



Impostare e configurare Keystone

Keystone

NetApp
September 09, 2024

Sommario

- Impostare e configurare Keystone 1
 - Requisiti 1
 - Installare Keystone Collector 7
 - Configurare Keystone Collector 11
 - Configura AutoSupport per Keystone 19
 - Sicurezza di Keystone Collector 20
 - Tipi di dati utente raccolti da Keystone 21

Impostare e configurare Keystone

Requisiti

Requisiti dell'infrastruttura virtuale

Prima di poter installare Keystone Collector, il tuo sistema VMware vSphere deve soddisfare diversi requisiti.

Prerequisiti per la macchina virtuale del server Keystone Collector:

- Sistema operativo: Server VMware vCenter e ESXi 6.7 o versione successiva
- Core: 1 CPU
- RAM: 2 GB DI RAM
- Spazio su disco: Disco virtuale da 20 GB

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

I requisiti di rete di Keystone Collector sono elencati nella seguente tabella.



Keystone Collector richiede la connettività a Internet. È possibile fornire la connettività a Internet tramite il routing diretto tramite il gateway predefinito (via NAT) o il proxy HTTP. Entrambe le varianti sono descritte qui.

Origine	Destinazione	Servizio	Protocollo e porte	Categoria	Scopo
Keystone Collector (per Keystone ONTAP)	Active IQ Unified Manager (gestore unificato)	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone ONTAP)	Raccolta di metriche sull'utilizzo di Keystone Collector per ONTAP
Keystone Collector (per Keystone StorageGRID)	Nodi di amministrazione StorageGRID	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone StorageGRID)	Raccolta di metriche sull'utilizzo di Keystone Collector per StorageGRID

Keystone Collector (generico)	Internet (in base ai requisiti URL forniti in seguito)	HTTPS	TCP 80, TCP 443	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche
Keystone Collector (generico)	Proxy HTTP del cliente	Proxy HTTP	Porta proxy del cliente	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche
Keystone Collector (generico)	Server DNS del cliente	DNS	TCP/UDP 53	Obbligatorio	Risoluzione DNS
Keystone Collector (generico)	Server NTP del cliente	NTP	UDP 123	Obbligatorio	Sincronizzazione dell'ora
Keystone Collector (per Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funzionalità opzionale	Raccolta di metriche delle performance per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 7777	Funzionalità opzionale	Reporting sullo stato di salute di Keystone Collector
Workstation operative del cliente	Keystone Collector	SSH	TCP 22	Gestione	Accesso a Keystone Collector Management
Indirizzi di gestione di cluster e nodi NetApp ONTAP	Keystone Collector	HTTP_8000, PING	TCP 8000, richiesta/risposta eco ICMP	Funzionalità opzionale	Webserver per gli aggiornamenti del firmware ONTAP



La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante una nuova installazione di Unified Manager, che impedisce la raccolta delle metriche di performance per Keystone Collector. Per ulteriori informazioni, vedere "[Requisiti ONTAP](#)".

Accesso all'URL

Keystone Collector deve accedere ai seguenti host Internet:

Indirizzo	Motivo
https://keystone.netapp.com	Aggiornamenti software e report sull'utilizzo di Keystone Collector
https://support.netapp.com	NetApp HQ per informazioni di fatturazione e consegna AutoSupport

Requisiti di sistema per Linux

La preparazione del sistema Linux con il software richiesto garantisce un'installazione e una raccolta di dati precisi da parte di Keystone Collector.

Assicurati che la tua VM del server di raccolta Linux e Keystone disponga di queste configurazioni.

Server Linux:

- Sistema operativo: CentOS 7 o Red Hat Enterprise Linux 8.6 o versione successiva
- Tempo cronyd sincronizzato
- Accesso ai repository software Linux standard

Lo stesso server deve avere anche i seguenti pacchetti di terze parti:

- Podman (gestore POD)
- sos
- cronic
- python 3 (da 3.6.8 a 3.9.13)

Macchina virtuale del server collettore di Keystone:

- Core: 2 CPU
- RAM: 4 GB DI RAM
- Spazio su disco: Disco virtuale da 50 GB

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

I requisiti di rete di Keystone Collector sono elencati nella seguente tabella.



Keystone Collector richiede la connettività a Internet. È possibile fornire la connettività a Internet tramite il routing diretto tramite il gateway predefinito (via NAT) o il proxy HTTP. Entrambe le varianti sono descritte qui.

Origine	Destinazione	Servizio	Protocollo e porte	Categoria	Scopo
Keystone Collector (per Keystone ONTAP)	Active IQ Unified Manager (gestore unificato)	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone ONTAP)	Raccolta di metriche sull'utilizzo di Keystone Collector per ONTAP
Keystone Collector (per Keystone StorageGRID)	Nodi di amministrazione StorageGRID	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone StorageGRID)	Raccolta di metriche sull'utilizzo di Keystone Collector per StorageGRID
Keystone Collector (generico)	Internet (in base ai requisiti URL forniti in seguito)	HTTPS	TCP 80, TCP 443	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche
Keystone Collector (generico)	Proxy HTTP del cliente	Proxy HTTP	Porta proxy del cliente	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche
Keystone Collector (generico)	Server DNS del cliente	DNS	TCP/UDP 53	Obbligatorio	Risoluzione DNS
Keystone Collector (generico)	Server NTP del cliente	NTP	UDP 123	Obbligatorio	Sincronizzazione dell'ora

Keystone Collector (per Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funzionalità opzionale	Raccolta di metriche delle performance per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 7777	Funzionalità opzionale	Reporting sullo stato di salute di Keystone Collector
Workstation operative del cliente	Keystone Collector	SSH	TCP 22	Gestione	Accesso a Keystone Collector Management
Indirizzi di gestione di cluster e nodi NetApp ONTAP	Keystone Collector	HTTP_8000, PING	TCP 8000, richiesta/risposta e ICMP	Funzionalità opzionale	Webserver per gli aggiornamenti del firmware ONTAP



La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante una nuova installazione di Unified Manager, che impedisce la raccolta delle metriche di performance per Keystone Collector. Per ulteriori informazioni, vedere "[Requisiti ONTAP](#)".

Accesso all'URL

Keystone Collector deve accedere ai seguenti host Internet:

Indirizzo	Motivo
https://keystone.netapp.com	Aggiornamenti software e report sull'utilizzo di Keystone Collector
https://support.netapp.com	NetApp HQ per informazioni di fatturazione e consegna AutoSupport

Requisiti per ONTAP e StorageGRID

Prima di iniziare con Keystone, devi assicurarti che i cluster ONTAP e i sistemi StorageGRID soddisfino alcuni requisiti.

ONTAP

Versioni software

1. ONTAP 9,8 o versione successiva
2. Active IQ Unified Manager (Unified Manager) 9,10 o versione successiva

Prima di iniziare

1. Verificare che Unified Manager 9,10 o versione successiva sia configurato. Per informazioni sull'installazione di Unified Manager, consultare i seguenti collegamenti:
 - ["Installazione di Unified Manager su sistemi VMware vSphere"](#)
 - ["Installazione di Unified Manager su sistemi Linux"](#)
2. Assicurarsi che il cluster ONTAP sia stato aggiunto a Unified Manager. Per informazioni sull'aggiunta di cluster, vedere ["Aggiunta di cluster"](#).
3. Creare utenti di Unified Manager con ruoli specifici per la raccolta di dati relativi a utilizzo e performance. Eseguire questa procedura. Per informazioni sui ruoli utente, vedere ["Definizioni dei ruoli utente"](#).
 - a. Accedere all'interfaccia utente Web di Unified Manager con le credenziali utente predefinite dell'amministratore dell'applicazione generate durante l'installazione. Vedere ["Accesso all'interfaccia utente Web di Unified Manager"](#).
 - b. Creare un account di servizio per Keystone Collector con `Operator` ruolo dell'utente. Le API del servizio Keystone Collector utilizzano questo account di servizio per comunicare con Unified Manager e raccogliere i dati di utilizzo. Vedere ["Aggiunta di utenti"](#).
 - c. Creare un Database account utente, con `Report Schema` ruolo. Questo utente è necessario per la raccolta dei dati sulle performance. Vedere ["Creazione di un utente di database"](#).



La porta predefinita per MySQL, 3306, è limitata solo all'host locale durante una nuova installazione di Unified Manager, il che impedisce la raccolta dei dati di performance per Keystone ONTAP. È possibile modificare questa configurazione e rendere la connessione disponibile ad altri host utilizzando l'opzione presente `Control access to MySQL port 3306` nella console di manutenzione di Unified Manager. Per informazioni, vedere ["Opzioni di menu aggiuntive"](#).

4. Abilitare API Gateway in Unified Manager. Keystone Collector utilizza la funzione di gateway API per comunicare con i cluster ONTAP. È possibile attivare API Gateway dall'interfaccia utente Web o eseguendo alcuni comandi tramite Unified Manager CLI.

Interfaccia utente Web

Per abilitare API Gateway dall'interfaccia utente Web di Unified Manager, accedere all'interfaccia utente Web di Unified Manager e abilitare API Gateway. Per ulteriori informazioni, vedere ["Abilitazione di API Gateway"](#).

CLI

Per abilitare API Gateway tramite Unified Manager CLI, attenersi alla seguente procedura:

- a. Sul server Unified Manager, avviare una sessione SSH e accedere a Unified Manager CLI.
``um cli login -u <umadmin>`` Per informazioni sui comandi CLI, vedere ["Comandi CLI di Unified Manager supportati"](#).
- b. Verificare che il gateway API sia già abilitato.

`um option list api.gateway.enabled`R `true` Valore indica che il gateway API è attivato.

c. Se il valore restituito è `false`, eseguire questo comando:

`um option set api.gateway.enabled=true`

d. Riavviare il server Unified Manager:

- Linux: ["Riavvio di Unified Manager"](#).
- VMware vSphere: ["Riavvio della macchina virtuale di Unified Manager"](#).

StorageGRID

Per installare Keystone Collector su StorageGRID sono necessarie le seguenti configurazioni.

- StorageGRID 11.6.0 o versioni successive. Per informazioni sull'aggiornamento di StorageGRID, vedere ["Aggiornamento del software StorageGRID: Panoramica"](#).
- Per la raccolta dei dati di utilizzo, è necessario creare un account utente amministratore locale di StorageGRID. Questo account di servizio viene utilizzato dal servizio di raccolta Keystone per comunicare con StorageGRID tramite API del nodo amministratore.

Fasi

- a. Accedere a Grid Manager. Vedere ["Accedi a Grid Manager"](#).
- b. Creare un gruppo di amministratori locale con `Access mode: Read-only`. Vedere ["Creare un gruppo di amministratori"](#).
- c. Aggiungere le seguenti autorizzazioni:
 - Account tenant
 - Manutenzione
 - Query metriche
- d. Creare un utente dell'account del servizio Keystone e associarlo al gruppo di amministratori. Vedere ["Gestire gli utenti"](#).

Installare Keystone Collector

Implementare Keystone Collector su sistemi VMware vSphere

L'implementazione di Keystone Collector su sistemi VMware vSphere include il download del modello OVA, l'implementazione del modello mediante la procedura guidata **Deploy OVF Template**, la verifica dell'integrità dei certificati e la verifica della preparazione della macchina virtuale.

Implementazione del modello OVA

Attenersi alla seguente procedura:

Fasi

1. Scaricare il file OVA da ["questo link"](#) E memorizzarlo sul sistema VMware vSphere.
2. Sul sistema VMware vSphere, accedere alla vista **macchine virtuali e modelli**.
3. Fare clic con il pulsante destro del mouse sulla cartella desiderata per la macchina virtuale (VM) (o il data

center, se non si utilizzano cartelle VM) e selezionare **Deploy OVF Template** (implementa modello OVF).

4. Nella *fase 1* della procedura guidata **Deploy OVF Template**, fare clic su **Select and OVF template** (Seleziona e modello OVF) per selezionare il modello scaricato `KeystoneCollector-latest.ova` file.
5. Al *passaggio 2*, specificare il nome della macchina virtuale e selezionare la cartella della macchina virtuale.
6. Nel *passaggio 3*, specificare la risorsa di calcolo richiesta per l'esecuzione della macchina virtuale.
7. Al *passaggio 4: Verifica dei dettagli*, verifica la correttezza e l'autenticità del file OVA.

Le versioni di vCenter precedenti al 7.0u2 non sono in grado di verificare automaticamente l'autenticità del certificato con firma del codice. VCenter 7.0u2 e versioni successive possono eseguire le verifiche; tuttavia, a tale scopo, l'autorità di certificazione della firma deve essere aggiunta a vCenter. Seguire queste istruzioni per la versione di vCenter in uso:

VCenter 7.0u1 e versioni precedenti: Ulteriori informazioni

VCenter convalida l'integrità del contenuto del file OVA e fornisce un digest valido per la firma del codice per i file contenuti nel file OVA. Tuttavia, non convalida l'autenticità del certificato con firma del codice. Per verificare l'integrità, devi scaricare il certificato digest completo della firma e verificarlo rispetto al certificato pubblico pubblicato da Keystone.

- a. Fare clic sul collegamento **Publisher** per scaricare il certificato di digest completo della firma.
- b. Scarica il certificato pubblico di fatturazione Keystone da "[questo link](#)".
- c. Verificare l'autenticità del certificato di firma OVA rispetto al certificato pubblico utilizzando

OpenSSL:

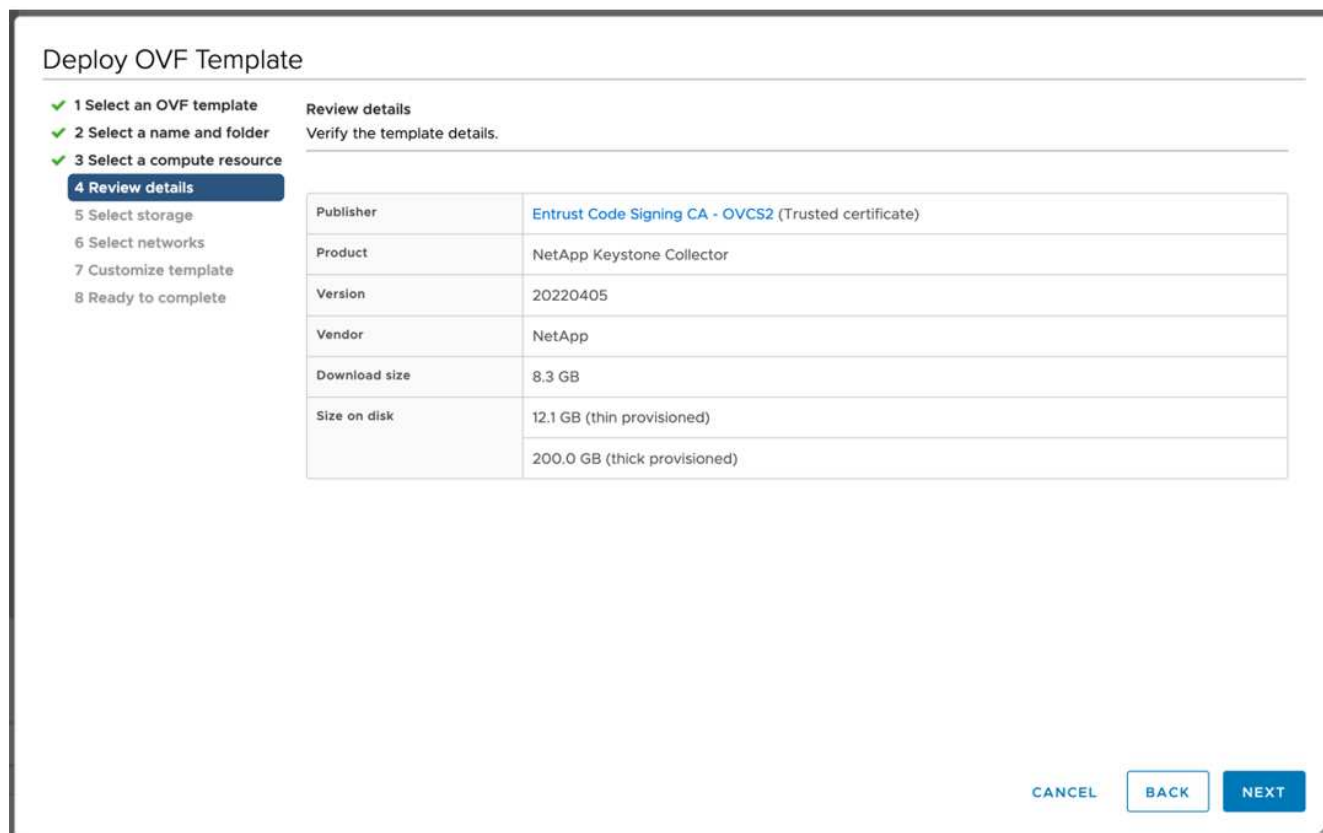
```
openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert
```

VCenter 7.0u2 e versioni successive: Ulteriori informazioni

7.0u2 e le versioni successive di vCenter sono in grado di validare l'integrità del contenuto del file OVA e l'autenticità del certificato di firma del codice, quando viene fornito un digest valido per la firma del codice. L'archivio root trust vCenter contiene solo certificati VMware. NetApp utilizza Entrust come autorità di certificazione e tali certificati devono essere aggiunti all'archivio di fiducia di vCenter.

- a. Scaricare il certificato CA con firma codice da Entrust "[qui](#)".
- b. Seguire la procedura descritta in *Resolution* Sezione di questo articolo della Knowledge base (KB): <https://kb.vmware.com/s/article/84240>.

Una volta convalidate l'integrità e l'autenticità di Keystone Collector OVA, è possibile visualizzare il testo (Trusted certificate) con l'editore.



8. Nella *fase 5* della procedura guidata **Deploy OVF Template**, specificare la posizione in cui memorizzare la macchina virtuale.
9. Nel *passaggio 6*, selezionare la rete di destinazione per la macchina virtuale da utilizzare.
10. Nella sezione *fase 7 personalizzare il modello*, specificare l'indirizzo di rete e la password iniziali per l'account utente amministratore.



La password amministratore è memorizzata in un formato reversibile in vCentre e deve essere utilizzata come credenziale di bootstrap per ottenere l'accesso iniziale al sistema VMware vSphere. Durante la configurazione iniziale del software, è necessario modificare questa password di amministrazione. La subnet mask dell'indirizzo IPv4 deve essere fornita con la notazione CIDR. Ad esempio, utilizzare il valore 24 per una subnet mask di 255.255.255.0.

11. Nella *fase 8 Pronto per il completamento* della procedura guidata **Deploy OVF Template**, esaminare la configurazione e verificare di aver impostato correttamente i parametri per l'implementazione di OVA.

Una volta implementata la macchina virtuale dal modello e accesa, aprire una sessione SSH sulla macchina virtuale e accedere con le credenziali amministrative temporanee per verificare che sia pronta per la configurazione.

Configurazione iniziale del sistema

Eseguire questi passaggi sui sistemi VMware vSphere per una configurazione iniziale dei server Keystone Collector implementati tramite OVA:



Una volta completata la distribuzione, è possibile utilizzare l'utility Keystone Collector Management Terminal User Interface (TUI) per eseguire le attività di configurazione e monitoraggio. Per selezionare le opzioni e spostarsi all'interno dell'interfaccia telefonica utente, è possibile utilizzare diversi comandi della tastiera, ad esempio i tasti Invio e freccia.

1. Aprire una sessione SSH sul server di Keystone Collector. Quando si effettua la connessione, il sistema richiede di aggiornare la password dell'amministratore. Completare l'aggiornamento della password amministratore come richiesto.
2. Accedere utilizzando la nuova password per accedere all'interfaccia telefonica utente. All'accesso, viene visualizzata l'interfaccia telefonica utente (TUI).

In alternativa, è possibile avviarlo manualmente eseguendo il `keystone-collector-tui` Comando CLI.

3. Se necessario, configurare i dettagli del proxy nella sezione **Configurazione > rete** dell'interfaccia telefonica utente.
4. Configurare il nome host, la posizione e il server NTP del sistema nella sezione **Configurazione > sistema**.
5. Aggiornare Keystone Collector utilizzando l'opzione **manutenzione > Aggiorna Collector**. Dopo l'aggiornamento, riavviare l'utility Keystone Collector management TUI per applicare le modifiche.

Installare Keystone Collector su sistemi Linux

Il software Keystone Collector è distribuito da un repository di software YUM online. È necessario importare e installare il file su un server Linux.

Per installare il software sul server Linux, procedere come segue:

1. SSH al server di Keystone Collector e passare a `root` privilegio.
2. Importare la firma pubblica Keystone:

```
# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101
```
3. Verificare che sia stato importato il certificato pubblico corretto controllando l'impronta digitale per Keystone Billing Platform nel database RPM:

```
# rpm -qa gpg-pubkey --qf '%<Description>' | gpg --show-keys --fingerprint
```

L'impronta digitale corretta è simile al seguente:
90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D
4. Scaricare il `kestonerepo.rpm` file:

```
curl -O https://keystone.netapp.com/repo/kestonerepo.rpm
```
5. Verificare l'autenticità del file:

```
rpm --checksig -v kestonerepo.rpm`Una firma per un file autentico è simile a questa:  
`Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK
```
6. Installare il file repository del software YUM:

```
# yum install kestonerepo.rpm
```
7. Una volta installato Keystone repo, installare il pacchetto `keystone-collector` tramite YUM Package Manager:

```
# yum install keystone-collector
```



Una volta completata l'installazione, è possibile utilizzare l'utility Keystone Collector Management Terminal User Interface (TUI) per eseguire le attività di configurazione e monitoraggio. Per selezionare le opzioni e spostarsi all'interno dell'interfaccia telefonica utente, è possibile utilizzare diversi comandi della tastiera, ad esempio i tasti Invio e freccia. Vedere ["Configurare Keystone Collector"](#) e ["Monitorare lo stato del sistema"](#) per informazioni.

Convalida automatica del software Keystone

Il repository Keystone è configurato per convalidare automaticamente l'integrità del software Keystone in modo che venga installato presso la tua sede solo software valido e autentico.

La configurazione del client del repository Keystone YUM fornita in `keystonerepo.rpm` utilizza il controllo GPG forzato (`gpgcheck=1`) su tutto il software scaricato attraverso questo repository. Qualsiasi RPM scaricato attraverso il repository Keystone che non supera la convalida della firma non può essere installato. Questa funzionalità viene utilizzata nella funzionalità di aggiornamento automatico pianificato di Keystone Collector per garantire che nel sito sia installato solo software valido e autentico.

Configurare Keystone Collector

È necessario completare alcune attività di configurazione per consentire a Keystone Collector di raccogliere i dati di utilizzo nell'ambiente di storage. Si tratta di un'attività una tantum che consente di attivare e associare i componenti richiesti al tuo ambiente di storage.



Keystone Collector offre l'utility Keystone Collector Management Terminal User Interface (TUI) per eseguire le attività di configurazione e monitoraggio. Per selezionare le opzioni e spostarsi all'interno dell'interfaccia telefonica utente, è possibile utilizzare diversi comandi della tastiera, ad esempio i tasti Invio e freccia.

Fasi

1. Avviare l'utility TUI di gestione di Keystone Collector:

```
$ keystone-collector-tui
```
2. Accedere a **Configura > KS-Collector** per aprire la schermata di configurazione di Keystone Collector e visualizzare le opzioni disponibili per l'aggiornamento.
3. Aggiornare le opzioni richieste.

 FOR ONTAP

- **Collect ONTAP Use:** Questa opzione consente di raccogliere i dati di utilizzo per ONTAP. Aggiungere i dettagli del server Active IQ Unified Manager (Unified Manager) e dell'account di servizio.
- **Collect ONTAP dati sulle prestazioni:** Questa opzione consente la raccolta di dati sulle performance per ONTAP. Questa opzione è disattivata per impostazione predefinita. Attivare questa opzione se il monitoraggio delle performance è richiesto nel proprio ambiente per scopi SLA. Fornire i dettagli dell'account utente di Unified Manager Database. Per informazioni sulla creazione di utenti di database, vedere "[Creare utenti di Unified Manager](#)".
- **Remove Private Data (Rimuovi dati privati):** Questa opzione rimuove dati privati specifici dei clienti ed è attivata per impostazione predefinita. Per informazioni sui dati esclusi dalle metriche se questa opzione è attivata, vedere "[Limita la raccolta di dati privati](#)".

 FOR StorageGRFunded

- **Collect StorageGRID Use (Raccogli utilizzo nodo):** Questa opzione consente di raccogliere i dettagli sull'utilizzo del nodo. Aggiungere l'indirizzo del nodo StorageGRID e i dettagli dell'utente.
- **Remove Private Data (Rimuovi dati privati):** Questa opzione rimuove dati privati specifici dei clienti ed è attivata per impostazione predefinita. Per informazioni sui dati esclusi dalle metriche se questa opzione è attivata, vedere "[Limita la raccolta di dati privati](#)".

4. Attivare il campo **Avvia KS-Collector con sistema**.

5. Fare clic su **Salva**

```
NetApp Keystone Collector - Configure - KS Collector
[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:          123.123.123.123
AIQUM Username:        collector-user
AIQUM Password:        -----
[X] Collect StorageGRID usage
StorageGRID Address:   sgadminnode.address
StorageGRID Username:  collector-user
StorageGRID Password:  -----
[X] Collect ONTAP Performance Data
AIQUM Database Username: sla-reporter
AIQUM Database Password: -----
[X] Remove Private Data
Mode                   Standard
Logging Level          info
                       Tunables
                       Save
                       Clear Config
                       Back
```

6. Assicurarsi che Keystone Collector sia in buono stato tornando alla schermata principale dell'interfaccia telefonica utente e verificando le informazioni **Stato del servizio**. Il sistema dovrebbe mostrare che i servizi sono in uno stato **generale: Sano**

```
Service Status
Overall: Healthy
UM: Running
chronyd: Running
ks-collector: Running
```

7. Uscire dalla TUI di gestione di Keystone Collector selezionando l'opzione **Esci dalla shell** nella schermata iniziale.

Configurare il proxy HTTP su Keystone Collector

Il software Collector supporta l'utilizzo di un proxy HTTP per comunicare con Internet. Questa opzione può essere configurata nell'interfaccia telefonica utente (TUI).

Fasi

1. Riavviare l'utility TUI di gestione di Keystone Collector, se già chiusa:
`$ keystone-collector-tui`
2. Attivare il campo **Proxy HTTP** e aggiungere i dettagli relativi al server proxy HTTP, alla porta e alle credenziali, se è richiesta l'autenticazione.
3. Fare clic su **Salva**

```
NetApp Keystone Collector - Configure - Network
[X] HTTP Proxy
Proxy Server Address: example_proxy_server
Proxy Server Port: 8088
[ ] Proxy Auth
Proxy Username:
Proxy Password:
Save
Back
```

Limita la raccolta di dati privati

Keystone Collector raccoglie informazioni limitate relative a configurazione, stato e performance per eseguire la misurazione delle iscrizioni. È possibile limitare ulteriormente le informazioni raccolte mascherando le informazioni sensibili dal contenuto caricato. Ciò non influisce sul calcolo della fatturazione. Tuttavia, la limitazione delle informazioni potrebbe influire sull'usabilità delle informazioni di reporting, poiché alcuni elementi, facilmente identificabili dagli utenti, come il nome del volume, vengono sostituiti con UUID.

La limitazione della raccolta di dati specifici del cliente è un'opzione configurabile nella schermata TUI di Keystone Collector. Questa opzione, **Rimuovi dati privati**, è attivata per impostazione predefinita.

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:      123.123.123.123
AIQUM Username:    collector
AIQUM Password:    -----
[ ] Collect StorageGRID usage

[ ] Collect ONTAP Performance Data

[X] Remove Private Data
Mode                Standard
Logging Level      info
                   Tunables
                   Save
                   Clear Config
                   Back
```

Per informazioni sugli elementi rimossi per limitare l'accesso privato ai dati in ONTAP e StorageGRID, vedere ["Elenco degli elementi rimossi in caso di limitazione dell'accesso ai dati privati"](#).

Considerare attendibile una CA principale personalizzata

La verifica dei certificati rispetto a un'autorità di certificazione pubblica di origine (CA) fa parte delle funzionalità di protezione di Keystone Collector. Tuttavia, se necessario, è possibile configurare Keystone Collector in modo che consideri attendibile una CA principale personalizzata.

Se si utilizza l'ispezione SSL/TLS nel firewall di sistema, il traffico basato su Internet viene ricodificato con il certificato CA personalizzato. È necessario configurare le impostazioni per verificare l'origine come CA attendibile prima di accettare il certificato di origine e consentire le connessioni. Attenersi alla seguente procedura:

Fasi

1. Preparare il certificato CA. Dovrebbe essere in formato di file X.509_ codificato in base64.



Le estensioni file supportate sono .pem, .crt, .cert. Verificare che il certificato sia in uno di questi formati.

2. Copiare il certificato nel server Keystone Collector. Prendere nota della posizione in cui viene copiato il file.
3. Aprire un terminale sul server ed eseguire l'utilità TUI di gestione.
`$ keystone-collector-tui`
4. Andare a **Configurazione > Avanzate**.
5. Attivare l'opzione **attiva certificato root personalizzato**.
6. Per **selezionare il percorso personalizzato del certificato di origine:**, selezionare `- Unset -`
7. Premere Invio. Viene visualizzata una finestra di dialogo per la selezione del percorso del certificato.
8. Selezionare il certificato di origine dal browser del file system o immettere il percorso esatto.
9. Premere Invio. Viene nuovamente visualizzata la schermata **Avanzate**.
10. Selezionare **Salva**. La configurazione viene applicata.

```
NetApp Keystone Collector - Configure - Advanced
[ ] Darksite Mode
[X] TLS Verify on Connections to Internet
[X] Enable custom root certificate
Select custom root certificate path:
    - Unset -
[X] Finished Initial OVA Install
[X] Collector Auto-Update
Override Collector Images
Save
Back
```

Crea livelli di servizio delle performance

È possibile creare livelli di servizio delle performance (PSL) utilizzando l'utilità TUI di gestione del Collector Keystone. La creazione di PSL tramite l'interfaccia telefonica utente seleziona automaticamente i valori predefiniti impostati per ciascun livello di servizio, riducendo la possibilità di errori che potrebbero verificarsi quando si impostano manualmente questi valori durante la creazione di PSL tramite Active IQ Unified Manager.

Per ulteriori informazioni sui PSL, fare riferimento alla sezione ["Performance livelli di servizio"](#).

Per ulteriori informazioni sui livelli di servizio, fare riferimento a "[Livelli di servizio in Keystone](#)".

Fasi

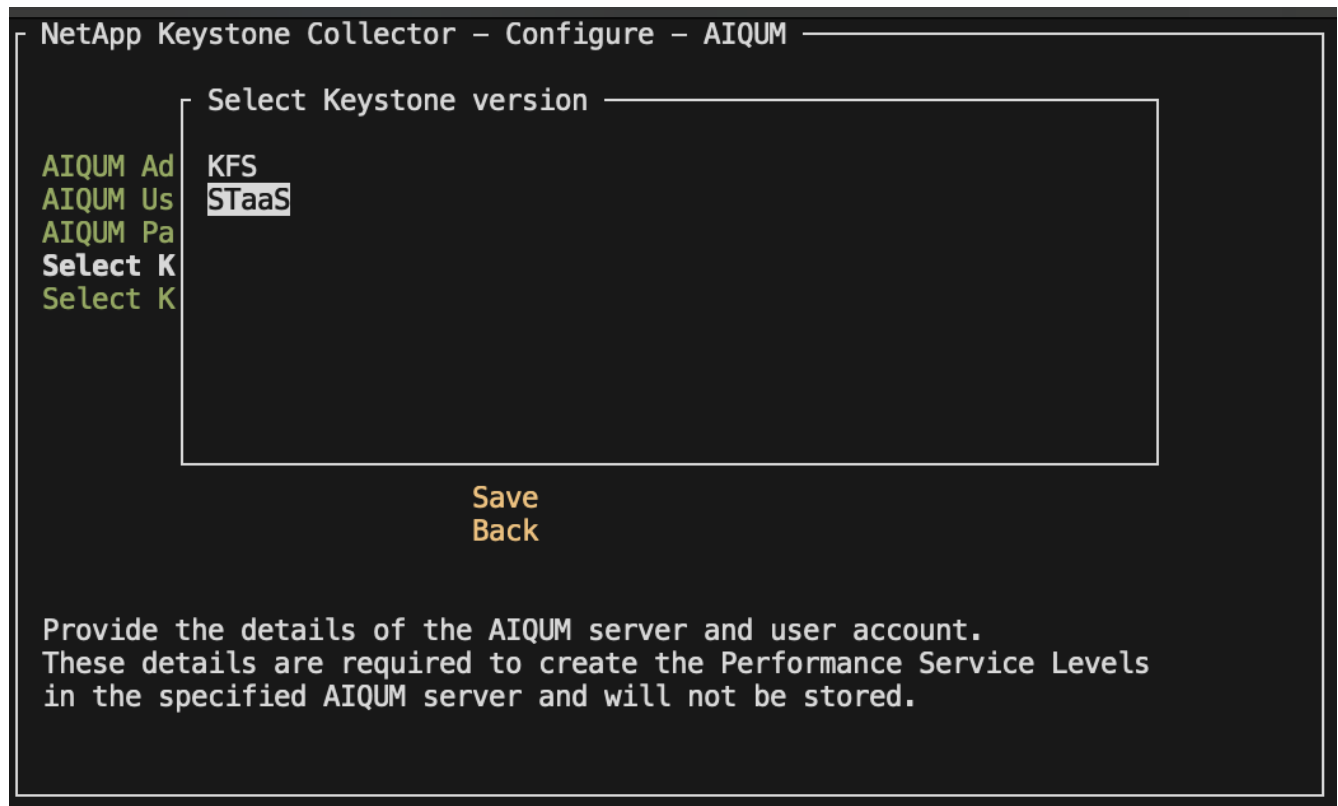
1. Avviare l'utilità TUI di gestione di Keystone Collector:
\$ keystone-collector-tui
2. Andare a **Configure>AIQUM** per aprire la schermata AIQUM.
3. Attivare l'opzione **Crea profili prestazioni AIQUM**.
4. Immettere i dettagli del server Active IQ Unified Manager e dell'account utente. Questi dettagli sono necessari per creare PSL e non verranno memorizzati.

```
NetApp Keystone Collector - Configure - AIQUM
[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles
AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version          -unset-
Select Keystone Service Levels

Save
Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```

5. Per **Seleziona versione Keystone**, selezionare `-unset-`.
6. Premere Invio. Viene visualizzata una finestra di dialogo per la selezione della versione Keystone.
7. Evidenziare **STaaS** per specificare la versione Keystone per Keystone STaaS, quindi premere Invio.



È possibile evidenziare l'opzione **KFS** per i servizi di abbonamento Keystone versione 1. I servizi di iscrizione Keystone sono diversi da Keystone STaaS per quanto riguarda i livelli di servizio, le offerte di servizio e i principi di fatturazione. Per ulteriori informazioni, fare riferimento a "[Servizi di iscrizione Keystone | versione 1](#)".

8. Tutti i livelli di servizio Keystone supportati verranno visualizzati all'interno dell'opzione **Select Keystone Service Levels** per la versione Keystone specificata. Attivare i livelli di servizio desiderati dall'elenco.

```
NetApp Keystone Collector - Configure - AIQUM
[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles
AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version
Select Keystone Service Levels
-----
STaaS
[X] Extreme
[X] Premium
[ ] Performance
[ ] Standard
[ ] Value

Save
Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```




Puoi selezionare più livelli di servizio simultaneamente per creare PSL.





9. Selezionare **Salva** e premere Invio. Verranno creati i livelli di servizio delle prestazioni.




Puoi visualizzare gli elenchi di gestione dei dati creati, come Premium-KS-STaaS per STaaS o Extreme KFS per KFS, nella pagina **livelli di servizio delle performance** in Active IQ Unified Manager. Se i PSL creati non soddisfano i requisiti, è possibile modificare i PSL in base alle proprie esigenze. Per ulteriori informazioni, fare riferimento a ["Creazione e modifica dei livelli di Performance Service"](#).

Performance Service Levels

View and manage the Performance Service Levels that you can assign to workloads.

Search Performance Service Levels  Filter

 Add  Modify  Remove 

<input type="checkbox"/>	Name ^	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
	Extreme - KFS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
	Extreme - KS-STaaS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
Overview								
		Description	Extreme - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					
	Premium ...S-STaaS	User-defined	2048	4096	500	2	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
Overview								
		Description	Premium - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					

Se esiste già un PSL per il livello di servizio selezionato sul server Active IQ Unified Manager specificato, non è possibile crearlo di nuovo. Se si tenta di farlo, viene visualizzato un messaggio di errore.

```
NetApp Keystone Collector - Configure - AIQUM

Warning
-----
AIQUM Ad Failed to create Performance Service Level for:
AIQUM Us Extreme. Error: <Response [400]>
AIQUM Pa
Select K
Select K

OK

> Save <
  Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```

Configura AutoSupport per Keystone

Quando si utilizza il meccanismo telemetrico di AutoSupport, Keystone calcola l'utilizzo in base ai dati telemetrici di AutoSupport. Per raggiungere il livello necessario di granularità,

È necessario configurare AutoSupport in modo da incorporare i dati Keystone nei bundle di supporto giornaliero inviati dai cluster ONTAP.

A proposito di questa attività

Prima di configurare AutoSupport in modo da includere i dati Keystone, devi prendere nota di quanto segue.

- È possibile modificare le opzioni di telemetria di AutoSupport utilizzando l'interfaccia CLI di ONTAP. Per informazioni sulla gestione dei servizi AutoSupport e del ruolo di amministratore del sistema (cluster), vedere ["Panoramica di Manage AutoSupport"](#) e ["Amministratori di cluster e SVM"](#).
- Includere i sottosistemi nei pacchetti AutoSupport giornalieri e settimanali per garantire una raccolta precisa dei dati per Keystone. Per informazioni sui sottosistemi AutoSupport, vedere ["Che cosa sono i sottosistemi AutoSupport"](#).

Fasi

1. Come utente di amministratore di sistema, effettuare l'accesso al cluster Keystone ONTAP utilizzando SSH. Per ulteriori informazioni, vedere ["Accedere al cluster utilizzando SSH"](#).
2. Modificare il contenuto del registro.
 - Eseguire questo comando per modificare il contenuto quotidiano del registro:

```
autosupport trigger modify -node * -autosupport-message  
management.log -basic-additional  
waf1,performance,snapshot,platform,object_store_server,san,raid,snapm  
irror -troubleshooting-additional waf1
```

- Eseguire questo comando per modificare il contenuto del registro settimanale:

```
autosupport trigger modify -autosupport-message weekly  
-troubleshooting-additional waf1 -node *
```

Per ulteriori informazioni su questo comando, vedere ["modifica trigger AutoSupport nodo di sistema"](#).

Sicurezza di Keystone Collector

Keystone Collector include funzionalità di sicurezza che monitorano le metriche di performance e utilizzo dei sistemi Keystone, senza rischiare la sicurezza dei dati dei clienti.

Il funzionamento di Keystone Collector si basa sui seguenti principi di sicurezza:

- **Privacy by design**-Keystone Collector raccoglie i dati minimi per eseguire la misurazione dell'utilizzo e il monitoraggio delle prestazioni. Per ulteriori informazioni, vedere ["Dati raccolti per la fatturazione"](#). Il ["Rimuovi dati privati"](#) l'opzione è attivata per impostazione predefinita, che maschera e protegge le informazioni riservate.
- **Accesso con privilegi minimi**-Keystone Collector richiede autorizzazioni minime per monitorare i sistemi di storage, minimizzando i rischi per la sicurezza e impedendo qualsiasi modifica involontaria dei dati. Questo approccio è in linea con il principio del minimo privilegio, migliorando la sicurezza generale degli

ambienti monitorati.

- **Framework di sviluppo software sicuro-** Keystone utilizza un framework di sviluppo software sicuro durante tutto il ciclo di sviluppo, che riduce i rischi, riduce le vulnerabilità e protegge il sistema da potenziali minacce.

Protezione avanzata

Per impostazione predefinita, Keystone Collector è configurato per l'utilizzo di configurazioni ottimizzate per la sicurezza. Di seguito sono riportate le configurazioni di protezione consigliate:

- Il sistema operativo della macchina virtuale Keystone Collector:
 - Conforme allo standard CIS Debian Linux 12 Benchmark. Apportare modifiche alla configurazione del sistema operativo al di fuori del software di gestione Keystone Collector può ridurre la sicurezza del sistema. Per ulteriori informazioni, vedere ["Guida al benchmark CIS"](#).
 - Riceve e installa automaticamente le patch di sicurezza verificate da Keystone Collector tramite la funzionalità di aggiornamento automatico. La disattivazione di questa funzionalità può causare la mancata applicazione di patch al software vulnerabile.
 - Autentica gli aggiornamenti ricevuti da Keystone Collector. La disattivazione della verifica del repository APT può portare all'installazione automatica di patch non autorizzate, introducendo potenzialmente delle vulnerabilità.
- Keystone Collector convalida automaticamente i certificati HTTPS per garantire la sicurezza della connessione. La disattivazione di questa funzione può comportare la rappresentazione di endpoint esterni e la perdita di dati sull'utilizzo.
- Keystone Collector supporta ["CA attendibile personalizzata"](#) certificazione. Per impostazione predefinita, considera attendibili i certificati firmati dalle CA principali pubbliche riconosciute da ["Programma di certificazione Mozilla CA"](#). Attivando altre CA attendibili, Keystone Collector abilita la convalida del certificato HTTPS per le connessioni agli endpoint che presentano tali certificati.
- Keystone Collector abilita l'opzione **Rimuovi dati privati** per impostazione predefinita, che maschera e protegge le informazioni riservate. Per ulteriori informazioni, vedere ["Limita la raccolta di dati privati"](#). La disattivazione di questa opzione comporta la comunicazione di dati aggiuntivi al sistema Keystone. Ad esempio, può includere le informazioni immesse dall'utente, ad esempio i nomi dei volumi, che possono essere considerati informazioni sensibili.

Informazioni correlate

- ["Panoramica di Keystone Collector"](#)
- ["Requisiti dell'infrastruttura virtuale"](#)
- ["Configurare Keystone Collector"](#)

Tipi di dati utente raccolti da Keystone

Keystone raccoglie informazioni sulla configurazione, sullo stato e sull'utilizzo per i tuoi abbonamenti Keystone ONTAP e Keystone StorageGRID. Può anche raccogliere i dati sulle prestazioni solo per ONTAP, se l'opzione è attivata in Keystone Collector.

Raccolta di dati ONTAP

** - dati raccolti per ONTAP: Scopri la tecnologia **

Il seguente elenco è un esempio rappresentativo dei dati sul consumo di capacità raccolti per ONTAP:

- Cluster
 - ClusterUID
 - Nome cluster
 - Numero di serie
 - Posizione (in base all'input di valore nel cluster ONTAP)
 - Contatto
 - Versione
- Nodi
 - Numero di serie
 - Nome del nodo
- Volumi
 - Nome dell'aggregato
 - Volume Name (Nome volume)
 - VolumeInstanceUID
 - Flag IsCloneVolume
 - Flag IsFlexGroupConstituent
 - Flag IsSpaceEnforcementLogical
 - Flag IsSpaceReportingLogical
 - LogicalSpaceUsedByAfs
 - PercentSnapshotSpace
 - PerformanceTierInactiveUserData
 - PerformanceTierInactiveUserDataPercent
 - QoSAdaptivePolicyNome del gruppo
 - QoSPolicyGroup Name
 - Dimensione
 - Utilizzato
 - PhysicalUsed
 - SizeUsedBySnapshot
 - Tipo
 - VolumeStyleExtended
 - Nome del server virtuale
 - Flag IsVsRoot
- VServer
 - VserverName

- VserverUID
- Sottotipo
- Aggregati di storage
 - StorageType
 - Nome aggregato
 - UUID aggregato
- Aggregare gli archivi di oggetti
 - ObjectStoreName
 - ObjectStoreUID
 - ProviderType
 - Nome aggregato
- Clonare i volumi
 - FlexClone
 - Dimensione
 - Utilizzato
 - Server virtuale
 - Tipo
 - ParentVolume
 - ParentVserver
 - IsConstituent
 - SplitEstimate
 - Stato
 - FlexCloneUsedPercent
- LUN dello storage
 - UUID LUN
 - LUN Name (Nome LUN)
 - Dimensione
 - Utilizzato
 - Allarme isriservato
 - Flag IsRequested
 - LogicalUnit Name (Nome unità logica)
 - QoSPolicyUID
 - QoSPolicyName
 - VolumeUID
 - VolumeName
 - SVMUID
 - Nome SVM

- Volumi di storage
 - VolumeInstanceUID
 - VolumeName
 - Nome SVMName
 - SVMUID
 - QoSPolicyUID
 - QoSPolicyName
 - CapacityTierFootprint
 - PerformanceTierFootprint
 - TotalFootprint
 - Policy di tieringPolicy
 - Flag IsProtected
 - Flag ISDestination
 - Utilizzato
 - PhysicalUsed
 - UID CloneParentUID
 - LogicalSpaceUsedByAfs
- Gruppi di policy QoS
 - PolicyGroup
 - QoSPolicyUID
 - MaxThroughput
 - MinThroughput
 - MaxThroughputIOPS
 - MaxThroughputMBps
 - MinThroughputIOPS
 - MinThroughputMBps
 - Flag IsShared
- Gruppi di criteri QoS adattivi ONTAP
 - QoSPolicyName
 - QoSPolicyUID
 - PeakIOPS
 - PeakIOPSAllocation
 - AbsoluteMinIOPS
 - ExpectedIOPS
 - ExpectedIOPSAllocation
 - Dimensione blocco
- Impronte

- Server virtuale
- Volume
- TotalFootprint
- VolumeBlocksFootprintBin0
- VolumeBlocksFootprintBin1
- Cluster MetroCluster
 - ClusterUID
 - Nome cluster
 - RemoteClusterUID
 - RemoteClusterName
 - LocalConfigurationState
 - RemoteConfigurationState
 - Modalità
- Metriche di osservabilità del collettore
 - Tempo di raccolta
 - Endpoint API Active IQ Unified Manager interrogato
 - Tempi di risposta
 - Numero di record
 - IP istanza AIQUMInstance
 - ID istanza CollectorInstance

** - dati raccolti per ONTAP: Scopri la tecnologia **

Il seguente elenco è un esempio rappresentativo dei dati sulle performance raccolti per ONTAP:

- Nome cluster
- UUID cluster
- ObjectID (ID oggetto)
- VolumeName
- UUID istanza volume
- Server virtuale
- VserverUID
- Nodo seriale
- ONTAPVersion
- Versione di AIQUM
- Aggregato
- AggregateUID
- ResourceKey
- Data e ora
- IOPSPerTb
- Latenza
- ReadLatency
- WriteMBps
- QoSMinThroughputLatency
- QoSNBladeLatency
- UsedHeadRoom
- CacheMissRatio
- OtherLatency
- QoSAggregateLatency
- IOPS
- QoSNetworkLatency
- AvailableOps
- WriteLatency
- QoSCLoudLatency
- QoSClusterInterconnectLatency
- OtherMBps
- QoSCopLatency
- QoSDBladeLatency
- Utilizzo

- ReadIOPS
- Mbps
- OtherIOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncSnapmirrorLatency
- WriteIOPS

Rimozione di un numero di elementi in seguito alla limitazione dell'accesso ai dati privati: Scopri il più discontinuo

Quando l'opzione **Rimuovi dati privati** è attivata in Keystone Collector, le seguenti informazioni di utilizzo vengono eliminate per ONTAP. Questa opzione è attivata per impostazione predefinita.

- Nome cluster
- Ubicazione del cluster
- Contatto del cluster
- Nome del nodo
- Nome dell'aggregato
- Volume Name (Nome volume)
- QoSAdaptivePolicyNome del gruppo
- QoSPolicyGroup Name
- Nome del server virtuale
- Nome del LUN dello storage
- Nome aggregato
- LogicalUnit Name (Nome unità logica)
- Nome SVM
- IP istanza AIQUMInstance
- FlexClone
- RemoteClusterName

Raccolta di dati StorageGRID

** - dati raccolti per StorageGRID: Scopri la tecnologia **

L'elenco seguente è un esempio rappresentativo di `Logical Data` Raccolti per StorageGRID:

- ID StorageGRID
- ID account
- Nome account
- Byte di quota account
- Nome bucket
- Conteggio oggetti bucket
- Byte di dati bucket

L'elenco seguente è un esempio rappresentativo di `Physical Data` Raccolti per StorageGRID:

- ID StorageGRID
- ID nodo
- ID sito
- Nome del sito
- Istanza
- Byte di utilizzo dello storage StorageGRID
- Byte di metadati per l'utilizzo dello storage StorageGRID

Rimozione di un numero di elementi in seguito alla limitazione dell'accesso ai dati privati: Scopri il più discontinuo

Quando l'opzione **Rimuovi dati privati** è attivata in Keystone Collector, le seguenti informazioni di utilizzo vengono eliminate per StorageGRID. Questa opzione è attivata per impostazione predefinita.

- Nome account
- Nome BucketName
- Nome del sito
- Instance/nodename

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.