Impostare e configurare Keystone

Keystone

NetApp
January 15, 2026

Sommario

Impostare e configurare Keystone

Requisiti

Requisiti dell'infrastruttura virtuale per Keystone Collector

Per poter installare Keystone Collector, il sistema VMware vSphere deve soddisfare diversi requisiti.

Prerequisiti per la VM del server Keystone Collector:

- Sistema operativo: VMware vCenter Server ed ESXi 8.0 o versioni successive
- Nucleo: 1 CPU
- Memoria RAM: 2 GB di RAM
- Spazio su disco: 20 GB vDisk

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

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

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

Fonte	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 di utilizzo di Keystone Collector per ONTAP
Keystone Collector (per Keystone StorageGRID)	Nodi amministrativi StorageGRID	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone StorageGRID)	Raccolta di metriche di utilizzo di Keystone Collector per StorageGRID

Keystone Collector (generico)	Internet (secondo i requisiti URL forniti in seguito)	HTTPS	TCP 443	Obbligatorio (connettività internet)	Software Keystone Collector, aggiornamenti del sistema operativo e caricamento delle metriche
Keystone Collector (generico)	Proxy HTTP del cliente	Proxy HTTP	Porta proxy cliente	Obbligatorio (connettività internet)	Software Keystone Collector, aggiornamenti del sistema operativo e caricamento delle 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 oraria
Keystone Collector (per Keystone ONTAP)	Gestore unificato	MYSQL	TCP 3306	Funzionalità facoltativa	Raccolta di metriche di prestazione per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 7777	Funzionalità facoltativa	Segnalazione dello stato di salute di Keystone Collector
Postazioni di lavoro operative del cliente	Collezionista Keystone	SSH	TCP 22	Gestione	Accesso alla gestione Keystone Collector
Indirizzi di gestione dei nodi e dei cluster NetApp ONTAP	Collezionista Keystone	HTTP_8000, PING	TCP 8000, richiesta/risposta eco ICMP	Funzionalità facoltativa	Webserver per gli aggiornamenti del firmware ONTAP

La porta predefinita per MySQL, 3306, è limitata solo a localhost durante una nuova installazione di Unified Manager, il che impedisce la raccolta di metriche sulle prestazioni per Keystone Collector. Per ulteriori informazioni, consultare "Requisiti ONTAP" .

Accesso URL

Keystone Collector necessita dell'accesso ai seguenti host Internet:

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

Requisiti Linux per Keystone Collector

Preparando il sistema Linux con il software necessario si garantisce un'installazione e una raccolta dati precise da parte di Keystone Collector.

Assicurati che la tua VM del server Linux e Keystone Collector abbia queste configurazioni.

Server Linux:

- Sistema operativo: uno qualsiasi dei seguenti:
  - Debian 12
  - Red Hat Enterprise Linux 8.6 o versioni successive 8.x
  - Red Hat Enterprise Linux 9.0 o versioni successive
  - CentOS 7 (solo per ambienti esistenti)
- Tempo di sincronizzazione Chronyd
- Accesso ai repository software standard di Linux

Lo stesso server dovrebbe disporre anche dei seguenti pacchetti di terze parti:

- podman (gestore POD)
- sos
- cronia
- python 3 (da 3.9.14 a 3.11.8)

VM del server Keystone Collector:

- Core: 2 CPU
- Memoria RAM: 4 GB di RAM
- Spazio su disco: 50 GB vDisk

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

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

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

Fonte	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 di utilizzo di Keystone Collector per ONTAP
Keystone Collector (per Keystone StorageGRID)	Nodi amministrativi StorageGRID	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone StorageGRID)	Raccolta di metriche di utilizzo di Keystone Collector per StorageGRID
Keystone Collector (generico)	Internet (secondo i requisiti URL forniti in seguito)	HTTPS	TCP 443	Obbligatorio (connettività internet)	Software Keystone Collector, aggiornamenti del sistema operativo e caricamento delle metriche
Keystone Collector (generico)	Proxy HTTP del cliente	Proxy HTTP	Porta proxy cliente	Obbligatorio (connettività internet)	Software Keystone Collector, aggiornamenti del sistema operativo e caricamento delle 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 oraria
Keystone Collector (per Keystone ONTAP)	Gestore unificato	MYSQL	TCP 3306	Funzionalità facoltativa	Raccolta di metriche di prestazione per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 7777	Funzionalità facoltativa	Segnalazione dello stato di salute di Keystone Collector
Postazioni di lavoro operative del cliente	Collezionista Keystone	SSH	TCP 22	Gestione	Accesso alla gestione Keystone Collector
Indirizzi di gestione dei nodi e dei cluster NetApp ONTAP	Collezionista Keystone	HTTP_8000, PING	TCP 8000, richiesta/risposta eco ICMP	Funzionalità facoltativa	Webserver per gli aggiornamenti del firmware ONTAP

La porta predefinita per MySQL, 3306, è limitata solo a localhost durante una nuova installazione di Unified Manager, il che impedisce la raccolta di metriche sulle prestazioni per Keystone Collector. Per ulteriori informazioni, consultare "Requisiti ONTAP" .

Accesso URL

Keystone Collector necessita dell'accesso ai seguenti host Internet:

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

Requisiti per ONTAP e StorageGRID per Keystone

Prima di iniziare a utilizzare Keystone, è necessario assicurarsi che i cluster ONTAP e i sistemi StorageGRID soddisfino alcuni requisiti.

ONTAP

Versioni del software

1. ONTAP 9.8 o successivo
2. Active IQ Unified Manager (Unified Manager) 9.10 o successivo

Prima di iniziare

Se si intende raccogliere dati di utilizzo solo tramite ONTAP, soddisfare i seguenti requisiti:

1. Assicurarsi che sia configurato ONTAP 9.8 o versione successiva. Per informazioni sulla configurazione di un nuovo cluster, consultare i seguenti xref:./installation/+
   - "Configurare ONTAP su un nuovo cluster con System Manager"
   - "Configurare un cluster con la CLI"
2. Crea account di accesso ONTAP con ruoli specifici. Per saperne di più, fare riferimento a "Scopri come creare account di accesso ONTAP" .
   - **Interfaccia utente Web**
     i. Accedi a ONTAP System Manager utilizzando le tue credenziali predefinite. Per saperne di più, fare riferimento a "Gestione dei cluster con System Manager" .
     ii. Creare un utente ONTAP con ruolo "readonly" e tipo di applicazione "http" e abilitare l'autenticazione tramite password andando su **Cluster > Impostazioni > Sicurezza > Utenti**.
   - **CLI**
     i. Accedi a ONTAP CLI utilizzando le tue credenziali predefinite. Per saperne di più, fare riferimento a "Gestione dei cluster con CLI" .
     ii. Creare un utente ONTAP con ruolo "readonly" e tipo di applicazione "http" e abilitare l'autenticazione tramite password. Per saperne di più sull'autenticazione, fare riferimento a "Abilita l'accesso alla password dell'account ONTAP" .

Se intendi raccogliere dati di utilizzo tramite Active IQ Unified Manager, soddisfa i seguenti requisiti:

1. Assicurarsi che sia configurato Unified Manager 9.10 o versione successiva. Per informazioni sull'installazione di Unified Manager, consultare i seguenti xref:./installation/+
   - "Installazione di Unified Manager sui 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. Crea utenti Unified Manager con ruoli specifici per la raccolta di dati sull'utilizzo e sulle prestazioni. Eseguire questi passaggi. Per informazioni sui ruoli utente, vedere "Definizioni dei ruoli utente" .
   a. Accedi 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. Crea un account di servizio per Keystone Collector con `Operator` ruolo utente. Le API del servizio Keystone Collector utilizzano questo account di servizio per comunicare con Unified Manager e raccogliere dati di utilizzo. Vedere "Aggiunta di utenti" .
   c. Crea un `Database` account utente, con il `Report Schema` ruolo. Questo utente è necessario per la raccolta dei dati sulle prestazioni. Vedere "Creazione di un utente del database" .

La porta predefinita per MySQL, 3306, è limitata solo a localhost durante una nuova installazione di Unified Manager, il che impedisce la raccolta di dati sulle prestazioni per Keystone ONTAP. Questa configurazione può essere modificata e la connessione può essere resa disponibile ad altri host utilizzando `Control access to MySQL port 3306` opzione nella console di manutenzione di Unified Manager. Per informazioni, vedere"Opzioni di menu aggiuntive" .

4. Abilita API Gateway in Unified Manager. Keystone Collector sfrutta la funzionalità API Gateway per comunicare con i cluster ONTAP . È possibile abilitare API Gateway dall'interfaccia utente Web oppure eseguendo alcuni comandi tramite Unified Manager CLI.

   Interfaccia utente Web

   Per abilitare API Gateway dall'interfaccia utente Web di Unified Manager, accedi all'interfaccia utente Web di Unified Manager e abilita API Gateway. Per informazioni, vedere "Abilitazione dell'API Gateway" .

   Interfaccia a riga di comando

   Per abilitare API Gateway tramite Unified Manager CLI, seguire questi passaggi:

   a. Sul server Unified Manager, avviare una sessione SSH e accedere alla CLI di Unified Manager. `um cli login -u <umadmin>` Per informazioni sui comandi CLI, vedere "Comandi CLI di Unified Manager supportati" .

   b. Verificare se API Gateway è già abilitato. `um option list api.gateway.enabled` UN `true` Il valore indica che l'API Gateway è abilitato.

   c. Se il valore restituito è `false` , esegui 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 Unified Manager" .

StorageGRID

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

- StorageGRID `11.6.0` o versione successiva dovrebbe essere installata. Per informazioni sull'aggiornamento di StorageGRID, vedere"Aggiorna il software StorageGRID : Panoramica" .
- Per la raccolta dei dati di utilizzo è necessario creare un account utente amministratore locale StorageGRID . Questo account di servizio viene utilizzato dal servizio Keystone Collector per comunicare con StorageGRID tramite le API del nodo amministratore.

  Passi

  a. Accedi a Grid Manager. Vedere "Sign in a Grid Manager" .

  b. Crea un gruppo di amministratori locali con `Access mode: Read-only` . Vedere "Crea un gruppo di amministratori" .

  c. Aggiungere le seguenti autorizzazioni:

     - Conti degli inquilini
     - Manutenzione
     - Query sulle metriche

d. Creare un utente con account di servizio Keystone e associarlo al gruppo admin. Vedere "Gestisci utenti" .

Installa Keystone Collector

Distribuisci Keystone Collector sui sistemi VMware vSphere

La distribuzione Keystone Collector sui sistemi VMware vSphere include il download del modello OVA, la distribuzione del modello tramite la procedura guidata **Distribuisci modello OVF**, la verifica dell'integrità dei certificati e la verifica della prontezza della VM.

Distribuzione del modello OVA

Segui questi passaggi:

Passi

1. Scarica il file OVA da "questo collegamento" e memorizzarlo sul tuo sistema VMware vSphere.
2. Nel sistema VMware vSphere, vai alla vista **VM e modelli**.
3. Fare clic con il pulsante destro del mouse sulla cartella richiesta per la macchina virtuale (VM) (o sul data center, se non si utilizzano cartelle VM) e selezionare **Distribuisci modello OVF**.
4. Nel *Passaggio 1* della procedura guidata **Distribuisci modello OVF**, fai clic su **Seleziona un modello OVF** per selezionare il modello scaricato `KeystoneCollector-latest.ova` file.
5. Nel *Passaggio 2*, specificare il nome della VM e selezionare la cartella della VM.
6. Nel *Passaggio 3*, specificare la risorsa di elaborazione richiesta per eseguire la VM.
7. Nel *Passaggio 4: Verifica i dettagli*, verifica la correttezza e l'autenticità del file OVA.

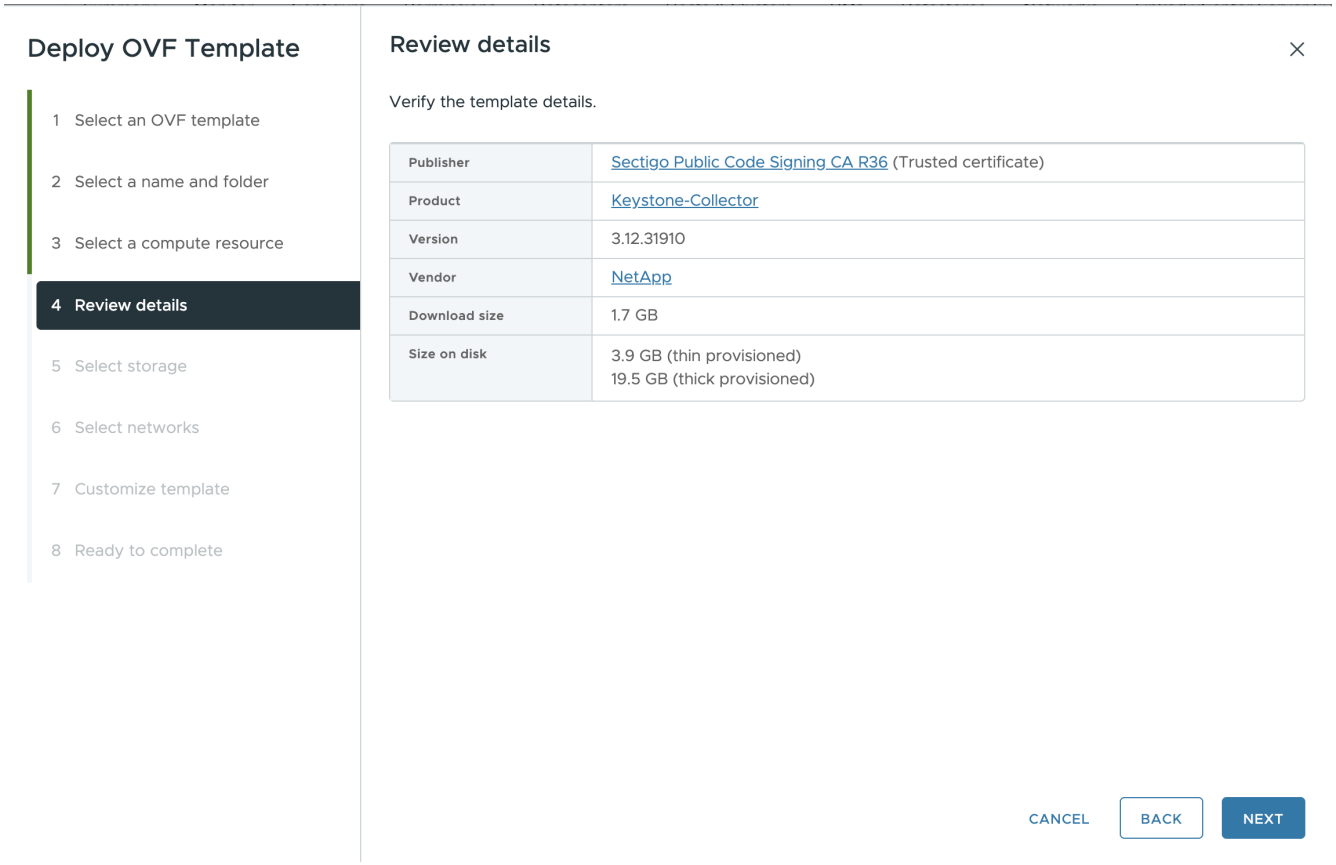
   L'archivio attendibilità radice di vCenter contiene solo certificati VMware. NetApp utilizza Entrust come autorità di certificazione e tali certificati devono essere aggiunti all'archivio attendibile di vCenter.

   a. Scarica il certificato CA di firma del codice da Sectigo "Qui".

   b. Seguire i passaggi nel `Resolution` sezione di questo articolo della knowledge base (KB): https://kb.vmware.com/s/article/84240 .

   > ⓘ Per le versioni vCenter 7.x e precedenti, è necessario aggiornare vCenter ed ESXi alla versione 8.0 o successiva. Le versioni precedenti non sono più supportate.

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



8. Nel *Passaggio 5* della procedura guidata **Distribuisci modello OVF**, specificare la posizione in cui archiviare la VM.
9. Nel *Passaggio 6*, selezionare la rete di destinazione che la VM dovrà utilizzare.
10. Nel *Passaggio 7 Personalizza modello*, specificare l'indirizzo di rete iniziale e la password per l'account utente amministratore.

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

11. Al *Passaggio 8 Pronto per il completamento* della procedura guidata **Distribuisci modello OVF**, rivedere la configurazione e verificare di aver impostato correttamente i parametri per la distribuzione OVA.

Dopo aver distribuito la VM dal modello e averla accesa, aprire una sessione SSH sulla VM e accedere con le credenziali di amministratore temporanee per verificare che la VM sia pronta per la configurazione.

Configurazione iniziale del sistema

Per una configurazione iniziale dei server Keystone Collector distribuiti tramite OVA, eseguire questi passaggi sui sistemi VMware vSphere:

Una volta completata la distribuzione, è possibile utilizzare l'utilità Keystone Collector Management Terminal User Interface (TUI) per eseguire le attività di configurazione e monitoraggio. È possibile utilizzare vari comandi da tastiera, come Invio e i tasti freccia, per selezionare le opzioni e navigare all'interno di questa TUI.

1. Aprire una sessione SSH sul server Keystone Collector. Quando ti connetti, il sistema ti chiederà di aggiornare la password di amministratore. Completare l'aggiornamento della password di amministrazione come richiesto.
2. Accedi utilizzando la nuova password per accedere al TUI. All'accesso viene visualizzata la TUI.

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

3. Se necessario, configurare i dettagli del proxy nella sezione **Configurazione > Rete** sulla TUI.
4. Configurare il nome host del sistema, la posizione e il server NTP nella sezione **Configurazione > Sistema**.
5. Aggiornare i Keystone Collector utilizzando l'opzione **Manutenzione > Aggiorna Collector**. Dopo l'aggiornamento, riavviare l'utilità TUI di gestione Keystone Collector per applicare le modifiche.

Installa Keystone Collector sui sistemi Linux

È possibile installare il software Keystone Collector su un server Linux utilizzando un pacchetto RPM o Debian. Seguire i passaggi di installazione in base alla distribuzione Linux in uso.

Utilizzo di RPM

1. Accedi tramite SSH al server Keystone Collector ed elevalo a `root` privilegio.
2. Importa la firma pubblica Keystone :
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
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 si presenta così:
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Scarica il `keystonerepo.rpm` file:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Verificare l'autenticità del file:
   `rpm --checksig -v keystonerepo.rpm` La firma di un file autentico si presenta così:
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. Installare il file del repository software YUM:
   `# yum install keystonerepo.rpm`
7. Una volta installato il repository Keystone , installare il pacchetto keystone-collector tramite il gestore pacchetti YUM:

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

   Per Red Hat Enterprise Linux 9, eseguire il seguente comando per installare il pacchetto keystone-collector:
   `# yum install keystone-collector-rhel9`

Utilizzo di Debian

1. Accedi tramite SSH al server Keystone Collector ed elevalo a `root` privilegio.
   `sudo su`
2. Scarica il `keystone-sw-repo.deb` file:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Installare il file del repository software Keystone :
   `# dpkg -i keystone-sw-repo.deb`
4. Aggiorna l'elenco dei pacchetti:
   `# apt-get update`
5. Una volta installato il repository Keystone , installare il pacchetto keystone-collector:
   `# apt-get install keystone-collector`

Una volta completata l'installazione, è possibile utilizzare l'utilità Keystone Collector Management Terminal User Interface (TUI) per eseguire le attività di configurazione e monitoraggio. È possibile utilizzare vari comandi da tastiera, come Invio e i tasti freccia, per selezionare le opzioni e navigare all'interno di questa TUI. Vedere"Configura Keystone Collector" E"Monitorare lo stato di salute del sistema" per informazioni.

Validazione automatica del software Keystone

Il repository Keystone è configurato per convalidare automaticamente l'integrità del software Keystone , in modo che nel tuo sito vengano installati solo software validi e autentici.

La configurazione del client del repository Keystone YUM fornita in `keystonerepo.rpm` utilizza il controllo GPG forzato(`gpgcheck=1`) su tutti i software scaricati tramite questo repository. Qualsiasi RPM scaricato tramite il repository Keystone che non supera la convalida della firma non potrà essere installato. Questa funzionalità viene utilizzata nella funzionalità di aggiornamento automatico programmato di Keystone Collector per garantire che nel tuo sito vengano installati solo software validi e autentici.

Configura Keystone Collector

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

- Keystone Collector fornisce l'utilità Keystone Collector Management Terminal User Interface (TUI) per eseguire attività di configurazione e monitoraggio. È possibile utilizzare vari comandi da tastiera, come Invio e i tasti freccia, per selezionare le opzioni e navigare all'interno di questa TUI.
- Keystone Collector può essere configurato per le organizzazioni che non hanno accesso a Internet, anche noto come *dark site* o *modalità privata*. Per saperne di più, fare riferimento a"Keystone in modalità privata" .

Passi

1. Avviare l'utilità TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vai su **Configura > KS-Collector** per aprire la schermata di configurazione di Keystone Collector e visualizzare le opzioni disponibili per l'aggiornamento.
3. Aggiorna le opzioni richieste.

   Per ONTAP

   - *Raccogli utilizzo ONTAP *: questa opzione consente la raccolta dei dati di utilizzo per ONTAP. Aggiungere i dettagli del server Active IQ Unified Manager (Unified Manager) e dell'account di servizio.
   - *Raccogli dati sulle prestazioni ONTAP *: questa opzione consente la raccolta di dati sulle prestazioni per ONTAP. Questa opzione è disabilitata per impostazione predefinita. Abilitare questa opzione se nel proprio ambiente è richiesto il monitoraggio delle prestazioni per scopi SLA. Fornire i dettagli dell'account utente del database Unified Manager. Per informazioni sulla creazione di utenti del database, vedere"Creare utenti Unified Manager" .
   - **Rimuovi dati privati**: questa opzione rimuove specifici dati privati dei clienti ed è abilitata per impostazione predefinita. Per informazioni sui dati esclusi dalle metriche se questa opzione è abilitata, vedere"Limitare la raccolta di dati privati" .

Per StorageGRID

- *Raccogli utilizzo StorageGRID *: questa opzione consente la raccolta dei dettagli sull'utilizzo dei nodi. Aggiungere l'indirizzo del nodo StorageGRID e i dettagli dell'utente.
- **Rimuovi dati privati**: questa opzione rimuove specifici dati privati dei clienti ed è abilitata per impostazione predefinita. Per informazioni sui dati esclusi dalle metriche se questa opzione è abilitata, vedere"Limitare la raccolta di dati privati" .

4. Attivare il campo **Avvia KS-Collector con il sistema**.
5. Fare clic su **Salva**
.

6. Per verificare che Keystone Collector sia in buone condizioni, tornare alla schermata principale della TUI e verificare le informazioni sullo **Stato del servizio**. Il sistema dovrebbe mostrare che i servizi sono in uno stato **Complessivo: Integro**.

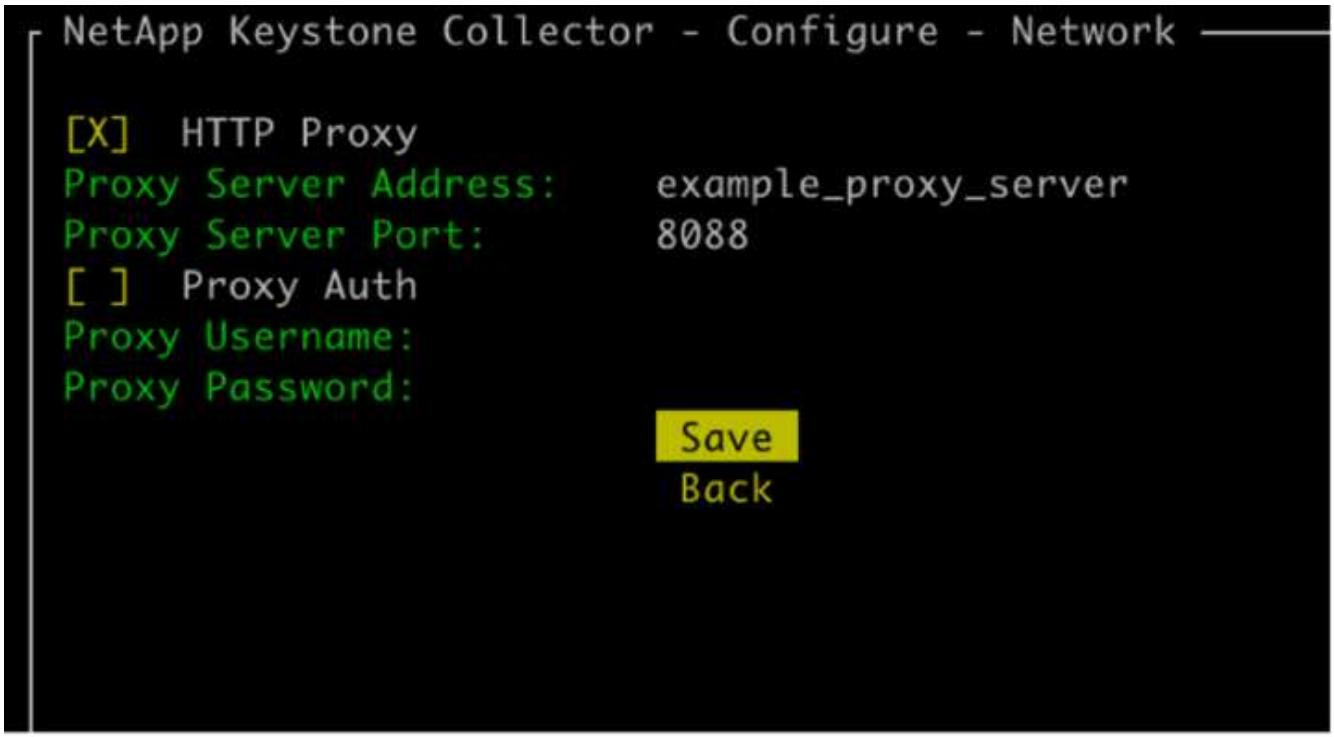
7. Uscire dall'interfaccia utente terminale di gestione Keystone Collector selezionando l'opzione **Esci a Shell** nella schermata iniziale.

Configurare il proxy HTTP su Keystone Collector

Il software Collector supporta l'utilizzo di un proxy HTTP per comunicare con Internet. Questa configurazione può essere effettuata nella TUI.

Passi

1. Riavviare l'utilità TUI di gestione Keystone Collector se già chiusa:
   ```
   $ keystone-collector-tui
   ```
2. Attiva il campo **Proxy HTTP** e aggiungi i dettagli del server proxy HTTP, della porta e delle credenziali, se è richiesta l'autenticazione.
3. Fare clic su **Salva**
   .



Limitare la raccolta di dati privati

Keystone Collector raccoglie informazioni limitate su configurazione, stato e prestazioni, necessarie per eseguire la misurazione degli abbonamenti. Esiste un'opzione per limitare ulteriormente le informazioni raccolte mascherando le informazioni sensibili dai contenuti caricati. Ciò non influisce sul calcolo della fatturazione. Tuttavia, limitare le 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 dei clienti è un'opzione configurabile nella schermata TUI di Keystone Collector. Questa opzione, **Rimuovi dati privati**, è abilitata per impostazione predefinita.

Per informazioni sugli elementi rimossi durante la limitazione dell'accesso ai dati privati in ONTAP e StorageGRID, vedere"Elenco degli elementi rimossi limitando l'accesso ai dati privati" .

Considera attendibile una CA radice personalizzata

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

Se utilizzi l'ispezione SSL/TLS nel firewall del tuo sistema, il traffico basato su Internet verrà nuovamente crittografato con il tuo certificato CA personalizzato. È necessario configurare le impostazioni per verificare la fonte come CA attendibile prima di accettare il certificato radice e consentire le connessioni. Segui questi passaggi:

Passi

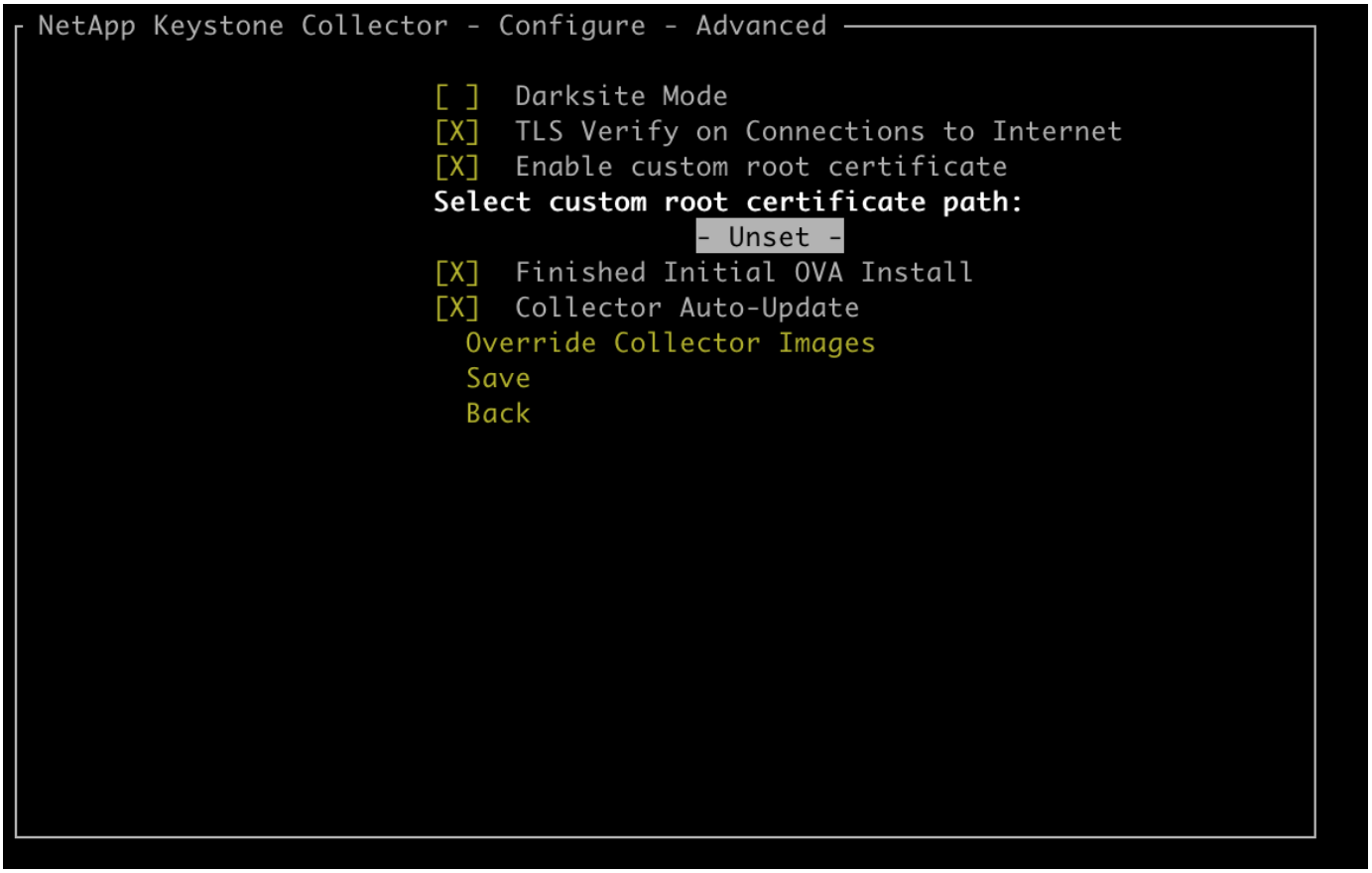
1. Preparare il certificato CA. Dovrebbe essere in formato file X.509 codificato in base64.

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

2. Copiare il certificato sul server Keystone Collector. Prendi nota della posizione in cui viene copiato il file.
3. Aprire un terminale sul server ed eseguire l'utilità di gestione TUI.
   `$ keystone-collector-tui`
4. Vai su **Configurazione > Avanzate**.
5. Abilitare l'opzione **Abilita certificato radice personalizzato**.

6. Per **Seleziona percorso certificato radice personalizzato:**, seleziona `- Unset -`
7. Premere Invio. Viene visualizzata una finestra di dialogo per la selezione del percorso del certificato.
8. Selezionare il certificato radice dal browser del file system oppure immettere il percorso esatto.
9. Premere Invio. Si ritorna alla schermata **Avanzate**.
10. Seleziona **Salva**. La configurazione è applicata.

Il certificato CA viene copiato in `/opt/netapp/ks-collector/ca.pem` sul server Keystone Collector.



Creare livelli di servizio prestazionali

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

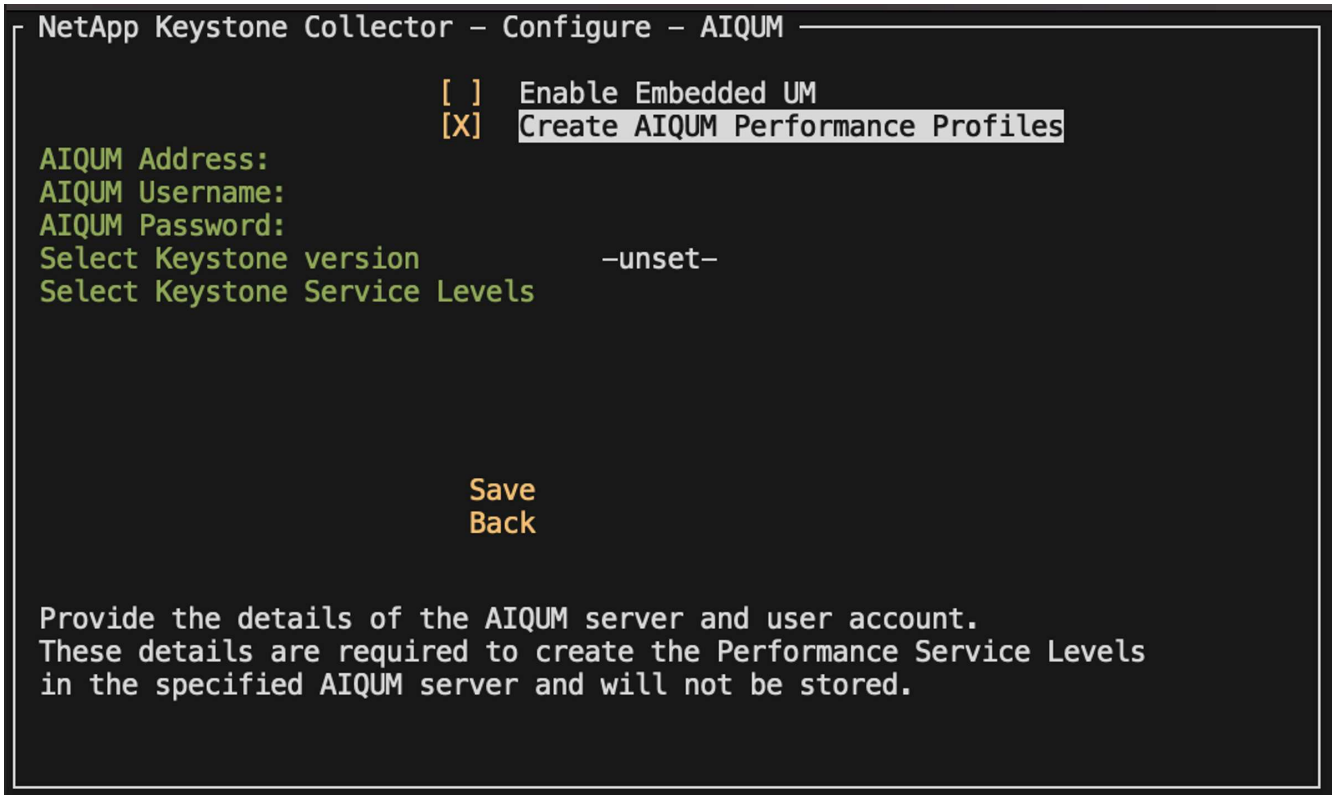
Per saperne di più sui PSL, fare riferimento a"Livelli di servizio prestazionali" .

Per saperne di più sui livelli di servizio, fare riferimento a"Livelli di servizio a Keystone" .

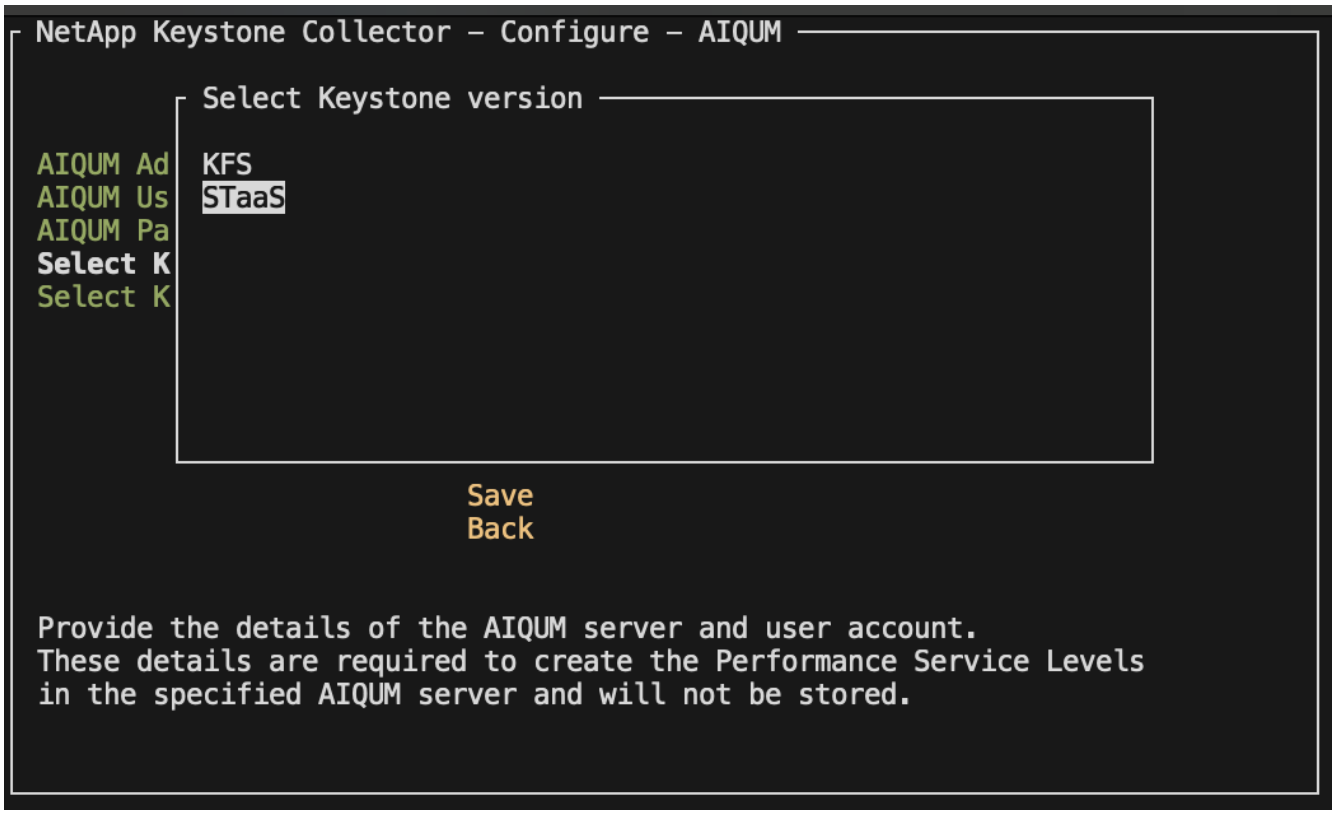
Passi

1. Avviare l'utilità TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vai su **Configura>AIQUM** per aprire la schermata AIQUM.

3. Abilitare l'opzione **Crea profili di prestazioni AIQUM**.
4. Immettere i dettagli del server Active IQ Unified Manager e dell'account utente. Questi dettagli sono necessari per creare i PSL e non verranno memorizzati.

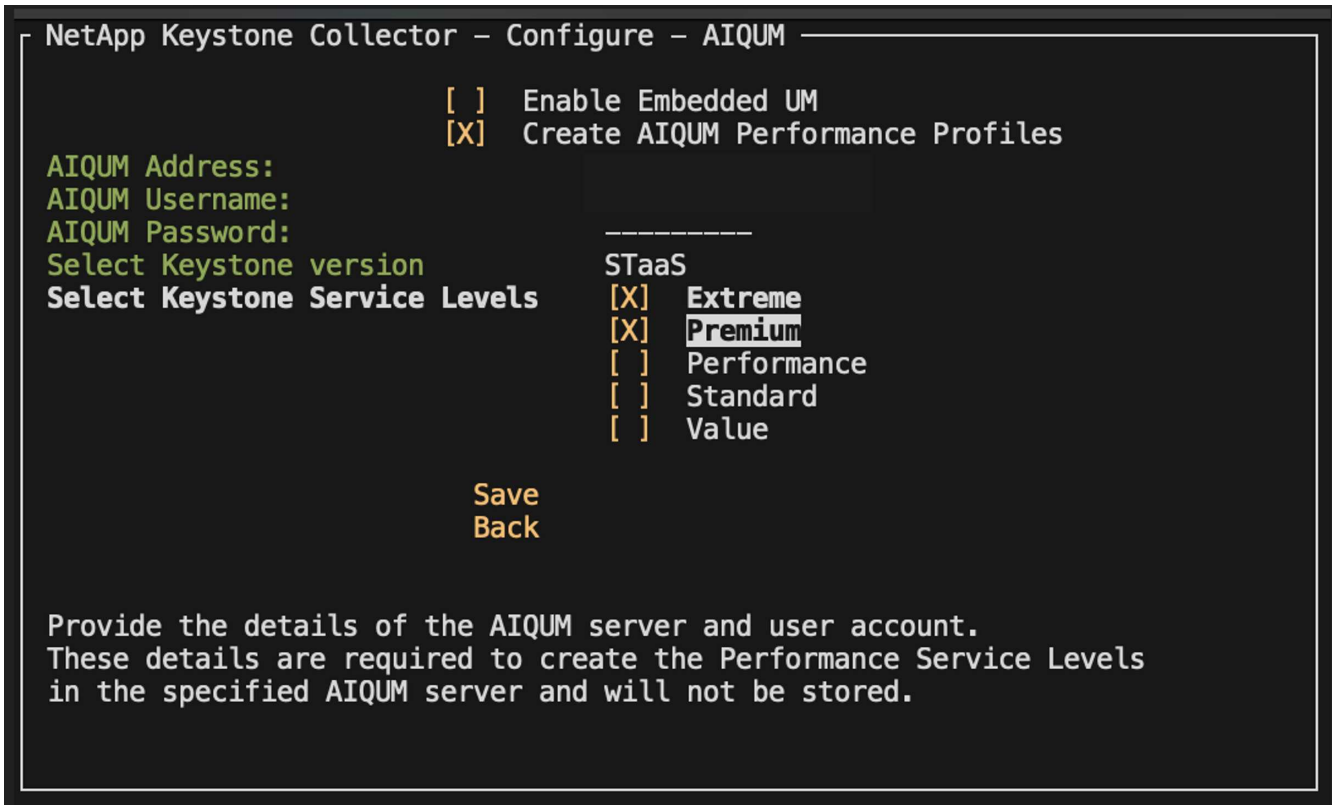


5. Per *Seleziona versione Keystone *, seleziona `–unset–` .
6. Premere Invio. Viene visualizzata una finestra di dialogo per la selezione della versione Keystone .
7. Evidenziare **STaaS** per specificare la versione Keystone per Keystone STaaS, quindi premere Invio.



È possibile evidenziare l'opzione **KFS** per i servizi di abbonamento Keystone versione 1. I servizi di abbonamento Keystone differiscono da Keystone STaaS per i livelli di servizio delle prestazioni costituenti, le offerte di servizi e i principi di fatturazione. Per saperne di più, fare riferimento a"Servizi di abbonamento Keystone | Versione 1" .

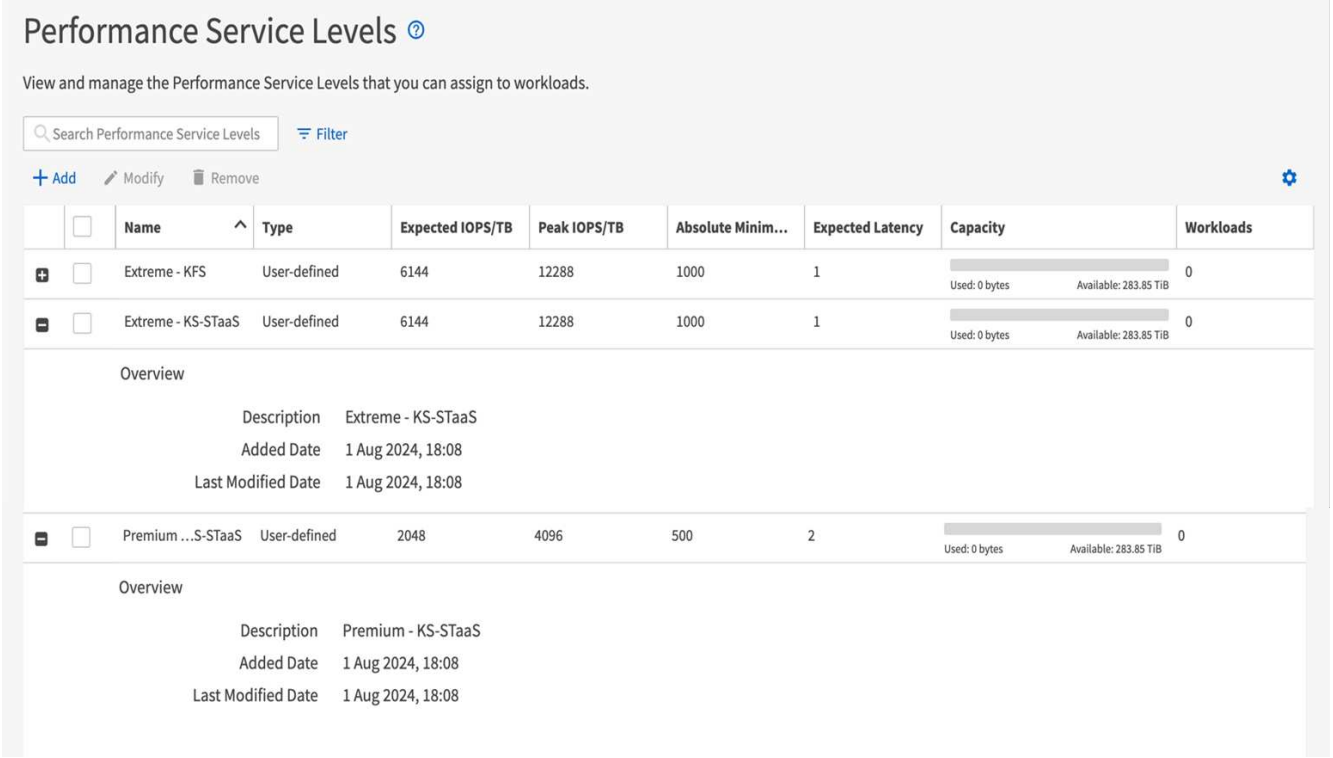
8. Tutti i livelli di servizio Keystone supportati verranno visualizzati nell'opzione *Seleziona livelli di servizio Keystone * per la versione Keystone specificata. Abilitare i livelli di servizio delle prestazioni desiderati dall'elenco.



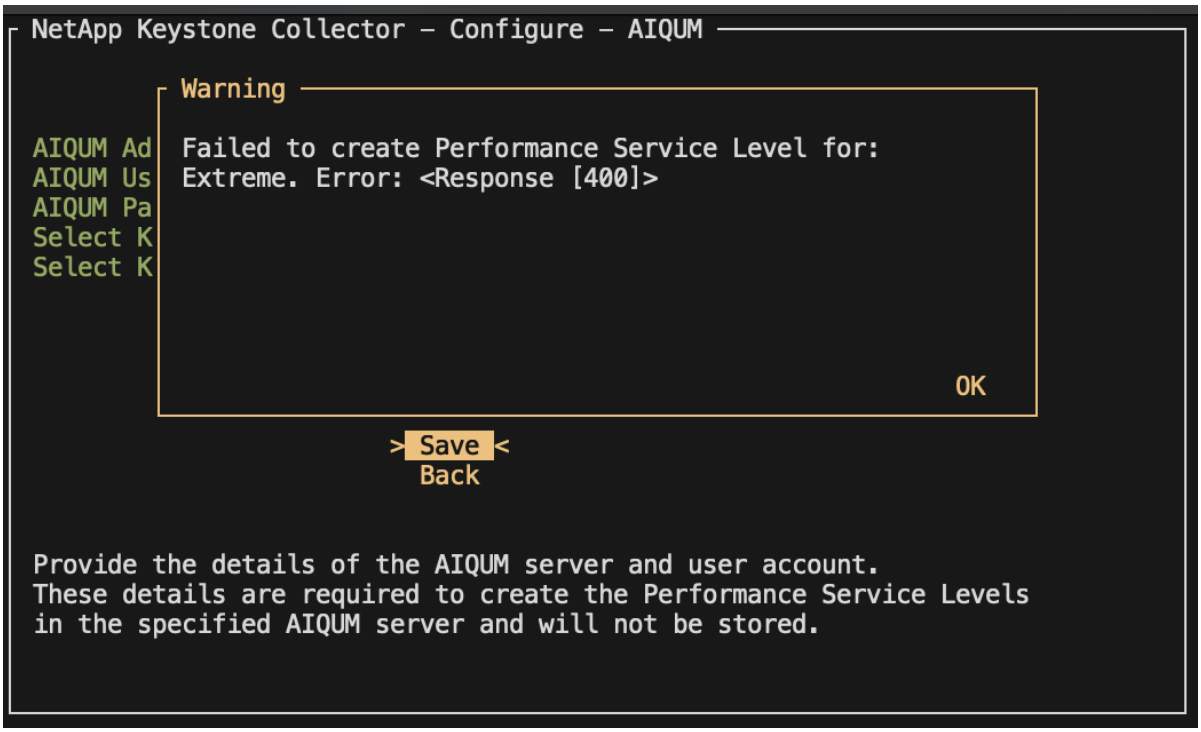
È possibile selezionare contemporaneamente più livelli di servizio prestazionali per creare PSL.

9. Selezionare **Salva** e premere Invio. Verranno creati livelli di servizio prestazionali.

   È possibile visualizzare i PSL creati, ad esempio Premium-KS-STaaS per STaaS o Extreme KFS per KFS, nella pagina **Livelli di servizio delle prestazioni** in Active IQ Unified Manager. Se i PSL creati non soddisfano i tuoi requisiti, puoi modificarli per adattarli alle tue esigenze. Per saperne di più, fare riferimento a"Creazione e modifica dei livelli di servizio delle prestazioni" .



Se sul server Active IQ Unified Manager specificato esiste già un PSL per il livello di servizio delle prestazioni selezionato, non sarà possibile crearlo di nuovo. Se provi a farlo, riceverai un messaggio di
errore.



Installa ITOM Collector

Requisiti di installazione per Keystone ITOM Collector

Prima di installare ITOM Collector, assicurati che i tuoi sistemi siano preparati con il software necessario e soddisfino tutti i prerequisiti richiesti.

Prerequisiti per la VM del server ITOM Collector:

- Sistema operativo supportato:
  - Debian 12 o successiva
  - Windows Server 2016 o successivo
  - Ubuntu 20.04 LTS o successivo
  - Red Hat Enterprise Linux (RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 o successivo
  - Amazon Linux 2023 o successivo

> I sistemi operativi consigliati sono Debian 12, Windows Server 2016 o versioni successive.

- Requisiti di risorse: i requisiti di risorse della VM in base al numero di nodi NetApp monitorati sono i seguenti:
  - 2-10 nodi: 4 CPU, 8 GB RAM, disco 40 GB
  - 12-20 nodi: 8 CPU, 16 GB RAM, 40 GB disco
- Requisiti di configurazione: assicurarsi che sui dispositivi monitorati siano configurati un account di sola lettura e SNMP. La VM del server ITOM Collector deve inoltre essere configurata come host trap SNMP e server Syslog sul cluster NetApp e sugli switch del cluster, se applicabile.

Requisiti di rete

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

Fonte	Destinazione	Protocollo	porti	Descrizione
Collezionista ITOM	IP di gestione del cluster NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Monitoraggio dei controllori ONTAP
IP di gestione dei cluster e dei nodi NetApp ONTAP	Collezionista ITOM	SNMP, Syslog	UDP 162, UDP 514	Trappole SNMP e Syslog dai controller
Collezionista ITOM	Interruttori a grappolo	SNMP	UDP 161	Monitoraggio degli switch
Interruttori a grappolo	Collezionista ITOM	SNMP, Syslog	UDP 162, UDP 514	Trappole SNMP e Syslog dagli switch
Collezionista ITOM	IP dei nodi StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitoraggio SNMP di StorageGRID
IP dei nodi StorageGRID	Collezionista ITOM	SNMP, Syslog	UDP 162, UDP 514	Trappole SNMP da StorageGRID

Collezionista ITOM	Collezionista Keystone	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Monitoraggio e gestione remota di Keystone Collector
Collezionista ITOM	DNS locale	DNS	UDP 53	Servizi DNS pubblici o privati
Collezionista ITOM	Server NTP di scelta	NTP	UDP 123	cronometraggio

Installa Keystone ITOM Collector sui sistemi Linux

Completa alcuni passaggi per installare ITOM Collector, che raccoglie i dati delle metriche nel tuo ambiente di archiviazione. È possibile installarlo su sistemi Windows o Linux, a seconda delle proprie esigenze.

Il team di supporto Keystone fornisce un collegamento dinamico per scaricare il file di installazione di ITOM Collector, che scade tra due ore.

Per installare ITOM Collector sui sistemi Windows, fare riferimento a"Installa ITOM Collector sui sistemi Windows" .

Per installare il software sul tuo server Linux, segui questi passaggi:

Prima di iniziare

- Verificare che la shell Bourne sia disponibile per lo script di installazione di Linux.
- Installare il `vim-common` pacchetto per ottenere il binario **xxd** necessario per il file di installazione di ITOM Collector.
- Assicurare il `sudo package` è installato se si prevede di eseguire ITOM Collector come utente non root.

Passi

1. Scarica il file di installazione di ITOM Collector sul tuo server Linux.
2. Aprire un terminale sul server ed eseguire il seguente comando per modificare i permessi e rendere eseguibili i file binari:
   `# chmod +x <installer_file_name>.bin`
3. Eseguire il comando per avviare il file di installazione del collettore ITOM:
   `#./<installer_file_name>.bin`
4. L'esecuzione del file di installazione richiede di:
   a. Accettare il contratto di licenza con l'utente finale (EULA).
   b. Inserisci i dettagli dell'utente per l'installazione.
   c. Specificare la directory padre di installazione.
   d. Selezionare la dimensione del collettore.
   e. Se applicabile, fornire i dettagli del proxy.

   Per ogni richiesta viene visualizzata un'opzione predefinita. Si consiglia di selezionare l'opzione predefinita, a meno che non si abbiano esigenze specifiche. Premere il tasto **Invio** per scegliere l'opzione predefinita. Al termine dell'installazione, un messaggio conferma che ITOM Collector è stato installato correttamente.

- Il file di installazione di ITOM Collector apporta aggiunte a `/etc/sudoers` per gestire i riavvii dei servizi e i dump della memoria.
- L'installazione di ITOM Collector sul server Linux crea un utente predefinito denominato **ITOM** per eseguire ITOM Collector senza privilegi di root. È possibile scegliere un utente diverso o eseguirlo come root, ma è consigliabile utilizzare l'utente ITOM creato dallo script di installazione di Linux.

Cosa succederà ora?

Una volta completata l'installazione, contattare il team di supporto Keystone per convalidare la corretta installazione di ITOM Collector tramite il portale di supporto ITOM. Dopo la verifica, il team di supporto Keystone configurerà ITOM Collector da remoto, inclusa l'ulteriore configurazione del rilevamento e del monitoraggio dei dispositivi, e invierà una conferma una volta completata la configurazione. Per qualsiasi domanda o informazione aggiuntiva, contattare keystone.services@netapp.com.

Installa Keystone ITOM Collector sui sistemi Windows

Installa ITOM Collector su un sistema Windows scaricando il file di installazione di ITOM Collector, eseguendo la procedura guidata InstallShield e immettendo le credenziali di monitoraggio richieste.

Il team di supporto Keystone fornisce un collegamento dinamico per scaricare il file di installazione di ITOM Collector, che scade tra due ore.

Puoi installarlo sui sistemi Linux in base alle tue esigenze. Per installare ITOM Collector su sistemi Linux, fare riferimento a"Installa ITOM Collector sui sistemi Linux" .

Per installare il software ITOM Collector sul tuo server Windows, segui questi passaggi:

Prima di iniziare

Assicurarsi che al servizio ITOM Collector sia concesso **Accedi come servizio** in Criteri locali/Assegnazione diritti utente nelle impostazioni dei criteri di sicurezza locali del server Windows.

Passi

1. Scarica il file di installazione di ITOM Collector sul tuo server Windows.
2. Aprire il file di installazione per avviare la procedura guidata InstallShield.
3. Accettare il contratto di licenza con l'utente finale (EULA). La procedura guidata InstallShield estrae i file binari necessari e richiede di immettere le credenziali.
4. Inserisci le credenziali per l'account con cui verrà eseguito ITOM Collector:
   - Se ITOM Collector non monitora altri server Windows, utilizzare il sistema locale.
   - Se ITOM Collector monitora altri server Windows nello stesso dominio, utilizzare un account di dominio con autorizzazioni di amministratore locale.
   - Se ITOM Collector monitora altri server Windows che non fanno parte dello stesso dominio, utilizzare un account amministratore locale e connettersi a ciascuna risorsa con le credenziali di amministratore locale. È possibile scegliere di impostare la password in modo che non scada, per ridurre i problemi di autenticazione tra ITOM Collector e le sue risorse monitorate.
5. Selezionare la dimensione del collettore. La dimensione predefinita è quella consigliata in base al file di installazione. Procedere con la dimensione suggerita, a meno che non si abbiano esigenze specifiche.

6. Selezionare *Avanti* per iniziare l'installazione. È possibile utilizzare la cartella popolata oppure sceglierne una diversa. Una casella di stato visualizza l'avanzamento dell'installazione, seguita dalla finestra di dialogo InstallShield Wizard completato.

Cosa succederà ora?

Una volta completata l'installazione, contattare il team di supporto Keystone per convalidare la corretta installazione di ITOM Collector tramite il portale di supporto ITOM. Dopo la verifica, il team di supporto Keystone configurerà ITOM Collector da remoto, inclusa l'ulteriore configurazione del rilevamento e del monitoraggio dei dispositivi, e invierà una conferma una volta completata la configurazione. Per qualsiasi domanda o informazione aggiuntiva, contattare keystone.services@netapp.com.

Configurare AutoSupport per Keystone

Quando si utilizza il meccanismo di telemetria AutoSupport , Keystone calcola l'utilizzo in base ai dati di telemetria AutoSupport . Per raggiungere il livello di granularità necessario, è necessario configurare AutoSupport in modo da incorporare i dati Keystone nei bundle di supporto giornalieri inviati dai cluster ONTAP .

Informazioni su questo compito

Prima di configurare AutoSupport in modo da includere i dati Keystone , è necessario tenere presente quanto segue.

- È possibile modificare le opzioni di telemetria AutoSupport utilizzando ONTAP CLI. Per informazioni sulla gestione dei servizi AutoSupport e sul ruolo di amministratore di sistema (cluster), vedere "Panoramica di Gestisci AutoSupport" E "Amministratori di cluster e SVM" .
- È possibile includere i sottosistemi nei pacchetti AutoSupport giornalieri e settimanali per garantire una raccolta dati precisa per Keystone. Per informazioni sui sottosistemi AutoSupport , vedere "Cosa sono i sottosistemi AutoSupport" .

Passi

1. Come utente amministratore di sistema, accedi al cluster Keystone ONTAP tramite SSH. Per informazioni, vedere "Accedi al cluster tramite SSH" .
2. Modificare il contenuto del registro.
    - Per ONTAP 9.16.1 e versioni successive, eseguire questo comando per modificare il contenuto del registro giornaliero:

      ```
      autosupport trigger modify -node * -autosupport-message
      management.log -basic-additional
      wafl,performance,snapshot,object_store_server,san,raid,snapmirror
      -troubleshooting-additional wafl
      ```

      Se il cluster è in una configurazione MetroCluster , eseguire questo comando:

```
autosupport trigger modify -node * -autosupport-message
management.log -basic-additional
wafl,performance,snapshot,object_store_server,san,raid,snapmirror,met
rocluster -troubleshooting-additional wafl
```

- Per le versioni precedenti ONTAP , eseguire questo comando per modificare il contenuto del registro giornaliero:

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

Se il cluster è in una configurazione MetroCluster , eseguire questo comando:

```
autosupport trigger modify -node * -autosupport-message management.log
-basic-additional
wafl,performance,snapshot,platform,object_store_server,san,raid,snapmirr
or,metrocluster -troubleshooting-additional wafl
```

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

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

Per ulteriori informazioni su questo comando, vedere "modifica del trigger di supporto automatico del nodo di sistema" .

Monitorare e aggiornare

Monitora lo stato di salute di Keystone Collector

È possibile monitorare lo stato di Keystone Collector utilizzando qualsiasi sistema di monitoraggio che supporti le richieste HTTP. Il monitoraggio dello stato di salute può aiutare a garantire che i dati siano disponibili sulla dashboard Keystone .

Per impostazione predefinita, i servizi sanitari Keystone non accettano connessioni da IP diversi da localhost. L'endpoint sanitario Keystone è `/uber/health` e ascolta su tutte le interfacce del server Keystone Collector sulla porta `7777` . Alla richiesta, l'endpoint restituisce come risposta un codice di stato della richiesta HTTP con un output JSON, che descrive lo stato del sistema Keystone Collector. Il corpo JSON fornisce uno stato di salute generale per il `is_healthy` attributo, che è un valore booleano; e un elenco dettagliato degli stati per componente per il `component_details` attributo. Ecco un esempio:

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

Vengono restituiti i seguenti codici di stato:

- **200**: indica che tutti i componenti monitorati sono integri
- **503**: indica che uno o più componenti non sono integri
- **403**: indica che il client HTTP che interroga lo stato di integrità non è presente nell'elenco *allow*, ovvero un elenco di CIDR di rete consentiti. Per questo stato non vengono restituite informazioni sanitarie. L'elenco *allow* utilizza il metodo CIDR di rete per controllare quali dispositivi di rete sono autorizzati a interrogare il sistema sanitario Keystone . Se ricevi questo errore, aggiungi il tuo sistema di monitoraggio all'elenco *consentito* da * Keystone Collector management TUI > Configura > Monitoraggio integrità*.

> **Utenti Linux, tenete presente questo problema noto:**
>
> **Descrizione del problema**: Keystone Collector esegue una serie di contenitori come parte del sistema di misurazione dell'utilizzo. Quando il server Red Hat Enterprise Linux 8.x è protetto con le policy Security Technical Implementation Guides (STIG) della USA Defense Information Systems Agency (DISA), si è verificato a intermittenza un problema noto con fapolicyd (File Access Policy Daemon). Questo problema è identificato come"errore 1907870" . **Soluzione alternativa**: finché non verrà risolto da Red Hat Enterprise, NetApp consiglia di aggirare questo problema inserendo `fapolicyd` in modalità permissiva.
> In`/etc/fapolicyd/fapolicyd.conf` , imposta il valore di `permissive = 1` .

Visualizza i registri di sistema

È possibile visualizzare i registri di sistema di Keystone Collector per esaminare le informazioni di sistema ed eseguire la risoluzione dei problemi utilizzando tali registri. Keystone Collector utilizza il sistema di registrazione *journald* dell'host e i registri di sistema possono essere esaminati tramite l'utilità di sistema standard *journalctl*. Per esaminare i registri è possibile avvalersi dei seguenti servizi chiave:

- ks-collector
- ks-salute
- ks-aggiornamento automatico

Il servizio principale di raccolta dati *ks-collector* produce log in formato JSON con un `run-id` attributo associato a ciascun processo di raccolta dati pianificato. Di seguito è riportato un esempio di un lavoro riuscito per la raccolta di dati di utilizzo standard:

```
{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdflm0f74cgphgfon8cg","run-id":"cdflm0f74cgphgfon8cg"}
{"level":"info","time":"2022-10-
31T05:20:04.624Z","caller":"ontap/service.go:215","msg":"223 volumes
collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:18.821Z","caller":"ontap/service.go:215","msg":"697 volumes
collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:41.598Z","caller":"ontap/service.go:215","msg":"7 volumes
collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.247Z","caller":"ontap/service.go:215","msg":"24 volumes
collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.786Z","caller":"worker/collector.go:75","msg":"4 clusters
collected","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.839Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193648.tar.gz type=ontap to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.840Z","caller":"reception/reception.go:76","msg":"File bytes
123425","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}
```

Di seguito è riportato un esempio di un lavoro riuscito per la raccolta facoltativa di dati sulle prestazioni:

```
{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:28","msg":"initialising MySql
service at 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:55","msg":"Opening MySql db
connection at server 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:39","msg":"Creating MySql db
config object"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:69","msg":"initialisi
ng SLA service"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:71","msg":"SLA
service successfully initialised"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"worker/collector.go:217","msg":"Performance
data would be collected for timerange: 2022-10-31T10:24:52~2022-10-
31T10:29:52"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file
generated: 65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz type=ontap-perf to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes
17767","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-
collector/main.go:88","msg":"exiting","run-id":"cdflm0f74cgphgfon8cg"}
```

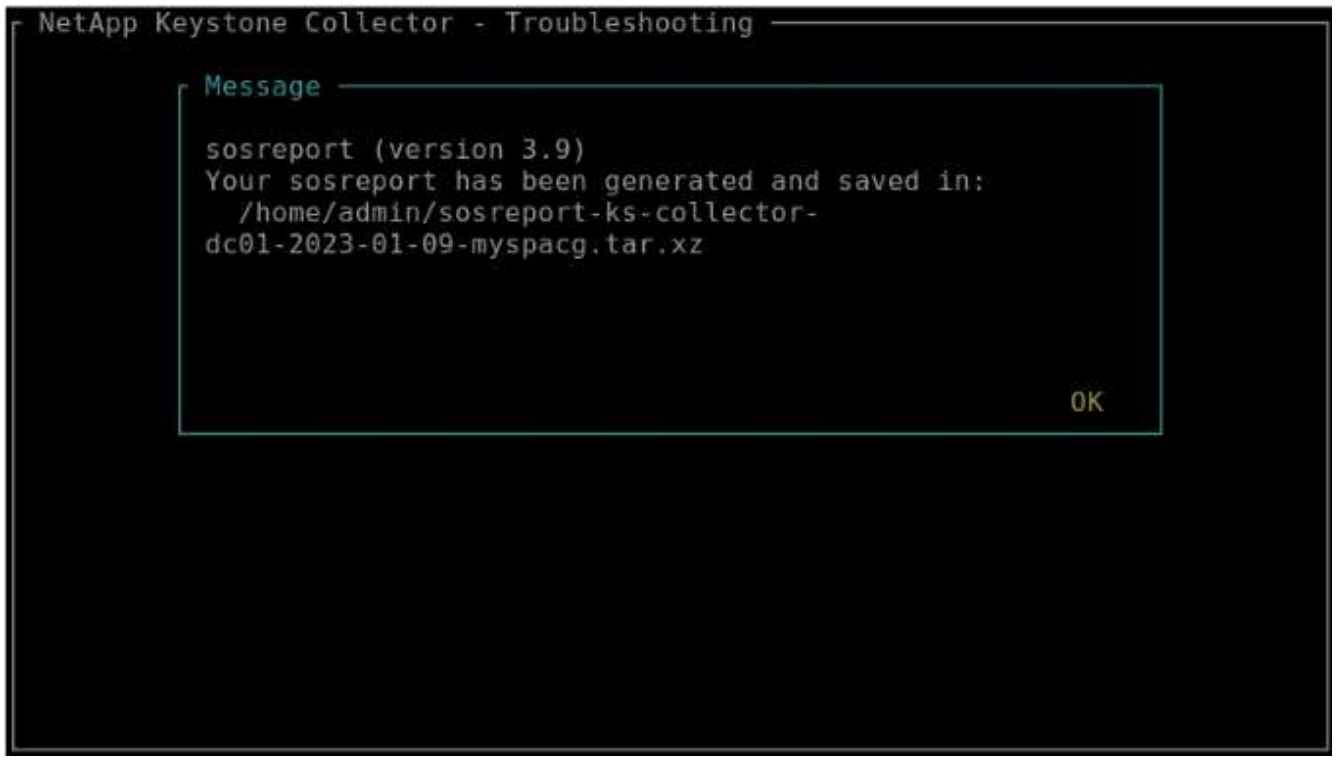
Genera e raccogli pacchetti di supporto

Keystone Collector TUI consente di generare pacchetti di supporto e di aggiungerli alle richieste di servizio per risolvere i problemi di supporto. Seguire questa procedura:

Passi

1. Avviare l'utilità TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vai a **Risoluzione dei problemi > Genera pacchetto di supporto**
   .

3. Una volta generato, viene visualizzata la posizione in cui è salvato il bundle. Utilizzare FTP, SFTP o SCP per connettersi alla posizione e scaricare il file di registro su un sistema locale.



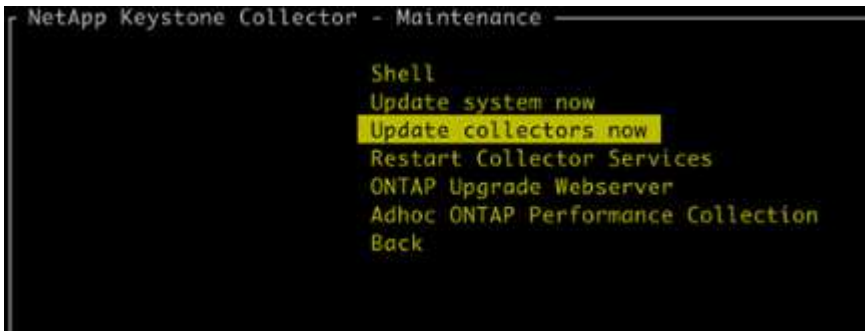
4. Una volta scaricato il file, è possibile allegarlo al ticket di supporto Keystone ServiceNow. Per informazioni sull'emissione dei biglietti, vedere "Generazione di richieste di servizio".

Aggiorna manualmente Keystone Collector

La funzione di aggiornamento automatico di Keystone Collector è abilitata per impostazione predefinita e aggiorna automaticamente il software Keystone Collector a ogni nuova versione. Tuttavia, è possibile disattivare questa funzione e aggiornare manualmente il software.

Passi

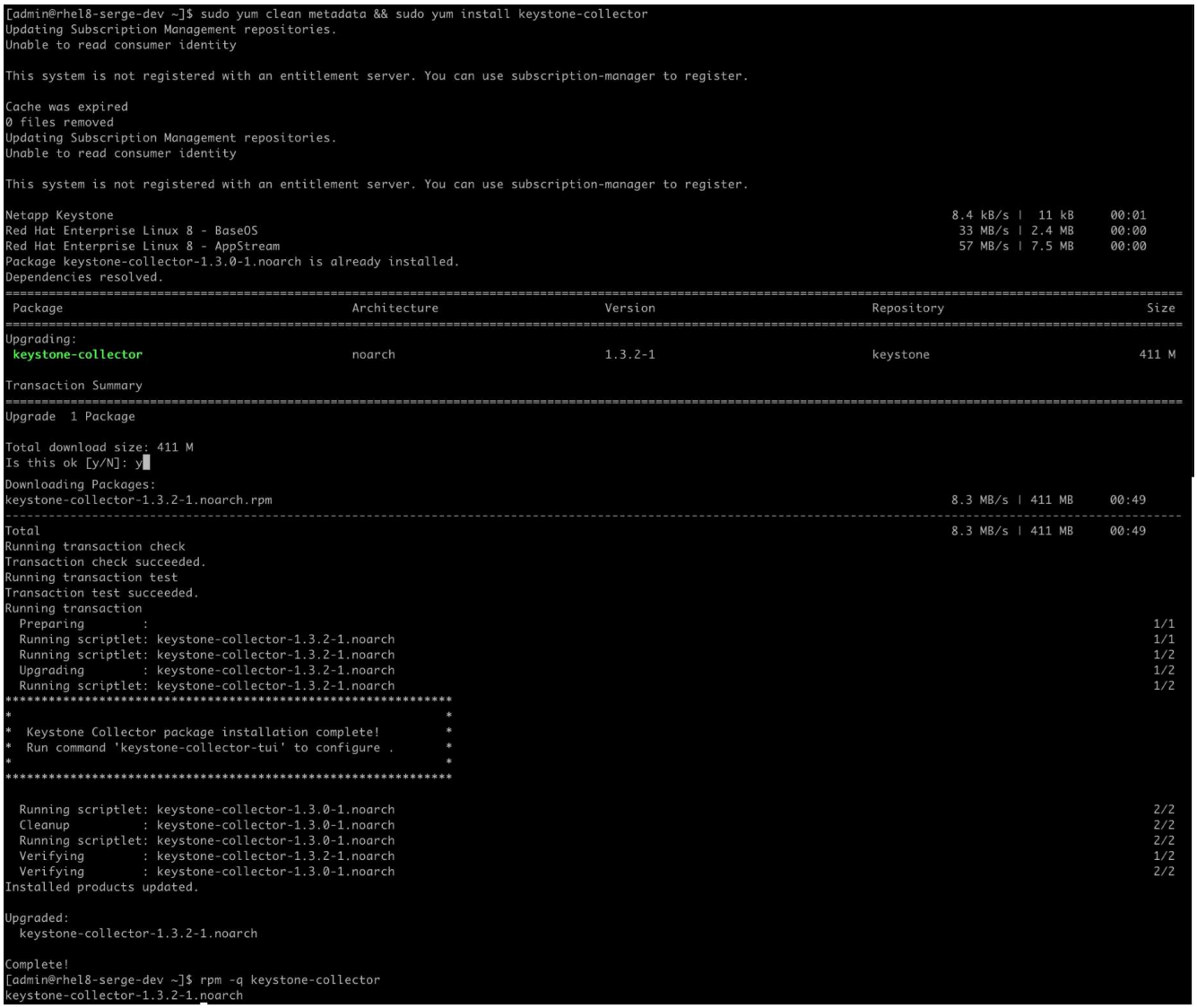
1. Avviare l'utilità TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Nella schermata di manutenzione, selezionare l'opzione **Aggiorna collettori ora**.



In alternativa, eseguire questi comandi per aggiornare la versione:

Per CentOS:

```
sudo yum clean metadata && sudo yum install keystone-collector
```



Per Debian:

```
sudo apt-get update && sudo apt-get upgrade keystone-collector
```

3. Riavviare Keystone Collector Management TUI; è possibile visualizzare la versione più recente nella parte in alto a sinistra della schermata iniziale.

   In alternativa, esegui questi comandi per visualizzare la versione più recente:

   Per CentOS:

   ```
   rpm -q keystone-collector
   ```

   Per Debian:

```
dpkg -l | grep keystone-collector
```

Sicurezza di Keystone Collector

Keystone Collector include funzionalità di sicurezza che monitorano le prestazioni e le metriche di utilizzo dei sistemi Keystone , senza mettere a rischio la sicurezza dei dati dei clienti.

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

- **Privacy by design**: Keystone Collector raccoglie dati minimi per eseguire la misurazione dell'utilizzo e il monitoraggio delle prestazioni. Per ulteriori informazioni, consultare "Dati raccolti per la fatturazione" . IL"Rimuovi dati privati" L'opzione è abilitata per impostazione predefinita e maschera e protegge le informazioni sensibili.
- **Accesso con privilegi minimi**: Keystone Collector richiede autorizzazioni minime per monitorare i sistemi di archiviazione, il che riduce al minimo i rischi per la sicurezza e impedisce qualsiasi modifica indesiderata ai dati. Questo approccio è in linea con il principio del privilegio minimo, migliorando la sicurezza complessiva degli ambienti monitorati.
- **Framework di sviluppo software sicuro**: Keystone utilizza un framework di sviluppo software sicuro durante l'intero ciclo di sviluppo, che mitiga i rischi, riduce le vulnerabilità e protegge il sistema da potenziali minacce.

Rafforzamento della sicurezza

Per impostazione predefinita, Keystone Collector è configurato per utilizzare configurazioni con protezione rafforzata. Di seguito sono riportate le configurazioni di sicurezza 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 potrebbe ridurre la sicurezza del sistema. Per ulteriori informazioni, consultare "Guida CIS Benchmark" .
  - Riceve e installa automaticamente le patch di sicurezza verificate da Keystone Collector tramite la funzione di aggiornamento automatico. La disattivazione di questa funzionalità potrebbe comportare la presenza di software vulnerabile e non aggiornato.
  - Autentica gli aggiornamenti ricevuti da Keystone Collector. La disabilitazione della verifica del repository APT può comportare l'installazione automatica di patch non autorizzate, con conseguente potenziale introduzione di vulnerabilità.
- Keystone Collector convalida automaticamente i certificati HTTPS per garantire la sicurezza della connessione. La disattivazione di questa funzionalità potrebbe comportare l'impersonificazione di endpoint esterni e la perdita di dati di utilizzo.
- Keystone Collector supporta"CA attendibile personalizzata" certificazione. Per impostazione predefinita, considera attendibili i certificati firmati da CA radice pubbliche riconosciute da"Programma di certificazione CA di Mozilla" . Abilitando CA attendibili aggiuntive, Keystone Collector consente la convalida dei certificati HTTPS per le connessioni agli endpoint che presentano tali certificati.
- Keystone Collector abilita per impostazione predefinita l'opzione **Rimuovi dati privati**, che maschera e protegge le informazioni sensibili. Per ulteriori informazioni, consultare "Limitare la raccolta di dati privati" . Disattivando questa opzione verranno comunicati dati aggiuntivi al sistema Keystone . Ad esempio, può

includere informazioni immesse dall'utente, come i nomi dei volumi, che potrebbero essere considerate informazioni sensibili.

Informazioni correlate

- "Panoramica di Keystone Collector"
- "Requisiti dell'infrastruttura virtuale"
- "Configura Keystone Collector"

Tipi di dati utente raccolti da Keystone

Keystone raccoglie informazioni sulla configurazione, sullo stato e sull'utilizzo dagli abbonamenti Keystone ONTAP e Keystone StorageGRID , nonché dati di telemetria dalla macchina virtuale (VM) che ospita Keystone Collector. Può raccogliere dati sulle prestazioni solo per ONTAP , se questa opzione è abilitata in Keystone Collector.

Raccolta dati ONTAP

Dati di utilizzo raccolti per ONTAP: Scopri di più

L’elenco seguente è un campione rappresentativo dei dati sul consumo di capacità raccolti per ONTAP:

- Cluster
  - ClusterUUID
  - Nome del cluster
  - Numero di serie
  - Posizione (in base al valore immesso nel cluster ONTAP)
  - Contatto
  - Versione
- Nodi
  - Numero di serie
  - Nome del nodo
- Volumi
  - Nome aggregato
  - Nome del volume
  - VolumeInstanceUUID
  - Flag IsCloneVolume
  - Flag IsFlexGroupConstituent
  - Flag IsSpaceEnforcementLogical
  - Flag IsSpaceReportingLogical
  - Spazio logico utilizzato da Afs
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - Nome QoSAdaptivePolicyGroup
  - Nome QoSPolicyGroup
  - Misurare
  - Usato
  - FisicoUsato
  - Dimensioni utilizzate dalle istantanee
  - Tipo
  - VolumeStyleExtended
  - Nome del server virtuale
  - Flag IsVsRoot
- VServer
  - NomeVserver

    - VserverUUID
    - Sottotipo
- Aggregati di stoccaggio
    - Tipo di archiviazione
    - Nome aggregato
    - UUID aggregato
    - Fisico utilizzato
    - Dimensioni disponibili
    - Misurare
    - Dimensioni utilizzate
- Archivi di oggetti aggregati
    - NomeArchivioOggetto
    - ObjectStoreUUID
    - Tipo di fornitore
    - Nome aggregato
- Clona volumi
    - FlexClone
    - Misurare
    - Usato
    - Vserver
    - Tipo
    - ParentVolume
    - ParentVserver
    - IsConstituent
    - SplitEstimate
    - Stato
    - FlexCloneUsedPercent
- LUN di archiviazione
    - UUID LUN
    - Nome LUN
    - Misurare
    - Usato
    - Flag IsReserved
    - Flag IsRequested
    - Nome unità logica
    - QoSPolicyUUID
    - Nome della politica QoSPolicy

    - VolumeUUID
    - NomeVolume
    - SVMUUID
    - Nome SVM
- Volumi di archiviazione
    - VolumeInstanceUUID
    - NomeVolume
    - Nome SVM
    - SVMUUID
    - QoSPolicyUUID
    - Nome della politica QoSPolicy
    - CapacitàTierFootprint
    - Impronta di livello di prestazione
    - Impronta totale
    - Politica di suddivisione in livelli
    - Flag IsProtected
    - Flag IsDestination
    - Usato
    - FisicoUsato
    - CloneParentUUID
    - Spazio logico utilizzato da Afs
- Gruppi di policy QoS
    - PolicyGroup
    - QoSPolicyUUID
    - Massima produttività
    - Portata minima
    - Massima capacità IOPS
    - Velocità massima in MBps
    - MinThroughputIOPS
    - Velocità minima di trasmissione MBps
    - Flag condiviso
- Gruppi di policy QoS adattive ONTAP
    - Nome della politica QoSPolicy
    - QoSPolicyUUID
    - Picco IOPS
    - PeakIOPSAllocation
    - Minimo IOPS assoluto

    - IOPS previsti
    - Allocazione IOPS prevista
    - Dimensione del blocco
- Impronte
    - Vserver
    - Volume
    - Impronta totale
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Nodo
    - Aggregato
    - LIF
    - Replica della configurazione
    - Connessioni
    - Cluster
    - Volumi
- Cluster MetroCluster
    - ClusterUUID
    - Nome del cluster
    - RemoteClusterUUID
    - NomeCluserRemoto
    - Stato di configurazione locale
    - Stato di configurazione remoto
- Nodi MetroCluster
    - Stato di mirroring DR
    - Intercluster LIF
    - Raggiungibilità del nodo
    - Nodo partner DR
    - Nodo partner DR Aux
    - Relazione simmetrica tra i nodi DR, DR Aux e HA
    - Passaggio automatico non pianificato
- Replica della configurazione MetroCluster
    - Battito cardiaco remoto
    - Ultimo battito cardiaco inviato
    - Ultimo battito cardiaco ricevuto
    - Flusso Vserver

    - Flusso di cluster
    - Magazzinaggio
    - Volume di stoccaggio in uso
- Mediatori MetroCluster
    - Indirizzo del mediatore
    - Porto mediatore
    - Mediatore configurato
    - Mediatore raggiungibile
    - Modalità
- Metriche di osservabilità del collettore
    - Orario di raccolta
    - Interrogazione dell'endpoint API Active IQ Unified Manager
    - Tempo di risposta
    - Numero di record
    - IP dell'istanza AIQUMInstance
    - ID CollectorInstance

Dati sulle prestazioni raccolti per ONTAP: Scopri di più

L’elenco seguente è un campione rappresentativo dei dati sulle prestazioni raccolti per ONTAP:

- Nome del cluster
- UUID del cluster
- ID oggetto
- NomeVolume
- UUID dell’istanza del volume
- Vserver
- VserverUUID
- Nodo seriale
- Versione ONTAP
- Versione AIQUM
- Aggregato
- AggregateUUID
- ResourceKey
- Marca temporale
- IOPSPerTb
- Latenza
- ReadLatency
- Scrivi MBps
- QoSMinThroughputLatency
- Latenza QoSNBlade
- UsedHeadRoom
- CacheMissRatio
- AltroLatenza
- QoSAggregateLatency
- IOPS
- QoSNetworkLetency
- AvailableOps
- Latenza di scrittura
- Latenza QoSCloud
- QoSClusterInterconnectLatency
- Altri MBps
- Latenza QoSCop
- Latenza QoSDBlade
- Utilizzo

- LeggiIOPS
- MBps
- Altri IOPS
- QoSPolicyGroupLatency
- Lettura MBps
- QoSSyncSnapmirrorLatency
- Dati a livello di sistema
  - Scrittura/Lettura/Altro/IOPS totali
  - Scrittura/Lettura/Altro/Rendimento totale
  - Scrittura/Lettura/Altro/Latenza totale
- ScriviIOPS

Elenco degli elementi rimossi limitando l’accesso ai dati privati: Scopri di più

Quando l’opzione **Rimuovi dati privati** è abilitata su Keystone Collector, le seguenti informazioni sull’utilizzo vengono eliminate per ONTAP. Questa opzione è abilitata per impostazione predefinita.

- Nome del cluster
- Posizione del cluster
- Contatto del cluster
- Nome del nodo
- Nome aggregato
- Nome del volume
- Nome QoSAdaptivePolicyGroup
- Nome QoSPolicyGroup
- Nome del server virtuale
- Nome LUN di archiviazione
- Nome aggregato
- Nome unità logica
- Nome SVM
- IP dell’istanza AIQUMInstance
- FlexClone
- NomeClusterRemoto

Raccolta dati StorageGRID

Dati di utilizzo raccolti per StorageGRID: Scopri di più

L'elenco seguente è un campione rappresentativo del `Logical Data` raccolti per StorageGRID:

- ID StorageGRID
- ID account
- Nome utente
- Quota account in byte
- Nome del bucket
- Conteggio oggetti bucket
- Byte di dati del bucket

L'elenco seguente è un campione rappresentativo del `Physical Data` raccolti per StorageGRID:

- ID StorageGRID
- Nodo ID
- ID del sito
- Nome del sito
- Esempio
- Byte di utilizzo dello storage StorageGRID
- Metadati di utilizzo dello storage StorageGRID Byte

L'elenco seguente è un campione rappresentativo del `Availability/Uptime Data` raccolti per StorageGRID:

- Percentuale di uptime SLA

Elenco degli elementi rimossi limitando l'accesso ai dati privati: Scopri di più

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

- Nome utente
- Nome del secchio
- Nome del sito
- Nome istanza/nodo

Raccolta dati di telemetria

Dati di telemetria raccolti da Keystone Collector VM: Scopri di più

L'elenco seguente è un campione rappresentativo dei dati di telemetria raccolti per i sistemi Keystone :

- Informazioni di sistema
  - Nome del sistema operativo
  - Versione del sistema operativo
  - ID del sistema operativo
  - Nome host del sistema
  - Indirizzo IP predefinito del sistema
- Utilizzo delle risorse di sistema
  - Tempo di attività del sistema
  - Numero di core della CPU
  - Carico di sistema (1 min, 5 min, 15 min)
  - Memoria totale
  - Memoria libera
  - Memoria disponibile
  - Memoria condivisa
  - Memoria buffer
  - Memoria memorizzata nella cache
  - Scambio totale
  - Scambio gratuito
  - Scambio memorizzato nella cache
  - Nome del file system del disco
  - Dimensione del disco
  - Disco utilizzato
  - Disco disponibile
  - Percentuale di utilizzo del disco
  - Punto di montaggio del disco
- Pacchetti installati
- Configurazione del collettore
- Registri di servizio
  - Registri di servizio dai servizi Keystone

Keystone in modalità privata

Scopri di più su Keystone (modalità privata)

Keystone offre una modalità di distribuzione *privata*, nota anche come *dark site*, per

soddisfare le tue esigenze aziendali e di sicurezza. Questa modalità è disponibile per le organizzazioni con limitazioni di connettività.

NetApp offre una distribuzione specializzata di Keystone STaaS, pensata appositamente per ambienti con connettività Internet limitata o assente (noti anche come dark site). Si tratta di ambienti sicuri o isolati in cui la comunicazione esterna è limitata per motivi di sicurezza, conformità o requisiti operativi.

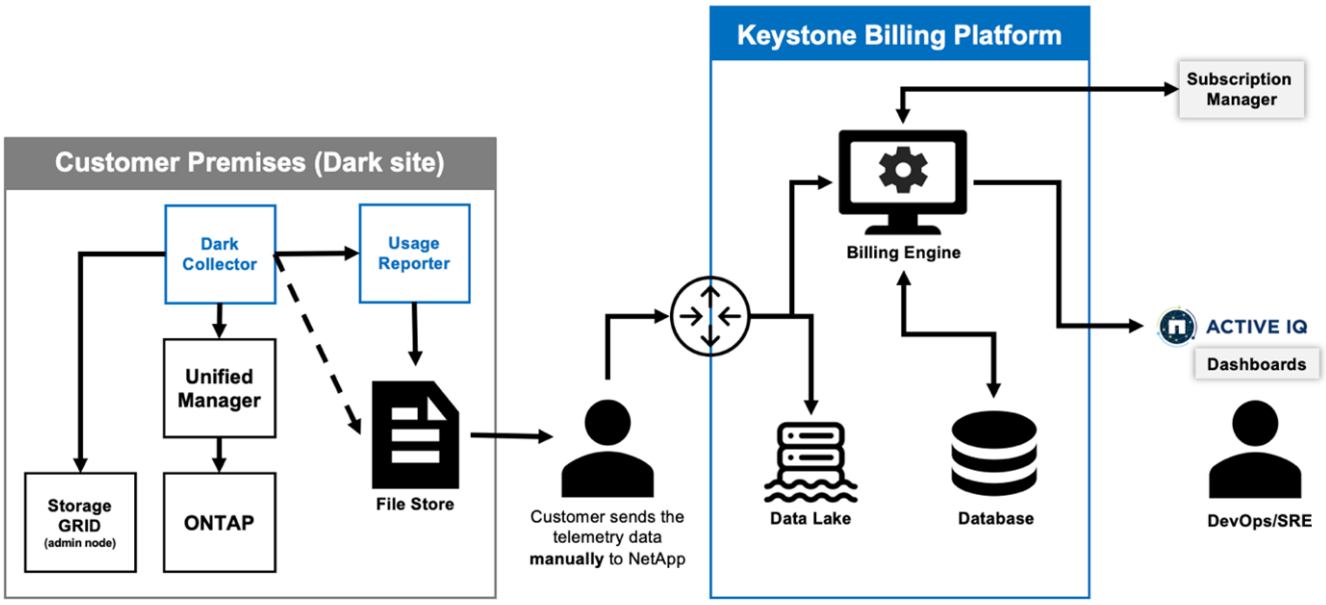
Per NetApp Keystone, offrire servizi per i dark site significa fornire il servizio di abbonamento allo storage flessibile Keystone in un modo che rispetti i vincoli di questi ambienti. Ciò comporta:

- **Implementazione locale**: Keystone può essere configurato in modo indipendente all'interno di ambienti isolati, senza necessità di connettività Internet o di personale esterno per l'accesso alla configurazione.
- **Operazioni offline**: tutte le funzionalità di gestione dell'archiviazione con controlli di integrità e fatturazione sono disponibili offline per le operazioni.
- **Sicurezza e conformità**: Keystone garantisce che l'implementazione soddisfi i requisiti di sicurezza e conformità dei siti oscuri, che possono includere crittografia avanzata, controlli di accesso sicuri e funzionalità di auditing dettagliate.
- **Assistenza e supporto**: NetApp fornisce supporto globale 24 ore su 24, 7 giorni su 7, con un responsabile Keystone dedicato assegnato a ciascun account per assistenza e risoluzione dei problemi.

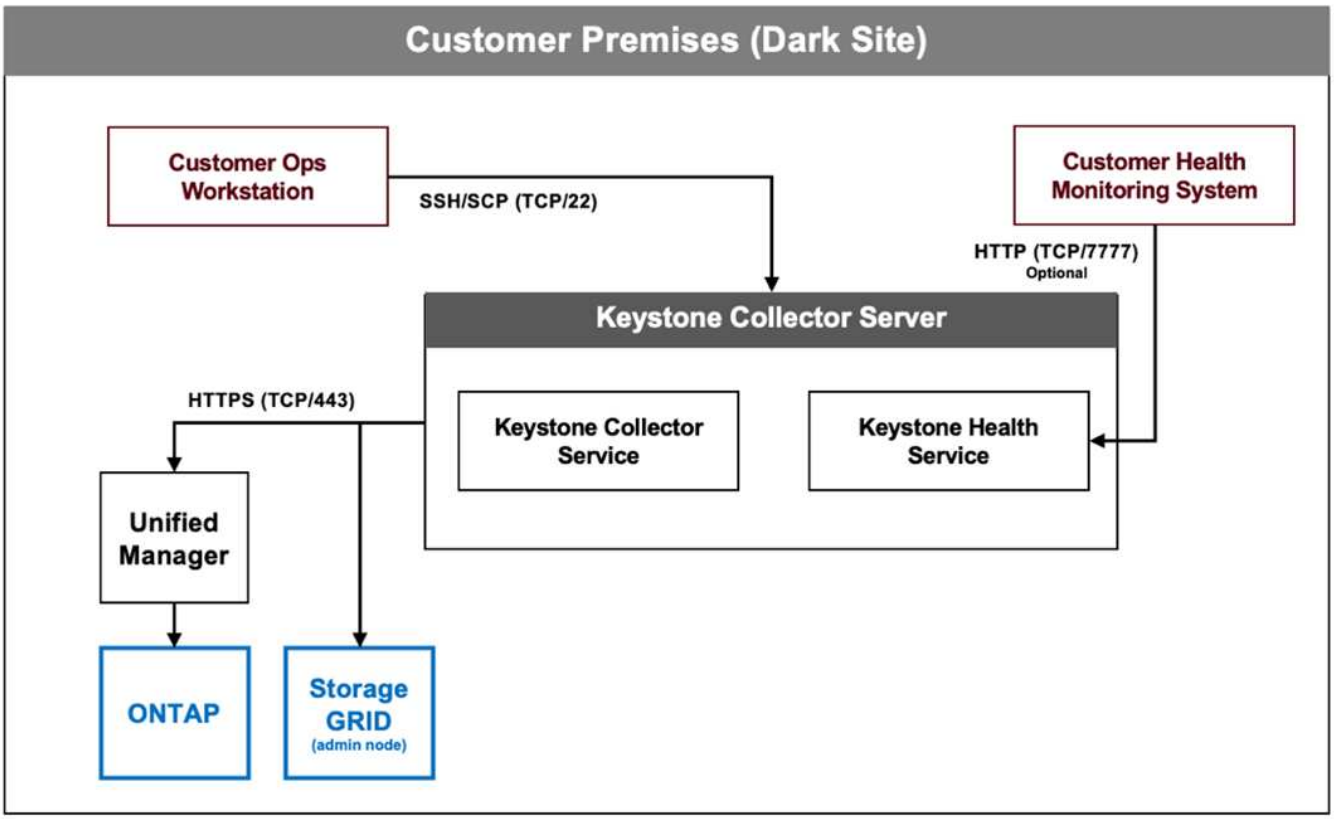
Keystone Collector può essere configurato senza restrizioni di connettività, modalità nota anche come *modalità* standard. Per saperne di più, fare riferimento a"Scopri di più su Keystone Collector" .

Keystone Collector in modalità privata

Keystone Collector è responsabile della raccolta periodica dei dati di utilizzo dai sistemi di archiviazione e dell'esportazione delle metriche in un report di utilizzo offline e in un archivio file locale. I file generati, creati sia in formato crittografato che in formato testo normale, vengono poi inoltrati manualmente a NetApp dall'utente dopo i controlli di convalida. Una volta ricevuti, la piattaforma di fatturazione Keystone di NetApp autentica ed elabora questi file, integrandoli nei sistemi di fatturazione e gestione degli abbonamenti per calcolare gli addebiti mensili.



Il servizio Keystone Collector sul server ha il compito di raccogliere periodicamente i dati di utilizzo, elaborare queste informazioni e generare un file di utilizzo localmente sul server. Il servizio sanitario esegue controlli sullo stato di salute del sistema ed è progettato per interfacciarsi con i sistemi di monitoraggio sanitario utilizzati dal cliente. Questi report sono disponibili per l'accesso offline da parte degli utenti, consentendo la convalida e aiutando nella risoluzione dei problemi.



Prepararsi all'installazione Keystone Collector in modalità privata

Prima di installare Keystone Collector in un ambiente senza accesso a Internet, noto anche come *sito oscuro* o *modalità privata*, assicurati che i tuoi sistemi siano preparati con il software necessario e soddisfino tutti i prerequisiti richiesti.

Requisiti per VMware vSphere

- Sistema operativo: VMware vCenter Server ed ESXi 8.0 o versioni successive
- Nucleo: 1 CPU
- RAM: 2 GB
- Spazio su disco: 20 GB vDisk

Requisiti per Linux

- Sistema operativo (scegline uno):
  - Red Hat Enterprise Linux (RHEL) 8.6 o qualsiasi serie successiva 8.x
  - Red Hat Enterprise Linux 9.0 o versioni successive
  - Debian 12

- Core: 2 CPU
- RAM: 4 GB
- Spazio su disco: 50 GB vDisk
  - Almeno 2 GB liberi in `/var/lib/`
  - Almeno 48 GB liberi in `/opt/netapp`

Sullo stesso server dovrebbero essere installati anche i seguenti pacchetti di terze parti. Se disponibili tramite il repository, questi pacchetti verranno installati automaticamente come prerequisiti:

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versione-blocco
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versione-blocco
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - podman
  - sosreport

Requisiti di rete

I requisiti di rete per Keystone Collector includono quanto segue:

- Active IQ Unified Manager (Unified Manager) 9.10 o versione successiva, configurato su un server con la funzionalità API Gateway abilitata.
- Il server Unified Manager dovrebbe essere accessibile dal server Keystone Collector sulla porta 443 (HTTPS).
- È necessario configurare un account di servizio con autorizzazioni di utente applicazione per Keystone Collector sul server Unified Manager.
- Non è richiesta la connettività Internet esterna.
- Ogni mese, esporta un file da Keystone Collector e invialo via e-mail al team di supporto NetApp . Per maggiori informazioni su come contattare il team di supporto, fare riferimento a "Ottieni assistenza con Keystone".

Installa Keystone Collector in modalità privata

Completa alcuni passaggi per installare Keystone Collector in un ambiente senza accesso a Internet, noto anche come *sito oscuro* o *modalità privata*. Questo tipo di installazione è perfetto per i tuoi siti sicuri.

A seconda delle esigenze, è possibile distribuire Keystone Collector sui sistemi VMware vSphere oppure installarlo sui sistemi Linux. Seguire i passaggi di installazione corrispondenti all'opzione selezionata.

Distribuisci su VMware vSphere

Segui questi passaggi:

1. Scarica il file modello OVA da "Portale web NetApp Keystone" .
2. Per i passaggi per distribuire il raccoglitore Keystone con il file OVA, fare riferimento alla sezione"Distribuzione del modello OVA" .

Installa su Linux

Il software Keystone Collector viene installato sul server Linux utilizzando i file .deb o .rpm forniti, in base alla distribuzione Linux.

Per installare il software sul tuo server Linux, segui questi passaggi:

1. Scarica o trasferisci il file di installazione di Keystone Collector sul server Linux:

   ```
   keystone-collector-<version>.noarch.rpm
   ```

2. Aprire un terminale sul server ed eseguire i seguenti comandi per avviare l'installazione.

   - **Utilizzando il pacchetto Debian**

     ```
     dpkg -i keystone-collector_<version>_all.deb
     ```

   - **Utilizzando il file RPM**

     ```
     yum install keystone-collector-<version>.noarch.rpm
     ```

     O

   ```
   rpm -i keystone-collector-<version>.noarch.rpm
   ```

3. Entra `y` quando viene richiesto di installare il pacchetto.

Configura Keystone Collector in modalità privata

Completa alcune attività di configurazione per consentire a Keystone Collector di raccogliere dati di utilizzo in un ambiente che non ha accesso a Internet, noto anche come *sito oscuro* o *modalità privata*. Si tratta di un'attività una tantum che serve ad attivare e associare i componenti richiesti al tuo ambiente di archiviazione. Una volta configurato, Keystone Collector monitorerà tutti i cluster ONTAP gestiti da Active IQ Unified Manager.

Keystone Collector fornisce l'utilità Keystone Collector Management Terminal User Interface (TUI) per eseguire attività di configurazione e monitoraggio. È possibile utilizzare vari comandi da tastiera, come Invio e i tasti freccia, per selezionare le opzioni e navigare all'interno di questa TUI.

Passi

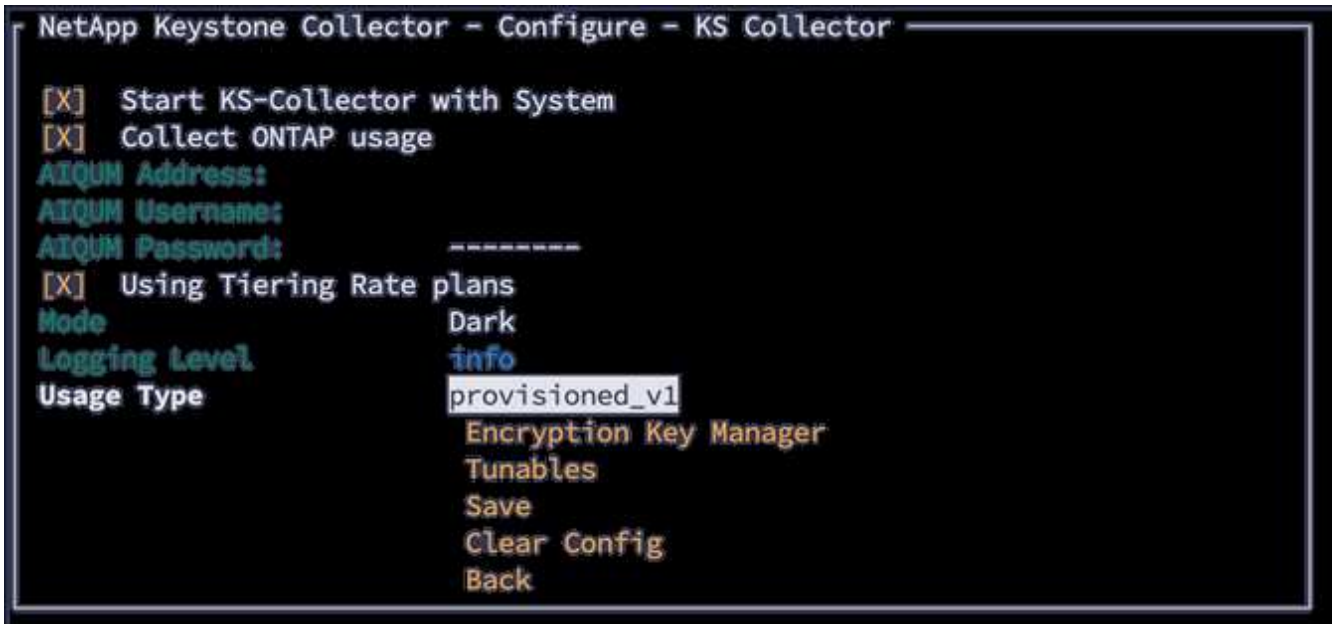
1. Avviare l'utilità TUI di gestione di Keystone Collector:

   ```
   keystone-collector-tui
   ```

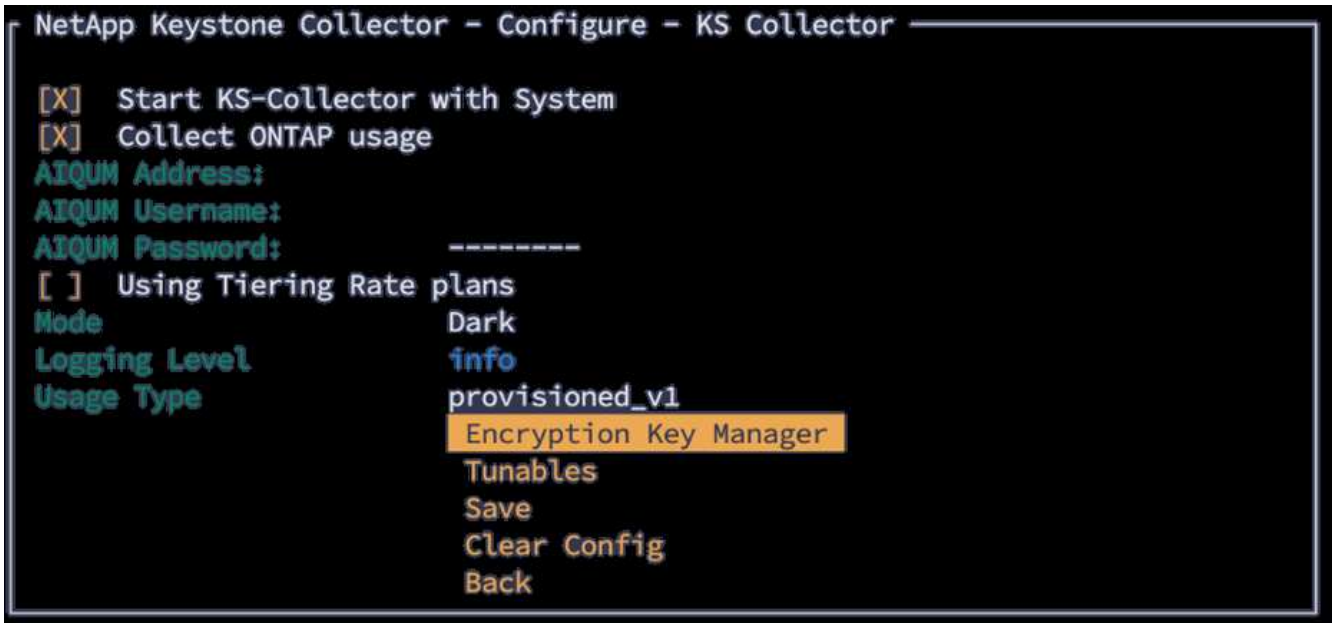
2. Vai su **Configura > Avanzate**.
3. Attiva l'opzione **Modalità Darksite**.

4. Seleziona **Salva**.
5. Vai su **Configura > KS-Collector** per configurare Keystone Collector.
6. Attivare o disattivare il campo **Avvia KS Collector con il sistema**.
7. Attiva/disattiva il campo *Raccogli utilizzo ONTAP *. Aggiungere i dettagli del server Active IQ Unified Manager (Unified Manager) e dell'account utente.
8. **Facoltativo**: attiva il campo **Utilizzo di piani tariffari a livelli** se per l'abbonamento è richiesta la suddivisione in livelli dei dati.
9. In base al tipo di abbonamento acquistato, aggiornare il **Tipo di utilizzo**.

Prima della configurazione, confermare il tipo di utilizzo associato all'abbonamento da NetApp.



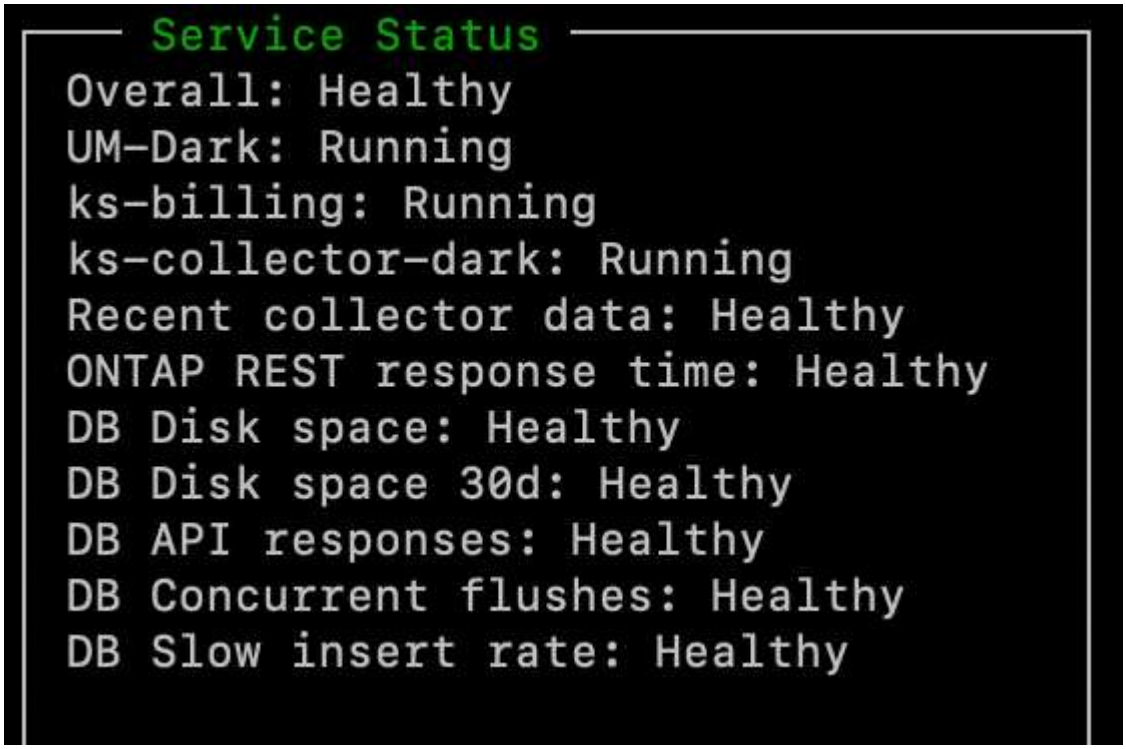
10. Seleziona **Salva**.
11. Vai su **Configura > KS-Collector** per generare la coppia di chiavi Keystone Collector.
12. Vai a **Encryption Key Manager** e premi Invio.



13. Selezionare **Genera coppia di chiavi del collezionista** e premere Invio.

14. Per verificare che Keystone Collector sia in buone condizioni, tornare alla schermata principale della TUI e verificare le informazioni sullo **Stato del servizio**. Il sistema dovrebbe mostrare che i servizi sono in uno stato **Complessivo: Integro**. Attendere fino a 10 minuti; se dopo questo periodo lo stato generale rimane

non funzionante, rivedere i passaggi di configurazione precedenti e contattare il team di supporto NetApp .



15. Uscire dall'interfaccia utente terminale di gestione di Keystone Collector selezionando l'opzione **Esci alla shell** nella schermata iniziale.
16. Recupera la chiave pubblica generata:

    ```
    ~/collector-public.pem
    ```

17. Invia un'e-mail con questo file a ng-keystone-secure-site-upload@netapp.com per siti non USPS sicuri, oppure a ng-keystone-secure-site-usps-upload@netapp.com per siti USPS sicuri.

Esporta il report di utilizzo

Dovresti inviare il report riepilogativo dell'utilizzo mensile a NetApp alla fine di ogni mese. È possibile generare questo report manualmente.

Per generare il report di utilizzo, seguire questi passaggi:

1. Vai su **Esporta utilizzo** nella schermata iniziale di Keystone Collector TUI.
2. Raccogli i file e inviali a ng-keystone-secure-site-upload@netapp.com per i siti non USPS sicuri, oppure a ng-keystone-secure-site-usps-upload@netapp.com per i siti USPS sicuri.

   Keystone Collector genera sia un file chiaro che un file crittografato, che devono essere inviati manualmente a NetApp. Il report Clear File contiene i seguenti dettagli che possono essere convalidati dal cliente.

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

Aggiorna ONTAP

Keystone Collector supporta gli aggiornamenti ONTAP tramite TUI.

Per aggiornare ONTAP, seguire questi passaggi:

1. Vai a *Manutenzione > Aggiornamento Webserver ONTAP *.
2. Copiare il file immagine di aggiornamento ONTAP in **/opt/netapp/ontap-upgrade/**, quindi selezionare **Avvia Webserver** per avviare il server Web.

3. Vai a `http://<collector-ip>:8000` utilizzando un browser web per assistenza nell'aggiornamento.

Riavvia Keystone Collector

È possibile riavviare il servizio Keystone Collector tramite TUI. Vai a **Manutenzione > Riavvia Collector** Servizi nella TUI. Questa operazione riavvierà tutti i servizi di raccolta e il loro stato potrà essere monitorato dalla schermata iniziale di TUI.

Monitora lo stato di salute di Keystone Collector in modalità privata

È possibile monitorare lo stato di Keystone Collector utilizzando qualsiasi sistema di monitoraggio che supporti le richieste HTTP.

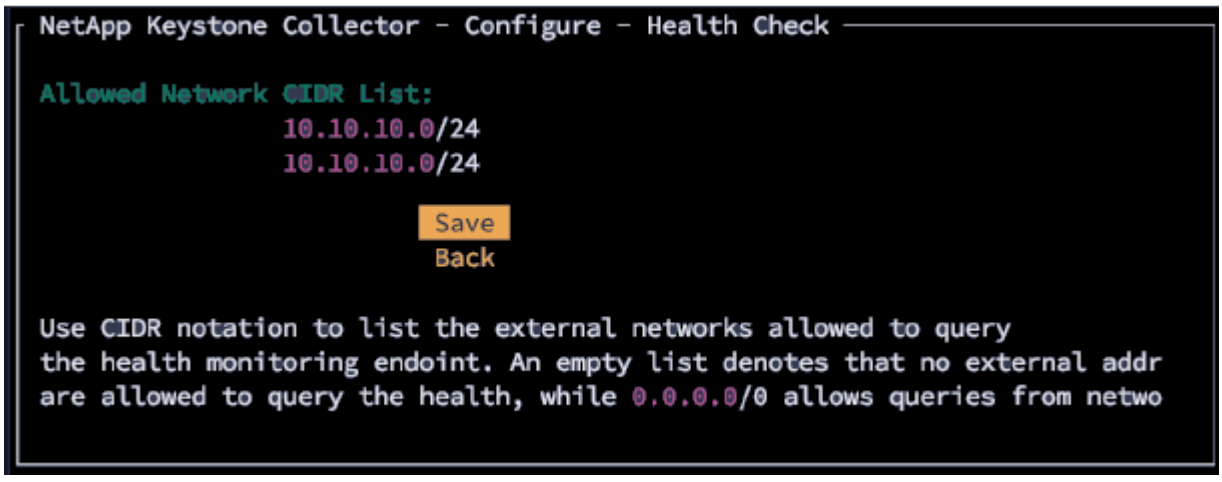
Per impostazione predefinita, i servizi sanitari Keystone non accettano connessioni da IP diversi da localhost. L'endpoint sanitario Keystone è `/uber/health` e ascolta su tutte le interfacce del server Keystone Collector sulla porta `7777` . Alla richiesta, l'endpoint restituisce come risposta un codice di stato della richiesta HTTP con un output JSON, che descrive lo stato del sistema Keystone Collector. Il corpo JSON fornisce uno stato di salute generale per il `is_healthy` attributo, che è un valore booleano; e un elenco dettagliato degli stati per componente per il `component_details` attributo. Ecco un esempio:

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

Vengono restituiti i seguenti codici di stato:

- **200**: indica che tutti i componenti monitorati sono integri
- **503**: indica che uno o più componenti non sono integri
- **403**: indica che il client HTTP che interroga lo stato di integrità non è presente nell'elenco *allow*, ovvero un elenco di CIDR di rete consentiti. Per questo stato non vengono restituite informazioni sanitarie.

  L'elenco *allow* utilizza il metodo CIDR di rete per controllare quali dispositivi di rete sono autorizzati a interrogare il sistema sanitario Keystone . Se viene visualizzato l'errore 403, aggiungere il sistema di monitoraggio all'elenco *consentito* da * Keystone Collector management TUI > Configura > Monitoraggio integrità*.

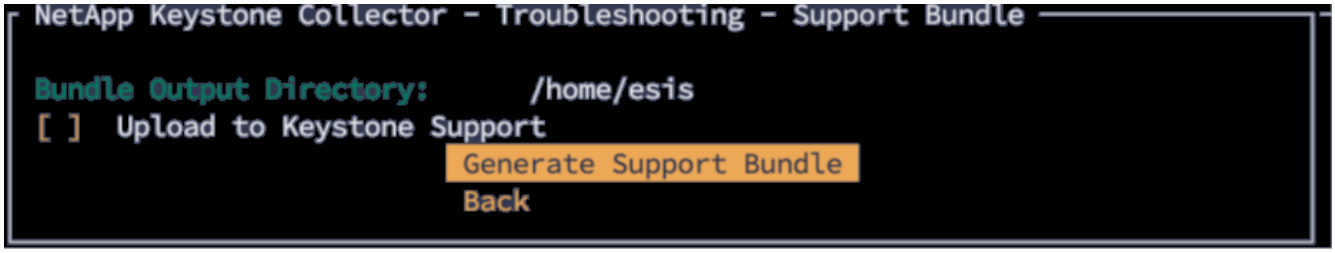


Genera e raccogli pacchetti di supporto

Per risolvere i problemi con Keystone Collector, puoi rivolgerti al supporto NetApp , che potrebbe richiedere un file *.tar*. È possibile generare questo file tramite l'utilità TUI di gestione Keystone Collector.

Per generare un file *.tar*, seguire questi passaggi:

1. Vai a **Risoluzione dei problemi > Genera pacchetto di supporto**.
2. Seleziona la posizione in cui salvare il pacchetto, quindi fai clic su **Genera pacchetto di supporto**.



Questo processo crea un `tar` pacchetto nella posizione indicata che può essere condiviso con NetApp per la risoluzione dei problemi.

3. Una volta scaricato il file, è possibile allegarlo al ticket di supporto Keystone ServiceNow. Per informazioni sull'emissione dei biglietti, vedere "Generazione di richieste di servizio".