Monitoraggio di eventi, performance e stato

ONTAP 9

NetApp
April 16, 2024

Sommario

Monitoraggio di eventi, performance e stato

Monitorare le performance del cluster con System Manager

Monitorare le performance del cluster utilizzando System Manager

Gli argomenti di questa sezione mostrano come gestire lo stato e le performance del cluster con Gestione di sistema in ONTAP 9.7 e versioni successive.

È possibile monitorare le prestazioni del cluster visualizzando le informazioni relative al sistema nella dashboard di System Manager. La dashboard visualizza informazioni su avvisi e notifiche importanti, l'efficienza e la capacità dei livelli e dei volumi di storage, i nodi disponibili in un cluster, lo stato dei nodi in una coppia ha, le applicazioni e gli oggetti più attivi, e le metriche delle performance di un cluster o di un nodo.

La dashboard consente di determinare le seguenti informazioni:

- * Health*: Quanto è sano il cluster?
- **Capacità**: Quale capacità è disponibile sul cluster?
- **Performance**: Quali sono le performance del cluster, in base a latenza, IOPS e throughput?
- **Rete**: Come viene configurata la rete con host e oggetti storage, come porte, interfacce e macchine virtuali di storage?

Nelle panoramiche su salute e capacità, fare clic su → per visualizzare informazioni aggiuntive ed eseguire attività.

Nella panoramica delle performance, puoi visualizzare le metriche in base all'ora, al giorno, alla settimana, al mese o all'anno.

Nella panoramica della rete viene visualizzato il numero di ciascun oggetto della rete (ad esempio, "8 porte NVMe/FC"). È possibile fare clic sui numeri per visualizzare i dettagli relativi a ciascun oggetto di rete.

Visualizza le performance sulla dashboard del cluster

Utilizza la dashboard per prendere decisioni informate sui carichi di lavoro che potresti voler aggiungere o spostare. Puoi anche considerare i tempi di utilizzo più elevati per pianificare potenziali cambiamenti.

I valori delle performance si aggiornano ogni 3 secondi e il grafico delle performance si aggiorna ogni 15 secondi.

Fasi

1. Fare clic su **Dashboard**.
2. In **Performance**, selezionare l'intervallo.

Identificare gli hot volumi e altri oggetti

Accelera le performance del tuo cluster identificando i volumi con accesso frequente (hot volumi) e i dati (hot objects).

A partire da ONTAP 9.10.1, è possibile utilizzare la funzione monitoraggio attività di analisi del file system per monitorare gli oggetti hot in un volume.

Fasi

1. Fare clic su **Storage > Volumes** (Storage > volumi)
2. Filtrare le colonne IOPS, latenza e throughput per visualizzare i volumi e i dati utilizzati di frequente.

Modificare QoS

A partire da ONTAP 9,8, per il provisioning dello storage, Qualità del servizio (QoS) è attivato per impostazione predefinita. È possibile disattivare la QoS o scegliere una policy QoS personalizzata durante il processo di provisioning. È inoltre possibile modificare la QoS dopo il provisioning dello storage.

Fasi

1. In Gestione sistema, selezionare **archiviazione**, quindi **volumi**.
2. Accanto al volume per cui si desidera modificare la qualità del servizio, selezionare ⋮ Quindi **Modifica**.

Monitorare i rischi

A partire da ONTAP 9.10.0, è possibile utilizzare Gestione di sistema per monitorare i rischi segnalati da Consulente digitale Active IQ. A partire da ONTAP 9.10.1, è possibile utilizzare Gestione di sistema per riconoscere i rischi.

Il consulente digitale NetApp Active IQ segnala le opportunità per ridurre i rischi e migliorare le performance e l'efficienza del tuo ambiente di storage. Con System Manager, puoi conoscere i rischi segnalati da Active IQ e ricevere informazioni utili per amministrare lo storage e ottenere una maggiore disponibilità, una maggiore sicurezza e migliori performance dello storage.

Collegamento all'account Active IQ

Per ricevere informazioni sui rischi da Active IQ, devi prima collegarti al tuo account Active IQ da Gestione sistema.

Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **registrazione Active IQ**, fare clic su **Registra**.
3. Immettere le credenziali per Active IQ.
4. Una volta autenticate le credenziali, fare clic su **Confirm (Conferma) per collegare Active IQ a Gestore di sistema**.

Visualizza il numero di rischi

A partire da ONTAP 9.10.0, è possibile visualizzare dal dashboard di Gestione sistema il numero di rischi segnalati da Active IQ.

Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a. Collegamento all'account Active IQ.

Fasi

1. In System Manager, fare clic su **Dashboard**.
2. Nella sezione **Health**, visualizzare il numero di rischi segnalati.

> È possibile visualizzare informazioni più dettagliate su ciascun rischio facendo clic sul messaggio che indica il numero di rischi. Vedere Visualizza i dettagli dei rischi.

Visualizza i dettagli dei rischi

A partire da ONTAP 9.10.0, è possibile visualizzare da System Manager come i rischi segnalati da Active IQ sono classificati in base alle aree di impatto. È inoltre possibile visualizzare informazioni dettagliate su ciascun rischio segnalato, il suo potenziale impatto sul sistema e le azioni correttive che è possibile intraprendere.

Prima di iniziare

È necessario stabilire una connessione da Gestore di sistema all'account Active IQ. Fare riferimento a. Collegamento all'account Active IQ.

Fasi

1. Fare clic su **Eventi > tutti gli eventi**.
2. Nella sezione **Panoramica**, sotto **Active IQ Suggerimenti**, visualizzare il numero di rischi in ciascuna categoria di area di impatto. Le categorie di rischio includono:
   - Performance ed efficienza
   - Disponibilità e protezione
   - Capacità
   - Configurazione
   - Sicurezza
3. Fare clic sulla scheda **Active IQ Suggerimenti** per visualizzare informazioni su ciascun rischio, tra cui:
   - Livello di impatto sul sistema
   - Categoria del rischio
   - Nodi interessati
   - Tipo di mitigazione necessaria
   - Azioni correttive da intraprendere

Riconoscere i rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per riconoscere i rischi aperti.

Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in Visualizza i dettagli dei rischi.
2. Fare clic sul nome del rischio di un rischio aperto che si desidera riconoscere.
3. Inserire le informazioni nei seguenti campi:
   - Promemoria (data)
   - Giustificazione

- Commenti

4. Fare clic su **Conferma**.

> Dopo aver riconosciuto un rischio, sono necessari alcuni minuti per riflettere la modifica nell'elenco dei suggerimenti di Active IQ.

Annullare il riconoscimento dei rischi

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per annullare qualsiasi rischio precedentemente riconosciuto.

Fasi

1. In System Manager, visualizzare l'elenco dei rischi eseguendo la procedura descritta in Visualizza i dettagli dei rischi.
2. Fare clic sul nome del rischio riconosciuto che si desidera annullare.
3. Inserire le informazioni nei seguenti campi:
   - Giustificazione
   - Commenti
4. Fare clic su **Annulla riconoscimento**.

> Una volta che si annulla la conferma di un rischio, sono necessari alcuni minuti affinché la modifica venga riflessa nell'elenco dei suggerimenti di Active IQ.

Informazioni su System Manager

A partire da ONTAP 9.11.1, System Manager visualizza *informazioni* che consentono di ottimizzare le prestazioni e la sicurezza del sistema.

> Per visualizzare, personalizzare e rispondere alle informazioni, fare riferimento a. "Ottieni informazioni utili per ottimizzare il tuo sistema"

Informazioni sulla capacità

System Manager può visualizzare le seguenti informazioni in risposta alle condizioni di capacità del sistema:

Insight	Severità	Condizione	Correzioni

Gli strati locali sono privi di spazio	Rimediare ai rischi	Uno o più Tier locali sono pieni e in rapida crescita di oltre il 95%. È possibile che i carichi di lavoro esistenti non siano in grado di crescere o, in casi estremi, che i carichi di lavoro esistenti esauriscano lo spazio ed effettuino un errore.	**Correzione consigliata**: Eseguire una delle seguenti opzioni. • Cancellare la coda di ripristino del volume. • Consentire il thin provisioning sui volumi con thick provisioning per liberare lo storage intrappolato. • Sposta i volumi in un altro Tier locale. • Elimina le copie Snapshot non necessarie. • Eliminare le directory o i file non necessari nei volumi. • Consenti a Fabric Pool di eseguire il tiering dei dati nel cloud.
Le applicazioni mancano di spazio	Richiede attenzione	Uno o più volumi sono pieni più del 95%, ma non hanno la funzione di crescita automatica attivata.	**Consigliato**: Consente di attivare la crescita automatica fino al 150% della capacità di corrente. **Altre opzioni**: • Recupera spazio eliminando le copie Snapshot. • Ridimensionare i volumi. • Eliminare directory o file.
La capacità del volume FlexGroup non è bilanciata	Ottimizzazione dello storage	Le dimensioni dei volumi costituenti di uno o più volumi FlexGroup sono cresciute in modo non uniforme nel tempo, portando a uno squilibrio nell'utilizzo della capacità. Se i volumi costituenti diventano pieni, potrebbero verificarsi errori di scrittura.	**Consigliato**: Riequilibrare i volumi FlexGroup.

La capacità delle macchine virtuali storage sta per esaurirsi	Ottimizzazione dello storage	Una o più macchine virtuali storage hanno una capacità quasi massima vicina a quella massima. Non sarà quindi possibile eseguire il provisioning di ulteriore spazio per volumi nuovi o esistenti se le Storage VM raggiungono la capacità massima.	**Consigliato**: Se possibile, aumentare il limite massimo di capacità della VM di storage.

Informazioni sulla sicurezza

System Manager può visualizzare le seguenti informazioni in risposta a condizioni che potrebbero compromettere la sicurezza dei dati o del sistema.

Insight	Severità	Condizione	Correzioni
I volumi sono ancora in modalità di apprendimento anti-ransomware	Richiede attenzione	Uno o più volumi sono in modalità di apprendimento anti-ransomware da 90 giorni.	**Consigliato**: Abilitare la modalità anti-ransomware attiva per questi volumi.
L'eliminazione automatica delle copie Snapshot è abilitata sui volumi	Richiede attenzione	L'eliminazione automatica dello snapshot è abilitata su uno o più volumi.	**Consigliato**: Disattiva l'eliminazione automatica delle copie Snapshot. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.
I volumi non dispongono di policy Snapshot	Richiede attenzione	Uno o più volumi non dispongono di una policy Snapshot adeguata.	**Consigliato**: Allegare un criterio Snapshot ai volumi che non ne hanno uno. In caso contrario, in caso di attacco ransomware, il recovery di dati per questi volumi potrebbe non essere possibile.
FPolicy nativo non è configurato	Best practice	FPolicy nativo non è configurato su una o più macchine virtuali storage NAS.	**Consigliato**: **IMPORTANTE**: Il blocco delle estensioni potrebbe causare risultati imprevisti. A partire dal 9.11.1, puoi abilitare FPolicy nativa per le macchine virtuali storage, che blocca oltre 3000 estensioni dei file conosciute per essere utilizzate per gli attacchi ransomware. "Configurare FPolicy nativo" Nelle macchine virtuali storage NAS per controllare le estensioni dei file consentite o non consentite per la scrittura sui volumi nel tuo ambiente.

Telnet è attivato	Best practice	Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.	**Consigliato**: Disattivare Telnet e utilizzare SSH per un accesso remoto sicuro.
Sono stati configurati troppi server NTP	Best practice	Il numero di server configurati per NTP è inferiore a 3.	**Consigliato**: Associare al cluster almeno tre server NTP. In caso contrario, possono verificarsi problemi con la sincronizzazione dell'ora del cluster.
Remote Shell (RSH) è attivato	Best practice	Secure Shell (SSH) deve essere utilizzato per un accesso remoto sicuro.	**Consigliato**: Disabilitare RSH e utilizzare SSH per un accesso remoto sicuro.
Banner di accesso non configurato	Best practice	I messaggi di accesso non sono configurati né per il cluster, né per la VM di storage, né per entrambi.	**Consigliato**: Configurare i banner di accesso per il cluster e la VM di storage e abilitarne l'utilizzo.
AutoSupport sta utilizzando un protocollo non sicuro	Best practice	AutoSupport non è configurato per comunicare tramite HTTPS.	**Consigliato**: Si consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per inviare messaggi AutoSupport al supporto tecnico.
L'utente amministratore predefinito non è bloccato	Best practice	Nessuno ha effettuato l'accesso utilizzando un account amministrativo predefinito (admin o diag) e questi account non sono bloccati.	**Consigliato**: Blocca gli account amministrativi predefiniti quando non vengono utilizzati.
Secure Shell (SSH) sta utilizzando cifrari non sicuri	Best practice	La configurazione corrente utilizza cifrari CBC non protetti.	**Raccomandato**: Si dovrebbe consentire solo cifrari sicuri sul server web per proteggere la comunicazione sicura con i visitatori. Rimuovere i cifrari con nomi contenenti "cbc", ad esempio "ais128-cbc", "AES192-cbc", "AES256-cbc" e "3DES-cbc".
La compliance FIPS globale 140-2 è disattivata	Best practice	La compliance FIPS globale 140-2 è disabilitata nel cluster.	**Consigliato**: Per motivi di sicurezza, è necessario abilitare la crittografia globale conforme a FIPS 140-2 per garantire che ONTAP possa comunicare in modo sicuro con client o client server esterni.

I volumi non vengono monitorati alla ricerca di attacchi ransomware	Richiede attenzione	La funzionalità anti-ransomware è disabilitata su uno o più volumi.	**Consigliato**: Abilitare l'anti-ransomware sui volumi. In caso contrario, potresti non accorgerti quando i volumi sono minacciati o sotto attacco.
Le macchine virtuali storage non sono configurate per anti-ransomware	Best practice	Una o più macchine virtuali storage non sono configurate per la protezione anti-ransomware.	**Consigliato**: Abilitare l'anti-ransomware sulle macchine virtuali storage. Altrimenti, potresti non notare quando le macchine virtuali storage sono minacciate o sottoposte a attacchi.

Informazioni di configurazione

System Manager può visualizzare le seguenti informazioni in risposta ai problemi relativi alla configurazione del sistema.

Insight	Severità	Condizione	Correzioni
Il cluster non è configurato per le notifiche	Best practice	Email, webhook o traphost SNMP non sono configurati per consentirti di ricevere notifiche su problemi con il cluster.	**Consigliato**: Configurare le notifiche per il cluster.
Il cluster non è configurato per gli aggiornamenti automatici.	Best practice	Il cluster non è stato configurato in modo da ricevere aggiornamenti automatici per il pacchetto di qualifica del disco più recente, il firmware del disco, il firmware dello shelf e i file del firmware SP/BMC quando sono disponibili.	**Consigliato**: Attivare questa funzione.

Il firmware del cluster non è aggiornato	Best practice	Il sistema non dispone dell'ultimo aggiornamento del firmware che potrebbe avere miglioramenti, patch di sicurezza o nuove funzioni che consentono di proteggere il cluster per prestazioni migliori.	**Consigliato**: Aggiornare il firmware ONTAP.

Ottieni informazioni utili per ottimizzare il tuo sistema

System Manager consente di visualizzare informazioni utili per ottimizzare il sistema.

A proposito di questa attività

A partire da ONTAP 9.11.0, puoi visualizzare informazioni in System Manager che ti aiutano a ottimizzare la capacità e la conformità alla sicurezza del tuo sistema.

A partire da ONTAP 9.11.1, è possibile visualizzare informazioni aggiuntive che consentono di ottimizzare la capacità, la conformità alla sicurezza e la configurazione del sistema.

> **Il blocco delle estensioni può causare risultati imprevisti.** a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Potresti ricevere un messaggio di System Manager Insight che ti consiglia di farlo "Configurare FPolicy nativo" Per una macchina virtuale di storage.
>
> Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.
>
> Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. "Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio".
>
> Per ulteriori informazioni su FPolicy nativo, vedere "Tipi di configurazione FPolicy".

In base alle Best practice, queste informazioni vengono visualizzate su una pagina da cui è possibile avviare azioni immediate per ottimizzare il sistema. Per ulteriori informazioni su ciascuna analisi, vedere "Informazioni su System Manager".

Visualizza informazioni sull'ottimizzazione

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.

   La pagina **Insights** mostra gruppi di informazioni. Ciascun gruppo di informazioni potrebbe contenere uno o più elementi. Vengono visualizzati i seguenti gruppi:

- Ha bisogno della vostra attenzione
- Rimediare ai rischi
- Ottimizza il tuo storage

2. (Facoltativo) filtrare le informazioni visualizzate facendo clic sui seguenti pulsanti nell'angolo in alto a destra della pagina:
   -  Visualizza le informazioni relative alla sicurezza.
   -  Visualizza le informazioni relative alla capacità.
   -  Visualizza le informazioni relative alla configurazione.
   -  Visualizza tutte le informazioni.

Rispondi alle informazioni per ottimizzare il tuo sistema

In System Manager, puoi rispondere alle informazioni sperdendole, esplorando diversi modi per risolvere i problemi o avviando il processo per risolverli.

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Passare il mouse su una panoramica per visualizzare i pulsanti per eseguire le seguenti azioni:
   - **Chiudi**: Elimina le informazioni dalla vista. Per "undisperdere" le informazioni, fare riferimento a. [customize-settings-insights].
   - **Esplora**: Scopri i vari modi per risolvere il problema menzionato nelle informazioni. Questo pulsante viene visualizzato solo se è presente più di un metodo di correzione.
   - **Fix**: Avviare il processo di risoluzione del problema menzionato nelle informazioni. Verrà richiesto di confermare se si desidera intraprendere l'azione necessaria per applicare la correzione.

Alcune di queste azioni possono essere avviate da altre pagine in System Manager, ma la pagina **Insights** ti aiuta a ottimizzare le attività quotidiane, consentendoti di avviare questa azione da questa pagina.

Personalizzare le impostazioni per ottenere informazioni dettagliate

Puoi personalizzare le informazioni che ti verranno notificate in System Manager.

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su , Quindi selezionare **Impostazioni**.
3. Nella pagina **Impostazioni**, verificare che le caselle di controllo accanto alle informazioni di cui si desidera ricevere la notifica siano selezionate. Se in precedenza si è respinto un dato Insight, è possibile "undischissarlo" verificando che sia presente un segno di spunta nella relativa casella di controllo.
4. Fare clic su **Save** (Salva).

Esportare le informazioni come file PDF

Puoi esportare tutte le informazioni pertinenti come file PDF.

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. Nell'angolo superiore destro della pagina, fare clic su ⋮, Quindi selezionare **Esporta**.

Configurare FPolicy nativo

A partire da ONTAP 9.11.1, quando ricevi un System Manager Insight che suggerisce l'implementazione di FPolicy nativo, puoi configurarlo sui volumi e sulle macchine virtuali di storage.

Prima di iniziare

Quando si accede a informazioni su System Manager, in **Applica procedure consigliate**, potrebbe essere visualizzato un messaggio che indica che FPolicy nativo non è configurato.

Per ulteriori informazioni sui tipi di configurazione FPolicy, fare riferimento a. "Tipi di configurazione FPolicy".

Fasi

1. In System Manager, fare clic su **Insights** nella colonna di navigazione a sinistra.
2. In **Applica Best practice**, individuare **Native FPolicy non è configurato**.
3. Leggere il seguente messaggio prima di intraprendere un'azione:

> **Il blocco delle estensioni può causare risultati imprevisti.** a partire da ONTAP 9.11.1, è possibile abilitare FPolicy nativo per le VM di archiviazione utilizzando Gestione sistema. Con la modalità nativa di FPolicy, è possibile consentire o negare estensioni di file specifiche. System Manager consiglia oltre 3000 estensioni di file non consentite che sono state utilizzate in precedenti attacchi ransomware. Alcune di queste estensioni potrebbero essere utilizzate da file legittimi nell'ambiente in uso e il loro blocco potrebbe causare problemi imprevisti.
>
> Pertanto, si consiglia di modificare l'elenco delle estensioni per soddisfare le esigenze dell'ambiente. Fare riferimento a. "Come rimuovere un'estensione di file da una configurazione FPolicy nativa creata da System Manager utilizzando System Manager per ricreare il criterio".

4. Fare clic su **Correggi**.
5. Selezionare le macchine virtuali storage a cui si desidera applicare FPolicy native.
6. Per ogni VM di storage, seleziona i volumi che riceveranno FPolicy nativa.
7. Fare clic su **Configura**.

Monitorare e gestire le performance del cluster utilizzando la CLI

Panoramica sulla gestione e sul monitoraggio delle performance

È possibile impostare attività di gestione e monitoraggio delle performance di base e identificare e risolvere problemi comuni relativi alle performance.

È possibile utilizzare queste procedure per monitorare e gestire le prestazioni del cluster se si applicano le seguenti ipotesi:

- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Si desidera visualizzare lo stato del sistema e gli avvisi, monitorare le prestazioni del cluster ed eseguire l'analisi delle cause principali utilizzando Active IQ Unified Manager (precedentemente noto come gestore unificato di OnCommand), oltre all'interfaccia della riga di comando di ONTAP.
- Si sta utilizzando l'interfaccia della riga di comando di ONTAP per configurare la qualità del servizio (QoS) dello storage.

  QoS è disponibile anche in System Manager, NSLM, Wfa, VSC (VMware Plug-in) e API.
- Si desidera installare Unified Manager utilizzando un'appliance virtuale invece di un'installazione basata su Linux o Windows.
- Si desidera utilizzare una configurazione statica piuttosto che DHCP per installare il software.
- È possibile accedere ai comandi ONTAP al livello di privilegio avanzato.
- Sei un amministratore del cluster con il ruolo di "amministratore".

Informazioni correlate

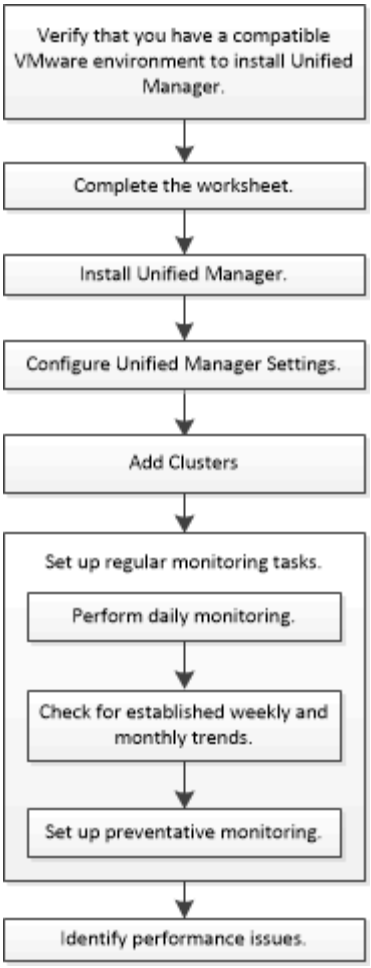
Se questi presupposti non sono corretti per la situazione, dovresti vedere le seguenti risorse:

- "Installazione di Active IQ Unified Manager 9.8"
- "Amministrazione del sistema"

Monitorare le performance

Panoramica del workflow di manutenzione e monitoraggio delle performance

Il monitoraggio e il mantenimento delle performance del cluster comportano l'installazione del software Active IQ Unified Manager, la configurazione di attività di monitoraggio di base, l'identificazione dei problemi di performance e la modifica secondo necessità.



Verificare che l'ambiente VMware sia supportato

Per installare correttamente Active IQ Unified Manager, è necessario verificare che l'ambiente VMware soddisfi i requisiti necessari.

Fasi

1. Verificare che l'infrastruttura VMware soddisfi i requisiti di dimensionamento per l'installazione di Unified Manager.
2. Accedere alla "Matrice di interoperabilità" per verificare di disporre di una combinazione supportata dei seguenti componenti:
   - Versione di ONTAP
   - Versione del sistema operativo ESXi
   - Versione di VMware vCenter Server
   - Versione di VMware Tools
   - Tipo e versione del browser

   Il "Matrice di interoperabilità" Elenca le configurazioni supportate per Unified Manager.
3. Fare clic sul nome della configurazione selezionata.

   I dettagli della configurazione vengono visualizzati nella finestra Dettagli configurazione.

4. Esaminare le informazioni nelle seguenti schede:
   - Note

     Elenca avvisi e informazioni importanti specifici della configurazione.

   - Policy e linee guida

     Fornisce linee guida generali per tutte le configurazioni.

Foglio di lavoro Active IQ Unified Manager

Prima di installare, configurare e connettere Active IQ Unified Manager, è necessario disporre di informazioni specifiche sull'ambiente in uso. È possibile registrare le informazioni nel foglio di lavoro.

Informazioni sull'installazione di Unified Manager

Macchina virtuale su cui viene implementato il software	Il tuo valore
Indirizzo IP del server ESXi	
Nome di dominio completo dell'host	
Host IP address (Indirizzo IP host)	
Maschera di rete	
Indirizzo IP del gateway	
Indirizzo DNS primario	
Indirizzo DNS secondario	
Cerca domini	
Nome utente manutenzione	
Password utente per la manutenzione	

Informazioni sulla configurazione di Unified Manager

Impostazione	Il tuo valore
Indirizzo e-mail utente manutenzione	
Server NTP	

Nome host o indirizzo IP del server SMTP	
Nome utente SMTP	
Password SMTP	
Porta predefinita SMTP	25 (valore predefinito)
E-mail da cui vengono inviate le notifiche di avviso	
Nome distinto bind LDAP	
Password bind LDAP	
Nome dell'amministratore di Active Directory	
Password di Active Directory	
Nome distinto della base del server di autenticazione	
Nome host o indirizzo IP del server di autenticazione	

Informazioni sul cluster

Acquisire le seguenti informazioni per ciascun cluster in Unified Manager.

Cluster 1 di N.	Il tuo valore
Nome host o indirizzo IP di gestione del cluster	
Nome utente amministratore di ONTAP All'amministratore deve essere stato assegnato il ruolo "admin".	
Password dell'amministratore di ONTAP	
Protocollo (HTTP o HTTPS)	

Informazioni correlate

"Autenticazione amministratore e RBAC"

Installare Active IQ Unified Manager

Scaricare e implementare Active IQ Unified Manager

Per installare il software, è necessario scaricare il file di installazione dell'appliance virtuale (VA) e utilizzare un client VMware vSphere per implementare il file su un server VMware ESXi. Il VA è disponibile in un file OVA.

Fasi

1. Accedere alla pagina **Download del software del sito di supporto NetApp** e individuare Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Selezionare **VMware vSphere** nel menu a discesa **Select Platform** e fare clic su **Go!**
3. Salvare il file "OVA" in una posizione locale o di rete accessibile al client VMware vSphere.
4. In VMware vSphere Client, fare clic su **file** > **Deploy OVF Template**.
5. Individuare il file "OVA" e utilizzare la procedura guidata per implementare l'appliance virtuale sul server ESXi.

   È possibile utilizzare la scheda **Proprietà** della procedura guidata per immettere le informazioni di configurazione statiche.

6. Accendere la macchina virtuale.
7. Fare clic sulla scheda **Console** per visualizzare il processo di avvio iniziale.
8. Seguire le istruzioni per installare VMware Tools sulla macchina virtuale.
9. Configurare il fuso orario.
10. Immettere un nome utente e una password per la manutenzione.
11. Accedere all'URL visualizzato dalla console della macchina virtuale.

Configurare le impostazioni Active IQ Unified Manager iniziali

La finestra di dialogo Configurazione iniziale di Active IQ Unified Manager viene visualizzata quando si accede per la prima volta all'interfaccia utente Web, che consente di configurare alcune impostazioni iniziali e aggiungere cluster.

Fasi

1. Accettare l'impostazione predefinita AutoSupport Enabled (attivato).
2. Immettere i dettagli del server NTP, l'indirizzo e-mail dell'utente di manutenzione, il nome host del server SMTP e le opzioni SMTP aggiuntive, quindi fare clic su **Salva**.

Al termine

Una volta completata la configurazione iniziale, viene visualizzata la pagina origini dati cluster, in cui è possibile aggiungere i dettagli del cluster.

Specificare i cluster da monitorare

È necessario aggiungere un cluster a un server Active IQ Unified Manager per monitorare il cluster, visualizzare lo stato di rilevamento del cluster e monitorarne le prestazioni.

Di cosa hai bisogno

- È necessario disporre delle seguenti informazioni:
  - Nome host o indirizzo IP di gestione del cluster

    Il nome host è il nome di dominio completo (FQDN, Fully Qualified Domain Name) o il nome breve utilizzato da Unified Manager per connettersi al cluster. Questo nome host deve essere risolto nell'indirizzo IP di gestione del cluster.

  L'indirizzo IP di gestione del cluster deve essere la LIF di gestione del cluster della SVM (Administrative Storage Virtual Machine). Se si utilizza una LIF di gestione dei nodi, l'operazione non riesce.

  - Nome utente e password dell'amministratore di ONTAP
  - Tipo di protocollo (HTTP o HTTPS) che è possibile configurare sul cluster e numero di porta del cluster
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- L'amministratore di ONTAP deve disporre dei ruoli di amministratore di ONTAPI e SSH.
- L'FQDN di Unified Manager deve essere in grado di eseguire il ping di ONTAP.

  Per verificarlo, utilizzare il comando ONTAP `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

A proposito di questa attività

Per una configurazione MetroCluster, è necessario aggiungere i cluster locali e remoti e i cluster devono essere configurati correttamente.

Fasi

1. Fare clic su **Configurazione** > **origini dati cluster**.
2. Dalla pagina Clusters, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi cluster**, specificare i valori richiesti, ad esempio il nome host o l'indirizzo IP (IPv4 o IPv6) del cluster, il nome utente, la password, il protocollo di comunicazione e il numero di porta.

   Per impostazione predefinita, il protocollo HTTPS è selezionato.

   È possibile modificare l'indirizzo IP di gestione del cluster da IPv6 a IPv4 o da IPv4 a IPv6. Il nuovo indirizzo IP viene visualizzato nella griglia del cluster e nella pagina di configurazione del cluster al termine del successivo ciclo di monitoraggio.

4. Fare clic su **Aggiungi**.
5. Se si seleziona HTTPS, attenersi alla seguente procedura:

   a. Nella finestra di dialogo **Authorize host** (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.

   b. Fare clic su **Sì**.

      Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente, ma non lo controlla per ogni chiamata API a ONTAP.

   Se il certificato è scaduto, non è possibile aggiungere il cluster. È necessario rinnovare il certificato SSL e aggiungere il cluster.

6. **Opzionale**: Visualizzazione dello stato di rilevamento del cluster:

   a. Esaminare lo stato di rilevamento del cluster dalla pagina **Cluster Setup**.

   Il cluster viene aggiunto al database di Unified Manager dopo l'intervallo di monitoraggio predefinito di circa 15 minuti.

Impostare attività di monitoraggio di base

Eseguire il monitoraggio giornaliero

È possibile eseguire il monitoraggio giornaliero per assicurarsi di non avere problemi immediati di performance che richiedono attenzione.

Fasi

1. Dall'interfaccia utente di Active IQ Unified Manager, accedere alla pagina **inventario eventi** per visualizzare tutti gli eventi correnti e obsoleti.
2. Dall'opzione **Visualizza**, selezionare `Active Performance Events` e determinare l'azione richiesta.

Utilizza le tendenze delle performance settimanali e mensili per identificare i problemi di performance

L'identificazione delle tendenze delle performance può aiutarti a identificare se il cluster viene utilizzato in eccesso o sottoutilizzato analizzando la latenza del volume. È possibile utilizzare procedure simili per identificare i colli di bottiglia della CPU, della rete o di altri sistemi.

Fasi

1. Individuare il volume che si sospetta sia sottoutilizzato o utilizzato in eccesso.
2. Nella scheda **Dettagli volume**, fare clic su **30 d** per visualizzare i dati storici.
3. Nel menu a discesa "Interrompi dati per", selezionare **latenza**, quindi fare clic su **Invia**.
4. Deselezionare **aggregate** nella tabella di confronto dei componenti del cluster, quindi confrontare la latenza del cluster con il grafico della latenza del volume.
5. Selezionare **aggregate** e deselezionare tutti gli altri componenti nel grafico di confronto dei componenti del cluster, quindi confrontare la latenza aggregata con il grafico di latenza del volume.
6. Confrontare il grafico della latenza di lettura/scrittura con il grafico della latenza del volume.
7. Determinare se i carichi delle applicazioni client hanno causato un conflitto di carichi di lavoro e ribilanciare i carichi di lavoro in base alle necessità.
8. Determinare se l'aggregato è utilizzato in eccesso e causa conflitti e ribilanciare i carichi di lavoro in base alle necessità.

Utilizza le soglie delle performance per generare notifiche di eventi

Gli eventi sono notifiche generate automaticamente da Active IQ Unified Manager quando si verifica una condizione predefinita o quando un valore del contatore delle prestazioni supera una soglia. Gli eventi consentono di identificare i problemi di performance nei cluster monitorati. È possibile configurare gli avvisi in modo che inviino automaticamente una notifica via email quando si verificano eventi di determinati tipi di gravità.

Impostare le soglie delle performance

È possibile impostare soglie di performance per monitorare i problemi critici di performance. Le soglie definite dall'utente attivano un avviso o una notifica di eventi critici quando il sistema si avvicina o supera la soglia definita.

Fasi

1. Creare le soglie degli eventi critici e di avviso:
   a. Selezionare **Configurazione** > **soglie delle prestazioni**.
   b. Fare clic su **Create** (Crea).
   c. Selezionare il tipo di oggetto e specificare un nome e una descrizione del criterio.
   d. Selezionare la condizione di contatore oggetti e specificare i valori limite che definiscono gli eventi di avviso e critici.
   e. Selezionare il periodo di tempo in cui i valori limite devono essere violati per l'invio di un evento, quindi fare clic su **Salva**.
2. Assegnare il criterio di soglia all'oggetto di storage.
   a. Accedere alla pagina Inventory (inventario) per lo stesso tipo di oggetto cluster selezionato in precedenza e scegliere **Performance** dall'opzione View (Visualizza).
   b. Selezionare l'oggetto a cui si desidera assegnare il criterio di soglia, quindi fare clic su **Assegna criterio di soglia**.
   c. Selezionare il criterio creato in precedenza, quindi fare clic su **Assegna policy**.

Esempio

È possibile impostare soglie definite dall'utente per ottenere informazioni sui problemi critici relativi alle performance. Ad esempio, se si dispone di un Microsoft Exchange Server e si sa che si blocca se la latenza del volume supera i 20 millisecondi, è possibile impostare una soglia di avviso a 12 millisecondi e una soglia critica a 15 millisecondi. Con questa impostazione di soglia, è possibile ricevere notifiche quando la latenza del volume supera il limite.

Aggiungere avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

Di cosa hai bisogno

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager

utilizzando la pagina script.

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

A proposito di questa attività

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.

   Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.

   Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

   È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

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

Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome avviso: HealthTest
- Risorse: Include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: Include tutti gli eventi sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

1. Fare clic su **Nome** e digitare `HealthTest` Nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Invio `abc` Nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
   c. Fare clic su **Escludi** e digitare `xyz` Nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.
4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare `sample@domain.com` Nel campo Alert these users (Avvisa questi utenti).
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.

7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test** script.
8. Fare clic su **Save** (Salva).

Configurare le impostazioni degli avvisi

È possibile specificare quali eventi di Active IQ Unified Manager attivano gli avvisi, i destinatari e-mail degli avvisi e la frequenza degli stessi.

Di cosa hai bisogno

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

È possibile configurare impostazioni di avviso univoche per i seguenti tipi di eventi relativi alle prestazioni:

- Eventi critici attivati da violazioni di soglie definite dall'utente
- Eventi di avviso attivati da violazioni di soglie definite dall'utente, soglie definite dal sistema o soglie dinamiche

Per impostazione predefinita, gli avvisi e-mail vengono inviati agli utenti amministratori di Unified Manager per tutti i nuovi eventi. È possibile inviare avvisi e-mail ad altri utenti aggiungendo gli indirizzi e-mail di tali utenti.

Per disattivare l'invio di avvisi per determinati tipi di eventi, è necessario deselezionare tutte le caselle di controllo di una categoria di eventi. Questa azione non interrompe la visualizzazione degli eventi nell'interfaccia utente.

Fasi

1. Nel riquadro di navigazione a sinistra, selezionare **Storage Management** > **Alert Setup**.

   Viene visualizzata la pagina Alert Setup.

2. Fare clic su **Add** (Aggiungi) e configurare le impostazioni appropriate per ciascun tipo di evento.

   Per inviare avvisi e-mail a più utenti, inserire una virgola tra ciascun indirizzo e-mail.

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

Identificare i problemi di performance in Active IQ Unified Manager

Se si verifica un evento di performance, è possibile individuare l'origine del problema in Active IQ Unified Manager e utilizzare altri strumenti per risolverlo. È possibile ricevere una notifica via email di un evento o notarlo durante il monitoraggio giornaliero.

Fasi

1. Fare clic sul collegamento nella notifica e-mail, che consente di accedere direttamente all'oggetto di storage che ha un evento di performance.

Se…	Quindi…
Ricevere una notifica via email di un evento	Fare clic sul collegamento per accedere direttamente alla pagina dei dettagli dell'evento.
Notare l'evento durante l'analisi della pagina inventario eventi	Selezionare l'evento per accedere direttamente alla pagina dei dettagli dell'evento.

2. Se l'evento ha superato una soglia definita dal sistema, seguire le azioni suggerite nell'interfaccia utente per risolvere il problema.
3. Se l'evento ha superato una soglia definita dall'utente, analizzarlo per determinare se è necessario intraprendere un'azione.
4. Se il problema persiste, verificare le seguenti impostazioni:
   - Impostazioni del protocollo sul sistema di storage
   - Impostazioni di rete su qualsiasi switch Ethernet o fabric
   - Impostazioni di rete sul sistema di storage
   - Layout dei dischi e metriche aggregate sul sistema storage
5. Se il problema persiste, contattare il supporto tecnico per assistenza.

Utilizza il consulente digitale Active IQ per visualizzare le prestazioni del sistema

Per qualsiasi sistema ONTAP che invia la telemetria AutoSupport a NetApp, è possibile visualizzare dati completi sulle performance e sulla capacità. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema.

È possibile visualizzare grafici relativi a utilizzo della CPU, latenza, IOPS, IOPS in base al protocollo e throughput di rete. È inoltre possibile scaricare questi dati in formato .csv per l'analisi in altri strumenti.

Oltre a questi dati sulle performance, Active IQ può mostrarti l'efficienza dello storage in base al carico di lavoro e confrontarla con l'efficienza prevista per quel tipo di carico di lavoro. È possibile visualizzare le tendenze della capacità e visualizzare una stima della quantità di storage aggiuntivo che potrebbe essere

necessaria per aggiungere in un determinato intervallo di tempo.

- L'efficienza dello storage è disponibile a livello di cliente, cluster e nodo sul lato sinistro del dashboard principale.
- Le performance sono disponibili a livello di cluster e nodo sul lato sinistro del dashboard principale.

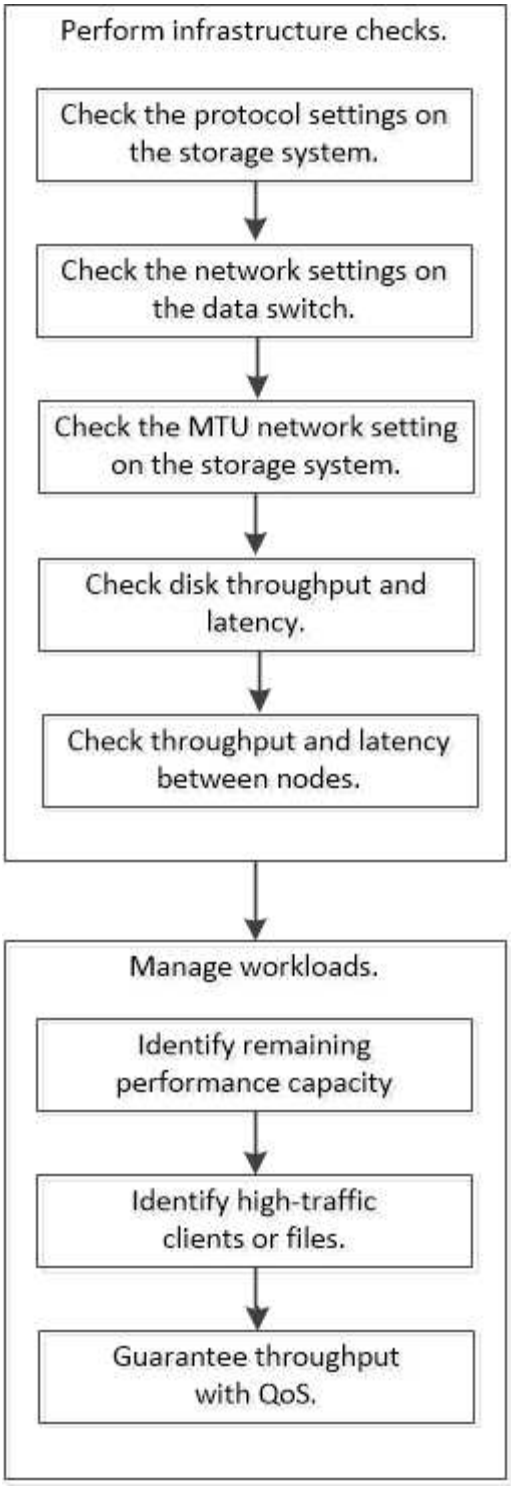
Informazioni correlate

- "Documentazione di Active IQ Digital Advisor"
- "Playlist video di Active IQ Digital Advisor"
- "Portale web Active IQ"

Gestire i problemi di performance

Workflow di gestione delle performance

Una volta identificato un problema di performance, è possibile eseguire alcuni controlli diagnostici di base dell'infrastruttura per escludere errori di configurazione evidenti. Se questi non individuano il problema, è possibile iniziare a esaminare i problemi di gestione del carico di lavoro.



Eseguire controlli di base dell'infrastruttura

Verificare le impostazioni del protocollo sul sistema di storage

Controllare le dimensioni massime di trasferimento TCP NFS

Per NFS, è possibile verificare se le dimensioni massime di trasferimento TCP per le operazioni di lettura e scrittura potrebbero causare problemi di performance. Se pensi che le dimensioni rallentino le performance, puoi aumentarle.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario disporre dei privilegi di amministratore del cluster.
- Per questa attività, è necessario utilizzare i comandi avanzati del livello di privilegio.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Verificare le dimensioni massime di trasferimento TCP:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

3. Se la dimensione massima di trasferimento TCP è troppo piccola, aumentarne la dimensione:

   ```
   vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer
   ```

4. Tornare al livello di privilegi amministrativi:

   ```
   set -privilege admin
   ```

Esempio

Nell'esempio seguente viene modificata la dimensione massima di trasferimento TCP di `SVM1` a 1048576:

```
cluster1::*> vserver nfs modify -vserver SVM1 -tcp-max-xfer-size 1048576
```

Controllare le dimensioni di lettura/scrittura TCP iSCSI

Per iSCSI, è possibile controllare le dimensioni di lettura/scrittura TCP per determinare se l'impostazione delle dimensioni sta creando un problema di prestazioni. Se le dimensioni sono la causa di un problema, è possibile correggerlo.

Di cosa hai bisogno

Per questa attività sono necessari comandi avanzati del livello di privilegio.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Verificare l'impostazione delle dimensioni della finestra TCP:

   ```
   vserver iscsi show -vserv,er vserver_name -instance
   ```

3. Modificare l'impostazione delle dimensioni della finestra TCP:

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

4. Tornare al privilegio amministrativo:

```
set -privilege admin
```

Esempio

Nell'esempio seguente viene modificata la dimensione della finestra TCP di `SVM1` fino a 131,400 byte:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size 131400
```

Controllare le impostazioni del multiplex CIFS

Se le prestazioni della rete CIFS lente causano un problema di performance, è possibile modificare le impostazioni multiplex per migliorarle e correggerle.

Fasi

1. Controllare l'impostazione del multiplex CIFS:

   ```
   vserver cifs options show -vserver –vserver_name -instance
   ```

2. Modificare l'impostazione del multiplex CIFS:

   ```
   vserver cifs options modify –vserver –vserver_name –max-mpx integer
   ```

Esempio

Nell'esempio seguente viene modificato il numero massimo di multiplex `SVM1` a 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Controllare la velocità della porta dell'adattatore FC

La velocità della porta di destinazione dell'adattatore deve corrispondere alla velocità del dispositivo a cui si connette, per ottimizzare le prestazioni. Se la porta è impostata sulla negoziazione automatica, la riconnessione potrebbe richiedere più tempo dopo un takeover e un giveback o un'altra interruzione.

Di cosa hai bisogno

Tutte le LIF che utilizzano questo adattatore come porta home devono essere offline.

Fasi

1. Portare l'adattatore offline:

   ```
   network fcp adapter modify -node nodename -adapter adapter -state down
   ```

2. Verificare la velocità massima dell'adattatore porta:

   ```
   fcp adapter show -instance
   ```

3. Modificare la velocità della porta, se necessario:

```
network fcp adapter modify -node nodename -adapter adapter -speed
{1|2|4|8|10|16|auto}
```

4. Portare l'adattatore online:

```
network fcp adapter modify -node nodename -adapter adapter -state up
```

5. Porta online tutti i LIF dell'adattatore:

```
network interface modify -vserver * -lif * { -home-node node1 -home-port e0c }
-status-admin up
```

Esempio

Nell'esempio seguente viene modificata la velocità della porta dell'adattatore `0d` acceso `node1` A 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -speed 2
```

Controllare le impostazioni di rete sugli switch dati

Sebbene sia necessario mantenere le stesse impostazioni MTU su client, server e sistemi di storage (ovvero endpoint di rete), i dispositivi di rete intermedi come NIC e switch devono essere impostati sui valori MTU massimi per garantire che le performance non vengano compromesse.

Per ottenere prestazioni ottimali, tutti i componenti della rete devono essere in grado di inoltrare frame jumbo (9000 byte IP, 9022 byte Ethernet inclusa). Gli switch dati devono essere impostati su almeno 9022 byte, ma con la maggior parte degli switch è possibile impostare un valore tipico di 9216.

Procedura

Per i commutatori di dati, verificare che la dimensione MTU sia impostata su 9022 o superiore.

Per ulteriori informazioni, consultare la documentazione del fornitore dello switch.

Controllare le impostazioni di rete MTU sul sistema di storage

È possibile modificare le impostazioni di rete sul sistema di storage se non corrispondono a quelle del client o di altri endpoint di rete. Mentre l'impostazione MTU della rete di gestione è impostata su 1500, la dimensione MTU della rete dati deve essere 9000.

A proposito di questa attività

Tutte le porte all'interno di un dominio di broadcast hanno le stesse dimensioni MTU, ad eccezione del traffico di gestione della porta e0M. Se la porta fa parte di un dominio di broadcast, utilizzare `broadcast-domain modify` Per modificare la MTU per tutte le porte all'interno del dominio di trasmissione modificato.

Si noti che i dispositivi di rete intermedi, come NIC e switch dati, possono essere impostati su dimensioni MTU più elevate rispetto agli endpoint di rete. Per ulteriori informazioni, vedere "Controllare le impostazioni di rete sugli switch dati".

Fasi

1. Verificare l'impostazione della porta MTU sul sistema di storage:

   ```
   network port show -instance
   ```

2. Modificare l'MTU sul dominio di trasmissione utilizzato dalle porte:

   ```
   network port broadcast-domain modify -ipspace ipspace -broadcast-domain
   broadcast_domain -mtu new _mtu
   ```

Esempio

Nell'esempio seguente viene modificata l'impostazione della porta MTU su 9000:

```
network port broadcast-domain modify -ipspace Cluster -broadcast-domain
Cluster -mtu 9000
```

Controllare il throughput e la latenza dei dischi

È possibile controllare il throughput dei dischi e le metriche di latenza per i nodi del cluster per agevolare la risoluzione dei problemi.

A proposito di questa attività

Per questa attività sono necessari comandi avanzati del livello di privilegio.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Controllare il throughput dei dischi e le metriche di latenza:

   ```
   statistics disk show -sort-key latency
   ```

Esempio

Nell'esempio seguente vengono visualizzati i totali di ciascuna operazione di lettura o scrittura dell'utente per `node2` acceso `cluster1`:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write   *Latency
  Disk       Node   (%)   Ops   Ops   Ops   (Bps)    (Bps)       (us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Controllare il throughput e la latenza tra i nodi

È possibile utilizzare `network test-path` comando per identificare i colli di bottiglia della rete o per prequalificare i percorsi di rete tra i nodi. È possibile eseguire il comando tra nodi di intercluster o nodi intracluster.

Di cosa hai bisogno

- Per eseguire questa attività, è necessario essere un amministratore del cluster.
- Per questa attività sono necessari comandi avanzati del livello di privilegio.
- Per un percorso intercluster, è necessario eseguire il peering dei cluster di origine e di destinazione.

A proposito di questa attività

Occasionalmente, le performance di rete tra i nodi potrebbero non soddisfare le aspettative per la configurazione del percorso. Una velocità di trasmissione di 1 Gbps per il tipo di trasferimenti di dati di grandi dimensioni, come ad esempio le operazioni di replica di SnapMirror, non sarebbe coerente con un collegamento a 10 GbE tra i cluster di origine e di destinazione.

È possibile utilizzare `network test-path` comando per misurare il throughput e la latenza tra i nodi. È possibile eseguire il comando tra nodi di intercluster o nodi intracluster.

Il test satura il percorso di rete con i dati, quindi è necessario eseguire il comando quando il sistema non è occupato e quando il traffico di rete tra i nodi non è eccessivo. Il test si esaurisce dopo dieci secondi. Il comando può essere eseguito solo tra i nodi ONTAP 9.

Il `session-type` L'opzione identifica il tipo di operazione in esecuzione sul percorso di rete, ad esempio "AsyncMirrorRemote" per la replica di SnapMirror su una destinazione remota. Il tipo determina la quantità di dati utilizzati nel test. La seguente tabella definisce i tipi di sessione:

Tipo di sessione	Descrizione
AsyncMirrorLocal	Impostazioni utilizzate da SnapMirror tra nodi nello stesso cluster

AsyncMirrorRemote	Impostazioni utilizzate da SnapMirror tra nodi in cluster diversi (tipo predefinito)
RemoteDataTransfer	Impostazioni utilizzate da ONTAP per l'accesso remoto ai dati tra nodi nello stesso cluster (ad esempio, una richiesta NFS a un nodo per un file memorizzato in un volume su un nodo diverso)

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Misurare il throughput e la latenza tra i nodi:

   ```
   network test-path -source-node source_nodename |local -destination-cluster
   destination_clustername -destination-node destination_nodename -session-type
   Default|AsyncMirrorLocal|AsyncMirrorRemote|SyncMirrorRemote|RemoteDataTransfer
   ```

   Il nodo di origine deve trovarsi nel cluster locale. Il nodo di destinazione può trovarsi nel cluster locale o in un cluster peered. Un valore "locale" per `-source-node` specifica il nodo su cui si esegue il comando.

   Il seguente comando misura il throughput e la latenza per le operazioni di replica di tipo SnapMirror tra `node1` sul cluster locale e. `node3` acceso `cluster2`:

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   Min latency in ms:  61.14
   Max latency in ms:  3056.86
   ```

3. Tornare al privilegio amministrativo:

   ```
   set -privilege admin
   ```

Al termine

Se le performance non soddisfano le aspettative per la configurazione del percorso, è necessario controllare le statistiche delle performance del nodo, utilizzare gli strumenti disponibili per isolare il problema nella rete, controllare le impostazioni dello switch e così via.

Gestire i carichi di lavoro

Identificare la capacità di performance rimanente

La capacità delle performance, o *headroom*, misura la quantità di lavoro che è possibile posizionare su un nodo o su un aggregato prima che le performance dei carichi di lavoro sulla risorsa comincino ad essere influenzate dalla latenza. La conoscenza della capacità di performance disponibile nel cluster consente di eseguire il provisioning e bilanciare i carichi di lavoro.

Di cosa hai bisogno

Per questa attività sono necessari comandi avanzati del livello di privilegio.

A proposito di questa attività

È possibile utilizzare i seguenti valori per `-object` opzione per raccogliere e visualizzare le statistiche di headroom:

- Per CPU, `resource_headroom_cpu`.
- Per gli aggregati, `resource_headroom_aggr`.

È inoltre possibile completare questa attività utilizzando Gestione di sistema e Active IQ Unified Manager.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Avvia la raccolta di statistiche in tempo reale:

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

3. Visualizzare in tempo reale le informazioni statistiche di headroom:

   ```
   statistics show -object resource_headroom_cpu|aggr
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

4. Tornare al privilegio amministrativo:

   ```
   set -privilege admin
   ```

Esempio

Nell'esempio seguente vengono visualizzate le statistiche medie orarie del headroom per i nodi del cluster.

È possibile calcolare la capacità di performance disponibile per un nodo sottraendo `current_utilization` contatore da `optimal_point_utilization` contatore. In questo esempio, la capacità di utilizzo per `CPU_sti2520-213` È -14% (72%-86%), il che suggerisce che la CPU è stata in media utilizzata in eccesso nell'ultima ora.

Potrebbe essere stato specificato `ewma_daily`, `ewma_weekly`, o. `ewma_monthly` ottenere le stesse informazioni in media per periodi di tempo più lunghi.

```
sti2520-2131454963690::*> statistics show -object resource_headroom_cpu
-raw -counter ewma_hourly
  (statistics show)

Object: resource_headroom_cpu
Instance: CPU_sti2520-213
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-213

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                             4376
                     current_latency                            37719
                 current_utilization                               86
                   optimal_point_ops                             2573
               optimal_point_latency                             3589
           optimal_point_utilization                               72
     optimal_point_confidence_factor                                1

Object: resource_headroom_cpu
Instance: CPU_sti2520-214
Start-time: 2/9/2016 16:06:27
End-time: 2/9/2016 16:06:27
Scope: sti2520-214

    Counter                                                     Value
    -------------------------------- --------------------------------
    ewma_hourly                                                     -
                         current_ops                                0
                     current_latency                                0
                 current_utilization                                0
                   optimal_point_ops                                0
               optimal_point_latency                                0
           optimal_point_utilization                               71
     optimal_point_confidence_factor                                1
2 entries were displayed.
```

Identificare i client o i file ad alto traffico

È possibile utilizzare la tecnologia ONTAP Active Objects per identificare client o file responsabili di una quantità sproporzionata di traffico cluster. Una volta identificati questi file o client "top", è possibile ribilanciare i carichi di lavoro del cluster o intraprendere altre azioni per risolvere il problema.

Di cosa hai bisogno

Per eseguire questa attività, è necessario essere un amministratore del cluster.

Fasi

1. Visualizzare i principali client che accedono al cluster:

   `statistics top client show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Il seguente comando visualizza i principali client che accedono `cluster1`:

```
cluster1::> statistics top client show

cluster1 : 3/23/2016 17:59:10


                                          *Total
        Client Vserver           Node Protocol    Ops
-------------- ------- -------------- -------- ------
172.17.180.170     vs4 siderop1-vsim4      nfs    668
172.17.180.169     vs3 siderop1-vsim3      nfs    337
172.17.180.171     vs3 siderop1-vsim3      nfs    142
172.17.180.170     vs3 siderop1-vsim3      nfs    137
172.17.180.123     vs3 siderop1-vsim3      nfs    137
172.17.180.171     vs4 siderop1-vsim4      nfs     95
172.17.180.169     vs4 siderop1-vsim4      nfs     92
172.17.180.123     vs4 siderop1-vsim4      nfs     92
172.17.180.153     vs3 siderop1-vsim3      nfs      0
```

2. Visualizzare i file principali a cui si accede dal cluster:

   `statistics top file show -node` *`node_name`* `-sort-key` *`sort_column`* `-interval` *`seconds_between_updates`* `-iterations` *`iterations`* `-max` *`number_of_instances`*

   Per la sintassi completa dei comandi, vedere la pagina man.

   Il seguente comando visualizza i file principali a cui si accede `cluster1`:

```
cluster1::> statistics top file show

cluster1 : 3/23/2016 17:59:10

                                    *Total
                     File Volume Vserver          Node    Ops
------------------------ ------ ------- -------------- ------
/vol/vol1/vm170-read.dat   vol1     vs4 siderop1-vsim4     22
/vol/vol1/vm69-write.dat   vol1     vs3 siderop1-vsim3      6
     /vol/vol2/vm171.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol2/vm169.dat   vol2     vs3 siderop1-vsim3      2
      /vol/vol2/p123.dat   vol2     vs4 siderop1-vsim4      2
      /vol/vol2/p123.dat   vol2     vs3 siderop1-vsim3      2
     /vol/vol1/vm171.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim4      2
     /vol/vol1/vm169.dat   vol1     vs4 siderop1-vsim3      2
      /vol/vol1/p123.dat   vol1     vs4 siderop1-vsim4      2
```

Throughput garantito con QoS

Garantire il throughput con la panoramica QoS

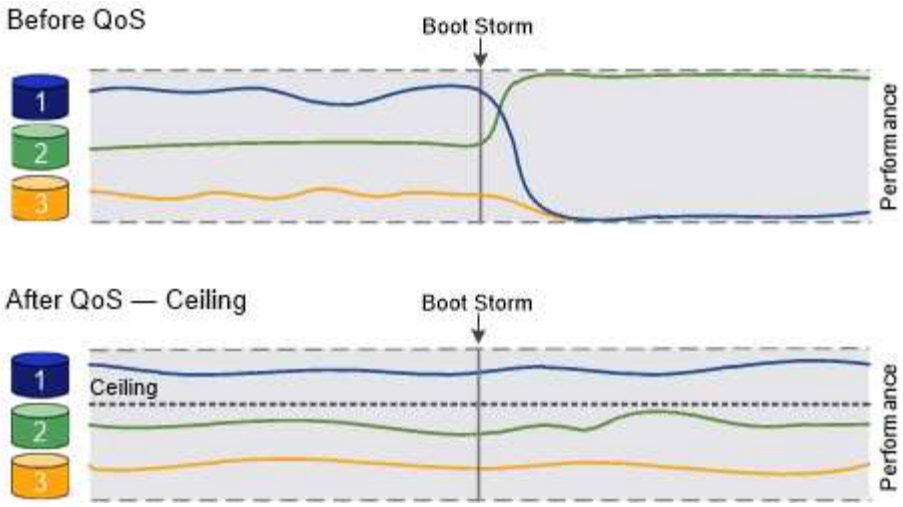
È possibile utilizzare la qualità del servizio (QoS) dello storage per garantire che le performance dei carichi di lavoro critici non vengano degradate dai carichi di lavoro concorrenti. È possibile impostare un *soffitto* di throughput su un carico di lavoro concorrente per limitarne l'impatto sulle risorse di sistema o impostare un *piano* di throughput per un carico di lavoro critico, garantendo che soddisfi gli obiettivi di throughput minimi, indipendentemente dalla domanda dei carichi di lavoro concorrenti. È anche possibile impostare un soffitto e un pavimento per lo stesso carico di lavoro.

Informazioni sui limiti di throughput (QoS Max)

Un limite massimo di throughput limita il throughput per un carico di lavoro a un numero massimo di IOPS o Mbps o IOPS e Mbps. Nella figura riportata di seguito, il limite massimo di throughput per il carico di lavoro 2 garantisce che i carichi di lavoro 1 e 3 non siano "ingombrati".

Un *gruppo di policy* definisce il limite massimo di throughput per uno o più carichi di lavoro. Un carico di lavoro rappresenta le operazioni di i/o per un *oggetto storage:* volume, file, qtree o LUN o tutti i volumi, file, qtree o LUN di una SVM. È possibile specificare il limite massimo quando si crea il gruppo di criteri oppure attendere che i carichi di lavoro vengano monitorati per specificarlo.

> Il throughput per i carichi di lavoro potrebbe superare il limite massimo specificato fino al 10%, soprattutto se un carico di lavoro subisce rapidi cambiamenti nel throughput. Il limite massimo potrebbe essere superato fino al 50% per gestire i burst. I burst si verificano su singoli nodi quando i token accumulano fino al 150%



Informazioni sui piani di throughput (QoS min)

Un piano di throughput garantisce che il throughput per un carico di lavoro non scenda al di sotto di un numero minimo di IOPS o Mbps o IOPS e Mbps. Nella figura riportata di seguito, i livelli di throughput per il carico di lavoro 1 e il carico di lavoro 3 garantiscono il raggiungimento degli obiettivi di throughput minimi, indipendentemente dalla domanda per carico di lavoro 2.

Come suggeriscono gli esempi, un limite di throughput rallenta direttamente il throughput. Un piano di throughput rallenta indirettamente il throughput, dando priorità ai carichi di lavoro per i quali è stato impostato il piano.

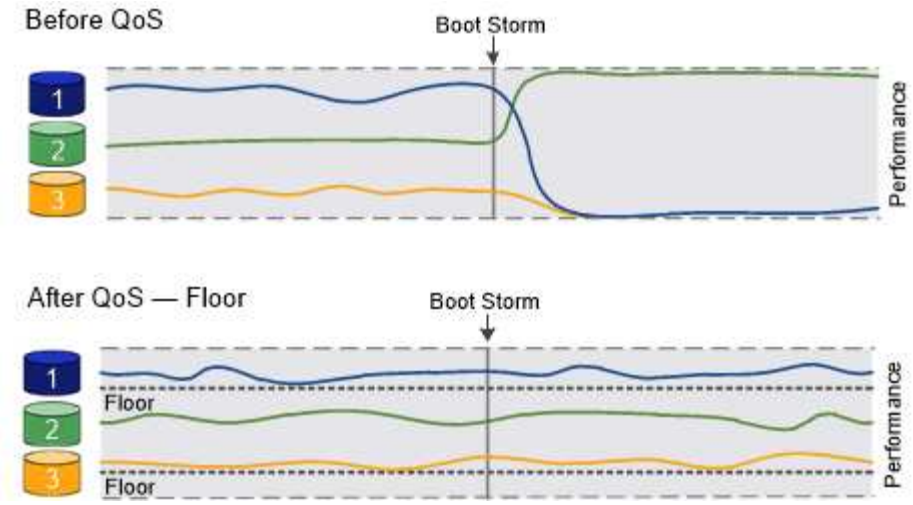
È possibile specificare il piano di lavoro quando si crea il gruppo di policy oppure attendere fino a quando non si monitorano i carichi di lavoro per specificarlo.

A partire da ONTAP 9.13.1, è possibile impostare i piani di throughput nell'ambito SVM con [adaptive-qos-templates]. Nelle versioni di ONTAP precedenti alla 9.13.1, un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM.

Nelle versioni precedenti a ONTAP 9.7, i piani di throughput sono garantiti quando è disponibile una capacità di performance sufficiente.

In ONTAP 9.7 e versioni successive, è possibile garantire il throughput anche quando la capacità delle performance è insufficiente. Questo nuovo comportamento si chiama Floors v2. Per soddisfare le garanzie, floors v2 può comportare una latenza maggiore sui carichi di lavoro senza un piano di throughput o sul lavoro che supera le impostazioni di base. Floors v2 si applica sia alla QoS che alla QoS adattiva.

L'opzione di attivazione/disattivazione del nuovo comportamento dei piani v2 è disponibile in ONTAP 9.7P6 e versioni successive. Un carico di lavoro potrebbe scendere al di sotto del piano specificato durante operazioni critiche come `volume move trigger-cutover`. Anche quando è disponibile una capacità sufficiente e non si svolgono operazioni critiche, il throughput di un workload potrebbe scendere al di sotto del piano specificato fino al 5%. Se il provisioning dei piani è eccessivo e non esiste una capacità di performance, alcuni carichi di lavoro potrebbero scendere al di sotto del piano specificato.



Informazioni sui gruppi di policy QoS condivisi e non condivisi

A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il limite di throughput definito o il piano si applica a ogni singolo carico di lavoro membro. Il comportamento dei gruppi di policy *shared* dipende dal tipo di policy:

- Per i limiti di throughput, il throughput totale per i carichi di lavoro assegnati al gruppo di criteri condivisi non può superare il limite massimo specificato.
- Per i piani di throughput, il gruppo di policy condiviso può essere applicato solo a un singolo workload.

Informazioni su QoS adattiva

Normalmente, il valore del gruppo di criteri assegnato a un oggetto di storage è fisso. È necessario modificare il valore manualmente quando la dimensione dell'oggetto di storage cambia. Un aumento della quantità di spazio utilizzata su un volume, ad esempio, richiede solitamente un aumento corrispondente del limite di throughput specificato per il volume.

QoS adattiva scala automaticamente il valore del gruppo di policy in base alle dimensioni del carico di lavoro, mantenendo il rapporto tra IOPS e TB|GB in base alle dimensioni del carico di lavoro. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

In genere, si utilizza la QoS adattiva per regolare i limiti di throughput, ma è anche possibile utilizzarla per gestire i piani di throughput (quando le dimensioni del carico di lavoro aumentano). La dimensione del carico di lavoro viene espressa come spazio allocato per l'oggetto di storage o come spazio utilizzato dall'oggetto di storage.

Lo spazio utilizzato è disponibile per i piani di throughput in ONTAP 9.5 e versioni successive. Non è supportato per i piani di throughput in ONTAP 9.4 e versioni precedenti.

- Una policy di *spazio allocato* mantiene il rapporto IOPS/TB|GB in base alle dimensioni nominali dell'oggetto di storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB avrà un limite di throughput di 15,000 IOPS, a condizione che il volume rimanga tale. Se il volume viene ridimensionato a 300 GB, la QoS adattiva regola il limite di throughput a 30,000 IOPS.
- Una policy *used space* (predefinita) mantiene il rapporto IOPS/TB|GB in base alla quantità di dati effettivi memorizzati prima dell'efficienza dello storage. Se il rapporto è di 100 IOPS/GB, un volume da 150 GB con 100 GB di dati memorizzati avrebbe un limite massimo di throughput di 10,000 IOPS. Man mano che la quantità di spazio utilizzato cambia, la QoS adattiva regola il limite di throughput in base al rapporto.

A partire da ONTAP 9.5, è possibile specificare una dimensione del blocco i/o per l'applicazione in uso che consenta di esprimere un limite di throughput in IOPS e Mbps. Il limite Mbps viene calcolato moltiplicando le dimensioni del blocco per il limite IOPS. Ad esempio, una dimensione del blocco i/o di 32K per un limite IOPS di 6144 IOPS/TB produce un limite di Mbps di 192 MBps.

È possibile prevedere il seguente comportamento sia per i limiti di throughput che per i piani:

- Quando un carico di lavoro viene assegnato a un gruppo di policy QoS adattivi, il soffitto o il piano vengono aggiornati immediatamente.
- Quando un carico di lavoro in un gruppo di policy QoS adattiva viene ridimensionato, il soffitto o il piano viene aggiornato in circa cinque minuti.

Il throughput deve aumentare di almeno 10 IOPS prima di eseguire gli aggiornamenti.

I gruppi di policy di QoS adattivi non sono sempre condivisi: Il limite di throughput definito o il piano si applica a ciascun carico di lavoro membro singolarmente.

A partire da ONTAP 9.6, i piani di throughput sono supportati da ONTAP Select Premium con SSD.

Modello di gruppo di policy adattive

A partire da ONTAP 9.13.1, è possibile impostare un modello QoS adattivo su una SVM. I modelli di gruppi di policy adattivi consentono di impostare i livelli e i limiti di throughput per tutti i volumi in una SVM.

È possibile impostare i modelli di gruppi di criteri adattivi solo dopo la creazione di SVM. Utilizzare `vserver modify` con il `-qos-adaptive-policy-group-template` parametro per impostare il criterio.

Quando si imposta un modello di gruppo di criteri adattativi, i volumi creati o migrati dopo l'impostazione del criterio ereditano automaticamente il criterio. Gli eventuali volumi presenti nella SVM non vengono influenzati quando si assegna il modello di policy. Se si disattiva il criterio su SVM, qualsiasi volume successivamente migrato o creato su SVM non riceverà il criterio. La disattivazione del modello di gruppo di criteri adattivi non influisce sui volumi che hanno ereditato il modello di criteri, poiché conservano il modello di criteri.

Per ulteriori informazioni, vedere Impostare un modello di gruppo di criteri adattativi.

Supporto generale

La seguente tabella mostra le differenze nel supporto per i limiti di throughput, i piani di throughput e la QoS adattiva.

Risorsa o funzione	Limite di throughput	Piano di throughput	Throughput floor v2	QoS adattiva
Versione di ONTAP 9	Tutto	9.2 e versioni successive	9.7 e versioni successive	9.3 e versioni successive
Piattaforme	Tutto	• AFF • C190 * • ONTAP Select premium con SSD *	• AFF • C190 • ONTAP Select Premium con SSD	Tutto

Risorsa o funzione	Limite di throughput	Piano di throughput	Throughput floor v2	QoS adattiva
Protocolli	Tutto	Tutto	Tutto	Tutto
FabricPool	Sì	Sì, se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud.	Sì, se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud.	No
SnapMirror sincrono	Sì	No	No	Sì

Il supporto di C190 e ONTAP Select è iniziato con la release ONTAP 9.6.

Carichi di lavoro supportati per i limiti di throughput

La tabella seguente mostra il supporto dei workload per i limiti di throughput per la versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

Supporto del carico di lavoro - soffitto	ONTAP 9.0	ONTAP 9.1	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 e versioni successive
Volume	sì	sì	sì	sì	sì	sì
File	sì	sì	sì	sì	sì	sì
LUN	sì	sì	sì	sì	sì	sì
SVM	sì	sì	sì	sì	sì	sì
Volume FlexGroup	no	no	no	sì	sì	sì
qtree*	no	no	no	no	no	sì
Carichi di lavoro multipli per gruppo di policy	sì	sì	sì	sì	sì	sì
Gruppi di criteri non condivisi	no	no	no	no	sì	sì

A partire da ONTAP 9.8, l'accesso NFS è supportato nei qtree dei volumi FlexVol e FlexGroup con NFS attivato. A partire da ONTAP 9.9.1, l'accesso SMB è supportato anche nei qtree dei volumi FlexVol e

FlexGroup con SMB attivato.

Carichi di lavoro supportati per i piani di throughput

La seguente tabella mostra il supporto dei workload per i piani di throughput in base alla versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

Supporto del workload - floor	ONTAP 9.2	ONTAP 9.3	ONTAP 9.4 - 9.7	ONTAP 9.8 - 9.13.0	ONTAP 9.13.1 e versioni successive
Volume	sì	sì	sì	sì	sì
File	no	sì	sì	sì	sì
LUN	sì	sì	sì	sì	sì
SVM	no	no	no	no	sì
Volume FlexGroup	no	no	sì	sì	sì
qtree *	no	no	no	sì	sì
Carichi di lavoro multipli per gruppo di policy	no	no	sì	sì	sì
Gruppi di criteri non condivisi	no	no	sì	sì	sì

A partire da ONTAP 9.8, l'accesso NFS è supportato nei qtree dei volumi FlexVol e FlexGroup con NFS attivato. A partire da ONTAP 9.9.1, l'accesso SMB è supportato anche nei qtree dei volumi FlexVol e FlexGroup con SMB attivato.

Carichi di lavoro supportati per QoS adattiva

La seguente tabella mostra il supporto dei carichi di lavoro per la QoS adattiva in base alla versione di ONTAP 9. I volumi root, i mirror di condivisione del carico e i mirror di protezione dei dati non sono supportati.

Supporto del carico di lavoro - QoS adattiva	ONTAP 9.3	ONTAP 9.4 - 9.13.0	ONTAP 9.13.1 e versioni successive
Volume	sì	sì	sì
File	no	sì	sì
LUN	no	sì	sì
SVM	no	no	sì
Volume FlexGroup	no	sì	sì
Carichi di lavoro multipli per gruppo di policy	sì	sì	sì
Gruppi di criteri non condivisi	sì	sì	sì

Numero massimo di workload e gruppi di policy

La seguente tabella mostra il numero massimo di workload e gruppi di policy per versione di ONTAP 9.

Supporto dei carichi di lavoro	ONTAP 9.3 e versioni precedenti	ONTAP 9.4 e versioni successive
Carichi di lavoro massimi per cluster	12,000	40,000
Carichi di lavoro massimi per nodo	12,000	40,000
Numero massimo di gruppi di criteri	12,000	12,000

Attiva o disattiva i piani di throughput v2

È possibile attivare o disattivare il throughput floors v2 su AFF. L'impostazione predefinita è Enabled (attivato). Con FLOors v2 abilitato, è possibile soddisfare i piani di throughput quando i controller vengono utilizzati in modo pesante a scapito di una maggiore latenza su altri carichi di lavoro. Floors v2 si applica sia a QoS che a QoS adattivo.

Fasi

1. Passare al livello di privilegio avanzato:

   ```
   set -privilege advanced
   ```

2. Immettere uno dei seguenti comandi:

Se si desidera…	Utilizzare questo comando:
Disattiva piani v2	`qos settings throughput-floors-v2 -enable false`
Abilitare i piani v2	`qos settings throughput-floors-v2 -enable true`

> Per disattivare il throughput floors v2 in un cluster MetroCluster, è necessario eseguire `qos settings throughput-floors-v2 -enable false` comando sui cluster di origine e di destinazione.

```
cluster1::*> qos settings throughput-floors-v2 -enable false
```

Workflow di QoS dello storage

Se si conoscono già i requisiti di performance per i carichi di lavoro che si desidera gestire con QoS, è possibile specificare il limite di throughput quando si crea il gruppo di

policy. In caso contrario, è possibile attendere fino a quando non si monitorano i carichi di lavoro per specificare il limite.

Impostare un limite massimo di throughput con QoS

È possibile utilizzare `max-throughput` Campo per un gruppo di criteri per definire un limite massimo di throughput per i carichi di lavoro degli oggetti di storage (QoS Max). È possibile applicare il gruppo di criteri quando si crea o si modifica l'oggetto di storage.

Di cosa hai bisogno

- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.
- Per applicare un gruppo di criteri a una SVM, è necessario essere un amministratore del cluster.

A proposito di questa attività

- A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il limite di throughput definito si applica a ogni singolo carico di lavoro membro. In caso contrario, il gruppo di criteri è *shared:* il throughput totale per i carichi di lavoro assegnati al gruppo di criteri non può superare il limite massimo specificato.

  Impostare `-is-shared=false` per `qos policy-group create` per specificare un gruppo di politiche non condiviso.

- È possibile specificare il limite di throughput per il limite massimo in IOPS, MB/s o IOPS, MB/s. Se si specificano IOPS e MB/s, viene applicato il limite raggiunto per primo.

  > Se si impostano un soffitto e un pavimento per lo stesso carico di lavoro, è possibile specificare il limite di throughput per il soffitto solo in IOPS.

- Un oggetto storage soggetto a un limite di QoS deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri. Più gruppi di criteri possono appartenere alla stessa SVM.
- Non è possibile assegnare un oggetto di storage a un gruppo di criteri se l'oggetto contenente o i relativi oggetti figlio appartengono al gruppo di criteri.
- È consigliabile applicare un gruppo di criteri allo stesso tipo di oggetti di storage.

Fasi

1. Creare un gruppo di criteri:

   `qos policy-group create -policy-group` *`policy_group`* `-vserver` *`SVM`* `-max -throughput` *`number_of_iops`*`|Mb/S|iops,Mb/S -is-shared true|false`

   Per la sintassi completa dei comandi, vedere la pagina man. È possibile utilizzare `qos policy-group modify` comando per regolare i limiti di throughput.

   Il comando seguente crea il gruppo di criteri condivisi `pg-vs1` Con un throughput massimo di 5,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy-group pg-vs1 -vserver vs1
   -max-throughput 5000iops -is-shared true
   ```

Il comando seguente crea il gruppo di criteri non condivisi `pg-vs3` Con un throughput massimo di 100 IOPS e 400 Kb/S:

```
cluster1::> qos policy-group create -policy-group pg-vs3 -vserver vs3
-max-throughput 100iops,400KB/s -is-shared false
```

Il comando seguente crea il gruppo di criteri non condivisi `pg-vs4` senza un limite di throughput:

```
cluster1::> qos policy-group create -policy-group pg-vs4 -vserver vs4
-is-shared false
```

2. Applicare un gruppo di criteri a una SVM, a un file, a un volume o a un LUN:

   storage_object `create -vserver` *SVM* `-qos-policy-group` *policy_group*

   Per la sintassi completa dei comandi, vedere le pagine man. È possibile utilizzare *storage_object* `modify` per applicare un gruppo di criteri diverso all'oggetto di storage.

   Il seguente comando applica il gruppo di criteri `pg-vs1` A SVM `vs1`:

   ```
   cluster1::> vserver create -vserver vs1 -qos-policy-group pg-vs1
   ```

   I seguenti comandi applicano il gruppo di criteri `pg-app` ai volumi `app1` e. `app2`:

   ```
   cluster1::> volume create -vserver vs2 -volume app1 -aggregate aggr1
   -qos-policy-group pg-app
   ```

   ```
   cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
   -qos-policy-group pg-app
   ```

3. Monitorare le performance dei gruppi di policy:

   `qos statistics performance show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

   Il seguente comando mostra le prestazioni del gruppo di criteri:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_vs1                   5008       19.56MB/s     2.45ms
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

4. Monitorare le performance dei carichi di lavoro:

   `qos statistics workload performance show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

   Il seguente comando mostra le performance del carico di lavoro:

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app1-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > È possibile utilizzare `qos statistics workload latency show` Comando per visualizzare statistiche dettagliate sulla latenza per i carichi di lavoro QoS.

Impostare un piano di throughput con QoS

È possibile utilizzare `min-throughput` Campo per un gruppo di policy per definire un piano di throughput per i carichi di lavoro degli oggetti storage (QoS min). È possibile applicare il gruppo di criteri quando si crea o si modifica l'oggetto di storage. A partire da ONTAP 9.8, è possibile specificare il volume di throughput in IOPS o Mbps o IOPS e Mbps.

Prima di iniziare

- È necessario eseguire ONTAP 9.2 o versione successiva. I piani di throughput sono disponibili a partire da ONTAP 9.2.
- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.
- A partire da ONTAP 9.13.1, è possibile applicare i piani di throughput a livello di SVM utilizzando un

modello di gruppo di policy adattive. Non è possibile impostare un modello di gruppo di criteri adattativi su una SVM con un gruppo di criteri QoS.

A proposito di questa attività

- A partire da ONTAP 9.4, è possibile utilizzare un gruppo di policy di qualità del servizio *non-shared* per specificare che il piano di throughput definito deve essere applicato a ogni singolo carico di lavoro membro. Questa è l'unica condizione in cui un gruppo di policy per un piano di throughput può essere applicato a più carichi di lavoro.

  Impostare `-is-shared=false` per `qos policy-group create` per specificare un gruppo di criteri non condiviso.

- Il throughput di un carico di lavoro potrebbe scendere al di sotto del piano specificato se la capacità delle performance (spazio di crescita) del nodo o dell'aggregato è insufficiente.
- Un oggetto storage soggetto a un limite di QoS deve essere contenuto dalla SVM a cui appartiene il gruppo di criteri. Più gruppi di criteri possono appartenere alla stessa SVM.
- È consigliabile applicare un gruppo di criteri allo stesso tipo di oggetti di storage.
- Un gruppo di criteri che definisce un piano di throughput non può essere applicato a una SVM.

Fasi

1. Controllare che le prestazioni sul nodo o sull'aggregato siano adeguate, come descritto nella "Identificazione della capacità di prestazioni rimanente".
2. Creare un gruppo di criteri:

   `qos policy-group create -policy group` *`policy_group`* `-vserver` *`SVM`* `-min -throughput` *`qos_target`* `-is-shared true|false`

   Per una sintassi completa dei comandi, consulta la pagina man della tua release ONTAP. È possibile utilizzare `qos policy-group modify` comando per regolare i piani di throughput.

   Il comando seguente crea il gruppo di criteri condivisi `pg-vs2` Con un throughput minimo di 1,000 IOPS:

   ```
   cluster1::> qos policy-group create -policy group pg-vs2 -vserver vs2
   -min-throughput 1000iops -is-shared true
   ```

   Il comando seguente crea il gruppo di criteri non condivisi `pg-vs4` senza un limite di throughput:

   ```
   cluster1::> qos policy-group create -policy group pg-vs4 -vserver vs4
   -is-shared false
   ```

3. Applicare un gruppo di criteri a un volume o a un LUN:

   `storage_object` `create -vserver` *`SVM`* `-qos-policy-group` *`policy_group`*

   Per la sintassi completa dei comandi, vedere le pagine man. È possibile utilizzare `_storage_object_modify` per applicare un gruppo di criteri diverso all'oggetto di storage.

   Il seguente comando applica il gruppo di criteri `pg-app2` al volume `app2`:

```
cluster1::> volume create -vserver vs2 -volume app2 -aggregate aggr1
-qos-policy-group pg-app2
```

4. Monitorare le performance dei gruppi di policy:

   `qos statistics performance show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

   Il seguente comando mostra le prestazioni del gruppo di criteri:

```
cluster1::> qos statistics performance show
Policy Group           IOPS      Throughput   Latency
-------------------- -------- --------------- ----------
-total-                 12316       47.76MB/s  1264.00us
pg_app2                  7216       28.19MB/s   420.00us
_System-Best-Effort        62       13.36KB/s     4.13ms
_System-Background         30           0KB/s        0ms
```

5. Monitorare le performance dei carichi di lavoro:

   `qos statistics workload performance show`

   Per la sintassi completa dei comandi, vedere la pagina man.

   > Monitorare le performance dal cluster. Non utilizzare uno strumento sull'host per monitorare le prestazioni.

   Il seguente comando mostra le performance del carico di lavoro:

```
cluster1::> qos statistics workload performance show
Workload          ID     IOPS      Throughput    Latency
--------------- ------ -------- ---------------- ----------
-total-              -    12320        47.84MB/s  1215.00us
app2-wid7967      7967     7219        28.20MB/s   319.00us
vs1-wid12279     12279     5026        19.63MB/s     2.52ms
_USERSPACE_APPS     14       55        10.92KB/s   236.00us
_Scan_Backgro..   5688       20            0KB/s        0ms
```

   > È possibile utilizzare `qos statistics workload latency show` Comando per visualizzare statistiche dettagliate sulla latenza per i carichi di lavoro QoS.

Utilizzare gruppi di policy QoS adattivi

È possibile utilizzare un gruppo di policy *Adaptive QoS* per scalare automaticamente un limite di throughput o le dimensioni da pavimento a volume, mantenendo il rapporto tra IOPS e TB|GB al variare delle dimensioni del volume. Si tratta di un vantaggio significativo quando si gestiscono centinaia o migliaia di carichi di lavoro in un'implementazione di grandi dimensioni.

Prima di iniziare

- È necessario eseguire ONTAP 9.3 o versione successiva. I gruppi di policy QoS adattivi sono disponibili a partire da ONTAP 9.3.
- Per creare un gruppo di criteri, è necessario essere un amministratore del cluster.

A proposito di questa attività

Un oggetto storage può essere membro di un gruppo di criteri adattivi o non adattivi, ma non di entrambi. La SVM dell'oggetto di storage e il criterio devono essere identici. L'oggetto di storage deve essere in linea.

I gruppi di policy di QoS adattivi non sono sempre condivisi: Il limite di throughput definito o il piano si applica a ciascun carico di lavoro membro singolarmente.

Il rapporto tra i limiti di throughput e le dimensioni degli oggetti di storage è determinato dall'interazione dei seguenti campi:

- `expected-iops` È il minimo IOPS previsto per TB|GB allocati.

> ℹ `expected-iops` È garantito solo sulle piattaforme AFF. `expected-iops` È garantito per FabricPool solo se la policy di tiering è impostata su "nessuno" e non ci sono blocchi nel cloud. `expected-iops` È garantito per i volumi che non sono in una relazione sincrona di SnapMirror.

- `peak-iops` È il massimo IOPS possibile per TB|GB allocati o utilizzati.
- `expected-iops-allocation` specifica se per gli iops previsti viene utilizzato lo spazio allocato (impostazione predefinita) o lo spazio utilizzato.

> ℹ `expected-iops-allocation` È disponibile in ONTAP 9.5 e versioni successive. Non è supportato in ONTAP 9.4 e versioni precedenti.

- `peak-iops-allocation` specifica se viene utilizzato lo spazio allocato o lo spazio utilizzato (impostazione predefinita) per `peak-iops`.
- `absolute-min-iops` È il numero minimo assoluto di IOPS. È possibile utilizzare questo campo con oggetti di storage molto piccoli. Sovrascrive entrambi `peak-iops` e/o. `expected-iops` quando `absolute-min-iops` è maggiore del valore calcolato `expected-iops`.

  Ad esempio, se si imposta `expected-iops` Fino a 1,000 IOPS/TB e le dimensioni del volume sono inferiori a 1 GB, il valore calcolato `expected-iops` Sarà un IOP frazionale. Il valore calcolato `peak-iops` sarà una frazione ancora più piccola. Per evitare questo problema, impostare `absolute-min-iops` a un

valore realistico.

- `block-size` Specifica la dimensione del blocco i/o dell'applicazione. L'impostazione predefinita è 32K. I valori validi sono 8K, 16K, 32K, 64K, QUALSIASI. QUALSIASI indica che la dimensione del blocco non viene applicata.

Sono disponibili tre gruppi di criteri QoS adattivi predefiniti, come mostrato nella tabella seguente. È possibile applicare questi gruppi di criteri direttamente a un volume.

Gruppo di criteri predefinito	IOPS/TB previsti	IOPS/TB di picco	IOPS minimo assoluto
`extreme`	6,144	12,288	1000
`performance`	2,048	4,096	500
`value`	128	512	75

Non è possibile assegnare un oggetto di storage a un gruppo di criteri se l'oggetto contenente o i relativi oggetti figlio appartengono a un gruppo di criteri. Nella tabella seguente sono elencate le restrizioni.

Se si assegna…	**Quindi non è possibile assegnare…**
SVM a un gruppo di criteri	Qualsiasi oggetto di storage contenuto dalla SVM a un gruppo di criteri
Su un gruppo di criteri	Volumi contenenti SVM o LUN figlio di un gruppo di criteri
LUN a un gruppo di criteri	I LUN contenenti un volume o una SVM in un gruppo di criteri
Su un gruppo di criteri	Il file contenente un volume o una SVM in un gruppo di criteri

Fasi

1. Creare un gruppo di criteri QoS adattivi:

   ```
   qos adaptive-policy-group create -policy group policy_group -vserver SVM
   -expected-iops number_of_iops/TB|GB -peak-iops number_of_iops/TB|GB -expected
   -iops-allocation-space|used-space -peak-iops-allocation allocated-space|used-
   space -absolute-min-iops number_of_iops -block-size 8K|16K|32K|64K|ANY
   ```

   Per la sintassi completa dei comandi, vedere la pagina man.

   > `-expected-iops-allocation` e. `-block-size` È disponibile in ONTAP 9.5 e versioni successive. Queste opzioni non sono supportate in ONTAP 9.4 e versioni precedenti.

   Il seguente comando crea un gruppo di criteri QoS adattivi `adpg-app1` con `-expected-iops` Impostato

su 300 IOPS/TB, `-peak-iops` Impostato su 1,000 IOPS/TB, `-peak-iops-allocation` impostare su `used-space`, e. `-absolute-min-iops` Impostato su 50 IOPS:

```
cluster1::> qos adaptive-policy-group create -policy group adpg-app1
-vserver vs2 -expected-iops 300iops/tb -peak-iops 1000iops/TB -peak-iops
-allocation used-space -absolute-min-iops 50iops
```

2. Applicare un gruppo di criteri QoS adattivi a un volume:

   `volume create -vserver SVM -volume volume -aggregate aggregate -size number_of TB|GB -qos-adaptive-policy-group policy_group`

   Per la sintassi completa dei comandi, vedere le pagine man.

   Il seguente comando applica il gruppo di criteri QoS adattivi `adpg-app1` al volume `app1`:

```
cluster1::> volume create -vserver vs1 -volume app1 -aggregate aggr1
-size 2TB -qos-adaptive-policy-group adpg-app1
```

   I seguenti comandi applicano il gruppo di criteri QoS adattivi predefinito `extreme` al nuovo volume `app4` e al volume esistente `app5`. Il limite di throughput definito per il gruppo di criteri si applica ai volumi `app4` e. `app5` singolarmente:

```
cluster1::> volume create -vserver vs4 -volume app4 -aggregate aggr4
-size 2TB -qos-adaptive-policy-group extreme
```

```
cluster1::> volume modify -vserver vs5 -volume app5 -qos-adaptive-policy
-group extreme
```

Impostare un modello di gruppo di criteri adattativi

A partire da ONTAP 9.13.1, è possibile applicare i livelli e i limiti di throughput a livello di SVM utilizzando un modello di gruppo di policy adattivo.

A proposito di questa attività

- Il modello di gruppo di criteri adattivi è un criterio predefinito `apg1`. Il criterio può essere modificato in qualsiasi momento. Può essere impostato solo con l'API REST CLI o ONTAP e può essere applicato solo alle SVM esistenti.
- Il modello di gruppo di policy adattive influisce solo sui volumi creati o migrati sulla SVM dopo aver impostato il criterio. I volumi esistenti sulla SVM mantengono lo stato esistente.

  Se si disattiva il modello di gruppo di criteri adattivi, i volumi su SVM conservano i criteri esistenti. Solo i volumi successivamente creati o migrati sulla SVM saranno influenzati dalla disabilitazione.

- Non è possibile impostare un modello di gruppo di criteri adattativi su una SVM con un gruppo di criteri QoS.
- I modelli di gruppi di policy adattivi sono progettati per le piattaforme AFF. È possibile impostare un modello di gruppo di policy adattivo su altre piattaforme, ma il criterio potrebbe non applicare un throughput minimo. Allo stesso modo, è possibile aggiungere un modello di gruppo di policy adattivo a una SVM in un aggregato FabricPool o in un aggregato che non supporta un throughput minimo, tuttavia il throughput non verrà applicato.
- Se la SVM si trova in una configurazione MetroCluster o in una relazione SnapMirror, il modello di gruppo di criteri adattativi verrà applicato alla SVM mirrorata.

Fasi

1. Modificare la SVM per applicare il modello di gruppo di criteri adattativi:
   `vserver modify -qos-adaptive-policy-group-template apg1`
2. Verificare che il criterio sia stato impostato:
   `vserver show -fields qos-adaptive-policy-group`

Monitorare le performance del cluster con Unified Manager

Con Active IQ Unified Manager, puoi massimizzare la disponibilità e mantenere il controllo della tua infrastruttura storage NetApp AFF e FAS per migliorare scalabilità, supportabilità, performance e sicurezza.

Active IQ Unified Manager monitora continuamente lo stato del sistema e invia avvisi, in modo che la tua organizzazione possa liberare risorse del personale IT. È possibile visualizzare istantaneamente lo stato dello storage da una singola dashboard e risolvere rapidamente i problemi attraverso le azioni consigliate.

La gestione dei dati è semplificata perché è possibile rilevare, monitorare e ricevere notifiche per gestire in modo proattivo lo storage e risolvere rapidamente i problemi. L'efficienza degli amministratori è migliorata grazie alla possibilità di monitorare petabyte di dati da un singolo dashboard e gestire i dati in modo scalabile.

Con Active IQ Unified Manager, puoi restare al passo con le esigenze di business fluttuanti, ottimizzando le performance utilizzando dati sulle performance e analytics avanzati. Le funzionalità di reporting consentono di accedere a report standard o creare report operativi personalizzati per soddisfare le esigenze specifiche del business.

Link correlati:

- "Scopri di più su Active IQ Unified Manager"
- "Inizia subito con Active IQ Unified Manager per VMware"
- "Inizia subito con Active IQ Unified Manager per Linus"
- "Introduzione a Active IQ Unified Manager per Windows"

Monitorare le performance del cluster con Cloud Insights

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

Cloud Insights è disponibile in due edizioni

L'edizione di base di Cloud Insights è progettata appositamente per monitorare e ottimizzare le risorse del data fabric NetApp. Fornisce analisi avanzate per le connessioni tra tutte le risorse NetApp, tra cui HCI e All Flash FAS (AFF) all'interno dell'ambiente, gratuitamente.

L'edizione standard di Cloud Insights si concentra non solo sui componenti dell'infrastruttura abilitati per il data fabric, ma anche sugli ambienti multi-vendor e multi-cloud. Grazie alle sue funzionalità avanzate, puoi accedere al supporto di oltre 100 servizi e risorse.

Nel mondo odierno, con risorse in gioco dai data center on-premise a più cloud pubblici, è fondamentale avere un quadro completo dell'applicazione stessa al disco back-end dello storage array. Il supporto aggiuntivo per il monitoraggio delle applicazioni (come Kafka, MongoDB e Nginx) fornisce le informazioni e le conoscenze necessarie per operare al livello di utilizzo ottimale e con il buffer di rischio perfetto.

Entrambe le edizioni (di base e standard) possono integrarsi con NetApp Active IQ Unified Manager. I clienti che utilizzano Active IQ Unified Manager possono visualizzare le informazioni di Unione all'interno dell'interfaccia utente di Cloud Insights. Le notifiche pubblicate su Active IQ Unified Manager non vengono trascurate e possono essere correlate agli eventi in Cloud Insights. In altre parole, otterrai il meglio di entrambi i mondi.

Monitorare, risolvere i problemi e ottimizzare tutte le risorse

Cloud Insights ti aiuta a ridurre significativamente il tempo necessario per risolvere i problemi e a evitare che incidano sugli utenti finali. Inoltre, ti aiuta a ridurre i costi dell'infrastruttura cloud. La tua esposizione alle minacce interne è ridotta proteggendo i tuoi dati con informazioni pratiche.

Cloud Insights ti offre visibilità sull'intera infrastruttura ibrida in un'unica posizione, dal cloud pubblico al data center. Puoi creare istantaneamente dashboard pertinenti che possono essere personalizzati in base alle tue esigenze specifiche. È inoltre possibile creare avvisi mirati e condizionali specifici e pertinenti alle esigenze dell'organizzazione.

Il rilevamento avanzato delle anomalie consente di risolvere in modo proattivo i problemi prima che si verifichino. È possibile visualizzare automaticamente i conflitti e il degrado delle risorse per ripristinare rapidamente i carichi di lavoro interessati. Il troubleshooting viene eseguito più rapidamente grazie alla gerarchia di relazioni creata automaticamente tra i diversi componenti dello stack.

Puoi identificare le risorse inutilizzate o abbandonate nel tuo ambiente, che ti aiuta a scoprire le opportunità di dimensionare correttamente l'infrastruttura e ottimizzare l'intera spesa.

Cloud Insights visualizza la topologia del sistema per comprendere l'architettura di Kubernetes. È possibile monitorare lo stato dei cluster Kubernetes, inclusi i nodi in difficoltà, e ingrandire quando si verifica un problema.

Cloud Insights ti aiuta a proteggere i dati dell'organizzazione dall'utilizzo improprio da parte di utenti malintenzionati o compromessi attraverso l'apprendimento automatico avanzato e il rilevamento delle anomalie che ti offrono informazioni pratiche sulle minacce interne.

Cloud Insights ti aiuta a visualizzare le metriche di Kubernetes in modo da poter comprendere appieno le relazioni tra pod, nodi e cluster. È possibile valutare lo stato di salute di un cluster o di un pod di lavoro, nonché il carico attualmente in elaborazione, consentendo di assumere il controllo del cluster K8S e di controllare sia lo stato di salute che il costo dell'implementazione.

Link correlati

- "Scopri di più su Cloud Insights"
- "Inizia subito con Cloud Insights"

Registrazione dell'audit

Come ONTAP implementa la registrazione dell'audit

Le attività di gestione registrate nel registro di audit sono incluse nei report standard di AutoSupport e alcune attività di registrazione sono incluse nei messaggi EMS. È inoltre possibile inoltrare il registro di controllo alle destinazioni specificate e visualizzare i file di registro di controllo utilizzando la CLI o un browser Web.

A partire da ONTAP 9.11.1, è possibile visualizzare il contenuto del registro di controllo utilizzando Gestione di sistema.

A partire da ONTAP 9.12.1, ONTAP fornisce avvisi di manomissione per i registri di controllo. ONTAP esegue un lavoro giornaliero in background per verificare la presenza di manomissioni di file audit.log e invia un avviso EMS se trova file di registro modificati o manomessi.

ONTAP registra le attività di gestione eseguite sul cluster, ad esempio la richiesta emessa, l'utente che ha attivato la richiesta, il metodo di accesso dell'utente e l'ora della richiesta.

Le attività di gestione possono essere di uno dei seguenti tipi:

- IMPOSTARE le richieste, che in genere si applicano a comandi o operazioni non di visualizzazione
  - Queste richieste vengono emesse quando si esegue un `create`, `modify`, o. `delete` ad esempio.
  - Le richieste di set vengono registrate per impostazione predefinita.
- OTTENERE richieste che recuperano le informazioni e le visualizzano nell'interfaccia di gestione
  - Queste richieste vengono emesse quando si esegue un `show` ad esempio.
  - LE richieste GET non vengono registrate per impostazione predefinita, ma è possibile controllare se LE richieste GET inviate dall'interfaccia CLI ONTAP (`-cliget`), dall'API ONTAP (`-ontapiget`) O dall'API REST (`-httpget`) sono registrati nel file.

ONTAP registra le attività di gestione in `/mroot/etc/log/mlog/audit.log` file di un nodo. I comandi delle tre shell per i comandi CLI—la clustershell, il nodeshell e la shell di sistema non interattiva (i comandi interattivi della shell di sistema non sono registrati)--così come i comandi API sono registrati qui. I registri di audit includono timestamp per mostrare se tutti i nodi di un cluster sono sincronizzati in base all'ora.

Il `audit.log` Il file viene inviato dallo strumento AutoSupport ai destinatari specificati. È inoltre possibile inoltrare il contenuto in modo sicuro alle destinazioni esterne specificate, ad esempio un server Splunk o syslog.

Il `audit.log` il file viene ruotato ogni giorno. La rotazione si verifica anche quando raggiunge 100 MB di dimensione e le precedenti 48 copie vengono conservate (con un totale massimo di 49 file). Quando il file di audit esegue la rotazione giornaliera, non viene generato alcun messaggio EMS. Se il file di audit ruota a causa del superamento del limite di dimensione del file, viene generato un messaggio EMS.

Modifiche alla registrazione dell'audit in ONTAP 9

A partire da ONTAP 9 `command-history.log` il file viene sostituito da `audit.log`e il `mgwd.log` il file non contiene più informazioni di audit. Se si esegue l'aggiornamento a ONTAP 9, è necessario esaminare gli script o gli strumenti che fanno riferimento ai file legacy e al loro contenuto.

Dopo l'aggiornamento a ONTAP 9, esistente `command-history.log` i file vengono conservati. Vengono ruotati verso l'esterno (cancellati) come nuovi `audit.log` i file vengono ruotati in (creati).

Strumenti e script che controllano `command-history.log` il file potrebbe continuare a funzionare, perché un collegamento soft da `command-history.log` a. `audit.log` viene creato al momento dell'aggiornamento. Tuttavia, strumenti e script che controllano `mgwd.log` il file non riesce, perché non contiene più informazioni di audit.

Inoltre, i registri di controllo di ONTAP 9 e versioni successive non includono più le seguenti voci, in quanto non sono considerate utili e causano attività di registrazione non necessarie:

- Comandi interni eseguiti da ONTAP (ovvero, dove username=root)
- Alias dei comandi (separatamente dal comando a cui puntano)

A partire da ONTAP 9, è possibile trasmettere i registri di controllo in modo sicuro a destinazioni esterne utilizzando i protocolli TCP e TLS.

Visualizzare il contenuto del registro di controllo

È possibile visualizzare il contenuto dei cluster `/mroot/etc/log/mlog/audit.log` Utilizzando l'interfaccia utente di ONTAP, Gestore di sistema o un browser Web.

Le voci del file di log del cluster includono quanto segue:

Ora
Data e ora della voce di registro.

Applicazione
L'applicazione utilizzata per connettersi al cluster. Esempi di valori possibili sono `internal, console, ssh, http, ontapi, snmp, rsh, telnet,` e. `service-processor`.

Utente
Il nome utente dell'utente remoto.

Stato
Lo stato corrente della richiesta di audit, che potrebbe essere `success, pending,` oppure `error`.

Messaggio
Campo facoltativo che potrebbe contenere informazioni aggiuntive o errori sullo stato di un comando.

ID sessione
L'ID della sessione in cui viene ricevuta la richiesta. A ogni *sessione* SSH viene assegnato un ID sessione, mentre a ogni *richiesta* HTTP, ONTAPI o SNMP viene assegnato un ID sessione univoco.

VM di storage

SVM attraverso cui l'utente si è connesso.

Scopo

Viene visualizzato `svm` Quando la richiesta si trova su una macchina virtuale per lo storage dei dati, altrimenti viene visualizzato `cluster`.

ID comando

L'ID di ciascun comando ricevuto in una sessione CLI. In questo modo è possibile correlare una richiesta e una risposta. Le richieste ZAPI, HTTP e SNMP non dispongono di ID comando.

È possibile visualizzare le voci di registro del cluster dall'interfaccia utente di ONTAP, da un browser Web e a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

- Per visualizzare l'inventario, selezionare **Eventi e processi > registri di controllo**. + ogni colonna dispone di controlli per filtrare, ordinare, cercare, mostrare e inventariare le categorie. I dettagli dell'inventario possono essere scaricati come guida Excel.
- Per impostare i filtri, fare clic sul pulsante **Filter** (filtro) in alto a destra, quindi selezionare i campi desiderati. + è inoltre possibile visualizzare tutti i comandi eseguiti nella sessione in cui si è verificato un errore facendo clic sul collegamento Session ID (ID sessione).

CLI

Per visualizzare le voci di audit unite da più nodi nel cluster, immettere:
`security audit log show` *`[parameters]`*

È possibile utilizzare `security audit log show` comando per visualizzare le voci di audit per i singoli nodi o unite da più nodi nel cluster. È inoltre possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. Per ulteriori informazioni, consulta la pagina man.

Browser Web

È possibile visualizzare il contenuto di `/mroot/etc/log/mlog` directory su un singolo nodo utilizzando un browser web. "Scopri come accedere ai file di log, core dump e MIB di un nodo utilizzando un browser Web".

Gestire le impostazioni di richiesta DI VERIFICA GET

Sebbene LE richieste SET siano registrate per impostazione predefinita, le richieste GET non lo sono. Tuttavia, è possibile controllare se LE richieste GET inviate dall'HTML di ONTAP (`-httpget`), l'interfaccia utente di ONTAP (`-cliget`), o dalle API ONTAP (`-ontapiget`) sono registrati nel file.

È possibile modificare le impostazioni di registrazione dell'audit dalla CLI di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

1. Selezionare **Eventi e processi > registri di controllo**.
2. Fare clic su  nell'angolo in alto a destra, scegliere le richieste da aggiungere o rimuovere.

CLI

- Per specificare che le richieste GET dall'interfaccia utente o dalle API ONTAP devono essere registrate nel registro di controllo (il file audit.log), oltre alle richieste set predefinite, immettere:
  `security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget {on|off}]`
- Per visualizzare le impostazioni correnti, immettere:
  `security audit show`

Per ulteriori informazioni, consulta le pagine man.

Gestire le destinazioni del registro di controllo

È possibile inoltrare il registro di controllo a un massimo di 10 destinazioni. Ad esempio, è possibile inoltrare il log a un server Splunk o syslog per scopi di monitoraggio, analisi o backup.

A proposito di questa attività

Per configurare l'inoltro, è necessario fornire l'indirizzo IP dell'host syslog o Splunk, il relativo numero di porta, un protocollo di trasmissione e la funzione syslog da utilizzare per i registri inoltrati. "Scopri le funzionalità di syslog".

È possibile selezionare uno dei seguenti valori di trasmissione:

UDP non crittografato
: User Datagram Protocol senza sicurezza (impostazione predefinita)

TCP non crittografato
: Transmission Control Protocol senza sicurezza

Crittografia TCP
: Transmission Control Protocol with Transport Layer Security (TLS) + Un'opzione **verify server** è disponibile quando si seleziona il protocollo crittografato TCP.

È possibile inoltrare i registri di controllo dall'interfaccia utente di ONTAP e, a partire da ONTAP 9.11.1, da Gestore di sistema.

System Manager

- Per visualizzare le destinazioni del registro di controllo, selezionare **Cluster > Impostazioni**. + Un numero di destinazioni del registro viene visualizzato nel riquadro **Gestione notifiche**. Fare clic su ⋮ per visualizzare i dettagli.
- Per aggiungere, modificare o eliminare le destinazioni del registro di controllo, selezionare **Eventi e processi > registri di controllo**, quindi fare clic su **Gestisci destinazioni di controllo** nella parte superiore destra della schermata. + clic + Add oppure fare clic su ⋮ Nella colonna **Indirizzo host** per modificare o eliminare le voci.

CLI

1. Per ciascuna destinazione a cui si desidera inoltrare il registro di controllo, specificare l'indirizzo IP o il nome host di destinazione e le opzioni di sicurezza.

```
cluster1::> cluster log-forwarding create -destination
192.168.123.96
-port 514 -facility user

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 514 -protocol tcp-encrypted -facility user
```

   - Se il `cluster log-forwarding create` impossibile eseguire il ping dell'host di destinazione per verificare la connettività, il comando non riesce e viene visualizzato un errore. Anche se non consigliato, utilizzare `-force` il parametro con il comando ignora la verifica della connettività.
   - Quando si imposta `-verify-server` parametro a. `true`, l'identità della destinazione di inoltro del log viene verificata convalidando il relativo certificato. È possibile impostare il valore su `true` solo quando si seleziona `tcp-encrypted` valore in `-protocol` campo.

2. Verificare che i record di destinazione siano corretti utilizzando `cluster log-forwarding show` comando.

```
cluster1::> cluster log-forwarding show

                                                 Verify Syslog
Destination Host          Port   Protocol        Server Facility
------------------------- ------ --------        ------ --------
192.168.123.96            514    udp-unencrypted false  user
192.168.123.98            514    tcp-encrypted   true   user
2 entries were displayed.
```

Per ulteriori informazioni, consulta le pagine man.

AutoSupport

Gestisci le impostazioni AutoSupport con Gestione di sistema

È possibile utilizzare Gestione di sistema per gestire le impostazioni dell'account AutoSupport.

È possibile eseguire le seguenti procedure:

Consente di visualizzare le impostazioni AutoSupport

È possibile utilizzare Gestione sistema per visualizzare le impostazioni dell'account AutoSupport.

Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).

   Nella sezione **AutoSupport** vengono visualizzate le seguenti informazioni:

   - Stato
   - Protocollo di trasporto
   - Server proxy
   - Da indirizzo e-mail
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **altre opzioni**.

   Vengono visualizzate ulteriori informazioni sulla connessione a AutoSupport e sulle impostazioni e-mail. Inoltre, viene elencata la cronologia di trasferimento dei messaggi.

Generare e inviare dati AutoSupport

In Gestore di sistema, è possibile avviare la generazione di messaggi AutoSupport e scegliere tra i nodi del cluster da cui vengono raccolti i dati.

Fasi

1. In System Manager, selezionare **Cluster > Settings**.
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **genera e Invia**.
3. Inserire un oggetto.
4. Selezionare la casella di controllo in **Raccogli dati da** per specificare i nodi da cui raccogliere i dati.

Verificare la connessione a AutoSupport

Da Gestione sistema, è possibile inviare un messaggio di prova per verificare la connessione a AutoSupport.

Fasi

1. In System Manager, fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **Test connettività**.
3. Inserire un oggetto per il messaggio.

Attiva o disattiva AutoSupport

AutoSupport garantisce ai clienti NetApp benefici di business comprovati, tra cui l'identificazione proattiva dei possibili problemi di configurazione e una risoluzione più rapida dei casi di supporto. Nei nuovi sistemi, AutoSupport è abilitato per impostazione predefinita. Se necessario, puoi utilizzare System Manager per disabilitare AutoSupport per monitorare lo stato di salute del tuo sistema storage e inviare messaggi di notifica. È possibile attivare nuovamente AutoSupport dopo averlo disattivato.

A proposito di questa attività

Prima di disattivare AutoSupport, tenere presente che si sta disattivando il sistema call-home di NetApp e che si perdono i seguenti benefici:

- **Monitoraggio dello stato**: AutoSupport monitora lo stato del sistema di archiviazione e invia notifiche al supporto tecnico e all'organizzazione di supporto interna.
- **Automazione**: AutoSupport automatizza il reporting dei casi di supporto. La maggior parte dei casi di supporto viene aperta automaticamente prima che i clienti si rendano conto che si è verificato un problema.
- **Risoluzione più rapida**: I sistemi che inviano dati AutoSupport hanno risolto i loro casi di supporto in metà del tempo rispetto ai casi dei sistemi che non inviano dati AutoSupport.
- **Aggiornamenti più veloci**: AutoSupport supporta i flussi di lavoro self-service dei clienti, come upgrade di versioni, componenti aggiuntivi, rinnovi e automazione degli aggiornamenti firmware in Gestione sistema.
- **Altre funzioni**: Alcune funzioni di altri strumenti funzionano solo quando AutoSupport è abilitato, ad esempio alcuni flussi di lavoro in BlueXP.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **Disabilita**.
3. Se si desidera riattivare AutoSupport, nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **Abilita**.

Elimina la generazione di casi di supporto

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per inviare una richiesta a AutoSupport per eliminare la generazione di casi di supporto.

A proposito di questa attività

Per eliminare la generazione di casi di supporto, specificare i nodi e il numero di ore per cui si desidera che venga eseguita la soppressione.

La soppressione dei casi di supporto può essere particolarmente utile se non si desidera che AutoSupport crei casi automatizzati durante la manutenzione dei sistemi.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **Sospendi generazione caso di supporto**.
3. Inserire il numero di ore in cui si desidera che venga eseguita la soppressione.
4. Selezionare i nodi per i quali si desidera eseguire la soppressione.

Riprendere la generazione di casi di supporto

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per riprendere la generazione di casi di supporto da AutoSupport, se questa è stata soppressa.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **Riprendi generazione caso di supporto**.
3. Selezionare i nodi per i quali si desidera riprendere la generazione.

Modificare le impostazioni AutoSupport

È possibile utilizzare Gestione sistema per modificare le impostazioni di connessione e di posta elettronica dell'account AutoSupport.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Nella sezione **AutoSupport**, selezionare ⋮, Quindi selezionare **altre opzioni**.
3. Nella sezione **connessioni** o nella sezione **e-mail**, selezionare Edit consente di modificare le impostazioni di una delle sezioni.

Gestire AutoSupport con l'interfaccia CLI

Panoramica di Manage AutoSupport

AutoSupport è un meccanismo che monitora in modo proattivo lo stato di salute del sistema e invia automaticamente messaggi al supporto tecnico NetApp, all'organizzazione di supporto interna e a un partner di supporto. Sebbene i messaggi AutoSupport per il supporto tecnico siano attivati per impostazione predefinita, è necessario impostare le opzioni corrette e disporre di un host di posta valido per l'invio dei messaggi all'organizzazione di supporto interna.

Solo l'amministratore del cluster può eseguire la gestione di AutoSupport. L'amministratore della macchina virtuale per lo storage (SVM) non ha accesso a AutoSupport.

AutoSupport è attivato per impostazione predefinita quando si configura il sistema di storage per la prima volta. AutoSupport inizia a inviare messaggi al supporto tecnico 24 ore dopo l'attivazione di AutoSupport. È possibile ridurre il periodo di 24 ore aggiornando o ripristinando il sistema, modificando la configurazione AutoSupport o modificando l'ora del sistema in modo che non sia un periodo di 24 ore.

È possibile disattivare AutoSupport in qualsiasi momento, ma si consiglia di lasciarlo attivato. L'abilitazione di AutoSupport può contribuire a velocizzare in modo significativo la determinazione e la risoluzione dei problemi in caso di problemi nel sistema storage. Per impostazione predefinita, il sistema raccoglie le informazioni AutoSupport e le memorizza localmente, anche se si disattiva AutoSupport.

Per ulteriori informazioni su AutoSupport, visitare il sito del supporto NetApp.

Informazioni correlate

- "Supporto NetApp"

- "Scopri di più sui comandi AutoSupport nella CLI di ONTAP"

Utilizza AutoSupport e Active IQ Digital Advisor

Il componente AutoSupport di ONTAP raccoglie la telemetria e la invia per l'analisi. Il consulente digitale Active IQ analizza i dati di AutoSupport e offre un'assistenza e un'ottimizzazione proattive. Utilizzando l'intelligenza artificiale, Active IQ è in grado di identificare i potenziali problemi e di risolverli prima che influiscano sul tuo business.

Active IQ ti consente di ottimizzare la tua infrastruttura dati nel tuo cloud ibrido globale offrendo analisi predittive e supporto proattivo attraverso un portale basato sul cloud e un'app mobile. Le informazioni e i consigli di Active IQ basati sui dati sono disponibili per tutti i clienti NetApp con un contratto SupportEdge attivo (le funzionalità variano in base al prodotto e al livello di supporto).

Ecco alcune cose che puoi fare con Active IQ:

- Pianificare gli aggiornamenti. Active IQ identifica i problemi dell'ambiente che possono essere risolti eseguendo l'aggiornamento a una versione più recente di ONTAP e il componente preparazione aggiornamento consente di pianificare un aggiornamento corretto.
- Visualizza lo stato di salute del sistema. La dashboard di Active IQ segnala eventuali problemi relativi allo stato di salute e ti aiuta a correggerli. Monitorare la capacità del sistema per assicurarsi di non esaurire mai lo spazio di storage. Visualizza i casi di supporto per il tuo sistema.
- Gestire le performance. Active IQ mostra le performance del sistema in un periodo più lungo di quello che puoi vedere in Gestione sistema. Identificare i problemi di configurazione e di sistema che influiscono sulle performance.
- Massimizza l'efficienza. Visualizza le metriche di efficienza dello storage e identifica i modi per memorizzare più dati in meno spazio.
- Visualizza l'inventario e la configurazione. Active IQ visualizza l'inventario completo e le informazioni di configurazione software e hardware. Controlla quando i contratti di servizio stanno per scadere e rinnovarli per assicurarti di rimanere supportati.

Informazioni correlate

"Documentazione NetApp: Consulente digitale Active IQ"

"Avviare Active IQ"

"Servizi SupportEdge"

Quando e dove vengono inviati i messaggi AutoSupport

AutoSupport invia messaggi a destinatari diversi, a seconda del tipo di messaggio. Imparare quando e dove AutoSupport invia i messaggi può aiutarti a comprendere i messaggi ricevuti tramite e-mail o a visualizzarli sul sito Web di Active IQ (precedentemente noto come My AutoSupport).

Se non diversamente specificato, le impostazioni nelle seguenti tabelle sono parametri di `system node autosupport modify` comando.

Messaggi attivati dagli eventi

Quando si verificano eventi nel sistema che richiedono un'azione correttiva, AutoSupport invia automaticamente un messaggio attivato da un evento.

Quando il messaggio viene inviato	Dove viene inviato il messaggio
AutoSupport risponde a un evento di attivazione nell'EMS	Indirizzi specificati in `-to` e. `-noteto`. (Vengono inviati solo eventi critici che influiscono sul servizio). Indirizzi specificati in `-partner-address` Supporto tecnico, se `-support` è impostato su `enable`

Messaggi pianificati

AutoSupport invia automaticamente diversi messaggi in base a una pianificazione regolare.

Quando il messaggio viene inviato	Dove viene inviato il messaggio
Giornaliero (per impostazione predefinita, inviato tra le 12:00 e alle 1:00 come messaggio di log)	Indirizzi specificati in `-partner-address` Supporto tecnico, se `-support` è impostato su `enable`
Giornaliero (per impostazione predefinita, inviato tra le 12:00 e alle 1:00 come messaggio di performance), se `-perf` il parametro è impostato su `true`	Indirizzi specificati in -partner-address`  Supporto tecnico, se `-support` è impostato su `enable`
Settimanale (per impostazione predefinita, la domenica viene inviata tra le 12:00 e 1:00)	Indirizzi specificati in `-partner-address` Supporto tecnico, se `-support` è impostato su `enable`

Messaggi attivati manualmente

È possibile avviare o inviare di nuovo un messaggio AutoSupport manualmente.

Quando il messaggio viene inviato	Dove viene inviato il messaggio
Viene avviato manualmente un messaggio utilizzando `system node autosupport invoke` comando	Se viene specificato un URI utilizzando `-uri` nel `system node autosupport invoke` Il messaggio viene inviato all'URI. Se `-uri` viene omesso, il messaggio viene inviato agli indirizzi specificati in `-to` e. `-partner-address`. Il messaggio viene inviato anche al supporto tecnico se `-support` è impostato su `enable`.
Viene avviato manualmente un messaggio utilizzando `system node autosupport invoke-core-upload` comando	Se viene specificato un URI utilizzando `-uri` nel `system node autosupport invoke-core-upload` Il messaggio viene inviato a quell'URI e il file core dump viene caricato nell'URI. Se `-uri` viene omesso in `system node autosupport invoke-core-upload` il messaggio viene inviato al supporto tecnico e il file core dump viene caricato nel sito del supporto tecnico. Entrambi gli scenari lo richiedono `-support` è impostato su `enable` e. `-transport` è impostato su `https` oppure `http`. A causa delle grandi dimensioni dei file core dump, il messaggio non viene inviato agli indirizzi specificati in `-to` e. `-partner-addresses` parametri.
Viene avviato manualmente un messaggio utilizzando `system node autosupport invoke-performance-archive` comando	Se viene specificato un URI utilizzando `-uri` nel `system node autosupport invoke-performance-archive` Il messaggio viene inviato a quell'URI e il file di archivio delle prestazioni viene caricato nell'URI. Se `-uri` viene omesso in `system node autosupport invoke-performance-archive`, il messaggio viene inviato al supporto tecnico e il file di archivio delle performance viene caricato sul sito del supporto tecnico. Entrambi gli scenari lo richiedono `-support` è impostato su `enable` e. `-transport` è impostato su `https` oppure `http`. A causa delle grandi dimensioni dei file di archiviazione delle prestazioni, il messaggio non viene inviato agli indirizzi specificati in `-to` e. `-partner-addresses` parametri.

Quando il messaggio viene inviato	Dove viene inviato il messaggio
È possibile inviare di nuovo manualmente un messaggio precedente utilizzando `system node autosupport history retransmit` comando	Solo all'URI specificato in `-uri` del parametro `system node autosupport history retransmit` comando

Messaggi attivati dal supporto tecnico

Il supporto tecnico può richiedere messaggi a AutoSupport utilizzando la funzione AutoSupport su richiesta.

Quando il messaggio viene inviato	Dove viene inviato il messaggio
Quando AutoSupport ottiene le istruzioni di consegna per generare nuovi messaggi AutoSupport	Indirizzi specificati in `-partner-address` Supporto tecnico, se `-support` è impostato su `enable` e. `-transport` è impostato su `https`
Quando AutoSupport ottiene le istruzioni di consegna per inviare nuovamente i messaggi AutoSupport precedenti	Supporto tecnico, se `-support` è impostato su `enable` e. `-transport` è impostato su `https`
Quando AutoSupport ottiene le istruzioni di consegna per generare nuovi messaggi AutoSupport che caricano i file core dump o di archivio delle performance	Supporto tecnico, se `-support` è impostato su `enable` e. `-transport` è impostato su `https`. Il core dump o il file di archivio delle performance viene caricato sul sito del supporto tecnico.

Modalità di creazione e invio dei messaggi attivati dagli eventi da parte di AutoSupport

AutoSupport crea messaggi AutoSupport attivati da eventi quando il servizio di emergenza elabora un evento di attivazione. Un messaggio AutoSupport attivato dall'evento avvisa i destinatari dei problemi che richiedono un'azione correttiva e contiene solo informazioni rilevanti per il problema. È possibile personalizzare i contenuti da includere e chi riceve i messaggi.

AutoSupport utilizza il seguente processo per creare e inviare messaggi AutoSupport attivati dagli eventi:

1. Quando EMS elabora un evento di attivazione, EMS invia una richiesta a AutoSupport.

   Un evento trigger è un evento EMS con una destinazione AutoSupport e un nome che inizia con a. `callhome.` prefisso.

2. AutoSupport crea un messaggio AutoSupport attivato dall'evento.

   AutoSupport raccoglie le informazioni di base e di troubleshooting dai sottosistemi associati al trigger per creare un messaggio che includa solo le informazioni pertinenti all'evento di trigger.

   A ciascun trigger viene associato un set predefinito di sottosistemi. Tuttavia, è possibile scegliere di associare altri sottosistemi a un trigger utilizzando `system node autosupport trigger modify` comando.

3. AutoSupport invia il messaggio AutoSupport attivato dagli eventi ai destinatari definiti da `system node autosupport modify` con il `-to`, `-noteto`, `-partner-address`, e. `-support` parametri.

   È possibile attivare e disattivare l'invio dei messaggi AutoSupport per trigger specifici utilizzando `system node autosupport trigger modify` con il `-to` e. `-noteto` parametri.

Esempio di dati inviati per un evento specifico

Il `storage shelf PSU failed` Evento EMS attiva un messaggio che contiene dati di base da obbligatorio, file di log, storage, RAID, ha, Piattaforma e sistemi secondari di rete e dati di troubleshooting dai sottosistemi obbligatori, file di log e storage.

Decidi di includere i dati relativi a NFS in qualsiasi messaggio AutoSupport inviato in risposta a un futuro `storage shelf PSU failed` evento. Immettere il seguente comando per attivare i dati a livello di risoluzione dei problemi per NFS per `callhome.shlf.ps.fault` evento:

```
        cluster1::\>
        system node autosupport trigger modify -node node1 -autosupport
-message shlf.ps.fault -troubleshooting-additional nfs
```

Tenere presente che il `callhome.` il prefisso viene eliminato da `callhome.shlf.ps.fault` quando si utilizza `system node autosupport trigger` O quando viene fatto riferimento da eventi AutoSupport e EMS nella CLI.

Tipi di messaggi AutoSupport e relativi contenuti

I messaggi AutoSupport contengono informazioni sullo stato dei sottosistemi supportati. L'apprendimento dei messaggi AutoSupport consente di interpretare o rispondere ai messaggi ricevuti tramite e-mail o di visualizzarli sul sito Web di Active IQ (in precedenza denominato My AutoSupport).

Tipo di messaggio	Tipo di dati contenuti nel messaggio
Attivato da eventi	File contenenti dati sensibili al contesto relativi al sottosistema specifico in cui si è verificato l'evento
Ogni giorno	File di log
Performance	Dati sulle performance campionati durante le 24 ore precedenti
Settimanale	Dati di configurazione e stato

Tipo di messaggio	Tipo di dati contenuti nel messaggio
Attivato da `system node autosupport invoke` comando	Dipende dal valore specificato in `-type` parametro: • `test` invia un messaggio attivato dall'utente con alcuni dati di base. Questo messaggio attiva anche una risposta email automatica dal supporto tecnico a qualsiasi indirizzo email specificato, utilizzando `-to` Per confermare la ricezione dei messaggi AutoSupport. • `performance` invia i dati delle performance. • `all` invia un messaggio attivato dall'utente con una serie completa di dati simili al messaggio settimanale, inclusi i dati di risoluzione dei problemi di ciascun sottosistema. Il supporto tecnico in genere richiede questo messaggio.
Attivato da `system node autosupport invoke-core-upload` comando	File core dump per un nodo
Attivato da `system node autosupport invoke-performance-archive` comando	File di archiviazione delle performance per un periodo di tempo specificato
Attivato da AutoSupport OnDemand	AutoSupport OnDemand può richiedere nuovi messaggi o messaggi precedenti: • I nuovi messaggi, a seconda del tipo di raccolta AutoSupport, possono essere `test`, `all`, o. `performance`. • I messaggi passati dipendono dal tipo di messaggio che viene inviato nuovamente. AutoSupport OnDemand può richiedere nuovi messaggi che caricano i seguenti file sul sito del supporto NetApp all'indirizzo "mysupport.netapp.com": • Core dump • Archivio delle performance

Che cosa sono i sottosistemi AutoSupport

Ogni sottosistema fornisce informazioni di base e di risoluzione dei problemi che AutoSupport utilizza per i propri messaggi. Ogni sottosistema è inoltre associato a eventi

di trigger che consentono a AutoSupport di raccogliere solo informazioni relative all'evento di trigger dai sottosistemi.

AutoSupport raccoglie contenuti sensibili al contesto. È possibile visualizzare informazioni sui sottosistemi e sugli eventi di attivazione utilizzando `system node autosupport trigger show` comando.

Dimensioni AutoSupport e budget temporali

AutoSupport raccoglie le informazioni, organizzate in base al sottosistema, e applica un budget di tempo e dimensioni sui contenuti per ciascun sottosistema. Con la crescita dei sistemi storage, i budget AutoSupport forniscono il controllo sul payload AutoSupport, che a sua volta fornisce un'erogazione scalabile dei dati AutoSupport.

AutoSupport interrompe la raccolta di informazioni e tronca il contenuto AutoSupport se il contenuto del sottosistema supera le dimensioni o il budget di tempo. Se il contenuto non può essere troncato facilmente (ad esempio, file binari), AutoSupport omette il contenuto.

È necessario modificare le dimensioni predefinite e i budget temporali solo se richiesto dal supporto NetApp. È inoltre possibile rivedere le dimensioni predefinite e i budget temporali dei sottosistemi utilizzando `autosupport manifest show` comando.

File inviati in messaggi AutoSupport attivati dagli eventi

I messaggi AutoSupport attivati dagli eventi contengono solo informazioni di base e di risoluzione dei problemi provenienti dai sottosistemi associati all'evento che ha causato la generazione del messaggio da parte di AutoSupport. I dati specifici aiutano i partner di supporto e supporto NetApp a risolvere il problema.

AutoSupport utilizza i seguenti criteri per controllare il contenuto dei messaggi AutoSupport attivati dagli eventi:

- Quali sottosistemi sono inclusi

  I dati sono raggruppati in sottosistemi, inclusi sottosistemi comuni, come file di registro, e sottosistemi specifici, come RAID. Ogni evento attiva un messaggio che contiene solo i dati di specifici sottosistemi.

- Il livello di dettaglio di ciascun sottosistema incluso

  I dati per ciascun sottosistema incluso vengono forniti a livello di base o di troubleshooting.

È possibile visualizzare tutti gli eventi possibili e determinare quali sottosistemi sono inclusi nei messaggi relativi a ciascun evento utilizzando `system node autosupport trigger show` con il `-instance` parametro.

Oltre ai sottosistemi inclusi per impostazione predefinita per ciascun evento, è possibile aggiungere altri sottosistemi a livello di base o di risoluzione dei problemi utilizzando `system node autosupport trigger modify` comando.

File di log inviati in messaggi AutoSupport

I messaggi AutoSupport possono contenere diversi file di log delle chiavi che consentono al personale del supporto tecnico di esaminare le recenti attività del sistema.

Tutti i tipi di messaggi AutoSupport possono includere i seguenti file di registro quando il sottosistema file di registro è attivato:

File di log	Quantità di dati inclusi nel file
• File di registro da `/mroot/etc/log/mlog/` directory • Il file di log DEI MESSAGGI	Solo le nuove righe aggiunte ai registri dall'ultimo messaggio AutoSupport fino a un massimo specificato. Ciò garantisce che i messaggi AutoSupport abbiano dati univoci, rilevanti, non sovrapposti. (I file di log dei partner rappresentano un'eccezione; per i partner sono inclusi i dati massimi consentiti).
• File di registro da `/mroot/etc/log/shelflog/` directory • File di registro da `/mroot/etc/log/acp/` directory • Dati di log del sistema di gestione degli eventi (EMS)	Le righe di dati più recenti fino a un massimo specificato.

Il contenuto dei messaggi AutoSupport può cambiare tra una versione e l'altra di ONTAP.

File inviati in messaggi AutoSupport settimanali

I messaggi AutoSupport settimanali contengono dati di configurazione e stato aggiuntivi utili per tenere traccia delle modifiche nel sistema nel tempo.

Le seguenti informazioni vengono inviate in messaggi AutoSupport settimanali:

- Informazioni di base su ogni sottosistema
- Contenuto di selezionato `/mroot/etc` file di directory
- File di log
- Output di comandi che forniscono informazioni di sistema
- Informazioni aggiuntive, tra cui le informazioni del database replicato (RDB), le statistiche di servizio e molto altro ancora

In che modo AutoSupport OnDemand ottiene le istruzioni di consegna dal supporto tecnico

AutoSupport OnDemand comunica periodicamente con il supporto tecnico per ottenere istruzioni di consegna per l'invio, il reinvio e il rifiuto di messaggi AutoSupport, nonché per il caricamento di file di grandi dimensioni sul sito di supporto NetApp. AutoSupport OnDemand consente l'invio on-demand dei messaggi AutoSupport invece di attendere l'esecuzione del processo AutoSupport settimanale.

AutoSupport OnDemand è costituito dai seguenti componenti:

- Client AutoSupport OnDemand eseguito su ciascun nodo

- Servizio AutoSupport OnDemand che risiede nel supporto tecnico

Il client AutoSupport OnDemand esegue periodicamente il polling del servizio AutoSupport OnDemand per ottenere le istruzioni di consegna dal supporto tecnico. Ad esempio, il supporto tecnico può utilizzare il servizio AutoSupport OnDemand per richiedere la generazione di un nuovo messaggio AutoSupport. Quando il client AutoSupport OnDemand esegue il polling del servizio AutoSupport OnDemand, il client ottiene le istruzioni di consegna e invia il nuovo messaggio AutoSupport on-demand come richiesto.

AutoSupport OnDemand è attivato per impostazione predefinita. Tuttavia, AutoSupport OnDemand si affida ad alcune impostazioni AutoSupport per continuare a comunicare con il supporto tecnico. AutoSupport OnDemand comunica automaticamente con il supporto tecnico quando vengono soddisfatti i seguenti requisiti:

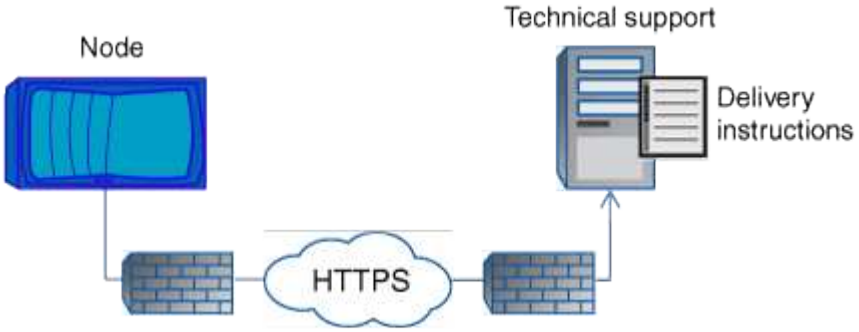
- AutoSupport è attivato.
- AutoSupport è configurato per inviare messaggi al supporto tecnico.
- AutoSupport è configurato per utilizzare il protocollo di trasporto HTTPS.

Il client AutoSupport OnDemand invia le richieste HTTPS alla stessa posizione del supporto tecnico a cui vengono inviati i messaggi AutoSupport. Il client AutoSupport OnDemand non accetta connessioni in entrata.

AutoSupport OnDemand utilizza l'account utente "AutoSupport" per comunicare con il supporto tecnico. ONTAP impedisce di eliminare questo account.

Se si desidera disattivare AutoSupport OnDemand, ma mantenere AutoSupport attivato, utilizzare il comando: Link:https://docs.netapp.com/us-en/ontap-cli-9121/system-node-autosupport-modify.html#parameters[`system node autosupport modify -ondemand-state disable`].

La figura seguente mostra come AutoSupport OnDemand invia le richieste HTTPS al supporto tecnico per ottenere le istruzioni di consegna.



Le istruzioni di consegna possono includere richieste di AutoSupport per effettuare le seguenti operazioni:

- Generare nuovi messaggi AutoSupport.

  Il supporto tecnico potrebbe richiedere nuovi messaggi AutoSupport per risolvere i problemi.

- Generare nuovi messaggi AutoSupport che caricano i file di dump core o i file di archivio delle performance sul sito di supporto NetApp.

  Il supporto tecnico potrebbe richiedere il core dump o i file di archivio delle performance per risolvere i problemi di triage.

- Ritrasmettere i messaggi AutoSupport generati in precedenza.

Questa richiesta si verifica automaticamente se non è stato ricevuto un messaggio a causa di un errore di consegna.

- Disattiva l'invio dei messaggi AutoSupport per eventi trigger specifici.

  Il supporto tecnico potrebbe disattivare la consegna dei dati non utilizzati.

Struttura dei messaggi AutoSupport inviati via email

Quando un messaggio AutoSupport viene inviato via email, il messaggio ha un oggetto standard, un corpo breve e un grande allegato in formato file 7z che contiene i dati.

Se AutoSupport è configurato per nascondere i dati privati, alcune informazioni, come il nome host, vengono omesse o mascherate nell'intestazione, nell'oggetto, nel corpo e negli allegati.

Soggetto

La riga dell'oggetto dei messaggi inviati dal meccanismo AutoSupport contiene una stringa di testo che identifica il motivo della notifica. Il formato dell'oggetto è il seguente:

Notifica gruppo HA da *Nome_sistema* (*messaggio*) *severità*

- *Nome_sistema* è il nome host o l'ID di sistema, a seconda della configurazione di AutoSupport

Corpo

Il corpo del messaggio AutoSupport contiene le seguenti informazioni:

- Data e ora del messaggio
- Versione di ONTAP sul nodo che ha generato il messaggio
- ID di sistema, numero di serie e nome host del nodo che ha generato il messaggio
- Numero di sequenza AutoSupport
- Nome e posizione del contatto SNMP, se specificati
- ID di sistema e nome host del partnernode ha

File allegati

Le informazioni chiave in un messaggio AutoSupport sono contenute in file compressi in un file 7z chiamato `body.7z` e allegato al messaggio.

I file contenuti nell'allegato sono specifici del tipo di messaggio AutoSupport.

Tipi di severità AutoSupport

I messaggi AutoSupport hanno tipi di severità che aiutano a comprendere lo scopo di ciascun messaggio, ad esempio per attirare l'attenzione immediata su un problema di emergenza o solo per fornire informazioni.

I messaggi hanno una delle seguenti severità:

- **Alert**: I messaggi di avviso indicano che potrebbe verificarsi un evento di livello superiore se non si esegue alcuna azione.

  È necessario intraprendere un'azione contro i messaggi di avviso entro 24 ore.

- **Emergenza**: I messaggi di emergenza vengono visualizzati quando si verifica un'interruzione.

  È necessario intraprendere immediatamente un'azione contro i messaggi di emergenza.

- **Error**: Le condizioni di errore indicano cosa potrebbe accadere se si ignora.
- **Avviso**: Condizione normale ma significativa.
- **Info**: Il messaggio informativo fornisce dettagli sul problema, che è possibile ignorare.
- **Debug**: I messaggi a livello di debug forniscono le istruzioni da eseguire.

Se l'organizzazione di supporto interna riceve messaggi AutoSupport tramite e-mail, la severità viene visualizzata nella riga dell'oggetto del messaggio.

Requisiti per l'utilizzo di AutoSupport

È necessario utilizzare HTTPS con TLSv1.2 o SMTP sicuro per l'invio dei messaggi AutoSupport per garantire la massima sicurezza e per supportare tutte le funzionalità AutoSupport più recenti. I messaggi AutoSupport inviati con qualsiasi altro protocollo verranno rifiutati.

Protocolli supportati

Tutti questi protocolli vengono eseguiti su IPv4 o IPv6, in base alla famiglia di indirizzi a cui il nome viene risolto.

Protocollo e porta	Descrizione
HTTPS sulla porta 443	Questo è il protocollo predefinito. Se possibile, utilizzare questa opzione. Questo protocollo supporta AutoSupport OnDemand e upload di file di grandi dimensioni. Il certificato proveniente dal server remoto viene convalidato in base al certificato root, a meno che non venga disattivata la convalida. Il recapito utilizza una richiesta HTTPS PUT. Con PUT, se la richiesta non riesce durante la trasmissione, la richiesta viene riavviata da dove è stata interrotta. Se il server che riceve la richiesta non supporta PUT, il recapito utilizza una richiesta HTTPS POST.

Protocollo e porta	Descrizione
HTTP sulla porta 80	Questo protocollo è preferito rispetto a SMTP. Questo protocollo supporta il caricamento di file di grandi dimensioni, ma non AutoSupport OnDemand. Il recapito utilizza una richiesta HTTPS PUT. Con PUT, se la richiesta non riesce durante la trasmissione, la richiesta viene riavviata da dove è stata interrotta. Se il server che riceve la richiesta non supporta PUT, il recapito utilizza una richiesta HTTPS POST.
SMTP sulla porta 25 o su un'altra porta	Utilizzare questo protocollo solo se la connessione di rete non consente HTTPS. Il valore predefinito della porta è 25, ma è possibile configurare AutoSupport in modo che utilizzi una porta diversa. Tenere presenti le seguenti limitazioni quando si utilizza SMTP: • AutoSupport OnDemand e upload di file di grandi dimensioni non sono supportati. • I dati non sono crittografati. SMTP invia i dati in testo chiaro, rendendo il testo nel messaggio AutoSupport facile da intercettare e leggere. • È possibile introdurre limitazioni sulla lunghezza del messaggio e della linea.

Se si configura AutoSupport con indirizzi e-mail specifici per l'organizzazione di supporto interna o per un'organizzazione di partner di supporto, tali messaggi vengono sempre inviati tramite SMTP.

Ad esempio, se si utilizza il protocollo consigliato per inviare messaggi al supporto tecnico e si desidera anche inviare messaggi all'organizzazione di supporto interna, i messaggi verranno trasportati utilizzando sia HTTPS che SMTP, rispettivamente.

AutoSupport limita le dimensioni massime dei file per ciascun protocollo. L'impostazione predefinita per i trasferimenti HTTP e HTTPS è 25 MB. L'impostazione predefinita per i trasferimenti SMTP è 5 MB. Se le dimensioni del messaggio AutoSupport superano il limite configurato, AutoSupport recapita la maggior parte del messaggio possibile. È possibile modificare le dimensioni massime modificando la configurazione di AutoSupport. Vedere `system node autosupport modify` pagina man per ulteriori informazioni.

AutoSupport sovrascrive automaticamente il limite massimo delle dimensioni dei file per i protocolli HTTPS e HTTP quando si generano e inviano messaggi AutoSupport che caricano i file core dump o di archivio delle performance al sito di supporto NetApp o a un URI specificato. L'override automatica si applica solo quando si caricano i file utilizzando `system node autosupport invoke-core-upload` o il `system node autosupport invoke-performance-archive` comandi.

Requisiti di configurazione

A seconda della configurazione di rete, il protocollo HTTPS potrebbe richiedere un'ulteriore configurazione di un URL proxy. Se HTTPS invia messaggi AutoSupport al supporto tecnico e si dispone di un proxy, è necessario identificare l'URL per tale proxy. Se il proxy utilizza una porta diversa da quella predefinita, ovvero 3128, è possibile specificare la porta per tale proxy. È inoltre possibile specificare un nome utente e una password per l'autenticazione del proxy.

Se si utilizza SMTP per inviare messaggi AutoSupport all'organizzazione di supporto interna o al supporto tecnico, è necessario configurare un server di posta esterno. Il sistema di storage non funziona come server di posta, ma richiede un server di posta esterno per l'invio della posta. Il server di posta deve essere un host in attesa sulla porta SMTP (25) o su un'altra porta e deve essere configurato per inviare e ricevere la codifica MIME (Multipurpose Internet Mail Extensions) a 8 bit. Gli host di posta di esempio includono un host UNIX che esegue un server SMTP come il programma sendmail e un server Windows che esegue il server Microsoft Exchange. È possibile disporre di uno o più host di posta.

Configurare AutoSupport

È possibile controllare se e come le informazioni AutoSupport vengono inviate al supporto tecnico e all'organizzazione di supporto interna, quindi verificare che la configurazione sia corretta.

A proposito di questa attività

In ONTAP 9.5 e versioni successive, è possibile attivare AutoSupport e modificarne la configurazione su tutti i nodi del cluster contemporaneamente. Quando un nuovo nodo si unisce al cluster, il nodo eredita automaticamente la configurazione del cluster AutoSupport. Non è necessario aggiornare la configurazione su ciascun nodo separatamente.

A partire da ONTAP 9.5, lo scopo di `system node autosupport modify` il comando è esteso a tutto il cluster. La configurazione AutoSupport viene modificata su tutti i nodi del cluster, anche quando `-node` opzione specificata. L'opzione viene ignorata, ma è stata mantenuta per la compatibilità con le versioni precedenti di CLI.

In ONTAP 9.4 e versioni precedenti, lo scopo di `system node autosupport modify` il comando è specifico del nodo. La configurazione AutoSupport deve essere modificata su ciascun nodo del cluster.

Per impostazione predefinita, AutoSupport è attivato su ciascun nodo per inviare messaggi al supporto tecnico utilizzando il protocollo di trasporto HTTPS.

È necessario utilizzare HTTPS con TLSv1.2 o SMTP sicuro per l'invio dei messaggi AutoSupport per garantire la massima sicurezza e per supportare tutte le funzionalità AutoSupport più recenti.

Fasi

1. Assicurarsi che AutoSupport sia attivato:

```
system node autosupport modify -state enable
```

2. Se si desidera che il supporto tecnico riceva messaggi AutoSupport, utilizzare il seguente comando:

```
system node autosupport modify -support enable
```

È necessario attivare questa opzione se si desidera attivare AutoSupport per lavorare con AutoSupport OnDemand o se si desidera caricare file di grandi dimensioni, come i file di archiviazione delle performance e dei core dump, sul supporto tecnico o su un URL specificato.

3. Se il supporto tecnico è abilitato a ricevere messaggi AutoSupport, specificare il protocollo di trasporto da utilizzare per i messaggi.

È possibile scegliere tra le seguenti opzioni:

Se si desidera…	Quindi, impostare i seguenti parametri di `system node autosupport modify` comando…
Utilizzare il protocollo HTTPS predefinito	a. Impostare `-transport` a. `https`. b. Se si utilizza un proxy, impostare `-proxy-url` All'URL del proxy. Questa configurazione supporta la comunicazione con AutoSupport OnDemand e il caricamento di file di grandi dimensioni.
USA SMTP	Impostare `-transport` a. `smtp`. Questa configurazione non supporta AutoSupport OnDemand o upload di file di grandi dimensioni.

4. Se si desidera che l'organizzazione di supporto interna o un partner di supporto riceva messaggi AutoSupport, eseguire le seguenti operazioni:
   a. Identificare i destinatari dell'organizzazione impostando i seguenti parametri di `system node autosupport modify` comando:

Imposta questo parametro…	A questo…
`-to`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno messaggi AutoSupport chiave

`-noteto`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione di supporto interna che riceveranno una versione abbreviata dei messaggi AutoSupport chiave progettati per telefoni cellulari e altri dispositivi mobili
`-partner-address`	Fino a cinque indirizzi e-mail o liste di distribuzione separati da virgole nell'organizzazione del partner di supporto che riceveranno tutti i messaggi AutoSupport

b. Verificare che gli indirizzi siano configurati correttamente elencando le destinazioni utilizzando `system node autosupport destinations show` comando.

5. Se si inviano messaggi all'organizzazione di supporto interna o si sceglie il trasporto SMTP per i messaggi all'assistenza tecnica, configurare SMTP impostando i seguenti parametri di `system node autosupport modify` comando:

   ◦ Impostare `-mail-hosts` a uno o più mail host, separati da virgole.

   È possibile impostare un massimo di cinque.

   È possibile configurare un valore di porta per ciascun host di posta specificando i due punti e il numero di porta dopo il nome host della posta: Ad esempio, `mymailhost.example.com:5678`, dove 5678 è la porta per l'host di posta.

   ◦ Impostare `-from` All'indirizzo e-mail che invia il messaggio AutoSupport.

6. Configurare il DNS.
7. Se si desidera modificare impostazioni specifiche, aggiungere opzioni di comando:

Se si desidera eseguire questa operazione…	Quindi, impostare i seguenti parametri di `system node autosupport modify` comando…
Nascondere i dati privati rimuovendo, mascherando o codificando i dati sensibili nei messaggi	Impostare `-remove-private-data` a. `true`. Se si cambia da `false` a. `true`, Vengono cancellati tutti i file della cronologia AutoSupport e tutti i file associati.
Interrompere l'invio dei dati relativi alle prestazioni nei messaggi AutoSupport periodici	Impostare `-perf` a. `false`.

8. Controllare la configurazione generale utilizzando `system node autosupport show` con il `-node` parametro.
9. Verificare il funzionamento di AutoSupport utilizzando `system node autosupport check show` comando.

   Se vengono segnalati problemi, utilizzare `system node autosupport check show-details` per visualizzare ulteriori informazioni.

10. Verifica dell'invio e della ricezione dei messaggi AutoSupport:

    a. Utilizzare `system node autosupport invoke` con il `-type` parametro impostato su `test`.

    ```
    cluster1::> system node autosupport invoke -type test -node node1
    ```

    b. Conferma che NetApp sta ricevendo i tuoi messaggi AutoSupport:

    la cronologia AutoSupport del nodo di sistema mostra -node local

Lo stato dell'ultimo messaggio AutoSupport in uscita dovrebbe cambiare in `sent-successful` per tutte le destinazioni del protocollo appropriate.

a. Se lo si desidera, verificare che il messaggio AutoSupport venga inviato all'organizzazione di supporto interna o al partner di supporto controllando l'indirizzo e-mail di qualsiasi indirizzo configurato per `-to`, `-noteto`, o. `-partner-address` parametri di `system node autosupport modify` comando.

Caricare i file core dump

Quando viene salvato un file core dump, viene generato un messaggio di evento. Se il servizio AutoSupport è abilitato e configurato per l'invio di messaggi al supporto NetApp, viene trasmesso un messaggio AutoSupport e viene inviato un messaggio e-mail di conferma automatico.

Di cosa hai bisogno

- È necessario configurare AutoSupport con le seguenti impostazioni:
  - AutoSupport è attivato sul nodo.
  - AutoSupport è configurato per inviare messaggi al supporto tecnico.
  - AutoSupport è configurato per utilizzare il protocollo di trasporto HTTP o HTTPS.

    Il protocollo di trasporto SMTP non è supportato quando si inviano messaggi che includono file di grandi dimensioni, come i file core dump.

A proposito di questa attività

È inoltre possibile caricare il file core dump tramite il servizio AutoSupport su HTTPS utilizzando `system node autosupport invoke-core-upload` Comando, se richiesto dal supporto NetApp.

"Come caricare un file su NetApp"

Fasi

1. Visualizzare i file di dump principali per un nodo utilizzando `system node coredump show` comando.

   Nell'esempio seguente, i file core dump vengono visualizzati per il nodo locale:

```
cluster1::> system node coredump show -node local
Node:Type Core Name Saved Panic Time
--------- ------------------------------------------ -----
-----------------
node:kernel
core.4073000068.2013-09-11.15_05_01.nz true 9/11/2013 15:05:01
```

2. Generare un messaggio AutoSupport e caricare un file core dump utilizzando `system node autosupport invoke-core-upload` comando.

   Nell'esempio seguente, viene generato un messaggio AutoSupport e inviato alla posizione predefinita, ovvero il supporto tecnico, e il file core dump viene caricato nella posizione predefinita, ovvero il sito di supporto NetApp:

   ```
   cluster1::> system node autosupport invoke-core-upload -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

   Nell'esempio seguente, viene generato e inviato un messaggio AutoSupport nella posizione specificata nell'URI e il file dump core viene caricato nell'URI:

   ```
   cluster1::> system node autosupport invoke-core-upload -uri
   https//files.company.com -core-filename
   core.4073000068.2013-09-11.15_05_01.nz -node local
   ```

Caricare i file di archivio delle performance

È possibile generare e inviare un messaggio AutoSupport contenente un archivio delle performance. Per impostazione predefinita, il supporto tecnico di NetApp riceve il messaggio AutoSupport e l'archivio delle performance viene caricato sul sito di supporto NetApp. È possibile specificare una destinazione alternativa per il messaggio e il caricamento.

Di cosa hai bisogno

- È necessario configurare AutoSupport con le seguenti impostazioni:
  - AutoSupport è attivato sul nodo.
  - AutoSupport è configurato per inviare messaggi al supporto tecnico.
  - AutoSupport è configurato per utilizzare il protocollo di trasporto HTTP o HTTPS.

    Il protocollo di trasporto SMTP non è supportato quando si inviano messaggi che includono file di grandi dimensioni, ad esempio file di archiviazione delle prestazioni.

A proposito di questa attività

È necessario specificare una data di inizio per i dati dell'archivio delle performance che si desidera caricare. La maggior parte dei sistemi storage conserva gli archivi delle performance per due settimane, consentendoti di

specificare una data di inizio fino a due settimane fa. Ad esempio, se oggi è il 15 gennaio, è possibile specificare una data di inizio del 2 gennaio.

Fase

1. Generare un messaggio AutoSupport e caricare il file di archivio delle performance utilizzando `system node autosupport invoke-performance-archive` comando.

   Nell'esempio seguente, 4 ore di file di archivio delle performance dal 12 gennaio 2015 vengono aggiunti a un messaggio AutoSupport e caricati nella posizione predefinita, che è il sito di supporto NetApp:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h
   ```

   Nell'esempio seguente, 4 ore di file di archivio delle performance dal 12 gennaio 2015 vengono aggiunti a un messaggio AutoSupport e caricati nella posizione specificata dall'URI:

   ```
   cluster1::> system node autosupport invoke-performance-archive -node
   local -start-date 1/12/2015 13:42:09 -duration 4h -uri
   https://files.company.com
   ```

Ottenere le descrizioni dei messaggi AutoSupport

Le descrizioni dei messaggi AutoSupport ricevuti sono disponibili tramite il convertitore Syslog di ONTAP.

Fasi

1. Accedere alla "Syslog Translator".
2. Nel campo **Release**, immettere la versione di ONTAP in uso. Nel campo **stringa di ricerca**, immettere "callhome". Selezionare **Translate** (Traduci).
3. Syslog Translator elenca in ordine alfabetico tutti gli eventi che corrispondono alla stringa di messaggi immessa.

Comandi per la gestione di AutoSupport

Si utilizza `system node autosupport` Comandi per modificare o visualizzare la configurazione AutoSupport, visualizzare le informazioni sui messaggi AutoSupport precedenti e inviare, reinviare o annullare un messaggio AutoSupport.

Configurare AutoSupport

Se si desidera…	Utilizzare questo comando…
Controlla se vengono inviati messaggi AutoSupport	`system node autosupport modify` con `-state` parametro

Se si desidera…	Utilizzare questo comando…
Controlla se i messaggi AutoSupport vengono inviati al supporto tecnico	`system node autosupport modify` con `-support` parametro
Impostare AutoSupport o modificare la configurazione di AutoSupport	`system node autosupport modify`
Abilitare e disabilitare i messaggi AutoSupport per i singoli eventi di attivazione e specificare report aggiuntivi del sottosistema da includere nei messaggi inviati in risposta ai singoli eventi di attivazione	`system node autosupport trigger modify`

Visualizza le informazioni sulla configurazione AutoSupport

Se si desidera…	Utilizzare questo comando…
Visualizzare la configurazione AutoSupport	`system node autosupport show` con `-node` parametro
Visualizza un riepilogo di tutti gli indirizzi e gli URL che ricevono messaggi AutoSupport	`system node autosupport destinations show`
Visualizza i messaggi AutoSupport inviati all'organizzazione di supporto interna per singoli eventi di attivazione	`system node autosupport trigger show`
Visualizza lo stato della configurazione AutoSupport e l'invio a varie destinazioni	`system node autosupport check show`
Visualizza lo stato dettagliato della configurazione AutoSupport e la consegna a varie destinazioni	`system node autosupport check show-details`

Visualizza le informazioni sui messaggi AutoSupport precedenti

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni su uno o più dei 50 messaggi AutoSupport più recenti	`system node autosupport history show`
Visualizza le informazioni sui messaggi AutoSupport recenti generati per caricare i file core dump o di archivio delle performance sul sito di supporto tecnico o su un URI specificato	`system node autosupport history show-upload-details`

Se si desidera…	Utilizzare questo comando…
Consente di visualizzare le informazioni contenute nei messaggi AutoSupport, inclusi il nome e le dimensioni di ciascun file raccolto per il messaggio e gli eventuali errori	`system node autosupport manifest show`

Inviare, inviare nuovamente o annullare i messaggi AutoSupport

Se si desidera…	Utilizzare questo comando…
Ritrasmettere un messaggio AutoSupport memorizzato localmente, identificato dal numero di sequenza AutoSupport Se si ritrasmette un messaggio AutoSupport e se il supporto ha già ricevuto tale messaggio, il sistema di supporto non crea un caso duplicato. Se, d'altra parte, il supporto non ha ricevuto quel messaggio, il sistema AutoSupport analizzerà il messaggio e, se necessario, creerà un caso.	`system node autosupport history retransmit`
Generare e inviare un messaggio AutoSupport, ad esempio a scopo di test	`system node autosupport invoke` Utilizzare `-force` Parametro per inviare un messaggio anche se AutoSupport è disattivato. Utilizzare `-uri` parametro per inviare il messaggio alla destinazione specificata al posto della destinazione configurata.
Consente di annullare un messaggio AutoSupport	`system node autosupport history cancel`

Informazioni correlate

"Comandi di ONTAP 9"

Informazioni incluse nel manifesto di AutoSupport

Il manifesto AutoSupport fornisce una vista dettagliata dei file raccolti per ciascun messaggio AutoSupport. Il manifesto di AutoSupport include anche informazioni sugli errori di raccolta quando AutoSupport non è in grado di raccogliere i file di cui ha bisogno.

Il manifesto di AutoSupport include le seguenti informazioni:

- Numero di sequenza del messaggio AutoSupport
- Quali file AutoSupport sono inclusi nel messaggio AutoSupport

- Dimensione di ogni file, in byte
- Stato dell'insieme di manifest AutoSupport
- Descrizione dell'errore, se AutoSupport non riesce a raccogliere uno o più file

È possibile visualizzare il manifesto AutoSupport utilizzando `system node autosupport manifest show` comando.

Il manifesto AutoSupport è incluso in ogni messaggio AutoSupport e presentato in formato XML, il che significa che è possibile utilizzare un visualizzatore XML generico per leggerlo o visualizzarlo utilizzando il portale Active IQ (precedentemente noto come My AutoSupport).

Soppressione del caso AutoSupport durante le finestre di manutenzione programmata

La soppressione dei casi AutoSupport consente di impedire la creazione di casi non necessari da parte dei messaggi AutoSupport attivati durante le finestre di manutenzione pianificate.

Per eliminare i casi AutoSupport, è necessario richiamare manualmente un messaggio AutoSupport con una stringa di testo appositamente formattata: `MAINT=xh`. `x` indica la durata della finestra di manutenzione in unità di ore.

Informazioni correlate

"Come eliminare la creazione automatica del caso durante le finestre di manutenzione pianificata"

Risolvere i problemi relativi a AutoSupport quando i messaggi non vengono ricevuti

Se il sistema non invia il messaggio AutoSupport, è possibile determinare se il messaggio non viene generato da AutoSupport o non è possibile recapitare il messaggio.

Fasi

1. Controllare lo stato di consegna dei messaggi utilizzando `system node autosupport history show` comando.
2. Leggere lo stato.

Questo stato	Significa
inizializzazione in corso	Il processo di raccolta è in corso. Se questo stato è temporaneo, va bene. Tuttavia, se lo stato persiste, si è verificato un problema.
raccolta non riuscita	AutoSupport non è in grado di creare il contenuto AutoSupport nella directory di spool. È possibile visualizzare i dati che AutoSupport sta tentando di raccogliere immettendo il `system node autosupport history show -detail` comando.
raccolta in corso	AutoSupport sta raccogliendo contenuti AutoSupport. È possibile visualizzare i dati raccolti da AutoSupport immettendo il `system node autosupport manifest show` comando.

Questo stato	Significa
in coda	I messaggi AutoSupport vengono messi in coda per la consegna, ma non ancora recapitati.
in trasmissione	AutoSupport sta attualmente distribuendo messaggi.
inviato correttamente	AutoSupport ha recapitato correttamente il messaggio. È possibile scoprire dove AutoSupport ha recapitato il messaggio immettendo il `system node autosupport history show -delivery` comando.
ignorare	AutoSupport non ha destinazioni per il messaggio. È possibile visualizzare i dettagli di consegna immettendo il `system node autosupport history show -delivery` comando.
riaccodato	AutoSupport ha tentato di inviare messaggi, ma il tentativo non è riuscito. Di conseguenza, AutoSupport ha riportato i messaggi nella coda di consegna per un altro tentativo. È possibile visualizzare l'errore immettendo il `system node autosupport history show` comando.
trasmissione non riuscita	AutoSupport non ha recapitato il messaggio il numero di volte specificato e ha smesso di provare a recapitare il messaggio. È possibile visualizzare l'errore immettendo il `system node autosupport history show` comando.
ondemand: ignora	Il messaggio AutoSupport è stato elaborato correttamente, ma il servizio AutoSupport su richiesta ha scelto di ignorarlo.

3. Eseguire una delle seguenti operazioni:

Per questo stato	Eseguire questa operazione
inizializzazione o raccolta non riuscita	Contattare il supporto NetApp perché AutoSupport non è in grado di generare il messaggio. Citare il seguente articolo della Knowledge base: "AutoSupport non riesce a consegnare: Lo stato è bloccato in inizializzazione"
ignorare, riaccodare o trasmettere non riuscita	Verificare che le destinazioni siano configurate correttamente per SMTP, HTTP o HTTPS, poiché AutoSupport non è in grado di inviare il messaggio.

Risolvere i problemi relativi all'erogazione dei messaggi AutoSupport su HTTP o HTTPS

Se il sistema non invia il messaggio AutoSupport previsto e si sta utilizzando HTTP o HTTPS, oppure se la funzione di aggiornamento automatico non funziona, è possibile verificare alcune impostazioni per risolvere il problema.

Di cosa hai bisogno

La connettività di rete di base e la ricerca DNS dovrebbero essere state confermate:

- La LIF di gestione dei nodi deve essere attiva per lo stato operativo e amministrativo.
- È necessario essere in grado di eseguire il ping di un host funzionante sulla stessa subnet dalla LIF di gestione del cluster (non una LIF su uno dei nodi).
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster.
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster utilizzando il nome dell'host (non l'indirizzo IP).

A proposito di questa attività

Questi passaggi si riferiscono ai casi in cui si è stabilito che AutoSupport è in grado di generare il messaggio, ma non è in grado di recapitare il messaggio su HTTP o HTTPS.

Se si verificano errori o non è possibile completare un passaggio di questa procedura, individuare e risolvere il problema prima di passare alla fase successiva.

Fasi

1. Visualizzare lo stato dettagliato del sottosistema AutoSupport:

   ```
   system node autosupport check show-details
   ```

   Ciò include la verifica della connettività alle destinazioni AutoSupport inviando messaggi di test e fornendo un elenco di possibili errori nelle impostazioni di configurazione di AutoSupport.

2. Verificare lo stato della LIF di gestione dei nodi:

   ```
   network interface show -home-node local -role node-mgmt -fields
   vserver,lif,status-oper,status-admin,address,role
   ```

   Il `status-oper` e. `status-admin` i campi devono restituire "up".

3. Registrare il nome SVM, il nome LIF e l'indirizzo IP LIF per un utilizzo successivo.
4. Assicurarsi che il DNS sia attivato e configurato correttamente:

   ```
   vserver services name-service dns show
   ```

5. Risolvere eventuali errori restituiti dal messaggio AutoSupport:

   ```
   system node autosupport history show -node * -fields node,seq-
   num,destination,last-update,status,error
   ```

   Per assistenza nella risoluzione di eventuali errori restituiti, consultare "Guida alla risoluzione di ONTAP AutoSupport (Transport HTTPS and HTTP)".

6. Verificare che il cluster sia in grado di accedere a Internet e ai server necessari:

   a. `network traceroute -lif node-management_LIF -destination DNS server`

   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

L'indirizzo `support.netapp.com` di per sé non risponde al ping/traceroute, ma le informazioni per-hop sono preziose.

c. `system node autosupport show -fields proxy-url`

d. `network traceroute -node node_management_LIF -destination proxy_url`

Se uno di questi percorsi non funziona, provare lo stesso percorso da un host funzionante sulla stessa sottorete del cluster, utilizzando l'utility "traceroute" o "tracert" presente sulla maggior parte dei client di rete di terze parti. Ciò consente di determinare se il problema riguarda la configurazione di rete o la configurazione del cluster.

7. Se si utilizza HTTPS per il protocollo di trasporto AutoSupport, assicurarsi che il traffico HTTPS possa uscire dalla rete:

   a. Configurare un client Web sulla stessa subnet della LIF di gestione del cluster.

      Assicurarsi che tutti i parametri di configurazione siano gli stessi valori della configurazione AutoSupport, incluso l'utilizzo dello stesso server proxy, nome utente, password e porta.

   b. Accesso `https://support.netapp.com` con il client web.

      L'accesso dovrebbe essere riuscito. In caso contrario, assicurarsi che tutti i firewall siano configurati correttamente per consentire il traffico HTTPS e DNS e che il server proxy sia configurato correttamente. Per ulteriori informazioni sulla configurazione della risoluzione statica dei nomi per support.netapp.com, consultare l'articolo della Knowledge base "Come aggiungere una voce HOST in ONTAP per support.netapp.com?"

8. A partire da ONTAP 9.10.1, se è stata attivata la funzione di aggiornamento automatico, assicurarsi di disporre della connettività HTTPS per i seguenti URL aggiuntivi:
   - https://support-sg-emea.netapp.com
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

Risolvere i problemi relativi all'invio dei messaggi AutoSupport su SMTP

Se il sistema non riesce a inviare messaggi AutoSupport tramite SMTP, è possibile controllare diverse impostazioni per risolvere il problema.

Di cosa hai bisogno

La connettività di rete di base e la ricerca DNS dovrebbero essere state confermate:

- La LIF di gestione dei nodi deve essere attiva per lo stato operativo e amministrativo.
- È necessario essere in grado di eseguire il ping di un host funzionante sulla stessa subnet dalla LIF di gestione del cluster (non una LIF su uno dei nodi).
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster.
- È necessario essere in grado di eseguire il ping di un host funzionante al di fuori della subnet dalla LIF di gestione del cluster utilizzando il nome dell'host (non l'indirizzo IP).

A proposito di questa attività

Questa procedura si verifica nei casi in cui AutoSupport sia in grado di generare il messaggio, ma non è in

grado di recapitare il messaggio tramite SMTP.

Se si verificano errori o non è possibile completare un passaggio di questa procedura, individuare e risolvere il problema prima di passare alla fase successiva.

Tutti i comandi vengono immessi nell'interfaccia della riga di comando di ONTAP, se non diversamente specificato.

Fasi

1. Verificare lo stato della LIF di gestione dei nodi:

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   Il `status-oper` e. `status-admin` i campi devono essere visualizzati `up`.

2. Registrare il nome SVM, il nome LIF e l'indirizzo IP LIF per un utilizzo successivo.
3. Assicurarsi che il DNS sia attivato e configurato correttamente:

   vserver services name-service dns show

4. Visualizza tutti i server configurati per l'utilizzo da parte di AutoSupport:

   system node autosupport show -fields mail-hosts

   Registrare tutti i nomi dei server visualizzati.

5. Per ciascun server visualizzato al punto precedente, e. `support.netapp.com`, Assicurarsi che il server o l'URL possa essere raggiunto dal nodo:

   network traceroute -node local -destination *server_name*

   Se uno di questi percorsi non funziona, provare lo stesso percorso da un host funzionante sulla stessa sottorete del cluster, utilizzando l'utility "traceroute" o "tracert" presente sulla maggior parte dei client di rete di terze parti. Ciò consente di determinare se il problema riguarda la configurazione di rete o la configurazione del cluster.

6. Accedere all'host designato come host di posta e assicurarsi che sia in grado di inviare richieste SMTP:

   netstat -aAn|grep 25

   `25` È il numero della porta SMTP del listener.

   Viene visualizzato un messaggio simile al seguente:

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. Da un altro host, aprire una sessione Telnet con la porta SMTP dell'host di posta:

   telnet *mailhost* 25

   Viene visualizzato un messaggio simile al seguente:

```
220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
10:49:04 PST
```

8. Al prompt di telnet, assicurarsi che sia possibile trasmettere un messaggio dal proprio host di posta:

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   `domain_name` è il nome di dominio della rete.

   Se viene visualizzato un messaggio di errore che indica che l'inoltro è negato, l'inoltro non viene attivato sull'host di posta. Contattare l'amministratore di sistema.

9. Al prompt di telnet, inviare un messaggio di test:

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   Assicurarsi di inserire l'ultimo punto (.) su una linea da sola. Il punto indica all'host di posta che il messaggio è completo.

   Se viene visualizzato un errore, l'host di posta non è configurato correttamente. Contattare l'amministratore di sistema.

10. Dall'interfaccia della riga di comando di ONTAP, inviare un messaggio di test AutoSupport a un indirizzo e-mail attendibile a cui si dispone dell'accesso:

    system node autosupport invoke -node local -type test

11. Individuare il numero di sequenza del tentativo:

    system node autosupport history show -node local -destination smtp

    Individuare il numero di sequenza per il tentativo in base all'indicatore data e ora. Si tratta probabilmente del tentativo più recente.

12. Visualizza l'errore per il tentativo di messaggio di test:

    system node autosupport history show -node local -seq-num seq_num -fields error

    Se l'errore visualizzato è `Login denied`, Il server SMTP non accetta le richieste di invio dalla LIF di gestione del cluster. Se non si desidera passare all'utilizzo di HTTPS come protocollo di trasporto, contattare l'amministratore di rete del sito per configurare i gateway SMTP per risolvere il problema.

Se il test ha esito positivo, ma lo stesso messaggio inviato a mailto:autosupport@netapp.com non lo ha, assicurarsi che l'inoltro SMTP sia attivato su tutti gli host di posta SMTP oppure utilizzare HTTPS come protocollo di trasporto.

Se anche il messaggio all'account di posta elettronica amministrato in locale non riesce, verificare che i server SMTP siano configurati per inoltrare gli allegati con entrambe le caratteristiche:

- Il suffisso "7z"
- Il tipo MIME "application/x-7x-compressed".

Risolvere i problemi del sottosistema AutoSupport

Il `system node check show` I comandi possono essere utilizzati per verificare e risolvere eventuali problemi relativi alla configurazione e all'erogazione di AutoSupport.

Fase

1. Utilizzare i seguenti comandi per visualizzare lo stato del sottosistema AutoSupport.

Utilizzare questo comando…	A tal fine…
`system node autosupport check show`	Visualizza lo stato generale del sottosistema AutoSupport, ad esempio lo stato della destinazione HTTP o HTTPS AutoSupport, le destinazioni SMTP AutoSupport, il server AutoSupport OnDemand e la configurazione AutoSupport
`system node autosupport check show-details`	Visualizza lo stato dettagliato del sottosistema AutoSupport, ad esempio descrizioni dettagliate degli errori e delle azioni correttive

Monitoraggio dello stato di salute

Monitorare lo stato di salute del sistema

I monitor dello stato di salute monitorano in modo proattivo determinate condizioni critiche nel cluster e avvisano se rilevano un guasto o un rischio. Se sono presenti avvisi attivi, lo stato di salute del sistema riporta uno stato degradato per il cluster. Gli avvisi includono le informazioni necessarie per rispondere a problemi di salute del sistema.

Se lo stato è degradato, è possibile visualizzare i dettagli del problema, incluse la probabile causa e le azioni di ripristino consigliate. Una volta risolto il problema, lo stato di salute del sistema torna automaticamente a OK.

Lo stato di salute del sistema riflette più monitor di stato separati. Uno stato degradato in un singolo monitor di salute causa uno stato degradato per lo stato generale del sistema.

Per ulteriori informazioni su come ONTAP supporta gli switch del cluster per il monitoraggio dello stato di salute del sistema nel cluster, fare riferimento alla *Hardware Universe*.

"Switch supportati in Hardware Universe"

Per informazioni dettagliate sulle cause dei messaggi AutoSupport relativi al monitoraggio dello stato di salute degli switch del cluster e sulle azioni necessarie per risolvere questi avvisi, consultare l'articolo della Knowledge base.

"Messaggio AutoSupport: CSHM processo di monitoraggio dello stato di salute"

Come funziona il monitoraggio dello stato di salute

I singoli monitor dello stato di salute dispongono di una serie di policy che attivano avvisi quando si verificano determinate condizioni. La comprensione del funzionamento del monitoraggio dello stato di salute può aiutarti a rispondere ai problemi e a controllare gli avvisi futuri.

Il monitoraggio dello stato di salute è costituito dai seguenti componenti:

- Monitoraggio dello stato di salute individuale per sottosistemi specifici, ciascuno dei quali ha un proprio stato di salute

  Ad esempio, il sottosistema di storage dispone di un monitor di stato della connettività del nodo.

- Un monitor generale dello stato di salute del sistema che consolida lo stato di salute dei singoli monitor

  Uno stato degradato in un singolo sottosistema determina uno stato degradato per l'intero sistema. Se nessun sottosistemi dispone di avvisi, lo stato generale del sistema è OK.

Ciascun monitor di stato è costituito dai seguenti elementi chiave:

- Avvisa che il monitor dello stato di salute può potenzialmente aumentare

  Ogni avviso ha una definizione che include dettagli come la severità dell'avviso e la sua probabile causa.

- Policy di integrità che identificano quando viene attivato ogni avviso

  Ogni policy di integrità ha un'espressione di regola, che è la condizione o la modifica esatta che attiva l'avviso.

Un monitor dello stato di salute monitora e convalida continuamente le risorse nel sottosistema per verificare la presenza di modifiche di stato o condizione. Quando una condizione o una modifica di stato corrisponde all'espressione di una regola in un criterio di integrità, il monitor dello stato genera un avviso. Un avviso causa il degrado dello stato di salute del sottosistema e dello stato di salute generale del sistema.

Modi per rispondere agli avvisi sullo stato di salute del sistema

Quando si verifica un avviso di stato di salute del sistema, è possibile riconoscerlo, ottenere ulteriori informazioni, riparare la condizione sottostante ed evitare che si verifichi di nuovo.

Quando un monitor dello stato di salute genera un avviso, è possibile rispondere in uno dei seguenti modi:

- Ottenere informazioni sull'avviso, che includono la risorsa interessata, la severità dell'avviso, la probabile causa, il possibile effetto e le azioni correttive.
- Ottenere informazioni dettagliate sull'avviso, ad esempio l'ora in cui l'avviso è stato generato e se altri

hanno già confermato l'avviso.

- Ottenere informazioni sullo stato della risorsa o del sottosistema interessato, ad esempio uno shelf o un disco specifico.
- Riconoscere l'avviso per indicare che qualcuno sta lavorando al problema e identificarsi come "Acknowledger".
- Risolvere il problema adottando le azioni correttive fornite nell'avviso, ad esempio la risoluzione di un problema di connettività tramite il cablaggio.
- Eliminare l'avviso, se il sistema non lo ha cancellato automaticamente.
- Eliminare un avviso per evitare che influisca sullo stato di salute di un sottosistema.

  La soppressione è utile quando si comprende un problema. Una volta eliminato un avviso, questo può comunque verificarsi, ma lo stato del sottosistema viene visualizzato come "ok-with-suppressed" (ok-with-suppressed). quando si verifica l'avviso sospeso.

Personalizzazione degli avvisi sullo stato di salute del sistema

È possibile controllare quali avvisi vengono generati da un monitor dello stato di salute attivando e disattivando le policy di stato del sistema che definiscono quando vengono attivati gli avvisi. Ciò consente di personalizzare il sistema di monitoraggio dello stato di salute per il proprio ambiente specifico.

È possibile conoscere il nome di un criterio visualizzando informazioni dettagliate su un avviso generato o visualizzando le definizioni dei criteri per uno specifico Health monitor, nodo o ID avviso.

La disattivazione delle policy di integrità è diversa dalla sospensione degli avvisi. La soppressione di un avviso non influisce sullo stato di salute del sottosistema, ma può comunque verificarsi.

Se si disattiva un criterio, la condizione o lo stato definito nell'espressione della regola dei criteri non attiva più un avviso.

Esempio di avviso che si desidera disattivare

Ad esempio, supponiamo che si verifichi un avviso non utile. Si utilizza `system health alert show -instance` Per ottenere l'ID policy per l'avviso. L'ID del criterio viene utilizzato in `system health policy definition show` per visualizzare le informazioni relative al criterio. Dopo aver esaminato l'espressione della regola e altre informazioni relative al criterio, si decide di disattivarlo. Si utilizza `system health policy definition modify` per disattivare il criterio.

Modalità di attivazione degli avvisi di integrità per i messaggi e gli eventi AutoSupport

Gli avvisi sullo stato di salute del sistema attivano messaggi ed eventi AutoSupport nel sistema di gestione degli eventi, consentendo di monitorare lo stato di salute del sistema utilizzando messaggi AutoSupport e EMS, oltre a utilizzare direttamente il sistema di monitoraggio dello stato di salute.

Il sistema invia un messaggio AutoSupport entro cinque minuti da un avviso. Il messaggio AutoSupport include tutti gli avvisi generati dal precedente messaggio AutoSupport, ad eccezione degli avvisi che duplicano un avviso per la stessa risorsa e la causa probabile entro la settimana precedente.

Alcuni avvisi non attivano i messaggi AutoSupport. Un avviso non attiva un messaggio AutoSupport se la relativa policy di integrità disattiva l'invio di messaggi AutoSupport. Ad esempio, per impostazione predefinita, un criterio di integrità potrebbe disattivare i messaggi AutoSupport perché AutoSupport già genera un messaggio quando si verifica il problema. È possibile configurare i criteri per non attivare i messaggi AutoSupport utilizzando `system health policy definition modify` comando.

È possibile visualizzare un elenco di tutti i messaggi AutoSupport attivati dagli avvisi inviati la settimana precedente utilizzando `system health autosupport trigger history show` comando.

Gli avvisi attivano anche la generazione di eventi al sistema EMS. Ogni volta che viene creato un avviso e ogni volta che viene cancellato, viene generato un evento.

Monitoraggio dello stato dei cluster disponibili

Esistono diversi monitor di stato che monitorano diverse parti di un cluster. I monitor di stato consentono di eseguire il ripristino dagli errori all'interno dei sistemi ONTAP rilevando gli eventi, inviando avvisi ed eliminando gli eventi non appena vengono eliminati.

Nome del monitor di stato (identificatore)	Nome del sottosistema (identificatore)	Scopo
Switch del cluster (switch del cluster)	Switch (stato dello switch)	Monitora gli switch di rete del cluster e gli switch di rete di gestione per la temperatura, l'utilizzo, la configurazione dell'interfaccia, la ridondanza (solo switch di rete del cluster) e il funzionamento di ventole e alimentatori. Il monitor di stato dello switch del cluster comunica con gli switch tramite SNMP. SNMPv2c è l'impostazione predefinita. A partire da ONTAP 9.2, questo monitor è in grado di rilevare e segnalare quando uno switch del cluster si è riavviato dall'ultimo periodo di polling.
Fabric MetroCluster	Switch	Monitora la topologia del fabric back-end di configurazione MetroCluster e rileva configurazioni errate, come cablaggio e zoning errati e errori ISL.

Nome del monitor di stato (identificatore)	Nome del sottosistema (identificatore)	Scopo
Salute di MetroCluster	Interconnessione, RAID e storage	Monitora adattatori FC-VI, adattatori FC Initiator, aggregati e dischi sinistri e porte tra cluster
Connettività del nodo (connessione al nodo)	Operazioni CIFS senza interruzioni (CIFS-NDO)	Monitora le connessioni SMB per le operazioni senza interruzioni alle applicazioni Hyper-V.
Storage (SAS-Connect)	Monitora shelf, dischi e adattatori a livello di nodo per verificare la presenza di percorsi e connessioni appropriati.	Sistema
non applicabile	Aggrega le informazioni provenienti da altri monitor dello stato di salute.	Connettività del sistema (connessione al sistema)

Ricevere automaticamente gli avvisi sullo stato di salute del sistema

È possibile visualizzare manualmente gli avvisi sullo stato di salute del sistema utilizzando `system health alert show` comando. Tuttavia, è necessario iscriversi a specifici messaggi EMS (Event Management System) per ricevere automaticamente le notifiche quando un monitor dello stato di salute genera un avviso.

A proposito di questa attività

La seguente procedura illustra come impostare le notifiche per tutti i messaggi hm.alert.Raised e per tutti i messaggi hm.alert.Cleared.

Tutti i messaggi hm.alert.Raised e tutti i messaggi hm.alert.Cleared includono una trap SNMP. I nomi dei trap SNMP sono `HealthMonitorAlertRaised` e. `HealthMonitorAlertCleared`. Per informazioni sui trap SNMP, consultare la *Network Management Guide*.

Fasi

1. Utilizzare `event destination create` Per definire la destinazione a cui si desidera inviare i messaggi EMS.

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

2. Utilizzare `event route add-destinations` per instradare `hm.alert.raised` e il `hm.alert.cleared` a una destinazione.

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

Informazioni correlate

"Gestione della rete"

Rispondere a uno stato di salute del sistema degradato

Quando lo stato di salute del sistema è degradato, è possibile visualizzare avvisi, leggere la causa probabile e le azioni correttive, visualizzare informazioni sul sottosistema degradato e risolvere il problema. Vengono inoltre visualizzati gli avvisi soppressi, in modo da poterli modificare e verificare se sono stati riconosciuti.

A proposito di questa attività

È possibile scoprire che è stato generato un avviso visualizzando un messaggio AutoSupport o un evento EMS oppure utilizzando `system health` comandi.

Fasi

1. Utilizzare `system health alert show` per visualizzare gli avvisi che compromettono lo stato di salute del sistema.
2. Leggi la probabile causa, il possibile effetto e le azioni correttive dell'avviso per determinare se puoi risolvere il problema o se hai bisogno di ulteriori informazioni.
3. Per ulteriori informazioni, utilizzare `system health alert show -instance` per visualizzare ulteriori informazioni disponibili per l'avviso.
4. Utilizzare `system health alert modify` con il `-acknowledge` parametro per indicare che si sta lavorando a un avviso specifico.
5. Intraprendere un'azione correttiva per risolvere il problema come descritto in `Corrective Actions` nel campo dell'avviso.

   Le azioni correttive potrebbero includere il riavvio del sistema.

   Una volta risolto il problema, l'avviso viene cancellato automaticamente. Se il sottosistema non dispone di altri avvisi, lo stato del sottosistema cambia in `OK`. Se lo stato di tutti i sottosistemi è corretto, lo stato generale del sistema diventa `OK`.

6. Utilizzare `system health status show` per confermare che lo stato di salute del sistema è `OK`.

   Se lo stato di salute del sistema non è `OK`, ripetere questa procedura.

Esempio di risposta a uno stato di salute del sistema degradato

Esaminando un esempio specifico di stato di salute del sistema degradato causato da uno shelf che non dispone di due percorsi per un nodo, è possibile visualizzare la CLI quando si risponde a un avviso.

Dopo aver avviato ONTAP, controllare lo stato del sistema e verificare che lo stato sia degradato:

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

Mostra gli avvisi per scoprire dove si trova il problema e scopri che lo shelf 2 non ha due percorsi per il node1:

```
cluster1::>system health alert show
             Node: node1
         Resource: Shelf ID 2
         Severity: Major
   Indication Time: Mon Nov 10 16:48:12 2013
 Probable Cause: Disk shelf 2 does not have two paths to controller
                 node1.
Possible Effect: Access to disk shelf 2 via controller node1 will be
                 lost with a single hardware component failure (e.g.
                 cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                 2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                 3. Reboot the halted controllers.
                 4. Contact support personnel if the alert persists.
```

Vengono visualizzati i dettagli dell'avviso per ottenere ulteriori informazioni, tra cui l'ID dell'avviso:

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

L'utente riconosce l'avviso per indicare che si sta lavorando.

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

Riparare il cablaggio tra lo shelf 2 e il nodo 1, quindi riavviare il sistema. Quindi, controllare nuovamente lo stato del sistema e verificare che lo stato sia `OK`:

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

Configurare il rilevamento degli switch di rete di gestione e del cluster

Il monitor di stato dello switch del cluster tenta automaticamente di rilevare gli switch del cluster e della rete di gestione utilizzando il protocollo Cisco Discovery (CDP). È necessario configurare il monitor dello stato di salute se non riesce a rilevare automaticamente uno switch o se non si desidera utilizzare CDP per il rilevamento automatico.

A proposito di questa attività

Il `system cluster-switch show` il comando elenca gli switch rilevati dal monitor dello stato di salute. Se non viene visualizzato uno switch che si prevede venga visualizzato nell'elenco, il monitor dello stato di salute non può rilevarlo automaticamente.

Fasi

1. Se si desidera utilizzare CDP per il rilevamento automatico, attenersi alla seguente procedura:

   a. Assicurarsi che il protocollo Cisco Discovery Protocol (CDP) sia attivato sugli switch.

      Per istruzioni, consultare la documentazione dello switch.

   b. Eseguire il seguente comando su ciascun nodo del cluster per verificare se CDP è attivato o disattivato:

      run -node *node_name* -command options cdpd.enable

      Se CDP è attivato, passare alla fase d. Se CDP è disattivato, passare alla fase c.

   c. Eseguire il seguente comando per attivare CDP:

      run -node *node_name* -command options cdpd.enable on

   Attendere cinque minuti prima di passare alla fase successiva.

   a. Utilizzare `system cluster-switch show` Per verificare se ONTAP è in grado di rilevare automaticamente gli switch.

2. Se il monitor dello stato di salute non rileva automaticamente uno switch, utilizzare `system cluster-switch create` comando per configurare il rilevamento dello switch:

   ```
   cluster1::> system cluster-switch create -device switch1 -address
   192.0.2.250 -snmp-version SNMPv2c -community cshm1! -model NX5020 -type
   cluster-network
   ```

   Attendere cinque minuti prima di passare alla fase successiva.

3. Utilizzare `system cluster-switch show` Per verificare che ONTAP sia in grado di rilevare lo switch per cui sono state aggiunte informazioni.

Al termine

Verificare che lo Health monitor sia in grado di monitorare gli switch.

Verificare il monitoraggio degli switch del cluster e della rete di gestione

Il monitor di stato dello switch del cluster tenta automaticamente di monitorare gli switch che rileva; tuttavia, il monitoraggio potrebbe non verificarsi automaticamente se gli switch non sono configurati correttamente. Verificare che il monitor dello stato di salute sia configurato correttamente per monitorare gli switch.

Fasi

1. Per identificare gli switch rilevati dal monitor di stato dello switch del cluster, immettere il seguente comando:

   ONTAP 9.8 e versioni successive

   `system switch ethernet show`

   ONTAP 9.7 e versioni precedenti

   `system cluster-switch show`

   Se il `Model` visualizza il valore `OTHER`, Quindi ONTAP non può monitorare lo switch. ONTAP imposta il valore su `OTHER` se uno switch che rileva automaticamente non è supportato per il monitoraggio dello stato di salute.

   Se uno switch non viene visualizzato nell'output del comando, è necessario configurare il rilevamento dello switch.

2. Eseguire l'aggiornamento al software dello switch più recente supportato e fare riferimento al file di configurazione (RCF) dal sito del supporto NetApp.

   "Pagina Support Downloads di NetApp"

   La stringa community nell'RCF dello switch deve corrispondere alla stringa community configurata per l'utilizzo da parte del monitor di stato. Per impostazione predefinita, il monitor di stato utilizza la stringa di comunità `cshm1!`.

   Attualmente, il monitor di stato supporta solo SNMPv2.

   Se è necessario modificare le informazioni relative a uno switch monitorato dal cluster, è possibile modificare la stringa di comunità utilizzata da Health monitor utilizzando il seguente comando:

ONTAP 9.8 e versioni successive

`system switch ethernet modify`

ONTAP 9.7 e versioni precedenti

`system cluster-switch modify`

3. Verificare che la porta di gestione dello switch sia collegata alla rete di gestione.

   Questa connessione è necessaria per eseguire query SNMP.

Comandi per il monitoraggio dello stato di salute del sistema

È possibile utilizzare `system health` comandi per visualizzare informazioni sullo stato delle risorse di sistema, rispondere agli avvisi e configurare gli avvisi futuri. L'utilizzo dei comandi CLI consente di visualizzare informazioni dettagliate sulla configurazione del monitoraggio dello stato di salute. Le pagine man dei comandi contengono ulteriori informazioni.

Visualizza lo stato dello stato di salute del sistema

Se si desidera…	Utilizzare questo comando…
Visualizza lo stato di salute del sistema, che riflette lo stato generale dei singoli monitor di salute	`system health status show`
Visualizza lo stato di salute dei sottosistemi per i quali è disponibile il monitoraggio dello stato di salute	`system health subsystem show`

Visualizza lo stato della connettività del nodo

Se si desidera…	Utilizzare questo comando…
Visualizza dettagli sulla connettività dal nodo allo shelf di storage, tra cui informazioni sulle porte, velocità della porta HBA, throughput i/o e velocità delle operazioni di i/o al secondo	`storage shelf show -connectivity` Utilizzare `-instance` parametro per visualizzare informazioni dettagliate su ogni shelf.
Visualizza informazioni su dischi e LUN di array, inclusi lo spazio utilizzabile, i numeri di shelf e alloggiamenti e il nome del nodo proprietario	`storage disk show` Utilizzare `-instance` per visualizzare informazioni dettagliate su ciascun disco.
Visualizza informazioni dettagliate sulle porte dello shelf storage, tra cui tipo di porta, velocità e stato	`storage port show` Utilizzare `-instance` parametro per visualizzare informazioni dettagliate su ciascun adattatore.

Gestire il rilevamento di switch di rete per cluster, storage e gestione

Se si desidera…	Utilizzare questo comando. (ONTAP 9.8 e versioni successive)	Utilizzare questo comando. (ONTAP 9.7 e versioni precedenti)
Visualizza gli switch che il cluster monitora	`system switch ethernet show`	`system cluster-switch show`
Visualizzare gli switch attualmente monitorati dal cluster, inclusi gli switch cancellati (visualizzati nella colonna Reason (motivo) nell'output del comando) e le informazioni di configurazione necessarie per l'accesso di rete al cluster e agli switch di rete di gestione. Questo comando è disponibile a livello di privilegio avanzato.	`system switch ethernet show-all`	`system cluster-switch show-all`
Configurare il rilevamento di uno switch non rilevato	`system switch ethernet create`	`system cluster-switch create`
Modificare le informazioni relative a uno switch che il cluster monitora (ad esempio, nome del dispositivo, indirizzo IP, versione SNMP e stringa di comunità)	`system switch ethernet modify`	`system cluster-switch modify`
Disattiva il monitoraggio di uno switch	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
Disattivare il rilevamento e il monitoraggio di uno switch ed eliminare le informazioni di configurazione dello switch	`system switch ethernet delete`	`system cluster-switch delete`
Rimuovere in modo permanente le informazioni di configurazione dello switch memorizzate nel database (in questo modo si riattiva il rilevamento automatico dello switch)	`system switch ethernet delete -force`	`system cluster-switch delete -force`
Abilitare la registrazione automatica per l'invio con messaggi AutoSupport.	`system switch ethernet log`	`system cluster-switch log`

Rispondere agli avvisi generati

Se si desidera…	Utilizzare questo comando…
Visualizza le informazioni sugli avvisi generati, ad esempio la risorsa e il nodo in cui è stato attivato l'avviso, la gravità e la probabile causa dell'avviso	`system health alert show`
Visualizza le informazioni relative a ciascun avviso generato	`system health alert show -instance`
Indica che qualcuno sta lavorando a un avviso	`system health alert modify`
Riconoscere un avviso	`system health alert modify -acknowledge`
Eliminare un avviso successivo in modo che non influisca sullo stato di salute di un sottosistema	`system health alert modify -suppress`
Eliminare un avviso non cancellato automaticamente	`system health alert delete`
Visualizza le informazioni sui messaggi AutoSupport attivati nell'ultima settimana, ad esempio per determinare se un avviso ha attivato un messaggio AutoSupport	`system health autosupport trigger history show`

Configurare gli avvisi futuri

Se si desidera…	Utilizzare questo comando…
Attivare o disattivare il criterio che controlla se uno stato di risorsa specifico genera un avviso specifico	`system health policy definition modify`

Visualizza informazioni sulla configurazione del monitoraggio dello stato di salute

Se si desidera…	Utilizzare questo comando…
Visualizzare informazioni sui monitor di stato, ad esempio nodi, nomi, sottosistemi e stato	`system health config show` Utilizzare `-instance` parametro per visualizzare informazioni dettagliate su ciascun monitor di salute.
Visualizza informazioni sugli avvisi potenzialmente generati da un monitor dello stato di salute	`system health alert definition show` Utilizzare `-instance` parametro per visualizzare informazioni dettagliate su ciascuna definizione di avviso.

Se si desidera…	Utilizzare questo comando…
Visualizza informazioni sui criteri di monitoraggio dello stato di salute, che determinano quando vengono generati gli avvisi	`system health policy definition show` Utilizzare `-instance` parametro per visualizzare informazioni dettagliate su ogni policy. Utilizzare altri parametri per filtrare l'elenco degli avvisi, ad esempio in base allo stato della policy (attivato o meno), al monitor dello stato di salute, agli avvisi e così via.

Visualizzare le informazioni ambientali

I sensori consentono di monitorare i componenti ambientali del sistema. Le informazioni che è possibile visualizzare sui sensori ambientali includono tipo, nome, stato, valore e avvisi di soglia.

Fase

1. Per visualizzare informazioni sui sensori ambientali, utilizzare `system node environment sensors show` comando.

Analisi del file system

Panoramica di file System Analytics

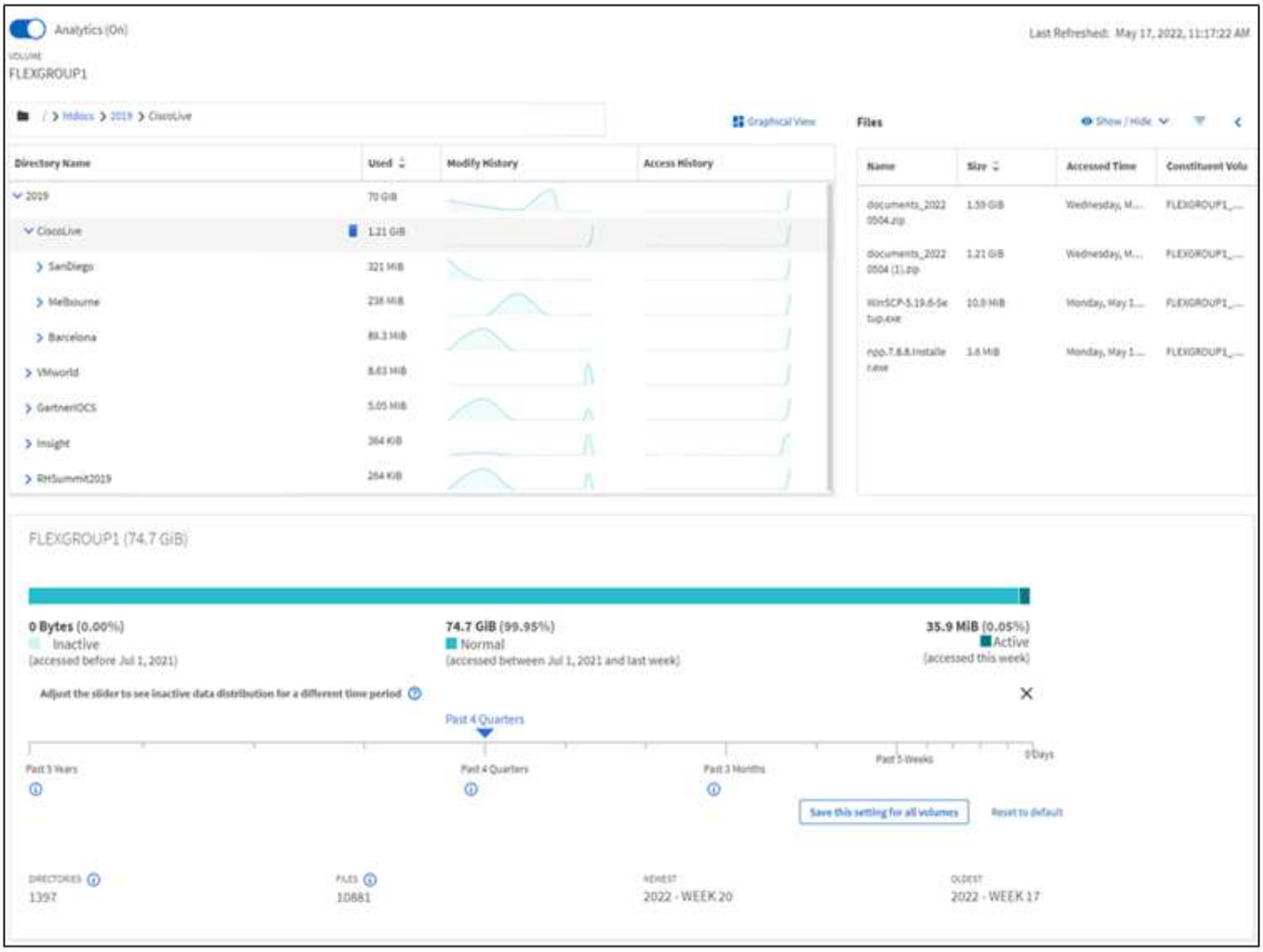
L'analisi del file system (FSA) è stata introdotta per la prima volta in ONTAP 9.8 per fornire visibilità in tempo reale sull'utilizzo dei file e sulle tendenze della capacità dello storage all'interno dei volumi ONTAP FlexGroup o FlexVol. Questa funzionalità nativa elimina la necessità di strumenti esterni e fornisce informazioni chiave sull'utilizzo dello storage e sull'opportunità di ottimizzare lo storage in base alle esigenze aziendali.

Con FSA, è possibile ottenere visibilità a tutti i livelli della gerarchia di file system di un volume in NAS. Ad esempio, è possibile ottenere informazioni sull'utilizzo e sulla capacità a livello di Storage VM (SVM), volume, directory e file. Puoi utilizzare FSA per rispondere a domande come:

- Cosa sta riempiendo lo storage e ci sono file di grandi dimensioni che è possibile spostare in un'altra posizione di storage?
- Quali sono i volumi, le directory e i file più attivi? Le performance dello storage sono ottimizzate per le esigenze dei miei utenti?
- Quanti dati sono stati aggiunti nell'ultimo mese?
- Chi sono i miei utenti di storage più attivi o meno attivi?
- Quanti dati inattivi o inattivi si trovano nello storage primario? Posso spostare questi dati in un cold Tier a costi inferiori?
- Le modifiche pianificate alla qualità del servizio avranno un impatto negativo sull'accesso ai file critici e ad accesso frequente?

L'analisi del file system è integrata in Gestione sistema ONTAP. Le visualizzazioni di System Manager offrono:

- Visibilità in tempo reale per una gestione e un funzionamento dei dati efficaci
- Raccolta e aggregazione dei dati in tempo reale
- Dimensioni e conteggi delle sottodirectory e dei file, insieme ai profili di performance associati
- Istogrammi di età dei file per la cronologia delle modifiche e degli accessi



Tipi di volume supportati

L'analisi del file system è progettata per fornire visibilità sui volumi con dati NAS attivi, ad eccezione delle cache FlexCache e dei volumi di destinazione SnapMirror.

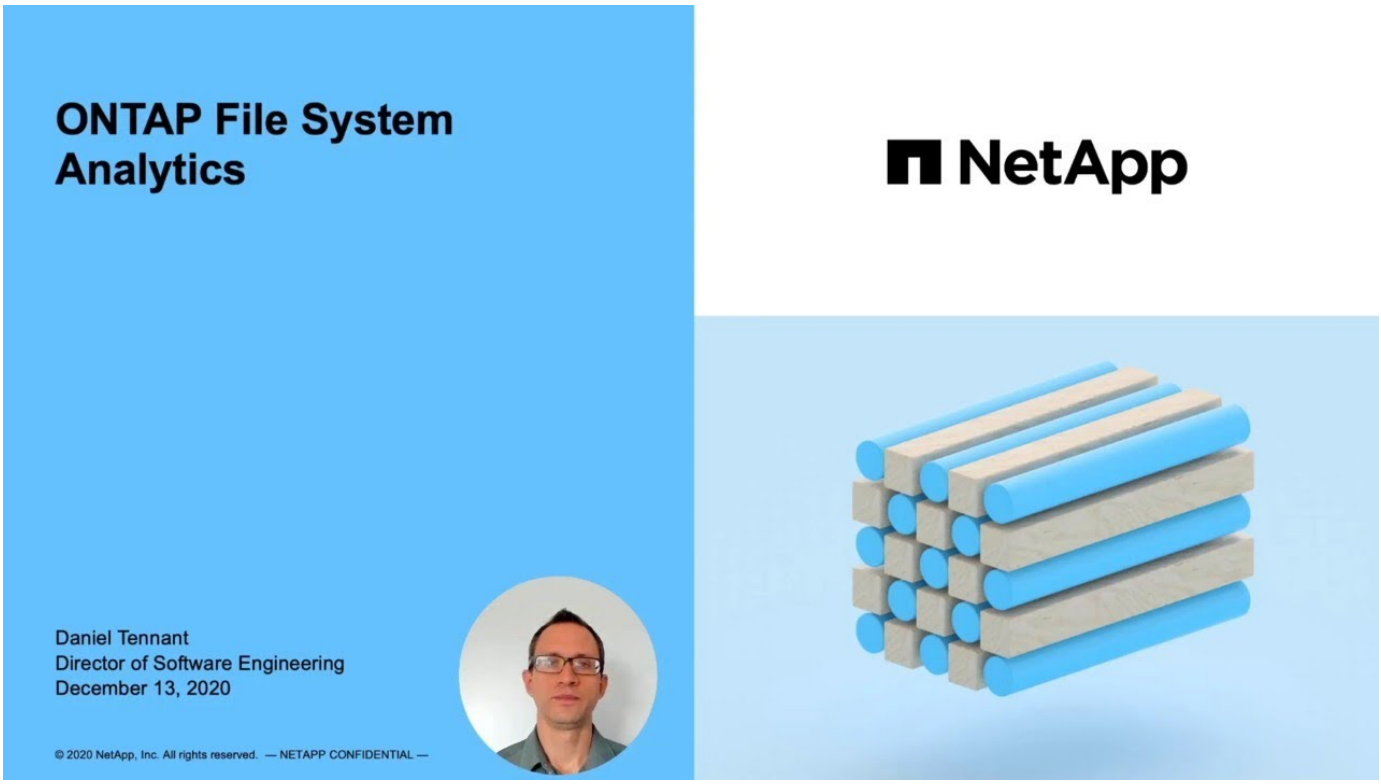
Disponibilità delle funzionalità di analisi del file system

Ogni release di ONTAP amplia l'ambito dell'analisi del file system.

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Visualizzazione in System Manager	✓	✓	✓	✓	✓	✓	✓

	ONTAP 9.14.1	ONTAP 9.13.1	ONTAP 9.12.1	ONTAP 9.11.1	ONTAP 9.10.1	ONTAP 9.9.1	ONTAP 9.8
Analisi della capacità	✓	✓	✓	✓	✓	✓	✓
Informazioni sui dati inattivi	✓	✓	✓	✓	✓	✓	✓
Supporto per volumi in transizione da Data ONTAP 7-Mode	✓	✓	✓	✓	✓	✓	
Possibilità di personalizzare il periodo inattivo in System Manager	✓	✓	✓	✓	✓	✓	
Monitoraggio delle attività a livello di volume	✓	✓	✓	✓	✓		
Scarica i dati di Activity Tracking in CSV	✓	✓	✓	✓	✓		
Monitoraggio delle attività a livello di SVM	✓	✓	✓	✓			
Tempistiche	✓	✓	✓	✓			
Analisi dell'utilizzo	✓	✓	✓				
Opzione per attivare l'analisi del file system per impostazione predefinita	✓	✓					
Monitor di avanzamento scansione inizializzazione	✓						

Scopri di più su file System Analytics



Ulteriori letture

- "TR 4687: Linee guida sulle Best practice per l'analisi del file system ONTAP"
- "Knowledge base: Latenza elevata o fluttuante dopo l'attivazione dell'analisi del file system NetApp ONTAP"

Abilita analisi del file system

Per raccogliere e visualizzare i dati di utilizzo, ad esempio l'analisi della capacità, è necessario attivare l'analisi del file system su un volume.

A proposito di questa attività

- A partire da ONTAP 9.8, è possibile attivare l'analisi del file system su un volume nuovo o esistente. Se si aggiorna un sistema a ONTAP 9.8 o versioni successive, assicurarsi che tutti i processi di aggiornamento siano stati completati prima di attivare l'analisi del file system.
- A seconda delle dimensioni e dei contenuti del volume, l'abilitazione delle analisi potrebbe richiedere tempo mentre ONTAP elabora i dati esistenti nel volume. System Manager visualizza l'avanzamento e presenta i dati di analisi una volta completati. Per informazioni più precise sull'avanzamento dell'inizializzazione, utilizzare il comando ONTAP CLI `volume analytics show`.

  A partire da ONTAP 9.14.1, ONTAP fornisce il monitoraggio dell'avanzamento della scansione di inizializzazione, oltre alle notifiche sugli eventi di rallentamento che influiscono sull'avanzamento della scansione.

  Per ulteriori considerazioni relative alla scansione di inizializzazione, vedere Considerazioni sulla scansione.

Fasi

È possibile attivare l'analisi del file system con Gestione di sistema di ONTAP o l'interfaccia CLI.

System Manager

In ONTAP 9.8 e 9.9.1	A partire da ONTAP 9.10.1
1. Selezionare **Storage > Volumes** (archiviazione > volumi). 2. Selezionare il volume desiderato, quindi selezionare **Explorer**. 3. Selezionare **Enable Analytics** (attiva analisi) o **Disable Analytics** (Disattiva analisi).	1. Selezionare **Storage > Volumes** (archiviazione > volumi). 2. Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare **file System > Explorer**. 3. Selezionare **Enable Analytics** (attiva analisi) o **Disable Analytics** (Disattiva analisi).

CLI

Abilitare l'analisi del file system con la CLI

1. Eseguire il seguente comando:
   `volume analytics on -vserver` *`svm_name`* `-volume` *`volume_name`* `[-foreground {true|false}]`` Per impostazione predefinita, il comando viene eseguito in primo piano; ONTAP visualizza l'avanzamento e presenta i dati di analisi al termine. Per informazioni più precise, è possibile eseguire il comando in background utilizzando `-foreground false` e quindi utilizzare `volume analytics show` Per visualizzare l'avanzamento dell'inizializzazione nella CLI.
2. Dopo aver attivato correttamente l'analisi del file system, utilizzare Gestione sistema o l'API REST di ONTAP per visualizzare i dati analitici.

Modificare le impostazioni predefinite di file System Analytics

A partire da ONTAP 9.13.1, è possibile modificare le impostazioni SVM o cluster per attivare l'analisi del file system per impostazione predefinita sui nuovi volumi.

System Manager

Se si utilizza System Manager, è possibile modificare le impostazioni della macchina virtuale dello storage o del cluster per abilitare l'analisi della capacità e il monitoraggio delle attività alla creazione del volume per impostazione predefinita. L'abilitazione predefinita si applica solo ai volumi creati dopo la modifica delle impostazioni, non ai volumi esistenti.

Modificare le impostazioni di analisi del file system su un cluster

1. In System Manager, accedere a **Impostazioni cluster**.
2. In **Impostazioni cluster**, esaminare la scheda Impostazioni file system. Per modificare le impostazioni, selezionare icona.
3. Nel campo **monitoraggio attività**, immettere i nomi delle SVM per cui attivare il monitoraggio attività per per impostazione predefinita. Se si lascia il campo vuoto, il monitoraggio attività viene disattivato su tutte le SVM.

   Deselezionare la casella **Enable on new storage vms** (attiva sulle nuove macchine virtuali storage) per disattivare il monitoraggio delle attività per impostazione predefinita sulle nuove macchine virtuali storage.

4. Nel campo **Analytics**, immettere i nomi delle VM di storage per le quali si desidera abilitare l'analisi della capacità per impostazione predefinita. Lasciando il campo vuoto, l'analisi della capacità viene disattivata su tutte le SVM.

   Deselezionare la casella **Enable on new storage VM** (attiva sulle nuove macchine virtuali storage) per disattivare l'analisi della capacità per impostazione predefinita sulle nuove macchine virtuali storage.

5. Selezionare **Salva**.

Modificare le impostazioni di analisi del file system su una SVM

1. Selezionare la SVM che si desidera modificare, quindi **Impostazioni Storage VM**.
2. Nella scheda **analisi del file system**, utilizzare i pulsanti per attivare o disattivare il monitoraggio delle attività e l'analisi della capacità per tutti i nuovi volumi sulla VM di storage.

CLI

È possibile configurare la VM di storage per abilitare l'analisi del file system per impostazione predefinita sui nuovi volumi utilizzando l'interfaccia CLI di ONTAP.

Abilitare l'analisi del file system per impostazione predefinita su una SVM

1. Modificare la SVM per attivare l'analisi della capacità e il monitoraggio delle attività per impostazione predefinita su tutti i volumi appena creati:
   `vserver modify -vserver svm_name -auto-enable-activity-tracking true -auto -enable-analytics true`

Visualizzare l'attività del file system

Dopo aver attivato file System Analytics (FSA), è possibile visualizzare il contenuto della directory principale di un volume selezionato, ordinato in base allo spazio utilizzato in ogni sottostruttura.

Selezionare qualsiasi oggetto del file system per esplorare il file system e visualizzare informazioni dettagliate su ciascun oggetto in una directory. Le informazioni sulle directory possono anche essere visualizzate graficamente. Nel tempo, vengono visualizzati i dati storici per ogni sottostruttura. Lo spazio utilizzato non viene ordinato se sono presenti più di 3000 directory.

Esplora risorse

La schermata file System Analytics **Explorer** è composta da tre aree:

- Visualizzazione ad albero di directory e sottodirectory; elenco espandibile con nome, dimensione, cronologia delle modifiche e cronologia degli accessi.
- File; mostra nome, dimensione e tempo di accesso per l'oggetto selezionato nell'elenco di directory.
- Confronto dei dati attivi e inattivi per l'oggetto selezionato nell'elenco delle directory.

  A partire da ONTAP 9.9.1, è possibile personalizzare l'intervallo da segnalare. Il valore predefinito è di un anno. In base a queste personalizzazioni, è possibile intraprendere azioni correttive, come lo spostamento di volumi e la modifica della policy di tiering.

L'ora di accesso viene visualizzata per impostazione predefinita. Tuttavia, se l'impostazione predefinita del volume è stata modificata dall'interfaccia CLI (impostando il `-atime-update` opzione a. `false` con `volume modify` comando), quindi viene visualizzata solo l'ora dell'ultima modifica. Ad esempio:

- La vista ad albero non visualizza la **cronologia di accesso**.
- La vista file viene modificata.
- La vista dati attiva/inattiva si basa sull'ora modificata (`mtime`).

Utilizzando queste schermate, è possibile esaminare quanto segue:

- Le posizioni del file system occupano la maggior parte dello spazio
- Informazioni dettagliate su un albero di directory, incluso il numero di file e sottodirectory all'interno di directory e sottodirectory
- Posizioni del file system che contengono dati vecchi (ad esempio, scratch, temp o log tree)

Tenere a mente i seguenti punti quando si interpreta l'output FSA:

- FSA mostra dove e quando i tuoi dati sono in uso, non la quantità di dati che vengono elaborati. Ad esempio, un elevato consumo di spazio da parte dei file recentemente utilizzati o modificati non indica necessariamente elevati carichi di elaborazione del sistema.
- Il modo in cui la scheda **Volume Explorer** calcola il consumo di spazio per FSA potrebbe differire da altri strumenti. In particolare, potrebbero esserci differenze significative rispetto al consumo riportato in **Volume Overview** se il volume dispone delle funzionalità di efficienza dello storage abilitate. Questo perché la scheda **Volume Explorer** non include i risparmi in termini di efficienza.
- A causa delle limitazioni di spazio nella visualizzazione della directory, non è possibile visualizzare una profondità della directory superiore a 8 livelli nella *visualizzazione elenco*. Per visualizzare le directory più profonde di 8 livelli, passare a *Graphical View*, individuare la directory desiderata, quindi tornare a *List View*. In questo modo si otterrà ulteriore spazio sullo schermo.

Fasi

1. Visualizzare il contenuto della directory principale di un volume selezionato:

In ONTAP 9.8 e 9.9.1	A partire da ONTAP 9.10.1
Fare clic su **Storage > Volumes** (archiviazione > volumi), selezionare il volume desiderato, quindi fare clic su **Explorer**.	Selezionare **Storage > Volumes** (archiviazione > volumi), quindi selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare **file System > Explorer**.

Attiva monitoraggio attività

A partire da ONTAP 9.10.1, l'analisi del file system include una funzione di monitoraggio delle attività che consente di identificare gli oggetti hot e scaricare i dati come file CSV. A partire da ONTAP 9.11.1, il monitoraggio delle attività viene esteso all'ambito SVM. Inoltre, a partire da ONTAP 9.11.1, System Manager dispone di una timeline per il monitoraggio delle attività, che consente di esaminare fino a cinque minuti di dati di monitoraggio delle attività.

Il monitoraggio delle attività consente il monitoraggio in quattro categorie:

- Directory
- File
- Client
- Utenti

Per ciascuna categoria monitorata, Activity Tracking visualizza IOPS di lettura, IOPS di scrittura, risultati di lettura e risultati di scrittura. Le query su Activity Tracking si aggiornano ogni 10 - 15 secondi relativi agli hot spot rilevati nel sistema nell'intervallo di cinque secondi precedente.

Le informazioni di monitoraggio dell'attività sono approssimative e la precisione dei dati dipende dalla distribuzione del traffico i/o in entrata.

Quando si visualizza Activity Tracking in System Manager a livello di volume, viene aggiornato attivamente solo il menu del volume espanso. Se la vista di qualsiasi volume viene compressa, non si aggiornerà fino a quando la visualizzazione del volume non viene espansa. È possibile interrompere gli aggiornamenti con il pulsante **Pause Refresh** (Pausa aggiornamento*). I dati delle attività possono essere scaricati in formato CSV che visualizza tutti i dati point-in-time acquisiti per il volume selezionato.

Con la funzione timeline disponibile a partire da ONTAP 9.11.1, è possibile registrare l'attività dell'hotspot su un volume o una SVM, aggiornando continuamente circa ogni cinque secondi e mantenendo i cinque minuti precedenti di dati. I dati della timeline vengono conservati solo per i campi che sono aree visibili della pagina. Se si comprime una categoria di rilevamento o si scorre in modo che la timeline non sia visualizzata, la timeline interrompe la raccolta dei dati. Per impostazione predefinita, le tempistiche sono disattivate e vengono disattivate automaticamente quando ci si allontana dalla scheda Activity (attività).

Attiva monitoraggio attività per un singolo volume

È possibile attivare il monitoraggio delle attività con Gestore di sistema di ONTAP o l'interfaccia CLI.

A proposito di questa attività

Se si utilizza RBAC con l'API REST di ONTAP o Gestione sistema, sarà necessario creare ruoli personalizzati per gestire l'accesso al monitoraggio delle attività. Vedere Controllo degli accessi in base al ruolo per questo processo.

System Manager

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare file System (file system), quindi selezionare la scheda Activity (attività).
2. Assicurarsi che l'opzione **Activity Tracking** sia attivata per visualizzare i singoli report su directory, file, client e utenti principali.
3. Per analizzare i dati in modo più approfondito senza aggiornamenti, selezionare **Pause Refresh** (Pausa aggiornamento*). È possibile scaricare i dati per ottenere anche un record CSV del report.

CLI

Fasi

1. Attiva monitoraggio attività:

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. Controllare se lo stato di monitoraggio attività di un volume è attivato o disattivato con il comando:

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. Una volta attivata, utilizzare Gestione di sistema ONTAP o l'API REST ONTAP per visualizzare i dati di monitoraggio delle attività.

Attiva monitoraggio attività per più volumi

Puoi attivare il monitoraggio delle attività per più volumi con System Manager o la CLI.

A proposito di questa attività

Se si utilizza RBAC con l'API REST di ONTAP o Gestione sistema, sarà necessario creare ruoli personalizzati per gestire l'accesso al monitoraggio delle attività. Vedere Controllo degli accessi in base al ruolo per questo processo.

System Manager

Abilitare per volumi specifici

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato. Dal menu dei singoli volumi, selezionare file System (file system), quindi selezionare la scheda Activity (attività).
2. Selezionare i volumi su cui si desidera attivare il monitoraggio attività. Nella parte superiore dell'elenco dei volumi, selezionare il pulsante **altre opzioni**. Selezionare **Enable Activity Tracking** (attiva monitoraggio attività).
3. Per visualizzare Activity Tracking a livello di SVM, selezionare la SVM specifica che si desidera visualizzare da **Storage > Volumes**. Accedere alla scheda file System (file system), quindi Activity (attività) per visualizzare i dati dei volumi per i quali è stata attivata l'opzione Activity Tracking (tracciamento attività).

Abilitare per tutti i volumi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare una SVM dal menu.
2. Accedere alla scheda **file System** e scegliere la scheda **More** per attivare il monitoraggio delle attività su tutti i volumi nella SVM.

CLI

A partire da ONTAP 9.13.1, è possibile attivare il monitoraggio delle attività per più volumi utilizzando l'interfaccia utente di ONTAP.

Fasi

1. Attiva monitoraggio attività:

   `volume activity-tracking on -vserver` *`svm_name`* `-volume [*|!`*`volume_names`*`]`

   Utilizzare `*` Per attivare il monitoraggio delle attività per tutti i volumi sulla VM di storage specificata.

   Utilizzare `!` Seguito dai nomi dei volumi per abilitare il monitoraggio delle attività per tutti i volumi su SVM, ad eccezione dei volumi denominati.

2. Confermare che l'operazione è riuscita:

   `volume show -fields activity-tracking-state`

3. Una volta attivata, utilizzare Gestione di sistema ONTAP o l'API REST ONTAP per visualizzare i dati di monitoraggio delle attività.

Abilita l'analisi dell'utilizzo

A partire da ONTAP 9.12.1, è possibile abilitare l'analisi dell'utilizzo per vedere quali directory all'interno di un volume utilizzano più spazio. È possibile visualizzare il numero totale di directory in un volume o il numero totale di file in un volume. Il reporting è limitato alle 25 directory che utilizzano la maggior parte dello spazio.

Gli analytics delle directory di grandi dimensioni vengono aggiornati ogni 15 minuti. È possibile monitorare l'aggiornamento più recente selezionando l'indicatore data e ora ultimo aggiornamento nella parte superiore della pagina. È inoltre possibile fare clic sul pulsante Download per scaricare i dati in una cartella di lavoro Excel. L'operazione di download viene eseguita in background e presenta le informazioni più recenti per il

volume selezionato. Se la scansione si ripresenta senza alcun risultato, assicurarsi che il volume sia online. Eventi come SnapRestore causeranno la ricostruzione dell'elenco di directory di grandi dimensioni da parte di analisi del file system.

Fasi

1. Selezionare **Storage > Volumes** (Storage > volumi). Selezionare il volume desiderato.
2. Dal menu dei singoli volumi, selezionare **file System**. Quindi selezionare la scheda **Usage** (utilizzo).
3. Attivare l'opzione **Analytics** per abilitare l'analisi dell'utilizzo.
4. System Manager visualizza un grafico a barre che identifica le directory con le dimensioni maggiori in ordine decrescente.

> ONTAP potrebbe visualizzare dati parziali o non visualizzare alcun dato durante la raccolta dell'elenco delle directory principali. L'avanzamento della scansione può essere nella scheda **Usage** (utilizzo) visualizzata durante la scansione.

Per ottenere ulteriori informazioni su una directory specifica, è possibile visualizzare l'attività su un file system.

Intraprendere azioni correttive basate sugli analytics

A partire da ONTAP 9.9.1, puoi intraprendere azioni correttive in base ai dati correnti e ai risultati desiderati direttamente dalle visualizzazioni di analisi del file system.

Eliminare directory e file

Nella visualizzazione Esplora risorse, è possibile selezionare le directory o i singoli file da eliminare. Le directory vengono eliminate con la funzionalità di eliminazione rapida delle directory a bassa latenza. (L'eliminazione rapida delle directory è disponibile anche a partire da ONTAP 9.9.1 senza l'opzione di analisi attivata).

Fasi

1. Fare clic su **Storage > Volumes**, quindi su **Explorer**.

   Quando si passa il mouse su un file o una cartella, viene visualizzata l'opzione da eliminare. È possibile eliminare un solo oggetto alla volta.

> Quando le directory e i file vengono cancellati, i nuovi valori di capacità dello storage non vengono visualizzati immediatamente.

Assegna il costo dei supporti nei Tier di storage per confrontare i costi delle posizioni di storage dei dati inattive

Il costo dei supporti è un valore assegnato in base alla valutazione dei costi di storage, rappresentato come valuta per GB. Una volta impostato, System Manager utilizza il costo dei supporti assegnato per proiettare i risparmi stimati quando si spostano i volumi.

Il costo dei supporti impostato non è persistente; può essere impostato solo per una singola sessione del browser.

Fasi

1. Fare clic su **Storage > Tier**, quindi fare clic su **Set Media Cost** (Imposta costo supporti) nei riquadri del

Tier locale (aggregato) desiderato.

Assicurarsi di selezionare i livelli attivi e inattivi per attivare il confronto.

2. Inserire un tipo di valuta e un importo.

   Quando si inserisce o si modifica il costo del supporto, la modifica viene apportata a tutti i tipi di supporto.

Spostamento dei volumi per ridurre i costi di storage

In base ai display analitici e al confronto dei costi multimediali, puoi spostare i volumi in uno storage meno costoso nei Tier locali.

È possibile confrontare e spostare un solo volume alla volta.

Fasi

1. Dopo aver attivato la visualizzazione dei costi dei supporti, fare clic su **Storage > Tier**, quindi su **Volumes**.
2. Per confrontare le opzioni di destinazione di un volume, fare clic su ⋮ Per il volume, fare clic su **Move** (Sposta).
3. Nella schermata **Select Destination Local Tier** (Seleziona livello locale di destinazione), selezionare i Tier di destinazione per visualizzare la differenza di costo stimata.
4. Dopo aver confrontato le opzioni, selezionare il livello desiderato e fare clic su **Move** (Sposta).

Controllo degli accessi in base al ruolo con file System Analytics

A partire da ONTAP 9.12.1, ONTAP include un ruolo predefinito RBAC (role-based access control) chiamato `admin-no-fsa`. Il `admin-no-fsa` il ruolo concede privilegi di livello amministratore, ma impedisce all'utente di eseguire operazioni correlate a `files` Endpoint (ad es. Analisi del file system) nell'interfaccia CLI di ONTAP, nell'API REST e in Gestore di sistema.

Per ulteriori informazioni su `admin-no-fsa` ruolo, fare riferimento a. Ruoli predefiniti per gli amministratori del cluster.

Se si utilizza una versione di ONTAP rilasciata prima di ONTAP 9.12.1, sarà necessario creare un ruolo dedicato per controllare l'accesso all'analisi del file system. Nelle versioni di ONTAP precedenti a ONTAP 9.12.1, è necessario configurare le autorizzazioni RBAC tramite l'interfaccia CLI di ONTAP o l'API REST di ONTAP.

System Manager

A partire da ONTAP 9.12.1, è possibile configurare le autorizzazioni RBAC per l'analisi del file system utilizzando Gestione sistema.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni). In **Security**, selezionare **Users and Roles** e scegliere →.
2. In **ruoli**, selezionare + Add .
3. Fornire un nome per il ruolo. Nella sezione attributi ruolo, configurare l'accesso o le restrizioni per il ruolo utente fornendo l'appropriato "Endpoint API". Consultare la tabella seguente per i percorsi primari e secondari per configurare l'accesso o le restrizioni di file System Analytics.

Restrizione	Percorso primario	Percorso secondario
Monitoraggio delle attività sui volumi	`/api/storage/volumes`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Monitoraggio delle attività su SVM	`/api/svm/svms`	• `/:uuid/top-metrics/directories` • `/:uuid/top-metrics/files` • `/:uuid/top-metrics/clients` • `/:uuid/top-metrics/users`
Tutte le operazioni di analisi del file system	`/api/storage/volumes`	`/:uuid/files`

   È possibile utilizzare `/*/` Invece di un UUID per impostare la policy per tutti i volumi o le SVM all'endpoint.

   Scegliere i privilegi di accesso per ciascun endpoint.

4. Selezionare **Salva**.
5. Per assegnare il ruolo a uno o più utenti, vedere Controllare l'accesso dell'amministratore.

CLI

Se si utilizza una versione di ONTAP rilasciata prima di ONTAP 9.12.1, utilizzare l'interfaccia utente di ONTAP per creare un ruolo personalizzato.

Fasi

1. Creare un ruolo predefinito per avere accesso a tutte le funzionalità.

   Questa operazione deve essere eseguita prima di creare un ruolo restrittivo per garantire che il ruolo sia limitato solo al monitoraggio attività:

   ```
   security login role create -cmddirname DEFAULT -access all -role
   storageAdmin
   ```

2. Creare il ruolo restrittivo:

   ```
   security login role create -cmddirname "volume file show-disk-usage"
   -access none -role storageAdmin
   ```

3. Autorizzare i ruoli ad accedere ai servizi Web di SVM:

   - `rest` Per chiamate API REST
   - `security` per la protezione tramite password
   - `sysmgr` Per l'accesso a System Manager

     ```
     vserver services web access create -vserver svm-name -name_ -name rest
     -role storageAdmin

     vserver services web access create -vserver svm-name -name security
     -role storageAdmin
     ```

   ```
   vserver services web access create -vserver svm-name -name sysmgr -role
   storageAdmin
   ```

4. Creare un utente.

   È necessario eseguire un comando di creazione distinto per ciascuna applicazione che si desidera applicare all'utente. La chiamata a create più volte sullo stesso utente applica semplicemente tutte le applicazioni a quell'utente e non crea un nuovo utente ogni volta. Il `http` Il parametro per il tipo di applicazione si applica all'API REST di ONTAP e al Gestore di sistema.

   ```
   security login create -user-or-group-name storageUser -authentication
   -method password -application http -role storageAdmin
   ```

5. Con le nuove credenziali utente, è ora possibile accedere a Gestore di sistema o utilizzare l'API REST di ONTAP per accedere ai dati di analisi dei file system.

Ulteriori informazioni

- Ruoli predefiniti per gli amministratori del cluster
- Controlla l'accesso dell'amministratore con System Manager
- "Scopri di più sui ruoli RBAC e sull'API REST ONTAP"

Considerazioni per l'analisi del file system

Devi essere consapevole di determinati limiti di utilizzo e potenziali impatti sulle

performance associati all'implementazione di file System Analytics.

Relazioni protette con SVM

Se sono state attivate le analisi del file system su volumi con SVM contenente una relazione di protezione, i dati di analisi non vengono replicati nella SVM di destinazione. Se la SVM di origine deve essere risincronizzata in un'operazione di recovery, è necessario riabilitare manualmente le analisi sui volumi desiderati dopo il recovery.

Considerazioni sulle performance

In alcuni casi, l'abilitazione di file System Analytics potrebbe avere un impatto negativo sulle performance durante la raccolta iniziale dei metadati. Ciò si verifica in genere nei sistemi che sono al massimo utilizzo. Per evitare di abilitare l'analisi su tali sistemi, è possibile utilizzare gli strumenti di monitoraggio delle performance di Gestore di sistema di ONTAP.

Se si verifica un notevole aumento della latenza, consultare l'articolo della Knowledge base "Latenza elevata o fluttuante dopo l'attivazione dell'analisi del file system NetApp ONTAP".

Considerazioni sulla scansione

Quando abiliti le analisi della capacità, ONTAP esegue una scansione di inizializzazione per l'analisi della capacità. La scansione accede ai metadati per tutti i file nei volumi per i quali è abilitata l'analisi della capacità. Durante la scansione non viene letto alcun dato di file. A partire da ONTAP 9.14.1, è possibile tenere traccia dell'avanzamento della scansione con l'API REST, nella scheda **Esplora risorse** di Gestione sistema o con `volume analytics show` Comando CLI. Se è presente un evento di rallentamento, ONTAP fornisce una notifica.

Al termine della scansione, file System Analytics viene continuamente aggiornato in tempo reale in base alle modifiche del file system senza dover eseguire nuovamente la scansione.

Il tempo richiesto per la scansione è proporzionale al numero di directory e file sul volume. Poiché la scansione raccoglie i metadati, le dimensioni del file non influiscono sul tempo di scansione.

Per ulteriori informazioni sulla scansione di inizializzazione, vedere "TR-4867: Linee guida sulle Best practice per l'analisi del file system".

Best practice

Si consiglia di avviare la scansione su volumi che non condividono aggregati. È possibile visualizzare gli aggregati che attualmente ospitano i volumi utilizzando il comando:

`volume show -volume` *`comma-separated-list_of_volumes`* `-fields aggr-list`

Durante l'esecuzione della scansione, i volumi continuano a servire il traffico client. Si consiglia di avviare la scansione durante i periodi in cui si prevede una riduzione del traffico client.

Se il traffico del client aumenta, consuma le risorse di sistema e la scansione richiede più tempo.

A partire da ONTAP 9.12.1, è possibile sospendere la raccolta dei dati in Gestore di sistema e con l'interfaccia utente di ONTAP.

- Se si utilizza l'interfaccia utente di ONTAP:
  - È possibile sospendere la raccolta dati con il comando: `volume analytics initialization`

`pause -vserver svm_name -volume volume_name`

- Una volta rallentato il traffico del client, è possibile riprendere la raccolta dei dati con il comando: `volume analytics initialization resume -vserver svm_name -volume volume_name`

- Se si utilizza System Manager, nella vista **Explorer** del menu del volume, utilizzare i pulsanti **Pause Data Collection** e **Resume Data Collection** per gestire la scansione.

Configurazione EMS

Panoramica della configurazione EMS

È possibile configurare ONTAP 9 in modo che invii notifiche di eventi EMS (sistema di gestione degli eventi) importanti direttamente a un indirizzo e-mail, a un server syslog, a un traphost SNMP (Simple Management Network Protocol) o a un'applicazione webhook, in modo da ricevere una notifica immediata dei problemi di sistema che richiedono un'attenzione immediata.

Poiché le notifiche di eventi importanti non sono attivate per impostazione predefinita, è necessario configurare EMS in modo che invii le notifiche a un indirizzo e-mail, a un server syslog, a un host trapSNMP o a un'applicazione webhook.

Esaminare le versioni specifiche della release di "Riferimento EMS ONTAP 9".

Se la mappatura degli eventi EMS utilizza set di comandi ONTAP deprecati (come destinazione dell'evento, percorso dell'evento), si consiglia di aggiornare la mappatura. "Scopri come aggiornare la mappatura EMS da comandi ONTAP non aggiornati".

Configurare le notifiche e i filtri degli eventi EMS con System Manager

È possibile utilizzare System Manager per configurare il modo in cui il sistema di gestione degli eventi (EMS) invia le notifiche degli eventi, in modo da poter essere avvisati dei problemi di sistema che richiedono una rapida attenzione.

Versione di ONTAP	Con System Manager, è possibile…
ONTAP 9.12.1 e versioni successive	Specificare il protocollo TLS (Transport Layer Security) quando si inviano eventi ai server syslog remoti.
ONTAP 9.10.1 e versioni successive	Configurare indirizzi e-mail, server syslog, applicazioni webhook e host SNMP.
ONTAP da 9.7 a 9.10.0	Configurare solo i traphost SNMP. È possibile configurare un'altra destinazione EMS con la CLI ONTAP. Vedere "Panoramica della configurazione EMS".

È possibile eseguire le seguenti procedure:

- [add-ems-destination]
- [create-ems-filter]

- [edit-ems-destination]
- [edit-ems-filter]
- [delete-ems-destination]
- [delete-ems-filter]

Informazioni correlate

- "Riferimento EMS ONTAP"
- "Utilizzo della CLI per configurare i traphost SNMP in modo che ricevano le notifiche degli eventi"

Aggiungere una destinazione di notifica degli eventi EMS

È possibile utilizzare System Manager per specificare dove si desidera inviare i messaggi EMS.

A partire da ONTAP 9.12.1, gli eventi EMS possono essere inviati a una porta designata su un server syslog remoto tramite il protocollo TLS (Transport Layer Security). Per ulteriori informazioni, vedere `event notification destination create` pagina man.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Fare clic su + Add .
5. Specificare un nome, un tipo di destinazione EMS e i filtri.

   Se necessario, è possibile aggiungere un nuovo filtro. Fare clic su **Aggiungi un nuovo filtro eventi**.

6. A seconda del tipo di destinazione EMS selezionato, specificare quanto segue:

Per configurare…	Specificare o selezionare…
SNMP traphost	• Nome TrapHost
E-mail (A partire da 9.10.1)	• Indirizzo e-mail di destinazione • Server di posta • Da indirizzo e-mail
Server syslog (A partire da 9.10.1)	• Nome host o indirizzo IP del server • Porta syslog (a partire da 9.12.1) • Trasporto syslog (a partire da 9.12.1) Selezionando **TCP Encrypted** si attiva il protocollo TLS (Transport Layer Security). Se non viene immesso alcun valore per **porta Syslog**, viene utilizzato un valore predefinito in base alla selezione **trasporto Syslog**.

Webhook (A partire da 9.10.1)	• URL Webhook • Autenticazione client (selezionare questa opzione per specificare un certificato client)

Creare un nuovo filtro per la notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per definire nuovi filtri personalizzati che specificano le regole per la gestione delle notifiche EMS.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Fare clic su + Add .
5. Specificare un nome e scegliere se si desidera copiare le regole da un filtro eventi esistente o aggiungere nuove regole.
6. A seconda della scelta, attenersi alla seguente procedura:

Se si sceglie….	Quindi, eseguire questi passaggi…
Copia delle regole dal filtro eventi esistente	1. Selezionare un filtro eventi esistente. 2. Modificare le regole esistenti. 3. Aggiungere altre regole, se necessario, facendo clic su + Add .
Aggiungi nuove regole	Specificare il tipo, il modello di nome, le severità e il tipo di trap SNMP per ogni nuova regola.

Modificare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare le informazioni di destinazione della notifica degli eventi.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su ⋮, Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni sulla destinazione dell'evento, quindi fare clic su **Salva**.

Modificare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per modificare i filtri personalizzati e modificare la modalità di gestione delle notifiche degli eventi.

Non è possibile modificare i filtri definiti dal sistema.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su ⋮, Quindi fare clic su **Edit** (Modifica).
5. Modificare le informazioni del filtro eventi, quindi fare clic su **Save** (Salva).

Eliminare una destinazione di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare una destinazione di notifica degli eventi EMS.

Non è possibile eliminare le destinazioni SNMP.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **Destinazioni eventi**.
4. Accanto al nome della destinazione dell'evento, fare clic su ⋮, Quindi fare clic su **Delete** (Elimina).

Eliminare un filtro di notifica degli eventi EMS

A partire da ONTAP 9.10.1, è possibile utilizzare Gestione sistema per eliminare i filtri personalizzati.

Non è possibile eliminare i filtri definiti dal sistema.

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Nella sezione **Gestione notifiche**, fare clic su ⋮, Quindi fare clic su **View Event Destinations** (Visualizza destinazioni evento).
3. Nella pagina **Gestione notifiche**, selezionare la scheda **filtri eventi**.
4. Accanto al nome del filtro eventi, fare clic su ⋮, Quindi fare clic su **Delete** (Elimina).

Configurare le notifiche degli eventi EMS con la CLI

Workflow di configurazione EMS

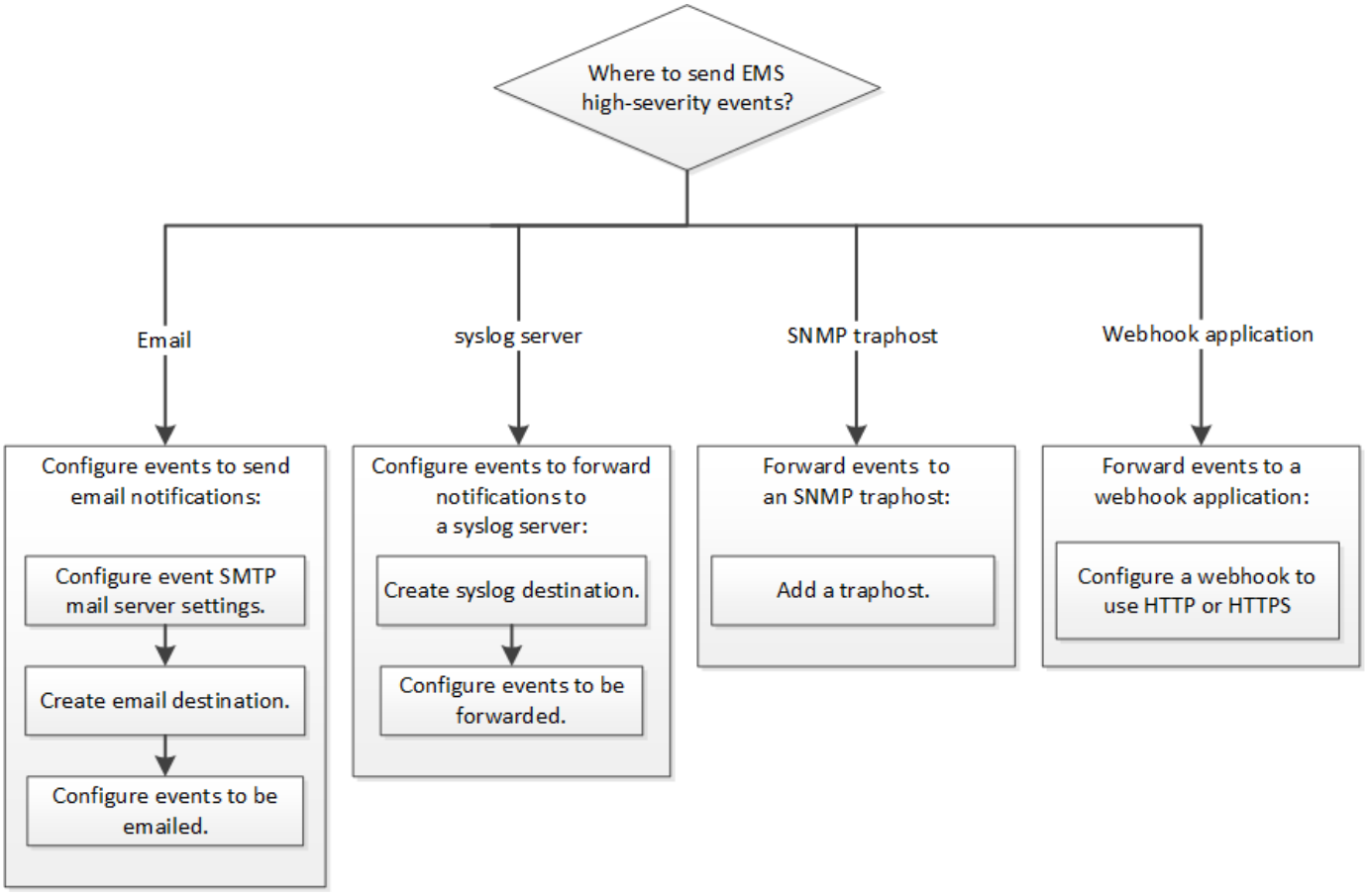
È necessario configurare le notifiche di eventi EMS importanti da inviare come email, inoltrate a un server syslog, inoltrate a un host traphost SNMP o inoltrate a un'applicazione webhook. In questo modo, è possibile evitare interruzioni del sistema adottando azioni correttive in modo tempestivo.

A proposito di questa attività

Se l'ambiente in uso contiene già un server syslog per l'aggregazione degli eventi registrati da altri sistemi, come server e applicazioni, è più semplice utilizzare tale server syslog anche per le notifiche di eventi importanti provenienti dai sistemi storage.

Se l'ambiente non contiene già un server syslog, è più semplice utilizzare l'e-mail per le notifiche di eventi importanti.

Se si inoltrano già notifiche di eventi a un host trapSNMP, potrebbe essere necessario monitorare tale host per rilevare eventi importanti.



Scelte

- Impostare EMS per l'invio delle notifiche degli eventi.

Se vuoi…	Fare riferimento a…
EMS per inviare notifiche di eventi importanti a un indirizzo e-mail	Configurare eventi EMS importanti per l'invio di notifiche e-mail
EMS per inoltrare notifiche di eventi importanti a un server syslog	Configurare eventi EMS importanti per inoltrare le notifiche a un server syslog
Se si desidera che EMS inoltri le notifiche degli eventi a un host trapSNMP	Configurare i traphost SNMP per ricevere le notifiche degli eventi

Se si desidera che EMS inoltri le notifiche degli eventi a un'applicazione webhook	Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook

Configurare eventi EMS importanti per l'invio di notifiche e-mail

Per ricevere notifiche via email degli eventi più importanti, è necessario configurare il servizio EMS in modo che invii messaggi di posta elettronica per gli eventi che segnalano attività importanti.

Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere gli indirizzi e-mail.

A proposito di questa attività

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

Fasi

1. Configurare le impostazioni del server di posta SMTP dell'evento:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

2. Creare una destinazione email per le notifiche degli eventi:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

3. Configurare gli eventi importanti per l'invio di notifiche e-mail:

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

Configurazione di eventi EMS importanti per inoltrare le notifiche a un server syslog

Per registrare le notifiche degli eventi più gravi su un server syslog, è necessario configurare EMS in modo che inoltri le notifiche per gli eventi che segnalano attività importanti.

Di cosa hai bisogno

Il DNS deve essere configurato sul cluster per risolvere il nome del server syslog.

A proposito di questa attività

Se l'ambiente non contiene già un server syslog per le notifiche degli eventi, è necessario crearne uno. Se l'ambiente in uso contiene già un server syslog per la registrazione degli eventi da altri sistemi, è possibile utilizzare tale server per le notifiche di eventi importanti.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nell'interfaccia utente di ONTAP.

A partire da ONTAP 9.12.1, gli eventi EMS possono essere inviati a una porta designata su un server syslog

remoto tramite il protocollo TLS (Transport Layer Security). Sono disponibili due nuovi parametri:

`tcp-encrypted`

Quando `tcp-encrypted` è specificato per `syslog-transport`, ONTAP verifica l'identità dell'host di destinazione convalidandone il certificato. Il valore predefinito è `udp-unencrypted`.

`syslog-port`

Il valore predefinito `syslog-port` il parametro dipende dall'impostazione di `syslog-transport` parametro. Se `syslog-transport` è impostato su `tcp-encrypted`, `syslog-port` ha il valore predefinito 6514.

Per ulteriori informazioni, vedere `event notification destination create` pagina man.

Fasi

1. Creare una destinazione del server syslog per eventi importanti:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   A partire da ONTAP 9.12.1, è possibile specificare i seguenti valori per `syslog-transport`:

   - `udp-unencrypted` - User Datagram Protocol senza sicurezza
   - `tcp-unencrypted` – Transmission Control Protocol senza sicurezza
   - `tcp-encrypted` - Transmission Control Protocol con Transport Layer Security (TLS)

   Il protocollo predefinito è `udp-unencrypted`.

2. Configurare gli eventi importanti per inoltrare le notifiche al server syslog:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

Configurare i traphost SNMP per ricevere le notifiche degli eventi

Per ricevere le notifiche degli eventi su un host trapSNMP, è necessario configurare un host traphost.

Di cosa hai bisogno

- I trap SNMP e SNMP devono essere attivati sul cluster.

  I trap SNMP e SNMP sono attivati per impostazione predefinita.

- Il DNS deve essere configurato sul cluster per risolvere i nomi degli host trapezoidali.

A proposito di questa attività

Se non si dispone già di un host trapSNMP configurato per ricevere notifiche di eventi (trap SNMP), è necessario aggiungerne uno.

È possibile eseguire questa attività ogni volta che il cluster è in esecuzione immettendo i comandi nella riga di comando ONTAP.

Fase

1. Se l'ambiente non dispone già di un host trapSNMP configurato per ricevere le notifiche degli eventi, aggiungerne uno:

   ```
   system snmp traphost add -peer-address snmp_traphost_name
   ```

   Tutte le notifiche degli eventi supportate da SNMP per impostazione predefinita vengono inoltrate all'host principale SNMP.

Configurare eventi EMS importanti per inoltrare le notifiche a un'applicazione webhook

È possibile configurare ONTAP per inoltrare notifiche di eventi importanti a un'applicazione webhook. I passaggi necessari per la configurazione dipendono dal livello di sicurezza scelto.

Prepararsi a configurare l'inoltro degli eventi EMS

Prima di configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook, è necessario prendere in considerazione diversi concetti e requisiti.

Applicazione Webhook

È necessaria un'applicazione webhook in grado di ricevere le notifiche degli eventi ONTAP. Un webhook è una routine di callback definita dall'utente che estende le funzionalità dell'applicazione o del server remoto in cui viene eseguito. I webhook vengono chiamati o attivati dal client (in questo caso ONTAP) inviando una richiesta HTTP all'URL di destinazione. In particolare, ONTAP invia una richiesta HTTP POST al server che ospita l'applicazione webhook insieme ai dettagli della notifica degli eventi formattati in XML.

Opzioni di sicurezza

Sono disponibili diverse opzioni di sicurezza a seconda di come viene utilizzato il protocollo TLS (Transport Layer Security). L'opzione scelta determina la configurazione ONTAP richiesta.

> TLS è un protocollo crittografico ampiamente utilizzato su Internet. Fornisce privacy, integrità dei dati e autenticazione utilizzando uno o più certificati a chiave pubblica. I certificati vengono emessi da autorità di certificazione attendibili.

HTTP

È possibile utilizzare HTTP per trasportare le notifiche degli eventi. Con questa configurazione, la connessione non è sicura. Le identità del client ONTAP e dell'applicazione webhook non vengono verificate. Inoltre, il traffico di rete non viene crittografato o protetto. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTP" per informazioni dettagliate sulla configurazione.

HTTPS

Per una maggiore sicurezza, è possibile installare un certificato sul server che ospita la routine webhook. Il protocollo HTTPS viene utilizzato da ONTAP per verificare l'identità del server applicazioni webhook e da entrambe le parti per garantire la privacy e l'integrità del traffico di rete. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTPS" per informazioni dettagliate sulla configurazione.

HTTPS con autenticazione reciproca

È possibile migliorare ulteriormente la protezione HTTPS installando un certificato client sul sistema ONTAP che invia le richieste del manuale. Oltre a verificare l'identità del server dell'applicazione webhook e

a proteggere il traffico di rete, ONTAP verifica l'identità del client ONTAP. Questa autenticazione peer bidirezionale è nota come *Mutual TLS*. Vedere "Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca" per informazioni dettagliate sulla configurazione.

Informazioni correlate

- "Il protocollo TLS (Transport Layer Security) versione 1.3"

Configurare una destinazione webhook per l'utilizzo di HTTP

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTP. Si tratta dell'opzione meno sicura, ma la più semplice da configurare.

Fasi

1. Creare una nuova destinazione `restapi-ems` per ricevere gli eventi:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   Nel comando precedente, è necessario utilizzare lo schema **HTTP** per la destinazione.

2. Creare una notifica che colleghi `important-events` filtrare con `restapi-ems` destinazione:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Configurare una destinazione webhook per l'utilizzo di HTTPS

È possibile configurare ONTAP in modo che inoltri le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete.

Prima di iniziare

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP

Fasi

1. Installare la chiave privata del server e i certificati appropriati sul server che ospita l'applicazione webhook. Le specifiche fasi di configurazione dipendono dal server.
2. Installare il certificato root del server in ONTAP:

   ```
   security certificate install -type server-ca
   ```

   Il comando chiederà il certificato.

3. Creare il `restapi-ems` destinazione per ricevere gli eventi:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

4. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

```
event notification create -filter-name important-events -destinations restapi-
ems
```

Configurare una destinazione webhook per l'utilizzo di HTTPS con autenticazione reciproca

È possibile configurare ONTAP per inoltrare le notifiche degli eventi a un'applicazione webhook utilizzando HTTPS con autenticazione reciproca. Con questa configurazione sono disponibili due certificati. ONTAP utilizza il certificato del server per confermare l'identità dell'applicazione webhook e proteggere il traffico di rete. Inoltre, l'applicazione che ospita il webhook utilizza il certificato client per confermare l'identità del client ONTAP.

Prima di iniziare

Prima di configurare ONTAP, è necessario effettuare le seguenti operazioni:

- Generare una chiave privata e un certificato per il server applicazioni webhook
- Disporre del certificato root per l'installazione in ONTAP
- Generare una chiave privata e un certificato per il client ONTAP

Fasi

1. Eseguire le prime due fasi dell'attività "Configurare una destinazione webhook per l'utilizzo di HTTPS" Per installare il certificato del server in modo che ONTAP possa verificare l'identità del server.
2. Installare i certificati root e intermedi appropriati nell'applicazione webhook per convalidare il certificato client.
3. Installare il certificato client in ONTAP:

   ```
   security certificate install -type client
   ```

   Il comando richiede la chiave privata e il certificato.

4. Creare il `restapi-ems` destinazione per ricevere gli eventi:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   Nel comando precedente, è necessario utilizzare lo schema **HTTPS** per la destinazione.

5. Creare la notifica che collega `important-events` filtra con il nuovo `restapi-ems` destinazione:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

Aggiornare la mappatura degli eventi EMS obsoleta

Modelli di mappatura degli eventi EMS

Prima di ONTAP 9.0, gli eventi EMS potevano essere mappati solo alle destinazioni degli eventi in base alla corrispondenza del modello di nome dell'evento. Il comando ONTAP viene impostato (`event destination`, `event route`) Che utilizzano questo modello

continuano a essere disponibili nelle ultime versioni di ONTAP, ma sono state deprecate a partire da ONTAP 9.0.

A partire da ONTAP 9.0, la Best practice per il mapping della destinazione degli eventi EMS di ONTAP consiste nell'utilizzare il modello di filtro eventi più scalabile in cui la corrispondenza dei modelli viene eseguita su più campi, utilizzando l' `event filter`, `event notification`, e. `event notification destination` set di comandi.

Se la mappatura EMS è configurata utilizzando i comandi non aggiornati, aggiornare la mappatura per utilizzare `event filter`, `event notification`, e. `event notification destination` set di comandi.

Esistono due tipi di destinazioni degli eventi:

1. **Destinazioni generate dal sistema**: Esistono cinque destinazioni di eventi generate dal sistema (create per impostazione predefinita)
   - `allevents`
   - `asup`
   - `criticals`
   - `pager`
   - `traphost`

     Alcune destinazioni generate dal sistema sono destinate a scopi speciali. Ad esempio, la destinazione asup instrada gli eventi callhome.* al modulo AutoSupport in ONTAP per generare messaggi AutoSupport.
2. **Destinazioni create dall'utente**: Vengono create manualmente utilizzando `event destination create` comando.

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

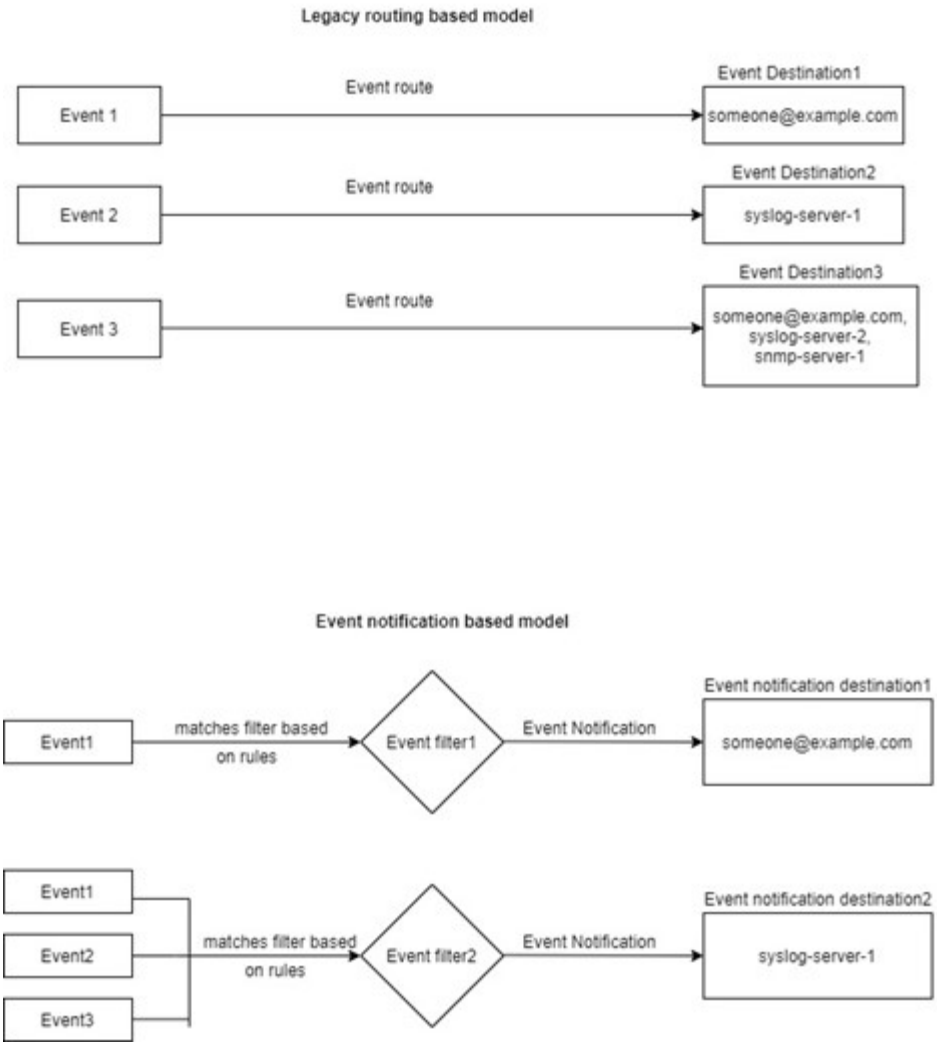
Nel modello obsoleto, gli eventi EMS vengono mappati singolarmente a una destinazione utilizzando `event route add-destinations` comando.

```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

Il nuovo meccanismo di notifica degli eventi EMS, più scalabile, si basa sui filtri degli eventi e sulle destinazioni di notifica degli eventi. Fare riferimento al seguente articolo della Knowledge base per informazioni dettagliate sul nuovo meccanismo di notifica degli eventi:

- "Panoramica del sistema di gestione degli eventi per ONTAP 9"



Aggiornare la mappatura degli eventi EMS dai comandi ONTAP non aggiornati

Se la mappatura degli eventi EMS è attualmente configurata utilizzando i set di comandi ONTAP deprecati (`event destination`, `event route`), seguire questa procedura per aggiornare la mappatura per utilizzare `event filter`, `event notification`, e. `event notification destination` set di comandi.

Fasi

1. Elencare tutte le destinazioni degli eventi nel sistema utilizzando `event destination show` comando.

```
cluster-1::event*> destination show

Hide
Name             Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents        -                 -                  -
false
asup             -                 -                  -
false
criticals        -                 -                  -
false
pager            -                 -                  -
false
test             test@xyz.com      -                  -
false
traphost         -                 -                  -
false
6 entries were displayed.
```

2. Per ciascuna destinazione, elencare gli eventi associati utilizzando `event route show -destinations <destination name>` comando.

```
cluster-1::event*> route show -destinations test
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

3. Creare un corrispondente `event filter` che include tutti questi sottoinsiemi di eventi. Ad esempio, se si desidera includere solo il `raid.aggr.*` eventi, utilizzare un carattere jolly per `message-name` quando si crea il filtro. È inoltre possibile creare filtri per singoli eventi.

   È possibile creare fino a 50 filtri per eventi.

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. Creare un `event notification destination` per ciascuno di `event destination` Endpoint (ad esempio, SMTP/SNMP/syslog)

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

5. Creare una notifica degli eventi mappando il filtro degli eventi alla destinazione di notifica degli eventi.

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. Ripetere i punti 1-5 per ciascuno `event destination` questo ha un `event route` mappatura.

Gli eventi instradati alle destinazioni SNMP devono essere mappati a. `snmp-traphost` destinazione della notifica degli eventi. La destinazione SNMP traphost utilizza l'host SNMP traphost configurato dal sistema.

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

               Destination Name: snmp-traphost
             Type of Destination: snmp
                     Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```