# Monitorare e gestire le performance del cluster utilizzando la CLI

ONTAP 9

NetApp
April 24, 2024

# Sommario

# 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**

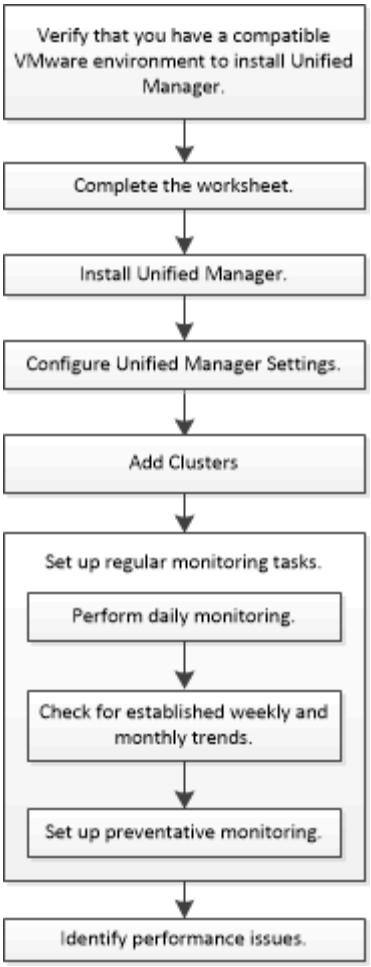
Se questi presupposti non sono corretti per la situazione, dovresti vedere le seguenti risorse:

- "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<br>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.

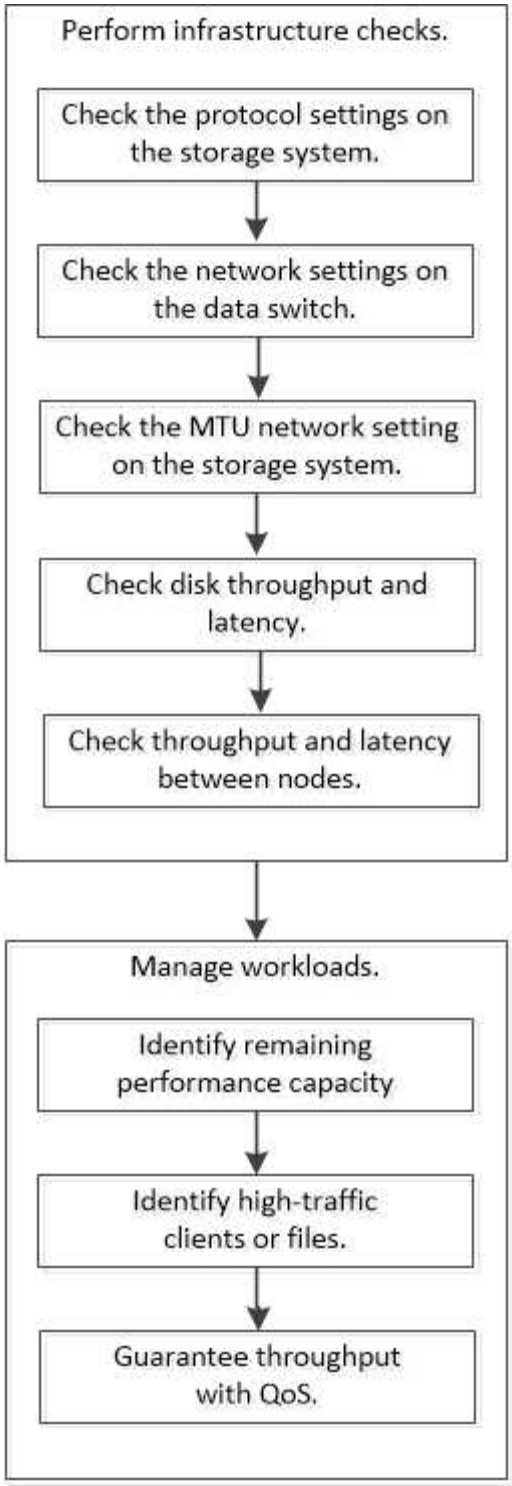
**Informazioni correlate**

- "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

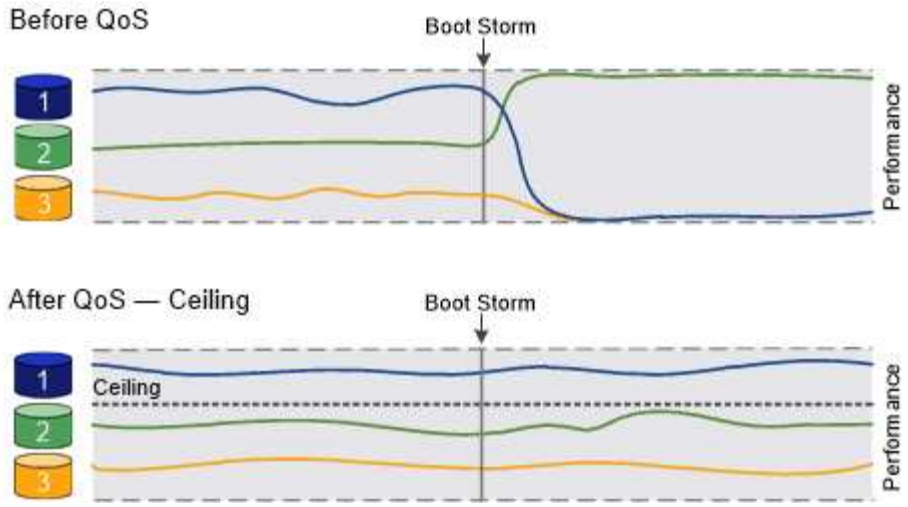
È possibile utilizzare la qualità del servizio (QoS) dello storage per garantire che le performance dei carichi di lavoro critici non vengano degradate dai carichi di lavoro concorrenti. È possibile impostare un *soffitto* di throughput su un carico di lavoro concorrente per limitarne l'impatto sulle 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)**

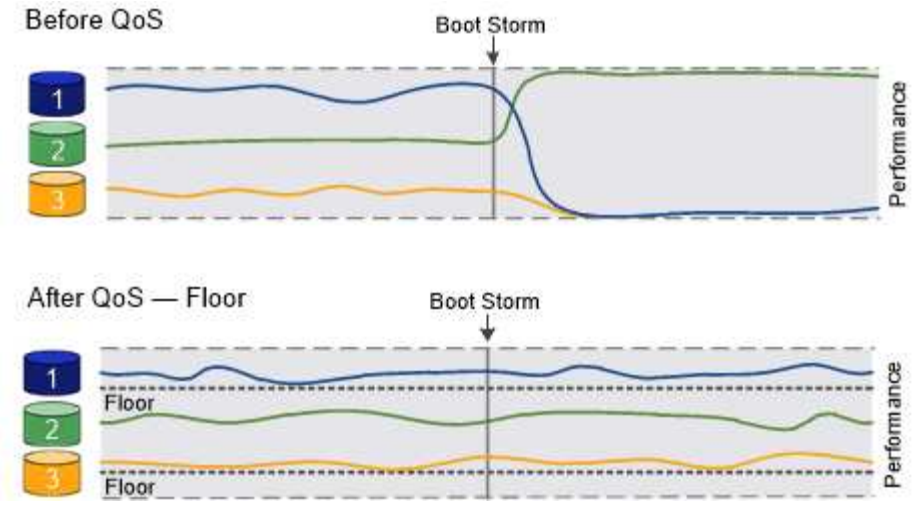
Un piano di throughput garantisce che il throughput per un carico di lavoro non scenda al di sotto di un numero minimo di IOPS o Mbps o IOPS e Mbps. Nella figura riportata di seguito, i livelli di throughput per il carico di lavoro 1 e il carico di lavoro 3 garantiscono il raggiungimento degli obiettivi 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<br>• C190 *<br>• ONTAP Select premium con SSD * | • AFF<br>• C190<br>• 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.

  ```
  `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.

  `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`