Monitor e avvisi

Data Infrastructure Insights

NetApp
February 03, 2026

Sommario

Monitor e avvisi . . . 1
- Avvisi con monitor . . . 1
  - Migliori pratiche di sicurezza . . . 1
  - Monitoraggio metrico o log? . . . 1
  - Elenco monitor . . . 8
  - Gruppi di monitoraggio . . . 8
  - Monitor definiti dal sistema . . . 11
- Visualizzazione e gestione degli avvisi dai monitor . . . 11
  - Visualizzazione e gestione degli avvisi . . . 11
  - Pannello dettagli avviso . . . 12
  - Avvisi quando mancano dati . . . 13
  - Avvisi "Permanentemente attivi" . . . 14
- Configurazione delle notifiche e-mail . . . 14
  - Destinatari della notifica di abbonamento . . . 14
  - Elenco globale dei destinatari per gli avvisi . . . 15
  - Modifica delle notifiche per ONTAP . . . 15
- Monitor di rilevamento delle anomalie . . . 17
  - Che cos’è il rilevamento delle anomalie? . . . 17
  - Quando avrei bisogno del rilevamento delle anomalie? . . . 18
  - Creazione di un monitor di rilevamento delle anomalie . . . 18
  - Visualizzazione delle anomalie . . . 20
- Monitor di sistema . . . 21
  - Descrizioni del monitor . . . 22
  - Ulteriori informazioni . . . 100
- Notifiche webhook . . . 100
  - Notifica tramite webhook . . . 100
  - Esempio di webhook per Discord . . . 104
  - Esempio di webhook per PagerDuty . . . 106
  - Esempio di webhook per Slack . . . 110
  - Esempio di webhook per Microsoft Teams . . . 112

Monitor e avvisi

Avvisi con monitor

Configura i monitor per monitorare le soglie di prestazione, registrare eventi e anomalie nelle risorse della tua infrastruttura. Crea avvisi personalizzati per parametri quali latenza di scrittura del nodo, capacità di archiviazione o prestazioni dell'applicazione e ricevi notifiche quando queste condizioni vengono soddisfatte.

I monitor consentono di impostare soglie sulle metriche generate da oggetti "infrastrutturali" quali storage, VM, EC2 e porte, nonché per dati di "integrazione" come quelli raccolti per Kubernetes, metriche avanzate ONTAP e plugin Telegraf. Questi monitor *metrici* ti avvisano quando vengono superate le soglie di livello di attenzione o di livello critico.

È anche possibile creare monitor per attivare avvisi di livello di avvertenza, critici o informativi quando vengono rilevati specifici *eventi di registro*.

Data Infrastructure Insights fornisce una serie di"Monitor definiti dal sistema" anche in base all'ambiente.

Migliori pratiche di sicurezza

Gli avvisi di Data Infrastructure Insights sono progettati per evidenziare punti dati e tendenze sul tenant e Data Infrastructure Insights consente di immettere qualsiasi indirizzo e-mail valido come destinatario dell'avviso. Se lavori in un ambiente sicuro, fai particolare attenzione a chi riceve la notifica o ha accesso all'avviso.

Monitoraggio metrico o log?

1. Dal menu Data Infrastructure Insights , fare clic su **Avvisi > Gestisci monitoraggi**

   Viene visualizzata la pagina 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 delle metriche o un monitor dei registri.

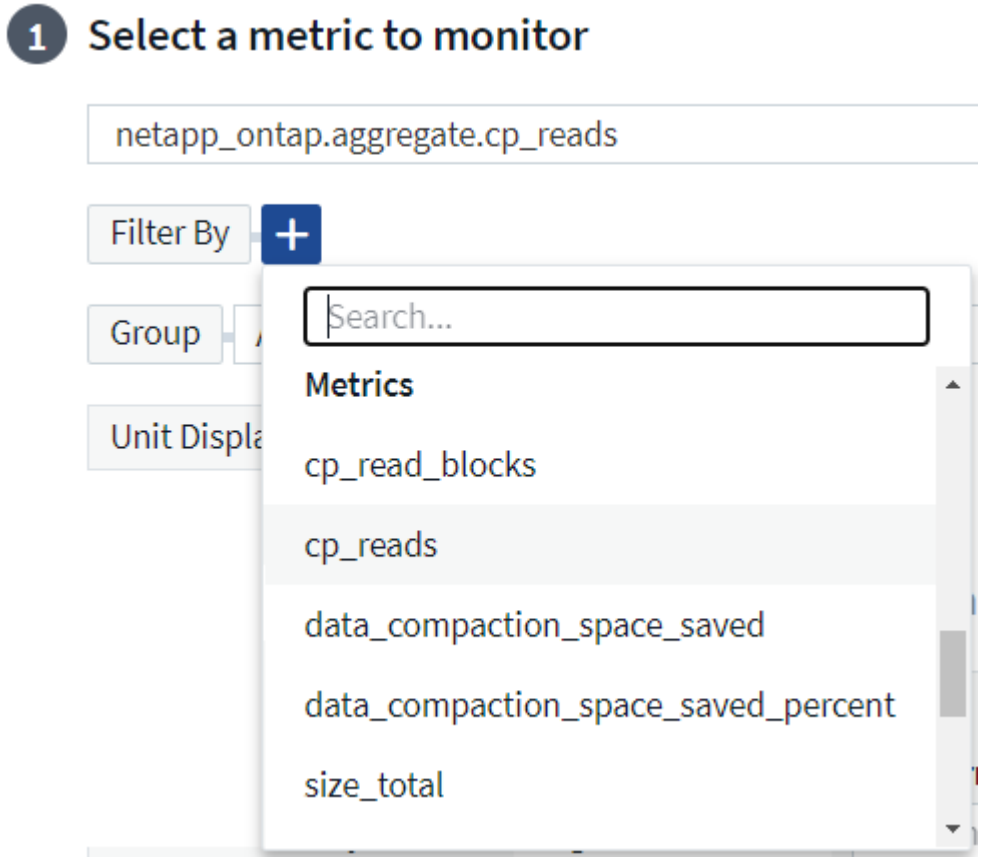
- *Metric* monitora gli avvisi sui trigger correlati all'infrastruttura o alle prestazioni
- *Log* monitora gli avvisi sulle attività correlate al registro

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 desidera creare.

Monitor metrico

1. Nel menu a discesa, cerca e scegli un tipo di oggetto e una metrica da monitorare.

È possibile impostare filtri per restringere il campo degli attributi o delle metriche degli oggetti da monitorare.



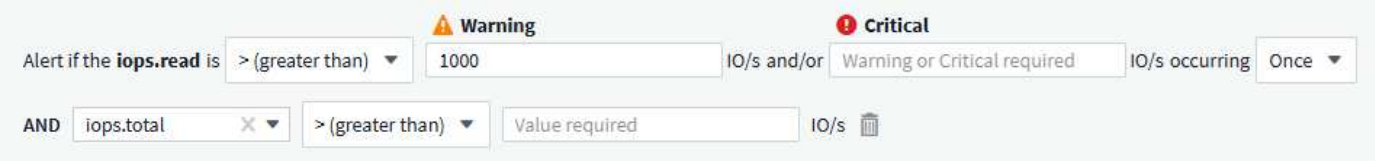
Quando si lavora con dati di integrazione (Kubernetes, ONTAP Advanced Data, ecc.), il filtraggio delle metriche rimuove i punti dati individuali/non corrispondenti dalla serie di dati tracciati, a differenza dei dati dell'infrastruttura (archiviazione, VM, porte, ecc.) in cui i filtri agiscono sul valore aggregato della serie di dati e potenzialmente rimuovono l'intero oggetto dal grafico.

I monitor delle metriche si applicano agli oggetti di inventario quali storage, switch, host, VM, ecc., nonché alle metriche di integrazione quali dati ONTAP Advanced o Kubernetes. Quando si monitorano gli oggetti dell'inventario, tenere presente che non è possibile selezionare il metodo "Raggruppa per". Tuttavia, il raggruppamento è consentito durante il monitoraggio dei dati di integrazione.

Monitor multi-condizione

Puoi scegliere di perfezionare ulteriormente il monitoraggio delle metriche aggiungendo una seconda

condizione. Basta espandere il prompt "+Aggiungi condizione metrica secondaria" e configurare la condizione aggiuntiva.



Il monitor emetterà un avviso se entrambe le condizioni sono soddisfatte.

Tieni presente che puoi usare solo l'opzione "AND" per una seconda condizione; non puoi scegliere di ricevere un avviso per una condizione OPPURE per l'altra.

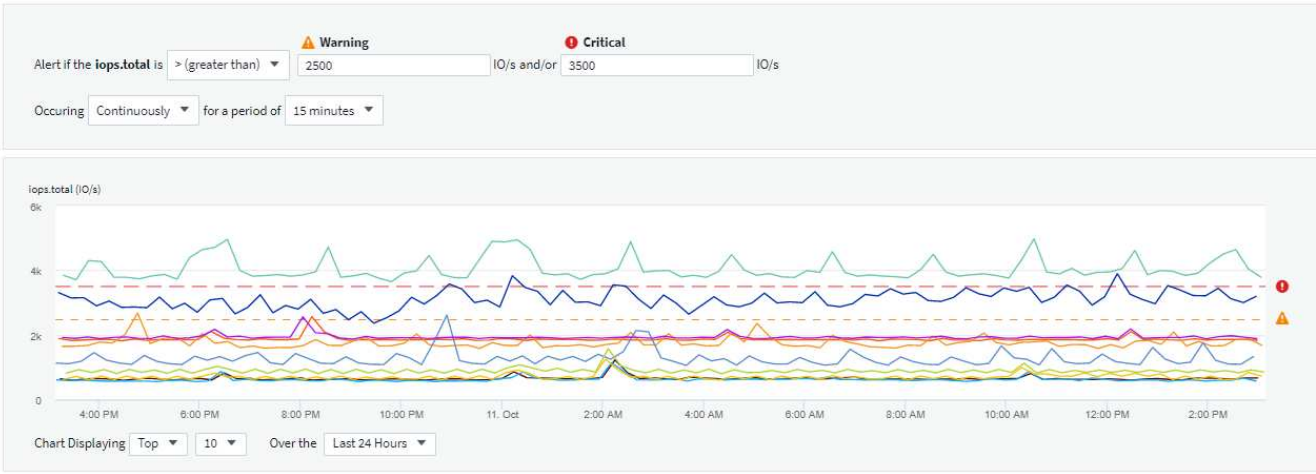
Definire le condizioni del monitor.

1. Dopo aver scelto l'oggetto e la metrica da monitorare, impostare le soglie di livello di avviso e/o di livello critico.
2. Per il livello *Avviso*, immettere 200 per il nostro 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 linee di livello di avviso e critico sul grafico sono una rappresentazione visiva del Monitor, in modo da poter vedere facilmente quando il Monitor potrebbe attivare un avviso in ciascun caso.

4. Per l'intervallo di occorrenza, selezionare *Continuamente* per un periodo di *15 minuti*.

   È possibile scegliere di attivare un avviso nel momento in cui viene superata una soglia oppure attendere che la soglia venga superata in modo continuativo per un determinato periodo di tempo. Nel nostro esempio, non vogliamo essere avvisati ogni volta che il valore IOPS totale supera il livello di avviso o critico, ma solo quando un oggetto monitorato supera continuamente uno di questi livelli per almeno 15 minuti.



Definire il comportamento di risoluzione degli avvisi

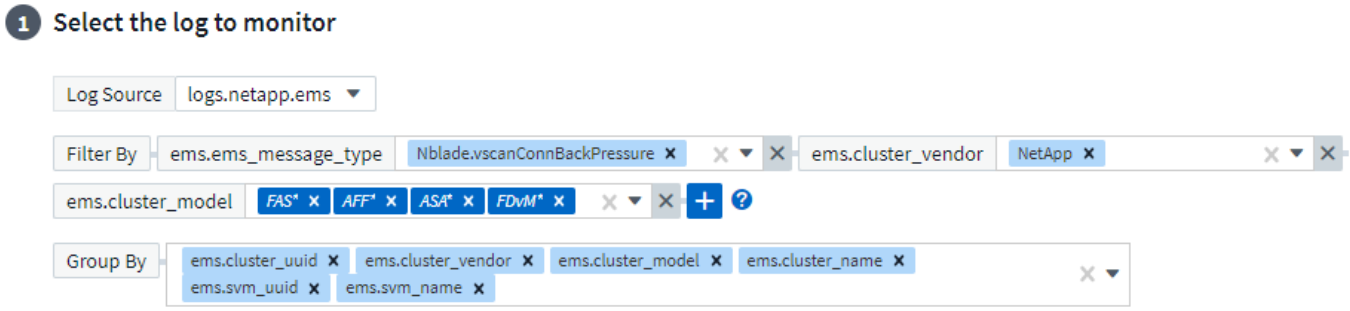
È possibile scegliere come risolvere un avviso di monitoraggio delle metriche. Ti vengono presentate due scelte:

- Risolvere quando la metrica torna nell'intervallo accettabile.
- Risolve quando la metrica rientra nell'intervallo accettabile per un periodo di tempo specificato, da 1 minuto a 7 giorni.

Monitoraggio dei registri

Quando si crea un **monitor dei log**, scegliere innanzitutto quale log monitorare dall'elenco dei log disponibili. È quindi possibile filtrare in base agli attributi disponibili come sopra. È anche possibile scegliere uno o più attributi "Raggruppa per".

Il filtro Log Monitor non può essere vuoto.



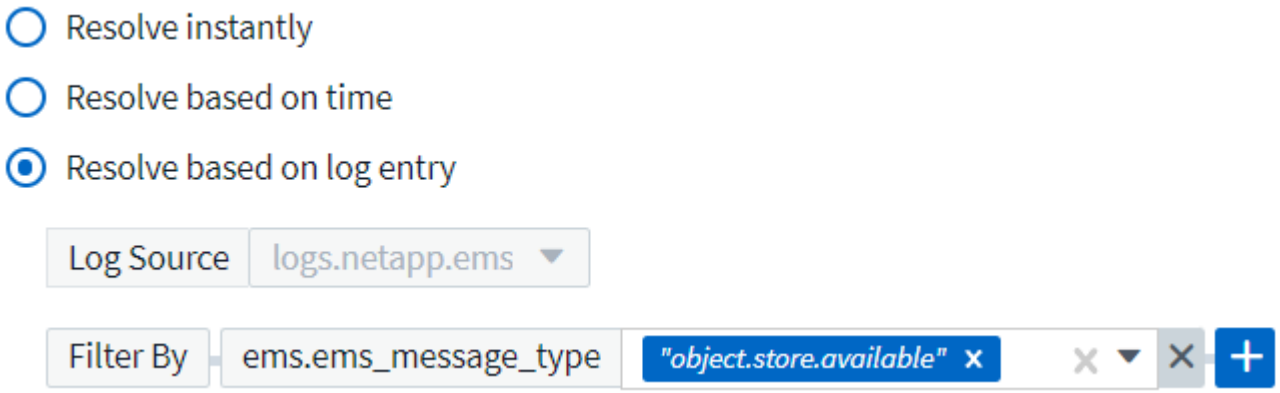
Definisci il comportamento dell'avviso

È possibile creare il monitor in modo che emetta un avviso con un livello di gravità *Critico*, *Avviso* o *Informativo* quando le condizioni definite sopra si verificano una volta (ovvero immediatamente) oppure attendere che l'avviso venga emesso finché le condizioni non si verificano 2 o più volte.

Definire il comportamento di risoluzione degli avvisi

È possibile scegliere come risolvere un avviso del monitoraggio dei log. Ti vengono presentate tre scelte:

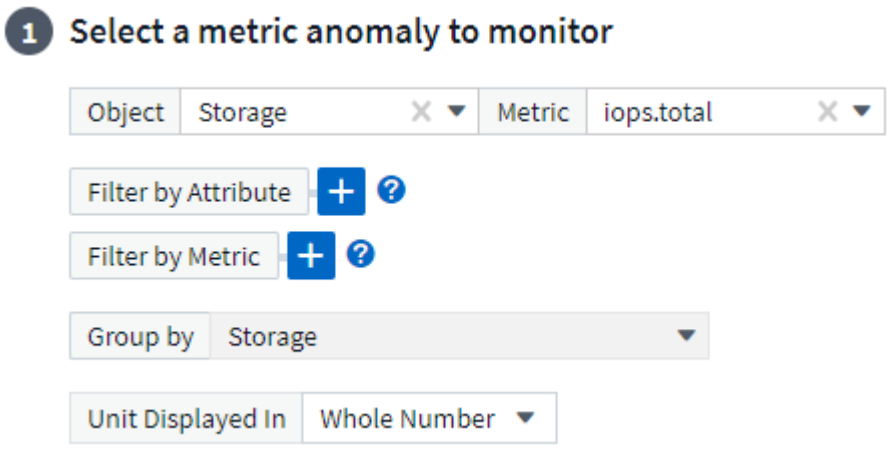
- **Risolvi istantaneamente**: l'avviso viene risolto immediatamente senza bisogno di ulteriori azioni
- **Risolvi in base al tempo**: l'avviso viene risolto dopo che è trascorso il tempo specificato
- **Risolvi in base alla voce di registro**: l'avviso viene risolto quando si verifica un'attività di registro successiva. Ad esempio, quando un oggetto viene registrato come "disponibile".



Monitoraggio del rilevamento delle anomalie

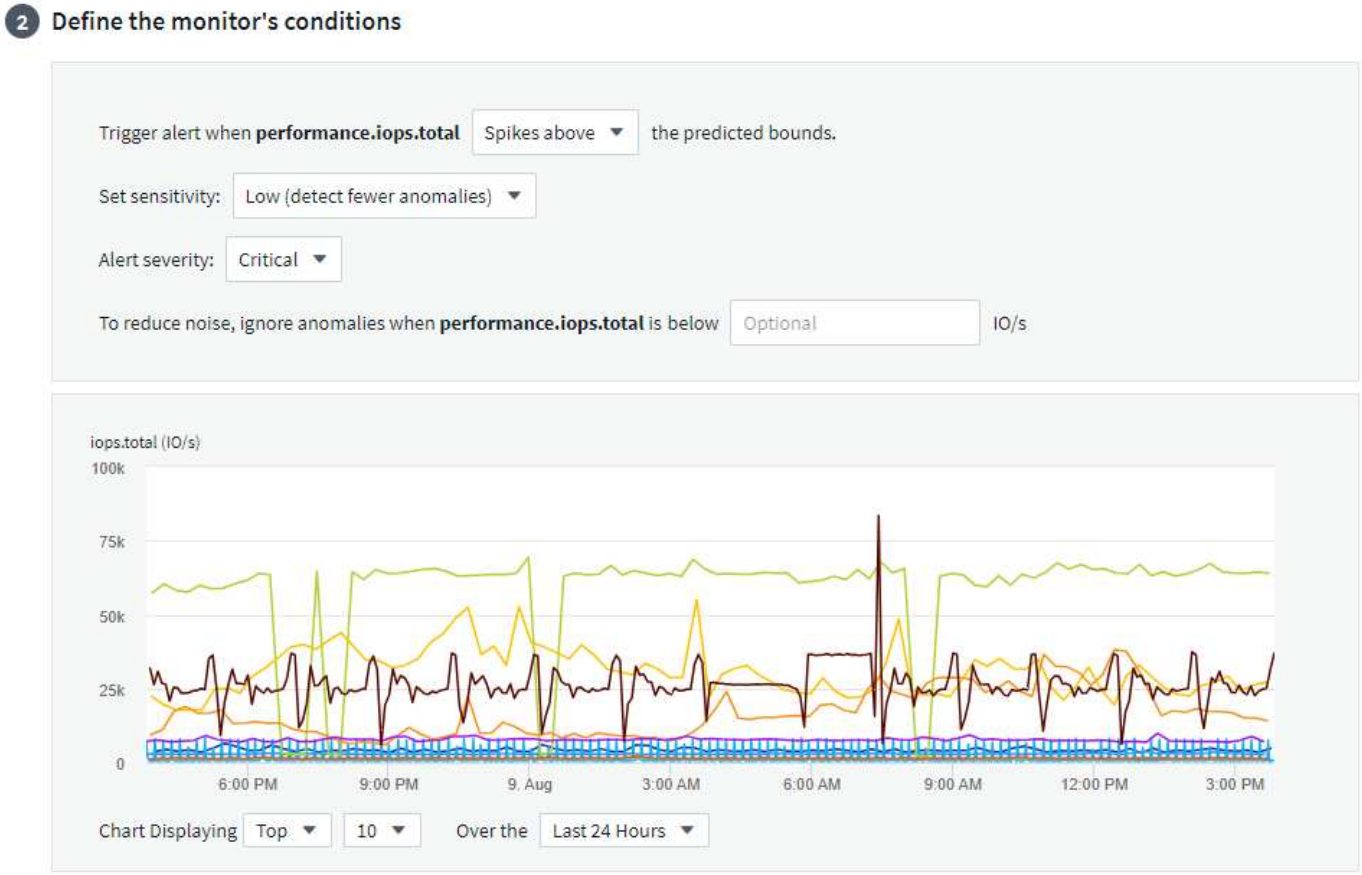
1. Nel menu a discesa, cerca e scegli un tipo di oggetto e una metrica da monitorare.

È possibile impostare filtri per restringere il campo degli attributi o delle metriche degli oggetti da monitorare.



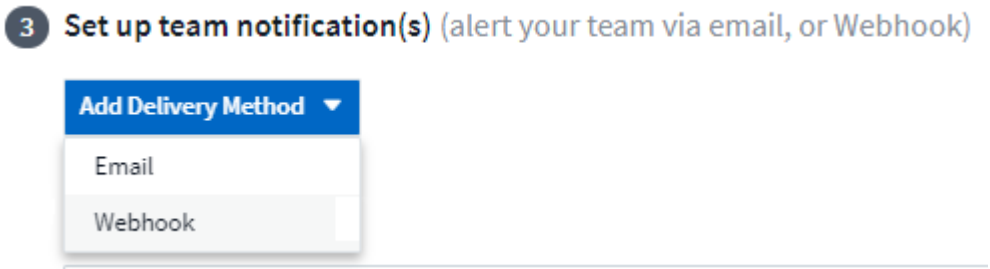
Definire le condizioni del monitor.

1. Dopo aver scelto l'oggetto e la metrica da monitorare, è necessario impostare le condizioni in cui viene rilevata un'anomalia.
   - Scegli se rilevare un'anomalia quando la metrica scelta **supera di un picco** i limiti previsti, **scende di un picco** rispetto a tali limiti oppure **supera di un picco o scende di un picco** rispetto ai limiti.
   - Imposta la **sensibilità** del rilevamento. **Basso** (vengono rilevate meno anomalie), **Medio** o **Alto** (vengono rilevate più anomalie).
   - Imposta gli avvisi come **Avviso** o **Critico**.
   - Se lo si desidera, è possibile scegliere di ridurre il rumore, ignorando le anomalie quando la metrica scelta è al di sotto di una soglia impostata.



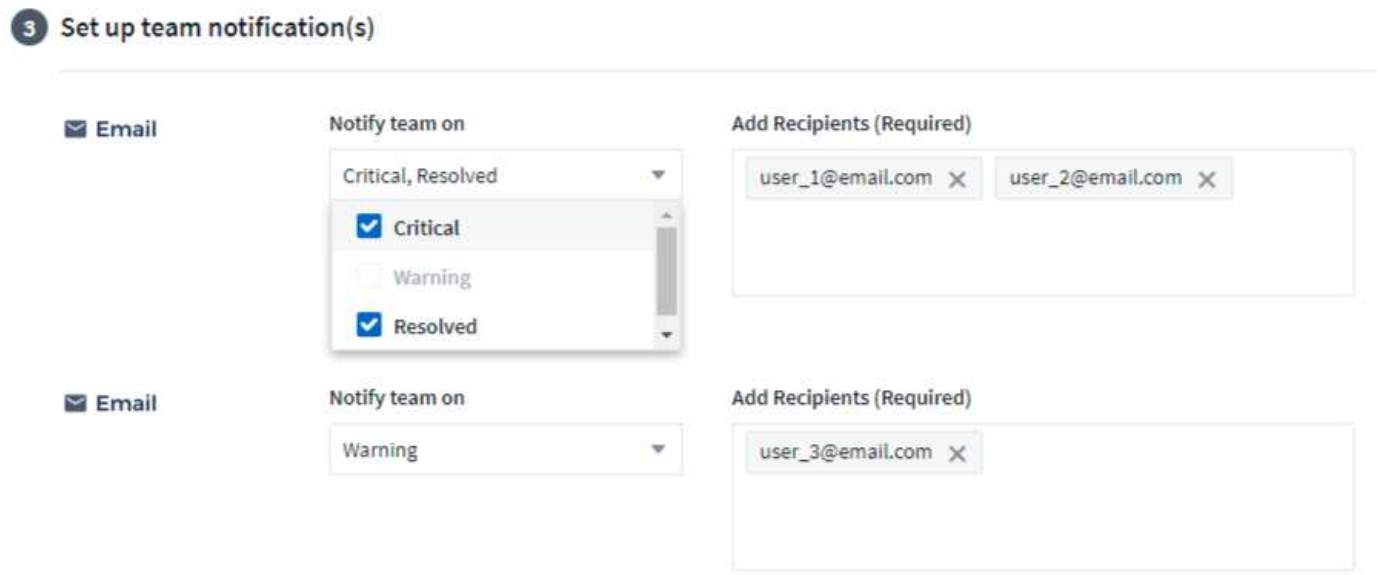
Seleziona il tipo di notifica e i destinatari

Nella sezione *Imposta notifiche al team* puoi scegliere se avvisare il tuo team tramite e-mail o Webhook.



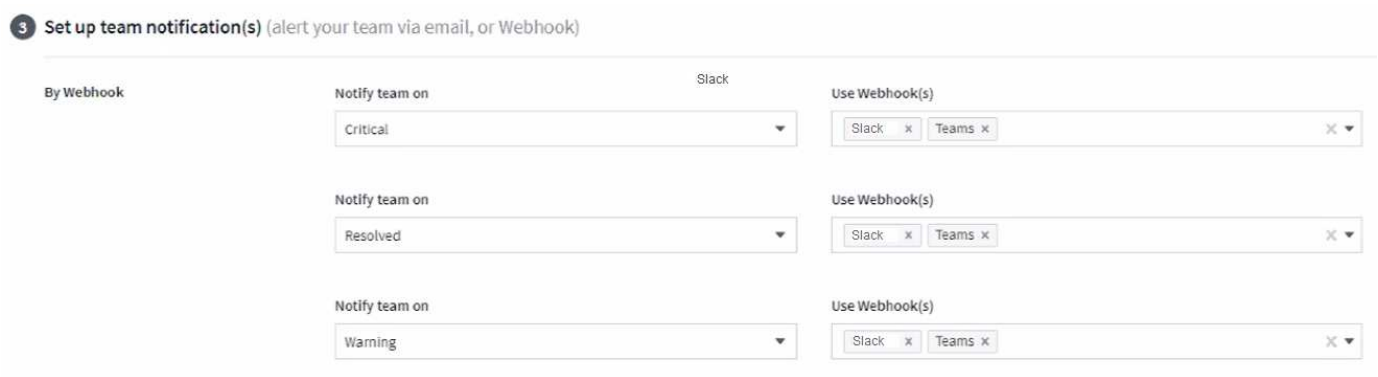
Avviso via e-mail:

Specificare i destinatari e-mail per le notifiche di avviso. Se lo desideri, puoi scegliere destinatari diversi per gli avvisi di avviso o gli avvisi critici.



Avviso tramite Webhook:

Specificare i webhook per le notifiche di avviso. Se lo desideri, puoi scegliere webhook diversi per avvisi di avviso o critici.



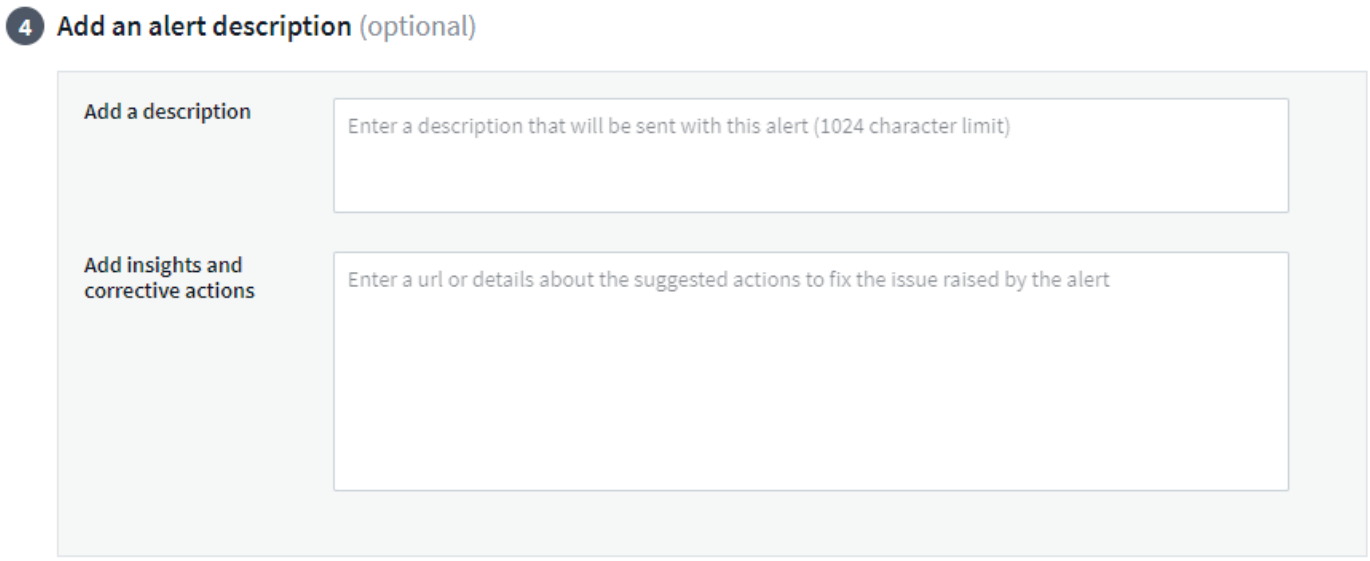
Le notifiche di ONTAP Data Collector hanno la precedenza su qualsiasi notifica specifica di Monitor pertinente al cluster/data collector. L'elenco dei destinatari impostato per il Data Collector riceverà gli avvisi del Data Collector. Se non sono presenti avvisi attivi del raccoglitore dati, gli avvisi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

Impostazione di azioni correttive o informazioni aggiuntive

È possibile aggiungere una descrizione facoltativa, nonché ulteriori approfondimenti e/o azioni correttive compilando la sezione **Aggiungi una descrizione dell'avviso**. La descrizione può contenere fino a 1024 caratteri e verrà inviata insieme all'avviso. Il campo approfondimenti/azioni correttive può contenere fino a 67.000 caratteri e verrà visualizzato nella sezione di riepilogo della landing page dell'avviso.

In questi campi è possibile fornire note, link o passaggi da seguire per correggere o altrimenti gestire l'avviso.

È possibile aggiungere qualsiasi attributo dell'oggetto (ad esempio, il nome dell'archivio) come parametro alla descrizione di un avviso. Ad esempio, è possibile impostare i parametri per il nome del volume e il nome dell'archiviazione in una descrizione come: "Latenza elevata per volume: *%%relatedObject.volume.name%%*, Archiviazione: *%%relatedObject.storage.name%%*".



Salva il tuo monitor

1. Se lo si desidera, è possibile aggiungere una descrizione del monitor.
2. Assegna al monitor un nome significativo e fai clic su **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 del monitor
- Stato
- Oggetto/metrica monitorata
- Condizioni del monitor

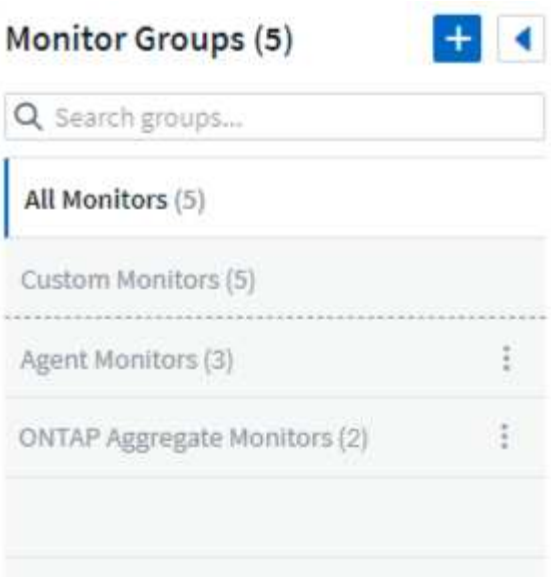
È possibile scegliere di sospendere temporaneamente il monitoraggio di un tipo di oggetto facendo clic sul menu a destra del monitor e selezionando **Pausa**. Quando sei pronto a riprendere il monitoraggio, fai clic su **Riprendi**.

È possibile copiare un monitor selezionando **Duplica** dal menu. È quindi possibile modificare il nuovo monitor e cambiare l'oggetto/la metrica, il filtro, le condizioni, i destinatari delle e-mail, ecc.

Se un monitor non è più necessario, è possibile eliminarlo selezionando **Elimina** dal menu.

Gruppi di monitoraggio

Il raggruppamento consente di visualizzare e gestire i monitor correlati. Ad esempio, è possibile avere un gruppo di monitoraggio dedicato all'archiviazione sul tenant oppure monitor rilevanti per un determinato elenco di destinatari.



Vengono mostrati i seguenti gruppi di monitor. Il numero di monitor contenuti in un gruppo è visualizzato accanto al nome del gruppo.

- **Tutti i monitor** elenca tutti i monitor.
- **Monitor personalizzati** elenca tutti i monitor creati dall'utente.
- **Monitor sospesi** elencherà tutti i monitor di sistema sospesi da Data Infrastructure Insights.
- Data Infrastructure Insights mostrerà anche un numero di **Gruppi di monitoraggio del sistema**, che elencheranno uno o più gruppi di"monitor definiti dal sistema" , inclusi i monitor di infrastruttura e carico di lavoro ONTAP .

I monitor personalizzati possono essere messi in pausa, ripresi, eliminati o spostati in un altro gruppo. I monitor definiti dal sistema possono essere messi in pausa e ripresi, ma non possono essere eliminati o spostati.

Monitor sospesi

Questo gruppo verrà visualizzato solo se Data Infrastructure Insights ha sospeso uno o più monitor. Un monitor può essere sospeso se genera avvisi eccessivi o continui. Se il monitor è personalizzato, modificare le condizioni per impedire l'avviso continuo, quindi riprendere il monitor. Il monitor verrà rimosso dal gruppo Monitor sospesi quando il problema che causa la sospensione sarà risolto.

Monitor definiti dal sistema

Questi gruppi mostreranno i monitor forniti da Data Infrastructure Insights, a condizione che l'ambiente contenga i dispositivi e/o la disponibilità dei registri richiesti dai monitor.

I monitor definiti dal sistema non possono essere modificati, spostati in un altro gruppo o eliminati. 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 (archiviazione, volume, ecc.) o carichi di lavoro (ad esempio monitor di log) o altri gruppi. NetApp valuta costantemente le esigenze dei clienti e le funzionalità dei prodotti e, se necessario, aggiorna o aggiunge funzionalità ai monitor e ai gruppi di sistema.

Gruppi di monitor personalizzati

È possibile creare gruppi personalizzati in cui inserire i monitor in base alle proprie esigenze. Ad esempio, potresti voler creare un gruppo per tutti i monitor correlati all'archiviazione.

Per creare un nuovo gruppo di monitor personalizzato, fare clic sul pulsante **"+" Crea nuovo gruppo di monitor**. Inserisci un nome per il gruppo e clicca su **Crea gruppo**. Viene creato un gruppo vuoto con quel nome.

Per aggiungere monitor al gruppo, vai al gruppo *Tutti i monitor* (consigliato) ed esegui una delle seguenti operazioni:

- Per aggiungere un singolo monitor, fare clic sul menu a destra del monitor e selezionare *Aggiungi al gruppo*. Selezionare 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*.

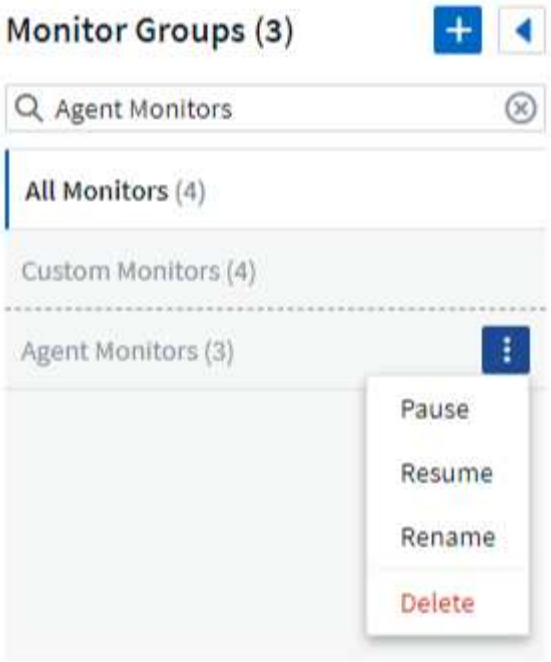
Per rimuovere i monitor, fare clic su un gruppo e selezionare *Rimuovi dal gruppo* dal menu. Non è possibile rimuovere i monitor dal gruppo *Tutti i monitor* o *Monitor personalizzati*. Per eliminare un monitor da questi gruppi, è necessario eliminare il monitor stesso.

La rimozione di un monitor da un gruppo non elimina il monitor da Data Infrastructure Insights. Per rimuovere completamente un monitor, selezionarlo e fare clic su *Elimina*. In questo modo l'utente verrà rimosso anche dal gruppo a cui apparteneva e non sarà più disponibile per nessun altro utente.

È anche possibile spostare un monitor in un gruppo diverso nello stesso modo, selezionando *Sposta nel gruppo*.

Per mettere in pausa o riprendere contemporaneamente tutti i monitor di un gruppo, selezionare il menu del gruppo e fare clic su *Pausa* o *Riprendi*.

Utilizzare lo stesso menu per rinominare o eliminare un gruppo. L'eliminazione di un gruppo non elimina i monitor da Data Infrastructure Insights; sono comunque disponibili in *Tutti i monitor*.



Monitor definiti dal sistema

Data Infrastructure Insights include una serie di monitor definiti dal sistema sia per le metriche che per i log. I monitor di sistema disponibili dipendono dai collettori di dati presenti sul tenant. Per questo motivo, i monitor disponibili in Data Infrastructure Insights potrebbero cambiare man mano che vengono aggiunti raccoglitori di dati o ne vengono modificate le configurazioni.

Visualizza il"Monitor definiti dal sistema" pagina per le descrizioni dei monitor inclusi in Data Infrastructure Insights.

Ulteriori informazioni

- "Visualizzazione e chiusura degli avvisi"

Visualizzazione e gestione degli avvisi dai monitor

Data Infrastructure Insights visualizza avvisi quando"soglie monitorate" vengono superati.

Monitor e avvisi sono disponibili in Data Infrastructure Insights Standard Edition e versioni successive.

Visualizzazione e gestione degli avvisi

Per visualizzare e gestire gli avvisi, procedere come segue.

1. Vai alla pagina **Avvisi > Tutti gli avvisi**.
2. Viene visualizzato un elenco contenente fino ai 1.000 avvisi più recenti. È possibile ordinare questo elenco in base a qualsiasi campo facendo clic sull'intestazione della colonna corrispondente. L'elenco visualizza le seguenti informazioni. Si noti che non tutte queste colonne vengono visualizzate per impostazione predefinita. È possibile selezionare le colonne da visualizzare cliccando sull'icona "ingranaggio":
   - **ID avviso**: ID avviso univoco generato dal sistema

- **Ora di attivazione**: l'ora in cui il monitor pertinente ha attivato l'avviso
- **Gravità attuale** (scheda Avvisi attivi): la gravità attuale dell'avviso attivo
- **Gravità massima** (scheda Avvisi risolti); la gravità massima dell'avviso prima che venisse risolto
- **Monitor**: Il monitor configurato per attivare l'avviso
- **Attivato su**: l'oggetto su cui è stata superata la soglia monitorata
- **Stato**: Stato attuale dell'avviso, *Nuovo* o *In elaborazione*
- **Stato attivo**: *Attivo* o *Risolto*
- **Condizione**: la condizione di soglia che ha attivato l'avviso
- **Metrica**: la metrica dell'oggetto su cui è stata superata la soglia monitorata
- **Stato del monitor**: Stato attuale del monitor che ha attivato l'avviso
- **Ha un'azione correttiva**: l'avviso ha suggerito azioni correttive. Per visualizzarli, apri la pagina degli avvisi.

È possibile gestire un avviso cliccando sul menu a destra dell'avviso e scegliendo una delle seguenti opzioni:

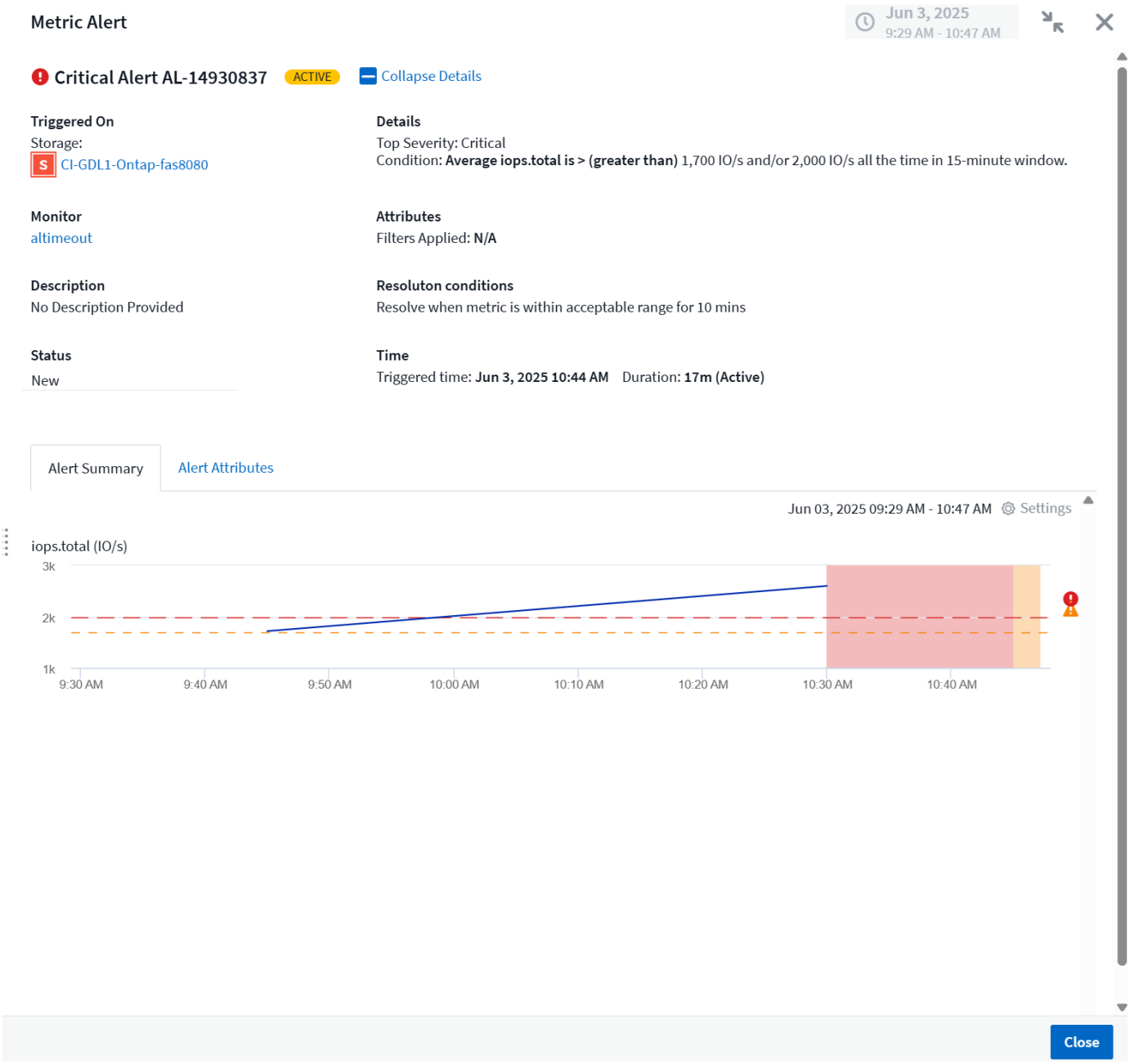
- **In corso** per indicare che l'avviso è sotto inchiesta o che deve comunque essere mantenuto aperto
- **Ignora** per rimuovere l'avviso dall'elenco degli avvisi attivi.

È possibile gestire più avvisi selezionando la casella di controllo a sinistra di ciascun avviso e facendo clic su *Modifica stato avvisi selezionati*.

Facendo clic su un ID avviso si apre la pagina dei dettagli dell'avviso.

Pannello dettagli avviso

Selezionare una riga di avviso per aprire il pannello dei dettagli dell'avviso. Il pannello dei dettagli dell'avviso fornisce ulteriori dettagli sull'avviso, tra cui un *Riepilogo*, una sezione *Prestazioni* che mostra grafici relativi ai dati dell'oggetto, eventuali *Risorse correlate* e *Commenti* inseriti dagli investigatori dell'avviso.



Avvisi quando mancano dati

In un sistema in tempo reale come Data Infrastructure Insights, per avviare l'analisi di un Monitor e decidere se generare un Alert, ci affidiamo a uno di questi due fattori:

- il prossimo punto dati ad arrivare
- un timer da attivare quando non c'è alcun punto dati e hai atteso abbastanza a lungo

Come nel caso di un arrivo lento dei dati, o di nessun arrivo dei dati, il meccanismo del timer deve subentrare poiché la velocità di arrivo dei dati non è sufficiente 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 cosa ho?" Se aspetti troppo a lungo, gli avvisi non verranno generati abbastanza velocemente da risultare utili.

Se si dispone di un Monitor con una finestra di 30 minuti che rileva che una condizione è stata violata dall'ultimo punto dati prima di una perdita di dati a lungo termine, verrà generato un avviso perché il Monitor

non ha ricevuto altre informazioni da utilizzare per confermare il ripristino della metrica o per rilevare che la condizione persiste.

Avvisi "Permanentemente attivi"

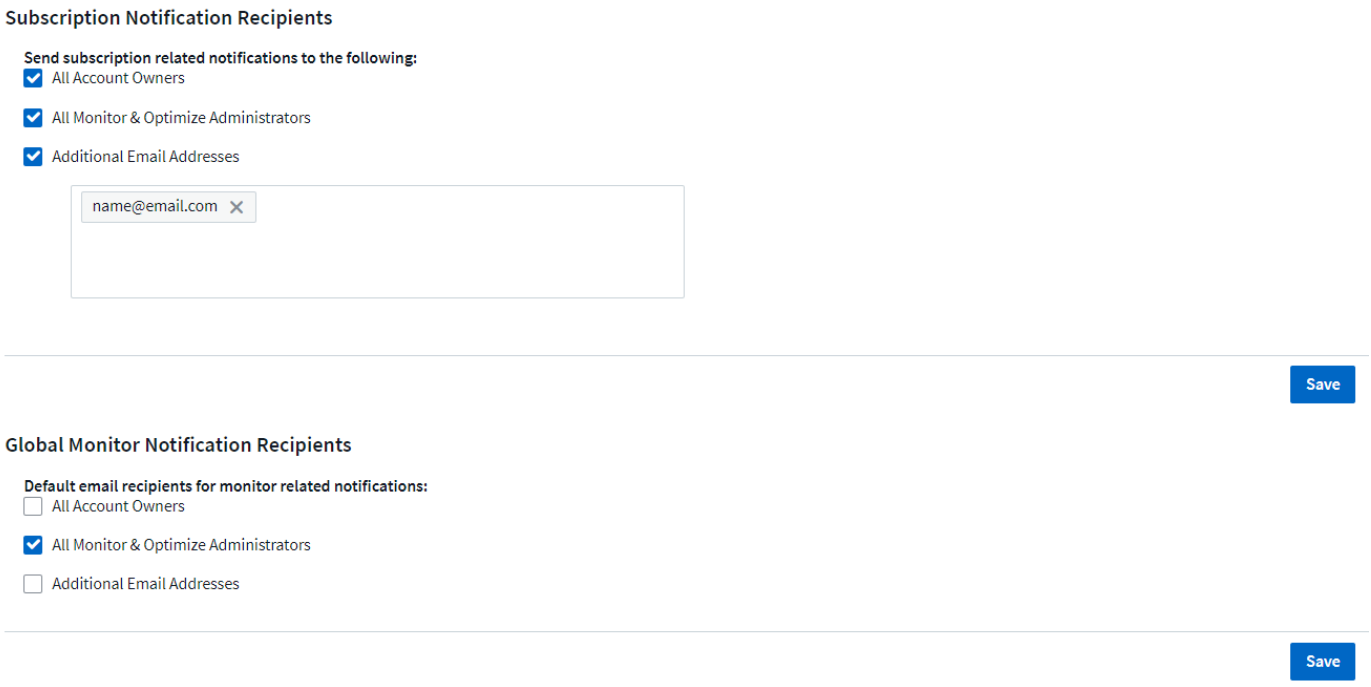
È possibile configurare un monitor in modo che la condizione sia **sempre** presente sull'oggetto monitorato, ad esempio IOPS > 1 o latenza > 0. Spesso vengono creati come monitor "di prova" e poi dimenticati. Tali monitor creano avvisi che rimangono costantemente aperti sugli oggetti costituenti, il che può causare stress al sistema e problemi di stabilità nel tempo.

Per evitare ciò, Data Infrastructure Insights chiuderà automaticamente tutti gli avvisi "permanentemente attivi" dopo 7 giorni. Si noti che le condizioni di monitoraggio sottostanti potrebbero (probabilmente) continuare a sussistere, causando l'emissione quasi immediata di un nuovo avviso, ma questa chiusura degli avvisi "sempre attivi" allevia parte dello stress del sistema che potrebbe altrimenti verificarsi.

Configurazione delle notifiche e-mail

È possibile configurare un elenco di posta elettronica per le notifiche relative agli abbonamenti, nonché un elenco di posta elettronica globale di destinatari per la notifica delle violazioni delle soglie dei criteri di prestazione.

Per configurare le impostazioni del destinatario delle notifiche via e-mail, vai alla pagina **Amministrazione > Notifiche** e seleziona la scheda *E-mail*.



Destinatari della notifica di abbonamento

Per configurare i destinatari delle notifiche degli eventi relativi all'abbonamento, vai alla sezione "Destinatari delle notifiche di abbonamento". Puoi scegliere di inviare notifiche e-mail per gli eventi relativi all'abbonamento a uno o a tutti i seguenti destinatari:

- Tutti i titolari di account

- Tutti gli amministratori di *Monitor & Optimize*
- Indirizzi email aggiuntivi che specifichi

Di seguito sono riportati alcuni esempi dei tipi di notifiche che potrebbero essere inviate e delle azioni che l'utente può intraprendere.

Notifica:	**Azione dell'utente:**
La versione di prova o l'abbonamento sono stati aggiornati	Rivedi i dettagli dell'abbonamento su"Sottoscrizione" pagina
L'abbonamento scadrà tra 90 giorni L'abbonamento scadrà tra 30 giorni	Nessuna azione necessaria se è abilitato il "Rinnovo automatico". Contattare il reparto vendite NetApp per rinnovare l'abbonamento.
Il processo termina tra 2 giorni	Rinnova la prova dal"Sottoscrizione" pagina. È possibile rinnovare la prova una sola volta. Contatta il reparto vendite NetApp per acquistare un abbonamento
La prova o l'abbonamento sono scaduti. L'account smetterà di raccogliere dati tra 48 ore. L'account verrà eliminato dopo 48 ore.	Contatta il reparto vendite NetApp per acquistare un abbonamento

Per assicurarti che i tuoi destinatari ricevano notifiche da Data Infrastructure Insights, aggiungi i seguenti indirizzi email a tutti gli elenchi "consentiti":

- accounts@service.cloudinsights.netapp.com
- DoNotReply@cloudinsights.netapp.com

Elenco globale dei destinatari per gli avvisi

Le notifiche e-mail degli avvisi vengono inviate all'elenco dei destinatari degli avvisi per ogni azione sull'avviso. È possibile scegliere di inviare notifiche di avviso a un elenco di destinatari globale.

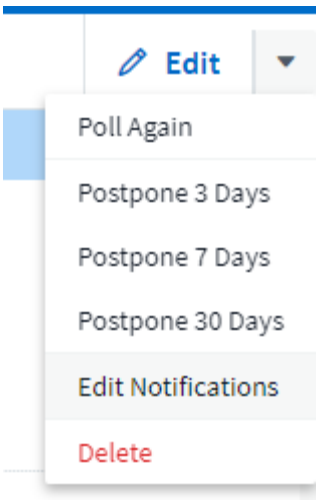
Per configurare i destinatari degli avvisi globali, selezionare i destinatari desiderati nella sezione **Destinatari delle notifiche di Global Monitor**.

È sempre possibile sovrascrivere l'elenco dei destinatari globali per un singolo monitor durante la creazione o la modifica del monitor.

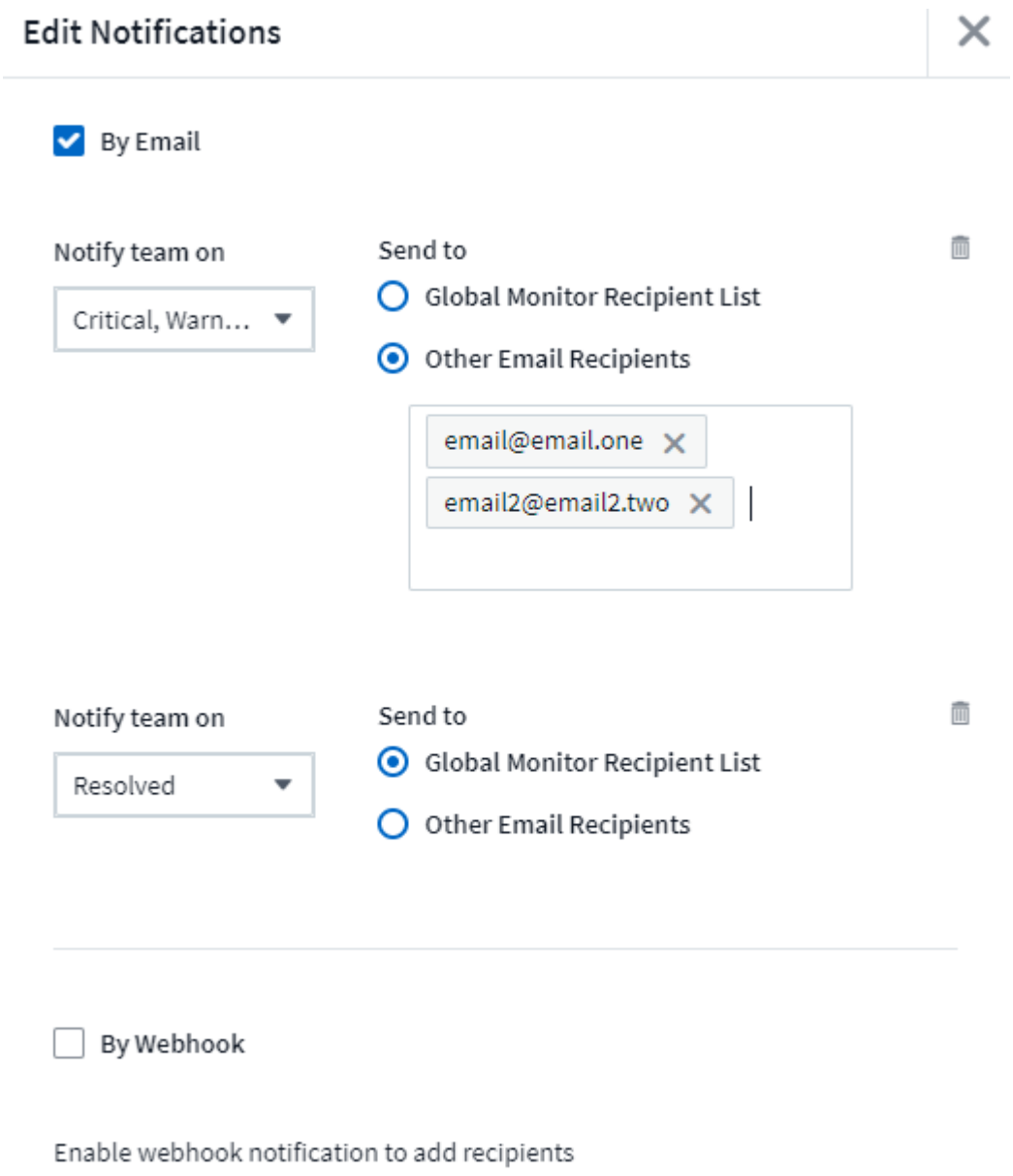
Le notifiche di ONTAP Data Collector hanno la precedenza su qualsiasi notifica specifica di Monitor pertinente al cluster/data collector. L'elenco dei destinatari impostato per il Data Collector riceverà gli avvisi del Data Collector. Se non sono presenti avvisi attivi del raccoglitore dati, gli avvisi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

Modifica delle notifiche per ONTAP

È possibile modificare le notifiche per i cluster ONTAP selezionando *Modifica notifiche* dal menu a discesa in alto a destra nella landing page di Storage.



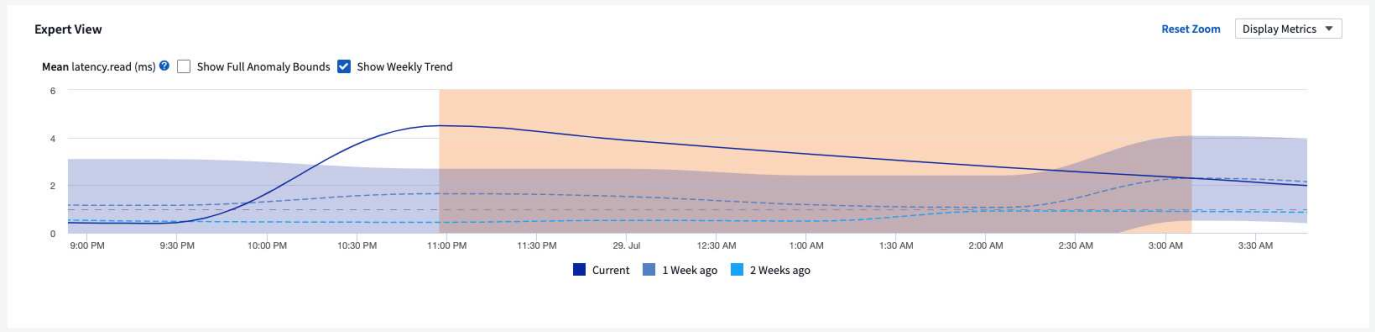
Da qui puoi impostare le notifiche per avvisi critici, di avviso, informativi e/o risolti. Ogni scenario può inviare notifiche all'elenco dei destinatari globali o ad altri destinatari scelti da te.



Monitor di rilevamento delle anomalie

Il rilevamento delle anomalie fornisce informazioni su cambiamenti imprevisti nei modelli di dati del tenant. Un'anomalia si verifica quando cambia il modello di comportamento di un oggetto, ad esempio se un oggetto presenta un certo livello di latenza a un certo orario di mercoledì, ma la latenza supera quel livello a quell'orario del mercoledì successivo, tale picco verrà considerato un'anomalia. Data Infrastructure Insights consente di creare monitor per avvisare quando si verificano anomalie di questo tipo.

Il rilevamento delle anomalie è adatto per metriche di oggetti che presentano uno schema ricorrente e prevedibile. Quando queste metriche degli oggetti superano o scendono al di sotto dei livelli previsti, Data Infrastructure Insights può generare un avviso per sollecitare un'indagine.



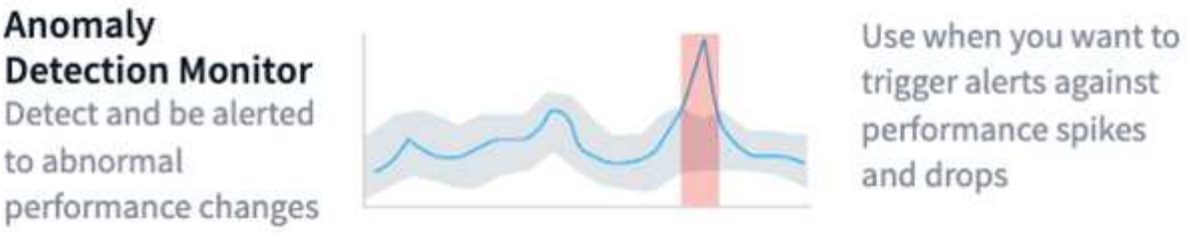
Che cos'è il rilevamento delle anomalie?

Si verifica un'anomalia quando il valore medio di una metrica si discosta di un certo numero di deviazioni standard dalla media ponderata di tale metrica per le settimane precedenti, con le settimane recenti che hanno un peso maggiore rispetto alle settimane precedenti. Data Infrastructure Insights offre la possibilità di monitorare i dati e di inviare avvisi quando vengono rilevate anomalie. È possibile impostare i livelli di "sensibilità" del rilevamento. Ad esempio, una sensibilità maggiore si avrebbe quando il valore medio si discosta dalla media con meno deviazioni standard, determinando così la generazione di più avvisi. Al contrario, minore sensibilità = più deviazioni standard dalla media = meno avvisi.

Il monitoraggio del rilevamento delle anomalie è diverso dal monitoraggio delle soglie.

- Il **monitoraggio basato su soglie** funziona quando si hanno soglie predefinite per metriche specifiche. In altre parole, quando si ha una chiara comprensione di cosa ci si aspetta (ovvero entro un intervallo normale).

- Il **monitoraggio tramite rilevamento delle anomalie** utilizza algoritmi di apprendimento automatico per identificare i valori anomali che si discostano dalla norma, quando la definizione di "normale" non è chiara.



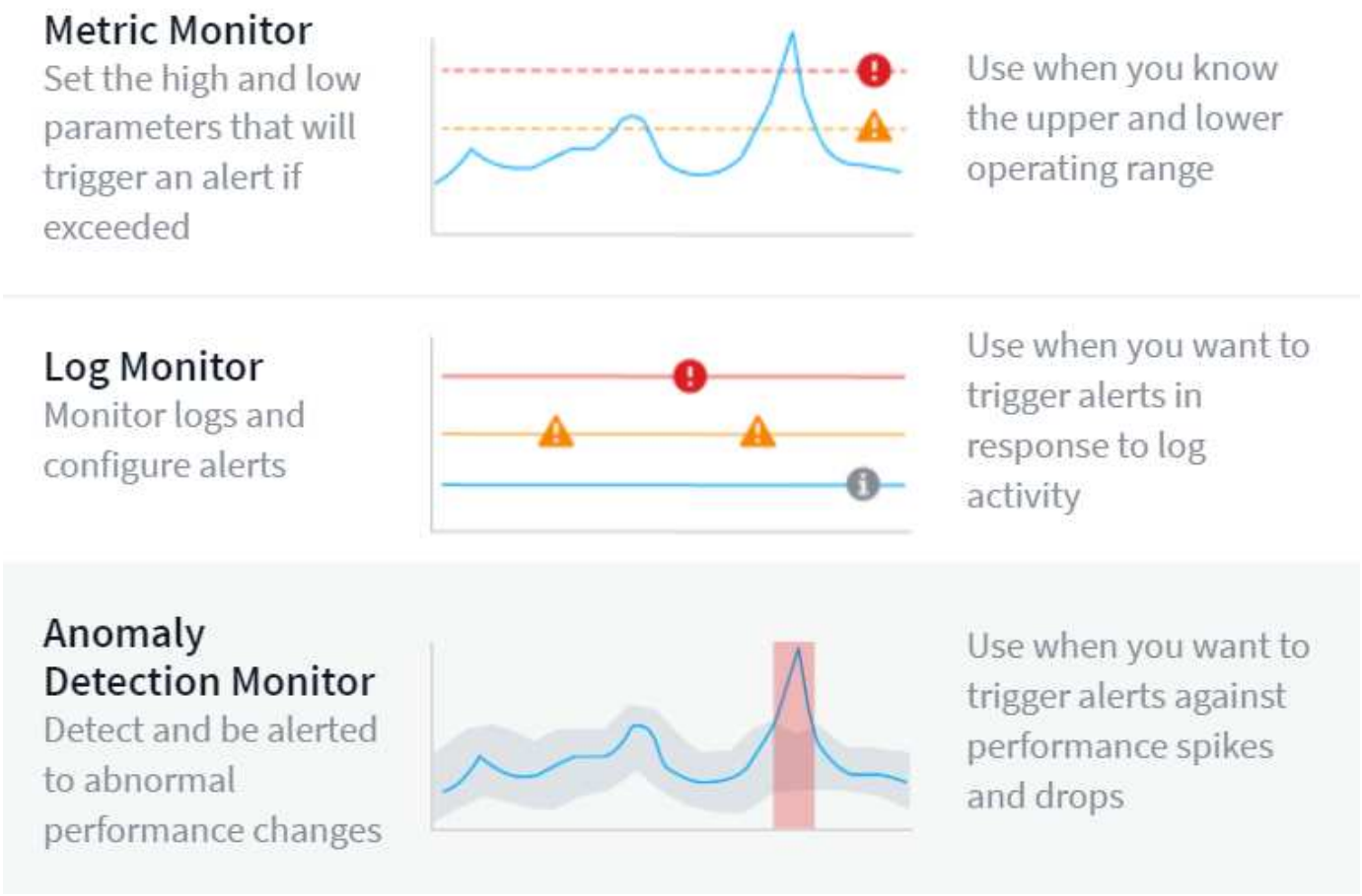
Quando avrei bisogno del rilevamento delle anomalie?

Il monitoraggio del rilevamento delle anomalie può fornire avvisi utili in molte situazioni, tra cui:

- Quando la definizione di *normale* non è chiara. Ad esempio, è possibile che i tassi di errore SAN varino a seconda della porta. Segnalare un errore è rumoroso e superfluo, ma un aumento improvviso o significativo potrebbe indicare un problema diffuso.
- Dove si verificano cambiamenti nel tempo. Carichi di lavoro che presentano stagionalità (ad esempio, sono intensi o silenziosi in determinati periodi). Ciò potrebbe includere periodi di silenzio inaspettati che potrebbero indicare un blocco del lotto.
- Lavorare con grandi quantità di dati in cui definire e regolare manualmente le soglie risulta poco pratico. Ad esempio, un tenant con un numero elevato di host e/o volumi con carichi di lavoro variabili. Ognuno di essi può avere SLA diversi, quindi è importante capire quali sono quelli che superano la norma.

Creazione di un monitor di rilevamento delle anomalie

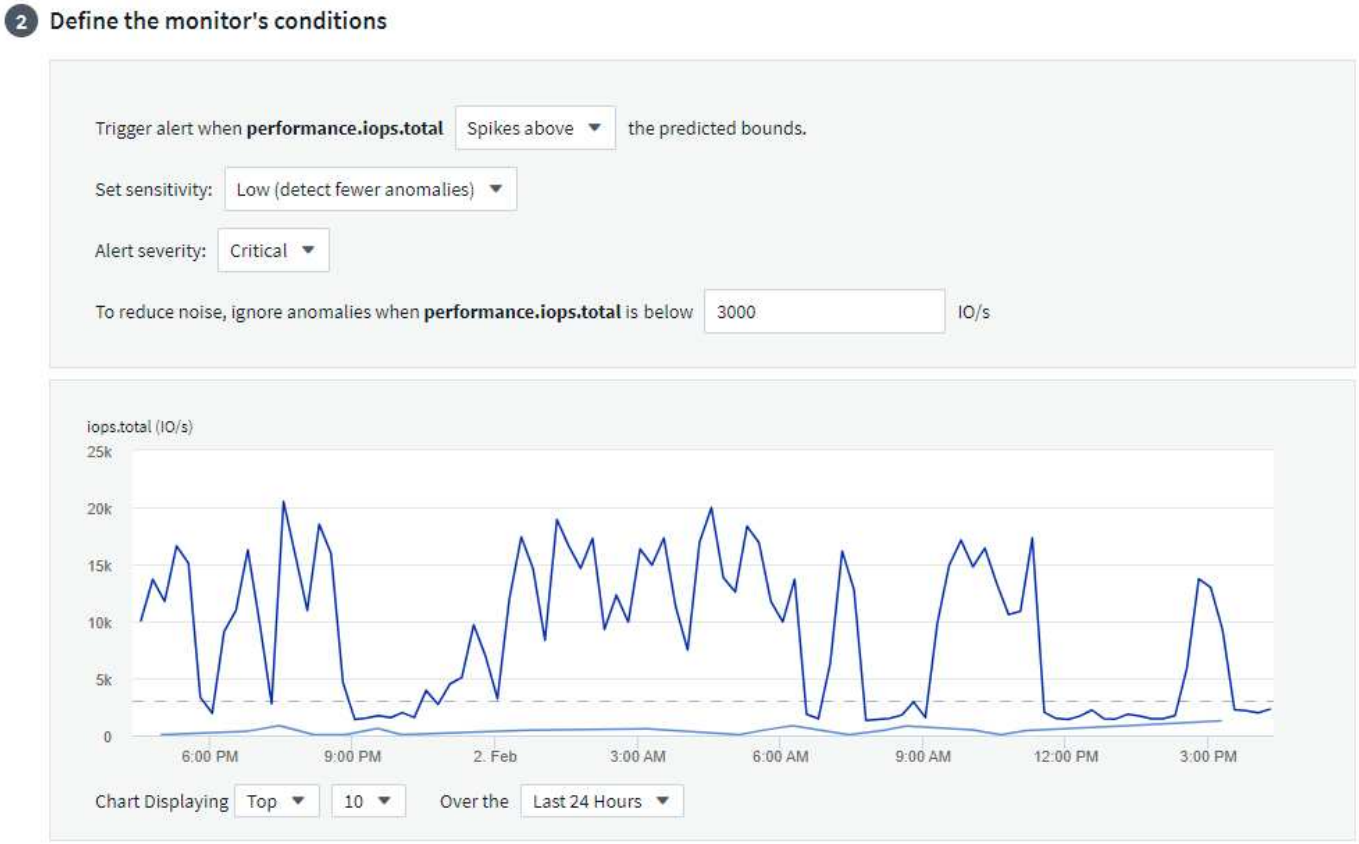
Per ricevere avvisi sulle anomalie, creare un monitor andando su **Osservabilità > Avvisi > +Monitor**. Selezionare *Anomaly Detection Monitor* come tipo di monitor.



Scegli l'oggetto e la metrica che vuoi monitorare. È possibile impostare filtri e raggruppamenti come con altri tipi di monitor.

Successivamente, impostare le condizioni per il monitor.

- Attiva un avviso quando la metrica selezionata *Raggiunge un picco* oltre i limiti previsti, *Scende al di sotto* di tali limiti o entrambe le cose.
- Impostare la sensibilità su *Media*, *Bassa* (vengono rilevate meno anomalie) o *Alta* (vengono rilevate più anomalie).
- Determina se il livello di allerta è *Critico* o *Avviso*.
- Facoltativamente, imposta un valore al di sotto del quale le anomalie vengono *ignorate*. Ciò può contribuire a ridurre il rumore. Questo valore è mostrato come una linea tratteggiata nel grafico di esempio.



Infine, è possibile configurare un metodo di recapito per gli avvisi (e-mail, webhook o entrambi), fornire al monitor una descrizione facoltativa o azioni correttive e aggiungere il monitor a un gruppo personalizzato, se lo si desidera.

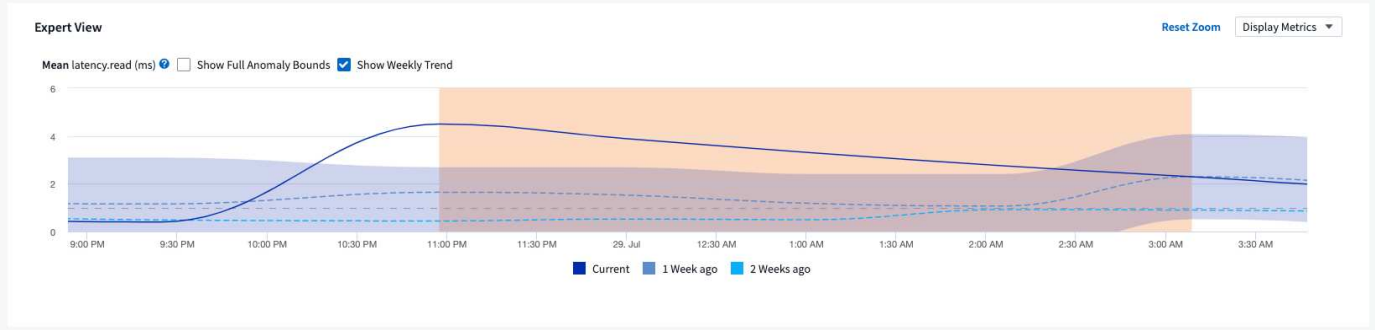
Salva il monitor con un nome significativo e il gioco è fatto.

Dopo la creazione, il monitor analizza i dati della settimana precedente per stabilire una base di riferimento iniziale. Il rilevamento delle anomalie diventa più accurato con il passare del tempo e con l'aumentare della cronologia.

> Quando viene creato un monitor, DII esamina tutti i dati esistenti della settimana precedente per individuare picchi o cali significativi; questi sono considerati anomalie. Durante la prima settimana successiva alla creazione del monitor (fase di "apprendimento"), è possibile che si verifichi un aumento del "rumore" negli avvisi. Per attenuare questo rumore, solo i picchi o i cali che durano più di 30 minuti vengono considerati anomalie e generano avvisi. Nella settimana successiva, man mano che vengono analizzati più dati, il rumore solitamente si riduce e un picco o un calo significativo che duri un certo periodo di tempo viene considerato un'anomalia.

Visualizzazione delle anomalie

Nella landing page di un avviso, gli avvisi attivati quando vengono rilevate anomalie mostreranno una banda evidenziata nel grafico, dal momento in cui la metrica ha raggiunto un picco al di fuori dei limiti previsti fino a quando è tornata all'interno di tali limiti.



Durante la visualizzazione di un grafico delle anomalie nella landing page di un avviso, è possibile scegliere le seguenti opzioni:

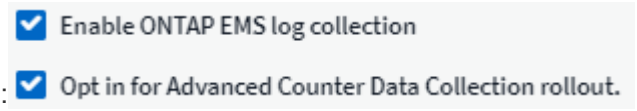
- Andamento settimanale: confronta i valori con la stessa ora, lo stesso giorno delle settimane precedenti, per un massimo di 5 settimane.
- Limiti di anomalia completi: per impostazione predefinita, il grafico si concentra sul valore della metrica, in modo da poterne analizzare meglio il comportamento. Selezionare per visualizzare i limiti completi delle anomalie (valore massimo, ecc.)

È anche possibile visualizzare gli oggetti che hanno contribuito all'anomalia selezionandoli nella sezione prestazioni della landing page. Il grafico mostrerà il comportamento degli oggetti selezionati.

Monitor di sistema

Data Infrastructure Insights include una serie di monitor definiti dal sistema sia per le metriche che per i log. I monitor di sistema disponibili dipendono dai collettori di dati presenti sul tenant. Per questo motivo, i monitor disponibili in Data Infrastructure Insights potrebbero cambiare man mano che vengono aggiunti raccoglitori di dati o ne vengono modificate le configurazioni.

Per impostazione predefinita, molti monitor di sistema sono in stato *In pausa*. È possibile abilitare un monitor di sistema selezionando l'opzione *Riprendi* per il monitor. Assicurarsi che le opzioni *Raccolta dati contatore avanzata* e *Abilita raccolta log ONTAP EMS* siano abilitate nel Data Collector. Queste opzioni sono disponibili in ONTAP Data Collector in *Configurazione avanzata*:



indice:[]

Descrizioni del monitor

I monitor definiti dal sistema sono composti da metriche e condizioni predefinite, nonché da 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 le metriche, le condizioni, la descrizione e le azioni correttive, oppure 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.

Sono disponibili i seguenti monitor definiti dal sistema, nei gruppi indicati.

- * ONTAP Infrastructure* include monitor per problemi relativi all'infrastruttura nei cluster ONTAP .
- * Esempi di carico di lavoro ONTAP * include monitor per problemi correlati al carico di lavoro.
- Per impostazione predefinita, i monitor di entrambi i gruppi sono impostati sullo stato *Paused*.

Di seguito sono elencati i monitor di sistema attualmente inclusi in Data Infrastructure Insights:

Monitor metrici

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva

Elevato utilizzo delle porte Fibre Channel	CRITICO	Le porte Fibre Channel Protocol vengono utilizzate per ricevere e trasferire il traffico SAN tra il sistema host del cliente e le LUN ONTAP . Se l'utilizzo delle porte è elevato, questo diventerà un collo di bottiglia e influirà in ultima analisi sulle prestazioni dei carichi di lavoro sensibili del protocollo Fibre Channel. Un avviso di avvertimento indica che è necessario adottare misure pianificate 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.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare i carichi di lavoro su un'altra porta FCP meno utilizzata. 2. Limitare il traffico di determinate LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP. Se la soglia di allerta viene superata, 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 determinate LUN solo al lavoro essenziale, tramite policy QoS in ONTAP o configurazione lato host per alleggerire l'utilizzo delle porte FCP.

Latenza LUN elevata	CRITICO	Le LUN sono oggetti che gestiscono il traffico I/O, spesso gestito da applicazioni sensibili alle prestazioni, come i database. Le latenze LUN elevate comportano che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Un avviso di avvertimento indica che è necessario intraprendere un'azione pianificata per spostare la LUN sul nodo o sull'aggregato appropriato. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per 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	Se viene superata la soglia critica, prendere in considerazione le seguenti azioni per ridurre al minimo l'interruzione del servizio: se alla LUN o al suo volume è associata una policy QoS, valutare i limiti di soglia e verificare se stanno causando la limitazione del carico di lavoro della LUN. Se la soglia di allerta viene superata, pianificare le seguenti azioni: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare la LUN su un altro aggregato. 2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se alla LUN o al suo volume è associata una policy QoS, valutare i limiti di soglia e verificare se stanno causando la limitazione del carico di lavoro della LUN.

Utilizzo elevato delle porte di rete	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, si crea un collo di bottiglia e in ultima analisi influirà sulle prestazioni dei carichi di lavoro NFS, CIFS e iSCSI. Un avviso di avviso indica che è necessario adottare misure pianificate 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.	Se viene superata la soglia critica, valutare 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. Se la soglia di allerta viene superata, 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 elevata dello spazio dei nomi NVMe	CRITICO	Gli spazi dei nomi NVMe sono oggetti che gestiscono il traffico I/O gestito da applicazioni sensibili alle prestazioni, come i database. Un'elevata latenza degli spazi dei nomi NVMe significa che le applicazioni stesse potrebbero risentirne e non essere in grado di svolgere le proprie attività. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per spostare la LUN sul nodo o sull'aggregato appropriato. Un avviso critico indica che l'interruzione del servizio è imminente e che è necessario adottare misure di emergenza per garantire la continuità del servizio.	Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: se allo spazio dei nomi NVMe o al suo volume è assegnata una policy QoS, valutare le relative soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro dello spazio dei nomi NVMe. Se la soglia di avviso viene superata, valutare di adottare le seguenti misure: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare la LUN su un altro aggregato. 2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo. 3. Se allo spazio dei nomi NVMe o al suo volume è assegnata una policy QoS, valutare le relative soglie limite nel caso in cui causino la limitazione del carico di lavoro dello spazio dei nomi NVMe.

Capacità QTree piena	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio predefinita o una quota definita da una politica di quota per limitare la quantità di dati archiviati nell'albero entro la capacità del volume. Un avviso di 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 che è necessario adottare misure di emergenza per liberare spazio e garantire la continuità del servizio.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del qtree per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio del qtree per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio.
Limite massimo di capacità QTree	CRITICO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che viene utilizzata per archiviare i dati in modo da controllare la crescita del volume dei dati dell'utente e non superare la sua capacità totale. Un qtree mantiene una quota di capacità di archiviazione flessibile che avvisa l'utente in modo proattivo prima che raggiunga il limite della quota di capacità totale nel qtree e non sia più in grado di archiviare i dati. Il monitoraggio della quantità di dati archiviati in un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota di spazio dell'albero per far fronte alla crescita 2. Chiedere all'utente di eliminare i dati indesiderati nell'albero per liberare spazio

Limite flessibile della capacità di QTree	AVVERTIMENTO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota di spazio misurata in KByte che può utilizzare per archiviare i dati, in modo da controllare la crescita del volume dei dati dell'utente e non superare la sua capacità totale. Un qtree mantiene una quota di capacità di archiviazione flessibile che avvisa l'utente in modo proattivo prima che raggiunga il limite della quota di capacità totale nel qtree e non sia più in grado di archiviare i dati. Il monitoraggio della quantità di dati archiviati in un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, prendere in considerazione le seguenti azioni immediate: 1. Aumentare la quota di spazio per gli alberi per far fronte 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 radice all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione gestibile del file system all'interno del volume. Un qtree mantiene una quota fissa del numero di file oltre la quale i nuovi file nell'albero vengono negati. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare la quota del numero di file per qtree. 2. Eliminare i file indesiderati dal file system qtree.

Limite flessibile dei file QTree	AVVERTIMENTO	Un qtree è un file system definito logicamente che può esistere come una sottodirectory speciale della directory radice all'interno di un volume. Ogni qtree ha una quota del numero di file che può contenere per mantenere una dimensione gestibile del file system all'interno del volume. Un qtree mantiene una quota flessibile del numero di file per avvisare l'utente in modo proattivo prima che raggiunga il limite di file nel qtree e non sia più possibile archiviare file aggiuntivi. Il monitoraggio del numero di file all'interno di un qtree garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare la quota del numero di file per qtree. 2. Eliminare i file indesiderati dal file system qtree.

Istantanea Riserva Spazio Pieno	CRITICO	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati archiviati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore è la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale per gli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e il livello di protezione dei dati nel volume potrebbe ridursi. Il monitoraggio della capacità snapshot del volume utilizzato garantisce la continuità dei servizi dati.	Se viene superata la soglia critica, prendere in considerazione misure immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Elimina alcuni vecchi snapshot indesiderati per liberare spazio. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita. 2. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena.

Limite di capacità di archiviazione	CRITICO	Quando un pool di archiviazione (aggregato) si riempie, le operazioni di I/O rallentano e infine si interrompono, causando un'interruzione dell'archiviazione. Un avviso di avviso indica che è necessario intraprendere al più 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.	Se viene superata la soglia critica, prendere immediatamente in considerazione le seguenti azioni per ridurre al minimo l'interruzione del servizio: 1. Eliminare gli snapshot sui volumi non critici. 2. Eliminare volumi o LUN che rappresentano carichi di lavoro non essenziali e che possono essere ripristinati da copie esterne all'archiviazione. Se la soglia di avviso viene superata, pianificare le seguenti azioni immediate: 1. Spostare uno o più volumi in una posizione di archiviazione diversa. 2. Aggiungere più capacità di archiviazione. 3. Modifica le impostazioni di efficienza dell'archiviazione o sposta i dati inattivi nell'archiviazione cloud.

Limite delle prestazioni di archiviazione	CRITICO	Quando un sistema di storage raggiunge il limite delle prestazioni, le operazioni rallentano, la latenza aumenta e i carichi di lavoro e le applicazioni potrebbero iniziare a non funzionare. ONTAP valuta l'utilizzo del pool di archiviazione per i carichi di lavoro e stima la percentuale di prestazioni consumata. Un avviso di avviso indica che è necessario intraprendere un'azione pianificata per ridurre il carico del pool di archiviazione e garantire che siano rimaste prestazioni sufficienti per gestire i picchi di carico di lavoro. Un avviso critico indica che è imminente un calo delle prestazioni e che è necessario adottare misure di emergenza per ridurre il carico del pool di archiviazione e garantire la continuità del servizio.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate come gli snapshot o la replica SnapMirror . 2. Carichi di lavoro inattivi non essenziali.… Se la soglia di allerta viene superata, adottare immediatamente le seguenti misure: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa. 2. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 3. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione).

Limite massimo della capacità della quota utente	CRITICO	ONTAP riconosce gli utenti dei sistemi Unix o Windows che hanno i diritti di accesso ai volumi, ai file o alle directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di archiviazione per i propri utenti o gruppi di utenti dei propri sistemi Linux o Windows. La quota dei criteri utente o di gruppo limita la quantità di spazio che l'utente può utilizzare per i propri dati. Un limite rigido di questa quota consente di notificare all'utente quando la quantità di capacità utilizzata all'interno del volume è appena prima di raggiungere la quota di capacità totale. Il monitoraggio della quantità di dati archiviati all'interno di una quota utente o di un gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio della quota utente o del gruppo per far fronte alla crescita. 2. Chiedere all'utente o al gruppo di eliminare i dati indesiderati per liberare spazio.

Limite flessibile della capacità della quota utente	AVVERTIMENTO	ONTAP riconosce gli utenti dei sistemi Unix o Windows che hanno i diritti di accesso ai volumi, ai file o alle directory all'interno di un volume. Di conseguenza, ONTAP consente ai clienti di configurare la capacità di archiviazione per i propri utenti o gruppi di utenti dei propri sistemi Linux o Windows. La quota dei criteri utente o di gruppo limita la quantità di spazio che l'utente può utilizzare per i propri dati. Un limite flessibile di questa quota consente di inviare notifiche proattive all'utente quando la quantità di capacità utilizzata all'interno del volume raggiunge la quota di capacità totale. Il monitoraggio della quantità di dati archiviati all'interno di una quota utente o di un gruppo garantisce che l'utente riceva un servizio dati ininterrotto.	Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare lo spazio della quota utente o del gruppo per far fronte alla crescita. 2. Elimina i dati indesiderati per liberare spazio.

Capacità del volume completa	CRITICO	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Maggiore è la quantità di dati memorizzati nel volume ONTAP , minore sarà la disponibilità di spazio di archiviazione per i dati futuri. Se la capacità di archiviazione dati all'interno di un volume raggiunge la capacità di archiviazione totale, il cliente potrebbe non essere in grado di archiviare i dati a causa della mancanza di capacità di archiviazione. Il monitoraggio del volume di capacità di archiviazione utilizzato garantisce la continuità dei servizi dati.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume per assecondare la crescita. 2. Elimina i dati indesiderati per liberare spazio. 3. Se le copie snapshot occupano più spazio della riserva snapshot, eliminare i vecchi snapshot o abilitare l'eliminazione automatica degli snapshot del volume. Se la soglia di avviso viene superata, pianificare di intraprendere le seguenti azioni immediate: 1. Aumentare lo spazio del volume per accogliere la crescita 2. Se le copie degli snapshot occupano più spazio della riserva di snapshot, eliminare i vecchi snapshot o abilitare l'eliminazione automatica degli snapshot del volume.

Limite di volume inode	CRITICO	I volumi che archiviano i file utilizzano nodi di indice (inode) per archiviare i metadati dei file. Quando un volume esaurisce la sua allocazione di inode, non è possibile aggiungervi altri file. Un avviso di avvertenza 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 e garantire la continuità del servizio.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare il valore degli inode per il volume. Se il valore degli inode è già al valore massimo, allora bisogna dividere il volume in due o più volumi perché il file system ha superato la dimensione massima. 2. Utilizzare FlexGroup perché aiuta a gestire file system di grandi dimensioni. Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti misure: 1. Aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora bisogna dividere il volume in due o più volumi perché il file system ha superato la dimensione massima. 2. Utilizzare FlexGroup poiché aiuta ad ospitare file system di grandi dimensioni

Latenza del volume elevata	CRITICO	I volumi sono oggetti che gestiscono il traffico I/O spesso gestito da applicazioni sensibili alle prestazioni, tra cui applicazioni DevOps, directory home e database. Le latenze elevate possono comportare problemi alle applicazioni stesse, che potrebbero non essere in grado di svolgere i propri compiti. Il monitoraggio delle latenze del volume è fondamentale per mantenere prestazioni costanti delle 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.	Se viene superata la soglia critica, valutare le seguenti azioni immediate per ridurre al minimo l'interruzione del servizio: se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro del volume. Se la soglia di allerta viene superata, prendere in considerazione le seguenti azioni immediate: 1. Se anche l'aggregato è molto utilizzato, spostare il volume su un altro aggregato. 2. Se al volume è assegnata una policy QoS, valutarne le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. 3. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.
Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva

Nodo ad alta latenza	ATTENZIONE / CRITICO	La latenza del nodo ha raggiunto livelli tali da poter influire sulle prestazioni delle applicazioni sul nodo. Una latenza dei nodi inferiore garantisce prestazioni 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.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Sospendere le attività pianificate, gli snapshot o la replica SnapMirror 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Disattivare i carichi di lavoro non essenziali. Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Limite delle prestazioni del nodo	ATTENZIONE / CRITICO	L'utilizzo delle prestazioni del nodo ha raggiunto livelli tali da poter influire sulle prestazioni degli I/O e delle applicazioni supportate dal nodo. Un basso utilizzo delle prestazioni dei nodi garantisce prestazioni costanti delle applicazioni.	È necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica: 1. Sospendere le attività pianificate, gli snapshot o la replica SnapMirror 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Disattivare i carichi di lavoro non essenziali. Prendere in considerazione le seguenti azioni se viene superata la soglia di avviso: 1. Spostare uno o più carichi di lavoro in una posizione di archiviazione diversa 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore tramite limiti QoS 3. Aggiungere più nodi di archiviazione (AFF) o ripiani di dischi (FAS) e ridistribuire i carichi di lavoro 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Storage VM ad alta latenza	ATTENZIONE / CRITICO	La latenza della VM di archiviazione (SVM) ha raggiunto livelli tali da poter influire sulle prestazioni delle applicazioni sulla VM di archiviazione. La latenza ridotta delle VM di archiviazione garantisce prestazioni 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.	Se viene superata la soglia critica, valutare immediatamente i limiti di soglia per i volumi della VM di archiviazione con una policy QoS assegnata, per verificare se stanno causando la limitazione dei carichi di lavoro del volume. Prendere in considerazione le seguenti azioni immediate quando viene superata la soglia di avviso: 1. Se anche l'aggregato è sottoposto a un utilizzo elevato, spostare alcuni volumi della VM di archiviazione su un altro aggregato. 2. Per i volumi della VM di archiviazione con una policy QoS assegnata, valutare i limiti di soglia se causano la limitazione dei carichi di lavoro del volume 3. Se il nodo è soggetto a un utilizzo elevato, spostare alcuni volumi della VM di archiviazione su un altro nodo o ridurre il carico di lavoro totale del nodo
Limite massimo dei file delle quote utente	CRITICO	Il numero di file creati nel volume ha raggiunto il limite critico e non è possibile creare file aggiuntivi. Il monitoraggio del numero di file archiviati garantisce all'utente un servizio dati ininterrotto.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica. Si consideri l'adozione delle seguenti misure: 1. Aumentare la quota del numero di file per l'utente specifico 2. Elimina i file indesiderati per ridurre la pressione sulla quota di file per l'utente specifico

Limite flessibile dei file delle quote utente	AVVERTIMENTO	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. Monitorando il numero di file archiviati da un utente si garantisce che l'utente riceva un servizio dati ininterrotto.	Prendere in considerazione azioni immediate se viene superata la soglia di allerta: 1. Aumentare la quota del numero di file per la quota utente specifica 2. Elimina i file indesiderati per ridurre la pressione sulla quota di file per l'utente specifico

Rapporto di mancata corrispondenza della cache del volume	ATTENZIONE / CRITICO	Il rapporto di mancata lettura nella cache del volume è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco anziché dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Se non è già presente sul nodo del volume, aumentare la cache WAFL acquistando e aggiungendo una Flash Cache 3. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS. Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Se non è già presente sul 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 limiti QoS 4. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Sovracommit della quota Qtree del volume	ATTENZIONE / CRITICO	Volume Qtree Quota Overcommit specifica la percentuale in cui un volume è considerato in eccesso rispetto alle quote qtree. È stata raggiunta la soglia impostata per la quota qtree per il volume. Il monitoraggio del superamento della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Aumentare lo spazio del volume 2. Eliminare i dati indesiderati Quando viene superata la soglia di avviso, valutare l'aumento dello spazio del volume.

Torna all'inizio

Monitor di registro

Nome del monitor	Gravità	Descrizione	Azione correttiva
Credenziali AWS non inizializzate	INFORMAZIONI	Questo evento si verifica quando un modulo tenta di accedere alle credenziali basate sui ruoli di Amazon Web Services (AWS) Identity and Access Management (IAM) dal thread delle credenziali cloud prima che vengano inizializzate.	Attendi che il thread delle credenziali cloud e il sistema completino l'inizializzazione.

Livello cloud non raggiungibile	CRITICO	Un nodo di archiviazione non riesce a connettersi all'API dell'archivio oggetti Cloud Tier. Alcuni dati saranno inaccessibili.	Se si utilizzano prodotti on-premise, eseguire le seguenti azioni correttive: …Verificare che il LIF 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 intercluster del nodo di destinazione….Assicurarsi di quanto segue:…La configurazione dell'archivio oggetti non è cambiata….Le informazioni di accesso e connettività sono ancora valide….Contattare l'assistenza tecnica NetApp se il problema persiste. Se si utilizza Cloud Volumes ONTAP, eseguire le seguenti azioni correttive: …Assicurarsi che la configurazione dell'archivio oggetti non sia cambiata…. Assicurarsi che le informazioni di accesso e connettività siano ancora valide. Se il problema persiste, contattare l'assistenza tecnica NetApp .
Disco fuori servizio	INFORMAZIONI	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come guasto, è in fase di sanificazione o è entrato nel Centro di manutenzione.	Nessuno.

Costituente FlexGroup completo	CRITICO	Un componente all'interno di un volume FlexGroup è pieno, il che potrebbe causare una potenziale interruzione del servizio. È ancora possibile creare o espandere file sul volume FlexGroup . Tuttavia, nessuno dei file memorizzati sul costituente può essere modificato. Di conseguenza, potrebbero verificarsi errori casuali di spazio insufficiente quando si tenta di eseguire operazioni di scrittura sul 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 stabilire quali fascicoli siano stati inoltrati al costituente.
Costituente Flexgroup quasi pieno	AVVERTIMENTO	Un componente all'interno di un volume FlexGroup ha quasi esaurito lo spazio, il che potrebbe causare una potenziale interruzione del servizio. I file possono essere creati ed espansi. Tuttavia, se lo spazio disponibile sul costituente esaurisce, potresti non essere in grado di 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 stabilire quali fascicoli siano stati inoltrati al costituente.
Il componente FlexGroup ha quasi esaurito gli inode	AVVERTIMENTO	Un componente all'interno di un volume FlexGroup è quasi senza inode, il che potrebbe causare una potenziale interruzione del servizio. Il costituente riceve meno richieste di creazione rispetto alla media. Ciò potrebbe avere un impatto sulle prestazioni complessive del volume FlexGroup , poiché le richieste vengono indirizzate 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 stabilire quali fascicoli siano stati inoltrati al costituente.

Costituente FlexGroup fuori dagli inode	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. Ciò potrebbe portare a una distribuzione complessivamente sbilanciata dei contenuti 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 stabilire quali fascicoli siano stati inoltrati al costituente.
LUN offline	INFORMAZIONI	Questo evento si verifica quando una LUN viene portata offline manualmente.	Riportare online la LUN.
Ventola dell'unità principale guasta	AVVERTIMENTO	Una o più ventole dell'unità principale sono guaste. Il sistema rimane operativo. Tuttavia, se la condizione persiste troppo a lungo, la sovratemperatura potrebbe innescare uno spegnimento automatico.	Riposizionare le ventole guaste. Se l'errore persiste, sostituirli.
Ventola dell'unità principale in stato di avviso	INFORMAZIONI	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	AVVERTIMENTO	La capacità della batteria NVRAM è estremamente bassa. Potrebbe verificarsi una potenziale perdita di dati se la batteria si scarica. Il sistema genera e trasmette un messaggio AutoSupport o "call home" al supporto tecnico NetApp e alle destinazioni configurate, se configurato per farlo. La corretta consegna di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Eseguire le seguenti azioni correttive:…Visualizzare lo stato attuale della batteria, la capacità e lo stato di carica utilizzando il comando "system node environment sensors show"….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 l'assistenza tecnica NetApp se l'autonomia della batteria continua a scendere al di sotto dei livelli critici e il sistema di storage si spegne automaticamente.
Processore di servizio non configurato	AVVERTIMENTO	Questo evento si verifica settimanalmente per ricordarti di configurare il Service Processor (SP). L' SP è un dispositivo fisico incorporato nel sistema per fornire funzionalità di accesso e gestione remota. È necessario configurare l' SP per sfruttarne tutte le funzionalità.	Eseguire le seguenti azioni correttive:…Configurare l' SP utilizzando il comando "system service-processor network modify"….Facoltativamente, ottenere l'indirizzo MAC SP utilizzando il comando "system service-processor network show"….Verificare la configurazione di rete SP utilizzando il comando "system service-processor network show"….Verificare che l' SP possa inviare un'e-mail di AutoSupport utilizzando il comando "system service-processor autosupport invoke". NOTA: gli host e i destinatari della posta elettronica AutoSupport devono essere configurati in ONTAP prima di emettere questo comando.

Processore di servizi offline	CRITICO	ONTAP non riceve più heartbeat dal Service Processor (SP), anche se sono state eseguite tutte le azioni di ripristino SP . ONTAP non può monitorare lo stato dell'hardware senza SP. …Il sistema si spegnerà per evitare danni all'hardware e perdita di dati. Imposta un avviso di panico per essere avvisato immediatamente se l' SP va offline.	Spegnere e riaccendere il sistema eseguendo le seguenti operazioni:… Estrarre il controller dallo chassis.… Reinserire il controller.… Riaccendere il controller.… Se il problema persiste, sostituire il modulo del controller.
I ventilatori dello scaffale sono guasti	CRITICO	La ventola di raffreddamento indicata o il modulo ventola dello scaffale sono guasti. I dischi nello scaffale potrebbero non ricevere un flusso d'aria di raffreddamento sufficiente, il che potrebbe causare guasti al disco.	Eseguire le seguenti azioni correttive:…Verificare che il modulo ventola sia completamente inserito e fissato. NOTA: la ventola è integrata nel modulo di alimentazione in alcuni alloggiamenti per dischi. Se il problema persiste, sostituire il modulo ventola. Se il problema persiste, contattare l'assistenza tecnica NetApp per ricevere assistenza.
Il sistema non può funzionare a causa di un guasto della ventola dell'unità principale	CRITICO	Una o più ventole dell'unità principale sono guaste, interrompendo il funzionamento del sistema. Ciò potrebbe comportare una potenziale perdita di dati.	Sostituire le ventole guaste.
Dischi non assegnati	INFORMAZIONI	Il sistema ha dischi non assegnati: la capacità viene sprecata e potrebbe essere stata applicata una configurazione errata o una modifica parziale della configurazione del sistema.	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	AVVERTIMENTO	Il server antivirus è troppo occupato per accettare nuove richieste di scansione.	Se questo messaggio si verifica frequentemente, assicurarsi che siano presenti abbastanza server antivirus per gestire il carico di scansione antivirus generato dall'SVM.
Credenziali AWS per il ruolo IAM scadute	CRITICO	Cloud Volume ONTAP è diventato inaccessibile. Le credenziali basate sul ruolo Identity and Access Management (IAM) sono scadute. Le credenziali vengono acquisite dal server di metadati di Amazon Web Services (AWS) tramite 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 AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…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 riesce ad acquisire le credenziali basate sul ruolo di Amazon Web Services (AWS) Identity and Access Management (IAM) dal server dei 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 AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…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 Identity and Access Management (IAM) non sono valide. Le credenziali vengono acquisite dal server di metadati di Amazon Web Services (AWS) tramite 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 AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…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 Identity and Access Management (IAM) non riesce a trovare un ruolo IAM di Amazon Web Services (AWS) sul server dei 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 AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo 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 metadati AWS non è valido. Cloud Volume ONTAP è diventato inaccessibile.	Eseguire le seguenti operazioni:…Accedere alla console di gestione AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…Verificare che il ruolo AWS IAM associato all'istanza sia valido e che siano stati concessi i privilegi appropriati all'istanza.

Errore di connessione al server metadati AWS	CRITICO	Il thread dei ruoli Identity and Access Management (IAM) non riesce a stabilire un collegamento di comunicazione con il server dei metadati di Amazon Web Services (AWS). È necessario stabilire una comunicazione per acquisire le credenziali AWS IAM basate sui ruoli necessarie, 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 AWS EC2.…Accedere alla pagina Istanze.…Trovare l'istanza per la distribuzione Cloud Volumes ONTAP e verificarne lo stato.…
Limite di utilizzo dello spazio FabricPool quasi raggiunto	AVVERTIMENTO	L'utilizzo totale dello spazio FabricPool a livello di cluster da parte degli archivi di oggetti provenienti da provider con licenza di capacità ha quasi raggiunto il limite di licenza.	Eseguire le seguenti azioni correttive:…Verificare la percentuale di capacità concessa in licenza utilizzata da ciascun livello di archiviazione FabricPool utilizzando il comando "storage aggregate object-store show-space".…Eliminare le copie snapshot dai volumi con il criterio di suddivisione in livelli "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 provenienti da provider con licenza di capacità ha raggiunto il limite di licenza.	Eseguire le seguenti azioni correttive:…Verificare la percentuale di capacità concessa in licenza utilizzata da ciascun livello di archiviazione FabricPool utilizzando il comando "storage aggregate object-store show-space"….Eliminare le copie snapshot dai volumi con il criterio di suddivisione in livelli "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.

Restituzione dell’aggregato fallita	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover di archiviazione (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive:…Verificare che il LIF 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 intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show"….In alternativa, è possibile ignorare l’errore specificando false per il parametro "require-partner-waiting" del comando giveback.…Per ulteriori informazioni o assistenza, contattare l’assistenza tecnica NetApp .

Interconnessione HA inattiva	AVVERTIMENTO	L'interconnessione ad alta disponibilità (HA) non funziona. 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 non funziona. …Se i collegamenti sono inattivi:…Verificare che entrambi i controller nella coppia HA siano operativi.…Per i collegamenti collegati esternamente, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i moduli SFP (Small Form-Factor Pluggable), se applicabili, siano posizionati correttamente su entrambi i controller.…Per i collegamenti collegati internamente, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on". …Se i collegamenti sono disabilitati, abilitarli utilizzando il comando "ic link on". …Se un peer non è connesso, disabilitare e riabilitare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on".…Se il problema persiste, contattare l'assistenza tecnica NetApp .

Numero massimo di sessioni per utente superato	AVVERTIMENTO	Hai superato il numero massimo di sessioni consentite per utente su una connessione TCP. Ogni richiesta di stabilire una sessione verrà respinta finché alcune sessioni non saranno rilasciate. …	Eseguire le seguenti azioni correttive: …Ispezionare 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-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere 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 l'assistenza tecnica NetApp .

Numero massimo di aperture per file superato	AVVERTIMENTO	Hai superato il numero massimo di volte in cui puoi aprire il file tramite una connessione TCP. Ogni richiesta di apertura di questo file verrà rifiutata finché non si chiudono alcune istanze aperte del file. Ciò 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 su di esso. 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-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere 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 l'assistenza tecnica NetApp .

Conflitto di nomi NetBIOS	CRITICO	Il servizio nomi NetBIOS ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. In genere ciò è causato 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 distribuzione dei dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive:…Se si verifica un conflitto nel nome NetBIOS o in un alias, eseguire una delle seguenti operazioni:…Eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -aliases 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 -aliases alias -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" 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 il NetBIOS sul computer remoto.
Pool di archiviazione NFSv4 esaurito	CRITICO	Un pool di archiviazione NFSv4 è esaurito.	Se il server NFS non risponde per più di 10 minuti dopo questo evento, contattare l'assistenza tecnica 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 mancata disponibilità dei dati se è abilitata l'opzione "scan-mandatory".	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 ha alcuna connessione Vscan per gestire le richieste di scansione antivirus. Ciò potrebbe causare la mancata disponibilità dei dati se è abilitata l'opzione "scan-mandatory".	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 disponibile nel volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che i LIF dei dati siano falliti all'interno del cluster, per cui l'accesso NFS e CIFS è limitato sul nodo. La capacità amministrativa è limitata alle procedure di ripristino locale del nodo per liberare spazio sul volume radice.	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 l'assistenza tecnica NetApp per ulteriori informazioni o assistenza.
Condivisione amministratore inesistente	CRITICO	Problema Vscan: un client ha tentato di connettersi a una condivisione ONTAP_ADMIN$ inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM menzionato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN$ per la SVM.

Spazio dei nomi NVMe esaurito	CRITICO	Uno spazio dei nomi NVMe è stato messo offline a causa di un errore di scrittura causato dalla mancanza di spazio.	Aggiungere spazio al volume e quindi portare online lo spazio dei nomi NVMe utilizzando il comando "vserver nvme namespace modify".
Periodo di grazia NVMe-oF attivo	AVVERTIMENTO	Questo evento si verifica quotidianamente quando è in uso il protocollo NVMe over Fabrics (NVMe-oF) e il periodo di grazia della licenza è attivo. La funzionalità NVMe-oF richiede una licenza dopo la scadenza del periodo di grazia della licenza. La funzionalità NVMe-oF viene disabilitata al termine del periodo di grazia della licenza.	Contatta il tuo rappresentante di vendita per ottenere una licenza NVMe-oF e aggiungerla al cluster oppure rimuovi tutte le istanze della configurazione NVMe-oF dal cluster.
Periodo di grazia NVMe-oF scaduto	AVVERTIMENTO	Il periodo di grazia della licenza NVMe over Fabrics (NVMe-oF) è terminato e la funzionalità NVMe-oF è disabilitata.	Contatta il tuo rappresentante commerciale per ottenere una licenza NVMe-oF e aggiungerla al cluster.
Inizio del periodo di grazia NVMe-oF	AVVERTIMENTO	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 grazia della licenza.	Contatta il tuo rappresentante commerciale per ottenere una licenza NVMe-oF e aggiungerla al cluster.
Host archivio oggetti non risolvibile	CRITICO	Il nome host del server di archiviazione degli oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio oggetti non può comunicare con il server dell'archivio oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero risultare inaccessibili.	Controllare la configurazione DNS per verificare che il nome host sia configurato correttamente con un indirizzo IP.

Object Store Intercluster LIF inattivo	CRITICO	Il client dell'archivio oggetti non riesce a trovare un LIF operativo per comunicare con il server dell'archivio oggetti. Il nodo non consentirà il traffico client dell'archivio oggetti finché il LIF intercluster non sarà operativo. Di conseguenza, i dati potrebbero risultare inaccessibili.	Eseguire le seguenti azioni correttive:…Verificare lo stato del LIF intercluster utilizzando il comando "network interface show -role intercluster"….Verificare che il LIF intercluster sia configurato correttamente e operativo.…Se un LIF intercluster non è configurato, aggiungerlo utilizzando il comando "network interface create -role intercluster".
Mancata corrispondenza della firma dell'archivio oggetti	CRITICO	La firma della richiesta inviata al server dell'archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero risultare inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per ricevere assistenza.
Timeout READDIR	CRITICO	Un'operazione sul file READDIR ha superato il timeout consentito per l'esecuzione in WAFL. Ciò può essere dovuto a directory molto grandi o sparse. Si raccomanda un'azione correttiva.	Eseguire le seguenti azioni correttive:…Trovare informazioni specifiche sulle directory recenti le cui operazioni sui file READDIR sono scadute utilizzando il seguente comando CLI nodeshell con privilegio 'diag': wafl readdir notice show.…Controllare se le directory sono indicate come sparse o meno:…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 della directory. …Se una directory non è indicata come sparse e la directory è di grandi dimensioni, si consiglia di ridurre le dimensioni del file della directory riducendo il numero di voci di file nella directory.

Trasferimento dell’aggregato non riuscito	CRITICO	Questo evento si verifica durante lo spostamento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi degli oggetti.	Eseguire le seguenti azioni correttive:…Verificare che il LIF 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 intercluster del nodo di destinazione. …Verificare che la configurazione dell’archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette 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 l’assistenza tecnica NetApp .
Copia shadow non riuscita	CRITICO	Si è verificato un errore nel servizio Copia Shadow del volume (VSS), un’operazione di backup e ripristino del servizio Microsoft Server.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio dell’evento:…La configurazione della copia shadow è abilitata?…Sono installate le licenze appropriate? …Su quali condivisioni viene eseguita l’operazione di copia shadow?…Il nome della condivisione è corretto?…Il percorso della condivisione esiste?…Quali sono gli stati del set di copie shadow e delle relative copie shadow?

Alimentatori dell'interruttore di archiviazione guasti	AVVERTIMENTO	Manca l'alimentatore nell'interruttore del cluster. La ridondanza è ridotta, il rischio di interruzioni in caso di ulteriori interruzioni di corrente.	Eseguire le seguenti azioni correttive:…Assicurarsi che l'alimentatore principale, che fornisce energia allo switch del cluster, sia acceso.…Assicurarsi che il cavo di alimentazione sia collegato all'alimentatore.…Contattare l'assistenza tecnica NetApp se il problema persiste.
Troppe autenticazioni CIFS	AVVERTIMENTO	Si sono verificate contemporaneamente numerose negoziazioni di autenticazione. Ci sono 256 richieste di nuove sessioni incomplete da questo client.	Indagare sul 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 per cui si è verificato l'errore.
Accesso utente non autorizzato alla condivisione amministratore	AVVERTIMENTO	Un client ha tentato di connettersi alla condivisione privilegiata ONTAP_ADMIN$ anche se l'utente connesso non è un utente autorizzato.	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 attivo utilizzando il comando "vserver vscan scanner pool show-active".

Virus rilevato	AVVERTIMENTO	Un server Vscan ha segnalato un errore al sistema di archiviazione. In genere questo indica che è stato trovato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento.…L'accesso del client al file è negato. A seconda delle impostazioni e della configurazione, il server Vscan potrebbe pulire il file, metterlo in quarantena o eliminarlo.	Controllare il registro del server Vscan riportato nell'evento "syslog" per verificare se è riuscito a pulire, mettere in quarantena o eliminare correttamente il file infetto. Se ciò non fosse possibile, un amministratore di sistema potrebbe dover eliminare manualmente il file.
Volume offline	INFORMAZIONI	Questo messaggio indica che un volume è stato reso offline.	Ripristinare il volume online.
Volume limitato	INFORMAZIONI	Questo evento indica che un volume flessibile è stato reso limitato.	Ripristinare il volume online.
Arresto della VM di archiviazione riuscito	INFORMAZIONI	Questo messaggio viene visualizzato quando un'operazione di 'arresto del vserver' riesce.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di archiviazione.
Nodo Panico	AVVERTIMENTO	Questo evento viene emesso quando si verifica un panico	Contattare l'assistenza clienti NetApp .

Torna all'inizio

Monitor di registro anti-ransomware

Nome del monitor	Gravità	Descrizione	Azione correttiva
Monitoraggio anti-ransomware VM di archiviazione disabilitato	AVVERTIMENTO	Il monitoraggio anti-ransomware per la VM di archiviazione è disabilitato. Abilitare l'anti-ransomware per proteggere la VM di archiviazione.	Nessuno
Monitoraggio anti-ransomware della VM di archiviazione abilitato (modalità di apprendimento)	INFORMAZIONI	Il monitoraggio anti-ransomware per la VM di archiviazione è abilitato in modalità di apprendimento.	Nessuno

Monitoraggio anti-ransomware del volume abilitato	INFORMAZIONI	Il monitoraggio anti-ransomware per il volume è abilitato.	Nessuno
Monitoraggio anti-ransomware del volume disabilitato	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è disabilitato. Abilitare l'anti-ransomware per proteggere il volume.	Nessuno
Monitoraggio anti-ransomware del volume abilitato (modalità di apprendimento)	INFORMAZIONI	Il monitoraggio anti-ransomware per il volume è abilitato in modalità di apprendimento.	Nessuno
Monitoraggio anti-ransomware del volume sospeso (modalità di apprendimento)	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è in pausa in modalità di apprendimento.	Nessuno
Monitoraggio anti-ransomware del volume sospeso	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è sospeso.	Nessuno
Disattivazione del monitoraggio anti-ransomware del volume	AVVERTIMENTO	Il monitoraggio anti-ransomware per il volume è disabilitato.	Nessuno
Attività ransomware rilevata	CRITICO	Per proteggere i dati dal ransomware rilevato, è stata creata una copia Snapshot che può essere utilizzata per ripristinare i dati originali. Il sistema genera e trasmette un messaggio AutoSupport o "chiama casa" al supporto tecnico NetApp e a tutte le destinazioni configurate. Il messaggio AutoSupport migliora la determinazione e la risoluzione dei problemi.	Fare riferimento a "FINAL-DOCUMENT-NAME" per adottare misure correttive in caso di attività ransomware.

Torna all'inizio

FSx per monitor NetApp ONTAP

Nome del monitor	Soglie	Descrizione del monitor	Azione correttiva

La capacità del volume FSx è piena	Attenzione @ > 85 %…Critico @ > 95 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Maggiore è la quantità di dati memorizzati nel volume ONTAP , minore sarà la disponibilità di spazio di archiviazione per i dati futuri. Se la capacità di archiviazione dati all'interno di un volume raggiunge la capacità di archiviazione totale, il cliente potrebbe non essere in grado di archiviare i dati a causa della mancanza di capacità di archiviazione. Il monitoraggio del volume di capacità di archiviazione 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. Valuta l'eliminazione dei dati che non ti servono più per liberare spazio
Volume FSx ad alta latenza	Attenzione @ > 1000 µs…Critico @ > 2000 µs	I volumi sono oggetti che servono il traffico di I/O spesso gestito da applicazioni sensibili alle prestazioni, tra cui applicazioni DevOps, directory home e database. Le latenze elevate possono comportare problemi alle applicazioni stesse, che potrebbero non essere in grado di svolgere i propri compiti. Il monitoraggio delle latenze del volume è fondamentale per mantenere prestazioni costanti dell'applicazione.	Sono necessarie azioni immediate per ridurre al minimo l'interruzione del servizio in caso di superamento della soglia critica:…1. Se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui stiano causando la limitazione del carico di lavoro del volume… Pianificare di intraprendere quanto segue al più presto se la soglia di avviso viene superata:…1. Se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume.…2. Se anche il nodo è sottoposto a un utilizzo elevato, spostare il volume su un altro nodo o ridurre il carico di lavoro totale del nodo.

Limite di inode del volume FSx	Attenzione @ > 85 %…Critico @ > 95 %	I volumi che archiviano i file utilizzano nodi di indice (inode) per archiviare i metadati dei file. Quando un volume esaurisce la sua allocazione di inode, non è possibile aggiungervi altri file. Un avviso di 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 dei 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. Si consiglia di aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora prendi in considerazione la possibilità di dividere il volume in due o più volumi perché il file system ha superato la dimensione massima… Pianifica di intraprendere presto le seguenti azioni se viene superata la soglia di avviso:…1. Si consiglia di aumentare il valore degli inode per il volume. Se il valore degli inode è già al massimo, allora prendi in considerazione la suddivisione del volume in due o più volumi perché il file system è cresciuto oltre la dimensione massima
Sovracommit della quota Qtree del volume FSx	Attenzione @ > 95 %…Critico @ > 100 %	Volume Qtree Quota Overcommit specifica la percentuale in cui un volume è considerato in eccesso rispetto alle quote qtree. È stata raggiunta la soglia impostata per la quota qtree per il volume. Il monitoraggio del superamento della quota qtree del volume garantisce che l'utente riceva un servizio dati ininterrotto.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Eliminare i dati indesiderati… Quando viene superata la soglia di avviso, valutare l'aumento dello spazio del volume.

Lo spazio di riserva dello snapshot FSx è pieno	Attenzione @ > 90 %…Critico @ > 95 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati memorizzati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore sarà la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale per gli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e il livello di protezione dei dati nel volume potrebbe ridursi. Il monitoraggio della capacità 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. Si consiglia di configurare gli snapshot in modo da utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena…2. Si consiglia di eliminare alcuni snapshot più vecchi che potrebbero non essere più necessari per liberare spazio… Si consiglia di intraprendere quanto segue al più presto se la soglia di avviso viene superata:…1. Valutare l'aumento dello spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita…2. Valutare la possibilità di configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena

Rapporto di mancata ricezione della cache del volume FSx	Attenzione @ > 95 %…Critico @ > 100 %	Il rapporto di mancata lettura nella cache del volume è la percentuale di richieste di lettura provenienti dalle applicazioni client che vengono restituite dal disco anziché dalla cache. Ciò significa che il volume ha raggiunto la soglia impostata.	Se viene superata la soglia critica, è necessario adottare misure immediate per ridurre al minimo l'interruzione del servizio: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS… Prendere in considerazione azioni immediate quando viene superata la soglia di avviso: 1. Spostare alcuni carichi di lavoro dal nodo del volume per ridurre il carico di I/O 2. Ridurre la richiesta di carichi di lavoro a priorità inferiore sullo stesso nodo tramite limiti QoS 3. Modificare le caratteristiche del carico di lavoro (dimensione del blocco, memorizzazione nella cache dell'applicazione, ecc.)

Torna all'inizio

Monitor K8s

Nome del monitor	Descrizione	Azioni correttive	Gravità/Soglia

Latenza del volume persistente elevata	Le latenze elevate e persistenti possono compromettere il funzionamento delle applicazioni stesse e impedirne lo svolgimento delle attività. Il monitoraggio delle latenze persistenti dei volumi è fondamentale per mantenere prestazioni costanti delle 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** Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: se al volume è assegnata una policy QoS, valutare le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. **Azioni da intraprendere al più presto** Se la soglia di allerta viene superata, pianificare le seguenti azioni immediate: 1. Se anche il pool di archiviazione è sottoposto a un utilizzo elevato, spostare il volume in un altro pool di archiviazione. 2. Se al volume è assegnata una policy QoS, valutarne le soglie limite nel caso in cui causino la limitazione del carico di lavoro del volume. 3. Se anche il controller è sottoposto a un utilizzo elevato, spostare il volume su un altro controller o ridurre il carico di lavoro totale del controller.	Attenzione @ > 6.000 µs Critico @ > 12.000 µs
Saturazione della memoria del cluster elevata	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 su tutti i nodi K8.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Attenzione @ > 80 % Critico @ > 90 %
Collegamento POD non riuscito	Questo avviso si verifica quando un collegamento di volume con POD non riesce.		Avvertimento

Alta velocità di ritrasmissione	Elevata velocità di ritrasmissione TCP	Verifica la congestione della rete: identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 10 % Critico @ > 25 %
Capacità elevata del file system del nodo	Capacità elevata del file system del nodo	- Aumentare le dimensioni dei dischi dei nodi per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo dei file dell'applicazione.	Attenzione @ > 80 % Critico @ > 90 %
Jitter di rete del carico di lavoro elevato	Elevato jitter TCP (elevate variazioni di latenza/tempo di risposta)	Verificare la congestione della rete. Identificare i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware	Attenzione @ > 30 ms Critico @ > 50 ms

Throughput del volume persistente	Le soglie MBPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di prestazioni predefinite, con un potenziale impatto su altri volumi persistenti. L'attivazione di questo monitor genererà avvisi appropriati per il tipico profilo di throughput dei volumi persistenti sugli SSD. Questo monitor coprirà tutti i volumi persistenti sul tuo tenant. I valori di soglia critici e di avviso possono essere regolati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando soglie appropriate per la classe di archiviazione. Un monitor duplicato può essere ulteriormente indirizzato a un sottoinsieme dei volumi persistenti sul tenant.	**Azioni immediate** Se viene superata la soglia critica, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introdurre limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie. **Azioni da intraprendere a breve** Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti azioni: 1. Introdurre limiti QoS MBPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie.	Attenzione @ > 10.000 MB/s Critico @ > 15.000 MB/s
Contenitore a rischio di OOM ucciso	I limiti di memoria del contenitore sono impostati troppo bassi. Il contenitore rischia di essere espulso (Out of Memory Kill).	Aumentare i limiti di memoria del contenitore.	Attenzione @ > 95 %
Carico di lavoro ridotto	Il carico di lavoro non ha pod sani.		Critico @ < 1
Vincolo di richiesta di volume persistente non riuscito	Questo avviso si verifica quando un collegamento su un PVC non riesce.		Avvertimento
I limiti di ResourceQuota Mem stanno per essere superati	I limiti di memoria per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %
Richieste di memoria ResourceQuota in procinto di superare	Le richieste di memoria per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %

Creazione del nodo non riuscita	Non è stato possibile pianificare il nodo a causa di un errore di configurazione.	Controllare il registro eventi di Kubernetes per individuare la causa dell'errore di configurazione.	Critico
Recupero del volume persistente non riuscito	Il volume non ha superato il recupero automatico.		Attenzione @ > 0 B
Limitazione della CPU del contenitore	I limiti della CPU del contenitore sono impostati su un valore troppo basso. I processi dei contenitori vengono rallentati.	Aumentare i limiti della CPU del contenitore.	Attenzione @ > 95 % Critico @ > 98 %
Impossibile eliminare il servizio Load Balancer			Avvertimento
IOPS del volume persistente	Le soglie IOPS sui volumi persistenti possono essere utilizzate per avvisare un amministratore quando i volumi persistenti superano le aspettative di prestazioni predefinite. L'attivazione di questo monitor genererà avvisi appropriati per il tipico profilo IOPS dei volumi di persistenza. Questo monitor coprirà tutti i volumi persistenti sul tuo tenant. I valori di soglia di avviso e critici possono essere regolati in base agli obiettivi di monitoraggio duplicando questo monitor e impostando soglie appropriate per il carico di lavoro.	**Azioni immediate** Se viene superata la soglia critica, pianificare azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Introdurre limiti QoS IOPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie. **Azioni da intraprendere al più presto** Se la soglia di allerta viene superata, pianificare le seguenti azioni immediate: 1. Introdurre limiti QoS IOPS per il volume. 2. Esaminare l'applicazione che gestisce il carico di lavoro sul volume per individuare eventuali anomalie.	Attenzione @ > 20.000 IO/s Critico @ > 25.000 IO/s
Impossibile aggiornare il servizio Load Balancer			Avvertimento
Montaggio POD non riuscito	Questo avviso si verifica quando un montaggio su un POD non riesce.		Avvertimento

Pressione PID del nodo	Gli identificatori di processo disponibili sul nodo (Linux) sono scesi al di sotto di una soglia di espulsione.	Trova e correggi i pod che generano molti processi e privano il nodo degli ID di processo disponibili. Imposta PodPidsLimit per proteggere il tuo nodo da pod o container che generano troppi processi.	Critico @ > 0
Errore di estrazione dell'immagine del pod	Kubernetes non è riuscito a estrarre l'immagine del contenitore pod.	- Assicurarsi che l'immagine del pod sia scritta correttamente nella configurazione del pod. - Controlla che il tag immagine esista nel tuo registro. - Verificare le credenziali per il registro delle immagini. - Verificare la presenza di problemi di connettività del registro. - Verificare di non superare i limiti di velocità imposti dai fornitori del registro pubblico.	Avvertimento
Lavoro in esecuzione da troppo tempo	Il lavoro è in esecuzione da troppo tempo		Attenzione @ > 1 ora Critico @ > 5 ore
Memoria del nodo elevata	L'utilizzo della memoria del nodo è elevato	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Attenzione @ > 85 % Critico @ > 90 %
I limiti della CPU di ResourceQuota stanno per essere superati	I limiti della CPU per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %
Pod Crash Loop Backoff	Pod si è bloccato e ha tentato di riavviarsi più volte.		Critico @ > 3
Nodo CPU alto	L'utilizzo della CPU del nodo è elevato.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare CPU sui nodi.	Attenzione @ > 80 % Critico @ > 90 %
Latenza di rete del carico di lavoro RTT elevata	Elevata latenza TCP RTT (tempo di andata e ritorno)	Verifica la congestione della rete ▒ Identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 150 ms Critico @ > 300 ms

Lavoro fallito	Il processo non è stato completato correttamente a causa di un arresto anomalo o riavvio del nodo, esaurimento delle risorse, timeout del processo o errore di pianificazione del pod.	Controllare i registri eventi di Kubernetes per individuare le cause degli errori.	Attenzione @ > 1
Volume persistente pieno in pochi giorni	Il volume persistente esaurirà lo spazio tra qualche giorno	-Aumentare le dimensioni del volume per garantire che ci sia spazio sufficiente per i file dell'applicazione. -Ridurre la quantità di dati memorizzati nelle applicazioni.	Attenzione @ < 8 giorni Critico @ < 3 giorni
Pressione della memoria del nodo	Il nodo sta esaurendo la memoria. La memoria disponibile ha raggiunto la soglia di espulsione.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare memoria sui nodi.	Critico @ > 0
Nodo non pronto	Il nodo non è pronto da 5 minuti	Verificare che il nodo disponga di risorse sufficienti di CPU, memoria e disco. Controllare la connettività della rete del nodo. Controllare i registri eventi di Kubernetes per individuare le cause degli errori.	Critico @ < 1
Capacità di volume persistente elevata	La capacità utilizzata dal backend del volume persistente è elevata.	- Aumentare le dimensioni del volume per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre la quantità di dati memorizzati nelle applicazioni.	Attenzione @ > 80 % Critico @ > 90 %
Impossibile creare il servizio di bilanciamento del carico	Creazione del servizio di bilanciamento del carico non riuscita		Critico
Mancata corrispondenza della replica del carico di lavoro	Alcuni pod non sono attualmente disponibili per un Deployment o un DaemonSet.		Attenzione @ > 1
Richieste CPU ResourceQuota in procinto di superare	Le richieste di CPU per Namespace stanno per superare ResourceQuota		Attenzione @ > 80 % Critico @ > 90 %

Alta velocità di ritrasmissione	Elevata velocità di ritrasmissione TCP	Verifica la congestione della rete: identifica i carichi di lavoro che consumano molta larghezza di banda della rete. Verificare l'elevato utilizzo della CPU del Pod. Controllare le prestazioni della rete hardware.	Attenzione @ > 10 % Critico @ > 25 %
Pressione del disco del nodo	Lo spazio su disco disponibile e gli inode sul file system radice o sul file system immagine del nodo hanno soddisfatto una soglia di espulsione.	- Aumentare le dimensioni dei dischi dei nodi per garantire che vi sia spazio sufficiente per i file dell'applicazione. - Ridurre l'utilizzo dei file dell'applicazione.	Critico @ > 0
Saturazione CPU cluster elevata	La saturazione della CPU allocabile nel cluster è elevata. La saturazione della CPU del cluster viene calcolata come la somma dell'utilizzo della CPU divisa per la somma delle CPU allocabili su tutti i nodi K8.	Aggiungi nodi. Correggere eventuali nodi non programmati. Pod di dimensioni adeguate per liberare CPU sui nodi.	Attenzione @ > 80 % Critico @ > 90 %

Torna all'inizio

Monitor del registro delle modifiche

Nome del monitor	Gravità	Descrizione del monitor
Volume interno scoperto	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 archiviazione scoperto	Informativo	Questo messaggio viene visualizzato quando viene rilevato un nodo di archiviazione.
Nodo di archiviazione rimosso	Informativo	Questo messaggio viene visualizzato quando viene rimosso un nodo di archiviazione.
Pool di archiviazione scoperto	Informativo	Questo messaggio viene visualizzato quando viene rilevato un pool di archiviazione.

Macchina virtuale di archiviazione scoperta	Informativo	Questo messaggio viene visualizzato quando viene rilevata una macchina virtuale di archiviazione.
Macchina virtuale di archiviazione modificata	Informativo	Questo messaggio viene visualizzato quando viene modificata una macchina virtuale di archiviazione.

Torna all'inizio

Monitor di raccolta dati

Nome del monitor	Descrizione	Azione correttiva
Arresto dell'unità di acquisizione	Le unità di acquisizione Data Infrastructure Insights vengono riavviate periodicamente come parte degli aggiornamenti per introdurre nuove funzionalità. In un ambiente tipico, questo accade una volta al mese o meno. Un avviso di avviso che segnala l'arresto di un'unità di acquisizione dovrebbe essere seguito subito dopo da una risoluzione che segnala che l'unità di acquisizione appena riavviata ha completato una registrazione con Data Infrastructure Insights. In genere, il ciclo di spegnimento-registrazione dura dai 5 ai 15 minuti.	Se l'avviso si verifica frequentemente o dura più di 15 minuti, verificare il funzionamento del sistema che ospita l'Unità di acquisizione, della rete e di qualsiasi proxy che collega l'AU a Internet.
Collettore fallito	Il sondaggio di un raccoglitore di dati ha riscontrato una situazione di errore imprevista.	Per saperne di più sulla situazione, visita la pagina del raccoglitore dati in Data Infrastructure Insights .
Avviso al collezionista	Questo avviso può in genere verificarsi a causa di una configurazione errata del raccoglitore dati o del sistema di destinazione. Rivedere le configurazioni per evitare futuri avvisi. Può anche essere dovuto al recupero di dati incompleti, mentre il raccoglitore di dati ha raccolto tutti i dati che poteva. Ciò può accadere 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 raccoglitore dati o del sistema di destinazione. Si noti che il monitor per Collector Warning può inviare più avvisi rispetto ad altri tipi di monitor, pertanto si consiglia di non impostare alcun destinatario di avviso, a meno che non si stia risolvendo un problema.

Torna all'inizio

Monitor di sicurezza

Nome del monitor	Soglia	Descrizione del monitor	Azione correttiva
AutoSupport HTTPS AutoSupport disabilitato	Attenzione @ < 1	AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei messaggi AutoSupport , NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio dei 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
Cifrari non sicuri del cluster per SSH	Attenzione @ < 1	Indica che SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere i cifrari CBC, eseguire il seguente comando ONTAP :…security ssh remove -vserver <admin vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner di accesso al cluster disabilitato	Attenzione @ < 1	Indica che il banner di accesso è disabilitato per gli utenti che accedono al sistema ONTAP . La visualizzazione di un banner di accesso è utile per stabilire le aspettative relative all'accesso e all'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 del cluster non crittografata	Attenzione @ < 1	Quando si replicano dati per il ripristino di emergenza, la memorizzazione nella cache o il backup, è necessario proteggere tali dati 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 tra peer del cluster create prima di ONTAP 9.6, il cluster di origine e quello di destinazione devono essere aggiornati alla versione 9.6. Quindi utilizzare il comando "cluster peer modify" per modificare sia i peer del cluster di origine che quelli di destinazione in modo che utilizzino la crittografia del peering del cluster. Per i dettagli, consultare la Guida al rafforzamento della sicurezza NetApp per ONTAP 9.
Utente amministratore locale predefinito abilitato	Attenzione @ > 0	NetApp consiglia di bloccare (disabilitare) tutti gli account utente amministratore predefiniti (integrati) non necessari con il comando lock. Si tratta principalmente di account predefiniti le cui password non sono mai state aggiornate o modificate.	Per bloccare l'account "admin" predefinito, eseguire il seguente comando ONTAP :…security login lock -username admin
Modalità FIPS disabilitata	Attenzione @ < 1	Quando è abilitata la conformità FIPS 140-2, TLSv1 e SSLv3 sono disabilitati e rimangono abilitati solo TLSv1.1 e TLSv1.2. ONTAP impedisce di abilitare TLSv1 e SSLv3 quando è abilitata la conformità FIPS 140-2.	Per abilitare la conformità FIPS 140-2 su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzata:…security config modify -interface SSL -is -fips-enabled true

Inoltro del registro non crittografato	Attenzione @ < 1	Lo scaricamento delle informazioni syslog è necessario per limitare la portata o l'impatto di una violazione su un singolo sistema o soluzione. Pertanto, NetApp consiglia di scaricare in modo sicuro le informazioni syslog in un luogo di archiviazione o conservazione sicuro.	Una volta creata una destinazione di inoltro dei log, il suo protocollo non può essere modificato. Per passare a un protocollo crittografato, eliminare e ricreare la destinazione di inoltro del registro utilizzando il seguente comando ONTAP :…cluster log-forwarding create -destination <destination ip> -protocol tcp-encrypted
Password con 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 dovrebbero migrare alla funzione hash SHA-512.	NetApp consiglia vivamente agli account utente di migrare alla soluzione SHA-512 più sicura, chiedendo agli utenti di modificare 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 è configurato	Attenzione @ < 1	Indica che il cluster non ha 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 <nome host o indirizzo IP del server ntp>
Il numero di server NTP è basso	Attenzione @ < 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 <nome host o indirizzo IP del server ntp>

Shell remota abilitata	Attenzione @ > 0	Remote Shell non è un metodo sicuro per stabilire l'accesso tramite riga di comando alla soluzione ONTAP . Per un accesso remoto sicuro, Remote Shell deve essere disabilitato.	NetApp consiglia Secure Shell (SSH) per l'accesso remoto sicuro. Per disabilitare la shell remota su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzato: security protocol modify -application rsh- enabled false
Registro di controllo della VM di archiviazione disabilitato	Attenzione @ < 1	Indica che la registrazione di controllo è disabilitata per SVM.	Per configurare il registro di controllo per un vserver, eseguire il seguente comando ONTAP :…vserver audit enable -vserver <svm>
Cifrature non sicure per SSH nella VM di archiviazione	Attenzione @ < 1	Indica che SSH utilizza cifrari non sicuri, ad esempio cifrari che iniziano con *cbc.	Per rimuovere i cifrari CBC, eseguire il seguente comando ONTAP :…security ssh remove -vserver <vserver> -ciphers aes256-cbc,aes192-cbc,aes128-cbc,3des-cbc
Banner di accesso alla VM di archiviazione disabilitato	Attenzione @ < 1	Indica che il banner di accesso è disabilitato per gli utenti che accedono alle SVM sul sistema. La visualizzazione di un banner di accesso è utile per stabilire le aspettative relative all'accesso e all'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 abilitato	Attenzione @ > 0	Telnet non è un metodo sicuro per stabilire l'accesso tramite riga di comando alla soluzione ONTAP . Per un accesso remoto sicuro, Telnet dovrebbe essere disabilitato.	NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro. Per disabilitare Telnet su un cluster, eseguire il seguente comando ONTAP in modalità privilegio avanzato:…security protocol modify -application telnet -enabled false

Torna all'inizio

Monitor della protezione dei dati

Nome del monitor	Soglie	Descrizione del monitor	Azione correttiva
Spazio insufficiente per la copia snapshot LUN	(Filtro contains_luns = Sì) Avviso @ > 95 %…Critico @ > 100 %	La capacità di archiviazione di un volume è necessaria per archiviare i dati delle applicazioni e dei clienti. Una parte di questo spazio, denominato spazio riservato agli snapshot, viene utilizzata per archiviare gli snapshot che consentono di proteggere i dati a livello locale. Maggiore è la quantità di dati nuovi e aggiornati memorizzati nel volume ONTAP , maggiore è la capacità di snapshot utilizzata e minore sarà la capacità di archiviazione snapshot disponibile per futuri dati nuovi o aggiornati. Se la capacità dei dati snapshot all'interno di un volume raggiunge lo spazio di riserva totale degli snapshot, il cliente potrebbe non essere in grado di archiviare nuovi dati snapshot e potrebbe verificarsi una riduzione del livello di protezione dei dati nelle LUN del volume. Il monitoraggio della capacità snapshot del volume utilizzato garantisce la continuità dei servizi dati.	**Azioni immediate** Se viene superata la soglia critica, prendere in considerazione azioni immediate per ridurre al minimo l'interruzione del servizio: 1. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena. 2. Elimina alcuni vecchi snapshot indesiderati per liberare spazio. **Azioni da intraprendere a breve** Se la soglia di allerta viene superata, pianificare di adottare immediatamente le seguenti azioni: 1. Aumentare lo spazio di riserva degli snapshot all'interno del volume per adattarsi alla crescita. 2. Configurare gli snapshot per utilizzare lo spazio dati nel volume quando la riserva di snapshot è piena.

Ritardo nella relazione SnapMirror	Attenzione @ > 150%…Critico @ > 300%	Il ritardo nella relazione SnapMirror è la differenza tra il timestamp 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 della policy SnapMirror . Se il tempo di ritardo è uguale all'intervallo di pianificazione, lag_time_percent sarà pari al 100%. Se il criterio SnapMirror non ha una pianificazione, lag_time_percent non verrà calcolato.	Monitorare lo stato SnapMirror utilizzando il comando "snapmirror show". Controlla la cronologia dei trasferimenti SnapMirror usando il comando "snapmirror show-history"

Torna all'inizio

Monitor del volume delle nuvole (CVO)

Nome del monitor	Gravità CI	Descrizione del monitor	Azione correttiva
Disco CVO fuori servizio	INFORMAZIONI	Questo evento si verifica quando un disco viene rimosso dal servizio perché è stato contrassegnato come guasto, è in fase di sanificazione o è entrato nel Centro di manutenzione.	Nessuno

Restituzione CVO del pool di archiviazione non riuscita	CRITICO	Questo evento si verifica durante la migrazione di un aggregato come parte di un giveback di failover di archiviazione (SFO), quando il nodo di destinazione non riesce a raggiungere gli archivi di oggetti.	Eseguire le seguenti azioni correttive: verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show". Verificare la connettività di rete al server di archiviazione degli oggetti utilizzando il comando "ping" sul nodo di destinazione intercluster LIF. Verificare che la configurazione dell'archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette utilizzando il comando "aggregate object-store config show". In alternativa, è possibile ignorare l'errore specificando false per il parametro "require-partner-waiting" del comando giveback. Per ulteriori informazioni o assistenza, contattare l'assistenza tecnica NetApp .

Interconnessione CVO HA inattiva	AVVERTIMENTO	L'interconnessione ad alta disponibilità (HA) non funziona. 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 non funziona. Se i collegamenti non funzionano: verificare che entrambi i controller nella coppia HA siano operativi. Per i collegamenti collegati esternamente, assicurarsi che i cavi di interconnessione siano collegati correttamente e che i moduli SFP (Small Form-Factor Pluggable), se applicabili, siano posizionati correttamente su entrambi i controller. Per i collegamenti collegati internamente, disattivare e riattivare i collegamenti, uno dopo l'altro, utilizzando i comandi "ic link off" e "ic link on". Se i collegamenti sono disabilitati, abilitarli utilizzando 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" e "ic link on". Se il problema persiste, contattare l'assistenza tecnica NetApp .

Superato il numero massimo di sessioni CVO per utente	AVVERTIMENTO	Hai superato il numero massimo di sessioni consentite per utente su una connessione TCP. Ogni richiesta di stabilire una sessione verrà respinta finché alcune sessioni non saranno rilasciate.	Eseguire le seguenti azioni correttive: ispezionare 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-opens-same -file-per-tree". In alcuni casi i clienti funzionano come previsto, ma richiedono una soglia più alta. Dovresti avere 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 l'assistenza tecnica NetApp .

Conflitto di nomi NetBIOS CVO	CRITICO	Il servizio nomi NetBIOS ha ricevuto una risposta negativa a una richiesta di registrazione del nome da un computer remoto. In genere ciò è causato 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 distribuzione dei dati corretto nel cluster.	Eseguire una delle seguenti azioni correttive: Se si verifica un conflitto nel nome NetBIOS o in un alias, eseguire una delle seguenti operazioni: Eliminare l'alias NetBIOS duplicato utilizzando il comando "vserver cifs delete -aliases 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 -aliases alias -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" 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 il NetBIOS sul computer remoto.
Pool di archiviazione CVO NFSv4 esaurito	CRITICO	Un pool di archiviazione NFSv4 è esaurito.	Se il server NFS non risponde per più di 10 minuti dopo questo evento, contattare l'assistenza tecnica NetApp .
Panico del nodo CVO	AVVERTIMENTO	Questo evento viene emesso quando si verifica un panico	Contattare l'assistenza clienti NetApp .

Spazio basso nel volume radice del nodo CVO	CRITICO	Il sistema ha rilevato che lo spazio disponibile nel volume root è pericolosamente basso. Il nodo non è completamente operativo. È possibile che i LIF dei dati siano falliti all'interno del cluster, per cui l'accesso NFS e CIFS è limitato sul nodo. La capacità amministrativa è limitata alle procedure di ripristino locale del nodo per liberare spazio sul volume radice.	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 l'assistenza tecnica NetApp .
Condivisione amministratore inesistente CVO	CRITICO	Problema Vscan: un client ha tentato di connettersi a una condivisione ONTAP_ADMIN$ inesistente.	Assicurarsi che Vscan sia abilitato per l'ID SVM menzionato. L'abilitazione di Vscan su una SVM determina la creazione automatica della condivisione ONTAP_ADMIN$ per la SVM.
Host archivio oggetti CVO non risolvibile	CRITICO	Il nome host del server di archiviazione degli oggetti non può essere risolto in un indirizzo IP. Il client dell'archivio oggetti non può comunicare con il server dell'archivio oggetti senza risolvere un indirizzo IP. Di conseguenza, i dati potrebbero risultare 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 oggetti non riesce a trovare un LIF operativo per comunicare con il server dell'archivio oggetti. Il nodo non consentirà il traffico client dell'archivio oggetti finché il LIF intercluster non sarà operativo. Di conseguenza, i dati potrebbero risultare inaccessibili.	Eseguire le seguenti azioni correttive: verificare lo stato LIF intercluster utilizzando il comando "network interface show -role intercluster". Verificare che il LIF intercluster sia configurato correttamente e operativo. Se non è configurato un LIF intercluster, aggiungerlo utilizzando il comando "network interface create -role intercluster".

Mancata corrispondenza della firma dell'archivio oggetti CVO	CRITICO	La firma della richiesta inviata al server dell'archivio oggetti non corrisponde alla firma calcolata dal client. Di conseguenza, i dati potrebbero risultare inaccessibili.	Verificare che la chiave di accesso segreta sia configurata correttamente. Se la configurazione è corretta, contattare il supporto tecnico NetApp per ricevere assistenza.
Memoria monitor QoS CVO esaurita	CRITICO	La memoria dinamica del sottosistema QoS ha raggiunto il limite per l'hardware della piattaforma attuale. Alcune funzionalità QoS potrebbero funzionare con 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 <nome carico di lavoro> *" per eliminare i flussi associati dal carico di lavoro attivo.

Timeout CVO READDIR	CRITICO	Un’operazione sul file READDIR ha superato il timeout consentito per l’esecuzione in WAFL. Ciò può essere dovuto a directory molto grandi o sparse. Si raccomanda un’azione correttiva.	Eseguire le seguenti azioni correttive: trovare informazioni specifiche sulle directory recenti le cui operazioni sui file READDIR sono scadute utilizzando il seguente comando CLI nodeshell con privilegio 'diag': wafl readdir notice show. Controllare se le directory sono indicate come sparse o meno: 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 della directory. Se una directory non è indicata come sparse e la directory è di grandi dimensioni, si consiglia di ridurre le dimensioni del file della directory riducendo il numero di voci di file nella directory.

Errore di rilocazione CVO del pool di archiviazione	CRITICO	Questo evento si verifica durante lo spostamento di un aggregato, quando il nodo di destinazione non riesce a raggiungere gli archivi degli oggetti.	Eseguire le seguenti azioni correttive: verificare che il LIF intercluster sia online e funzionante utilizzando il comando "network interface show". Verificare la connettività di rete al server di archiviazione degli oggetti utilizzando il comando "ping" sul nodo di destinazione intercluster LIF. Verificare che la configurazione dell'archivio oggetti non sia cambiata e che le informazioni di accesso e connettività siano ancora corrette 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 l'assistenza tecnica NetApp .
Copia shadow CVO non riuscita	CRITICO	Si è verificato un errore nel servizio Copia Shadow del volume (VSS), un'operazione di backup e ripristino del servizio Microsoft Server.	Verificare quanto segue utilizzando le informazioni fornite nel messaggio dell'evento: la configurazione della copia shadow è abilitata? Sono installate le licenze appropriate? Su quali condivisioni viene eseguita l'operazione di copia shadow? Il nome della condivisione è corretto? Esiste il percorso di condivisione? Quali sono gli stati del set di copie shadow e delle sue copie shadow?
Arresto riuscito della VM di archiviazione CVO	INFORMAZIONI	Questo messaggio viene visualizzato quando un'operazione di 'arresto del vserver' riesce.	Utilizzare il comando 'vserver start' per avviare l'accesso ai dati su una VM di archiviazione.

CVO Troppe autenticazioni CIFS	AVVERTIMENTO	Si sono verificate contemporaneamente numerose negoziazioni di autenticazione. Ci sono 256 richieste di nuove sessioni incomplete da questo client.	Indagare sul 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 per cui si è verificato l'errore.
Dischi CVO non assegnati	INFORMAZIONI	Il sistema ha dischi non assegnati: la capacità viene sprecata e potrebbe essere stata applicata una configurazione errata o una modifica parziale della configurazione del sistema.	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	AVVERTIMENTO	Un client ha tentato di connettersi alla condivisione privilegiata ONTAP_ADMIN$ anche se l'utente connesso non è un utente autorizzato.	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 attivo utilizzando il comando "vserver vscan scanner pool show-active".
Rilevato virus CVO	AVVERTIMENTO	Un server Vscan ha segnalato un errore al sistema di archiviazione. In genere questo indica che è stato trovato un virus. Tuttavia, altri errori sul server Vscan possono causare questo evento. L'accesso del client al file è negato. A seconda delle impostazioni e della configurazione, il server Vscan potrebbe pulire il file, metterlo in quarantena o eliminarlo.	Controllare il registro del server Vscan riportato nell'evento "syslog" per verificare se è riuscito a pulire, mettere in quarantena o eliminare correttamente il file infetto. Se ciò non fosse possibile, un amministratore di sistema potrebbe dover eliminare manualmente il file.
Volume CVO offline	INFORMAZIONI	Questo messaggio indica che un volume è stato reso offline.	Ripristinare il volume online.

Volume CVO limitato	INFORMAZIONI	Questo evento indica che un volume flessibile è stato reso limitato.	Ripristinare il volume online.

Torna all'inizio

Monitoraggio dei log dei mediatori SnapMirror for Business Continuity (SMBC)

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Aggiunto mediatore ONTAP	INFORMAZIONI	Questo messaggio viene visualizzato quando ONTAP Mediator viene aggiunto correttamente a un cluster.	Nessuno
Mediatore ONTAP non accessibile	CRITICO	Questo messaggio viene visualizzato quando ONTAP Mediator viene riadattato oppure il pacchetto Mediator non è più installato sul server Mediator. Di conseguenza, il failover SnapMirror non è possibile.	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Rimosso il mediatore ONTAP	INFORMAZIONI	Questo messaggio viene visualizzato quando ONTAP Mediator viene rimosso correttamente da un cluster.	Nessuno
Mediatore ONTAP irraggiungibile	AVVERTIMENTO	Questo messaggio viene visualizzato quando il mediatore ONTAP non è raggiungibile su un cluster. Di conseguenza, il failover SnapMirror non è possibile.	Verificare la connettività di rete al mediatore ONTAP utilizzando i comandi "network ping" e "network traceroute". Se il problema persiste, rimuovere la configurazione dell'attuale ONTAP Mediator utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Certificato CA SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato CA sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato CA SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato dell'autorità di certificazione (CA) ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato CA sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato client ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato client SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato client ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Relazione SMBC fuori sincrono Nota: UM non ha questo	CRITICO	Questo messaggio viene visualizzato quando una relazione SnapMirror for Business Continuity (SMBC) cambia stato da "in sincronia" a "non sincronizzata". A causa di questo RPO=0 la protezione dei dati verrà interrotta.	Controllare la connessione di rete tra i volumi di origine e di destinazione. Monitorare lo stato della relazione SMBC utilizzando il comando "snapmirror show" sulla destinazione e il comando "snapmirror list-destinations" sulla sorgente. La risincronizzazione automatica tenterà di riportare la relazione allo stato "sincronizzata". Se la risincronizzazione fallisce, verificare che tutti i nodi del cluster siano in quorum e integri.
Certificato del server SMBC scaduto	CRITICO	Questo messaggio viene visualizzato quando il certificato del server ONTAP Mediator è scaduto. Di conseguenza, non sarà possibile alcuna ulteriore comunicazione con il mediatore ONTAP .	Rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato server sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".
Certificato del server SMBC in scadenza	AVVERTIMENTO	Questo messaggio viene visualizzato quando il certificato del server ONTAP Mediator scade entro i prossimi 30 giorni.	Prima che questo certificato scada, rimuovere la configurazione dell'attuale mediatore ONTAP utilizzando il comando "snapmirror mediator remove". Aggiornare un nuovo certificato server sul server ONTAP Mediator. Riconfigurare l'accesso al mediatore ONTAP utilizzando il comando "snapmirror mediator add".

Torna all'inizio

Monitor di sistema aggiuntivi per alimentazione, battito cardiaco e altri parametri

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Scoperto l'alimentatore del ripiano del disco	INFORMATIVO	Questo messaggio viene visualizzato quando un alimentatore viene aggiunto allo scaffale dei dischi.	NESSUNO
Ripiani del disco Alimentatore rimosso	INFORMATIVO	Questo messaggio viene visualizzato quando un alimentatore viene rimosso dal ripiano del disco.	NESSUNO
Commutazione automatica non pianificata di MetroCluster disabilitata	CRITICO	Questo messaggio viene visualizzato quando la funzionalità di commutazione automatica non pianificata è disabilitata.	Eseguire il comando "metrocluster modify -node-name <nodename> -automatic-switchover -onfailure true" per ciascun nodo del cluster per abilitare il passaggio automatico.
MetroCluster Storage Bridge non raggiungibile	CRITICO	Il bridge di archiviazione non è raggiungibile tramite la rete di gestione	1) Se il bridge è monitorato da SNMP, verificare che il LIF di gestione del nodo sia attivo utilizzando il comando "network interface show". Verificare che il bridge sia attivo utilizzando il comando "network ping". 2) Se il bridge è monitorato in banda, controllare il cablaggio fabric al bridge e quindi verificare che il bridge sia acceso.
Temperatura anomala del ponte MetroCluster - inferiore al valore critico	CRITICO	Il sensore sul bridge Fibre Channel segnala una temperatura inferiore alla soglia critica.	1) Verificare lo stato operativo delle ventole sul ponte di accumulo. 2) Verificare che il ponte funzioni alle condizioni di temperatura consigliate.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Temperatura anomala del ponte MetroCluster - superiore al valore critico	CRITICO	Il sensore sul bridge Fibre Channel segnala una temperatura superiore alla soglia critica.	1) Verificare lo stato operativo del sensore di temperatura del telaio sullo storage bridge utilizzando il comando "storage bridge show -cooling". 2) Verificare che il ponte di archiviazione funzioni alle condizioni di temperatura consigliate.
MetroCluster Aggregate lasciato indietro	AVVERTIMENTO	L'aggregato è rimasto indietro durante il tornante.	1) Controllare lo stato dell'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 di Metrocluster sono inattivi	CRITICO	Gli adattatori di interconnessione RDMA e i LIF intercluster hanno interrotto le connessioni al cluster peered oppure il cluster peered è inattivo.	1) Assicurarsi che i LIF intercluster siano attivi e funzionanti. Riparare i LIF intercluster se sono inattivi. 2) Verificare che il cluster peer sia attivo e funzionante utilizzando il comando "cluster peer ping". Se il cluster peer è inattivo, consultare la Guida al ripristino di emergenza MetroCluster . 3) Per il fabric MetroCluster, verificare che gli ISL del fabric back-end siano attivi e funzionanti. Riparare gli ISL del fabric back-end se sono inattivi. 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 funzionano.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
I partner MetroCluster non sono raggiungibili tramite la rete di peering	CRITICO	La connettività al cluster peer è interrotta.	1) Assicurarsi che la porta sia collegata alla rete/switch corretto. 2) Assicurarsi che il LIF intercluster sia connesso al cluster peer. 3) Assicurarsi che il cluster peer sia attivo e funzionante utilizzando il comando "cluster peer ping". Se il cluster peer è inattivo, fare riferimento alla Guida al ripristino di emergenza MetroCluster .
MetroCluster Inter Switch Tutti i collegamenti non attivi	CRITICO	Tutti i collegamenti Inter-Switch (ISL) sullo switch di archiviazione sono inattivi.	1) Riparare gli ISL del fabric back-end sullo switch di archiviazione. 2) Assicurarsi che lo switch del partner sia attivo e che i suoi ISL siano operativi. 3) Assicurarsi che le apparecchiature intermedie, come i dispositivi xWDM, siano operative.
Collegamento SAS tra nodo MetroCluster e stack di archiviazione non attivo	AVVERTIMENTO	Il problema potrebbe essere dovuto all'adattatore SAS o al cavo collegato.	1. Verificare che l'adattatore SAS sia online e in esecuzione. 2. Verificare che il collegamento fisico del cavo sia sicuro e funzionante e, se necessario, sostituire il cavo. 3. Se l'adattatore SAS è collegato agli scaffali dei dischi, assicurarsi che gli IOM e i dischi siano posizionati correttamente.
Collegamenti dell'iniziatore MetroClusterFC non attivi	CRITICO	L'adattatore dell'iniziatore FC è difettoso.	1. Assicurarsi che il collegamento dell'iniziatore FC non sia stato manomesso. 2. Verificare lo stato operativo dell'adattatore dell'iniziatore FC utilizzando il comando "system node run -node local -command storage show adapter".

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Collegamento di 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" utilizzando il comando "metrocluster interconnect adapter show". 3. Se la configurazione include switch fabric, assicurarsi che siano cablati e configurati correttamente.
Dischi di riserva MetroCluster lasciati indietro	AVVERTIMENTO	Il disco di riserva è stato lasciato indietro durante il ritorno.	Se il disco non è danneggiato, restituirlo al proprietario originale utilizzando il comando "metrocluster switchback".
Porta del ponte di archiviazione MetroCluster inattiva	CRITICO	La porta sul bridge di archiviazione è offline.	1) Verificare lo stato operativo delle porte sullo storage bridge utilizzando il comando "storage bridge show -ports". 2) Verificare la connettività logica e fisica alla porta.
Ventole dello switch di archiviazione MetroCluster guaste	CRITICO	La ventola dell'interruttore di archiviazione è guasta.	1) Assicurarsi che le ventole dello switch funzionino correttamente utilizzando il comando "storage switch show -cooling". 2) Assicurarsi che le FRU delle ventole siano inserite correttamente e funzionanti.
Switch di archiviazione MetroCluster non raggiungibile	CRITICO	Lo switch di archiviazione non è raggiungibile tramite la rete di gestione.	1) Assicurarsi che il LIF di gestione del nodo sia attivo utilizzando il comando "network interface show". 2) Assicurarsi che lo switch sia attivo utilizzando il comando "network ping". 3) Assicurarsi che lo switch sia raggiungibile tramite SNMP controllando le impostazioni SNMP dopo aver effettuato l'accesso allo switch.

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Alimentatori MetroCluster Switch guasti	CRITICO	Un alimentatore sullo switch di archiviazione non è operativo.	1) Verificare i dettagli dell'errore utilizzando il comando "storage switch show -error -switch-name <nome switch>". 2) Identificare l'alimentatore difettoso utilizzando il comando "storage switch show -power -switch -name <nome switch>". 3) Assicurarsi che l'alimentatore sia correttamente inserito nel telaio dello switch di archiviazione e sia completamente funzionante.
Sensori di temperatura dell'interruttore MetroCluster guasti	CRITICO	Il sensore sullo switch Fibre Channel è guasto.	1) Verificare lo stato operativo dei sensori di temperatura sullo switch di accumulo utilizzando il comando "storage switch show -cooling". 2) Verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.
Temperatura anomala dell'interruttore MetroCluster	CRITICO	Il sensore di temperatura sullo switch Fibre Channel ha segnalato una temperatura anomala.	1) Verificare lo stato operativo dei sensori di temperatura sullo switch di accumulo utilizzando il comando "storage switch show -cooling". 2) Verificare che l'interruttore funzioni alle condizioni di temperatura consigliate.
Heartbeat del processore di servizio perso	INFORMATIVO	Questo messaggio viene visualizzato quando ONTAP non riceve il segnale "heartbeat" previsto dal Service Processor (SP). Insieme a questo messaggio, verranno inviati i file di registro di SP per il debug. ONTAP reimposterà l' SP per tentare di ripristinare la comunicazione. Durante il riavvio, l' SP non sarà disponibile per un massimo di due minuti.	Contattare l'assistenza tecnica NetApp .

Nome del monitor	Gravità	Descrizione del monitor	Azione correttiva
Heartbeat del processore di servizio arrestato	AVVERTIMENTO	Questo messaggio viene visualizzato quando ONTAP non riceve più heartbeat dal Service Processor (SP). A seconda della progettazione hardware, il sistema potrebbe continuare a fornire dati oppure potrebbe decidere di spegnersi per evitare perdite di dati o danni all'hardware. Il sistema continua a fornire dati, ma poiché il SP potrebbe non funzionare, non è in grado di inviare notifiche di dispositivi inattivi, 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 "chiamata a casa") al supporto tecnico NetApp e alle destinazioni configurate. La corretta consegna di un messaggio AutoSupport migliora significativamente la determinazione e la risoluzione dei problemi.	Se il sistema si è spento, provare a eseguire un hard power cycle: estrarre il controller dallo chassis, spingerlo nuovamente dentro e accendere il sistema. Contattare l'assistenza tecnica NetApp se il problema persiste dopo il ciclo di accensione e spegnimento o per qualsiasi altra condizione che potrebbe richiedere attenzione.

Torna all'inizio

Ulteriori informazioni

- "Visualizzazione e chiusura degli avvisi"

Notifiche webhook

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 supportano tutti i webhook. Grazie al supporto di un canale webhook generico e personalizzabile, Data Infrastructure Insights può supportare molti di questi canali di distribuzione. Le

informazioni sui webhook sono disponibili sui siti web di queste applicazioni. Ad esempio, Slack fornisce"questa guida utile" .

È possibile creare più canali webhook, ognuno dei quali è destinato a uno scopo diverso: applicazioni separate, destinatari diversi, ecc.

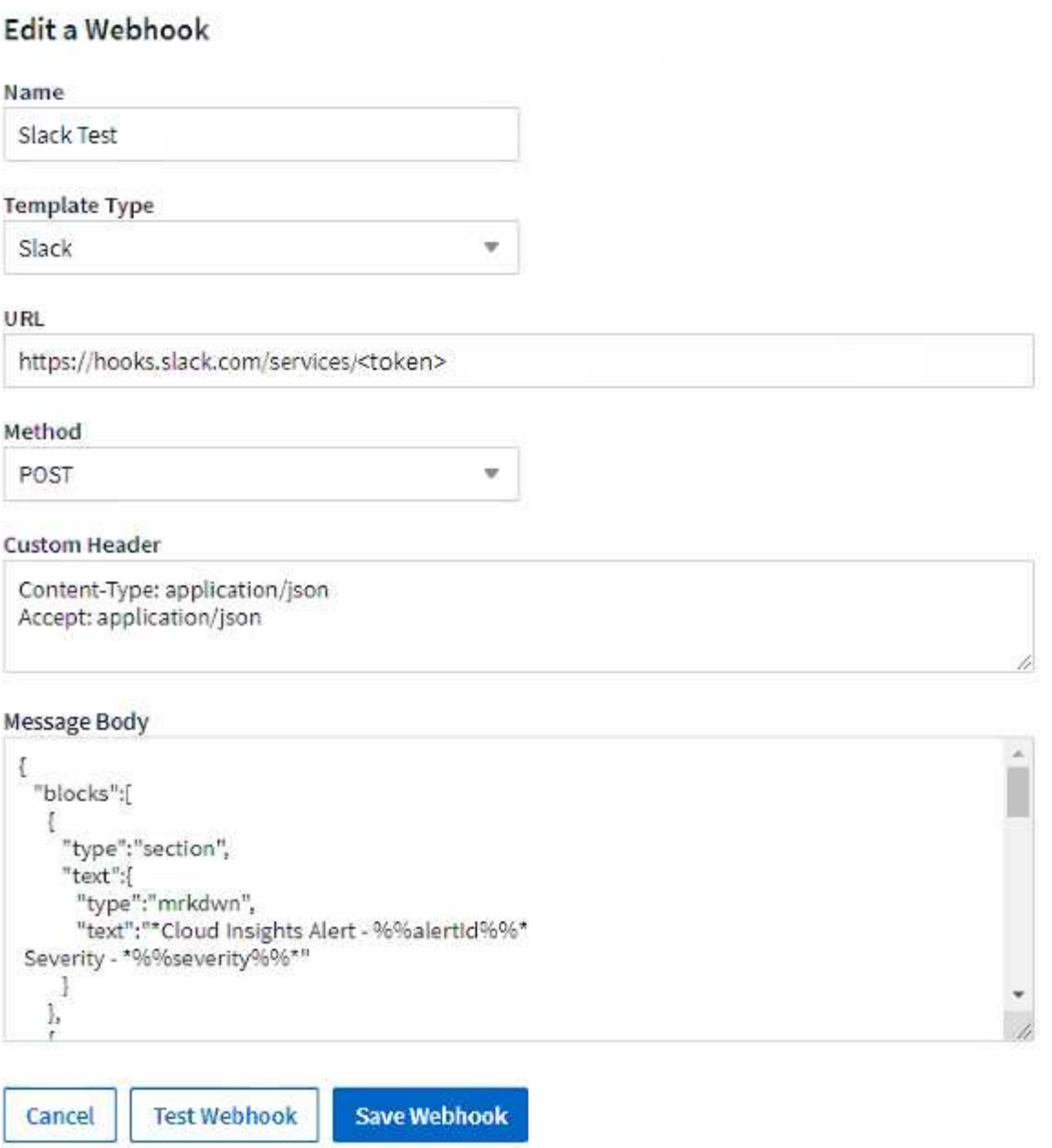
L'istanza del canale webhook è composta dai seguenti elementi:

Nome	Nome univoco
URL	URL di destinazione del webhook, incluso il prefisso *http://* o *https://* insieme ai parametri URL
Metodo	GET, POST - Il valore predefinito è POST
Intestazione personalizzata	Specifica qui eventuali righe di intestazione personalizzate
Corpo del messaggio	Inserisci qui il corpo del tuo messaggio
Parametri di avviso predefiniti	Elenca i parametri predefiniti per il webhook
Parametri e segreti personalizzati	I parametri personalizzati e i segreti consentono di aggiungere parametri univoci ed elementi sicuri come le password

Creazione di un webhook

Per creare un webhook Data Infrastructure Insights , vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**.

L'immagine seguente mostra un esempio di webhook configurato per Slack:



Inserisci le informazioni appropriate per ciascun campo e clicca su "Salva" al termine.

Puoi anche cliccare sul pulsante "Test Webhook" per testare la connessione. Si noti che in questo modo verrà inviato il "Corpo del messaggio" (senza sostituzioni) all'URL definito in base al metodo selezionato.

I webhook di Data Infrastructure Insights comprendono una serie di parametri predefiniti. Inoltre, puoi creare parametri o segreti 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: cosa sono e come si usano?

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.

È possibile aggiungere qualsiasi attributo dell'oggetto (ad esempio, il nome dell'archivio) come parametro a un webhook. Ad esempio, è possibile impostare parametri per il nome del volume e il nome dell'archiviazione in una descrizione webhook come: "Latenza elevata per volume: *%%relatedObject.volume.name%%*, Archiviazione: *%%relatedObject.storage.name%%*".

Si noti che in questa sezione le sostituzioni *non* vengono eseguite quando si fa 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

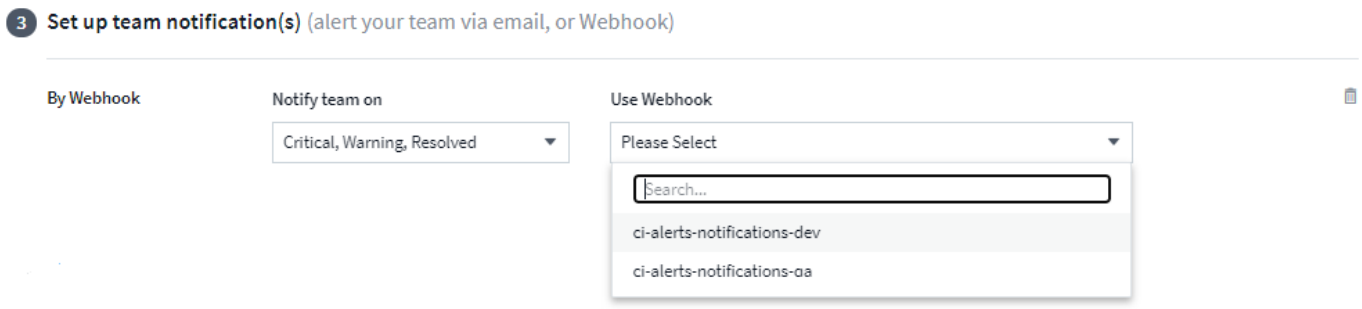
In questa sezione puoi aggiungere tutti i parametri personalizzati e/o segreti che desideri. Per motivi di sicurezza, se viene definito un segreto, solo il creatore del webhook può modificare questo canale webhook. Per gli altri è di sola lettura. È possibile utilizzare i segreti negli URL/intestazioni come *%%<secret_name>%%*.

Pagina elenco webhook

Nella pagina dell'elenco dei webhook vengono visualizzati i campi Nome, Creato da, Creato il, Stato, Sicuro e Ultimo segnalato.

Scelta della notifica webhook in un monitor

Per scegliere la notifica webhook in un"monitorare" , vai su **Avvisi > Gestisci monitor** e seleziona il monitor desiderato oppure aggiungine uno nuovo. Nella sezione *Imposta notifiche team*, seleziona *Webhook* come metodo di consegna. Selezionare i livelli di allerta (Critico, Avviso, Risolto), quindi scegliere il webhook desiderato.



Esempi di webhook:

Webhook per"Slack" Webhook per"PagerDuty" Webhook per"Squadre" Webhook per"Discordia"

Esempio di webhook per Discord

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Discord.

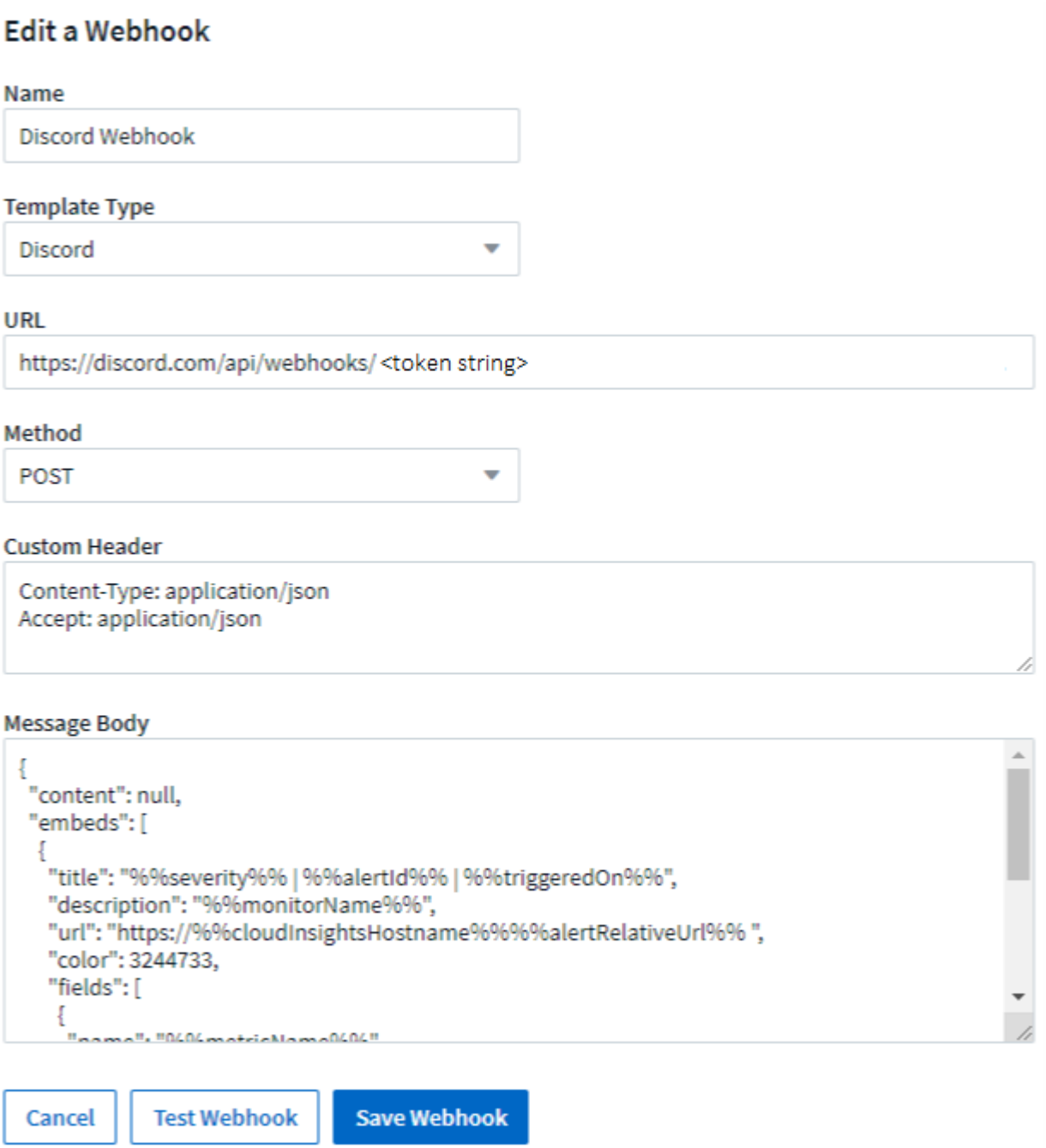
Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione Discord" per le informazioni più aggiornate.

Configurazione Discord:

- In Discord, seleziona il server, in Canali di testo, seleziona Modifica canale (icona a forma di ingranaggio)
- Seleziona **Integrazioni > Visualizza webhook** e fai clic su **Nuovo webhook**
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "Discord".
3. Nel menu a discesa *Tipo di modello*, seleziona **Discord**.
4. Incolla l'URL sopra nel campo *URL*.

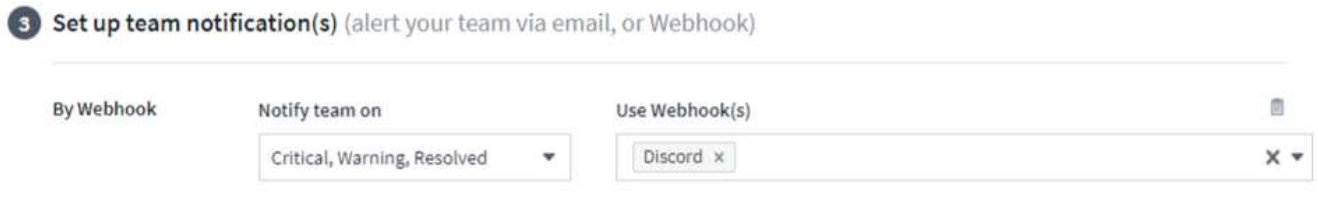


Per testare il webhook, sostituisci temporaneamente il valore URL nel corpo del messaggio con un URL valido (ad esempio *https://netapp.com*), quindi fai clic sul pulsante *Test Webhook*. Una volta completato il test, assicurati di reimpostare il corpo del messaggio.

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Seleziona il webhook "Discord" per gli eventi desiderati (Critico, Avviso, Risolto)



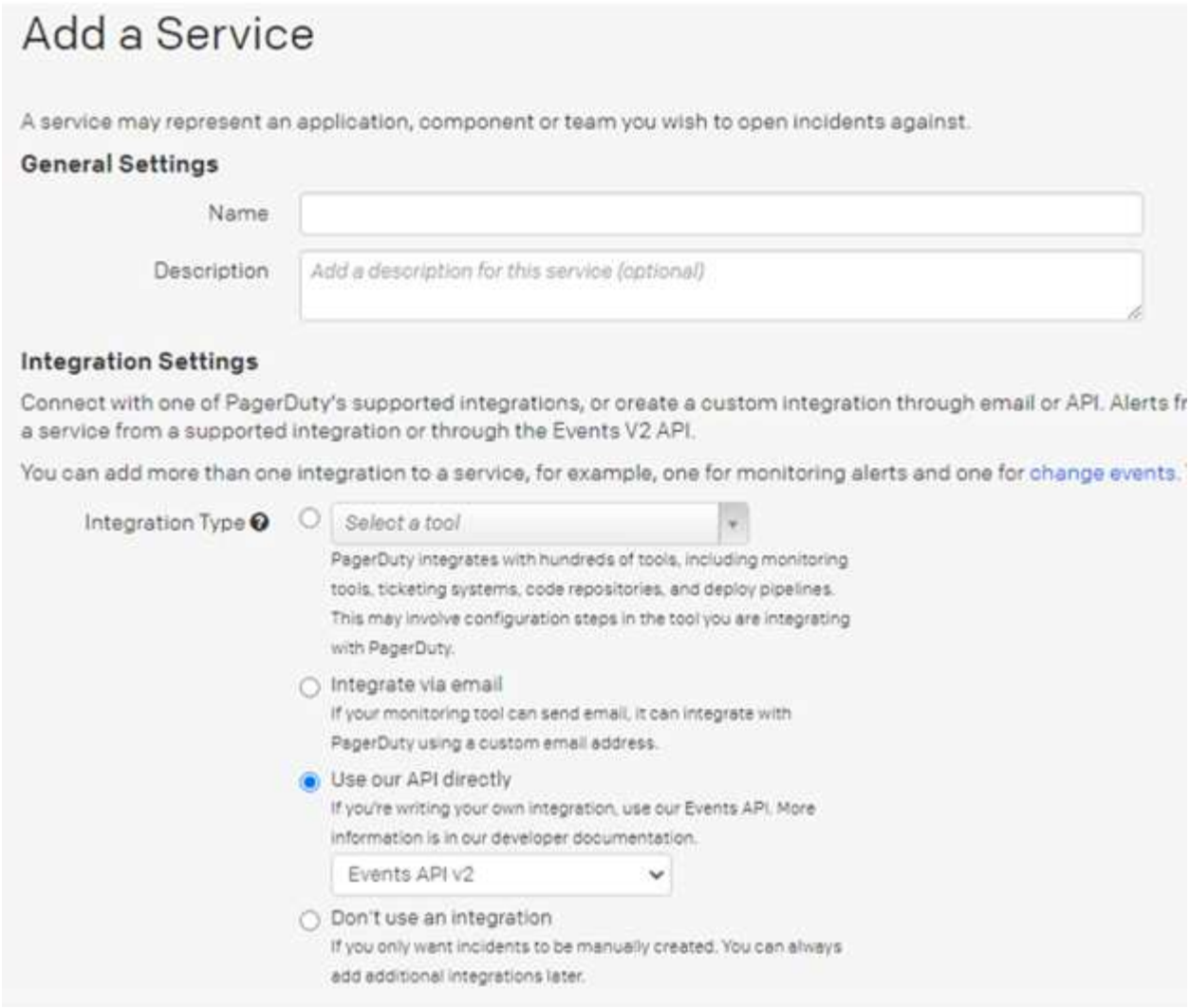
Esempio di webhook per PagerDuty

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per PagerDuty.

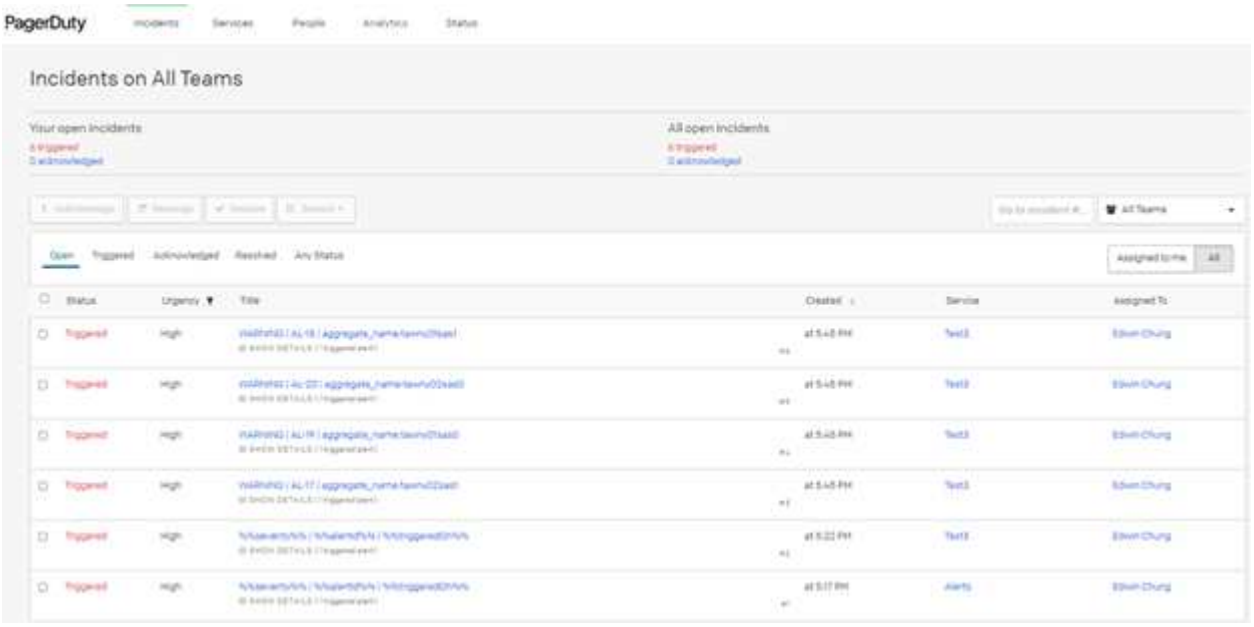
Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione PagerDuty" per le informazioni più aggiornate.

Configurazione PagerDuty:

1. In PagerDuty, vai su **Servizi > Directory dei servizi** e clicca sul pulsante **+Nuovo servizio**
2. Inserisci un *Nome* e seleziona *Usa direttamente la nostra API*. Fare clic su *Aggiungi servizio*.

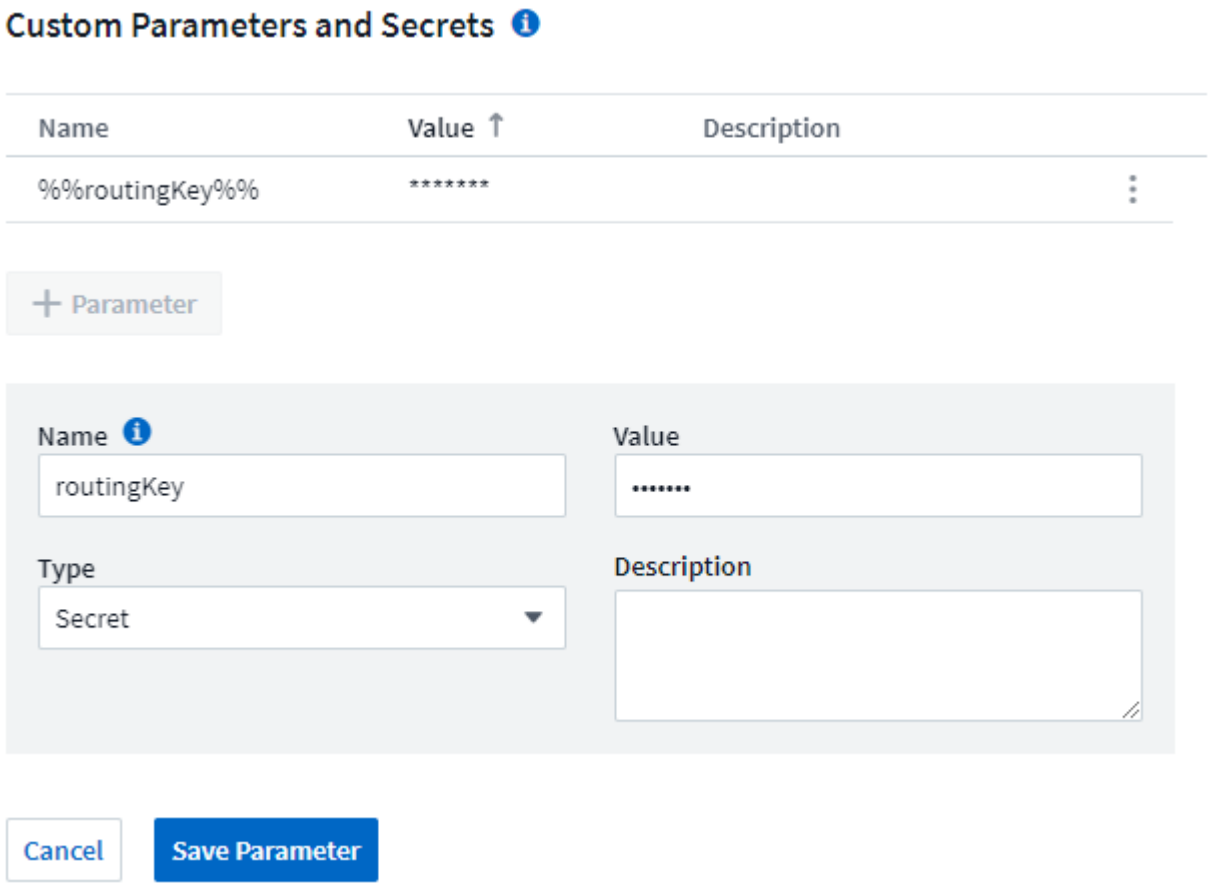


3. Fare clic sulla scheda *Integrazioni* per visualizzare la **Chiave di integrazione**. Questa chiave ti servirà quando creerai il webhook Data Infrastructure Insights riportato di seguito.
4. Vai a **Incidenti** o **Servizi** per visualizzare gli avvisi.



Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "PagerDuty Trigger". Utilizzerai questo webhook per eventi di livello critico e di avviso.
3. Nel menu a discesa *Tipo di modello*, seleziona **PagerDuty**.
4. Crea un parametro segreto personalizzato denominato *routingKey* e imposta il valore sul valore *Integration Key* di PagerDuty indicato sopra.



Ripetere questi passaggi per creare un webhook "PagerDuty Resolve" per gli eventi risolti.

Mappatura dei campi di PagerDuty per Data Infrastructure Insights

La tabella e l'immagine seguenti mostrano la mappatura dei campi tra PagerDuty e Data Infrastructure Insights:

PagerDuty	Data Infrastructure Insights
Tasto di avviso	ID avviso
Fonte	Attivato
Componente	Nome metrica
Gruppo	Tipo di oggetto

PagerDuty	Data Infrastructure Insights
Classe	Nome del monitor

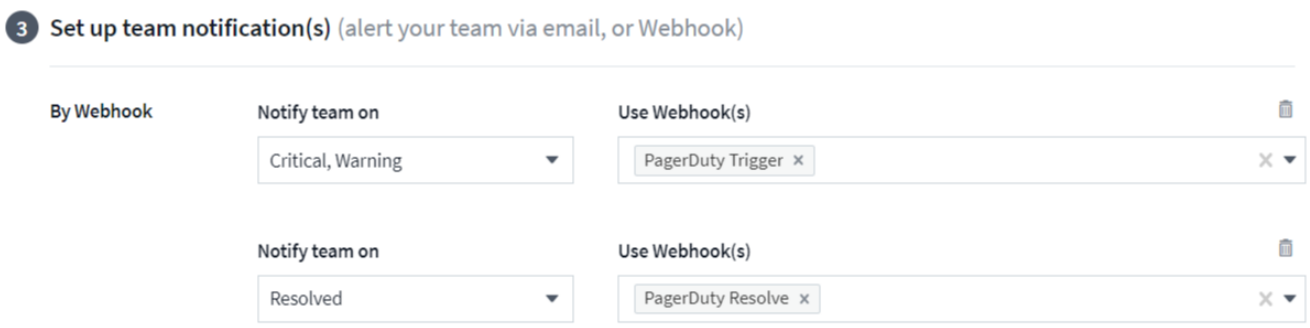
Message Body

```
{
 "dedup_key": "%%alertId%%",
 "event_action": "trigger",
 "links": [
  {
   "href": "https://%%cloudInsightsHostname%%%%alertRelativeUrl%%",
   "text": "'%%metricName%%' value of %%value%% (%%alertCondition%%) for
%%triggeredOn%%"
  }
 ],
 "payload": {
  "class": "%%monitorName%%",
  "component": "%%metricName%%",
  "group": "%%objectType%%",
  "severity": "critical",
  "source": "%%triggeredOn%%",
  "summary": "%%severity%% | %%alertId%% | %%triggeredOn%%"
 },
 "routing_key": "%%routingKey%%"
}
```

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Selezionare il webhook "PagerDuty Trigger" per gli eventi di livello critico e di avviso.
- Selezionare "PagerDuty Resolve" per gli eventi risolti.



Impostare notifiche separate per gli eventi trigger rispetto agli eventi risolti è una buona pratica, poiché PagerDuty gestisce gli eventi trigger in modo diverso rispetto agli eventi risolti.

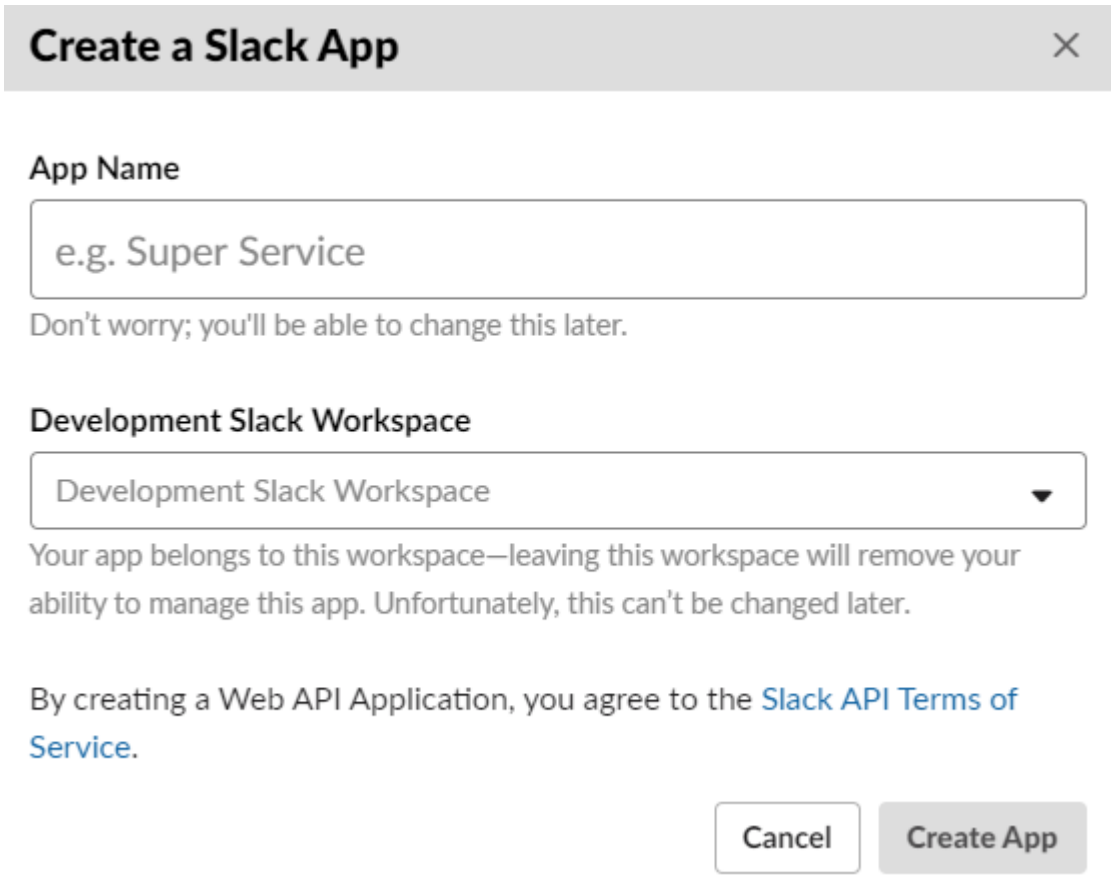
Esempio di webhook per Slack

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per impostare webhook per Slack.

Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione Slack" per le informazioni più aggiornate.

Esempio di Slack:

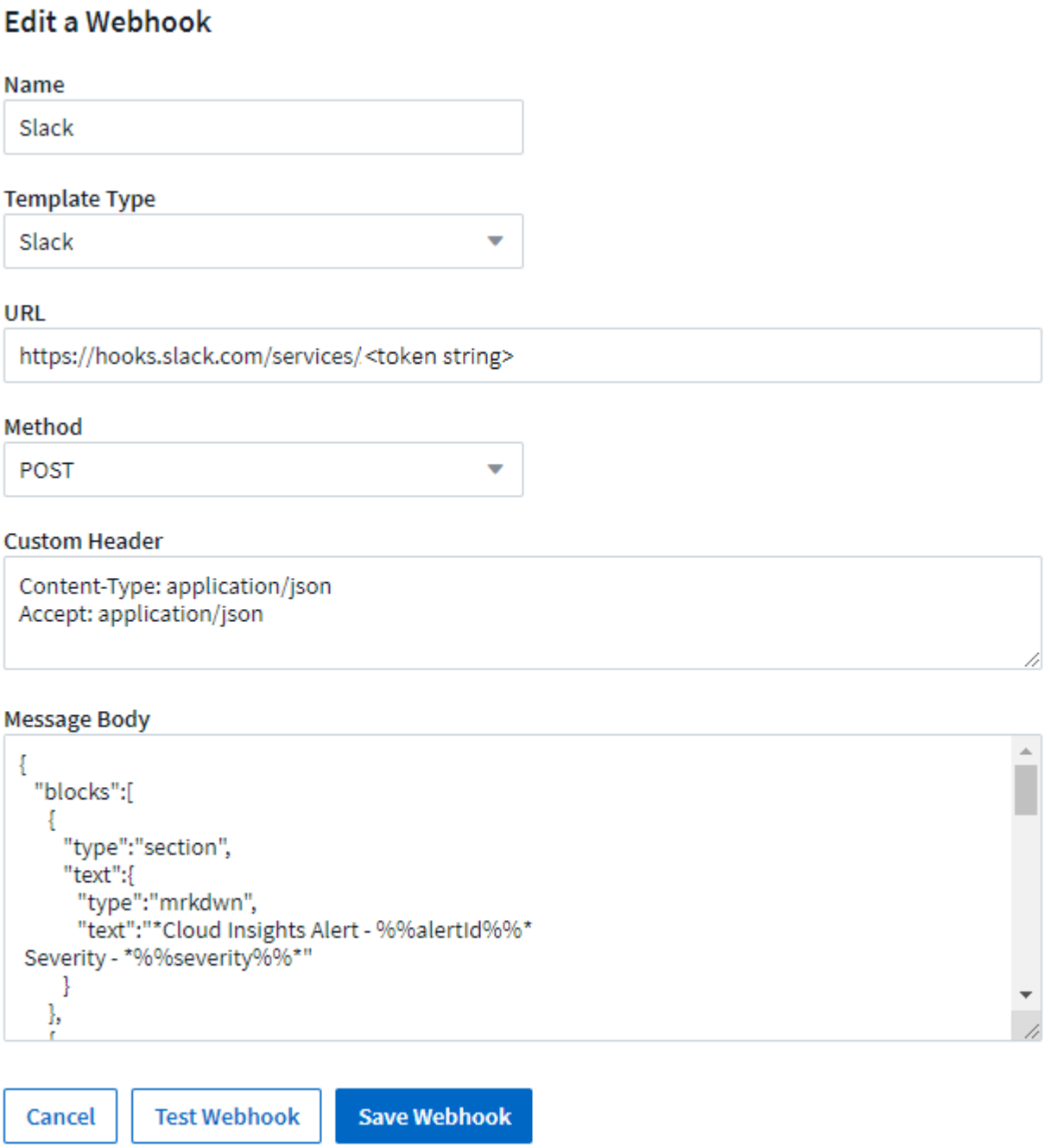
- Vai a https://api.slack.com/apps e crea una nuova app. Assegnagli un nome significativo e seleziona Slack Workspace.



- Vai a Webhook in arrivo, clicca su *Attiva webhook in arrivo*, Richiedi di *Aggiungere nuovo webhook* e seleziona il canale su cui pubblicare.
- Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

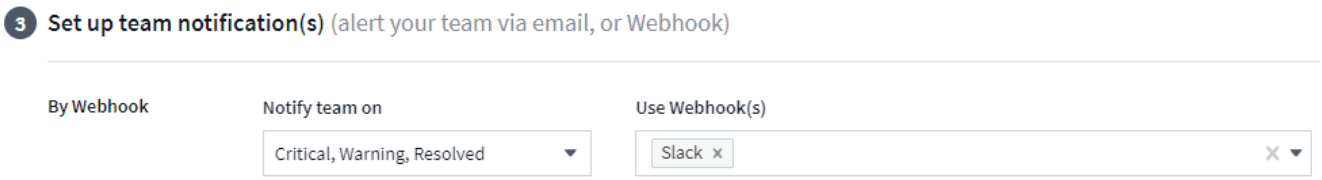
1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "Webhook Slack".
3. Nel menu a discesa *Tipo di modello*, seleziona **Slack**.
4. Incolla l'URL sopra nel campo *URL*.



Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Seleziona il webhook "Slack" per gli eventi desiderati (Critico, Avviso, Risolto)



Ulteriori informazioni:

- Per modificare il formato e il layout del messaggio, vedere https://api.slack.com/messaging/composing
- Gestione degli errori: https://api.slack.com/messaging/webhooks#handling_errors

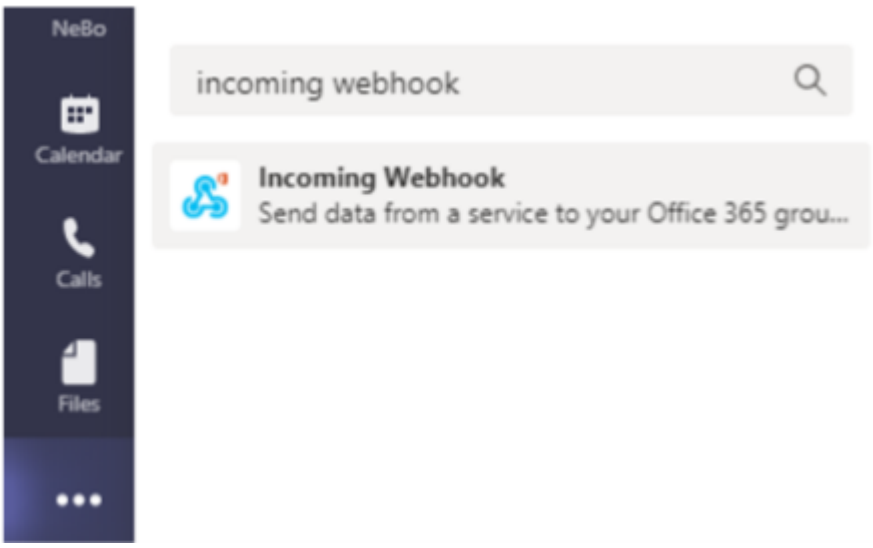
Esempio di webhook per Microsoft Teams

I webhook consentono agli utenti di inviare notifiche di avviso a varie applicazioni utilizzando un canale webhook personalizzato. Questa pagina fornisce un esempio per la configurazione di webhook per Teams.

Questa pagina fa riferimento a istruzioni di terze parti, che potrebbero essere soggette a modifiche. Fare riferimento al"Documentazione dei team" per le informazioni più aggiornate.

Configurazione delle squadre:

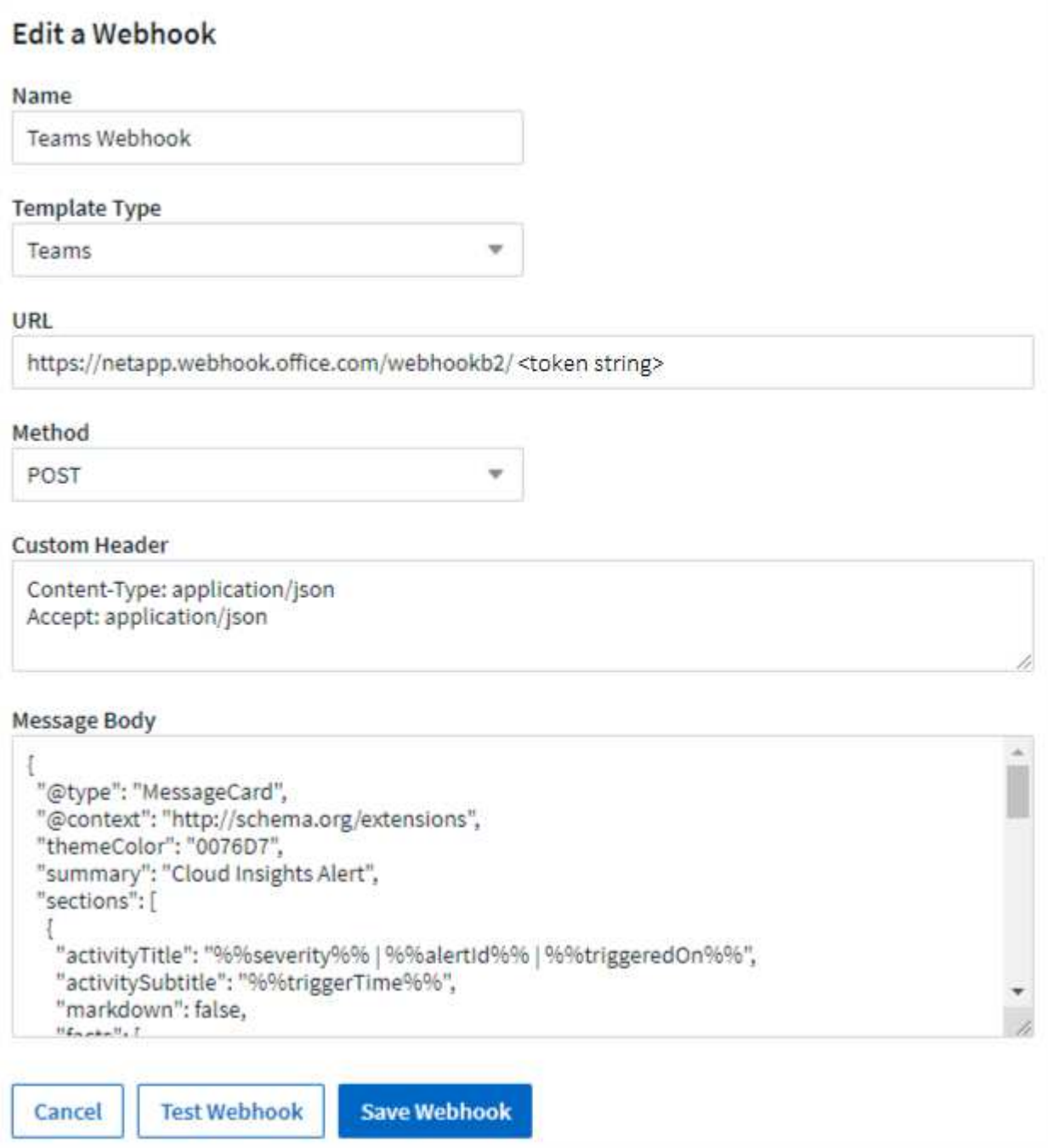
1. In Teams, seleziona il kebab e cerca Webhook in arrivo.



2. Seleziona **Aggiungi a un team > Seleziona un team > Imposta un connettore**.
3. Copia l'URL del webhook. Sarà necessario incollarlo nella configurazione del webhook di Data Infrastructure Insights .

Crea un webhook Data Infrastructure Insights :

1. In Data Infrastructure Insights, vai su **Amministrazione > Notifiche** e seleziona la scheda **Webhook**. Fare clic su **+Webhook** per creare un nuovo webhook.
2. Assegna al webhook un nome significativo, ad esempio "Teams Webhook".
3. Nel menu a discesa *Tipo di modello*, seleziona **Team**.



1. Incolla l'URL sopra nel campo *URL*.

Notifiche tramite Webhook

Per notificare gli eventi tramite webhook, in Data Infrastructure Insights vai su **Avvisi > Monitor** e fai clic su **+Monitor** per creare un nuovo"monitorare" .

- Selezionare una metrica e definire le condizioni del monitor.
- In _Imposta notifiche team, seleziona il metodo di recapito **Webhook**.
- Seleziona il webhook "Team" per gli eventi desiderati (Critico, Avviso, Risolto)