file-per-tree". In alcuni casi, i client funzionano come previsto, ma richiedono una soglia più alta. È necessario disporre di privilegi avanzati per impostare una soglia più alta per il client. …Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.

Conflitto nome NetBIOS	CRITICO	NetBIOS Name Service ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. Questo problema è causato in genere da un conflitto nel nome NetBIOS o in un alias. Di conseguenza, i client potrebbero non essere in grado di accedere ai dati o di connettersi al nodo di servizio dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive:…in caso di conflitto nel nome NetBIOS o in un alias, Eseguire una delle seguenti operazioni:…eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -alias -vserver vserver".…rinominare un alias NetBIOS eliminando il nome duplicato e aggiungendo un alias con un nuovo nome utilizzando il comando "vserver cifs create -alias -vserver vserver vserver". …Se non sono configurati alias e si verifica un conflitto nel nome NetBIOS, rinominare il server CIFS utilizzando i comandi "vserver cifs delete -vserver vserver vserver" e "vserver cifs create -cifs-server netbiosname". NOTA: L'eliminazione di un server CIFS può rendere i dati inaccessibili. …Rimuovere il nome NetBIOS o rinominare NetBIOS sul computer remoto.
Pool di store NFSv4 esaurito	CRITICO	Un pool di store NFSv4 è stato esaurito.	Se il server NFS non risponde per più di 10 minuti dopo l'evento, contattare il supporto tecnico di NetApp.

Nessun motore di scansione registrato	CRITICO	Il connettore antivirus ha notificato a ONTAP che non dispone di un motore di scansione registrato. Ciò potrebbe causare la non disponibilità dei dati se l'opzione "scansione obbligatoria" è attivata.	Eseguire le seguenti azioni correttive:…assicurarsi che il software del motore di scansione installato sul server antivirus sia compatibile con ONTAP.…assicurarsi che il software del motore di scansione sia in esecuzione e configurato per connettersi al connettore antivirus tramite loopback locale.
Nessuna connessione Vscan	CRITICO	ONTAP non dispone di una connessione Vscan per soddisfare le richieste di scansione virus. Ciò potrebbe causare la non disponibilità dei dati se l'opzione "scansione obbligatoria" è attivata.	Assicurarsi che il pool di scanner sia configurato correttamente e che i server antivirus siano attivi e connessi a ONTAP.
Spazio volume radice nodo basso	CRITICO	Il sistema ha rilevato che lo spazio del volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che si sia verificato un failover dei dati LIF all'interno del cluster, a causa del quale l'accesso NFS e CIFS è limitato sul nodo. La funzionalità amministrativa è limitata alle procedure di ripristino locali per consentire al nodo di liberare spazio sul volume root.	Eseguire le seguenti azioni correttive:…liberare spazio sul volume root eliminando le vecchie copie Snapshot, eliminando i file non più necessari dalla directory /mroot o espandendo la capacità del volume root.…riavviare il controller.…contattare il supporto tecnico NetApp per ulteriori informazioni o assistenza.
Condivisione amministrativa inesistente	CRITICO	Problema con Vscan: Un client ha tentato di connettersi a una condivisione ONTAP_ADMIN inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM specificato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN per la SVM.

Spazio vuoto NVMe	CRITICO	Uno spazio dei nomi NVMe è stato portato offline a causa di un errore di scrittura causato dalla mancanza di spazio.	Aggiungere spazio al volume, quindi portare online lo spazio dei nomi NVMe utilizzando il comando "vserver nvme namespace modify".
Periodo di tolleranza NVMe attivo	ATTENZIONE	Questo evento si verifica ogni giorno quando il protocollo NVMe over Fabrics (NVMe-of) è in uso e il periodo di tolleranza della licenza è attivo. La funzionalità NVMe-of richiede una licenza dopo la scadenza del periodo di tolleranza della licenza. La funzionalità NVMe-of viene disattivata quando il periodo di tolleranza della licenza è terminato.	Contattare il rappresentante commerciale per ottenere una licenza NVMe-of e aggiungerla al cluster oppure rimuovere tutte le istanze di configurazione NVMe-of dal cluster.
Periodo di tolleranza NVMe scaduto	ATTENZIONE	Il periodo di tolleranza della licenza NVMe over Fabrics (NVMe-of) è terminato e la funzionalità NVMe-of è disattivata.	Contattare il rappresentante commerciale per ottenere una licenza NVMe-of e aggiungerla al cluster.
Inizio del periodo di prova NVMe-of Grace	ATTENZIONE	La configurazione NVMe over Fabrics (NVMe-of) è stata rilevata durante l'aggiornamento al software ONTAP 9.5. La funzionalità NVMe-of richiede una licenza dopo la scadenza del periodo di tolleranza della licenza.	Contattare il rappresentante commerciale per ottenere una licenza NVMe-of e aggiungerla al cluster.
Host archivio oggetti non risolvibile	CRITICO	Il nome host del server archivio oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio di oggetti non può comunicare con il server dell'archivio di oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero essere inaccessibili.	Controllare la configurazione DNS per verificare che il nome host sia configurato correttamente con un indirizzo IP.

LIF dell’intercluster dell’archivio di oggetti non disponibile	CRITICO	Il client dell’archivio di oggetti non riesce a trovare una LIF operativa per comunicare con il server dell’archivio di oggetti. Il nodo non consentirà il traffico del client dell’archivio di oggetti fino a quando la LIF dell’intercluster non sarà operativa. Di conseguenza, i dati potrebbero essere inaccessibili.	Eseguire le seguenti azioni correttive:…controllare lo stato LIF dell’intercluster utilizzando il comando "network intercluster show -role intercluster".…verificare che la LIF dell’intercluster sia configurata correttamente e operativa.…se la LIF dell’intercluster non è configurata, aggiungerla utilizzando il comando "network intercluster create -role".
Mancata corrispondenza firma archivio oggetti	CRITICO	La firma della richiesta inviata al server archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero essere inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per assistenza.
Timeout DI READDIR	CRITICO	Un’operazione del file READDIR ha superato il timeout consentito per l’esecuzione in WAFL. Questo può essere dovuto a directory molto grandi o sparse. Si consiglia di intraprendere un’azione correttiva.	Eseguire le seguenti azioni correttive:…trovare informazioni specifiche per le directory recenti che hanno avuto la scadenza delle operazioni del file READDIR utilizzando il seguente comando 'diag' Privilege nodeshell CLI: WAFL readdir notice show.…controllare se le directory sono indicate come sparse o no:…se una directory è indicata come sparse, si consiglia di copiare il contenuto della directory in una nuova directory per rimuovere la scarsità del file di directory. …Se una directory non è indicata come sparse e la directory è grande, si consiglia di ridurre la dimensione del file di directory riducendo il numero di voci di file nella directory.

Trasferimento dell’aggregato non riuscito	CRITICO	Questo evento si verifica durante il trasferimento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive:…verificare che la LIF dell’intercluster sia online e funzionante utilizzando il comando "network interface show"….verificare la connettività di rete al server dell’archivio oggetti utilizzando il comando"'ping" sul LIF dell’intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio di oggetti non sia stata modificata e che le informazioni di accesso e connettività siano ancora accurate utilizzando il comando "aggregate object-store config show"….in alternativa, è possibile ignorare l’errore utilizzando il parametro "override-destination-checks" del comando di trasferimento.…contattare il supporto tecnico NetApp per ulteriori informazioni o assistenza.
Copia shadow non riuscita	CRITICO	Un servizio di copia shadow del volume (VSS), un’operazione del servizio di backup e ripristino di Microsoft Server, non è riuscita.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio di evento:…la configurazione della copia shadow è attivata?…sono installate le licenze appropriate? …Su quali condivisioni viene eseguita l’operazione di copia shadow?…il nome della condivisione è corretto?…il percorso di condivisione esiste?…quali sono gli stati del set di copie shadow e delle relative copie shadow?

Guasto agli alimentatori dello switch di storage	ATTENZIONE	Manca l'alimentazione nello switch del cluster. La ridondanza è ridotta, il rischio di interruzioni di corrente con ulteriori interruzioni dell'alimentazione.	Eseguire le seguenti azioni correttive:…assicurarsi che l'alimentazione di rete, che alimenta lo switch del cluster, sia accesa.…assicurarsi che il cavo di alimentazione sia collegato all'alimentatore.…se il problema persiste, contattare il supporto tecnico NetApp.
Troppe autenticazione CIFS	ATTENZIONE	Molte negoziazioni di autenticazione si sono verificate simultaneamente. Ci sono 256 richieste di nuova sessione incomplete da questo client.	Esaminare il motivo per cui il client ha creato 256 o più nuove richieste di connessione. Potrebbe essere necessario contattare il fornitore del client o dell'applicazione per determinare il motivo dell'errore.
Accesso utente non autorizzato alla condivisione amministrativa	ATTENZIONE	Un client ha tentato di connettersi alla condivisione con privilegi ONTAP_ADMIN, anche se l'utente connesso non è un utente consentito.	Eseguire le seguenti azioni correttive:…assicurarsi che il nome utente e l'indirizzo IP menzionati siano configurati in uno dei pool di scanner Vscan attivi.…controllare la configurazione del pool di scanner attualmente attiva utilizzando il comando "vserver vscan scanner pool show-Active".
Virus rilevato	ATTENZIONE	Un server Vscan ha segnalato un errore al sistema di storage. Questo indica in genere che è stato rilevato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento.…l'accesso client al file viene negato. Il server Vscan potrebbe, a seconda delle impostazioni e della configurazione, pulire il file, metterlo in quarantena o eliminarlo.	Controllare il log del server Vscan riportato nell'evento "syslog" per verificare se è stato in grado di pulire, mettere in quarantena o eliminare correttamente il file infetto. In caso contrario, l'amministratore di sistema potrebbe dover eliminare manualmente il file.

Volume offline	INFO	Questo messaggio indica che un volume viene reso offline.	Riportare il volume online.
Volume Restricted (Volume limitato)	INFO	Questo evento indica che un volume flessibile viene limitato.	Riportare il volume online.
Arresto VM storage riuscito	INFO	Questo messaggio viene visualizzato quando un'operazione di "vserver stop" ha esito positivo.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di storage.
Nodo Panic	ATTENZIONE	Questo evento viene generato quando si verifica un panico	Contattare l'assistenza clienti NetApp.

Torna all'inizio

Monitor di log anti-ransomware

Nome monitor	Severità	Descrizione	Azione correttiva
Monitoraggio Anti-ransomware di Storage VM disattivato	ATTENZIONE	Il monitoraggio anti-ransomware per la VM di storage è disattivato. Abilitare l'anti-ransomware per proteggere la VM di storage.	Nessuno
Monitoraggio Anti-ransomware Storage VM abilitato (modalità apprendimento)	INFO	Il monitoraggio anti-ransomware per la VM di storage è attivato in modalità di apprendimento.	Nessuno
Volume Anti-ransomware Monitoring abilitato	INFO	Il monitoraggio anti-ransomware per il volume è attivato.	Nessuno
Volume Anti-ransomware Monitoring Disabled (monitoraggio Anti-ransomware volume disabilitato)	ATTENZIONE	Il monitoraggio anti-ransomware per il volume è disattivato. Abilitare l'anti-ransomware per proteggere il volume.	Nessuno
Volume Anti-ransomware Monitoring Enabled (modalità apprendimento)	INFO	Il monitoraggio anti-ransomware per il volume è attivato in modalità di apprendimento.	Nessuno
Volume Anti-ransomware Monitoring Paused (modalità di apprendimento)	ATTENZIONE	Il monitoraggio anti-ransomware per il volume viene messo in pausa in modalità di apprendimento.	Nessuno

Volume Anti-ransomware Monitoring Paused (monitoraggio anti-ransomware volume in pausa)	ATTENZIONE	Il monitoraggio anti-ransomware per il volume viene messo in pausa.	Nessuno
Volume Anti-ransomware Monitoring (monitoraggio Anti-ransomware volume) Disattiva	ATTENZIONE	Il monitoraggio anti-ransomware per il volume è in corso di disattivazione.	Nessuno
Rilevata attività ransomware	CRITICO	Per proteggere i dati dal ransomware rilevato, è stata eseguita una copia Snapshot che può essere utilizzata per ripristinare i dati originali. Il sistema genera e trasmette un messaggio AutoSupport o "call home" al supporto tecnico NetApp e a qualsiasi destinazione configurata. Il messaggio AutoSupport migliora la determinazione e la risoluzione dei problemi.	Fare riferimento al "NOME-DOCUMENTO-FINALE" per prendere misure correttive per l'attività ransomware.

Torna all'inizio

FSX per i monitor ONTAP NetApp

Nome monitor	Soglie	Descrizione del monitor	Azione correttiva

La capacità del volume FSX è piena	Attenzione @ > 85 %…critico @ > 95 %	La capacità di storage di un volume è necessaria per memorizzare i dati delle applicazioni e dei clienti. Maggiore è il numero di dati memorizzati nel volume ONTAP, minore sarà la disponibilità dello storage per i dati futuri. Se la capacità di storage dei dati all'interno di un volume raggiunge la capacità di storage totale, il cliente potrebbe non essere in grado di memorizzare i dati a causa della mancanza di capacità di storage. Il monitoraggio della capacità di storage utilizzata per il volume garantisce la continuità dei servizi dati.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Prendere in considerazione l'eliminazione di dati non più necessari per liberare spazio
Volume FSX elevata latenza	Avviso @ > 1000 µs…critico @ > 2000 µs	I volumi sono oggetti che servono il traffico io spesso guidato da applicazioni sensibili alle performance, tra cui applicazioni DevOps, home directory e database. L'elevata latenze dei volumi implica che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Il monitoraggio delle latenze dei volumi è fondamentale per mantenere performance coerenti con le applicazioni.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Se al volume è stata assegnata una policy di QoS, valutarne le soglie limite nel caso in cui il carico di lavoro del volume venga rallentato……pianificare di intraprendere le seguenti azioni subito se la soglia di avviso viene violata:…1. Se al volume è stato assegnato un criterio QoS, valutarne le soglie limite nel caso in cui il carico di lavoro del volume venga rallentato.…2. Se anche il nodo presenta un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.

FSX Volume Inodes Limit (limite nodi volume FSX	Attenzione @ > 85 %…critico @ > 95 %	I volumi che memorizzano i file utilizzano i nodi indice (inode) per memorizzare i metadati dei file. Quando un volume esaurisce la propria allocazione inode, non è possibile aggiungervi altri file. Un avviso indica che è necessario intraprendere un'azione pianificata per aumentare il numero di inode disponibili. Un avviso critico indica che l'esaurimento del limite di file è imminente e che è necessario adottare misure di emergenza per liberare gli inode e garantire la continuità del servizio	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Considerare l'aumento del valore degli inode per il volume. Se il valore degli inode è già al massimo, considerare la possibilità di suddividere il volume in due o più volumi perché il file system è cresciuto oltre le dimensioni massime……pianificare di intraprendere le seguenti azioni al più presto in caso di superamento della soglia di avviso:…1. Considerare l'aumento del valore degli inode per il volume. Se il valore degli inode è già al massimo, considerare la possibilità di suddividere il volume in due o più volumi perché il file system è cresciuto oltre le dimensioni massime
Overcommit quota Qtree volume FSX	Attenzione @ > 95 %…critico @ > 100 %	Volume Qtree quota Overcommit specifica la percentuale in cui un volume viene considerato overcommit dalle quote del qtree. La soglia impostata per la quota qtree viene raggiunta per il volume. Il monitoraggio dell'overcommit della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	In caso di violazione della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Eliminare i dati indesiderati…in caso di superamento della soglia di avviso, prendere in considerazione l'aumento dello spazio del volume.

Spazio riserva snapshot FSX pieno	Attenzione @ > 90 %…critico @ > 95 %	La capacità di storage di un volume è necessaria per memorizzare i dati delle applicazioni e dei clienti. Una parte di tale spazio, denominata spazio riservato di snapshot, viene utilizzata per memorizzare le snapshot che consentono la protezione dei dati localmente. Maggiore è il numero di dati nuovi e aggiornati memorizzati nel volume ONTAP, maggiore sarà la capacità di snapshot utilizzata e minore sarà la capacità di storage di snapshot disponibile per i dati nuovi o aggiornati in futuro. Se la capacità dei dati di snapshot all'interno di un volume raggiunge lo spazio totale di riserva di snapshot, il cliente potrebbe non essere in grado di memorizzare nuovi dati di snapshot e ridurre il livello di protezione dei dati nel volume. Il monitoraggio della capacità di snapshot del volume utilizzato garantisce la continuità dei servizi dati.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Prendere in considerazione la configurazione delle snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena…2. Prendere in considerazione l'eliminazione di alcuni snapshot meno recenti che potrebbero non essere più necessari per liberare spazio……pianificare di intraprendere le seguenti azioni al più presto in caso di violazione della soglia di avviso:…1. Considerare l'aumento dello spazio di riserva snapshot all'interno del volume per adattarsi alla crescita…2. È consigliabile configurare le snapshot in modo che utilizzino lo spazio dati nel volume quando la riserva di snapshot è piena

FSX Volume cache Miss ratio (rapporto errori cache volume FSX)	Attenzione @ > 95 %…critico @ > 100 %	Volume cache Miss ratio (rapporto errori cache volume) è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco invece di essere restituite dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	In caso di violazione della soglia critica, è necessario intraprendere azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro fuori dal nodo del volume per ridurre il carico di i/o 2. Ridurre la richiesta di carichi di lavoro con priorità inferiore sullo stesso nodo tramite i limiti di QoS…considerare azioni immediate in caso di superamento della soglia di avviso: 1. Spostare alcuni carichi di lavoro fuori dal nodo del volume per ridurre il carico di i/o 2. Ridurre la domanda di carichi di lavoro con priorità inferiore sullo stesso nodo tramite i limiti di QoS 3. Modifica delle caratteristiche del carico di lavoro (dimensioni del blocco, caching delle applicazioni, ecc.)

Torna all'inizio

Monitor K8s

Nome monitor	Descrizione	Azioni correttive	Gravità/soglia

Latenza del volume persistente alta	Elevate latenze di volume persistente significano che le applicazioni stesse potrebbero soffrirne e non essere in grado di eseguire le loro attività. Il monitoraggio delle latenze dei volumi persistenti è fondamentale per mantenere performance coerenti con le applicazioni. Di seguito sono riportate le latenze previste in base al tipo di supporto: SSD fino a 1-2 millisecondi; SAS fino a 8-10 millisecondi e HDD SATA 17-20 millisecondi.	**Azioni immediate** In caso di violazione della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: Se al volume è assegnata una policy di QoS, valutarne le soglie limite in caso di rallentamento del carico di lavoro del volume. **Azioni da intraprendere a breve** Se la soglia di avviso viene violata, pianificare le seguenti azioni immediate: 1. Se anche il pool di storage sta riscontrando un elevato utilizzo, spostare il volume in un altro pool di storage. 2. Se al volume è stato assegnato un criterio QoS, valutarne le soglie limite nel caso in cui il carico di lavoro del volume venga rallentato. 3. Se anche il controller sta ricevendo un elevato utilizzo, sposta il volume su un altro controller o riduci il carico di lavoro totale del controller.	Avvertenza a > 6.000 µs Critico a > 12.000 µs
Saturazione memoria cluster alta	La saturazione della memoria allocabile del cluster è elevata. La saturazione della CPU del cluster viene calcolata come la somma dell'utilizzo della memoria divisa per la somma della memoria allocabile in tutti i K8s nodi.	Aggiungere nodi. Correggere eventuali nodi non pianificati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Avvertenza a > 80 % Critico a > 90%
Collegamento POD non riuscito	Questo avviso si verifica quando un allegato di un volume con POD non funziona.		Attenzione

Elevata velocità di ritrasmissione	Velocità di ritrasmissione TCP elevata	Controllare la congestione di rete - identificare i carichi di lavoro che consumano una grande quantità di larghezza di banda di rete. Controllare l'utilizzo elevato della CPU del pod. Controllare le prestazioni della rete hardware.	Avvertenza a > 10 % Critico a > 25%
Capacità file system nodo alta	Capacità file system nodo alta	- Aumentare le dimensioni dei dischi del nodo per assicurarsi che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo del file dell'applicazione.	Avvertenza a > 80 % Critico a > 90%
Jitter di rete del carico di lavoro alto	Jitter TCP elevato (variazioni dei tempi di risposta/latenza elevata)	Verificare la presenza di congestione della rete. Identifica i workload che consumano una notevole larghezza di banda della rete. Controllare l'utilizzo elevato della CPU del pod. Controllare le prestazioni della rete hardware	Avvertenza @ > 30 ms. Critico a > 50 ms.

Throughput del volume persistente	Le soglie di MBPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di performance predefinite, con un potenziale impatto su altri volumi persistenti. L'attivazione di questo monitor genera avvisi appropriati per il profilo di throughput tipico dei volumi persistenti su SSD. Questo monitor copre tutti i volumi persistenti dell'ambiente. I valori di soglia critici e di avvertenza possono essere modificati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando le soglie appropriate per la classe di archiviazione. Un monitor duplicato può essere ulteriormente indirizzato a un sottoinsieme dei volumi persistenti nell'ambiente.	**Azioni immediate** Se la soglia critica viene violata, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introdurre i limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per rilevare eventuali anomalie. **Azioni da intraprendere a breve** Se la soglia di avviso viene violata, pianificare di eseguire le seguenti azioni immediate: 1. Introdurre i limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per rilevare eventuali anomalie.	Avvertenza @ > 10.000 MB/s. Critico a > 15.000 MB/s.
Contenitore a rischio di morte OOM	I limiti di memoria del contenitore sono troppo bassi. Il contenitore è a rischio di sfratto (esaurimento della memoria).	Aumentare i limiti della memoria del contenitore.	Avvertenza a > 95 %
Riduzione del carico di lavoro	Il carico di lavoro non dispone di pod integri.		Critico a < 1
Persistente richiesta di rimborso del volume non riuscita	Questo avviso si verifica quando un'associazione su un PVC non riesce.		Attenzione
I limiti di ResourceQuota Mem stanno per superare	I limiti di memoria per lo spazio dei nomi stanno per superare ResourceQuota		Avvertenza a > 80 % Critico a > 90%
Le richieste di ResourceQuota Mem stanno per superare	Le richieste di memoria per lo spazio dei nomi stanno per superare ResourceQuota		Avvertenza a > 80 % Critico a > 90%

Creazione nodo non riuscita	Impossibile pianificare il nodo a causa di un errore di configurazione.	Controllare il registro eventi di Kubernetes per verificare la causa dell'errore di configurazione.	Critico
Recupero volume persistente non riuscito	Il recupero automatico del volume non è riuscito.		Avvertenza @ > 0 B.
Limitazione della CPU del container	I limiti della CPU del contenitore sono impostati su un valore troppo basso. I processi dei container vengono rallentati.	Aumentare i limiti della CPU del container.	Avvertenza a > 95 % Critico a > 98%
Impossibile eliminare il bilanciamento del carico del servizio			Attenzione
IOPS volume persistente	Le soglie di IOPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di performance predefinite. L'attivazione di questo monitor genera avvisi appropriati per il profilo IOPS tipico dei volumi di persistenza. Questo monitor copre tutti i volumi persistenti dell'ambiente. I valori di soglia critici e di avvertenza possono essere regolati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando le soglie appropriate per il carico di lavoro.	**Azioni immediate** Se la soglia critica viene violata, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introduciamo i limiti di IOPS di qualità del servizio per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per rilevare eventuali anomalie. **Azioni da intraprendere a breve** Se la soglia di avviso viene violata, pianificare le seguenti azioni immediate: 1. Introduciamo i limiti di IOPS di qualità del servizio per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per rilevare eventuali anomalie.	Avvertenza @ > 20.000 i/s. Critico a > 25.000 i/s.
Impossibile aggiornare il bilanciamento del carico del servizio			Attenzione
MONTAGGIO POD non riuscito	Questo avviso si verifica quando un montaggio su un POD non funziona.		Attenzione

Pressione PID nodo	Gli identificatori di processo disponibili sul nodo (Linux) sono scesi al di sotto di una soglia di sfratto.	Trova e correggi i pod che generano molti processi e occupano il nodo degli ID di processo disponibili. Configura PodPidsLimit per proteggere il tuo nodo da pod o container che generano troppi processi.	Critico a > 0
Errore estrazione immagine pod	Kubernetes non è riuscito a estrarre l'immagine del contenitore di pod.	- Assicurarsi che l'immagine del pod sia scritta correttamente nella configurazione del pod. - Verificare che il tag immagine esista nel registro. - Verificare le credenziali per il registro delle immagini. - Verificare la presenza di problemi di connettività del Registro di sistema. - Verificare di non aver raggiunto i limiti di velocità imposti dai provider pubblici del Registro di sistema.	Attenzione
Processo in esecuzione troppo lungo	Processo in esecuzione troppo a lungo		Avvertenza @ > 1 ore Critico a > 5 ore
Memoria nodo alta	L'utilizzo della memoria del nodo è elevato	Aggiungere nodi. Correggere eventuali nodi non pianificati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Avvertenza a > 85 % Critico a > 90%
I limiti CPU di ResourceQuota stanno per superare	I limiti CPU per lo spazio dei nomi stanno per superare ResourceQuota		Avvertenza a > 80 % Critico a > 90%
Backoff ciclo di arresto del pod	Pod si è bloccato e ha tentato di riavviarsi più volte.		Critico a > 3
CPU nodo alta	L'utilizzo della CPU del nodo è elevato.	Aggiungere nodi. Correggere eventuali nodi non pianificati. Pod ideali per liberare la CPU sui nodi.	Avvertenza a > 80 % Critico a > 90%

Latenza rete carico di lavoro RTT alta	Elevata latenza RTT TCP (tempo di andata e ritorno)	Controllare la congestione di rete ▒ identificare i carichi di lavoro che consumano una grande quantità di larghezza di banda di rete. Controllare l'utilizzo elevato della CPU del pod. Controllare le prestazioni della rete hardware.	Avvertenza @ > 150 ms. Critico a > 300 ms.
Processo non riuscito	Il processo non è stato completato correttamente a causa di un arresto anomalo del nodo o di un riavvio, di un esaurimento delle risorse, di un timeout del processo o di un errore di pianificazione del pod.	Controllare i registri eventi di Kubernetes per verificare le cause dei guasti.	Avvertenza @ > 1
Volume persistente pieno in pochi giorni	Il volume persistente esaurirà lo spazio nell'arco di pochi giorni	-Aumentare le dimensioni del volume per assicurarsi che vi sia spazio sufficiente per i file dell'applicazione. -Ridurre la quantità di dati memorizzati nelle applicazioni.	Avvertenza @ < 8 giorno Critico a < 3 giorno
Pressione memoria nodo	Il nodo sta esaurendo la memoria. La memoria disponibile ha raggiunto la soglia di evocazione.	Aggiungere nodi. Correggere eventuali nodi non pianificati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Critico a > 0
Nodo non pronto	Il nodo è stato non pronto per 5 minuti	Verificare che il nodo disponga di risorse sufficienti per CPU, memoria e disco. Controllare la connettività di rete del nodo. Controllare i registri eventi di Kubernetes per verificare le cause dei guasti.	Critico a < 1

Capacità volume persistente alta	La capacità utilizzata di backend del volume persistente è elevata.	- Aumentare le dimensioni del volume per assicurarsi che vi sia spazio sufficiente per i file dell'applicazione. Consente di ridurre la quantità di dati memorizzati nelle applicazioni.	Avvertenza a > 80 % Critico a > 90%
Impossibile creare il bilanciamento del carico del servizio	Creazione del bilanciamento del carico del servizio non riuscita		Critico
Mancata corrispondenza della replica del carico di lavoro	Alcuni pod non sono attualmente disponibili per una distribuzione o un DaemonSet.		Avvertenza @ > 1
Le richieste CPU di ResourceQuota stanno per superare	Le richieste CPU per lo spazio dei nomi stanno per superare ResourceQuota		Avvertenza a > 80 % Critico a > 90%
Elevata velocità di ritrasmissione	Velocità di ritrasmissione TCP elevata	Controllare la congestione di rete - identificare i carichi di lavoro che consumano una grande quantità di larghezza di banda di rete. Controllare l'utilizzo elevato della CPU del pod. Controllare le prestazioni della rete hardware.	Avvertenza a > 10 % Critico a > 25%
Pressione del disco del nodo	Lo spazio disponibile su disco e gli inodes sul filesystem root del nodo o sul filesystem di immagine hanno soddisfatto una soglia di eviction.	- Aumentare le dimensioni dei dischi del nodo per assicurarsi che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo del file dell'applicazione.	Critico a > 0
Saturazione CPU cluster alta	La saturazione della CPU allocabile del cluster è elevata. La saturazione della CPU del cluster viene calcolata come la somma dell'utilizzo della CPU divisa per la somma della CPU allocabile in tutti i K8s nodi.	Aggiungere nodi. Correggere eventuali nodi non pianificati. Pod ideali per liberare la CPU sui nodi.	Avvertenza a > 80 % Critico a > 90%

Torna all'inizio

Change Log Monitor (Modifica monitor registro)

Nome monitor	Severità	Descrizione del monitor
Volume interno rilevato	Informativo	Questo messaggio viene visualizzato quando viene rilevato un volume interno.
Volume interno modificato	Informativo	Questo messaggio viene visualizzato quando viene modificato un volume interno.
Nodo di storage rilevato	Informativo	Questo messaggio viene visualizzato quando viene rilevato un nodo di storage.
Nodo di storage rimosso	Informativo	Questo messaggio viene visualizzato quando viene rimosso un nodo di storage.
Pool di storage rilevato	Informativo	Questo messaggio viene visualizzato quando viene rilevato un pool di storage.
Macchina virtuale per lo storage rilevata	Informativo	Questo messaggio viene visualizzato quando viene rilevata una Storage Virtual Machine.
Macchina virtuale di storage modificata	Informativo	Questo messaggio viene visualizzato quando viene modificata una Storage Virtual Machine.

Torna all'inizio

Monitor per la raccolta dei dati

Nome monitor	Descrizione	Azione correttiva
Arresto dell'unità di acquisizione	Le unità di acquisizione Cloud Insights vengono riavviate periodicamente come parte degli aggiornamenti per introdurre nuove funzionalità. Questo avviene una volta al mese o meno in un ambiente tipico. Un avviso di avviso relativo allo spegnimento di un'unità di acquisizione deve essere seguito subito dopo da una risoluzione che indica che l'unità di acquisizione appena riavviata ha completato una registrazione con Cloud Insights. In genere, questo ciclo di shutdown-to-registration richiede da 5 a 15 minuti.	Se l'avviso si verifica frequentemente o dura più di 15 minuti, controllare il funzionamento del sistema che ospita l'unità di acquisizione, la rete e qualsiasi proxy che connette l'AU a Internet.

Collector non riuscito	Il sondaggio di un data collector ha riscontrato una situazione di errore imprevista.	Visita la pagina di raccolta dati di Cloud Insights per saperne di più sulla situazione.
Avviso di raccolta	Questo avviso può in genere verificarsi a causa di una configurazione errata del data collector o del sistema di destinazione. Rivedere le configurazioni per evitare avvisi futuri. Può anche essere dovuto a un recupero di dati meno completi in cui il data collector ha raccolto tutti i dati possibili. Ciò può verificarsi quando le situazioni cambiano durante la raccolta dei dati (ad esempio, una macchina virtuale presente all'inizio della raccolta dei dati viene eliminata durante la raccolta dei dati e prima che i dati vengano acquisiti).	Controllare la configurazione del data collector o del sistema di destinazione. Tenere presente che il monitor per Collector Warning può inviare più avvisi rispetto ad altri tipi di monitor, pertanto si consiglia di non impostare destinatari di avvisi a meno che non si stia eseguendo la risoluzione dei problemi.

Torna all'inizio

Monitor di sicurezza

Nome monitor	Soglia	Descrizione del monitor	Azione correttiva
Trasporto HTTPS AutoSupport disattivato	Avvertenza @ < 1	AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. A causa della natura sensibile dei messaggi AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.	Per impostare HTTPS come protocollo di trasporto per i messaggi AutoSupport, eseguire il seguente comando ONTAP:…system node AutoSupport modify -transport https
Crittografia non sicura del cluster per SSH	Avvertenza @ < 1	Indica che SSH sta utilizzando cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere le cifre CBC, eseguire il seguente comando ONTAP:…Security ssh remove -vserver <admin vserver> -cifers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc

Banner di accesso cluster disattivato	Avvertenza @ < 1	Indica che il banner di accesso è disattivato per gli utenti che accedono al sistema ONTAP. La visualizzazione di un banner di accesso è utile per stabilire le aspettative di accesso e utilizzo del sistema.	Per configurare il banner di accesso per un cluster, eseguire il seguente comando ONTAP:…Security login banner modify -vserver <admin svm> -message "accesso limitato agli utenti autorizzati"
Comunicazione peer cluster non crittografata	Avvertenza @ < 1	Durante la replica dei dati per il disaster recovery, il caching o il backup, è necessario proteggerli durante il trasporto via cavo da un cluster ONTAP a un altro. La crittografia deve essere configurata sia sul cluster di origine che su quello di destinazione.	Per abilitare la crittografia sulle relazioni peer del cluster create prima di ONTAP 9.6, è necessario aggiornare il cluster di origine e di destinazione alla versione 9.6. Quindi, utilizzare il comando "cluster peer modify" per modificare i peer del cluster di origine e di destinazione in modo da utilizzare la crittografia di peering dei cluster.…per ulteriori informazioni, consultare la Guida di protezione avanzata di NetApp per ONTAP 9.
Default Local Admin User Enabled (utente amministratore locale predefinito attivato	Attenzione @ > 0	NetApp consiglia di bloccare (disabilitare) gli account utente amministratore predefinito non necessari (integrati) con il comando lock. Si tratta principalmente di account predefiniti per i quali le password non sono mai state aggiornate o modificate.	Per bloccare l'account "admin" integrato, eseguire il seguente comando ONTAP:…Security login lock -nomeutente admin
Modalità FIPS disattivata	Avvertenza @ < 1	Quando la conformità FIPS 140-2 è attivata, TLSv1 e SSLv3 sono disattivati e rimangono attivati solo TLSv1.1 e TLSv1.2. ONTAP impedisce di abilitare TLSv1 e SSLv3 quando la conformità FIPS 140-2 è attivata.	Per abilitare la conformità FIPS 140-2 su un cluster, eseguire il seguente comando ONTAP in Advanced Privilege mode:…Security config modify -interface SSL -is -fips-enabled true

Inoltro log non crittografato	Avvertenza @ < 1	L'offload delle informazioni syslog è necessario per limitare l'ambito o l'impatto di una violazione a un singolo sistema o soluzione. Pertanto, NetApp consiglia di trasferire in modo sicuro le informazioni syslog in una posizione di storage o conservazione sicura.	Una volta creata una destinazione di inoltro del log, il protocollo non può essere modificato. Per passare a un protocollo crittografato, eliminare e ricreare la destinazione di inoltro del log utilizzando il seguente comando ONTAP:…cluster log-forwarding create -destination <destination ip> -Protocol tcp-Encrypted
Password hash MD5	Attenzione @ > 0	NetApp consiglia vivamente di utilizzare la funzione hash SHA-512 più sicura per le password degli account utente ONTAP. Gli account che utilizzano la funzione hash MD5 meno sicura devono migrare alla funzione hash SHA-512.	NetApp consiglia vivamente agli account utente di migrare verso la soluzione SHA-512 più sicura, facendo in modo che gli utenti modifichino le proprie password.…per bloccare gli account con password che utilizzano la funzione hash MD5, eseguire il seguente comando ONTAP:…Security login lock -vserver * -username * -hash-function md5
Nessun server NTP configurato	Avvertenza @ < 1	Indica che il cluster non dispone di server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp consiglia di associare almeno tre server NTP al cluster.	Per associare un server NTP al cluster, eseguire il seguente comando ONTAP: Cluster Time-service ntp server create -server <ntp server host name or ip address>
Il numero di server NTP è basso	Avvertenza @ < 3	Indica che il cluster ha meno di 3 server NTP configurati. Per garantire ridondanza e un servizio ottimale, NetApp consiglia di associare almeno tre server NTP al cluster.	Per associare un server NTP al cluster, eseguire il seguente comando ONTAP:…cluster time-service ntp server create -server <ntp server host name or ip address>

Shell remota attivata	Attenzione @ > 0	La shell remota non è un metodo sicuro per stabilire l'accesso dalla riga di comando alla soluzione ONTAP. La shell remota deve essere disattivata per un accesso remoto sicuro.	NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.…per disattivare la shell remota su un cluster, eseguire il seguente comando ONTAP in Advanced Privilege mode:…Security Protocol modify -application rsh-enabled false
Log di audit delle VM di storage disattivato	Avvertenza @ < 1	Indica che la registrazione dell'audit è disattivata per SVM.	Per configurare il registro di controllo per un vserver, eseguire il seguente comando ONTAP:…vserver audit enable -vserver <svm>
Crittografia non sicura delle VM di storage per SSH	Avvertenza @ < 1	Indica che SSH sta utilizzando cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere le cifre CBC, eseguire il seguente comando ONTAP:…Security ssh remove -vserver <vserver> -cifers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner di login Storage VM disattivato	Avvertenza @ < 1	Indica che il banner di accesso è disattivato per gli utenti che accedono alle SVM sul sistema. La visualizzazione di un banner di accesso è utile per stabilire le aspettative di accesso e utilizzo del sistema.	Per configurare il banner di accesso per un cluster, eseguire il seguente comando ONTAP:…Security login banner modify -vserver <svm> -message "accesso limitato agli utenti autorizzati"
Protocollo Telnet attivato	Attenzione @ > 0	Telnet non è un metodo sicuro per stabilire l'accesso dalla riga di comando alla soluzione ONTAP. Telnet deve essere disattivato per un accesso remoto sicuro.	NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro. Per disattivare Telnet su un cluster, eseguire il seguente comando ONTAP in Advanced Privilege mode:…Security Protocol modify -application telnet -enabled false

Torna all'inizio

Monitor per la protezione dei dati

Nome monitor	Soglie	Descrizione del monitor	Azione correttiva

Spazio insufficiente per la copia snapshot Lun	(Filter contains_lun = Yes) Avviso @ > 95 %…critico @ > 100 %	La capacità di storage di un volume è necessaria per memorizzare i dati delle applicazioni e dei clienti. Una parte di tale spazio, denominata spazio riservato di snapshot, viene utilizzata per memorizzare le snapshot che consentono la protezione dei dati localmente. Maggiore è il numero di dati nuovi e aggiornati memorizzati nel volume ONTAP, maggiore sarà la capacità di snapshot utilizzata e minore sarà la capacità di storage di snapshot disponibile per i dati nuovi o aggiornati in futuro. Se la capacità dei dati di snapshot all'interno di un volume raggiunge lo spazio totale di riserva di snapshot, il cliente potrebbe non essere in grado di memorizzare nuovi dati di snapshot e ridurre il livello di protezione dei dati nelle LUN del volume. Il monitoraggio della capacità di snapshot del volume utilizzato garantisce la continuità dei servizi dati.	**Azioni immediate** in caso di superamento della soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare le snapshot in modo che utilizzino lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Eliminare alcune istantanee indesiderate meno recenti per liberare spazio. **Azioni da intraprendere a breve** in caso di superamento della soglia di avviso, pianificare le seguenti azioni immediate: 1. Aumentare lo spazio di riserva snapshot all'interno del volume per adattarlo alla crescita. 2. Configurare le snapshot in modo che utilizzino lo spazio dati nel volume quando la riserva di snapshot è piena.

Ritardo relazione SnapMirror	Avvertenza @ > 150%…critica @ > 300%	Il ritardo di relazione di SnapMirror è la differenza tra l'indicatore di data e ora dello snapshot e l'ora sul sistema di destinazione. Lag_time_percent è il rapporto tra il tempo di ritardo e l'intervallo di pianificazione di SnapMirror Policy. Se il tempo di ritardo corrisponde all'intervallo di pianificazione, lag_time_percent sarà pari al 100%. Se la policy di SnapMirror non ha una pianificazione, lag_time_percent non verrà calcolata.	Monitorare lo stato di SnapMirror utilizzando il comando "snapmirror show". Controllare la cronologia di trasferimento di SnapMirror utilizzando il comando "snapmirror show-history"

Torna all'inizio

Monitoraggio del volume cloud (CVO)

Nome monitor	Severità ci	Descrizione del monitor	Azione correttiva
Disco CVO fuori servizio	INFO	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come non riuscito, viene sanificato o è entrato nel Centro di manutenzione.	Nessuno

Giveback CVO del pool di storage non riuscito	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover dello storage (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive: Verificare che la LIF dell'intercluster sia in linea e funzionante utilizzando il comando "network interface show" (mostra interfaccia di rete). Verificare la connettività di rete al server di archiviazione oggetti utilizzando il comando "'ping" sul LIF del nodo di destinazione dell'intercluster. Verificare che la configurazione dell'archivio di oggetti non sia stata modificata e che le informazioni di accesso e connettività siano ancora accurate utilizzando il comando "aggregate object-store config show". In alternativa, è possibile ignorare l'errore specificando false per il parametro "prescrivere-partner-waiting" del comando giveback. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.

Interconnessione CVO ha non disponibile	ATTENZIONE	L'interconnessione ad alta disponibilità (ha) non è disponibile. Rischio di interruzione del servizio quando il failover non è disponibile.	Le azioni correttive dipendono dal numero e dal tipo di collegamenti di interconnessione ha supportati dalla piattaforma, nonché dal motivo per cui l'interconnessione è inattiva. Se i collegamenti non sono attivi: Verificare che entrambi i controller della coppia ha siano operativi. Per i collegamenti esterni, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i Small Form-Factor pluggable (SFP), se presenti, siano posizionati correttamente su entrambi i controller. Per i collegamenti interni, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link Off" (collegamento ic disattivato) e "ic link on" (collegamento ic attivato). Se i collegamenti sono disattivati, abilitarlo usando il comando "ic link on". Se un peer non è connesso, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link Off" (collegamento ic disattivato) e "ic link on" (collegamento ic attivato). Se il problema persiste, contattare il supporto tecnico NetApp.

Numero massimo di sessioni CVO per utente superato	ATTENZIONE	È stato superato il numero massimo di sessioni consentite per utente su una connessione TCP. Qualsiasi richiesta di stabilire una sessione verrà rifiutata fino al rilascio di alcune sessioni.	Eseguire le seguenti azioni correttive: Esaminare tutte le applicazioni in esecuzione sul client e terminare quelle che non funzionano correttamente. Riavviare il client. Verificare se il problema è causato da un'applicazione nuova o esistente: Se l'applicazione è nuova, impostare una soglia più alta per il client utilizzando il comando "cifs option modify -max-opes-same -file-per-tree". In alcuni casi, i client funzionano come previsto, ma richiedono una soglia più alta. È necessario disporre di privilegi avanzati per impostare una soglia più alta per il client. Se il problema è causato da un'applicazione esistente, potrebbe esserci un problema con il client. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.

Conflitto nome NetBIOS CVO	CRITICO	NetBIOS Name Service ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. Questo problema è causato in genere da un conflitto nel nome NetBIOS o in un alias. Di conseguenza, i client potrebbero non essere in grado di accedere ai dati o di connettersi al nodo di servizio dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive: In caso di conflitto nel nome NetBIOS o in un alias, eseguire una delle seguenti operazioni: Eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -alias -vserver vserver vserver". Rinominare un alias NetBIOS eliminando il nome duplicato e aggiungendo un alias con un nuovo nome utilizzando il comando "vserver cifs create -alias -vserver vserver vserver". Se non sono configurati alias e si verifica un conflitto nel nome NetBIOS, rinominare il server CIFS utilizzando i comandi "vserver cifs delete -vserver vserver vserver" e "vserver cifs create -cifs-server netbiosname". NOTA: L'eliminazione di un server CIFS può rendere i dati inaccessibili. Rimuovere il nome NetBIOS o rinominare NetBIOS sul computer remoto.
Pool di store CVO NFSv4 esaurito	CRITICO	Un pool di store NFSv4 è stato esaurito.	Se il server NFS non risponde per più di 10 minuti dopo l'evento, contattare il supporto tecnico di NetApp.
Panic nodo CVO	ATTENZIONE	Questo evento viene generato quando si verifica un panico	Contattare l'assistenza clienti NetApp.

Spazio volume radice nodo CVO basso	CRITICO	Il sistema ha rilevato che lo spazio del volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che si sia verificato un failover dei dati LIF all'interno del cluster, a causa del quale l'accesso NFS e CIFS è limitato sul nodo. La funzionalità amministrativa è limitata alle procedure di ripristino locali per consentire al nodo di liberare spazio sul volume root.	Eseguire le seguenti azioni correttive: Liberare spazio sul volume root eliminando le vecchie copie Snapshot, eliminando i file non più necessari dalla directory /mroot o espandendo la capacità del volume root. Riavviare il controller. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.
Condivisione amministratore CVO inesistente	CRITICO	Problema con Vscan: Un client ha tentato di connettersi a una condivisione ONTAP_ADMIN inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM specificato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN per la SVM.
Host CVO Object Store non risolvibile	CRITICO	Il nome host del server archivio oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio di oggetti non può comunicare con il server dell'archivio di oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero essere inaccessibili.	Controllare la configurazione DNS per verificare che il nome host sia configurato correttamente con un indirizzo IP.

CVO Object Store Intercluster LIF inattivo	CRITICO	Il client dell'archivio di oggetti non riesce a trovare una LIF operativa per comunicare con il server dell'archivio di oggetti. Il nodo non consentirà il traffico del client dell'archivio di oggetti fino a quando la LIF dell'intercluster non sarà operativa. Di conseguenza, i dati potrebbero essere inaccessibili.	Eseguire le seguenti azioni correttive: Controllare lo stato LIF dell'intercluster utilizzando il comando "network intercluster show -role". Verificare che la LIF dell'intercluster sia configurata correttamente e che funzioni correttamente. Se un LIF di intercluster non è configurato, aggiungerlo utilizzando il comando "network intercluster create -role".
Mancata corrispondenza firma archivio oggetti CVO	CRITICO	La firma della richiesta inviata al server archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero essere inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per assistenza.
CVO QoS Monitor Memory maximed out (memoria monitor QoS CVO massima	CRITICO	La memoria dinamica del sottosistema QoS ha raggiunto il limite per l'hardware della piattaforma corrente. Alcune funzioni QoS potrebbero funzionare in una capacità limitata.	Eliminare alcuni carichi di lavoro o flussi attivi per liberare memoria. Utilizzare il comando "statistics show -object workload -counter Ops" per determinare quali carichi di lavoro sono attivi. I carichi di lavoro attivi mostrano operazioni diverse da zero. Quindi, utilizzare più volte il comando "workload DELETE <workload_name>" per rimuovere carichi di lavoro specifici. In alternativa, utilizzare il comando "stream delete -workload <workload name> *" per eliminare i flussi associati dal carico di lavoro attivo.

Timeout READDIR CVO	CRITICO	Un’operazione del file READDIR ha superato il timeout consentito per l’esecuzione in WAFL. Questo può essere dovuto a directory molto grandi o sparse. Si consiglia di intraprendere un’azione correttiva.	Eseguire le seguenti azioni correttive: Trovare le informazioni specifiche delle directory recenti che hanno avuto la scadenza delle operazioni del file READDIR utilizzando il seguente comando 'diag' Privilege nodeshell CLI: WAFL readdir notice show. Controllare se le directory sono indicate come sparse o no: Se una directory è indicata come sparse, si consiglia di copiare il contenuto della directory in una nuova directory per rimuovere la scarsità del file di directory. Se una directory non è indicata come sparse e la directory è grande, si consiglia di ridurre la dimensione del file di directory riducendo il numero di voci di file nella directory.

Trasferimento CVO del pool di storage non riuscito	CRITICO	Questo evento si verifica durante il trasferimento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive: Verificare che la LIF dell'intercluster sia in linea e funzionante utilizzando il comando "network interface show" (mostra interfaccia di rete). Verificare la connettività di rete al server di archiviazione oggetti utilizzando il comando "'ping" sul LIF del nodo di destinazione dell'intercluster. Verificare che la configurazione dell'archivio di oggetti non sia stata modificata e che le informazioni di accesso e connettività siano ancora accurate utilizzando il comando "aggregate object-store config show". In alternativa, è possibile ignorare l'errore utilizzando il parametro "override-destination-checks" del comando di rilocazione. Per ulteriori informazioni o assistenza, contattare il supporto tecnico NetApp.
Copia shadow CVO non riuscita	CRITICO	Un servizio di copia shadow del volume (VSS), un'operazione del servizio di backup e ripristino di Microsoft Server, non è riuscita.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio di evento: La configurazione della copia shadow è attivata? Sono installate le licenze appropriate? Su quali condivisioni viene eseguita l'operazione di copia shadow? Il nome della condivisione è corretto? Il percorso di condivisione esiste? Quali sono gli stati del set di copie shadow e delle relative copie shadow?
Interruzione VM storage CVO riuscita	INFO	Questo messaggio viene visualizzato quando un'operazione di "vserver stop" ha esito positivo.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di storage.

CVO troppi CIFS Authentication	ATTENZIONE	Molte negoziazioni di autenticazione si sono verificate simultaneamente. Ci sono 256 richieste di nuova sessione incomplete da questo client.	Esaminare il motivo per cui il client ha creato 256 o più nuove richieste di connessione. Potrebbe essere necessario contattare il fornitore del client o dell'applicazione per determinare il motivo dell'errore.
Dischi CVO non assegnati	INFO	Il sistema dispone di dischi non assegnati: La capacità viene sprecata e il sistema potrebbe presentare modifiche di configurazione errate o parziali.	Eseguire le seguenti azioni correttive: Determinare quali dischi non sono assegnati utilizzando il comando "disk show -n". Assegnare i dischi a un sistema utilizzando il comando "disk assign".
Accesso utente non autorizzato CVO alla condivisione amministrativa	ATTENZIONE	Un client ha tentato di connettersi alla condivisione con privilegi ONTAP_ADMIN, anche se l'utente connesso non è un utente consentito.	Eseguire le seguenti azioni correttive: Assicurarsi che il nome utente e l'indirizzo IP menzionati siano configurati in uno dei pool di scanner Vscan attivi. Verificare la configurazione del pool di scanner attualmente attiva utilizzando il comando "vserver vscan scanner pool show-Active".
Virus CVO rilevato	ATTENZIONE	Un server Vscan ha segnalato un errore al sistema di storage. Questo indica in genere che è stato rilevato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento. Accesso client al file negato. Il server Vscan potrebbe, a seconda delle impostazioni e della configurazione, pulire il file, metterlo in quarantena o eliminarlo.	Controllare il log del server Vscan riportato nell'evento "syslog" per verificare se è stato in grado di pulire, mettere in quarantena o eliminare correttamente il file infetto. In caso contrario, l'amministratore di sistema potrebbe dover eliminare manualmente il file.
Volume CVO non in linea	INFO	Questo messaggio indica che un volume viene reso offline.	Riportare il volume online.

Volume CVO limitato	INFO	Questo evento indica che un volume flessibile viene limitato.	Riportare il volume online.

Torna all'inizio

SnapMirror for Business Continuity (SMBC) Mediator Log Monitor

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Aggiunto mediatore ONTAP	INFO	Questo messaggio viene visualizzato quando il mediatore ONTAP viene aggiunto correttamente a un cluster.	Nessuno
Mediatore ONTAP non accessibile	CRITICO	Questo messaggio viene visualizzato quando il supporto ONTAP viene riassegnato o il pacchetto non viene più installato sul server. Di conseguenza, il failover di SnapMirror non è possibile.	Rimuovere la configurazione del supporto ONTAP corrente utilizzando il comando "rimozione del mediatore snapmirror". Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".
ONTAP Mediator rimosso	INFO	Questo messaggio viene visualizzato quando il mediatore ONTAP viene rimosso correttamente da un cluster.	Nessuno
Mediatore ONTAP non raggiungibile	ATTENZIONE	Questo messaggio viene visualizzato quando il mediatore ONTAP non è raggiungibile su un cluster. Di conseguenza, il failover di SnapMirror non è possibile.	Verificare la connettività di rete al mediatore ONTAP utilizzando i comandi "ping di rete" e "traceroute di rete". Se il problema persiste, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove" (Rimuovi mediatore snapmirror). Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".

Certificato CA SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) del mediatore ONTAP è scaduto. Di conseguenza, non sarà possibile effettuare ulteriori comunicazioni con il mediatore ONTAP.	Rimuovere la configurazione del supporto ONTAP corrente utilizzando il comando "rimozione del mediatore snapmirror". Aggiornare un nuovo certificato CA sul server del mediatore ONTAP. Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".
Certificato CA SMBC in scadenza	ATTENZIONE	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) del mediatore ONTAP scadrà entro i prossimi 30 giorni.	Prima della scadenza del certificato, rimuovere la configurazione del mediatore ONTAP corrente utilizzando il comando "snapmirror mediator remove" (Rimuovi mediatore snapmirror). Aggiornare un nuovo certificato CA sul server del mediatore ONTAP. Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato del client del mediatore ONTAP è scaduto. Di conseguenza, non sarà possibile effettuare ulteriori comunicazioni con il mediatore ONTAP.	Rimuovere la configurazione del supporto ONTAP corrente utilizzando il comando "rimozione del mediatore snapmirror". Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC in scadenza	ATTENZIONE	Questo messaggio viene visualizzato quando il certificato del client del mediatore ONTAP scadrà entro i prossimi 30 giorni.	Prima della scadenza del certificato, rimuovere la configurazione del mediatore ONTAP corrente utilizzando il comando "snapmirror mediator remove" (Rimuovi mediatore snapmirror). Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".

Relazione SMBC fuori sincronia Nota: UM non dispone di questa	CRITICO	Questo messaggio viene visualizzato quando una relazione SnapMirror for Business Continuity (SMBC) cambia stato da "in-Sync" a "out-of-Sync". A causa di questo RPO=0 la protezione dei dati verrà interrotta.	Verificare la connessione di rete tra il volume di origine e quello di destinazione. Monitorare lo stato della relazione SMBC utilizzando il comando "snapmirror show" (Mostra snapmirror) sulla destinazione e il comando "snapmirror list-destinations" (elenco destinazioni snapmirror) sull'origine. La risincronizzazione automatica tenterà di riportare la relazione allo stato "in-Sync". Se la risincronizzazione non riesce, verificare che tutti i nodi del cluster siano in quorum e integri.
Certificato server SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato del server del mediatore ONTAP è scaduto. Di conseguenza, non sarà possibile effettuare ulteriori comunicazioni con il mediatore ONTAP.	Rimuovere la configurazione del supporto ONTAP corrente utilizzando il comando "rimozione del mediatore snapmirror". Aggiorna un nuovo certificato server sul server ONTAP. Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".
Certificato server SMBC in scadenza	ATTENZIONE	Questo messaggio viene visualizzato quando il certificato del server del mediatore ONTAP scadrà entro i prossimi 30 giorni.	Prima della scadenza del certificato, rimuovere la configurazione del mediatore ONTAP corrente utilizzando il comando "snapmirror mediator remove" (Rimuovi mediatore snapmirror). Aggiorna un nuovo certificato server sul server ONTAP. Riconfigurare l'accesso al supporto ONTAP utilizzando il comando "snapmirror mediator add".

Torna all'inizio

Monitor di sistema aggiuntivi per alimentazione, Heartbeat e varie

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Rilevato alimentatore shelf di dischi	INFORMATIVO	Questo messaggio viene visualizzato quando un'unità di alimentazione viene aggiunta allo shelf di dischi.	NESSUNO
Shelf di dischi alimentatore rimosso	INFORMATIVO	Questo messaggio viene visualizzato quando un alimentatore viene rimosso dallo shelf di dischi.	NESSUNO
Switchover automatico non pianificato MetroCluster disattivato	CRITICO	Questo messaggio viene visualizzato quando la funzione di switchover automatico non pianificato è disattivata.	Eseguire il comando "MetroCluster modify -node-name <nodename> -automatic-switchover -onfailure true" per ciascun nodo del cluster per abilitare lo switchover automatico.
Bridge di storage MetroCluster non raggiungibile	CRITICO	Il bridge di storage non è raggiungibile tramite la rete di gestione	1) se il bridge è monitorato da SNMP, verificare che la LIF di gestione dei nodi sia attiva utilizzando il comando "network interface show" (mostra interfaccia di rete). Verificare che il bridge sia attivo utilizzando il comando "ping di rete". 2) se il bridge è monitorato in banda, controllare il cablaggio del fabric del bridge, quindi verificare che il bridge sia acceso.
Temperatura del ponte MetroCluster anomala - inferiore al valore critico	CRITICO	Il sensore sul bridge Fibre Channel segnala una temperatura inferiore alla soglia critica.	1) controllare lo stato operativo delle ventole sul bridge di storage. 2) verificare che il bridge funzioni alle condizioni di temperatura consigliate.

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Temperatura del ponte MetroCluster anomala - superiore al valore critico	CRITICO	Il sensore del bridge Fibre Channel segnala una temperatura superiore alla soglia critica.	1) controllare lo stato operativo del sensore di temperatura del telaio sul bridge di storage utilizzando il comando "storage bridge show -cooling". 2) verificare che lo storage bridge funzioni alle condizioni di temperatura consigliate.
Aggregato MetroCluster lasciato indietro	ATTENZIONE	L'aggregato è stato lasciato indietro durante lo switchback.	1) controllare lo stato aggregato utilizzando il comando "aggr show". 2) se l'aggregato è online, restituirlo al proprietario originale utilizzando il comando "MetroCluster switchback".
Tutti i collegamenti tra i partner MetroCluster non sono disponibili	CRITICO	Gli adattatori di interconnessione RDMA e i LIF intercluster hanno interrotto le connessioni al cluster peered o il cluster peered è inattivo.	1) assicurarsi che le LIF dell'intercluster siano attive. Riparare le LIF dell'intercluster se non sono attive. 2) verificare che il cluster peered sia attivo e in esecuzione utilizzando il comando "cluster peer ping". Se il cluster peered non è attivo, consultare la Guida al disaster recovery di MetroCluster. 3) per Fabric MetroCluster, verificare che gli ISL del fabric back-end siano attivi e in esecuzione. Riparare gli ISL del fabric back-end se non sono attivi. 4) per le configurazioni MetroCluster non fabric, verificare che il cablaggio tra gli adattatori di interconnessione RDMA sia corretto. Riconfigurare il cablaggio se i collegamenti non sono attivi.

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
I partner MetroCluster non sono raggiungibili tramite la rete peering	CRITICO	La connettività al cluster peer è interrotta.	1) assicurarsi che la porta sia collegata alla rete o allo switch corretto. 2) assicurarsi che la LIF dell'intercluster sia connessa al cluster peered. 3) assicurarsi che il cluster peered sia attivo e in esecuzione utilizzando il comando "cluster peer ping". Se il cluster peered non è attivo, consultare la Guida al disaster recovery di MetroCluster.
Inter MetroCluster Disattiva tutti i collegamenti	CRITICO	Tutti i collegamenti Inter-Switch (ISL) sullo switch di storage non sono attivi.	1) riparare gli ISL del fabric back-end sullo switch storage. 2) assicurarsi che lo switch del partner sia attivo e che i relativi ISL siano operativi. 3) assicurarsi che le apparecchiature intermedie, come i dispositivi xWDM, siano operative.
Collegamento SAS da nodo MetroCluster a stack di storage inattivo	ATTENZIONE	L'adattatore SAS o il relativo cavo collegato potrebbero essere guasti.	1. Verificare che l'adattatore SAS sia in linea e in esecuzione. 2. Verificare che il collegamento fisico del cavo sia corretto e funzionante, quindi sostituire il cavo se necessario. 3. Se l'adattatore SAS è collegato agli shelf di dischi, assicurarsi che gli IOM e i dischi siano inseriti correttamente.
Link di MetroClusterFC Initiator non attivi	CRITICO	L'adattatore iniziatore FC è guasto.	1. Assicurarsi che il collegamento FC Initiator non sia stato manomesso. 2. Verificare lo stato operativo della scheda FC Initiator utilizzando il comando "System node run -node local -command storage show adapter".

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Collegamento interconnessione FC-VI inattivo	CRITICO	Il collegamento fisico sulla porta FC-VI è offline.	1. Assicurarsi che il collegamento FC-VI non sia stato manomesso. 2. Verificare che lo stato fisico dell'adattatore FC-VI sia "Up" (attivo) utilizzando il comando "MetroCluster Interconnect Adapter show" (Mostra adattatore di interconnessione). 3. Se la configurazione include switch fabric, assicurarsi che siano cablati e configurati correttamente.
Dischi di riserva MetroCluster lasciati dietro	ATTENZIONE	Il disco spare è stato lasciato indietro durante lo switchback.	Se il disco non presenta guasti, restituirlo al proprietario originale utilizzando il comando "MetroCluster switchback".
Porta bridge storage MetroCluster inattiva	CRITICO	La porta dello storage bridge non è in linea.	1) controllare lo stato operativo delle porte sul bridge di storage utilizzando il comando "storage bridge show -ports". 2) verificare la connettività logica e fisica alla porta.
Guasto alle ventole dello switch di storage MetroCluster	CRITICO	La ventola dello switch di storage si è guastata.	1) assicurarsi che le ventole dell'interruttore funzionino correttamente utilizzando il comando "storage switch show -cooling". 2) assicurarsi che le FRU delle ventole siano inserite correttamente e funzionino correttamente.

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Switch storage MetroCluster non raggiungibile	CRITICO	Lo switch di storage non è raggiungibile tramite la rete di gestione.	1) assicurarsi che la LIF di gestione dei nodi sia attiva utilizzando il comando "network interface show". 2) assicurarsi che lo switch sia attivo utilizzando il comando "ping di rete". 3) assicurarsi che lo switch sia raggiungibile tramite SNMP controllando le relative impostazioni SNMP dopo aver effettuato l'accesso allo switch.
Guasto agli alimentatori dello switch MetroCluster	CRITICO	Un'unità di alimentazione dello switch di storage non è operativa.	1) controllare i dettagli dell'errore utilizzando il comando "storage switch show -error -switch-name <swtich name>". 2) identificare l'alimentatore difettoso utilizzando il comando "storage switch show -power -switch -name <switch name>". 3) assicurarsi che l'unità di alimentazione sia inserita correttamente nello chassis dello switch di storage e che sia completamente operativa.
Guasto dei sensori di temperatura dell'interruttore MetroCluster	CRITICO	Il sensore dello switch Fibre Channel si è guastato.	1) controllare lo stato di funzionamento dei sensori di temperatura sull'interruttore di memorizzazione utilizzando il comando "interruttore di memorizzazione mostra -raffreddamento". 2) verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Temperatura interruttore MetroCluster anomala	CRITICO	Il sensore di temperatura dello switch Fibre Channel ha rilevato una temperatura anomala.	1) controllare lo stato di funzionamento dei sensori di temperatura sull'interruttore di memorizzazione utilizzando il comando "interruttore di memorizzazione mostra -raffreddamento". 2) verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.
Heartbeat del Service Processor non rispettato	INFORMATIVO	Questo messaggio viene visualizzato quando ONTAP non riceve un segnale "heartbeat" previsto dal processore di servizio (SP). Insieme a questo messaggio, i file di log di SP verranno inviati per il debug. ONTAP ripristina l'SP per tentare di ripristinare la comunicazione. Durante il riavvio, l'SP non sarà disponibile per un massimo di due minuti.	Contattare il supporto tecnico di NetApp.

Nome monitor	Severità	Descrizione del monitor	Azione correttiva
Heartbeat del Service Processor interrotto	ATTENZIONE	Questo messaggio viene visualizzato quando ONTAP non riceve più heartbeat dal processore di servizio (SP). A seconda della progettazione dell'hardware, il sistema può continuare a fornire dati o determinare lo spegnimento per evitare la perdita di dati o danni all'hardware. Il sistema continua a fornire dati, ma poiché il SP potrebbe non funzionare, il sistema non può inviare notifiche di appliance non funzionanti, errori di avvio o errori POST (Power-on Self-Test) di Open firmware (OFW). Se il sistema è configurato per farlo, genera e trasmette un messaggio AutoSupport (o "call home") al supporto tecnico NetApp e alle destinazioni configurate. La corretta erogazione di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Se il sistema si è spento, provare a spegnere e riaccendere il sistema: Estrarre il controller dal telaio, reinserirlo e riaccenderlo. Contattare il supporto tecnico NetApp se il problema persiste dopo il ciclo di alimentazione o per qualsiasi altra condizione che possa richiedere attenzione.

Torna all'inizio

Ulteriori informazioni

- "Visualizzazione e disattivazione degli avvisi"

API Cloud Insights

L'API Cloud Insights consente ai clienti NetApp e ai vendor di software indipendenti (ISV) di integrare Cloud Insights con altre applicazioni, come CMDB o altri sistemi di ticketing.

Tenere presente che le API Cloud Insights sono disponibili in base all'edizione corrente:

Tipo API	Di base	Standard	Premium
Unità di acquisizione	✔	✔	✔
Raccolta di dati	✔	✔	✔
Avvisi		✔	✔
Risorse		✔	✔
Acquisizione dei dati		✔	✔
Gestione dei log		✔	✔

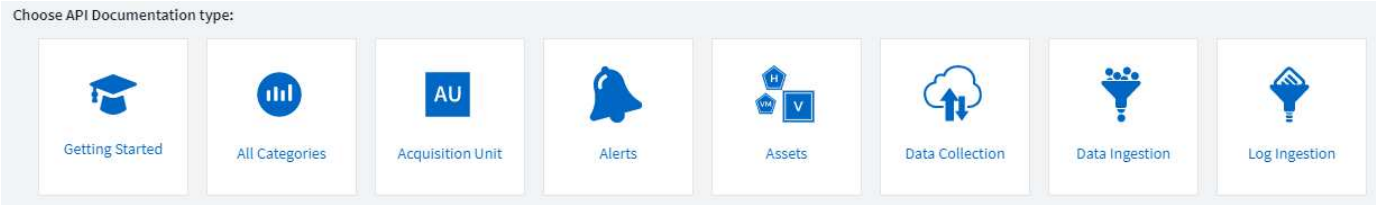
Inoltre, il tuo Cloud Insights "ruolo del set di funzionalità" Determina le API a cui è possibile accedere. I ruoli utente e ospite hanno meno privilegi rispetto al ruolo Amministratore. Ad esempio, se si ha il ruolo di amministratore in Monitor e Optimize, ma il ruolo di utente in Reporting, è possibile gestire tutti i tipi di API tranne Data Warehouse.

Requisiti per l'accesso API

- Per concedere l'accesso viene utilizzato un modello API Access Token.
- La gestione del token API viene eseguita dagli utenti Cloud Insights con il ruolo di amministratore.

Documentazione API (Swagger)

Le informazioni API più recenti si trovano accedendo a Cloud Insights e accedendo a **Amministratore > accesso API**. Fare clic sul collegamento **documentazione API**.



La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla nel proprio ambiente. A seconda del ruolo dell'utente e/o dell'edizione di Cloud Insights, i tipi di API disponibili possono variare.

ASSETS.annotations

POST `/assets/annotations` Create annotation definition

Parameters | Try it out

No parameters

Request body | application/json

Request body should include required name, type, optional description and enumValues (if enum type). Enums should contain name and label. Example:

```
{
    "name": "StorageLocation",
    "type": "FIXED_ENUM",
    "description": "Storage Location",
    "enumValues": [
        {
          "name": "PT_LISBON",
          "label": "Lisbon (Portugal)"
        },
        {
          "name": "US_WALTHAM",
          "label": "Waltham (USA)"
        }
    ]
}
```

Example Value | Schema

```
{}
```

Token di accesso API

Prima di utilizzare l'API Cloud Insights, è necessario creare uno o più **token di accesso API**. I token di accesso vengono utilizzati per tipi di API specifici e possono concedere permessi di lettura e/o scrittura. È inoltre possibile impostare la scadenza per ciascun token di accesso. Tutte le API dei tipi specificati sono valide per il token di accesso. Ogni token non contiene un nome utente o una password.

Per creare un token di accesso:

- Fare clic su **Admin > API Access** (Amministratore > accesso API)
- Fare clic su **+token di accesso API**
  - Immettere il nome del token
  - Selezionare i tipi di API
  - Specificare le autorizzazioni concesse per questo accesso API
  - Specificare la scadenza del token

> Il token sarà disponibile solo per la copia negli Appunti e il salvataggio durante il processo di creazione. I token non possono essere recuperati dopo la loro creazione, pertanto si consiglia vivamente di copiarli e salvarli in una posizione sicura. Verrà richiesto di fare clic sul pulsante **Copy API Access Token** (Copia token di accesso API) prima di chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. È possibile attivare i token disattivati.

I token garantiscono l'accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio tenant. Gli amministratori dei clienti possono concedere e revocare questi token senza il coinvolgimento diretto del personale back-end di Cloud Insights.

L'applicazione riceve un token di accesso dopo che un utente ha autenticato e autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token passato informa l'API che la portante del token è stata autorizzata ad accedere all'API ed eseguire azioni specifiche specificate dall'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-apiKey:**.

Ad esempio, utilizzare quanto segue per recuperare le risorse di storage:

```
 curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-
CloudInsights-ApiKey:<API_Access_Token>'
Dove _<API_Access_Token>_ è il token salvato durante la creazione
dell'accesso API.
```

Consulta le pagine swagger per esempi specifici dell'API che desideri utilizzare.

Tipo API

L'API Cloud Insights è basata sulle categorie e attualmente contiene i seguenti tipi:

- IL tipo DI ASSET contiene API di risorse, query e ricerca.
  - Asset: Enumerare gli oggetti di primo livello e recuperare un oggetto specifico o una gerarchia di oggetti.
  - Query: Recuperare e gestire le query Cloud Insights.
  - Import (Importa): Consente di importare annotazioni o applicazioni e assegnarle agli oggetti
  - Search (Cerca): Consente di individuare un oggetto specifico senza conoscere l'ID univoco o il nome completo dell'oggetto.
- Il tipo DI RACCOLTA DATI viene utilizzato per recuperare e gestire i data collection.
- Il tipo DI ACQUISIZIONE DEI DATI viene utilizzato per recuperare e gestire i dati di acquisizione e le metriche personalizzate, ad esempio da agenti di Telegraf
- L'ACQUISIZIONE DEI LOG viene utilizzata per recuperare e gestire i dati dei log

Altri tipi e/o API potrebbero diventare disponibili nel tempo. Le informazioni API più recenti sono disponibili in "Documentazione API Swagger".

Si noti che i tipi di API a cui un utente ha accesso dipendono anche da "Ruolo dell'utente" Sono presenti in

ogni set di funzionalità Cloud Insights (monitoraggio, sicurezza del carico di lavoro, reporting).

Attraversamento dell'inventario

In questa sezione viene descritto come attraversare una gerarchia di oggetti Cloud Insights.

Oggetti di livello superiore

I singoli oggetti vengono identificati nelle richieste tramite URL univoco (chiamato "self" in JSON) e richiedono la conoscenza del tipo di oggetto e dell'ID interno. Per alcuni degli oggetti di primo livello (host, storage e così via), L'API REST fornisce l'accesso all'insieme completo.

Il formato generale di un URL API è:

```
 https://<tenant>/rest/v1/<type>/<object>
Ad esempio, per recuperare tutti gli storage da un tenant denominato
_mysite.c01.cloudinsights.netapp.com_, l'URL della richiesta è:
```

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

Figli e oggetti correlati

Gli oggetti di livello superiore, come Storage, possono essere utilizzati per passare ad altri oggetti figlio e correlati. Ad esempio, per recuperare tutti i dischi per uno storage specifico, concatenare l'URL "self" dello storage con "/disks", ad esempio:

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

Si espande

Molti comandi API supportano il parametro **espandi**, che fornisce ulteriori dettagli sull'oggetto o sugli URL per gli oggetti correlati.

L'unico parametro di espansione comune è *Expands*. La risposta contiene un elenco di tutte le espansi specifiche disponibili per l'oggetto.

Ad esempio, quando si richiede quanto segue:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
L'API restituisce tutte le espansi disponibili per l'oggetto come segue:
```

```
{
    "id": "1247936",
      "self": "/rest/v1/assets/storages/1247936",
      "name": "amsprdclu01",
      "simpleName": "amsprdclu01",
      "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
      "ip": "10.64.0.132",
      "serialNumber": "1-80-000011",
      "model": "FAS3270,FAS6290",
      "vendor": "NetApp",
      "microcodeVersion": "8.1.3 clustered Data ONTAP",
      "capacity": {
        "description": "Storage Capacity",
        "unitType": "MB",
        "total": {
          "value": 8.23185105E8
        },
        "storagePools": {
          "value": 5.43220974E8
        }
      },
      "isActive": true,
      "createTime": "2013-05-07T16:52:21-0700",
      "family": "FAS3200,FAS6200",
      "managementUrl": null,
      "virtualizedType": "STANDARD",
      "protocols":
      [
        "NAS",
        "NFS",
        "CIFS",
        "FC",
        "ISCSI"
      ],
      "_expands": {
        "performance": {
          "url": "/rest/v1/assets/storages/1247936/performance",
          "name": "Performance Data"
        },
        "storageNodes": {
          "url": "/rest/v1/assets/storages/1247936/storageNodes",
          "name": "Storage Storage Nodes"
        },
        "storagePools": {
          "url": "/rest/v1/assets/storages/1247936/storagePools",
          "name": "Storage Storage Pools"
        },
        "storageResources": {
          "url": "/rest/v1/assets/storages/1247936/storageResources",
          "name": "Storage Storage Resourcs"
        },
        "internalVolumes": {
          "url": "/rest/v1/assets/storages/1247936/internalVolumes",
          "name": "Storage Internal Volumes"
        },
        "volumes": {
          "url": "/rest/v1/assets/storages/1247936/volumes",
          "name": "Storage Volumes"
        },
        "disks": {
          "url": "/rest/v1/assets/storages/1247936/disks",
          "name": "Disks"
        },
        "datasources": {
          "url": "/rest/v1/assets/storages/1247936/datasources",
          "name": "Storage Datasources"
        },
        "ports": {
          "url": "/rest/v1/assets/storages/1247936/ports",
          "name": "Storage Ports"
        },
        "annotations": {
          "url": "/rest/v1/assets/storages/1247936/annotations",
          "name": "Storage Annotations"
        },
        "qtrees": {
          "url": "/rest/v1/assets/storages/1247936/qtrees",
          "name": "Qtrees"
        },
```

Ogni espansione contiene dati, un URL o entrambi. Il parametro expand supporta attributi multipli e nidificati, ad esempio:

```
 https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageR
esources.storage
Expand consente di trasferire molti dati correlati in un'unica risposta.
NetApp consiglia di non richiedere troppe informazioni contemporaneamente;
ciò può causare un peggioramento delle performance.
```

Per scoraggiarlo, non è possibile espandere le richieste di raccolte di livello superiore. Ad esempio, non è possibile richiedere l'espansione dei dati per tutti gli oggetti di storage contemporaneamente. I client devono recuperare l'elenco di oggetti e scegliere gli oggetti specifici da espandere.

Dati sulle performance

I dati sulle performance vengono raccolti su molti dispositivi come campioni separati. Ogni ora (impostazione predefinita), Cloud Insights aggrega e riepiloga i campioni di performance.

L'API consente di accedere sia ai campioni che ai dati riepilogati. Per un oggetto con dati sulle performance, è disponibile un riepilogo delle performance come *expand=performance*. Le serie temporali della cronologia delle performance sono disponibili attraverso *expand=performance.history* annidato.

Esempi di oggetti dati sulle performance includono:

- StoragePerformance
- StoragePoolPerformance
- Performance di portperformance
- DiskPerformance

Una metrica delle performance ha una descrizione e un tipo e contiene una raccolta di riepiloghi delle performance. Ad esempio, latenza, traffico e velocità.

Un Riepilogo delle performance contiene una descrizione, un'unità, un'ora di inizio del campione, un'ora di fine del campione e un insieme di valori riepilogati (corrente, min, max, media, ecc.) calcolati da un singolo contatore delle performance in un intervallo di tempo (1 ora, 24 ore, 3 giorni e così via).

https://tenant.cloudinsights.netapp.com/rest/v1/assets/storages/1/performance?expand=history

Details

Response body


```
{
  "self": "/rest/v1/assets/storages/1/performance",
  "cacheHitRatio": {
    "read": {
      "description": "Cache Hit Ratio - Read",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null,
      "sum": null,
      "isDownsampled": false
    },
    "write": {
      "description": "Cache Hit Ratio - Write",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null
```


Self

Performance Metric

Response body


```
    }
  },
  "history": [
    [
      1578418848140,
      {
        "latency.total": 1.30578,
        "latency.read": 3.64681,
        "ioDensity.read": 9.62065,
        "iops.write": 686.35502,
        "ioDensity.total": 31.36259,
        "capacity.raw": 80024.92772,
        "throughput.read": 7.32371,
        "iops.total": 1488.7974,
        "latency.write": 0.39495,
        "ioDensity.write": 14.45856,
        "iops.read": 456.69703,
        "capacity.storagePools": 56058.1041,
        "throughput.write": 14.59581,
        "throughput.total": 21.91953
      }
    ],
    [
      1578419748198,
```


History

Timestamp

Counter Values

Il dizionario dei dati sulle prestazioni risultante dispone delle seguenti chiavi:

- "Self" è l’URL univoco dell’oggetto

- "cronologia" è l'elenco di coppie di valori di timestamp e mappa dei contatori
- Ogni altra chiave del dizionario ("diskThroughput" e così via) è il nome di una metrica delle performance.

Ogni tipo di oggetto dati sulle performance ha un insieme unico di metriche delle performance. Ad esempio, l'oggetto performance della macchina virtuale supporta "diskThroughput" come metrica delle performance. Ogni metrica di performance supportata è di una determinata "performanceCategory" presentata nel dizionario delle metriche. Cloud Insights supporta diversi tipi di metriche delle performance elencati più avanti in questo documento. Ogni dizionario delle metriche di performance avrà anche il campo "description" (Descrizione) che è una descrizione leggibile di questa metrica di performance e una serie di voci del contatore di riepilogo delle performance.

Il contatore Performance Summary è il riepilogo dei contatori delle performance. Presenta i valori aggregati tipici come min, max e AVG per un contatore e anche l'ultimo valore osservato, l'intervallo di tempo per i dati riepilogati, il tipo di unità per il contatore e le soglie per i dati. Solo le soglie sono facoltative; gli altri attributi sono obbligatori.

Sono disponibili riepiloghi delle performance per i seguenti tipi di contatori:

- Read – Riepilogo per le operazioni di lettura
- Scrittura – Riepilogo per operazioni di scrittura
- Total (totale): Riepilogo di tutte le operazioni. Può essere superiore alla semplice somma di lettura e scrittura; può includere altre operazioni.
- Total Max (massimo totale): Riepilogo di tutte le operazioni. Questo è il valore totale massimo nell'intervallo di tempo specificato.

Metriche delle performance degli oggetti

L'API può restituire metriche dettagliate per gli oggetti nel tuo ambiente, ad esempio:

- Metriche delle performance dello storage come IOPS (numero di richieste di input/output al secondo), latenza o throughput.
- Metriche delle prestazioni dello switch, ad esempio utilizzo del traffico, dati BB Credit Zero o errori delle porte.

Vedere "Documentazione API Swagger" per informazioni sulle metriche per ciascun tipo di oggetto.

Dati della cronologia delle performance

I dati della cronologia vengono presentati nei dati delle performance come un elenco di coppie di timestamp e mappe dei contatori.

I contatori della cronologia vengono denominati in base al nome dell'oggetto della metrica delle prestazioni. Ad esempio, l'oggetto performance della macchina virtuale supporta "diskThroughput", pertanto la mappa della cronologia conterrà chiavi denominate "diskThroughput.Read", "diskThroughput.write" e "diskThroughput.total".

Timestamp è in formato UNIX Time.

Di seguito viene riportato un esempio di dati JSON relativi alle performance per un disco:

```
"performance": {
    "self": "/rest/v1/assets/disks/4013931/performance",
    "iops": {
      "performanceCategory": "IOPS",
      "description": "Disk IOPS",
      "read": {
        "description": "Disk Read Iops",
        "unitType": "IO/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 1,
        "min": 0,
        "max": 6,
        "avg": 0.5532
      },
  […]
     "total": {
        "description": "Disk Total Throughput",
        "unitType": "MB/s",
        "start": 1399305599999,
        "end": 1402604368055,
        "current": 0,
        "min": 0,
        "max": 2,
        "avg": 0.1702
      }
    },
    "history":
    [
      [
        1399300412690,
        {
          "utilization.total": 12,
          "iops.total": 26,
          "iops.write": 22,
          "iops.read": 4,
          "throughput.read": 0,
          "utilization.read": 2.12,
          "throughput.total": 5,
          "utilization.write": 10.24,
          "throughput.write": 5
```


Oggetti con attributi di capacità

Gli oggetti con attributi di capacità utilizzano tipi di dati di base e CapacityItem per la rappresentazione.

CapacityItem

CapacityItem è una singola unità logica di capacità. Ha "valore" e "highThreshold" in unità definite dal relativo oggetto padre. Supporta inoltre una mappa di dettaglio opzionale che spiega come viene costruito il valore della capacità. Ad esempio, la capacità totale di uno storagePool da 100 TB sarebbe un CapacityItem con un valore di 100. La ripartizione potrebbe indicare 60 TB allocati per "dati" e 40 TB per "snapshot".

Nota

"HighThreshold" rappresenta le soglie definite dal sistema per le metriche corrispondenti, che un client può utilizzare per generare avvisi o segnali visivi su valori che non rientrano negli intervalli configurati accettabili.

Di seguito viene illustrata la capacità di StoragePools con contatori di capacità multipli:

StoragePoolCapacity

```
Model properties:
{
 description: string
 unitType: 'MB' or 'GB' or 'TB' or 'KiB' or 'MiB' or 'TiB'
 total: CapacityItem
 used: CapacityItem
 provisioned: CapacityItem
 reservedCapacity: CapacityItem
 softLimit: Double
 rawToUsableRatio: Double
 isDedupeEnabled: boolean
 dedupeSavings: NumericValueWithUnit
 isCompressionEnabled: boolean
 compressionSavings: NumericValueWithUnit
 isThinProvisioningSupported: boolean
}
```

close

Utilizzo di Search per cercare oggetti

L'API di ricerca è un semplice punto di accesso al sistema. L'unico parametro di input per l'API è una stringa in formato libero e il JSON risultante contiene un elenco categorizzato di risultati. I tipi sono diversi tipi di risorse dall'inventario, ad esempio storage, host, datastore e così via. Ogni tipo contiene un elenco di oggetti del tipo che corrispondono ai criteri di ricerca.

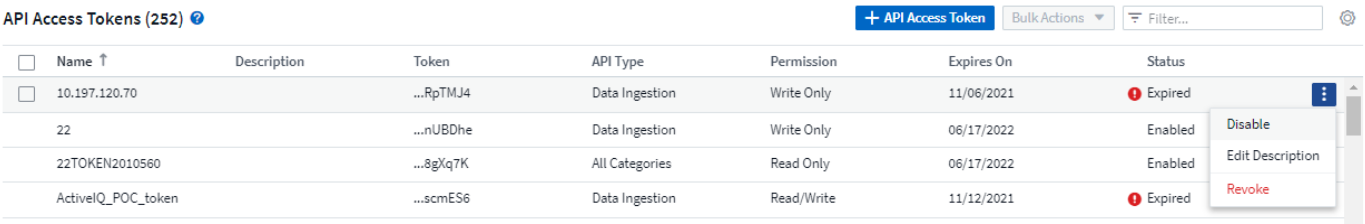
Cloud Insights è una soluzione estensibile (ampiamente aperta) che consente integrazioni con sistemi di orchestrazione, gestione aziendale, controllo delle modifiche e ticketing di terze parti, oltre a integrazioni CMDB personalizzate.

L'API RESTful di Cloud Insight è un punto primario di integrazione che consente uno spostamento semplice ed efficace dei dati e consente agli utenti di ottenere un accesso perfetto ai propri dati.

Disattivazione o revoca di un token API

Per disattivare temporaneamente un token API, nella pagina di elenco dei token API, fare clic sul menu "tre punti" dell'API e selezionare *Disable*. Puoi riattivare il token in qualsiasi momento utilizzando lo stesso menu e selezionando *Enable*.

Per rimuovere in modo permanente un token API, selezionare "revoca" dal menu. Non è possibile riattivare un token revocato; è necessario creare un nuovo token.



Rotazione dei token di accesso API scaduti

I token di accesso API hanno una data di scadenza. Quando un token di accesso API scade, gli utenti devono generare un nuovo token (di tipo *Data Ingestion* con permessi di lettura/scrittura) e riconfigurare Telegraf per utilizzare il token appena generato invece del token scaduto. La procedura riportata di seguito illustra in dettaglio la procedura da seguire.

Kubernetes

Si noti che questi comandi utilizzano lo spazio dei nomi predefinito "netapp-monitoring". Se è stato impostato uno spazio dei nomi personalizzato, sostituire tale spazio dei nomi in questi e in tutti i comandi e file successivi.

Nota: Se si dispone dell'ultimo NetApp Kubernetes Monitoring Operator installato e si utilizza un token di accesso API rinnovabile, i token in scadenza verranno sostituiti automaticamente da token di accesso API nuovi/aggiornati. Non è necessario eseguire i passaggi manuali elencati di seguito.

- Modifica l'operatore di monitoraggio NetApp Kubernetes.

```
 kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* Modificare il valore _spec.output-sink.api-key_, sostituendo il
vecchio token API con il nuovo token API.
```

```
spec:
…
  output-sink:
  - api-key:<NEW_API_TOKEN>
```

RHEL/CentOS e Debian/Ubuntu

- Modificare i file di configurazione di Telegraf e sostituire tutte le istanze del vecchio token API con il nuovo token API.

```
 sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* Riavviare Telegraf.
```

```
sudo systemctl restart telegraf
```

Windows

- Per ogni file di configurazione di Telegraf in *C: File di programma telegraf telegraf.d*, sostituire tutte le istanze del vecchio token API con il nuovo token API.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- Riavviare Telegraf.

```
Stop-Service telegraf
Start-Service telegraf
```

Notifica tramite webhook

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato.

Molte applicazioni commerciali supportano i webhook come interfaccia di input standard, ad esempio Slack, PagerDuty, Teams e Discord. Grazie al supporto di un canale webhook generico e personalizzabile, Cloud Insights è in grado di supportare molti di questi canali di delivery. Le informazioni sui webhook sono disponibili su questi siti Web delle applicazioni. Ad esempio, Slack fornisce "questa utile guida".

È possibile creare più canali webhook, ciascun canale destinato a uno scopo diverso; applicazioni separate, destinatari diversi, ecc.

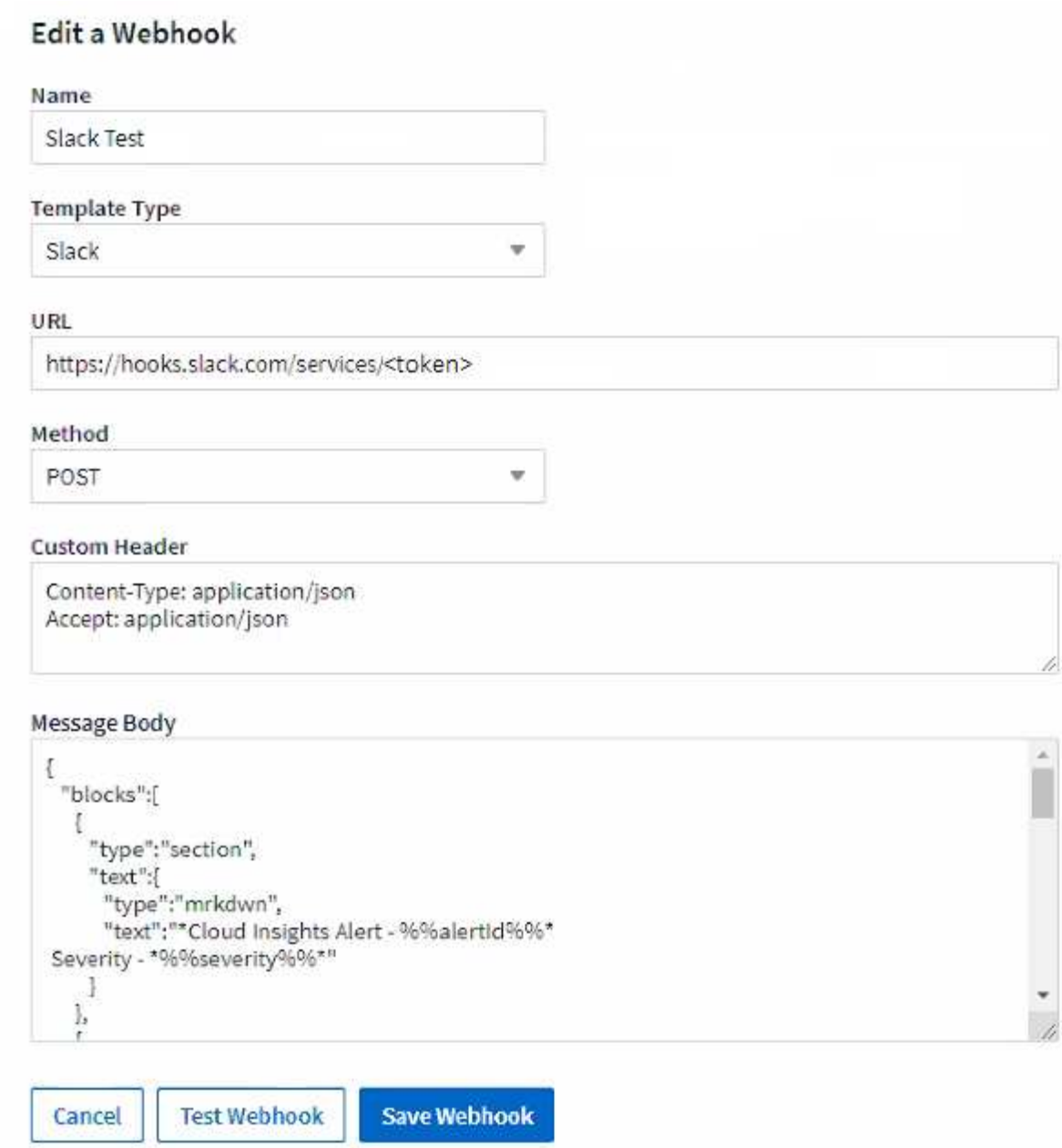
L'istanza del canale webhook comprende i seguenti elementi:

Nome	Nome univoco
URL	URL di destinazione di Webhook, incluso il prefisso *http://* o *https://* insieme ai parametri dell'URL
Metodo	GET, POST - l'impostazione predefinita è POST
Intestazione personalizzata	Specificare qui le righe di intestazione personalizzate
Corpo del messaggio	Inserisci il corpo del messaggio qui
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri e i segreti personalizzati consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook Cloud Insights, vai a **Amministratore > Notifiche** e seleziona la scheda **webhook**.

L'immagine seguente mostra un webhook di esempio configurato per l'allentamento:



Inserire le informazioni appropriate per ciascuno dei campi e fare clic su "Save" (Salva) al termine dell'operazione.

È inoltre possibile fare clic sul pulsante "Test Webhook" per verificare la connessione. Si noti che questo invierà il "corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.

I webhook Cloud Insights comprendono una serie di parametri predefiniti. Inoltre, è possibile creare i propri segreti o parametri personalizzati.

Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ('Tue, 27 Oct 2020 01:20:30 GMT')
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

Custom Parameters and Secrets

Name	Value	Description
No Data Available		

+ Parameter

Parametri: Quali sono e come li utilizzo?

I parametri di avviso sono valori dinamici popolati per avviso. Ad esempio, il parametro *%%TriggeredOn%%* verrà sostituito con l'oggetto su cui è stato attivato l'avviso.

Si noti che in questa sezione, le sostituzioni vengono *non* eseguite facendo clic sul pulsante "Test Webhook"; il pulsante invia un payload che mostra le sostituzioni %, ma non le sostituisce con i dati.

Parametri e segreti personalizzati

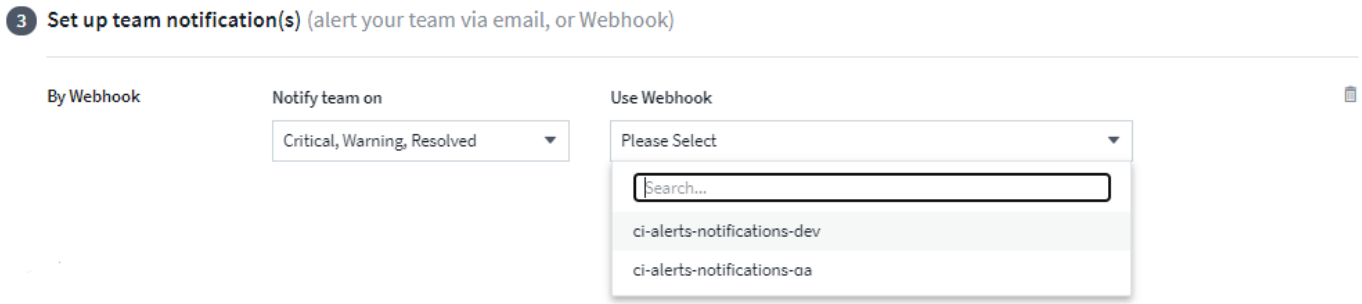
In questa sezione è possibile aggiungere i parametri e/o i segreti personalizzati desiderati. Per motivi di sicurezza, se viene definito un segreto, solo il creatore di webhook può modificare questo canale webhook. È di sola lettura per gli altri. Puoi utilizzare i segreti in URL/intestazioni come *%%<secret_name>%%*.

Pagina elenco webhook

Nella pagina dell'elenco dei webhook, vengono visualizzati il nome, creato da, creato da, Stato, protetto, e ultimi campi segnalati.

Scelta di Webhook Notification in a Monitor

Per scegliere la notifica webhook in un "monitorare", Accedere a **Alerts > Manage Monitors** (Avvisi > Gestione monitor) e selezionare il monitor desiderato oppure aggiungere un nuovo monitor. Nella sezione *Imposta notifiche team*, scegli *Webhook* come metodo di consegna. Selezionare i livelli di avviso (critico, Avviso, risolto), quindi scegliere il webhook desiderato.



Esempi di webhook:

Webhook per "Lasco"Webhook per "PagerDuty"Webhook per "Team"Webhook per "Discordare"

Monitoraggio dell’ambiente

Controllo

Per identificare le modifiche previste (per il monitoraggio) o impreviste (per la risoluzione dei problemi), è possibile visualizzare un audit trail degli eventi del sistema Cloud Insights e delle attività dell’utente.

Visualizzazione degli eventi controllati

Per visualizzare la pagina Audit, fare clic su **Admin > Audit** nel menu. Viene visualizzata la pagina Audit, che fornisce i seguenti dettagli per ciascuna voce di audit:

- **Ora** - Data e ora dell’evento o dell’attività
- **Utente** - l’utente che ha avviato l’attività
- **Ruolo** - ruolo dell’utente in Cloud Insights (guest, utente, amministratore)
- **IP** - l’indirizzo IP associato all’evento
- **Azione** - tipo di attività, ad esempio Login, Crea, Aggiorna
- **Categoria** - la categoria di attività
- **Dettagli** - Dettagli dell’attività

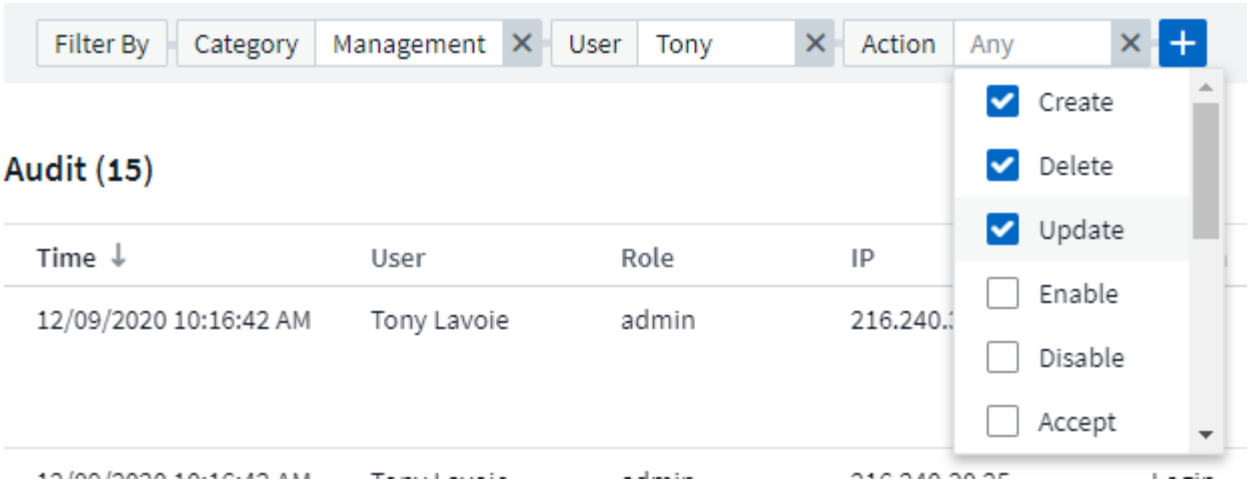
Visualizzazione delle voci di audit

Esistono diversi modi per visualizzare le voci di audit:

- È possibile visualizzare le voci di audit scegliendo un periodo di tempo specifico (1 ora, 24 ore, 3 giorni, ecc.).
- È possibile modificare l’ordinamento delle voci in crescente (freccia su) o decrescente (freccia giù) facendo clic sulla freccia nell’intestazione della colonna.

  Per impostazione predefinita, la tabella visualizza le voci in ordine decrescente.

- È possibile utilizzare i campi di filtro per visualizzare solo le voci desiderate nella tabella. Fare clic sul pulsante [+] per aggiungere altri filtri.



Ulteriori informazioni sul filtraggio

Per perfezionare il filtro, è possibile utilizzare una delle seguenti opzioni:

Filtro	Che cosa fa	Esempio	Risultato
* (Asterisco)	consente di cercare tutto	vol*rhel	restituisce tutte le risorse che iniziano con "vol" e terminano con "rhel"
? (punto interrogativo)	consente di cercare un numero specifico di caratteri	BOS-PRD??-S12	Restituisce BOS-PRD***12***-S12, BOS-PRD***23***-S12 e così via
OPPURE	consente di specificare più entità	FAS2240, CX600 O FAS3270	Restituisce FAS2440, CX600 o FAS3270
NO	consente di escludere il testo dai risultati della ricerca	NON EMC*	Restituisce tutto ciò che non inizia con "EMC"
Nessuno	Cerca vuoto/NULL/None in qualsiasi campo dove selezionato	*Nessuno*	restituisce risultati in cui il campo di destinazione non è vuoto
Non *	Come per *None*, ma puoi anche utilizzare questo modulo per cercare i valori NULL nei campi *text-only*	Non *	restituisce risultati in cui il campo di destinazione non è vuoto.
""	ricerca una corrispondenza esatta	"NetApp*"	Restituisce i risultati contenenti la stringa letterale esatta *NetApp**

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 "*" restituirà risultati che sono un asterisco letterale; in questo caso, l'asterisco non verrà trattato come carattere jolly. Gli operatori O e NON verranno trattati come stringhe letterali se racchiusi tra virgolette doppie.

Eventi e azioni verificati

Gli eventi e le azioni controllati da Cloud Insights possono essere classificati nelle seguenti aree:

- **Account utente**: Accesso, disconnessione, modifica del ruolo, ecc.

  Esempio: *Utente **Tony Lavoie** connesso da **10.1.120.15**, agente utente **Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/85.0.4183.121 Safari/537.36**, metodi di login **Cloud Central Portal Login***

- **Acquisition Unit** (unità di acquisizione): Creare, eliminare, ecc.

  Esempio: *Unità di acquisizione **AU-Boston-1** rimossa*.

- **Data Collector**: Aggiungere, rimuovere, modificare, posticipare/riprendere, modificare l'unità di acquisizione, avvio/arresto, ecc.

  Esempio: *Origine dati **laboratorio FlexPod** rimosso, vendor **NetApp**, modello **Software di gestione dati ONTAP**, ip **192.168.106.5***.

- **Applicazione**: Aggiungere, assegnare a un oggetto, rimuovere, ecc.

  Esempio: *Volume interno **ocisedev:t1appSVM01:t1appFlexVol01** aggiunto all'applicazione **Test App***.

- **Annotation**: Aggiunta, assegnazione, rimozione, azioni delle regole di annotazione, modifiche dei valori delle annotazioni, ecc.

  Esempio: *Valore di annotazione **Boston** aggiunto al tipo di annotazione **SalesOffice***.

- **Query**: Aggiungere, rimuovere, ecc.

  Esempio: Aggiunta di _query **query di vendita TL**.

- **Monitor**: Aggiungere, rimuovere, ecc.

  Esempio: Monitor *AGGR Size - Avvisi ci Notifications Dev* aggiornato

- **Notifica**: Modifica email, ecc.

  Esempio: Creazione del destinatario *ci-alerts-notifications-dl*

Esportazione di eventi di audit

È possibile esportare i risultati della visualizzazione Audit in un file .CSV, che consente di analizzare i dati o importarli in un'altra applicazione.

Fasi

1. Nella pagina Audit, impostare l'intervallo di tempo desiderato e i filtri desiderati. Cloud Insights esporterà solo le voci di audit che corrispondono al filtro e all'intervallo di tempo impostati.
2. Fare clic sul pulsante *Export* nella parte superiore destra della tabella.

Gli eventi di audit visualizzati verranno esportati in un file .CSV, fino a un massimo di 10,000 righe.

Conservazione dei dati di audit

La quantità di tempo in cui Cloud Insights conserva i dati di audit si basa sull'edizione:

- Basic Edition: I dati di audit vengono conservati per 30 giorni
- Edizioni Standard e Premium: I dati di audit vengono conservati per 1 anno più 1 giorno

Le voci di audit precedenti al tempo di conservazione vengono eliminate automaticamente. Non è richiesta alcuna interazione da parte dell'utente.

Risoluzione dei problemi

Qui troverai suggerimenti per la risoluzione dei problemi con Audit.

Problema:	Provare questo:
Vengono visualizzati messaggi di audit che indicano che un monitor è stato esportato.	L'esportazione di una configurazione di monitor personalizzata viene generalmente utilizzata dai tecnici NetApp durante lo sviluppo e il test delle nuove funzionalità. Se non si prevede di visualizzare questo messaggio, esaminare le azioni dell'utente indicato nell'azione verificata o contattare il supporto.

Informazioni sulla pagina delle risorse

Panoramica della pagina delle risorse

Le pagine delle risorse riepilogano lo stato corrente di una risorsa e contengono collegamenti a informazioni aggiuntive sulla risorsa e sulle risorse correlate.

Tipi di pagine di risorse

Cloud Insights fornisce pagine di risorse per le seguenti risorse:

- Macchina virtuale
- SVM (Storage Virtual Machine)
- Volume
- Volume interno
- Host (incluso hypervisor)
- Pool di storage
- Storage
- Datastore
- Applicazione
- Nodo storage
- Qtree
- Disco
- VMDK
- Porta
- Switch
- Fabric

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 intervallo di tempo fisso o un intervallo di tempo personalizzato per visualizzare un numero inferiore o superiore di dati.

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. Per modificare l’intervallo di tempo, fare clic sull’intervallo di tempo visualizzato nella barra superiore e scegliere uno dei seguenti segmenti di tempo:

- Ultimi 15 minuti
- Ultimi 30 minuti
- Ultimi 60 minuti
- Ultime 2 ore
- Ultime 3 ore (impostazione predefinita)

- Ultime 6 ore
- Ultime 12 ore
- Ultime 24 ore
- Ultimi 2 giorni
- Ultimi 3 giorni
- Ultimi 7 giorni
- Ultimi 30 giorni
- Intervallo di tempo personalizzato

L'intervallo di tempo personalizzato consente di selezionare fino a 31 giorni consecutivi. È inoltre possibile impostare l'ora di inizio e l'ora di fine del giorno per questo intervallo. L'ora di inizio predefinita è 12:00 AM nel primo giorno selezionato e l'ora di fine predefinita è 11:59 PM nell'ultimo giorno selezionato. Fare clic su Apply (Applica) per applicare l'intervallo di tempo personalizzato alla pagina delle risorse.

Le informazioni contenute in una sezione di riepilogo delle pagine di asset, nonché in qualsiasi tabella o widget personalizzati sulla pagina, vengono aggiornate automaticamente in base all'intervallo di tempo selezionato. La frequenza di aggiornamento corrente viene visualizzata nell'angolo in alto a destra della sezione Riepilogo e in tutte le tabelle o i widget pertinenti della pagina.

Aggiungi widget personalizzati

È possibile aggiungere widget personalizzati a qualsiasi pagina di risorse. I widget aggiunti verranno visualizzati nelle pagine delle risorse per tutti gli oggetti di quel tipo. Ad esempio, l'aggiunta di un widget personalizzato a una pagina di risorse di storage consente di visualizzare tale widget nelle pagine di risorse per tutte le risorse di storage.

Filtraggio degli oggetti nel contesto

Durante la configurazione di un widget nella landing page di una risorsa, è possibile impostare i filtri *in-context* in modo da visualizzare solo gli oggetti direttamente correlati alla risorsa corrente. Per impostazione predefinita, quando si aggiunge un widget, vengono visualizzati *tutti* oggetti del tipo selezionato nell'ambiente. I filtri contestuali consentono di visualizzare solo i dati relativi alla risorsa corrente.

Nella maggior parte delle pagine di destinazione delle risorse, i widget consentono di filtrare gli oggetti correlati alla risorsa corrente. Nei menu a discesa dei filtri, i tipi di oggetti che visualizzano un'icona di collegamento  può essere filtrato nel contesto in base alla risorsa corrente.

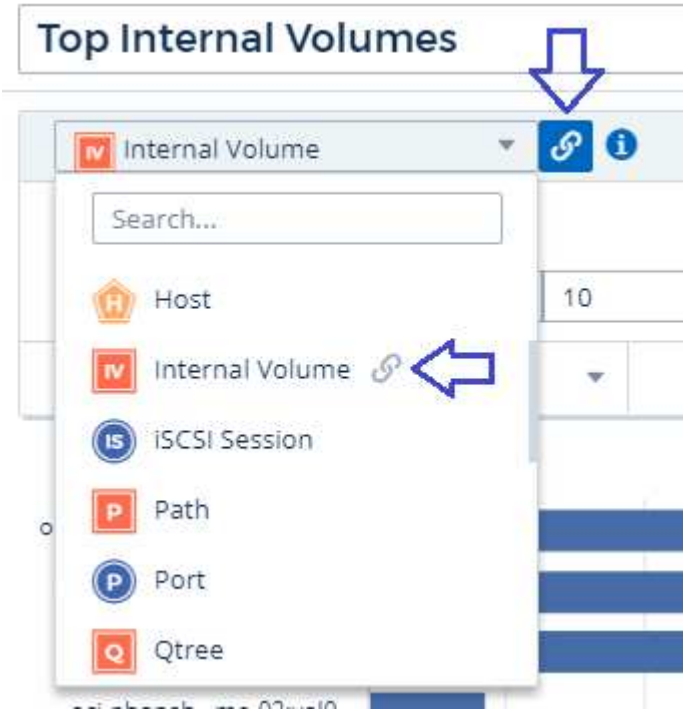
Ad esempio, in una pagina di risorse di storage, è possibile aggiungere un widget di grafico a barre per visualizzare i principali IOPS sui volumi interni solo su tale storage. Per impostazione predefinita, quando si aggiunge un widget, vengono visualizzati *tutti* i volumi interni nell'ambiente.

Per visualizzare solo i volumi interni sulla risorsa di storage corrente, procedere come segue:

Fasi

1. Aprire una pagina delle risorse per qualsiasi risorsa **Storage**.
2. Fare clic su **Edit** (Modifica) per aprire la pagina delle risorse in modalità Edit (Modifica).

3. Fare clic su **Add Widget** (Aggiungi widget) e selezionare *Bar Chart*.
4. Selezionare **Internal Volume** (Volume interno) per il tipo di oggetto da visualizzare sul grafico a barre. Si noti che il tipo di oggetto del volume interno presenta un'icona di collegamento accanto ad esso. L'icona "Linked" è attivata per impostazione predefinita.



5. Scegli *IOPS - Total* e imposta eventuali filtri aggiuntivi.
6. Chiudere il campo **Roll Up** facendo clic sulla [X] accanto. Viene visualizzato il campo **Mostra**.
7. Scegli di mostrare i primi 10.
8. Salvare il widget.

   Il grafico a barre mostra solo i volumi interni che risiedono nella risorsa di storage corrente.

Il widget viene visualizzato nelle pagine delle risorse per tutti gli oggetti di storage. Quando il collegamento in-context è attivato nel widget, il grafico a barre mostra i dati dei volumi interni relativi solo alla risorsa di storage attualmente visualizzata.

Per scollegare i dati dell'oggetto, modificare il widget e fare clic sull'icona del collegamento accanto al tipo di oggetto. Il collegamento viene disattivato il grafico mostra i dati per *tutti* gli oggetti nel tuo ambiente.

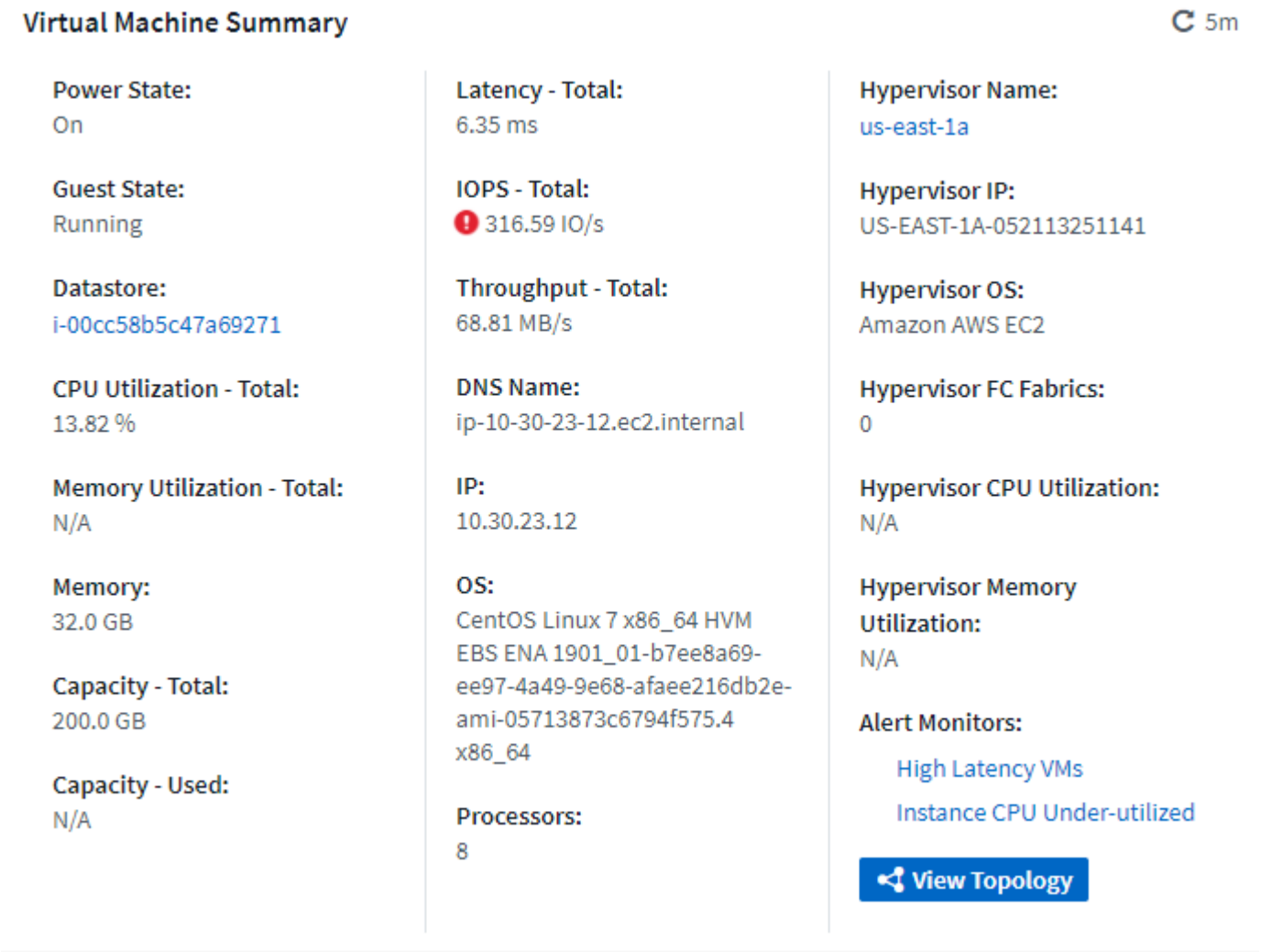
È anche possibile utilizzare **"variabili speciali nei widget"** per visualizzare le informazioni relative alle risorse nelle landing page.

Sezione Riepilogo pagina risorse

La sezione Summary (Riepilogo) di una pagina asset visualizza informazioni generali su una risorsa, tra cui se le metriche o le policy sulle performance sono fonte di preoccupazione. Le aree potenzialmente problematiche sono indicate da un cerchio

rosso.

Le informazioni contenute nella sezione di riepilogo, nonché in qualsiasi tabella o widget personalizzati nella pagina di asset, vengono aggiornate automaticamente in base all'intervallo di tempo selezionato. È possibile visualizzare la frequenza di aggiornamento corrente nell'angolo superiore destro della sezione Riepilogo, nelle tabelle e in qualsiasi widget personalizzato.



Nota: Le informazioni visualizzate nella sezione Riepilogo variano a seconda del tipo di risorsa visualizzata.

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.

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.

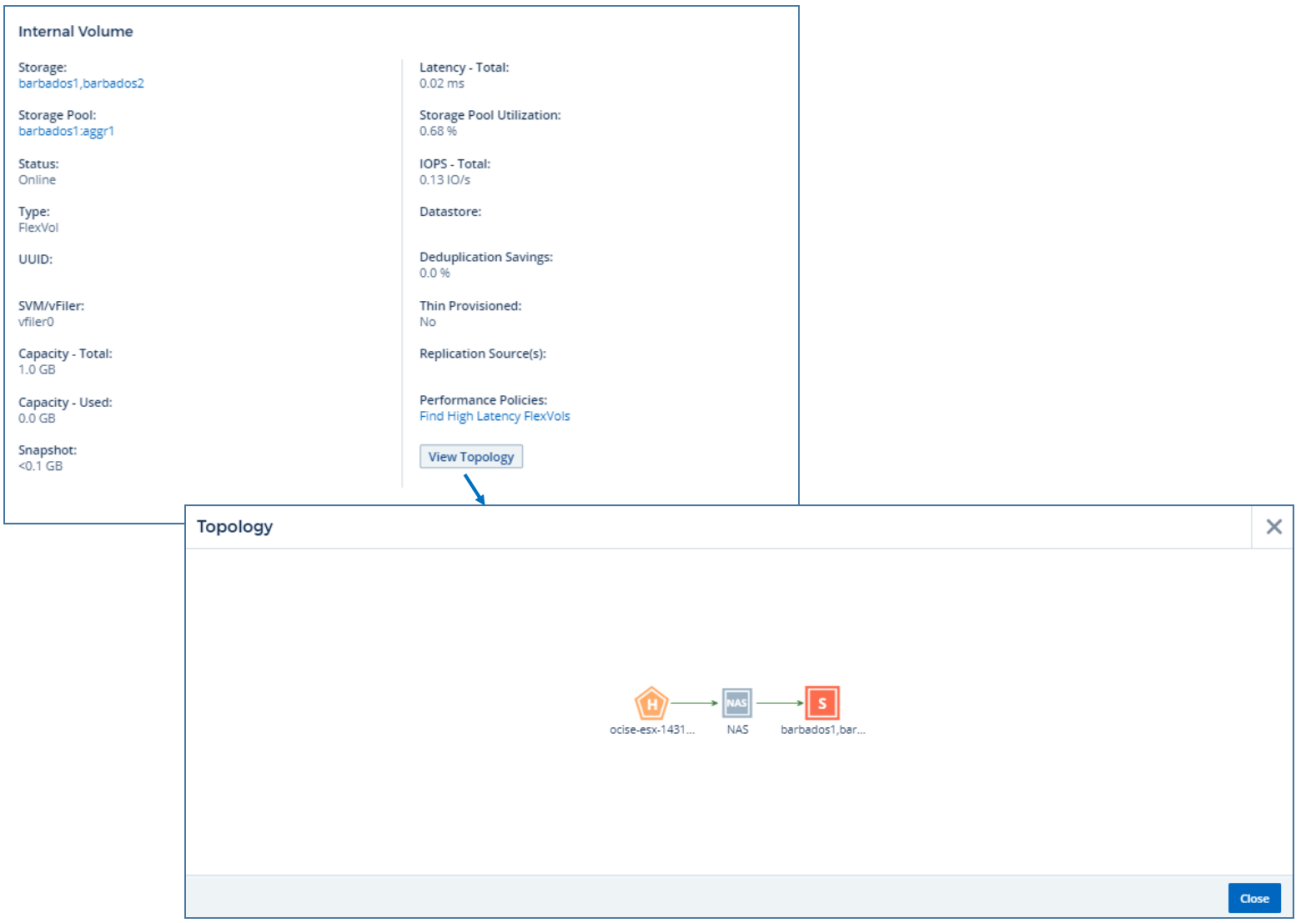
Se applicabile, è possibile fare clic su un collegamento di avviso per visualizzare l'avviso e il monitor associati alla risorsa.

Topologia

In alcune pagine di risorse, la sezione di riepilogo contiene un collegamento per visualizzare la topologia della risorsa e le relative connessioni.

La topologia è disponibile per i seguenti tipi di risorse:

- Applicazione
- Disco
- Fabric
- Host
- Volume interno
- Porta
- Switch
- Macchina virtuale
- VMDK
- Volume

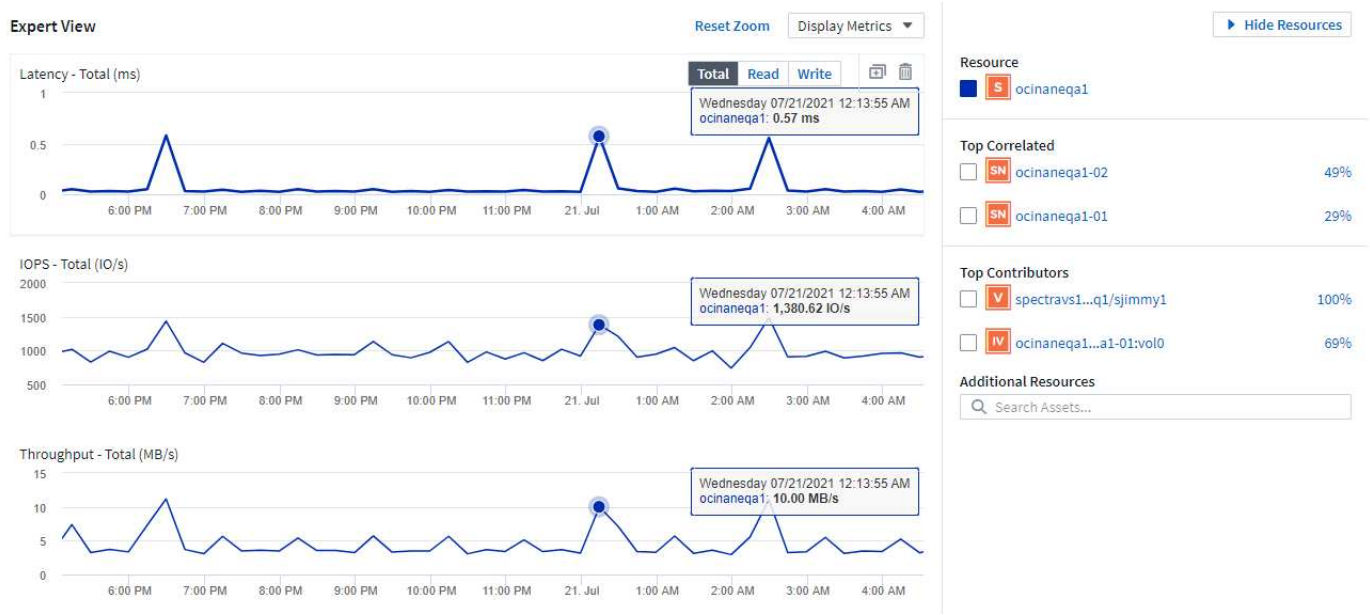


Vista degli esperti

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 selezionato nel grafico delle performance e le risorse ad essa correlate. I dati nei grafici si aggiornano automaticamente quando i data collector effettuano il polling e vengono acquisiti i dati aggiornati.

Utilizzando la sezione visualizzazione avanzata

Di seguito viene riportato un esempio della sezione Expert View in una pagina di risorse di storage:



È possibile selezionare le metriche che si desidera visualizzare nel grafico delle performance per il periodo di tempo selezionato. Fare clic sull'elenco a discesa *Display Metrics* e scegliere una delle metriche elencate.

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

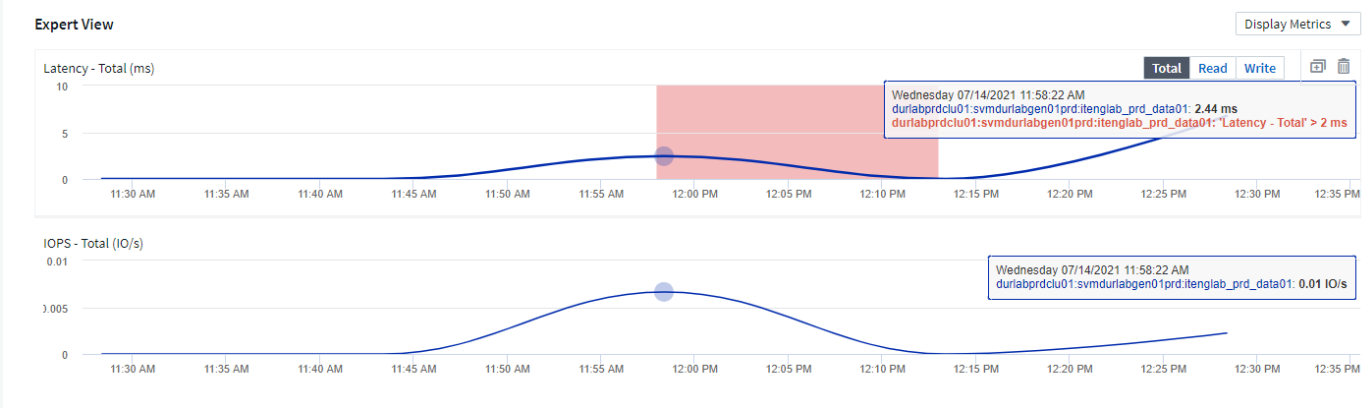
  Mostra le risorse che contribuiscono (percentuale) alla risorsa di base.

- Carichi di lavoro contenuti

Mostra le risorse che influiscono o sono influenzate da altre risorse condivise, come host, reti e storage. Queste risorse sono talvolta denominate risorse *greedy* e *degradate*.

Avvisi in visualizzazione esperti

Gli avvisi vengono visualizzati anche nella sezione visualizzazione esperti di una landing page di risorsa, che mostra l'ora e la durata dell'avviso, nonché la condizione di monitoraggio che lo ha attivato.



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. Le metriche che puoi scegliere variano a seconda del tipo di risorsa.

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):	Tasso medio di ricezione dei dati IP in megabyte al secondo.
Scrittura: Throughput IP (trasmissione):	Tasso medio 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 medio di risposta 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. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   - Cercare e selezionare una risorsa specifica.
   - Selezionare una risorsa da un widget della dashboard.
   - Cercare un insieme di risorse e selezionarne uno dall'elenco dei risultati.

     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. Se non sono presenti risorse pertinenti a queste sezioni, non vengono visualizzate.

2. È possibile aggiungere un grafico delle performance per una metrica facendo clic su **Display Metrics** (Visualizza metriche) e selezionando le metriche che si desidera visualizzare.

   Viene visualizzato un grafico separato per ciascuna 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 destra della pagina delle risorse o ingrandendo qualsiasi grafico.

   Fare clic su **Display Metrics** (Visualizza metriche) per deselezionare un grafico. Il grafico delle performance per la metrica viene rimosso da Expert View.

3. È possibile posizionare il cursore sul grafico e modificare i dati metrici visualizzati per tale grafico facendo clic su una delle seguenti opzioni, a seconda della risorsa:

   - Lettura, scrittura o totale
   - TX, Rx o Total (totale)

     Total (totale) è l'impostazione predefinita.

   È possibile trascinare il cursore sui punti dati nel grafico per vedere come cambia il valore della metrica nel periodo di tempo selezionato.

4. Nella sezione risorse, è possibile aggiungere qualsiasi risorsa correlata ai grafici delle performance:
   - È possibile selezionare una risorsa correlata nelle sezioni **Top Correlated**, **Top Contributors**, **greedy** e **Degraded** per aggiungere i dati da tale risorsa al grafico delle performance per ciascuna metrica selezionata.

     Dopo aver selezionato la risorsa, viene visualizzato un blocco di colori accanto alla risorsa per indicare il colore dei punti dati nel grafico.

5. Fare clic su **Hide Resources** (Nascondi risorse) per nascondere il riquadro delle risorse aggiuntive. Fare clic su **risorse** per visualizzare il riquadro.

- 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 sulla relazione della risorsa con la 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 delle risorse aggiuntive. Se non si desidera più visualizzare informazioni sulla risorsa, fare clic su 🗑.

Sezione dati 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 le applicazioni e le annotazioni.

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, qtree, e hypervisor). La sezione User Data (dati utente) consente di aggiungere, modificare o rimuovere le applicazioni assegnate a una risorsa. Per tutti questi tipi di risorse, ad eccezione dei volumi, è possibile assegnare più di un'applicazione.

Fasi

1. Individuare una pagina di risorse effettuando una delle seguenti operazioni:
   a. Cercare un elenco di risorse, quindi selezionarne uno dall'elenco.
   b. In una dashboard, individuare il nome di una risorsa e fare clic su di essa.
   c. Eseguire una ricerca e scegliere una risorsa dai risultati.

      Viene visualizzata la pagina delle risorse. La sezione User Data (dati utente) della pagina mostra le applicazioni o le annotazioni attualmente assegnate.

Per modificare l'applicazione assegnata o per assegnare un'applicazione o applicazioni aggiuntive, selezionare l'elenco **applicazione** e scegliere le applicazioni che si desidera assegnare alla risorsa. È possibile digitare per cercare un'applicazione o selezionarne una dall'elenco.

Per rimuovere un'applicazione, selezionare l'elenco a discesa e deselezionare l'applicazione.

Utilizzare la sezione User Data (dati utente) per assegnare o modificare le annotazioni

Quando si personalizza Cloud Insights 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. Per aggiungere un'annotazione alla risorsa, nella sezione User Data (dati utente) della pagina delle risorse, fare clic su **+Annotation (Annotazione)**.
2. Selezionare un'annotazione dall'elenco.
3. Fare clic su Value (valore) ed eseguire una delle seguenti operazioni, a seconda del tipo di annotazione selezionato:
   a. Se il tipo di annotazione è list, date o booleano, selezionare un valore dall'elenco.
   b. Se il tipo di annotazione è testo, digitare un valore.
4. Fare clic su Salva.

L'annotazione viene assegnata alla risorsa. È possibile filtrare le risorse in un secondo momento mediante un'annotazione utilizzando una query.

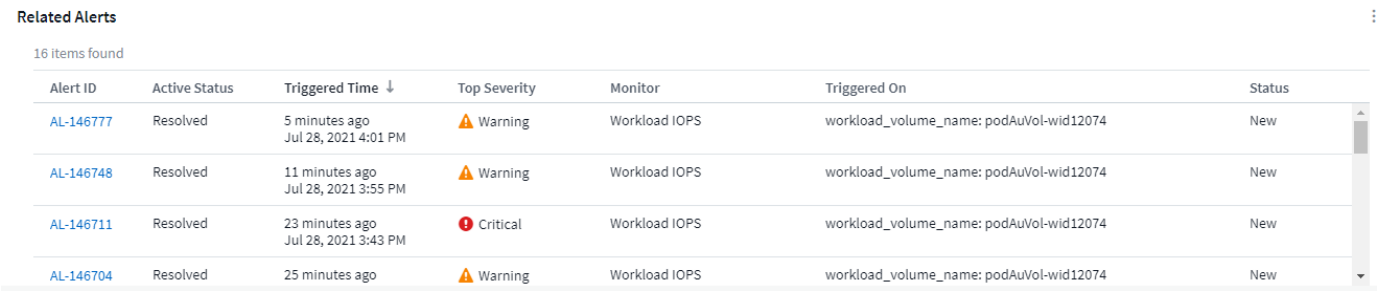
Se si desidera modificare il valore dell'annotazione dopo averlo assegnato, selezionare l'elenco delle annotazioni e immettere un valore diverso.

Se l'annotazione è di tipo elenco per cui è selezionata l'opzione *Add new values on the fly*, è possibile digitare per aggiungere un nuovo valore oltre alla selezione di un valore esistente.

Sezione Avvisi correlati alla pagina risorse

È possibile utilizzare la sezione Avvisi correlati di una pagina di risorse per visualizzare gli avvisi che si verificano nell'ambiente in uso a seguito di un monitor assegnato a una risorsa. I monitor generano avvisi in base alle condizioni impostate e consentono di identificare l'implicazione e analizzare l'impatto e la causa del problema in modo da consentire una correzione rapida ed efficace.

Nell'esempio seguente viene illustrata una tipica sezione Avvisi correlati che viene visualizzata in una pagina di risorse:



La sezione Avvisi correlati consente di visualizzare e gestire gli avvisi che si verificano nella rete in seguito alle condizioni di monitoraggio assegnate a una risorsa.

Fasi

- Individuare una pagina di risorse effettuando una delle seguenti operazioni:
  - Digitare il nome della risorsa nell'area di ricerca, quindi selezionarla dall'elenco.
  - In un widget dashboard, fare clic sul nome di una risorsa.
  - Eseguire una query per un set di risorse e selezionare on dall'elenco dei risultati.

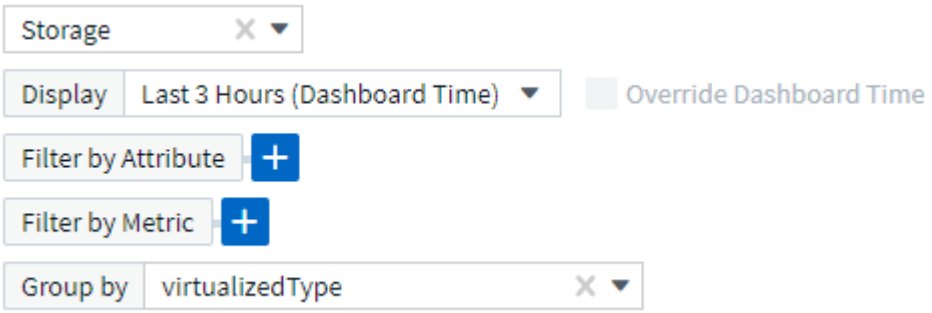
Viene visualizzata la pagina delle risorse. La sezione Related Alerts (Avvisi correlati) visualizza l'ora di attivazione dell'avviso, lo stato corrente dell'avviso e il monitor che lo ha attivato. È possibile fare clic sull'ID avviso per aprire la landing page dell'avviso per ulteriori indagini.

Virtualizzazione dello storage

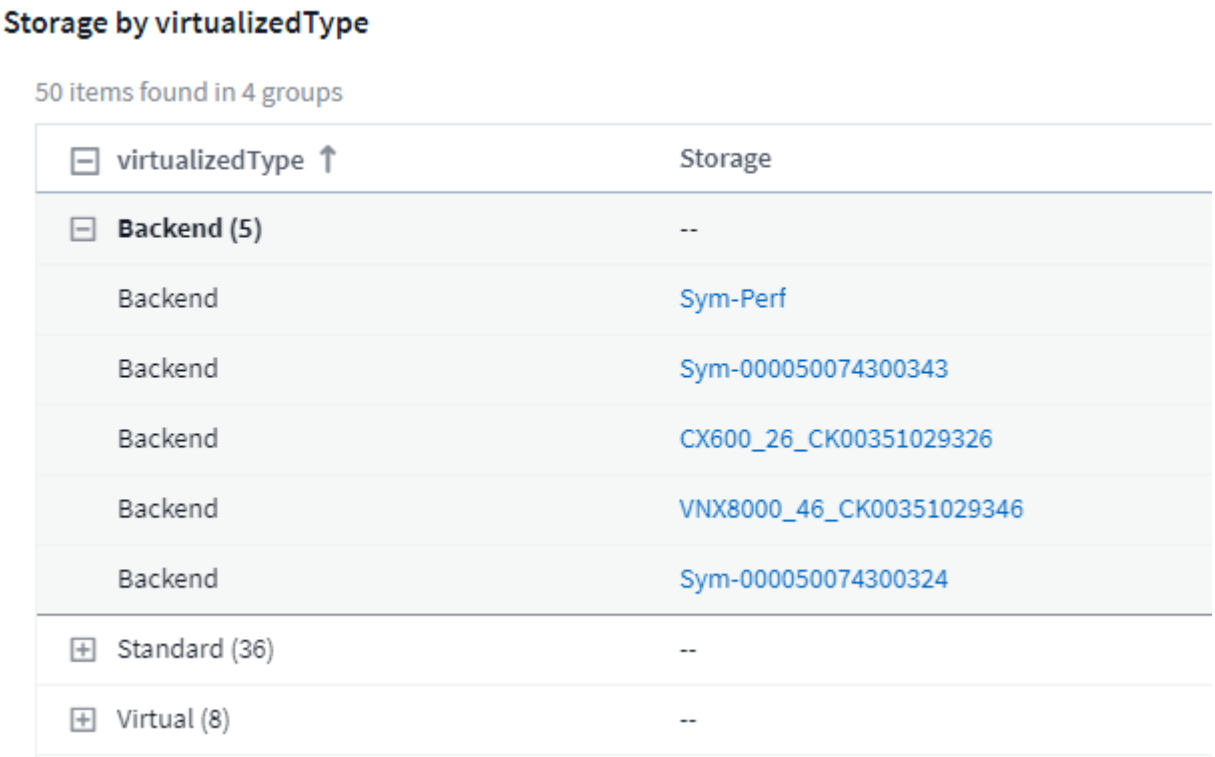
Cloud Insights è in grado di distinguere tra un array di storage con storage locale o virtualizzazione di altri array di storage. In questo modo è possibile correlare i costi e distinguere le performance dal front-end fino al back-end dell'infrastruttura.

Virtualizzazione in un widget tabella

Uno dei modi più semplici per iniziare a esaminare la virtualizzazione dello storage consiste nella creazione di un widget della tabella della dashboard che mostri il tipo virtualizzato. Quando si crea la query per il widget, è sufficiente aggiungere "virtualizedType" al raggruppamento o al filtro.

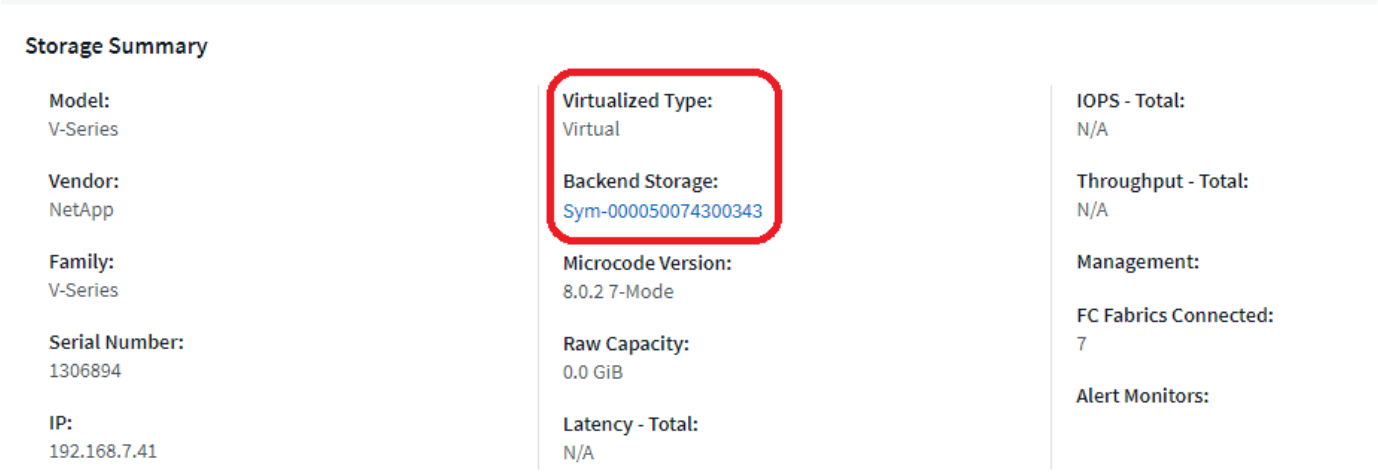


Il widget della tabella risultante mostra gli storage *Standard*, *backend* e *Virtual* nel tuo ambiente.



Le landing page mostrano informazioni virtualizzate

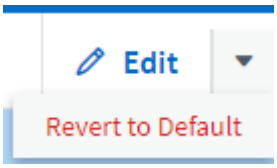
Su una landing page di storage, volume, volume interno o disco, è possibile visualizzare informazioni sulla virtualizzazione rilevanti. Ad esempio, osservando la pagina di destinazione dello storage riportata di seguito, è possibile vedere che si tratta di uno storage virtuale e quale sistema di storage back-end si applica. Tutte le tabelle pertinenti nelle landing page mostreranno anche le informazioni sulla virtualizzazione, se applicabili.



Landing page e dashboard esistenti

Tenere presente che se nel proprio ambiente sono presenti landing page o dashboard personalizzati, per impostazione predefinita non verranno visualizzate automaticamente tutte le informazioni sulla virtualizzazione. Tuttavia, è possibile *ripristinare le impostazioni predefinite* qualsiasi dashboard o landing page personalizzata (sarà necessario implementare nuovamente le personalizzazioni) oppure modificare i widget pertinenti per includere gli attributi o le metriche di virtualizzazione desiderati.

L'opzione *Ripristina impostazioni predefinite* è disponibile nell'angolo in alto a destra di una dashboard personalizzata o di una landing page.



Suggerimenti e suggerimenti per la ricerca di risorse e avvisi

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* restituisce *application*.

- **Frasi utilizzate nella ricerca**

  Una frase è un gruppo di parole racchiuse tra virgolette doppie, ad esempio "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 O, E e NON, è possibile combinare più termini per formare una query più complessa.

  OPPURE

  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 O netapp* ricerca 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, *storage E netapp* ricerca i documenti che contengono sia *storage* che *netapp*.

  È possibile utilizzare il simbolo **&&** invece della parola E.

  NO

  Quando si utilizza L'operatore NOT, tutti i documenti che contengono il termine After NOT vengono esclusi dai risultati della ricerca. Ad esempio, *storage NON netapp* ricerca documenti che contengono solo *storage* e non *netapp*.

  È possibile utilizzare il simbolo **!** invece della parola NO.

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 al modello.

L'interfaccia utente visualizza i risultati della ricerca in diverse categorie, con i tre risultati principali per categoria. Se non è stato trovato un oggetto 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	modello di vendor del nome "storage"
StoragePool	Nome "storagepool" degli indirizzi IP dello storage del numero di serie dello storage dei nomi dei modelli di storage del vendor dello storage per tutti i nomi dei volumi interni associati a tutti i dischi associati
Volume interno	Nome "internalvolume" degli indirizzi IP dello storage del numero di serie dello storage del fornitore dello storage nome del modello dello storage dei nomi dei pool di storage di tutti i nomi delle condivisioni associati di tutte le applicazioni associate
Volume	Nome "volume" nomi etichetta di tutti i volumi interni nome del pool di storage nome degli indirizzi IP dello storage del numero di serie dello storage del modello di storage del vendor
Nodo di storage	Nome "storagenode" degli indirizzi IP dello storage del numero di serie dello storage del modello di storage del vendor
Host	Nome "host" indirizzi IP nomi di tutte le applicazioni associate
Datastore	Nome "datastore" Virtual Center nomi IP di tutti i volumi nomi di tutti i volumi interni
Macchine virtuali	Nome "virtualmachine" Nome DNS indirizzi IP nome dell'host indirizzi IP dei nomi host di tutti i nomi degli archivi dati di tutte le applicazioni associate
Switch (Regular e NPV)	"Switch" Indirizzo IP Nome wwn numero di serie modello nome di dominio del fabric wwn del fabric
Applicazione	nome "applicazione" linea tenant del progetto di business unit
Nastro	Indirizzo IP "nastro" nome numero di serie fornitore
Porta	nome wwn "porta"
Fabric	nome wwn "fabric"
SVM (Storage Virtual Machine)	UUID nome "storagevirtualmachine"

Creazione di report

Panoramica dei report Cloud Insights

Cloud Insights Reporting è uno strumento di business intelligence che consente di visualizzare report predefiniti o creare report personalizzati.

La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

Con il reporting Cloud Insights è possibile eseguire le seguenti attività:

- Eseguire un report predefinito
- Creare un report personalizzato
- Personalizzare il formato e il metodo di consegna di un report
- Pianificare l'esecuzione automatica dei report
- Invia report via email
- Utilizzare i colori per rappresentare le soglie sui dati

I report Cloud Insights possono generare report personalizzati per aree come chargeback, analisi dei consumi e previsioni e possono aiutare a rispondere a domande come:

- 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?
- 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?

Accesso ai report di Cloud Insights

È possibile accedere ai report di Cloud Insights facendo clic sul collegamento **Report** nel menu.

Viene quindi utilizzata l'interfaccia di reporting. Cloud Insights utilizza IBM Cognos Analytics per il suo motore di reporting.

Che cos'è ETL?

Quando si lavora con Reporting, si sentiranno i termini "Data Warehouse" e "ETL". ETL sta per "Estrai, trasforma e carica". Il processo ETL recupera i dati raccolti in Cloud Insights e li trasforma in un formato da utilizzare in Reporting. Per "Data Warehouse" si intendono i dati raccolti disponibili per il reporting.

Il processo ETL include i seguenti processi:

- **Estrai**: Prende i dati da Cloud Insights.
- **Trasformazione**: Applica le regole o le funzioni della logica di business ai dati quando vengono estratti da

Cloud Insights.

- **Load**: Consente di salvare i dati trasformati nel data warehouse per utilizzarli in Reporting.

Ruoli utente dei report Cloud Insights

Se si dispone di Cloud Insights Premium Edition con Reporting, ogni utente Cloud Insights dell'ambiente dispone anche di un accesso Single Sign-on (SSO) all'applicazione di reporting (ad esempio Cognos). Basta fare clic sul collegamento **Report** nel menu per accedere automaticamente a Reporting.

Il tuo ruolo utente in Cloud Insights determina il tuo ruolo utente di reporting:

Ruolo di Cloud Insights	Ruolo di reporting	Autorizzazioni di reporting
Ospite	Consumatore	Consente di visualizzare, pianificare ed eseguire report e di impostare preferenze personali, ad esempio per lingue e fusi orari. Gli utenti non possono creare report o eseguire attività amministrative.
Utente	Autore	Può eseguire tutte le funzioni Consumer, nonché creare e gestire report e dashboard.
Amministratore	Amministratore	Può eseguire tutte le funzioni di autore e tutte le attività amministrative, come la configurazione dei report e l'arresto e il riavvio delle attività di reporting.

La tabella seguente mostra le funzioni disponibili per ciascun ruolo di reporting.

Funzione	Consumatore	Autore	Amministratore
Visualizzare i report nella scheda contenuto team	Sì	Sì	Sì
Eseguire i report	Sì	Sì	Sì
Pianifica i report	Sì	Sì	Sì
Caricare file esterni	No	Sì	Sì
Creare lavori	No	Sì	Sì
Crea storie	No	Sì	Sì
Creare report	No	Sì	Sì
Creare pacchetti e moduli dati	No	Sì	Sì
Eseguire attività amministrative	No	No	Sì

Aggiungi/Modifica elemento HTML	No	No	Sì
Esegui report con HTML Item	Sì	Sì	Sì
Aggiungi/Modifica SQL personalizzato	No	No	Sì
Esegui report con SQL personalizzato	Sì	Sì	Sì

Impostazione delle preferenze e-mail di Reporting (Cognos)

Se si modificano le preferenze e-mail dell'utente all'interno di Report Cloud Insights (ad esempio, l'applicazione Cognos), tali preferenze sono attive *solo per la sessione corrente*. Disconnettendo da Cognos e tornando, verranno ripristinate le preferenze e-mail.

Nota importante per i clienti esistenti

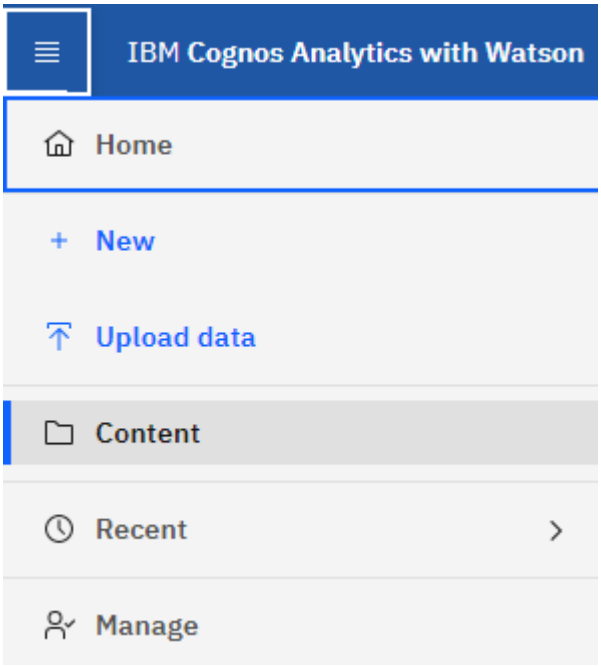
Se non hai ancora accesso a Cloud Insights con Reporting, benvenuto! Non c'è altro da fare per iniziare a utilizzare il reporting.

Se sei un cliente Premium Edition, SSO non viene attivato automaticamente per il tuo ambiente. Quando si attiva SSO, l'utente amministratore del portale di reporting (Cognos) cessa di esistere. Ciò significa che tutti i report contenuti nella cartella *My Content* vengono rimossi e devono essere reinstallati o ricreati in *Team Content*. Inoltre, una volta attivato SSO, è necessario configurare i report pianificati.

Quali sono i passaggi da seguire per preparare l'ambiente esistente per l'abilitazione di SSO?

Per garantire la conservazione dei report, migrare tutti i report da *My Content* a *Team Content* seguendo la procedura riportata di seguito. È necessario eseguire questa operazione prima di attivare SSO nell'ambiente:

1. Selezionare **Menu > contenuto**



1. Creare una nuova cartella in ***Team Content***
    a. Se sono stati creati più utenti, creare una cartella separata per ciascun utente per evitare di sovrascrivere i report con nomi duplicati
2. Accedere a *My Content*
3. Selezionare tutti i report che si desidera conservare.
4. Nell'angolo superiore destro del menu, selezionare "Copia o Sposta"
5. Accedere alla cartella appena creata in *contenuto del team*
6. Incollare i report nella cartella appena creata utilizzando i pulsanti "Copia in" o "Sposta in"
7. Una volta abilitato SSO per Cognos, accedere a Cloud Insights con l'indirizzo e-mail utilizzato per creare l'account.
8. Accedere alla cartella *Team Content* all'interno di Cognos e copiare o spostare i report precedentemente salvati in *My Content*.

Creazione semplificata di report predefiniti

Il reporting Cloud Insights 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.

> La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

È possibile generare report predefiniti dal portale di reporting Cloud Insights, 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.

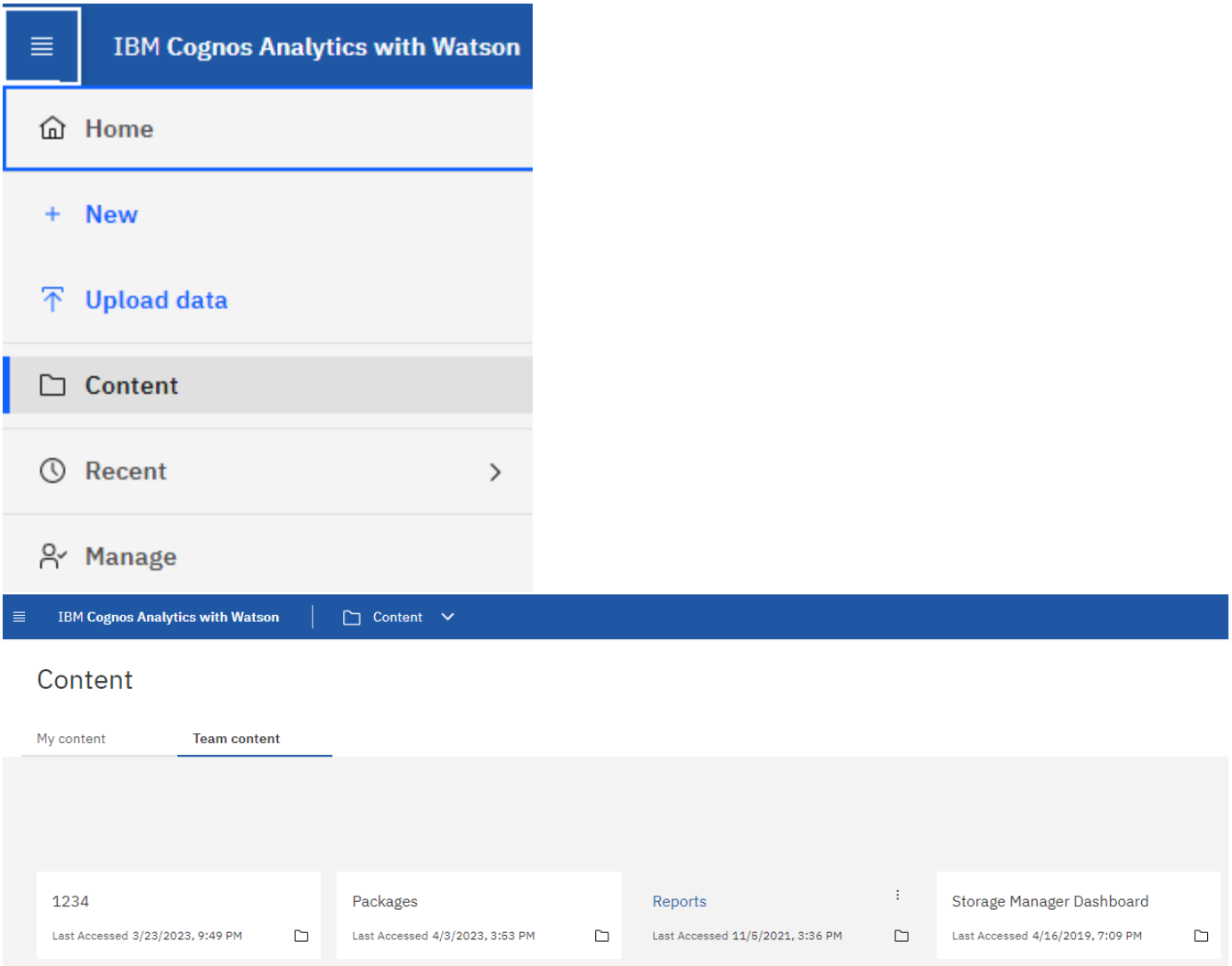
I report predefiniti mostrano l'inventario, la capacità dello storage, il chargeback, le performance, l'efficienza dello storage, e dati sui costi del cloud. È possibile modificare questi report predefiniti e salvare le modifiche.

È possibile generare report in diversi formati, tra cui HTML, PDF, CSV, XML, Ed Excel.

Accedere ai report predefiniti

Quando si apre il portale di reporting, la cartella *contenuto del team* rappresenta il punto di partenza per selezionare il tipo di informazioni necessarie nei report di Cloud Insights.

1. Nel riquadro di navigazione a sinistra, selezionare **contenuto > contenuto del team**.
2. Selezionare **Report** per accedere ai report predefiniti.



Utilizzo di report predefiniti per rispondere a domande comuni

I seguenti report predefiniti sono disponibili in **contenuto del team > Report**.

Performance e capacità 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.

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 sulla precisione dei report e sull'usabilità generale del

prodotto.

Performance di ESX e 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 di 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.

Scorecard

Il report Scorecard fornisce un riepilogo e lo stato generale di tutte le risorse acquisite da Cloud Insights. 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 Data Dictionary 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.

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 per 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.

Capacità Symmetrix per thick array

Il report Symmetrix Capacity by Thick Array mostra capacità raw, capacità utilizzabile, capacità libera, mappata, mascherata, e capacità libera totale.

Capacità di Symmetrix per 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.

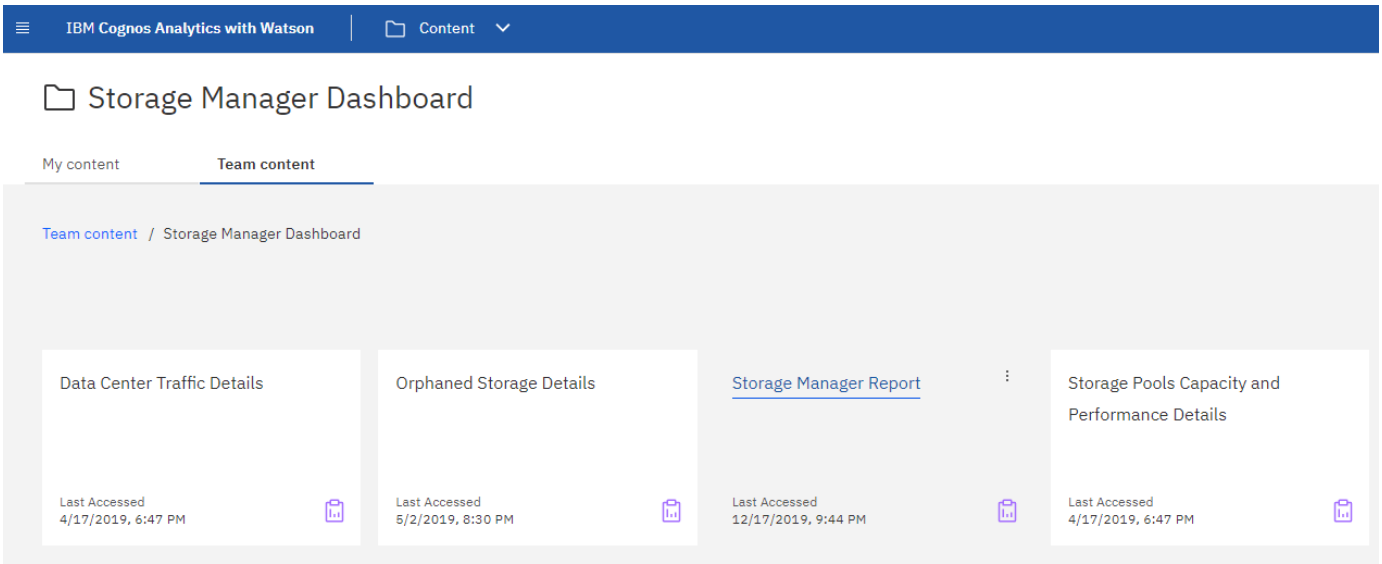
Dashboard di Storage Manager

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.

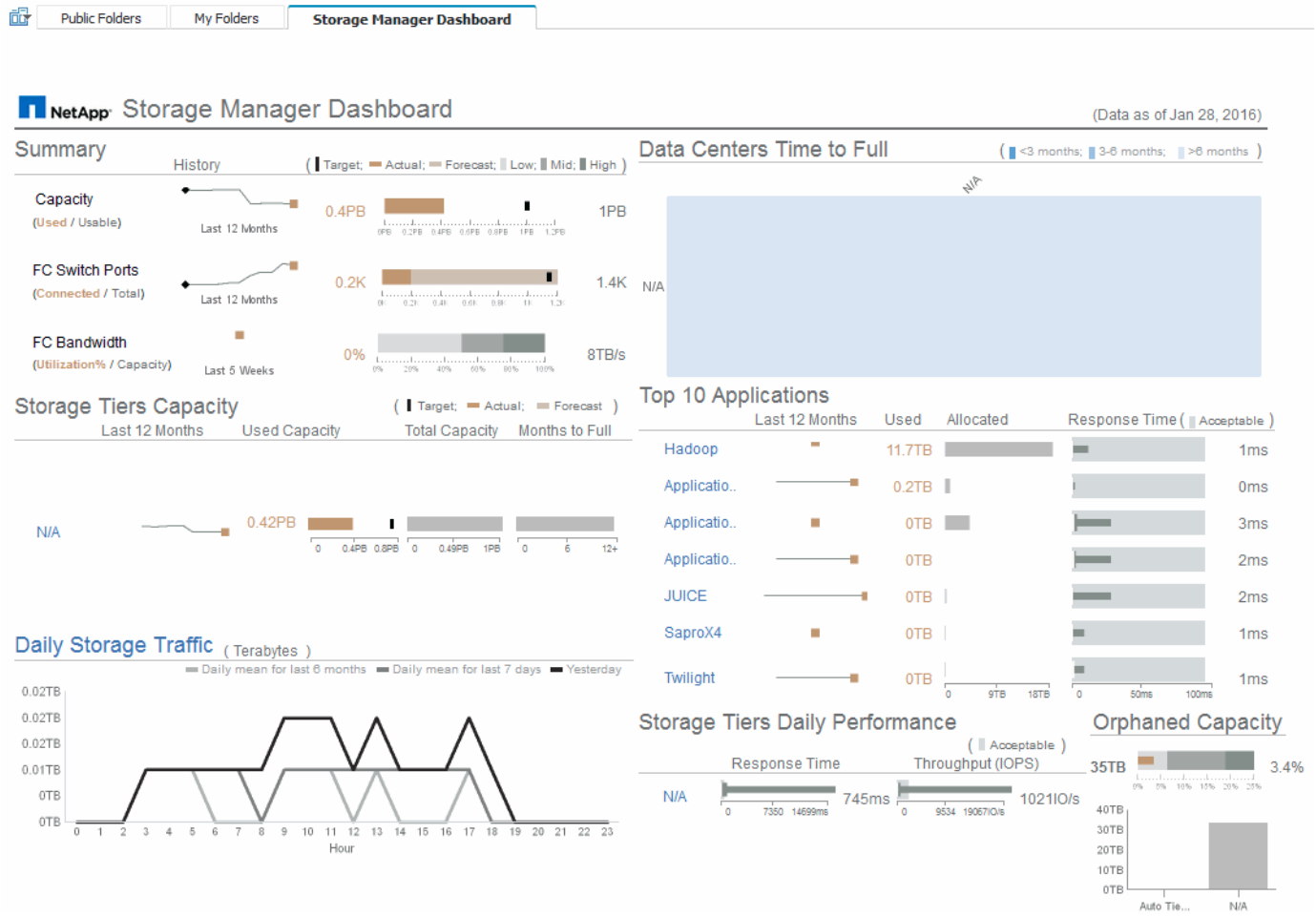
La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

Riepilogo

Selezionando **Storage Manager Dashboard** da Team Content, vengono forniti diversi report che forniscono informazioni sul traffico e sullo storage.



Per una visualizzazione immediata, il report * Storage Manager comprende sette componenti che contengono informazioni contestuali su molti 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.



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 bassi, medi e alti, che consente di confrontare e confrontare l'utilizzo tra le proiezioni 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, la previsione di utilizzo e una destinazione 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. 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. Lo storage orfano in base alla 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. Le performance sono orfane 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.

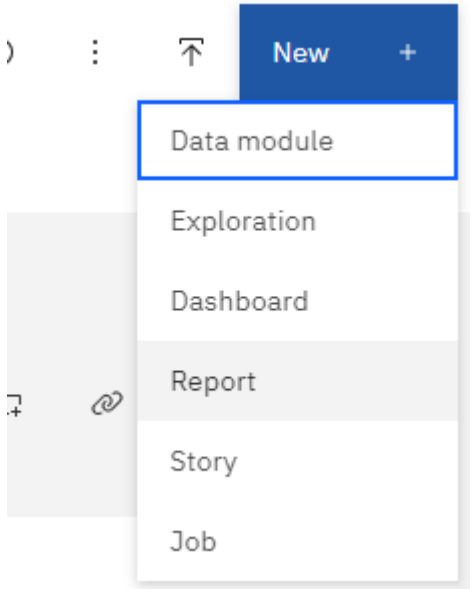
È possibile fare clic su un Tier per visualizzare il report "Orphaned Storage Details" (Dettagli storage orfani), che mostra tutti i volumi identificati come orfani in base alla configurazione e alle performance per il Tier selezionato. Fare clic su qualsiasi storage, pool di storage o volume in questo report per visualizzare la pagina delle risorse che riepiloga lo stato corrente della risorsa.

Creazione di un report (esempio)

Utilizzare i passaggi descritti in questo esempio per generare un semplice report sulla capacità fisica dei pool di storage e storage in diversi data center.

Fasi

1. Accedere a **Menu > contenuto > contenuto del team > Report**
2. Nella parte superiore destra dello schermo, selezionare **[nuovo +]**
3. Selezionare **Report**



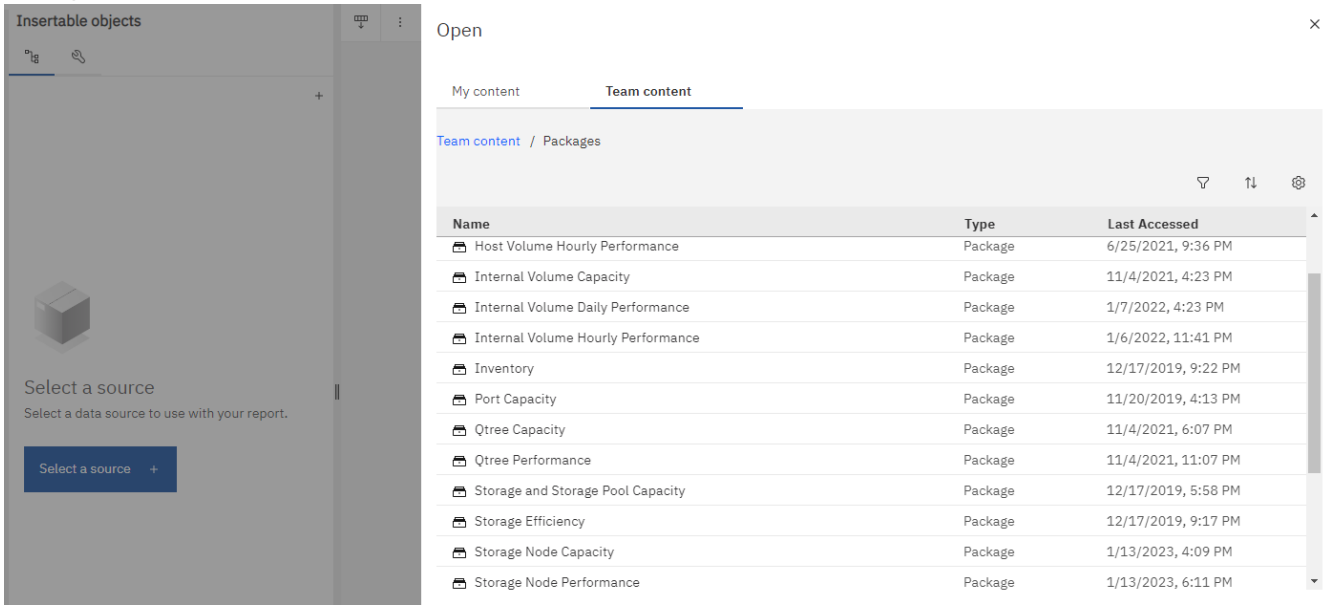
4. Nella scheda **Templates**, selezionare *blank*

   Vengono visualizzate le schede origine e dati

5. Aprire **selezionare un'origine +**
6. In **contenuto del team**, aprire **pacchetti**

Viene visualizzato un elenco dei pacchetti disponibili.

7. Scegliere *capacità del pool di storage e storage*



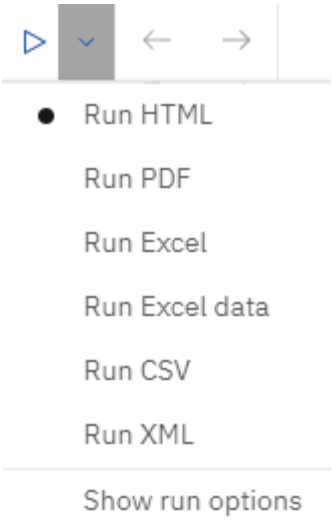
8. Selezionare **Apri**

   Vengono visualizzati gli stili disponibili per il report.

9. Selezionare **elenco**

   Aggiungere i nomi appropriati per elenco e query

10. Selezionare **OK**
11. Espandere *capacità fisica*
12. Espandere al livello più basso di *Data Center*
13. Trascinare *Data Center* sul tavolozza 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 selezionando un tipo di output dal menu **Esegui**.



Risultato

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

Top Page up Page down Bottom

Gestione dei report

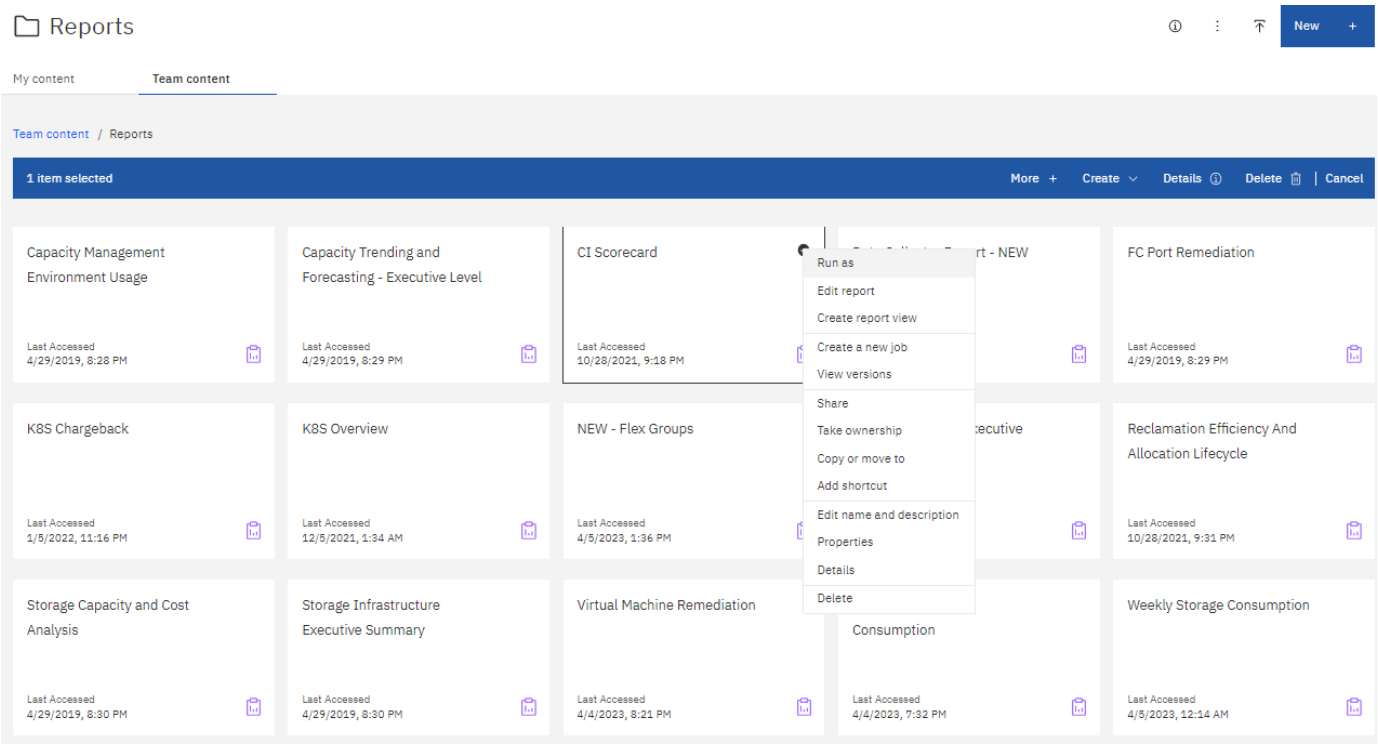
È possibile personalizzare il formato di output e la consegna di un report, impostare le proprietà o le pianificazioni del report e inviare i report via email.

La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

Personalizzazione del formato di output e della consegna di un report

È possibile personalizzare il formato e il metodo di consegna dei report.

1. Nel portale di reporting Cloud Insights, andare a **Menu > contenuto > contenuti personali/contenuto del team**. Passare il mouse sul report che si desidera personalizzare e aprire il menu "tre punti".

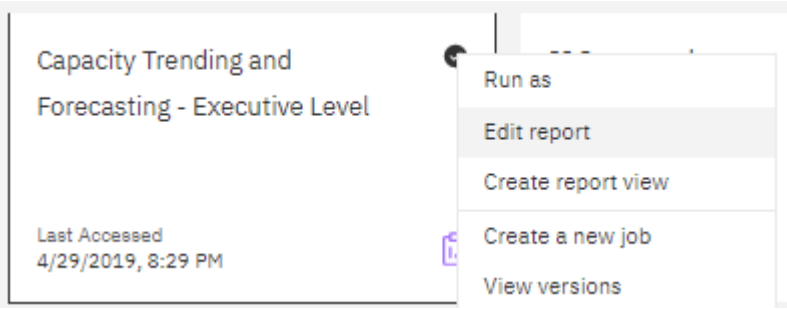


1. Fare clic su **Proprietà > Pianificazione**
2. È possibile impostare le seguenti opzioni:
   - **Pianificazione** per l'esecuzione dei report.
   - Scegliere **Opzioni** per il formato e l'invio del report (Salva, Stampa, e-mail) e le lingue per il report.
3. Fare clic su **Save** (Salva) per produrre il report utilizzando le selezioni effettuate.

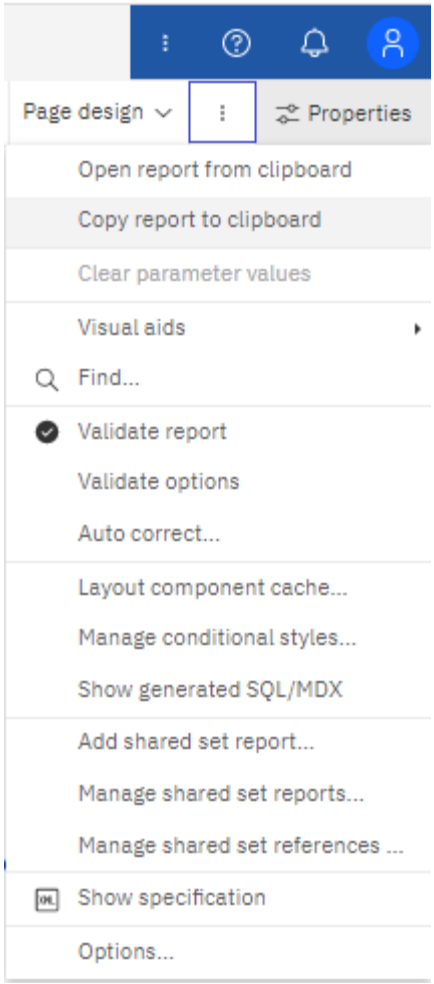
Copia di un report negli Appunti

Questa procedura consente di copiare un report negli Appunti.

1. Selezionare un report da cui copiare (**Menu > contenuto > contenuto personale o contenuto del team**)
2. Scegliere *Modifica report* dal menu a discesa del report



3. Nella parte superiore destra dello schermo, aprire il menu "tre punti" accanto a "Proprietà".
4. Selezionare **Copia report negli Appunti**.

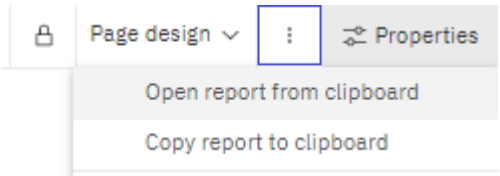


Apertura di report dagli Appunti

È possibile aprire una specifica del report precedentemente copiata negli Appunti.

A proposito di questa attività iniziare creando un nuovo report o aprendo un report esistente che si desidera sostituire con il report copiato. La procedura riportata di seguito riguarda un nuovo report.

1. Selezionare **Menu > +New > Report** e creare un report vuoto.
2. Nella parte superiore destra dello schermo, aprire il menu "tre punti" accanto a "Proprietà".
3. Selezionare **Apri report dagli Appunti**.



1. Incollare il codice copiato nella finestra e selezionare **OK**.
2. Selezionare l'icona del disco floppy per salvare il report.
3. Scegliere dove salvare il report (*My Content*, *Team Content* o creare una nuova cartella).
4. Assegnare un nome significativo al nuovo report e selezionare **Salva**.

Modifica di un report esistente

Tenere presente che la modifica dei file nella posizione predefinita comporta il rischio di sovrascrittura dei report al successivo aggiornamento del catalogo dei report. Si consiglia di salvare il report modificato con un nuovo nome o di memorizzarlo in una posizione non predefinita.

Risoluzione dei problemi

Qui troverai suggerimenti per la risoluzione dei problemi con Reporting.

Problema:	Provare questo:
Quando si pianifica l'invio di un report via email, il nome dell'utente che ha effettuato l'accesso viene precompilato nel campo "a" dell'email. Tuttavia, il nome è sotto forma di "firstname lastname" (nome, spazio, cognome). Poiché non si tratta di un indirizzo e-mail valido, l'e-mail non viene inviata quando viene eseguito il report pianificato.	Quando si pianifica l'invio del report via e-mail, cancellare il nome precompilato e inserire un indirizzo e-mail valido e correttamente formattato nel campo "a".

Creazione di report personalizzati

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.

La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

Gli esempi di questa sezione mostrano il seguente processo, che può essere utilizzato per qualsiasi modello di dati di reporting Cloud Insights:

- 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

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 o mostrare "N/A" per alcuni data point.

Prima di progettare i report, completare le seguenti attività:

- Configura tutto "raccolta di dati" correttamente.
- 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 i report, perché Cloud Insights Reporting raccoglie informazioni cronologiche.

Processo di creazione dei report

Il processo di creazione di report personalizzati (denominati anche "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.

Pianificazione dei risultati del report personalizzato

Prima di aprire gli strumenti di creazione 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 vedere 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 in Cloud Insights.

- Il reporting Cloud Insights 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.

Modelli di dati di reporting

Cloud Insights 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 fornisce 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.

Modelli di 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

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 interno sulla capacità del volume

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? 8 Qual è la capacità utilizzata rispetto alla capacità allocata sui nostri volumi interni?

Modello di 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 posso 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 di 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 Cloud Insights, 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 di 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 ai report 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. Domande a cui puoi rispondere con questi dati

- 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 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 sulle 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. Molti di questi report riportano i dati *Hourly*, *Daily* o entrambi. 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, Cloud Insights 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.

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.

Accedere al database dei report tramite API

La potente API di Cloud Insights consente agli utenti di eseguire query direttamente nel database dei report di Cloud Insights, senza utilizzare l'ambiente di reporting di Cognos.

> La presente documentazione fa riferimento alla funzione di reporting di Cloud Insights, disponibile in "Premium Edition".

OData

L'API di reporting Cloud Insights segue "OData v4" (Open Data Protocol) standard per la query del database di

Reporting. Per ulteriori informazioni o per saperne di più, consulta l'articolo "questo tutorial" Su OData.

Tutte le richieste inizieranno con l'URL */https://<Cloud Insights URL>/REST/v1/dwh-management/odata*

Generazione di una apiKey

Scopri di più "API Cloud Insights".

Per generare una chiave API, procedere come segue:

- Accedere all'ambiente Cloud Insights e selezionare **Amministratore > accesso API**.
- Fare clic su "+ API Access Token".
- Immettere un Nome e una Descrizione.
- Per tipo, scegliere *Data Warehouse*.
- Impostare le autorizzazioni come lettura/scrittura.
- Impostare una data di scadenza desiderata.
- Fare clic su "Save" (Salva), quindi **copiare la chiave e salvarla** in un luogo sicuro. Non sarà possibile accedere alla chiave completa in un secondo momento.

Gli APIkeys sono validi per *Sync* o *Async*.

Query diretta delle tabelle

Con la chiave API in uso, sono ora possibili query dirette del database di Reporting. Gli URL lunghi possono essere semplificati fino a https://…/odata/ per scopi di visualizzazione piuttosto che per l’intero <a href="https://<Cloud" class="bare">https://<Cloud Insights URL>/REST/v1/dwh-management/odata/

Prova semplici query come

- Https://<Cloud Insights URL>/REST/v1/dwh-management/odata/dwh_custom
- Https://<Cloud Insights URL>/REST/v1/dwh-management/odata/dwh_inventory
- Https://<Cloud Insights URL>/REST/v1/dwh-management/odata/dwh_inventory/storage
- Https://<Cloud Insights URL>/REST/v1/gestione dwh/odata/inventario dwh/disco
- https://…/odata/dwh_custom/custom_queries

Esempi di API REST

L'URL per tutte le chiamate è */https://<Cloud Insights URL>/REST/v1/dwh-management/odata*.

- GET /{schema}/** - Recupera i dati dal database dei report.

Formato: */https://<Cloud Insights URL>/REST/v1/dwh-management/odata/<schema_name>/<query>*

Esempio:

```
 https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
Risultato:
```


```
{
   "@odata.context": "$metadata#fabric",
   "@odata.count": 2,
   "value": [
       {
           "id": 851,
           "identifier": "10:00:50:EB:1A:40:3B:44",
           "wwn": "10:00:50:EB:1A:40:3B:44",
           "name": "10:00:50:EB:1A:40:3B:44",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941716"
       },
       {
           "id": 852,
           "identifier": "10:00:50:EB:1A:40:44:0C",
           "wwn": "10:00:50:EB:1A:40:44:0C",
           "name": "10:00:50:EB:1A:40:44:0C",
           "vsanEnabled": "0",
           "vsanId": null,
           "zoningEnabled": "0",
           "url": "https://<domain>/web/#/assets/fabrics/941836"
        }
    ]
}
```


Suggerimenti utili

Quando si utilizzano le query API di reporting, tenere presente quanto segue.

- Il payload della query deve essere una stringa JSON valida
- Il payload della query deve essere contenuto in una singola riga
- Le virgolette doppie devono essere escapate, ad esempio "
- Le schede sono supportate come
- Evitare i commenti
- Sono supportati i nomi delle tabelle in minuscolo

Inoltre:

- Sono richieste 2 intestazioni:
  - Nome "X-CloudInsights-apiKey"
  - Valore attributo "<apikey>"

La chiave API sarà specifica per l'ambiente Cloud Insights.

Come vengono conservati i dati storici per il reporting

Cloud Insights conserva i dati storici da utilizzare nei report 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	35 giorni
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	35 giorni
Performance mart	Performance dell'hypervisor	Ogni giorno	13 mesi
Performance mart	Performance VMDK	Ogni ora	35 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)

Diagrammi dello schema di reporting di Cloud Insights

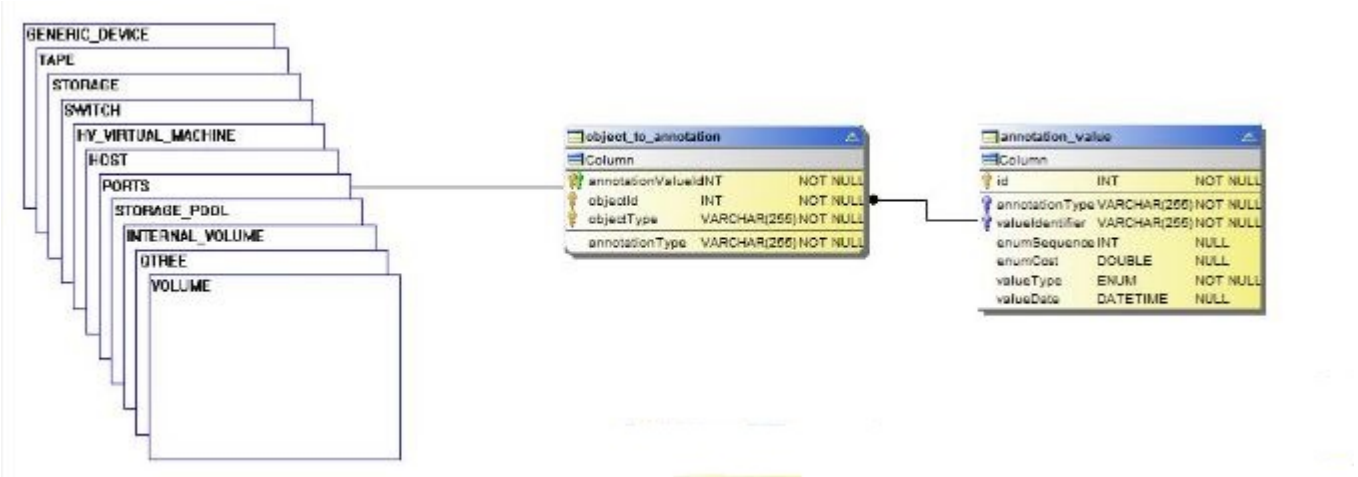
Questo documento fornisce i diagrammi dello schema per il database dei report. È inoltre possibile scaricare un file contenente "tabelle dello schema".

La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

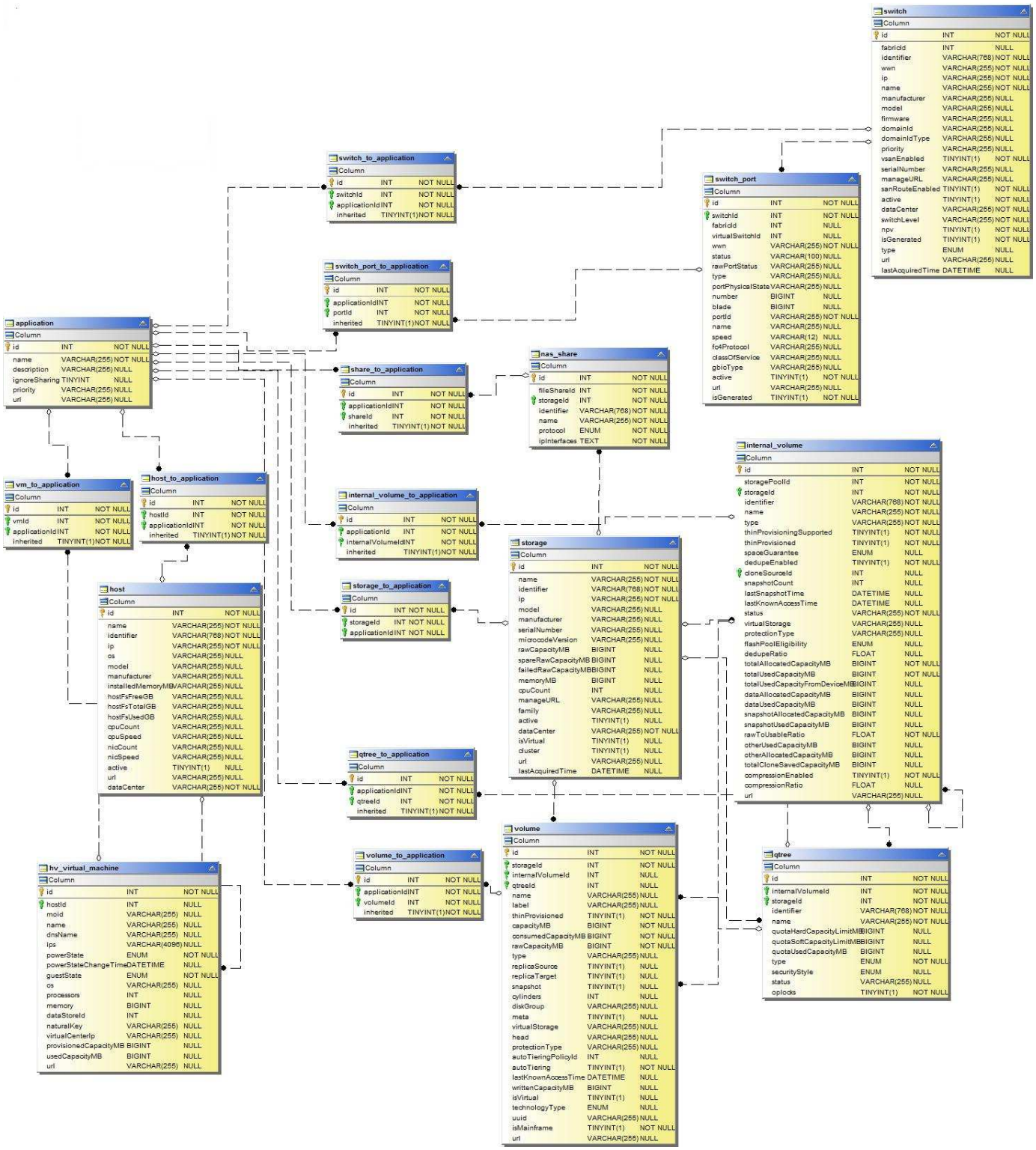
Datamart dell'inventario

Le immagini seguenti descrivono il datamart dell'inventario.

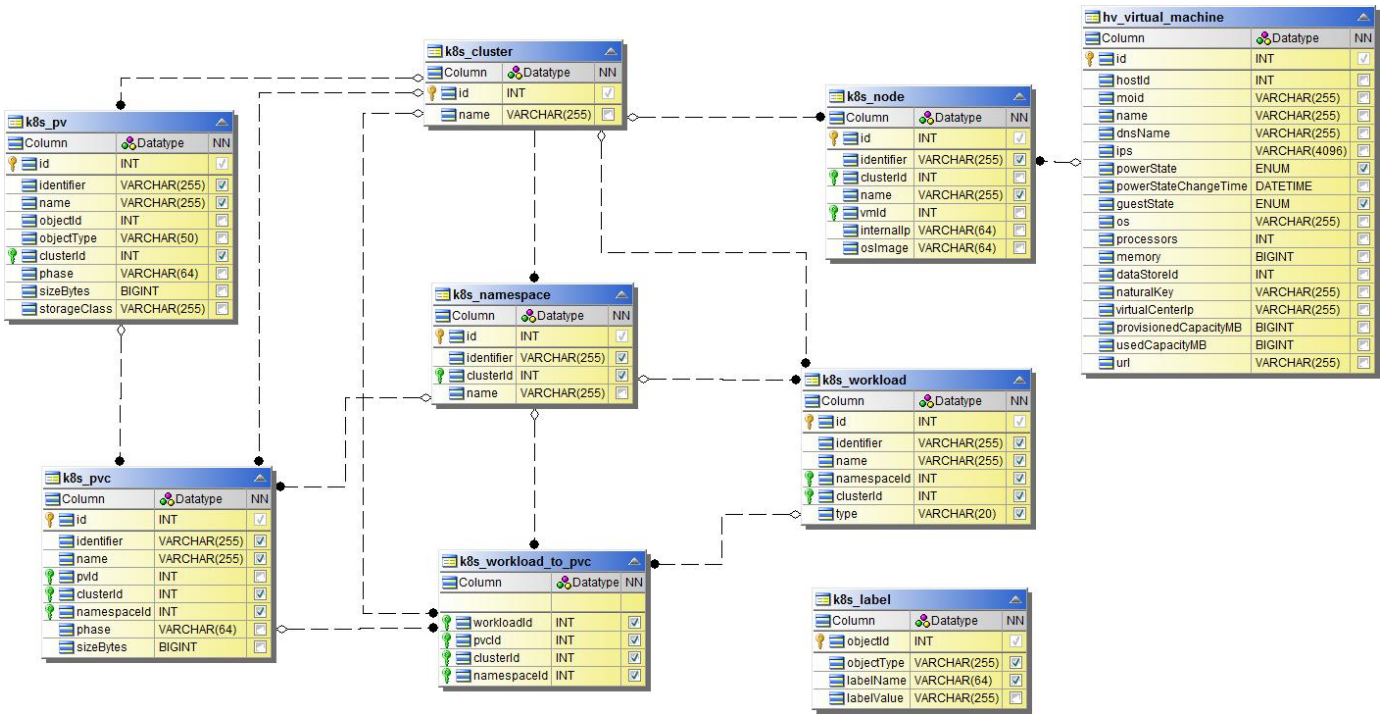
Annotazioni



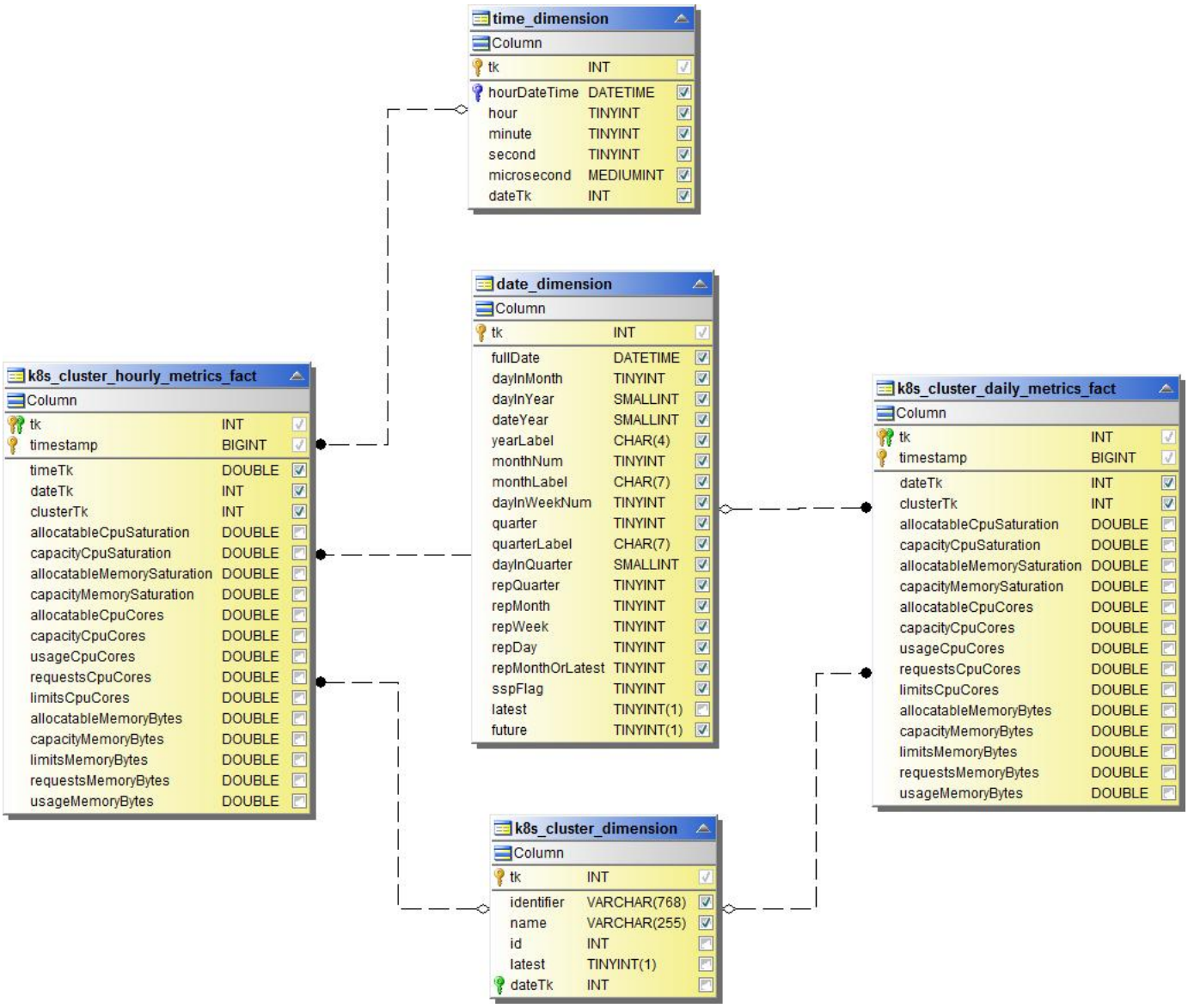
Applicazioni



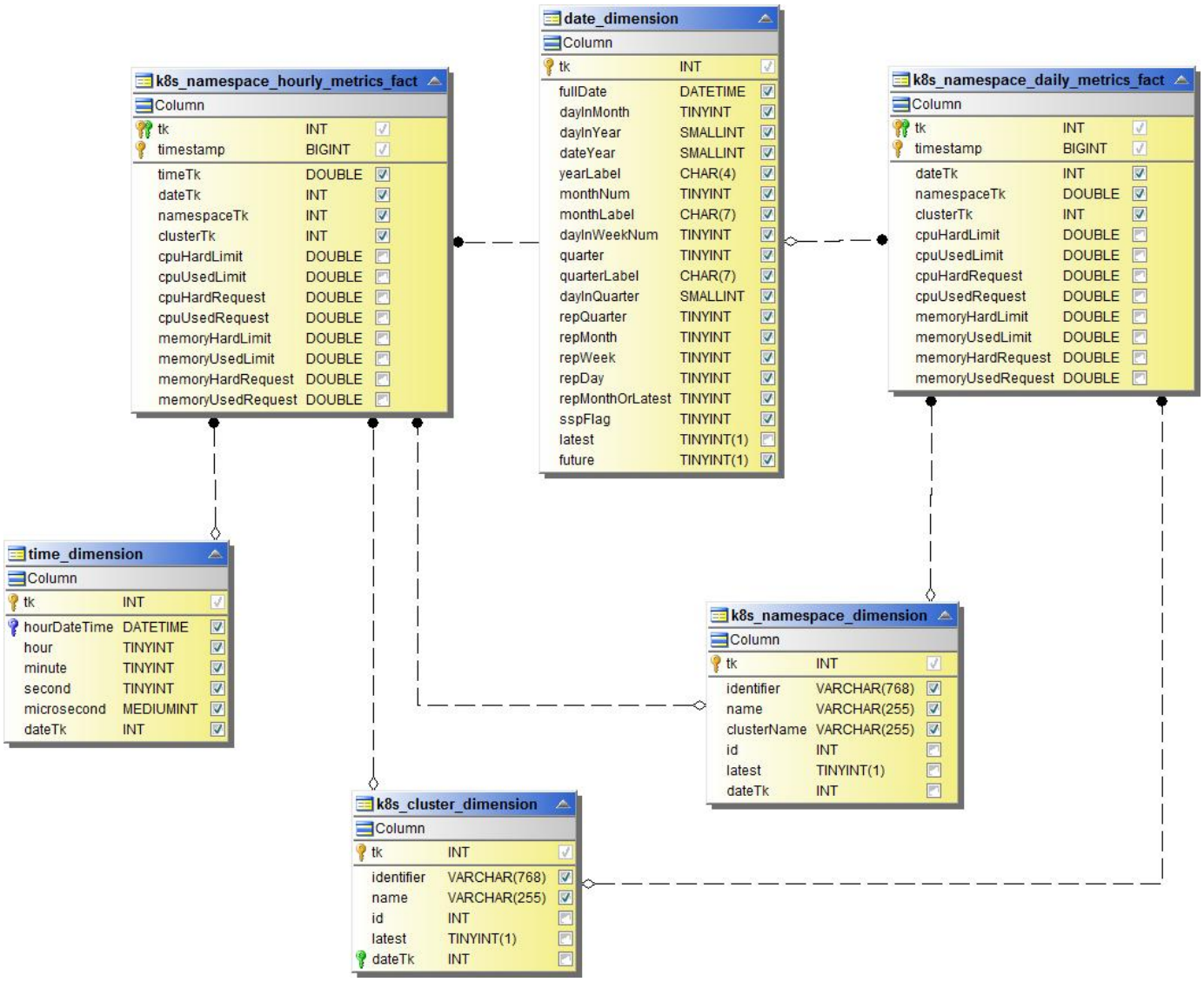
Metriche Kubernetes



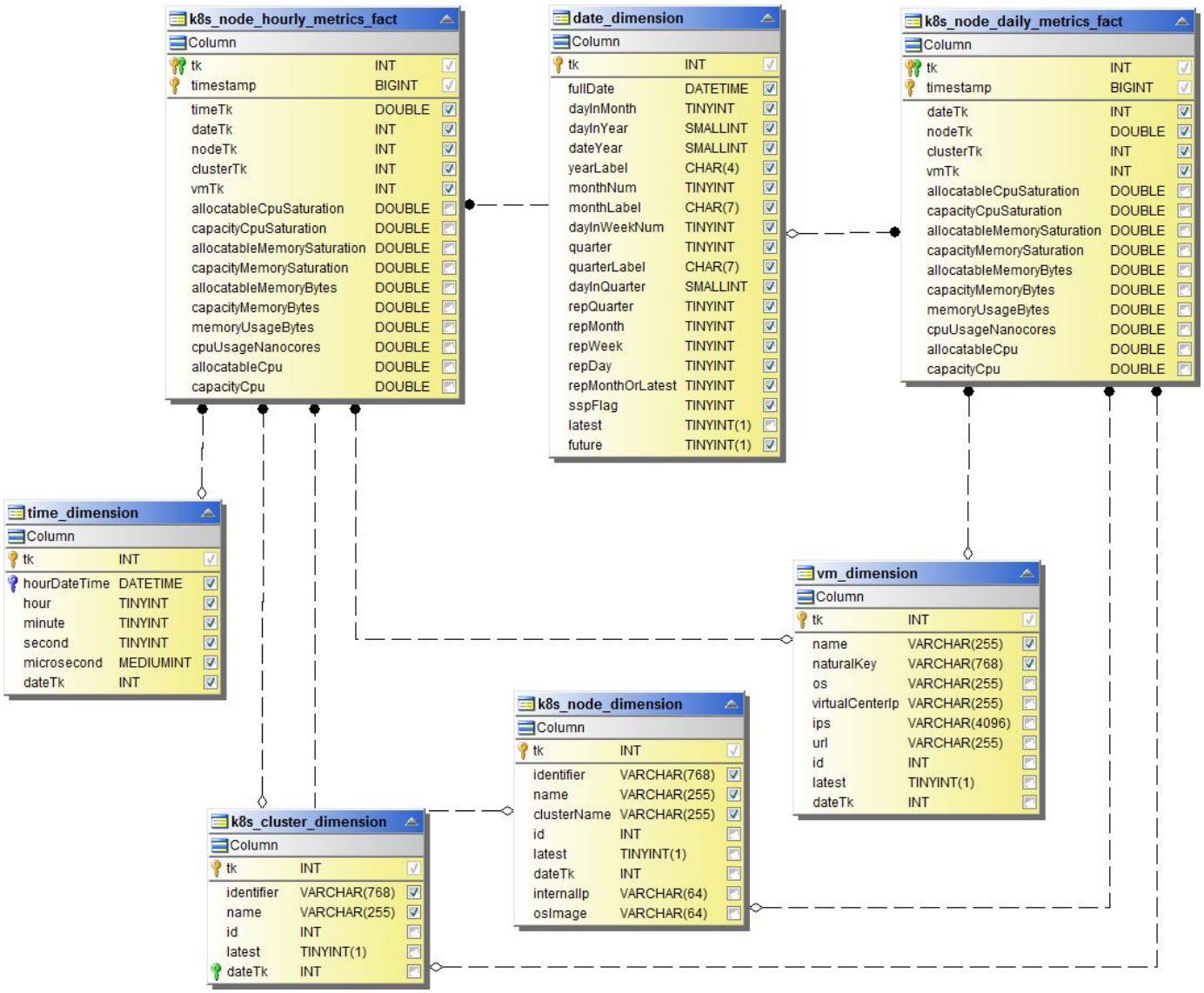
Dati sulle metriche dei cluster di Kubernetes



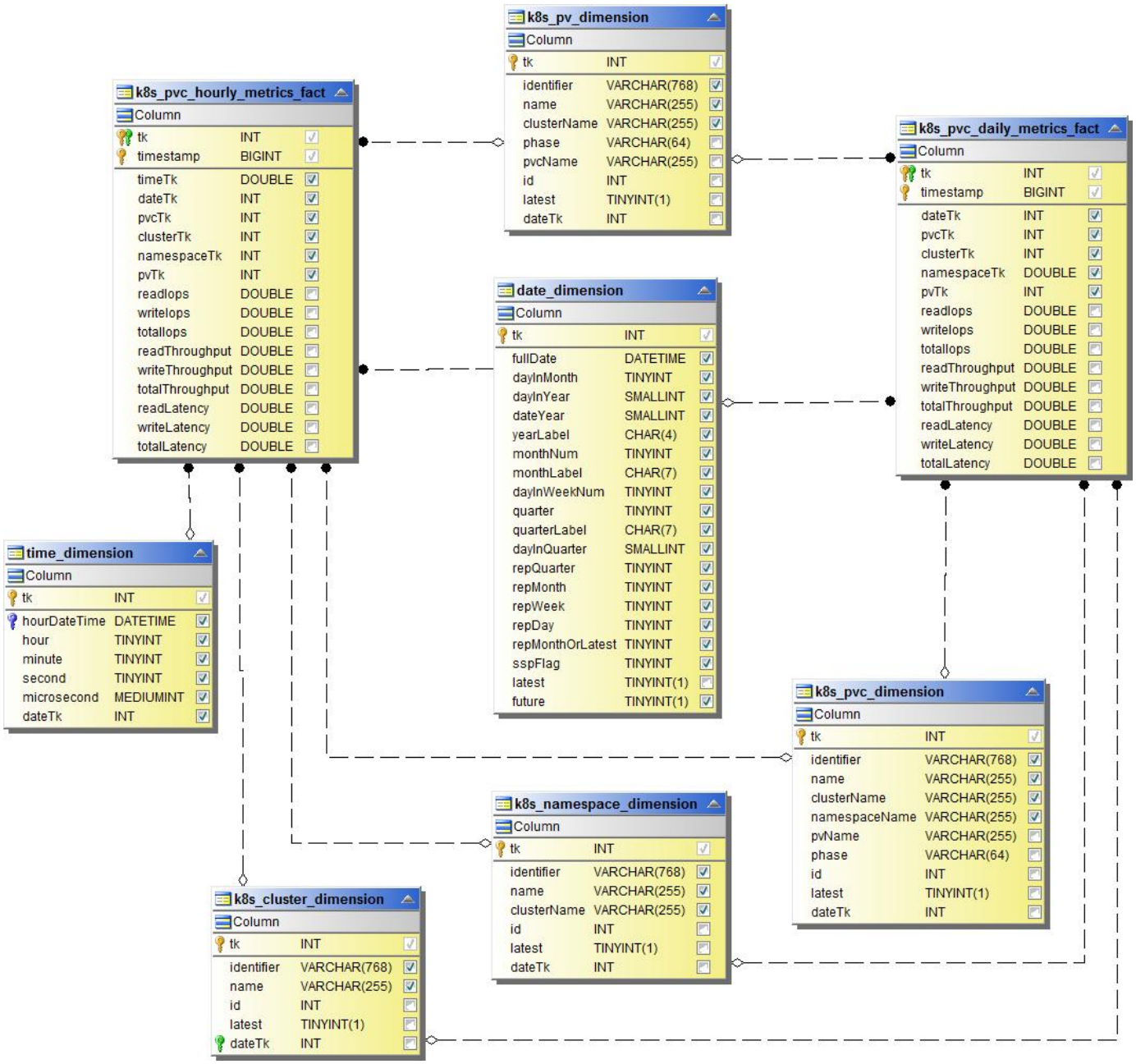
Il fatto delle metriche dello spazio dei nomi Kubernetes



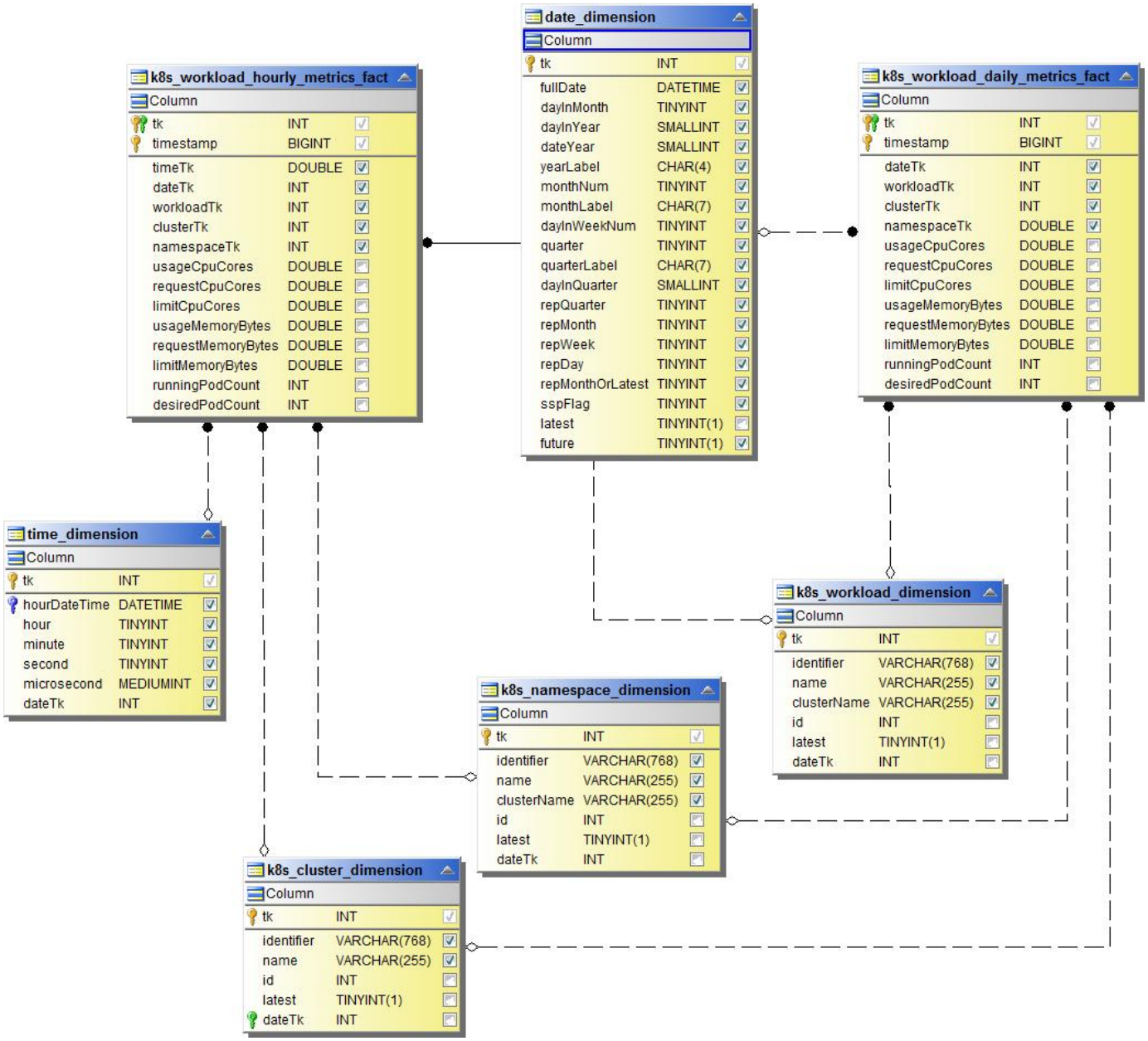
Dati relativi alle metriche dei nodi di Kubernetes



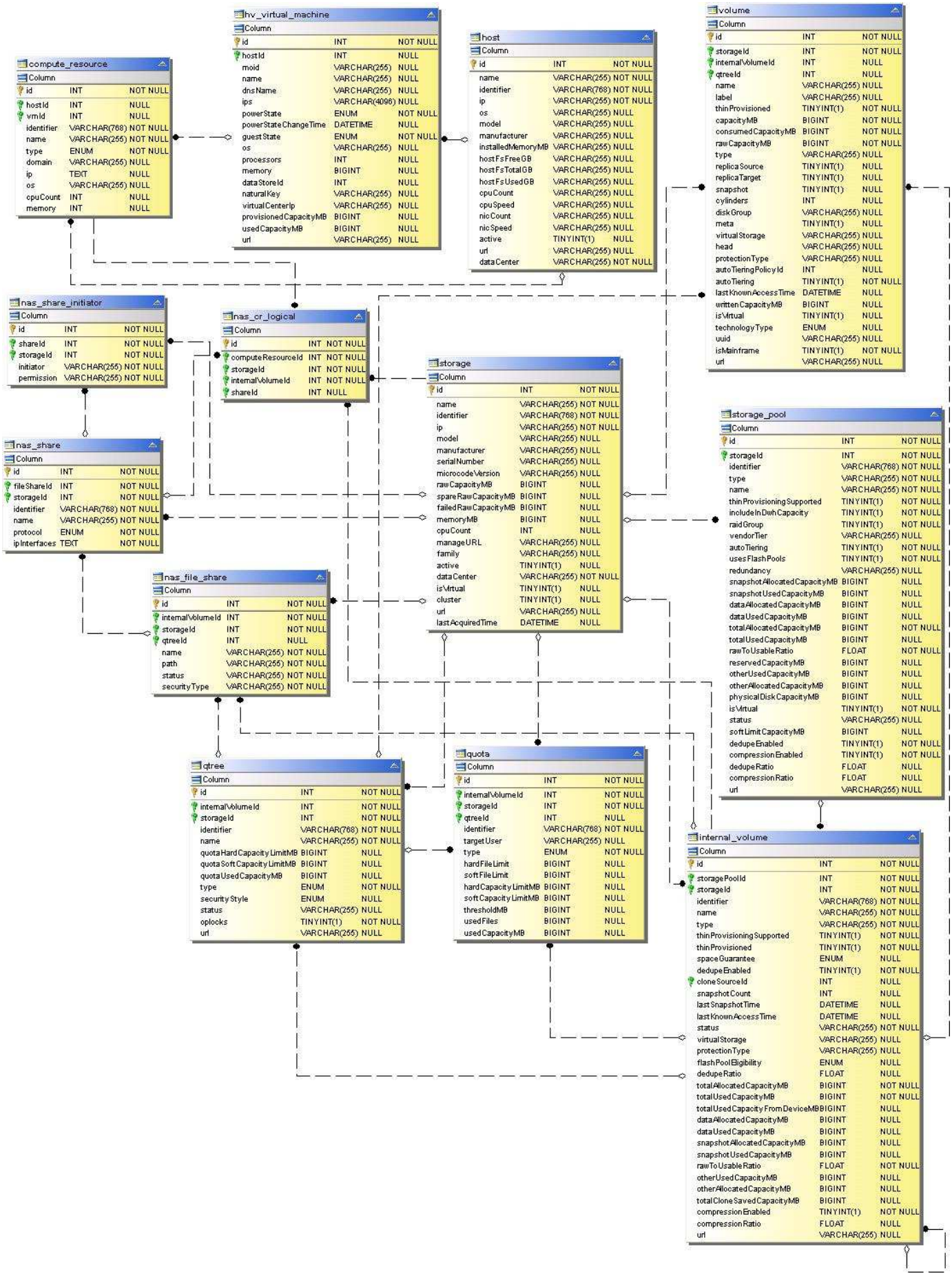
Kubernetes PVC Metrics fatto



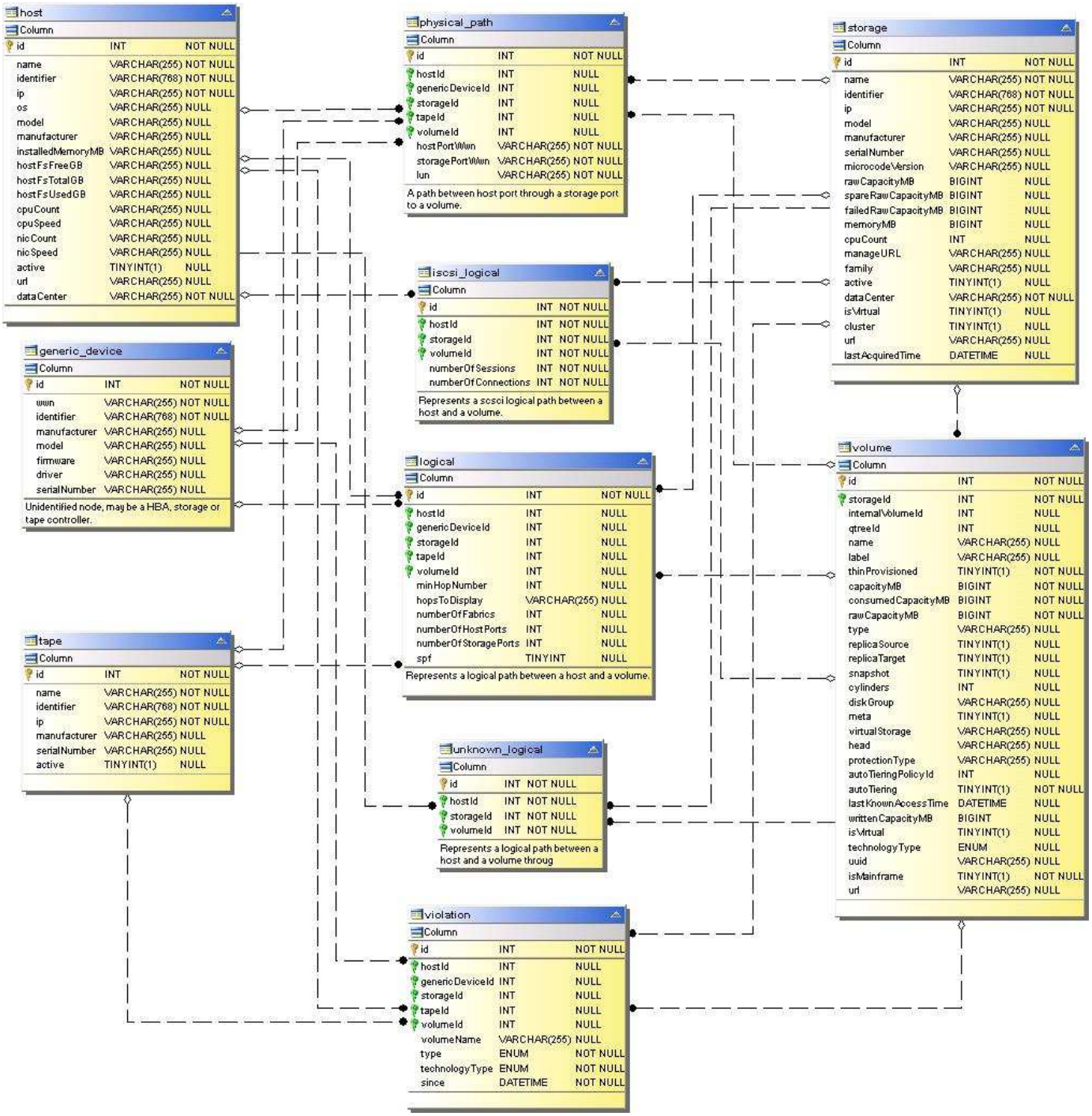
Kubernetes Workload Metrics


k8s_workload_hourly_metrics_fact
Column
tk INT
timestamp BIGINT
timeTk DOUBLE
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk INT
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
sspFlag TINYINT
latest TINYINT(1)
future TINYINT(1)
k8s_workload_daily_metrics_fact
Column
tk INT
timestamp BIGINT
dateTk INT
workloadTk INT
clusterTk INT
namespaceTk DOUBLE
usageCpuCores DOUBLE
requestCpuCores DOUBLE
limitCpuCores DOUBLE
usageMemoryBytes DOUBLE
requestMemoryBytes DOUBLE
limitMemoryBytes DOUBLE
runningPodCount INT
desiredPodCount INT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT
k8s_workload_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_namespace_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
clusterName VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
k8s_cluster_dimension
Column
tk INT
identifier VARCHAR(768)
name VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT

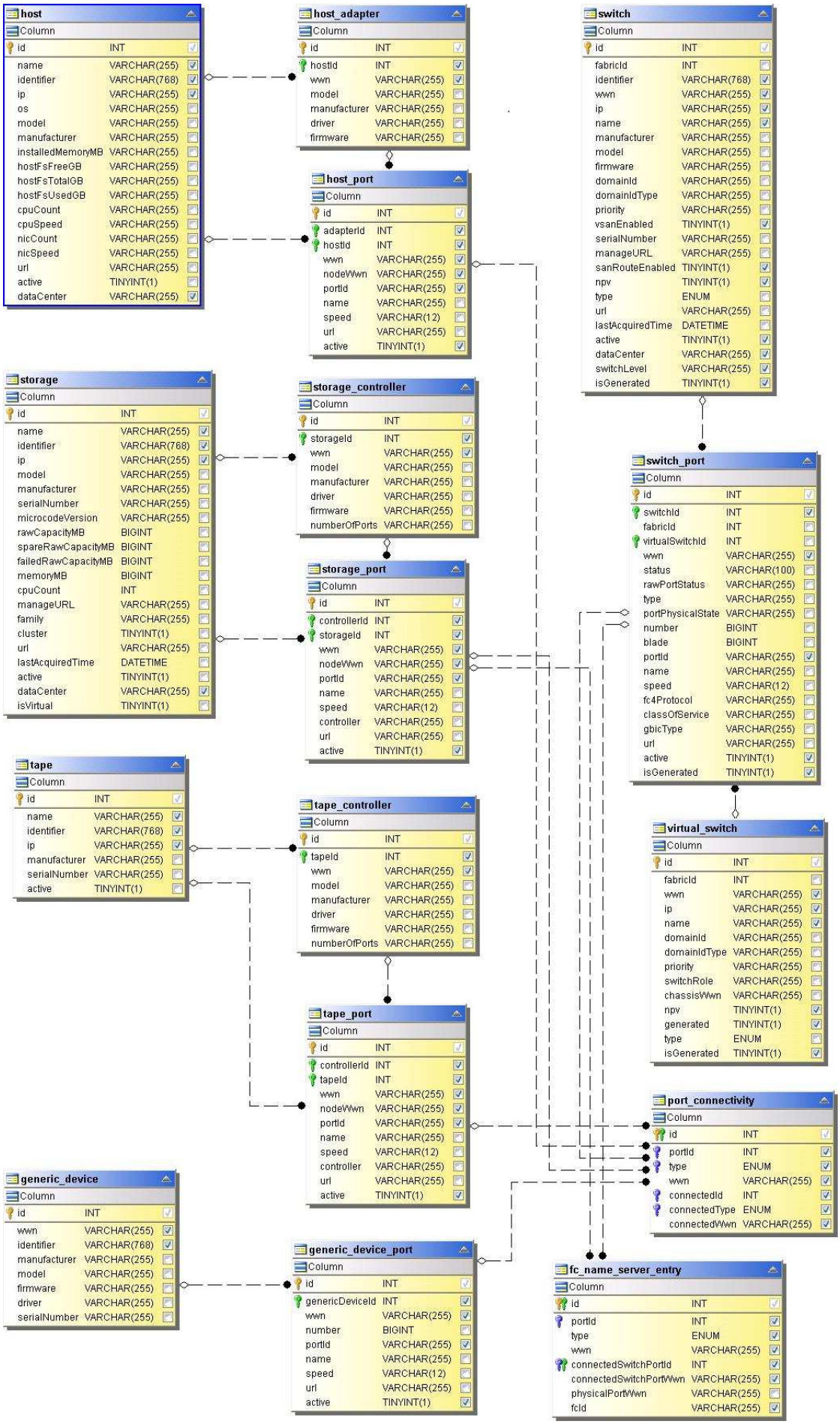
NAS


compute_resource
Column
id INT NOT NULL
hostId INT NULL
vmId INT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type ENUM NOT NULL
domain VARCHAR(255) NULL
ip TEXT NULL
os VARCHAR(255) NULL
cpuCount INT NULL
memory INT NULL
hv_virtual_machine
Column
id INT NOT NULL
hostId INT NULL
moid VARCHAR(255) NULL
name VARCHAR(255) NULL
dnsName VARCHAR(255) NULL
ips VARCHAR(4096) NULL
powerState ENUM NOT NULL
powerStateChangeTime DATETIME NULL
guestState ENUM NOT NULL
os VARCHAR(255) NULL
processors INT NULL
memory BIGINT NULL
dataStoreId INT NULL
naturalKey VARCHAR(255) NULL
virtualCenterIp VARCHAR(255) NULL
provisionedCapacityMB BIGINT NULL
usedCapacityMB BIGINT NULL
url VARCHAR(255) NULL
host
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
os VARCHAR(255) NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
installedMemoryMB VARCHAR(255) NULL
hostFsFreeGB VARCHAR(255) NULL
hostFsTotalGB VARCHAR(255) NULL
hostFsUsedGB VARCHAR(255) NULL
cpuCount VARCHAR(255) NULL
cpuSpeed VARCHAR(255) NULL
nicCount VARCHAR(255) NULL
nicSpeed VARCHAR(255) NULL
active TINYINT(1) NULL
url VARCHAR(255) NULL
dataCenter VARCHAR(255) NOT NULL
volume
Column
id INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NULL
qtreeId INT NULL
name VARCHAR(255) NULL
label VARCHAR(255) NULL
thinProvisioned TINYINT(1) NOT NULL
capacityMB BIGINT NOT NULL
consumedCapacityMB BIGINT NOT NULL
rawCapacityMB BIGINT NOT NULL
type VARCHAR(255) NULL
replicaSource TINYINT(1) NULL
replicaTarget TINYINT(1) NULL
snapshot TINYINT(1) NULL
cylinders INT NULL
diskGroup VARCHAR(255) NULL
meta TINYINT(1) NULL
virtualStorage VARCHAR(255) NULL
head VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
autoTieringPolicyId INT NULL
autoTiering TINYINT(1) NOT NULL
lastKnownAccessTime DATETIME NULL
writtenCapacityMB BIGINT NULL
isVirtual TINYINT(1) NULL
technologyType ENUM NULL
uuid VARCHAR(255) NULL
isMainframe TINYINT(1) NOT NULL
url VARCHAR(255) NULL
nas_share_initiator
Column
id INT NOT NULL
shareId INT NOT NULL
storageId INT NOT NULL
initiator VARCHAR(255) NOT NULL
permission VARCHAR(255) NOT NULL
nas_cr_logical
Column
id INT NOT NULL
computeResourceId INT NOT NULL
storageId INT NOT NULL
internalVolumeId INT NOT NULL
shareId INT NULL
storage
Column
id INT NOT NULL
name VARCHAR(255) NOT NULL
identifier VARCHAR(768) NOT NULL
ip VARCHAR(255) NOT NULL
model VARCHAR(255) NULL
manufacturer VARCHAR(255) NULL
serialNumber VARCHAR(255) NULL
microcodeVersion VARCHAR(255) NULL
rawCapacityMB BIGINT NULL
spareRawCapacityMB BIGINT NULL
failedRawCapacityMB BIGINT NULL
memoryMB BIGINT NULL
cpuCount INT NULL
manageURL VARCHAR(255) NULL
family VARCHAR(255) NULL
active TINYINT(1) NULL
dataCenter VARCHAR(255) NOT NULL
isVirtual TINYINT(1) NULL
cluster TINYINT(1) NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
storage_pool
Column
id INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
type VARCHAR(255) NOT NULL
name VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
includeInDwhCapacity TINYINT(1) NOT NULL
raidGroup TINYINT(1) NOT NULL
vendorTier VARCHAR(255) NULL
autoTiering TINYINT(1) NOT NULL
usesFlashPools TINYINT(1) NOT NULL
redundancy VARCHAR(255) NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
reservedCapacityMB BIGINT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
physicalDiskCapacityMB BIGINT NULL
isVirtual TINYINT(1) NOT NULL
status VARCHAR(255) NULL
softLimitCapacityMB BIGINT NULL
dedupeEnabled TINYINT(1) NOT NULL
compressionEnabled TINYINT(1) NOT NULL
dedupeRatio FLOAT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL
nas_share
Column
id INT NOT NULL
fileShareId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
protocol ENUM NOT NULL
ipInterfaces TEXT NOT NULL
nas_file_share
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
name VARCHAR(255) NOT NULL
path VARCHAR(255) NOT NULL
status VARCHAR(255) NOT NULL
securityType VARCHAR(255) NOT NULL
qtree
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
quotaHardCapacityLimitMB BIGINT NULL
quotaSoftCapacityLimitMB BIGINT NULL
quotaUsedCapacityMB BIGINT NULL
type ENUM NOT NULL
securityStyle ENUM NULL
status VARCHAR(255) NULL
oplocks TINYINT(1) NOT NULL
url VARCHAR(255) NULL
quota
Column
id INT NOT NULL
internalVolumeId INT NOT NULL
storageId INT NOT NULL
qtreeId INT NULL
identifier VARCHAR(768) NOT NULL
targetUser VARCHAR(255) NULL
type ENUM NOT NULL
hardFileLimit BIGINT NULL
softFileLimit BIGINT NULL
hardCapacityLimitMB BIGINT NULL
softCapacityLimitMB BIGINT NULL
thresholdMB BIGINT NULL
usedFiles BIGINT NULL
usedCapacityMB BIGINT NULL
internal_volume
Column
id INT NOT NULL
storagePoolId INT NOT NULL
storageId INT NOT NULL
identifier VARCHAR(768) NOT NULL
name VARCHAR(255) NOT NULL
type VARCHAR(255) NOT NULL
thinProvisioningSupported TINYINT(1) NOT NULL
thinProvisioned TINYINT(1) NOT NULL
spaceGuarantee ENUM NULL
dedupeEnabled TINYINT(1) NOT NULL
cloneSourceId INT NULL
snapshotCount INT NULL
lastSnapshotTime DATETIME NULL
lastKnownAccessTime DATETIME NULL
status VARCHAR(255) NOT NULL
virtualStorage VARCHAR(255) NULL
protectionType VARCHAR(255) NULL
flashPoolEligibility ENUM NULL
dedupeRatio FLOAT NULL
totalAllocatedCapacityMB BIGINT NOT NULL
totalUsedCapacityMB BIGINT NOT NULL
totalUsedCapacityFromDeviceMB BIGINT NULL
dataAllocatedCapacityMB BIGINT NULL
dataUsedCapacityMB BIGINT NULL
snapshotAllocatedCapacityMB BIGINT NULL
snapshotUsedCapacityMB BIGINT NULL
rawToUsableRatio FLOAT NOT NULL
otherUsedCapacityMB BIGINT NULL
otherAllocatedCapacityMB BIGINT NULL
totalCloneSavedCapacityMB BIGINT NULL
compressionEnabled TINYINT(1) NOT NULL
compressionRatio FLOAT NULL
url VARCHAR(255) NULL

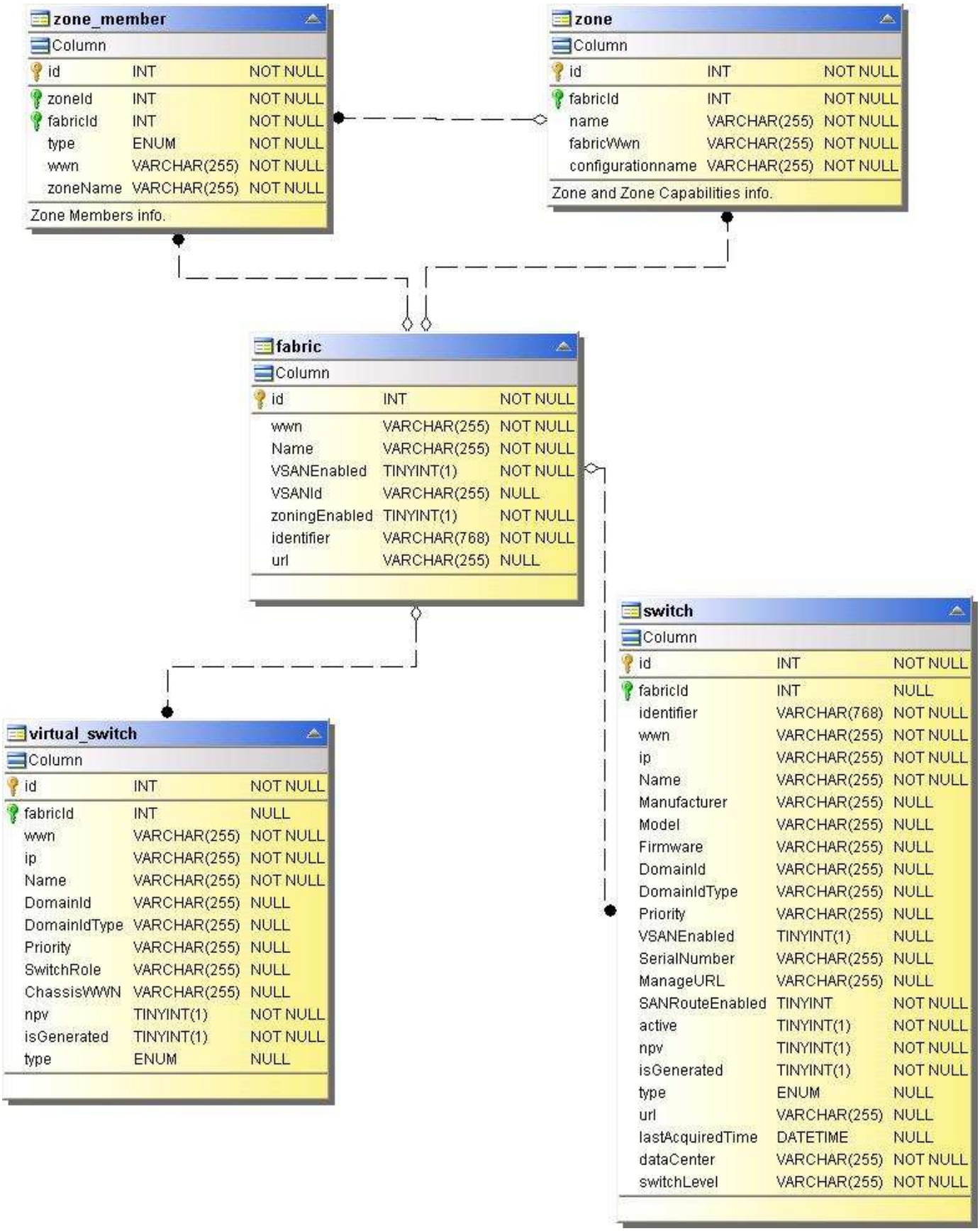
Percorsi e violazioni



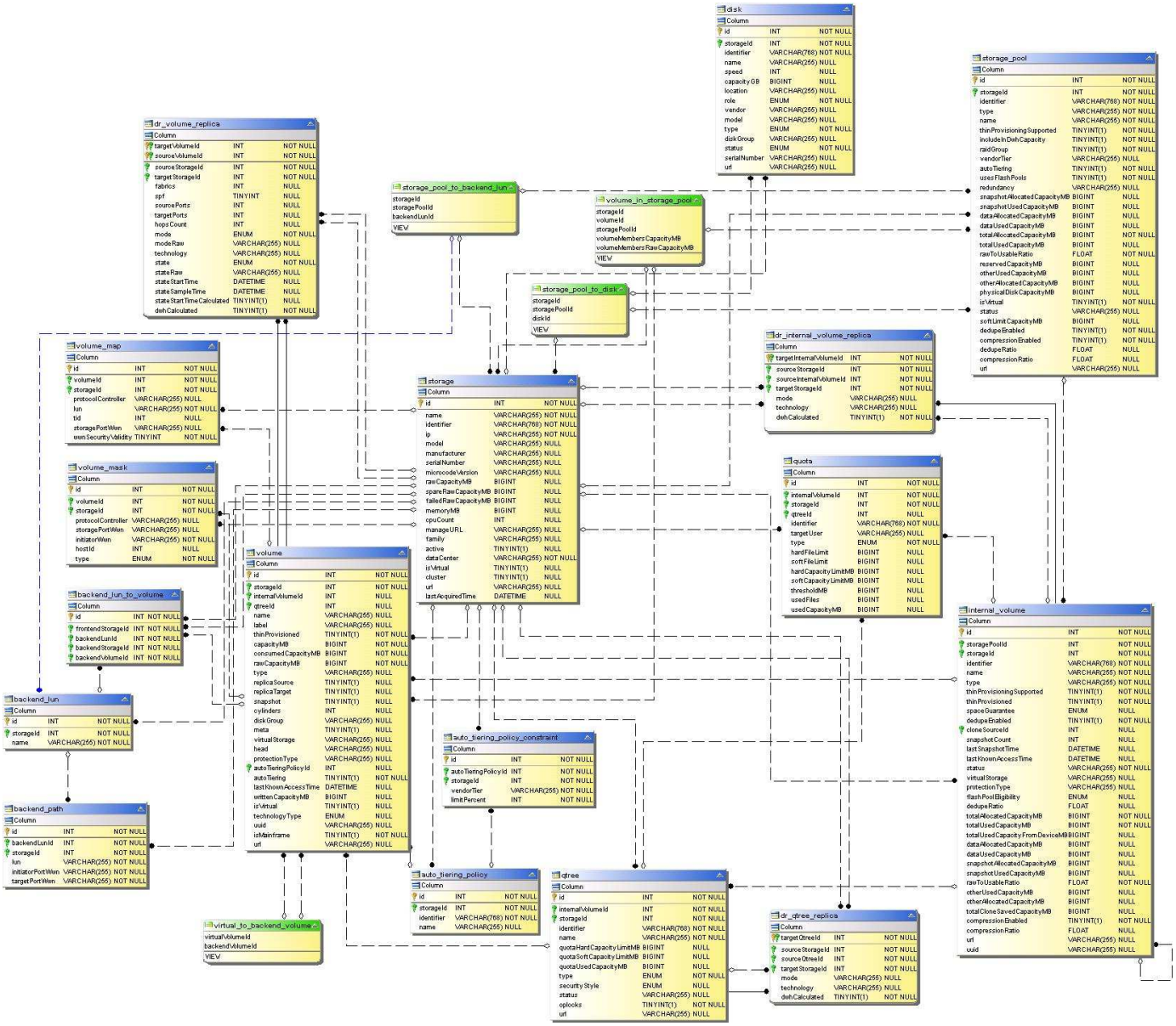
Connettività delle porte


host
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
os VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
installedMemoryMB VARCHAR(255)
hostFsFreeGB VARCHAR(255)
hostFsTotalGB VARCHAR(255)
hostFsUsedGB VARCHAR(255)
cpuCount VARCHAR(255)
cpuSpeed VARCHAR(255)
nicCount VARCHAR(255)
nicSpeed VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
dataCenter VARCHAR(255)
host_adapter
Column
id INT
hostId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
host_port
Column
id INT
adapterId INT
hostId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
switch
Column
id INT
fabricId INT
identifier VARCHAR(768)
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
vsanEnabled TINYINT(1)
serialNumber VARCHAR(255)
manageURL VARCHAR(255)
sanRouteEnabled TINYINT(1)
npv TINYINT(1)
type ENUM
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
switchLevel VARCHAR(255)
isGenerated TINYINT(1)
storage
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
rawCapacityMB BIGINT
spareRawCapacityMB BIGINT
failedRawCapacityMB BIGINT
memoryMB BIGINT
cpuCount INT
manageURL VARCHAR(255)
family VARCHAR(255)
cluster TINYINT(1)
url VARCHAR(255)
lastAcquiredTime DATETIME
active TINYINT(1)
dataCenter VARCHAR(255)
isVirtual TINYINT(1)
storage_controller
Column
id INT
storageId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
storage_port
Column
id INT
controllerId INT
storageId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
switch_port
Column
id INT
switchId INT
fabricId INT
virtualSwitchId INT
wwn VARCHAR(255)
status VARCHAR(100)
rawPortStatus VARCHAR(255)
type VARCHAR(255)
portPhysicalState VARCHAR(255)
number BIGINT
blade BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
fc4Protocol VARCHAR(255)
classOfService VARCHAR(255)
gbicType VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
isGenerated TINYINT(1)
tape
Column
id INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
active TINYINT(1)
tape_controller
Column
id INT
tapeId INT
wwn VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
driver VARCHAR(255)
firmware VARCHAR(255)
numberOfPorts VARCHAR(255)
virtual_switch
Column
id INT
fabricId INT
wwn VARCHAR(255)
ip VARCHAR(255)
name VARCHAR(255)
domainId VARCHAR(255)
domainIdType VARCHAR(255)
priority VARCHAR(255)
switchRole VARCHAR(255)
chassisWwn VARCHAR(255)
npv TINYINT(1)
generated TINYINT(1)
type ENUM
isGenerated TINYINT(1)
tape_port
Column
id INT
controllerId INT
tapeId INT
wwn VARCHAR(255)
nodeWwn VARCHAR(255)
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
controller VARCHAR(255)
url VARCHAR(255)
active TINYINT(1)
port_connectivity
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedId INT
connectedType ENUM
connectedWwn VARCHAR(255)
generic_device
Column
id INT
wwn VARCHAR(255)
identifier VARCHAR(768)
manufacturer VARCHAR(255)
model VARCHAR(255)
firmware VARCHAR(255)
driver VARCHAR(255)
serialNumber VARCHAR(255)
generic_device_port
Column
id INT
genericDeviceId INT
wwn VARCHAR(255)
number BIGINT
portId VARCHAR(255)
name VARCHAR(255)
speed VARCHAR(12)
url VARCHAR(255)
active TINYINT(1)
fc_name_server_entry
Column
id INT
portId INT
type ENUM
wwn VARCHAR(255)
connectedSwitchPortId INT
connectedSwitchPortWwn VARCHAR(255)
physicalPortWwn VARCHAR(255)
fcId VARCHAR(255)

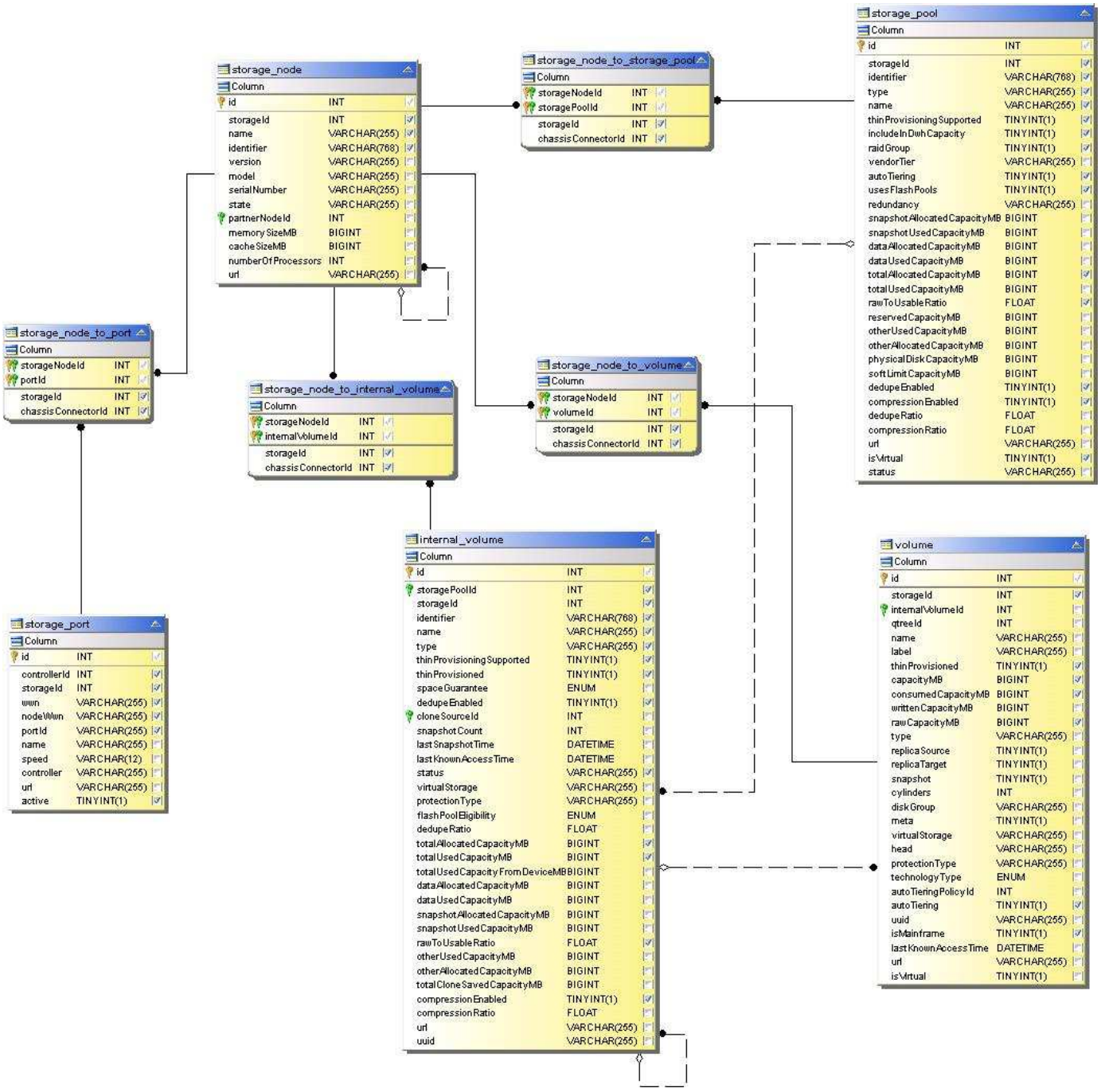
Fabric SAN


zone_member
Column
id INT NOT NULL
zoneId INT NOT NULL
fabricId INT NOT NULL
type ENUM NOT NULL
wwn VARCHAR(255) NOT NULL
zoneName VARCHAR(255) NOT NULL
Zone Members info.
zone
Column
id INT NOT NULL
fabricId INT NOT NULL
name VARCHAR(255) NOT NULL
fabricWwn VARCHAR(255) NOT NULL
configurationname VARCHAR(255) NOT NULL
Zone and Zone Capabilities info.
fabric
Column
id INT NOT NULL
wwn VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
VSANEnabled TINYINT(1) NOT NULL
VSANId VARCHAR(255) NULL
zoningEnabled TINYINT(1) NOT NULL
identifier VARCHAR(768) NOT NULL
url VARCHAR(255) NULL
switch
Column
id INT NOT NULL
fabricId INT NULL
identifier VARCHAR(768) NOT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
Manufacturer VARCHAR(255) NULL
Model VARCHAR(255) NULL
Firmware VARCHAR(255) NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
VSANEnabled TINYINT(1) NULL
SerialNumber VARCHAR(255) NULL
ManageURL VARCHAR(255) NULL
SANRouteEnabled TINYINT NOT NULL
active TINYINT(1) NOT NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL
url VARCHAR(255) NULL
lastAcquiredTime DATETIME NULL
dataCenter VARCHAR(255) NOT NULL
switchLevel VARCHAR(255) NOT NULL
virtual_switch
Column
id INT NOT NULL
fabricId INT NULL
wwn VARCHAR(255) NOT NULL
ip VARCHAR(255) NOT NULL
Name VARCHAR(255) NOT NULL
DomainId VARCHAR(255) NULL
DomainIdType VARCHAR(255) NULL
Priority VARCHAR(255) NULL
SwitchRole VARCHAR(255) NULL
ChassisWWN VARCHAR(255) NULL
npv TINYINT(1) NOT NULL
isGenerated TINYINT(1) NOT NULL
type ENUM NULL

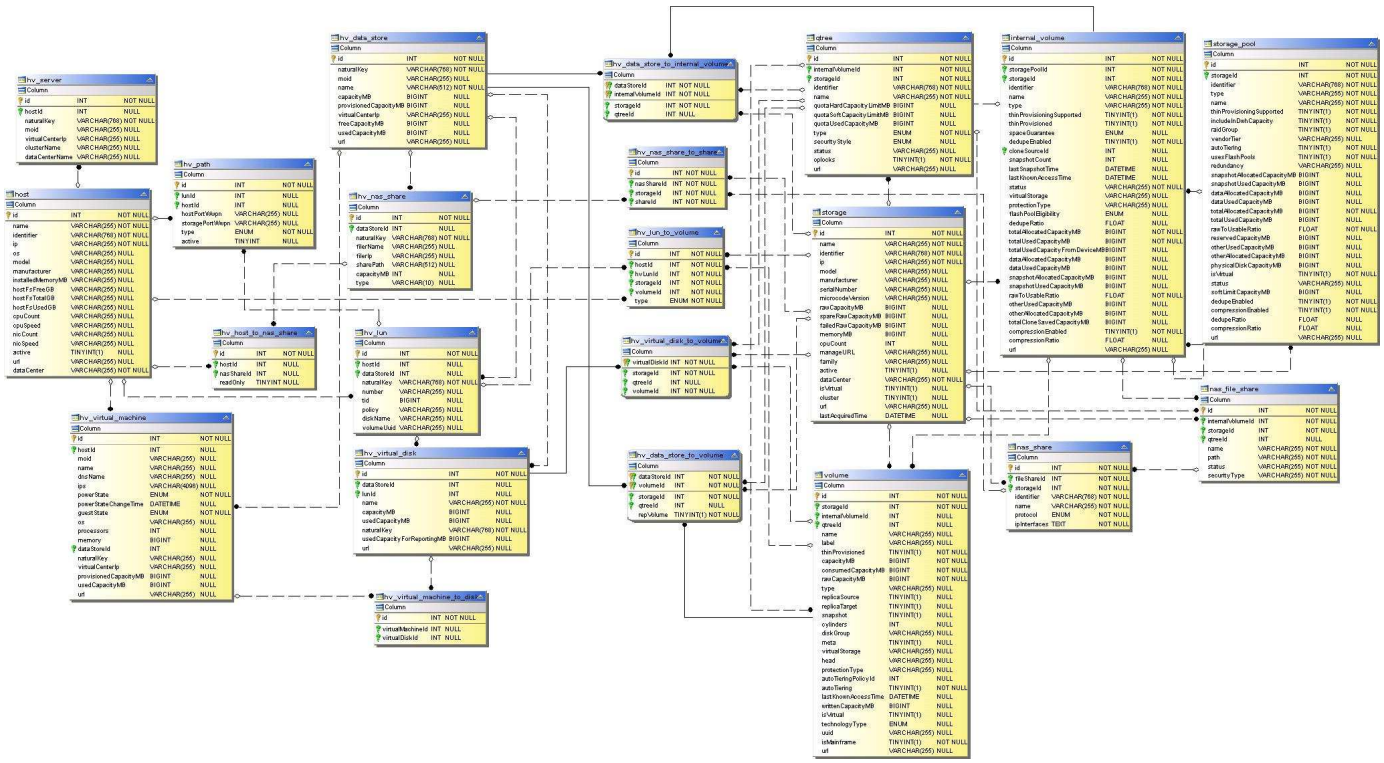
Storage



Nodo di storage



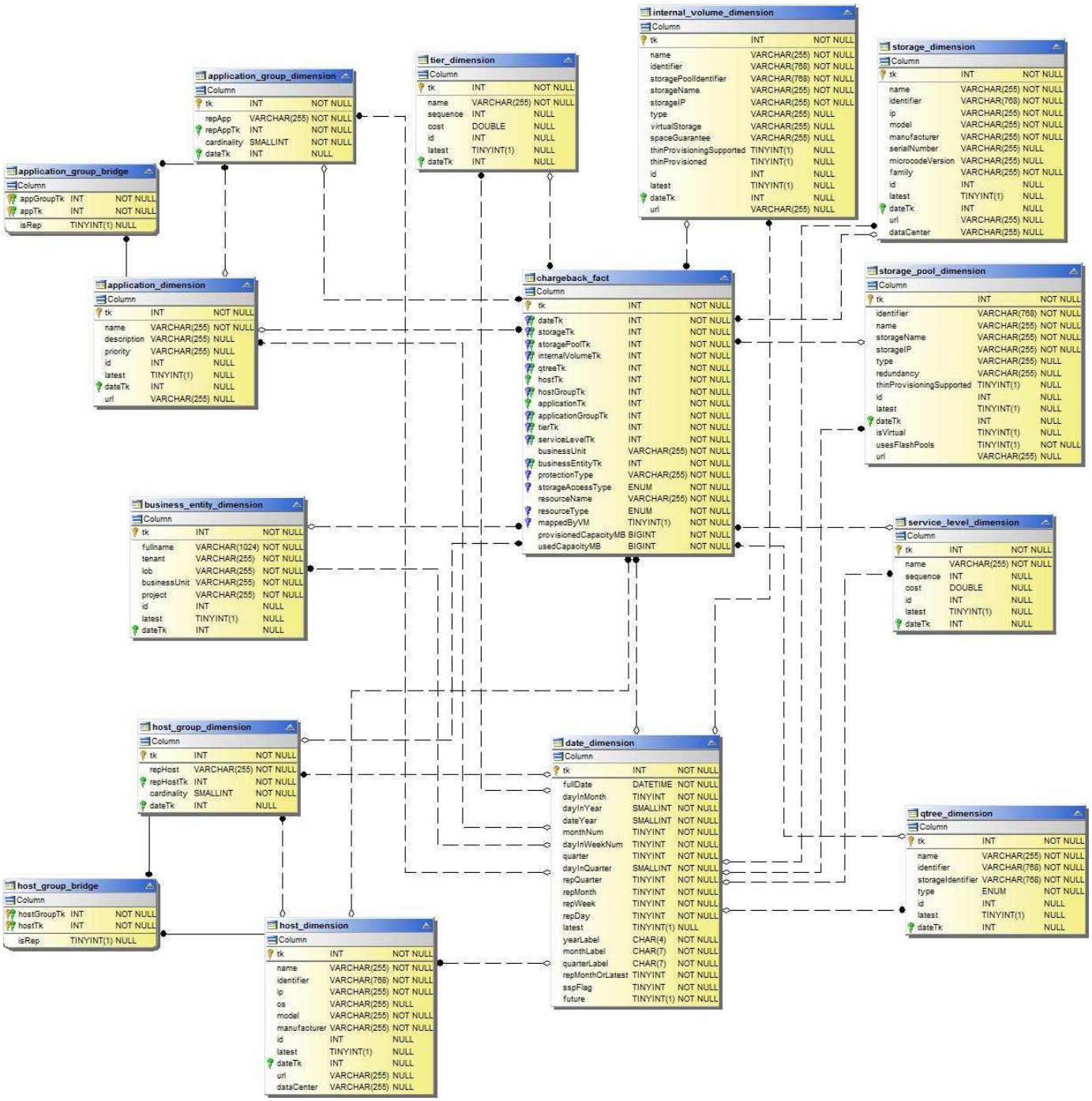
MACCHINA VIRTUALE



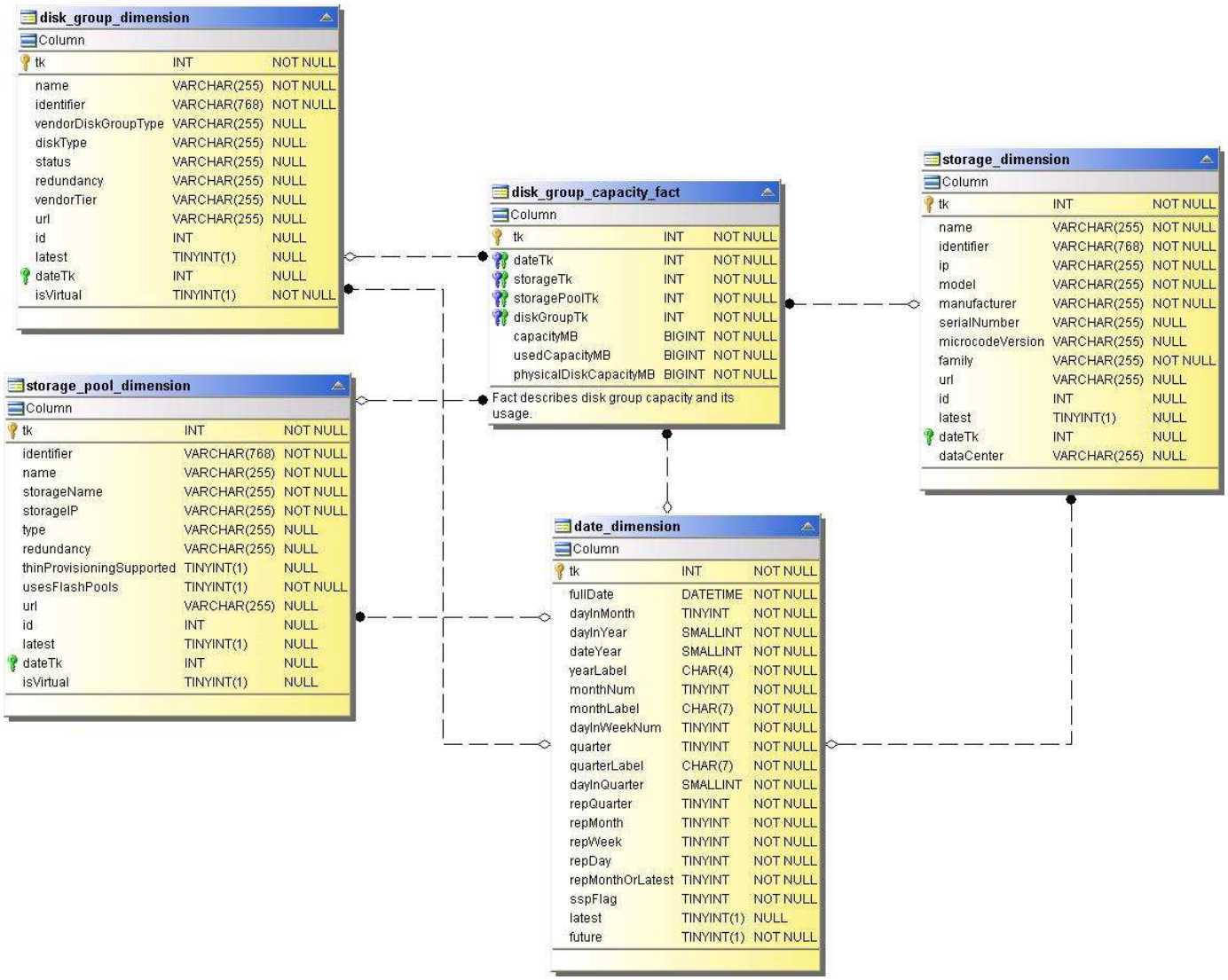
Capacity Datamart

Le immagini seguenti descrivono il datamart della capacità.

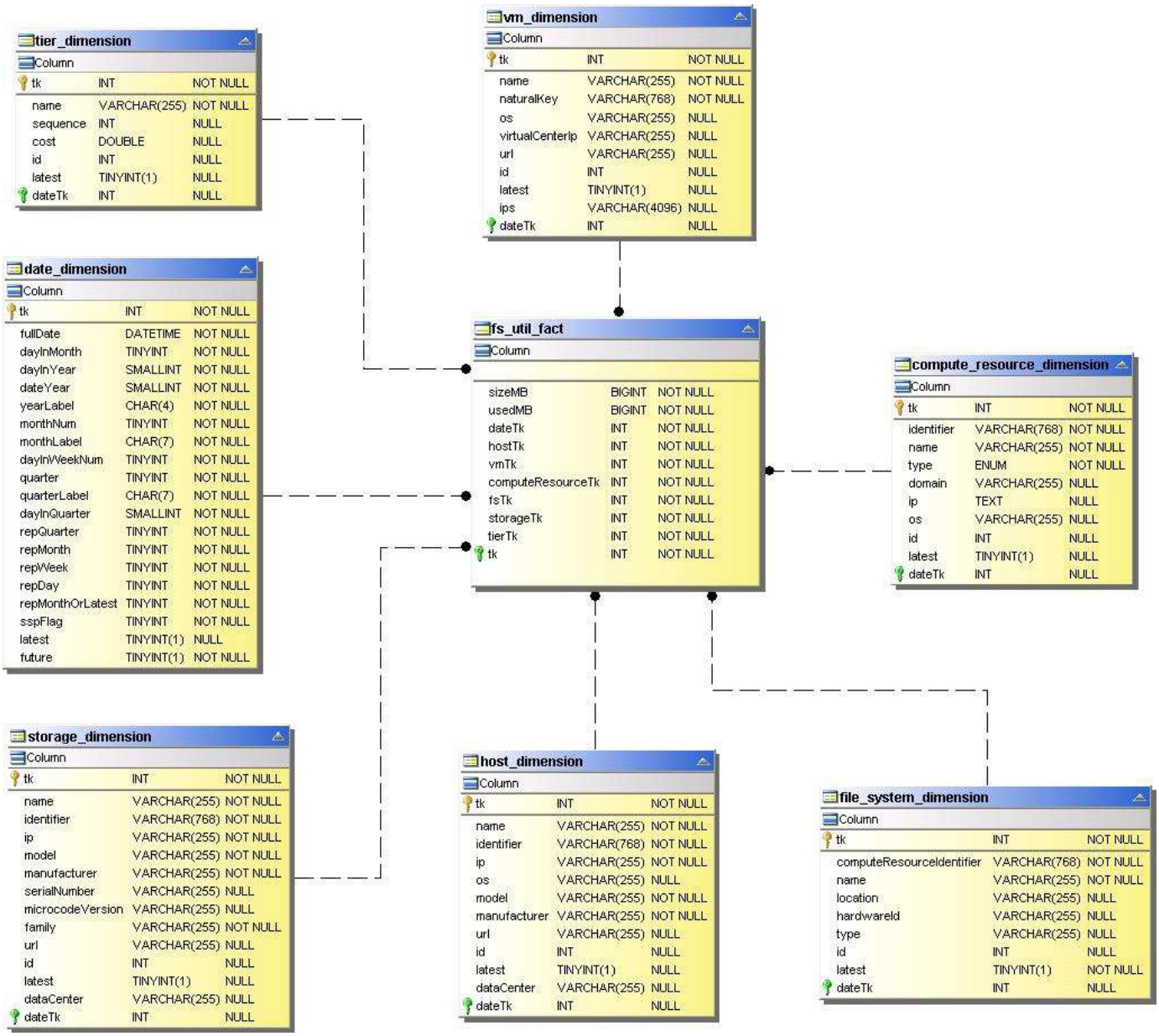
Chargeback



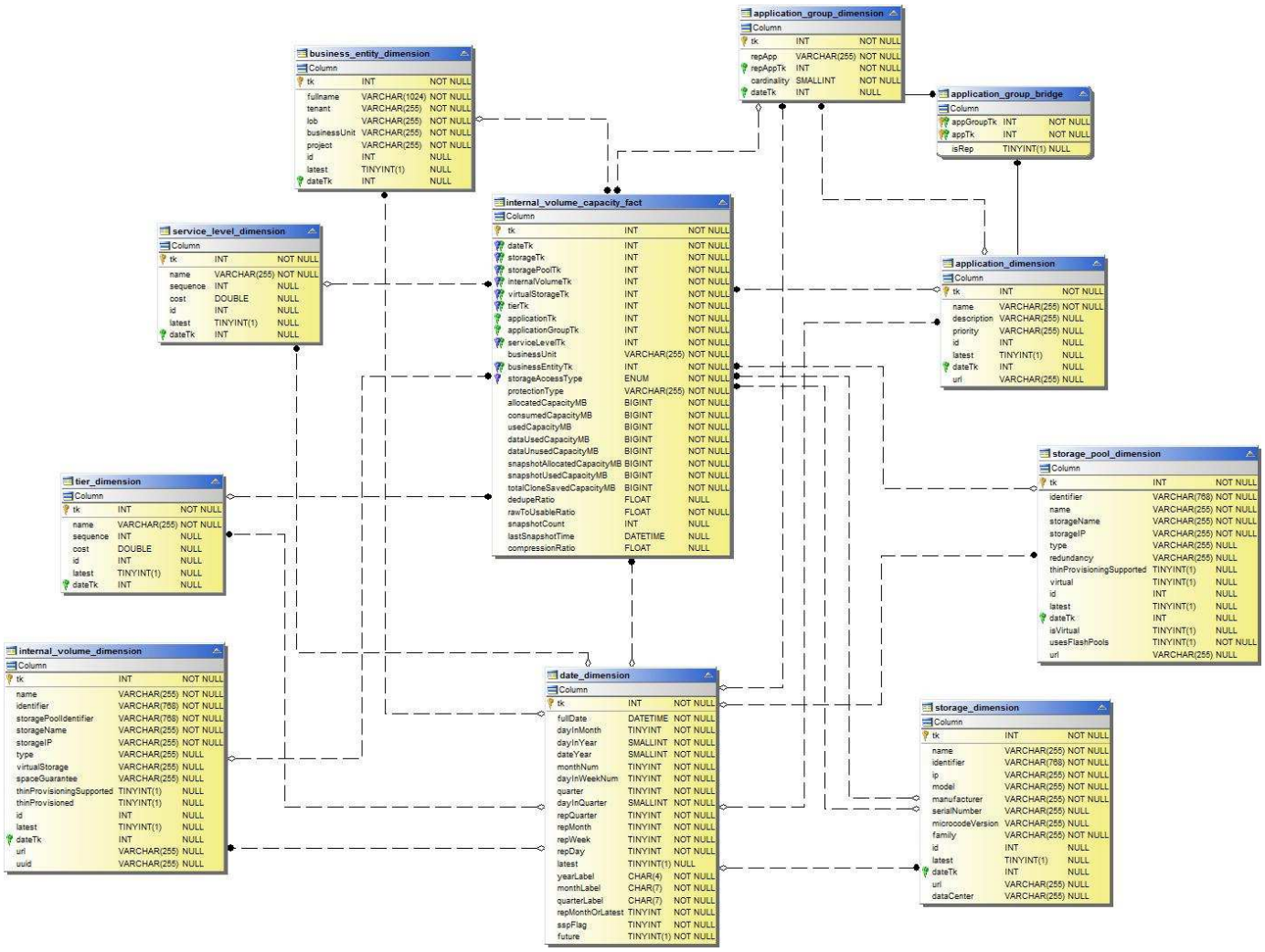
Capacità del gruppo di dischi



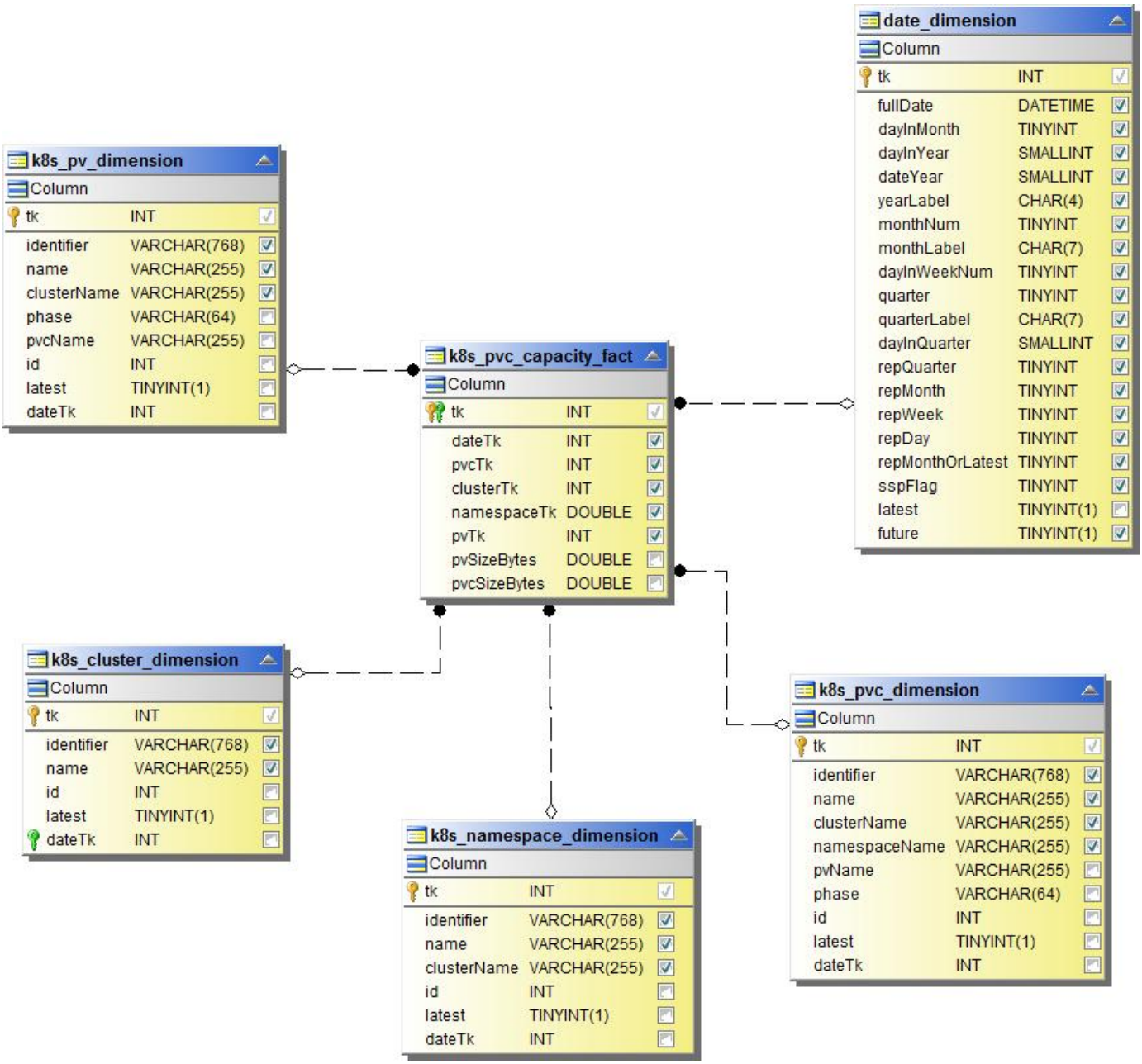
Utilizzo del file system



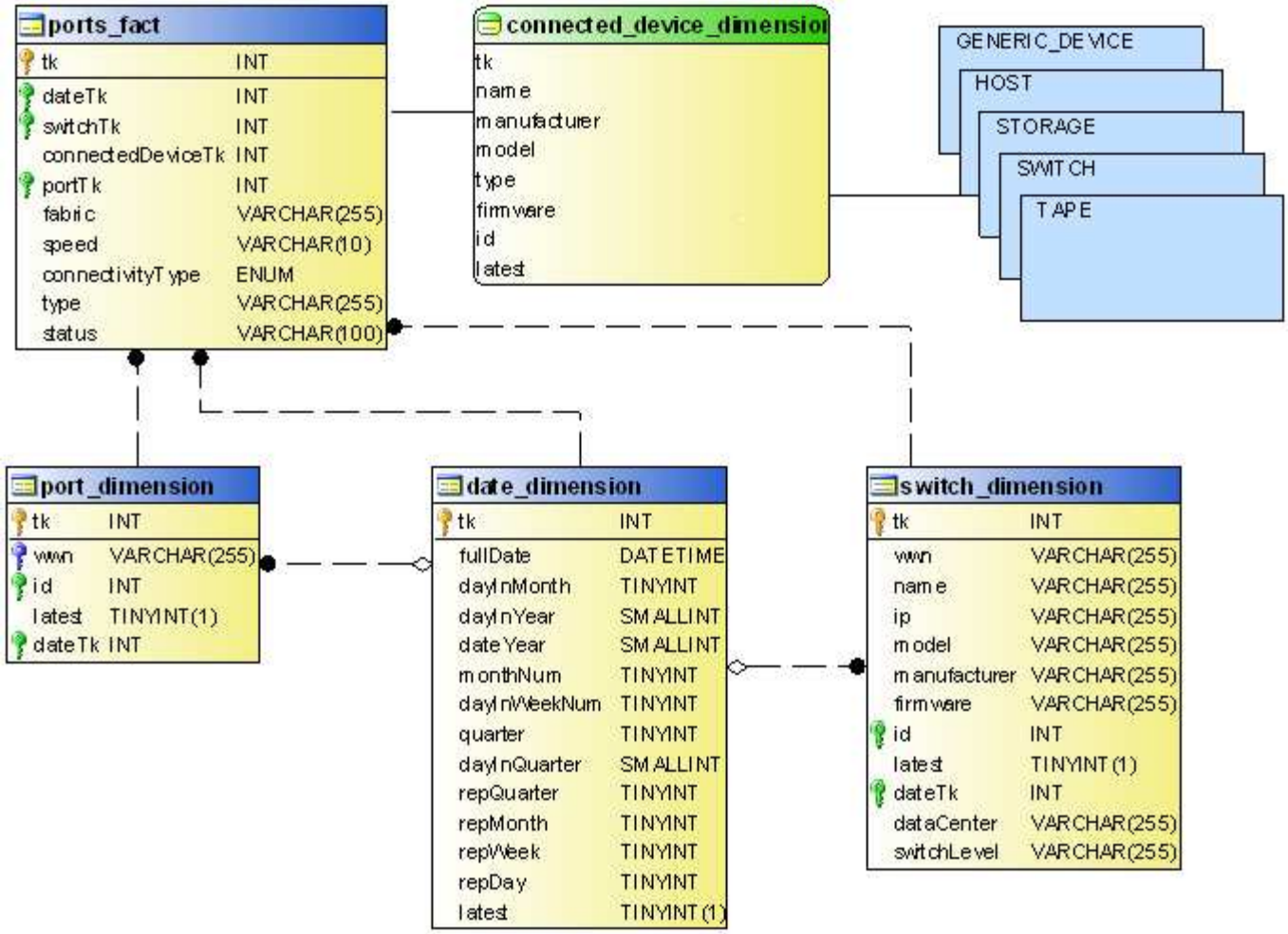
Capacità del volume interno



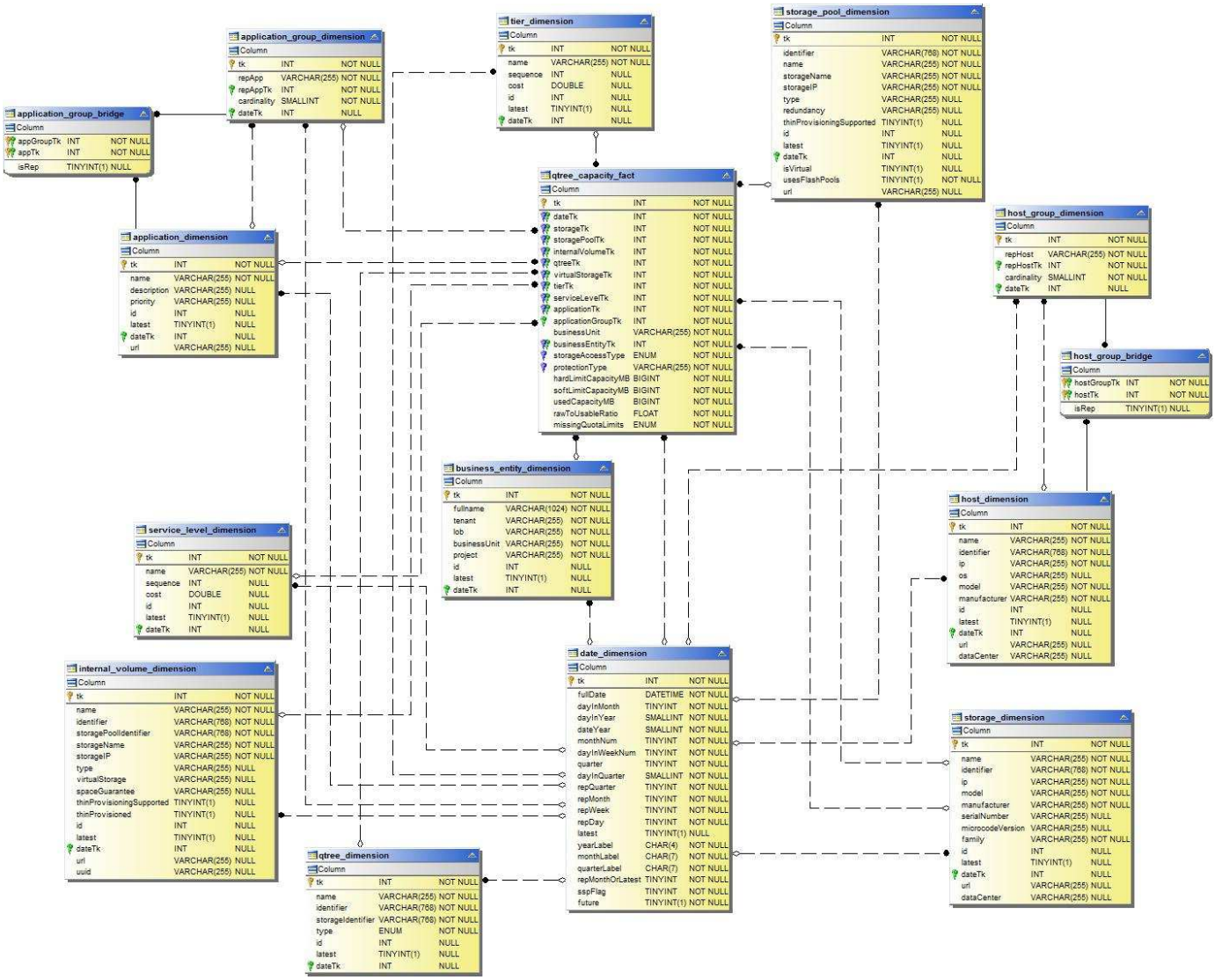
Kubernetes PV Capacity (capacità PV Kubernetes)



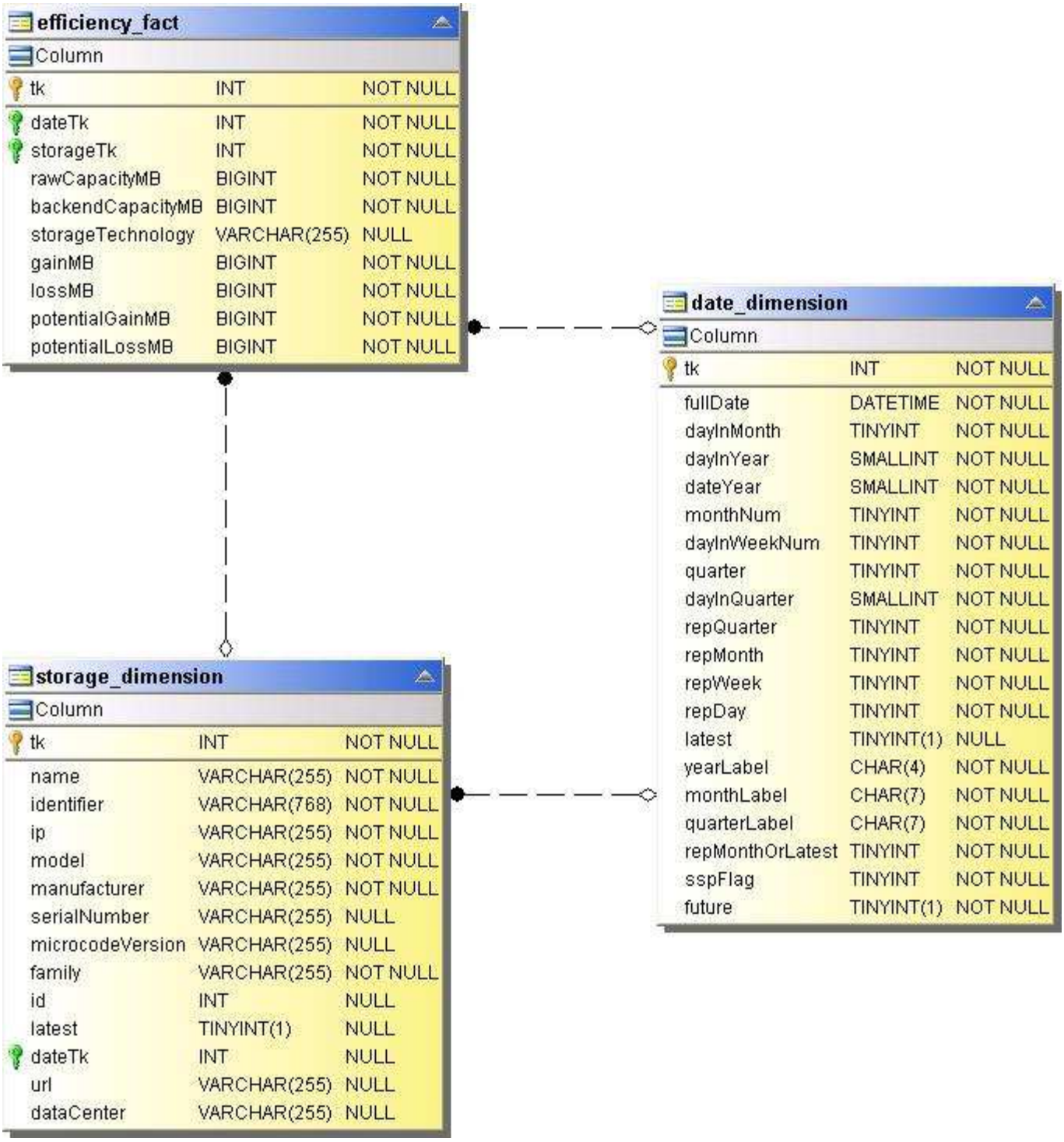
Capacità della porta



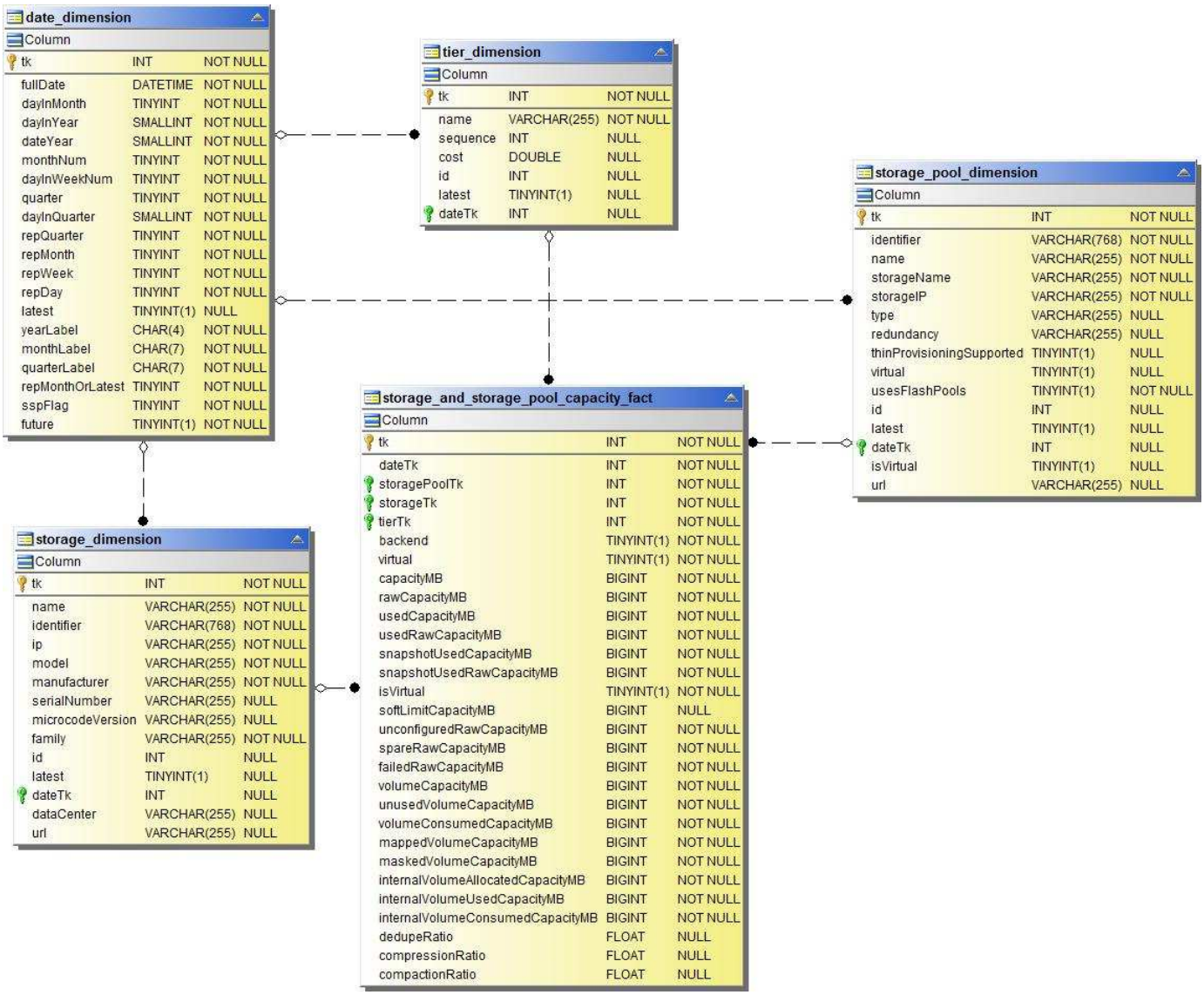
Capacità del qtree



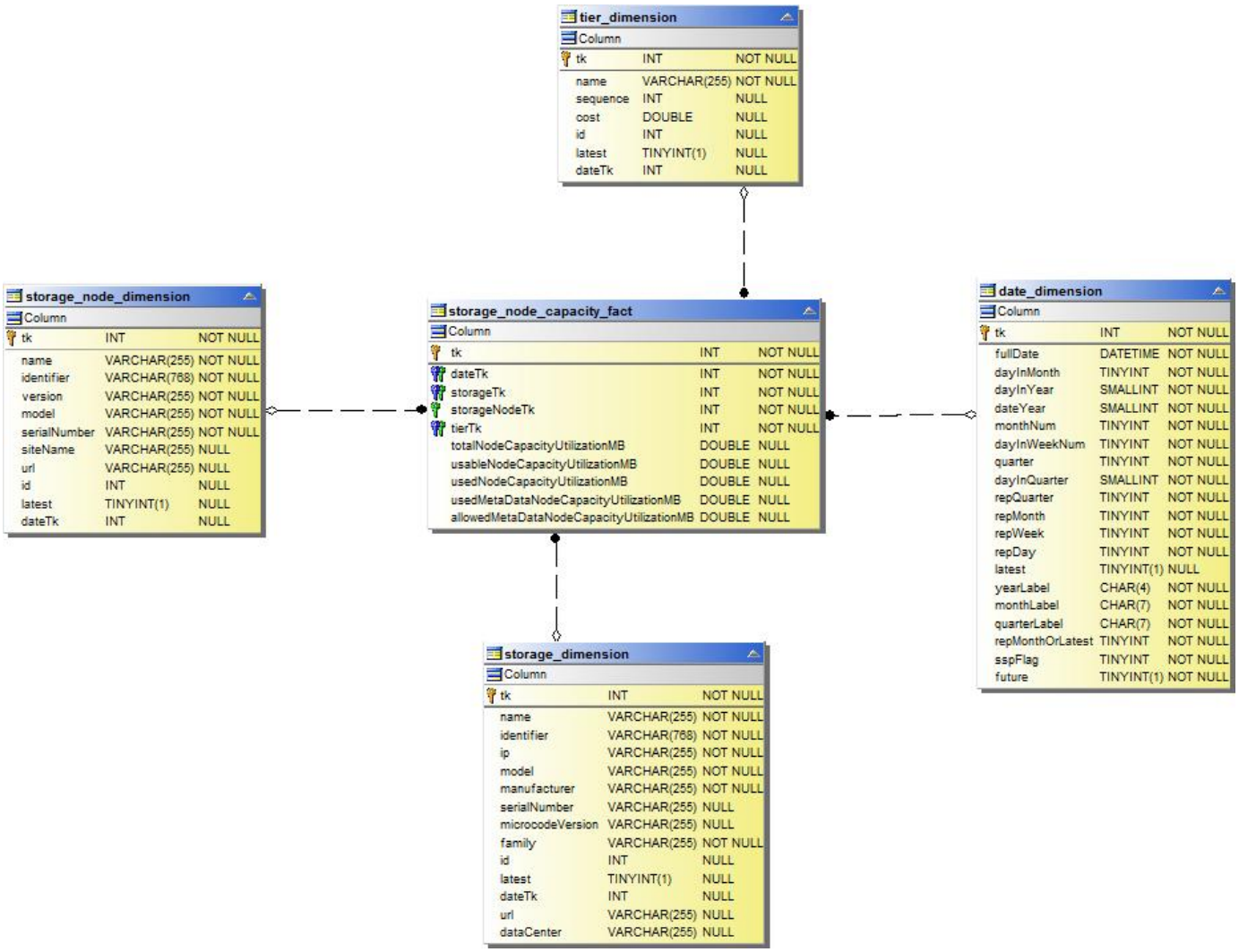
Efficienza della capacità dello storage



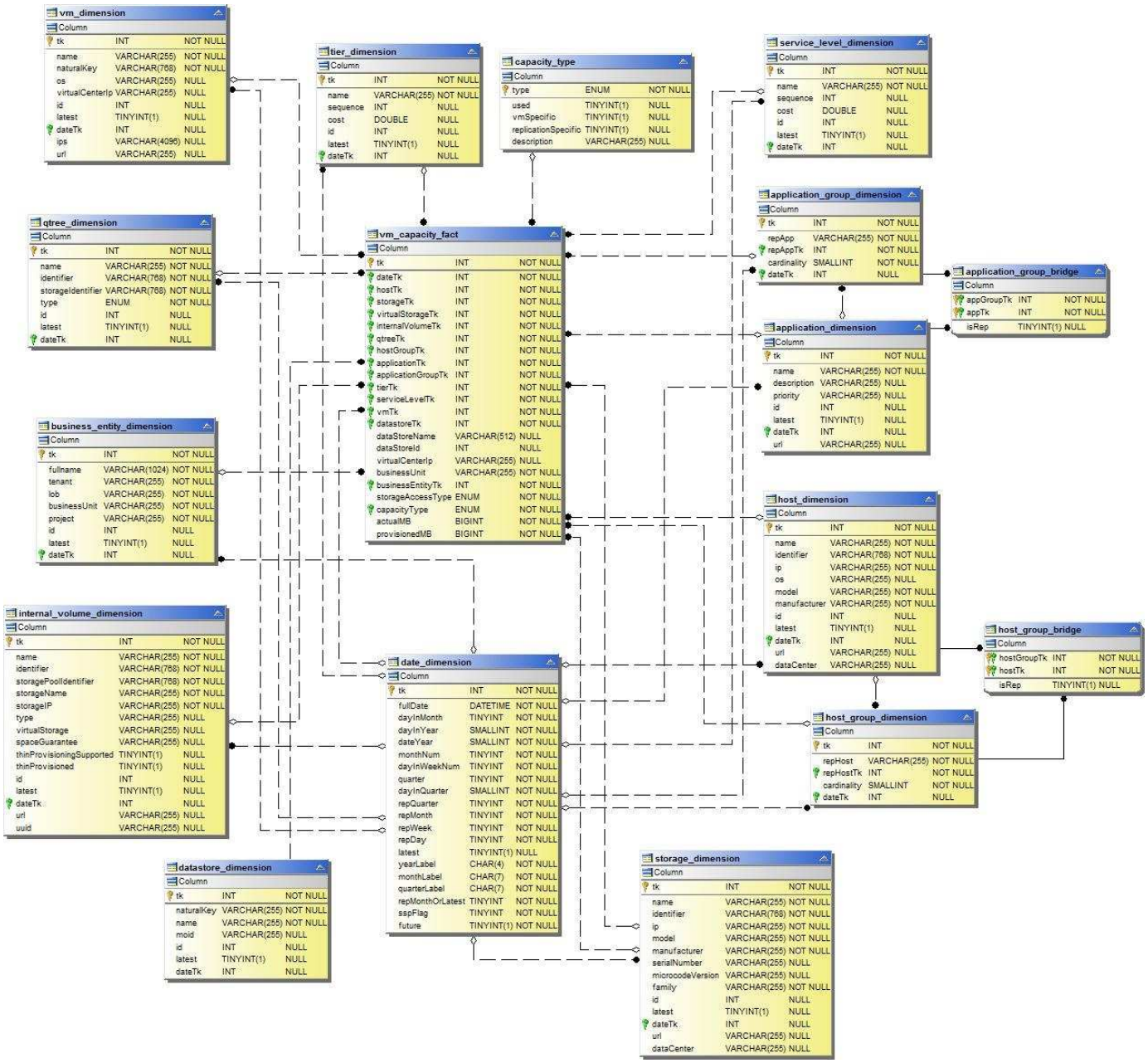
Capacità dello storage e del pool di storage



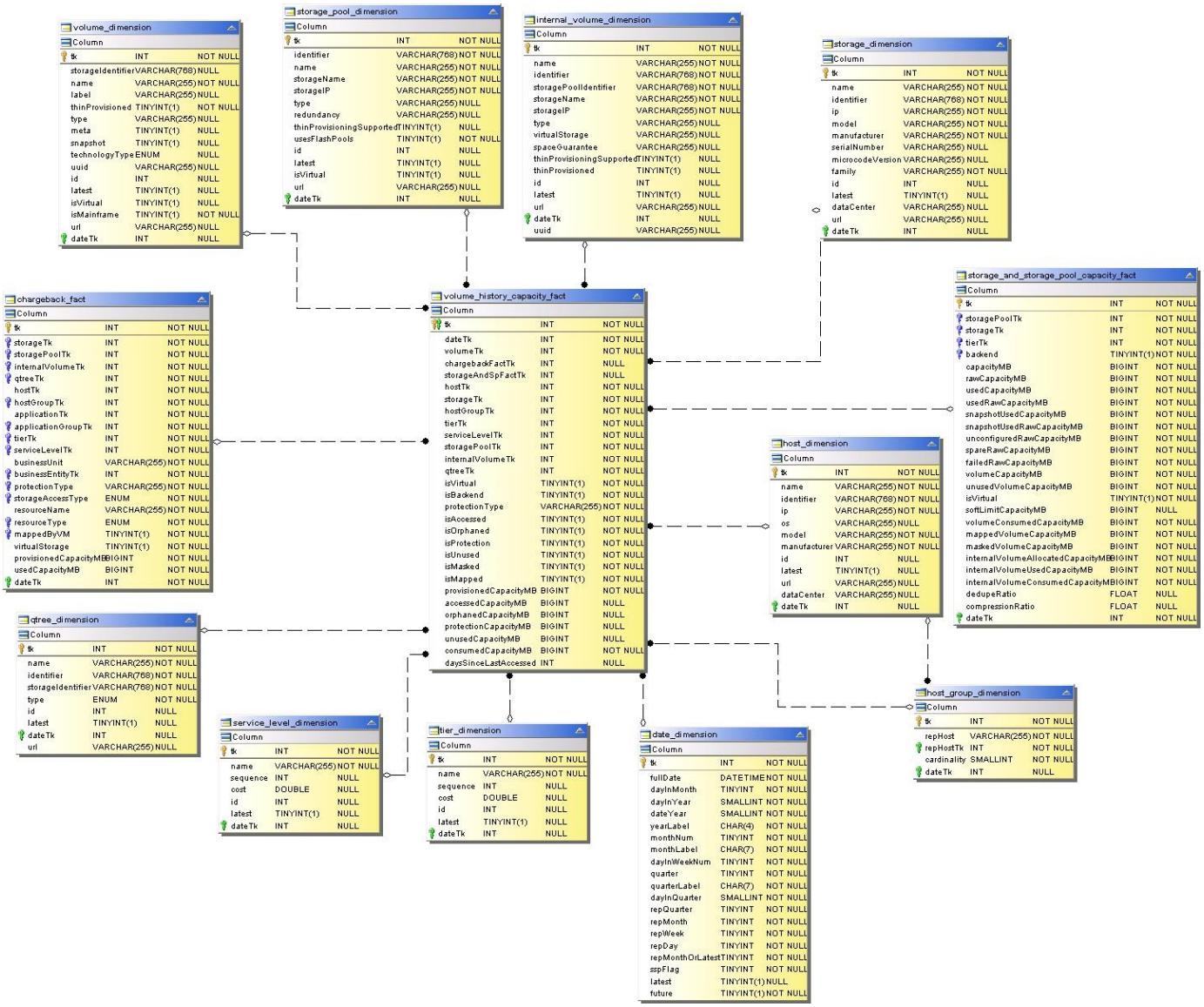
Capacità del nodo di storage



Capacità delle macchine virtuali



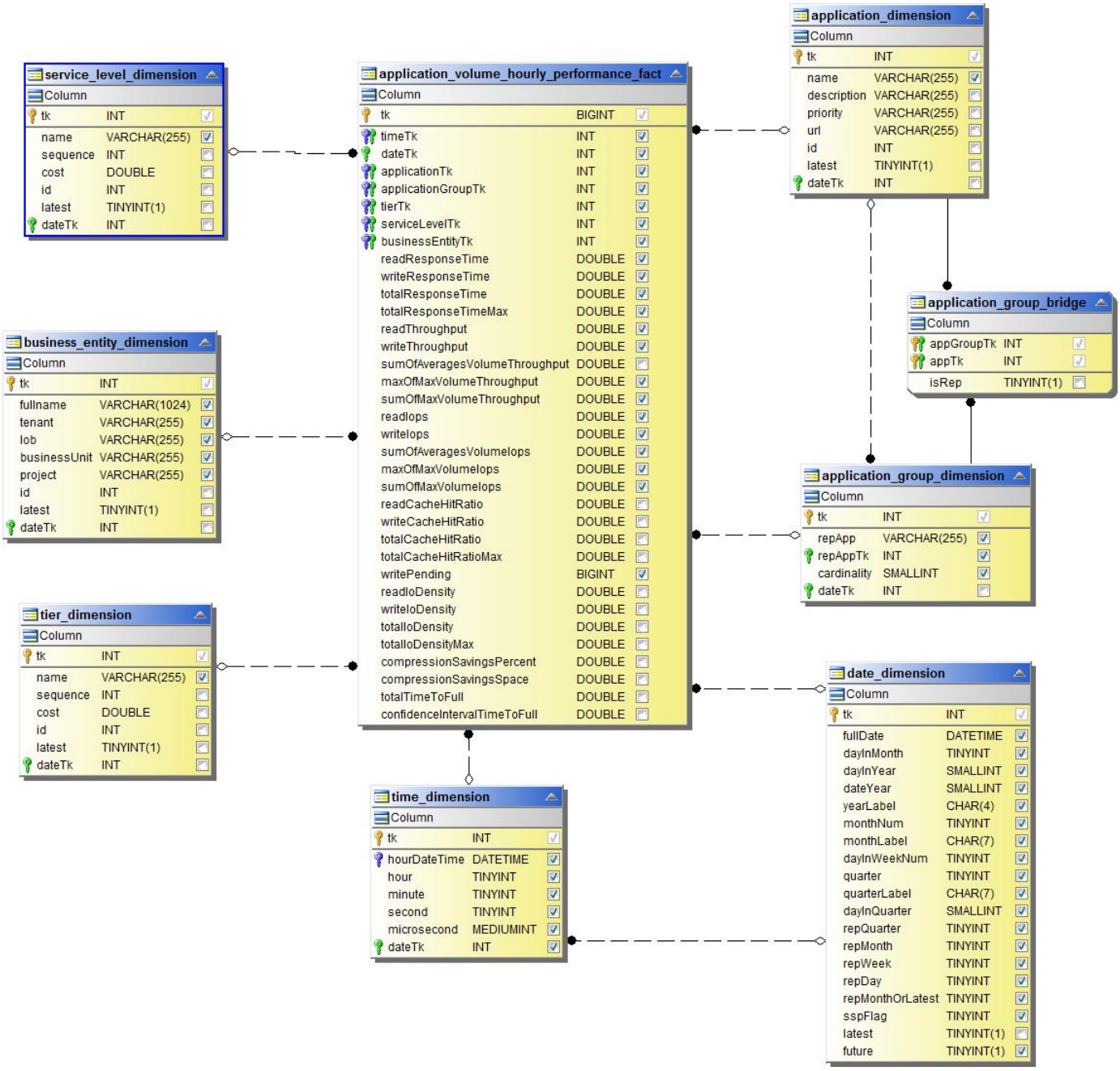
Capacità del volume



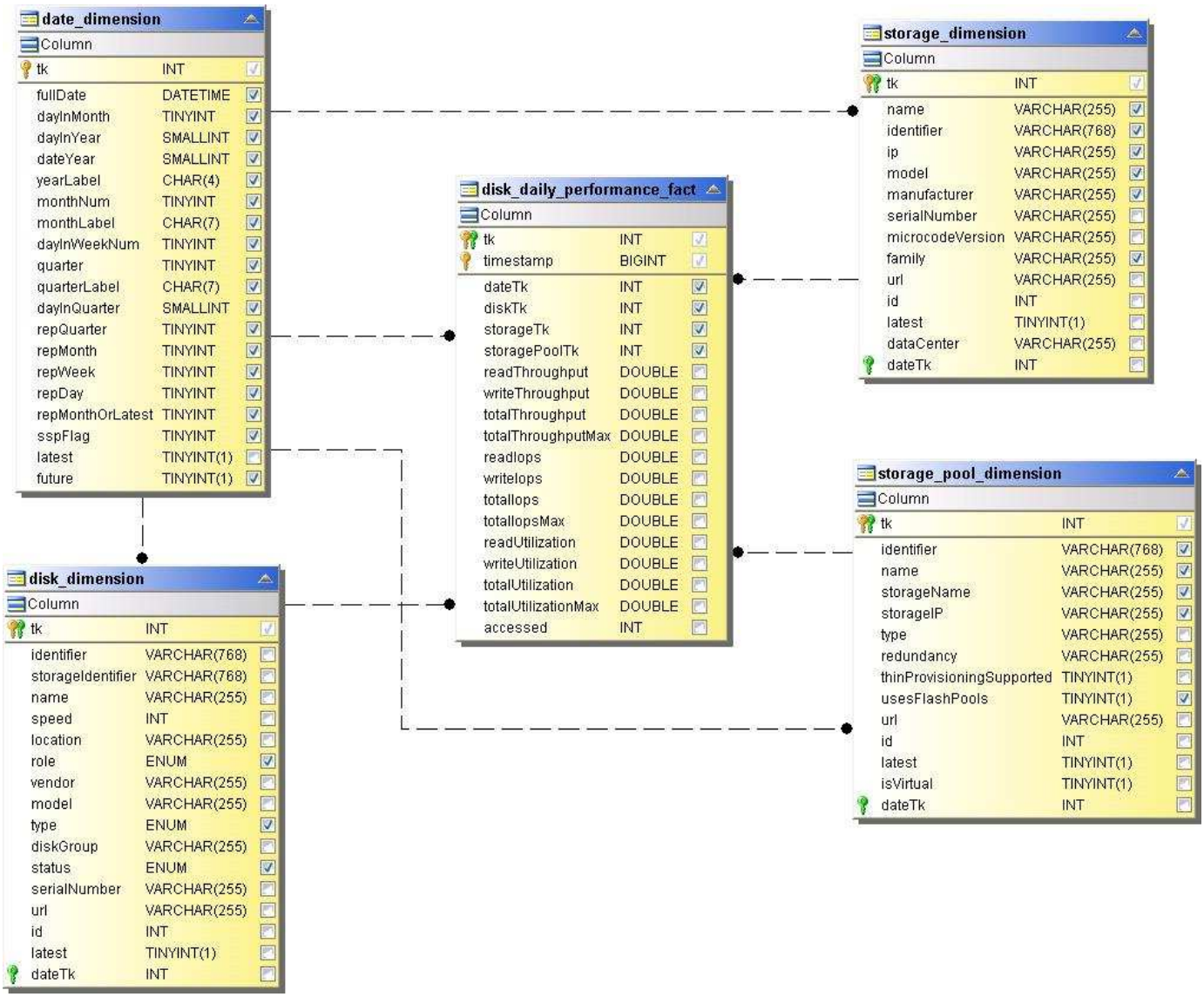
Performance Datamart

Le immagini seguenti descrivono il datamart delle performance.

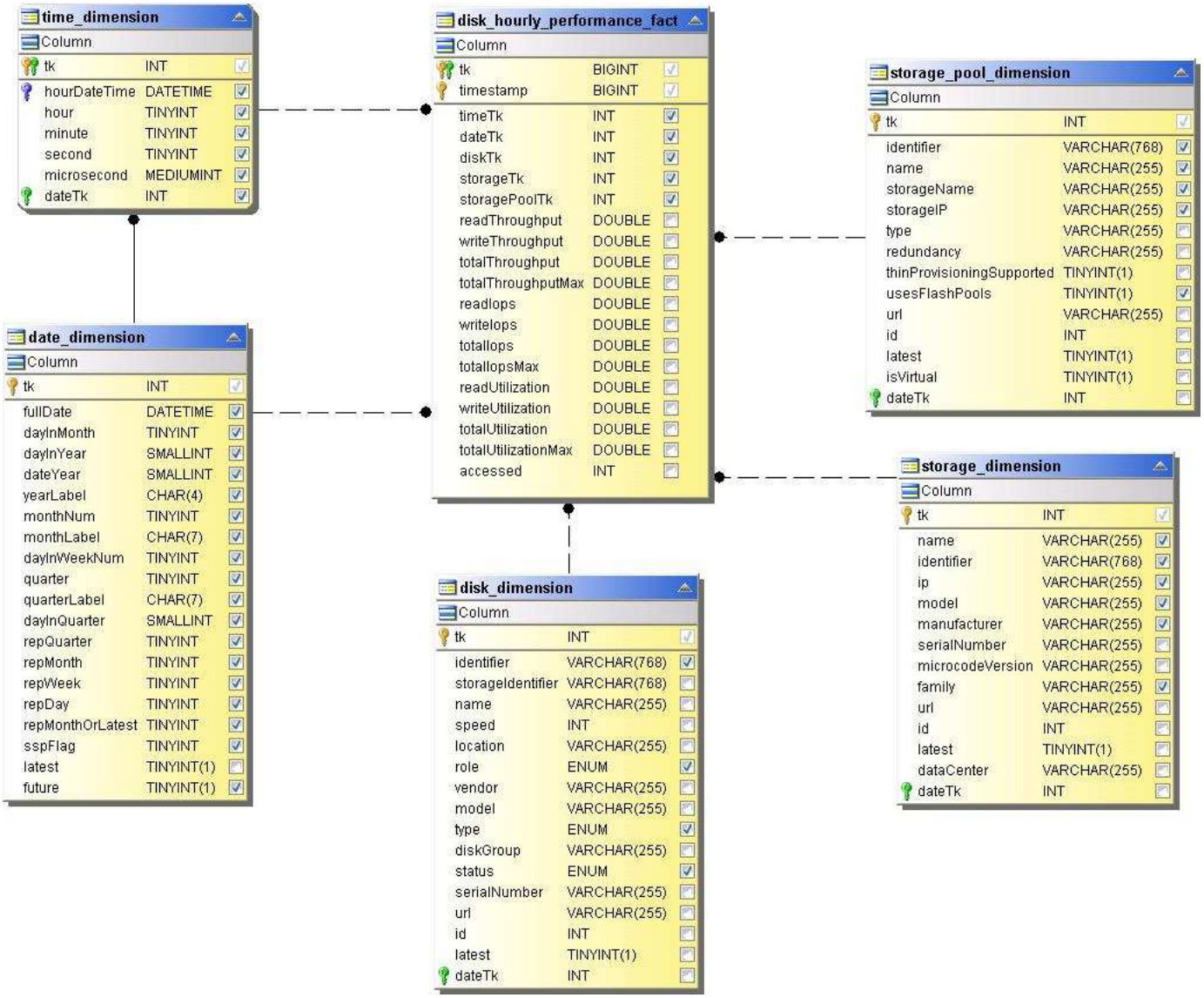
Performance orarie del volume applicativo



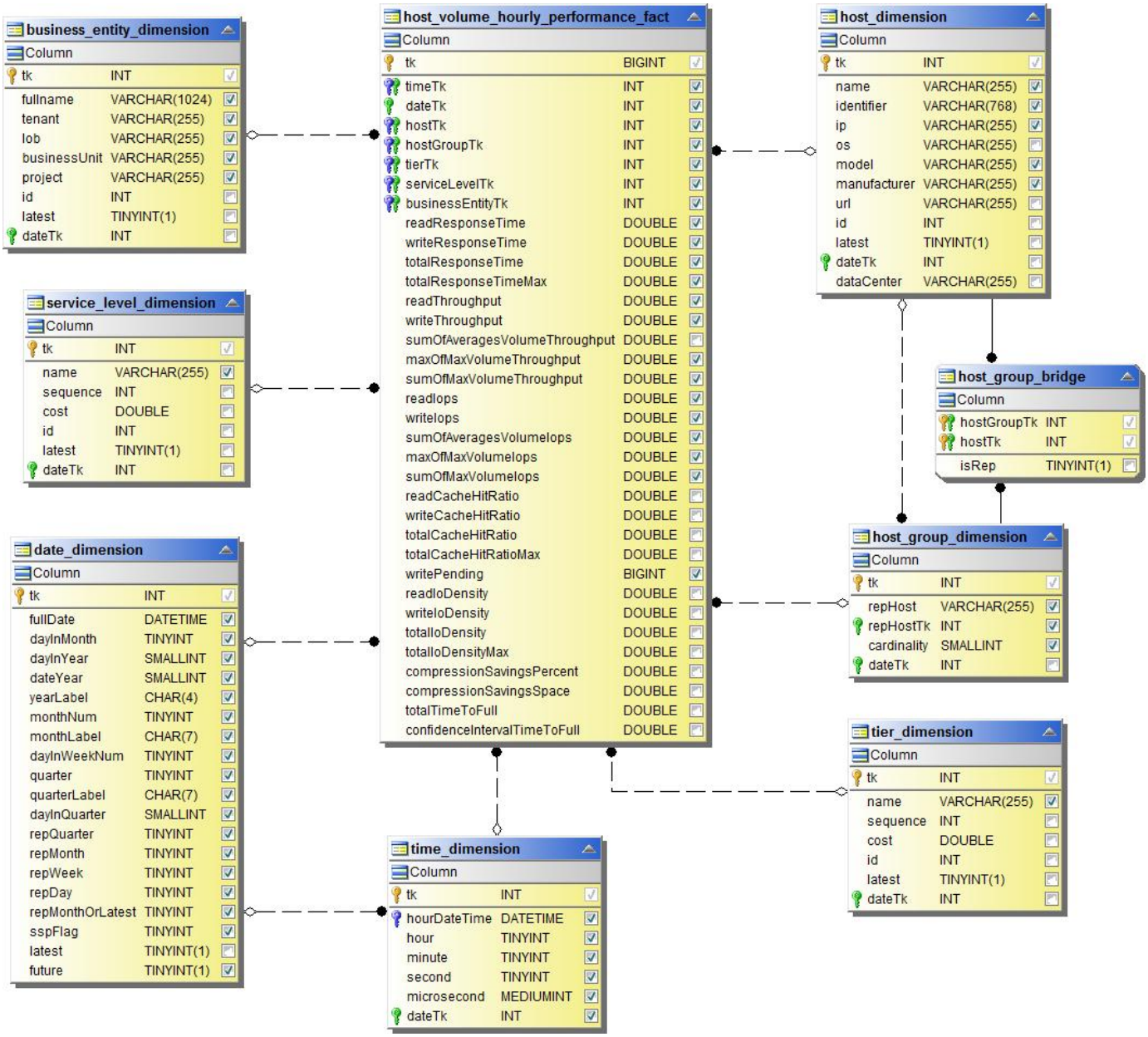
Performance giornaliere dei dischi



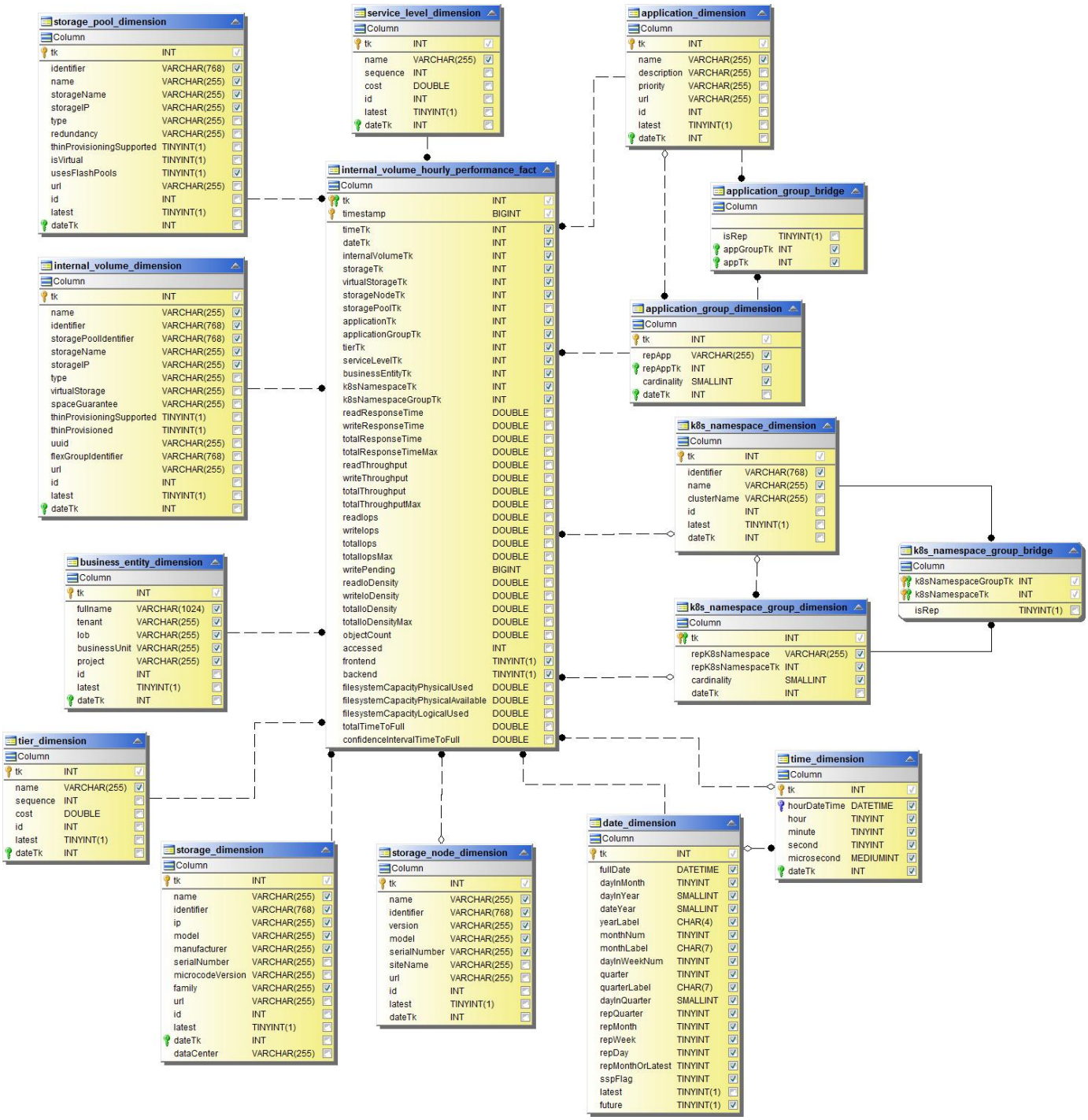
Performance orarie del disco



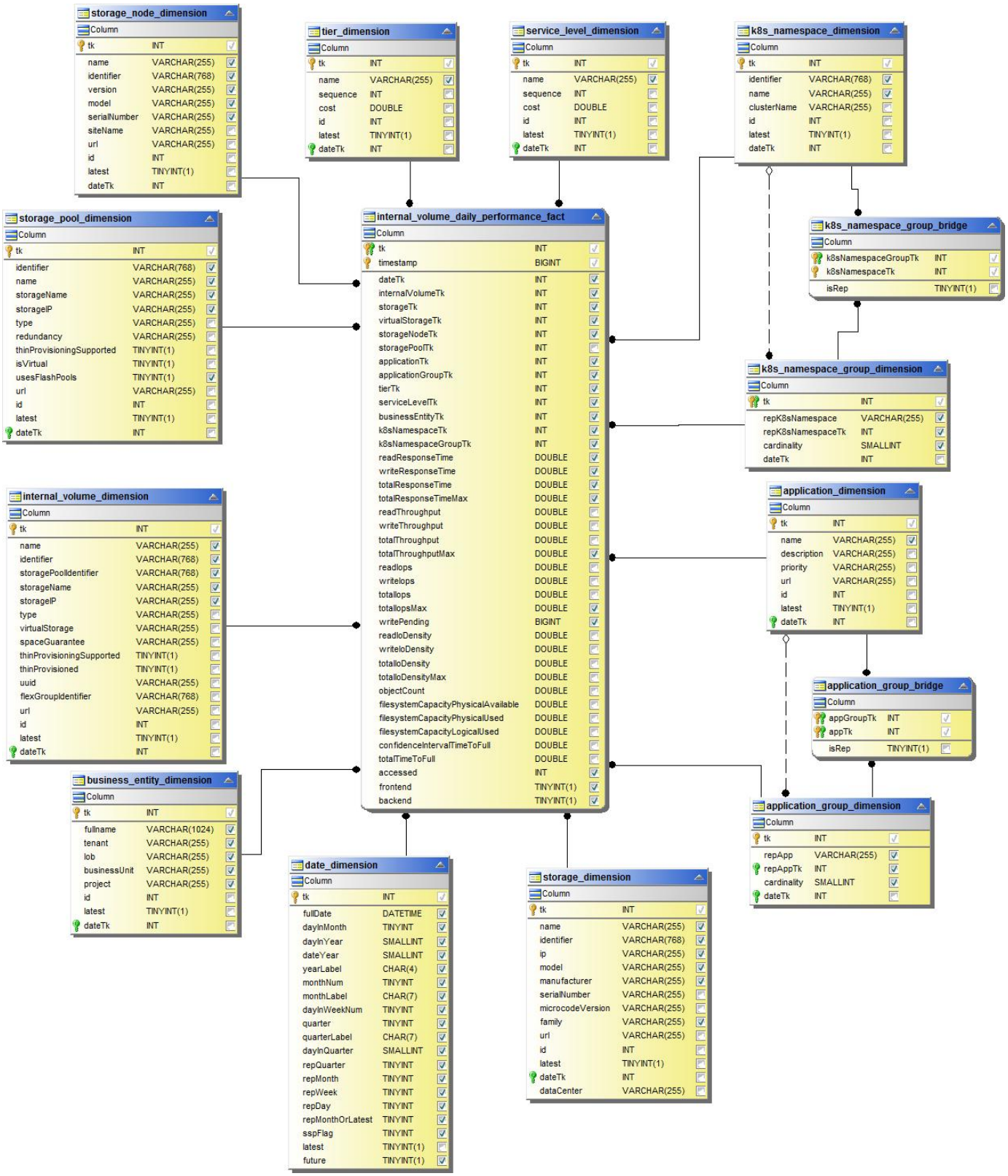
Performance orarie dell'host



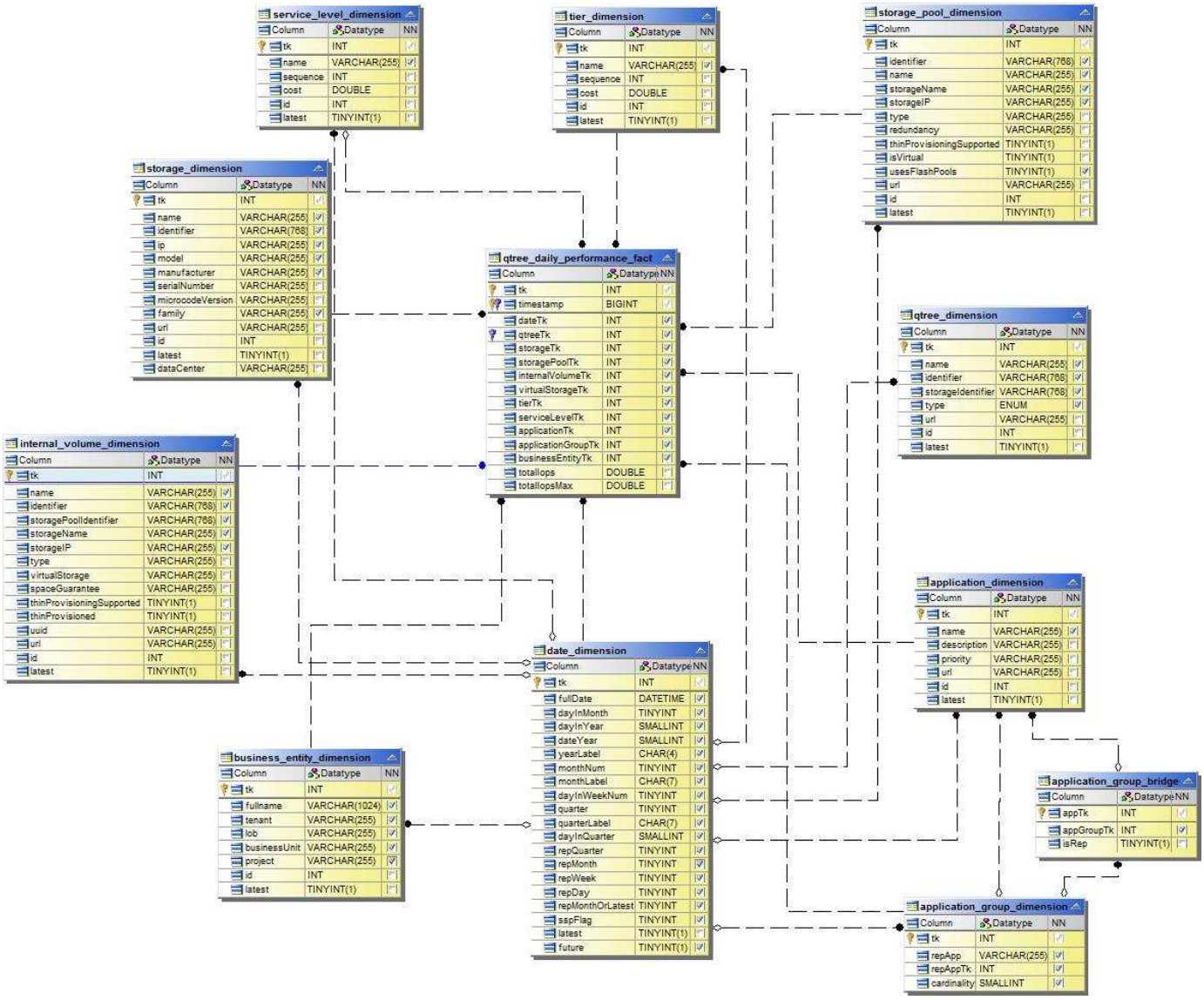
Performance orarie del volume interno



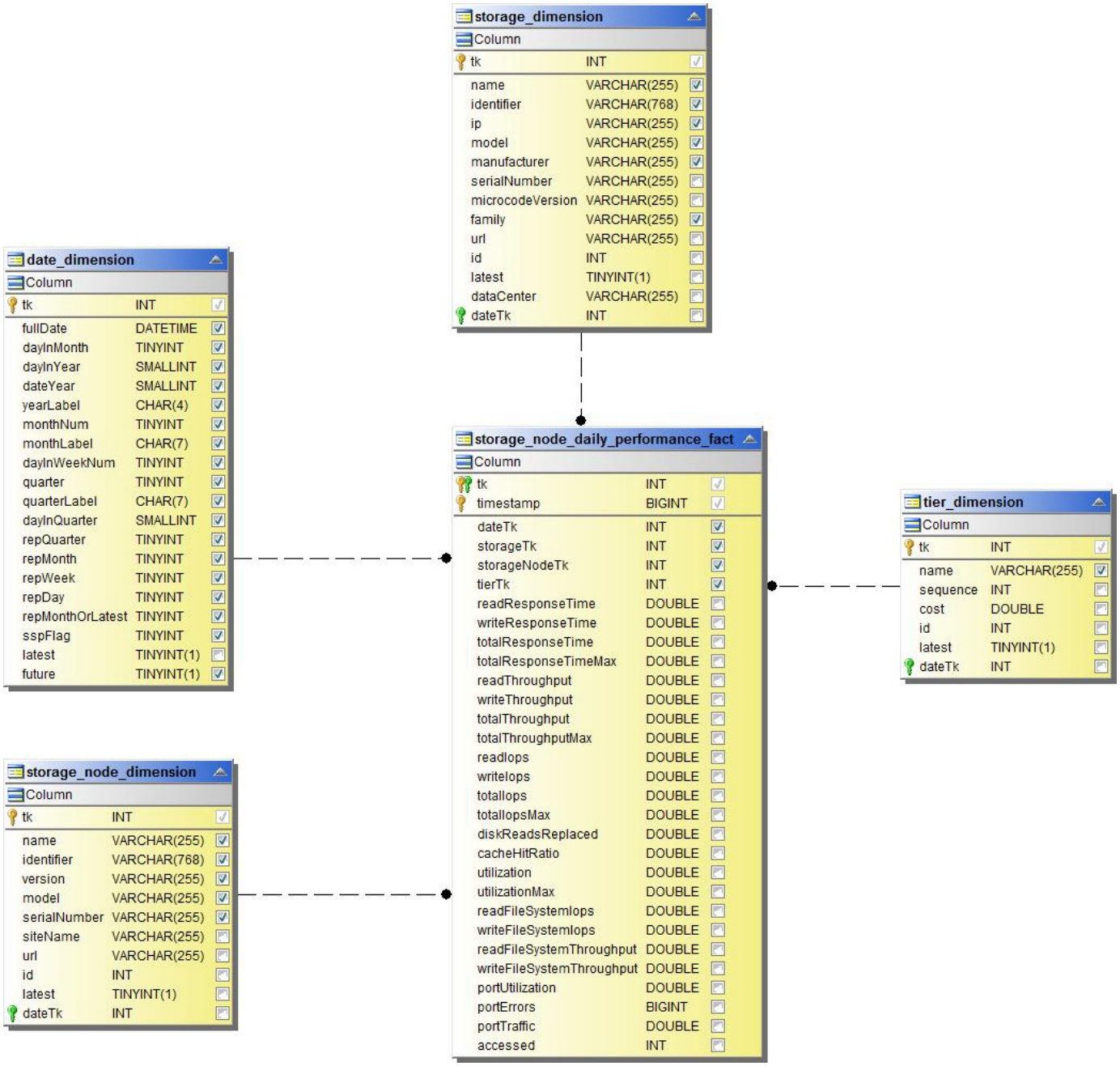
Performance giornaliera del volume interno



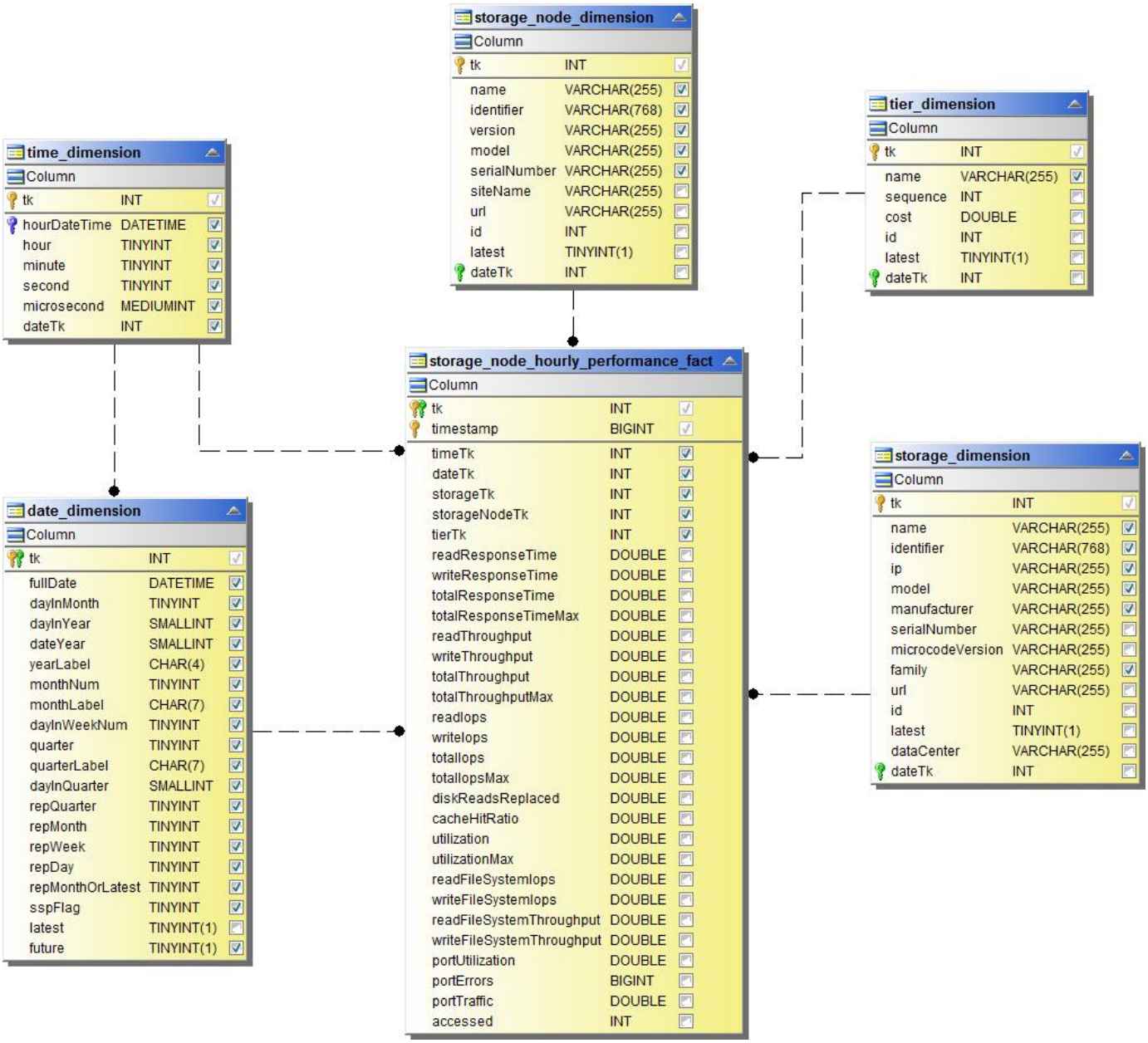
Performance giornaliere di qtree



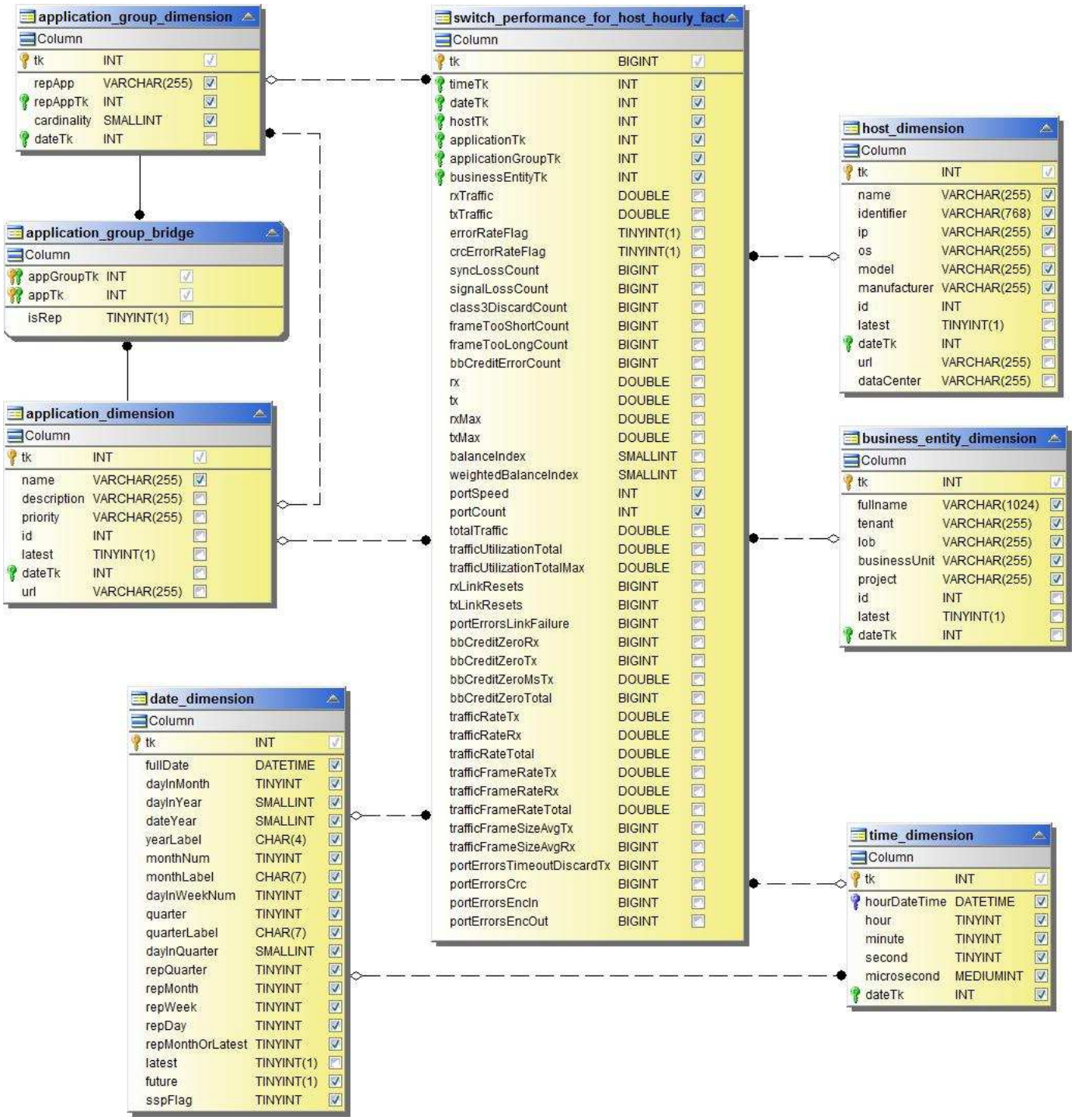
Performance giornaliere dei nodi di storage



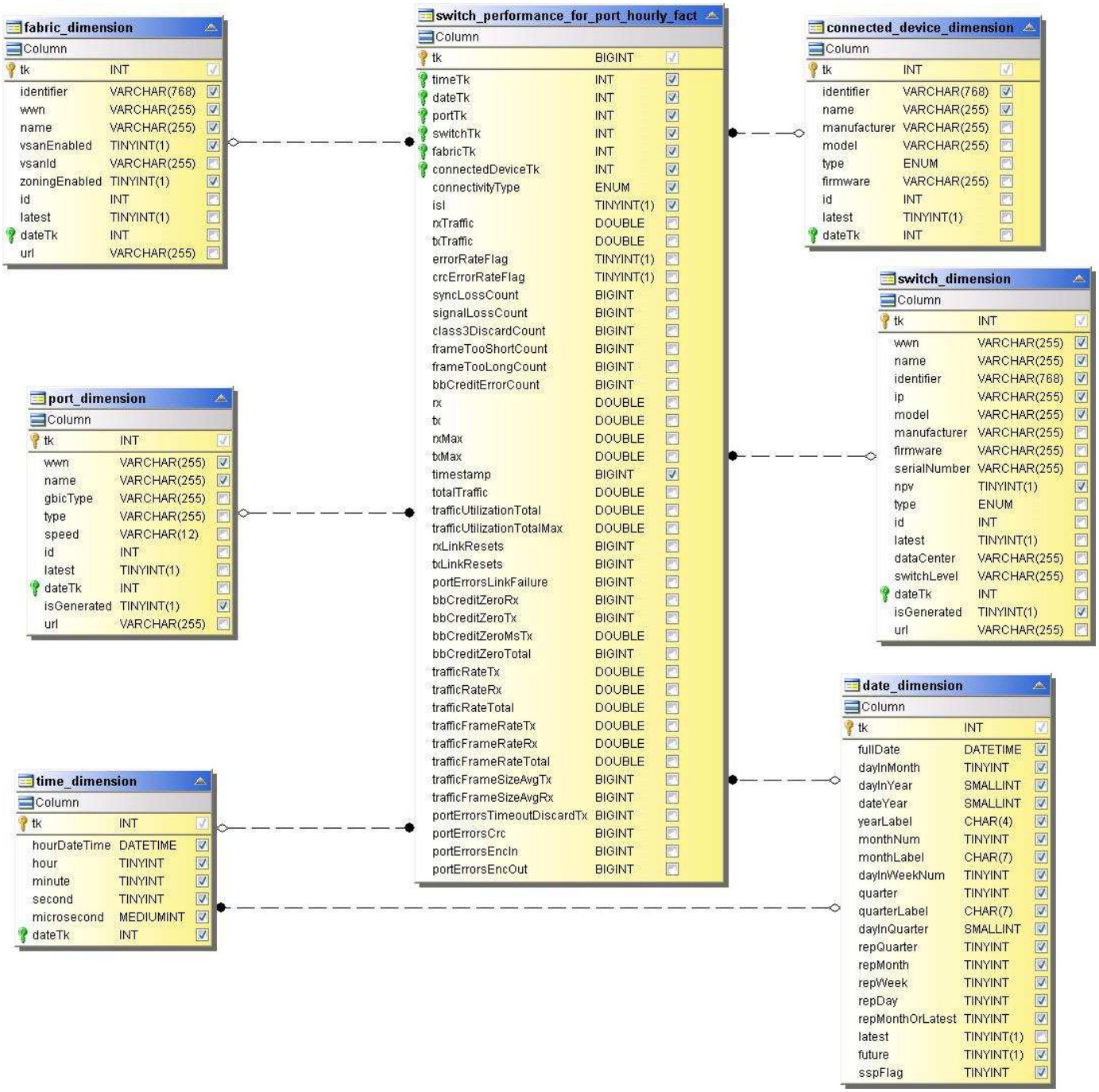
Performance orarie del nodo di storage



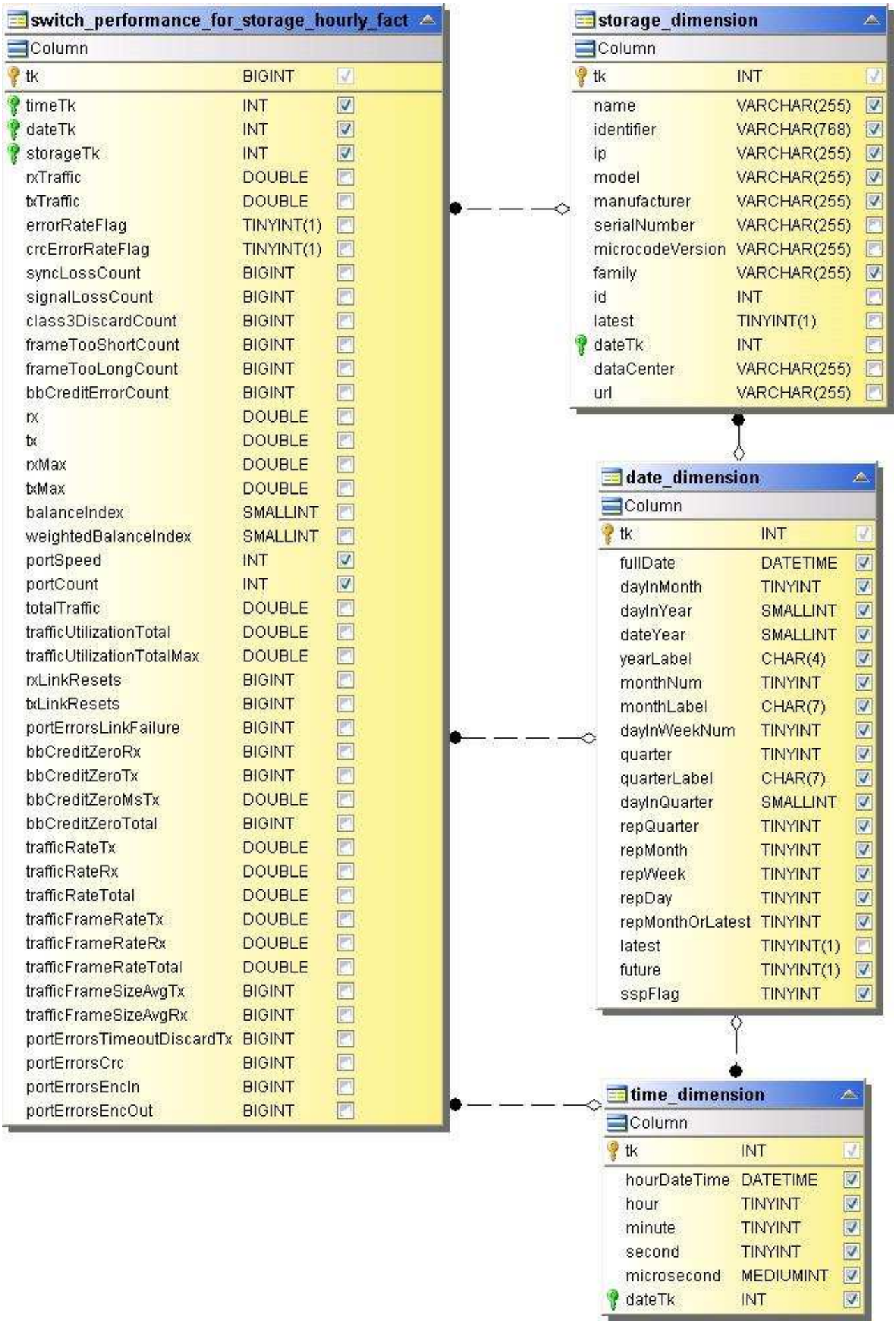
Prestazioni orarie dello switch per host



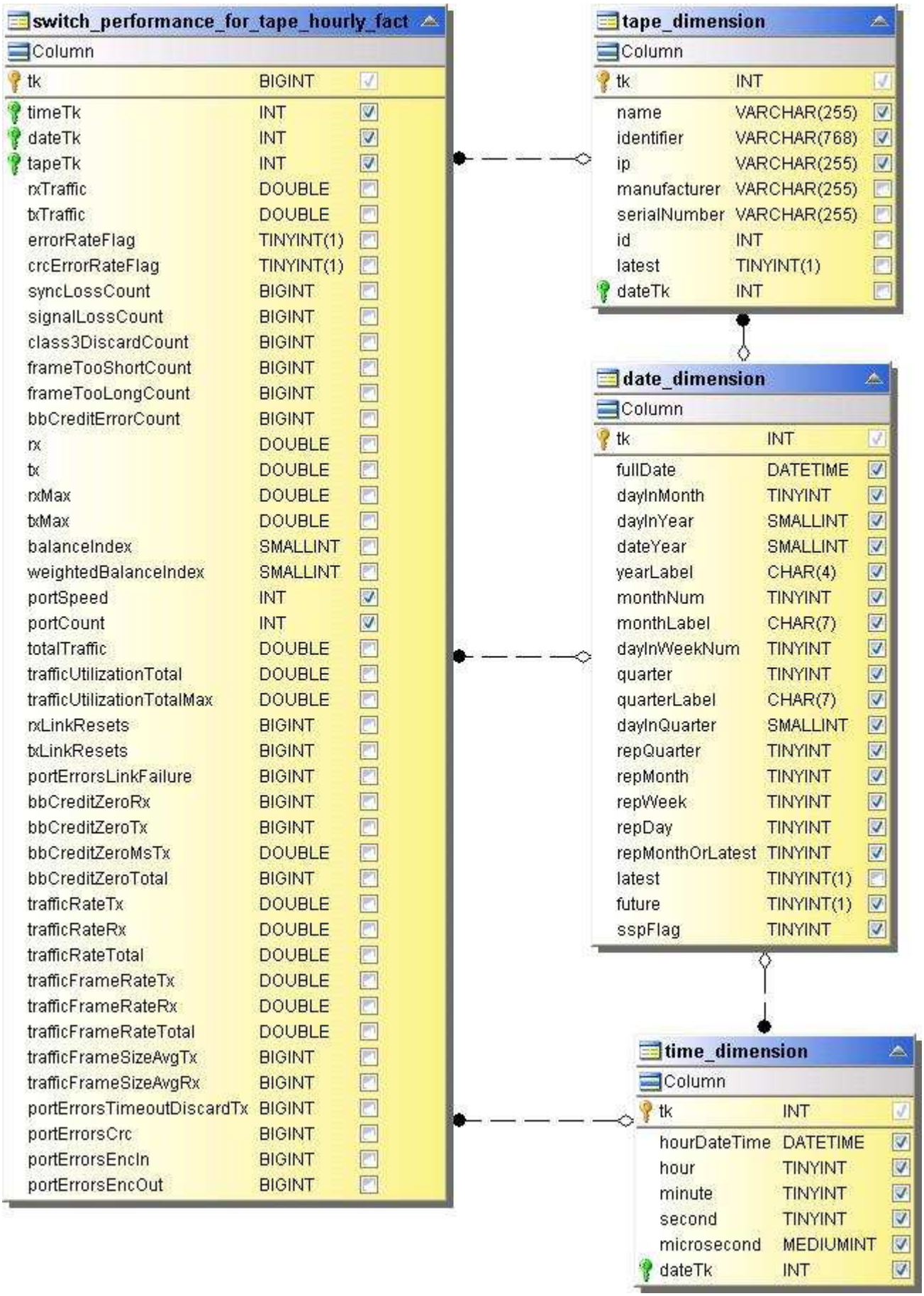
Prestazioni orarie dello switch per la porta



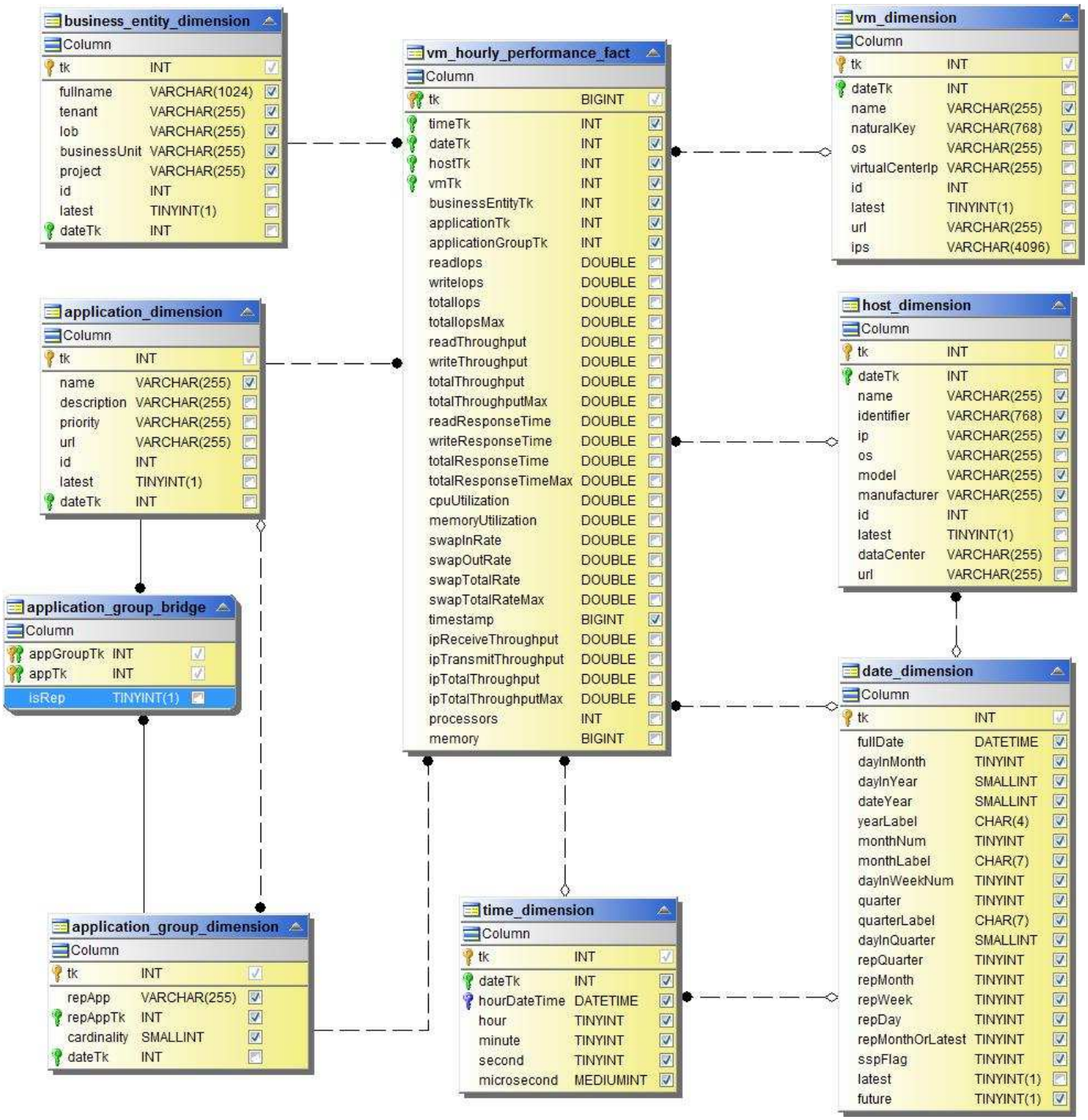
Performance orarie dello switch per lo storage


switch_performance_for_storage_hourly_fact
Column
tk BIGINT
timeTk INT
dateTk INT
storageTk INT
rxTraffic DOUBLE
txTraffic DOUBLE
errorRateFlag TINYINT(1)
crcErrorRateFlag TINYINT(1)
syncLossCount BIGINT
signalLossCount BIGINT
class3DiscardCount BIGINT
frameTooShortCount BIGINT
frameTooLongCount BIGINT
bbCreditErrorCount BIGINT
rx DOUBLE
tx DOUBLE
rxMax DOUBLE
txMax DOUBLE
balanceIndex SMALLINT
weightedBalanceIndex SMALLINT
portSpeed INT
portCount INT
totalTraffic DOUBLE
trafficUtilizationTotal DOUBLE
trafficUtilizationTotalMax DOUBLE
rxLinkResets BIGINT
txLinkResets BIGINT
portErrorsLinkFailure BIGINT
bbCreditZeroRx BIGINT
bbCreditZeroTx BIGINT
bbCreditZeroMsTx DOUBLE
bbCreditZeroTotal BIGINT
trafficRateTx DOUBLE
trafficRateRx DOUBLE
trafficRateTotal DOUBLE
trafficFrameRateTx DOUBLE
trafficFrameRateRx DOUBLE
trafficFrameRateTotal DOUBLE
trafficFrameSizeAvgTx BIGINT
trafficFrameSizeAvgRx BIGINT
portErrorsTimeoutDiscardTx BIGINT
portErrorsCrc BIGINT
portErrorsEncIn BIGINT
portErrorsEncOut BIGINT
storage_dimension
Column
tk INT
name VARCHAR(255)
identifier VARCHAR(768)
ip VARCHAR(255)
model VARCHAR(255)
manufacturer VARCHAR(255)
serialNumber VARCHAR(255)
microcodeVersion VARCHAR(255)
family VARCHAR(255)
id INT
latest TINYINT(1)
dateTk INT
dataCenter VARCHAR(255)
url VARCHAR(255)
date_dimension
Column
tk INT
fullDate DATETIME
dayInMonth TINYINT
dayInYear SMALLINT
dateYear SMALLINT
yearLabel CHAR(4)
monthNum TINYINT
monthLabel CHAR(7)
dayInWeekNum TINYINT
quarter TINYINT
quarterLabel CHAR(7)
dayInQuarter SMALLINT
repQuarter TINYINT
repMonth TINYINT
repWeek TINYINT
repDay TINYINT
repMonthOrLatest TINYINT
latest TINYINT(1)
future TINYINT(1)
sspFlag TINYINT
time_dimension
Column
tk INT
hourDateTime DATETIME
hour TINYINT
minute TINYINT
second TINYINT
microsecond MEDIUMINT
dateTk INT

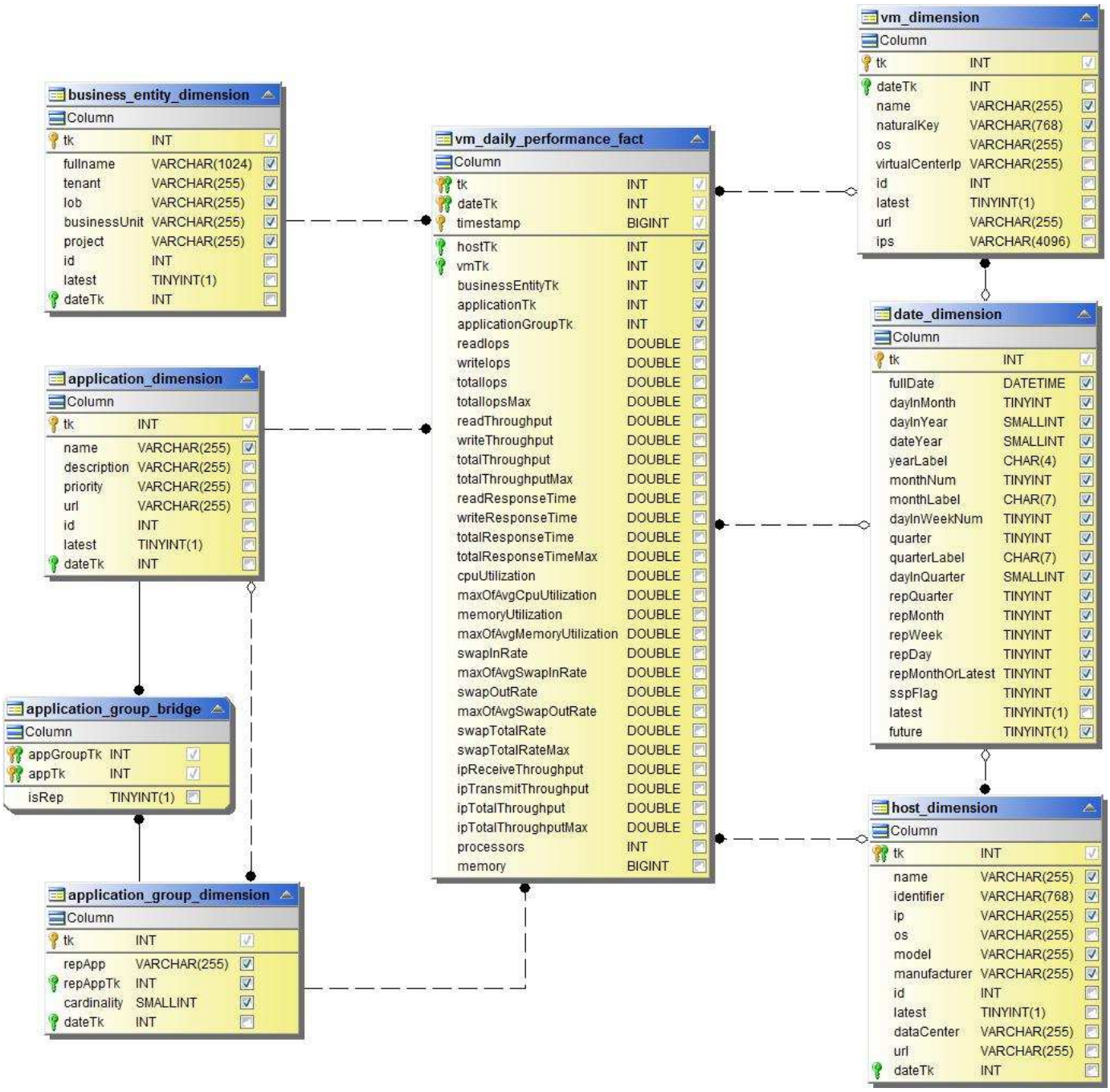
Prestazioni orarie dello switch per il nastro



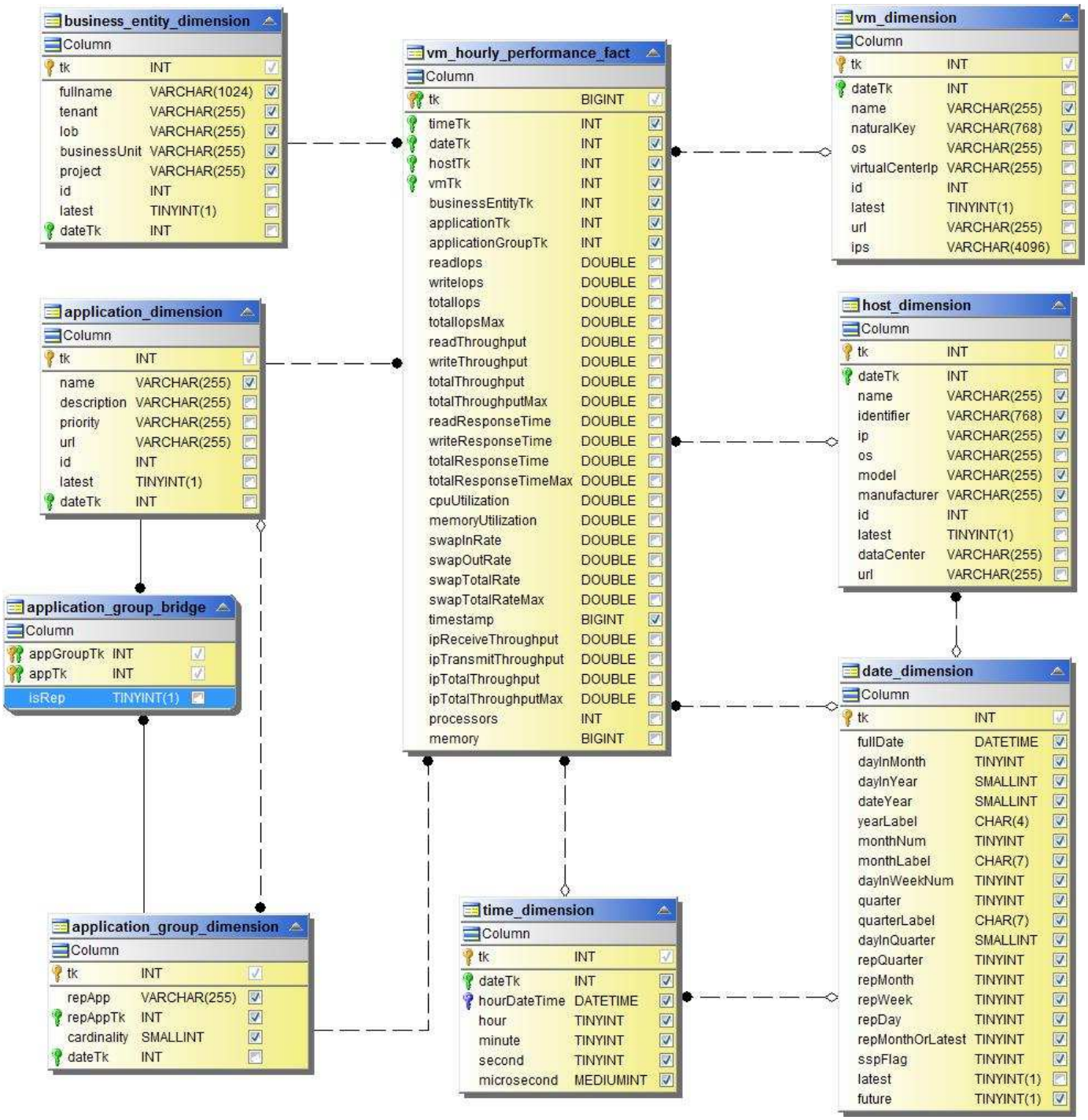
Performance delle macchine virtuali



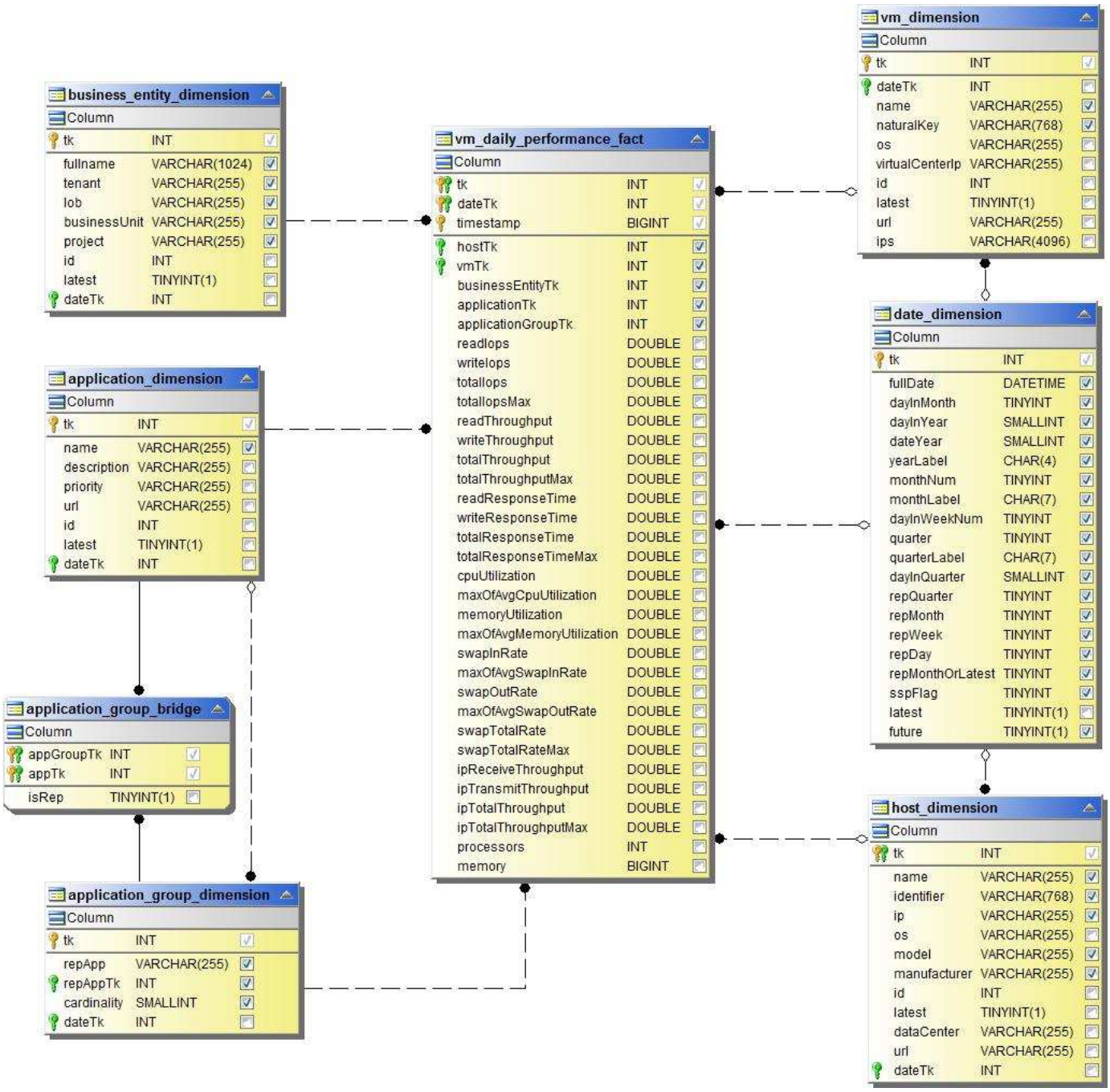
Performance giornaliere delle macchine virtuali per host



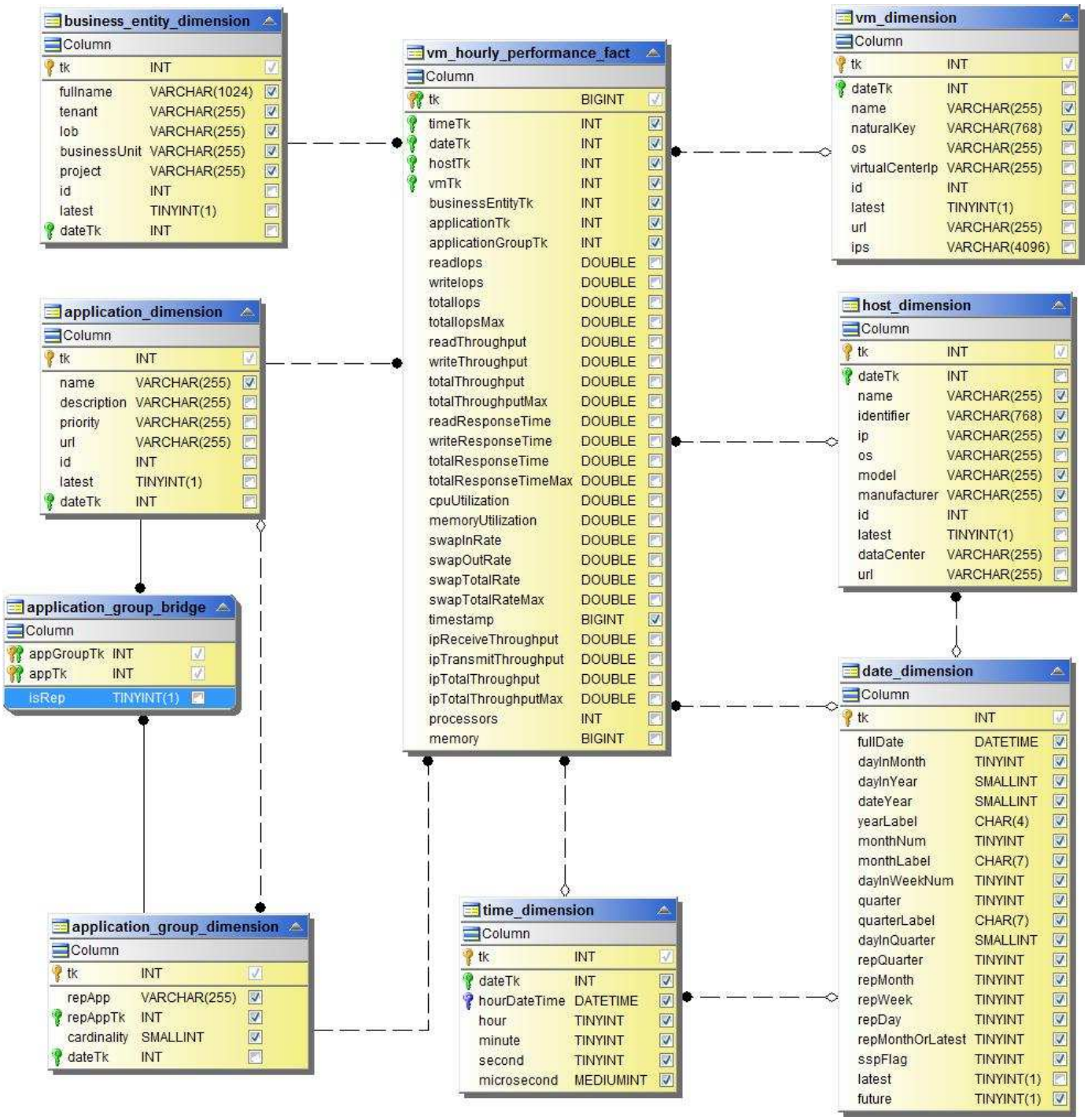
Performance orarie delle macchine virtuali per host



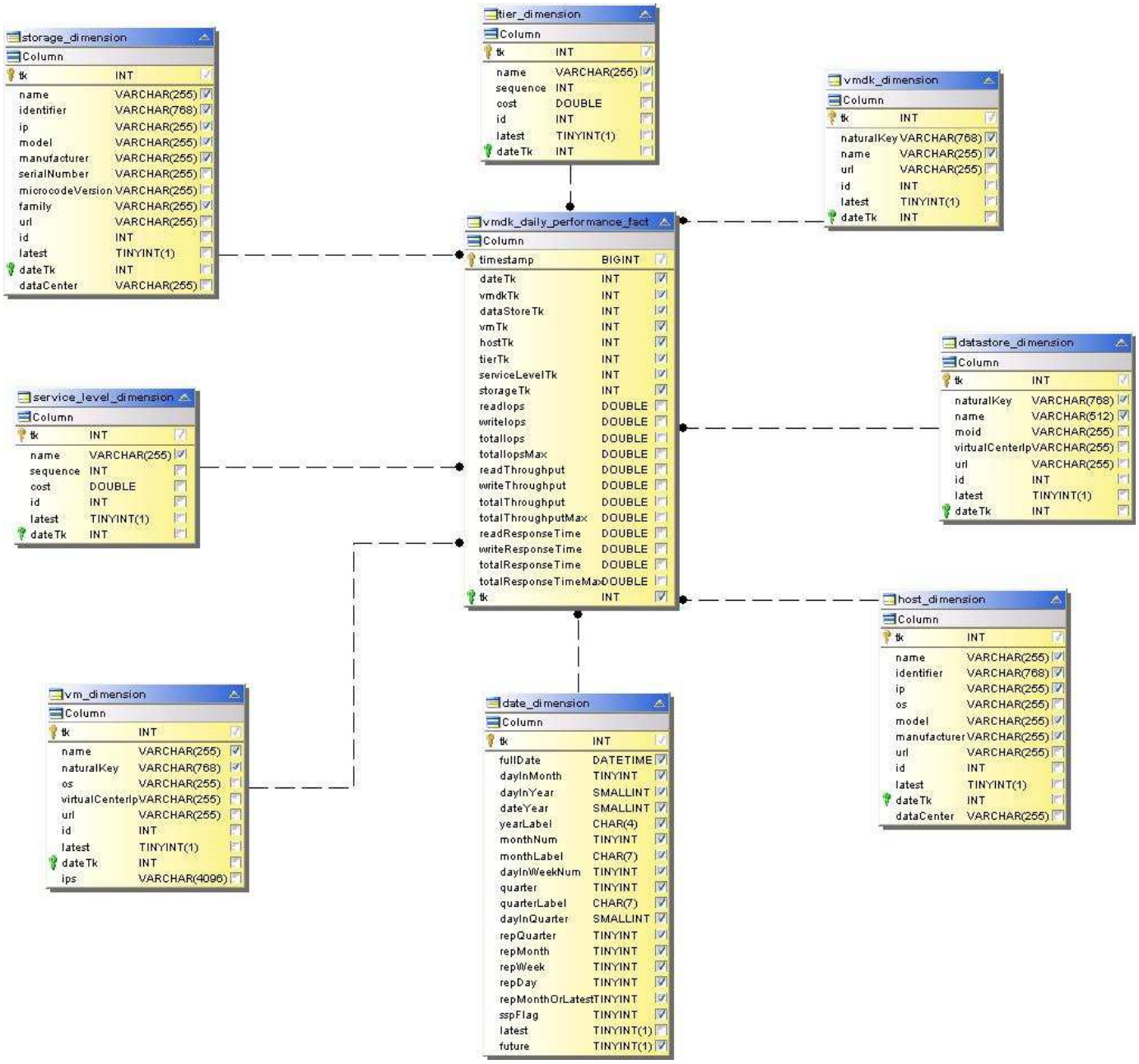
Performance giornaliere delle macchine virtuali per host



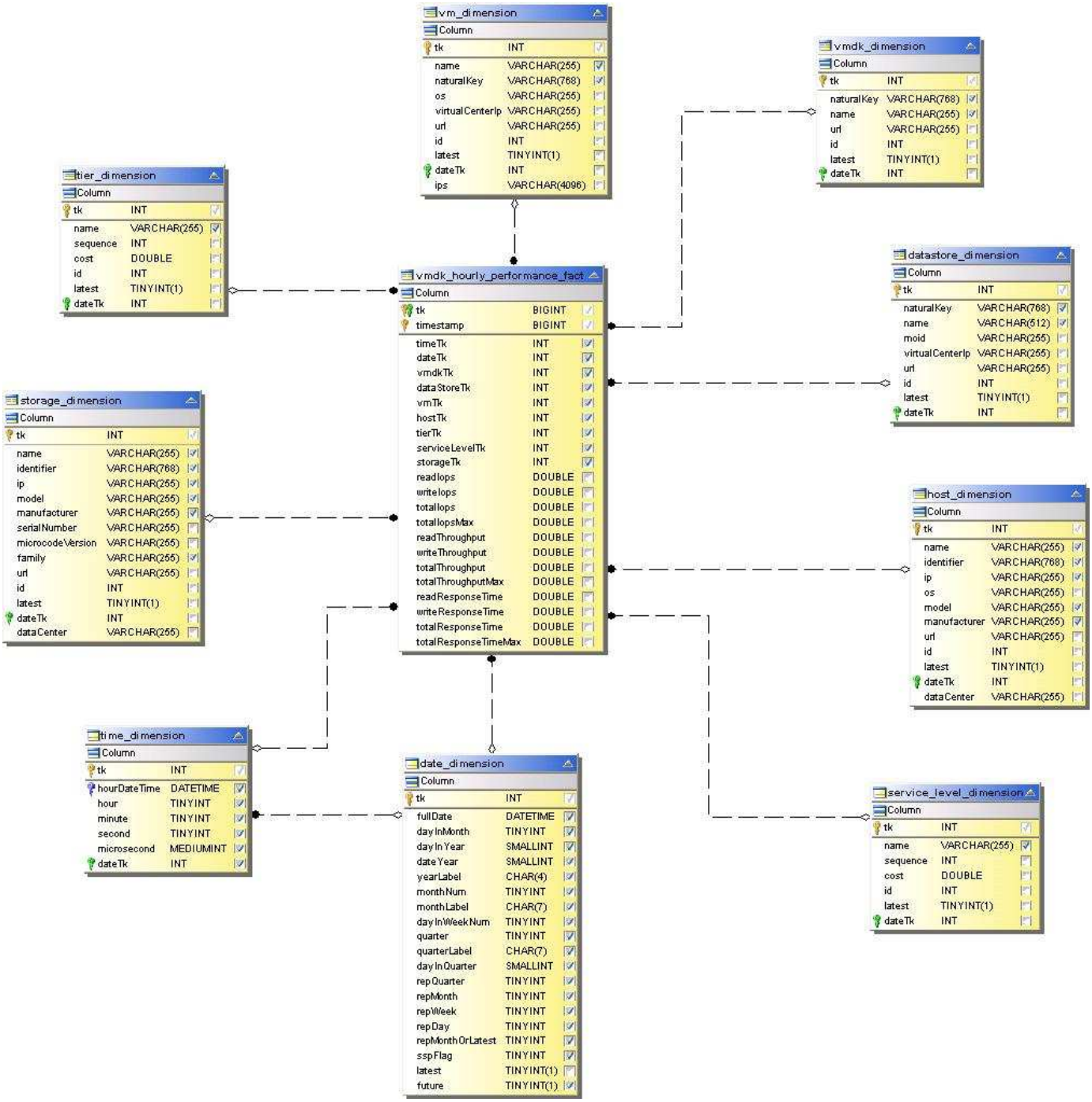
Performance orarie delle macchine virtuali per host



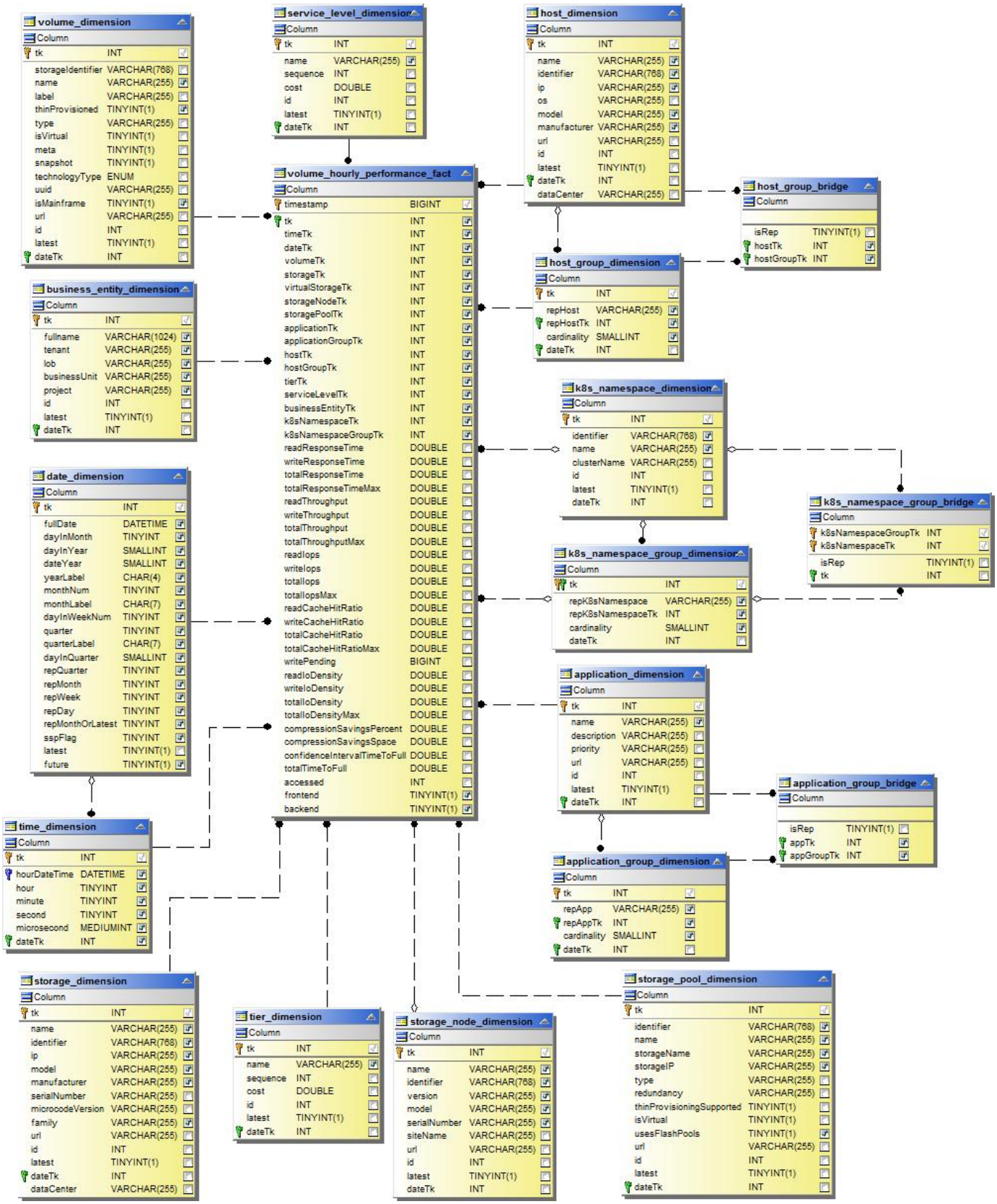
Performance giornaliera di VMDK



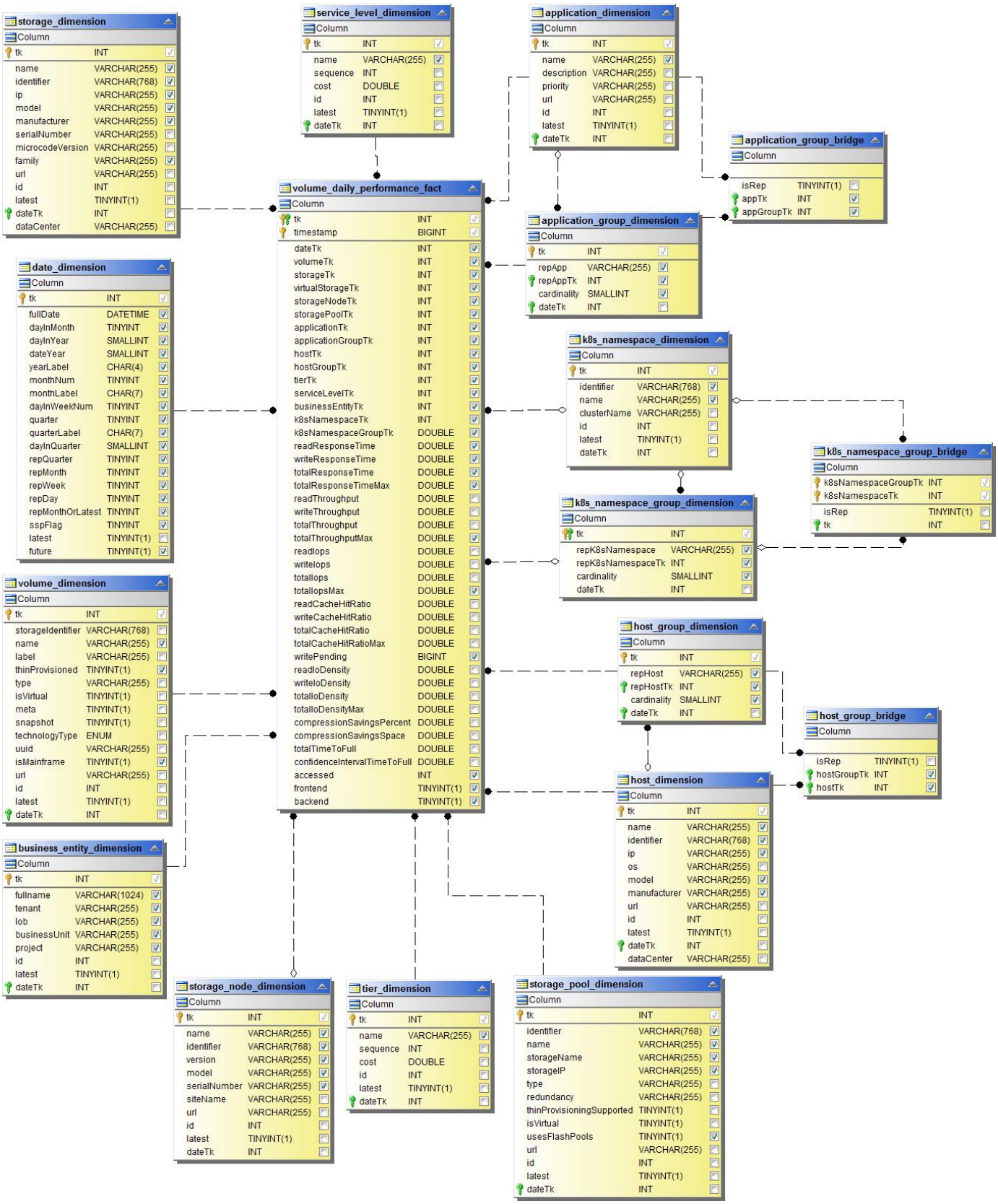
Performance orarie di VMDK



Performance orarie del volume



Volume Daily Performance



Schemi Cloud Insights per il reporting

Le tabelle e i diagrammi degli schemi sono forniti qui come riferimento per i report Cloud Insights.

"Tabelle dello schema" In formato .PDF. Fare clic sul collegamento per aprire o fare clic con il pulsante destro del mouse e scegliere *Save As…* per scaricare.

"Diagrammi dello schema"

La funzione di reporting è disponibile in Cloud Insights "Premium Edition".

Sicurezza del carico di lavoro

Informazioni su Storage workload Security

La sicurezza del carico di lavoro dello storage Cloud Insights (in precedenza Cloud Secure) aiuta a proteggere i tuoi dati con informazioni pratiche sulle minacce interne. Offre visibilità e controllo centralizzati di tutti gli accessi ai dati aziendali negli ambienti di cloud ibrido per garantire il rispetto degli obiettivi di sicurezza e conformità.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Visibilità

Ottieni visibilità e controllo centralizzati dell'accesso degli utenti ai tuoi dati aziendali critici memorizzati on-premise o nel cloud.

Sostituire strumenti e processi manuali che non forniscono una visibilità puntuale e precisa dell'accesso e del controllo dei dati. Workload Security funziona in modo esclusivo sia sul cloud che sui sistemi storage on-premise per fornire avvisi in tempo reale di comportamenti dannosi degli utenti.

Protezione

Proteggi i dati dell'organizzazione da un utilizzo improprio da parte di utenti malintenzionati o compromessi attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie.

Avvisa l'utente in caso di accesso anomalo ai dati attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie del comportamento dell'utente.

Conformità

Garantire la conformità aziendale verificando l'accesso dei dati degli utenti ai dati aziendali critici memorizzati on-premise o nel cloud.

Per iniziare

Introduzione alla sicurezza del carico di lavoro

È necessario completare alcune attività di configurazione prima di poter iniziare a utilizzare workload Security per monitorare l'attività dell'utente.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Il sistema workload Security utilizza un agente per raccogliere i dati di accesso dai sistemi storage e le informazioni utente dai server Directory Services.

Prima di iniziare la raccolta dei dati, è necessario configurare quanto segue:

Attività	Informazioni correlate

Configurare un agente	"Requisiti dell'agente" "Aggiungi agente" "**Video**: Implementazione dell'agente"
Configurare un connettore di directory utente	"Aggiungi connettore directory utente" "**Video**: Connessione Active Directory"
Configurare i data colleziones	Fare clic su **sicurezza del carico di lavoro > Collector** Fare clic sul data collector che si desidera configurare. Consultare la sezione Data Collector Vendor Reference della documentazione. "**Video**: Connessione SVM ONTAP"
Creare account utente	"Gestire gli account utente"
Risoluzione dei problemi	"**Video**: Risoluzione dei problemi"

Workload Security può integrarsi anche con altri strumenti. Ad esempio, "consultare questa guida" Sull'integrazione con Splunk.

Requisiti dell'agente per la sicurezza del carico di lavoro

È necessario "Installare un Agent" al fine di acquisire informazioni dai tuoi data colleziones. Prima di installare l'Agent, assicurarsi che l'ambiente soddisfi i requisiti di sistema operativo, CPU, memoria e spazio su disco.

> La protezione del carico di lavoro dello storage non è disponibile nell'edizione federale di Cloud Insights.

Componente	Requisiti Linux
Sistema operativo	Un computer che esegue una versione con licenza di uno dei seguenti componenti: Red Hat Enterprise Linux 7.x, 8.x 64 bit, SELinux CentOS 7.x a 64 bit, SELinux CentOS 8 Stream, SELinux Ubuntu 20 fino a 22 64 bit Rocky 8.x 64 bit, Rocky 9.x 64 bit, SELinux SUSE Linux Enterprise Server 15 SP3, SUSE Linux Enterprise Server 15 SP4, SELinux su SUSE 15 SP3 Questo computer non deve eseguire alcun altro software a livello di applicazione. Si consiglia di utilizzare un server dedicato.

Componente	Requisiti Linux
Comandi	per l'installazione è necessario decomprimere. Inoltre, il comando 'sudo su –' è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
CPU	4 core CPU
Memoria	16 GB DI RAM
Spazio su disco disponibile	Lo spazio su disco deve essere allocato in questo modo: /Opt/netapp 35 GB (minimo) Nota: Si consiglia di allocare un po' di spazio su disco in più per consentire la creazione del filesystem. Assicurarsi che ci siano almeno 35 GB di spazio libero nel filesystem. Se /opt è una cartella montata da un dispositivo di archiviazione NAS, assicurarsi che gli utenti locali abbiano accesso a questa cartella. L'installazione dell'agente o del Data Collector potrebbe non riuscire se gli utenti locali non dispongono dell'autorizzazione per questa cartella. vedere "risoluzione dei problemi" per ulteriori dettagli.
Rete	Connessione Ethernet da 100 Mbps a 1 Gbps, indirizzo IP statico, connettività IP a tutti i dispositivi e porta richiesta per l'istanza di workload Security (80 o 443).

Nota: L'agente workload Security può essere installato sullo stesso computer di un'unità di acquisizione e/o agente Cloud Insights. Tuttavia, è consigliabile installarli in computer separati. Nel caso in cui siano installati sullo stesso computer, allocare lo spazio su disco come mostrato di seguito:

Spazio su disco disponibile	50-55 GB per Linux, lo spazio su disco deve essere allocato in questo modo: /Opt/netapp 25-30 GB /var/log/netapp 25 GB

Consigli aggiuntivi

- Si consiglia vivamente di sincronizzare l'ora sul sistema ONTAP e sul computer dell'agente utilizzando **protocollo NTP (Network Time Protocol)** o **SNTP (Simple Network Time Protocol)**.

Regole di accesso alla rete cloud

Per ambienti di workload Security * basati su * Stati Uniti:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01.cloudinsights.netapp.com <site_name>.c01.cloudinsights.netapp.com <site_name>.c02.cloudinsights.netapp.com	Accesso a Cloud Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza dei workload **basati sull'Europa**:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01-eu-1.cloudinsights.netapp.com <site_name>.c01-eu-1.cloudinsights.netapp.com <site_name>.c02-eu-1.cloudinsights.netapp.com	Accesso a Cloud Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Per ambienti di sicurezza dei workload * basati su APAC*:

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	443	Agente di sicurezza del carico di lavoro	<site_name>.cs01-ap-1.cloudinsights.netapp.com <site_name>.c01-ap-1.cloudinsights.netapp.com <site_name>.c02-ap-1.cloudinsights.netapp.com	Accesso a Cloud Insights
TCP	443	Agente di sicurezza del carico di lavoro	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	Accesso ai servizi di autenticazione

Regole in-network

Protocollo	Porta	Origine	Destinazione	Descrizione
TCP	389 (LDAP) 636 (LDAPS / start-tls)	Agente di sicurezza del carico di lavoro	URL del server LDAP	Connettersi a LDAP
TCP	443	Agente di sicurezza del carico di lavoro	Cluster o SVM Management IP Address (a seconda della configurazione del collettore SVM)	Comunicazione API con ONTAP
TCP	35000 - 55000	Indirizzi IP LIF dati SVM	Agente di sicurezza del carico di lavoro	Comunicazione da ONTAP all'agente di sicurezza del carico di lavoro per gli eventi Fpolicy. Affinché ONTAP possa inviarvi eventi, compresi eventuali firewall presenti nell'agente di protezione del carico di lavoro stesso (se presente), è necessario aprire queste porte verso l'agente di protezione del carico di lavoro.
TCP	7	Agente di sicurezza del carico di lavoro	Indirizzi IP LIF dati SVM	Eco dai Agent ai LIF dati SVM

Protocollo	Porta	Origine	Destinazione	Descrizione
SSH	22	Agente di sicurezza del carico di lavoro	Gestione del cluster	Necessario per il blocco degli utenti CIFS/SMB.

Dimensionamento del sistema

Vedere "Controllo della velocità degli eventi" documentazione per informazioni sul dimensionamento.

Installazione di workload Security Agent

Workload Security (in precedenza Cloud Secure) raccoglie i dati delle attività degli utenti utilizzando uno o più agenti. Gli agenti si connettono ai dispositivi del tuo ambiente e raccolgono i dati inviati al livello SaaS per la sicurezza del carico di lavoro per l'analisi. Vedere "Requisiti dell'agente" Per configurare una macchina virtuale dell'agente.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

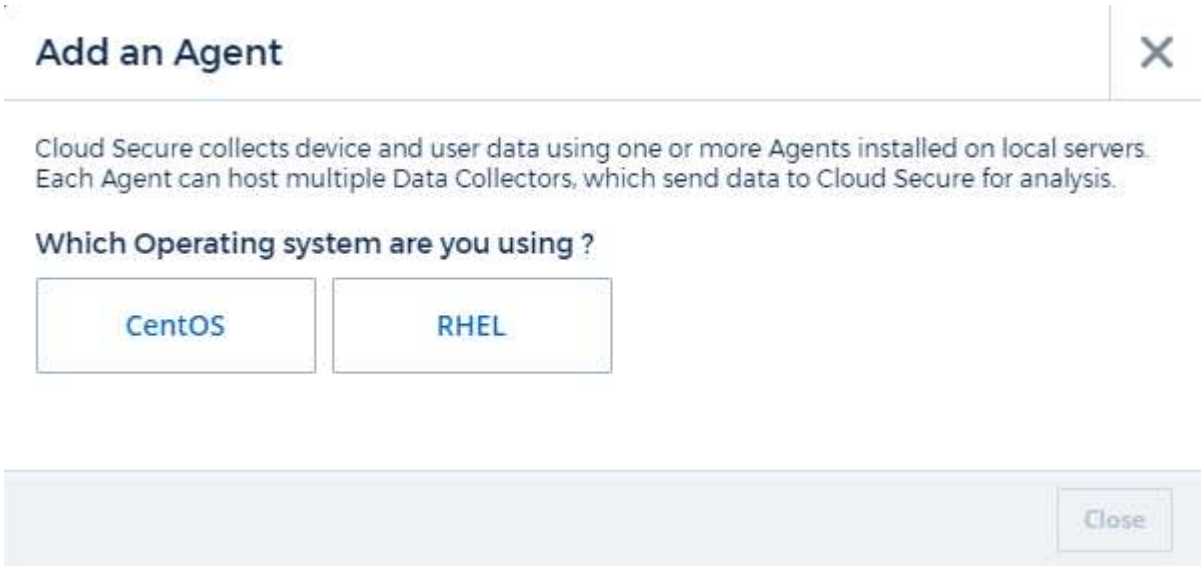
Prima di iniziare

- Il privilegio sudo è necessario per l'installazione, l'esecuzione di script e la disinstallazione.
- Durante l'installazione dell'agente, sul computer vengono creati un utente locale *cssys* e un gruppo locale *cssys*. Se le impostazioni di autorizzazione non consentono la creazione di un utente locale e richiedono invece Active Directory, nel server Active Directory deve essere creato un utente con il nome utente *cssys*.
- Informazioni sulla sicurezza di Cloud Insights "qui".

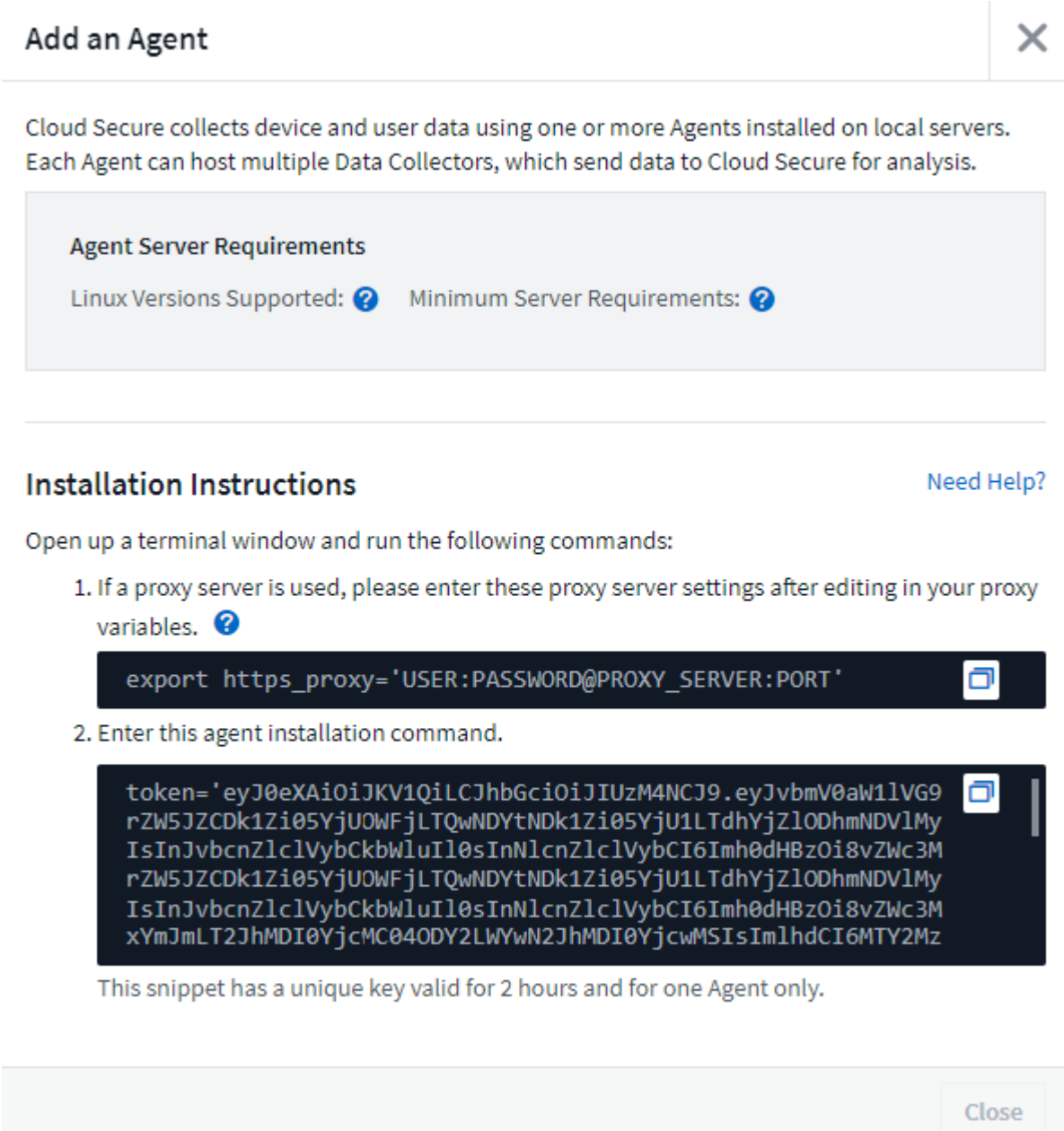
Procedura per l'installazione dell'agente

1. Accedere come Amministratore o Proprietario dell'account all'ambiente workload Security.
2. Selezionare **Collector > Agents > +Agent**

   Viene visualizzata la pagina Add an Agent (Aggiungi un agente):



3. Verificare che il server degli agenti soddisfi i requisiti minimi di sistema.
4. Per verificare che sul server degli agenti sia in esecuzione una versione supportata di Linux, fare clic su *versioni supportate (i)*.
5. Se la rete utilizza un server proxy, impostare i dettagli del server proxy seguendo le istruzioni nella sezione Proxy.



6. Fare clic sull'icona Copia negli Appunti per copiare il comando di installazione.
7. Eseguire il comando di installazione in una finestra del terminale.
8. Al termine dell'installazione, il sistema visualizza il seguente messaggio:

Una volta terminato

1. È necessario configurare un "User Directory Collector".
2. È necessario configurare uno o più Data Collector.

Configurazione di rete

Eseguire i seguenti comandi sul sistema locale per aprire le porte che verranno utilizzate da workload Security. In caso di problemi di sicurezza relativi all'intervallo di porte, è possibile utilizzare un intervallo di porte inferiore, ad esempio *35000:35100*. Ogni SVM utilizza due porte.

Fasi

1. `sudo firewall-cmd --permanent --zone=public --add-port=35000-55000/tcp`
2. `sudo firewall-cmd --reload`

Segui i passaggi successivi in base alla piattaforma:

CentOS 7.x/RHEL 7.x:

1. `sudo iptables-save | grep 35000`

Output di esempio:

```
 -A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
*CentOS 8.x/RHEL 8.x*:
```

1. `sudo firewall-cmd --zone=public --list-ports | grep 35000` (Per CentOS 8)

Output di esempio:

```
35000-55000/tcp
```

Risoluzione dei problemi relativi agli errori dell'agente

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema:	Risoluzione:
L'installazione dell'agente non riesce a creare la cartella /opt/netapp/cloudsecsicuro/Agent/logs/agent.log e il file install.log non fornisce informazioni rilevanti.	Questo errore si verifica durante il bootstrap dell'agente. L'errore non viene registrato nei file di log perché si verifica prima dell'inizializzazione del logger. L'errore viene reindirizzato all'output standard ed è visibile nel log di servizio utilizzando `journalctl -u cloudsecure-agent.service` comando. Questo comando può essere utilizzato per risolvere ulteriormente il problema.

Problema:	Risoluzione:
L'installazione dell'agente non riesce 'questa distribuzione linux non è supportata. Uscire dall'installazione'.	Questo errore viene visualizzato quando si tenta di installare l'agente su un sistema non supportato. Vedere "Requisiti dell'agente".
Installazione dell'agente non riuscita con l'errore: "-bash: Unzip: Command not found"	Installare unzip ed eseguire nuovamente il comando di installazione. Se Yum è installato sul computer, provare a "yum install unzip" per installare il software unzip. Quindi, copiare nuovamente il comando dall'interfaccia utente di installazione dell'agente e incollarlo nell'interfaccia utente per eseguire nuovamente l'installazione.

L'agente è stato installato ed era in esecuzione. Tuttavia, l'agente si è arrestato improvvisamente.	SSH al computer dell'agente. Controllare lo stato del servizio dell'agente tramite `sudo systemctl status cloudsecure-agent.service`. 1. Controllare se nei registri viene visualizzato il messaggio "Impossibile avviare il servizio daemon di sicurezza workload" . 2. Controllare se l'utente cssys esiste o meno nel computer dell'agente. Eseguire i seguenti comandi uno alla volta con l'autorizzazione root e controllare se l'utente e il gruppo cssys esistono.
	`sudo id cssys`
	`sudo groups cssys`3. Se non ne esiste alcuna, è possibile che un criterio di monitoraggio centralizzato abbia eliminato l'utente cssys. 4. Creare manualmente un utente e un gruppo cssys eseguendo i seguenti comandi.
	`sudo useradd cssys`
	`sudo groupadd cssys`5. Riavviare il servizio dell'agente eseguendo il seguente comando:
	`sudo systemctl restart cloudsecure-agent.service`6. Se non è ancora in esecuzione, controllare le altre opzioni di risoluzione dei problemi.

Impossibile aggiungere più di 50 Data colleziones a un Agente.	È possibile aggiungere solo 50 Data colleziones a un Agente. Questa può essere una combinazione di tutti i tipi di collector, ad esempio Active Directory, SVM e altri tipi di raccolta.
L'interfaccia utente mostra che l'agente è in stato NOT_CONNECTED.	Procedura per riavviare l'agente. 1. SSH al computer dell'agente. 2. Riavviare il servizio dell'agente eseguendo il seguente comando: `sudo systemctl restart cloudsecure-agent.service`3. Controllare lo stato del servizio dell'agente tramite `sudo systemctl status cloudsecure-agent.service`. 4. L'agente deve passare allo stato CONNESSO.

Problema:	Risoluzione:
La macchina virtuale dell'agente è dietro il proxy Zscaler e l'installazione dell'agente non riesce. A causa dell'ispezione SSL del proxy Zscaler, i certificati di workload Security vengono presentati in quanto firmati da Zscaler CA, in modo che l'agente non stia fidando della comunicazione.	Disattivare l'ispezione SSL nel proxy Zscaler per l'URL *.cloudinsights.netapp.com. Se Zscaler esegue l'ispezione SSL e sostituisce i certificati, la sicurezza del carico di lavoro non funzionerà.
Durante l'installazione dell'agente, l'installazione si blocca dopo la decompressione.	Il comando "chmod 755 -RF" non funziona correttamente. Il comando non riesce quando il comando di installazione dell'agente viene eseguito da un utente sudo non root che ha file nella directory di lavoro, appartenenti a un altro utente, e le autorizzazioni di tali file non possono essere modificate. A causa del comando chmod non funzionante, il resto dell'installazione non viene eseguito. 1. Creare una nuova directory denominata "cloudSecure". 2. Accedere alla directory. 3. Copiare e incollare il "token=…… completo … ./cloudsecure-agent-install.sh" e premere invio. 4. L'installazione dovrebbe essere in grado di procedere.
Se l'Agente non riesce ancora a connettersi a Saas, aprire un caso con il supporto NetApp. Fornire il numero di serie Cloud Insights per aprire un caso e allegare i registri al caso come indicato.	Per allegare i registri al caso: 1. Eseguire il seguente script con il permesso root e condividere il file di output (cloudSecure-Agent-symptoms.zip). a. /opt/netapp/cloudsecsicuro/agent/bin/cloudsecure-agent-symptom-collector.sh 2. Eseguire i seguenti comandi uno alla volta con l'autorizzazione root e condividere l'output. a. id cssys b. gruppi cssys c. cat /etc/os-release
Lo script cloudsecure-agent-symptom-collector.sh non riesce e viene visualizzato il seguente errore. [Root@machine tmp] n. /opt/netapp/cloudsecure/Agent/bin/cloudsecure-agent-symptom-collector.sh raccolta log del servizio raccolta log dell'applicazione raccolta di configurazioni dell'agente acquisizione di snapshot dello stato del servizio acquisizione di snapshot della struttura della directory dell'agente …… . …… . /Opt/netapp/cloudsecura/Agent/bin/cloudsecura-Agent-Symptom-collector.sh: Riga 52: zip: Errore comando non trovato: Impossibile creare /tmp/cloudsecure-agent-symptoms.zip	Lo strumento ZIP non è installato. Installare lo strumento zip eseguendo il comando "yum install zip". Quindi eseguire di nuovo il file cloudsecure-agent-symptom-collector.sh.

Problema:	Risoluzione:
L'installazione dell'agente non riesce con useradd: Impossibile creare la directory /home/cssys	Questo errore può verificarsi se la directory di login dell'utente non può essere creata in /home, a causa della mancanza di permessi. La soluzione consiste nel creare un utente cssys e aggiungerne manualmente la directory di accesso utilizzando il seguente comando: *Sudo useradd user_name -m -d HOME_DIR* -m :creare la home directory dell'utente se non esiste. -D : il nuovo utente viene creato utilizzando HOME_DIR come valore per la directory di accesso dell'utente. Ad esempio, *sudo useradd cssys -m -d /cssys*, aggiunge un utente *cssys* e crea la directory di login sotto root.
L'agente non è in esecuzione dopo l'installazione. Systemctl status cloudsecure-agent.service_ mostra quanto segue: [Root@demo ~] systemctl status cloudsecure-agent.service agent.service – workload Security Agent Daemon Service Loaded: Loaded (/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: Disabled) Active: Attivazione (riavvio automatico) (risultato: Codice di uscita) dal mar 2021 26 alle 08-03 21:12 126 PDT; 2s fa processo: 25889 Start/unloopt/stato principale/unbin/unbin/aft/unbin/unload/unload/unbin/unload/unload/it/unbin/it/it/it/it/it/it/it/it/it/it 25889 (code=exited, status=126), 03 21 agosto:12:26 sistema dimostrativo[1]: cloudsecure-agent.service: processo principale terminato, code=exited, status=126/n/a 03 21 agosto:12:26 sistema dimostrativo[1]: L'unità cloudsecure-agent.service è entrata nello stato di errore. Agosto 03 21:12:26 sistema dimostrativo[1]: cloudsecure-agent.service non riuscito.	Questo potrebbe non riuscire perché l'utente *cssys* potrebbe non disporre dell'autorizzazione per l'installazione. Se /opt/netapp è un mount NFS e l'utente *cssys* non ha accesso a questa cartella, l'installazione avrà esito negativo. *Cssys* è un utente locale creato dal programma di installazione di workload Security che potrebbe non disporre dell'autorizzazione per accedere alla condivisione montata. Per verificarlo, tentare di accedere a /opt/netapp/cloudsecrect/Agent/bin/cloudsecrect-Agent utilizzando *cssys* user. Se restituisce "autorizzazione negata", l'autorizzazione all'installazione non è presente. Invece di una cartella montata, installarla in una directory locale del computer.
L'agente era inizialmente connesso tramite un server proxy e il proxy era impostato durante l'installazione dell'agente. Ora il server proxy è cambiato. Come si può modificare la configurazione del proxy dell'Agente?	È possibile modificare agent.properties per aggiungere i dettagli del proxy. Attenersi alla seguente procedura: 1. Passare alla cartella contenente il file di proprietà: cd /opt/netapp/cloudsecsicuro/conf 2. Utilizzando l'editor di testo preferito, aprire il file *agent.properties* per la modifica. 3. Aggiungere o modificare le seguenti righe: AGENT_PROXY_HOST=scspa1950329001.vm.netapp.com AGENT_PROXY_PORT=80 AGENT_PROXY_USER=pxuser AGENT_PROXY_PASSWORD=pass1234 4. Salvare il file. 5. Riavviare l'agente: Sudo systemctl riavviare cloudsecure-agent.service

Eliminazione di un agente di sicurezza del carico di lavoro

Quando si elimina un agente di sicurezza del carico di lavoro, è necessario eliminare prima tutti i dati di raccolta associati all'agente.

Eliminazione di un agente

> L'eliminazione di un agente comporta l'eliminazione di tutti i Data Collector associati all'agente. Se si prevede di configurare i data collector con un agente diverso, è necessario creare un backup delle configurazioni di Data Collector prima di eliminare l'agente.

Prima di iniziare

1. Assicurarsi che tutti i data raccoglitori associati all'agente siano eliminati dal portale workload Security.

   Nota: Ignorare questo passaggio se tutti i collettori associati sono in stato DI ARRESTO.

Procedura per l'eliminazione di un agente:

1. SSH nella macchina virtuale dell'agente ed eseguire il seguente comando. Quando richiesto, immettere "y" per continuare.

   ```
   sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-
   uninstall.sh
   Uninstall CloudSecure Agent? [y|N]:
   ```

2. Fare clic su **sicurezza del carico di lavoro > Collector > Agenti**

   Viene visualizzato l'elenco degli agenti configurati.

3. Fare clic sul menu delle opzioni dell'agente che si desidera eliminare.
4. Fare clic su **Delete** (Elimina).

   Viene visualizzata la pagina **Delete Agent** (Elimina agente).

5. Fare clic su **Delete** (Elimina) per confermare l'eliminazione.

Configurazione di un servizio di raccolta directory utente Active Directory (ad)

Workload Security può essere configurato per raccogliere gli attributi utente dai server Active Directory.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore o un proprietario di account Cloud Insights.
- È necessario disporre dell'indirizzo IP del server che ospita il server Active Directory.
- Prima di configurare un connettore di directory utente, è necessario configurare un agente.

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu workload Security (sicurezza del carico di lavoro), fare clic su:
   Collector > User Directory Collector > + User Directory Collector e selezionare **Active Directory**

   Viene visualizzata la schermata Add User Directory (Aggiungi directory utente).

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco della directory utente. Ad esempio *GlobalADCollector*
Agente	Selezionare un agente configurato dall'elenco
IP del server/Nome dominio	Indirizzo IP o FQDN (Fully-qualified Domain Name) del server che ospita la directory attiva
Nome foresta	Livello di foresta della struttura di directory. Il nome della foresta consente di utilizzare entrambi i seguenti formati: *X. y.y.z* ⇒ nome di dominio diretto così come lo si dispone sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nomi distinti relativi [esempio: DC=hq,DC= nomeazienda,DC=com] oppure è possibile specificare quanto segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [per filtrare in base all'ingegneria specifica dell'unità organizzativa] *CN=nome utente,OU=engineering,DC=companyname, DC=netapp, DC=com* [per ottenere solo un utente specifico con <username> da OU <engineering>] *CN=utenti Acrobat,CN=utenti,DC=hq,DC=companyname,DC=co mpanyname,DC=companyname,o=tutti gli utenti attendibili all'interno di quest'organizzazione sono supportati da Acrobat_S=i domini che sono supportati da Microsoft,S=i domini Microsoft,S=IT*.
DN di binding	Utente autorizzato a cercare nella directory. Ad esempio: *username@companyname.com* o *username@domainname.com* Inoltre, è richiesta l'autorizzazione di sola lettura del dominio. L'utente deve essere membro del gruppo di protezione *Controller di dominio di sola lettura*.
ASSOCIARE la password	Password del server di directory (ad es. Password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls
Porte	Selezionare la porta

Se i nomi degli attributi predefiniti sono stati modificati in Active Directory, immettere i seguenti attributi richiesti per il server di directory. Nella maggior parte dei casi, questi nomi di attributi vengono *non* modificati in Active Directory, nel qual caso è possibile semplicemente procedere con il nome dell'attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome visualizzato	nome
SID	objectsid
Nome utente	SAMAccountName

Fare clic su Includi attributi facoltativi per aggiungere uno dei seguenti attributi:

Attributi	Nome attributo in Directory Server
Indirizzo e-mail	mail
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato
Reparto	reparto
Foto	thumbnailphoto
ManagerDN	manager
Gruppi	MemberOf

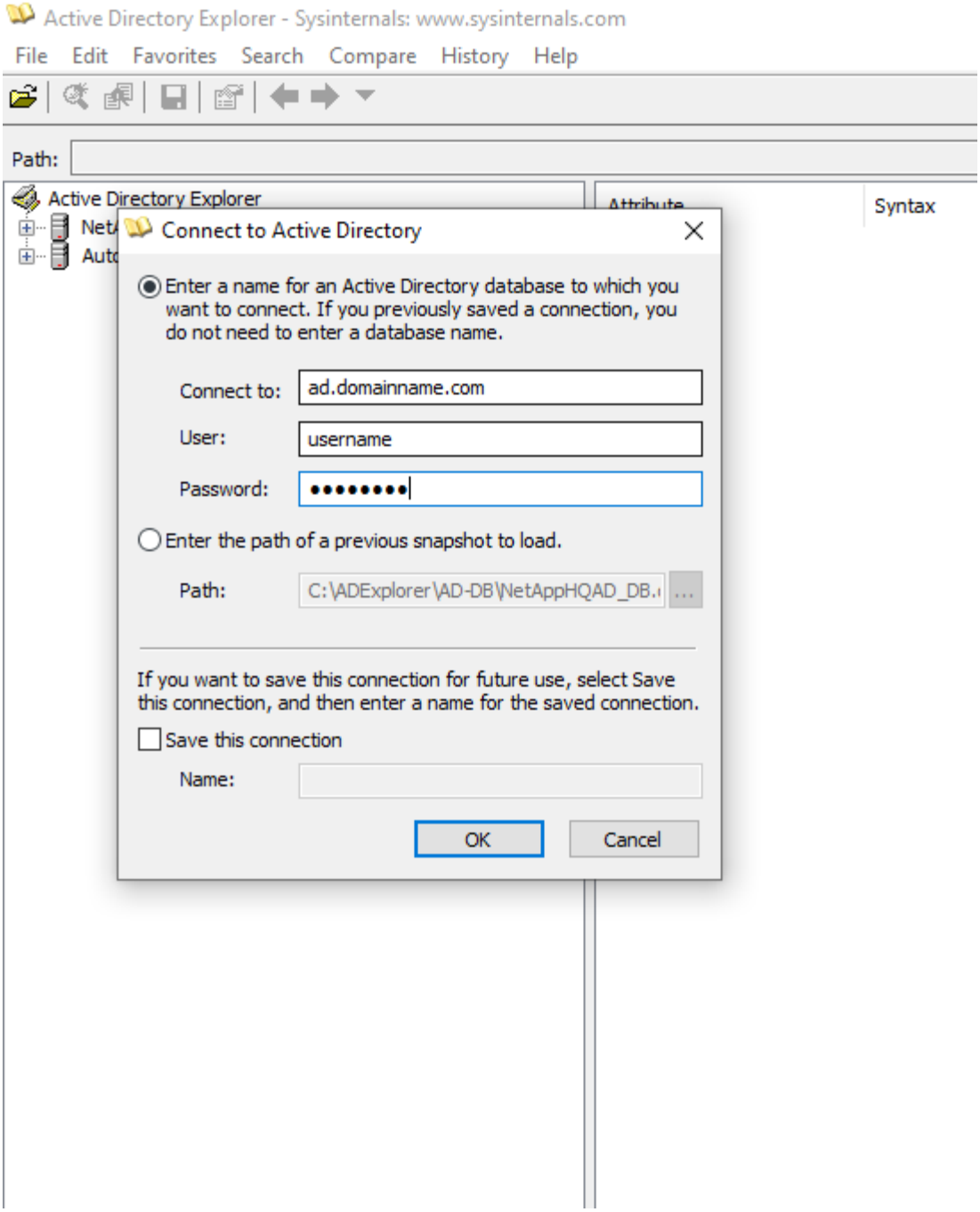
Verifica della configurazione di User Directory Collector

È possibile convalidare le autorizzazioni utente LDAP e le definizioni degli attributi utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP per la sicurezza del carico di lavoro:

  ```
  ldapsearch -o ldif-wrap=no -LLL -x -b "dc=netapp,dc=com" -h 10.235.40.29 -p
  389 -D Administrator@netapp.com -W
  ```

- Utilizzare ad Explorer per navigare in un database ad, visualizzare le proprietà e gli attributi degli oggetti, visualizzare le autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche sofisticate che è possibile salvare ed eseguire nuovamente.
  - Installare "AD Explorer" Su qualsiasi computer Windows in grado di connettersi al server ad.
  - Connettersi al server ad utilizzando il nome utente/la password del server di directory ad.



Risoluzione degli errori di configurazione di User Directory Collector

La seguente tabella descrive i problemi noti e le risoluzioni che possono verificarsi durante la configurazione di Collector:

Problema:	Risoluzione:
L'aggiunta di un connettore directory utente determina lo stato 'Error'. Viene visualizzato il messaggio di errore "credenziali non valide fornite per il server LDAP".	Nome utente o password forniti non corretti. Modificare e fornire il nome utente e la password corretti.

Problema:	Risoluzione:
L'aggiunta di un connettore directory utente determina lo stato 'Error'. L'errore dice: "Impossibile ottenere l'oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome della foresta".	Nome di foresta specificato errato. Modificare e fornire il nome corretto della foresta.
Gli attributi facoltativi dell'utente di dominio non vengono visualizzati nella pagina Profilo utente sicurezza workload.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire i nomi degli attributi facoltativi corretti.
Data collector in stato di errore con "Impossibile recuperare utenti LDAP. Motivo dell'errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore facendo clic sul pulsante *Restart*.
L'aggiunta di un connettore directory utente determina lo stato 'Error'.	Assicurarsi di aver fornito valori validi per i campi obbligatori (Server, nome-foresta, BIND-DN, BIND-Password). Assicurarsi che l'input bind-DN sia sempre fornito come 'Amministratore@<domain_forest_name>' o come account utente con privilegi di amministratore di dominio.
L'aggiunta di un connettore directory utente determina lo stato 'RETENTATIVO'. Mostra l'errore "Impossibile definire lo stato del raccoglitore, motivo comando TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] non riuscito a causa di java.net.ConnectionException:Connection rifiutato."	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l'indirizzo IP o l'FQDN corretto.
L'aggiunta di un connettore directory utente determina lo stato 'Error'. Viene visualizzato il messaggio di errore "Impossibile stabilire la connessione LDAP".	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l'indirizzo IP o l'FQDN corretto.
L'aggiunta di un connettore directory utente determina lo stato 'Error'. L'errore indica che non è stato possibile caricare le impostazioni. Motivo: Si è verificato un errore nella configurazione dell'origine dati. Motivo specifico: /Connector/conf/application.conf: 70: ldap.ldap-port ha una STRINGA di tipo piuttosto che UN NUMERO"	Valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server ad.
Ho iniziato con gli attributi obbligatori e ho funzionato. Dopo aver aggiunto i dati facoltativi, i dati degli attributi facoltativi non vengono recuperati da ad.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi opzionali aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire il nome dell'attributo obbligatorio o facoltativo corretto.
Dopo aver riavviato il collector, quando avverrà la sincronizzazione ad?	LA sincronizzazione AD avverrà immediatamente dopo il riavvio del collector. Il recupero dei dati utente di circa 300.000 utenti richiede circa 15 minuti e viene aggiornato automaticamente ogni 12 ore.

Problema:	Risoluzione:
I dati dell'utente vengono sincronizzati da ad a CloudSecure. Quando verranno cancellati i dati?	I dati dell'utente vengono conservati per 13 mesi in caso di mancato aggiornamento. Se il tenant viene cancellato, i dati verranno cancellati.
User Directory Connector si trova nello stato 'Error'. "Connettore in stato di errore. Nome del servizio: UsersLdap. Motivo dell'errore: Impossibile recuperare gli utenti LDAP. Motivo del guasto: 80090308: LdapErr: DSID-0C090453, commento: AcceptSecurityContext error, data 52e, v3839"	Nome di foresta specificato errato. Vedere sopra per informazioni su come fornire il nome corretto della foresta.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Ciò è probabilmente dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico Active Directory Collector che sta recuperando le informazioni dell'utente da Active Directory. 2. Nota sotto gli attributi facoltativi, è presente un nome di campo "numero di telefono" mappato all'attributo Active Directory 'numero di telefono'. 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto in precedenza per esplorare Active Directory e visualizzare il nome dell'attributo corretto. 3. Assicurarsi che in Active Directory sia presente un attributo denominato 'Telephonenumber' che abbia effettivamente il numero di telefono dell'utente. 5. Diciamo che in Active Directory è stato modificato in 'phonenumber'. 6. Quindi, modificare CloudSecure User Directory Collector. Nella sezione opzionale degli attributi, sostituire 'Telephonenumber' con 'phonenumber'. 7. Salvare Active Directory Collector, il Collector si riavvierà e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è attivato sul server Active Directory (ad), il servizio di raccolta directory utente di workload Security non può connettersi al server ad.	Disattivare la crittografia ad Server prima di configurare un User Directory Collector. Una volta recuperato il dettaglio dell'utente, questo sarà disponibile per 13 mesi. Se il server ad si disconnette dopo aver recuperato i dettagli dell'utente, i nuovi utenti aggiunti in ad non verranno recuperati. Per recuperare di nuovo, è necessario connettere ad ad il raccoglitore di directory dell'utente.
I dati di Active Directory sono presenti in CloudInsights Security. Eliminare tutte le informazioni utente da CloudInsights.	Non è possibile eliminare SOLO le informazioni utente di Active Directory da CloudInsights Security. Per eliminare l'utente, è necessario eliminare l'intero tenant.

Configurazione di un servizio di raccolta LDAP Directory Server

È possibile configurare la sicurezza del carico di lavoro per raccogliere gli attributi utente dai server di directory LDAP.

Prima di iniziare

- Per eseguire questa attività, è necessario essere un amministratore o un proprietario di account Cloud Insights.
- È necessario disporre dell'indirizzo IP del server che ospita il server di directory LDAP.
- Prima di configurare un connettore di directory LDAP, è necessario configurare un agente.

Procedura per la configurazione di un servizio di raccolta directory utente

1. Nel menu workload Security (sicurezza del carico di lavoro), fare clic su: **Collector > User Directory Collector > + User Directory Collector** e selezionare **LDAP Directory Server**

   Viene visualizzata la schermata Add User Directory (Aggiungi directory utente).

Configurare User Directory Collector inserendo i dati richiesti nelle seguenti tabelle:

Nome	Descrizione
Nome	Nome univoco della directory utente. Ad esempio *GlobalLDAPCollector*
Agente	Selezionare un agente configurato dall'elenco
IP del server/Nome dominio	Indirizzo IP o FQDN (Fully-qualified Domain Name) del server che ospita il server di directory LDAP
Base di ricerca	Search base (base di ricerca) del server LDAP Search base (base di ricerca) consente di utilizzare entrambi i seguenti formati: *X. y.y.z* ⇒ nome di dominio diretto, così come lo si dispone sulla SVM. [Esempio: hq.companyname.com] *DC=x,DC=y,DC=z* ⇒ nomi distinti relativi [esempio: DC=hq,DC= nomeazienda,DC=com] oppure è possibile specificare quanto segue: *OU=engineering,DC=hq,DC= companyname,DC=com* [to filtering by specific ou engineering] *CN=Username,OU=engineering,DC=companyname, DC=netapp, DC=com* [to get only specific user with <username> from OU <engineering>] _CN=Acrobat Users,CN=Users,DC=hq,DC=companyname,DC=com panyname,DC=com,o=companyname of the U.S.
DN di binding	Utente autorizzato a cercare nella directory. Ad esempio: uid=ldapuser,cn=users,cn=accounts,DC=domain,DC= companyname,DC=com uid=john,cn=users,cn=accounts,DC=dorp,DC=Compa ny,DC=com per un utente john@dorp.company.com. dorp.company.com
--account	--utenti
--giovanni	--anna
ASSOCIARE la password	Password del server di directory (ad es. Password per il nome utente utilizzato in Bind DN)
Protocollo	ldap, ldaps, ldap-start-tls

Porte	Selezionare la porta

Se i nomi degli attributi predefiniti sono stati modificati in LDAP Directory Server, immettere i seguenti attributi richiesti per Directory Server. Nella maggior parte dei casi, questi nomi di attributi vengono *non* modificati in LDAP Directory Server, nel qual caso è possibile semplicemente procedere con il nome di attributo predefinito.

Attributi	Nome dell'attributo nel server di directory
Nome visualizzato	nome
UNIXID	uidnumber
Nome utente	uid

Fare clic su Includi attributi facoltativi per aggiungere uno dei seguenti attributi:

Attributi	Nome attributo in Directory Server
Indirizzo e-mail	mail
Numero di telefono	numero di telefono
Ruolo	titolo
Paese	co
Stato	stato
Reparto	numero di parte
Foto	foto
ManagerDN	manager
Gruppi	MemberOf

Verifica della configurazione di User Directory Collector

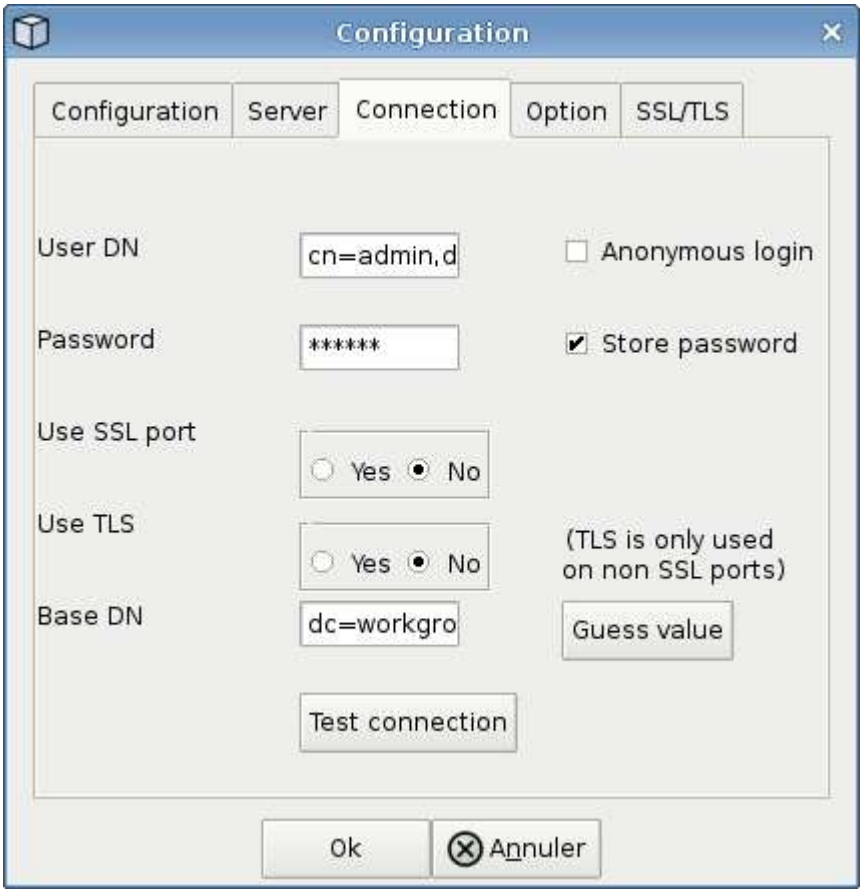
È possibile convalidare le autorizzazioni utente LDAP e le definizioni degli attributi utilizzando le seguenti procedure:

- Utilizzare il seguente comando per convalidare l'autorizzazione utente LDAP per la sicurezza del carico di lavoro:

```
 ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* Utilizzare LDAP Explorer per navigare in un database LDAP,
visualizzare le proprietà e gli attributi degli oggetti, visualizzare le
autorizzazioni, visualizzare lo schema di un oggetto, eseguire ricerche
sofisticate che è possibile salvare ed eseguire nuovamente.
```

  - Installare LDAP Explorer (http://ldaptool.sourceforge.net/) O Java LDAP Explorer (http://jxplorer.org/) Su qualsiasi computer Windows in grado di connettersi al server LDAP.

- Connettersi al server LDAP utilizzando il nome utente/la password del server di directory LDAP.



Risoluzione degli errori di configurazione di LDAP Directory Collector

La seguente tabella descrive i problemi noti e le risoluzioni che possono verificarsi durante la configurazione di Collector:

Problema:	Risoluzione:
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. Viene visualizzato il messaggio di errore "credenziali non valide fornite per il server LDAP".	DN di binding o password di binding o base di ricerca forniti non corretti. Modificare e fornire le informazioni corrette.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. L'errore dice: "Impossibile ottenere l'oggetto corrispondente a DN=DC=hq,DC=domainname,DC=com fornito come nome della foresta".	Base di ricerca fornita errata. Modificare e fornire il nome corretto della foresta.
Gli attributi facoltativi dell'utente di dominio non vengono visualizzati nella pagina Profilo utente sicurezza workload.	Ciò è probabilmente dovuto a una mancata corrispondenza tra i nomi degli attributi facoltativi aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. I campi distinguono tra maiuscole e minuscole. Modificare e fornire i nomi degli attributi facoltativi corretti.

Problema:	Risoluzione:
Data collector in stato di errore con "Impossibile recuperare utenti LDAP. Motivo dell'errore: Impossibile connettersi al server, la connessione è nulla"	Riavviare il raccoglitore facendo clic sul pulsante *Restart*.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'.	Assicurarsi di aver fornito valori validi per i campi obbligatori (Server, nome-foresta, BIND-DN, BIND-Password). Assicurarsi che l'input bind-DN sia sempre fornito come uid=ldapuser,cn=users,cn=accounts,DC=domain,DC=companyname,DC=com.
L'aggiunta di un connettore di directory LDAP determina lo stato 'RETENTATIVO'. Mostra l'errore "Impossibile determinare lo stato del raccoglitore e riprovare"	Verificare che siano forniti l'indirizzo IP del server e la base di ricerca corretti ///
Durante l'aggiunta della directory LDAP viene visualizzato il seguente messaggio di errore: "Impossibile determinare lo stato del raccoglitore entro 2 tentativi, riavviare nuovamente il raccoglitore (codice errore: AGENT008)"	Verificare che siano forniti l'indirizzo IP del server e la base di ricerca corretti
L'aggiunta di un connettore di directory LDAP determina lo stato 'RETENTATIVO'. Mostra l'errore "Impossibile definire lo stato del raccoglitore, motivo comando TCP [Connect(localhost:35012,None,List(),some(,seconds),true)] non riuscito a causa di java.net.ConnectionException:Connection rifiutato."	IP o FQDN non corretti forniti per il server ad. Modificare e fornire l'indirizzo IP o l'FQDN corretto. ////
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. Viene visualizzato il messaggio di errore "Impossibile stabilire la connessione LDAP".	Indirizzo IP o FQDN errato fornito per il server LDAP. Modificare e fornire l'indirizzo IP o l'FQDN corretto. O valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server LDAP.
L'aggiunta di un connettore di directory LDAP determina lo stato 'Error'. L'errore indica che non è stato possibile caricare le impostazioni. Motivo: Si è verificato un errore nella configurazione dell'origine dati. Motivo specifico: /Connector/conf/application.conf: 70: ldap.ldap-port ha una STRINGA di tipo piuttosto che UN NUMERO"	Valore errato per la porta fornita. Provare a utilizzare i valori di porta predefiniti o il numero di porta corretto per il server ad.
Ho iniziato con gli attributi obbligatori e ho funzionato. Dopo aver aggiunto i dati facoltativi, i dati degli attributi facoltativi non vengono recuperati da ad.	Ciò è probabilmente dovuto a una mancata corrispondenza tra gli attributi opzionali aggiunti in CloudSecure e i nomi degli attributi effettivi in Active Directory. Modificare e fornire il nome dell'attributo obbligatorio o facoltativo corretto.

Problema:	Risoluzione:
Dopo aver riavviato il collector, quando avverrà la sincronizzazione LDAP?	La sincronizzazione LDAP viene eseguita immediatamente dopo il riavvio del collector. Il recupero dei dati utente di circa 300.000 utenti richiede circa 15 minuti e viene aggiornato automaticamente ogni 12 ore.
I dati dell'utente vengono sincronizzati da LDAP a CloudSecure. Quando verranno cancellati i dati?	I dati dell'utente vengono conservati per 13 mesi in caso di mancato aggiornamento. Se il tenant viene cancellato, i dati verranno cancellati.
LDAP Directory Connector si trova nello stato 'Error'. "Connettore in stato di errore. Nome del servizio: UsersLdap. Motivo dell'errore: Impossibile recuperare gli utenti LDAP. Motivo del guasto: 80090308: LdapErr: DSID-0C090453, commento: AcceptSecurityContext error, data 52e, v3839"	Nome di foresta specificato errato. Vedere sopra per informazioni su come fornire il nome corretto della foresta.
Il numero di telefono non viene inserito nella pagina del profilo utente.	Ciò è probabilmente dovuto a un problema di mappatura degli attributi con Active Directory. 1. Modificare lo specifico Active Directory Collector che sta recuperando le informazioni dell'utente da Active Directory. 2. Nota sotto gli attributi facoltativi, è presente un nome di campo "numero di telefono" mappato all'attributo Active Directory 'numero di telefono'. 4. Ora, utilizzare lo strumento Active Directory Explorer come descritto in precedenza per esplorare il server LDAP Directory e visualizzare il nome dell'attributo corretto. 3. Assicurarsi che nella directory LDAP sia presente un attributo denominato 'Telephonenumber' che abbia effettivamente il numero di telefono dell'utente. 5. Diciamo che nella directory LDAP è stato modificato in 'phonenumber'. 6. Quindi, modificare CloudSecure User Directory Collector. Nella sezione opzionale degli attributi, sostituire 'Telephonenumber' con 'phonenumber'. 7. Salvare Active Directory Collector, il Collector si riavvierà e otterrà il numero di telefono dell'utente e lo visualizzerà nella pagina del profilo utente.
Se il certificato di crittografia (SSL) è attivato sul server Active Directory (ad), il servizio di raccolta directory utente di workload Security non può connettersi al server ad.	Disattivare la crittografia ad Server prima di configurare un User Directory Collector. Una volta recuperato il dettaglio dell'utente, questo sarà disponibile per 13 mesi. Se il server ad si disconnette dopo aver recuperato i dettagli dell'utente, i nuovi utenti aggiunti in ad non verranno recuperati. Per recuperare di nuovo, è necessario connettere ad ad ad il raccoglitore di directory dell'utente.

Configurazione del Data Collector SVM di ONTAP

Workload Security utilizza i data colleator per raccogliere i dati di accesso ai file e agli utenti dai dispositivi.

Prima di iniziare

- Questo data collector è supportato con i seguenti elementi:
  - Data ONTAP 9.2 e versioni successive. Per prestazioni ottimali, utilizzare una versione Data ONTAP superiore a 9.13.1.
  - Protocollo SMB versione 3.1 e precedenti.
  - Protocollo NFS versione 4.0 e precedenti
  - FlexGroup è supportato da ONTAP 9.4 e versioni successive
  - ONTAP Select è supportato
- Sono supportati solo i tipi di dati SVM. Le SVM con volumi infiniti non sono supportate.
- SVM ha diversi sottotipi. Di questi, sono supportati solo *default*, *Sync_source* e *Sync_destination*.
- Un Agente "deve essere configurato" prima di poter configurare i data colleziones.
- Assicurarsi di disporre di un connettore User Directory configurato correttamente, altrimenti gli eventi mostreranno i nomi utente codificati e non il nome effettivo dell'utente (come memorizzato in Active Directory) nella pagina "Activity Forensics" (analisi delle attività).
- Per ottenere prestazioni ottimali, è necessario configurare il server FPolicy in modo che si trova sulla stessa subnet del sistema di storage.
- È necessario aggiungere una SVM utilizzando uno dei due metodi seguenti:
  - Utilizzando l'IP del cluster, il nome SVM e il nome utente e la password di gestione del cluster. ***questo è il metodo consigliato.***
    - Il nome SVM deve essere identico a quello mostrato in ONTAP ed è sensibile al maiuscolo/minuscolo.
  - Utilizzando SVM Vserver Management IP, Username e Password
  - Se non si è in grado o non si è disposti a utilizzare il nome utente e la password completi di Administrator Cluster/SVM Management, è possibile creare un utente personalizzato con privilegi inferiori, come indicato nella ""Nota sulle autorizzazioni"" di seguito. Questo utente personalizzato può essere creato per l'accesso a SVM o Cluster.
    - o è anche possibile utilizzare un utente ad con un ruolo che disponga almeno delle autorizzazioni di csrole, come indicato nella sezione "A note about permissions" (Nota sulle autorizzazioni) riportata di seguito. Consultare anche la "Documentazione ONTAP".
- Assicurarsi che siano impostate le applicazioni corrette per SVM eseguendo il seguente comando:

```
clustershell::> security login show -vserver <vservername> -user-or
-group-name <username>
```

Output di esempio:

```
Vserver: svmname
                                                                    Second
User/Group                  Authentication                  Acct    Authentication
Name            Application Method        Role Name        Locked  Method
--------------- ----------- ------------- ---------------- ------  --------------
vsadmin         http        password      vsadmin          no      none
vsadmin         ontapi      password      vsadmin          no      none
vsadmin         ssh         password      vsadmin          no      none
3 entries were displayed.
```

- Assicurarsi che la SVM abbia un server CIFS configurato: Clustershell::> `vserver cifs show`

  Il sistema restituisce il nome del server Vserver, il nome del server CIFS e i campi aggiuntivi.

- Impostare una password per l'utente vsadmin di SVM. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. shell cluster::> `security login password -username vsadmin -vserver svmname`
- Sbloccare l'utente vsadmin di SVM per l'accesso esterno. Se si utilizza un utente personalizzato o un utente amministratore del cluster, saltare questo passaggio. shell cluster::> `security login unlock -username vsadmin -vserver svmname`
- Assicurarsi che la policy firewall della LIF dati sia impostata su 'mgmt' (non su 'dATA'). Saltare questo passaggio se si utilizza una scheda di gestione dedicata per aggiungere la SVM. shell cluster::> `network interface modify -lif <SVM_data_LIF_name> -firewall-policy mgmt`
- Quando un firewall è attivato, è necessario definire un'eccezione per consentire il traffico TCP per la porta che utilizza il servizio di raccolta dati Data ONTAP.

  Vedere "Requisiti dell'agente" per informazioni sulla configurazione. Ciò vale per gli agenti e gli agenti on-premise installati nel cloud.

- Quando un agente viene installato in un'istanza di AWS EC2 per monitorare una SVM Cloud ONTAP, l'agente e lo storage devono trovarsi nello stesso VPC. Se si trovano in VPC separati, deve esserci un percorso valido tra i VPC.

Prerequisiti per il blocco dell'accesso utente

Tenere presente quanto segue per "Blocco degli accessi degli utenti":

Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni a workload Security per bloccare l'utente.

Per gli utenti csuser con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Nota sulle autorizzazioni

Autorizzazioni per l'aggiunta tramite Cluster Management IP:

Se non è possibile utilizzare l'utente amministratore della gestione del cluster per consentire a workload Security di accedere al data collector SVM di ONTAP, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il data collector di workload Security per l'utilizzo di Cluster Management IP.

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore della gestione del cluster ed eseguire i seguenti comandi sul server ONTAP:

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```
security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole
```

Autorizzazioni per l'integrazione ONTAP ARP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Autorizzazioni per accesso ONTAP negato:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Nota: Se è già stato aggiunto un ruolo di pausa, *arwrole* o *csrestrole*, non è necessario aggiungere un secondo ruolo di pausa. È possibile aggiungere semplicemente le autorizzazioni API come nell'esempio seguente.

Esempio: *Csrestrole* è già presente, per cui dobbiamo abilitare la protezione anti-ransomware e assegnare autorizzazioni API al *csrestrole* esistente:

```
security login rest-role create -role csrestrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
```

Autorizzazioni per l'aggiunta tramite Vserver Management IP:

Se non è possibile utilizzare l'utente amministratore della gestione del cluster per consentire a workload Security di accedere al data collector SVM di ONTAP, è possibile creare un nuovo utente denominato "csuser" con i ruoli indicati nei comandi seguenti. Utilizzare il nome utente "csuser" e la password per "csuser" quando si configura il data collector di workload Security per utilizzare Vserver Management IP.

Per creare il nuovo utente, accedere a ONTAP con il nome utente/password dell'amministratore della gestione del cluster ed eseguire i seguenti comandi sul server ONTAP. Per semplicità, copiare questi comandi in un editor di testo e sostituire <vservername> con il nome del server virtuale prima di eseguire questi comandi su ONTAP:

```
security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly
```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
 security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
Autorizzazioni per accesso ONTAP negato:
```

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Autorizzazioni per la protezione autonoma da ransomware ONTAP

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni alla sicurezza del carico di lavoro per raccogliere informazioni relative all'ARP da ONTAP.

Per *csuser* con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Per ulteriori informazioni, consultare la sezione "Integrazione con la protezione ransomware autonoma di ONTAP"

Autorizzazioni per accesso ONTAP negate

Se Data Collector viene aggiunto utilizzando le credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se il servizio di raccolta viene aggiunto utilizzando un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, attenersi alla procedura riportata di seguito per assegnare a sicurezza del carico di lavoro l'autorizzazione necessaria per registrare gli eventi di accesso negato con ONTAP.

Per csuser con credenziali *cluster*, eseguire i seguenti comandi dalla riga di comando di ONTAP. Si noti che *csrestrole* è un ruolo personalizzato e *csuser* è un utente personalizzato di ONTAP.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Per csuser con credenziali *SVM*, eseguire i seguenti comandi dalla riga di comando di ONTAP:

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Per ulteriori informazioni, consultare la sezione "Integrazione con accesso ONTAP negato"

Configurare il data collector

Procedura per la configurazione

1. Accedere come amministratore o come proprietario dell'account all'ambiente Cloud Insights.
2. Fare clic su **sicurezza del carico di lavoro > Collector > +Data Collector**

   Il sistema visualizza i Data Collector disponibili.

3. Passare il mouse sul riquadro **NetApp SVM e fare clic su *+Monitor**.

   Viene visualizzata la pagina di configurazione SVM di ONTAP. Inserire i dati richiesti per ciascun campo.

Campo	Descrizione
Nome	Nome univoco del Data Collector
Agente	Selezionare un agente configurato dall'elenco.
Connessione tramite IP di gestione per:	Selezionare Cluster IP (IP cluster) o SVM Management IP (IP gestione SVM)
Cluster / SVM Management IP Address (Indirizzo IP gestione cluster/SVM)	L'indirizzo IP del cluster o della SVM, a seconda della selezione effettuata in precedenza.
Nome SVM	Il nome della SVM (questo campo è obbligatorio quando ci si connette tramite l'IP del cluster)
Nome utente	Nome utente per accedere a SVM/Cluster quando si aggiunge tramite l'IP del cluster, le opzioni sono: 1. Cluster-admin 2. 'csuser' 3. AD-user che ha un ruolo simile a csuser. Quando si aggiunge tramite SVM IP, le opzioni sono: 4. vsadmin 5. 'csuser' 6. NOME utente AD con ruolo simile a csuser.
Password	Password per il nome utente sopra indicato
Filtra condivisioni/volumi	Scegliere se includere o escludere condivisioni/volumi dalla raccolta eventi
Inserire i nomi di condivisione completi da escludere/includere	Elenco di condivisioni separate da virgole da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Inserire i nomi completi dei volumi da escludere/includere	Elenco separato da virgole di volumi da escludere o includere (a seconda dei casi) dalla raccolta di eventi
Monitorare l'accesso alle cartelle	Se selezionata, questa opzione attiva gli eventi per il monitoraggio dell'accesso alle cartelle. Tenere presente che la creazione/ridenominazione e l'eliminazione delle cartelle verranno monitorate anche senza selezionare questa opzione. L'attivazione di questa opzione aumenta il numero di eventi monitorati.
Impostare la dimensione del buffer di invio ONTAP	Imposta la dimensione del buffer di invio ONTAP Fpolicy. Se si utilizza una versione di ONTAP precedente a 9.8p7 e si verifica un problema di prestazioni, è possibile modificare le dimensioni del buffer di invio ONTAP per migliorare le prestazioni di ONTAP. Contatta il supporto NetApp se non vedi questa opzione e desideri esplorarla.

Al termine

- Nella pagina dei Data Collector installati, utilizzare il menu delle opzioni a destra di ciascun collector per modificare il data collector. È possibile riavviare il data collector o modificare gli attributi di configurazione del data collector.

Configurazione consigliata per Metro Cluster

Per Metro Cluster si consiglia quanto segue:

1. Collegare due data collettori, uno alla SVM di origine e l'altro alla SVM di destinazione.
2. I data collezioner devono essere collegati da *Cluster IP*.
3. In qualsiasi momento, un data collector dovrebbe essere in esecuzione, un altro potrebbe essere in errore.

   L'attuale data collector SVM 'in esecuzione' viene visualizzato come *in esecuzione*. L'attuale data collector SVM 'sin cima' viene visualizzato come *Error*.

4. Ogni volta che si verifica uno switchover, lo stato del data collector passa da 'in esecuzione' a 'errore' e viceversa.
5. Il data collector richiede fino a due minuti per passare dallo stato di errore allo stato di esecuzione.

Policy di servizio

Se si utilizza la policy di servizio di ONTAP versione 9.9.1, per connettersi al servizio di raccolta origine dati, è necessario il servizio *data-fpolicy-client* insieme al servizio dati *data-nfs* e/o *data-cifs*.

Esempio:

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

Nelle versioni di ONTAP precedenti alla 9.9 non è necessario impostare *data-fpolicy-client*.

Riproduci-Pausa Data Collector

2 nuove operazioni sono ora visualizzate sul menu kebab del raccoglitore (PAUSA e RIPRESA).

Se Data Collector è in stato *running*, è possibile sospendere la raccolta. Aprire il menu "tre punti" per il raccoglitore e selezionare PAUSA. Mentre il raccoglitore è in pausa, non vengono raccolti dati da ONTAP e non vengono inviati dati dal raccoglitore a ONTAP. Ciò significa che nessun evento Fpolicy passerà da ONTAP al data collector e da lì a Cloud Insights.

Tenere presente che se in ONTAP vengono creati nuovi volumi e così via mentre il collector è in pausa, workload Security non raccoglierà i dati e quei volumi, ecc. non verranno riflessi in dashboard o tabelle.

Tenere presente quanto segue:

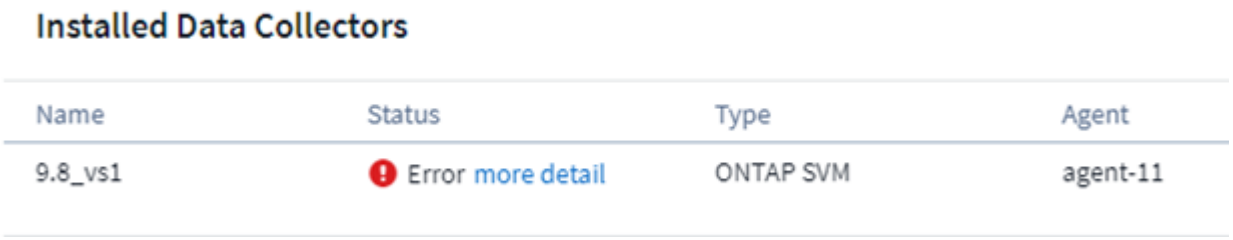
- L'eliminazione degli snapshot non avviene in base alle impostazioni configurate su un raccoglitore in pausa.
- Gli eventi EMS (come ONTAP ARP) non verranno elaborati su un raccoglitore in pausa. Ciò significa che se ONTAP identifica un attacco ransomware, Cloud Insights workload Security non sarà in grado di acquisire quell'evento.
- Le e-mail di notifica dello stato NON verranno inviate per un raccoglitore in pausa.
- Le azioni manuali o automatiche (come Snapshot o blocco utente) non sono supportate in un raccoglitore in pausa.
- In caso di aggiornamenti dell'agente o del raccoglitore, di riavvio/riavvio della VM dell'agente o di riavvio del servizio dell'agente, un raccoglitore in pausa rimarrà nello stato *Paused*.

- Se il data collector si trova nello stato *Error*, il collector non può essere modificato nello stato *Paused*. Il pulsante Pausa viene attivato solo se lo stato del raccoglitore è *in esecuzione*.
- Se l'agente è disconnesso, non è possibile modificare lo stato del collettore in *Paused*. Il raccoglitore passerà allo stato *Stopped* e il pulsante Pausa verrà disattivato.

Risoluzione dei problemi

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

In caso di errore, fare clic su *More Detail* nella colonna *Status* per informazioni dettagliate sull'errore.



Problema:	Risoluzione:
Data Collector viene eseguito per un certo periodo di tempo e si arresta dopo un periodo di tempo casuale, con il messaggio di errore: "Messaggio di errore: Connettore in stato di errore. Nome del servizio: Audit. Motivo del guasto: Server fpolicy esterno sovraccarico."	La percentuale di eventi di ONTAP era molto superiore a quella che la casella Agente è in grado di gestire. Di conseguenza, la connessione è stata interrotta. Controllare il picco di traffico in CloudSecure quando si è verificata la disconnessione. Questa opzione è disponibile nella pagina **CloudSecure > Activity Forensics > All Activity**. Se il picco di traffico aggregato è superiore a quello che Agent Box è in grado di gestire, fare riferimento alla pagina Event Rate Checker per informazioni su come dimensionare l'implementazione di Collector in un Agent Box. Se l'agente è stato installato nella casella Agent prima del 4 marzo 2021, eseguire i seguenti comandi nella casella Agent: ECHO 'net.core.rmem_max=8388608' >> /etc/sysctl.conf echo 'net.ipv4.tcp_rmem = 4096 2097152 8388608' >> /etc/sysctl.conf sysctl -p riavviare il raccoglitore dall'interfaccia utente dopo il ridimensionamento.

Problema:	Risoluzione:
"Collector riporta il messaggio di errore "Nessun indirizzo IP locale trovato sul connettore che può raggiungere le interfacce dati della SVM"."	Questo è probabilmente dovuto a un problema di rete sul lato ONTAP. Attenersi alla seguente procedura: 1. Assicurarsi che non vi siano firewall sui dati della SVM lif o sul lif di gestione che bloccano la connessione dalla SVM. 2. Quando si aggiunge una SVM tramite un IP di gestione del cluster, assicurarsi che il file di dati e il file di gestione della SVM siano in grado di eseguire il ping dalla macchina virtuale dell'agente. In caso di problemi, controllare il gateway, la netmask e i percorsi per la lif. È anche possibile provare ad accedere al cluster tramite ssh utilizzando l'IP di gestione del cluster e ping dell'IP dell'agente. Verificare che l'indirizzo IP dell'agente sia associabile: *Ping di rete -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* Se non è possibile eseguire il ping, verificare che le impostazioni di rete in ONTAP siano corrette, in modo che il computer dell'agente possa essere collegato. 3. Se hai provato a connetterti tramite Cluster IP e non funziona, prova a connetterti direttamente tramite SVM IP. Vedere sopra per la procedura di connessione tramite SVM IP. 4. Durante l'aggiunta del collector tramite le credenziali SVM IP e vsadmin, controllare se il ruolo Data Plus Mgmt di SVM LIF è attivato. In questo caso il ping alla LIF SVM funzionerà, tuttavia SSH alla LIF SVM non funzionerà. In caso affermativo, creare una LIF solo gestione SVM e provare a connettersi tramite questa LIF solo gestione SVM. 5. Se il problema persiste, creare una nuova LIF SVM e provare a connettersi tramite tale LIF. Assicurarsi che la subnet mask sia impostata correttamente. 6. Debug avanzato: A) avviare una traccia di pacchetto in ONTAP. b) provare a collegare un data collector alla SVM dall'interfaccia utente di CloudSecure. c) attendere che venga visualizzato l'errore. Interrompere la traccia dei pacchetti in ONTAP. d) aprire la traccia del pacchetto da ONTAP. È disponibile in questa località *https://<cluster_mgmt_ip>/spi/<clustername>/etc/log/p*

Problema:	Risoluzione:
Messaggio: "Impossibile determinare il tipo di ONTAP per [hostname: <IP Address>. Motivo: Errore di connessione al <IP Address> del sistema di storage: Host irraggiungibile (host irraggiungibile)"	1. Verificare che sia stato fornito l'indirizzo IP di gestione SVM o l'IP di gestione del cluster corretto. 2. SSH alla SVM o al cluster a cui si intende connettersi. Una volta stabilita la connessione, assicurarsi che il nome SVM o il nome del cluster sia corretto.
Messaggio di errore: "Il connettore è in stato di errore. Service.name: Audit. Motivo del guasto: Server fpolicy esterno terminato."	1. È molto probabile che un firewall blocchi le porte necessarie nel computer dell'agente. Verificare che l'intervallo di porte 35000-55000/tcp sia aperto affinché il computer dell'agente si connetta da SVM. Assicurarsi inoltre che non vi siano firewall abilitati dal lato ONTAP che bloccano la comunicazione con il computer dell'agente. 2. Digitare il seguente comando nella casella Agente e verificare che l'intervallo di porte sia aperto. _Sudo iptables-Save

Problema:	Risoluzione:
grep 3500*_ l'output di esempio dovrebbe essere simile a: *-A IN_public_allow -p tcp -m tcp --dport 35000 -m conntrack -ctstate NEW -j ACCEPT* 3. Accedere a SVM, immettere i seguenti comandi e verificare che nessun firewall sia impostato per bloccare la comunicazione con ONTAP. *visualizzazione firewall servizi di sistema visualizzazione policy firewall servizi di sistema_"Controllare i comandi del firewall" Sul lato ONTAP. 4. SSH alla SVM/Cluster che si desidera monitorare. Eseguire il ping della casella Agent dal file di dati SVM (con il supporto dei protocolli CIFS e NFS) e assicurarsi che il ping funzioni: _Ping di rete -vserver <vserver name> -destination <Agent IP> -lif <Lif Name> -show-detail* se non è possibile eseguire il ping, assicurarsi che le impostazioni di rete in ONTAP siano corrette, in modo che il computer dell'agente possa eseguire il ping. 5.se una singola SVM viene aggiunta due volte a un tenant tramite 2 data collettori, viene visualizzato questo errore. Eliminare uno dei data collezionisti attraverso l'interfaccia utente. Quindi riavviare l'altro data collector tramite l'interfaccia utente. Il data collector mostrerà lo stato "IN ESECUZIONE" e inizierà a ricevere gli eventi da SVM. In sostanza, in un tenant, 1 SVM deve essere aggiunto una sola volta, tramite 1 data collector. 1 SVM non deve essere aggiunto due volte tramite 2 data collezioner. 6. Nei casi in cui la stessa SVM è stata aggiunta in due diversi ambienti di workload Security (tenant), l'ultimo avrà sempre successo. Il secondo collector configurerà fpolicy con il proprio indirizzo IP e eseguirà il kick out del primo. In questo modo, il collector del primo interrompe la ricezione degli eventi e il servizio di "audit" entra in stato di errore. Per evitare questo problema, configurare ogni SVM in un singolo ambiente. 7. Questo errore può verificarsi anche se le policy di servizio non sono configurate correttamente. Con ONTAP 9.8 o versione successiva, per connettersi al Data Source Collector, è necessario il servizio client data-fpolicy insieme al servizio dati data-nfs e/o data-cifs. Inoltre, il servizio data-fpolicy-client deve essere associato ai lif di dati per la SVM monitorata.	Nessun evento visualizzato nella pagina delle attività.

Problema:	Risoluzione:
1. Verificare che ONTAP Collector sia in esecuzione. In caso affermativo, assicurarsi che alcuni eventi cifs vengano generati sulle macchine virtuali del client cifs aprendo alcuni file. 2. Se non vengono visualizzate attività, accedere a SVM e immettere il seguente comando. *<SVM> ftllog show -source fpolicy* assicurarsi che non ci siano errori relativi a fpolicy. 3. Se non vengono visualizzate attività, accedere a SVM. Immettere il seguente comando *<SVM> policy show* controllare se la policy fpolicy denominata con il prefisso "cloudSecure_" è stata impostata e lo stato è "on". Se non impostato, molto probabilmente l'agente non è in grado di eseguire i comandi nella SVM. Assicurarsi di aver seguito tutti i prerequisiti descritti all'inizio della pagina.	SVM Data Collector si trova in stato di errore e il messaggio di errore indica che l'agente non è riuscito a connettersi al collector.
1. Molto probabilmente l'Agente è sovraccarico e non riesce a connettersi ai Data Source collettori. 2. Verificare quanti Data Source collettori sono connessi all'Agente. 3. Controllare anche la velocità di flusso dei dati nella pagina "All Activity" (tutte le attività) dell'interfaccia utente. 4. Se il numero di attività al secondo è significativamente elevato, installare un altro Agent e spostare alcuni Data Source Collector nel nuovo Agent.	SVM Data Collector visualizza il messaggio di errore "fpolicy.server.connectError: Node failed to stabiling a Connection with the FPolicy server "12.195.15.146" (Reason: "Select Timed out")"
Il firewall è attivato in SVM/Cluster. Pertanto, il motore fpolicy non è in grado di connettersi al server fpolicy. I CLIS in ONTAP che possono essere utilizzati per ottenere ulteriori informazioni sono: Registro eventi show -source fpolicy che mostra il registro eventi di errore show -source fpolicy -fields event,action,description che mostra ulteriori dettagli."Controllare i comandi del firewall" Sul lato ONTAP.	Messaggio di errore: "Il connettore è in stato di errore. Nome del servizio:audit. Motivo del guasto: Nessuna interfaccia dati valida (ruolo: Dati, protocolli dati: NFS o CIFS o entrambi, stato: Up) trovata su SVM."
Assicurarsi che sia presente un'interfaccia operativa (con ruolo di protocollo dati e dati come CIFS/NFS).	Il data collector passa allo stato di errore, quindi PASSA ALLO stato DI ESECUZIONE dopo un certo periodo di tempo, quindi torna a Error. Questo ciclo si ripete.
Ciò si verifica in genere nel seguente scenario: 1. Sono stati aggiunti più data colleziones. 2. I data collezioner che mostrano questo tipo di comportamento avranno 1 SVM aggiunto a questi data collezioner. Ciò significa che 2 o più data collezioner sono collegati a 1 SVM. 3. Assicurarsi che 1 data collector si connetta a una sola SVM. 4. Eliminare gli altri data collezioner collegati alla stessa SVM.	Il connettore è in stato di errore. Nome del servizio: Audit. Motivo dell'errore: Configurazione non riuscita (policy su SVM svmname. Motivo: Valore non valido specificato per l'elemento 'shares-to-include' all'interno di 'fpolicy.policy.scope-modify: "Federal"

Problema:	Risoluzione:
I nomi delle condivisioni devono essere forniti senza virgolette. Modificare la configurazione DSC SVM ONTAP per correggere i nomi delle condivisioni. *Include ed exclude share* non è destinato a un lungo elenco di nomi di share. Utilizzare invece il filtraggio per volume se si dispone di un elevato numero di condivisioni da includere o escludere.	Nel cluster sono presenti fpolicy inutilizzate. Cosa fare con quelli prima dell'installazione di workload Security?
Si consiglia di eliminare tutte le impostazioni fpolicy inutilizzate esistenti anche se si trovano in stato disconnesso. Workload Security creerà fpolicy con il prefisso "cloudSecure_". Tutte le altre configurazioni fpolicy inutilizzate possono essere eliminate. Comando CLI per visualizzare l'elenco fpolicy: *Fpolicy show* passi per eliminare le configurazioni fpolicy: *Fpolicy disable -vserver <svmname> -policy-name <policy_name> fpolicy policy policy policy scope delete -vserver <svmname> -policy-name <policy_name> fpolicy policy policy delete -vserver <svmname> <event_list> -policy-name <policy_name> <svmname>* _fpolicy policy policy event delete -vserver <svmname> <engine_name> -nome-motore-esterno -server_vpolicy	Dopo aver attivato la sicurezza dei workload, le performance di ONTAP ne risentono: La latenza diventa sporadicamente elevata, gli IOPS diventano sporadicamente bassi.
Mentre si utilizza ONTAP con sicurezza del carico di lavoro, a volte i problemi di latenza possono essere riscontrati in ONTAP. Le ragioni possibili sono diverse, come indicato di seguito: "1372994", "1415152", "1438207", "1479704", "1354659". Tutti questi problemi sono stati risolti in ONTAP 9.13.1 e versioni successive; si consiglia vivamente di utilizzare una di queste versioni successive.	Data Collector in error, visualizza questo messaggio di errore. "Errore: Il connettore è in stato di errore. Nome del servizio: Audit. Motivo dell'errore: Impossibile configurare il criterio su SVM svm_test. Motivo: Valore mancante per il campo zapi: Eventi. "
Inizia con una nuova SVM con solo il servizio NFS configurato. Aggiungere un data collector SVM ONTAP in sicurezza del carico di lavoro. CIFS viene configurato come protocollo consentito per SVM mentre si aggiunge il Data Collector SVM ONTAP in sicurezza del carico di lavoro. Attendere che il Data Collector in workload Security visualizzi un errore. Poiché il server CIFS NON è configurato su SVM, questo errore, come mostrato a sinistra, viene visualizzato da workload Security. Modificare il data collector ONTAP SVM e deselezionare CIFS come protocollo consentito. Salvare il data collector. Verrà avviato solo con il protocollo NFS attivato.	Data Collector visualizza il messaggio di errore: "Errore: Impossibile determinare lo stato di salute del raccoglitore entro 2 tentativi, provare a riavviare nuovamente il Collector (codice di errore: AGENT008)".

Se i problemi persistono, accedere ai collegamenti di supporto indicati nella pagina **Guida > supporto**.

Configurazione di Cloud Volumes ONTAP e Amazon FSX per NetApp ONTAP Collector

Workload Security utilizza i data colleator per raccogliere i dati di accesso ai file e agli

utenti dai dispositivi.

Configurazione dello storage Cloud Volumes ONTAP

Consultare la documentazione di OnCommand Cloud Volumes ONTAP per configurare un'istanza di ha AWS a nodo singolo per ospitare l'agente di sicurezza del carico di lavoro:https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html[]

Una volta completata la configurazione, seguire la procedura per configurare SVM:https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html[]

Piattaforme supportate

- Cloud Volumes ONTAP, supportato in tutti i provider di servizi cloud disponibili, ovunque sia disponibile. Ad esempio: Amazon, Azure, Google Cloud.
- ONTAP, Amazon FSX

Configurazione del computer dell'agente

Il computer dell'agente deve essere configurato nelle rispettive subnet dei provider di servizi cloud. Per ulteriori informazioni sull'accesso alla rete, consultare [requisiti dell'agente].

Di seguito sono riportati i passaggi per l'installazione dell'agente in AWS. Per l'installazione, è possibile seguire procedure equivalenti, applicabili al provider di servizi cloud, in Azure o Google Cloud.

In AWS, attenersi alla seguente procedura per configurare il computer in modo che venga utilizzato come agente di sicurezza del carico di lavoro:

Per configurare il computer in modo che venga utilizzato come agente di sicurezza del carico di lavoro, procedere come segue:

Fasi

1. Accedere alla console AWS, accedere alla pagina EC2-Instances e selezionare *Launch instance*.
2. Selezionare un file RHEL o CentOS AMI con la versione appropriata, come indicato in questa pagina:https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html[]
3. Selezionare il VPC e la subnet in cui risiede l'istanza di Cloud ONTAP.
4. Selezionare *t2.xlarge* (4 vcpus e 16 GB di RAM) come risorse allocate.
    a. Creare l'istanza EC2.
5. Installare i pacchetti Linux richiesti utilizzando il gestore dei pacchetti YUM:
    a. Installare *wget* e *unzip* pacchetti Linux nativi.

Installare Workload Security Agent

1. Accedere come amministratore o come proprietario dell'account all'ambiente Cloud Insights.
2. Accedere a sicurezza del carico di lavoro **Collectors** e fare clic sulla scheda **Agenti**.
3. Fare clic su **+Agent** e specificare RHEL come piattaforma di destinazione.
4. Copiare il comando Installazione agente.
5. Incollare il comando Installazione agente nell'istanza RHEL EC2 a cui si è connessi. In questo modo viene installato l'agente workload Security, fornendo tutte le funzioni di "Prerequisiti dell'agente" sono soddisfatti.

Per informazioni dettagliate, fare riferimento a questo xref:./ https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent

Risoluzione dei problemi

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema	Risoluzione
"Sicurezza del carico di lavoro: Impossibile determinare il tipo di ONTAP per il data collector Amazon FxSN" viene visualizzato dal Data Collector." Il cliente non riesce ad aggiungere il nuovo data collector Amazon FSxN in workload Security. La connessione al cluster FSxN sulla porta 443 dell'agente è in timeout. I gruppi di protezione firewall e AWS dispongono delle regole necessarie per consentire la comunicazione. Un agente è già implementato e si trova nello stesso account AWS. Lo stesso agente viene utilizzato per connettere e monitorare i dispositivi NetApp rimanenti (e tutti funzionano).	Risolvere questo problema aggiungendo il segmento di rete LIF fsxadmin alla regola di sicurezza dell'agente. Permesso a tutte le porte se non si è sicuri delle porte.

Gestione utenti

Workload gli account utente di sicurezza vengono gestiti tramite Cloud Insights.

Cloud Insights offre quattro livelli di account utente: Proprietario dell'account, amministratore, utente e ospite. A ciascun account vengono assegnati livelli di autorizzazione specifici. Un account utente con privilegi di amministratore può creare o modificare gli utenti e assegnare a ciascun utente uno dei seguenti ruoli di workload Security:

Ruolo	Accesso alla sicurezza del carico di lavoro
Amministratore	È in grado di eseguire tutte le funzioni di workload Security, incluse quelle per Avvisi, analisi, raccolta dati, policy di risposta automatizzate e API per workload Security. Un amministratore può anche invitare altri utenti, ma può assegnare solo ruoli di sicurezza del carico di lavoro.
Utente	Consente di visualizzare e gestire gli avvisi e visualizzare le analisi. Il ruolo dell'utente può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente e limitare l'accesso dell'utente.
Ospite	Consente di visualizzare avvisi e analisi. Il ruolo ospite non può modificare lo stato degli avvisi, aggiungere una nota, creare snapshot manualmente o limitare l'accesso dell'utente.

Fasi

1. Accedere a workload Security

2. Nel menu, fare clic su **Admin > User Management**

   Sarai inoltrato alla pagina User Management di Cloud Insights.

3. Selezionare il ruolo desiderato per ciascun utente.

Durante l'aggiunta di un nuovo utente, è sufficiente selezionare il ruolo desiderato (di solito utente o ospite).

Ulteriori informazioni sugli account utente e sui ruoli sono disponibili in Cloud Insights "Ruolo dell'utente" documentazione.

SVM Event Rate Checker (Guida al dimensionamento dell'agente)

La funzione di verifica del tasso di eventi viene utilizzata per controllare la velocità di eventi combinata NFS/SMB nella SVM prima di installare un data collector SVM ONTAP, per verificare il numero di macchine SVM che un agente è in grado di monitorare. Utilizza Event Rate Checker come guida al dimensionamento per pianificare il tuo ambiente di sicurezza.

Un agente può supportare fino a un massimo di 50 raccoglitori di dati.

Requisiti:

- IP del cluster
- Nome utente e password dell'amministratore del cluster

> Durante l'esecuzione di questo script, non deve essere eseguito alcun Data Collector SVM ONTAP per la SVM per la quale viene determinata la frequenza degli eventi.

Fasi:

1. Installare l'Agent seguendo le istruzioni in CloudSecure.
2. Una volta installato l'agente, eseguire lo script *server_data_rate_checker.sh* come utente sudo:

```
 /opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
. Questo script richiede l'installazione di _sshpass_ nella macchina
linux. Esistono due modi per installarlo:
```

   a. Eseguire il seguente comando:

```
 linux_prompt> yum install sshpass
.. Se questo non funziona, scaricare _sshpass_ sulla macchina linux
dal web ed eseguire il seguente comando:
```

```
linux_prompt> rpm -i sshpass
```

3. Fornire i valori corretti quando richiesto. Per un esempio, vedere di seguito.
4. L'esecuzione dello script richiede circa 5 minuti.
5. Al termine dell'esecuzione, lo script stampa la frequenza degli eventi dalla SVM. È possibile controllare il tasso di eventi per SVM nell'output della console:

```
"Svm svm_rate is generating 100 events/sec".
```

Ciascun Data Collector SVM di ONTAP può essere associato a una singola SVM, il che significa che ciascun data collector potrà ricevere il numero di eventi generati da una singola SVM.

Tenere presente quanto segue:

A) utilizzare questa tabella come guida generale al dimensionamento. È possibile aumentare il numero di core e/o memoria per aumentare il numero di data collector supportati, fino a un massimo di 50 data collector:

Configurazione del computer dell'agente	Numero di Data Collector SVM	Tasso massimo di eventi che il computer dell'agente può gestire
4 core, 16 GB	10 raccolta di dati	20.000 eventi/sec
4 core, 32 GB	20 raccolta di dati	20.000 eventi/sec

B) per calcolare il totale degli eventi, aggiungere gli eventi generati per tutte le SVM per quell'agente.

C) se lo script non viene eseguito durante le ore di punta o se il traffico di picco è difficile da prevedere, mantenere un buffer del tasso di eventi del 30%.

B + C deve essere inferiore A A, altrimenti il computer dell'agente non potrà eseguire il monitoraggio.

In altre parole, il numero di raccolta dati che è possibile aggiungere a una macchina a singolo agente deve essere conforme alla formula seguente:

```
 Sum of all Event rate of all Data Source Collectors + Buffer Event rate
of 30% < 20000 events/second
Vedere xref:{relative_path}concept_cs_agent_requirements.html["Requisiti
dell'agente"] pagina per ulteriori prerequisiti e requisiti.
```

Esempio

Diciamo che abbiamo tre SVM che generano percentuali di eventi rispettivamente di 100, 200 e 300 eventi al secondo.

Applichiamo la formula:

```
 (100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored
via one agent box.
```

L'output della console è disponibile nella macchina Agente nel nome del file *fpolicy_stat_<SVM Name>.log* nella directory di lavoro corrente.

Lo script può fornire risultati errati nei seguenti casi:

- Vengono fornite credenziali, IP o nome SVM errati.
- Un fpolicy già esistente con lo stesso nome, numero di sequenza, ecc. genera un errore.
- Lo script viene arrestato bruscamente durante l'esecuzione.

Di seguito è riportato un esempio di esecuzione di script:

```
[root@ci-cs-data agent]#
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166
Enter the username to SSH: admin
Enter the password:
Getting event rate for NFS and SMB events.
Available SVMs in the Cluster
-----------------------------
QA_SVM
Stage_SVM
Qa-fas8020
Qa-fas8020-01
Qa-fas8020-02
audit_svm
svm_rate
vs_new
vs_new2
```

```
-----------------------------
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec
```

```
[root@ci-cs-data agent]#
```

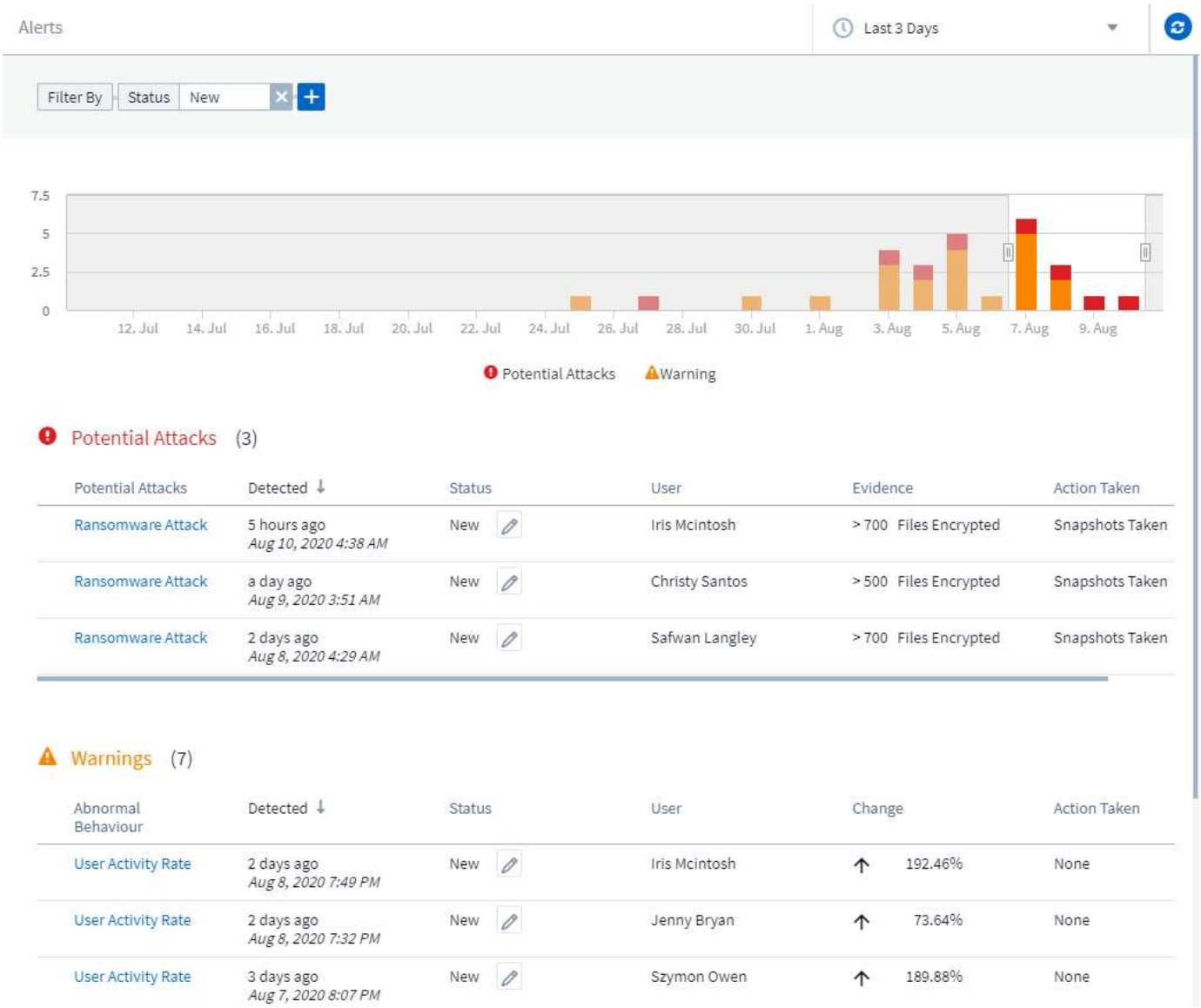
Risoluzione dei problemi

Domanda	Risposta
Se si esegue questo script su una SVM già configurata per la sicurezza del carico di lavoro, viene utilizzata solo la configurazione fpolicy esistente sulla SVM oppure viene impostata una configurazione temporanea ed è possibile eseguire il processo?	La funzione Event Rate Checker può essere eseguita correttamente anche per una SVM già configurata per la sicurezza del carico di lavoro. Non dovrebbe esserci alcun impatto.
È possibile aumentare il numero di SVM su cui è possibile eseguire lo script?	Sì. È sufficiente modificare lo script e modificare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se si aumenta il numero di SVM, si aumenterà il tempo di esecuzione dello script?	No Lo script viene eseguito per un massimo di 5 minuti, anche se il numero di SVM aumenta.
È possibile aumentare il numero di SVM su cui è possibile eseguire lo script?	Sì. È necessario modificare lo script e modificare il numero massimo di SVM da 5 a qualsiasi numero desiderato.
Se si aumenta il numero di SVM, si aumenterà il tempo di esecuzione dello script?	No Lo script viene eseguito per un massimo di 5 minuti, anche se il numero di SVM viene aumentato.
Cosa succede se si esegue Event Rate Checker con un agente esistente?	L'esecuzione di Event Rate Checker con un agente già esistente può causare un aumento della latenza sulla SVM. Questo aumento sarà temporaneo durante l'esecuzione di Event Rate Checker.

Avvisi

La pagina Workload Security Alerts (Avvisi di sicurezza del carico di lavoro) mostra una tempistica degli attacchi e/o degli avvisi recenti e consente di visualizzare i dettagli relativi a ciascun problema.

La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.



Avviso

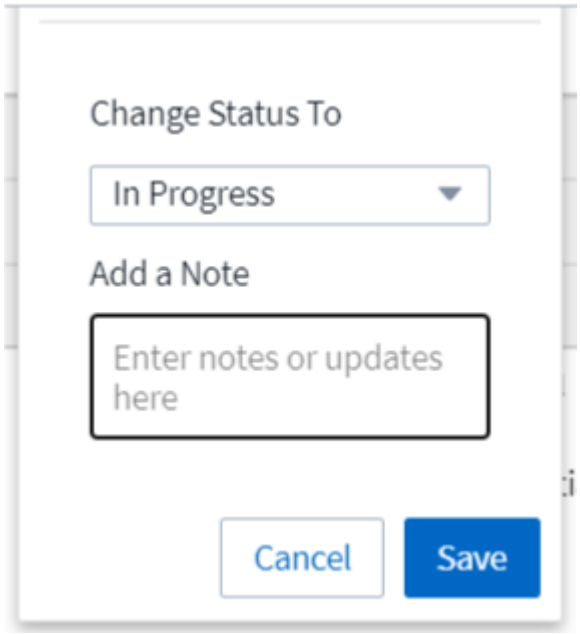
L'elenco degli avvisi visualizza un grafico che mostra il numero totale di potenziali attacchi e/o avvisi che sono stati generati nell'intervallo di tempo selezionato, seguito da un elenco degli attacchi e/o avvisi che si sono verificati in quell'intervallo di tempo. È possibile modificare l'intervallo di tempo regolando i cursori ora di inizio e ora di fine nel grafico.

Per ogni avviso viene visualizzato quanto segue:

Potenziali attacchi:

- Il tipo di *potenziale attacco* (ad esempio ransomware o Sabotage)
- La data e l'ora in cui il potenziale attacco è stato *rilevato*
- Il *Stato* dell'avviso:
  - **Nuovo**: Impostazione predefinita per i nuovi avvisi.
  - **In corso**: L'avviso è sotto esame da uno o più membri del team.
  - **Resolved**: L'avviso è stato contrassegnato come risolto da un membro del team.
  - **Respinto**: L'avviso è stato respinto come comportamento falso positivo o previsto.

  Un amministratore può modificare lo stato dell'avviso e aggiungere una nota per agevolare l'analisi.



- L' *utente* il cui comportamento ha attivato l'avviso
- *Prova* dell'attacco (ad esempio, un gran numero di file è stato crittografato)
- L' *azione intrapresa* (ad esempio, è stata scattata una snapshot)

Avvertenze:

- Il *comportamento anomalo* che ha attivato l'avviso
- La data e l'ora in cui il comportamento è stato *rilevato*
- Il *Stato* dell'avviso (nuovo, in corso, ecc.)
- L' *utente* il cui comportamento ha attivato l'avviso
- Una descrizione di *Change* (ad esempio, un aumento anomalo dell'accesso al file)
- L' *azione intrapresa*

Opzioni filtro

È possibile filtrare gli avvisi in base a quanto segue:

- Il *Stato* dell'avviso

- Testo specifico nella *Nota*
- Il tipo di *attacchi/Avvertenze*
- L' *utente* le cui azioni hanno attivato l'avviso/avviso

La pagina Dettagli avviso

È possibile fare clic su un collegamento di avviso nella pagina dell'elenco degli avvisi per aprire una pagina dei dettagli per l'avviso. I dettagli degli avvisi possono variare in base al tipo di attacco o avviso. Ad esempio, una pagina dei dettagli di un attacco ransomware potrebbe mostrare le seguenti informazioni:

Sezione riepilogativa:

- Tipo di attacco (ransomware, Sabotage) e ID avviso (assegnato da workload Security)
- Data e ora in cui è stato rilevato l'attacco
- Azione intrapresa (ad esempio, è stata eseguita una snapshot automatica. L'ora dell'istantanea viene visualizzata immediatamente sotto la sezione riepilogativa)
- Stato (nuovo, in corso, ecc.)

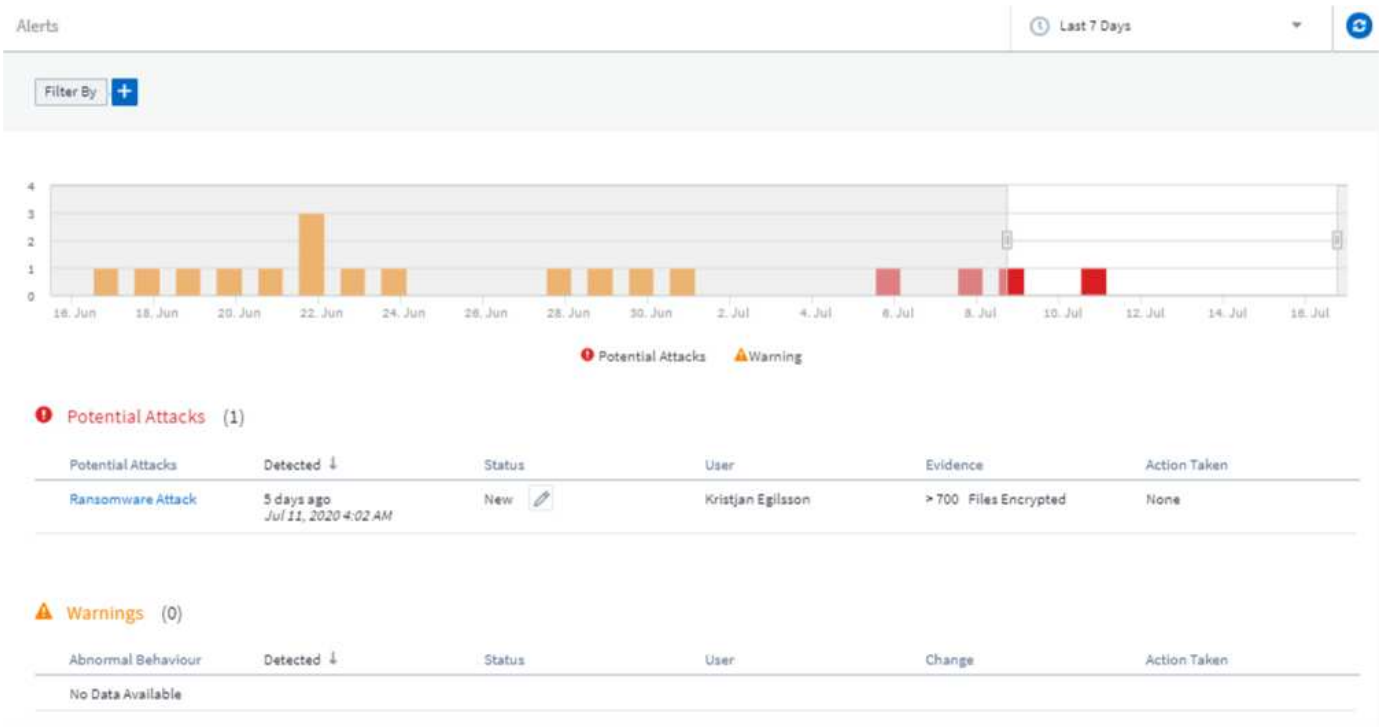
Sezione dei risultati degli attacchi:

- Numero di volumi e file interessati
- Un riepilogo del rilevamento
- Un grafico che mostra l'attività del file durante l'attacco

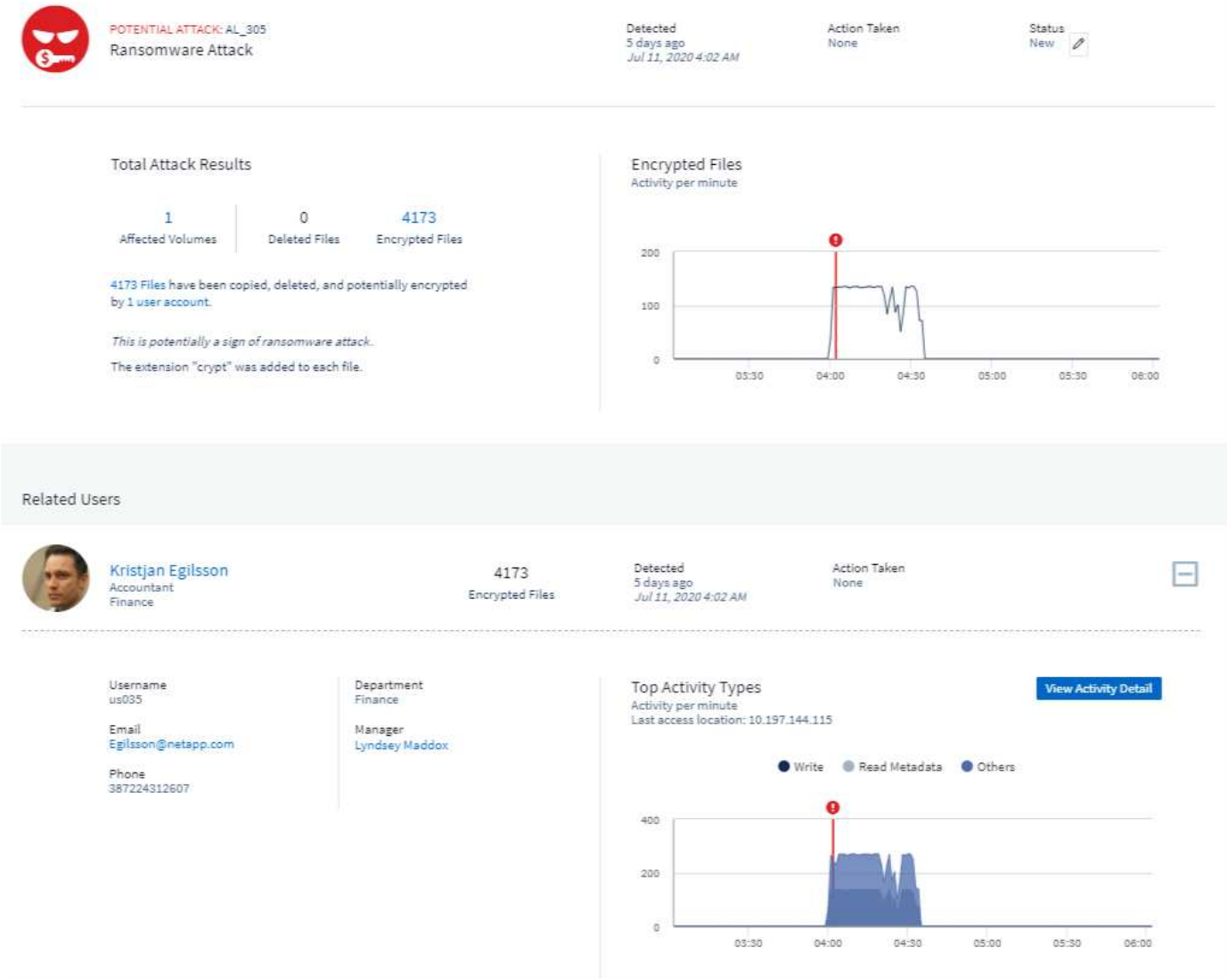
Sezione utenti correlati:

Questa sezione mostra i dettagli relativi all'utente coinvolto nel potenziale attacco, incluso un grafico delle attività principali per l'utente.

Pagina Alerts (questo esempio mostra un potenziale attacco ransomware):



Pagina dei dettagli (questo esempio mostra un potenziale attacco ransomware):

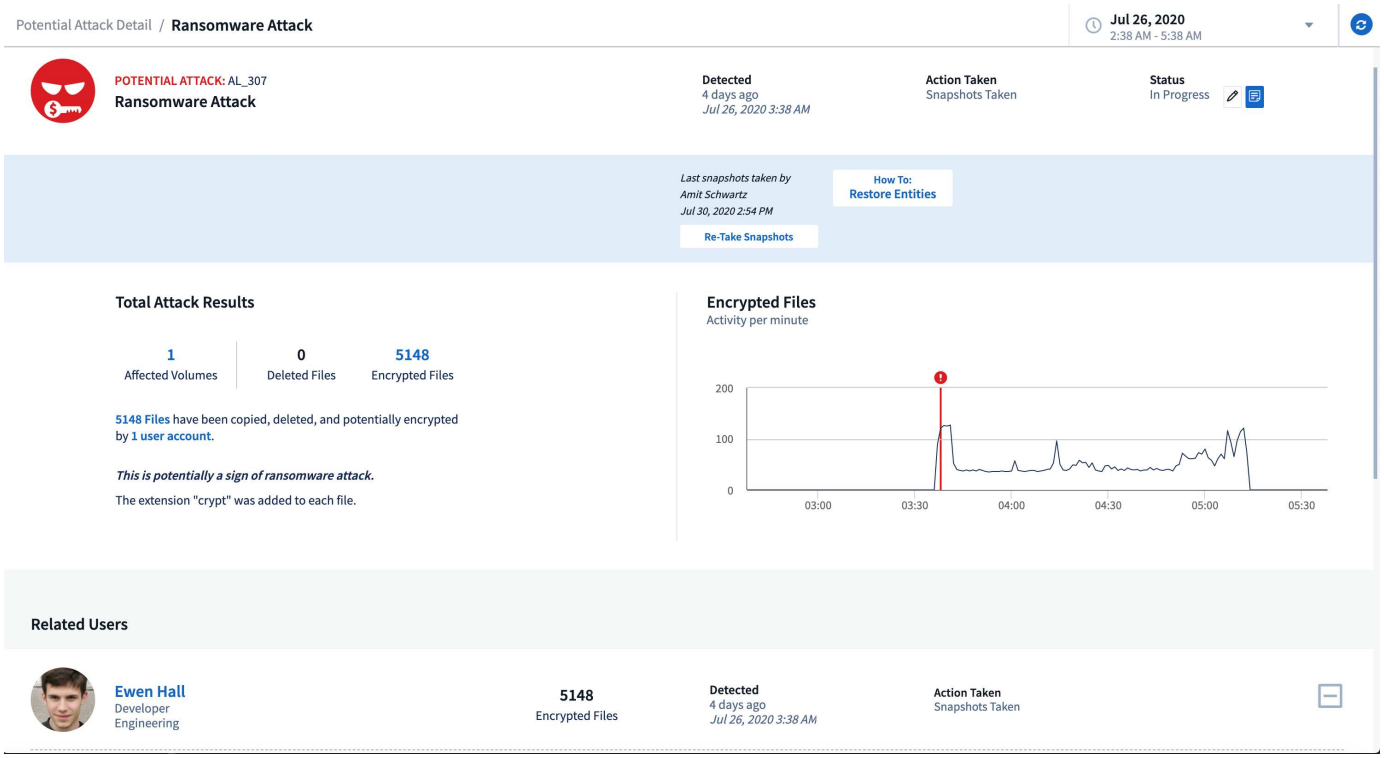


Eseguire un'azione Snapshot

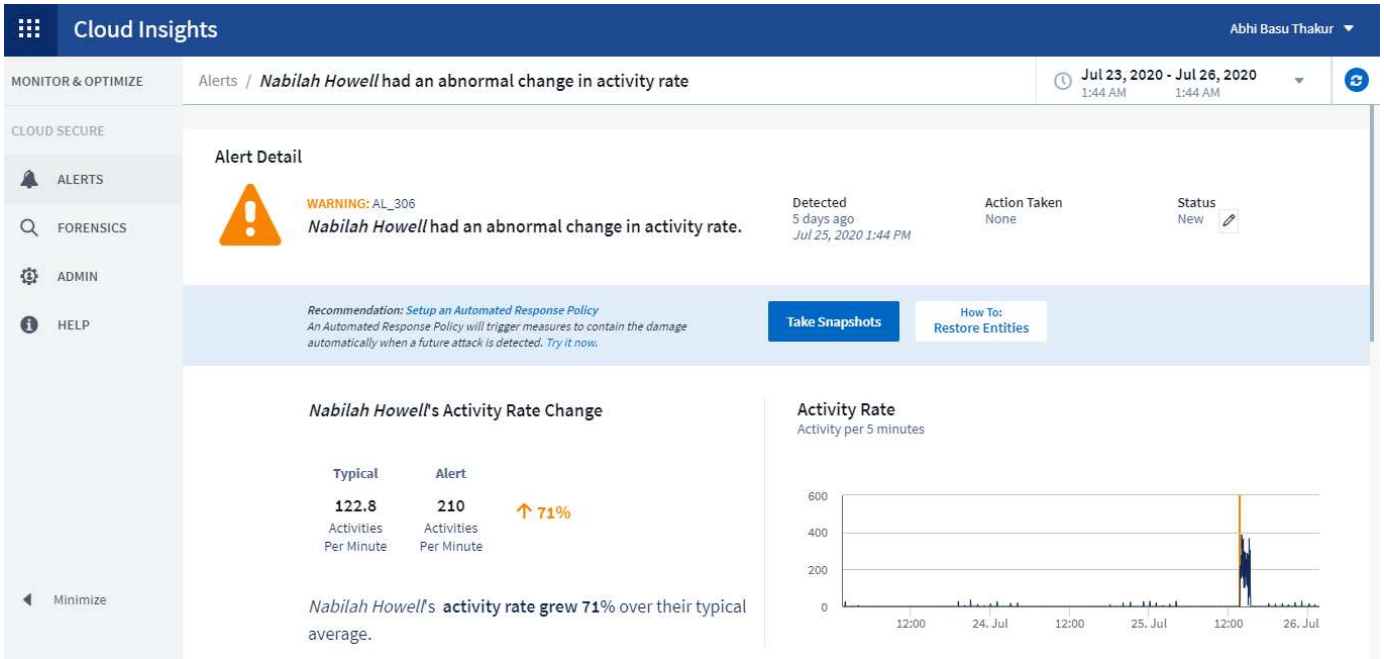
Workload Security protegge i tuoi dati eseguendo automaticamente un'istantanea quando vengono rilevate attività dannose, garantendo un backup sicuro dei tuoi dati.

È possibile definire "policy di risposta automatizzate" che prendono un'istantanea quando viene rilevato un attacco ransomware o un'altra attività utente anomala. È anche possibile acquisire un'istantanea manualmente dalla pagina di avviso.

Snapshot
automatica:



Snapshot manuale:



Notifiche di avviso

Le notifiche e-mail degli avvisi vengono inviate a un elenco di destinatari degli avvisi per ogni azione dell'avviso. Per configurare i destinatari degli avvisi, fare clic su **Admin > Notifiche** e inserire un indirizzo e-mail per ciascun destinatario.

Policy di conservazione

Gli avvisi e le avvertenze vengono conservati per 13 mesi. Gli avvisi e le avvertenze di età superiore a 13 mesi

verranno eliminati. Se si elimina l'ambiente workload Security, vengono eliminati anche tutti i dati associati all'ambiente.

Risoluzione dei problemi

Problema:	Prova:
Esiste una situazione in cui ONTAP esegue snapshot orarie al giorno. Le snapshot di workload Security (WS) ne influenzeranno? WS Snapshot prenderà lo snapshot orario? Lo snapshot orario predefinito viene arrestato?	Le snapshot di workload Security non influiscono sulle snapshot orarie. Le snapshot WS non acquisiranno lo spazio orario delle snapshot e questo dovrebbe continuare come prima. Lo snapshot orario predefinito non viene arrestato.
Cosa accade se viene raggiunto il numero massimo di snapshot in ONTAP?	Se viene raggiunto il numero massimo di snapshot, l'acquisizione successiva di Snapshot non riesce e Workload Security visualizza un messaggio di errore che indica che Snapshot è pieno. L'utente deve definire le policy di Snapshot per eliminare le snapshot meno recenti, altrimenti non verranno eseguite. In ONTAP 9.3 e versioni precedenti, un volume può contenere fino a 255 copie Snapshot. In ONTAP 9.4 e versioni successive, un volume può contenere fino a 1023 copie Snapshot. Per informazioni su, consultare la documentazione di ONTAP "Impostazione del criterio di eliminazione Snapshot".
Workload Security non è in grado di acquisire snapshot.	Assicurarsi che il ruolo utilizzato per creare snapshot abbia il xref:./ proper diritti assegnati. Assicurarsi che *csrole* sia creato con i diritti di accesso appropriati per lo snapshot: Ruolo di login di sicurezza create -vserver <vservername> -role csrole -cmddirname "volume snapshot" -access all
Gli snapshot non riescono per gli avvisi precedenti sulle SVM che sono stati rimossi da workload Security e successivamente aggiunti di nuovo. Per i nuovi avvisi che si verificano dopo l'aggiunta di SVM, vengono create delle istantanee.	Si tratta di uno scenario raro. In caso di problemi, accedere a ONTAP e acquisire manualmente le istantanee per gli avvisi precedenti.
Nella pagina *Dettagli avviso*, sotto il pulsante *Esegui snapshot* viene visualizzato il messaggio di errore "ultimo tentativo non riuscito". Passando il mouse sull'errore viene visualizzato il messaggio "Invoke API command has timeout for the data collector with id" (il comando API Invoke è scaduto per il data collector con id).	Questo può accadere quando un data collector viene aggiunto alla sicurezza del carico di lavoro tramite l'IP di gestione SVM, se la LIF della SVM è nello stato *disabled* in ONTAP. Attivare la LIF specifica in ONTAP e attivare *Take Snapshot Manually* dalla sicurezza del carico di lavoro. L'azione Snapshot avrà esito positivo.

Analisi

Forensics - tutte le attività

La pagina All Activity (tutte le attività) consente di comprendere le azioni eseguite sulle entità nell'ambiente workload Security.

Esame di tutti i dati delle attività

Fare clic su **Forensics > Activity Forensics** (analisi > analisi delle attività) e fare clic sulla scheda **All Activity** (tutte le attività) per accedere alla pagina All Activity (tutte le attività). Questa pagina fornisce una panoramica delle attività nel proprio ambiente, evidenziando le seguenti informazioni:

- Un grafico che mostra *Cronologia attività* (accessibile al minuto/ogni 5 minuti/ogni 10 minuti in base all'intervallo di tempo globale selezionato)

  È possibile ingrandire il grafico trascinando un rettangolo nel grafico. L'intera pagina viene caricata per visualizzare l'intervallo di tempo di zoom. Quando si esegue lo zoom avanti, viene visualizzato un pulsante che consente all'utente di eseguire lo zoom indietro.

- Un grafico di *tipi di attività*. Per ottenere i dati della cronologia delle attività in base al tipo di attività, fare clic sul link corrispondente all'etichetta dell'asse X.
- Un grafico delle attività su *tipi di entità*. Per ottenere i dati della cronologia delle attività in base al tipo di entità, fare clic sul link corrispondente all'etichetta dell'asse X.
- Un elenco dei dati di *tutte le attività*

La tabella **tutte le attività** mostra le seguenti informazioni. Nota: Non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare facendo clic sull'icona "ingranaggio" .

- L'ora * in cui è stato effettuato l'accesso a un'entità, inclusi l'anno, il mese, il giorno e l'ora dell'ultimo accesso.
- Il **utente** che ha effettuato l'accesso all'entità con un collegamento a "Informazioni sull'utente".
- L'attività * eseguita dall'utente. I tipi supportati sono:
  - **Cambia proprietà del gruppo** - la proprietà del gruppo è del file o della cartella è stata modificata. Per ulteriori informazioni sulla proprietà del gruppo, consulta "questo link."
  - **Cambia proprietario** - la proprietà del file o della cartella viene modificata in un altro utente.
  - **Cambia permesso** - l'autorizzazione per file o cartelle viene modificata.
  - **Crea** - Crea file o cartella.
  - **Delete** - Elimina file o cartella. Se una cartella viene eliminata, si ottengono gli eventi *delete* per tutti i file in quella cartella e sottocartelle.
  - **Read** - il file viene letto.
  - **Read Metadata** - solo se si attiva l'opzione di monitoraggio delle cartelle. Verrà generato all'apertura di una cartella su Windows o all'esecuzione di "ls" all'interno di una cartella in Linux.
  - **Rinomina** - Rinomina il file o la cartella.
  - **Write** - i dati vengono scritti in un file.
  - **Write Metadata** - i metadati del file vengono scritti, ad esempio, i permessi modificati.
  - **Altra modifica** - qualsiasi altro evento non descritto in precedenza. Tutti gli eventi non mappati vengono mappati al tipo di attività "Altro cambiamento". Applicabile a file e cartelle.
- Il percorso * all'entità con un collegamento a. "Dati di dettaglio dell'entità"
- Il **Entity Type**, inclusa l'estensione dell'entità (ad es. File) (.doc, .docx, .tmp, ecc.)
- Il **dispositivo** in cui risiedono le entità

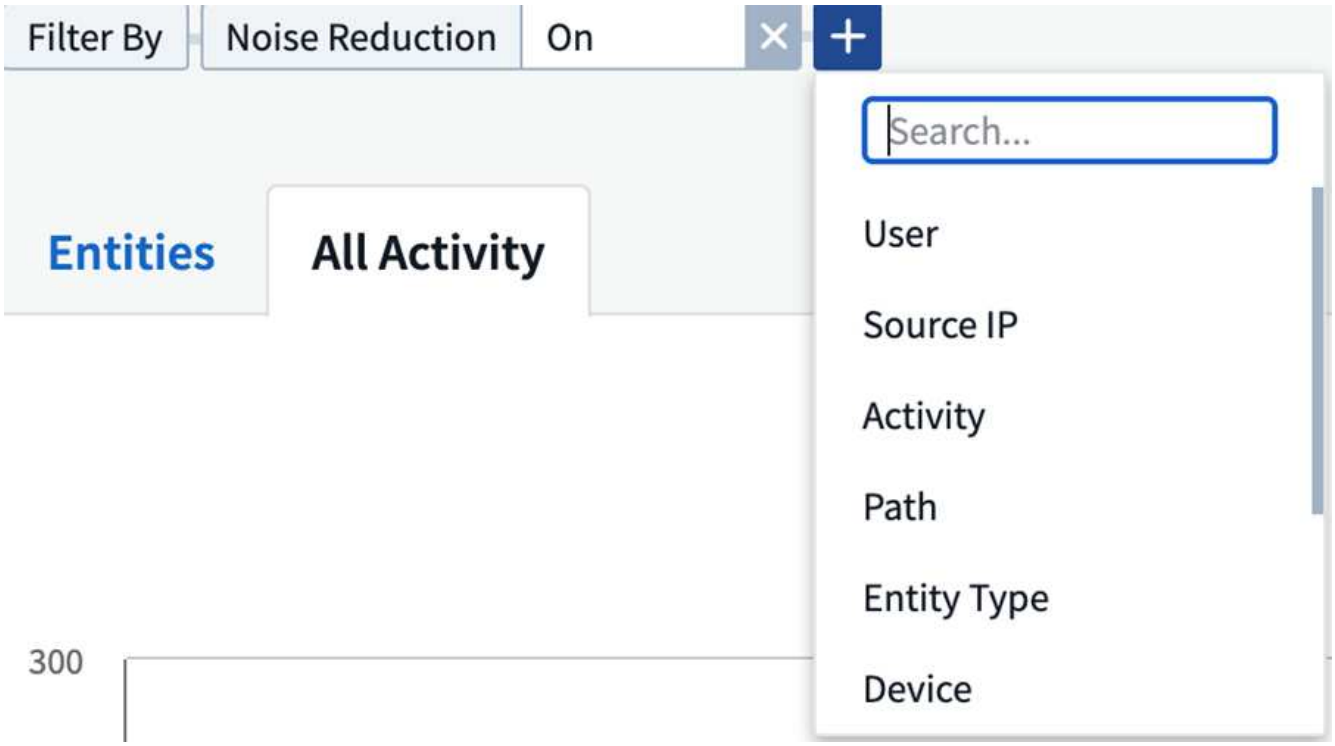
- Il **protocollo** utilizzato per recuperare gli eventi.
- Il percorso **originale** utilizzato per rinominare gli eventi quando il file originale è stato rinominato. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.
- Il **Volume** in cui risiedono le entità. Questa colonna non è visibile nella tabella per impostazione predefinita. Utilizzare il selettore di colonna per aggiungere questa colonna alla tabella.

Filtraggio dei dati Forensic Activity History

Per filtrare i dati è possibile utilizzare due metodi.

1. Passare il mouse sul campo nella tabella e fare clic sull'icona del filtro visualizzata. Il valore viene aggiunto ai filtri appropriati nell'elenco *Filter by* principale.
2. Filtrare i dati digitando il campo *Filtra per*:

   Selezionare il filtro appropriato dal widget 'Filtra per' in alto facendo clic sul pulsante **[+]**:



   Inserire il testo di ricerca

   Premere Invio o fare clic all'esterno della casella del filtro per applicare il filtro.

È possibile filtrare i dati delle attività forensi in base ai seguenti campi:

- Il tipo **Activity**.
- **IP di origine** da cui è stato effettuato l'accesso all'entità. È necessario fornire un indirizzo IP di origine valido tra virgolette doppie, ad esempio "10.1.1.1". Gli IP incompleti come "10.1.1.**", "10.1.**.*", ecc. non funzionano.
- **Protocollo** per recuperare le attività specifiche del protocollo.
- **Nome utente** dell'utente che esegue l'attività. Specificare il nome utente esatto da filtrare. La ricerca con il

nome utente parziale o con il prefisso ‘*’ non funziona.

- **Riduzione del rumore** per filtrare i file creati nelle ultime 2 ore dall’utente. Viene inoltre utilizzato per filtrare i file temporanei (ad esempio, i file .tmp) a cui l’utente accede.

I seguenti campi sono soggetti a speciali regole di filtraggio:

- **Entity Type**, usando l’estensione dell’entità (file)
- **Percorso** dell’entità
- **Utente** che esegue l’attività
- **Dispositivo** (SVM) in cui risiedono le entità
- **Volume** dove risiedono le entità
- Il percorso **originale** utilizzato per rinominare gli eventi quando il file originale è stato rinominato.

I campi precedenti sono soggetti a quanto segue durante il filtraggio:

- Il valore esatto deve essere compreso tra virgolette: Esempio: "Searchtext"
- Le stringhe con caratteri jolly non devono contenere virgolette: Esempio: Searchtext, ‘s*searchtext*, filtrerà le stringhe contenenti il carattere 'earchtext'.
- Stringa con un prefisso, ad esempio: Searchtext* , cerca le stringhe che iniziano con ‘searchtext’.

Ordinamento dei dati Forensic Activity History

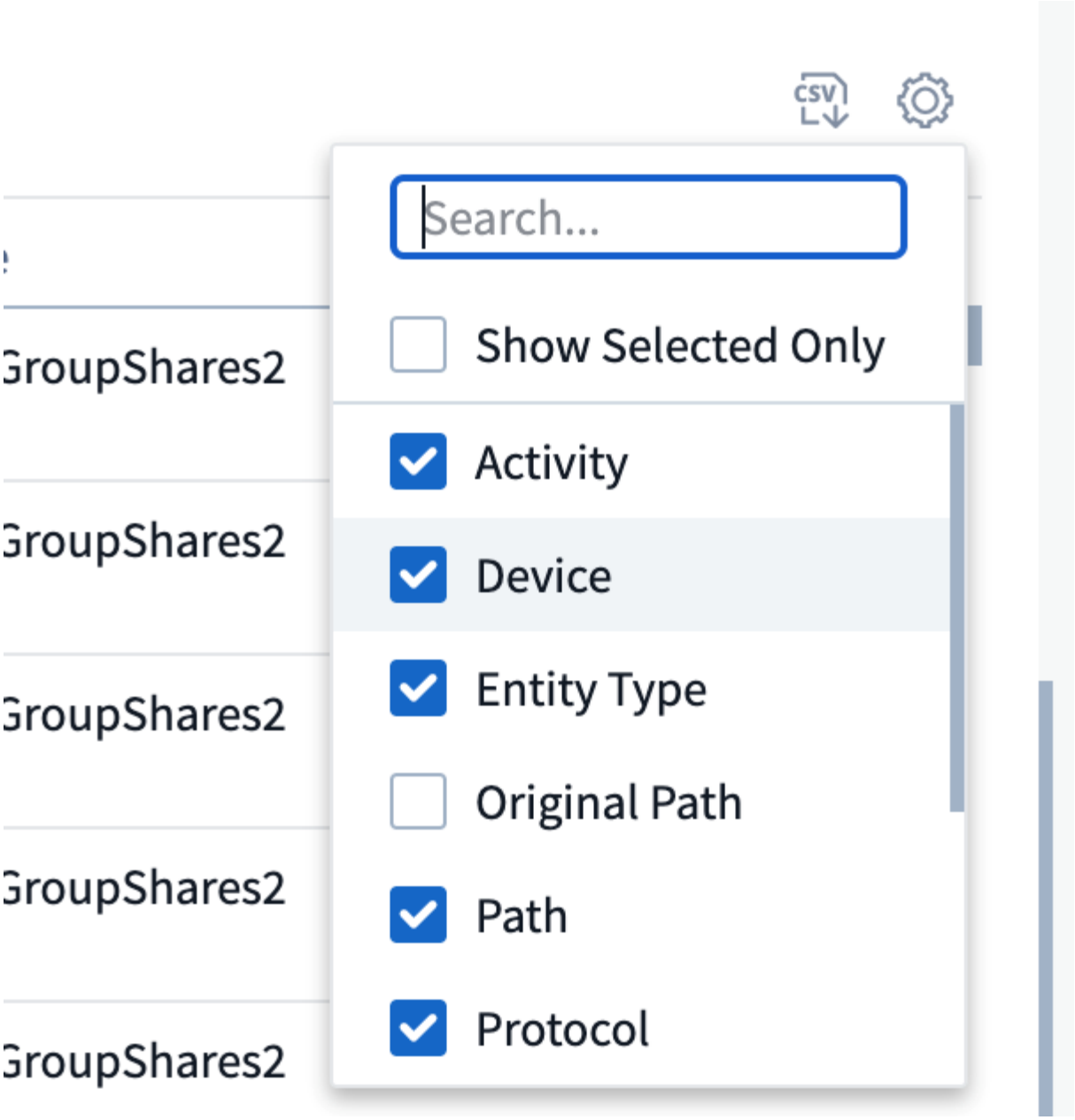
È possibile ordinare i dati della cronologia delle attività in base a *Time, User, Source IP, Activity, Path* e *Entity Type*. Per impostazione predefinita, la tabella viene ordinata in base a un ordine *time* decrescente, il che significa che i dati più recenti verranno visualizzati per primi. L’ordinamento è disattivato per i campi *Device* e *Protocol*.

Esportazione di tutte le attività

È possibile esportare la cronologia delle attività in un file .CSV facendo clic sul pulsante *Export* sopra la tabella Activity History (Cronologia attività). Si noti che vengono esportati solo i primi 100,000 record. A seconda della quantità di dati, l’esportazione potrebbe richiedere da pochi secondi a diversi minuti.

Selezione colonna per tutte le attività

La tabella *All activity* mostra le colonne Select per impostazione predefinita. Per aggiungere, rimuovere o modificare le colonne, fare clic sull’icona a forma di ingranaggio a destra della tabella e selezionare dall’elenco delle colonne disponibili.



Conservazione della cronologia delle attività

La cronologia delle attività viene mantenuta per 13 mesi per gli ambienti di sicurezza dei workload attivi.

Applicabilità dei filtri nella pagina Forensics

Filtro	Che cosa fa	Esempio	Quali filtri sono applicabili?	Non applicabile per i filtri	Risultato
* (Asterisco)	consente di cercare tutto	Auto*03172022	Utente, PERCORSO, tipo di entità, tipo di dispositivo, volume, Percorso originale		Restituisce tutte le risorse che iniziano con "Auto" e terminano con "03172022"

? (punto interrogativo)	consente di cercare un numero specifico di caratteri	AutoSabotageUser1_03172022?	Utente, tipo di entità, dispositivo, volume		Restituisce AutoSabotageUser1_03172022A, AutoSabotageUser1_03172022AB, AutoSabotageUser1_031720225 e così via
OPPURE	consente di specificare più entità	AutoSabotageUser1_03172022 O AutoRansomUser4_03162022	Utente, dominio, Nome utente, PERCORSO, tipo di entità, Periferica, percorso originale		Restituisce uno qualsiasi di AutoSabotageUser1_03172022 O AutoRansomUser4_03162022
NO	consente di escludere il testo dai risultati della ricerca	NON AutoRansomUser4_03162022	Utente, dominio, Nome utente, PERCORSO, tipo di entità, PERCORSO originale, Volume	Dispositivo	Restituisce tutto ciò che non inizia con "AutoRansomUser4_03162022"
Nessuno	Ricerca i valori NULL in tutti i campi	Nessuno	Dominio		restituisce risultati in cui il campo di destinazione è vuoto

Ricerca percorso / percorso originale

I risultati della ricerca con e senza / saranno diversi

/AutoDir1/AutoFile	Funziona
AutoDir1/Autofile	Non funziona
/AutoDir1/AutoFile (Dir1)	Dir1 la sottostringa parziale non funziona
"/AutoDir1/AutoFile03242022"	La ricerca esatta funziona
Auto*03242022	Non funziona
AutoSabotageUser1_03172022?	Non funziona
/AutoDir1/AutoFile03242022 O /AutoDir1/AutoFile03242022	Funziona
NON /AutoDir1/AutoFile03242022	Funziona
NON /AutoDir1	Funziona
NON /AutoFile03242022	Non funziona
*	Mostra tutte le voci

Risoluzione dei problemi

Problema	Provare
Nella tabella "tutte le attività", sotto la colonna ‘utente’, il nome utente viene visualizzato come: "ldap:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” o "ldap:default:80038003"	Possibili motivi: 1. Non è stato ancora configurato alcun servizio di raccolta elenchi in linea utenti. Per aggiungerne uno, andare a **sicurezza workload > Collector > User Directory Collector** e fare clic su **+User Directory Collector**. Scegliere *Active Directory* o *LDAP Directory Server*. 2. È stato configurato un User Directory Collector, ma si è arrestato o si trova in stato di errore. Andare a **Collector > User Directory Collectors** e controllare lo stato. Fare riferimento a. "Risoluzione dei problemi di User Directory Collector" sezione della documentazione per suggerimenti per la risoluzione dei problemi. Una volta eseguita la configurazione corretta, il nome verrà risolto automaticamente entro 24 ore. Se il problema persiste, verificare di aver aggiunto il Data Collector utente corretto. Assicurarsi che l’utente faccia effettivamente parte del server Active Directory/LDAP Directory aggiunto.
Alcuni eventi NFS non vengono visualizzati nell’interfaccia utente.	Controllare quanto segue: 1. È necessario eseguire un User Directory Collector per server ad con attributi POSIX impostati con l’attributo unixid attivato dall’interfaccia utente. 2. Qualsiasi utente che esegue l’accesso NFS deve essere visualizzato quando effettua una ricerca nella pagina utente dall’interfaccia utente 3. Gli eventi raw (eventi per i quali l’utente non è ancora stato scoperto) non sono supportati per NFS 4. L’accesso anonimo all’esportazione NFS non verrà monitorato. 5. Assicurarsi che la versione di NFS utilizzata sia inferiore a NFS4.1.

Dopo aver digitato alcune lettere contenenti un carattere jolly come l'asterisco (*) nei filtri delle pagine Forensics *All Activity* o *Entities*, le pagine vengono caricate molto lentamente.	Un asterisco (**) nella stringa di ricerca cerca tutto. Tuttavia, le stringhe con caratteri jolly come <searchTerm>** o *<searchTerm>* causano una query lenta. Per ottenere prestazioni migliori, utilizzare le stringhe di prefisso nel formato *<searchTerm>** (in altre parole, aggiungere l'asterisco (*) *dopo* un termine di ricerca). Esempio: Utilizzare la stringa *testvolume**, invece di **testvolume* o **test*volume*. Utilizza una ricerca basata su prefisso per visualizzare tutte le attività sotto una data cartella in modo ricorrente (ricerca gerarchica). ad esempio */path1/path2/path3* o *"/path1/path2/path3"* elenchiamo tutte le attività in modo ricorrente sotto */path1/path2/path3*. In alternativa, utilizzare l'opzione "Add to Filter" (Aggiungi al filtro) nella scheda All Activity (tutte le attività).
Si verifica un errore di richiesta non riuscita con codice di stato 500/503 quando si utilizza un filtro percorso.	Provare a utilizzare un intervallo di date più piccolo per filtrare i record.

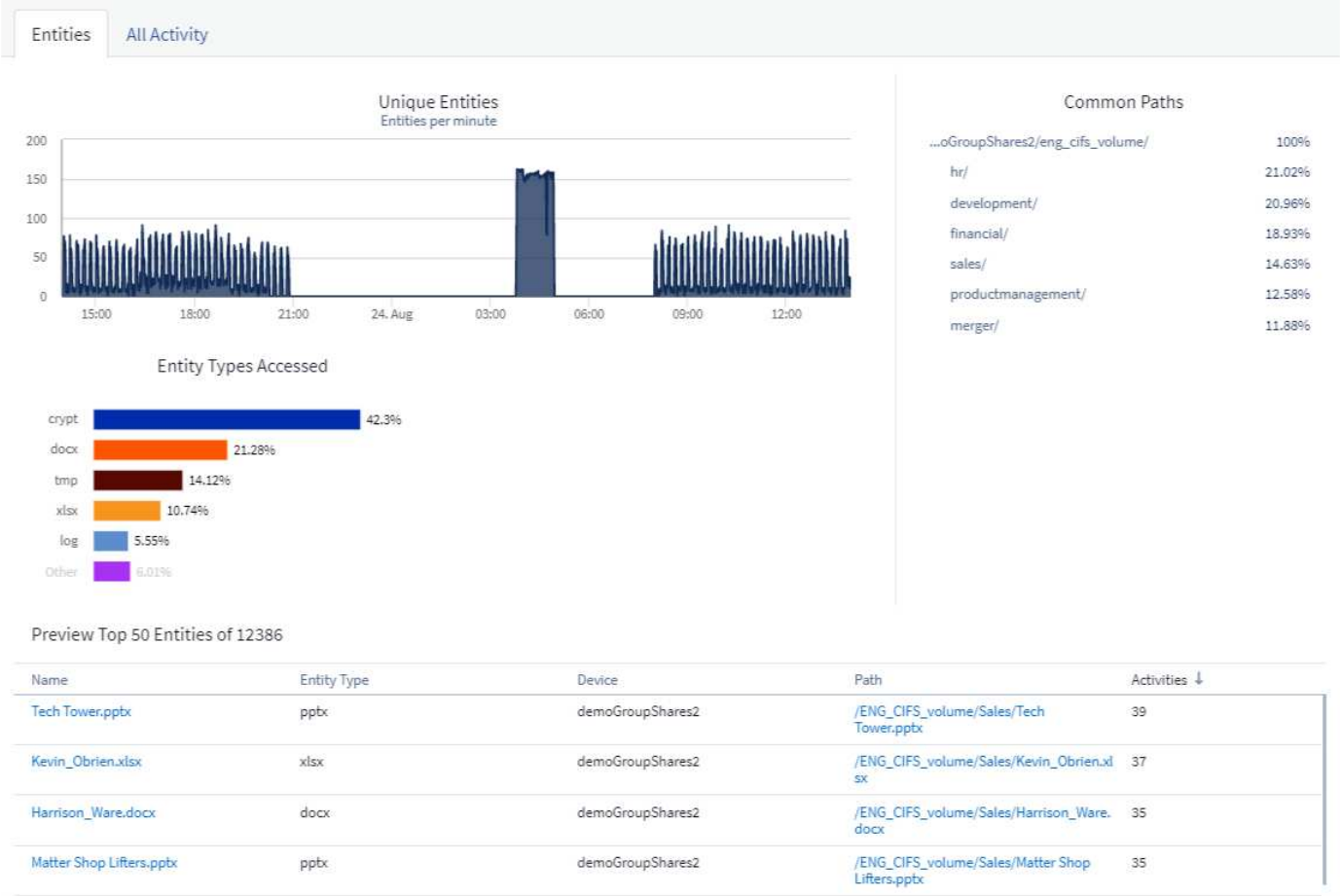
Pagina delle entità forensi

La pagina delle entità Forensics fornisce informazioni dettagliate sull'attività delle entità nell'ambiente.

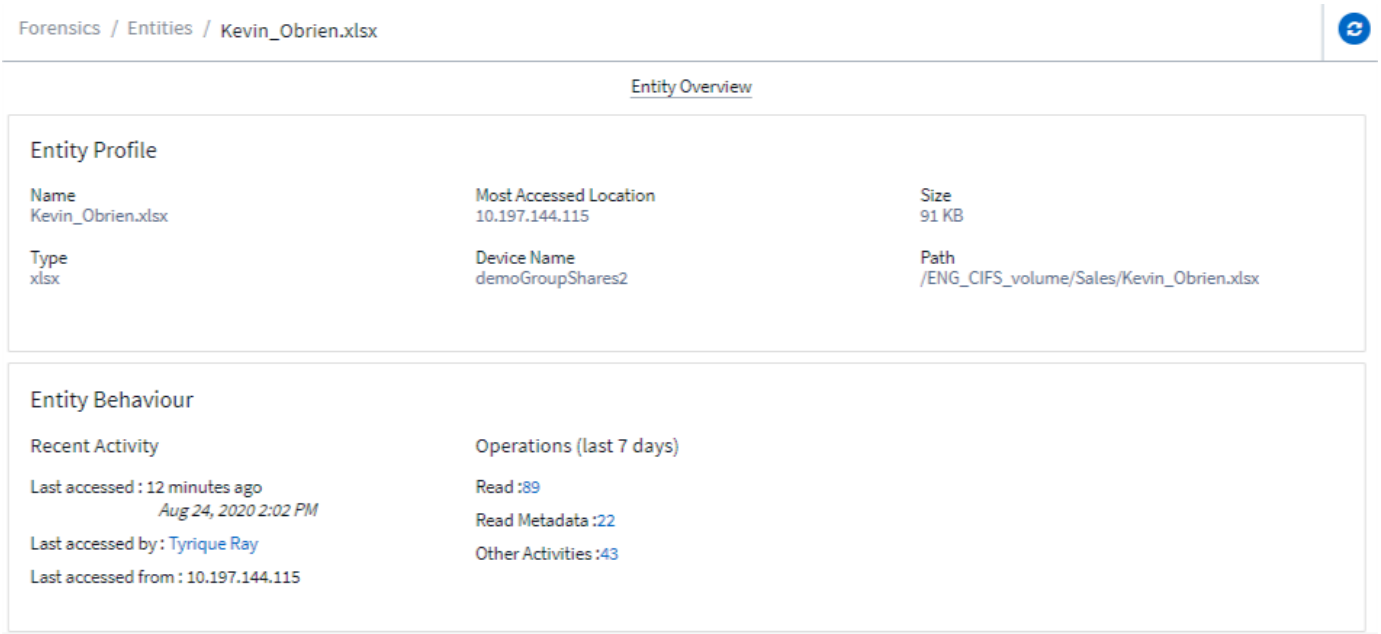
Esame delle informazioni sull'entità

Fare clic su **Forensics > Activity Forensics** e fare clic sulla scheda *Entities* per accedere alla pagina Entities.

Questa pagina fornisce una panoramica dell'attività dell'entità nel proprio ambiente, evidenziando le seguenti informazioni: * Un grafico che mostra *entità univoche* cui si accede al minuto * Un grafico di *tipi di entità a cui si accede* * una suddivisione dei *percorsi comuni* * Un elenco delle *prime 50 entità* rispetto al numero totale di entità



Facendo clic su un'entità nell'elenco, viene visualizzata una pagina panoramica dell'entità, che mostra un profilo dell'entità con dettagli come nome, tipo, nome del dispositivo, indirizzo IP e percorso più utilizzati, oltre al comportamento dell'entità come l'utente, l'IP, e ora dell'ultimo accesso all'entità.



Panoramica dell'utente legale

Le informazioni per ciascun utente sono fornite nella Panoramica utente. Utilizzare queste viste per comprendere le caratteristiche dell'utente, le entità associate e le attività recenti.

Profilo utente

Le informazioni del profilo utente includono le informazioni di contatto e la posizione dell'utente. Il profilo fornisce le seguenti informazioni:

- Nome dell'utente
- Indirizzo e-mail dell'utente
- Manager dell'utente
- Contatto telefonico per l'utente
- Posizione dell'utente

Comportamento dell'utente

Le informazioni sul comportamento dell'utente identificano le attività e le operazioni recenti eseguite dall'utente. Queste informazioni includono:

- Attività recente
  - Ultima posizione di accesso
  - Grafico delle attività
  - Avvisi
- Operazioni per gli ultimi sette giorni
  - Numero di operazioni

Intervallo di refresh

L'elenco utenti viene aggiornato ogni 12 ore.

Policy di conservazione

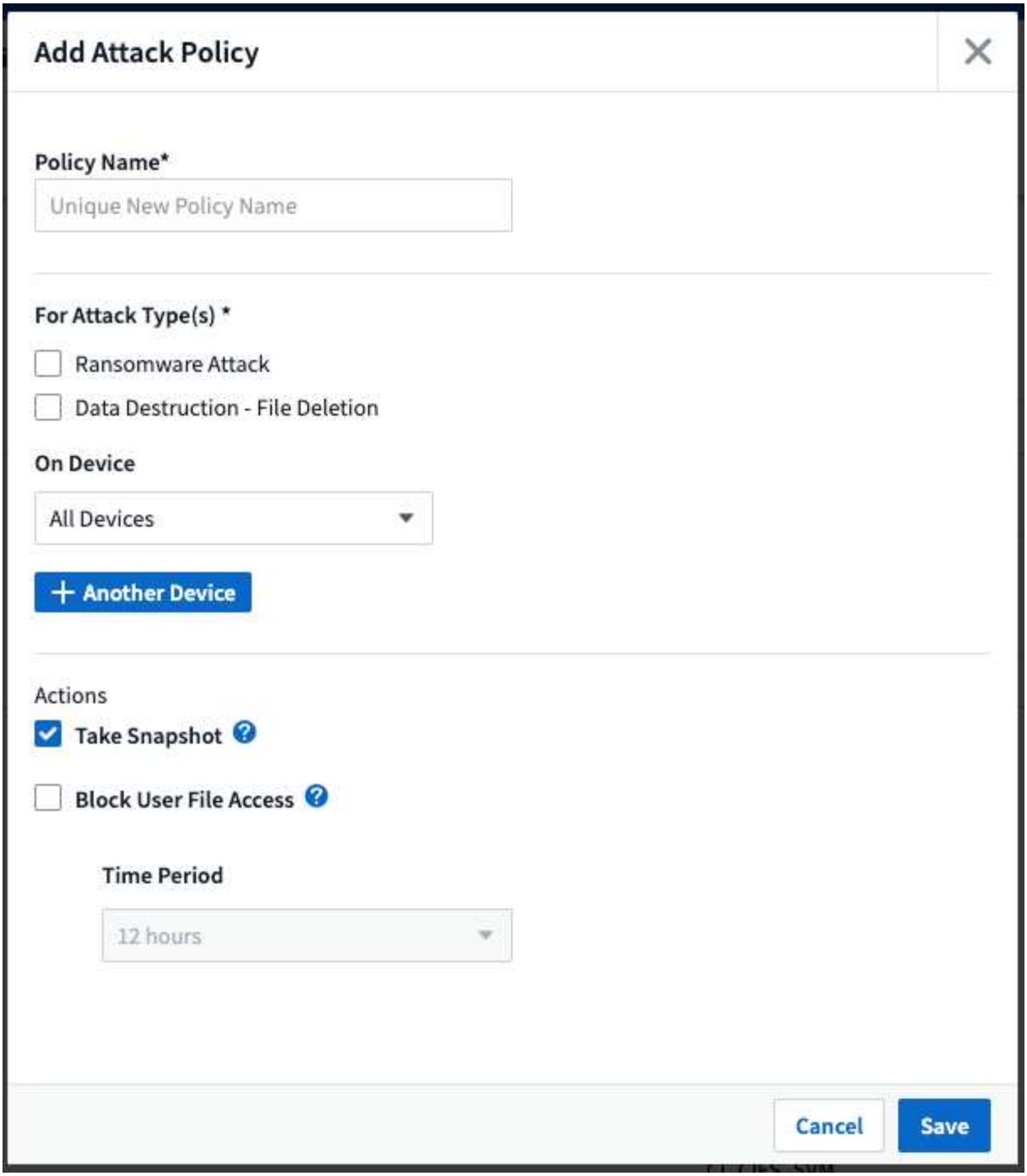
Se non viene aggiornato nuovamente, l'elenco utenti viene conservato per 13 mesi. Dopo 13 mesi, i dati verranno cancellati. Se l'ambiente workload Security viene cancellato, tutti i dati associati all'ambiente vengono cancellati.

Policy di risposta automatizzate

Le policy di risposta attivano azioni come l'esecuzione di uno snapshot o la limitazione dell'accesso dell'utente in caso di attacco o comportamento anomalo dell'utente.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

È possibile impostare criteri su dispositivi specifici o su tutti i dispositivi. Per impostare un criterio di risposta, selezionare **Admin > Automated Response Policies** (Amministrazione > Criteri di risposta automatici) e fare clic sul pulsante **+Policy** appropriato. È possibile creare policy per gli attacchi o per gli avvisi.



È necessario salvare il criterio con un nome univoco.

Per disattivare un'azione di risposta automatica (ad esempio, Take Snapshot), è sufficiente deselezionare l'azione e salvare la policy.

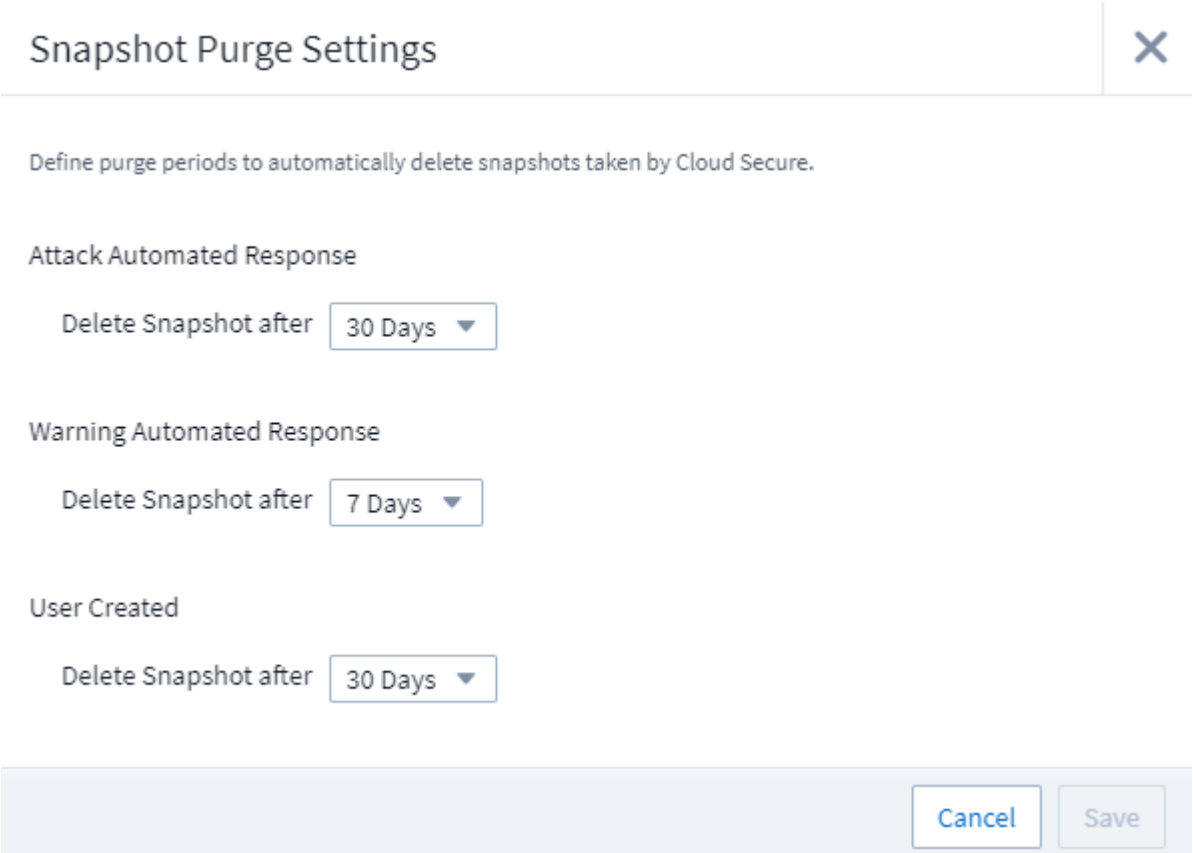
Quando viene attivato un avviso relativo ai dispositivi specificati (o a tutti i dispositivi, se selezionati), la policy di risposta automatica esegue un'istantanea dei dati. È possibile visualizzare lo stato dello snapshot su "Pagina dei dettagli degli avvisi".

Vedere "Limitare l'accesso dell'utente" Per ulteriori informazioni sulla limitazione dell'accesso dell'utente tramite IP.

È possibile modificare o sospendere una policy di risposta automatica scegliendo l'opzione nel menu a discesa

della policy.

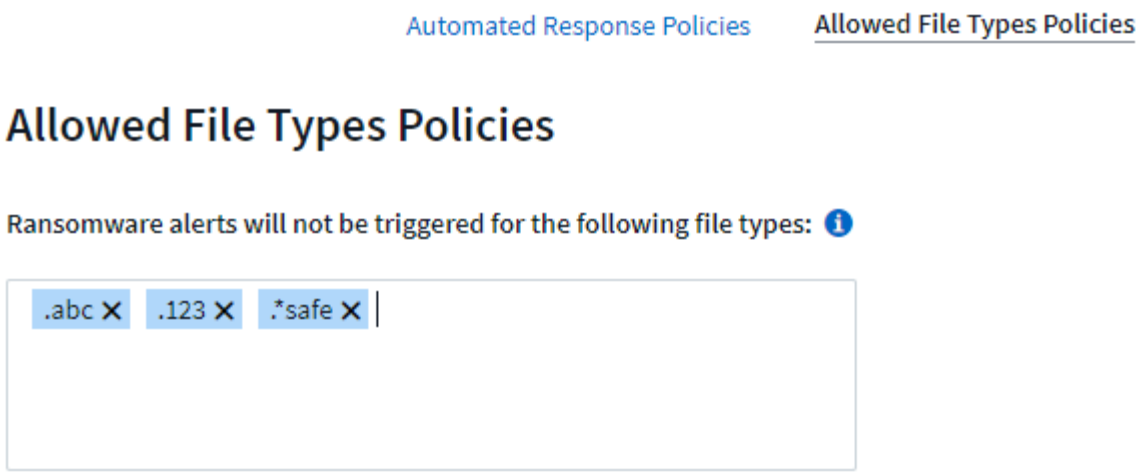
Workload Security elimina automaticamente le snapshot una volta al giorno in base alle impostazioni di Snapshot Purge.



Criteri tipi di file consentiti

Se viene rilevato un attacco ransomware per un'estensione di file nota e vengono generati degli avvisi nella schermata Alerts, è possibile aggiungere tale estensione a un elenco dei tipi di file *consentiti* per evitare avvisi non necessari.

Accedere a **sicurezza del carico di lavoro > Criteri** e andare alla scheda *Criteri del tipo di file consentiti*.



Una volta aggiunto all'elenco *allowed file types*, non verrà generato alcun avviso di attacco ransomware per quel tipo di file consentito. Si noti che la policy *tipi di file consentiti* è applicabile solo per il rilevamento del ransomware.

Ad esempio, se un file denominato *test.txt* viene rinominato *test.txt.abc* e workload Security rileva un attacco ransomware a causa dell'estensione *.abc*, l'estensione *.abc* può essere aggiunta all'elenco *allowed file types*. Dopo essere stati aggiunti all'elenco, gli attacchi ransomware non verranno più generati sui file con estensione *.abc*.

I tipi di file consentiti possono essere corrispondenze esatte (ad esempio, ".abc") o espressioni (ad esempio, "**.type", ".type**" o "**type**"). Le espressioni di tipo ".a*c", ".p*f" non sono supportate.

Integrazione con la protezione ransomware autonoma di ONTAP

La funzionalità ARP (Autonomous ransomware Protection) di ONTAP utilizza l'analisi dei carichi di lavoro in ambienti NAS (NFS e SMB) per rilevare e avvisare in modo proattivo circa attività anomale nel file che potrebbero indicare un attacco ransomware.

Ulteriori dettagli e requisiti di licenza su ARP sono disponibili "qui".

La sicurezza del carico di lavoro si integra con ONTAP per ricevere eventi ARP e fornire un ulteriore livello di analisi e risposte automatiche.

Workload Security riceve gli eventi ARP da ONTAP e intraprende le seguenti azioni:

1. Correla gli eventi di crittografia dei volumi con l'attività dell'utente per identificare chi sta causando il danno.
2. Implementa policy di risposta automatica (se definite)
3. Offre funzionalità di analisi legale:
    - Consentire ai clienti di condurre indagini sulle violazioni dei dati.
    - Identificare i file interessati, contribuendo a ripristinarli più rapidamente e a condurre indagini sulle violazioni dei dati.

Prerequisiti

1. Versione minima di ONTAP: 9.11.1
2. Volumi abilitati ARP. Per ulteriori informazioni sull'abilitazione di ARP, consultare la sezione "qui". ARP deve essere abilitato tramite Gestore di sistema di OnCommand. La sicurezza del carico di lavoro non può abilitare ARP.
3. Workload Security Collector deve essere aggiunto tramite l'IP del cluster.
4. Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster. In altre parole, è necessario utilizzare le credenziali a livello di cluster quando si aggiunge la SVM.

Autorizzazioni utente richieste

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni alla sicurezza del carico di lavoro per raccogliere informazioni relative all'ARP da ONTAP.

Per *csuser* con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly  -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole
```

Ulteriori informazioni sulla configurazione di Altro "Permessi ONTAP".

Avviso di esempio

Di seguito è riportato un esempio di avviso generato a causa di un evento ARP:

POTENTIAL ATTACK: AL_1315
Ransomware Attack

Detected
5 months ago
Oct 20, 2022 3:06 AM

Action Taken
Access Blocked on 5 SVMs
Snapshots Taken

Status
New

Blocked permanently by auto response policy
Change Block Period
Unblock User

Last snapshots taken by auto response policy
Oct 20, 2022 3:09 AM
Re-Take Snapshots

How To:
Restore Entities

Total Attack Results

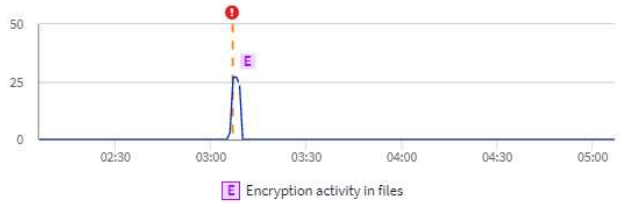
1	83	81
Affected Volumes	Deleted Files	Encrypted Files

81 Files have been copied, deleted, and potentially encrypted by 1 user account.

The extension "osiris" was added to each file.

High Confidence Detection
Ransomware behavior and in-file encryption activities were detected.

Encrypted Files
Activity per minute



Related Users

Jamelia Graham
Business Partner
HR

User/IP Access
Blocked

81
Encrypted Files

Detected
5 months ago
Oct 20, 2022 3:06 AM

Username
us024

Domain
cslab.netapp.com

Email
Graham@netapp.com

Phone
9251140014

Department
HR

Manager
Iwan Holt

Location
WA

Top Activity Types
Activity per minute
Last accessed from: 10.193.113.247

View Activity Detail

Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	Block more detail	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	Block more detail	1h		Automatic	10.197.144.115

Affected Devices/Volumes

Device	Volume	Encrypted Files	Associated Snapshot Taken			
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM	cloudsecure_attack_auto_1666249787062	Automatic	Take Snapshot

Un banner di alta fiducia indica che l'attacco ha mostrato un comportamento ransomware insieme alle attività di crittografia dei file. Il grafico dei file crittografati indica la data e l'ora in cui l'attività di crittografia del volume è stata rilevata dalla soluzione ARP.

Limitazioni

Nel caso in cui una SVM non venga monitorata dalla sicurezza del carico di lavoro, ma vi siano eventi ARP generati da ONTAP, gli eventi verranno comunque ricevuti e visualizzati dalla sicurezza del carico di lavoro. Tuttavia, le informazioni Forensic relative all'avviso, così come la mappatura dell'utente, non verranno acquisite o visualizzate.

Risoluzione dei problemi

I problemi noti e le relative risoluzioni sono descritti nella seguente tabella.

Problema:	Risoluzione:
Gli avvisi e-mail vengono ricevuti 24 ore dopo il rilevamento di un attacco. Nell'interfaccia utente, gli avvisi vengono visualizzati 24 ore prima quando le e-mail vengono ricevute da Cloud Insights workload Security.	Quando ONTAP invia l'evento *ransomware Detected* alla sicurezza del carico di lavoro Cloud Insights (ad esempio, sicurezza del carico di lavoro), l'e-mail viene inviata. L'evento contiene un elenco di attacchi e i relativi indicatori di data e ora. L'interfaccia utente di workload Security visualizza la data e l'ora di avviso del primo file attaccato. ONTAP invia l'evento *ransomware Detected* a Cloud Insights quando viene codificato un certo numero di file. Pertanto, potrebbe esserci una differenza tra l'ora in cui l'avviso viene visualizzato nell'interfaccia utente e l'ora in cui l'e-mail viene inviata.

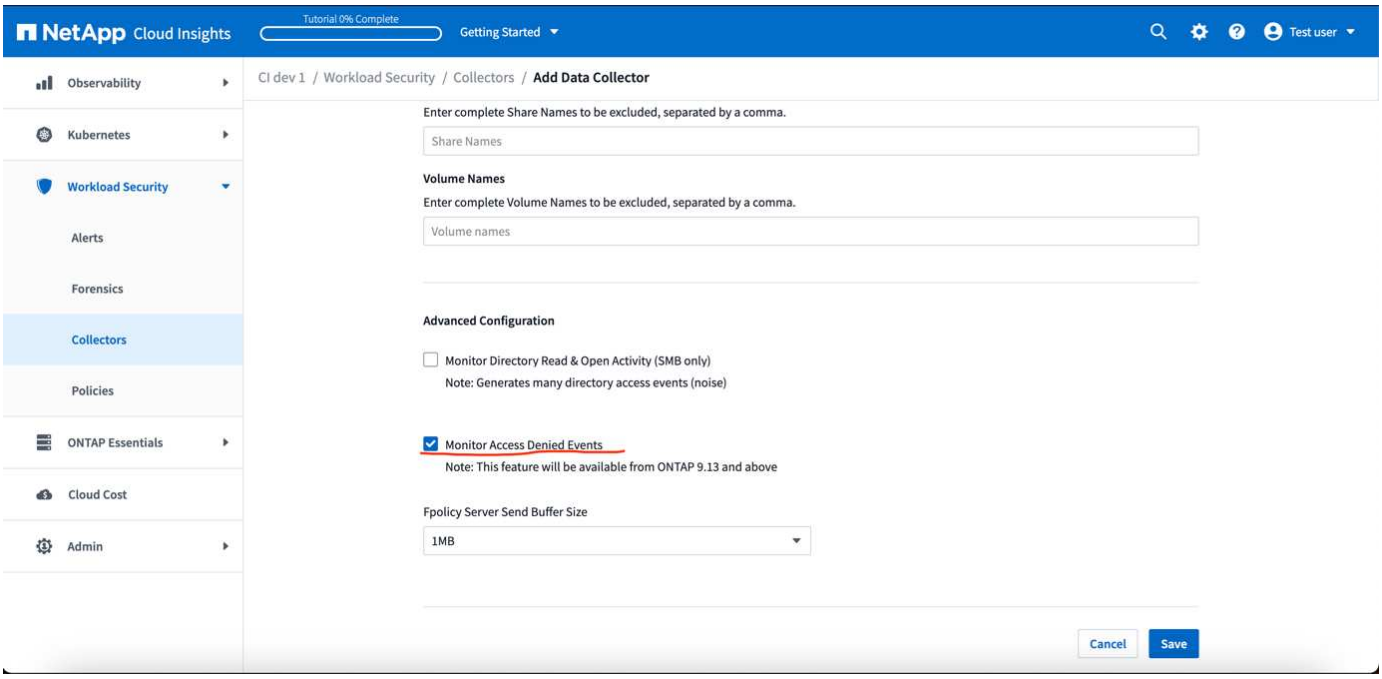
Integrazione con accesso ONTAP negato

La funzionalità accesso negato di ONTAP utilizza l'analisi dei carichi di lavoro negli ambienti NAS (NFS e SMB) per rilevare in modo proattivo e informare l'utente in caso di operazioni sui file non riuscite (ad esempio, un utente che tenta di eseguire un'operazione per cui non dispone dell'autorizzazione). Queste notifiche delle operazioni sui file non riuscite, specialmente in caso di errori relativi alla sicurezza, aiuteranno ulteriormente a bloccare gli attacchi interni nelle prime fasi.

Cloud Insights workload Security si integra con ONTAP per ricevere eventi di accesso negato e fornire un livello di risposta automatico e analitico aggiuntivo.

Prerequisiti

- Versione ONTAP minima: 9.13.0.
- Un amministratore della protezione del carico di lavoro deve attivare la funzione accesso negato durante l'aggiunta di un nuovo agente di raccolta o la modifica di un agente di raccolta esistente, selezionando la casella di controllo *Monitor Access Denied Events* in Configurazione avanzata.



Autorizzazioni utente richieste

Se Data Collector viene aggiunto utilizzando le credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se il servizio di raccolta viene aggiunto utilizzando un utente personalizzato (ad esempio, *csuser*) con autorizzazioni assegnate all'utente, attenersi alla procedura riportata di seguito per assegnare a sicurezza del carico di lavoro l'autorizzazione necessaria per registrare gli eventi di accesso negato con ONTAP.

Per csuser con credenziali *cluster*, eseguire i seguenti comandi dalla riga di comando di ONTAP. Si noti che *csrestrole* è un ruolo personalizzato e *csuser* è un utente personalizzato di ONTAP.

```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

Per csuser con credenziali *SVM*, eseguire i seguenti comandi dalla riga di comando di ONTAP:

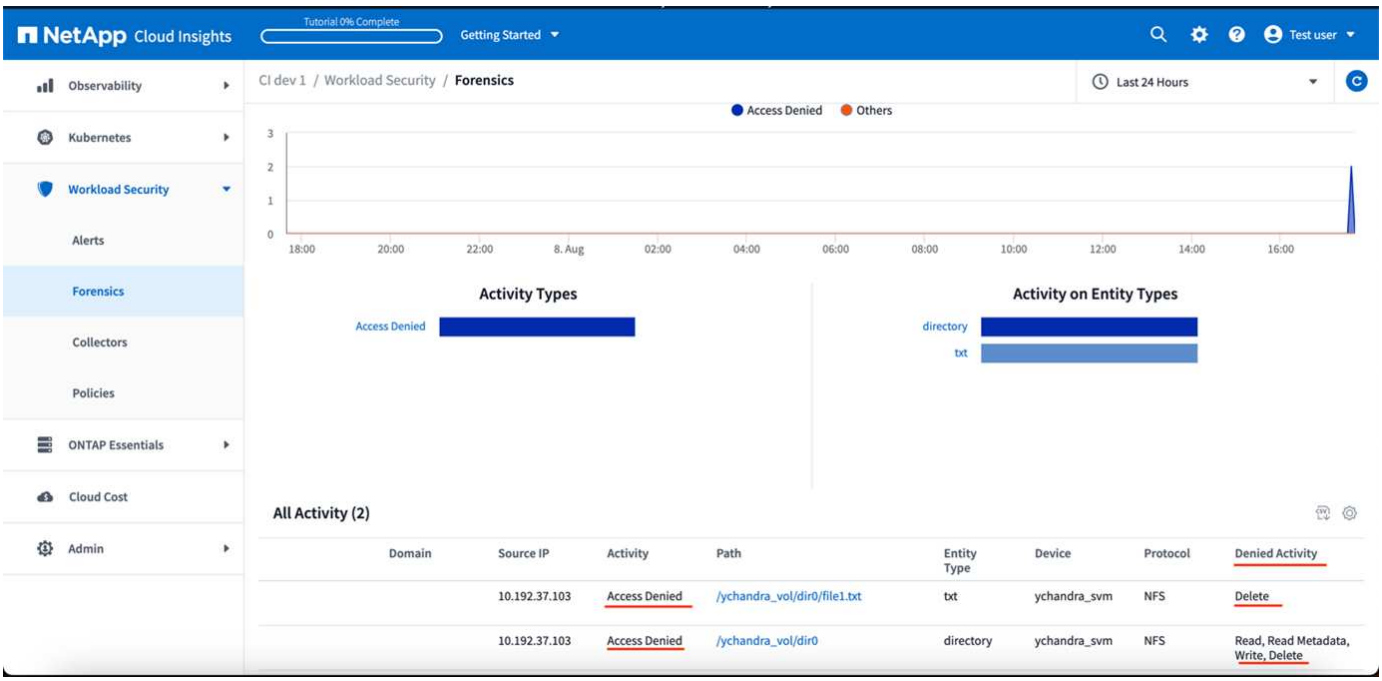
```
 security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
 security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

Ulteriori informazioni sulla configurazione di Altro "Permessi ONTAP".

Eventi di accesso negato

Una volta acquisiti gli eventi dal sistema ONTAP, la pagina analisi della sicurezza del workload mostra gli

eventi di accesso negato. Oltre alle informazioni visualizzate, è possibile visualizzare i permessi utente mancanti per una particolare operazione aggiungendo la colonna *attività desiderata* alla tabella dall'icona a forma di ingranaggio.



Blocco dell'accesso utente

Una volta rilevato un attacco, Workload Security può arrestare l'attacco bloccando l'accesso dell'utente al file system. L'accesso può essere bloccato automaticamente, utilizzando le policy di risposta automatica o manualmente dalle pagine degli avvisi o dei dettagli dell'utente.

La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Quando si blocca l'accesso dell'utente, è necessario definire un periodo di tempo di blocco. Al termine del periodo di tempo selezionato, l'accesso dell'utente viene ripristinato automaticamente. Il blocco degli accessi è supportato per i protocolli SMB e NFS.

L'utente è direttamente bloccato per SMB e l'indirizzo IP dei computer host che causano l'attacco sarà bloccato per NFS. Gli indirizzi IP di tali macchine non potranno accedere alle macchine virtuali di storage (SVM) monitorate da workload Security.

Ad esempio, supponiamo che Workload Security gestisca 10 SVM e che la policy di risposta automatica sia configurata per quattro di queste SVM. Se l'attacco ha origine in una delle quattro SVM, l'accesso dell'utente viene bloccato in tutte le 10 SVM. Viene ancora eseguita un'istantanea sulla SVM di origine.

Se sono presenti quattro SVM con una SVM configurata per SMB, una configurata per NFS e le restanti due configurate per NFS e SMB, tutte le SVM verranno bloccate se l'attacco ha origine in una qualsiasi delle quattro SVM.

Prerequisiti per il blocco dell'accesso utente

Per il funzionamento di questa funzionalità sono necessarie credenziali a livello di cluster.

Se si utilizzano credenziali di amministrazione del cluster, non sono necessarie nuove autorizzazioni.

Se si utilizza un utente personalizzato (ad esempio *csuser*) con autorizzazioni assegnate all'utente, seguire la procedura riportata di seguito per assegnare le autorizzazioni a workload Security per bloccare l'utente.

Per gli utenti csuser con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP:

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

Assicurarsi di esaminare la sezione autorizzazioni di "Configurazione del Data Collector SVM di ONTAP" pagina pure.

Come attivare la funzione?

- In sicurezza del carico di lavoro, accedere a **sicurezza del carico di lavoro > Criteri > Criteri di risposta automatizzati**. Scegliere **+Criteri attacco**.
- Selezionare (selezionare) *Blocca accesso file utente*.

Come si imposta il blocco automatico degli accessi degli utenti?

- Creare una nuova policy di attacco o modificare una policy di attacco esistente.
- Selezionare le SVM su cui monitorare la policy di attacco.
- Fare clic sulla casella di controllo "Block User file Access" (Blocca accesso file utente). La funzione viene attivata quando viene selezionata.
- In "Time Period" (periodo di tempo), selezionare l'intervallo di tempo fino al quale applicare il blocco.
- Per testare il blocco automatico dell'utente, è possibile simulare un attacco tramite un "script simulato".

Come verificare se nel sistema sono presenti utenti bloccati?

- Nella pagina degli elenchi degli avvisi, viene visualizzato un banner nella parte superiore della schermata in caso di blocco di un utente.
- Facendo clic sul banner si accede alla pagina "utenti", in cui è possibile visualizzare l'elenco degli utenti bloccati.
- Nella pagina "utenti", all'interno di una colonna denominata "accesso utente/IP". In questa colonna viene visualizzato lo stato corrente di blocco dell'utente.

Limitare e gestire l'accesso utente manualmente

- È possibile accedere alla schermata dei dettagli degli avvisi o dei dettagli dell'utente, quindi bloccare o ripristinare manualmente un utente da tali schermate.

Cronologia delle limitazioni di accesso dell'utente

Nella pagina dei dettagli degli avvisi e dei dettagli dell'utente, nel pannello utente, è possibile visualizzare un audit della cronologia delle limitazioni di accesso dell'utente: Tempo, azione (blocco, sblocco), durata, azione intrapresa da, Manuale/automatico e IP interessati per NFS.

Come si disattiva la funzione?

È possibile disattivare la funzione in qualsiasi momento. Se nel sistema sono presenti utenti con restrizioni, è necessario ripristinarne l'accesso.

- In sicurezza del carico di lavoro, accedere a **sicurezza del carico di lavoro > Criteri > Criteri di risposta automatizzati**. Scegliere **+Criteri attacco**.
- Deselezionare *Blocca accesso al file utente*.

La funzione verrà nascosta da tutte le pagine.

Ripristinare manualmente gli IP per NFS

Attenersi alla seguente procedura per ripristinare manualmente gli IP da ONTAP se la versione di prova di workload Security scade o se l'agente/collector non è attivo.

1. Elencare tutti i criteri di esportazione su una SVM.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0        default         1       nfs3,    cloudsecure_rule,     never
                                    nfs4,    10.11.12.13
                                    cifs
svm1        default         4       cifs,    0.0.0.0/0             any
                                    nfs
svm2        test            1       nfs3,    cloudsecure_rule,     never
                                    nfs4,    10.11.12.13
                                    cifs
svm3        test            3       cifs,    0.0.0.0/0             any
                                    nfs,
                                    flexcache
4 entries were displayed.
```

2. Eliminare le regole di tutti i criteri sulla SVM che hanno "cloudSecure_rule" come corrispondenza client specificando il rispettivo RuleIndex. La regola di sicurezza del carico di lavoro è solitamente 1.

```
 contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>
-policyname * -ruleindex 1
. Assicurarsi che la regola di sicurezza del carico di lavoro sia
eliminata (passaggio facoltativo per confermare).
```

```
contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
             Policy          Rule    Access   Client                RO
Vserver      Name            Index   Protocol Match                 Rule
------------ --------------- ------  -------- ---------------------
---------
svm0         default         4       cifs,    0.0.0.0/0             any
                                    nfs
svm2         test            3       cifs,    0.0.0.0/0             any
                                    nfs,
                                    flexcache
2 entries were displayed.
```

Ripristinare manualmente gli utenti per SMB

Attenersi alla seguente procedura per ripristinare manualmente gli utenti da ONTAP se la versione di prova di workload Security scade o se l'agente/collector non è attivo.

È possibile ottenere l'elenco degli utenti bloccati in workload Security dalla pagina dell'elenco utenti.

1. Accedere al cluster ONTAP (dove si desidera sbloccare gli utenti) con le credenziali *admin* del cluster. (Per Amazon FSX, accedi con le credenziali FSX).
2. Eseguire il seguente comando per elencare tutti gli utenti bloccati da workload Security per SMB in tutte le SVM:

```
vserver name-mapping show -direction win-unix -replacement " "
```

```
Vserver:   <vservername>
Direction: win-unix
Position Hostname         IP Address/Mask
-------- ---------------- ----------------
1       -                 -                   Pattern: CSLAB\\US040
                                         Replacement:
2       -                 -                   Pattern: CSLAB\\US030
                                         Replacement:
2 entries were displayed.
```

Nel suddetto output, 2 utenti sono stati bloccati (US030, US040) con il dominio CSLAB.

1. Una volta identificata la posizione dall'output precedente, eseguire il seguente comando per sbloccare l'utente:

```
 vserver name-mapping delete -direction win-unix -position <position>
. Verificare che gli utenti siano sbloccati eseguendo il comando:
```

```
vserver name-mapping show -direction win-unix -replacement " "
```

Non devono essere visualizzate voci per gli utenti precedentemente bloccati.

Risoluzione dei problemi

Problema	Provare
Alcuni utenti non sono soggetti a restrizioni, anche se si verifica un attacco.	1. Assicurarsi che Data Collector e Agent per le SVM siano in stato *running*. Workload Security non sarà in grado di inviare comandi se Data Collector e Agent vengono arrestati. 2. Questo perché l'utente potrebbe aver effettuato l'accesso allo storage da un computer con un nuovo IP che non è stato utilizzato in precedenza. La limitazione avviene tramite l'indirizzo IP dell'host attraverso il quale l'utente accede allo storage. Controllare nell'interfaccia utente (Dettagli avviso > Cronologia limiti di accesso per questo utente > IP interessati) l'elenco degli indirizzi IP con restrizioni. Se l'utente accede allo storage da un host che ha un IP diverso dagli IP con restrizioni, l'utente potrà comunque accedere allo storage attraverso l'IP senza restrizioni. Se l'utente sta tentando di accedere dagli host i cui indirizzi IP sono limitati, lo storage non sarà accessibile.
Facendo clic manualmente su Restricate Access (limita accesso) si ottiene "gli indirizzi IP di questo utente sono già stati limitati".	L'IP da limitare è già stato limitato da un altro utente.
Impossibile modificare il criterio. Motivo: Non autorizzato per quel comando.	Controllare se si utilizza csuser, le autorizzazioni vengono assegnate all'utente come indicato in precedenza.

Problema	Provare
Il blocco dell'utente (indirizzo IP) per NFS funziona, ma per SMB / CIFS viene visualizzato un messaggio di errore: "Trasformazione SID in DomainName non riuscita. Timeout motivo: Socket non stabilito"	Ciò può accadere se *csuser* non dispone dell'autorizzazione per eseguire ssh. (Verificare la connessione a livello di cluster, quindi assicurarsi che l'utente possa eseguire ssh). il ruolo *csuser* richiede queste autorizzazioni. https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blockingPer *csuser* con credenziali cluster, eseguire le seguenti operazioni dalla riga di comando ONTAP: ruolo di login di sicurezza create -role csrole -cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create -role csrole -cmddirname "vserver cifs session" -access all security login role create -role csrole role -role csrole -cmddirname -cmddirname "vserver access service access service access-check authentication" Role create -role csrole -cmddirname "vserver name-mapping" -access all se *csuser* non viene utilizzato e se viene utilizzato l'utente admin a livello di cluster, assicurarsi che l'utente admin disponga dell'autorizzazione ssh per ONTAP.

Sicurezza del carico di lavoro: Simulazione di un attacco

È possibile utilizzare le istruzioni riportate in questa pagina per simulare un attacco per il test o la dimostrazione di workload Security utilizzando lo script ransomware Simulation incluso.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Cose da notare prima di iniziare

- Lo script di simulazione ransomware funziona solo su Linux.
- Lo script viene fornito con i file di installazione dell'agente workload Security. È disponibile su qualsiasi computer su cui è installato un agente workload Security.
- È possibile eseguire lo script sul computer dell'agente workload Security; non è necessario preparare un'altra macchina Linux. Tuttavia, se si preferisce eseguire lo script su un altro sistema, è sufficiente copiare lo script ed eseguirlo.

Avere almeno 1,000 file di esempio

Questo script deve essere eseguito su una SVM con una cartella contenente file da crittografare. Si consiglia di avere almeno 1,000 file all'interno di tale cartella e di qualsiasi sottocartella. I file non devono essere vuoti. Non creare i file e crittografarli utilizzando lo stesso utente. Workload Security considera questa attività a basso rischio e pertanto non genera un avviso (ad esempio, lo stesso utente modifica i file appena creati).

Vedere di seguito per le istruzioni su "creare a livello di codice file non vuoti".

Linee guida prima di eseguire il simulatore:

1. Assicurarsi che i file crittografati non siano vuoti.
2. Assicurarsi di crittografare > 50 file. Un numero limitato di file verrà ignorato.
3. Non eseguire più attacchi con lo stesso utente. Dopo alcune volte, workload Security apprenderà questo comportamento dell'utente e supporrà che si tratti del comportamento normale dell'utente.
4. Non crittografare i file creati dallo stesso utente. La modifica di un file appena creato da un utente non è considerata un'attività rischiosa. Utilizzare invece i file creati da un altro utente O attendere qualche ora tra la creazione e la crittografia dei file.

Preparare il sistema

Per prima cosa, montare il volume di destinazione sulla macchina. È possibile montare un montaggio NFS o un'esportazione CIFS.

Per montare l'esportazione NFS in Linux:

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvol1 /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

Non montare NFS versione 4.1; non è supportato da Fpolicy.

Per montare CIFS in Linux:

```
 mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
Quindi, configurare un Data Collector:
```

1. Configurare l'agente workload Security, se non è già stato fatto.
2. Configurare il data collector SVM se non è già stato fatto.

Eseguire lo script ransomware Simulator

1. Accedere (ssh) al computer dell'agente workload Security.
2. Accedere a: */opt/netapp/cloudSecure/Agent/install*
3. Chiamare lo script del simulatore senza parametri per visualizzare l'utilizzo:

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory  provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
       -e to encrypt files (default)
       -d to restore files
       -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```

Crittografare i file di test

Per crittografare i file, eseguire il seguente comando:

```
# ./ransomware_simulator.sh -e -i /root/for/
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-
1.251.0/install/encryption-key,
which can be used for restoring the files.
Encrypted /root/for/File000.txt
Encrypted /root/for/File001.txt
Encrypted /root/for/File002.txt
...
```

Ripristinare i file

Per decrittare, eseguire il seguente comando:

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/
File /root/for/File000.txt is restored.
File /root/for/File001.txt is restored.
File /root/for/File002.txt is restored.
...
```

Eseguire lo script più volte

Dopo aver generato un attacco ransomware per un utente, passare a un altro utente per generare un attacco aggiuntivo. Workload Security apprende il comportamento dell'utente e non avvisa in caso di ripetuti attacchi ransomware entro un breve periodo di tempo per lo stesso utente.

Creare file a livello di codice

Prima di creare i file, è necessario interrompere o sospendere l'elaborazione del Data Collector.
Prima di aggiungere il data collector all'agente, attenersi alla procedura riportata di seguito. Se è già stato aggiunto il data collector, è sufficiente modificare il data collector, inserire una password non valida e salvarla. In questo modo, il data collector viene temporaneamente messo in stato di errore. NOTA: Annotare la password originale.

> L'opzione consigliata è da a. "mettere in pausa il raccoglitore" prima di creare i file.]

Prima di eseguire la simulazione, è necessario aggiungere i file da crittografare. È possibile copiare manualmente i file da crittografare nella cartella di destinazione oppure utilizzare uno script (vedere l'esempio seguente) per creare i file a livello di programmazione. Copiare almeno 1,000 file, indipendentemente dal metodo utilizzato.

Se si sceglie di creare i file a livello di programmazione, attenersi alla seguente procedura:

1. Accedere alla casella Agente.
2. Montare un'esportazione NFS dalla SVM del filer alla macchina Agent. Su tale cartella.
3. In tale cartella creare un file denominato createfiles.sh
4. Copiare le seguenti righe nel file.

```
for i in {000..1000}
do
   echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. Salvare il file.
6. Assicurarsi che il permesso di esecuzione sul file sia:

```
 chmod 777 ./createfiles.sh
. Eseguire lo script:
```

```
./createfiles.sh
```

   nella cartella corrente verranno creati 1000 file.

7. Riattivare il data collector

   Se il data collector è stato disattivato al punto 1, modificare il data collector, inserire la password corretta e salvare. Assicurarsi che il data collector sia nuovamente in esecuzione.

8. Se il raccoglitore è stato messo in pausa prima di procedere come indicato di seguito, assicurarsi di "riprendere il raccoglitore".

Configurazione delle notifiche e-mail per gli avvisi, gli avvisi e lo stato del servizio di raccolta origine dati/agente

Per configurare i destinatari degli avvisi di workload Security, fare clic su **Admin > Notifiche** e inserire gli indirizzi e-mail nelle sezioni appropriate per ciascun destinatario.

La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Avvisi e avvisi di potenziali attacchi

Per inviare notifiche di avviso di *potenziali attacchi*, inserire gli indirizzi e-mail dei destinatari nella sezione *Invia avvisi potenziali attacchi*. Le notifiche e-mail vengono inviate all'elenco dei destinatari degli avvisi per ogni azione dell'avviso.

Per inviare notifiche di tipo *Warning*, inserire gli indirizzi e-mail dei destinatari nella sezione *Send Warning Alerts*.

Monitoraggio dello stato di salute di Agent e Data Collector

È possibile monitorare lo stato degli agenti e delle origini dati attraverso le notifiche.

Per ricevere notifiche in caso di mancato funzionamento di un agente o di un Data Source Collector, inserire gli indirizzi e-mail dei destinatari nella sezione *Data Collection Health Alerts*.

Tenere presente quanto segue:

- Gli avvisi sullo stato di salute verranno inviati solo dopo che l'agente/raccoglitore ha interrotto la segnalazione per almeno un'ora.
- Viene inviata una sola notifica via email ai destinatari in un dato periodo di 24 ore, anche se l'agente o il Data Collector sono disconnessi per un periodo di tempo più lungo.
- In caso di guasto di un Agente, verrà inviato un avviso (non uno per raccoglitore). L'e-mail includerà un elenco di tutte le SVM interessate.
- Un errore di raccolta Active Directory viene segnalato come avviso e non influisce sul rilevamento ransomware.
- L'elenco di configurazione per iniziare ora include una nuova fase di *Configurazione delle notifiche e-mail*.

Ricezione delle notifiche di aggiornamento di Agent e Data Collector

- Inserire gli ID e-mail in "Avvisi sullo stato di salute della raccolta dati".
- La casella di controllo "Enable upgrade notifications" (attiva notifiche di aggiornamento) viene attivata.
- Le notifiche e-mail di aggiornamento di Agent e Data Collector vengono inviate agli ID e-mail un giorno prima dell'aggiornamento pianificato.

Risoluzione dei problemi

Problema:	Provare questo:
Gli ID e-mail sono presenti negli "Avvisi sullo stato di salute di Data Collector", ma non ricevo notifiche.	Le e-mail di notifica vengono inviate dal dominio NetApp Cloud Insights, ad esempio da *accounts@service.cloudinsights.netapp.com*. Alcune aziende bloccano le e-mail in arrivo se provengono da un dominio esterno. Assicurarsi che le notifiche esterne dai domini NetApp Cloud Insights siano inseriti nella whitelist.

API per la sicurezza del carico di lavoro

L'API workload Security consente ai clienti NetApp e ai vendor di software indipendenti (ISV) di integrare workload Security con altre applicazioni, come CMDB o altri sistemi di ticketing.

> La sicurezza del carico di lavoro non è disponibile nell'edizione federale di Cloud Insights.

Requisiti per l'accesso API:

- Per concedere l'accesso viene utilizzato un modello API Access Token.
- La gestione del token API viene eseguita dagli utenti di workload Security con il ruolo di Amministratore.

Documentazione API (Swagger)

Le informazioni API più recenti si trovano accedendo a workload Security e accedendo a **Admin > API Access**. Fare clic sul collegamento **documentazione API**. La documentazione API è basata su Swagger, che fornisce una breve descrizione e informazioni sull'utilizzo dell'API e consente di provarla nel proprio ambiente.

Token di accesso API

Prima di utilizzare l'API workload Security, è necessario creare uno o più **API Access Token**. I token di accesso concedono le autorizzazioni di lettura. È inoltre possibile impostare la scadenza per ciascun token di accesso.

Per creare un token di accesso:

- Fare clic su **Admin > API Access** (Amministratore > accesso API)
- Fare clic su **+token di accesso API**
- Inserire **Nome token**
- Specificare **scadenza token**

> Il token sarà disponibile solo per la copia negli Appunti e il salvataggio durante il processo di creazione. I token non possono essere recuperati dopo la loro creazione, pertanto si consiglia vivamente di copiarli e salvarli in una posizione sicura. Viene richiesto di fare clic sul pulsante Copy API Access Token (Copia token di accesso API) prima di chiudere la schermata di creazione del token.

È possibile disattivare, attivare e revocare i token. È possibile attivare i token disattivati.

I token garantiscono l'accesso generico alle API dal punto di vista del cliente, gestendo l'accesso alle API nell'ambito del proprio ambiente.

L'applicazione riceve un token di accesso dopo che un utente ha autenticato e autorizzato l'accesso, quindi passa il token di accesso come credenziale quando chiama l'API di destinazione. Il token passato informa l'API che la portante del token è stata autorizzata ad accedere all'API ed eseguire azioni specifiche in base all'ambito concesso durante l'autorizzazione.

L'intestazione HTTP in cui viene passato il token di accesso è **X-CloudInsights-apiKey:**

Ad esempio, utilizzare quanto segue per recuperare le risorse di storage:

```
 curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-
CloudInsights-ApiKey: <API_Access_Token>'
Dove _<API_Access_Token>_ è il token salvato durante la creazione della
chiave di accesso API.
```

Informazioni dettagliate sono disponibili nel link *documentazione API* sotto **Admin > accesso API**.

Active IQ

NetApp "Active IQ" Offre una serie di visualizzazioni, analytics e altri servizi di supporto ai clienti NetApp per i loro sistemi hardware/software. I dati riportati da Active IQ possono migliorare la risoluzione dei problemi di sistema e fornire informazioni sull'ottimizzazione e sull'analisi predittiva dei dispositivi.

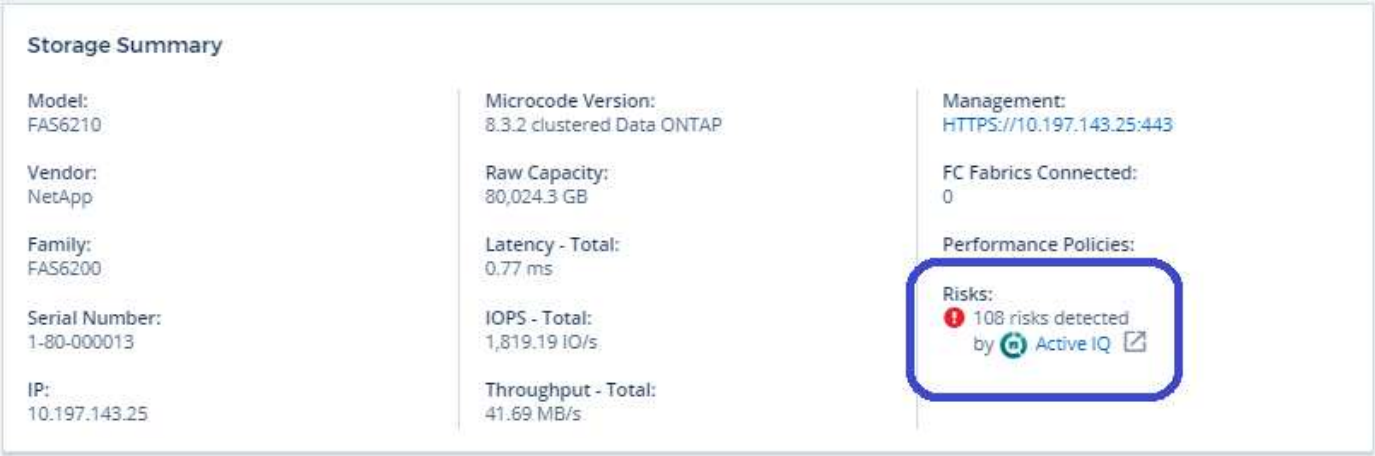
ActiveIQ non è disponibile nell'edizione federale di Cloud Insights.

Cloud Insights raccoglie i **rischi** per qualsiasi sistema storage NetApp Clustered Data ONTAP monitorato e segnalato da Active IQ. I rischi segnalati per i sistemi storage vengono raccolti automaticamente da Cloud Insights nell'ambito della raccolta dei dati da tali dispositivi. È necessario aggiungere il data collector appropriato a Cloud Insights per raccogliere le informazioni sui rischi Active IQ.

Cloud Insights non mostra i dati di rischio per i sistemi ONTAP che non sono monitorati e segnalati da Active IQ.

I rischi riportati sono riportati in Cloud Insights nelle pagine di destinazione delle risorse di *storage* e *storage node*, nella tabella "rischi". La tabella mostra i dettagli del rischio, la categoria di rischio e il potenziale impatto del rischio e fornisce anche un link alla pagina Active IQ che riepiloga tutti i rischi per il nodo di storage (è richiesto l'accesso all'account di supporto NetApp).

Il numero di rischi segnalati viene visualizzato anche nel widget Riepilogo della landing page, con un link alla pagina Active IQ appropriata. In una landing page di *storage*, il conteggio è una somma dei rischi di tutti i nodi di storage sottostanti.



Apertura della pagina Active IQ

Quando si fa clic sul collegamento a una pagina Active IQ, se non si è ancora effettuato l'accesso all'account Active IQ, attenersi alla seguente procedura per visualizzare la pagina Active IQ relativa al nodo di storage.

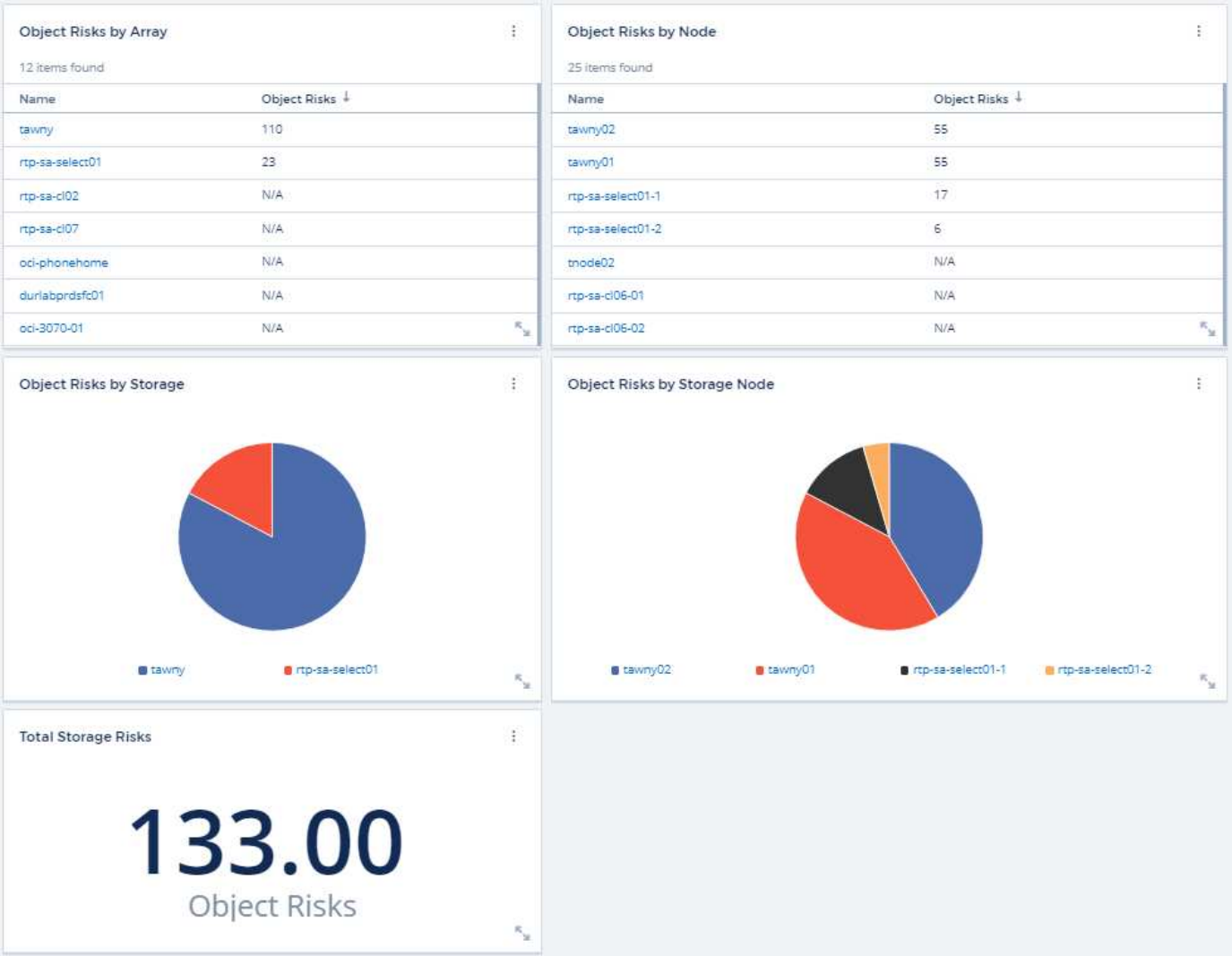
1. Nel widget Riepilogo Cloud Insights o nella tabella rischi, fai clic sul link "Active IQ".
2. Accedi al tuo account NetApp Support. Viene visualizzata direttamente la pagina del nodo di storage in Active IQ.

Query per i rischi

In Cloud Insights, è possibile aggiungere la colonna **monitoring.count** a una query del nodo storage o storage. Se il risultato restituito include sistemi storage monitorati con Active IQ, la colonna monitoring.count visualizza il numero di rischi per il sistema o il nodo storage.

Dashboard

È possibile creare widget (ad esempio grafico a torta, widget tabella, barra, colonna, grafico a dispersione, E single value widgets) per visualizzare i rischi di oggetti per i nodi storage e storage per i sistemi NetApp Clustered Data ONTAP monitorati da Active IQ. È possibile selezionare "rischi oggetto" come colonna o metrica in questi widget, dove Storage o Storage Node sono l'oggetto di interesse.


Object Risks by Array
12 items found
Name
Object Risks
tawny
110
rtp-sa-select01
23
rtp-sa-cl02
N/A
rtp-sa-cl07
N/A
oci-phonehome
N/A
durlabprdsfc01
N/A
oci-3070-01
N/A
Object Risks by Node
25 items found
Name
Object Risks
tawny02
55
tawny01
55
rtp-sa-select01-1
17
rtp-sa-select01-2
6
tnode02
N/A
rtp-sa-cl06-01
N/A
rtp-sa-cl06-02
N/A
Object Risks by Storage
tawny
rtp-sa-select01
Object Risks by Storage Node
tawny02
tawny01
rtp-sa-select01-1
rtp-sa-select01-2
Total Storage Risks
133.00
Object Risks

Risoluzione dei problemi

Risoluzione dei problemi generali di Cloud Insights

Qui troverai suggerimenti per la risoluzione dei problemi di Cloud Insights.

Vedere anche "Risoluzione dei problemi relativi all'unità di acquisizione Linux" e. "Risoluzione dei problemi relativi all'unità di acquisizione di Windows".

Problemi di accesso

Problema:	Provare questo:
Cloud Insights si disconnette ogni 5 minuti	Consentire l'accettazione da parte di terzi dei cookie NetApp e auth0 necessari. Esempio: In Chrome, immettere "Chrome://settings/cookies" nell'URL del browser. Selezionare l'opzione "Allow all cookies" (Consenti tutti i cookie). **O** selezionare "Blocca cookie di terze parti" e aggiungere eccezioni per [**.]auth0.com e [**.]netapp.com. Nota: Quando si crea un'eccezione, assicurarsi di selezionare l'opzione "includere cookie di terze parti in questo sito".
Dispongo di un account Cloud Central ma non riesco ad accedere a Cloud Central.	Aprire un ticket da https://mysupport.netapp.com/site/help. Selezionare la categoria **cloud.netapp.com › account/problemi di accesso** o **cloud.netapp.com › problemi relativi alla federazione**. Questo è specifico per problemi o domande di Cloud Central. Per tutti gli altri problemi di supporto tecnico Cloud Insights, contattare "Supporto NetApp".
Ho ricevuto un invito a Cloud Insights ma ricevo un messaggio "non autorizzato".	Verifica di aver effettuato la registrazione per un account Cloud Central o che la tua organizzazione utilizzi l'accesso SSO con Cloud Central. Verifica che l'indirizzo e-mail del tuo profilo Cloud Central corrisponda all'indirizzo e-mail visualizzato nell'e-mail di benvenuto di Cloud Insights. Se l'indirizzo e-mail non corrisponde, richiedere un nuovo invito con l'indirizzo e-mail corretto.
Mi sono disconnesso da Cloud Central o Cloud Secure e sono stato disconnesso automaticamente da Cloud Insights.	Single Sign-on (SSO) nel cloud NetApp disconnette tutte le sessioni di Cloud Insights, Cloud Secure e reporting. Se si dispone dell'accesso a più account Cloud Insights, la disconnessione da uno qualsiasi disconnette tutte le sessioni attive. Effettua nuovamente l'accesso per accedere all'account.
Sono stato disconnesso automaticamente dopo diversi giorni.	Gli account NetApp Cloud richiedono una nuova autenticazione ogni pochi giorni (l'attuale impostazione Cloud Central è di 7 giorni). Effettua nuovamente l'accesso per accedere all'account.

Problema:	Provare questo:
Viene visualizzato il messaggio di errore "non più autorizzato all'accesso".	Contattare l'amministratore dell'account per verificare l'accesso a Cloud Insights. Verifica che l'indirizzo e-mail del tuo profilo Cloud Central corrisponda all'indirizzo e-mail visualizzato nell'e-mail di benvenuto di Cloud Insights
Altri errori di accesso	Provare la modalità incognito in Chrome o cancellare la cronologia del browser, i cookie e la cache. Provare con un profilo del browser diverso (ad esempio Chrome - Aggiungi persona).

Altri problemi

Domanda:	Risposta:
Le mie quote rigide Qtree vengono visualizzate correttamente nelle query, ma le mie quote morbide vengono visualizzate come capacità totale del volume. È corretto?	Solo le quote rigide, impostate manualmente o tramite Trident, verranno visualizzate come quote impostate; se non vengono specificate quote rigide, la capacità Qtree sarà la capacità del volume interno.
Ho impostato manualmente una quota soft e una hard nello stesso Qtree, ma la capacità totale indicata è la quota hard; è corretto?	Sì, se viene specificata una quota rigida, questa verrà visualizzata come capacità totale.
Quando si inserisce un tempo di pianificazione del rapporto Cognos, a volte mi ritrovo con una "m" extra nel tempo di programmazione. Ad esempio, se si immette l'ora come "02:15 PM", è possibile aggiungere un carattere extra: "02:15 PMM" (o PMM). Quando clicco all'esterno, lo cambia in "2:15:00 AM". È possibile salvare il report, ma quando si riapre il report salvato, l'ora pianificata viene visualizzata come AM (ad esempio, mattina), indipendentemente dal fatto che sia stato inserito AM o PM nell'ora pianificata.	Immettere nuovamente l'ora di programmazione, facendo attenzione a non inserire i caratteri "AM" o "PM" completi; è sufficiente digitare "A" per "AM o "P" per "PM". Se non viene visualizzato il carattere extra, l'ora di programmazione verrà impostata correttamente.

Risorse

Ulteriori suggerimenti per la risoluzione dei problemi sono disponibili nella "Knowledge base di NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili sul sito Cloud Insights "Supporto" pagina.

Se disponi di un abbonamento Cloud Insights attivo, puoi utilizzare le seguenti opzioni di supporto:

"Telefono"
"Ticket di supporto"

Per ulteriori informazioni, consultare "Documentazione di supporto Cloud Insights".

Risoluzione dei problemi relativi all'unità di acquisizione su Linux

Qui troverai suggerimenti per la risoluzione dei problemi relativi alle unità di acquisizione su un server Linux.

Problema:	**Provare questo:**
Lo stato AU nella pagina **osservabilità > Collector** della scheda **unità di acquisizione** visualizza "certificato scaduto" o "certificato revocato" .	Fare clic sul menu a destra dell'AU e selezionare **Restore Connection** (Ripristina connessione). Seguire le istruzioni per ripristinare l'unità di acquisizione: 1. Arrestare il servizio dell'unità di acquisizione (AU). È possibile fare clic sul pulsante *Copy Stop Command* per copiare rapidamente il comando negli Appunti, quindi incollare questo comando in un prompt dei comandi sul computer dell'unità di acquisizione. 2. Creare un file denominato "token" nella cartella */var/lib/netapp/cloudintives/acq/conf* sull'AU. 3. Fare clic sul pulsante *Copy Token* e incollare il token nel file creato. 4. Riavviare il servizio AU. Fare clic sul pulsante *Copy Restart Command* e incollare il comando in un prompt dei comandi sull'AU.
Autorizzazione negata all'avvio del servizio Acquisition Unit Server	Quando l'AU viene installato su SELINUX, se deve essere impostato su *permissive* mode. La modalità *enforcing* non è supportata. Dopo aver impostato SELINUX in modalità permissiva, riavviare il servizio AU. "Scopri di più".
Requisiti del server non soddisfatti	Assicurarsi che il server o la macchina virtuale dell'unità di acquisizione soddisfi i requisiti "requisiti"
Requisiti di rete non soddisfatti	Assicurarsi che il server/VM dell'unità di acquisizione possa accedere all'ambiente Cloud Insights (<environment-name>.c01.cloudinsights.netapp.com) tramite connessione SSL sulla porta 443. Provare i seguenti comandi: *Ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com*
Server proxy non configurato correttamente	Verificare le impostazioni del proxy e, se necessario, disinstallare/reinstallare il software dell'unità di acquisizione per immettere le impostazioni proxy corrette. 1. Provare a "arricciare". Fare riferimento alle informazioni/alla documentazione "man curl" relative ai proxy: --preproxy, --proxy-* (si tratta di un carattere jolly "*" perché curl supporta molte impostazioni proxy). 2. Prova "wget". Consultare la documentazione per le opzioni proxy.

Installazione dell'unità di acquisizione non riuscita in Cloud Insights con errori di credenziale durante l'avvio del servizio di acquisizione (e visibile nel log acq.).	Ciò può essere causato dall'inclusione di caratteri speciali nelle credenziali proxy. Disinstallare l'AU (*sudo cloudindsights-uninstall.sh*) e reinstallarlo senza utilizzare caratteri speciali.
Linux: Libreria mancante / file non trovato	Assicurarsi che il server/VM dell'unità di acquisizione Linux disponga di tutte le librerie necessarie. Ad esempio, è necessario che la libreria *unzip* sia installata sul server. Per installare la libreria *unzip*, eseguire il comando **sudo yum install unzip** prima di eseguire lo script di installazione dell'unità di acquisizione
Problemi di autorizzazione	Assicurati di aver effettuato l'accesso come utente con autorizzazioni *sudo*
Acquisizione non in esecuzione:	Ottenere il acq.log da /opt/netapp/cloudindsights/acq/logs (Linux) riavviare il servizio di acquisizione: Sudo cloudinsights-service.sh riavviare l'acquisizione
Problemi di raccolta dati:	Inviare un report degli errori dalla landing page di Data Collector facendo clic sul pulsante "Send Error Report" (Invia report errori)
Stato: Heartbeat non riuscito	L'unità di acquisizione (AU) invia un heartbeat a Cloud Insights ogni 60 secondi per rinnovarne il lease. Se la chiamata heartbeat non riesce a causa di un problema di rete o di un Cloud Insights che non risponde, il tempo di lease dell'AU non viene aggiornato. Allo scadere del tempo di lease dell'AU, Cloud Insights mostra lo stato "Heartbeat Failed" (battito cardiaco non riuscito). Procedura per la risoluzione dei problemi: Controllare la connessione di rete tra il server dell'unità di acquisizione e CloudInsights. Verificare che il servizio Acquisition Unit sia in esecuzione. Se il servizio non è in esecuzione, avviarlo. Controllare il log dell'unità di acquisizione (/var/log/netapp/cloudintives/acq/acq.log) per verificare la presenza di errori.
Viene visualizzato il messaggio "Heartbeat Error: (Errore heartbeat: Errore heartbeat	Questo errore può verificarsi se si verifica un'interruzione di rete che causa l'interruzione della comunicazione tra l'unità di acquisizione e l'ambiente Cloud Insights per più di un minuto. Verificare che la connessione tra AU e Cloud Insights sia stabile e attiva.

Considerazioni su Proxy e Firewall

Se l'organizzazione richiede l'utilizzo del proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy dell'organizzazione e cercare alcune eccezioni per il funzionamento di Cloud Insights. Tenere presente quanto segue:

- Innanzitutto, l'organizzazione blocca l'accesso per impostazione predefinita e consente solo l'accesso a siti/domini Web specifici per eccezione? In tal caso, sarà necessario aggiungere il seguente dominio

all'elenco delle eccezioni:

```
*.cloudinsights.netapp.com
```

L'unità di acquisizione Cloud Insights, così come le interazioni in un browser Web con Cloud Insights, andranno tutti agli host con quel nome di dominio.

- In secondo luogo, alcuni proxy tentano di eseguire l'ispezione TLS/SSL impersonando i siti Web Cloud Insights con certificati digitali non generati da NetApp. Il modello di sicurezza dell'unità di acquisizione Cloud Insights è fondamentalmente incompatibile con queste tecnologie. Per consentire all'unità di acquisizione Cloud Insights di accedere correttamente a Cloud Insights e facilitare il rilevamento dei dati, è necessario anche il nome di dominio sopra indicato, ad eccezione di questa funzionalità.

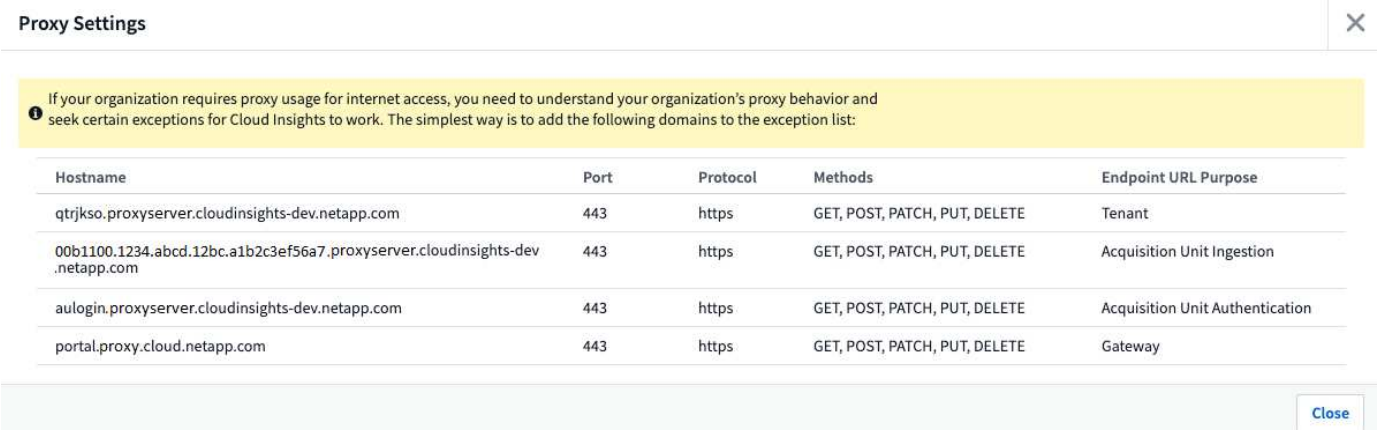
Nel caso in cui il proxy sia impostato per l'ispezione del traffico, l'ambiente Cloud Insights deve essere aggiunto a un elenco di eccezioni nella configurazione del proxy. Il formato e la configurazione di questo elenco di eccezioni variano in base all'ambiente e agli strumenti proxy, ma in generale è necessario aggiungere gli URL dei server Cloud Insights a questo elenco di eccezioni per consentire all'AU di comunicare correttamente con tali server.

Il modo più semplice per farlo è aggiungere il dominio Cloud Insights stesso all'elenco delle eccezioni:

```
 *.cloudinsights.netapp.com
Nel caso in cui il proxy non sia configurato per l'ispezione del traffico,
potrebbe essere necessario un elenco di eccezioni. Se non si è sicuri
della necessità di aggiungere Cloud Insights a un elenco di eccezioni o se
si riscontrano difficoltà nell'installazione o nell'esecuzione di Cloud
Insights a causa della configurazione del proxy e/o del firewall,
rivolgersi al team di amministrazione del proxy per impostare la gestione
dell'intercettazione SSL da parte del proxy.
```

Visualizzazione degli endpoint proxy

Per visualizzare gli endpoint proxy, fare clic sul collegamento **Proxy Settings** (Impostazioni proxy) quando si sceglie un data collector durante l'acquisizione oppure sul collegamento *Proxy Settings* (Impostazioni proxy) nella pagina **Help > Support** (Guida > supporto). Viene visualizzata una tabella simile alla seguente. Se nel proprio ambiente si dispone di workload Security, in questo elenco vengono visualizzati anche gli URL degli endpoint configurati.



Risorse

Ulteriori suggerimenti per la risoluzione dei problemi sono disponibili nella "Knowledge base di NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili sul sito Cloud Insights "Supporto" pagina.

Risoluzione dei problemi relativi all'unità di acquisizione su Windows

Qui troverai suggerimenti per la risoluzione dei problemi relativi alle unità di acquisizione su un server Windows.

Problema:	Provare questo:
Lo stato AU nella pagina **osservabilità > Collector** della scheda **unità di acquisizione** visualizza "certificato scaduto" o "certificato revocato" .	Fare clic sul menu a destra dell'AU e selezionare **Restore Connection** (Ripristina connessione). Seguire le istruzioni per ripristinare l'unità di acquisizione: 1. Arrestare il servizio dell'unità di acquisizione (AU). È possibile fare clic sul pulsante *Copy Stop Command* per copiare rapidamente il comando negli Appunti, quindi incollare questo comando in un prompt dei comandi sul computer dell'unità di acquisizione. Creare un file denominato "token" nella cartella *c:/programmi/Cloud Insights/Acquisition Unit/conf dell'AU. 3. Fare clic sul pulsante _Copy Token* e incollare il token nel file creato. 4. Riavviare il servizio AU. Fare clic sul pulsante *Copy Restart Command* e incollare il comando in un prompt dei comandi sull'AU.
Requisiti del server non soddisfatti	Assicurarsi che il server o la macchina virtuale dell'unità di acquisizione soddisfi i requisiti "requisiti"

Requisiti di rete non soddisfatti	Assicurarsi che il server/VM dell'unità di acquisizione possa accedere all'ambiente Cloud Insights (<environment-name>.c01.cloudinsights.netapp.com) tramite connessione SSL sulla porta 443. Provare i seguenti comandi: *Ping <environment-name>.c01.cloudinsights.netapp.com traceroute <environment-name>.c01.cloudinsights.netapp.com curl https://<environment-name>.c01.cloudinsights.netapp.com wget https://<environment-name>.c01.cloudinsights.netapp.com*
Server proxy non configurato correttamente	Verificare le impostazioni del proxy e, se necessario, disinstallare/reinstallare il software dell'unità di acquisizione per immettere le impostazioni proxy corrette. 1. Provare a "arricciare". Fare riferimento alle informazioni/alla documentazione "man curl" relative ai proxy: --preproxy, --proxy-* (si tratta di un carattere jolly "*" perché curl supporta molte impostazioni proxy). 2. Prova "wget". Consultare la documentazione per le opzioni proxy.
Installazione dell'unità di acquisizione non riuscita in Cloud Insights con errori di credenziale durante l'avvio del servizio di acquisizione (e visibile nel log acq.).	Ciò può essere causato dall'inclusione di caratteri speciali nelle credenziali proxy. Disinstallare l'AU (*sudo cloudindsights-uninstall.sh*) e reinstallarlo senza utilizzare caratteri speciali.
Problemi di autorizzazione	Assicurarsi di aver effettuato l'accesso come utente con autorizzazioni di amministratore
Acquisizione non in esecuzione	Le informazioni sono disponibili nel file acq.log nella cartella *<install directory>/informazioni sul cloud/unità di acquisizione/log*. Riavviare l'acquisizione tramite i servizi Windows
Problemi di raccolta dati	Inviare un report degli errori dalla landing page di Data Collector facendo clic sul pulsante "Send Error Report" (Invia report errori)
Stato: Heartbeat non riuscito	L'unità di acquisizione (AU) invia un heartbeat a Cloud Insights ogni 60 secondi per rinnovarne il lease. Se la chiamata heartbeat non riesce a causa di un problema di rete o di un Cloud Insights che non risponde, il tempo di lease dell'AU non viene aggiornato. Allo scadere del tempo di lease dell'AU, Cloud Insights mostra lo stato "Heartbeat Failed" (battito cardiaco non riuscito). Procedura per la risoluzione dei problemi: * Controllare la connessione di rete tra il server dell'unità di acquisizione e CloudInsights. * Controllare se il servizio dell'unità di acquisizione è in esecuzione. Se il servizio non è in esecuzione, avviarlo. * Controllare il registro dell'unità di acquisizione (<Install dir>: File di programma/informazioni cloud/unità di acquisizione/log) per verificare se sono presenti errori.

Viene visualizzato il messaggio "Heartbeat Error: (Errore heartbeat: Errore heartbeat	Questo errore può verificarsi se si verifica un'interruzione di rete che causa l'interruzione della comunicazione tra l'unità di acquisizione e l'ambiente Cloud Insights per più di un minuto. Verificare che la connessione tra AU e Cloud Insights sia stabile e attiva.

Considerazioni su Proxy e Firewall

Se l'organizzazione richiede l'utilizzo del proxy per l'accesso a Internet, potrebbe essere necessario comprendere il comportamento del proxy dell'organizzazione e cercare alcune eccezioni per il funzionamento di Cloud Insights. Tenere presente quanto segue:

- Innanzitutto, l'organizzazione blocca l'accesso per impostazione predefinita e consente solo l'accesso a siti/domini Web specifici per eccezione? In tal caso, sarà necessario aggiungere il seguente dominio all'elenco delle eccezioni:

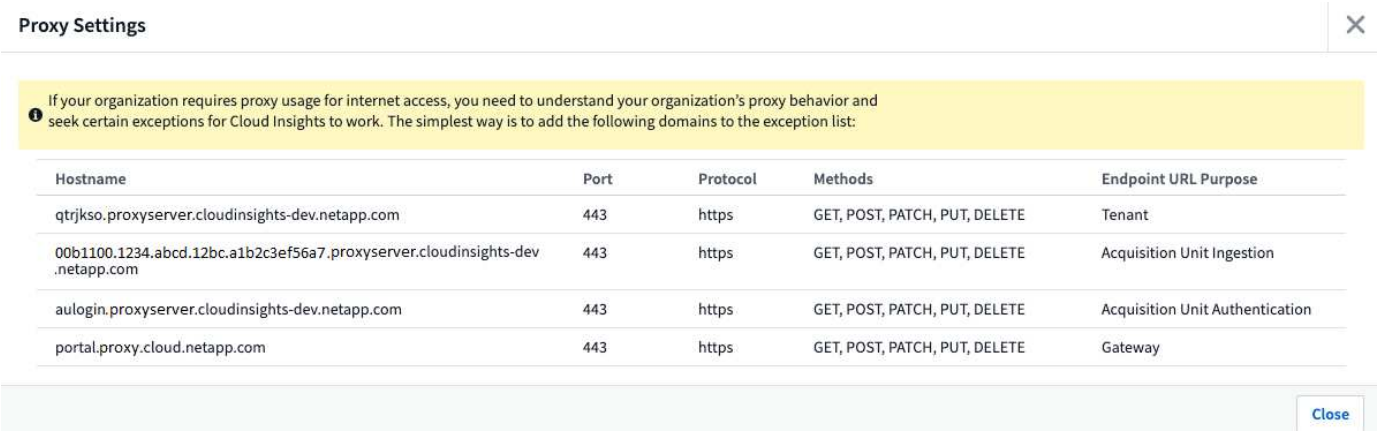
  ```
  *.cloudinsights.netapp.com
  ```

  L'unità di acquisizione Cloud Insights, così come le interazioni in un browser Web con Cloud Insights, andranno tutti agli host con quel nome di dominio.

- In secondo luogo, alcuni proxy tentano di eseguire l'ispezione TLS/SSL impersonando i siti Web Cloud Insights con certificati digitali non generati da NetApp. Il modello di sicurezza dell'unità di acquisizione Cloud Insights è fondamentalmente incompatibile con queste tecnologie. Per consentire all'unità di acquisizione Cloud Insights di accedere correttamente a Cloud Insights e facilitare il rilevamento dei dati, è necessario anche il nome di dominio sopra indicato, ad eccezione di questa funzionalità.

Visualizzazione degli endpoint proxy

Per visualizzare gli endpoint proxy, fare clic sul collegamento **Proxy Settings** (Impostazioni proxy) quando si sceglie un data collector durante l'acquisizione oppure sul collegamento *Proxy Settings* (Impostazioni proxy) nella pagina **Help > Support** (Guida > supporto). Viene visualizzata una tabella simile alla seguente. Se nel proprio ambiente si dispone di workload Security, in questo elenco vengono visualizzati anche gli URL degli endpoint configurati.



Risorse

Ulteriori suggerimenti per la risoluzione dei problemi sono disponibili nella "Knowledge base di NetApp" (è richiesto l'accesso al supporto).

Ulteriori informazioni di supporto sono disponibili sul sito Cloud Insights "Supporto" pagina.

Ricerca di un data collector guasto

Se un data collector presenta un messaggio di errore e un impatto alto o medio, è necessario ricercare il problema utilizzando la pagina di riepilogo del data collector con le relative informazioni collegate.

Attenersi alla seguente procedura per determinare la causa dei dati non riusciti. I messaggi di errore di Data Collector vengono visualizzati nel menu **Admin** e nella pagina **Installed Data Collector**.

Fasi

1. Fare clic su **Admin** > **Data Collector** > **Installed Data Collector**.
2. Fare clic sul Linked Name (Nome collegato) del data collector in errore per aprire la pagina Summary (Riepilogo).
3. Nella pagina Summary (Riepilogo), consultare l'area Comments (commenti) per leggere eventuali note lasciate da un altro tecnico che potrebbe anche esaminare questo guasto.
4. Annotare eventuali messaggi relativi alle prestazioni.
5. Spostare il puntatore del mouse sui segmenti del grafico della cronologia degli eventi per visualizzare ulteriori informazioni.
6. Selezionare un messaggio di errore per un dispositivo e visualizzato sotto la cronologia degli eventi, 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 dispositivi segnalati da questo Data Collector, è possibile filtrare l'elenco in modo da visualizzare solo i dispositivi di interesse ed è possibile fare clic sul collegamento **Nome** di un dispositivo per visualizzare la pagina delle risorse per tale dispositivo.
8. Quando si torna alla pagina di riepilogo del data collector, controllare l'area **Show Recent Changes** (Mostra modifiche recenti) nella parte inferiore della pagina per verificare se le modifiche recenti potrebbero aver causato il problema.

Matrice di supporto per data collector Cloud Insights

La matrice di supporto del Data Collector fornisce riferimenti per i Data Collector supportati da Cloud Insights, incluse informazioni su vendor e modello.

Storage HP Enterprise 3PAR/Alletra 9000/Primera StoreServ

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
HPE Alletra 9080 HPE_3PAR 20450 HPE_3PAR 20800 HPE_3PAR 20850 HPE_3PAR 20850_R2 HPE_3PAR 7200c HPE_3PAR 7400 HPE_3PAR 7440c HPE_3PAR 7450c HPE_3PAR 8200 HPE_3PAR 8400 HPE_3PAR 8440 HPE_3PAR 8450 HPE_3PAR 9450 HPE_3PAR A630 HPE_3PAR A650 HPE_3PAR A670 HP_3PAR 20800 HP_3PAR 7200 HP_3PAR 7200c HP_3PAR 7400 HP_3PAR 7400c HP_3PAR 7450c HP_3PAR 8200 HP_3PAR 8400 InServ F400 InServ T400 InServ T800 InServ V400	N. 3.1.1 (MU1) N. 3.1.2 (MU3) N. 3.1.3 (MU1) N. 3.1.3 (MU2) N. 3.1.3 (MU3) N. 3.2.1 (MU3) N. 3.2.1 (MU5) 3.2.2 N. 3.2.2 (MU2) N. 3.2.2 (MU4) N. 3.2.2 (MU6) N. 3.3.1 (MU1) N. 3.3.1 (MU2) N. 3.3.1 (MU5) 3.3.2 N. 3.3.2 (MU1) 4.4.1 tipo di rilascio: Versione di supporto standard 4.5.11 tipo di rilascio: Versione con supporto esteso 4.5.3 tipo di rilascio: Versione con supporto esteso 4.5.7 tipo di rilascio: Versione con supporto esteso 9.5.8 tipo di rilascio: Versione con supporto esteso

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
618					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		(Controller protocollo)			
		Porta storage	Implementato	SSH	
		Tipo	Distanza	SSH	
	Maschera di volume	Iniziatore	Implementato	SSH	
		Protocol Controller (Controller protocollo)	Implementato	SSH	
		Porta storage	Implementato	SSH	
		Tipo	Distanza	SSH	
	Rif. Volume	Nome	Implementato	SSH	
		IP dello storage	Implementato	SSH	
	Alias WWN	Alias host	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		Origine	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Throughput	Implementato	SMI-S.	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	SMI-S.	
		Totale rapporto di hit della cache	Implementato	SMI-S.	
		Cache hit ratio Write	Implementato	SMI-S.	
		Capacità raw	Implementato	SMI-S.	
		Capacità totale	Implementato	SMI-S.	
		Capacità utilizzata	Implementato	SMI-S.	
		Rapporto capacità utilizzata	Implementato	SMI-S.	
		CapacityRatio scritto	Implementato	SMI-S.	
		IOPS Read (lettura IOPS)	Implementato	SMI-S.	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	SMI-S.	
		Scrittura IOPS	Implementato	SMI-S.	
		Latenza di lettura	Implementato	SMI-S.	
		Latenza totale	Implementato	SMI-S.	
		Scrittura latenza	Implementato	SMI-S.	
		Rapporto di blocco parziale	Implementato	SMI-S.	
		Throughput Read (lettura throughput)	Implementato	SMI-S.	
		Throughput totale	Implementato	SMI-S.	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	SMI-S.	
		Scrittura in sospeso	Implementato	SMI-S.	totale scrittura in sospeso

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
3PAR SMI-S	SMI-S.	HTTP/HTTPS	5988/5989		vero	vero	vero	vero
CLI 3PAR	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

Amazon AWS EC2

Modelli e versioni supportati da questo data collector:

Versioni API
2014-10-01

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Disco VirtualMachine	OID	Implementato	HTTPS	
		OID VirtualDisk	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		OID VirtualMachine	Implementato	HTTPS	
	Host	Sistema operativo host	Implementato	HTTPS	
		IPS	Implementato	HTTPS	
		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		OID	Implementato	HTTPS	
	Info	Descrizione API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome origine dati	Implementato	HTTPS	Info
		Data	Implementato	HTTPS	
		ID mittente	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	macchina virtuale	Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Utilizzo totale della CPU	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		DiskIops.total	Implementato	HTTPS	
		IOPS su disco in scrittura	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Lettura throughput disco	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	throughput totale del disco letto
		Scrittura throughput disco	Implementato	HTTPS	
		Lettura throughput IP	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Throughput IP totale
		IpThroughput.write	Implementato	HTTPS	
		Utilizzo totale della memoria	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API EC2	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all’inizio

Amazon AWS S3

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
S3	2010-08-01

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
640					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dischi spare)
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Pool di storage	Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
performance	Volume interno	Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Oggetti totali	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API S3	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Microsoft Azure NetApp Files

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli
2019-06-01	Azure NetApp Files

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dischi spare)
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Pool di storage	Capacità allocata dei dati	Distanza	HTTPS	capacità allocata per i dati
		Data used Capacity (capacità utilizzata dati)	Implementato	HTTPS	
		Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		Stato	Implementato	HTTPS	
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

		(capacità utilizzata dati)			
		Capacità Snapshot	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Disco StoragePool	IOPS Read (lettura IOPS)	Implementato		Numero di IOPS letti sul disco
		Totale IOPS	Implementato		
		Scrittura IOPS	Implementato		
		Throughput Read (lettura throughput)	Implementato		
		Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato		

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Azure NetApp Files	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Switch Fibre Channel Brocade

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
178,0	v5,3.2c
183,0	v6,2.1b
Brocade 200E	v6,2.2g
Brocade 300E	v6,3.2
Brocade 3900	v6,4.1a
Brocade 4024 integrato	v6,4.2
Brocade 48000	v6,4.2a
Brocade 5000	v7,0.0
Brocade 5100	v7,0.1b
Brocade 5300	v7,1.0c
Brocade 5480 integrato	v7,3.0c
Brocade 6505	v7,3.1d
Brocade 6510	v7,4.1d
Brocade 6520	v7,4.1f
Brocade 6548	v7,4.2a
Brocade 7800	v7,4.2c
Brocade 7840	v7,4.2d
Brocade DCX	v7,4.2g
Backbone Brocade DCX-4S	v7,4.2g_cvr_824494_01
Brocade DCX8510-4	v7,4.2h
Brocade DCX8510-8	v7,4.2j1
Brocade G610	v8,0.2a
Brocade G620	v8,0.2c
Brocade G630	v8,0.2d
Brocade G720	v8,1.2g
Brocade M5424 integrato	v8,1.2j
Brocade X6-4	v8,1.2k
Brocade X6-8	v8,2.0
Brocade X7-4	v8,2.0b
Brocade X7-8	v8,2.1c
	v8,2.1d
	v8,2.2a
	v8,2.2b
	v8,2.2c
	v8,2.2d
	v8,2.2d4
	v8,2.3
	v8,2.3a
	v8,2.3a1
	v8,2.3b
	v8,2.3c
	v8,2.3c1
	v9,0.0b
	v9,0.1a
	v9,0.1b4
	v9,0.1c
	v9,0.1d
	v9,0.1e
	v9,0.1e1
	v9,1.0b
	v9,1.1
	v9,1.1_01
	v9,1.1b

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
654					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		WWN	Implementato	SSH	
	Zona	Nome zona	Implementato	SSH	
	Membro di zona	Tipo	Distanza	SSH	
		WWN	Implementato	SSH	
	Funzionalità di zoning	Configurazione attiva	Implementato	SSH	
		Nome configurazione	Implementato	SSH	
		Comportamento predefinito dello zoning	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

		Frame rate del traffico	Implementato	SNMP	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Traffico totale	Implementato	SNMP	
		Frame rate del traffico	Implementato	SNMP	
		Dimensione media dei fotogrammi	Implementato	SNMP	Dimensione media del traffico dei frame
		Frame TX	Implementato	SNMP	dimensione media del frame del traffico
		Velocità di traffico	Implementato	SNMP	
		Tasso di traffico totale	Implementato	SNMP	
		Velocità di traffico	Implementato	SNMP	
		Utilizzo del traffico	Implementato	SNMP	
		Utilizzo del traffico	Implementato	SNMP	Utilizzo totale del traffico
		Utilizzo del traffico	Implementato	SNMP	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
SNMP Brocade	SNMP	SNMPv1, SNMPv2, SNMPv3	161		vero	vero	vero	vero
SSH Brocade	SSH	SSH	22		falso	falso	vero	vero
Configurazione guidata origine dati	Immissione manuale				vero	vero	vero	vero

Torna all'inizio

HTTP di Brocade Network Advisor

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
14.4.1 14.4.3 14.4.4 14.4.5	Brocade 5300 Brocade 6510 Brocade 6520 Brocade 6548 Brocade DCX 8510-8 Brocade G620 DS-6620B EMC CONNECTIX ED-DCX8510-8B	v7,2.1a v7,3.1a v7,4.1b v7,4.2d v8,2.3b v8,2.3c v9,0.1a v9,0.1b v9,0.1e1

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Stato dello switch	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
		WWN	Implementato	HTTP/S	
	Sconosciuto	Driver	Implementato	HTTP/S	
		Firmware	Implementato	HTTP/S	
		Produttore	Implementato	HTTP/S	
		Modello	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	
	Alias WWN	Alias host	Implementato	HTTP/S	
		Tipo di oggetto	Implementato	HTTP/S	
		Origine	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	
	Zona	Nome zona	Implementato	HTTP/S	
	Membro di zona	Tipo	Distanza	HTTP/S	
		WWN	Implementato	HTTP/S	
	Funzionalità di zoning	Configurazione attiva	Implementato	HTTP/S	
		Nome configurazione	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance	porta	BbCreditZero.total	Implementato	HTTP/S	
		Credito BB	Implementato	HTTP/S	
		BbCreditZeroms	Implementato	HTTP/S	
		PortErrors.class3 Discard	Implementato	HTTP/S	
		PortErrors.crc	Implementato	HTTP/S	
		Errore porta	Implementato	HTTP/S	
		Errore porta	Implementato	HTTP/S	Errori di porta dovuti a frame breve
		PortErrors.linkFailure	Implementato	HTTP/S	Errori di porta errore di collegamento
		Errore porta	Implementato	HTTP/S	Errori di porta perdita del segnale
		Errore porta	Implementato	HTTP/S	Errore di porta perdita di sincronizzazione
		Errore porta	Implementato	HTTP/S	timeout errori porta scartato
		Errore porta	Implementato	HTTP/S	Totale errori di porta
		Velocità di traffico	Implementato	HTTP/S	
		Tasso di traffico totale	Implementato	HTTP/S	
		Velocità di traffico	Implementato	HTTP/S	
		Utilizzo del traffico	Implementato	HTTP/S	
		Utilizzo del traffico	Implementato	HTTP/S	Utilizzo totale del traffico
		Utilizzo del traffico	Implementato	HTTP/S	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Brocade Network Advisor	HTTP/HTTPS	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

Brocade FOS REST

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
Brocade 6505 Brocade G720 Brocade X6-8	v8,2.3c v8,2.3c1 v9,0.1e1 v9,1.1b

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		WWN	Implementato	HTTPS	
	Zona	Nome zona	Implementato	HTTPS	
	Membro di zona	Tipo	Distanza	HTTPS	
		WWN	Implementato	HTTPS	
	Funzionalità di zoning	Configurazione attiva	Implementato	HTTPS	
		Nome configurazione	Implementato	HTTPS	
		Comportamento predefinito dello zoning	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

		Frame rate traffico totale	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Dimensione media dei fotogrammi	Implementato	HTTPS	Dimensione media del traffico dei frame
		Frame TX	Implementato	HTTPS	dimensione media del frame del traffico
		Velocità di traffico	Implementato	HTTPS	
		Tasso di traffico totale	Implementato	HTTPS	
		Velocità di traffico	Implementato	HTTPS	
		Utilizzo del traffico	Implementato	HTTPS	
		Utilizzo del traffico	Implementato	HTTPS	Utilizzo totale del traffico
		Utilizzo del traffico	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST FOS BROCADE	HTTPS		443		vero	vero	vero	vero

Torna all'inizio

Switch Cisco MDS e Nexus Fabric

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
8978-E04 CN1610 DS-C9124-2-K9 DS-C9124-K9 DS-C9132T-K9 DS-C9134-K9 DS-C9148-16P-K9 DS-C9148-32P-K9 DS-C9148-48P-K9 DS-C9148S-K9 DS-C9148T-K9 DS-C9222I-K9 DS-C9250I-K9 DS-C9396S-K9 DS-C9396T-K9 DS-C9506 DS-C9509 DS-C9513 DS-C9706 DS-C9710 DS-C9718 DS-HP-8GFC-K9 DS-HP-FC-K9 N5K-C5548UP N5K-C5596UP N5K-C56128P N5K-C5696Q UCS-FI-6248UP UCS-FI-6296UP UCS-FI-6332 UCS-FI-6332-16UP UCS-FI-6454	n. 3,3 (1c) n. 4,1 (3a) n. 5,0 (1a) 5,0 (3)N2 (3,11e) 5,0 (3)N2 (3,23o) 5,0 (3)N2 (4,01d) 5,0 (3)N2 (4,04e) 5,0 (3)N2 (4,13e) 5,0 (3)N2 (4,13i) 5,0 (3)N2 (4,21e) 5,0 (3)N2 (4,21j) 5,0 (3)N2 (4,21k) 5,0 (3)N2 (4,22c) N. 5,0 (8) n. 5,2 (2d) 5,2 (3)N2 (2,28g) n. 5,2 (6a) N. 5,2 (8) n. 5,2 (8b) n. 5,2 (8c) n. 5,2 (8d) n. 5,2 (8f) n. 5,2 (8g) n. 5,2 (8h) n. 5,2 (8i) N. 6,2 (1) N. 6,2 (11) n. 6,2 (11b) n. 6,2 (11c) n. 6,2 (11e) N. 6,2 (13) n. 6,2 (13a) N. 6,2 (15) N. 6,2 (17) N. 6,2 (19) N. 6,2 (21) N. 6,2 (23) N. 6,2 (25) N. 6,2 (27) N. 6,2 (29) N. 6,2 (31) N. 6,2 (33) N. 6,2 (5) n. 6,2 (5a) N. 6,2 (7) N. 6,2 (9) n. 6,2 (9a) n. 6,2 (9c) 7,3 (0)D1 (1) 7,3(0)DY(1) 7,3(1)DY(1) 7,3 (1)N1 (1) 7,3 (13)N1 (1) 7,3 (6)N1 (1)

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
676					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		WWN	Implementato	SNMP	
		Tipo	Distanza	SNMP	
		VSAN attivato	Implementato	SNMP	
		WWN	Implementato	SNMP	
	Sconosciuto	Driver	Implementato	SNMP	
		Firmware	Implementato	SNMP	
		Generato	Implementato	SNMP	
		Produttore	Implementato	SNMP	
		Modello	Implementato	SNMP	
		Nome	Implementato	SNMP	
		WWN	Implementato	SNMP	
	Alias WWN	Alias host	Implementato	SNMP	
		Tipo di oggetto	Implementato	SNMP	
		Origine	Implementato	SNMP	
		WWN	Implementato	SNMP	
	Zona	Nome zona	Implementato	SNMP	
		Tipo di zona	Implementato	SNMP	
	Membro di zona	Tipo	Distanza	SNMP	
		WWN	Implementato	SNMP	
	Funzionalità di zoning	Configurazione attiva	Implementato	SNMP	
		Nome configurazione	Implementato	SNMP	
		Comportamento predefinito dello zoning	Implementato	SNMP	
		Controllo Unione	Implementato	SNMP	
		WWN	Implementato	SNMP	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

		Frame rate traffico totale	Implementato	SNMP	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Dimensione media dei fotogrammi	Implementato	SNMP	Dimensione media del traffico dei frame
		Frame TX	Implementato	SNMP	dimensione media del frame del traffico
		Velocità di traffico	Implementato	SNMP	
		Tasso di traffico totale	Implementato	SNMP	
		Velocità di traffico	Implementato	SNMP	
		Utilizzo del traffico	Implementato	SNMP	
		Utilizzo del traffico	Implementato	SNMP	Utilizzo totale del traffico
		Utilizzo del traffico	Implementato	SNMP	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
SNMP Cisco	SNMP	SNMPv1 (solo inventario), SNMPv2, SNMPv3	161		vero	vero	vero	vero

Torna all'inizio

Cohesity

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
C2500 C2505 Nodo di calcolo c4000 C4600 C5036 C5066 C6025 C6035 C6055 PXG1 UCS-C240M5H10	6,5.1f_release-20210913_13f6a4bf 6,5.1f_u1_release-20211027_9e40cb 6,6.0d_u6_release-20221204_c03629f0 6,8.1_release-20220807_6c9115ef 6,8.1_u1_release-20221022_6f58ed2a 6,8.1_u2_release-20230412_5ced2ed3 6,8.1_u3_release-20230509_1e641b74 7,0_u1_release-20230222_8995f044

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			
		Capacità totale utilizzata	Implementato		Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza		
		Virtuale	Implementato		Si tratta di un dispositivo per la virtualizzazione dello storage?
		Crittografato	Implementato		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
688					

					scrittura su tutti i dischi) in MB/s.
	Totale IOPS	Implementato			Scrittura latenza
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato			Totale utilizzo	Implementato
			Disco StoragePool	IOPS Read (lettura IOPS)	Implementato
		Numero di IOPS letti sul disco		Scrittura IOPS	Implementato
				Throughput Read (lettura throughput)	Implementato
				Scrittura throughput	Implementato
				Throughput totale	Implementato
		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Totale IOPS	Implementato

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Cohesity	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

EMC Celerra (SSH)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
NS-480FC NSX VG8 VNX5200 VNX5300 VNX5400 VNX5600 VNX7600	5,5.38-1 6,0.65-2 7,1.76-4 7,1.79-8 7,1.83-2 8,1.21-266 8,1.21-303 8,1.9-155

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo per la virtualizzazione dello storage?

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
Celerra CLI	SSH	SSH			vero	falso	vero	vero

Torna all'inizio

EMC CLARiiON (navicli)

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
6,23 6,26 6,28 7,30 7,32 7,33	AX4-5F8 CX3-20f CX3-40f CX4-480 VNX5100 VNX5200 VNX5300 VNX5400 VNX5500 VNX5600 VNX5700 VNX5800 VNX7600 VNX8000	04.28.000.5.710 04.30.000.5.525 05.32.000.5.218 05.32.000.5.219 05.32.000.5.221 05.32.000.5.225 05.32.000.5.249 05.33.000.5.074 05.33.009.5.155 05.33.009.5.184 05.33.009.5.186 05.33.009.5.218 05.33.009.5.231 05.33.009.5.236 05.33.009.5.238 05.33.009.6.305 05.33.021.5.256 05.33.021.5.266 2.23.50.5.710 3.26.20.5.011 3.26.40.5.029

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		storage			
		Con thin provisioning	Implementato	CLI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza	CLI	
		UUID	Implementato	CLI	
		Capacità utilizzata	Implementato	CLI	
	Mappa del volume	LUN	Implementato	CLI	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	CLI	
		Porta storage	Implementato	CLI	
		Tipo	Distanza	CLI	
	Maschera di volume	Iniziatore	Implementato	CLI	
		Protocol Controller (Controller protocollo)	Implementato	CLI	
		Porta storage	Implementato	CLI	
		Tipo	Distanza	CLI	
	Membro del volume	Capacità	Implementato	CLI	Snapshot ha utilizzato la capacità in MB
		Nome	Implementato	CLI	
		Classifica	Implementato	CLI	
		Capacità raw totale	Implementato	CLI	Capacità raw totale (somma di tutti i dischi dell’array)
		Ridondanza	Implementato	CLI	Livello di ridondanza
		ID pool di storage	Implementato	CLI	
		Capacità utilizzata	Implementato	CLI	
	Alias WWN	Alias host	Implementato	CLI	
		IP	Implementato	CLI	
		Tipo di oggetto	Implementato	CLI	
		Origine	Implementato	CLI	
		WWN	Implementato	CLI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dischi) in MB/s.
		Scrittura throughput	Implementato	CLI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Utilizzo in lettura	Implementato	CLI	
		Totale utilizzo	Implementato	CLI	
		Scrittura utilizzo	Implementato	CLI	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	CLI	
		Totale rapporto di hit della cache	Implementato	CLI	
		Cache hit ratio Write	Implementato	CLI	
		Capacità raw	Implementato	CLI	
		Capacità totale	Implementato	CLI	
		Capacità utilizzata	Implementato	CLI	
		Rapporto capacità utilizzata	Implementato	CLI	
		IOPS Read (lettura IOPS)	Implementato	CLI	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	CLI	
		Scrittura IOPS	Implementato	CLI	
		Latenza di lettura	Implementato	CLI	
		Latenza totale	Implementato	CLI	
		Scrittura latenza	Implementato	CLI	
		Rapporto di blocco parziale	Implementato	CLI	
		Throughput Read (lettura throughput)	Implementato	CLI	
		Throughput totale	Implementato	CLI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	CLI	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI navi	CLI		6389,2162,2163,443(HTTPS)/80(HTTP)		vero	vero	vero	falso

Torna all'inizio

EMC Data Domain (SSH)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
GG VE DD2200 DD2500 DD3300 DD4200 DD6300 DD6800 DD6900 DD7200 DD9300 DD9400 DD9500 DD9800 DD990 DD9900	6,1.2.051-633576 6,1.2.20-606786 6,1.2.50-632120 6,2.0.30-629757 6,2.0.35-635767 6,2.1.30-663869 6,2.1.40-671977 6,2.1.60-686365 7.10.0.0-1017741 7.10.1.0-1042928 7,2.0.30-663847 7,2.0.50-671975 7,2.0.60-682124 7,2.0.70-686759 7,2.0.90-692270 7,6.0.20-689174 7,6.0.30-690691 7,7.0.7-1007134 7,7.1.10-1011247 7,7.2.011-1011427 7,7.2.10-1011249 7,7.3.0-1011963 7,7.4.0-1017976 7,7.5.1-1040473 7,7.5.11-1046187 7,8.0.0-1008134

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
712					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dalla capacità utilizzabile alla capacità raw
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Thin provisioning supportato	Implementato	SSH	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	SSH	
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
		Tipo	Distanza	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo per la virtualizzazione dello storage?

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI del dominio dati	SSH	SSH	22		vero	vero	vero	vero

Torna all'inizio

EMC ECS

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
ECS	3.6.1.1 3.6.1.3 3.6.2.1 3.6.2.4 3.7.0.0 3.7.0.3 3.7.0.4 3.7.0.5 3.8.0.1 3.8.0.2

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		in MB			
		Utilizzo della capacità del	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Pool di storage	Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
726					

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Disco StoragePool	Provisioning della capacità	Implementato	HTTPS	
		Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto di capacità di overcommit	Implementato	HTTPS	Riportato come serie temporale
		Rapporto capacità utilizzata	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC ECS	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Dell EMC Isilon e PowerScale REST

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
R200 A2000 R300 A3000 F200 F600 F800 F900 H400 H500 NL410 S210 X210 X400 X410	9.1.0.11 9.1.0.6 9.2.1.10 9.2.1.11 9.2.1.12 9.2.1.16 9.2.1.19 9.2.1.21 9.2.1.6 9.2.1.7 9.2.1.9 9.4.0.11 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.5 9.4.0.7 9.5.0.3 v8,0.0,4 v8,0.0,6 v8,0.0,7 v8,1.2,0 v8,2.2,0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		di Snapshot			di snapshot in MB
		Capacità	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Snapshot			
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
740					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		utilizzata Snapshot			
		Throughput	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Read (lettura throughput)			
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC Isilon e PowerScale	HTTPS		443		vero	vero	vero	vero

Torna all'inizio

Dell EMC Isilon/PowerScale (CLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
R200 A2000 R300 F200 F800 F900 H400 H500 H600 H700 NL400 NL410 S210 X200 X210 X400 X410	9.1.0.10 9.1.0.12 9.1.0.16 9.1.0.18 9.1.0.19 9.1.0.7 9.2.1.11 9.2.1.13 9.2.1.15 9.2.1.22 9.2.1.7 9.2.1.9 9.3.0.3 9.4.0.0 9.4.0.10 9.4.0.12 9.4.0.13 9.4.0.14 9.4.0.6 9.4.0.7 v7,1.1,8 v7,2.0,5 v7,2.1,3 v7,2.1,6 v8,0.0,4 v8,0.0,6 v8,0.0,7 v8,0.1,1 v8,1.2,0 v8,2.2,0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza	SSH	
		Virtuale	Implementato	SSH	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
756					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dischi) in MB/s.
		Scrittura throughput	Implementato	SSH	
		Tributo utilizzo	Implementato	SSH	
	Disco StoragePool	Provisioning della capacità	Implementato	SSH	
		Capacità raw	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		Capacità utilizzata	Implementato	SSH	
		Rapporto di capacità di overcommit	Implementato	SSH	Riportato come serie temporale
		Rapporto capacità utilizzata	Implementato	SSH	
		Capacità totale dei dati	Implementato	SSH	
		Data used Capacity (capacità utilizzata dati)	Implementato	SSH	
		Capacità riservata di Snapshot	Implementato	SSH	
		Capacità utilizzata di Snapshot	Implementato	SSH	
		Rapporto capacità utilizzata Snapshot	Implementato	SSH	Riportato come serie temporale

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
SSH Isilon	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

EMC PowerStore REST

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
PowerStore 1000T PowerStore 1200T PowerStore 3000T PowerStore 3200T PowerStore 5000T PowerStore 5000X PowerStore 9000T PowerStore 9200T	2.0.1.3 2.1.1.0 2.1.1.1 3.0.0.1 3.2.0.0 3.2.0.1 3.2.1.0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Tipo	Distanza		
		Virtuale	Implementato		Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità	Implementato		Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato		
		Nome	Implementato		
		Capacità raw totale	Implementato		Capacità raw totale (somma di tutti i dischi dell'array)
		ID pool di storage	Implementato		
		Con thin provisioning	Implementato		
		Tipo	Distanza		
		UUID	Implementato		
		Capacità utilizzata	Implementato		
		QoS - policy	Implementato		
	Mappa del volume	LUN	Implementato		Nome del lun back-end
		Mascheratura necessaria	Implementato		
		Protocol Controller (Controller protocollo)	Implementato		
		Porta storage	Implementato		
		Tipo	Distanza		
	Maschera di volume	Iniziatore	Implementato		
		Protocol Controller (Controller protocollo)	Implementato		
		Tipo	Distanza		
	Alias WWN	Alias host	Implementato		
		Tipo di oggetto	Implementato		
		Origine	Implementato		
		WWN	Implementato		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato			Volume	Capacità raw
	Implementato				Capacità totale
	Implementato				Capacità utilizzata
	Implementato				Rapporto capacità utilizzata
	Implementato				IOPS Read (lettura IOPS)
	Implementato		Numero di IOPS letti sul disco		Totale IOPS
	Implementato				Scrittura IOPS
	Implementato				Latenza di lettura
	Implementato				Latenza totale
	Implementato				Scrittura latenza
	Implementato				Throughput Read (lettura throughput)
	Implementato				Throughput totale
	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC POWERSTORE	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

EMC RecoverPoint (HTTP)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
RecoverPoint	5,1.P1(c.175) 5,1.SP4.P1(h.89) 5,1.SP4.P2(h.101) 5,1.SP4.P3(h.109) 5,1.SP4.P4(h.97)

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

					dischi spare)
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Nodo di storage	Dimensioni della memoria	Distanza	HTTPS	Memoria del dispositivo in MB
		Modello	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Numero di processori	Implementato	HTTPS	CPU del dispositivo
		Numero di serie	Implementato	HTTPS	
		Stato	Implementato	HTTPS	testo libero che descrive lo stato del dispositivo
		UUID	Implementato	HTTPS	
		Versione	Implementato	HTTPS	versione del software
	Sincronizzazione dello storage	Modalità	Implementato	HTTPS	
		Mode Enum	Implementato	HTTPS	
		Storage di origine	Implementato	HTTPS	
		Volume di origine	Implementato	HTTPS	
		Stato	Implementato	HTTPS	testo libero che descrive lo stato del dispositivo
		Num. Stato	Implementato	HTTPS	
		Storage di destinazione	Implementato	HTTPS	
		Volume di destinazione	Implementato	HTTPS	
		Tecnologia	Implementato	HTTPS	la tecnologia che causa l'efficienza dello storage è cambiata

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST RecoverPoint	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all’inizio

EMC ScaleIO e PowerFlex REST

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
ScaleIO	R2_6.11000.113 R2_6.11000.115 R3_0.1400.101 R3_5.1200.104 R3_6.500.113 R3_6.700.103

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
776					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dell'archiviazione?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità	Implementato	HTTPS	Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità raw totale	Implementato	HTTPS	Capacità raw totale (somma di tutti i dischi dell'array)
		ID pool di storage	Implementato	HTTPS	
		Con thin provisioning	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		IP host	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
780					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Totale IOPS	Implementato		
	Volume	Capacità raw	Implementato		
		Capacità totale	Implementato		
		IOPS Read (lettura IOPS)	Implementato		Numero di IOPS letti sul disco
		Totale IOPS	Implementato		
		Scrittura IOPS	Implementato		
		Throughput Read (lettura throughput)	Implementato		
		Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato		

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC ScaleIO e PowerFlex	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

EMC Symmetrix CLI

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
V10,0.0,0 V10,0.1,0 V7,6.2,67 V8,3.0,22 V8,3.0,6 V8,4.0,7 V8,4.0,9 V9,1.0,18 V9,1.0,5 V9,1.0,6 V9,2.0,0 V9,2.1,0 V9,2.1,1 V9,2.1,2 V9,2.2,0 V9,2.3,0 V9,2.3,1 V9,2.3,4 V9,2.3,5 V9,2.3,6 V9,2.4,1 V9,2.4,2	DMX3-24 DMX4-24 PMax2000 PowerMax_2000 PowerMax_8000 VMAX-1 VMAX100K VMAX10K VMAX200K VMAX250F VMAX400K VMAX40K VMAX450F VMAX850F VMAX950F	5773.198.142 (168D0000) build 5 5876.272.177 (16F40000) build 39 5876.286.194 (16F40000) build 115 5876.309.196 (16F40000) build 162 5977.1131.1131(17590000) build 551 5977.1151.1151(17590000) build 45 5977.1151.1151(17590000) build 59 5977.1151.1151(17590000) build 60 5977.1151.1151(17590000) build 9 5978.479.479 (175A0000) build 195 5978.711.711 (175A0000) build 113 5978.711.711 (175A0000) build 139 5978.711.711 (175A0000) build 149 5978.711.711 (175A0000) build 194 5978.711.711 (175A0000) build 196 5978.711.711 (175A0000) build 220 5978.711.711 (175A0000) build 239 5978.711.711 (175A0000) build 252 5978.711.711 (175A0000) build 267 5978.711.711 (175A0000) build 278 5978.711.711 (175A0000) build 287 5978.711.711 (175A0000) build 335 5978.711.711 (175A0000) build 365 5978.711.711 (175A0000) build 366 5978.711.711 (175A0000) build 388 5978.711.711 (175A0000) build 416 5978.711.711 (175A0000) build 436 5978.711.711 (175A0000) build 438 5978.711.711 (175A0000) build 448 5978.711.711 (175A0000) build 461 5978.711.711 (175A0000) build 480 5978.711.711 (175A0000) build 484 5978.711.711 (175A0000) build 502 5978.711.711 (175A0000) build 529 5978.711.711 (175A0000) build 8

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
784					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		(Controller protocollo)			
		Porta storage	Implementato		
		Tipo	Distanza		
	Membro del volume	Tiering automatico	Implementato		indica se questo storagepool sta partecipando al tiering automatico con altri pool
		Capacità	Implementato		Snapshot ha utilizzato la capacità in MB
		Cilindri	Implementato		
		Nome	Implementato		
		Classifica	Implementato		
		Capacità raw totale	Implementato		Capacità raw totale (somma di tutti i dischi dell'array)
		Ridondanza	Implementato		Livello di ridondanza
		ID pool di storage	Implementato		
		UUID	Implementato		
		Capacità utilizzata	Implementato		
	Rif. Volume	Nome	Implementato		
		IP dello storage	Implementato		
	Alias WWN	Alias host	Implementato		
		Tipo di oggetto	Implementato		
		Origine	Implementato		
		WWN	Implementato		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
794					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato		
		Totale rapporto di hit della cache	Implementato		
		Cache hit ratio Write	Implementato		
		Capacità raw	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Capacità scritta	Implementato		
		Rapporto capacità utilizzata	Implementato		
		CapacityRatio scritto	Implementato		
		IOPS Read (lettura IOPS)	Implementato		Numero di IOPS letti sul disco
		Totale IOPS	Implementato		
		Scrittura IOPS	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Scrittura latenza	Implementato		
		Throughput Read (lettura throughput)	Implementato		
		Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato		
		Scrittura in sospeso	Implementato		totale scrittura in sospeso

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
simpli	CLI		2707		vero	vero	vero	vero
Symmetrix SMI-S.	SMI-S.	HTTP/HTTPS	5988/5989		vero	falso	falso	vero

Torna all'inizio

DELL Unisphere REST

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
V10,0.0,5 V10,0.1,3 V9,2.1,6 V9,2.3,20 V9,2.3,22 V9,2.3,4 V9,2.4,1	PowerMax_2000 PowerMax_2500 PowerMax_8000 VMAX250F VMAX950F	5978.479.479 build 350 5978.711.711 build 252 5978.711.711 build 278 build 278 5978.711.711 build 287 5978.711.711 build 329 build 329 5978.711.711 build 365 5978.711.711 build 365 build 365 5978.711.711 build 376 5978.711.711 build 388 build 388 5978.711.711 build 416 5978.711.711 build 435 5978.711.711 build 448 5978.711.711 build 461 build 461 5978.711.711 build 481 build 481 5978.711.711 build 484 5978.711.711 build 484 build 484 5978.711.711 build 502 6079.125.0 build 53 build 53 6079.175.0 build 0 build 0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
800					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		(Controller protocollo)			
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Alias WWN	Alias host	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	
		Origine	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
806					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria** throughput	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato	HTTPS		Volume	Capacità raw
	Implementato	HTTPS			Capacità totale
	Implementato	HTTPS			Capacità utilizzata
	Implementato	HTTPS			Rapporto capacità utilizzata
	Implementato	HTTPS			CapacityRatio scritto
	Implementato	HTTPS			IOPS Read (lettura IOPS)
	Implementato	HTTPS	Numero di IOPS letti sul disco		Totale IOPS
	Implementato	HTTPS			Scrittura IOPS
	Implementato	HTTPS			Latenza di lettura
	Implementato	HTTPS			Latenza totale
	Implementato	HTTPS			Scrittura latenza
	Implementato	HTTPS			Throughput Read (lettura throughput)
	Implementato	HTTPS			Throughput totale
	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API Dell Unisphere	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

EMC VNX (SSH)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
VNX5300 VNX5400 VNX5700 VNX5800	05.33.009.5.231 7,1.76-4 7,1.80-3 8,1.9-232

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
810					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		utilizzata			
		Ridondanza	Implementato	SSH	Livello di ridondanza
		Tipo di disco	Non disponibile	SSH	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Mappa del volume	LUN	Implementato	SSH	Nome del lun back-end
		Porta storage	Implementato	SSH	
		Protocol Controller (Controller protocollo)	Implementato	SSH	
		Tipo	Distanza	SSH	
	Maschera di volume	Porta storage	Implementato	SSH	
		Iniziatore	Implementato	SSH	
		Protocol Controller (Controller protocollo)	Implementato	SSH	
		Tipo	Distanza	SSH	
	Alias WWN	Origine	Implementato	SSH	
		Alias host	Implementato	SSH	
		WWN	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		IP	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Utilizzo in lettura	Implementato	SSH	
		Totale utilizzo	Implementato	SSH	
		Scrittura utilizzo	Implementato	SSH	
	Storage	Capacità raw non riuscita	Implementato	SSH	
		Capacità raw	Implementato	SSH	
		Capacità raw di riserva	Implementato	SSH	Capacità raw dei dischi spare (somma di tutti i dischi spare)
		Capacità di StoragePools	Implementato	SSH	
		IOPS Altro	Implementato	SSH	
		IOPS Read (lettura IOPS)	Implementato	SSH	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	SSH	
		Scrittura IOPS	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Latenza totale	Implementato	SSH	
		Scrittura latenza	Implementato	SSH	
		Throughput Read (lettura throughput)	Implementato	SSH	
		Throughput totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	SSH	
	Nodo di storage	IOPS Read (lettura IOPS)	Implementato	SSH	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	SSH	
		Scrittura IOPS	Implementato	SSH	
		Totale utilizzo	Implementato	SSH	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
VNX SSH E CLI	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

EMC VNXe & Unity Unisphere (CLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
Unità 300 Unità 300F Unità 350F Unità 380 Unità 380F Unità 400 Unità 400F Unità 450F Unità 480F Unità 500 Unità 550F Unità 600 Unità 600F Unità 650F Unità 680F Unità 880 VNXe3200	3.1.17.10223906 3.1.17.10229825 4.1.2.9257522 4.2.1.9535982 4.2.3.9670635 4.5.1.0.5.001 5.0.2.0.5.009 5.0.6.0.5.008 5.0.8.0.5.007 5.1.2.0.5.007 5.1.3.0.5.003 5.2.1.0.5.013 5.2.2.0.5.004 5.2.2.0.6.201 5.3.0.0.5.120

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
824					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		destinazione			
		Tecnologia	Implementato	HTTPS	la tecnologia che causa l'efficienza dello storage è informazioni
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità	Implementato	HTTPS	Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità raw totale	Implementato	HTTPS	Capacità raw totale (somma di tutti i dischi dell'array)
		ID pool di storage	Implementato	HTTPS	
		Con thin provisioning	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
832					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato	HTTPS		Volume	Capacità raw
	Implementato	HTTPS			Capacità totale
	Implementato	HTTPS			Capacità utilizzata
	Implementato	HTTPS			Rapporto capacità utilizzata
	Implementato	HTTPS			IOPS Read (lettura IOPS)
	Implementato	HTTPS	Numero di IOPS letti sul disco		Totale IOPS
	Implementato	HTTPS			Scrittura IOPS
	Implementato	HTTPS			Latenza totale
	Implementato	HTTPS			Throughput Read (lettura throughput)
	Implementato	HTTPS			Throughput totale
	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
VNXe e Unisphere CLI	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

EMC VPLEX

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
VPLEX	5.4.1.00.00.07 5.4.1.01.00.05 6.2.0.03.00.02 6.2.0.04.00.07 6.2.0.05.00.11 6.2.0.07.00.02

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
836					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		UUID	Implementato	HTTP/S	
		Virtuale	Implementato	HTTP/S	Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Mappa del volume	LUN	Implementato	HTTP/S	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTP/S	
		Porta storage	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
	Maschera di volume	Iniziatore	Implementato	HTTP/S	
		Protocol Controller (Controller protocollo)	Implementato	HTTP/S	
		Porta storage	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

					dischi) in MB/s.
		Scrittura throughput	Implementato	SSH	
		Tributo utilizzo	Implementato	SSH	
	Disco StoragePool	Provisioning della capacità	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		Capacità utilizzata	Implementato	SSH	
		Rapporto di capacità di overcommit	Implementato	SSH	Riportato come serie temporale
		Rapporto capacità utilizzata	Implementato	SSH	
		Altra capacità totale	Implementato	SSH	
		Altra capacità utilizzata	Implementato	SSH	
	Volume	Capacità raw	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		Totale IOPS	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Latenza totale	Implementato	SSH	
		Scrittura latenza	Implementato	SSH	
		Throughput Read (lettura throughput)	Implementato	SSH	
		Throughput totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	SSH	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI EMC VPLEX	SSH	SSH	22		vero	vero	vero	vero

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API EMC VPLEX	HTTP/HTTPS	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

EMC XtremIO (HTTP)

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
6.2.1 6.2.2 6.3.1 6.3.2 6.3.3 6.4.0	1 mattoni e 125TB 1 mattoni e 24TB 1 mattoni e 26TB 1 mattoni e 31TB 1 mattoni e 62TB 1 mattoni e 8TB 1X10 TB 1X20 TB 1X40 TB 2 mattoni e 52TB 2 mattoni e 62TB 2 mattoni e 76TB 2 mattoni e 83TB 2 X 10 TB 2 X 20 TB 2X40 TB 3 mattoni e 251TB 3 mattoni e 283TB 4 mattoni e 125TB 4 mattoni e 503TB 4 mattoni e 628TB 4 mattoni e 754TB 4 X 20 TB 4X40 TB 6X20 TB	4,0.27-1 4,0.31-11 6,1.0-99_X2 6,3.3-8_X2 6,4.0-22_X2 6,4.0-36_HotFix_2_X2

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
844					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
852					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		dei dati			
		Data used Capacity (capacità utilizzata dati)	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST EMC XTREMIO	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

NetApp e-Series

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
2600 2660 2680 2702 2704 2800B 2804 2806 3000 5480 5486 5488 5504 5564 5600 5700 5700B 6000	08.40.60.01 8.10.14.0 8.20.11.0 8.20.27.0 8.20.30.0 8.20.5.0 8.20.8.0 8.25.14.0 8.25.6.0 8.30.1.0 8.40.0.1 8.40.0.3 8.40.20.0 8.40.30.3 8.40.40.0 8.40.50.0 8.40.60.1 8.40.60.2 8.40.60.3 8.42.20.0 8.50.0.3 8.50.0.4 8.51.0.0 8.52.0.0 8.52.0.1 8.53.0.1 8.53.0.4 8.62.0.0 8.62.0.2 8.63.0.2 8.70.0.3 8.71.2.0 8.71.3.0 8.72.0.0 8.72.1.0 8.72.2.0 8.73.0.0 8.74.0.0 8.74.1.0 8.74.2.0 8.74.3.0 8.75.0.0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dello storage?
		Capacità scritta	Implementato	RMI	Capacità totale scritta su questo volume da un host MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Mappa del volume	LUN	Implementato	RMI	Nome del lun back-end
		Porta storage	Implementato	RMI	
		Tipo	Distanza	RMI	
	Maschera di volume	Iniziatore	Implementato	RMI	
		Porta storage	Implementato	RMI	
		Tipo	Distanza	RMI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
864					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Utilizzo in lettura	Implementato	RMI	
		Totale utilizzo	Implementato	RMI	
		Scrittura utilizzo	Implementato	RMI	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	RMI	
		Totale rapporto di hit della cache	Implementato	RMI	
		Cache hit ratio Write	Implementato	RMI	
		Capacità raw	Implementato	RMI	
		Capacità totale	Implementato	RMI	
		Capacità utilizzata	Implementato	RMI	
		Capacità scritta	Implementato	RMI	
		Rapporto capacità utilizzata	Implementato	RMI	
		CapacityRatio scritto	Implementato	RMI	
		IOPS Read (lettura IOPS)	Implementato	RMI	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	RMI	
		Scrittura IOPS	Implementato	RMI	
		Latenza di lettura	Implementato	RMI	
		Latenza totale	Implementato	RMI	
		Scrittura latenza	Implementato	RMI	
		Throughput Read (lettura throughput)	Implementato	RMI	
		Throughput totale	Implementato	RMI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	RMI	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API SANtricity	RMI	TCP			vero	vero	falso	falso

Torna all'inizio

Calcolo cloud Google

Modelli e versioni supportati da questo data collector:

Versioni API
v1

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
870					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		ID	Implementato	HTTPS	
	Info	Descrizione API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome origine dati	Implementato	HTTPS	Info
		Data	Implementato	HTTPS	
		ID mittente	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	macchina virtuale	Capacità totale	Implementato	HTTPS	
		Utilizzo totale della CPU	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		DiskIops.total	Implementato	HTTPS	
		IOPS su disco in scrittura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Lettura throughput disco	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	throughput totale del disco letto
		Scrittura throughput disco	Implementato	HTTPS	
		Lettura throughput IP	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Throughput IP totale
		IpThroughput.write	Implementato	HTTPS	
		Utilizzo totale della memoria	Implementato	HTTPS	
		swapRate.inRate	Implementato	HTTPS	
		Tasso di swap	Implementato	HTTPS	
		Tasso di swap totale	Implementato	HTTPS	
		Tempo di attesa pianificato	Implementato	HTTPS	Tempo di attesa pianificato in percentuale

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Google Compute Platform	HTTPS		443		vero	vero	vero	vero

Torna all'inizio

HCP HDS (HTTPS)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
Hitachi Content Platform	9.3.7.2 9.5.0.121

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
876					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
					virtualizzazione dello storage?
	Nodo di storage	Nome	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
	Pool di storage	Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		Limite di tolleranza (MB)	Implementato	HTTPS	dimensione del volume logico definita durante le operazioni di creazione o ridimensionamento del volume
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

					dischi) in MB/s.
		Scrittura throughput	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tributo utilizzo	Implementato		
	Disco StoragePool	Capacità totale	Implementato		
		Rapporto capacità utilizzata	Implementato		
		Provisioning della capacità	Implementato		
		Capacità utilizzata	Implementato		
		Capacità raw	Implementato		
		Limite di tolleranza della capacità	Implementato		
		Rapporto di capacità di overcommit	Implementato		Riportato come serie temporale

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
HDS HCP REST API	HTTPS	HTTPS	9090		vero	vero	vero	vero

Torna all'inizio

Gestione dispositivi HiCommand

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
7.6.1 8.7.7 8.8.1 8.8.3 8.8.5	DF850MH DF850S HM800 HM850 P9500 RAID700 RAID800 VSP5000 XP24000 XP7	0983/A-H. 0988/H-S. DKC:60-08-22 DKC:60-08-65 DKC:70-06-46 DKC:70-06-67-00/00 DKC:80-06-80 DKC:80-06-82-00/00 DKC:80-06-86-00/00 DKC:80-06-87 DKC:80-06-88-00/00 DKC:80-06-91 DKC:80-06-91-00/00 DKC:80-06-93-00/00 DKC:83-05-45-40/00 DKC:83-05-45-60/00 DKC:83-05-46-60/00 DKC:83-05-47-60/00 DKC:83-05-48-40/00 DKC:83-05-48-60/00 DKC:88-08-08-60/00 DKC:88-08-09-60/00 DKC:90-08-81-00/00 DKC:90-08-83-00/01 SVP:60-08-21/00 SVP:60-08-54/00 SVP:70-06-32/00 SVP:70-06-51/00 SVP:80-06-76/02 SVP:80-06-78/00 SVP:80-06-81/00 SVP:80-06-82/00 SVP:80-06-83/00 SVP:80-06-86/00 SVP:80-06-88/00 SVP:83-05-49-40/00 SVP:83-05-49-60/00 SVP:83-05-50-60/00 SVP:83-05-51-60/00 SVP:83-05-52-40/00 SVP:83-05-52-60/00 SVP:88-08-10-60/00 SVP:88-08-11-60/00 SVP:90-08-81/00 SVP:90-08-83/00

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		storage			
		Con thin provisioning	Implementato	API XML HDS	
		Tipo	Distanza	API XML HDS	
		Capacità utilizzata	Implementato	API XML HDS	
		Virtuale	Implementato	API XML HDS	Si tratta di un dispositivo per la virtualizzazione dello storage?
	Mappa del volume	LUN	Implementato	API XML HDS	Nome del lun back-end
		Mascheratura necessaria	Implementato	API XML HDS	
		Protocol Controller (Controller protocollo)	Implementato	API XML HDS	
		Porta storage	Implementato	API XML HDS	
	Maschera di volume	Iniziatore	Implementato	API XML HDS	
		Protocol Controller (Controller protocollo)	Implementato	API XML HDS	
		Porta storage	Implementato	API XML HDS	
	Membro del volume	Nome	Implementato	API XML HDS	
		ID pool di storage	Implementato	API XML HDS	
		Classifica	Implementato	API XML HDS	
		Cilindri	Implementato	API XML HDS	
		Capacità	Implementato	API XML HDS	Snapshot ha utilizzato la capacità in MB
		Capacità raw totale	Implementato	API XML HDS	Capacità raw totale (somma di tutti i dischi dell'array)
		Capacità utilizzata	Implementato	API XML HDS	
	Alias WWN	Alias host	Implementato	API XML HDS	
		Tipo di oggetto	Implementato	API XML HDS	
		Origine	Implementato	API XML HDS	
		WWN	Implementato	API XML HDS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
890					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		tolleranza della capacità			
		Rapporto di commit	Implementato	Esportazione/CLI	Riportato come serie temporale
	Volume	Latenza totale	Implementato	Esportazione/CLI	
		IOPS Read (lettura IOPS)	Implementato	Esportazione/CLI	Numero di IOPS letti sul disco
		Latenza di lettura	Implementato	Esportazione/CLI	
		Cache hit ratio Read (rapporto di successo cache	Implementato	Esportazione/CLI	
		Scrittura IOPS	Implementato	Esportazione/CLI	
		Totale rapporto di hit della cache	Implementato	Esportazione/CLI	
		Cache hit ratio Write	Implementato	Esportazione/CLI	
		Throughput Read (lettura throughput)	Implementato	Esportazione/CLI	
		Scrittura throughput	Implementato	Esportazione/CLI	
		Throughput totale	Implementato	Esportazione/CLI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Totale IOPS	Implementato	Esportazione/CLI	
		Scrittura latenza	Implementato	Esportazione/CLI	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
Utility di esportazione (USPV) / SNM CLI (AMS)	Esportazione/CLI				falso	falso	falso	falso
API XML di HiCommand Device Manager	API XML HDS	HTTP/HTTPS	2001		vero	vero	vero	vero

Torna all’inizio

Hitachi Ops Center

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
VSP 5100 VSP 5500 VSP F1500 VSP F600 VSP G800	80-06-92-00/00:01-65-03/05 83-05-46-60/00:01-65-03/05 83-05-47-40/00:01-65-03/05 83-05-48-40/00:01-65-03/05 90-08-81-00/00:01-65-03/05 90-08-82-00/00:01-65-03/05

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		destinazione			
		Tecnologia	Implementato		la tecnologia che causa l'efficienza dello storage è informata
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità	Implementato		Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato		
		Nome	Implementato		
		Tipo di protezione	Implementato		
		Capacità raw totale	Implementato		Capacità raw totale (somma di tutti i dischi dell'array)
		ID pool di storage	Implementato		
		Con thin provisioning	Implementato		
		Tipo	Distanza		
		Capacità utilizzata	Implementato		
		Compressione attivata	Implementato		
	Mappa del volume	LUN	Implementato		Nome del lun back-end
		Mascheratura necessaria	Implementato		
		Protocol Controller (Controller protocollo)	Implementato		
		Porta storage	Implementato		
		Tipo	Distanza		
	Maschera di volume	Iniziatore	Implementato		
		Protocol Controller (Controller protocollo)	Implementato		
		Porta storage	Implementato		
		Tipo	Distanza		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
902					

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Nodo di storage	Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Totale IOPS	Implementato		
	Disco StoragePool	Capacità totale	Implementato		
		Rapporto capacità utilizzata	Implementato		
		Provisioning della capacità	Implementato		
		Capacità utilizzata	Implementato		
		Capacità raw	Implementato		
		Limite di tolleranza della capacità	Implementato		
		Rapporto di capacità di overcommit	Implementato		Riportato come serie temporale

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Hitachi Ops Center	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

HDS HNAS (CLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
G600 G800 HNAS 4080 HNAS 4100 N800	13.9.6918.05 14.5.7413.01 14.6.7520.04

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Dimensioni della memoria	Distanza	SSH	Memoria del dispositivo in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Processori	Implementato	SSH	Processori
	Pool di storage	ID pool di storage	Implementato	SSH	
		Nome	Implementato	SSH	
		Tipo	Distanza	SSH	
		Thin provisioning supportato	Implementato	SSH	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Includere nella capacità DWH	Implementato	SSH	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Deduplica attivata	Implementato	SSH	La deduplica è abilitata nel pool di storage
		Virtuale	Implementato	SSH	Si tratta di un dispositivo per la virtualizzazione dello storage?
		Gruppo RAID	Implementato	SSH	Indica se questo storagePool è un gruppo raid
		Capacità utilizzata di Snapshot	Implementato	SSH	
		Data used Capacity (capacità utilizzata dati)	Implementato	SSH	
		Capacità totale utilizzata	Implementato	SSH	Capacità totale in MB
		Capacità allocata totale	Implementato	SSH	
		Rapporto raw/usable	Implementato	SSH	rapporto per la conversione dalla capacità utilizzabile alla capacità raw

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
HDS HNAS CLI	SSH	SSH	22		vero	vero	vero	vero

Torna all'inizio

Storage HPE nimble / Alletra 6000

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
v1	6030 AF1000 AF20Q AF3000 AF40 AF5000 CS1000 CS300 CS3000 CS500 CS5000 HF20 HF20H HF40 HF60	5,0.10,0-742719-opz 5,0.7,0-604814-opz 5,0.8,0-677726-opz 5,2.1,1000-1017822-opz 5,2.1,400-796142-opz 5,2.1,600-841103-opz 5,2.1,700-882343-opz 5,2.1,800-930936-opz 5,2.1,900-1003439-opz 6,0.0,300-956221-opz 6,0.0,400-991061-opz 6,1.1,200-1020304-opz 6,1.1,300-1028597-opz

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
914					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dello storage?
		Compressione attivata	Implementato	HTTPS	
		Crittografato	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Mascheratura necessaria	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Alias WWN	Alias host	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	
		Origine	Implementato	HTTPS	
		WWN	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Risparmi totali di compressione	Implementato	HTTPS	
		Spazio per il risparmio di compressione	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST HP	HTTPS	HTTPS	5392		vero	falso	vero	vero

Torna all'inizio

Huawei OceanStor (REST/HTTPS)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
5300 V5 5500 V3 5500 V5 5800 V3 Dorado 5000 V6 SAS Dorado 6000 V3 Dorado 6000 V6 NVMe	V300R001C01 V300R002C10 V300R006C20 V300R006C50 V500R007C10 V500R007C30 V600R003C00 V600R005C03

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità	Implementato	HTTPS	Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		Capacità raw totale	Implementato	HTTPS	Capacità raw totale (somma di tutti i dischi dell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di storage	Implementato	HTTPS	
		Con thin provisioning	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Totale IOPS	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Totale utilizzo	Implementato	HTTPS	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	HTTPS	
		Totale rapporto di hit della cache	Implementato	HTTPS	
		Cache hit ratio Write	Implementato	HTTPS	
		Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Huawei OceanStor	HTTPS	HTTPS	8088		vero	vero	vero	vero
API REST Huawei OceanStor Performance	HTTPS	HTTPS	8088		vero	falso	vero	vero

Torna all'inizio

IBM Cleversafe

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
938					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Versione	Implementato	HTTPS	versione del software
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Versione	Implementato	HTTPS	
	Pool di storage	Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST IBM CLEVERSAFE	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

IBM DS 8K (DSCLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
2107-951 2107-961 2107-985 2107-996	7.6.31.4250 7.7.51.1400 7.8.57.18 7.9.21.91 7.9.32.126

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Protocol Controller (Controller protocollo)	Implementato	DSNI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Prodotto storage	Implementato	DSNI	
	Alias WWN	Alias host	Implementato	DSNI	
		Sistema operativo host	Implementato	DSNI	
		Tipo di oggetto	Implementato	DSNI	
		Origine	Implementato	DSNI	
		WWN	Implementato	DSNI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
948					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Utilizzo in lettura	Implementato	DSNI	
		Totale utilizzo	Implementato	DSNI	
		Scrittura utilizzo	Implementato	DSNI	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	DSNI	
		Totale rapporto di hit della cache	Implementato	DSNI	
		Cache hit ratio Write	Implementato	DSNI	
		Capacità raw	Implementato	DSNI	
		Capacità totale	Implementato	DSNI	
		IOPS Read (lettura IOPS)	Implementato	DSNI	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	DSNI	
		Scrittura IOPS	Implementato	DSNI	
		Latenza di lettura	Implementato	DSNI	
		Latenza totale	Implementato	DSNI	
		Scrittura latenza	Implementato	DSNI	
		Throughput Read (lettura throughput)	Implementato	DSNI	
		Throughput totale	Implementato	DSNI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	DSNI	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
Configurazione guidata origine dati	Immissione manuale				vero	vero	vero	vero
CLI IBM DS	DSNI	DSNI			vero	vero	vero	vero

Torna all’inizio

IBM PowerVM (SSH)

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Disco VirtualMachine	OID	Implementato	SSH	
		OID VirtualDisk	Implementato	SSH	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		OID VirtualMachine	Implementato	SSH	
	Host	Numero di CPU host	Implementato	SSH	
		Memoria installata sull'host	Implementato	SSH	
		Modello host	Implementato	SSH	
		Numero NIC	Implementato	SSH	
		IPS	Implementato	SSH	
		Produttore	Implementato	SSH	
		Nome	Implementato	SSH	
		OID	Implementato	SSH	
		Tipo di piattaforma	Implementato	SSH	
	Info	Nome origine dati	Implementato	SSH	Info
		Data	Implementato	SSH	
		ID mittente	Implementato	SSH	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
Accesso SSH IBM hardware Management Console	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

SVC IBM (CLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
2072-12F 2072-12G 2072-2N4 2072-324 2072-3H4 2072-3N4 2076-124 2076-12F 2076-224 2076-24F 2076-24G 2076-624 2076-724 2076-824 2076-AF6 2076-AFF 2077-24F 2077-424 2078-12F 2078-224 2078-24C 2078-24F 2078-324 2078-424 2078-4H4 2078-92G 2078-AF3 4657-924 4662-12G 4662-6H2 4666-AH8 9843-AE2 9843-AE3 9846-AG8 9848-AE2 9848-AF7 9848-AF8 9848-AG8 SVC	1.5.2.7 1.6.1.2 1.6.1.4 1.6.1.5 7.5.0.11 7.5.0.12 7.7.1.8 7.8.1.14 7.8.1.6 7.8.1.8 8.2.1.10 8.2.1.11 8.2.1.14 8.2.1.9 8.3.1.1 8.3.1.2 8.3.1.5 8.3.1.6 8.3.1.7 8.3.1.9 8.4.0.10 8.4.0.11 8.4.0.6 8.4.0.7 8.4.0.8 8.4.0.9 8.5.0.5 8.5.0.6 8.5.0.7 8.5.0.8 8.5.0.9 8.5.2.2 8.5.3.1 8.5.4.0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		utilizzata			
		Virtuale	Implementato	SSH	Si tratta di un dispositivo per la virtualizzazione dell'archiviazione?
		Capacità scritta	Implementato	SSH	Capacità totale scritta su questo volume da un host in MB
		Compressione attivata	Implementato	SSH	
		Crittografato	Implementato	SSH	
	Mappa del volume	LUN	Implementato	SSH	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	SSH	
		Porta storage	Implementato	SSH	
	Maschera di volume	Iniziatore	Implementato	SSH	
		Protocol Controller (Controller protocollo)	Implementato	SSH	
		Porta storage	Implementato	SSH	
		Tipo	Distanza	SSH	
	Alias WWN	Alias host	Implementato	SSH	
		Tipo di oggetto	Implementato	SSH	
		Origine	Implementato	SSH	
		WWN	Implementato	SSH	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
964					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Utilizzo in lettura	Implementato	SSH	
		Totale utilizzo	Implementato	SSH	
		Scrittura utilizzo	Implementato	SSH	
	Volume	Cache hit ratio Read (rapporto di successo cache	Implementato	SSH	
		Totale rapporto di hit della cache	Implementato	SSH	
		Cache hit ratio Write	Implementato	SSH	
		Capacità raw	Implementato	SSH	
		Capacità totale	Implementato	SSH	
		Capacità utilizzata	Implementato	SSH	
		Capacità scritta	Implementato	SSH	
		Rapporto capacità utilizzata	Implementato	SSH	
		CapacityRatio scritto	Implementato	SSH	
		IOPS Read (lettura IOPS)	Implementato	SSH	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	SSH	
		Scrittura IOPS	Implementato	SSH	
		Latenza di lettura	Implementato	SSH	
		Latenza totale	Implementato	SSH	
		Scrittura latenza	Implementato	SSH	
		Throughput Read (lettura throughput)	Implementato	SSH	
		Throughput totale	Implementato	SSH	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	SSH	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI IBM SVC	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

IBM XIV E A9000 (XIVCLI)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
415 A14	10,2.4.e 12,3.2.c

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
970					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Maschera di volume	Iniziatore	Implementato	XIV CLI	
		Protocol Controller	Implementato	XIV CLI	
Prodotto	**Categoria**	**Caratteristica/attributo** (protocollo)	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Alias WWN	Alias host	Implementato	XIV CLI	
		Sistema operativo host	Implementato	XIV CLI	
		Tipo di oggetto	Implementato	XIV CLI	
		Origine	Implementato	XIV CLI	
		WWN	Implementato	XIV CLI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

		Capacità raw	Implementato	DSNI	
		Rapporto di commit	Implementato	DSNI	Riportato come serie temporale
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Latenza totale	Implementato	DSNI	
		Latenza di lettura	Implementato	DSNI	
		Scrittura IOPS	Implementato	DSNI	
		Spazio per il risparmio di compressione	Implementato	DSNI	
		Throughput Read (lettura throughput)	Implementato	DSNI	
		Totale IOPS	Implementato	DSNI	
		Scrittura latenza	Implementato	DSNI	
		IOPS Read (lettura IOPS)	Implementato	DSNI	Numero di IOPS letti sul disco
		Cache hit ratio Read (rapporto di successo cache	Implementato	DSNI	
		Risparmi totali di compressione	Implementato	DSNI	
		Totale rapporto di hit della cache	Implementato	DSNI	
		Cache hit ratio Write	Implementato	DSNI	
		Scrittura throughput	Implementato	DSNI	
		Throughput totale	Implementato	DSNI	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
CLI IBM DS	DSNI	DSNI			vero	vero	vero	vero
CLI IBM XIV	XIV CLI	TCP	7778		vero	falso	vero	falso

Torna all’inizio

Infinidat Infinibox (HTTP)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
F6230 F6240 F6303 F6304	6.0.31.0 7.0.14.20

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
980					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			totale (somma di tutti i dischi dell'array)
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		capacità utilizzata	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
		Porta storage	Implementato	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
		Porta storage	Implementato	HTTPS	
	Alias WWN	Origine	Implementato	HTTPS	
		Alias host	Implementato	HTTPS	
		WWN	Implementato	HTTPS	
		Tipo di oggetto	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Infinidat	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Calcolo Microsoft Azure

Modelli e versioni supportati da questo data collector:

Versioni API
2018-06-01

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
988					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Produttore	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		ID	Implementato	HTTPS	
	Info	Descrizione API	Implementato	HTTPS	
		Nome API	Implementato	HTTPS	
		Versione API	Implementato	HTTPS	
		Nome origine dati	Implementato	HTTPS	Info
		Data	Implementato	HTTPS	
		ID mittente	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	macchina virtuale	Utilizzo totale della CPU	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		DiskIops.total	Implementato	HTTPS	
		IOPS su disco in scrittura	Implementato	HTTPS	
		Lettura throughput disco	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	throughput totale del disco letto
		Scrittura throughput disco	Implementato	HTTPS	
		Lettura throughput IP	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Throughput IP totale
		IpThroughput.write	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di calcolo Microsoft Azure	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Microsoft Hyper-V.

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
994					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Processori	Implementato	WMI	
		Capacità fornita	Implementato	WMI	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Capacità utilizzata	Implementato	WMI	
	Disco VirtualMachine	OID	Implementato	WMI	
		OID VirtualDisk	Implementato	WMI	
		OID VirtualMachine	Implementato	WMI	
	Host	Numero di CPU host	Implementato	WMI	
		Velocità CPU host	Implementato	WMI	
		Dominio host	Implementato	WMI	
		Memoria installata sull'host	Implementato	WMI	
		Modello host	Implementato	WMI	
		Numero NIC	Implementato	WMI	
		Velocità NIC	Implementato	WMI	
		IPS	Implementato	WMI	
		Produttore	Implementato	WMI	
		Nome	Implementato	WMI	
		OID	Implementato	WMI	
		Tipo di piattaforma	Implementato	WMI	
	Nodo ISCSI	Alias host	Implementato	WMI	
		Nome del nodo	Implementato	WMI	
		OID	Implementato	WMI	
		Tipo	Distanza	WMI	
	Info	Nome origine dati	Implementato	WMI	Info
		Data	Implementato	WMI	
		ID mittente	Implementato	WMI	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
998					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	macchina virtuale	Capacità totale	Implementato	WS-Management	
		Capacità utilizzata	Implementato	WS-Management	
		Rapporto capacità utilizzata	Implementato	WS-Management	
		Utilizzo totale della CPU	Implementato	WS-Management	
		IOPS Read (lettura IOPS)	Implementato	WS-Management	Numero di IOPS letti sul disco
		DiskIops.total	Implementato	WS-Management	
		IOPS su disco in scrittura	Implementato	WS-Management	
		Latenza totale	Implementato	WS-Management	
		Lettura throughput disco	Implementato	WS-Management	
		Throughput Read (lettura throughput)	Implementato	WS-Management	throughput totale del disco letto
		Scrittura throughput disco	Implementato	WS-Management	
		Lettura throughput IP	Implementato	WS-Management	
		Throughput totale	Implementato	WS-Management	Throughput IP totale
		IpThroughput.write	Implementato	WS-Management	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
PowerShell	WS-Management	HTTP	5985		vero	falso	falso	vero
WMI	WMI	WMI	135		vero	falso	vero	vero

Torna all’inizio

Modalità NetApp 7

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
1,12 1,14 1,17 1,19 1,20 1,21	FAS2040 FAS2050 FAS2220 FAS2240-2 FAS2240-4 FAS2520 FAS2554 FAS3140 FAS3160 FAS3210 FAS3220 FAS3240 FAS3250 FAS3270 FAS6240 FAS6290 FAS8020 FAS8040 FAS8060 FAS8080 N6070 N6240 V3240	7.3.6 8.1.1 7-Mode 8,1.3P2 7-Mode 8,1.4P1 7-Mode 8,1.4P10 7-Mode 8,1.4P9D18 7-Mode 8.2.1 7-Mode 8.2.2 7-Mode 8.2.3 7-Mode 8,2.3P2 7-Mode 8,2.3P3 7-Mode 8.2.4 7-Mode 8,2.4P2 7-Mode 8,2.4P4 7-Mode 8,2.4P5 7-Mode 8,2.4P6 7-Mode 8.2.5 7-Mode 8,2.5P1 7-Mode 8,2.5P2 7-Mode 8,2.5P4 7-Mode 8,2.5P5 7-Mode 8.2P3 7-Mode 8.2P4 7-Mode Data ONTAP versione 7.3.3 Data ONTAP versione 7.3.4 Data ONTAP versione 8.2.5 7-Mode

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1002					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Protocol Controller (Controller protocollo)	Implementato		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza		
	Maschera di volume	Iniziatore	Implementato		
		Protocol Controller (Controller protocollo)	Implementato		
		Porta storage	Implementato		
		Tipo	Distanza		

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1016					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Throughput	Implementato		
		Utilizzo in lettura	Implementato		
		Totale utilizzo	Implementato		
		Scrittura utilizzo	Implementato		
	Volume	Capacità raw	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto capacità utilizzata	Implementato		
		Lettura densità io	Implementato		
		Densità io totale	Implementato		
		Densità io di scrittura	Implementato		
		IOPS Read (lettura IOPS)	Implementato		Numero di IOPS letti sul disco
		Totale IOPS	Implementato		
		Scrittura IOPS	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Scrittura latenza	Implementato		
		Rapporto di blocco parziale	Implementato		
		Throughput Read (lettura throughput)	Implementato		
		Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato		
		Scrittura in sospeso	Implementato		totale scrittura in sospeso

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
NetApp 7 modalità ZAPI	ZAPI	ZAPI			vero	vero	vero	vero

Torna all'inizio

NetApp Cloud Volumes Service

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
AWS Cloud Volumes	v1

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					dischi spare)
		Capacità raw non riuscita	Implementato		Capacità raw dei dischi guasti
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Pool di storage	ID pool di storage	Implementato		
		Nome	Implementato		
		Tipo	Distanza		
		Thin provisioning supportato	Implementato		Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Includere nella capacità DWH	Implementato		Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Virtuale	Implementato		Si tratta di un dispositivo per la virtualizzazione dello storage?
		Gruppo RAID	Implementato		Indica se questo storagePool è un gruppo raid
		Capacità utilizzata di Snapshot	Implementato		
		Data used Capacity (capacità utilizzata dati)	Implementato		
		Capacità allocata dei dati	Distanza		capacità allocata per i dati
		Capacità totale utilizzata	Implementato		Capacità totale in MB
		Capacità allocata totale	Implementato		
		Capacità disco fisico (MB)	Implementato		utilizzato come capacità raw per il pool di storage
		Rapporto raw/usable	Implementato		rapporto per la conversione dalla capacità utilizzabile alla capacità raw

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Cloud Volumes Service	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Amazon FSX per NetApp ONTAP

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
FSX per ONTAP	Data ONTAP

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1028					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		(Controller protocollo)			
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
performance	Qtree.1+	Storage	Dischi guasti	Implementato	HTTPS
		Nodo di storage	Totale rapporto di hit della cache	Implementato	HTTPS
			Totale lettura disco sostituita	Implementato	HTTPS
			Totale utilizzo	Implementato	HTTPS

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

NetApp Clustered Data ONTAP 8.1.1+

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
AFF-A150	8,2.3P5
AFF-A200	8.3.0
AFF-A220	8.3.1
AFF-A250	8,3.1P2
AFF-A300	8.3.2
AFF-A320	8,3.2P12
AFF-A400	8,3.2P2
AFF-A700	8,3.2P5
AFF-A700s	9.0.1
AFF-A800	9.1.0
AFF-A900	9,1.0P1
AFF-C190	9,1.0P10
AFF-C250	9,1.0P11
AFF-C400	9,1.0P12
AFF-C800	9,1.0P14
AFF8020	9,1.0P15
AFF8040	9,1.0P17
AFF8060	9,1.0P19
AFF8080	9,1.0P20
CDvM100	9,1.0P5
CDvM200	9,1.0P7
DM5000H	9,1.0P8
FAS2240-2	9.10.0
FAS2240-4	9.10.1
FAS2520	9.10.1P1
FAS2552	9.10.1P10
FAS2554	9.10.1P11
FAS2620	9.10.1P12
FAS2650	9.10.1P13
FAS2720	9.10.1P2
FAS2750	9.10.1P3
FAS3220	9.10.1P4
FAS3250	9.10.1P5
FAS3270	9.10.1P6
FAS500f	9.10.1P7
FAS6210	9.10.1P8
FAS6220	9.10.1P9
FAS8020	9.11.0P1
FAS8040	9.11.1
FAS8060	9.11.1P1
FAS8080	9.11.1P10
FAS8200	9.11.1P2
FAS8300	9.11.1P3
FAS8700	9.11.1P4
FAS9000	9.11.1P5
FAS9500	9.11.1P6
FASDvM300	9.11.1P7
SIMBOX	9.11.1P8
V6240	9.11.1P9
	9.11.1X12
	9.11.1X26
	9.12.1
	9.12.1P1
	9.12.1P2

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1048					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Crittografato	Implementato	HTTPS	
		IOPS limite QoS	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		QoS Limit Raw	Implementato	HTTPS	
		QoS - policy	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

					(lettura e scrittura su tutti i dischi) in MB/s.
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Lettura densità io	Implementato	HTTPS	
		Densità io totale	Implementato	HTTPS	
		Densità io di scrittura	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API NetApp ONTAP	HTTP/HTTPS	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all’inizio

NetApp SolidFire 8.1+

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
H410S-2 H610S-2 H610S-4 SF19210 SF2405 SF38410 SF4805 SF9605 SF9608 FCN001 H300S H410S-0 H410S-1 H410S-2 H500S H610S-1 H610S-2 H610S-4 H610S2 SF19210 SF38410 SF4805 SF9605	11.1.0.72 11.5.0.63 11.7.0.76 11.8.0.23 12.0.0.333 12.2.0.777 12.3.0.958 12.3.1.103 12.3.1.165 12.3.2.3 12.5.0.897 12.7.0.380

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		IOPS burst QoS	Implementato	HTTPS	
		IOPS limite QoS	Implementato	HTTPS	
		qos min IOPS	Implementato	HTTPS	
		QoS policy	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Mascheratura necessaria	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Altra capacità totale	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Risparmi totali di compressione	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Latenza di lettura	Implementato	HTTPS	
		Latenza totale	Implementato	HTTPS	
		Scrittura latenza	Implementato	HTTPS	
		Rapporto di blocco parziale	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	
		Totale utilizzo	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST SolidFire	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

NetApp StorageGRID (HTTPS)

Modelli e versioni supportati da questo data collector:

Versioni API	Modelli	Versioni del firmware
3,0 3,2 3,3 3,4 3.5	Webscale	11.2.0 11.4.0 11.4.0.3 11.4.0.4 11.5.0.1 11.5.0.11 11.5.0.2 11.5.0.3 11.5.0.6 11.5.0.7 11.5.0.8 11.5.0.9 11.6.0 11.6.0.1 11.6.0.10 11.6.0.2 11.6.0.4 11.6.0.5 11.6.0.7 11.6.0.8 11.6.0.9 11.7.0

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Utilizzo della capacità del nodo dati Meta utilizzati in MB	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Nome del sito	Implementato	HTTPS	
	Pool di storage	Includere nella capacità DWH	Implementato	HTTPS	Un modo per passare da ACQ a cottrol, i pool di stroage sono interessanti nella capacità di DWH
		Nome	Implementato	HTTPS	
		Capacità disco fisico (MB)	Implementato	HTTPS	utilizzato come capacità raw per il pool di storage
		Gruppo RAID	Implementato	HTTPS	Indica se questo storagePool è un gruppo raid
		Rapporto raw/usable	Implementato	HTTPS	rapporto per la conversione dalla capacità utilizzabile alla capacità raw
		ID pool di storage	Implementato	HTTPS	
		Thin provisioning supportato	Implementato	HTTPS	Se questo volume interno supporta il thin provisioning per il layer di volume sopra di esso
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato			Disco StoragePool	Provisioning della capacità
	Implementato				Capacità raw
	Implementato				Capacità totale
	Implementato				Capacità utilizzata
	Implementato				Rapporto di capacità di overcommit
	Implementato		Riportato come serie temporale		Rapporto capacità utilizzata

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di StorageGRID	HTTPS	HTTPS	443		vero	falso	vero	vero

Torna all'inizio

Storage Nutanix (REST)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
HPE DL360-8 G10 NX-3060-G6 NX-3170-G6 NX-8035-G6 NX-8150-G7 HPE DL360-8 G10 HPE DL380-12 G10 NX-3060-G5 NX-3170-G7 NX-5155-G6 NX-8035-G6 NX-8035-G7 NX-8150-G7 NX-8150-G8	6.5.1.6 6.5.2 6.5.2.5 6.5.2.6 6.5.2.7 6.5.3 6.5.3.1

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1100					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristiche/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		Capacità allocata totale	Implementato	HTTPS	
		Capacità totale/utilizzata	Implementato	HTTPS	Capacità totale in MB
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
	Volume	Capacità	Implementato	HTTPS	Snapshot ha utilizzato la capacità in MB
		Percorso di giunzione	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
		ID qtree	Implementato	HTTPS	id univoco del qtree
		Capacità raw totale	Implementato	HTTPS	Capacità raw totale (somma di tutti i dischi dell'array)
		Ridondanza	Implementato	HTTPS	Livello di ridondanza
		ID pool di storage	Implementato	HTTPS	
		Con thin provisioning	Implementato	HTTPS	
		UUID	Implementato	HTTPS	
	Mappa del volume	LUN	Implementato	HTTPS	Nome del lun back-end
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Maschera di volume	Iniziatore	Implementato	HTTPS	
		Protocol Controller (Controller protocollo)	Implementato	HTTPS	
		Porta storage	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

			totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Implementato	HTTPS		Disco StoragePool	Scrittura latenza
	Implementato	HTTPS			IOPS Read (lettura IOPS)
	Implementato	HTTPS	Numero di IOPS letti sul disco		Totale IOPS
	Implementato	HTTPS			Scrittura IOPS
	Implementato	HTTPS			Throughput Read (lettura throughput)
	Implementato	HTTPS			Throughput totale
	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput
	Implementato	HTTPS		Volume	IOPS Read (lettura IOPS)
	Implementato	HTTPS	Numero di IOPS letti sul disco		Totale IOPS
	Implementato	HTTPS			Scrittura IOPS
	Implementato	HTTPS			Latenza di lettura
	Implementato	HTTPS			Latenza totale
	Implementato	HTTPS			Scrittura latenza
	Implementato	HTTPS			Throughput Read (lettura throughput)
	Implementato	HTTPS			Throughput totale
	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.		Scrittura throughput

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Nutanix	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

OPENSTACK (API REST/SSH)

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Operative host			
		IPS	Implementato	HTTPS	
		Nome	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		OID	Implementato	HTTPS	
	Nodo ISCSI	Alias host	Implementato	HTTPS	
		Nome del nodo	Implementato	HTTPS	
		OID	Implementato	HTTPS	
		Tipo	Distanza	HTTPS	
	Info	Nome origine dati	Implementato	HTTPS	Info
		Data	Implementato	HTTPS	
		ID mittente	Implementato	HTTPS	
		Chiave di origine	Implementato	HTTPS	
performance	Data Store	Capacità totale	Implementato		
		Rapporto capacità utilizzata	Implementato		
		Provisioning della capacità	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto di capacità di overcommit	Implementato		Riportato come serie temporale
	Host	Utilizzo totale della CPU	Implementato		
		Utilizzo totale della memoria	Implementato		
	Disco virtuale	Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Scrittura latenza	Implementato		

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di OpenStack	HTTPS	HTTPS	443		vero	falso	vero	vero
SSH OpenStack	SSH	SSH	22		vero	falso	vero	vero

Torna all'inizio

Oracle ZFS (HTTPS)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
Storage Sun ZFS 7330 Storage Sun ZFS 7335 Storage Sun ZFS 7350 Storage Sun ZFS 7370 Storage Sun ZFS 7420 Storage Sun ZFS 7430 Storage Sun ZFS 7450	1-1,1 1-1,2 1-1,3 1-1,34 1-1,4 2013.06.05.6.12 2013.06.05.6.15 2013.06.05.7.21 2013.06.05.7.24 2013.06.05.7.25 2013.06.05.7.26 2013.06.05.8.0 2013.06.05.8.26 2013.06.05.8.29 2013.06.05.8.35 2013.06.05.8.37 2013.06.05.8.47 2013.06.05.8.50 2013.06.05.8.53 2013.06.05.8.6 2013.06.05.8.7

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1118					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Capacità utilizzata	Implementato	HTTP/S	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Mappa del volume	LUN	Implementato	HTTP/S	Nome del lun back-end
		Porta storage	Implementato	HTTP/S	
		Mascheratura necessaria	Implementato	HTTP/S	
		Protocol Controller (Controller protocollo)	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
	Maschera di volume	Porta storage	Implementato	HTTP/S	
		Iniziatore	Implementato	HTTP/S	
		Protocol Controller (Controller protocollo)	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1128					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Totale IOPS	Implementato		
		Totale rapporto di hit della cache	Implementato		
		Totale utilizzo	Implementato		
	Disco StoragePool	Totale IOPS	Implementato		
		Capacità totale	Implementato		
		Rapporto capacità utilizzata	Implementato		
		Capacità totale dei dati	Implementato		
		Provisioning della capacità	Implementato		
		Data used Capacity (capacità utilizzata dati)	Implementato		
		Capacità utilizzata	Implementato		
		Altra capacità utilizzata	Implementato		
		Capacità raw	Implementato		
		Rapporto di capacità di overcommit	Implementato		Riportato come serie temporale
		Capacità utilizzata di Snapshot	Implementato		
		Rapporto capacità utilizzata Snapshot	Implementato		Riportato come serie temporale

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST ORACLE ZFS	HTTP/HTTPS	HTTP/HTTPS	215		vero	vero	vero	vero

Torna all'inizio

Pure Storage FlashArray (HTTP)

Modelli e versioni supportati da questo data collector:

Modelli	Versioni del firmware
DFSC1 FA-420 FA-450 FA-C40R3 FA-C60 FA-C60R3 FA-X10R2 FA-X10R3 FA-X20R2 FA-X20R3 FA-X50R2 FA-X50R3 FA-X70R2 FA-X70R3 FA-X90R2 FA-X90R3 FA-XL130 FA-XL170 Fa-m10r2 Fa-M20 Fa-m20r2 Fa-M50 Fa-m50r2 Fa-M70 Fa-m70r2 Fa-x70	4.8.8 5.3.14 5.3.15 5.3.17 5.3.18 5.3.20 5.3.21 5.3.6 5.3.8 6.1.10 6.1.11 6.1.13 6.1.14 6.1.15 6.1.17 6.1.18 6.1.19 6.1.21 6.1.22 6.1.23 6.1.5 6.2.13 6.2.7 6.2.9 6.3.10 6.3.11 6.3.12 6.3.2 6.3.5 6.3.6 6.3.7 6.3.9 6.4.3 6.4.4 6.4.5

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1132					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
		(Controller protocollo)			
		Porta storage	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
	Maschera di volume	Iniziatore	Implementato	HTTP/S	
		Protocol Controller (Controller protocollo)	Implementato	HTTP/S	
		Porta storage	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
	Alias WWN	Alias host	Implementato	HTTP/S	
		Tipo di oggetto	Implementato	HTTP/S	
		Origine	Implementato	HTTP/S	
		WWN	Implementato	HTTP/S	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1140					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Snapshot			
		Rapporto capacità Snapshot	Implementato		Riportato come serie temporale
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
	Volume	Capacità raw	Implementato		
		Capacità totale	Implementato		
		Capacità utilizzata	Implementato		
		Rapporto capacità utilizzata	Implementato		
		IOPS Read (lettura IOPS)	Implementato		Numero di IOPS letti sul disco
		Totale IOPS	Implementato		
		Scrittura IOPS	Implementato		
		Latenza di lettura	Implementato		
		Latenza totale	Implementato		
		Scrittura latenza	Implementato		
		Throughput Read (lettura throughput)	Implementato		
		Throughput totale	Implementato		Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato		

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di pure Storage	HTTP/HTTPS	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

Red Hat RHV (REST)

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1144					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

	Disco VirtualMachine	OID	Implementato	HTTP/S	
		OID VirtualMachine	Implementato	HTTP/S	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		OID VirtualDisk	Implementato	HTTP/S	
	Host	OID	Implementato	HTTP/S	
		Nome	Implementato	HTTP/S	
		IPS	Implementato	HTTP/S	
		Tipo di piattaforma	Implementato	HTTP/S	
		Memoria installata sull'host	Implementato	HTTP/S	
		Produttore	Implementato	HTTP/S	
		Modello host	Implementato	HTTP/S	
		Numero di CPU host	Implementato	HTTP/S	
		Velocità CPU host	Implementato	HTTP/S	
		Numero NIC	Implementato	HTTP/S	
		Velocità NIC	Implementato	HTTP/S	
	Nodo ISCSI	OID	Implementato	HTTP/S	
		Nome del nodo	Implementato	HTTP/S	
		Tipo	Distanza	HTTP/S	
	Info	Nome origine dati	Implementato	HTTP/S	Info
		ID mittente	Implementato	HTTP/S	
		Data	Implementato	HTTP/S	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST Red Hat RHEV	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Storage Rubrik

Modelli e versioni supportati da questo data collector:

Versioni API	Versioni del firmware
v5,3	5,3.3-p1-19391 6,0.3-p3-13584 7,0.2-p4-15876 7,0.3-p1-15949 8,0.3-p2-22743

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		totale			
		Capacità totale utilizzata	Implementato	HTTPS	Capacità totale in MB
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tipo	Distanza	HTTPS	
		Virtuale	Implementato	HTTPS	Si tratta di un dispositivo per la virtualizzazione dello storage?
		Percentuale capacità effettiva utilizzata	Implementato	HTTPS	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1154					

					dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Tribù utilizzo	Implementato	HTTPS	
	Disco StoragePool	Capacità raw	Implementato	HTTPS	
		Capacità totale	Implementato	HTTPS	
		Capacità utilizzata	Implementato	HTTPS	
		Rapporto capacità utilizzata	Implementato	HTTPS	
		Data used Capacity (capacità utilizzata dati)	Implementato	HTTPS	
		IOPS Read (lettura IOPS)	Implementato	HTTPS	Numero di IOPS letti sul disco
		Totale IOPS	Implementato	HTTPS	
		Scrittura IOPS	Implementato	HTTPS	
		Altra capacità utilizzata	Implementato	HTTPS	
		Capacità utilizzata di Snapshot	Implementato	HTTPS	
		Throughput Read (lettura throughput)	Implementato	HTTPS	
		Throughput totale	Implementato	HTTPS	Velocità media totale del disco (lettura e scrittura su tutti i dischi) in MB/s.
		Scrittura throughput	Implementato	HTTPS	

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST di Rubrik Storage	HTTPS	HTTPS	443		vero	vero	vero	vero

Torna all'inizio

Centro virtuale NetApp HCI

Modelli e versioni supportati da questo data collector:

Versioni API
VMware vCenter Server 6.7.0 Build-10244857 VMware vCenter Server 6.7.0 Build-14368073 VMware vCenter Server 7.0.3 Build-19234570 VMware vCenter Server 7.0.3 Build-20150588 VMware vCenter Server 7.0.3 Build-20395099 VMware vCenter Server 7.0.3 Build-20990077 VMware vCenter Server 7.0.3 Build-21477706 VMware vCenter Server 7.0.3 Build-21784236 VMware vCenter Server 8.0.1 Build-21815093

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
	Nodo ISCSI	Alias nodo	Implementato	Servizi Web	
		Nome del nodo	Implementato	Servizi Web	
		OID	Implementato	Servizi Web	
		Tipo	Distanza	Servizi Web	
	Info	Descrizione API	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Client API Name (Nome API client)	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	
		Nome origine dati	Implementato	Servizi Web	Info
		Data	Implementato	Servizi Web	
		ID mittente	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1162					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Utilizzo totale della memoria	Implementato	Servizi Web	
		swapRate.inRate	Implementato	Servizi Web	
		Tasso di swap	Implementato	Servizi Web	
		Tasso di swap totale	Implementato	Servizi Web	
		Tempo di attesa pianificato	Implementato	Servizi Web	Tempo di attesa pianificato in percentuale

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

VMware Cloud su AWS

Modelli e versioni supportati da questo data collector:

Versioni API
VMware vCenter Server 7.0.3 Build-20532039 VMware vCenter Server 7.0.3 Build-20870699 VMware vCenter Server 8.0.0 Build-21709157

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					
1166					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
	Disco VirtualMachine	OID	Implementato	Servizi Web	
		OID VirtualMachine	Implementato	Servizi Web	
		OID VirtualDisk	Implementato	Servizi Web	
	Host	OID	Implementato	Servizi Web	
		Nome	Implementato	Servizi Web	
		IPS	Implementato	Servizi Web	
		Dominio host	Implementato	Servizi Web	
		Tipo di piattaforma	Implementato	Servizi Web	
		Memoria installata sull'host	Implementato	Servizi Web	
		Produttore	Implementato	Servizi Web	
		Modello host	Implementato	Servizi Web	
		Numero di CPU host	Implementato	Servizi Web	
		Velocità CPU host	Implementato	Servizi Web	
		Numero NIC	Implementato	Servizi Web	
		Velocità NIC	Implementato	Servizi Web	
	Info	Nome origine dati	Implementato	Servizi Web	Info
		ID mittente	Implementato	Servizi Web	
		Data	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Descrizione API	Implementato	Servizi Web	
		Client API Name (Nome API client)	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Tempo di attesa pianificato	Implementato	Servizi Web	Tempo di attesa pianificato in percentuale
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		Disk.ops.total	Implementato	Servizi Web	
		Tasso di swap totale	Implementato	Servizi Web	
		Throughput Read (lettura throughput)	Implementato	Servizi Web	throughput totale del disco letto

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		vero	vero	vero	vero

Torna all'inizio

VMware vSphere (servizi Web)

Modelli e versioni supportati da questo data collector:

Versioni API
VMware ESXi 6.0.0 build-10719132 VMware ESXi 6.0.0 build-2494585 VMware ESXi 6.0.0 build-5572656 VMware ESXi 6.0.0 build-9313334 VMware ESXi 6.5.0 build-14990892 VMware ESXi 6.5.0 build-5969303 VMware ESXi 7.0.0 build-15843807 VMware ESXi 7.0.3 build-20036589 VMware ESXi 7.0.3 build-20328353 VMware ESXi 7.0.3 build-20842708 VMware vCenter Server 5.0.0 Build-3073236 VMware vCenter Server 5.0.0 Build-455964 VMware vCenter Server 5.0.0 Build-623373 VMware vCenter Server 5.1.0 Build-3814779 VMware vCenter Server 5.5.0 Build-1750787 VMware vCenter Server 5.5.0 Build-2442329 VMware vCenter Server 5.5.0 Build-3000241 VMware vCenter Server 5.5.0 Build-3252642 VMware vCenter Server 5.5.0 Build-3721164 VMware vCenter Server 5.5.0 Build-4180647 VMware vCenter Server 5.5.0 Build-6516310 VMware vCenter Server 5.5.0 Build-9911218 VMware vCenter Server 6.0.0 Build-13638472 VMware vCenter Server 6.0.0 Build-14510545 VMware vCenter Server 6.0.0 Build-2776511 VMware vCenter Server 6.0.0 Build-3634793 VMware vCenter Server 6.0.0 Build-3634794 VMware vCenter Server 6.0.0 Build-5960847 VMware vCenter Server 6.0.0 Build-7924803 VMware vCenter Server 6.0.0 Build-8803875 VMware vCenter Server 6.0.0 Build-9313458 VMware vCenter Server 6.5.0 Build-10964411 VMware vCenter Server 6.5.0 Build-15679215 VMware vCenter Server 6.5.0 Build-17590285 VMware vCenter Server 6.5.0 Build-17994927 VMware vCenter Server 6.5.0 Build-18499837 VMware vCenter Server 6.5.0 Build-18711281 VMware vCenter Server 6.5.0 Build-19261680 VMware vCenter Server 6.5.0 Build-20510539 VMware vCenter Server 6.5.0 Build-7119157 VMware vCenter Server 6.7.0 Build-10244857 VMware vCenter Server 6.7.0 Build-11727113 VMware vCenter Server 6.7.0 Build-13007421 VMware vCenter Server 6.7.0 Build-13639324 VMware vCenter Server 6.7.0 Build-14368073 VMware vCenter Server 6.7.0 Build-15129973 VMware vCenter Server 6.7.0 Build-15679289 VMware vCenter Server 6.7.0 Build-17137327 VMware vCenter Server 6.7.0 Build-18010599 VMware vCenter Server 6.7.0 Build-18485185 VMware vCenter Server 6.7.0 Build-18831049 VMware vCenter Server 6.7.0 Build-19299595 VMware vCenter Server 6.7.0 Build-19832247 VMware vCenter Server 6.7.0 Build-19832280

Prodotti supportati da questo data collector:

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
base					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
	Nodo IGSI	Alias nodo	Implementato	Servizi Web	
		Nome del nodo	Implementato	Servizi Web	
		OID	Implementato	Servizi Web	
		Tipo	Distanza	Servizi Web	
	Info	Descrizione API	Implementato	Servizi Web	
		Nome API	Implementato	Servizi Web	
		Versione API	Implementato	Servizi Web	
		Client API Name (Nome API client)	Implementato	Servizi Web	
		Versione API client	Implementato	Servizi Web	
		Nome origine dati	Implementato	Servizi Web	Info
		Data	Implementato	Servizi Web	
		ID mittente	Implementato	Servizi Web	

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni
performance					
1182					

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

Prodotto	Categoria	Caratteristica/attributo	Stato	Protocollo utilizzato	Ulteriori informazioni

		Lettura throughput IP	Implementato	Servizi Web	
Prodotto	**Categoria**	**Caratteristica/attributo**	**Stato**	**Protocollo utilizzato**	**Ulteriori informazioni**
		IpThroughput.write	Implementato	Servizi Web	
		Utilizzo totale della memoria	Implementato	Servizi Web	
		swapRate.inRate	Implementato	Servizi Web	
		Tasso di swap	Implementato	Servizi Web	
		Tasso di swap totale	Implementato	Servizi Web	
		Tempo di attesa pianificato	Implementato	Servizi Web	Tempo di attesa pianificato in percentuale

API di gestione utilizzate da questo data collector:

API	Protocollo utilizzato	Protocollo Transport Layer utilizzato	Porte in entrata utilizzate	Porte in uscita utilizzate	Supporta l'autenticazione	Richiede solo credenziali di sola lettura	Supporta la crittografia	Compatibile con firewall (porte statiche)
API REST VMware	Servizi Web	HTTP/HTTPS	80/443		vero	vero	vero	vero

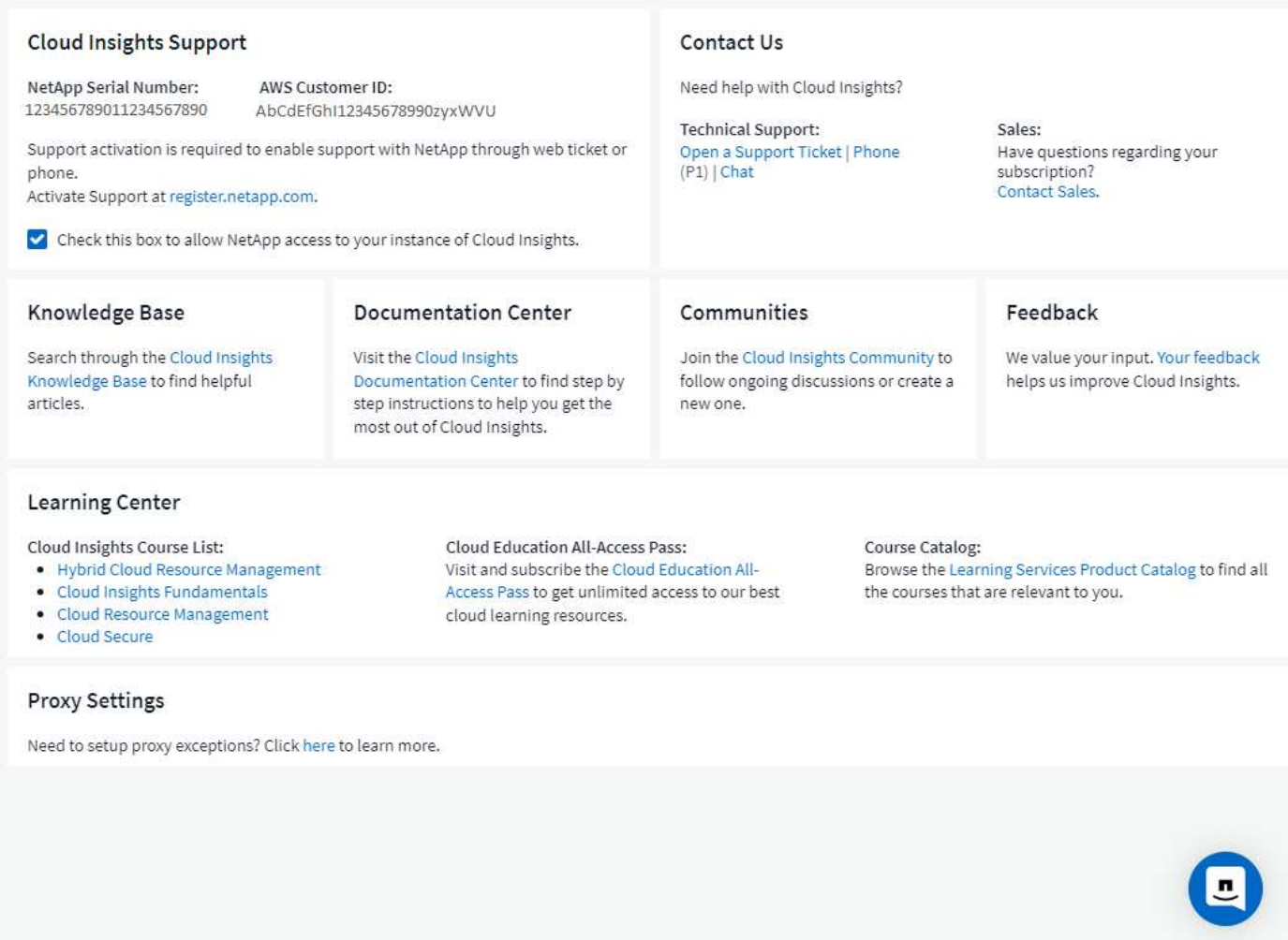
Torna all'inizio

Riferimento e supporto

Richiesta di supporto

È possibile accedere alle opzioni di supporto in Cloud Insights facendo clic su **Guida > supporto**. Le opzioni di supporto disponibili dipendono dall'edizione Cloud Insights.

> L'opzione di supporto della chat live non è disponibile nell'edizione federale di Cloud Insights.



Attivazione dei diritti di supporto

Cloud Insights offre supporto self-service ed e-mail quando viene eseguito in modalità di prova. Una volta effettuato l'abbonamento al servizio, si consiglia di attivare il diritto al supporto. L'attivazione dei diritti di supporto consente di accedere al supporto tecnico tramite chat online, sistema di web ticketing e telefono. La modalità di supporto predefinita è self-service fino al completamento della registrazione. Vedere "dettagli" di seguito.

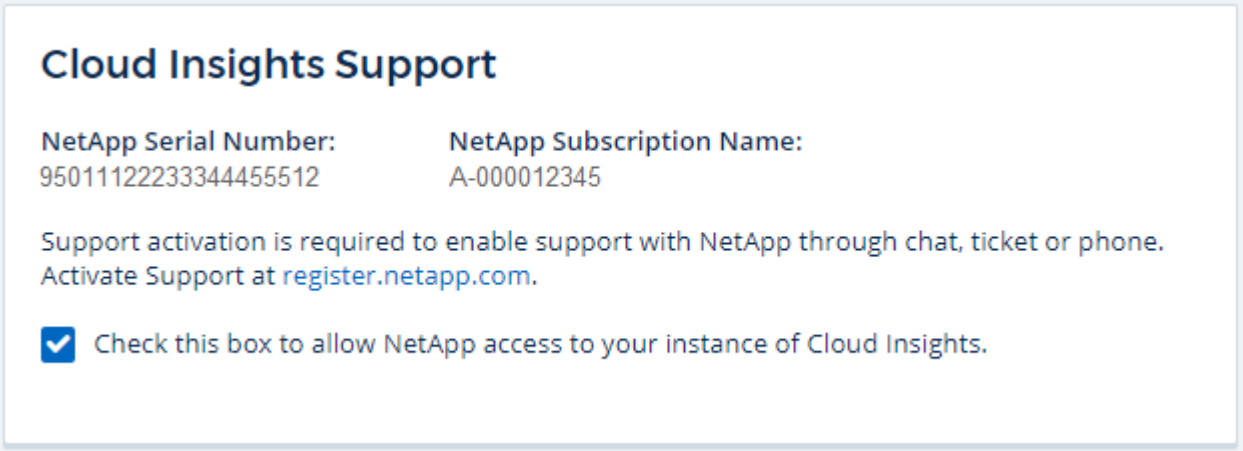
Durante il processo di sottoscrizione iniziale, l'istanza di Cloud Insights genererà un numero seriale NetApp a 20 cifre che inizia con "950". Questo numero di serie NetApp rappresenta l'abbonamento Cloud Insights associato al tuo account. È necessario registrare il numero di serie NetApp per attivare il supporto. Offriamo due opzioni per la registrazione del supporto:

1. Utente con account SSO NetApp Support Site (NSS) preesistente (ad es. Cliente NetApp attuale)
2. Nuovo cliente NetApp senza account SSO NetApp Support Site (NSS) preesistente

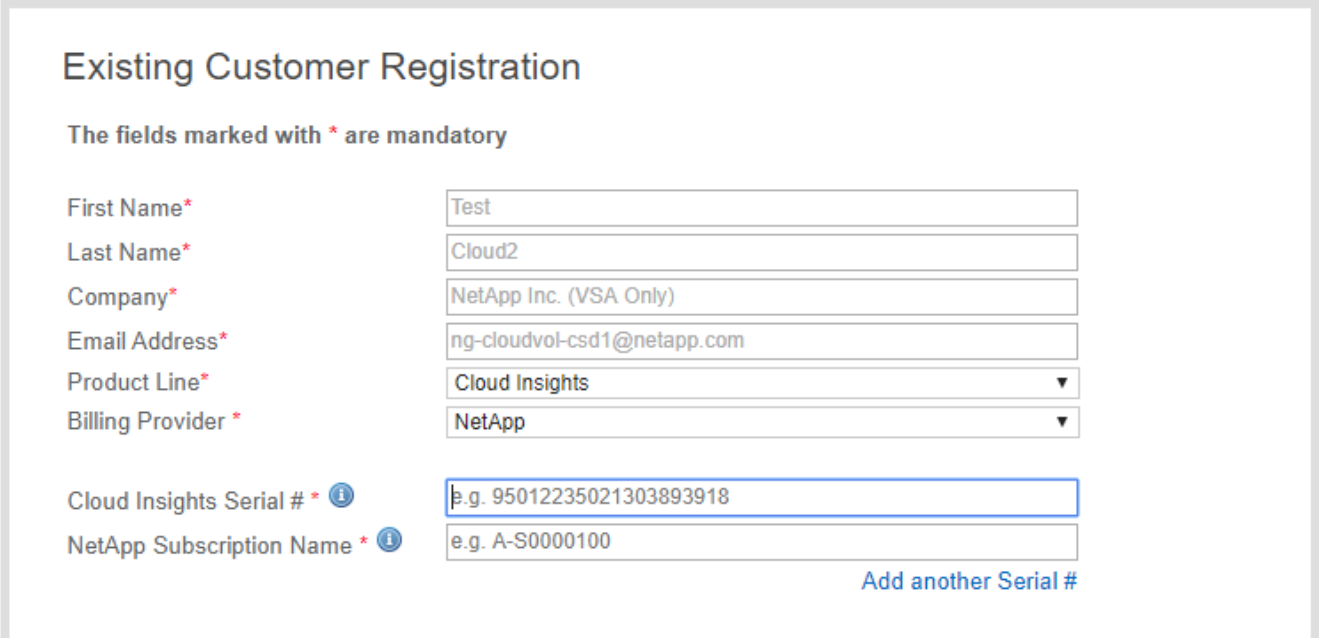
Opzione 1: Procedura per un utente con un account SSO NetApp Support Site (NSS) preesistente

Fasi

1. Accedere al sito Web di registrazione di NetApp https://register.netapp.com
2. Selezionare "sono già registrato come cliente NetApp" e scegliere *Cloud Insights* come linea di prodotti. Selezionare il proprio provider di fatturazione (NetApp o AWS) e fornire il numero di serie e il nome dell'abbonamento NetApp o l'ID cliente AWS facendo riferimento al menu **Guida › supporto** nell'interfaccia utente di Cloud Insights:



3. Compilare il modulo di registrazione cliente esistente e fare clic su **Invia**.

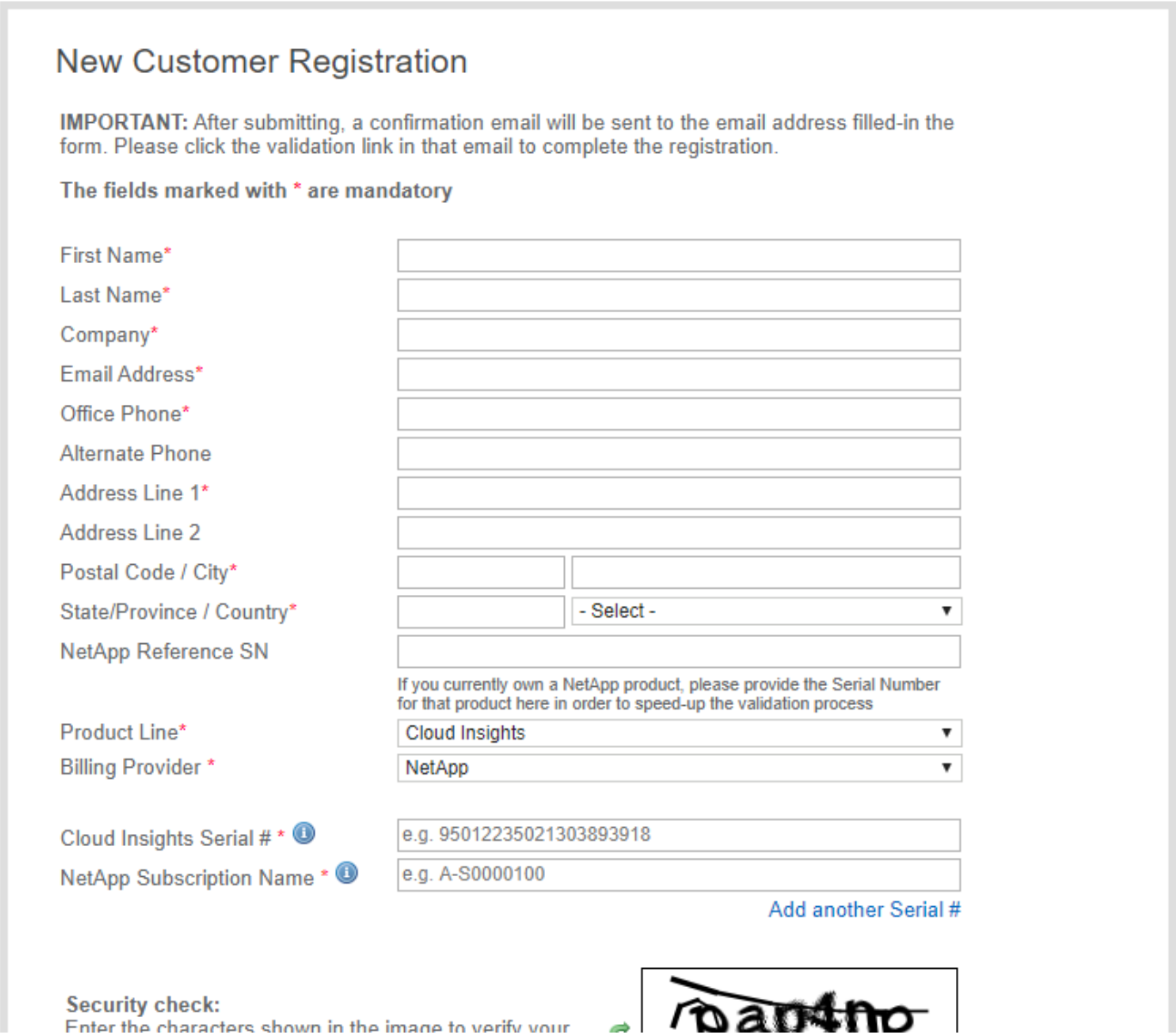


4. Se non si verificano errori, l'utente viene indirizzato a una pagina "registrazione inviata correttamente". L'indirizzo e-mail associato al nome utente SSO NSS utilizzato per la registrazione riceverà un'e-mail entro un paio di minuti con la dicitura "il prodotto è ora idoneo per il supporto".
5. Si tratta di una registrazione una tantum per il numero di serie NetApp di Cloud Insights.

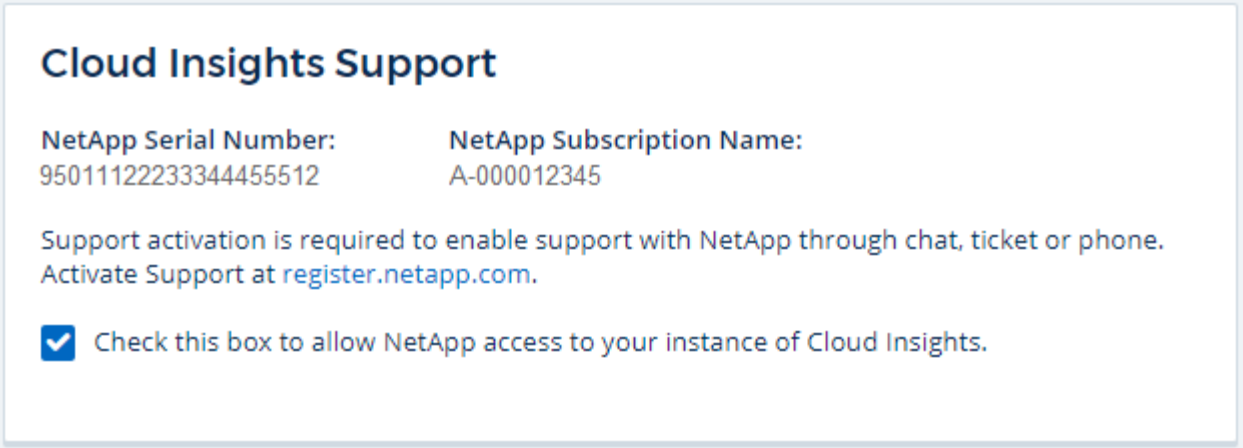
Opzione 2: Passaggi per un nuovo cliente NetApp senza account SSO NetApp Support Site (NSS) preesistente

Fasi

1. Accedere al sito Web di registrazione di NetApp https://register.netapp.com
2. Selezionare "non sono un cliente NetApp registrato" e compilare le informazioni richieste nel modulo di esempio riportato di seguito:



1. Selezionare *Cloud Insights* come linea di prodotti. Selezionare il proprio provider di fatturazione (NetApp o AWS) e fornire il numero di serie e il nome dell'abbonamento NetApp o l'ID cliente AWS facendo riferimento al menu **Guida › supporto** nell'interfaccia utente di Cloud Insights:



2. Se non si verificano errori, l'utente viene indirizzato a una pagina "registrazione inviata correttamente". L'indirizzo e-mail associato al nome utente SSO NSS utilizzato per la registrazione riceverà un'e-mail entro poche ore con la dicitura "il prodotto è ora idoneo per il supporto".
3. In qualità di nuovo cliente NetApp, dovrai anche creare un account utente NetApp Support Site (NSS) per le registrazioni future e accedere al portale di supporto per chat di supporto tecnico e ticketing web. Questo link si trova all'indirizzo https://mysupport.netapp.com/eservice/public/now.do. Per accelerare il processo, è possibile fornire il numero di serie Cloud Insights appena registrato.
4. Si tratta di una registrazione unica per il numero di serie NetApp di Cloud Insights.

Ottenere informazioni di supporto

NetApp fornisce supporto per Cloud Insights in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) o la community NetApp. Per gli utenti che hanno sottoscritto una qualsiasi delle edizioni Cloud Insights (di base*, standard, premium), il supporto tecnico è disponibile tramite telefono o ticketing web. Per il ticket Web e la gestione del caso è necessario un account SSO NetApp Support Site (NSS).

*Il supporto è disponibile con Basic Edition purché tutti i sistemi storage NetApp siano coperti almeno al livello Premium Support.

Supporto self-service:

Queste opzioni di supporto sono disponibili in modalità di prova e sono disponibili gratuitamente 24 ore su 24, 7 giorni su 7:

- **"Knowledge base"**

  Facendo clic sui collegamenti in questa sezione, si passa alla Knowledge base di NetApp, dove è possibile cercare articoli, procedure e altro ancora.

- **"Documentazione"**

  Facendo clic sul collegamento Documentation (documentazione) si passa a questo centro di documentazione.

- **"Comunità"**

  Facendo clic sul link della community, potrai accedere alla community NetApp Cloud Insights, dove potrai entrare in contatto con colleghi ed esperti.

Esiste anche un link da fornire xref:./**"Feedback"** Per aiutarci a migliorare Cloud Insights.

Supporto in abbonamento

Oltre alle opzioni di supporto autonomo descritte in precedenza, se si dispone di un abbonamento Cloud Insights o di un supporto a pagamento per prodotti o servizi NetApp monitorati, è possibile collaborare con un tecnico del supporto NetApp per risolvere il problema.

> Per eseguire questa operazione, è necessario registrarsi attivare il supporto Per i prodotti NetApp Cloud. Per registrarti, visita il sito di NetApp "Registrazione del supporto Cloud Data Services".

Si consiglia vivamente di selezionare la casella per consentire a un tecnico del supporto NetApp di accedere al proprio ambiente Cloud Insights durante la sessione di supporto. In questo modo, il tecnico potrà risolvere il problema e risolverlo rapidamente. Una volta risolto il problema o terminata la sessione di supporto, è possibile deselezionare la casella.

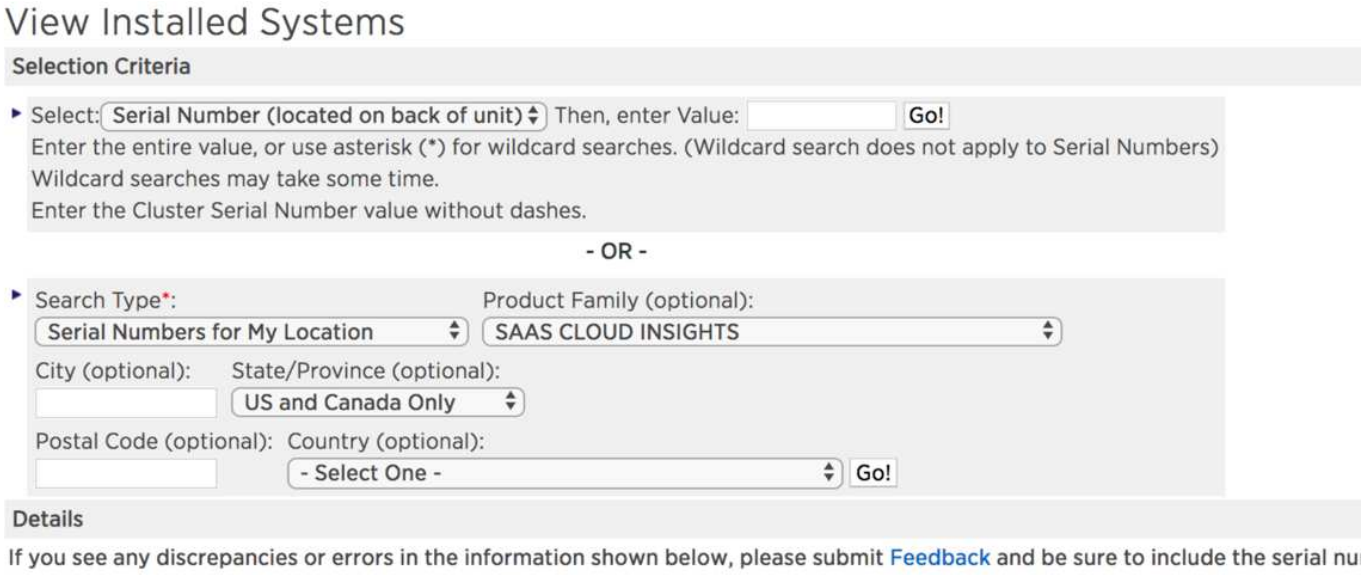
È possibile richiedere il supporto utilizzando uno dei seguenti metodi. Per utilizzare queste opzioni di supporto, è necessario disporre di un abbonamento Cloud Insights attivo:

- **"Telefono"**
- **"Support Ticket"**
- **Chat** - sarai in contatto con il personale di supporto di NetApp per ricevere assistenza (solo nei giorni feriali). La chat è disponibile nell'opzione di menu **Guida > Chat live** in alto a destra di qualsiasi schermata di Cloud Insights.

È inoltre possibile richiedere il supporto alle vendite facendo clic sul pulsante **"Contattare il reparto vendite"** collegamento.

Il numero di serie di Cloud Insights è visibile nel servizio dal menu **Guida > supporto**. In caso di problemi di accesso al servizio e se in precedenza si è registrato un numero di serie con NetApp, è possibile visualizzare l'elenco dei numeri di serie Cloud Insights dal sito del supporto NetApp come segue:

- Accedere a mysupport.netapp.com
- Dalla scheda del menu prodotti > prodotti personali, utilizzare la famiglia di prodotti "SaaS Cloud Insights" per individuare tutti i numeri di serie registrati:



Matrice di supporto per data collector Cloud Insights

È possibile visualizzare o scaricare informazioni e dettagli sui Data Collector supportati in **Matrice di supporto per data collector Cloud Insights**, role=.

Centro di apprendimento

Indipendentemente dal tuo abbonamento, **Guida > supporto** si collega a diverse offerte di corsi NetApp University per aiutarti a ottenere il massimo da Cloud Insights. Dai un'occhiata!

Data Collector Reference - infrastruttura

Riferimento specifico del vendor

Gli argomenti di questa sezione forniscono informazioni di riferimento specifiche del vendor. Nella maggior parte dei casi, la configurazione di un data collector è semplice. In alcuni casi, potrebbero essere necessarie informazioni o comandi aggiuntivi per configurare correttamente il data collector.

Fare clic su un **vendor** nel menu a sinistra per visualizzare le informazioni relative ai data collezionisti.

Configurazione del data collector Amazon EC2

Cloud Insights utilizza il data collector Amazon EC2 per acquisire dati di inventario e performance dalle istanze EC2.

Requisiti

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

- È necessario disporre di una delle seguenti opzioni:
  - Il ruolo **IAM** del tuo account cloud Amazon EC2, se utilizzi l'autenticazione ruolo IAM. Il ruolo IAM si applica solo se l'unità di acquisizione è installata su un'istanza di AWS.

    - L'ID **IAM Access Key** e la chiave di accesso segreta per l'account cloud Amazon EC2, se si utilizza l'autenticazione IAM Access Key.
- È necessario disporre del privilegio "list organization"
- Porta 443 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). I tasti di accesso consentono di firmare le richieste programmatiche inviate a EC2 se si utilizzano le operazioni API REST o Query di Amazon EC2 SDK. Queste chiavi vengono fornite con il contratto di Amazon.

Configurazione

Inserire i dati nei campi di raccolta dati in base alla tabella riportata di seguito:

Campo	Descrizione
Regione AWS	Scegliere la regione AWS
Ruolo IAM	Da utilizzare solo se acquisito su un AU in AWS. Per ulteriori informazioni su, vedere di seguito "Ruoli IAM".
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.
Capisco che AWS mi fattura per le richieste API	Verificare che AWS sia in grado di fornire una fattura per le richieste API effettuate tramite il polling Cloud Insights.

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)	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 'Includi', il campo Tag Key non può essere vuoto.

Campo	Descrizione
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.
Intervallo di polling delle performance (sec)	Il valore predefinito è 1800
Namespace CloudWatch Agent Metrics	Namespace in EC2/EBS da cui raccogliere i dati. Si noti che se i nomi delle metriche predefinite in questo namespace vengono modificati, Cloud Insights potrebbe non essere in grado di raccogliere i dati rinominati. Si consiglia di lasciare i nomi delle metriche di default.

Chiave di accesso IAM

Le chiavi di accesso sono credenziali a lungo termine per un utente IAM o per l'utente root dell'account AWS. Le chiavi di accesso vengono utilizzate per firmare le richieste programmatiche all'API AWS CLI o AWS (direttamente o utilizzando l'SDK AWS).

Le chiavi di accesso sono composte da due parti: Un ID della chiave di accesso e una chiave di accesso segreta. Quando si utilizza l'autenticazione *IAM Access Key* (invece dell'autenticazione *IAM role*), è necessario utilizzare sia l'ID della chiave di accesso che la chiave di accesso segreta per l'autenticazione delle richieste. Per ulteriori informazioni, consulta la documentazione Amazon all'indirizzo "Access Key (chiavi di accesso".

Ruolo IAM

Quando si utilizza l'autenticazione *IAM role* (invece dell'autenticazione IAM Access Key), 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.

Per ulteriori informazioni, consulta la documentazione Amazon all'indirizzo "Ruoli IAM".

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

Mappatura dei tag Amazon alle annotazioni Cloud Insights

Il data collector Amazon EC2 include un'opzione che consente di popolare le annotazioni Cloud Insights con

tag configurati su EC2. Le annotazioni devono essere denominate esattamente come tag EC2. Cloud Insights compila 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 il data collector non riesce a compilarla, potrebbe essere necessario rimuovere l'annotazione e ricrearla come testo.

Si noti che AWS fa distinzione tra maiuscole e minuscole, mentre Cloud Insights non fa distinzione tra maiuscole e minuscole. Pertanto, se si crea un'annotazione denominata "OWNER" (PROPRIETARIO) in Cloud Insights e si assegnano tag denominati "OWNER" (PROPRIETARIO), "Owner" (proprietario) e "Owner" (proprietario) in EC2, tutte le variazioni EC2 del "OWNER" (proprietario) verranno mappate all'annotazione "OWNER" (PROPRIETARIO) di Cloud Insight.

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

Cloud Insights 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 principale 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 **Configurazione avanzata** del Data Collector AWS di Cloud Insights, nel campo **ruolo account incrociato**.

Best practice: Si consiglia vivamente di assegnare il criterio *AmazonEC2ReadOnlyAccess* predefinito di AWS all'account principale EC2. Inoltre, l'utente configurato nell'origine dati deve avere assegnato almeno il criterio *AWSOrganizationsReadOnlyAccess* predefinito, per eseguire query su AWS.

Per informazioni sulla configurazione dell'ambiente in modo da consentire la raccolta di Cloud Insights dagli account secondari 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"

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Amazon FSX per NetApp ONTAP data collector

Questo data collector acquisisce i dati di inventario e performance da Amazon FSX per NetApp ONTAP. Questo data collector sarà reso disponibile in modo incrementale in tutte

le regioni del servizio Cloud Insights. Se l'icona di questo collector non viene visualizzata nel tuo ambiente Cloud Insights, contatta il tuo addetto alle vendite.

> Questo Cloud Insights Collector richiede un utente ONTAP con un ruolo *filesystem-scoped*. Consulta l'AWS "Ruoli e regole" documentazione per le opzioni disponibili. Attualmente AWS supporta solo un tipo di ruolo utente con ambito filesystem, che è *fsxadmin*. Questo è il ruolo appropriato da utilizzare per il Collector Cloud Insights. All'utente dovrebbero essere assegnate anche tutte e tre le seguenti applicazioni: http, ontapi, ssh.

Terminologia

Cloud Insights acquisisce i dati di inventario e performance dal data collector FSX-NetApp. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine Cloud Insights
Cluster	Storage
LUN	Volume
Volume	Volume interno

Terminologia FSX-NetApp

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

Storage

- Modello – un elenco delimitato da virgole dei nomi di modelli univoci e discreti all'interno di questo cluster.
- Vendor – AWS
- Serial Number (numero di serie): Il numero di serie dell'array.
- IP (IP): Generalmente corrisponde agli IP o ai nomi host configurati nell'origine dati.
- Raw Capacity (capacità raw): Somma di base 2 di tutto lo storage SSD assegnato al file system FSX.
- Latenza: Una rappresentazione di ciò che stanno sperimentando i carichi di lavoro dell'host, sia in lettura che in scrittura. Idealmente, Cloud Insights sta reperendo questo valore direttamente, ma spesso non è così. Al posto dell'array che offre questa opzione, Cloud Insights esegue in genere un calcolo ponderato per gli IOPS derivato dalle statistiche dei singoli volumi interni.
- Throughput: Aggregato da volumi interni. Gestione – può contenere un collegamento ipertestuale per l'interfaccia di gestione del dispositivo. Creato a livello di programmazione dall'origine dati Cloud Insights come parte del reporting dell'inventario.

Pool di storage

- Storage: Su quale array di storage vive questo pool. Obbligatorio.
- Type (tipo) – un valore descrittivo da un elenco di possibilità enumerate. La maggior parte dei casi sarà "aggregato" o "RAID Group".
- Capacity (capacità): I valori qui riportati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata in tali valori.

- IOPS: La somma degli IOPS di tutti i volumi allocati in questo pool di storage.
- Throughput (throughput): La somma del throughput di tutti i volumi allocati in questo pool di storage.

Requisiti

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

- È necessario avere accesso a un account con il ruolo "fsxadmin", con tre applicazioni assegnate - ssh, ontapi, http
- I dettagli dell'account includono nome utente e password.
- Requisiti di porta: 443

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

Metriche avanzate

Questo data collector raccoglie le seguenti metriche avanzate da FSX per lo storage NetApp ONTAP:

- fpolicy
- nfsv3
- nfsv3:nodo
- nfsv4
- nfsv4_1
- nfsv4_1:nodo
- nfsv4:nodo
- policy_group
- qtree
- volume
- workload_volume

Si noti che i comandi CLI e API di FSX recuperano alcuni valori di capacità che Cloud Insights ZAPI non raccoglie, pertanto alcuni valori di capacità (come quelli per i pool di storage) potrebbero essere diversi in Cloud Insights rispetto ad FSX stesso.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Ricevi una risposta HTTP 401 o un codice di errore ZAPI 13003 e ZAPI restituisce "privilegi insufficienti" o "non autorizzati per questo comando"	Controllare nome utente e password e privilegi/permessi dell'utente.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, modificarlo
Il comando ZAPI non riesce dopo il tentativo	Au ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.
L'AU non è riuscito a connettersi a ZAPI tramite HTTP	Controllare se la porta ZAPI accetta testo non crittografato. Se AU tenta di inviare testo non crittografato a un socket SSL, la comunicazione non riesce.
Comunicazione non riuscita con SSLException	AU sta tentando di inviare SSL a una porta di testo normale su un filer. Controllare se la porta ZAPI accetta SSL o utilizza una porta diversa.
Ulteriori errori di connessione: La risposta ZAPI ha il codice di errore 13001, il codice di errore "database non aperto" ZAPI è 60 e la risposta contiene "API non è stata completata in tempo" la risposta ZAPI contiene "initialize_session() ha restituito l'ambiente NULL" il codice di errore ZAPI è 14007 e la risposta contiene "nodo non è integro"	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione di Azure Compute Data Collector

Cloud 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
- URI di reindirizzamento Azure OAuth 2.0 (login.microsoftonline.com)
- IP REST di Azure Management (management.azure.com)
- IP di Azure Resource Manager (management.core.windows.net)
- Azure Service Principal Application (Client) ID (ruolo di lettore richiesto)
- Chiave di autenticazione principale del servizio Azure (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

Inserire i dati nei campi di raccolta 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

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 'Includi', 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.
Intervallo di polling delle performance (sec)	Il valore predefinito è 300

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Broadcom

Data collector di Brocade Network Advisor

Cloud Insights utilizza il data collector di Brocade Network Advisor per acquisire dati di inventario e performance dagli switch Brocade.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector di Brocade Network Advisor. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Switch	Switch
Porta	Porta
Fabric virtuale, fabric fisico	Fabric
Switch logico	Switch logico

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

Requisiti

Per configurare questo data collector sono necessari i seguenti requisiti:

- L'unità di acquisizione Cloud Insights inita le connessioni alla porta TCP 443 sul server BNA. Il server BNA deve eseguire la versione 14.2.1 o superiore.
- Indirizzo IP del server Brocade Network Advisor
- Nome utente e password di un account amministratore
- Requisito porta: HTTP/HTTPS 443

Configurazione

Campo	Descrizione
IP del server Brocade Network Advisor	Indirizzo IP del server Network Advisor
Nome utente	Nome utente dello switch
Nome utente	Nome utente amministratore
Password	Password dell'amministratore

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS (porta predefinita 443) o HTTP (porta predefinita 80)
Sovrascrivere la porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
Password	Password per lo switch
Intervallo di polling dell'inventario (min)	Il valore predefinito è 40

Campo	Descrizione
Gateway di accesso ai report	Selezionare questa opzione per includere i dispositivi in modalità Access Gateway
Intervallo di polling delle performance (sec)	Il valore predefinito è 1800

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Ricevere un messaggio che indica che più di un nodo è connesso alla porta di Access Gateway o che il data collector non riesce a rilevare il dispositivo Access Gateway.	Verificare che il dispositivo NPV funzioni correttamente e che siano presenti tutti i WWN collegati. Non acquisire direttamente il dispositivo NPV. Invece, l'acquisizione dello switch fabric core raccoglierà i dati del dispositivo NPV.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector per switch Brocade FC

Cloud Insights 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

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector dello switch FC Brocade. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Switch	Switch
Porta	Porta
Fabric virtuale, fabric fisico	Fabric
Zona	Zona
Switch logico	Switch logico
Volume virtuale	Volume
Zona LSAN	Zona IVR

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

Requisiti

- L'unità di acquisizione Cloud Insights (AU) 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), Cloud Insights identifica tutti gli switch del fabric; tuttavia, per rilevarli, è necessaria la connettività IP per 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.
- 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 del server EFC
Nome utente	Nome utente dello switch
Password	Password per lo switch
SNMP	Versione SNMP
Stringa di comunità SNMP	Stringa di comunità di sola lettura SNMP utilizzata per accedere allo switch
Nome utente SNMP	Nome utente SNMP
Password SNMP	Password SNMP

Configurazione avanzata

Campo	Descrizione
Nome fabric	Nome del fabric che deve essere segnalato dal data collector. Lasciare vuoto per riportare il nome del fabric come WWN.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 15.
Dispositivi esclusi	Elenco separato da virgole degli ID dei dispositivi da escludere dal polling
Domini amministrativi attivi	Selezionare se si utilizzano i domini di amministrazione
Recuperare i dati MPR	Selezionare questa opzione per acquisire i dati di routing dal router multiprotocollo.
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.

Campo	Descrizione
Tempo minimo tra trap (sec)	Tempo minimo tra i tentativi di acquisizione attivati dalle trap. Il valore predefinito è 10.
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 performance. Il valore predefinito è 300.
Protocollo SNMP Auth	Protocollo di autenticazione SNMP (solo SNMP v3)
Password per la privacy SNMP	Password per la privacy SNMP (solo SNMP v3)
Tentativi SNMP	Numero di tentativi SNMP

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
L'acquisizione dell'inventario dell'origine dati Brocade non riesce e viene visualizzato l'errore: ERRORE <date> <time> [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] errore 2 su 2: <datasource name> [errore interno] - Impossibile generare il modello per Device <IP>. Richiesta di rilevamento degli errori ([Device name <name>]): Impossibile generare il modello per Device <IP>. Richiesta di rilevamento degli errori)	Il problema potrebbe essere causato quando lo switch Brocade impiega troppo tempo per tornare con un prompt, superando il timeout predefinito di 5 secondi. Nelle impostazioni di configurazione avanzata del data collector in Cloud Insights, provare ad aumentare il valore di *timeout attesa banner SSH (sec)*.
Errore: "Cloud Insights ha ricevuto un ruolo chassis non valido"	Verificare che all'utente configurato in questa origine dati sia stata concessa l'autorizzazione per il ruolo dello chassis.
Errore: "Indirizzo IP chassis non corrispondente"	Modificare la configurazione dell'origine dati per utilizzare l'indirizzo IP dello chassis.
Viene visualizzato un messaggio che indica che più di un nodo è connesso alla porta Access Gateway	Verificare che il dispositivo NPV funzioni correttamente e che siano presenti tutti i WWN collegati. Non acquisire direttamente il dispositivo NPV. Invece, l'acquisizione dello switch fabric core raccoglierà i dati del dispositivo NPV.
La raccolta delle prestazioni non riesce e viene visualizzato il messaggio "Timed out during sending SNMP request".	A seconda delle variabili di query e della configurazione dello switch, alcune query potrebbero superare il timeout predefinito. "Scopri di più".

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Brocade FOS REST Data Collector

Cloud Insights utilizza il REST Collector Brocade FOS per rilevare l'inventario e le prestazioni dei dispositivi switch Brocade che eseguono il firmware FabricOS (FOS) 8,2 e versioni successive.

Per impostazione predefinita, questo raccoglitore tenterà di scoprire tutti i dispositivi FOS che fanno parte di tutti i tessuti di cui fa parte lo switch.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal raccoglitore di dati REST Brocade FOS. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Switch	Switch
Porta	Porta
Fabric virtuale, fabric fisico	Fabric
Zona	Zona
Switch logico	Switch logico
Volume virtuale	Volume
Zona LSAN	Zona IVR

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

Requisiti

- Deve essere presente una connettività TCP a tutti gli switch del fabric. Questo tipo di raccolta dati proverà senza problemi sia HTTP che HTTPS per ogni dispositivo nel fabric. Se si seleziona la casella di controllo *rileva tutti gli switch nel fabric*, Cloud Insights identifica tutti gli switch nel fabric; tuttavia, per scoprirli è necessaria la connettività TCP a tali switch aggiuntivi.
- Lo stesso account è necessario a livello globale per tutti gli switch del fabric. È possibile utilizzare l'interfaccia Web della periferica per confermare l'accesso.

Configurazione

Campo	Descrizione
IP dello switch	Indirizzo IP o nome di dominio completo dello switch FOS
Nome utente	Nome utente dello switch
Password	Password per lo switch

Configurazione avanzata

Campo	Descrizione
Dispositivi esclusi	Elenco separato da virgole degli indirizzi del dispositivo IPv4 da escludere dal polling.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 60.
Scopri tutti gli switch del fabric	Selezionare per rilevare tutti gli switch nel fabric.
Scegli di favorire HBA vs Alias zona	Scegliere se privilegiare gli alias HBA o zone.
Tipo di connessione	HTTP o HTTPS.
Tenere presente che questa impostazione modifica solo il ci del protocollo che tenta di utilizzare per primo per dispositivo; se l'impostazione predefinita non riesce, il ci tenta automaticamente il protocollo opposto	Sovrascrivere la porta TCP
Specificare una porta se non si utilizza l'impostazione predefinita.	Intervallo di polling delle performance (sec)

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
La funzione Test indica che un protocollo non è accessibile	Un determinato dispositivo Brocade FOS 8,2+ desidera parlare solo su HTTP o HTTPS. Se uno switch dispone di un certificato digitale installato, lo switch genera errori HTTP se si tenta di comunicare con HTTP non crittografato rispetto a HTTPS. La funzione di test tenta di comunicare sia con HTTP che con HTTPS. Se il test indica che un protocollo viene superato, è possibile salvare il collettore senza preoccuparsi che l'altro protocollo non sia riuscito. Il collettore tenta entrambi i protocolli durante la raccolta e non riesce solo se nessuno dei due funziona.
Errore: "Cloud Insights ha ricevuto un ruolo chassis non valido"	Verificare che all'utente configurato in questa origine dati sia stata concessa l'autorizzazione per il ruolo dello chassis.
Errore: "Indirizzo IP chassis non corrispondente"	Modificare la configurazione dell'origine dati per utilizzare l'indirizzo IP dello chassis.
Viene visualizzato un messaggio che indica che più di un nodo è connesso alla porta Access Gateway	Verificare che il dispositivo NPV funzioni correttamente e che siano presenti tutti i WWN collegati. Non acquisire direttamente il dispositivo NPV. Invece, l'acquisizione dello switch fabric core raccoglierà i dati del dispositivo NPV.

Problema:	Prova:
La raccolta delle prestazioni non riesce e viene visualizzato il messaggio "Timed out during sending SNMP request".	A seconda delle variabili di query e della configurazione dello switch, alcune query potrebbero superare il timeout predefinito. "Scopri di più".

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector degli switch Cisco MDS Fabric

Cloud Insights utilizza il data collector degli switch Cisco MDS Fabric per rilevare l'inventario degli switch Cisco MDS Fabric e una serie di switch Cisco Nexus FCoE su cui è abilitato il servizio FC.

Inoltre, con questo data collector è possibile scoprire molti modelli di dispositivi Cisco in esecuzione in modalità NPV.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector dello switch FC Cisco. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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

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

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

Configurazione

Campo	Descrizione
IP switch Cisco	Indirizzo IP o nome di dominio completo dello switch
Versione SNMP	Selezionare V1, V2 o V3. Per l'acquisizione delle performance è necessario V2 o successivo.
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
Dispositivi esclusi	Elenco separato da virgole degli IP delle periferiche da escludere dal polling
Dispositivi inclusi	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

Campo	Descrizione
Primo tipo di alias	Fornire una prima preferenza per la risoluzione dell'alias. Scegliere tra le seguenti opzioni: **Device Alais** (Nome dispositivo). Si tratta di un nome di facile utilizzo per una porta WWN (pWWN) che può essere utilizzata in tutti i comandi di configurazione, a seconda delle esigenze. Tutti gli switch della famiglia Cisco MDS 9000 supportano i servizi Distributed Device Alias (alias del dispositivo). **Nessuno** non segnalare alcun alias. **Port Description** Descrizione della porta che consente di identificarla in un elenco di porte. **Zone Alias (All)** Nome di facile utilizzo per una porta che può essere utilizzata solo per la configurazione attiva. Questa è l'impostazione predefinita.
Secondo tipo di alias	Specificare una seconda preferenza per la risoluzione dell'alias
Terzo tipo di alias	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)

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: Impossibile rilevare lo chassis. Non sono stati rilevati switch	• Eseguire il ping del dispositivo con l'indirizzo IP configurato • accedere al dispositivo utilizzando la GUI di Cisco Device Manager • accedere al dispositivo utilizzando la CLI • provare a eseguire il percorso SNMP
Errore: Il dispositivo non è uno switch Cisco MDS	• Assicurarsi che l'IP dell'origine dati configurato per il dispositivo sia corretto • accedere al dispositivo utilizzando la GUI di Cisco Device Manager • accedere al dispositivo utilizzando la CLI
Errore: Cloud Insights non è in grado di ottenere il WWN dello switch.	Questo potrebbe non essere uno switch FC o FCoE e pertanto potrebbe non essere supportato. Assicurarsi che l'IP/FQDN configurato nell'origine dati sia uno switch FC/FCoE.
Errore: Trovati più di un nodo collegato alla porta dello switch NPV	Disattiva l'acquisizione diretta dello switch NPV

Problema:	Prova:
Errore: Impossibile connettersi allo switch	• Assicurarsi che il dispositivo sia ATTIVO • controllare l'indirizzo IP e la porta di ascolto • eseguire il ping del dispositivo • accedere al dispositivo utilizzando la GUI di Cisco Device Manager • accedere al dispositivo utilizzando CLI • eseguire il controllo SNMP

Performance

Problema:	Prova:
Errore: Acquisizione delle prestazioni non supportata da SNMP v1	• Modifica origine dati e disattiva prestazioni switch • Modifica origine dati e configurazione switch per utilizzare SNMP v2 o superiore

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector SmartFiles di Cohesity

Questo collector basato su API REST acquisirà un cluster di Cohesity, scoprendo le "viste" (come volumi interni Cloud Insights), i vari nodi e raccogliendo le metriche delle performance.

Configurazione

Campo	Descrizione
IP del cluster di Cohesity	Indirizzo IP del cluster Cohesity
Nome utente	Nome utente del cluster Cohesity
Password	Password utilizzata per il cluster Cohesity

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta utilizzata per la comunicazione TCP con il cluster Cohesity
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (min)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 900 secondi.

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Dell

Data collector Dell EMC serie XC

Cloud Insights utilizza questo data collector per rilevare le informazioni sull'inventario e sulle performance degli array di storage Dell EMC serie XC.

Configurazione

Campo	Descrizione
Indirizzo IP esterno PRISM	Indirizzo IP del server XC
Nome utente	Nome utente del server XC
Password	Password utilizzata per il server XC

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta utilizzata per la comunicazione TCP con il server XC
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (min)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Dell EMC

Data collector DELL EMC Data Domain

Questo data collector raccoglie le informazioni di inventario e performance dai sistemi storage DI deduplica DELL EMC Data Domain. Per configurare questo data collector, è necessario seguire specifiche istruzioni di configurazione e consigli sull'utilizzo.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector del dominio dati. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Array	Storage
Porta FC	Porta
File System	Volume interno

Vendor/modello	Termine Cloud Insights
Quota	Quota
Condivisione NFS e CIFS	FileShare

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- 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. Il valore predefinito è 20.
Porta SSH	Porta di servizio SSH

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector 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 o un nome host del cluster ECS e un nome utente e una password.

> Dell EMC ECS viene misurato a un tasso diverso da TB raw a unità gestite. Ogni 40 TB di capacità ECS non formattata viene addebitato come 1 "Unità gestita (MU)".

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector ECS. 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 Cloud Insights
Cluster	Storage
Tenant	Pool di storage
Bucket	Volume interno
Disco	Disco

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

Requisiti

- Un indirizzo IP o un nome host del cluster ECS
- Un nome utente e una password per il sistema ECS
- Porta 4443 (HTTPS). Richiede la connettività in uscita alla porta TCP 4443 sul sistema ECS.

Configurazione

Campo	Descrizione
Host ECS	Indirizzo IP o nome di dominio completo del sistema ECS
Porta host ECS	Porta utilizzata per la comunicazione con l'host ECS
ID utente ECS	ID utente per ECS
Password	Password utilizzata per ECS

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	L'impostazione predefinita è 360 minuti.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: Autenticazione dell'utente non riuscita.	Assicurarsi che le credenziali per questa periferica siano corrette.

Performance

Problema:	Prova:
Errore: Dati non raccolti a sufficienza.	• Controllare la data e l'ora di raccolta nel file di log e modificare di conseguenza l'intervallo di polling • attendere più a lungo
Errore: L'intervallo di polling delle prestazioni è troppo grande.	Controllare la data e l'ora di raccolta nel file di registro{logfile} e modificare di conseguenza l'intervallo di polling

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Dell EMC PowerScale

Cloud Insights utilizza il data collector SSH Dell EMC PowerScale (in precedenza Isilon) per acquisire dati di inventario e performance dallo storage NAS scale-out PowerScale.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
File System	Volume interno

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Autorizzazioni di amministratore per lo storage PowerScale
- Indirizzo IP del cluster PowerScale
- Accesso SSH alla porta 22

Configurazione

Campo	Descrizione
Indirizzo IP	L'indirizzo IP o il nome di dominio completo del cluster PowerScale
Nome utente	Nome utente del cluster PowerScale
Password	Password utilizzata per il cluster PowerScale

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. Il valore predefinito è 300.
Porta SSH	Porta di servizio SSH. Il valore predefinito è 22.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Credenziali di accesso non valide" con messaggi di errore "i comandi non abilitati per l'amministrazione basata sul ruolo richiedono l'accesso dell'utente root"	* Verificare che l'utente disponga delle autorizzazioni per eseguire i seguenti comandi sul dispositivo: > versione isi osrelease > stato isi -q > stato isi -n > dispositivi isi -d %s > licenza isi * verificare che le credenziali utilizzate nella procedura guidata corrispondano alle credenziali del dispositivo
"Errore interno" con messaggi di errore "esecuzione del comando <Your command> non riuscita con permesso: <Your current permission>. Problema di autorizzazione per l'esecuzione del comando sudo"	Verificare che l'utente disponga delle autorizzazioni sudo per eseguire il seguente comando sul dispositivo

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Dell EMC Isilon/PowerScale REST Data Collector

Cloud Insights utilizza il data collector REST di Dell EMC ISILON/PowerScale per acquisire dati di inventario e performance dallo storage Dell EMC ISILON o PowerScale. Questo collector supporta gli array che eseguono OneFS 8.0.0+.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
File system OneFS	Volume interno
File system OneFS	Pool di storage

Vendor/modello	Termine Cloud Insights
Qtree	Qtree

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Un account utente e una password. Non è necessario che questo account sia admin/root, ma È NECESSARIO concedere un numero considerevole di privilegi di sola lettura all'account di servizio (vedere la tabella riportata di seguito)
- Indirizzo IP/Nome di dominio completo del cluster Dell EMC Isilon/PowerScale
- Accesso HTTPS alla porta 8080
- Cluster Isilon/PowerScale con OneFS 8.0.0 o superiore

Nome privilegio	Descrizione	r(lettura) o rw (lettura+scrittura)
ISI_PRIV_LOGIN_PAPI	API della piattaforma	r
ISI_PRIV_SYS_TIME	Ora	r
ISI_PRIV_AUTH	Auth	r
ISI_PRIV_ROLE	Privilegio	r
ISI_PRIV_DEVICES	Dispositivi	r
ISI_PRIV_EVENT	Evento	r
ISI_PRIV_HDFS	HDFS	r
ISI_PRIV_NDMP	NDMP	r
ISI_PRIV_NETWORK	Rete	r
ISI_PRIV_NFS	NFS	r
ISI_PRIV_PAPI_CONFIG	Configurare l'API della piattaforma	r
ISI_PRIV_QUOTA	Quota	r
ISI_PRIV_SMARTPOOLS	SmartPools	r
ISI_PRIV_SMB	PMI	r
ISI_PRIV_STATISTICS	Statistiche	r
ISI_PRIV_SWIFT	Rapido	r
ISI_PRIV_JOB_ENGINE	Motore di lavoro	r

Configurazione

Campo	Descrizione
Indirizzo IP Isilon	L'indirizzo IP o il nome di dominio completo dello storage Isilon
Nome utente	Nome utente di Isilon
Password	Password utilizzata per Isilon

Configurazione avanzata

Campo	Descrizione
Porta HTTPS	Il valore predefinito è 8080.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 20.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. Il valore predefinito è 300.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Credenziali di accesso non valide" con messaggi di errore "i comandi non abilitati per l'amministrazione basata sul ruolo richiedono l'accesso dell'utente root"	* Verificare che l'utente disponga delle autorizzazioni per eseguire i seguenti comandi sul dispositivo: > versione isi osrelease > stato isi -q > stato isi -n > dispositivi isi -d %s > licenza isi * verificare che le credenziali utilizzate nella procedura guidata corrispondano alle credenziali del dispositivo
"Errore interno" con messaggi di errore "esecuzione del comando <Your command> non riuscita con permesso: <Your current permission>. Problema di autorizzazione per l'esecuzione del comando sudo"	Verificare che l'utente disponga delle autorizzazioni sudo per eseguire il seguente comando sul dispositivo

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Dell EMC PowerStore

Il data collector EMC PowerStore raccoglie le informazioni di inventario dallo storage 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.

Il data collector EMC PowerStore raccoglie le relazioni di replica volume-volume che PowerStore coordina tra altri array di storage. Cloud Insights mostra un array di storage per ciascun cluster PowerStore 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.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Indirizzo IP o nome di dominio completo del processore di storage
- Nome utente e password di sola lettura

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 PowerStore di Cloud Insight utilizza i dati di origine della granularità di 5 minuti di PowerStore. Di conseguenza, Cloud Insights esegue il polling dei dati ogni cinque minuti e questo non è

configurabile.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector Dell EMC RecoverPoint

Il caso d'utilizzo principale del data collector EMC RecoverPoint consiste nel rilevare le relazioni di replica volume-volume che l'appliance di storage RecoverPoint facilita. Questo collector rileverà anche l'appliance Recoverpoint. Dell/EMC vende una soluzione di backup VMware per macchine virtuali --"RecoverPoint per macchine virtuali" - che non è supportata da questo collector

Per la configurazione, il data collector richiede l'indirizzo IP dei processori di storage e un nome utente e una password di sola lettura.

Il data collector EMC RecoverPoint raccoglie le relazioni di replica volume-volume che RecoverPoint coordina tra altri storage array. Cloud Insights 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

Per configurare questo data collector sono necessarie le seguenti informazioni:

- 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

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 utilizzata 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. L'impostazione predefinita è 20 minuti.
Cluster esclusi	Elenco separato da virgole di ID cluster o nomi da escludere durante il polling.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Raccolta dati DELL EMC ScaleIO / PowerFlex

Il data collector ScaleIO/PowerFlex raccoglie le informazioni di inventario dallo storage ScaleIO e PowerFlex. Per la configurazione, questo data collector richiede l'indirizzo del gateway ScaleIO/PowerFlex e un nome utente e una password amministratore.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector ScaleIO/PowerFlex. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Cluster MDM (Meta Data Manager)	Storage
SDS (server dati ScaleIO/PowerFlex)	Nodo di storage
Pool di storage	Pool di storage
Volume	Volume
Dispositivo	Disco

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

Requisiti

- Accesso in sola lettura all'account utente Admin
- Requisito della porta: Porta HTTPS 443

Configurazione

Campo	Descrizione
Gateway ScaleIO/PowerFlex	Indirizzi IP o FQDN dei gateway ScaleIO/PowerFlex, separati da virgola (,) o punto e virgola (;)
Nome utente	Nome utente amministratore utilizzato per accedere al dispositivo ScaleIO/PowerFlex
Password	Password utilizzata per accedere al dispositivo ScaleIO/PowerFlex

Configurazione avanzata

Fare clic sulla casella di controllo Inventory (inventario) per attivare la raccolta dell'inventario.

Campo	Descrizione
Porta HTTPS	443
Intervallo di polling dell'inventario (min)	Il valore predefinito è 60.
Timeout connessione (sec)	Il valore predefinito è 60.

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector EMC Unity

IL data collector DELL EMC Unity (precedentemente noto come VNXe) fornisce il supporto dell'inventario per gli array di storage unificati VNXe. Cloud Insights attualmente supporta i protocolli iSCSI e NAS.

Requisiti

- Unity data Collector è basato su CLI; è necessario installare Unisphere for Unity CLI (uemcli.exe) sull'unità di acquisizione in cui risiede il data collector VNXe.
- uemcli.exe utilizza HTTPS come protocollo di trasporto, pertanto l'unità di acquisizione deve essere in grado di avviare connessioni HTTPS con l'unità.
- Indirizzo IP o nome di dominio completo del dispositivo Unity
- È necessario disporre di almeno un utente di sola lettura per l'utilizzo da parte del data collector.
- HTTPS sulla porta 443 è obbligatorio
- Il data collector EMC Unity fornisce supporto NAS e iSCSI per l'inventario; verranno rilevati volumi Fibre Channel, ma Cloud Insights non esegue report su mappatura FC, mascheratura o porte di storage.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector Unity. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Array di storage	Storage
Del processore	Nodo di storage
Pool di storage	Pool di storage
Informazioni generali blocco iSCSI, VMware VMFS	Condividere
Sistema remoto di replica	Sincronizzazione
Nodo iSCSI	Nodo di destinazione iSCSI
ISCSI Initiator	ISCSI Target Initiator

Nota: Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare tutti i casi per questa

origine dati.

Configurazione

Campo	Descrizione
Storage unificato	Indirizzo IP o nome di dominio completo del dispositivo Unity
Nome utente	Nome utente del dispositivo Unity
Password	Password per il dispositivo Unity
Percorso completo all'UEMCLI eseguibile	Percorso completo della cartella contenente l'eseguibile *uemcli.exe*

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 40 minuti
Porta CLI Unity	Porta utilizzata per l'unità CLI
Intervallo di polling delle performance (sec)	Il valore predefinito è 300.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Impossibile eseguire l'utility esterna" con il messaggio di errore "Impossibile trovare l'eseguibile Unisphere uemcli"	* Verificare l'indirizzo IP, il nome utente e la password corretti * verificare che l'interfaccia CLI di Unisphere sia installata sull'unità di acquisizione Cloud Insights * verificare che la directory di installazione dell'interfaccia CLI di Unisphere sia corretta nella configurazione dell'origine dati * verificare che l'indirizzo IP dell'unità sia corretto nella configurazione dell'origine dati. Dall'unità di acquisizione Cloud Insights, aprire un CMD e passare alla directory di installazione configurata:{INSTALLDIR. Provare a stabilire una connessione con il dispositivo VNXe digitando: Uemcli -d <Your IP> -u <Your ID> /sys/General show

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Raccolta dati dei dispositivi Dell EMC VMAX e PowerMax

Cloud Insights rileva gli array di storage EMC VMAX e PowerMax utilizzando i comandi simcli di Solutions Enabler insieme a un server di Solutions Enabler esistente nel tuo ambiente. Il server Solutions Enabler esistente dispone della connettività all'array di

storage VMAX/PowerMax attraverso l'accesso ai volumi di gatekeeper.

Requisiti

Prima di configurare questo data collector, assicurarsi che Cloud Insights disponga della connettività TCP alla porta 2707 sul server di abilitazione soluzioni esistente. Cloud Insights 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 sul server dell'unità di acquisizione e la versione deve corrispondere o essere precedente alla versione in esecuzione sul server Solutions Enabler.
- È necessario un file {installdir} EMC SYMAPI config netcnfg configurato correttamente. 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.
- Indirizzo IP del server Solutions Enabler di gestione
- Autorizzazioni di amministratore per il server Solutions Enabler (se)
- Nome utente e password di sola lettura per il software se
- L'applicazione UNISPHERE for VMAX deve essere in esecuzione e raccogliere statistiche per gli array Sstorage EMC VMAX e PowerMax gestiti dall'installazione del provider SMI-S.
- Convalida dell'accesso per le prestazioni: In un browser Web dell'unità di acquisizione, andare a _ https://<SMI-S Hostname or IP>:5989/ecomconfig_ dove "SMI-S Hostname or IP" (Nome host SMI-S o IP) è l'indirizzo IP o il nome host del server SMI-S. Questo URL è destinato a un portale amministrativo per il servizio EMC SMI-S (noto anche come "ECOM"). Viene visualizzata una finestra a comparsa per l'accesso.
- Le autorizzazioni devono essere dichiarate nel file di configurazione daemon del server Solutions Enabler, generalmente trovato qui: */var/symapi/config/daemon_users*

  Di seguito viene riportato un file di esempio con le autorizzazioni cisys appropriate.

```
root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###     Refer to the storrdfd(3) man page for additional details.
###
###     As noted above, only authorized users can perform stordaemon
control
###     operations (e.g., shutdown).
#######################################################################
########
# smith         storrdfd
cisys storapid <all>
```

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dall'origine dati EMC VMAX/PowerMax. 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 Cloud Insights
Disco	Disco
Gruppo di dischi	Gruppo di dischi
Storage	Storage array
Direttore	Nodo di storage
Pool di dispositivi, Storage Resource Pool (SRP)	Pool di storage
Sviluppo del dispositivo	Volume

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

Configurazione

Nota: se l'autenticazione utente SMI-S non è attivata, i valori predefiniti nel data collector Cloud Insights vengono ignorati.

Campo	Descrizione
Nome servizio	Nome del servizio specificato nel file *netcnfg*
Percorso completo alla CLI	Percorso completo della cartella contenente l'interfaccia CLI di Symmetrix
Indirizzo IP host SMI-S.	Indirizzo IP dell'host SMI-S.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 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.
Elenco dispositivi filtro inventario	Elenco separato da virgole degli ID dei dispositivi da includere o escludere

Campo	Descrizione
Caching della connessione	Scegliere il metodo di caching della connessione: * LOCALE significa che il servizio di acquisizione Cloud Insights 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 del 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 falliti 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. **Nota:** questa impostazione non modifica il comportamento di Cloud Insights rispetto agli array elencati COME REMOTI dall'output "symcfg list". Cloud Insights raccoglie i dati solo sui dispositivi indicati COME LOCALI da questo comando.
Protocollo SMI-S.	Protocollo utilizzato per connettersi al provider SMI-S. Visualizza anche la porta predefinita utilizzata.
Eseguire l'override di SMIS-Port	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
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)
Selezionare 'Escludi' o 'Includi' per specificare un elenco	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

Risoluzione dei problemi

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

Problema:	Prova:
Errore: La funzione richiesta non è attualmente concessa in licenza	Installare la licenza del server SYMAPI.
Errore: Nessun dispositivo trovato	Assicurarsi che i dispositivi Symmetrix siano configurati per essere gestiti dal server Solutions Enabler: - Eseguire symcfg list -v per visualizzare l'elenco dei dispositivi Symmetrix configurati.
Errore: Non è stato trovato un servizio di rete richiesto nel file di servizio	Assicurarsi che il nome del servizio Solutions Enabler sia definito come file netcnfg per Solutions Enabler. Questo file si trova in genere sotto SYMAPI nell'installazione del client Solutions Enabler.
Errore: Handshake del client/server remoto non riuscito	Controllare i file storsrvd.log* più recenti sull'host Solutions Enabler che si sta cercando di scoprire.
Errore: Nome comune nel certificato client non valido	Modificare il file *hosts* sul server Solutions Enabler in modo che il nome host dell'unità di acquisizione si risolva nell'indirizzo IP riportato in storsrvd.log sul server Solutions Enabler.
Errore: La funzione non ha potuto ottenere memoria	Assicurarsi che la memoria disponibile nel sistema sia sufficiente per eseguire Solutions Enabler
Errore: Solutions Enabler non è stato in grado di fornire tutti i dati richiesti.	Esaminare lo stato di salute e il profilo di carico di Solutions Enabler
Errore: • Il comando CLI "symcfg list -tdev" potrebbe restituire dati errati quando viene raccolto con Solutions Enabler 7.x da un server Solutions Enabler 8.x. • Il comando CLI "symcfg list -srp" potrebbe restituire dati non corretti se raccolti con Solutions Enabler 8.1.0 o versioni precedenti da un server Solutions Enabler 8.3 o versioni successive.	Assicurarsi di utilizzare la stessa release principale di Solutions Enabler
Vengono visualizzati errori di raccolta dati con il messaggio "Unknown code" (Codice sconosciuto)	Questo messaggio potrebbe essere visualizzato se le autorizzazioni non sono dichiarate nel file di configurazione daemon del server Solutions Enabler (vedere la Requisiti sopra). Si presuppone che la versione del client se corrisponda alla versione del server se. Questo errore può verificarsi anche se l'utente *cisys* (che esegue i comandi di Solutions Enabler) non è stato configurato con le autorizzazioni daemon necessarie nel file di configurazione /var/symapi/config/daemon_users. Per risolvere questo problema, modificare il file /var/symapi/config/daemon_users e assicurarsi che l'utente cisys disponga dell'autorizzazione <all> specificata per il daemon storapid. Esempio: 14:11:25 tail /var/symapi/config/daemon_users … <all> storapid cisys

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Dell EMC VNX Block Storage (navicli)

Cloud Insights utilizza il data collector Dell EMC VNX Block Storage (Navisec) (in precedenza CLARiiON) per acquisire dati di inventario e performance.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector dello storage a blocchi EMC VNX. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Storage	Storage
Processore per lo storage	Nodo di storage
Questo pool, gruppo RAID	Pool di storage
LUN	Volume

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

Requisiti

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

- Un indirizzo IP di ciascun processore di storage a blocchi VNX
- Nome utente e password Navisphere di sola lettura per gli array di storage a blocchi VNX
- NaviSecCli deve essere installato su Cloud Insights AU
- Convalida degli accessi: Eseguire NaviSecCLI dall'AU Cloud Insights a ciascun array utilizzando il nome utente e la password.
- Requisiti delle porte: 80, 443
- La versione di NaviSecCLI deve corrispondere al codice FLARE più recente sull'array
- Per le performance, è necessario attivare la registrazione delle statistiche.

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 comando <use 443 by default>

Configurazione

Campo	Descrizione
Indirizzo IP dello storage a blocchi VNX	Indirizzo IP o nome di dominio completo dello storage a blocchi VNX
Nome utente	Nome utilizzato per accedere al dispositivo di storage a blocchi VNX.

Campo	Descrizione
Password	Password utilizzata per accedere al dispositivo di storage a blocchi VNX.
Percorso CLI a naviseccli.exe	Percorso completo della cartella contenente l'eseguibile *navigeccli.exe*

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. Il valore predefinito è 40 minuti.
Scopo	L'ambito del client sicuro. L'impostazione predefinita è Globale.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: • Agente non in esecuzione • Impossibile trovare navigli • Impossibile eseguire qualsiasi comando	• Verificare che Navisphere CLI sia installato sull'unità di acquisizione Cloud Insight • non è stata selezionata l'opzione "Usa client sicuro" nella configurazione guidata del data collector e non è installata una versione non sicura di Navisphere CLI. • Verificare che la directory di installazione di Navisphere CLI sia corretta nella configurazione del data collector • verificare che l'IP dello storage a blocchi VNX sia corretto nella configurazione del data collector: • Dall'unità di acquisizione Cloud Insights: - Aprire un CMD. - Cambiare la directory nella directory di installazione configurata - provare a stabilire una connessione con il dispositivo di storage a blocchi VNX digitando "navicli -h {ip} getagent" (sostituire l' {ip} con l'IP effettivo)
Errore: 4.29 emc235848 emc241018 getall Impossibile analizzare le informazioni alias host	Questo è probabilmente causato da un problema DI corruzione FLARE 29 del database iniziatore host sull'array stesso. Consulta gli articoli della Knowledge base EMC: Emc235848, emc241018. Puoi anche controllare https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128

Problema:	Prova:
Errore: Impossibile recuperare i Meta LUN. Errore durante l'esecuzione di java -jar navicli.jar	• Modificare la configurazione del data collector per utilizzare il client sicuro (scelta consigliata) • installare navicli.jar nel percorso CLI a navicli.exe O naviseccli.exe • Nota: navicli.jar è obsoleto a partire dalla versione 6.26 di EMC Navisphere • il navicli.jar potrebbe essere disponibile su http://powerlink.emc.com
Errore: I pool di storage non riportano i dischi sul Service Processor all'indirizzo IP configurato	Configurare il data collector con entrambi gli IP del Service Processor, separati da una virgola
Errore: Errore di mancata corrispondenza della revisione	• Questo problema è dovuto in genere all'aggiornamento del firmware sul dispositivo di storage a blocchi VNX, ma non all'aggiornamento dell'installazione di navicli.exe. Questo potrebbe essere causato anche dalla presenza di dispositivi diversi con firmware diversi, ma solo una CLI installata (con una versione firmware diversa). • Verificare che il dispositivo e l'host eseguano versioni identiche del software: - Dall'unità di acquisizione Cloud Insights, aprire una finestra della riga di comando - modificare la directory nella directory di installazione configurata - stabilire una connessione con il dispositivo CLARiiON digitando "navicli -h{ip} getagent" - cercare il numero di versione sulle prime due righe. Esempio: "Agent Rev: 6.16.2 (0.1)" - cercare e confrontare la versione sulla prima riga. Esempio: "Navisphere CLI Revisione 6.07.00.04.07"
Errore: Configurazione non supportata - Nessuna porta Fibre Channel	Il dispositivo non è configurato con porte Fibre Channel. Attualmente, sono supportate solo le configurazioni FC. Verificare che questa versione/firmware sia supportata.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector DELL EMC VNX file (precedentemente noto come Celerra Unified Storage System)

Questo data collector acquisisce le informazioni di inventario dal file Storage System VNX. Per la configurazione, questo data collector richiede l'indirizzo IP dei processori di storage e un nome utente e una password di sola lettura.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector del file VNX. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Server di rete Celerra/Pool di storage Celerra	Pool di storage

Vendor/modello	Termine Cloud Insights
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

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

Requisiti

Per configurare questo data collector sono necessari i seguenti elementi:

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

Configurazione

Campo	Descrizione
Indirizzo IP del file VNX	Indirizzo IP o nome di dominio completo del file device VNX
Nome utente	Nome utilizzato per accedere al file device VNX
Password	Password utilizzata per accedere al file device VNX

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (minuti)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 20 minuti.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: Impossibile continuare mentre è in corso l'aggiornamento DART	Soluzione possibile: Mettere in pausa il data collector e attendere il completamento dell'aggiornamento DART prima di tentare un'altra richiesta di acquisizione.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione di Dell EMC VNX Unified Data Collector

Per la configurazione, il data collector Dell EMC VNX Unified (SSH) richiede l'indirizzo IP della stazione di controllo e un nome utente e una password di sola lettura.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Disk Folder (cartella disco	Gruppo di dischi
File system	Volume interno
Storage	Storage
Processore per lo storage	Nodo di storage
Pool di storage, gruppo RAID	Pool di storage
LUN	Volume
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

Requisiti

Per configurare il data collector VNX (SSH) sono necessari i seguenti elementi:

- Indirizzo IP VNX e credenziali per la stazione di controllo Celerra.
- Nome utente e password di sola lettura.
- Il data collector è in grado di eseguire comandi navicli/NaviSecCLI sull'array di back-end utilizzando le testine NAS del sistema operativo DART

Configurazione

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

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 40 minuti.
Performance poll Interval (sec).	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector EMC VPLEX

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

> La raccolta delle performance di Cloud Insights dai cluster Vplex richiede che il servizio di archiviazione delle performance sia operativo, al fine di popolare i file .CSV e i log che Cloud Insights recupera tramite copie di file basate su SCP. NetApp ha osservato che molti aggiornamenti delle stazioni di gestione/aggiornamento del firmware Vplex non funzioneranno. I clienti che pianificano tali aggiornamenti potrebbero voler chiedere in maniera proattiva a Dell/EMC se l'upgrade pianificato non consente di utilizzare questa funzionalità e, in caso affermativo, come possono riattivarla per ridurre al minimo le lacune nella visibilità delle performance? Il codice delle performance di cloud Insight valuterà in ogni sondaggio se esistono tutti i file previsti e se vengono aggiornati correttamente; se mancano o sono obsoleti, Cloud Insights registrerà gli errori di raccolta delle performance.

Terminologia

Cloud Insightst acquisisce le seguenti informazioni di inventario dal data collector VPLEX. 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 Cloud Insights
Cluster	Storage
Motore	Nodo di storage
Dispositivo, estensione del sistema	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

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

data collector.

Requisiti

- Indirizzo IP della console di gestione 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.

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 performance)	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. Il valore predefinito è 443.
Intervallo polling inventario (min)	L'impostazione predefinita è 20 minuti.
Numero di tentativi di connessione	Il valore predefinito è 3.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 600 secondi.
Numero di tentativi	Il valore predefinito è 2.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: Autenticazione dell'utente non riuscita.	Assicurarsi che le credenziali per questa periferica siano corrette.

Performance

Problema:	Prova:
Errore: Le prestazioni VPLEX per la versione inferiore alla 5.3 non sono supportate.	Aggiornare VPLEX alla versione 5.3 o superiore
Errore: Dati non raccolti a sufficienza.	• Controllare la data e l'ora di raccolta nel file di log e modificare di conseguenza l'intervallo di polling • attendere più a lungo
Errore: I file di log perpetui non vengono aggiornati.	Contattare il supporto EMC per consentire l'aggiornamento dei file di log perpetui
Errore: L'intervallo di polling delle prestazioni è troppo grande.	Controllare la data e l'ora di raccolta nel file di registro{logfile} e modificare di conseguenza l'intervallo di polling
Errore: L'indirizzo IP remoto delle prestazioni della console di gestione VPLEX non è configurato.	Modificare l'origine dati per impostare l'indirizzo IP remoto delle prestazioni della console di gestione VPLEX.
Errore: Nessun dato di performance segnalato da Director	• Verificare che i monitor delle performance di sistema funzionino correttamente • contattare il supporto EMC per abilitare l'aggiornamento dei file di log del monitor delle performance di sistema

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Dell EMC XtremeIO

Il data collector EMC XtremIO acquisisce i dati di inventario e performance dal sistema storage EMC XtremIO.

Requisiti

Per configurare il data collector EMC XtremIO (HTTP), è necessario disporre di:

- L'indirizzo host di XtremIO Management Server (XMS)
- Un account con privilegi di amministratore
- Accesso alla porta 443 (HTTPS)

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector EMC XtremIO. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco (SSD)	Disco
Cluster	Storage
Controller	Nodo di storage
Volume	Volume
Mappa LUN	Mappa del volume
Iniziatore FC di destinazione	Maschera di volume

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

Requisiti

- L'indirizzo IP dell'host XtremIO Management Server (XMS)
- Nome utente e password dell'amministratore per XtremIO

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. Il valore predefinito è 443.
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector Fujitsu Eternus

Il data collector Fujitsu Eternus acquisisce i dati di inventario utilizzando l'accesso a livello di amministrazione al sistema storage.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dallo storage Fujitsu Eternus. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Storage	Storage
Thin Pool, Flexible Tier Pool, RAID Group	Pool di storage
Volume standard, Snap Data Volume (SDV), Snap Data Pool Volume (SDPV), Thin Provisioning Volume (TPV), Flexible Tier Volume (FTV), Wide Striping Volume (WSV)	Volume
Adattatore di canale	Controller

Nota: Si tratta solo di mappature terminologiche comuni e potrebbero non rappresentare ogni caso per questo data collectior.

Requisiti

Per configurare questo data collector sono necessari i seguenti 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 (disattivazione di Clienv-show-more-scroll)

Configurazione

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

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	L’impostazione predefinita è 20 minuti.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Errore durante il recupero dei dati" con i messaggi di errore "Error Finding prompt CLI" o "Error Finding prompt at the end of shell results"	Probabile causa: Lo scorrimento delle pagine del sistema di storage è attivato. Soluzione possibile: * Provare a disattivare lo scorrimento delle pagine eseguendo il seguente comando: Set clientv-show-more -scroll disable
"Errore di connessione" con messaggi di errore "Impossibile creare un'istanza di connessione SSH allo storage" o "Impossibile creare un'istanza di connessione a VirtualCenter"	Cause probabili: * Credenziali errate. * Indirizzo IP errato. * Problema di rete. * Lo storage potrebbe essere inattivo o non rispondere. Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Provare a comunicare con lo storage utilizzando il client SSH.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

NetApp Google Compute Data Collector

Questo data collector supporta l'inventario e la raccolta delle performance dalle configurazioni della piattaforma cloud di Google Compute. Questo collector cercherà di scoprire tutte le risorse di calcolo all'interno di tutti i progetti all'interno di un'organizzazione Google. Se si desidera scoprire più organizzazioni Google con Cloud Insights, è necessario implementare un Cloud Insights Collector per organizzazione.

Configurazione

Campo	Descrizione
ID organizzazione	L'ID dell'organizzazione che si desidera scoprire con questo collector. Questo campo è obbligatorio se l'account di servizio è in grado di visualizzare più organizzazioni
Scegliere 'Escludi' o 'Includi' per filtrare i progetti GCP in base agli ID	Se si desidera limitare le risorse dei progetti che vengono introdotte in Cloud Insights.
ID progetto	L'elenco degli ID progetto che si desidera filtrare in entrata o in uscita dal rilevamento, a seconda del valore di "Choose 'Exclude'…." valore. L'elenco predefinito è vuoto
ID client	ID client per la configurazione di Google Cloud Platform
Copia e incolla il contenuto del tuo Google Credential file qui	Copia le tue credenziali Google per l'account Cloud Platform in questo campo

Configurazione avanzata

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

Campo	Descrizione
Scegliere "Escludi" o "Includi" per applicare il filtro delle macchine virtuali in base alle etichette	Consente di specificare se includere o escludere le macchine virtuali in base alle etichette durante la raccolta dei dati. Se si seleziona 'Includi', il campo Label Key non può essere vuoto.
Label Key e valori su cui filtrare le macchine virtuali	Fare clic su **+ Filter Label** (etichetta filtro) per scegliere quali macchine virtuali (e dischi associati) includere/escludere filtrando le chiavi e i valori corrispondenti alle chiavi e ai valori delle etichette sulla macchina virtuale. Label Key (chiave etichetta) è obbligatorio, Label Value (valore etichetta) è facoltativo. Quando il valore Label è vuoto, la VM viene filtrata fino a quando corrisponde alla chiave Label.
Intervallo di polling delle performance (sec)	Il valore predefinito è 1800 secondi

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

HP Enterprise

Data collector per lo storage HP Enterprise Alletra 9000 / Primera

Cloud Insights utilizza il data collector HP Enterprise Alletra 9000 / HP Enterprise Primera (in precedenza 3PAR) per rilevare l'inventario e le performance.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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:

Campo	Descrizione
Disco fisico	Disco
Sistema storage	Storage
Nodo controller	Nodo di storage
Gruppo di provisioning comune	Pool di storage
Volume virtuale	Volume

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

Requisiti

Per configurare questo data colletor sono necessari i seguenti requisiti:

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

Configurazione

Campo	Descrizione
Indirizzo IP dello storage	Indirizzo IP dello storage o nome di dominio completo del cluster StoreServ
Nome utente	Nome utente del server StoreServ
Password	Password utilizzata per il server StoreServ
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. L'impostazione predefinita è 40 minuti.
Connettività SMI-S.	Protocollo utilizzato per connettersi al provider SMI-S.
Eseguire l'override della porta predefinita SMI-S.	Se vuoto, utilizzare la porta predefinita di connettività SMI-S, altrimenti inserire la porta di connessione da utilizzare
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
il comando "showsys" non restituisce alcun risultato.	Eseguire "showsys" e "showversion -a" dalla riga di comando e verificare se la versione è supportata dall'array.

Performance

Problema:	Prova:
Connessione o accesso non riusciti. Inizializzazione del provider non riuscita.	Un nome di array completamente numerico può causare problemi con il server SMI-S. Provare a modificare il nome dell'array.
L'utente SMI-S configurato non dispone di alcun dominio	Assegnare i privilegi di dominio appropriati all'utente SMI-S configurato
Cloud Insights afferma che non è possibile connettersi/accedere al servizio SMI-S.	Verificare che non vi sia alcun firewall tra l'AU ci e l'array che impedisce all'AU ci di effettuare connessioni TCP a 5988 o 5989. Una volta fatto questo, e se hai confermato che non c'è alcun firewall, dovresti eseguire l'SSH sull'array e utilizzare il comando "showcim" per confermare. Verificare che: * Il servizio sia abilitato * HTTPS sia abilitato * la porta HTTPS deve essere 5989. In tal caso, provare a "stopcim" e quindi a "startcim" per riavviare il CIM (ad esempio, il servizio SMI-S).

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector HP Enterprise Command View

Il data collector HP Enterprise Command View Advanced Edition supporta il rilevamento degli array XP e P9500 tramite il server Command View Advanced Edition (CVAE). Cloud Insights comunica con CVAE utilizzando l'API Command View standard per raccogliere dati di inventario e performance.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector HP Enterprise Command View. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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

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 del server CVAE
- Nome utente e password di sola lettura per il software CVAE e privilegi peer
- Requisiti delle porte: 2001

Requisiti relativi alle performance

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

- 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 nell'AU di Cloud Insights ed estratto in una posizione. Su ci Linux aus, assicurarsi che "cisys" disponga dei permessi di lettura ed esecuzione.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell'array di destinazione.
- Performance AMS:
  - Performance Monitor deve essere concesso in licenza.
  - L'utility CLI Storage Navigator Modular 2 (SNM2) deve essere installata sull'AU Cloud Insights.
- Requisiti di rete
  - Gli strumenti di esportazione sono basati su Java e utilizzano RMI per comunicare con l'array. Questi strumenti potrebbero non essere compatibili con il firewall, in quanto potrebbero negoziare dinamicamente le porte TCP di origine e di destinazione su ogni chiamata. Inoltre, gli strumenti di esportazione di diversi array di modelli possono comportarsi in modo diverso in tutta la rete. Consulta HPE per conoscere i requisiti del tuo modello

Configurazione

Campo	Descrizione
Server Command View	Indirizzo IP o nome di dominio completo del server Command View
Nome utente	Nome utente del server Command View.
Password	Password utilizzata per il server Command View.
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 * Nome utente: Nome utente dello storage * Password: Password dello storage * cartella contenente file JAR dell'utility di esportazione
SNM2Devices - Storage WMS/SMS/AMS	Elenco dei dispositivi per gli storage WMS/SMS/AMS. Ogni storage richiede: * IP dell'array: Indirizzo IP dello storage * Storage Navigator CLI Path: SNM2 CLI path * account Authentication Valid: Select to Choose Valid account Authentication * User Name: User name for the storage * Password: Password for the storage
Scegli Tuning Manager per le performance	Eseguire l'override di altre opzioni di performance

Campo	Descrizione
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

Nota: 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 Command View	Porta utilizzata per Command View Server
HTTPS attivato	Selezionare per attivare HTTPS
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.
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
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. Il valore predefinito è 300.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: L'utente non dispone di autorizzazioni sufficienti	Utilizzare un account utente diverso con più privilegi o aumentare il privilegio dell'account utente configurato nel data collector
Errore: L'elenco di storage è vuoto. I dispositivi non sono configurati o l'utente non dispone di autorizzazioni sufficienti	* Utilizzare DeviceManager per verificare se i dispositivi sono configurati. * Utilizzare un account utente diverso con più privilegi o aumentare il privilegio dell'account utente
Errore: L'array di storage HDS non è stato aggiornato per alcuni giorni	Esaminare il motivo per cui questo array non viene aggiornato in HP CommandView AE.

Performance

Problema:	Prova:
Errore: * Errore durante l'esecuzione dell'utility di esportazione * errore durante l'esecuzione di un comando esterno	* Verificare che l'utility di esportazione sia installata sull'unità di acquisizione Cloud Insights * verificare che la posizione dell'utility di esportazione sia corretta nella configurazione del data collector * verificare che l'IP dell'array USP/R600 sia corretto nella configurazione del data collector * confermare che il nome utente sia corretto E la password sono corrette nella configurazione del data collector * verificare che la versione dell'utility di esportazione sia compatibile con la versione del microcodice dello storage array * dall'unità di acquisizione Cloud Insights, aprire un prompt CMD ed eseguire le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - provare a stabilire una connessione con lo storage array configurato eseguendo il file batch runWin.bat
Errore: Accesso allo strumento di esportazione non riuscito per l'IP di destinazione	* Confermare che nome utente/password sono corretti * creare un ID utente principalmente per questo data collector HDS * verificare che nessun altro data collector sia configurato per acquisire questo array
Errore: Gli strumenti di esportazione hanno registrato "Impossibile ottenere l'intervallo di tempo per il monitoraggio".	* Verificare che il monitoraggio delle performance sia attivato sull'array. * Prova a invocare i tool di esportazione al di fuori di Cloud Insights per confermare che il problema si trova al di fuori di Cloud Insights.
Errore: * Errore di configurazione: Storage Array non supportato da Export Utility * errore di configurazione: Storage Array non supportato da Storage Navigator Modular CLI	* Configurare solo gli array di storage supportati. * Utilizzare l'opzione "Filter Device List" (Filtra elenco dispositivi) per escludere gli array di storage non supportati.
Errore: * Errore durante l'esecuzione del comando esterno * errore di configurazione: Storage Array non segnalato dall'inventario * errore di configurazione: La cartella di esportazione non contiene file jar	* Controllare la posizione dell'utility di esportazione. * Controllare se l'array di storage in questione è configurato nel server Command View * impostare l'intervallo di polling delle prestazioni su più di 60 secondi.

Problema:	Prova:
Errore: * Errore CLI di Storage Navigator * errore durante l'esecuzione del comando auPerform * errore durante l'esecuzione del comando esterno	* Verificare che l'interfaccia CLI modulare di Storage Navigator sia installata sull'unità di acquisizione Cloud Insights * verificare che la posizione dell'interfaccia CLI modulare di Storage Navigator sia corretta nella configurazione di data collector * verificare che l'indirizzo IP dell'array WMS/SMS/SMS sia corretto nella configurazione di data collector * confermare La versione dell'interfaccia CLI modulare di Storage Navigator è compatibile con la versione del microcodice dello storage array configurato nel data collector * dall'unità di acquisizione Cloud Insights, aprire un prompt CMD ed eseguire le seguenti operazioni: - Modificare la directory nella directory di installazione configurata - provare a stabilire una connessione con lo storage array configurato eseguendo il comando "auunitref.exe"
Errore: Errore di configurazione: Storage Array non segnalato dall'inventario	Controllare se lo Storage Array in questione è configurato nel server Command View
Errore: * Nessun array registrato con la CLI modulare 2 di Storage Navigator * l'array non è registrato con la CLI modulare 2 di Storage Navigator * errore di configurazione: Storage Array non registrato con la CLI modulare di StorageNavigator	* Aprire il prompt dei comandi e modificare la directory nel percorso configurato * eseguire il comando "set=STONAVM_HOME=". * Eseguire il comando "auunitref" * verificare che l'output del comando contenga i dettagli dell'array con IP * se l'output non contiene i dettagli dell'array, registrare l'array con la CLI di Storage Navigator: - Aprire il prompt dei comandi e modificare la directory nel percorso configurato - eseguire il comando "set=STONAVM_HOME=". - Eseguire il comando "auunitaddauto -ip{ip}". Sostituire{ip} con un IP reale

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector HPE Alletra 6000

Il data collector HP Enterprise Alletra 6000 (precedentemente agile) supporta i dati di inventario e performance per gli array di storage Alletra 6000.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da questo collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Array	Storage
Disco	Disco
Volume	Volume
Piscina	Pool di storage

Vendor/modello	Termine Cloud Insights
Iniziatore	Alias host storage
Controller	Nodo di storage
Interfaccia Fibre Channel	Controller

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

Requisiti

Per raccogliere i dati di inventario e configurazione dall'array di storage, è necessario disporre di quanto segue:

- 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 con un ruolo di almeno livello "operatore". Il ruolo "Guest" non dispone di un accesso sufficiente per comprendere le configurazioni dell'iniziatore.
- La porta 5392 deve essere aperta sull'array.

Per raccogliere i dati sulle prestazioni dall'array di storage, è necessario disporre di quanto segue:

- L'array deve eseguire NimbleOS 4.0.0 o versione successiva
- L'array deve avere volumi configurati. L'unica API di performance di NimbleOS è per i volumi e qualsiasi report Cloud Insights di statistiche deriva dalle statistiche sui volumi

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
Password	Password per l'array

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. L'impostazione predefinita è 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 HPE Alletra 6000.

Hitachi Data Systems

Data collector Hitachi Vantara Command Suite

Il data collector Hitachi Vantara Command Suite supporta il server HiCommand Device Manager. Cloud Insights comunica con il server di gestione dispositivi HiCommand utilizzando l'API HiCommand standard.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector della suite di comandi Hitachi Vantara. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
PDEV	Disco
Pool di giornale	Gruppo di dischi
Array di storage	Storage
Port Controller (Controller porta)	Nodo di storage
Gruppo di array, HDS Pool	Pool di storage
Unità logica, LDEV	Volume

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

Storage

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 (Nome) – 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

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 (Gruppo RAID): È probabile che non si vedano questi dati per alcuni motivi:

    Cloud Insights 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 Cloud Insights riportasse i gruppi RAID sottostanti così come i pool, la somma della loro capacità raw supererebbe enormemente la somma dei dischi.

  Al contrario, il data collector della suite di comandi HDS di Cloud Insights riduce arbitrariamente le dimensioni dei gruppi RAID in base alla capacità dei volumi del pool. Ciò potrebbe causare la mancata segnalazione del gruppo RAID da parte di Cloud Insights. Inoltre, tutti i gruppi RAID risultanti vengono contrassegnati in modo che non siano visibili nell'interfaccia Web di Cloud Insights, ma fluiscano nel data warehouse di Cloud Insights (DWH). Lo scopo di queste decisioni è quello di evitare il disordine dell'interfaccia utente per le cose che la maggior parte degli utenti non ha a cuore: Se l'array HDS dispone di gruppi RAID con 50 MB di spazio libero, probabilmente non sarà possibile utilizzare tale spazio libero per ottenere risultati significativi.

- 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 di storage

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

Requisiti di inventario

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

- 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)
- Accedere al software HiCommand Device Manager utilizzando il nome utente e la password

- Verificare l'accesso a HiCommand Device Manager http://<HiCommand_Device_Manager_IP>:2001/service/StorageManager

Requisiti relativi alle performance

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

- 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 nell'AU di Cloud Insights.
  - La versione dello strumento di esportazione deve corrispondere alla versione del microcodice dell'array di destinazione.
- Performance AMS:
  - NetApp consiglia vivamente di creare un account di servizio dedicato sugli array AMS per Cloud Insights da utilizzare per recuperare i dati delle performance. Storage Navigator consente a un account utente di accedere contemporaneamente all'array. Se Cloud Insights utilizza lo stesso account utente degli script di gestione o HiCommand, Cloud Insights, gli script di gestione o HiCommand potrebbero non comunicare con l'array a causa del limite di accesso di un account utente simultaneo
  - Performance Monitor deve essere concesso in licenza.
  - L'utility CLI Storage Navigator Modular 2 (SNM2) deve essere installata sull'AU Cloud Insights.

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 * Nome utente: Nome utente dello storage * Password: Password dello storage * cartella contenente file JAR dell'utility di esportazione
SNM2Devices - Storage WMS/SMS/AMS	Elenco dei dispositivi per gli storage WMS/SMS/AMS. Ogni storage richiede: * IP dell'array: Indirizzo IP dello storage * Storage Navigator CLI Path: SNM2 CLI path * account Authentication Valid: Select to Choose Valid account Authentication * User Name: User name for the storage * Password: Password for the storage
Scegli Tuning Manager per le performance	Eseguire l'override di altre opzioni di performance
Tuning Manager host	Indirizzo IP o nome di dominio completo del tuning manager

Campo	Descrizione
Eseguire l’override della porta di Tuning Manager	Se vuoto, utilizzare la porta predefinita nel campo Choose Tuning Manager for Performance (scegliere Tuning Manager per le prestazioni), altrimenti inserire la porta da utilizzare
Nome utente Tuning Manager	Nome utente di Tuning Manager
Password Tuning Manager	Password per Tuning Manager

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

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Porta del server HiCommand	Porta utilizzata per HiCommand Device Manager
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.
Timeout di esportazione in secondi	Timeout utility di esportazione. Il valore predefinito è 300.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: L’utente non dispone di autorizzazioni sufficienti	Utilizzare un account utente diverso con più privilegi o aumentare il privilegio dell’account utente configurato nel data collector
Errore: L’elenco di storage è vuoto. I dispositivi non sono configurati o l’utente non dispone di autorizzazioni sufficienti	* Utilizzare DeviceManager per verificare se i dispositivi sono configurati. * Utilizzare un account utente diverso con più privilegi o aumentare il privilegio dell’account utente
Errore: L’array di storage HDS non è stato aggiornato per alcuni giorni	Esaminare il motivo per cui questo array non viene aggiornato in HDS HiCommand.

Performance

Problema:	Prova:
Errore: * Errore durante l'esecuzione dell'utility di esportazione * errore durante l'esecuzione di un comando esterno	* Verificare che l'utility di esportazione sia installata sull'unità di acquisizione Cloud Insights * verificare che la posizione dell'utility di esportazione sia corretta nella configurazione del data collector * verificare che l'IP dell'array USP/R600 sia corretto nella configurazione del data collector * confermare che il nome utente sia corretto E la password sono corrette nella configurazione del data collector * verificare che la versione dell'utility di esportazione sia compatibile con la versione del microcodice dello storage array * dall'unità di acquisizione Cloud Insights, aprire un prompt CMD ed eseguire le seguenti operazioni: - Cambiare la directory nella directory di installazione configurata - provare a stabilire una connessione con lo storage array configurato eseguendo il file batch runWin.bat
Errore: Accesso allo strumento di esportazione non riuscito per l'IP di destinazione	* Confermare che nome utente/password sono corretti * creare un ID utente principalmente per questo data collector HDS * verificare che nessun altro data collector sia configurato per acquisire questo array
Errore: Gli strumenti di esportazione hanno registrato "Impossibile ottenere l'intervallo di tempo per il monitoraggio".	* Verificare che il monitoraggio delle performance sia attivato sull'array. * Prova a invocare i tool di esportazione al di fuori di Cloud Insights per confermare che il problema si trova al di fuori di Cloud Insights.
Errore: * Errore di configurazione: Storage Array non supportato da Export Utility * errore di configurazione: Storage Array non supportato da Storage Navigator Modular CLI	* Configurare solo gli array di storage supportati. * Utilizzare l'opzione "Filter Device List" (Filtra elenco dispositivi) per escludere gli array di storage non supportati.
Errore: * Errore durante l'esecuzione del comando esterno * errore di configurazione: Storage Array non segnalato dall'inventario * errore di configurazione: La cartella di esportazione non contiene file jar	* Controllare la posizione dell'utility di esportazione. * Controllare se lo storage array in questione è configurato nel server HiCommand * impostare l'intervallo di polling delle prestazioni su più di 60 secondi.

Problema:	Prova:
Errore: * Errore CLI di Storage Navigator * errore durante l'esecuzione del comando auPerform * errore durante l'esecuzione del comando esterno	* Verificare che l'interfaccia CLI modulare di Storage Navigator sia installata sull'unità di acquisizione Cloud Insights * verificare che la posizione dell'interfaccia CLI modulare di Storage Navigator sia corretta nella configurazione di data collector * verificare che l'indirizzo IP dell'array WMS/SMS/SMS sia corretto nella configurazione di data collector * confermare La versione dell'interfaccia CLI modulare di Storage Navigator è compatibile con la versione del microcodice dello storage array configurato nel data collector * dall'unità di acquisizione Cloud Insights, aprire un prompt CMD ed eseguire le seguenti operazioni: - Modificare la directory nella directory di installazione configurata - provare a stabilire una connessione con lo storage array configurato eseguendo il comando "auunitref.exe"
Errore: Errore di configurazione: Storage Array non segnalato dall'inventario	Controllare se lo Storage Array in questione è configurato nel server HiCommand
Errore: * Nessun array registrato con la CLI modulare 2 di Storage Navigator * l'array non è registrato con la CLI modulare 2 di Storage Navigator * errore di configurazione: Storage Array non registrato con la CLI modulare di StorageNavigator	* Aprire il prompt dei comandi e modificare la directory nel percorso configurato * eseguire il comando "set=STONAVM_HOME=". * Eseguire il comando "auunitref" * verificare che l'output del comando contenga i dettagli dell'array con IP * se l'output non contiene i dettagli dell'array, registrare l'array con la CLI di Storage Navigator: - Aprire il prompt dei comandi e modificare la directory nel percorso configurato - eseguire il comando "set=STONAVM_HOME=". - Eseguire il comando "auunitaddauto -ip{ip}". Sostituire{ip} con un IP reale

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector Hitachi Vantara NAS

Hitachi Vantara NAS data collector è un data collector per l'inventario e la configurazione che supporta il rilevamento di cluster NAS HDS. Cloud Insights supporta il rilevamento di condivisioni NFS e CIFS, file system (volumi interni) e span (pool di storage).

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector HNAS. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Tier	Gruppo di dischi
Cluster	Storage

Vendor/modello	Termine Cloud Insights
Nodo	Nodo di storage
Intervallo	Pool di storage
Disco di sistema	LUN. Back-end
File System	Volume interno

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

Requisiti

- 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.

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. L'impostazione predefinita è 30 minuti.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Error connecting" (errore di connessione) con il messaggio di errore "Error setup shell channel:"or "Error opening shell channel" (errore durante la configurazione del canale della shell	Probabilmente causato da problemi di connettività di rete o SSH non configurato correttamente. Confermare la connessione con un client SSH alternativo
"Timeout" o "errore durante il recupero dei dati" con il messaggio di errore "comando: XXX scaduto."	* Provare il comando con un client SSH alternativo * aumentare il timeout

Problema:	Prova:
"Errore di connessione " o "credenziali di accesso non valide" con messaggi di errore "Impossibile comunicare con la periferica:"	* Controllare l'indirizzo IP * controllare nome utente e password * confermare la connessione con un client SSH alternativo

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

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

Cloud Insights acquisisce le seguenti informazioni di inventario da questo data collector. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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:

Il modulo "Analyzer" di HDS Ops Center deve essere installato 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.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Infinidat InfiniBox

Il data collector Infinidat InfiniBox (HTTP) viene utilizzato per raccogliere le informazioni di inventario dal sistema storage Infinidat InfiniBox.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector Infinidat InfiniBox. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Pool di storage	Pool di storage

Vendor/modello	Termine Cloud Insights
Nodo	Controller
Filesystem	Volume interno
Filesystem	Condivisione file
Esportazioni di file system	Condividere

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questo data collector.

- Indirizzo IP o FQDN del nodo di gestione InfiniBox
- Admin userid e password
- Porta 443 tramite API REST

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. Il valore predefinito è 443.
Intervallo polling inventario	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector di Huawei OceanStor

Cloud Insights utilizza il data collector REST/HTTPS (Huawei OceanStor) per rilevare l'inventario e le performance dello storage di Huawei OceanStor e OceanStor Dorado.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario e performance da Huawei OceanStor. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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
Destinazione del collegamento iSCSI	Nodo di destinazione iSCSI
ISCSI link Initiator	Nodo iniziatore iSCSI
Disco	Disco
LUN	Volume

Requisiti

Per configurare questo data collector sono necessari i seguenti requisiti:

- Indirizzo 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. Il valore predefinito è 8088.
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (sec).	L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data

Collector".

IBM

Data collector IBM Cleversafe

Cloud Insights utilizza questo data collector per rilevare i dati relativi all'inventario e alle performance dei sistemi storage IBM Cleversafe.

> IBM Cleversafe viene misurato a un tasso diverso da TB raw a unità gestite. Ogni 40 TB di capacità IBM Cleversafe non formattata viene addebitato come 1 "Unità gestita (MU)".

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector IBM Cleversafe. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Pool di storage	Pool di storage
Container	Volume interno
Container	Condivisione file
Condivisione NFS	Condividere

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

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password dell'amministratore
- Porta 9440

Configurazione

Campo	Descrizione
IP del gestore o nome host	Indirizzo IP o nome host del nodo di gestione
Nome utente	Nome utente dell'account utente con ruolo di super utente o amministratore di sistema
Password	Password per l'account utente con ruolo di super utente o amministratore di sistema

Configurazione avanzata

Campo	Descrizione
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario.
Timeout connessione HTTP (sec)	Timeout HTTP in secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector IBM CS

Cloud Insights utilizza questo data collector per rilevare i dati relativi all'inventario e alle performance dei sistemi storage IBM CS.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector IBM CS. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Pool di storage	Pool di storage
Container	Volume interno
Container	Condivisione file
Condivisione NFS	Condividere

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

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password dell'amministratore
- Porta 9440

Configurazione

Campo	Descrizione
Indirizzo IP esterno PRISM	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account Admin
Password	Password per l'account Admin

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione all'array IBM CS. Il valore predefinito è 9440.
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

IBM System Storage serie DS8000 Data Collector

Il data collector IBM DS (CLI) supporta l'acquisizione di dati relativi a inventario e performance per i dispositivi DS6xxx e DS8xxx.

I dispositivi DS3xxx, DS4xxx e DS5xxx sono supportati da "Data collector NetApp e-Series". Fare riferimento alla matrice di supporto Cloud Insights per i modelli e le versioni del firmware supportati.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector IBM DS. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Modulo unità disco	Disco
Immagine di storage	Storage
Pool di estensione	Nodo di storage
Volume a blocchi fisso	Volume
Iniziatore FC host (mappato)	Maschera di volume

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

Requisiti

Per configurare questo data collector sono necessari i seguenti elementi:

- Indirizzo IP di ciascun array DS
- Nome utente e password di sola lettura su ciascun array DS
- Software di terze parti installato su Cloud Insights AU: IBM *dscli*
- Convalida dell'accesso: Eseguire i comandi *dscli* utilizzando 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 del dispositivo DS
Nome utente	Nome utente per la CLI DS
Password	Password per la CLI DS
percorso eseguibile *dscli*	Percorso completo dell'eseguibile *dscli*

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario (min). Il valore predefinito è 40.
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)	Il valore predefinito è 300.
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

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore contenente: CMUC00192E, CMUC00191E o CMUC00190E	* Verificare le credenziali e l'indirizzo IP immessi. * Provare a comunicare con l'array tramite la console di gestione Web https://${ip}:8452/DS8000/Console. Sostituire l'indirizzo{ip} con l'indirizzo IP configurato per il data collector.

Problema:	Prova:
Errore: * Impossibile eseguire il programma * errore durante l'esecuzione del comando	* Dall'unità di acquisizione Cloud Insights aprire un file CMD * aprire il file CLI.CFG nella directory home di CLI e controllare la proprietà JAVA_INSTALL, modificare il valore in modo che corrisponda all'ambiente * visualizzare la versione di Java installata su questa macchina, digitando: "java -version" * Ping l'indirizzo IP del dispositivo di storage IBM specificato nel comando CLI emesso. * Se tutte le operazioni descritte in precedenza funzionavano correttamente, eseguire manualmente un comando CLI

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector IBM PowerVM

Il data collector IBM PowerVM (SSH) viene utilizzato per raccogliere informazioni sulle partizioni virtuali in esecuzione sulle istanze hardware IBM POWER gestite da una console di gestione hardware (HMC).

Terminologia

Cloud Insights acquisisce le informazioni di inventario dalle partizioni virtuali in esecuzione sulle istanze dell'hardware IBM POWER. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine Cloud Insights
hdisk	Disco virtuale
Sistema gestito	Host
Server LPAR, VIO	Macchina virtuale
Gruppo di volumi	Data Store
Volume fisico	LUN

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

Requisiti

Per configurare e utilizzare questo data collector devono essere soddisfatti i seguenti requisiti:

- Indirizzo IP della console di gestione hardware (HMC)
- Nome utente e password che consentono di accedere a hardware Management Console (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 IP della console di gestione hardware (HMC)	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. L'impostazione predefinita è 20 minuti.
Porta SSH	Porta utilizzata per SSH su PowerVM
Password	Password utilizzata per la console di gestione hardware
Numero di tentativi	Numero di tentativi di inventario
Escludi dispositivi	Elenco separato da virgole degli ID dei dispositivi o dei nomi visualizzati da escludere

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Configurazione di IBM SAN Volume Controller Data Collector

Il data collector IBM SAN Volume Controller (SVC) raccoglie i 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. Fare riferimento alla matrice di supporto Cloud Insights per i modelli e le versioni firmware supportati.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector IBM SVC. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco	Disco
Cluster	Storage
Nodo	Nodo di storage
Gruppo Mdisk	Pool di storage
Disco virtuale	Volume
Mdisk	LUN e percorsi back-end

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

Requisiti di inventario

- Indirizzo IP di ciascun cluster SVC
- Porta 22 disponibile
- Nome utente e password di sola lettura

Requisiti relativi alle performance

- SVC Console, obbligatoria per qualsiasi cluster SVC e richiesta per il pacchetto di base Discovery SVC.
- Le credenziali richiedono un livello di accesso amministrativo solo per copiare i file delle prestazioni dai nodi del cluster al nodo di configurazione.
- Abilitare la raccolta dati connettendosi al cluster SVC tramite SSH ed eseguendo: *Svctask startstats -interval 1*

  Nota: In alternativa, abilitare la raccolta dati utilizzando l’interfaccia utente di gestione SVC.

Configurazione

Campo	Descrizione
Indirizzi IP del cluster	Indirizzi IP o nomi di dominio pienamente qualificati dello storage SVC
Nome utente inventario	Nome utente per la CLI SVC
Password inventario	Password per la CLI SVC

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 40 minuti.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.
Per ripulire i file stats scaricati	Selezionare questa casella di controllo per eliminare i file di statistiche scaricati

Risoluzione dei problemi

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

Problema:	Prova:
Errore: "Impossibile avviare il comando perché non è stato eseguito sul nodo di configurazione."	Il comando deve essere eseguito sul nodo di configurazione.

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

Problema:	Prova:
Errore: "Impossibile avviare il comando perché non è stato eseguito sul nodo di configurazione."	Il comando deve essere eseguito sul nodo di configurazione.

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector IBM XIV/A9000

Il data collector IBM XIV e A9000 (CLI) utilizza l'interfaccia della riga di comando XIV per raccogliere i dati di inventario, mentre la raccolta delle performance viene eseguita effettuando chiamate SMI-S all'array XIV/A9000, che esegue un provider SMI-S sulla porta 7778.

Terminologia

Vendor/modello	Termine Cloud Insights
Disco	Disco
Sistema storage	Storage
Pool di storage	Pool di storage
Volume	Volume

Requisiti

Per configurare e utilizzare questo data collector devono essere soddisfatti i seguenti requisiti:

- Requisiti della porta: Porta TCP 7778
- Nome utente e password di sola lettura

- XIV CLI deve essere installato sull'AU

Requisiti relativi alle performance

Di seguito sono riportati i requisiti per la raccolta delle performance:

- Agente SMI-S 1.4 o superiore
- CIMService compatibile con SMI-S in esecuzione su array. La maggior parte degli array XIV dispone di un CIMServer installato per impostazione predefinita.
- È necessario fornire l'accesso utente per CIMServer. L'accesso deve avere accesso completo in lettura alla configurazione e alle proprietà dell'array.
- Spazio dei nomi SMI-S. Il valore predefinito è root/ibm. È configurabile in CIMServer.
- Requisiti delle porte: 5988 per HTTP, 5989 per HTTPS.
- Fare riferimento al seguente link per informazioni su come creare un account per la raccolta di performance SMI-S: http://publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp?topic=%2Fcom.ibm.tpc_V41.doc%2Ffqz0_t_adding_cim_agent.html

Configurazione

Campo	Descrizione
XIV indirizzo IP	Indirizzo IP o nome di dominio completo dello storage XIV
Nome utente	Nome utente dello storage XIV
Password	Password per lo storage XIV
Percorso completo alla directory CLI XIV	Percorso completo della cartella contenente la CLI XIV
Indirizzo IP host SMI-S.	Indirizzo IP dell'host SMI-S.

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 40 minuti.
Protocollo SMI-S.	Protocollo utilizzato per connettersi al provider SMI-S. Visualizza anche la porta predefinita.
Eseguire l'override della porta SMI-S.	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
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 performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector Lenovo

Cloud Insights utilizza il data collector Lenovo per rilevare i dati relativi all'inventario e alle performance dei sistemi storage Lenovo HX.

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

Requisiti

- Indirizzo IP esterno PRISM
- Nome utente e password dell'amministratore
- Requisiti della porta TCP: 9440

Configurazione

Campo	Descrizione
Indirizzo IP esterno PRISM	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account Admin
Password	Password per l'account Admin

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione all'array. Il valore predefinito è 9440.
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Microsoft

Configurazione del data collector Azure NetApp Files

Cloud Insights utilizza il data collector Azure NetApp Files per acquisire dati di inventario e performance.

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni.

- Requisito porta: 443 HTTPS
- IP REST di Azure Management (management.azure.com)
- ID client principale del servizio Azure (account utente)
- Chiave di autenticazione principale del servizio Azure (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

Inserire i dati nei campi di raccolta dati in base alla tabella riportata di seguito:

Campo	Descrizione
ID client principale del servizio Azure	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

Risoluzione dei problemi

- Le credenziali utilizzate dal data collector ANF non devono avere accesso a sottoscrizioni Azure che contengono volumi ANF.
- Se l'accesso a Reader causa un errore nella raccolta delle performance, provare a concedere l'accesso del collaboratore a livello di gruppo di risorse.

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector Microsoft Hyper-V.

Il data collector Microsoft Hyper-V acquisisce i dati di inventario e performance dall'ambiente di elaborazione server virtualizzato. Questo data collector è in grado di rilevare un host Hyper-V standalone o un intero cluster, creando un collector per host o

cluster standalone.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario da Microsoft Hyper-V (WMI). Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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

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

Requisiti

Per configurare questo data collector sono necessari i seguenti requisiti:

- Hyper-V richiede l'apertura della porta 5985 per la raccolta dei dati e l'accesso/gestione remota.
- Indirizzo IP o FQDN del cluster o dell'hypervisor standalone. L'utilizzo del nome host o dell'IP del cluster mobile è probabilmente l'approccio più affidabile rispetto al fatto di puntare il collector su un solo nodo specifico di un cluster.
- Account utente di livello amministrativo che funziona su tutti gli hypervisor del cluster.
- WinRM deve essere attivato e in ascolto su tutti gli hypervisor
- Requisiti delle porte: Porta 135 via WMI 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"

> Il data collector Hyper-V richiede un'unità di acquisizione Windows.

Configurazione

Campo	Descrizione
Indirizzo IP del cluster o FQDN del cluster mobile	L'indirizzo IP o il nome di dominio completo per il cluster o un hypervisor standalone non in cluster
Nome utente	Nome utente amministratore dell'hypervisor
Password	Password per l'hypervisor
Suffisso del dominio DNS	Il suffisso del nome host che si combina con il nome host semplice per eseguire il rendering dell'FQDN di un hypervisor

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	L'impostazione predefinita è 20 minuti.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

NetApp

Connessione cloud NetApp per data collector ONTAP 9.9+

Questo data collector crea una connessione cloud per supportare la raccolta di dati dai sistemi CVO, AFF e FAS di ONTAP 9.9+.

> Questo data collector non è più disponibile per l'installazione in Cloud Insights a partire dal 4 aprile 2023 e verrà rimosso da tutte le installazioni di Cloud Insights a luglio 2023. Per informazioni sulla transizione alla raccolta di dati basata su AU, vedere "Knowledge base".

Data collector NetApp Cloud Volumes ONTAP

Questo data collector supporta la raccolta dell'inventario dalle configurazioni Cloud Volumes ONTAP.

Configurazione

Campo	Descrizione
Indirizzo IP di gestione NetApp	Indirizzo IP per Cloud Volumens ONTAP
Nome utente	Nome utente per Cloud Volumes ONTAP
Password	Password per l'utente sopra indicato

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	HTTPS consigliato. Mostra anche la porta predefinita.
Ignora porta di comunicazione	Porta da utilizzare se non predefinita.
Intervallo polling inventario (min)	Il valore predefinito è 60 minuti.
Inventario Conteggio thread simultanei	Numero di thread simultanei.
Forza TLS per HTTPS	Forza TLS su HTTPS
Cerca automaticamente i netgroup	Cerca automaticamente i netgroup
Espansione netgroup	Selezionare Shell o file
Timeout di lettura HTTP in secondi	Il valore predefinito è 30 secondi
Forzare le risposte come UTF-8	Forzare le risposte come UTF-8
Intervallo di polling delle performance (min)	Il valore predefinito è 900 secondi.
Performance Concurrent thread Count	Numero di thread simultanei.
Advanced Counter Data Collection	Selezionare questa opzione per fare in modo che Cloud Insights raccolga le metriche avanzate dall'elenco riportato di seguito.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

NetApp Cloud Volumes Services per data collector AWS

Questo data collector supporta la raccolta dell'inventario da NetApp Cloud Volumes Services per le configurazioni AWS.

Configurazione

Campo	Descrizione
Area volumi cloud	Regione di NetApp Cloud Volumes Services per AWS
Chiave API	Chiave API Cloud Volumes
Chiave segreta	Chiave segreta Cloud Volumes

Configurazione avanzata

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

Risoluzione dei problemi

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

Problema:	Prova:
Si è verificato un errore simile a questo: "Impossibile eseguire la richiesta: Connessione a <AWS region endpoint>:8080 [IP endpoint regione <AWS region endpoint>/AWS>] non riuscita: Timeout connessione: GET https://<AWS Region Endpoint FQDN>:8080/v1/Storage/IPRanges HTTP/1.1'	Il "proxy" Utilizzato da Cloud Insights per comunicare con l'unità di acquisizione, non comunica tra Cloud Insights e il Data Collector stesso. Di seguito sono riportate alcune operazioni da eseguire: Assicurarsi che l'unità di acquisizione sia in grado di risolvere l'fqdn e di raggiungere la porta richiesta. Verificare che non sia necessario un proxy per raggiungere l'endpoint specificato nel messaggio di errore. Il comando curl può essere utilizzato per verificare la comunicazione tra l'unità di acquisizione e l'endpoint. Assicurarsi di utilizzare **non** un proxy per questo test. Esempio: Root@acquisitionunit curl -s -H accept:application/json -H "Content-type: Application/json" -H api-key:<api key used in the data collector credentials -H secret-key:<secret key used in the data collector credentials> -X GET https://<AWS Regional Endpoint>:8080/v1/Storage/IPRanges Vedi questo "Articolo della Knowledge base di NetApp".

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector del software di gestione dei dati NetApp ONTAP

Questo data collector acquisisce i dati di inventario e performance dai sistemi storage che eseguono ONTAP utilizzando chiamate API di sola lettura da un account ONTAP. Questo data collector crea anche un record nel registro dell'applicazione del cluster per accelerare il supporto.

Terminologia

Cloud Insights acquisisce i dati di inventario e performance dal data collector ONTAP. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

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

Terminologia per la gestione dei dati ONTAP

I seguenti termini si applicano agli oggetti o ai riferimenti presenti nelle landing page delle risorse di storage per la gestione dei dati di ONTAP. Molti di questi termini si applicano anche ad altri data collezionisti.

Storage

- Modello – un elenco delimitato da virgole dei nomi dei modelli di nodi univoci e discreti 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 (vendor): Stesso nome del vendor che si potrebbe vedere se si configurava una nuova origine dati.
- Serial Number (numero di serie): Il numero di serie dell'array. Nei sistemi storage con architettura cluster come la gestione dei dati ONTAP, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie dei "nodi di storage".
- IP (IP): Generalmente corrisponde agli IP o ai 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 ruolo.
- Latenza: Una rappresentazione di ciò che stanno sperimentando i carichi di lavoro dell'host, sia in lettura che in scrittura. Idealmente, Cloud Insights sta reperendo questo valore direttamente, ma spesso non è così. Al posto dell'array che offre questa opzione, Cloud Insights esegue in genere un calcolo ponderato per gli IOPS derivato dalle statistiche dei singoli volumi interni.
- Throughput: Aggregato da volumi interni. Gestione – può contenere un collegamento ipertestuale per l'interfaccia di gestione del dispositivo. Creato a livello di programmazione dall'origine dati Cloud Insights come parte del reporting dell'inventario.

Pool di storage

- Storage: Su quale array di storage vive questo pool. Obbligatorio.
- Type (tipo) – un valore descrittivo da un elenco di possibilità enumerate. La maggior parte dei casi sarà "aggregato" 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 ha 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.
- Capacity (capacità): I valori qui riportati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata in tali valori.
- 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: Capacità di snapshot utilizzate e totali, se l'architettura del pool di storage dedica parte della sua capacità a segmentare 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 - 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 favorire l'utilizzo del disco senza essere visualizzate come volume interno o

workload di volume.

- IOPS: La somma degli IOPS di tutti i dischi che contribuiscono alla capacità di questo pool di storage. Throughput (throughput): La somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di storage.

Nodo di storage

- Storage – a quale array di storage fa parte questo nodo. Obbligatorio.
- Partner HA: Nelle piattaforme in cui un nodo eseguirà il failover su un nodo e solo su un altro, questo verrà generalmente visualizzato qui.
- State (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 (versione) – nome della versione del dispositivo.
- Serial number (numero di serie) – il numero di serie del nodo.
- Memory (memoria): Memoria base 2, se disponibile.
- Utilization (utilizzo) – in ONTAP, si tratta di un indice di stress del controller di 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: Un controller/nodo potrebbe non essere abbastanza grande o i dischi rotanti non sono sufficienti 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.

Requisiti

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

- È necessario disporre dell'accesso a un account Administrator configurato per le chiamate API di sola lettura.
- I dettagli dell'account includono nome utente e password.
- Requisiti delle porte: 80 o 443
- Permessi dell'account:
  - Nome del ruolo di sola lettura per l'applicazione ontapi sul Vserver predefinito
  - Potrebbero essere necessarie ulteriori autorizzazioni di scrittura opzionali. Vedere la nota sulle autorizzazioni riportata di seguito.
- Requisiti di licenza per ONTAP:
  - Licenza FCP e volumi mappati/mascherati necessari per il rilevamento Fibre Channel

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
Tipo di connessione	Scegliere HTTP (porta predefinita 80) o HTTPS (porta predefinita 443). L'impostazione predefinita è HTTPS
Ignora porta di comunicazione	Specificare un'altra porta se non si desidera utilizzare l'impostazione predefinita
Intervallo polling inventario (min)	Il valore predefinito è 60 minuti.
Per TLS per HTTPS	Consenti TLS solo come protocollo quando si utilizza HTTPS
Cerca automaticamente i netgroup	Attivare le ricerche automatiche dei netgroup per le regole dei criteri di esportazione
Espansione netgroup	Strategia di espansione dei netgroup. Scegliere *file* o *shell*. L'impostazione predefinita è *shell*.
Timeout di lettura HTTP in secondi	Il valore predefinito è 30
Forzare le risposte come UTF-8	Forza il codice data collector a interpretare le risposte dalla CLI come in UTF-8
Intervallo di polling delle performance (sec)	Il valore predefinito è 900 secondi.
Advanced Counter Data Collection	Abilitare l'integrazione ONTAP. Selezionare questa opzione per includere i dati del contatore avanzato ONTAP nei sondaggi. Scegliere i contatori desiderati dall'elenco.
Metriche switch cluster	Consentire a Cloud Insights di raccogliere i dati degli switch del cluster. Oltre ad attivare questa funzione sul lato Cloud Insights, è necessario configurare anche il sistema ONTAP in modo che fornisca "informazioni sull'interruttore", e verificare che sia corretto permessi Sono impostati, per consentire l'invio dei dati dello switch a Cloud Insights. Vedere "Nota sulle autorizzazioni" di seguito.

Metriche di potenza ONTAP

Diversi modelli ONTAP forniscono metriche di alimentazione per Cloud Insights che possono essere utilizzate per il monitoraggio o gli avvisi. Gli elenchi dei modelli supportati e non supportati riportati di seguito non sono completi, ma devono fornire alcune indicazioni; in generale, se un modello appartiene alla stessa famiglia di un modello presente nell'elenco, il supporto deve essere lo stesso.

Modelli supportati:

R200
R220
R250
R300
R320
R400
R700
A700s
R800
R900
C190
FAS2240-4
FAS2552
FAS2650
FAS2720
FAS2750
FAS8200
FAS8300
FAS8700
FAS9000

Modelli non supportati:

FAS2620
FAS3250
FAS3270
FAS500f
FAS6280
FAS/AFF 8020
FAS/AFF 8040
FAS/AFF 8060
FAS/AFF 8080

Nota sulle autorizzazioni

Poiché alcuni dashboard ONTAP di Cloud Insights si basano su contatori ONTAP avanzati, è necessario attivare **raccolta dati contatore avanzata** nella sezione Configurazione avanzata del data collector.

Assicurarsi inoltre che l'autorizzazione di scrittura per l'API ONTAP sia attivata. In genere, questo richiede un account a livello di cluster con le autorizzazioni necessarie.

Per creare un account locale per Cloud Insights a livello di cluster, accedere a ONTAP con il nome utente/password dell'amministratore della gestione del cluster ed eseguire i seguenti comandi sul server ONTAP:

1. Prima di iniziare, devi aver effettuato l'accesso a ONTAP con un account *Amministratore* e abilitare i comandi a livello di diagnostica_.
2. Creare un ruolo di sola lettura utilizzando i seguenti comandi.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. Creare l'utente di sola lettura utilizzando il seguente comando. Una volta eseguito il comando create, viene richiesto di inserire una password per questo utente.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

Se si utilizza un account ad/LDAP, il comando deve essere

```
 security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
Se si raccolgono dati sugli switch del cluster:
```

```
 security login rest-role create -role ci_readonly -api
/api/network/ethernet -access readonly
Il ruolo e l'accesso utente risultanti saranno simili a quanto segue.
L'output effettivo può variare:
```

```
Role Command/ Access
Vserver Name Directory Query Level
---------- ------------- --------- ------------------ --------
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1::security login> show
Vserver: cluster1
Authentication Acct
UserName    Application   Method      Role Name      Locked
---------   -------      ----------- -------------- --------
ci_user     ontapi      password    ci_readonly   no
```

Se il controllo dell'accesso ONTAP non è impostato correttamente, le chiamate di PAUSA Cloud Insights potrebbero non riuscire, con conseguenti interruzioni nei dati per il dispositivo. Ad esempio, se è stato attivato nel raccoglitore Cloud Insights ma non sono state configurate le autorizzazioni sul ONTAP, l'acquisizione non verrà eseguita correttamente. Inoltre, se il ruolo è precedentemente definito in ONTAP e si aggiungono le capacità dell'API REST, assicurarsi che *http* sia aggiunto al ruolo.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Ricevi una risposta HTTP 401 o un codice di errore ZAPI 13003 e ZAPI restituisce "privilegi insufficienti" o "non autorizzati per questo comando"	Controllare nome utente e password e privilegi/permessi dell'utente.
La versione del cluster è < 8.1	La versione minima supportata del cluster è 8.1. Eseguire l'aggiornamento alla versione minima supportata.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, modificarlo
Errore: "I filer 7 Mode non sono supportati"	Questo può accadere se si utilizza questo data collector per rilevare il filer in modalità 7. Modificare l'IP in modo che punti al cluster cdot.
Il comando ZAPI non riesce dopo il tentativo	Au ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.
L'AU non è riuscito a connettersi a ZAPI tramite HTTP	Controllare se la porta ZAPI accetta testo non crittografato. Se AU tenta di inviare testo non crittografato a un socket SSL, la comunicazione non riesce.
Comunicazione non riuscita con SSLException	AU sta tentando di inviare SSL a una porta di testo normale su un filer. Controllare se la porta ZAPI accetta SSL o utilizza una porta diversa.
Ulteriori errori di connessione: La risposta ZAPI ha il codice di errore 13001, il codice di errore "database non aperto" ZAPI è 60 e la risposta contiene "API non è stata completata in tempo" la risposta ZAPI contiene "initialize_session() ha restituito l'ambiente NULL" il codice di errore ZAPI è 14007 e la risposta contiene "nodo non è integro"	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.

Performance

Problema:	Prova:
Errore "Impossibile raccogliere le prestazioni da ZAPI"	Questo è dovuto in genere al mancato funzionamento di perf stat. Provare il seguente comando su ciascun nodo: > *system node systemshell -node * -command "spmctl -h cmd –stop; spmctl -h cmd –exec"*

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

NetApp Data ONTAP opera in data collector 7-Mode

Per i sistemi storage che utilizzano il software Data ONTAP in 7-Mode, si utilizza il data collector 7-mode, che utilizza l'interfaccia CLI per ottenere dati su capacità e performance.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector NetApp 7-mode. 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:

Questo data collector è "obsoleto".

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

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

Requisiti

Per configurare e utilizzare questo data collector sono necessari i seguenti elementi:

- Indirizzi IP del partner e del controller di storage FAS.
- Porta 443
- 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 sistema storage	Indirizzo IP o nome di dominio completo per il sistema di storage NetApp
Nome utente	Nome utente del sistema storage NetApp
Password	Password per il sistema storage NetApp
Indirizzo del partner ha nel cluster	Indirizzo IP o nome di dominio completo per il partner ha
Nome utente del partner ha nel cluster	Nome utente del partner ha
Password di ha Partner Filer nel cluster	Password per il partner ha

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 20 minuti.
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Sovrascrivere la porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Connessione ai sistemi storage

In alternativa all'utilizzo dell'utente amministrativo predefinito per questo data collector, è possibile configurare un utente con diritti amministrativi direttamente sui sistemi storage NetApp in modo che questo data collector 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 Cloud Insights di eseguire tutti i comandi API dello storage NetApp.

  Questo comando è necessario per utilizzare ZAPI.

- "Login-http-admin": Consente a Cloud Insights di connettersi allo storage NetApp tramite HTTP. Questo comando è necessario per utilizzare ZAPI.
- "Security-api-vfiler": Utilizzare questa opzione per consentire a Cloud Insights 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,_
- login-http-admin,api-*,security-api-vfile,cli-

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Ricevi una risposta HTTP 401 o un codice di errore ZAPI 13003 e ZAPI restituisce "privilegi insufficienti" o "non autorizzati per questo comando"	Controllare nome utente e password e privilegi/permessi dell'utente.
Errore "Impossibile eseguire il comando"	Verificare che l'utente disponga delle seguenti autorizzazioni sul dispositivo: • api-* • cli-date • cli-df • cli-ifconfig • cli-lun • cli-Operations • cli-rdfile • cli-SNAP • login-http-admin • Security-api-vfiler verifica anche se la versione di ONTAP è supportata da Cloud Insights e verifica se le credenziali utilizzate corrispondono alle credenziali del dispositivo

Problema:	Prova:
La versione del cluster è < 8.1	La versione minima supportata del cluster è 8.1. Eseguire l'aggiornamento alla versione minima supportata.
ZAPI restituisce "il ruolo del cluster non è cluster_mgmt LIF"	L'AU deve comunicare con l'IP di gestione del cluster. Controllare l'IP e, se necessario, modificarlo
Errore: "I filer 7 Mode non sono supportati"	Questo può accadere se si utilizza questo data collector per rilevare il filer in modalità 7. Modificare l'IP in modo che punti al filer ccot.
Il comando ZAPI non riesce dopo il tentativo	Au ha problemi di comunicazione con il cluster. Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.
Impossibile connettersi a ZAPI	Controllare la connettività IP/porta e attivare la configurazione ZAPI.
L'AU non è riuscito a connettersi a ZAPI tramite HTTP	Controllare se la porta ZAPI accetta testo non crittografato. Se AU tenta di inviare testo non crittografato a un socket SSL, la comunicazione non riesce.
Comunicazione non riuscita con SSLException	AU sta tentando di inviare SSL a una porta di testo normale su un filer. Controllare se la porta ZAPI accetta SSL o utilizza una porta diversa.
Ulteriori errori di connessione: La risposta ZAPI ha il codice di errore 13001, il codice di errore "database non aperto" ZAPI è 60 e la risposta contiene "API non è stata completata in tempo" la risposta ZAPI contiene "initialize_session() ha restituito l'ambiente NULL" il codice di errore ZAPI è 14007 e la risposta contiene "nodo non è integro"	Controllare la rete, il numero di porta e l'indirizzo IP. L'utente dovrebbe anche provare ad eseguire un comando dalla riga di comando dalla macchina AU.
Errore di timeout socket con ZAPI	Controllare la connettività del filer e/o aumentare il timeout.
"I cluster C Mode non sono supportati dall'origine dati 7 Mode".	Selezionare IP e impostare l'IP su un cluster 7 Mode.
Errore "Impossibile connettersi a vFiler"	Verificare che le funzionalità dell'utente in fase di acquisizione includano almeno quanto segue: api-* Security-api-vfiler login-http-admin verificare che il filer utilizzi almeno ONTAPI versione 1.7.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector NetApp e-Series

Il data collector NetApp e-Series raccoglie dati relativi a inventario e performance. Il collector supporta il firmware 7.x+ utilizzando le stesse configurazioni e riportando gli stessi dati.

Terminologia

Cloud Insight acquisisce le seguenti informazioni di inventario dal data collector NetApp e-Series. 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 Cloud Insights
Disco	Disco
Gruppo di volumi	Gruppo di dischi
Array di storage	Storage
Controller	Nodo di storage
Gruppo di volumi	Pool di storage
Volume	Volume

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

Terminologia e-Series (pagina iniziale)

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

Storage

- Modello – nome del modello del dispositivo.
- Vendor (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 storage con architettura cluster come NetApp Clustered Data ONTAP, questo numero di serie potrebbe essere meno utile dei singoli numeri di serie dei "nodi di storage"
- IP (IP): Generalmente corrisponde agli IP o ai 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 ruolo
- Latenza: Una rappresentazione di ciò che stanno sperimentando i carichi di lavoro dell'host, sia in lettura che in scrittura. Idealmente, Cloud Insights sta reperendo questo valore direttamente, ma spesso non è così. Al posto dell'array che offre questa opzione, Cloud Insights esegue in genere un calcolo ponderato per gli IOPS derivato dalle statistiche dei singoli volumi.
- Throughput: Throughput totale dell'host dell'array. Idealmente generato direttamente dall'array, se non disponibile, Cloud Insights somma il throughput dei volumi per derivare questo valore
- Gestione – può contenere un collegamento ipertestuale per l'interfaccia di gestione del dispositivo. Creato a livello di programmazione dall'origine dati Cloud Insights come parte del reporting dell'inventario

Pool di storage

- Storage: Su quale array di storage vive questo pool. Obbligatorio
- Type (tipo) – un valore descrittivo da un elenco di possibilità enumerate. 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
- Capacity (capacità): I valori qui riportati sono la capacità logica utilizzata, la capacità utilizzabile e la capacità logica totale, nonché la percentuale utilizzata in tali valori. Entrambi questi valori includono la capacità di "conservazione" di e-Series, con il risultato che i numeri e la percentuale sono superiori a quanto potrebbe essere visualizzato dall’interfaccia utente di e-Series
- Capacità con overcommit – se tramite 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: Capacità di snapshot utilizzate e totali, se l’architettura del pool di storage dedica parte della sua capacità a segmentare 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 favorire 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. Se gli IOPS dei dischi non sono disponibili su una determinata piattaforma, questo valore verrà generato dalla somma degli IOPS dei volumi per tutti i volumi presenti in questo pool di storage
- Throughput (throughput): La somma del throughput di tutti i dischi che contribuiscono alla capacità di questo pool di storage. Se il throughput del disco non è disponibile su una determinata piattaforma, questo valore viene generato dalla somma del volume per tutti i volumi presenti in questo pool di storage

Nodo di storage

- Storage – a quale array di storage fa parte questo nodo. Obbligatorio
- Partner HA: Nelle piattaforme in cui un nodo eseguirà il failover su un nodo e solo su un altro, questo verrà generalmente visualizzato qui
- State (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 (versione) – nome della versione del dispositivo.
- Serial number (numero di serie) – il numero di serie del nodo
- Memory (memoria): Memoria base 2, se disponibile
- Utilizzo: Generalmente un numero di utilizzo della CPU o, nel caso di NetApp ONTAP, un indice di stress del controller. L’utilizzo non è attualmente disponibile per NetApp e-Series
- IOPS: Un numero che rappresenta gli IOPS basati su host su questo controller. Idealmente, originata direttamente dall’array, se non disponibile, verrà calcolata 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. Idealmente originata direttamente dall’array, se non disponibile, verrà calcolata eseguendo un calcolo ponderato degli IOPS dai volumi che appartengono esclusivamente a questo nodo.
- Throughput (throughput): Un numero che rappresenta il throughput basato su host su questo controller.

Idealmente originata direttamente dall'array, se non disponibile, verrà calcolata sommando tutto il throughput per i volumi che appartengono esclusivamente a questo nodo.

- Processori: Numero di CPU

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)	Il valore predefinito è 30 minuti
Intervallo di polling delle performance fino a 3600 secondi	Il valore predefinito è 300 secondi

Risoluzione dei problemi

Per ulteriori informazioni su questo data collector, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione del data collector del server di gestione NetApp HCI

Il data collector del server di gestione NetApp HCI raccoglie le informazioni sull'host NetApp HCI e richiede privilegi di sola lettura per tutti gli oggetti all'interno del server di gestione.

Questo data collector acquisisce solo dal server di gestione NetApp HCI*. Per raccogliere i dati dal sistema di storage, è necessario configurare anche "NetApp SolidFire" data collector.

Terminologia

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

Vendor/modello	Termine Cloud Insights
Disco virtuale	Disco
Host	Host
Macchina virtuale	Macchina virtuale
Archivio di dati	Archivio di dati

Vendor/modello	Termine Cloud Insights
LUN	Volume
Porta Fibre Channel	Porta

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Indirizzo IP del server di gestione NetApp HCI
- Nome utente e password di sola lettura per il server di gestione NetApp HCI
- Privilegi di sola lettura su tutti gli oggetti nel server di gestione NetApp HCI.
- Accesso all'SDK sul server di gestione NetApp HCI, normalmente già configurato.
- Requisiti delle porte: http-80 https-443
- Convalidare l'accesso:
  - Accedere al server di gestione NetApp HCI utilizzando il nome utente e la password indicati sopra
  - Verificare che SDK sia abilitato: telnet <vc_ip> 443

Installazione e connessione

Campo	Descrizione
Nome	Nome univoco del data collector
Unità di acquisizione	Nome dell'unità di acquisizione

Configurazione

Campo	Descrizione
Cluster di storage NetApp HCI MVIP	Indirizzo IP virtuale di gestione
Nodo di gestione SolidFire (mNode)	Indirizzo IP del nodo di gestione
Nome utente	Nome utente utilizzato per accedere al server di gestione NetApp HCI
Password	Password utilizzata per accedere al server di gestione NetApp HCI
Nome utente vCenter	Nome utente per vCenter
Password vCenter	Password per vCenter

Configurazione avanzata

Nella schermata Advanced Configuration (Configurazione avanzata), selezionare la casella **VM Performance** (prestazioni macchina virtuale) per raccogliere i dati sulle prestazioni. La raccolta dell'inventario è attivata per impostazione predefinita. È possibile configurare i seguenti campi:

Campo	Descrizione
Intervallo di polling dell'inventario (min)	Il deafult è 20
Filtra le VM in base a.	Selezionare CLUSTER, DATA CENTER o HOST ESX
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Specificare se includere o escludere macchine virtuali
Filtra elenco dispositivi	Elenco delle macchine virtuali da filtrare (separate da virgole o da punto e virgola se nel valore viene utilizzata una virgola) per il filtraggio solo da parte di ESX_HOST, CLUSTER e DATA CENTER
Intervallo di polling delle performance (sec)	Il valore predefinito è 300

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: L'elenco di inclusione per il filtro delle macchine virtuali non può essere vuoto	Se è selezionata l'opzione Includi elenco, elencare i nomi di DataCenter, cluster o host validi per filtrare le macchine virtuali
Errore: Impossibile creare un'istanza di connessione a VirtualCenter su IP	Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Provare a comunicare con Virtual Center utilizzando Infrastructure Client. * Provare a comunicare con Virtual Center utilizzando Managed Object browser (ad esempio MOB).
Errore: VirtualCenter AT IP dispone di un certificato non conforme richiesto da JVM	Possibili soluzioni: * Consigliato: Ricreare il certificato per Virtual Center utilizzando una chiave RSA più potente (ad esempio 1024 bit). * Non consigliato: Modificare la configurazione di JVM java.security per sfruttare il vincolo jdk.certpath.disabledAlgorithms per consentire la chiave RSA a 512 bit. Vedere le note sulla versione di JDK 7 update 40 all’indirizzo "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector per array all-flash NetApp SolidFire

Il data collector per array all-flash NetApp SolidFire supporta la raccolta di inventario e performance da configurazioni SolidFire iSCSI e Fibre Channel.

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

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector degli array all-flash SolidFire di NetApp. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
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

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

Requisiti

Di seguito sono riportati i requisiti per la configurazione di questo data collector:

- Indirizzo IP virtuale di gestione
- Nome utente e credenziali di sola lettura
- 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
Tipo di connessione	Scegliere il tipo di connessione
Porta di comunicazione	Porta utilizzata per le API NetApp
Intervallo polling inventario (min)	Il valore predefinito è 20 minuti
Intervallo di polling delle performance (sec)	Il valore predefinito è 300 secondi

Risoluzione dei problemi

Quando SolidFire segnala un errore, viene visualizzato in Cloud Insights come segue:

È stato ricevuto un messaggio di errore da un dispositivo SolidFire durante il tentativo di recuperare i dati. La chiamata era <method> (<parameterString>). Il messaggio di errore del dispositivo era (consultare il manuale del dispositivo): <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.

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector NetApp StorageGRID

Il data collector NetApp StorageGRID supporta la raccolta di inventario e performance dalle configurazioni StorageGRID.

> Il StorageGRID viene misurato a un tasso diverso da TB raw a unità gestite. Ogni 40 TB di capacità StorageGRID non formattata viene addebitato come 1 "Unità gestita (MU)".

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal NetApp StorageGRID 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 Cloud Insights
StorageGRID	Storage
Nodo	Nodo
Tenant	Pool di storage
Bucket	Volume interno

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	Gestione Indirizzo IP virtuale dell'appliance StorageGRID
Nome utente	Nome utilizzato per accedere all'appliance StorageGRID
Password	Password utilizzata per accedere all'appliance StorageGRID

Configurazione avanzata

Campo	Descrizione
Intervallo polling inventario (min)	Il valore predefinito è 60 minuti
Intervallo di polling delle performance (sec)	Il valore predefinito è 900 secondi

Single Sign-on (SSO)

Il "StorageGRID" Le versioni del firmware hanno le corrispondenti versioni API; 3.0 API e le versioni più recenti supportano l'accesso SSO (Single Sign-on).

Versione del firmware	Versione API	Supporto SSO (Single Sign-on)
11.1	2	No
11.2	3.0	Sì
11.5	3.3	Sì

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector Nutanix NX

Cloud Insights utilizza il data collector Nutanix per rilevare i dati di inventario e performance dei sistemi storage Nutanix NX.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector Nutanix. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Pool di storage	Pool di storage
Contenitore Nutanix	Volume interno
Contenitore Nutanix	Condivisione file

Vendor/modello	Termine Cloud Insights
Condivisione NFS	Condividere

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

Requisiti

- L'indirizzo IP dei servizi dati esterni per il cluster
- Nome utente e password di sola lettura, a meno che non siano in uso gruppi_volumi, nel qual caso sono richiesti nome utente e password amministratore
- Requisito della porta: HTTPS 443

Configurazione

Campo	Descrizione
Indirizzo IP esterno PRISM	L'indirizzo IP dei servizi dati esterni per il cluster
Nome utente	Nome utente per l'account Admin
Password	Password per l'account Admin

Configurazione avanzata

Campo	Descrizione
Porta TCP	Porta TCP utilizzata per la connessione all'array Nutanix. Il valore predefinito è 9440.
Intervallo di polling dell'inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 60 minuti.
Intervallo di polling delle performance (sec)	Intervallo tra i sondaggi delle performance. L'impostazione predefinita è 300 secondi.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Data collector OpenStack

Il data collector OpenStack (REST API / KVM) acquisisce i dati di inventario per tutte le istanze di OpenStack e, facoltativamente, i dati sulle performance delle macchine virtuali.

Requisiti

- Indirizzo IP del controller OpenStack
- Credenziali del ruolo di amministratore di OpenStack e accesso sicuro all'hypervisor KVM Linux. Se non si utilizza l'account admin o privilegi equivalenti, sarà necessario utilizzare la versione di prova e gli errori per identificare le policy predefinite per rendere più semplice l'ID utente del data collector.

- Il modulo OpenStack Gnocchi deve essere installato e configurato per la raccolta delle prestazioni. La configurazione di Gnocchi avviene modificando il file nova.conf per ogni hypervisor e riavviando il servizio Nova Compute su ogni 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 Gnocchi Performance Service
  - 9292 per Glance Image Service **Nota** la porta si collega 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	Nome tenant amministratore OpenStack
Utente KVM sudo	Nome utente di KVM sudo
Scegliere 'Password' o 'OpenSSH Key file' per specificare il tipo di credenziale	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

Campo	Descrizione
Porta URL OpenStack Admin	Porta URL OpenStack Admin
Utilizzare HTTPS	Selezionare per utilizzare HTTP sicuro
Porta SSH	Porta utilizzata per SSH
Tentativi di processo SSH	Numero di tentativi di inventario
Intervallo polling inventario (min)	Intervallo tra i sondaggi di inventario. L'impostazione predefinita è 20 minuti.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Errore di configurazione" con messaggi di errore che iniziano con "la policy non consente" o "non sei autorizzato"	* Controllare l'indirizzo ip * controllare il nome utente e la password

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector di Oracle ZFS Storage Appliance

Cloud Insights utilizza il data collector dell'appliance di storage Oracle ZFS per raccogliere i dati relativi all'inventario e alle performance.

Terminologia

Cloud Insights acquisisce le informazioni di inventario con il data collector Oracle ZFS. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Disco (SSD)	Disco
Cluster	Storage
Controller	Nodo di storage
LUN	Volume
Mappa LUN	Mappa del volume
Iniziatore, destinazione	Maschera di volume
Condividere	Volume interno

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

Requisiti

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

Metriche di performance richieste

Le appliance Oracle ZFS offrono agli amministratori dello storage una grande flessibilità per acquisire le statistiche delle performance. Cloud Insights prevede che *ciascun* controller in una coppia ad alta disponibilità sia configurato per acquisire le seguenti metriche:

- smb2.ops[share]
- nfs3.ops[condividere]
- nfs4.ops[condividere]
- nfs4-1.ops[condividere]

Il mancato rilevamento di una o di tutte queste informazioni da parte del controller potrebbe causare il mancato o la creazione di un report insufficiente del carico di lavoro in Cloud Insights sui "volumi interni".

Configurazione

Campo	Descrizione
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
Tipo di connessione	HTTPS o HTTP, visualizza anche la porta predefinita
Sovrascrivere la porta di connessione	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
Intervallo di polling dell'inventario	L'impostazione predefinita è 60 secondi
Intervallo di polling delle performance (sec)	Il valore predefinito è 300.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Credenziali di accesso non valide"	Convalidare l'account utente e la password ZFS
"Errore di configurazione" con messaggio di errore "Servizio REST disattivato"	Verificare che il servizio REST sia attivato su questo dispositivo.
"Errore di configurazione " con messaggio di errore "utente non autorizzato per 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) a destra. - Fare clic sul pulsante Apply (Applica) nella parte superiore destra della finestra a comparsa. La finestra a comparsa si chiude.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Pure Storage FlashArray data collector

Cloud Insights utilizza il data collector FlashArray per lo storage puro per raccogliere dati relativi a inventario e performance.

Terminologia

Per ogni tipo di risorsa acquisita da Cloud Insights, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

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

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

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
Indirizzo IP host FlashArray	Indirizzo IP del sistema di storage
Nome utente	Nome utente con privilegi di amministratore
Password per l'account con privilegi di amministratore	Password

Configurazione avanzata

Campo	Descrizione
Tipo di connessione	Scegliere HTTP o HTTPS. Visualizza anche la porta predefinita.
Eseguire l'override della porta TCP	Se vuoto, utilizzare la porta predefinita nel campo Connection Type (tipo di connessione), altrimenti inserire la porta di connessione da utilizzare
Intervallo di polling dell'inventario (min)	L'impostazione predefinita è 60 minuti
Intervallo di polling delle performance (sec)	Il valore predefinito è 300

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
"Credenziali di accesso non valide" con messaggi di errore "la policy non consente" o "non sei autorizzato"	Convalidare l'account utente e la password pure tramite l'interfaccia pure http

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Data collector Red Hat Virtualization

Cloud Insights utilizza il data collector per la virtualizzazione Red Hat per raccogliere i dati di inventario dai carichi di lavoro virtualizzati di Linux e Microsoft Windows.

Terminologia

Per ogni tipo di risorsa acquisita da Cloud Insights, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine Cloud Insights
Disco	Disco virtuale
Host	Host
Macchina virtuale	Macchina virtuale
Dominio di storage	Data Store
Unità logica	LUN

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

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 del sistema di storage
Nome utente	Nome utente con privilegi di amministratore
Password per l'account con privilegi di amministratore	Password

Configurazione avanzata

Campo	Descrizione
Porta di comunicazione HTTPS	Porta utilizzata per la comunicazione HTTPS con RHEV
Intervallo di polling dell'inventario (min)	L'impostazione predefinita è 20 minuti.

Risoluzione dei problemi

Per ulteriori informazioni su questo Data Collector, consultare il "Supporto" o in "Matrice di supporto Data Collector".

Rubrik CDM Data Collector

Cloud Insights utilizza il data collector Rubrik per acquisire dati di inventario e performance dalle appliance di storage Rubrik.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector Rubrik. Per ogni tipo di risorsa acquisita da Cloud Insights, 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 Cloud Insights
Cluster	Storage, pool di storage
Nodo	Nodo di storage
Disco	Disco

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

Requisiti

Per configurare questo data collector sono necessari i seguenti requisiti:

- L'unità di acquisizione Cloud Insights avvia le connessioni alla porta TCP 443 al cluster Rubrik. Un collector per cluster.
- Indirizzo IP del cluster Rubrik.
- Nome utente e password del cluster.
- Requisito della porta: HTTPS 443

Configurazione

Campo	Descrizione
IP	Indirizzo IP del cluster Rubrik
Nome utente	Nome utente del cluster
Password	Password per il cluster

Configurazione avanzata

Intervallo di polling dell'inventario (min)	Il valore predefinito è 60
Intervallo di polling delle performance (sec)	Il valore predefinito è 300

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Ho ricevuto un messaggio che indica la creazione di più storage.	Verificare che il cluster sia configurato correttamente e che il raccoglitore faccia riferimento a un singolo cluster.
Ho ricevuto un avviso che indica che l'API del disco ha restituito più dati	Rivolgersi al supporto per ottenere ulteriori dati.

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Configurazione di VMware vSphere data collector

Il data collector per VMware vSphere raccoglie le informazioni dell'host ESX e richiede privilegi di sola lettura per tutti gli oggetti all'interno del Virtual Center.

Terminologia

Cloud Insights acquisisce le seguenti informazioni di inventario dal data collector VMware vSphere. Per ogni tipo di risorsa acquisita, viene visualizzata la terminologia più comune utilizzata per la risorsa. Durante la visualizzazione o la risoluzione dei problemi di questo data collector, tenere presente la seguente terminologia:

Vendor/modello	Termine Cloud Insights
Disco virtuale	Disco
Host	Host
Macchina virtuale	Macchina virtuale
Archivio di dati	Archivio di dati
LUN	Volume
Porta Fibre Channel	Porta

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

Requisiti

Per configurare questo data collector sono necessarie le seguenti informazioni:

- Indirizzo IP del server Virtual Center
- Nome utente e password di sola lettura in Virtual Center
- Sono necessari privilegi di sola lettura per tutti gli oggetti all'interno di Virtual Center.
- Accesso all'SDK sul server Virtual Center, normalmente già configurato.
- Requisiti delle porte: http-80 https-443
- Convalidare l'accesso:
  - Accedere a Virtual Center Client utilizzando il nome utente e la password indicati sopra
  - Verificare che SDK sia abilitato: telnet <vc_ip> 443

Installazione e connessione

Campo	Descrizione
Nome	Nome univoco del data collector
Unità di acquisizione	Nome dell'unità di acquisizione

Configurazione

Campo	Descrizione
Indirizzo IP del centro virtuale	Indirizzo IP del Virtual Center
Nome utente	Nome utente utilizzato per accedere a Virtual Center
Password	Password utilizzata per accedere al Virtual Center

Configurazione avanzata

Nella schermata Advanced Configuration (Configurazione avanzata), selezionare la casella **VM Performance** (prestazioni macchina virtuale) per raccogliere i dati sulle prestazioni. La raccolta dell'inventario è attivata per impostazione predefinita. È possibile configurare i seguenti campi:

Campo	Descrizione
Intervallo di polling dell'inventario (min)	Il valore predefinito è 20
Filtrare le macchine virtuali	Selezionare CLUSTER, DATA CENTER o HOST ESX
Scegliere 'Escludi' o 'Includi' per specificare un elenco	Creare un elenco di filtri (CLUSTER, DATA CENTER e/o ESX_HOST)
Numero di tentativi	Il valore predefinito è 3
Porta di comunicazione	Il valore predefinito è 443
Filtra elenco dispositivi…	Questo elenco deve essere composto da corrispondenze di stringhe esatte. Se si intende filtrare in base a ESX_HOST, è necessario creare un elenco delimitato da virgole dei "nomi" esatti degli host ESX, come riportato in Cloud Insights e vSphere. Questi "nomi" possono essere indirizzi IP, semplici nomi host o FQDN (Fully Qualified Domain Name), in base al modo in cui questi host sono stati nominati al momento dell'aggiunta iniziale a vSphere. Durante il filtraggio in base AL CLUSTER, Utilizzare i nomi dei cluster in stile Cloud Insights come riportato dal ci sugli hypervisor. Cloud Insights precede il nome del cluster vSphere con il nome del datacenter vSphere e una barra in avanti. "DC1/clusterA" è il nome del cluster che Cloud Insights potrebbe riportare su un hypervisor in clusterA all'interno del data center DC1.
Intervallo di polling delle performance (sec)	Il valore predefinito è 300

Associazione dei tag VMware alle annotazioni Cloud Insights

VMware Data Collector consente di popolare le annotazioni Cloud Insights con tag configurati su VMware. Le annotazioni devono essere denominate esattamente come i tag VMware. Cloud Insights compila 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 il data collector non riesce a compilarla, potrebbe essere necessario rimuovere l'annotazione e ricrearla come testo.

Tenere presente che i tag VMware possono fare distinzione tra maiuscole e minuscole, mentre i tag Cloud Insights non fanno distinzione tra maiuscole e minuscole. Quindi, se si crea un'annotazione denominata "PROPRIETARIO" in Cloud Insights e i tag denominati "PROPRIETARIO", "proprietario" e "proprietario" in

VMware, tutte queste variazioni di "proprietario" verranno associate all'annotazione "PROPRIETARIO" di Cloud Insight.

Tenere presente quanto segue:

- Attualmente Cloud Insights pubblica automaticamente solo le informazioni di supporto per i dispositivi NetApp.
- Poiché queste informazioni di supporto sono contenute in forma di annotazione, è possibile eseguirne una query o utilizzarle nei dashboard.
- Se un utente sovrascrive o svuota il valore dell'annotazione, il valore viene riempito automaticamente quando Cloud Insights aggiorna le annotazioni, che viene eseguito una volta al giorno.

Risoluzione dei problemi

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

Inventario

Problema:	Prova:
Errore: L'elenco di inclusione per il filtro delle macchine virtuali non può essere vuoto	Se è selezionata l'opzione Includi elenco, elencare i nomi di DataCenter, cluster o host validi per filtrare le macchine virtuali
Errore: Impossibile creare un'istanza di connessione a VirtualCenter su IP	Possibili soluzioni: * Verificare le credenziali e l'indirizzo IP immessi. * Prova a comunicare con Virtual Center utilizzando VMware Infrastructure Client. * Provare a comunicare con Virtual Center utilizzando Managed Object browser (ad esempio MOB).
Errore: VirtualCenter AT IP dispone di un certificato non conforme richiesto da JVM	Possibili soluzioni: * Consigliato: Ricreare il certificato per Virtual Center utilizzando una chiave RSA più potente (ad esempio 1024 bit). * Non consigliato: Modificare la configurazione di JVM java.security per sfruttare il vincolo jdk.certpath.disabledAlgorithms per consentire la chiave RSA a 512 bit. Vedere le note sulla versione di JDK 7 update 40 all’indirizzo "http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"

Per ulteriori informazioni, consultare "Supporto" o in "Matrice di supporto Data Collector".

Riferimento Data Collector - servizi

Raccolta dati nodo

Cloud Insights raccoglie le metriche dal nodo su cui si installa un agente.

Installazione

1. Da **osservabilità > Collector**, scegliere un sistema operativo/piattaforma. Si noti che l'installazione di qualsiasi data collector di integrazione (Kubernetes, Docker, Apache, ecc.) configurerà anche la raccolta di dati dei nodi.
2. Seguire le istruzioni per configurare l'agente. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

Oggetti e contatori

I seguenti oggetti e i relativi contatori vengono raccolti come metriche del nodo:

Oggetto:	Identificatori:	Attributi:	Punti dati:
File system del nodo	Nodo UUID Device Path Type (tipo percorso dispositivo UUID nodo)	Nodo IP Node Name Node OS Mode	Nodi liberi nodi liberi nodi totali utilizzati totale utilizzato totale utilizzato
Disco del nodo	Disco UUID nodo	Nodo IP Node Name Node OS	Tempo di io totale IOPS in corso byte di lettura (per sec) tempo di lettura totale letture (per sec) tempo di io ponderato totale byte di scrittura (per sec) tempo di scrittura totale scritture (per sec) lunghezza corrente della coda del disco tempo di scrittura tempo di lettura tempo di io
CPU del nodo	CPU UUID nodo	Nodo IP Node Name Node OS	Utilizzo della CPU utilizzo della CPU utente utilizzo della CPU inattivo utilizzo della CPU utilizzo della CPU interruzione utilizzo della CPU utilizzo della CPU DPC utilizzo della CPU

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo	UUID nodo	Nodo IP Node Name Node OS	Tempo di avvio del kernel kernel Opzioni di contesto del kernel (per sec) intropia del kernel disponibile interrupt del kernel (per sec) processi del kernel forcati (per sec) Memoria attiva memoria disponibile memoria totale disponibile memoria con buffer memoria cache limite di impegno memoria allocata come memoria memoria sporca memoria libera memoria libera elevata memoria totale elevata memoria enorme dimensione pagina memoria pagine enormi memoria libera pagine enormi memoria totale bassa memoria libera memoria totale bassa memoria mappata memoria tabelle pagine Memoria Shared Memory Slab Memory Swap cache Memory Swap Free Memory Swap Total Memory memoria totale utilizzata memoria totale utilizzata memoria utilizzata memoria Vmalloc Chunk Memory Vmalloc Total Memory Vmalloc Used Memory Wired Memory Writeback Total Memory Writeback TMP Memory cache FLAUTS Memory Demand Zero FLAUTS Memory Page FLAUTS Memory Memory Memory Memory Memoria NONPAGED memoria paging cache Core memoria Standby cache memoria normale Standby cache riserva memoria errori di transizione processi bloccati processi inattivi processi inattivi processi di paging processi in esecuzione processi in sospensione processi

Oggetto:	Identificatori:	Attributi:	Punti dati:
Rete di nodi	UUID nodo interfaccia di rete	Nome nodo nodo nodo IP nodo SO	Byte ricevuti byte inviati pacchetti Outboud scartati pacchetti Outboud errori pacchetti ricevuti pacchetti scartati ricevuti errori ricevuti pacchetti ricevuti pacchetti inviati

Setup (Configurazione)

Le informazioni relative all'installazione e alla risoluzione dei problemi sono disponibili sul "Configurazione di un agente" pagina.

ActiveMQ Data Collector

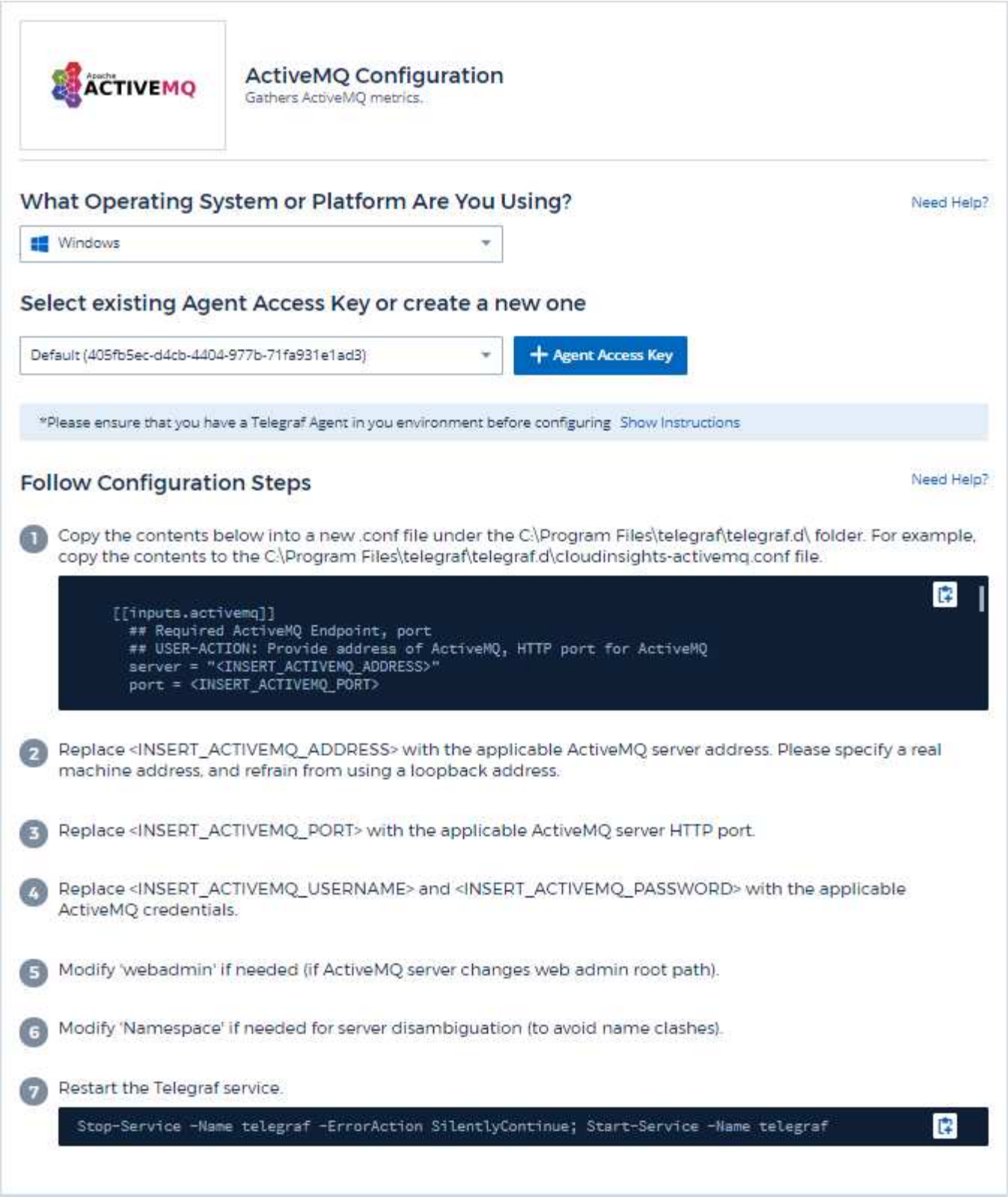
Cloud Insights utilizza questo data collector per raccogliere le metriche da ActiveMQ.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere ActiveMQ.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione ActiveMQ"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Coda ActiveMQ	Namespace Queue Port Server	Node Name Node IP Node UID	Consumer Count Dequeue Count Enqueue Count dimensione coda
Abbonato ActiveMQ	ID client ID Connection ID Port Server namespace	È attivo Node di destinazione Node Node IP Node UID Node OS Selector Subscription	Numero di dequeue numero di invii dimensione coda spedita Conteggio coda in attesa dimensione coda
Argomento ActiveMQ	Argomento namespace Port Server	Node Name Node IP Node UID Node OS	Dimensioni Conteggio incoditi Conteggio incoditi Conte clienti

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Apache Data Collector

Questo data collector consente la raccolta di dati dai server Apache nel tuo ambiente.

Prerequisiti

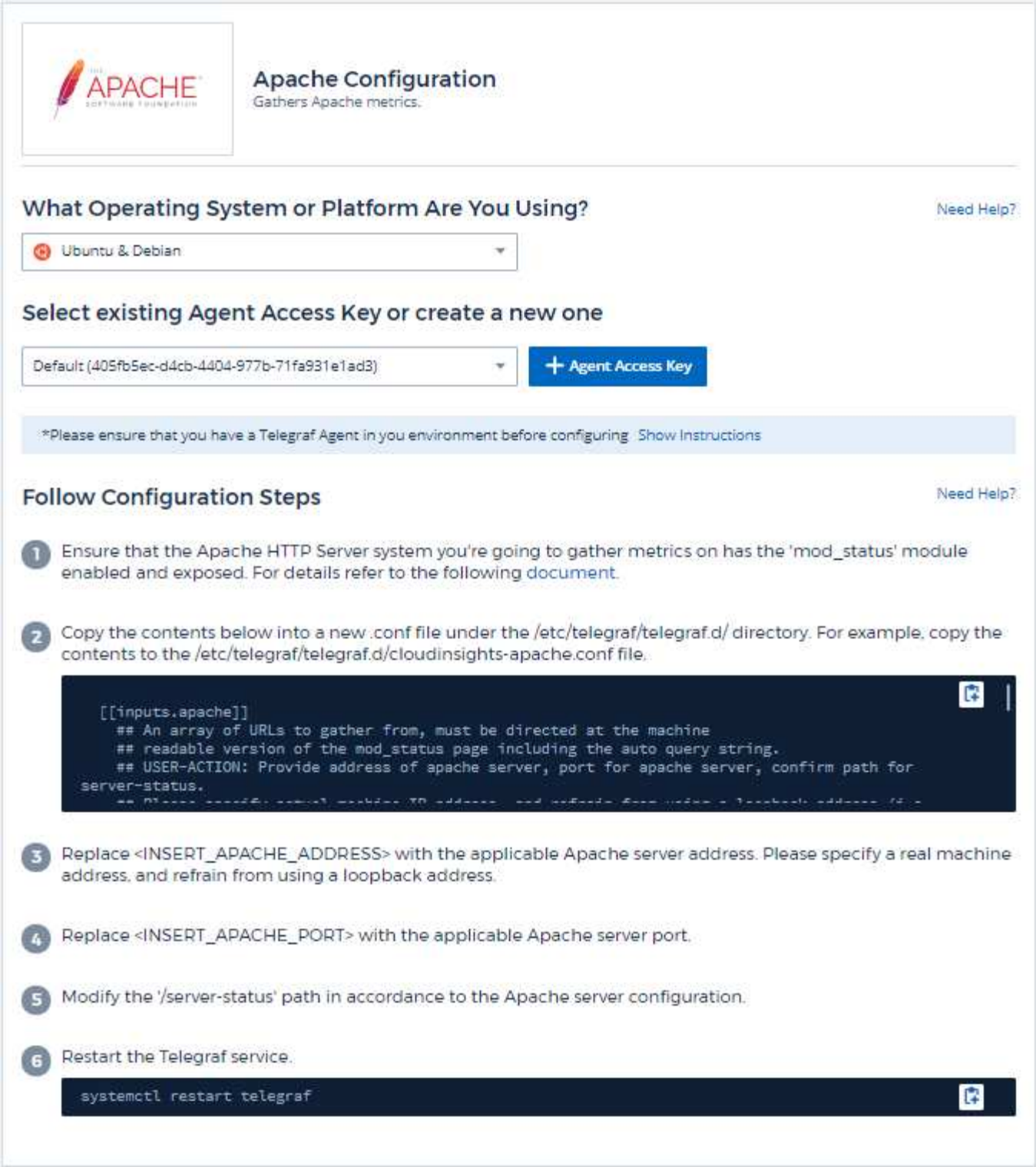
- Il server HTTP Apache deve essere configurato e correttamente in esecuzione
- È necessario disporre delle autorizzazioni di sudo o amministratore per l'host/VM dell'agente
- In genere, il modulo Apache *mod_status* è configurato per esporre una pagina nella posizione '/server-status?auto' del server Apache. L'opzione *ExtendedStatus* deve essere attivata per raccogliere tutti i campi disponibili. Per informazioni su come configurare il server, consulta la documentazione del modulo Apache: https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Apache.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Il plug-in di Telegraf per HTTP Server di Apache si basa sul modulo 'mod_status' per essere attivato. Quando questa opzione è attivata, il server HTTP di Apache espone un endpoint HTML che può essere visualizzato sul browser o scartato per l'estrazione dello stato di tutte le configurazioni HTTP Server di Apache.

Compatibilità:

La configurazione è stata sviluppata rispetto al server HTTP Apache versione 2.4.38.

Abilitazione mod_status:

L'attivazione e l'esposizione dei moduli "mod_status" richiede due passaggi:

- Modulo di abilitazione
- Esposizione delle statistiche dal modulo

Modulo di abilitazione:

Il caricamento dei moduli è controllato dal file di configurazione sotto '/usr/local/apache/conf/httpd.conf'. Modificare il file di configurazione e rimuovere il commento dalle seguenti righe:

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

Esposizione delle statistiche dal modulo:

L'esposizione di 'mod_status' è controllata dal file di configurazione in '/usr/local/apache2/conf/extra/httpd-info.conf'. Assicurarsi di avere quanto segue nel file di configurazione (almeno altre direttive saranno presenti):

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

Per istruzioni dettagliate sul modulo "mod_status", vedere "Documentazione di Apache"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Apache	Server namespace	Nodo IP Node Name Port Parent Server Config Generation Parent Server MPM Generation Server uptime is stopping	Occupati byte per richiesta byte per secondo CPU bambini CPU sistema bambini CPU utente carico CPU sistema CPU utente connessioni asincrone chiusura connessioni asincrone mantenimento connessioni asincrone scrittura connessioni totale durata per richiesta lavoratori inattivi carico medio (ultimi 1 m) carico medio (ultimi 15 m) carico medio (ultimi 5 m) Elabora le richieste al secondo accessi totali durata totale KByte Scoreboard chiusura Scoreboard Lookups DNS Scoreboard finitura Scoreboard Idle Cleanup Scoreboard Keep Alive Scoreboard Logging Scoreboard Open Scoreboard Reading Scoreboard Sending Scoreboard Starting Scoreboard Waiting

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Consul Data Collector

Cloud Insights utilizza questo data collector per raccogliere le metriche da console.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Console.

   Se non è stato configurato un agente per la raccolta, viene richiesto di "installare un agente" nel tuo ambiente.

   Se si dispone di un agente già configurato, selezionare il sistema operativo o la piattaforma appropriati e fare clic su **continua**.

2. Seguire le istruzioni nella schermata Consul Configuration (Configurazione console) per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione di Consul".

Oggetti e contatori per console

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Console	Namespace Check ID Service Node	Nodo IP nodo SO nodo UUID nodo Nome nodo Nome servizio Nome controllo ID servizio Stato	Avviso di passaggio critico

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Couchbase Data Collector

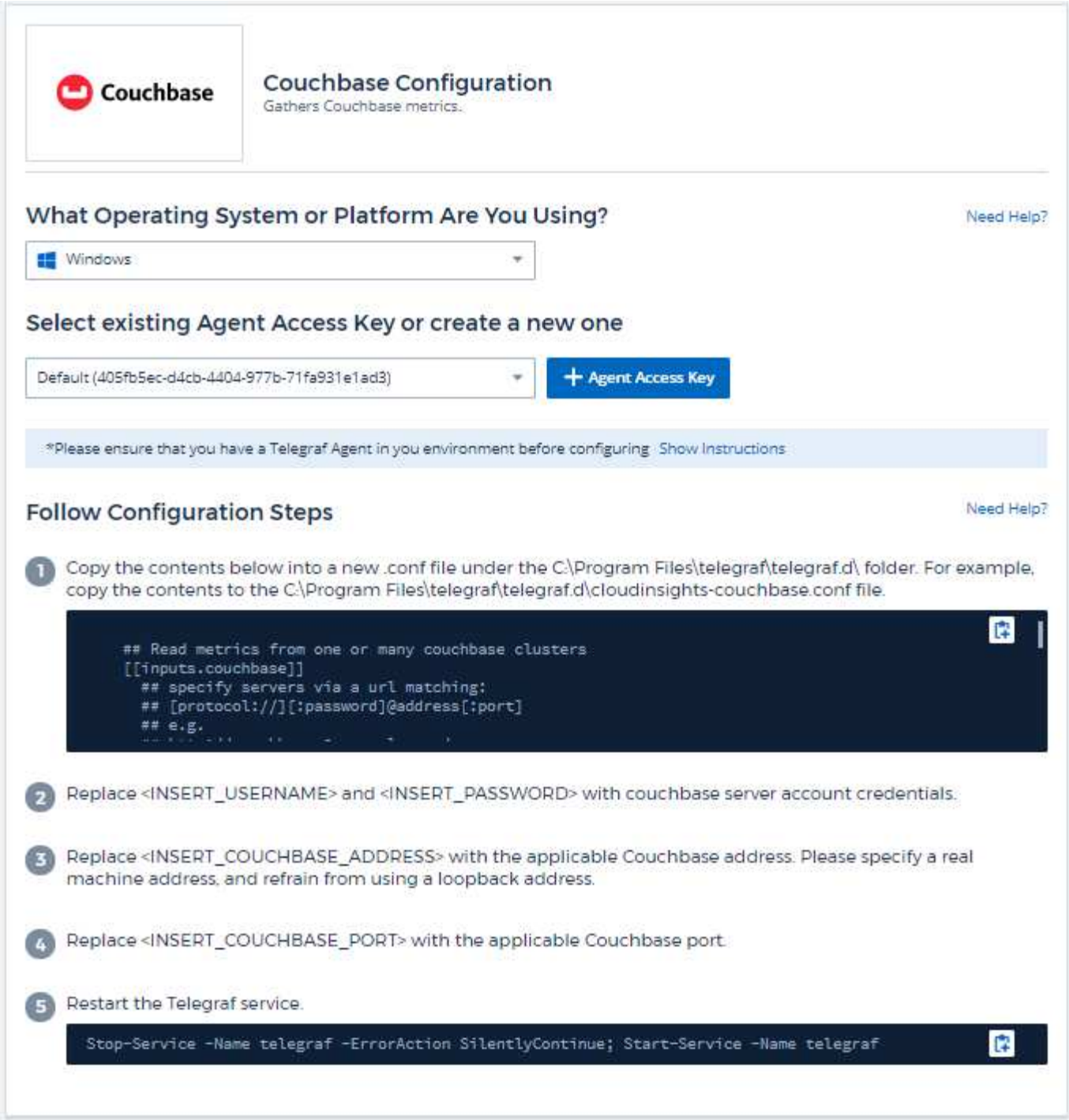
Cloud Insights utilizza questo data collector per raccogliere le metriche da Couchbase.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Couchbase.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione di Couchbase".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo Couchbase	Namespace Cluster Couchbase Node Hostname	Nome nodo IP nodo	Memoria libera totale
Bucket Couchbase	Cluster bucket namespace	Nome nodo IP nodo	Data used Data Fetches Disk used Item Count Memory used Operations per second quota utilizzata

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector di CouchDB

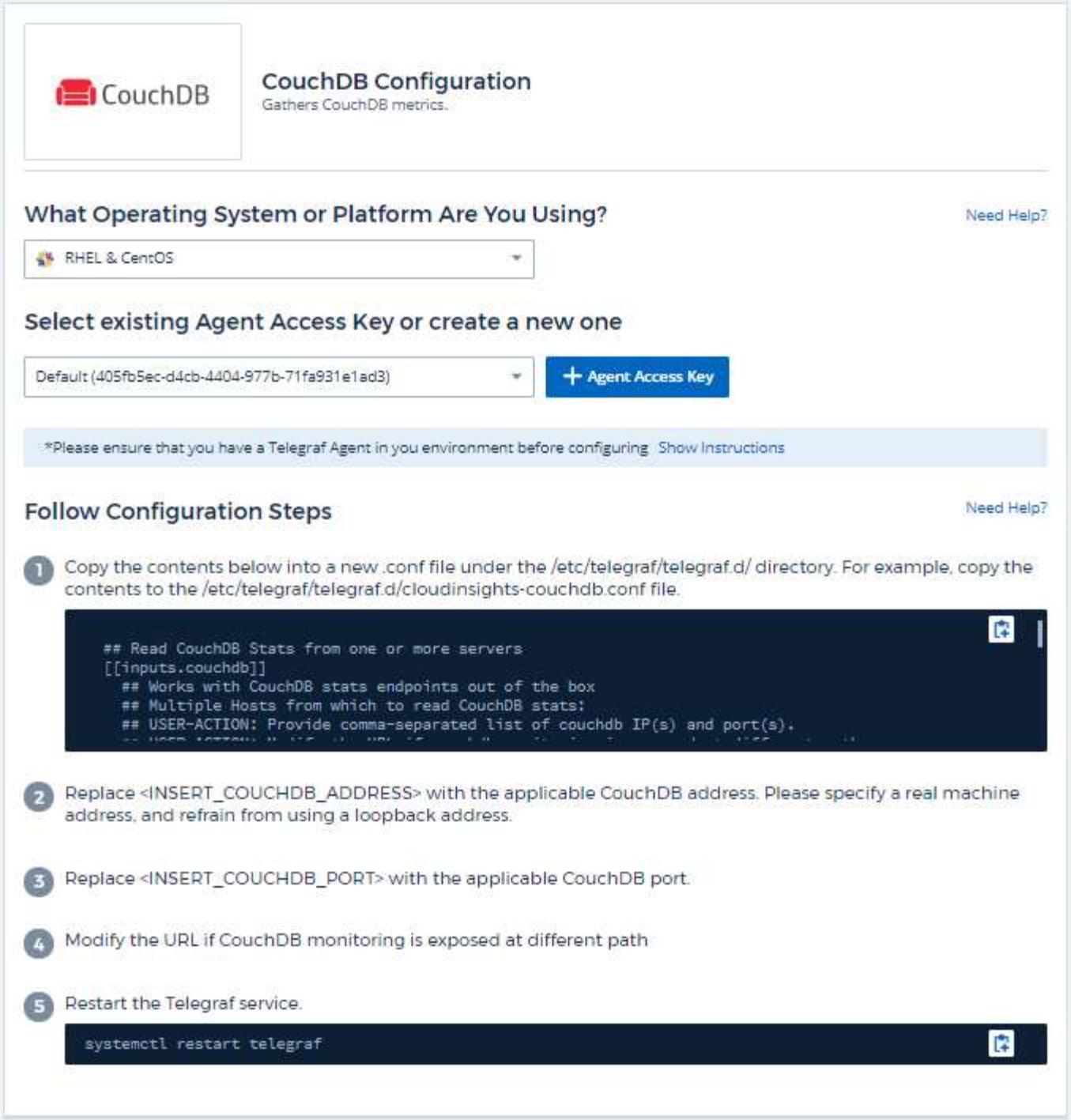
Cloud Insights utilizza questo data collector per raccogliere le metriche da CouchDB.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere CouchDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione di CouchDB".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Database dei CouchDB	Server namespace	Nome nodo IP nodo	Authentication cache Hits Authentication cache Miss Database Reads Database Scritture Database Open Open OS Files Max Request Time min Request Time httpd Request Methods Copy httpd Request Methods Delete httpd Request Methods Get httpd Request Methods Head httpd Request Methods Put Status Codes 200 Status Codes 201 codici di stato 202 codici di stato 301 codici di stato 304 codici di stato 400 codici di stato 401 codici di stato 403 codici di stato 404 codici di stato 405 codici di stato 409 codici di stato 412 codici di stato 500

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Docker Data Collector

Cloud Insights utilizza questo data collector per raccogliere le metriche da Docker.

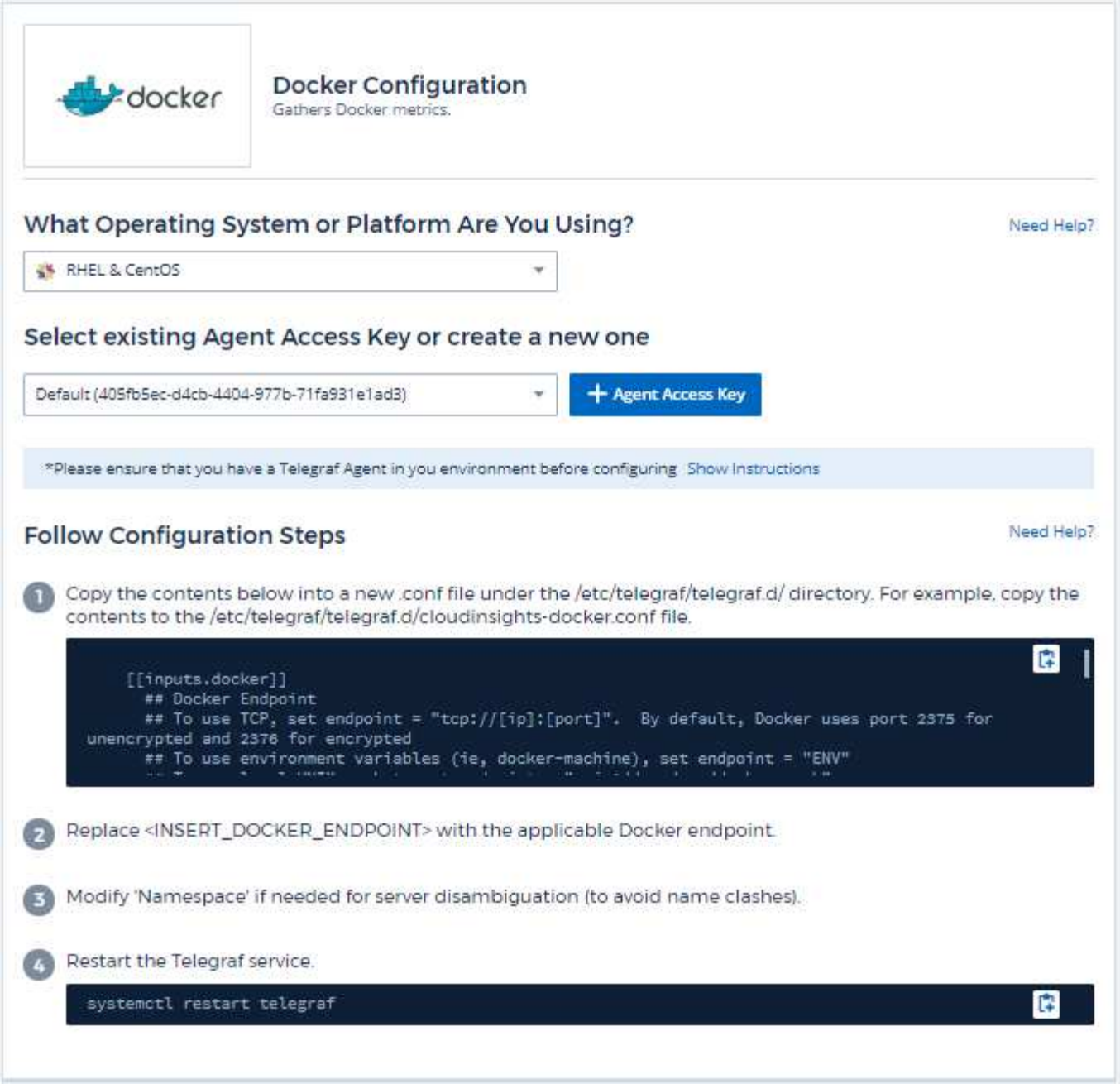
Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Docker.

   Se non è stato configurato un agente per la raccolta, viene richiesto di "installare un agente" nel tuo ambiente.

   Se si dispone di un agente già configurato, selezionare il sistema operativo o la piattaforma appropriati e fare clic su **continua**.

2. Seguire le istruzioni nella schermata Configurazione Docker per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Il plug-in di input Telegraf per Docker raccoglie le metriche attraverso un socket UNIX specificato o un endpoint TCP.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 1.12.6 di Docker.

Configurazione

Accesso a Docker tramite un socket UNIX

Se l'agente Telegraf è in esecuzione su baretal, aggiungere l'utente telegraf Unix al gruppo docker Unix eseguendo quanto segue:

```
 sudo usermod -aG docker telegraf
Se l'agente Telegraf viene eseguito all'interno di un pod Kubernetes,
esporre il socket Unix di Docker mappando il socket nel pod come volume e
montandolo su /var/run/docker.sock. Ad esempio, aggiungere quanto segue al
PodSpec:
```

```
volumes:
...
- name: docker-sock
hostPath:
path: /var/run/docker.sock
type: File
```

Quindi, aggiungere quanto segue al contenitore:

```
volumeMounts:
...
- name: docker-sock
mountPath: /var/run/docker.sock
```

Si noti che il programma di installazione di Cloud Insights fornito per la piattaforma Kubernetes si occupa automaticamente di questa mappatura.

Accedere a Docker tramite un endpoint TCP

Per impostazione predefinita, Docker utilizza la porta 2375 per l'accesso non crittografato e la porta 2376 per l'accesso crittografato.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Motore Docker	Namespace Docker Engine	Node Name Node IP Node UID Node OS Kubernetes Cluster Docker Version Unit	Container di memoria Container in pausa Container in esecuzione Container CPU interrotte Vai routine immagini listener Eventi utilizzati descrittori di file dati disponibili dati totali utilizzati metadati disponibili metadati totali utilizzati dimensione blocco pool

Oggetto:	Identificatori:	Attributi:	Punti dati:
Container Docker	Namespace Container Name Docker Engine	Kubernetes container Hash Kubernetes container Ports Kubernetes container Restart Count Kubernetes container Termination message Path Kubernetes container Termination message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes io Config visto Kubernetes io Config Source OpenShift io SCC Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Kompose Service Pod Template Hash Controller Revisione Hash Pod Pod generazione Template License Schema build Date Schema License Schema Name Schema URL Schema URL VCS Schema fornitore Schema versione Schema versione Maintainer Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Architecture Authoritative Source URL Data di build RH host RH Component Distribution Scope Install Release Run Summary Uninstall VCS Ref VCS Type VCS Version Vendor Version Health Status Container ID	Memoria attiva Anonymous Memory Active file Memory cache Memory Hierarchical Limit Memory Inactive Anonymous Memory Inactive file Memory Limit Memory Mapped file Memory Max Usage Memory Page Fault Memory Memory Pageed out Memory Resident Set Size Memory Resident Set Size memoria enorme memoria totale attiva Memoria anonima totale memoria file attiva totale memoria cache totale memoria non attiva memoria anonima totale memoria file inattiva memoria totale file mappato memoria totale memoria errori pagine totali memoria principale errori pagine totali memoria totale pagine in uscita memoria totale dimensioni set residenti memoria totale set residenti dimensioni memoria enorme memoria totale Memoria unevictable utilizzo della memoria utilizzo della memoria percentuale di utilizzo Codice di uscita OOM Killed PID Started at Finding Streak

Oggetto:	Identificatori:	Attributi:	Punti dati:
Io blocco container Docker	Namespace Container Name Device Docker Engine	Kubernetes container Hash Kubernetes container Ports Kubernetes container Restart Count Kubernetes container Termination message Path Kubernetes container Termination message Policy Kubernetes Pod Termination Grace Period Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Name Kubernetes Docker Type Kubernetes Pod Name Pod UID Kubernetes Sandbox ID Node IP Node UUID Docker Version Kubernetes Config visto Kubernetes Config Source OpenShift SCC Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Schema versione modello modello Pod Hash Controller Revisione modello Hash Pod generazione modello Kompose Service Schema Data build Schema licenza Schema Nome Schema fornitore cliente Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Data di build licenza Vendor Architecture Authoritative Source URL RH build host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Type Version Schema URL Schema VCS URL Schema versione Container ID	Io Service Bytes Recursive Async io Service Bytes Recursive Read io Service Bytes Recursive Sync io Service Bytes Recursive io Recursive Serviced Async io Serviced Recursive Read io Serviced Recursive io Serviced Recursive Total io Serviced Recursive Recursive Write

Oggetto:	Identificatori:	Attributi:	Punti dati:
Docker Container Network	Namespace Container Name Network Docker Engine	Container Image Container Status Container Version Node Name Node IP Node UUID Node OS K8s Cluster Docker Version Container ID	RX dromed RX bytes RX errors RX packets TX dromed TX bytes TX errors TX packets

Oggetto:	Identificatori:	Attributi:	Punti dati:
CPU Docker Container	Namespace Container Name CPU Docker Engine	Contenitore Kubernetes Hash Kubernetes Container Ports Kubernetes Container Restart Count Kubernetes Container Termination message Path Kubernetes Container Termination message Policy Kubernetes Pod Termination Grace Period Kubernetes Config Sawed Kubernetes Config Source OpenShift SCC Container Image Container Status Container Version Node Name Kubernetes Container Log Path Kubernetes Container Digitare Kubernetes Pod Name Kubernetes Pod namespace Kubernetes Pod UID Kubernetes Sandbox ID Node IP Node UUID Node OS Kubernetes Cluster Docker Version Kubernetes Descrizione Kubernetes Display Name OpenShift Tags Schema versione modello Pod modello Hash Controller Revisione modello Hash Pod generazione Servizio Kompose Schema Data di costruzione Schema Schema Schema licenza Schema Nome Schema Vendor Customer Pod Kubernetes StatefulSet Pod Name Tenant Webconsole Data di build License Vendor Architecture Authitative Source URL RH build host RH Component Distribution Scope Install Maintainer Release Run Summary Uninstall VCS Ref VCS Type Version Schema URL Schema VCS URL Schema Version Container ID	Periodi di rallentamento periodi di rallentamento periodi di rallentamento riduzione tempi di rallentamento utilizzo in modalità kernel utilizzo in modalità utente percentuale utilizzo sistema totale

Risoluzione dei problemi

Problema:	Prova:
Dopo aver seguito le istruzioni riportate nella pagina di configurazione, non riesco a visualizzare le metriche di Docker in Cloud Insights.	Controllare i registri degli agenti di Telegraf per verificare se riporta il seguente errore: E! Errore nel plug-in [inputs.docker]: Permesso ottenuto negato durante il tentativo di connessione al socket del daemon Docker. In caso contrario, eseguire i passaggi necessari per fornire all'agente Telegrafo l'accesso al socket Docker Unix come specificato sopra.

Per ulteriori informazioni, consultare "Supporto" pagina.

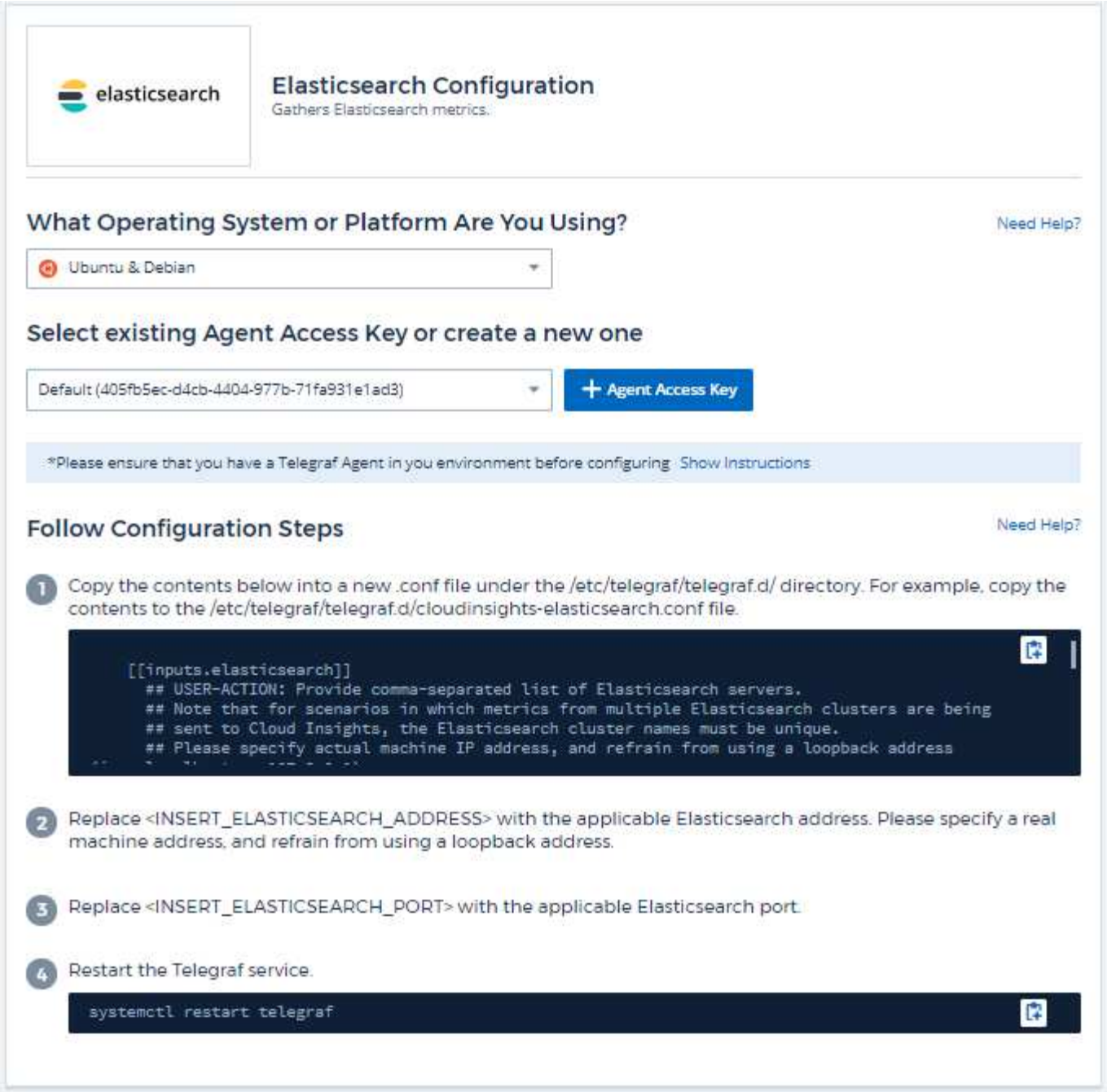
Elasticsearch Data Collector

Cloud Insights utilizza questo data collector per raccogliere le metriche da Elasticsearch.

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Elasticsearch.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione Elasticsearch".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Cluster Elasticsearch	Cluster di namespace	Nodo IP Node Name Cluster Status (Nome nodo IP Stato cluster)	Numero di nodi master numero totale di nodi filesystem dati disponibili (byte) filesystem dati liberi (byte) filesystem dati totali (byte) JVM thread OS assegnati Processori OS processori disponibili OS Mem Free (byte) OS Mem Free OS Mem totale (byte) OS Mem Used (byte) OS Mem Used Process CPU Indices Completion Size (byte) Indici numero indici indici documenti numero indici documenti indici documenti indici campi Data Evictions indici campo Data Memory Size (byte) indici Query cache Count indici cache Size indici segmenti numero indici segmenti valori doc memoria (byte) indici Shards Index Primaries Avg Indices Shards Index Primaries Max Indices Shards Index Primaries min Indices Shards Index Replication Avg Indices Shards Index Replication Max Indices Shards Index Replication min Indices Shards Avg Indices Shards Max Indices Shards Indices Shards Indices Total Indices Store Size (Bytes)

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nodo Elasticsearch	Namespace Cluster ES Node ID ES Node IP ES Node	ID zona	Machine Learning Enabled Machine Learning Memory Machine Learning Max Open Jobs X-Pack Installed Breakers Accounting Estimated Size (Bytes) Breakers Accounting Overhead Breakers Accounting inciamped Breakers Field Data Estimated Size (Bytes) Breakers Field Data Limit Size (Bytes) Breakers Field Data Overhead Breakers Field Data Breakers Field Data Tripped Breakers Dimensioni stimolate in-flight (byte) Breaker limite in-flight dimensione (byte) Breaker in-flight Overhead Breakers in-flight Breaker in-flight Bracciatori in-flight Parent dimensioni stimate (byte) Breaker Parent Overhead Breakers richiesta Parent Breakers dimensione stimata (byte) Breaker richiesta dimensione limite (byte) Breakers in overhead Request Request Data Available Filesystem (Byte) dati del filesystem liberi (byte) dati del filesystem totale (byte) filesystem io Stats Devices Ops filesystem io Stats Devices Read (kb) filesystem io Stats Devices Read Ops filesystem io Stats Devices Erite (kb) filesystem io Stats Devices Write Ops filesystem Stats Total Ops filesystem io Stats Total Ops filesystem io Stats Total Read (kb) filesystem Statistiche io Read Ops filesystem io Stats Total Write (kb) filesystem io Stats Write Ops filesystem Least Usage Estimate

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Flink Data Collector

Cloud Insights utilizza questo data collector per raccogliere le metriche da Flink.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Flink.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.

Flink

Flink Configuration

Gathers Flink metrics.

What Operating System or Platform Are You Using?

Need Help?

Windows

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

*Please ensure that you have a Telegraf Agent in you environment before configuring Show Instructions

Follow Configuration Steps

Need Help?

1. Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following document.
2. Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## ##########################
## JobManager
## ##########################
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL
```

3. Replace <INSERT_FLINK_JOBMANAGER_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
4. Replace <INSERT_FLINK_TASKMANAGER_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
5. Replace <INSERT_JOLOKIA_PORT> with the applicable jolokia port.
6. Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
7. Modify 'Cluster' if needed for Flink cluster designation.
8. Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

Setup (Configurazione)

Un’implementazione Flink completa comprende i seguenti componenti:

JobManager: Il sistema primario Flink. Coordina una serie di TaskManager. In una configurazione ad alta disponibilità, il sistema avrà più di un JobManager. Taskmanager: Qui vengono eseguiti gli operatori Flink. Il plugin Flink si basa sul plugin di telegraf, Jolokia. Come requisito per la raccolta di informazioni da tutti i componenti Flink, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 1.7 di Flink.

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jlokia. La versione testata con è stata "Agente di Jookia 1.6.0".

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) sia posizionato nella posizione '/opt/flink/lib/'.

JobManager

Per configurare JobManager in modo da esporre l'API di Jookia, è possibile impostare la seguente variabile di ambiente sui nodi e riavviare JobManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
È possibile scegliere una porta diversa per Jlokia (8778). Se si dispone
di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch
all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere
accessibile dal plugin telegraf.
```

Taskmanager

Per configurare TaskManager in modo che esponga l'API di Jookia, è possibile impostare la seguente variabile di ambiente sui nodi e riavviare TaskManager:

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0"
È possibile scegliere una porta diversa per Jlokia (8778). Se si dispone
di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch
all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere
accessibile dal plugin telegraf.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Task Manager Flink	Server dello spazio dei nomi del cluster	Nome nodo Task Manager ID nodo IP	Rete disponibile segmenti di memoria rete totale segmenti di memoria Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory memoria allocata memoria heap Init memoria heap Max memoria utilizzata Conteggio thread Demon Conteggio thread massimo Conteggio thread Conteggio thread Conteggio thread Conteggio thread Conteggio thread Totale iniziato
Flink Job (collega lavoro)	ID lavoro del server dello spazio dei nomi del cluster	Nome nodo Nome processo IP nodo ultimo punto di controllo percorso esterno tempo di riavvio	Downtime riavvio completo ultimo allineamento checkpoint buffer durata ultimo checkpoint dimensione checkpoint numero di checkpoint completati numero di checkpoint non riusciti numero di checkpoint in corso numero di checkpoint in corso tempo di attività

Oggetto:	Identificatori:	Attributi:	Punti dati:
Flink Job Manager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Garbage Collection PS MarkSweep Count Garbage Collection PS MarkSweep Time Garbage Collection PS Scavenge Count Garbage Collection PS Scavenge Time Heap Memory memoria memoria heap impegnata memoria heap Init memoria heap massima memoria heap utilizzata numero di gestori di attività registrati numero di processi in esecuzione slot di attività disponibili numero totale di thread Demon thread Count Numero massimo di thread Conteggio totale dei thread iniziato

Oggetto:	Identificatori:	Attributi:	Punti dati:
Attività Flink	ID attività ID lavoro spazio dei nomi cluster	Server Node Name Job Name Sub Task Index Task ID tentativo attività numero tentativo attività Nome attività ID Task Manager ID nodo IP Current Input Watermark	Buffer in buffer di utilizzo del pool in buffer di lunghezza della coda buffer di utilizzo del pool out buffer di lunghezza della coda buffer di numero in buffer di numero locale in buffer di numero locale al secondo buffer di numero locale al secondo buffer di numero remoto in buffer di numero remoto al secondo buffer di numero in remoto per Numero di seconda velocità buffer di numero in uscita buffer di numero in uscita al secondo numero di numero di velocità buffer in uscita al secondo numero di velocità byte in numero locale byte in numero di secondo numero di velocità byte in numero remoto byte in numero di secondo numero di numero di byte in remoto Numero di tasso al secondo byte in uscita numero byte in uscita al secondo numero di byte in uscita al secondo numero di tasso Record in numero record in per secondo numero di conteggio Record in per secondo numero di tasso Record in uscita numero record in uscita al secondo numero di conteggio Record in uscita al secondo tasso

Oggetto:	Identificatori:	Attributi:	Punti dati:
Operatore attività Flink	Namespace del cluster ID del job ID dell'operatore ID del task	Server Nome nodo Nome lavoro Nome operatore attività secondaria Indice attività ID tentativo attività numero tentativo attività Nome attività ID gestore attività IP nodo	Input corrente filigrana Output corrente numero filigrana Record in numero Record in per secondo numero numero Record in per secondo numero tasso Record out numero Records out per secondo numero numero Records out per secondo numero Rate out per secondo numero Records ultimi Records abbandonati partizioni assegnate byte consumati Rate Commit latenza Avg Commit latenza Max commit Rate commits Failed Commits successed Connection Close Rate Connection Count Connection Creation Rate Conteggio Fetch Latency Avg Fetch Latency Max Fetch Rate Fetch Size Avg Fetch Size Max Fetch Throttle Time Avg Fetch Throttle Time Max Heartbeat Rate Incoming Byte Rate io Ratio Ratio Time Avg (ns) io Rapporto di attesa io tempo di attesa medio (ns) tasso di adesione tempo di adesione tempo medio ultimo battito cardiaco fa rete io tasso di uscita byte tasso record di tasso consumato record di tasso massimo di ritardo record per richiesta media velocità richiesta dimensione media richiesta dimensione massima risposta velocità di selezione velocità di sincronizzazione tempo di sincronizzazione tempo di risposta medio battito cardiaco Tempo max. Di Unione tempo max. Di sincronizzazione

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector Hadoop

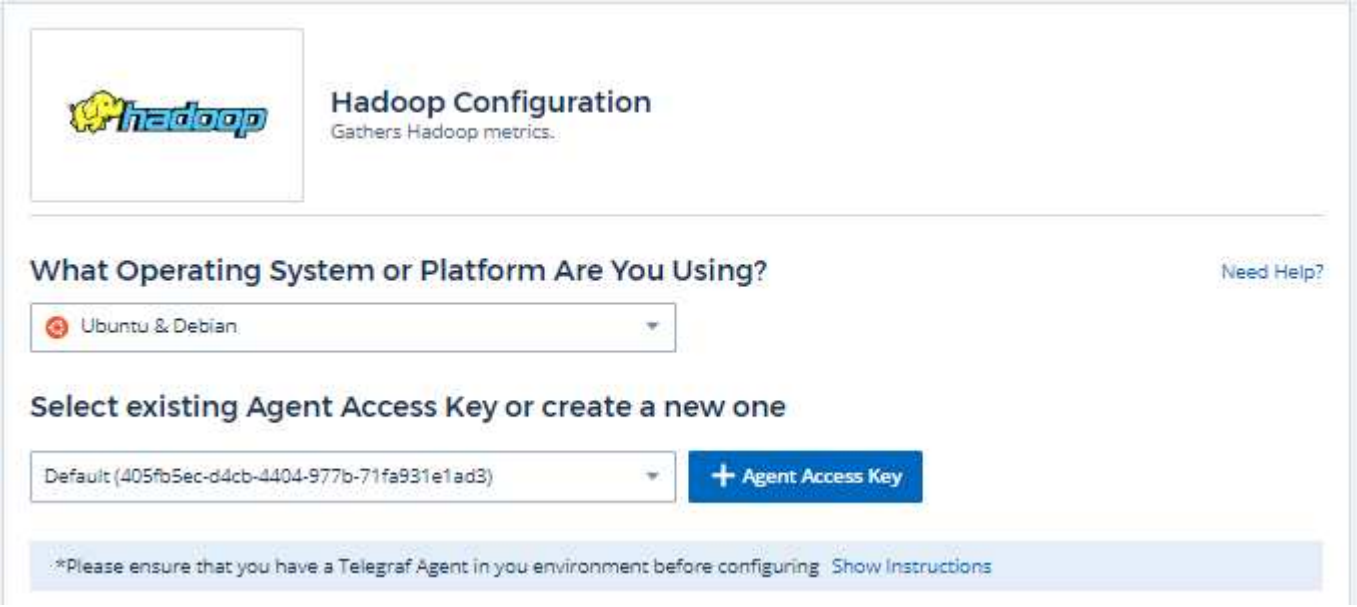
Cloud Insights utilizza questo data collector per raccogliere le metriche da Hadoop.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Hadoop.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Follow Configuration Steps

Need Help?

1. Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following document.

2. Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-hadoop.conf file.

```
################
# NAMENODE     #
################
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia
```

3. Replace <INSERT_HADOOP_NAMENODE_ADDRESS> with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NameNode's assigned Jolokia port.

4. Replace <INSERT_HADOOP_SECONDARYNAMENODE_ADDRESS> with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Secondary NameNode's assigned Jolokia port.

5. Replace <INSERT_HADOOP_DATANODE_ADDRESS> with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the DataNode's assigned Jolokia port.

6. Replace <INSERT_HADOOP_RESOURCEMANAGER_ADDRESS> with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the ResourceManager's assigned Jolokia port.

7. Replace <INSERT_HADOOP_NODEMANAGER_ADDRESS> with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the NodeManager's assigned Jolokia port.

8. Replace <INSERT_HADOOP_JOBHISTORYSERVER_ADDRESS> with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT_JOLOKIA_PORT> with the Job History Server's assigned Jolokia port.

9. Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).

10. Modify 'Cluster' if needed for Hadoop cluster designation.

11. Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

Un'implementazione Hadoop completa comprende i seguenti componenti:

- NameNode: Il sistema primario HDFS (Distributed file System) di Hadoop. Coordina una serie di DataNode.

- Secondary NameNode (nodo secondario): Un failover a caldo per il nodo principale di NameNode. In Hadoop la promozione a NameNode non avviene automaticamente. Secondary NameNode raccoglie le informazioni da NameNode per essere pronto per essere promosso quando necessario.
- DataNode: Proprietario effettivo dei dati.
- ResourceManager: Il sistema primario di calcolo (yarn). Coordina una serie di NodeManager.
- NodeManager: La risorsa per il calcolo. Posizione effettiva per l'esecuzione delle applicazioni.
- JobHistoryServer: Responsabile della manutenzione di tutte le richieste relative alla cronologia del lavoro.

Il plugin Hadoop si basa sul plugin di telegraf, Jolokia. Come requisito per raccogliere informazioni da tutti i componenti Hadoop, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 2.9 di Hadoop.

Configurazione

Jolokia Agent Jar

Per tutti i singoli componenti, è necessario scaricare una versione del file Jar dell'agente di Jlokia. La versione testata con è stata "Agente di Jookia 1.6.0".

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) sia posizionato nella posizione '/opt/hadoop/lib/'.

NameNode

Per configurare NameNode in modo da esporre l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Node secondario

Per configurare il nodo del nome secondario in modo che esponga l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8002 above) and Jolokia (7802).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

DataNode

Per configurare i DataNode in modo che espongano l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8001 above) and Jolokia (7801).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

ResourceManager

Per configurare ResourceManager in modo da esporre l'API di Jlokia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8003 above) and Jolokia (7803).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

NodeManager

Per configurare i NodeManager in modo che espongano l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8004 above) and Jolokia (7804).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Server JobHistory

Per configurare il server di StoriaLavoro in modo che esponga l'API di Jookia, è possibile configurare quanto segue in <HADOOP_HOME>/etc/hadoop/hadoop-env.sh:

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8005 above) and Jolokia (7805).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Node secondario Hadoop	Server dello spazio dei nomi del cluster	Nome nodo nodo IP Compile Info versione	Conteggio GC copie GC Conteggio GC Marks Sweep Conteggio compact numero GC Info soglia superata numero GC soglia di avviso superata tempo GC tempo di copia GC Marchi GC Sweep tempo compatto GC totale tempo di inattività extra registri numero di errori registri numero di errori registri Info Conteggio registri Avvisi Conteggio memoria heap commesso Memoria Heap Max memoria Heap memoria utilizzata memoria massima memoria memoria non Heap memoria impegnata non Heap memoria massima non Heap thread utilizzati thread bloccati nuovi thread runnable thread terminati thread in attesa di tempo in attesa

Oggetto:	Identificatori:	Attributi:	Punti dati:
Hadoop NodeManager	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Containers Allocated Memory Allocated Oportunistic Virtual Core allocati Oportunistic Virtual Core allocati memoria allocata Virtual Core disponibili Directory disponibili Directory locali non funzionanti Log cache Size before clean container Launch Duration Avg Time container Launch Duration Number of Operations Containers Completed Containers Failed Containers Initing Killed Containers laun Container Reiniting Containers rolled on Failure Containers Running Disk Utilization Good Local Directories Disk Log Directories Bytes deleted Private Bytes deleted Public Containers Running opportunistic Bytes deleted Total Shuffle Connections Shuffle Output Bytes Shuffle output Failed Shuffle Outputs OK GC Count GC Marks Sweep Conteggio compatto numero GC Info soglia superata numero GC soglia di avviso superata tempo GC tempo di copia contrassegni GC Sweep tempo compatto GC totale tempo di inattività totale registri di errori numero di errori registri di conteggio irreversibile Info numero di registri Avvisi numero memoria memoria memoria memoria memoria impegnata heap memoria massima memoria memoria utilizzata memoria massima Memoria memoria non heap memoria impegnata non heap memoria massima non heap thread utilizzati

Oggetto:	Identificatori:	Attributi:	Punti dati:
ResourceManager di Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	ApplicationMaster Launch Delay Avg ApplicationMaster Launch Delay Number ApplicationMaster Register Delay Avg ApplicationMaster Register Delay Number NodeManager numero attivo NodeManager numero dismesso NodeManager numero dismesso NodeManager numero dismesso NodeManager numero dismesso NodeManager numero disattivo NodeManager limite di memoria NodeManager numero di dismesso Virtual Core usato Capacity Active Applications utenti attivi Aggregate Container allocati Container aggregati presvuotati Container aggregati rilasciati memoria aggregata secondi nodo aggregato presvuotato Container locali allocati aggregato off Container allocati Container locali allocati aggregato core virtuali allocati secondi Container presvuotati memoria allocata core virtuali allocati tentativo di applicazione primo Container ritardo di allocazione tempo medio tentativo di applicazione Ritardo di allocazione del primo container numero di applicazioni completate applicazioni non riuscite applicazioni in sospeso applicazioni in esecuzione applicazioni inviate memoria disponibile Virtual Core disponibili Container in sospeso memoria in sospeso Virtual Core in sospeso Container in sospeso

Oggetto:	Identificatori:	Attributi:	Punti dati:
DataNode Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID cluster versione	Numero di transceiver trasmessi in corso capacità cache capacità utilizzata DFS capacità stimata capacità persa totale ultimo volume guasto numero blocchi numero blocchi memorizzati numero blocchi non riusciti a cache numero non riuscito a dismemorizzare nella cache volumi numero non riuscito capacità rimanente GC Conteggio copie GC Conteggio segni GC Sweep Conteggio compatto numero GC Info Threshold exceeded GC Number Warning Threshold exceeded GC Time GC Copy Time GC Marks Sweep Compact Time GC Total Extra Sleep Time Logs Error Count Logs Fatal Count Log Info Count WARN Count Memory Heap committed Memory Heap Max Memory Heap Used Memory non Heap Memoria memoria non heap Max thread non heap utilizzati thread bloccati nuovi thread runnable thread terminati thread in attesa di tempo thread in attesa

Oggetto:	Identificatori:	Attributi:	Punti dati:
Node di Hadoop	Server dello spazio dei nomi del cluster	Nome nodo IP nodo ID transazione ultimo tempo di scrittura dall'ultimo caricamento modifiche ha Stato file sistema Stato blocco ID pool ID cluster informazioni di compilazione versione distinta Conteggio versione	Blocchi capacità capacità totale capacità totale capacità utilizzata capacità utilizzata blocchi non DFS corrotti capacità stimata perdita totale blocchi heartbeat in eccesso file scaduti totale blocco file system lunghezza coda blocchi mancanti replica con client fattore uno nodi dati attivi dead nodi dati decommissioning nodi dati morti decommissioning Live Nodi di dati disattivazione zone di crittografia numero nodi di dati in entrata file di manutenzione sotto nodi di dati di costruzione morti in manutenzione nodi di dati in corso di manutenzione nodi di dati in tempo reale storage in tempo reale replica in attesa di timeout messaggio del nodo di dati in attesa di eliminazione blocchi di replica in sospeso blocchi di replica non replicati blocchi posticipati replica pianificati Snapshot Snapshot schotable Directories Nodi di dati file obsoleti carico totale totale numero di sincronizzazioni totale transazioni dall'ultimo punto di controllo transazioni dall'ultimo log blocchi di rollio errori di volumi sottoreplicati totale tempi di sincronizzazione totale oggetti Max blocco operazioni Aggiungi operazioni Consenti operazioni di snapshot blocco operazioni in batch blocco operazioni in coda blocco operazioni ricevute ed eliminate tempo medio di report operazioni ricevute ed eliminate

Oggetto:	Identificatori:	Attributi:	Punti dati:
Hadoop JobHistoryServer	Server dello spazio dei nomi del cluster	Nome nodo IP nodo	Conteggio GC copie GC Conteggio GC Marks Sweep Conteggio compact numero GC Info soglia superata numero GC soglia di avviso superata tempo GC tempo di copia GC Marchi GC Sweep tempo compatto GC totale tempo di inattività extra registri numero di errori registri numero di errori registri Info Conteggio registri Avvisi Conteggio memoria heap commesso Memoria Heap Max memoria Heap memoria utilizzata memoria massima memoria memoria non Heap memoria impegnata non Heap memoria massima non Heap thread utilizzati thread bloccati nuovi thread runnable thread terminati thread in attesa di tempo in attesa

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

HAProxy Data Collector

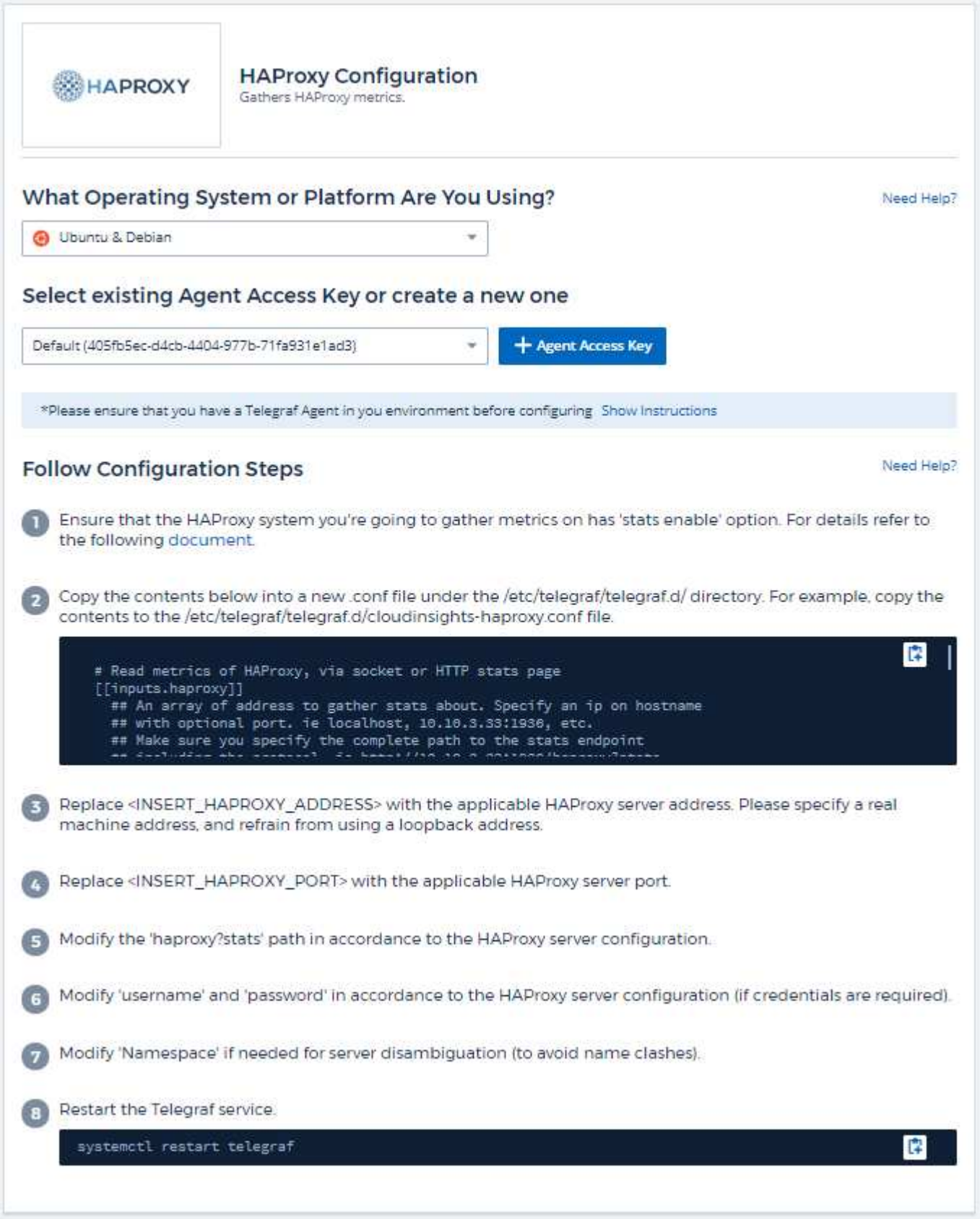
Cloud Insights utilizza questo data collector per raccogliere le metriche da HAProxy.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere HAProxy.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Il plug-in di Telegraf per HAProxy si basa sull'abilitazione delle statistiche HAProxy. Si tratta di una configurazione integrata in HAProxy, ma non è attivata subito. Se attivato, HAProxy espone un endpoint HTML

che può essere visualizzato sul browser o scartato per l'estrazione dello stato di tutte le configurazioni HAProxy.

Compatibilità:

La configurazione è stata sviluppata con la versione 1.9 di HAProxy.

Configurazione:

Per abilitare le statistiche, modificare il file di configurazione hadproxy e aggiungere le seguenti righe dopo la sezione 'default', utilizzando il proprio utente/password e/o URL hadproxy:

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

Di seguito viene riportato un esempio semplificato di file di configurazione con le statistiche attivate:

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

Per istruzioni complete e aggiornate, consultare "Documentazione HAProxy".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
HAProxy Frontend	Proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name Proxy ID Mode Process id Sessions Rate Limit Server id Sessions Limit Status	Byte in byte in uscita cache riscontri cache ricerche cache byte di compressione bypassati byte di compressione in byte di compressione in uscita risposte di compressione velocità di connessione velocità di connessione connessioni max Richieste totali negate da richieste di regole di connessione negate da problemi di sicurezza risposte negate da problemi di sicurezza Richieste negate da richieste di regole di sessione errori risposte 1xx Risposte 2xx risposte 3xx risposte 4xx risposte 5xx risposte altre richieste intercettate sessioni Rate numero massimo di richieste Rate numero massimo di richieste Rate numero massimo di richieste sessioni totali sessioni numero massimo di sessioni totale di richieste riscritte

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server HAProxy	Server proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name Check Time to Finish Check Fall Configuration Check Health Value Check Rise Configuration Check Status Proxy ID Last Change Time Last Session Time Mode Process id Server id Status Weight	Server attivi Server di backup byte in byte out Check Downs Check fails il client interrompe le connessioni tempo medio downtime totale Denied Responses errori di connessione Responses 1xx Responses 2xx Responses 3xx Responses 4xx Responses 5xx Responses Other Server Selected Total Queue Current Queue Max Time Sessions Average per Seconda sessione al secondo Max Connection Reuse Response Time Sessions Average Sessions Max Server Transfer Aborts Sessions Total Time Average Requests Repatches Requests Requests Requests Requests Rewrite

Oggetto:	Identificatori:	Attributi:	Punti dati:
HAProxy back-end	Proxy degli indirizzi dello spazio dei nomi	Nodo IP Node Name ID proxy Last Change Time Last Session Time Mode Process id Server id Sessions Limit Status Weight	Server attivi Server di backup byte in byte out cache Hits Lookup cache Check Downs il client interrompe la compressione byte bypassati byte di compressione in byte di compressione out risposte di compressione connessioni tempo medio downtime totale richieste negate da problemi di sicurezza risposte negate da problemi di sicurezza errori di connessione errori di risposta risposte 1xx risposte 2xx risposte 3xx risposte 4xx risposte 5xx risposte Altro server selezionato coda totale coda corrente coda massima durata media sessioni al secondo Richieste max connessione tempo di risposta tempo di risposta sessioni max Server Transfer interrompe le sessioni totale sessioni tempo totale media richieste di reinvio Richieste tentativi Riscrive

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector JVM

Cloud Insights utilizza questo data collector per raccogliere le metriche da JVM.

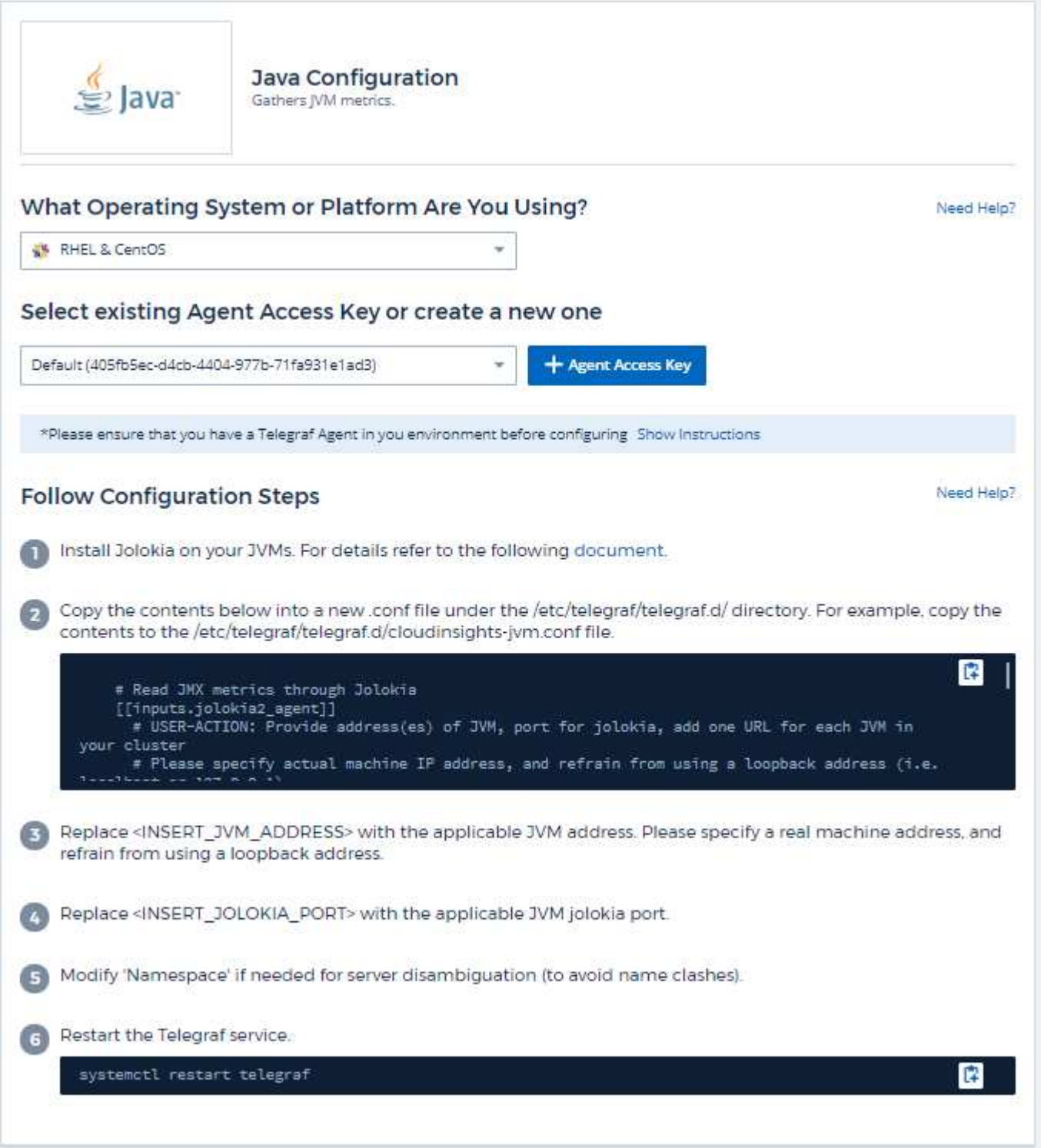
Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere JVM.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.

3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione JVM".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
JVM	JVM dello spazio dei nomi	Architettura del sistema operativo Nome del sistema operativo versione Runtime specifica del runtime fornitore specifica del runtime versione tempo di attività Runtime Nome della macchina virtuale Runtime fornitore versione della macchina virtuale Nome del nodo IP	Classe caricata Classe totale caricata Classe scaricata memoria heap memoria impegnata heap Init memoria heap utilizzata memoria massima heap utilizzata memoria non heap memoria impegnata memoria non heap memoria init memoria non heap memoria massima non heap oggetti memoria utilizzati in attesa di finalizzazione OS processori disponibili OS memoria virtuale impegnata dimensione OS libero Memoria fisica dimensione OS spazio libero di swap dimensione OS massimo file descrittore Conteggio OS Open file Descriptors Conteggio OS processore CPU carico OS processore tempo SO sistema operativo carico sistema operativo carico sistema operativo medio totale memoria fisica dimensione OS spazio totale di swap dimensione thread Conteggio dei demon thread Conteggio dei picchi di thread Conteggio thread totale iniziato Conteggio Garbage Collector Copy Collection Conteggio Garbage Collector tempo di raccolta Garbage Collector Mark-sweep Collector Conteggio Garbage Collector tempo di raccolta Garbage Collector G1 tempo di raccolta Old Generation Garbage Collector G1 Conteggio raccolta Young Generation Garbage Collector G1 Tempo di raccolta di giovani generazioni Garbage Collector tempo di

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector Kafka

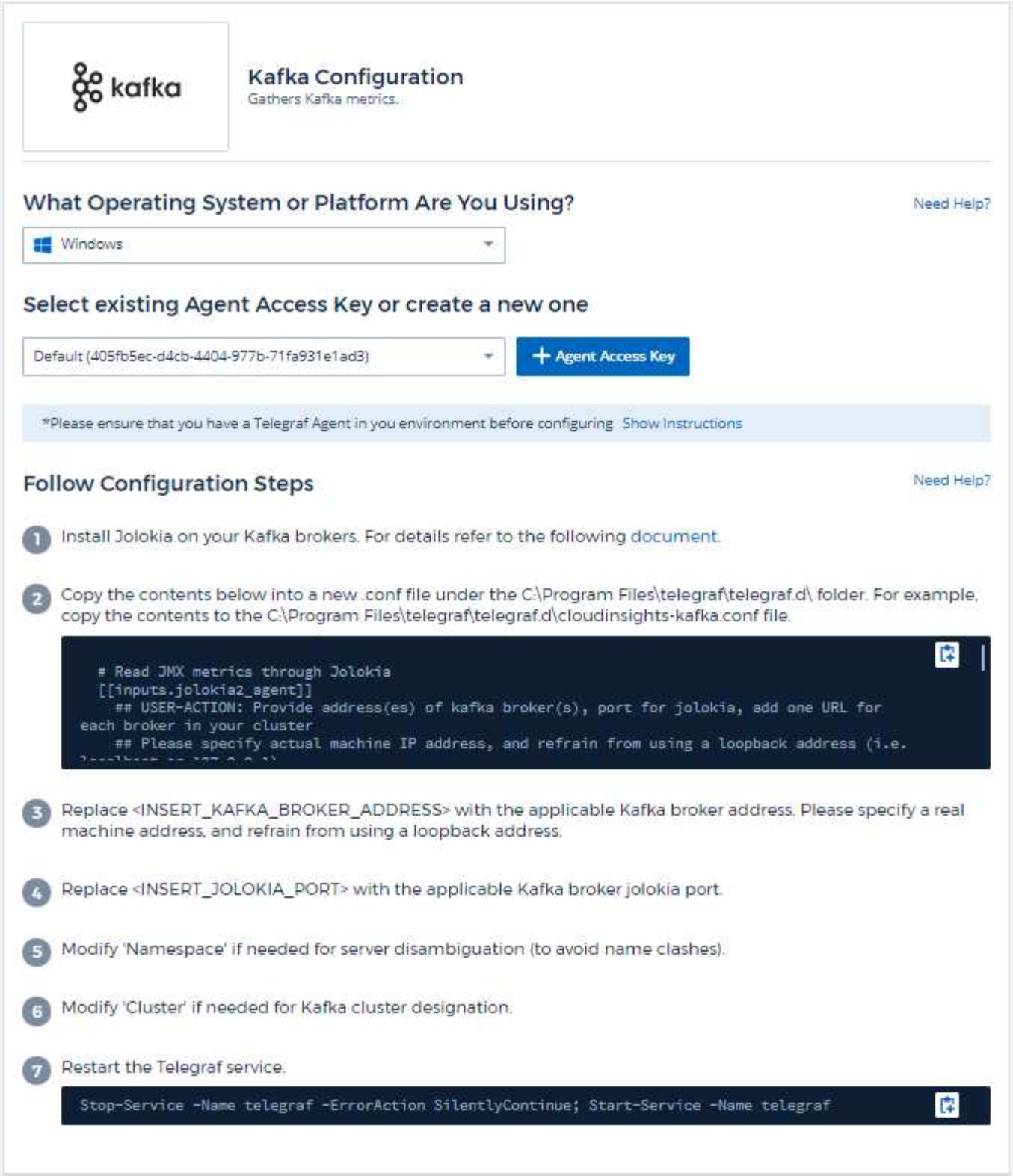
Cloud Insights utilizza questo data collector per raccogliere le metriche da Kafka.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Kafka.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Il plugin Kafka si basa sul plugin di telegraf, Jolokia. Come requisito per raccogliere informazioni da tutti i broker Kafka, JMX deve essere configurato ed esposto tramite Jolokia su tutti i componenti.

Compatibilità

La configurazione è stata sviluppata rispetto alla versione 0.11.0 di Kafka.

Configurazione

Tutte le istruzioni riportate di seguito presuppongono che la posizione di installazione di kafka sia "/opt/kafka". È possibile adattare le istruzioni riportate di seguito in base alla posizione di installazione.

Jolokia Agent Jar

Una versione del file Jar dell'agente di Jlokia "scaricato". La versione testata era l'agente di Jookia 1.6.0.

Le istruzioni riportate di seguito presuppongono che il file jar scaricato (jookia-jvm-1.6.0-Agent.jar) si trovi nella posizione '/opt/kafka/libs/'.

Kafka Brokers

Per configurare i broker Kafka in modo che espongano l'API di Jokia, è possibile aggiungere quanto segue in <KAFKA_HOME>/bin/kafka-server-start.sh, appena prima della chiamata 'kafka-run-class.sh':

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -I`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

Si noti che l'esempio precedente utilizza 'hostname -i' per impostare la variabile di ambiente 'RMI_HOSTNAME'. In più computer IP, questo dovrà essere modificato per raccogliere l'IP che si occupa delle connessioni RMI.

È possibile scegliere una porta diversa per JMX (9999 sopra) e Jlokia (8778). Se si dispone di un IP interno su cui bloccare Jolokia, è possibile sostituire il "catch all" 0.0.0.0 con il proprio IP. Si noti che questo IP deve essere accessibile dal plugin telegraf. Se non si desidera autenticare, è possibile utilizzare l'opzione '-Dcom.sun.management.jmxremote.authenticate=false'. Utilizzare a proprio rischio.

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Broker Kafka	Cluster namespace Broker	Nome nodo IP nodo	Replica Manager Fetcher Max Lag Zooseeper connessioni client Zooseeper connessioni client (velocità di 15 m) Zooseeper connessioni client (velocità di 5 m) Zooseeper connessioni client (velocità media) Zooseeper connessioni client (velocità di 1 m) Replica Manager Conteggio partizioni Conteggio thread Demon Conteggio thread picco Conteggio thread corrente Conteggio thread totale iniziato le partizioni offline producono le richieste tempo totale (50° percentile) produrre le richieste tempo totale (75° percentile) produrre le richieste tempo totale (95° percentile) produrre le richieste tempo totale (98° percentile) produrre le richieste tempo totale (999° percentile) Richieste di produzione tempo totale (99a percentile) Richieste di produzione tempo totale richieste di produzione tempo totale richieste di produzione tempo totale richieste di produzione media tempo totale richieste di produzione minima tempo totale Stddev Replica Manager ISR si restringe Replica Manager ISR si restringe (15m rate) Replica Manager ISR si restringe (5 m rate) Replica Manager ISR si restringe (Velocità media) Replicate Manager ISR (velocità 1 m) Request Handler AVG Idle Request Handler AVG Idle Handler (velocità 15 m) Request Handler AVG Idle (velocità 5 m) Request Handler AVG Idle (velocità media) Request

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Kibana Data Collector

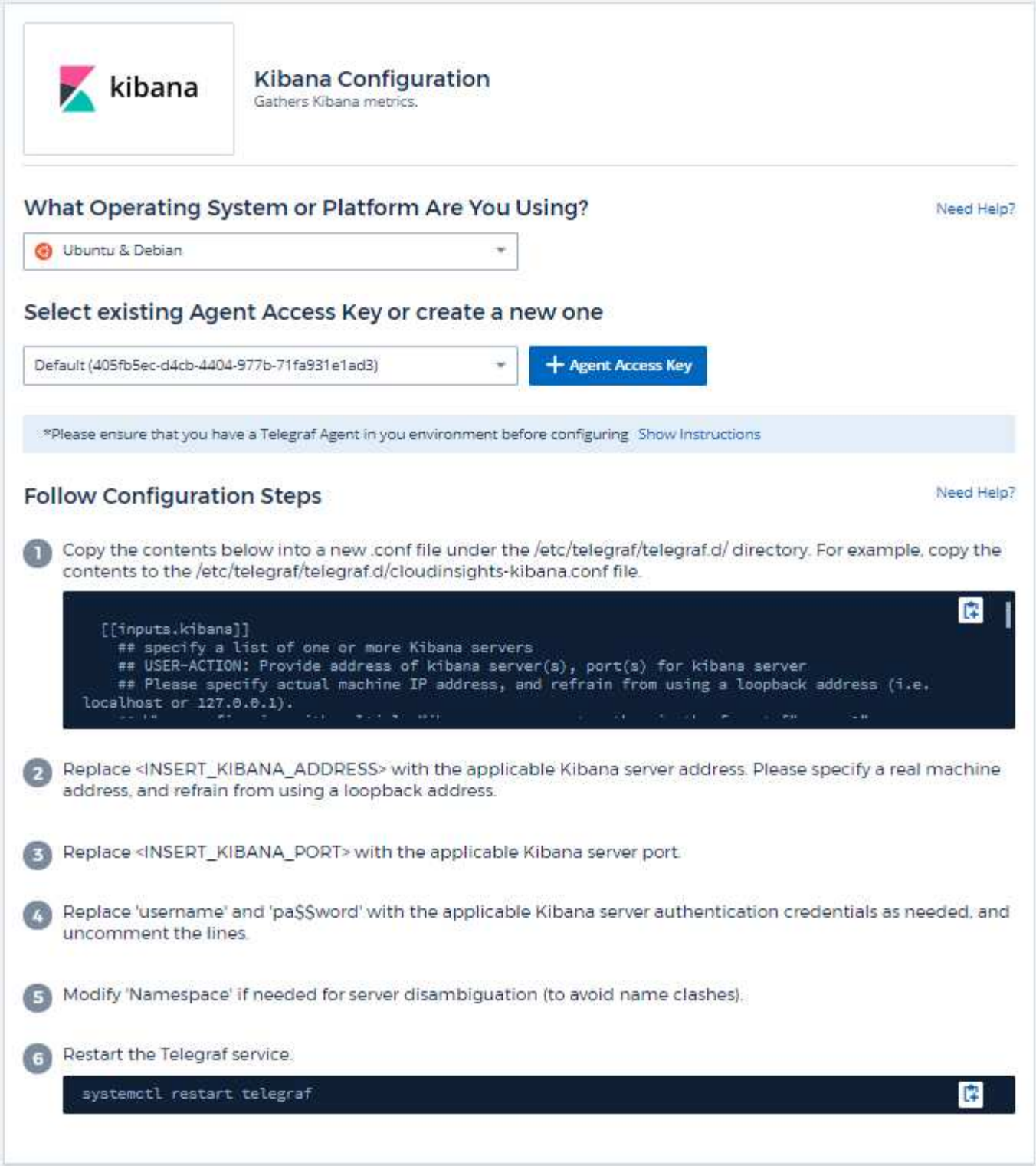
Cloud Insights utilizza questo data collector per raccogliere le metriche da Kibana.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli Kibana.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione di Kibana".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Kibana	Indirizzo dello spazio dei nomi	Nodo IP Node Name Version Status (Stato versione nome nodo IP)	Connessioni simultanee heap massimo heap richieste utilizzate al secondo tempo di risposta medio tempo di risposta tempo di attività massimo

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector Memcached

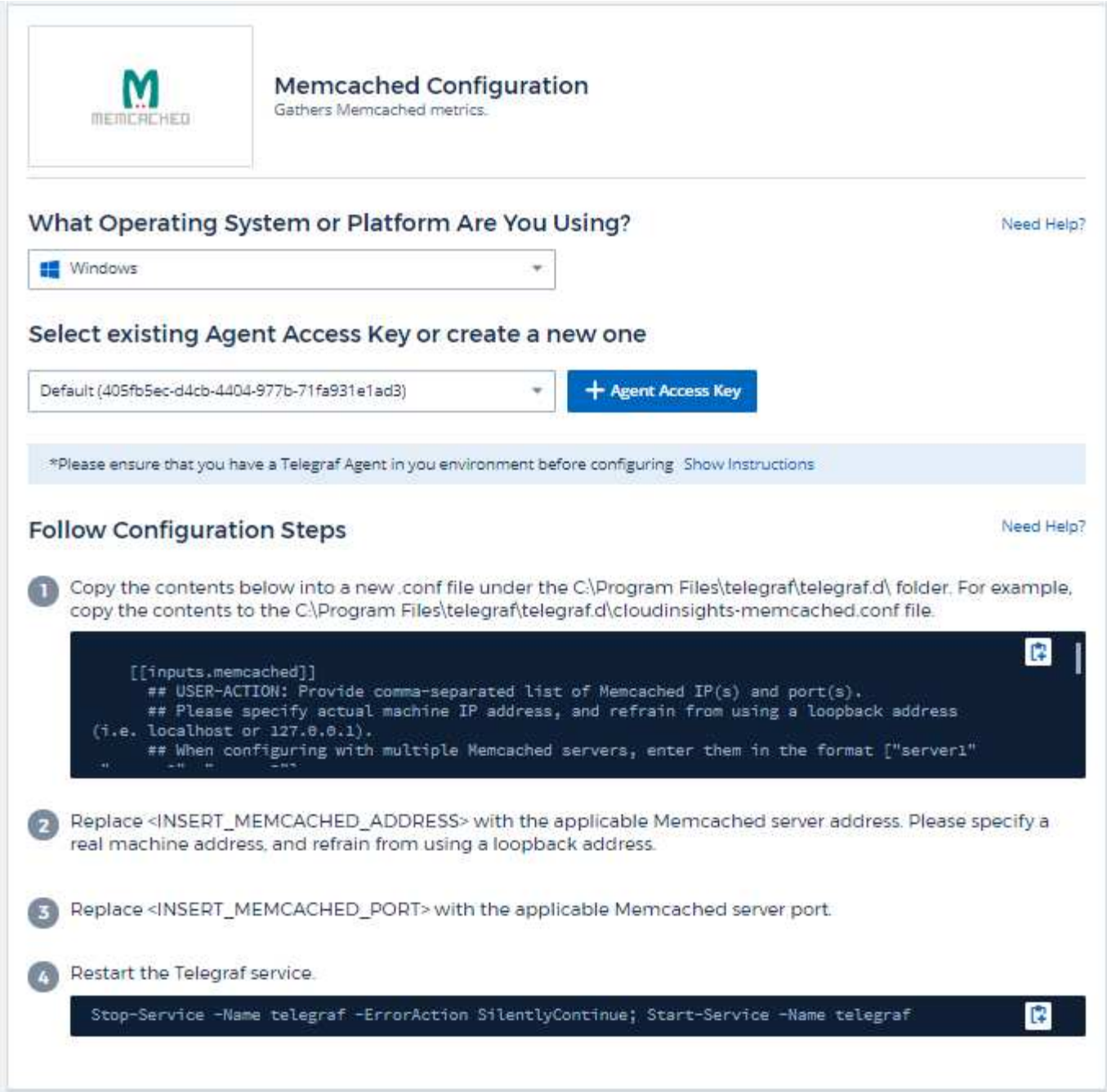
Cloud Insights utilizza questo data collector per raccogliere le metriche da Memcached.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Memcached.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Wiki Memcached".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Memcached	Server namespace	Nome nodo IP	Accettazione delle connessioni richieste di autenticazione gestite autenticazioni non riuscite byte utilizzati byte lettura (per sec) byte scritti (per sec) CAS Badval CAS accessi CAS errori requisiti di flusso (per sec) ottenere requisiti (per sec) requisiti impostati (per sec) requisiti di tocco (per sec) rese di connessione (per sec) Strutture di connessione connessioni aperte elementi memorizzati correnti Richieste di decr riscontri (per sec) Richieste di decr perse (per sec) Richieste di eliminazione riscontri (per sec) Richieste di eliminazione mancati (per sec) elementi sfratti validi elementi scaduti riscontri (per sec) Hash byte utilizzati Hash sta espandendo Hash Power Level Incr Requests Hits (per sec) Incr Requests miss (per sec) Server Max byte Listen Disabled Num Reclaimed Worker Threads Conteggio totale connessioni aperte totale elementi memorizzati Touch Hits Touch manca il tempo di attività del server

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

MongoDB Data Collector

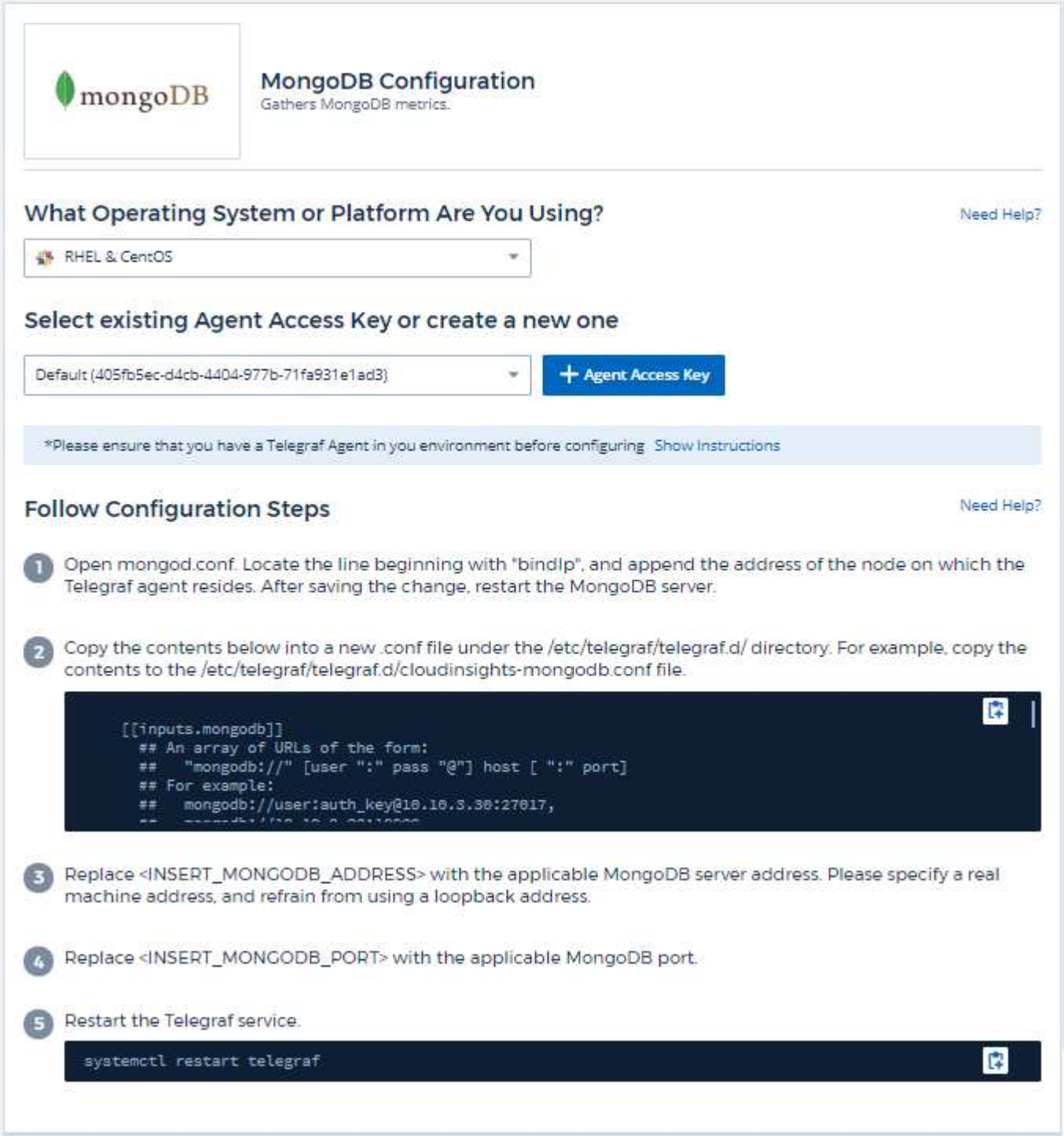
Cloud Insights utilizza questo data collector per raccogliere le metriche da MongoDB.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli MongoDB.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione MongoDB".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MongoDB	Nome host dello spazio dei nomi		
Database MongoDB	Nome host dello spazio dei nomi Nome database		

Risoluzione dei problemi

Le informazioni sono disponibili in "Supporto" pagina.

MySQL Data Collector

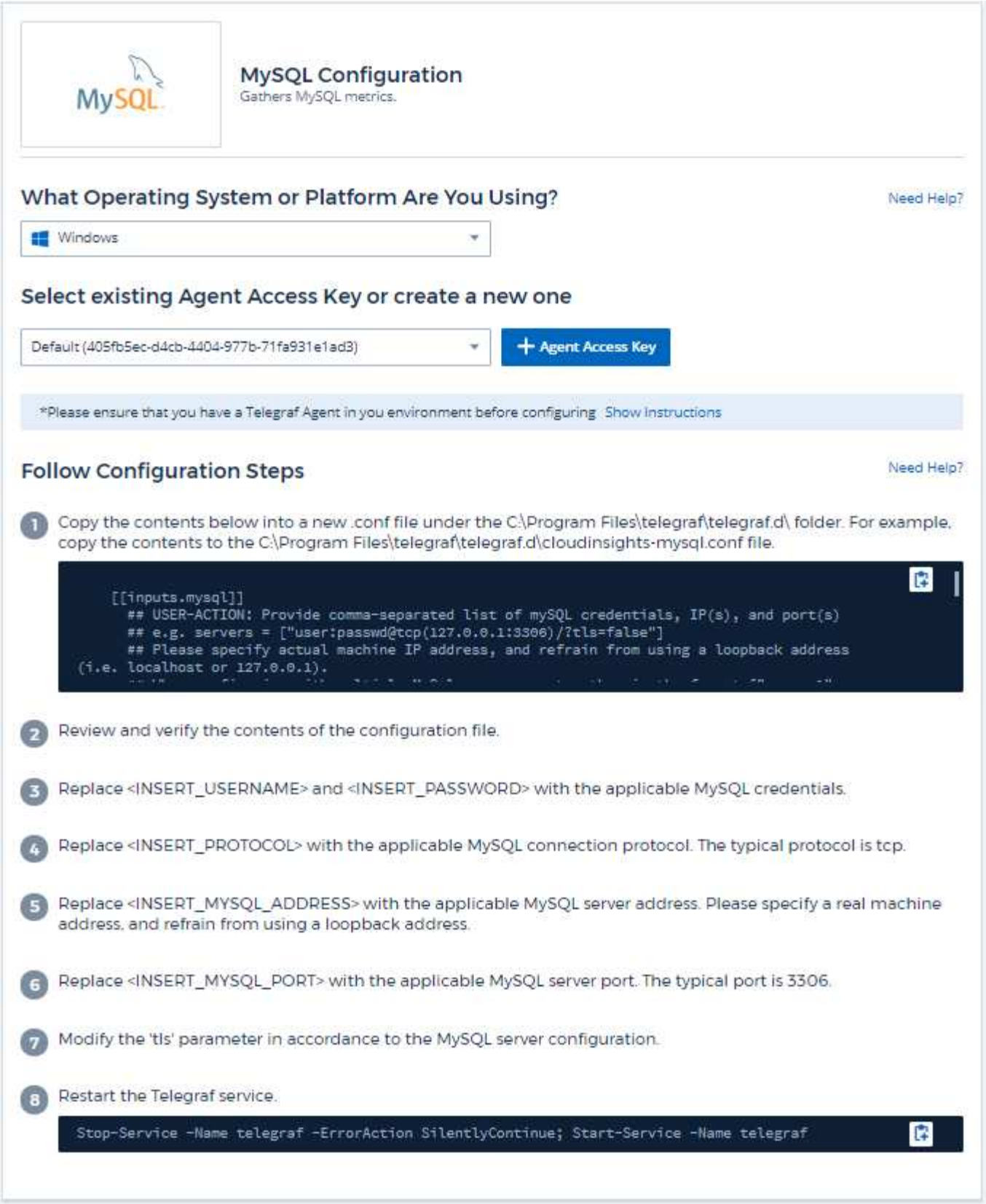
Cloud Insights utilizza questo data collector per raccogliere metriche da MySQL.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegli MySQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione MySQL".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
MySQL	Namespace server MySQL	Nome nodo IP	Client interrotti (per sec) connessioni interrotte (per sec) byte RX (per sec) byte TX (per sec) comandi Admin (per sec) Comandi Alter comandi evento Alter comandi funzione Alter comandi istanza Alter comandi procedura Alter comandi server comandi Alter comandi tabella Alter comandi tablespace Alter comandi utente Analyze comandi Assegna a Keycache comandi Begin comandi Binlog comandi procedura di chiamata comandi Cambia comandi DB Cambia comandi master Cambia comandi filtro Repl comandi di controllo Comandi checksum comandi commit Crea comandi DB Crea comandi evento Crea comandi funzione Crea comandi indice Crea comandi procedura Crea comandi server Crea comandi tabella Crea comandi trigger Crea comandi UDF Crea comandi utente Crea comandi Visualizza Dealloc SQL errori di connessione Accetta tabelle dischi tmp creati errori ritardati comandi Flush Handler Commit InnoDB buffer Pool byte Data Key Blocks Not Flushed Key Requests Key Write Key Write Max Execution Time Exceeded Max Connections Open Files Performance Schema Accounts Lost Prepared stmt Count Qcache Free Blocks Questions Select Full Join Select Full Range Join Select Range Check Selezionare Scan Table Locks immediate (blocco immediato tavolo di

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Netstat Data Collector

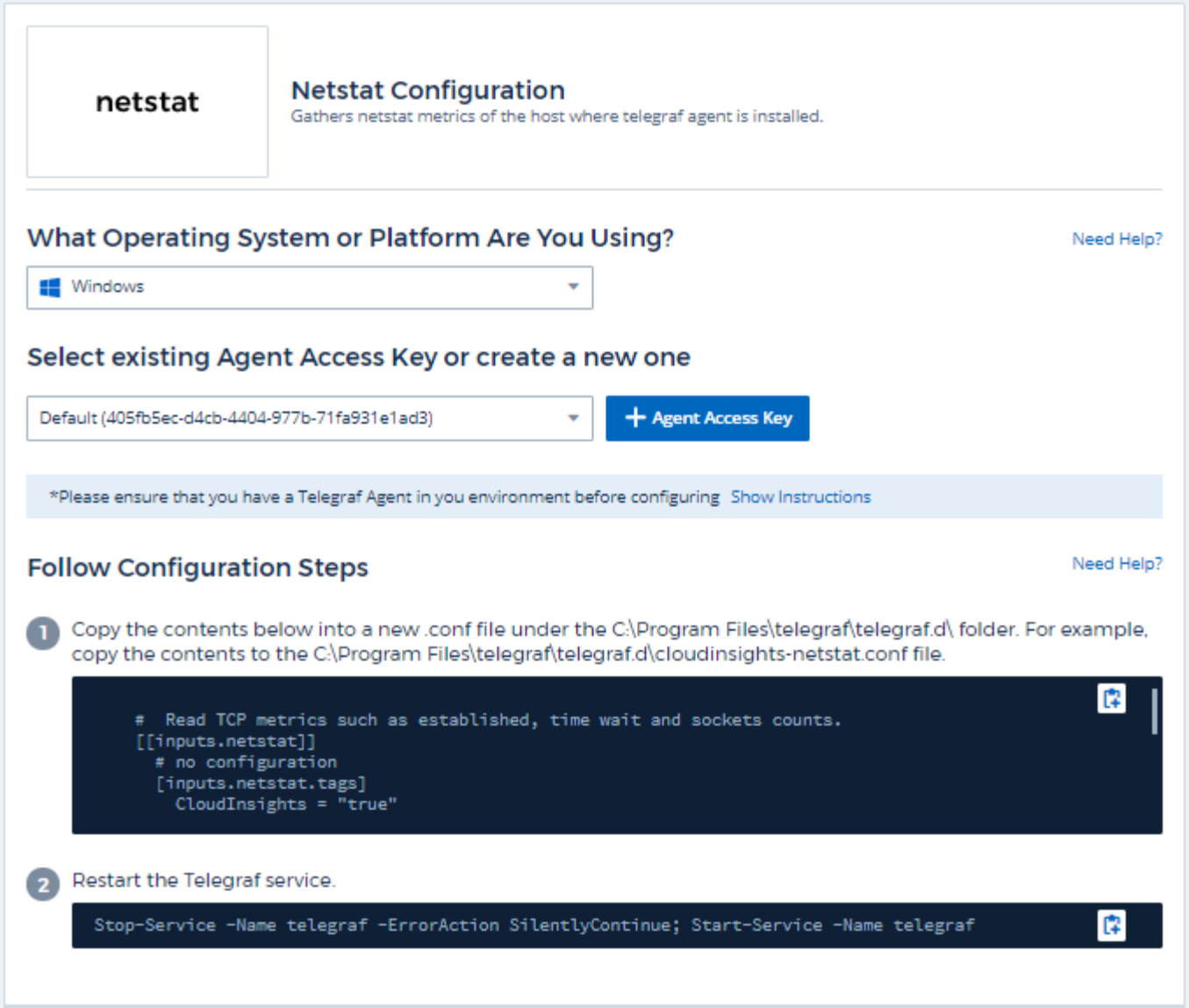
Cloud Insights utilizza questo data collector per raccogliere le metriche Netstat.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Netstat.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Netstat	UUID nodo	Nome nodo IP	

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Data Collector nginx

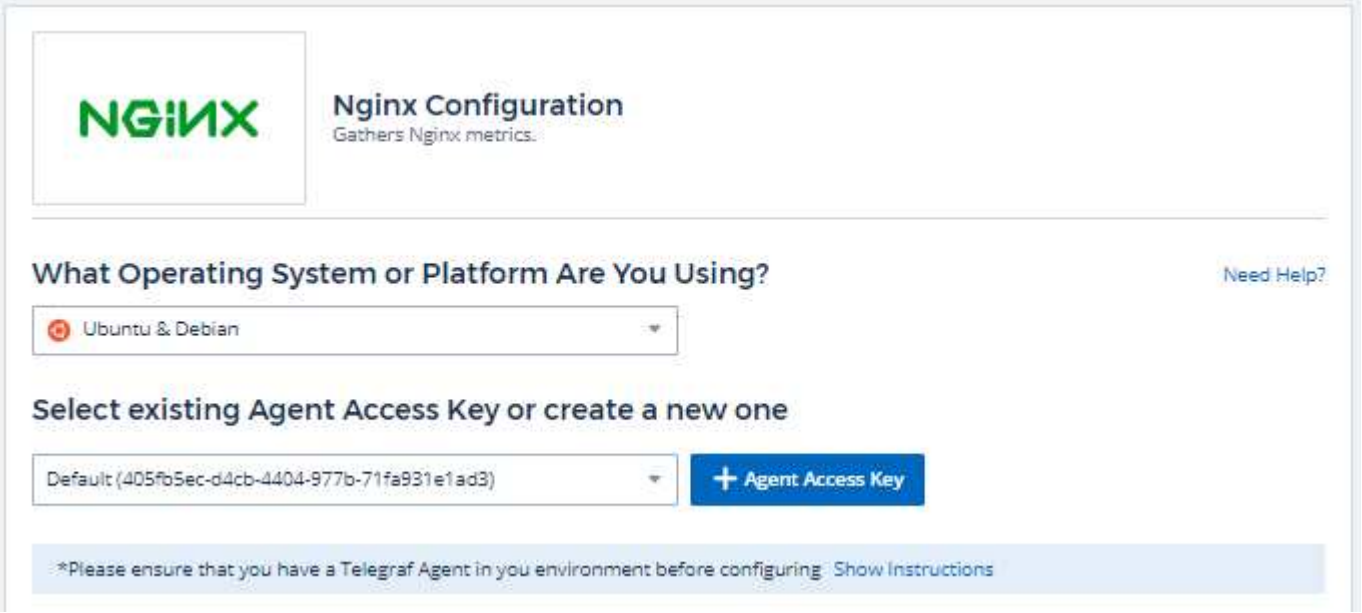
Cloud Insights utilizza questo data collector per raccogliere metriche da Nginx.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Nginx.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Follow Configuration Steps

Need Help?

1. If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.

2. Nginx metrics are available through a status page when the HTTP stub status module is enabled.Refer to the below link for verifying/enabling http_stub_status_module.

```
http://nginx.org/en/docs/http/ngx_http_stub_status_module.html
```

3. After verifying the module is enabled ,modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {
   listen   <PORT NUMBER>;
   Please specify actual machine IP address, and refrain from using a loopback address (i.e.
localhost or 127.0.0.1)
   server_name  <IP ADDRESS>;
   location /nginx_status {
```

4. Reload the configuration:

```
nginx -s reload
```

5. Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-nginx.conf file.

```
    [[inputs.nginx]]
      ## USER-ACTION: Provide Nginx status url
      ## Please specify actual machine IP address where nginx_status is enabled, and refrain from
using a loopback address (i.e. localhost or 127.0.0.1).
      ## When configuring with multiple Nginx servers, enter them in the format ["url1" ,"url2",
```

6. Replace <INSERT_NGINX_ADDRESS> with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.

7. Replace <INSERT_NGINX_PORT> with the applicable Nginx port.

8. Restart the Telegraf service.

```
systemctl restart telegraf
```

Setup (Configurazione)

La raccolta di metriche nginx richiede che Nginx "http_stub_status_module" essere attivato.

Per ulteriori informazioni, consultare "Documentazione nginx".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Nginx	Server namespace	Nodo IP Node Name Port (porta nome nodo IP)	Accetta richieste di lettura gestite attive in attesa di scrittura

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

PostgreSQL Data Collector

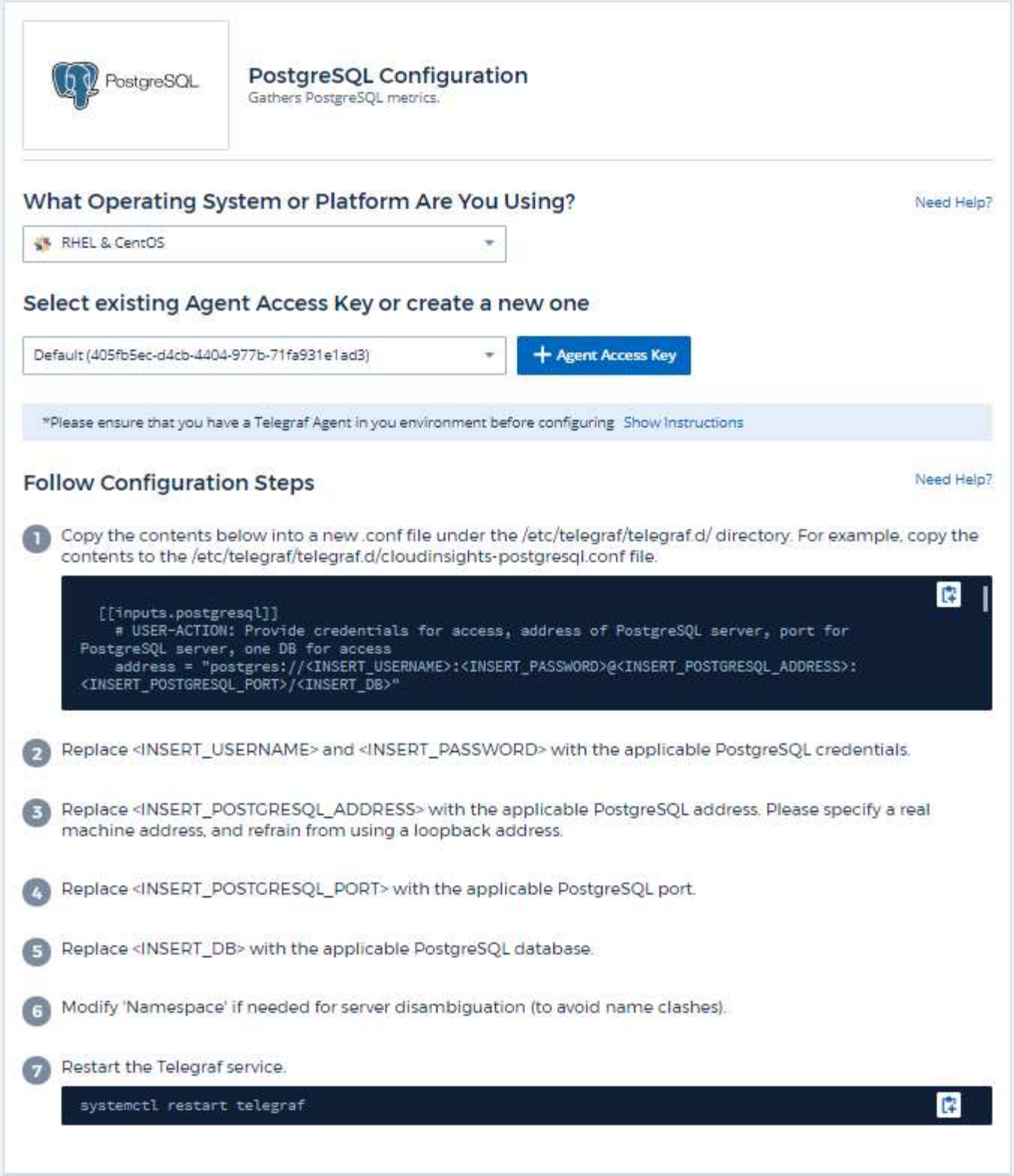
Cloud Insights utilizza questo data collector per raccogliere le metriche da PostgreSQL.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere PostgreSQL.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione PostgreSQL".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Server PostgreSQL	Server database namespace	Nome nodo IP nodo	Buffer allocati buffer backend buffer di sincronizzazione file backend buffer di controllo buffer di controllo punti di controllo puliti punti di controllo di sincronizzazione tempo di scrittura punti di controllo Richieste punti di controllo Timed Max scritto pulito
Database PostgreSQL	Server database namespace	Database OID Node Name Node IP	Blocchi di tempo di lettura blocchi di tempo di scrittura blocchi di accessi blocchi di lettura conflitti deadlock numero di client file di temperatura byte file di temperatura numero di righe cancellate righe recuperate righe inserite righe restituite transazioni aggiornate transazioni impegnate operazioni supportate dal rollback

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Puppet Agent Data Collector

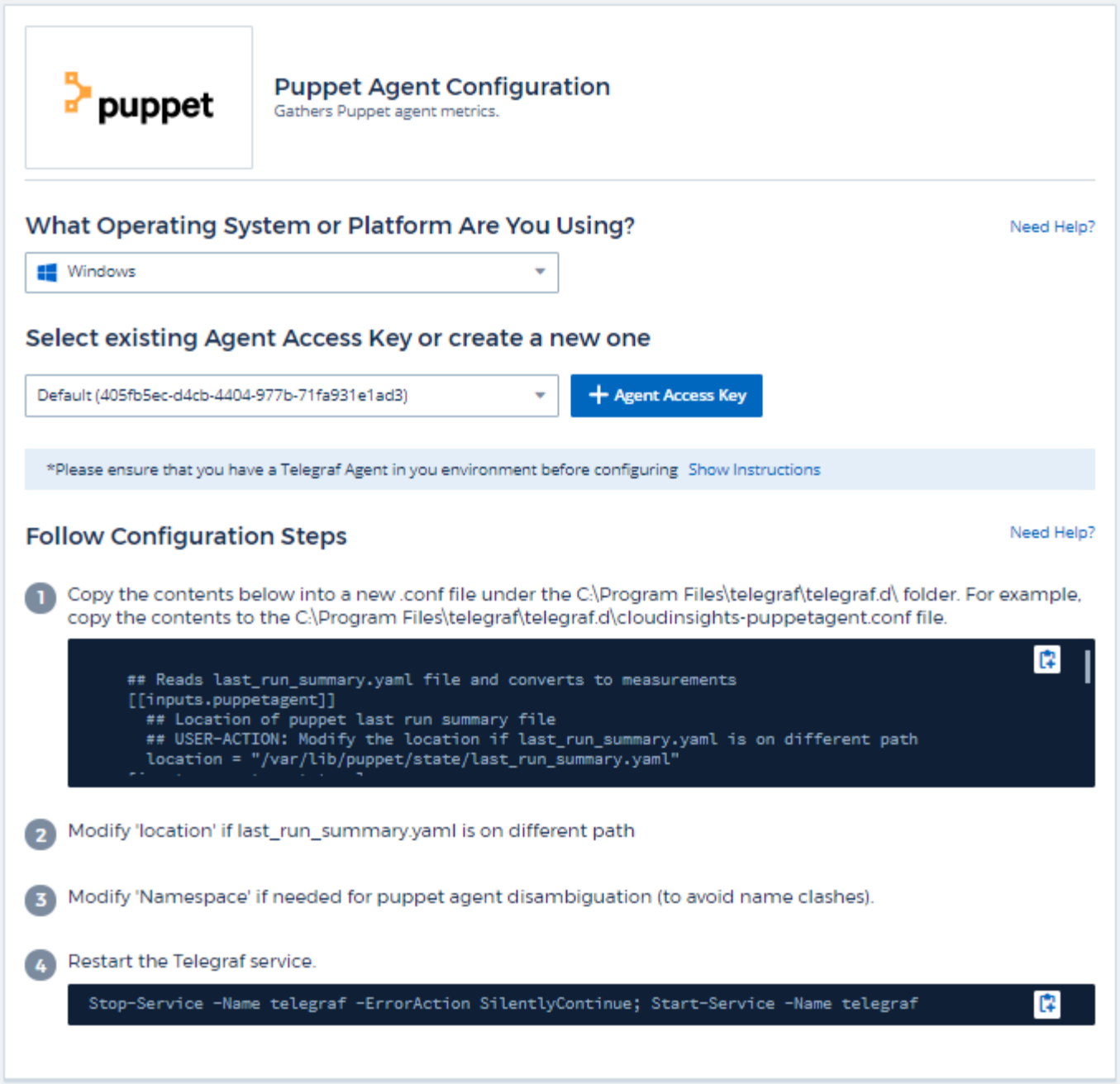
Cloud Insights utilizza questo data collector per raccogliere le metriche dall'Agente di Puppet.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Puppet.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione delle marionette"

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:

Agente di puppet	UUID nodo spazio dei nomi	Nome nodo posizione nodo versione IP stringa di configurazione versione Puppet	Modifiche eventi totali Eventi di errore Eventi di successo risorse totali risorse modificate risorse non riuscite riavvio risorse risorse Outofsync risorse riavviate risorse pianificate risorse ignorate tempo totale di ancoraggio tempo di recupero tempo di configurazione tempo di esecuzione tempo di esecuzione tempo di esecuzione file tempo di caricamento tempo di esecuzione tempo di esecuzione tempo tempo di esecuzione tempo tempo tempo di servizio tempo di gestione tempo totale Time User

Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Redis Data Collector

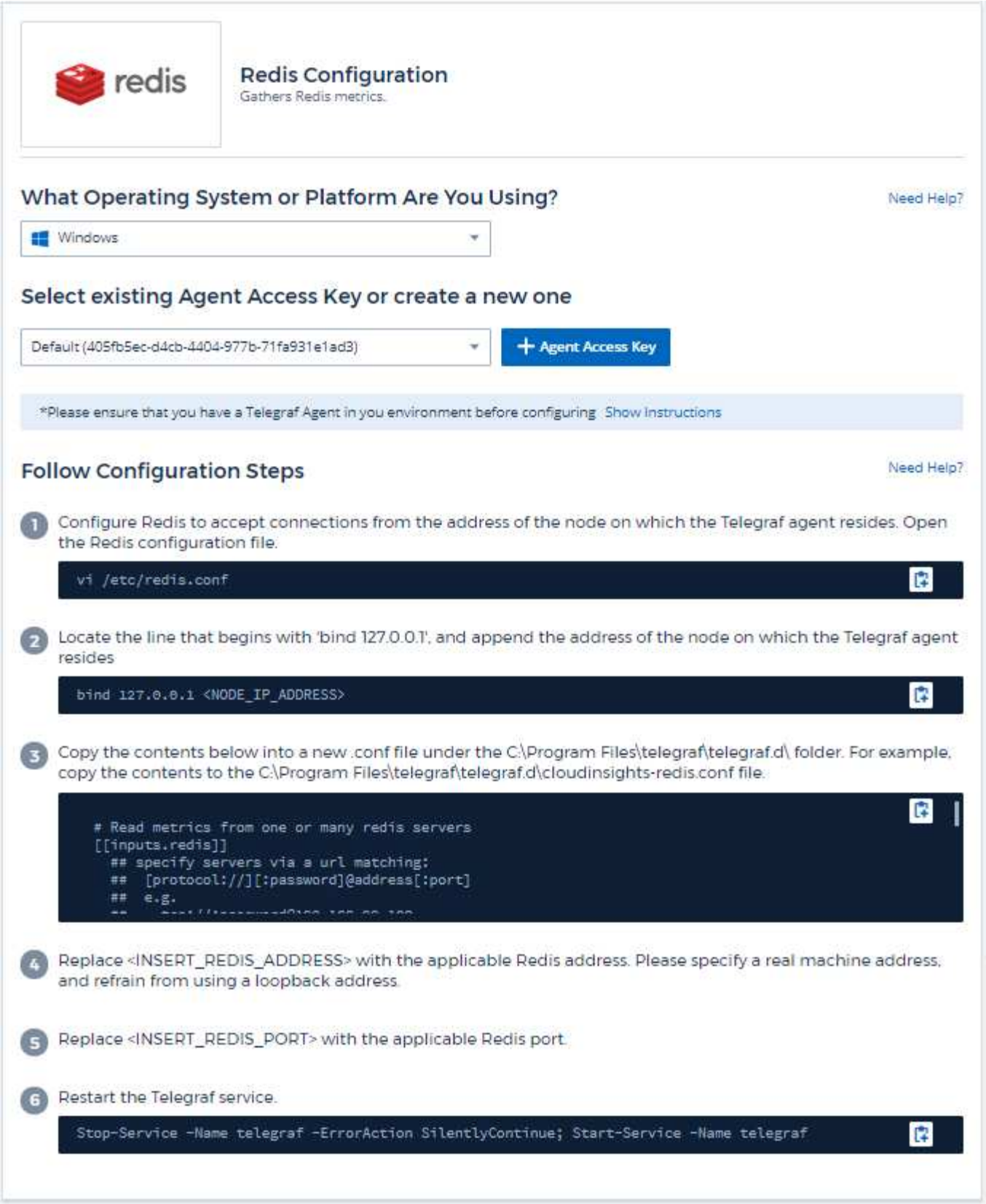
Cloud Insights utilizza questo data collector per raccogliere metriche da Redis. Redis è un archivio di strutture di dati in-memory open source utilizzato come database, cache e message broker, che supporta le seguenti strutture di dati: Stringhe, hash, elenchi, set e molto altro.

Installazione

1. Da **osservabilità > Collector**, fare clic su **+Data Collector**. Scegliere Redis.

   Selezionare il sistema operativo o la piattaforma su cui è installato Telegraf Agent.

2. Se non è già stato installato un Agent per la raccolta o se si desidera installare un Agent per un sistema operativo o una piattaforma differente, fare clic su *Show Instructions* (Mostra istruzioni) per espandere la "Installazione dell'agente" istruzioni.
3. Selezionare il tasto di accesso dell'agente da utilizzare con questo data collector. È possibile aggiungere un nuovo Agent Access Key facendo clic sul pulsante **+ Agent Access Key**. Best practice: Utilizzare un Agent Access Key diverso solo quando si desidera raggruppare i data raccoglitori, ad esempio per sistema operativo/piattaforma.
4. Seguire la procedura di configurazione per configurare il data collector. Le istruzioni variano a seconda del tipo di sistema operativo o piattaforma utilizzata per la raccolta dei dati.



Setup (Configurazione)

Le informazioni sono disponibili in "Documentazione Redis".

Oggetti e contatori

Vengono raccolti i seguenti oggetti e i relativi contatori:

Oggetto:	Identificatori:	Attributi:	Punti dati:
Redis	Server namespace		

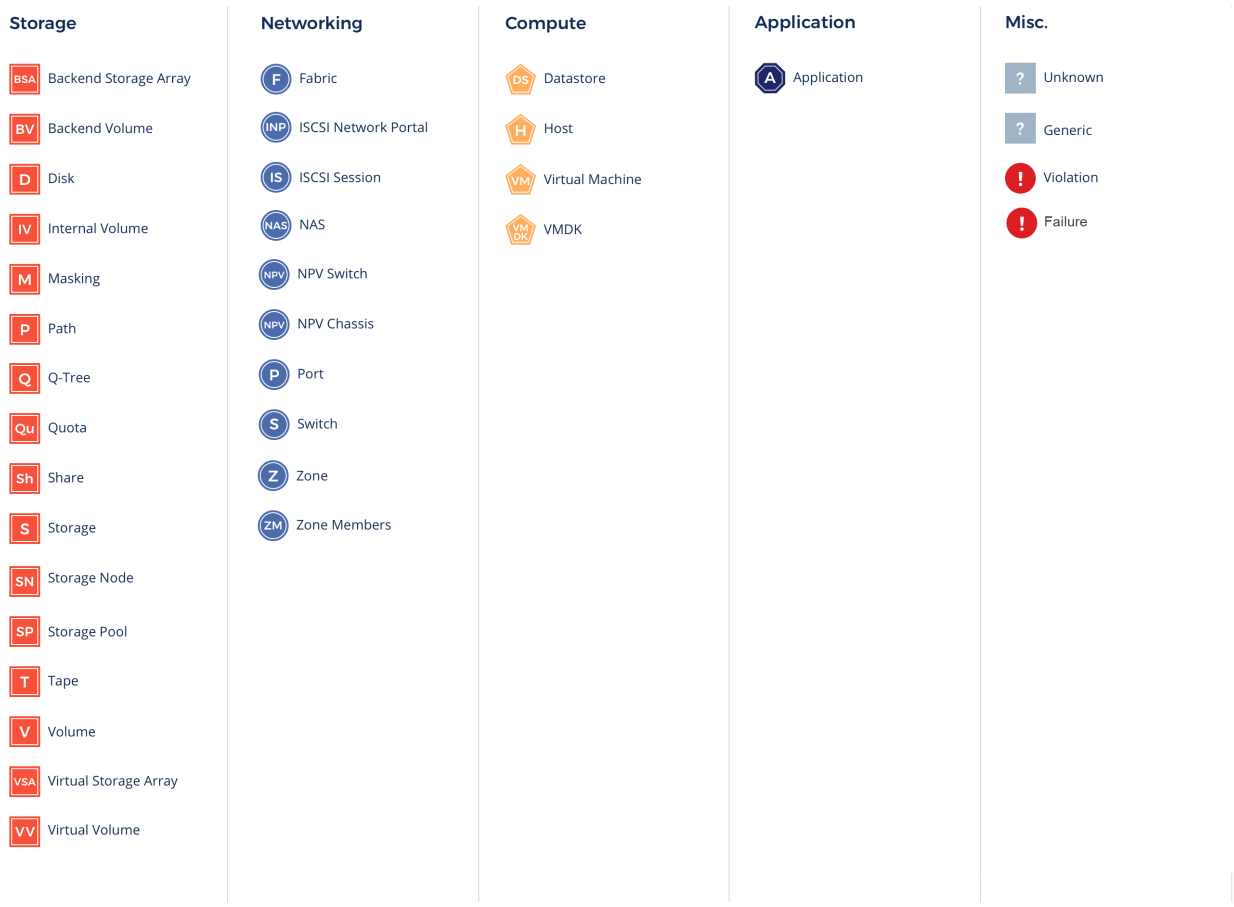
Risoluzione dei problemi

Per ulteriori informazioni, consultare "Supporto" pagina.

Riferimento icona oggetto

Un riferimento rapido per le icone degli oggetti utilizzate in Cloud Insights.

Icone dell'infrastruttura:



Icone Kubernetes:

Icone mappa e monitoraggio delle performance di rete di Kubernetes:

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

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per Cloud Insights"
"Avviso per la sicurezza del carico di lavoro (in precedenza Cloud Secure)"