Impostare e configurare Keystone

Keystone

NetApp
January 14, 2026

Sommario

Impostare e configurare Keystone

Requisiti

Requisiti dell'infrastruttura virtuale per Keystone Collector

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: VMware vCenter Server ed ESXi 8.0 o versioni successive
- 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 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 Linux per Keystone Collector

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: Una delle seguenti opzioni:
  - 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 gli ambienti esistenti)
- 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
- cronico
- python 3 (da 3.9.14 a 3.11.8)

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 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 per ONTAP e StorageGRID per Keystone

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

Soddisfare i seguenti requisiti se si intende raccogliere i dati di utilizzo solo tramite ONTAP:

1. Assicurarsi che sia configurato ONTAP 9,8 o versione successiva. Per informazioni sulla configurazione di un nuovo cluster, vedere i seguenti collegamenti:
   - "Configurare ONTAP su un nuovo cluster con Gestione di sistema"
   - "Configurare un cluster con la CLI"
2. Creare account di accesso ONTAP con ruoli specifici. Per ulteriori informazioni, fare riferimento a "Ulteriori informazioni sulla creazione di account di accesso ONTAP".
   - **Interfaccia utente Web**
     i. Accedere a Gestione di sistema di ONTAP utilizzando le credenziali predefinite. Per ulteriori informazioni, fare riferimento a "Gestione del cluster con System Manager".
     ii. Creare un utente ONTAP con il ruolo "sola lettura" e il tipo di applicazione "http" e abilitare l'autenticazione della password accedendo a **Cluster > Impostazioni > sicurezza > utenti**.
   - **CLI**
     i. Accedere alla CLI di ONTAP utilizzando le credenziali predefinite. Per ulteriori informazioni, fare riferimento a "Gestione cluster con CLI".
     ii. Creare un utente ONTAP con il ruolo "sola lettura" e il tipo di applicazione "http" e abilitare l'autenticazione della password. Per ulteriori informazioni sull'autenticazione, fare riferimento a "Attiva l'accesso alla password dell'account ONTAP".

Se si intende raccogliere dati di utilizzo tramite Active IQ Unified Manager, soddisfare i seguenti requisiti:

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

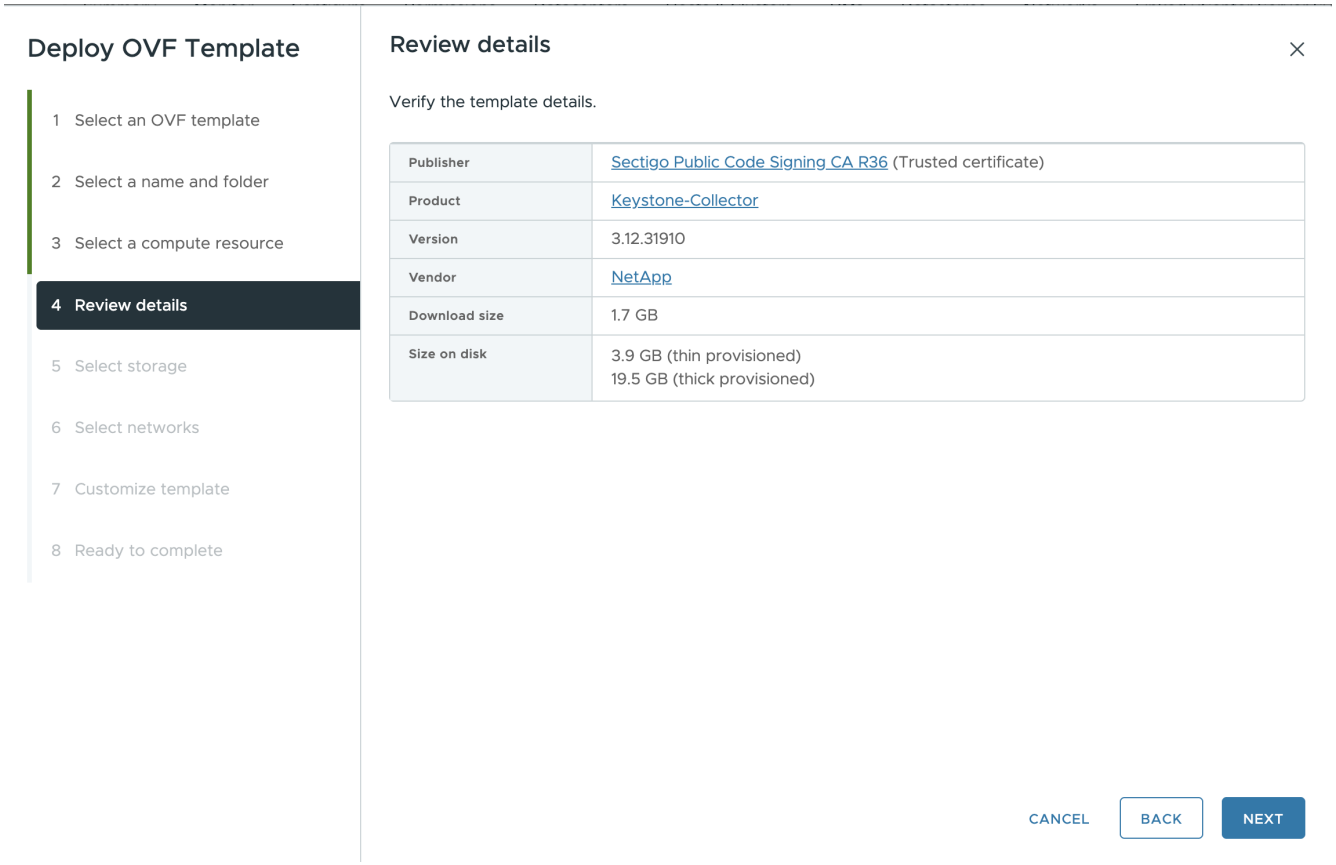
1. Scaricare il file OVA da "questo link" E memorizzarlo sul sistema VMware vSphere.
2. Sul sistema VMware vSphere, accedere alla vista **macchine virtuali e modelli**.
3. Fare clic con il pulsante destro del mouse sulla cartella desiderata per la macchina virtuale (VM) (o il data center, se non si utilizzano 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. 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 la procedura descritta in `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. 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

Si può installare il software Keystone Collector su un server Linux usando un RPM o un pacchetto Debian. Seguire la procedura di installazione a seconda della distribuzione Linux in uso.

Utilizzo di RPM

1. SSH al server di Keystone Collector e passare 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 repository del software YUM:
   `# yum install keystonerepo.rpm`
7. Una volta installato Keystone repo, installare il pacchetto keystone-collector tramite YUM Package Manager:

   ```
   # 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`

Uso di Debian

1. SSH al server Keystone Collector e privilegi più elevati `root`.
   `sudo su`
2. Scaricare il `keystone-sw-repo.deb` file:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Installare il file repository del software Keystone:
   `# dpkg -i keystone-sw-repo.deb`
4. Aggiornare l'elenco dei pacchetti:
   `# apt-get update`
5. Una volta installato Keystone repo, installare il pacchetto keystone-collector:
   `# apt-get 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.
- Keystone Collector può essere configurato per le organizzazioni che non dispongono di accesso a Internet, anche note come *dark site* o *private mode*. Per ulteriori informazioni, fare riferimento alla sezione "Keystone in modalità privata".

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".

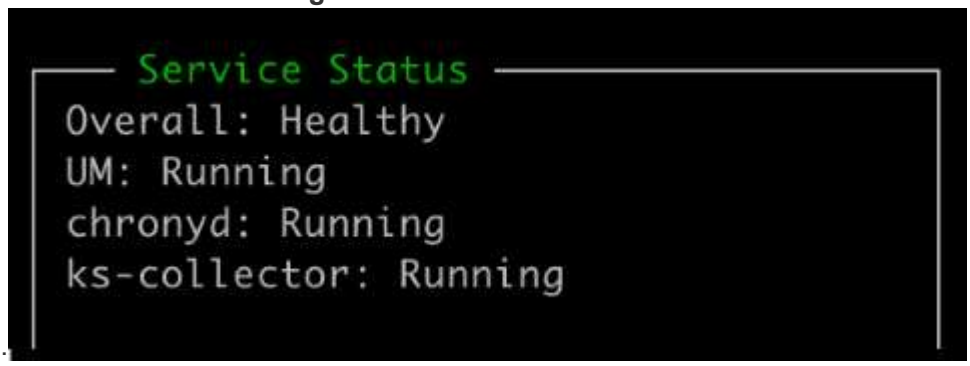
** FOR StorageGRFunded **

- **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**

.

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**



.

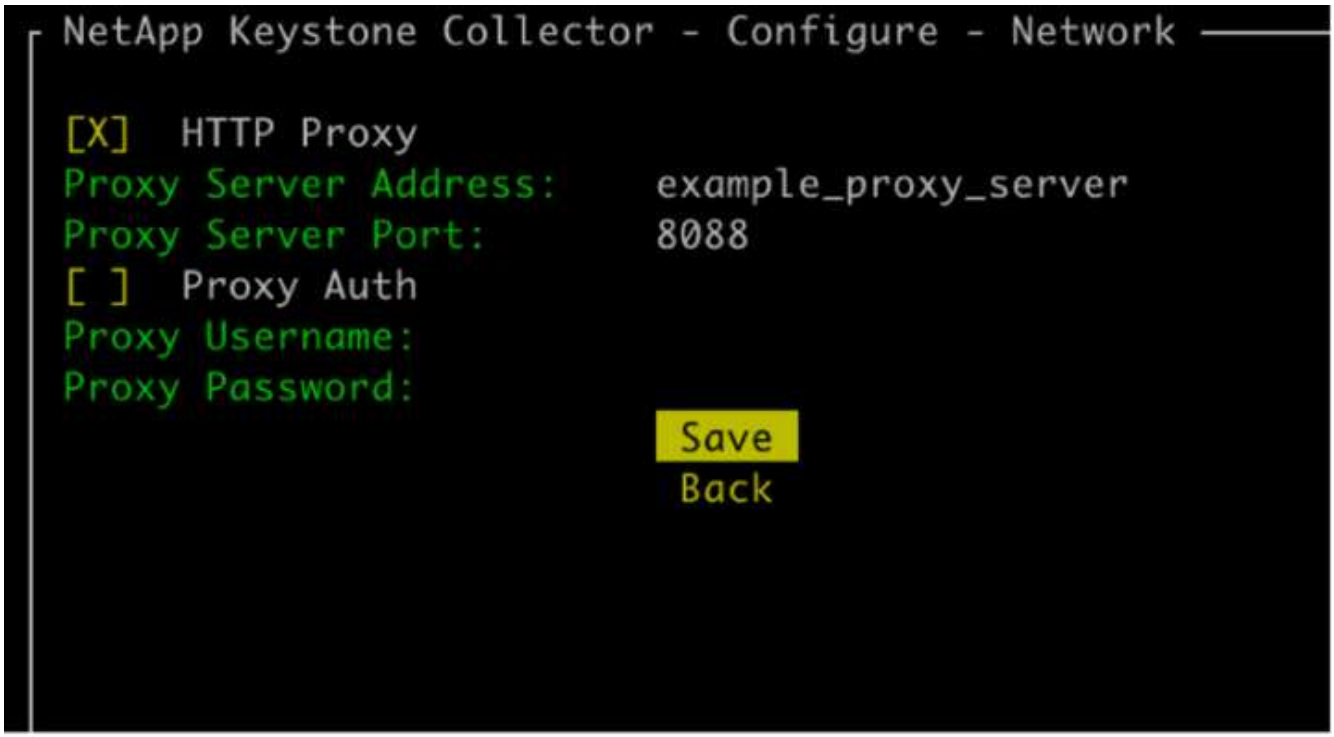
7. Uscire dalla TUI di gestione di Keystone Collector selezionando l'opzione **Esci dalla shell** nella schermata iniziale.

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**
   .



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.

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

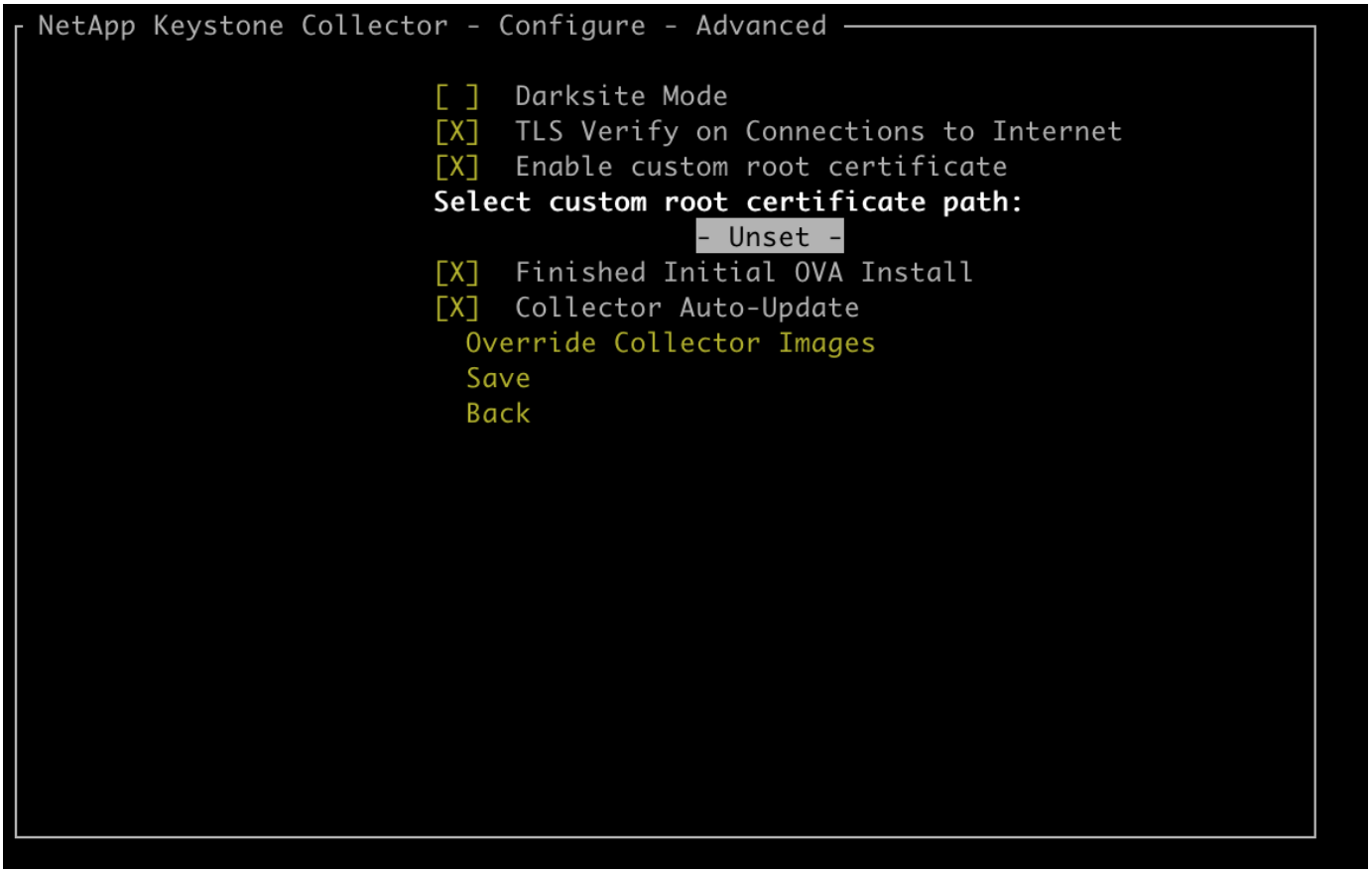
1. Preparare il certificato CA. Dovrebbe essere in formato di file X.509_ codificato in base64.

   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.

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



Crea livelli di servizio delle performance

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.

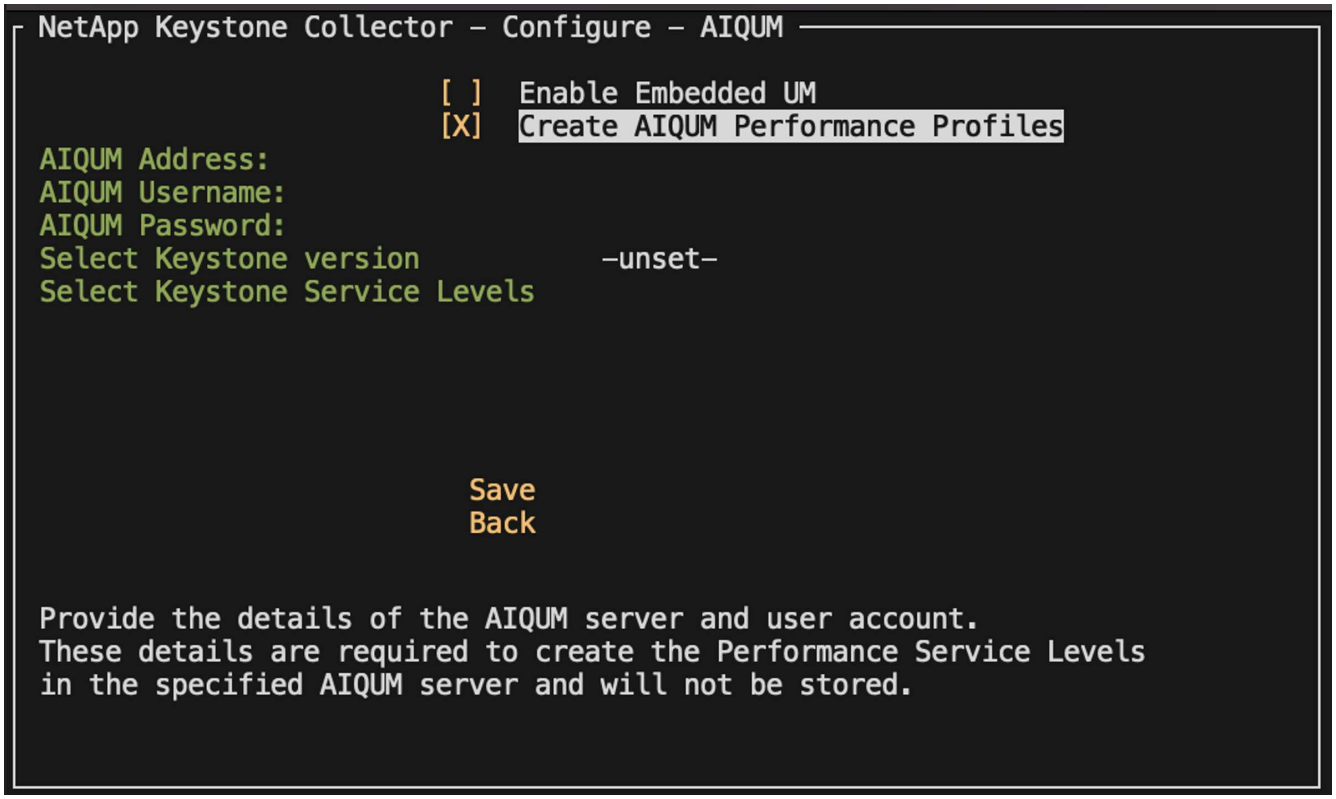
Per ulteriori informazioni sui PSL, fare riferimento alla sezione "Performance livelli di servizio".

Per ulteriori informazioni sui livelli di servizio, fare riferimento a "Livelli di servizio in Keystone".

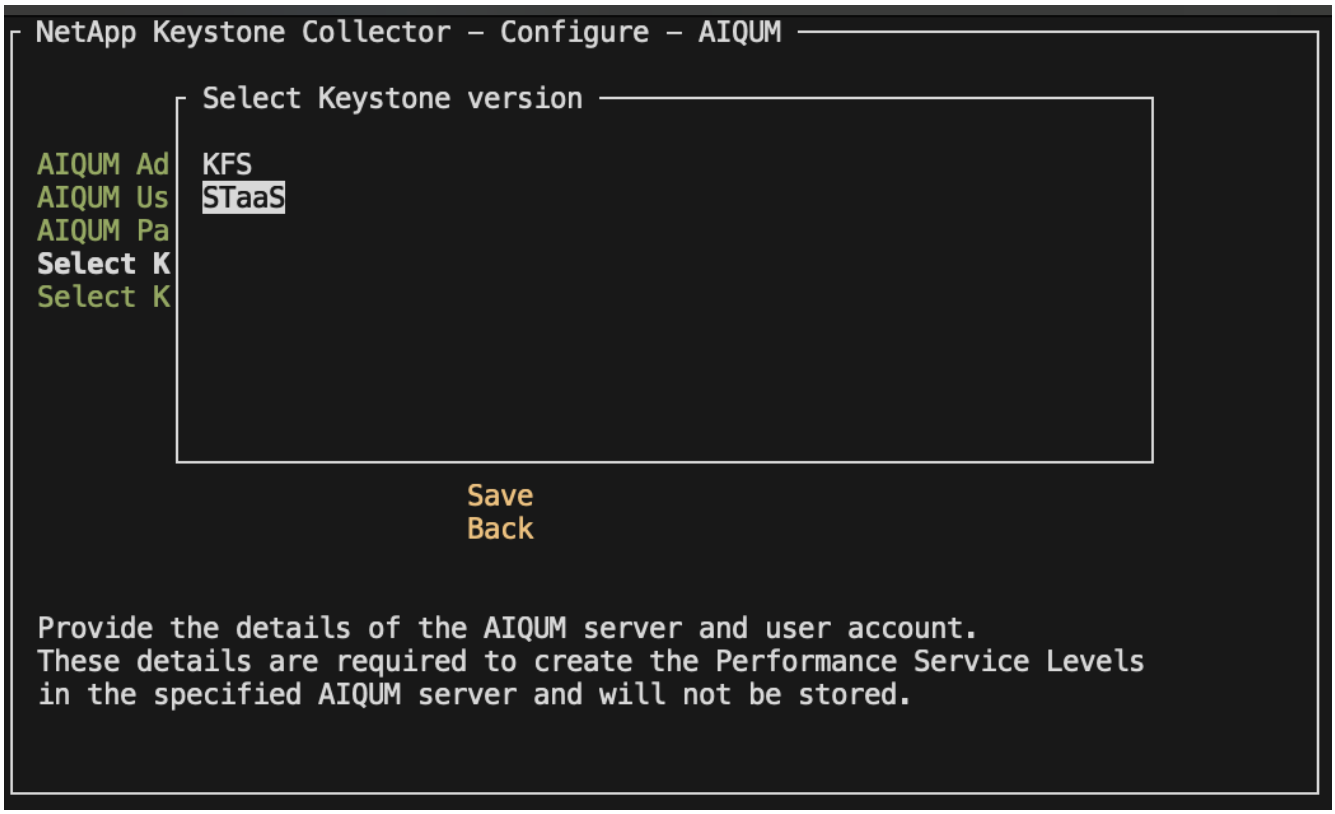
Fasi

1. Avviare l'utility 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.

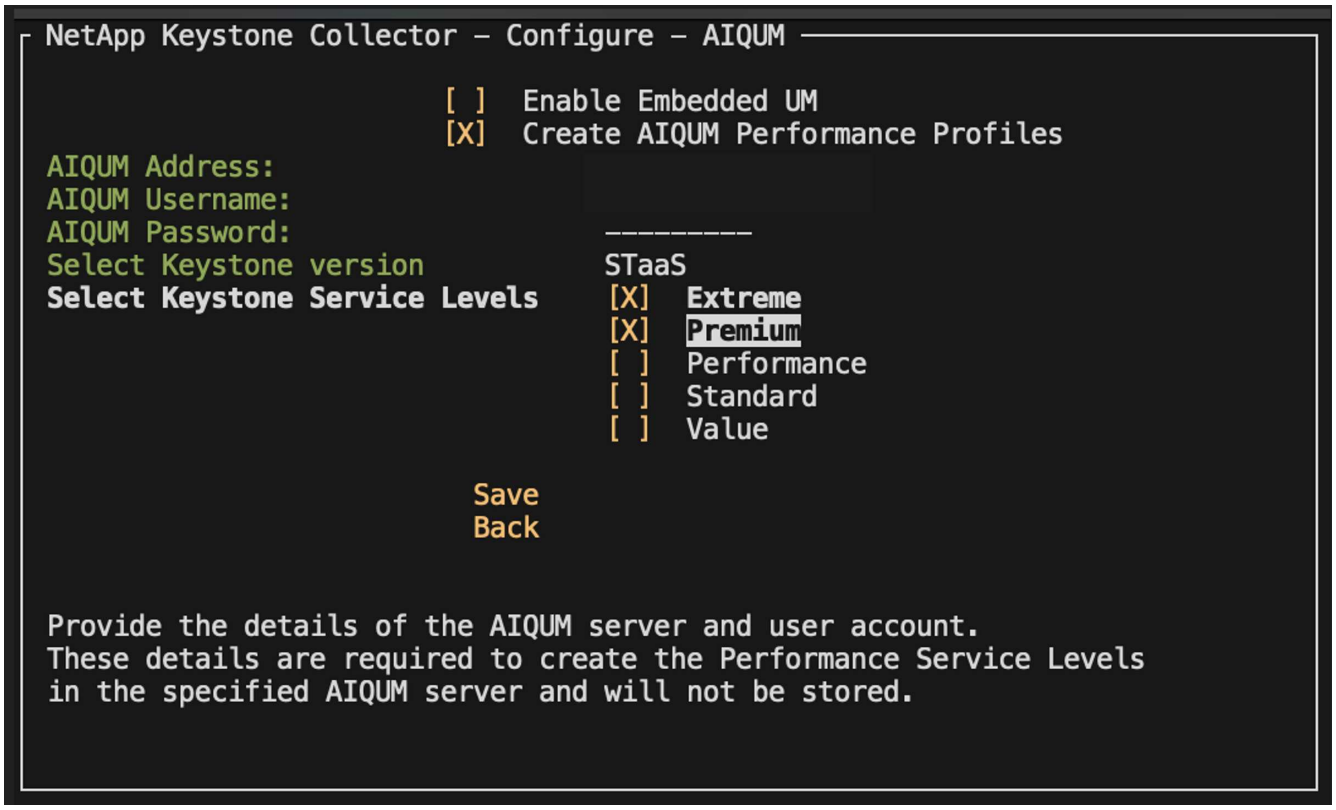


5. Per **Seleziona versione Keystone**, selezionare `-unset-`.
6. Premere Invio. Viene visualizzata una finestra di dialogo per la selezione della versione Keystone.
7. Evidenziare **STaaS** per specificare la versione Keystone per Keystone STaaS, quindi premere Invio.



È possibile evidenziare l'opzione **KFS** per i servizi di abbonamento Keystone versione 1. I servizi di 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 iscrizione Keystone | versione 1" .

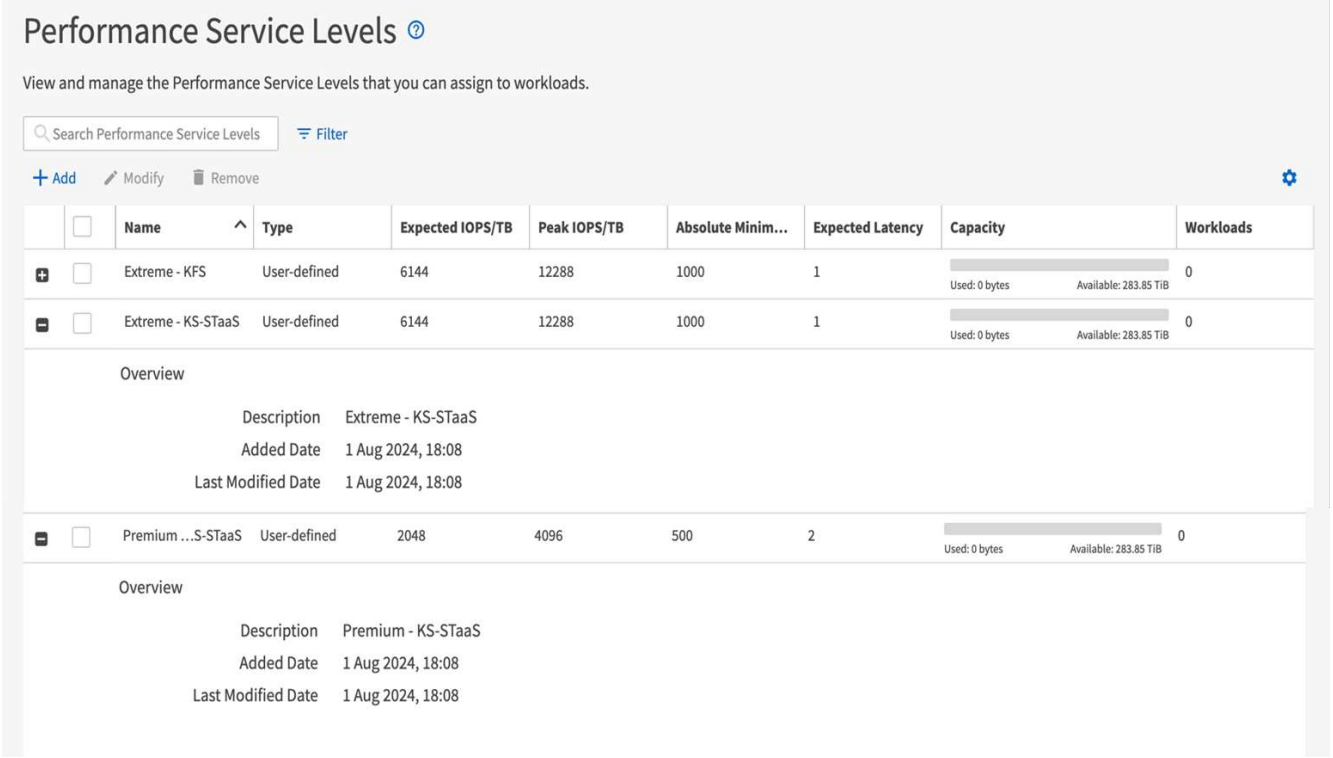
8. Tutti i livelli di servizio Keystone supportati verranno visualizzati nell'opzione *Seleziona livelli di servizio Keystone * per la versione Keystone specificata. Abilitare i livelli di servizio delle prestazioni desiderati dall'elenco.



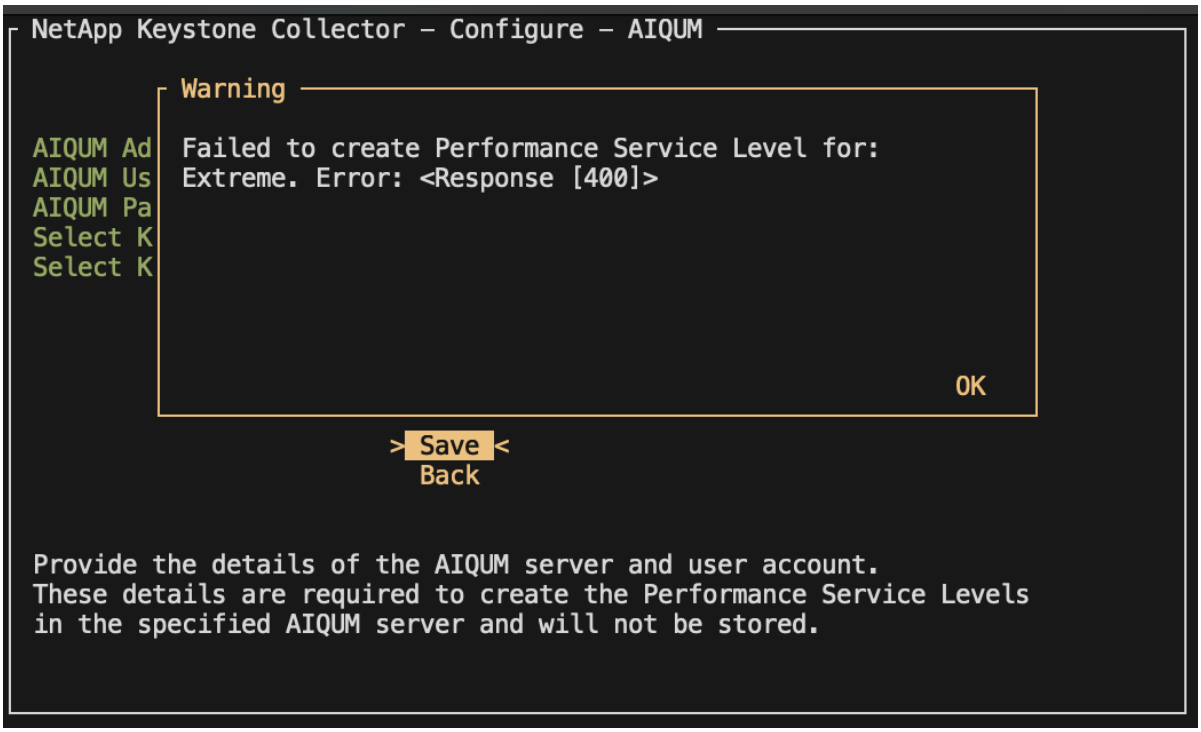
È possibile selezionare contemporaneamente più livelli di servizio prestazionali per creare PSL.

9. Selezionare **Salva** e premere Invio. Verranno creati 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".



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.



Installare ITOM Collector

Requisiti di installazione per Keystone ITOM Collector

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

Prerequisiti per la VM del server di raccolta ITOM:

- 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 più recenti.

- Requisito delle risorse: I requisiti delle risorse delle macchine virtuali in base al numero di nodi NetApp monitorati sono i seguenti:
  - 2-10 nodi: 4 CPU, 8 GB di RAM, disco da 40 GB
  - 12-20 nodi: 8 CPU, 16 GB di RAM, disco da 40 GB
- Requisito di configurazione: Verificare che un account di sola lettura e SNMP siano configurati sui dispositivi monitorati. La VM del server di raccolta ITOM 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.

Origine	Destinazione	Protocollo	Porte	Descrizione
Collettore ITOM	IP di gestione del cluster NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Monitoraggio delle centraline ONTAP
IP di gestione dei nodi e del cluster NetApp ONTAP	Collettore ITOM	SNMP, Syslog	UDP 162, UDP 514	Trap SNMP e Syslog dai controller
Collettore ITOM	Switch del cluster	SNMP	UDP 161	Monitoraggio degli interruttori
Switch del cluster	Collettore ITOM	SNMP, Syslog	UDP 162, UDP 514	Trap SNMP e Syslog dagli switch
Collettore ITOM	IP dei nodi StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitoraggio SNMP di StorageGRID
IP dei nodi StorageGRID	Collettore ITOM	SNMP, Syslog	UDP 162, UDP 514	Trap SNMP da StorageGRID

Collettore ITOM	Keystone Collector	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Monitoring e gestione remota Keystone Collector
Collettore ITOM	Local DNS (DNS locale)	DNS	UDP 53	Servizi DNS pubblici o privati
Collettore ITOM	Server NTP a scelta	NTP	UDP 123	Mantenimento del tempo

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 dei requisiti.

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

Per installare ITOM Collector su sistemi Windows, fare riferimento alla sezione "Installare ITOM Collector su sistemi Windows".

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

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** richiesto per il file di installazione di ITOM Collector.
- Assicurarsi che `sudo package` sia installato se si prevede di eseguire ITOM Collector come utente non root.

Fasi

1. Scaricare il file di configurazione di ITOM Collector sul server Linux.
2. Aprire un terminale sul server ed eseguire il comando seguente per modificare le autorizzazioni e rendere eseguibili i file binari:
   `# chmod +x <installer_file_name>.bin`
3. Eseguire il comando per avviare il file di configurazione di ITOM Collector:
   `#./<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. Immettere i dettagli utente per l'installazione.
   c. Specificare la directory principale di installazione.
   d. Selezionare la dimensione del raccoglitore.
   e. Fornisci i dettagli del proxy, se applicabile.

      Per ogni richiesta, viene visualizzata un'opzione predefinita. Si consiglia di selezionare l'opzione predefinita a meno che non si disponga di requisiti specifici. Premere il tasto **Invio** per scegliere l'opzione predefinita. Al termine dell'installazione, viene visualizzato un messaggio che conferma che

ITOM Collector è stato installato correttamente.

- Il file di configurazione di ITOM Collector aggiunge a `/etc/sudoers` per gestire i riavvii del servizio e i dump di memoria.
- L'installazione di ITOM Collector sul server Linux crea un utente predefinito chiamato **ITOM** per eseguire ITOM Collector senza root Privileges. È possibile scegliere un altro utente o eseguirlo come root, ma si consiglia di utilizzare l'utente ITOM creato dallo script di installazione di Linux.

Quali sono le prossime novità?

Una volta completata l'installazione, contattare il team di supporto Keystone per convalidare l'installazione di ITOM Collector attraverso il portale di supporto ITOM. Dopo la verifica, il team di supporto Keystone configurerà l'ITOM Collector in remoto, includendo ulteriori impostazioni di rilevamento e monitoraggio dei dispositivi, e invierà una conferma al termine della configurazione. Per qualsiasi domanda o informazione aggiuntiva, contattare keystone.services@NetApp.com.

Installa Keystone ITOM Collector sui sistemi Windows

Installare ITOM Collector su un sistema Windows scaricando il file di configurazione 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 configurazione di ITOM Collector, che scade tra due ore.

È possibile installarlo su sistemi Linux in base alle proprie esigenze. Per installare ITOM Collector su sistemi Linux, fare riferimento a "Installare ITOM Collector su sistemi Linux".

Per installare il software ITOM Collector sul server Windows, procedere come segue:

Prima di iniziare

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

Fasi

1. Scaricare il file di configurazione di ITOM Collector sul 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. Immettere le credenziali per l'account in cui verrà eseguito ITOM Collector:
   - Se ITOM Collector non sta monitorando altri server Windows, utilizzare il sistema locale.
   - Se ITOM Collector sta monitorando altri server Windows nello stesso dominio, utilizzare un account di dominio con autorizzazioni di amministratore locale.
   - Se ITOM Collector sta monitorando altri server Windows che non fanno parte dello stesso dominio, utilizzare un account amministratore locale e connettersi a ciascuna risorsa con 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 risorse monitorate.
5. Selezionare la dimensione del raccoglitore. La dimensione predefinita è quella consigliata in base al file di

installazione. Procedere con il formato consigliato a meno che non si disponga di requisiti specifici.

6. Selezionare *Avanti* per iniziare l'installazione. È possibile utilizzare la cartella popolata o sceglierne una diversa. Una finestra di stato visualizza l'avanzamento dell'installazione, seguito dalla finestra di dialogo InstallShield Wizard Completed (Installazione guidata InstallShield completata).

Quali sono le prossime novità?

Una volta completata l'installazione, contattare il team di supporto Keystone per convalidare l'installazione di ITOM Collector attraverso il portale di supporto ITOM. Dopo la verifica, il team di supporto Keystone configurerà l'ITOM Collector in remoto, includendo ulteriori impostazioni di rilevamento e monitoraggio dei dispositivi, e invierà una conferma al termine della configurazione. Per qualsiasi domanda o informazione aggiuntiva, contattare keystone.services@NetApp.com.

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.
    - 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 trigger AutoSupport nodo di sistema".

Monitoraggio e aggiornamento

Monitora la salute di Keystone Collector

Puoi monitorare lo stato di salute di Keystone Collector utilizzando qualsiasi sistema di monitoring che supporti le richieste HTTP. Il monitoraggio della salute può aiutare ad assicurare che i dati siano disponibili nella dashboard Keystone.

Per impostazione predefinita, i servizi sanitari Keystone non accettano connessioni da alcun IP diverso da localhost. L'endpoint di salute di Keystone è `/uber/health`E ascolta su tutte le interfacce del server Keystone Collector sulla porta `7777`. In caso di query, un codice di stato della richiesta HTTP con un output JSON viene restituito dall'endpoint come risposta, descrivendo lo stato del sistema Keystone Collector.
Il corpo JSON fornisce uno stato di salute generale per `is_healthy` attribute, che è un booleano, e un elenco dettagliato degli stati per componente per `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 esegue la query sullo stato di salute non è nell'elenco *allow*, che è un elenco di CIDR di rete consentiti. Per questo stato, non vengono restituite informazioni sullo stato di salute. L'elenco *allow* utilizza il metodo CIDR di rete per controllare quali dispositivi di rete sono autorizzati a eseguire query nel sistema di salute Keystone. Se si riceve questo errore, aggiungere il sistema di monitoraggio all'elenco *allow* da **Keystone Collector management TUI > Configure > Health Monitoring**.

> **Gli utenti Linux, notano questo problema noto:**
>
> **Descrizione del problema**: Keystone Collector esegue diversi container come parte del sistema di misurazione dell'utilizzo. Quando il server Red Hat Enterprise Linux 8.x viene rafforzato con le policy STIG (Security Technical Implementation Guide) della DISA (Defense Information Systems Agency) USA, si è verificato un problema noto con il demone delle policy di accesso ai file (Fapolicyd) in modo intermittente. Questo problema è identificato come "bug 1907870". **Soluzione**: Fino alla risoluzione da parte di Red Hat Enterprise, NetApp consiglia di risolvere questo problema mettendo in pratica `fapolicyd` in modalità permissiva. Poll `/etc/fapolicyd/fapolicyd.conf`, impostare il valore di `permissive = 1`.

Visualizzare i log 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 log di sistema possono essere rivisti attraverso l'utility di sistema standard *journalctl*. Per esaminare i registri, è possibile utilizzare i seguenti servizi chiave:

- ks-collector
- salute ks
- ks-autoupdate

Il principale servizio 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 viene riportato un esempio di successo di un processo per la raccolta di dati sull'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 viene riportato un esempio di successo di un lavoro per la raccolta opzionale dei dati sulle performance:

```
{"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"}
```

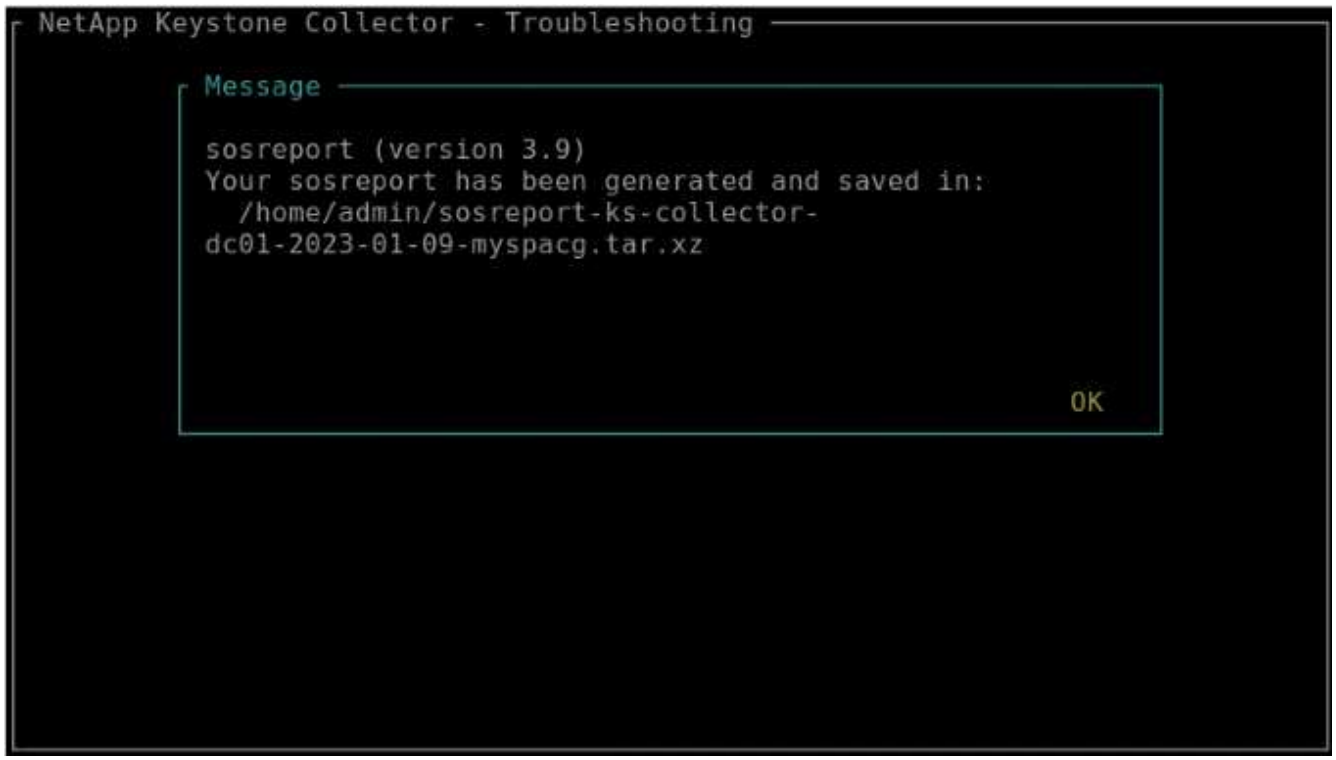
Generare e raccogliere pacchetti di supporto

L'interfaccia telefonica utente di Keystone Collector consente di generare bundle di supporto e di aggiungerli alle richieste di servizio per risolvere i problemi di supporto. Seguire questa procedura:

Fasi

1. Avviare l'utility TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Accedere a **risoluzione dei problemi > genera bundle di supporto**
   .

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



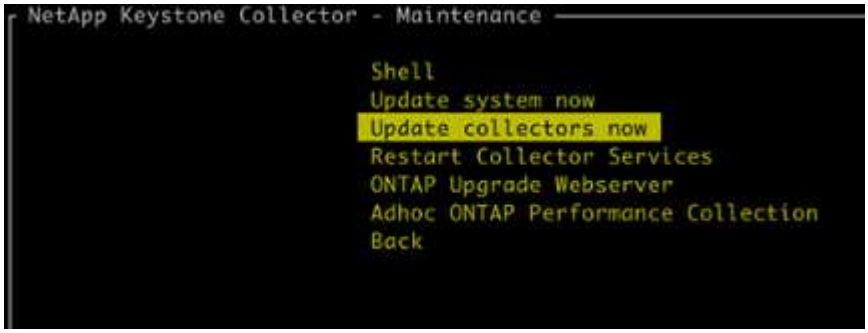
4. Una volta scaricato il file, è possibile allegarlo al ticket di supporto Keystone ServiceNow. Per informazioni sull'emissione dei biglietti, vedere "Generazione di richieste di servizio".

Aggiorna manualmente Keystone Collector

La funzione di aggiornamento automatico di Keystone Collector è attivata per impostazione predefinita, che aggiorna automaticamente il software Keystone Collector ad ogni nuova release. Tuttavia, è possibile disattivare questa funzione e aggiornare manualmente il software.

Fasi

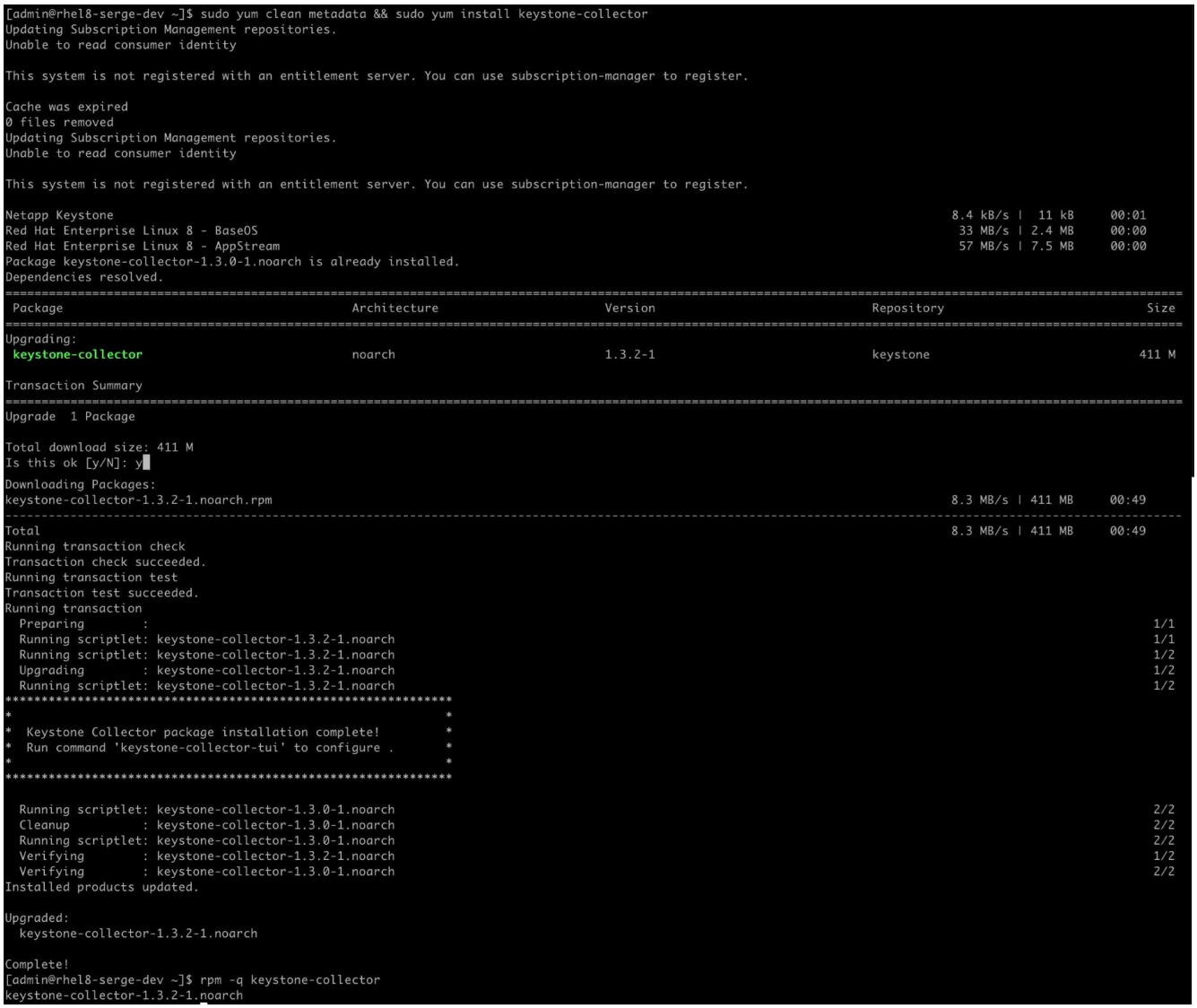
1. Avviare l'utility TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Nella schermata di manutenzione, selezionare l'opzione **Aggiorna raccolta ora**.



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 la TUI di gestione di Keystone Collector, è possibile visualizzare l'ultima versione nella parte superiore sinistra della schermata iniziale.

   In alternativa, eseguire 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 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 su configurazione, stato e 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 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
    - Fisico utilizzato
    - Dimensioni disponibili
    - Dimensione
    - Dimensioni utilizzate
- Aggregare gli archivi di oggetti
    - ObjectStoreName
    - ObjectStoreUID
    - ProviderType
    - Nome aggregato
- Clonare i volumi
    - FlexClone
    - Dimensione
    - Utilizzato
    - Server virtuale
    - Tipo
    - ParentVolume
    - ParentVserver
    - IsConstituent
    - SplitEtimate
    - 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
- MetroCluster
    - Nodo
    - Aggregato
    - LIF
    - Replica della configurazione
    - Connessioni
    - Cluster
    - Volumi
- Cluster MetroCluster
    - ClusterUID
    - Nome cluster
    - RemoteClusterUID
    - RemoteCluserName
    - LocalConfigurationState
    - RemoteConfigurationState
- 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
    - Storage
    - Volume di stoccaggio in uso
- Mediatori MetroCluster
    - Indirizzo del mediatore
    - Porto mediatore
    - Mediatore configurato
    - Mediatore raggiungibile
    - 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
- QoSNetworkLetency
- AvailableOps
- WriteLatency
- QoSCloudLatency
- QoSClusterInterconnectLatency
- OtherMBps
- QoSCopLatency
- QoSDBladeLatency
- Utilizzo

- ReadIOPS
- Mbps
- OtherIOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncSnapmirrorLatency
- Dati a livello di sistema
  - Scrittura/Lettura/Altro/IOPS totali
  - Scrittura/Lettura/Altro/Rendimento totale
  - Scrittura/Lettura/Altro/Latenza totale
- 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

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

- Percentuale di uptime SLA

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

Raccolta dati di telemetria

Dati di telemetria raccolti dalla VM Keystone Collector: 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
  - Dimensioni 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

Ulteriori informazioni su Keystone (modalità privata)

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

soddisfare i tuoi requisiti di business e di sicurezza. Questa modalità è disponibile per le organizzazioni con limitazioni di connettività.

NetApp offre un'implementazione specializzata di Keystone STaaS personalizzata per ambienti con connettività Internet limitata o assente (nota anche come siti dark). Si tratta di ambienti sicuri o isolati in cui la comunicazione esterna è limitata a causa di requisiti di sicurezza, conformità o operativi.

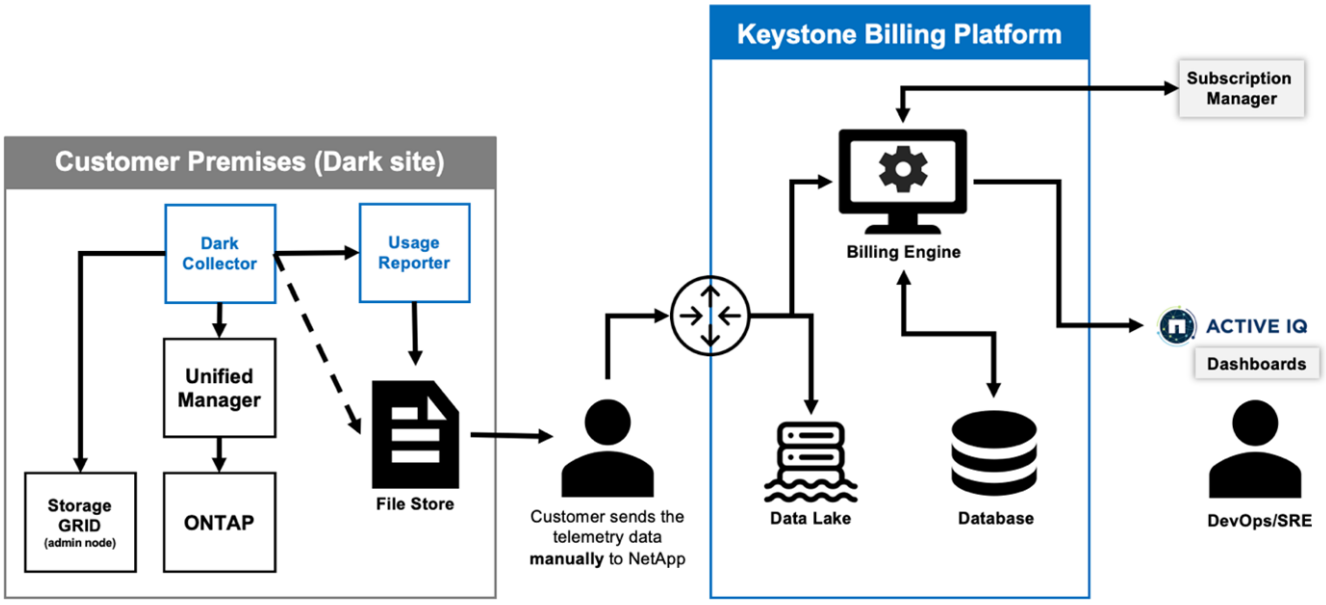
Per NetApp Keystone, offrire servizi per siti oscuri significa fornire il servizio di abbonamento storage flessibile di Keystone in un modo che rispetti i vincoli di questi ambienti. Ciò comporta:

- **Implementazione locale**: Keystone può essere configurato in modo indipendente all'interno di ambienti isolati, garantendo l'assenza di connettività Internet o di personale esterno per l'accesso all'installazione.
- **Operazioni offline**: Tutte le funzionalità di gestione dello storage con controlli dello stato di salute e fatturazione sono disponibili offline per le operazioni.
- **Sicurezza e conformità**: Keystone garantisce che la distribuzione soddisfi i requisiti di sicurezza e conformità dei siti oscuri, che possono includere crittografia avanzata, controlli di accesso sicuri e funzionalità di controllo dettagliate.
- **Guida e supporto**: NetApp offre un supporto globale 24/7 ore su 24, 7 giorni su 7 con un responsabile del successo Keystone dedicato assegnato a ciascun account per assistenza e risoluzione dei problemi.

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

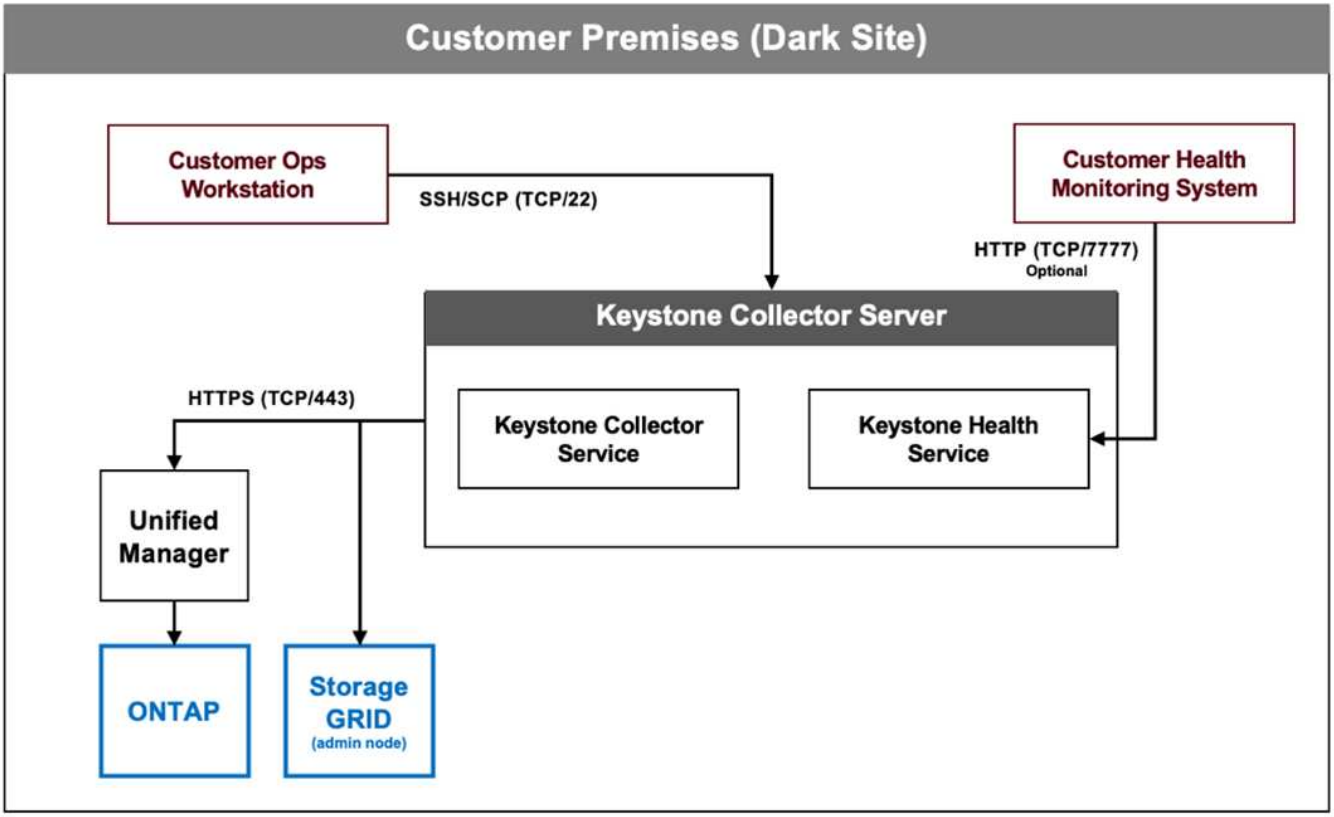
Keystone Collector in modalità privata

Keystone Collector è responsabile della raccolta periodica dei dati sull'utilizzo dai sistemi storage e dell'esportazione delle metriche in un reporter di utilizzo offline e in un archivio file locale. I file generati, creati sia in formato crittografato che in formato testo normale, vengono quindi inoltrati manualmente a NetApp dall'utente dopo i controlli di convalida. Al ricevimento, la piattaforma di fatturazione Keystone di NetApp autentica ed elabora questi file, integrandoli nei sistemi di fatturazione e gestione degli abbonamenti per calcolare le spese 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 di salute esegue controlli dello stato del sistema ed è progettato per interfacciarsi con i sistemi di monitoraggio dello stato utilizzati dal cliente. Questi rapporti sono disponibili per l'accesso offline da parte degli utenti, consentendo la convalida e agevolando la 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 *dark site* o *private mode*, assicurarsi che i sistemi siano preparati con il software necessario e soddisfino tutti i prerequisiti richiesti.

Requisiti di VMware vSphere

- Sistema operativo: VMware vCenter Server ed ESXi 8.0 o versioni successive
- Core: 1 CPU
- RAM: 2 GB
- Spazio su disco: Disco virtuale da 20 GB

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: Disco virtuale da 50 GB
  - Almeno 2 GB di spazio libero in `/var/lib/`
  - Almeno 48 GB di spazio libero 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-versionlock
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionlock
- Debian V12
  - python3 >= v3,9.0, python3 <= v3.12.0
  - podman
  - report sul sistema

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 del gateway API attivata.
- Il server Unified Manager deve essere accessibile dal server Keystone Collector sulla porta 443 (HTTPS).
- È necessario configurare un account di servizio con autorizzazioni Application User per Keystone Collector sul server Unified Manager.
- La connettività Internet esterna non è necessaria.
- 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 aiuto con Keystone".

Installare Keystone Collector in modalità privata

Completare alcuni passaggi per installare Keystone Collector in un ambiente che non

dispone di accesso a Internet, noto anche come *dark site* o *private mode*. Questo tipo di installazione è perfetto per i siti sicuri.

A seconda dei requisiti, puoi implementare Keystone Collector sui sistemi VMware vSphere o installarlo su sistemi Linux. Seguire la procedura di installazione corrispondente all'opzione selezionata.

Implementazione su VMware vSphere

Attenersi alla seguente procedura:

1. Scaricare il file del modello OVA da "Portale web NetApp Keystone".
2. Per la procedura di distribuzione di Keystone Collector con il file OVA, fare riferimento alla sezione "Implementazione del modello OVA".

Installare 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 server Linux, procedere come segue:

1. Scaricare o trasferire il file di installazione di Keystone Collector al server Linux:

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

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

   - **Usare il pacchetto Debian**

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

   - **Utilizzando il file RPM**

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

     oppure

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

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

Configurare Keystone Collector in modalità privata

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

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

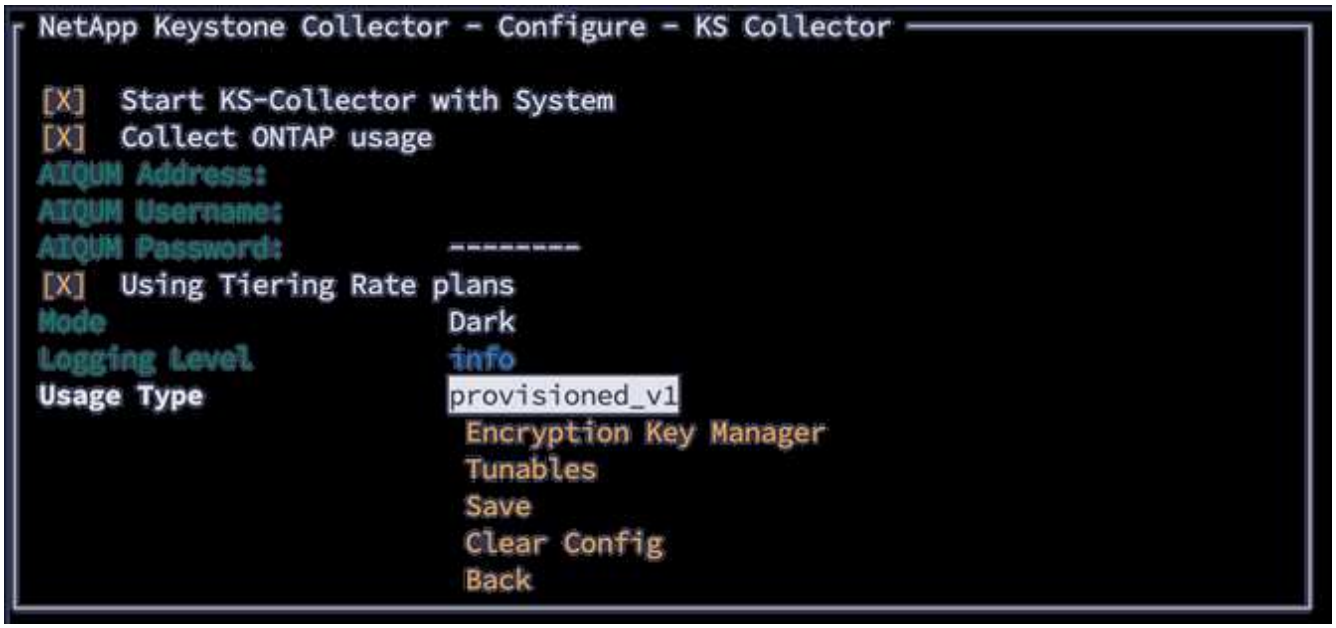
1. Avviare l'utility TUI di gestione di Keystone Collector:

   ```
   keystone-collector-tui
   ```

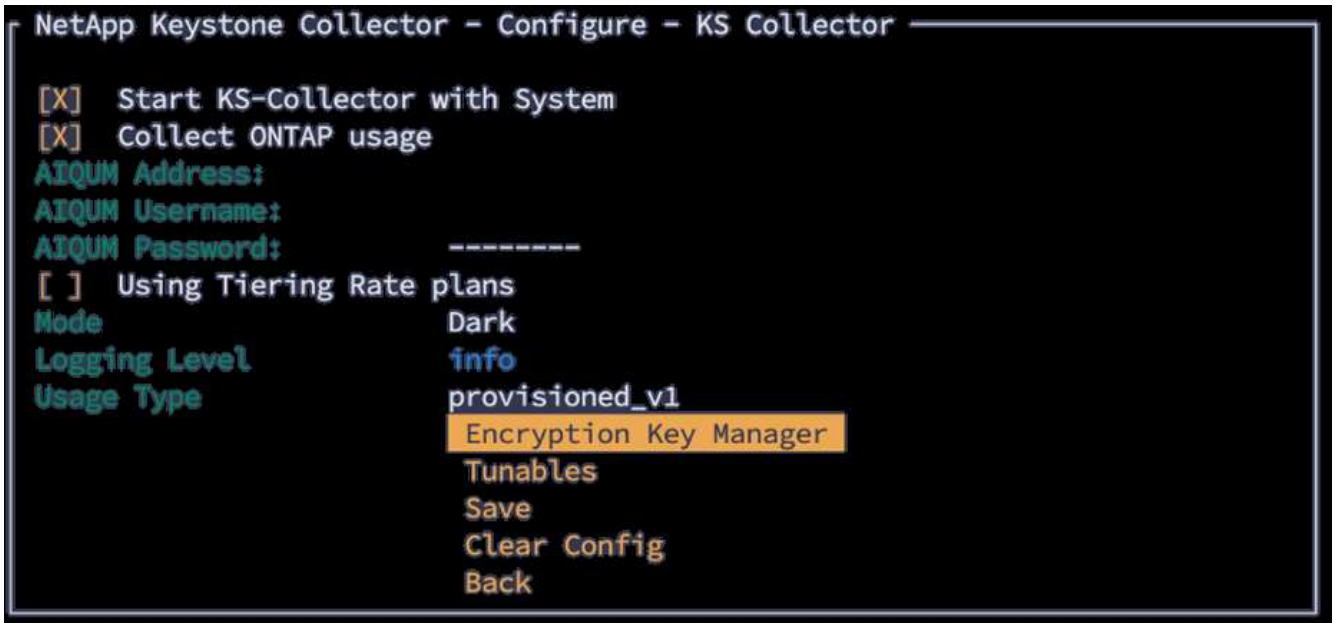
2. Andare a **Configura > Avanzate**.
3. Attivare/disattivare l'opzione **modalità Darksite**.

4. Selezionare **Salva**.
5. Andare a **Configure > KS-Collector** per configurare Keystone Collector.
6. Attivare/disattivare il campo **Avvia KS Collector con sistema**.
7. Attivare/disattivare il campo **Collect ONTAP Usage**. Aggiungere i dettagli del server Active IQ Unified Manager (Unified Manager) e dell'account utente.
8. **Opzionale**: Attivare il campo **utilizzo dei piani di velocità di tiering** se è necessario il tiering dei dati per l'abbonamento.
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.



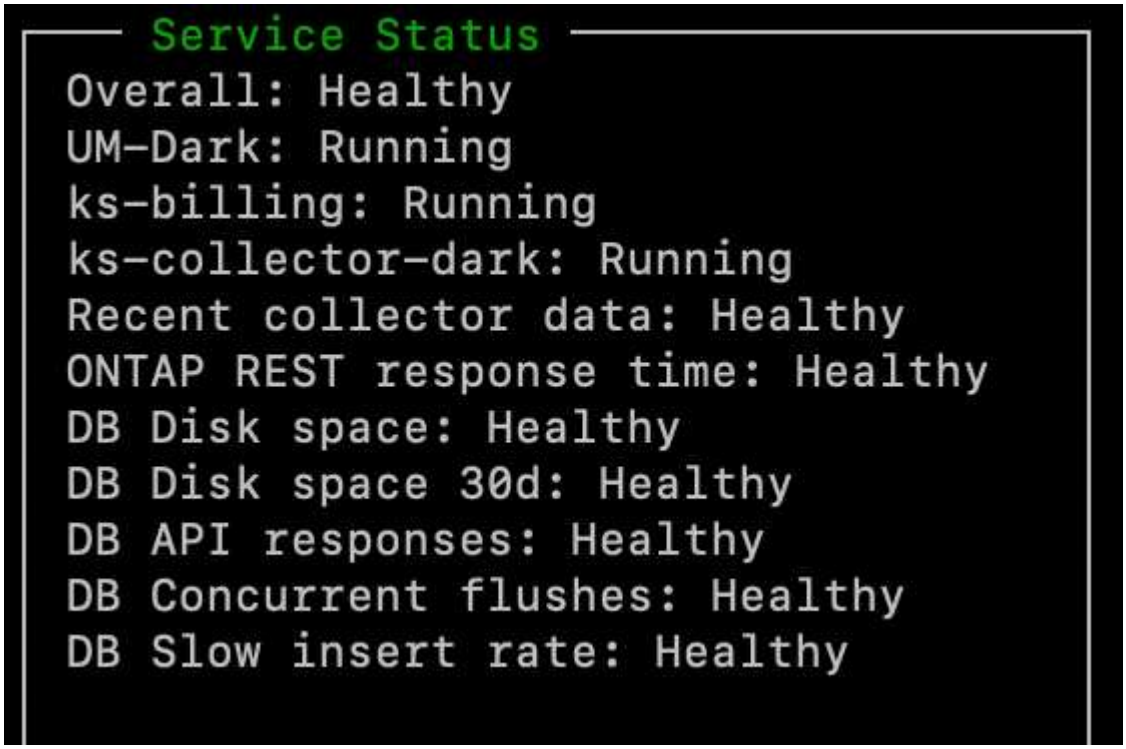
10. Selezionare **Salva**.
11. Andare a **Configure > KS-Collector** per generare il keypad di Keystone Collector.
12. Accedere a **Encryption Key Manager** e premere Invio.



13. Selezionare **generate Collector KeyPair** e premere Invio.

14. Verificare che Keystone Collector sia in uno stato integro tornando alla schermata principale dell'interfaccia telefonica utente e verificando le informazioni **Stato servizio**. Il sistema dovrebbe mostrare che i servizi sono in uno stato **generale: Sano**. Attendere fino a 10 minuti, se lo stato generale rimane non corretto

dopo questo periodo, rivedere i passaggi di configurazione precedenti e contattare il team di supporto NetApp.



15. Uscire dalla TUI di gestione di Keystone Collector selezionando l'opzione **Esci alla shell** nella schermata iniziale.
16. Recuperare 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 report di utilizzo

Alla fine di ogni mese, dovresti inviare il report mensile di riepilogo dell'utilizzo a NetApp. È possibile generare questo rapporto manualmente.

Per generare il rapporto di utilizzo, procedere come segue:

1. Andare a **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 non crittografato che un file crittografato, che devono essere inviati manualmente a NetApp. Il report su file in chiaro 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-----
```

Aggiornamento ONTAP

Keystone Collector supporta gli aggiornamenti di ONTAP tramite TUI.

Per aggiornare ONTAP, procedere come segue:

1. Andare a **manutenzione > ONTAP Server Web di aggiornamento**.
2. Copiare il file immagine di aggiornamento ONTAP in **/opt/NetApp/ONTAP-upgrade/**, quindi selezionare **Avvia server Web** per avviare il server Web.

3. `http://<collector-ip>:8000`Per assistenza sull'aggiornamento, visitare il sito Web utilizzo di un browser Web.

Riavvia Keystone Collector

È possibile riavviare il servizio Keystone Collector tramite l'interfaccia telefonica utente (TUI). Accedere a **manutenzione > Riavvia servizi Collector** nella TUI. Tutti i servizi di raccolta verranno riavviati e il relativo stato può essere monitorato dalla schermata iniziale dell'interfaccia telefonica utente (TUI).

Monitorare la salute di Keystone Collector in modalità privata

Puoi monitorare lo stato di salute di Keystone Collector utilizzando qualsiasi sistema di monitoring che supporti le richieste HTTP.

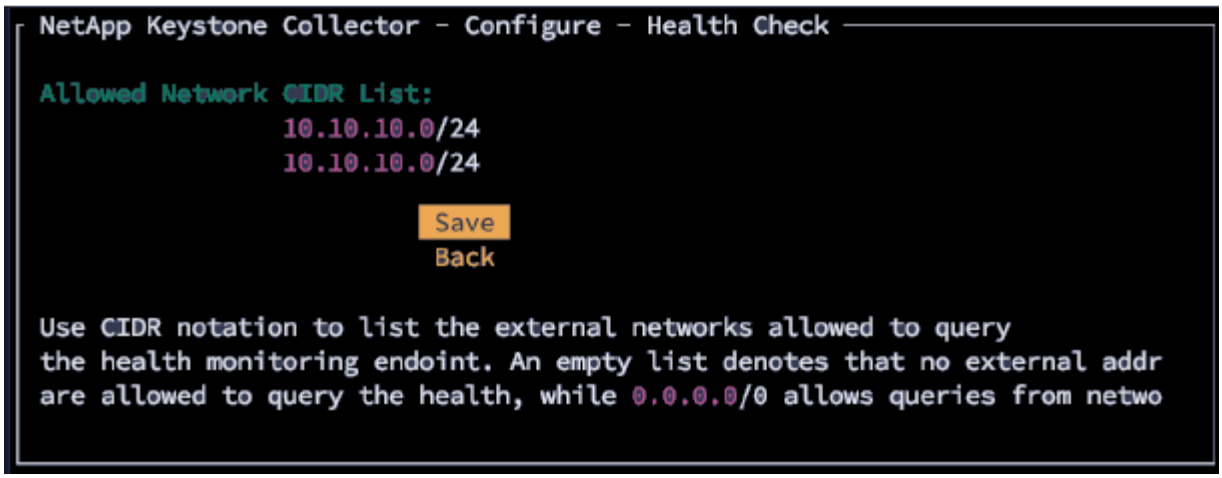
Per impostazione predefinita, i servizi sanitari Keystone non accettano connessioni da alcun IP diverso da localhost. L'endpoint di salute di Keystone è `/uber/health`E ascolta su tutte le interfacce del server Keystone Collector sulla porta `7777`. In caso di query, un codice di stato della richiesta HTTP con un output JSON viene restituito dall'endpoint come risposta, descrivendo lo stato del sistema Keystone Collector.
Il corpo JSON fornisce uno stato di salute generale per `is_healthy` attribute, che è un booleano, e un elenco dettagliato degli stati per componente per `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 esegue la query sullo stato di salute non è nell'elenco *allow*, che è un elenco di CIDR di rete consentiti. Per questo stato, non vengono restituite informazioni sullo stato di salute.

  L'elenco *allow* utilizza il metodo CIDR di rete per controllare quali dispositivi di rete sono autorizzati a eseguire query nel sistema di salute Keystone. Se si riceve l'errore 403, aggiungere il sistema di monitoraggio all'elenco *allow* da **Keystone Collector management TUI > Configure > Health Monitoring**.

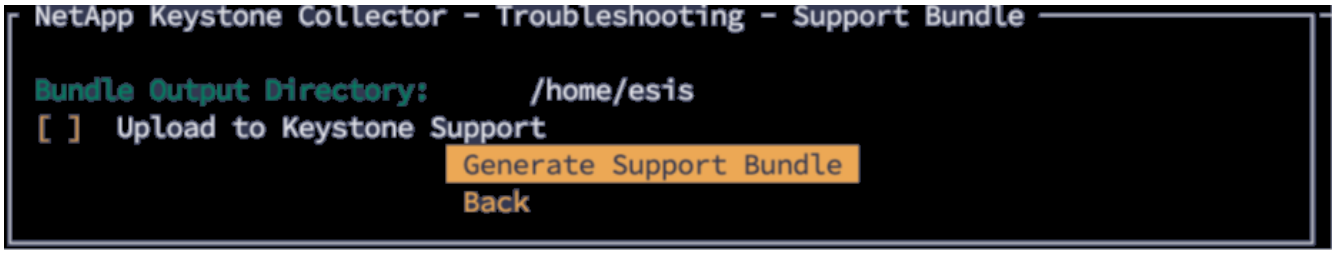


Generare e raccogliere pacchetti di supporto

Per risolvere i problemi con Keystone Collector, puoi collaborare con il supporto NetApp che potrebbe richiedere un file *.tar*. È possibile generare questo file tramite l'utility Keystone Collector management TUI.

Per generare un file *.tar*, procedere come segue:

1. Accedere a **risoluzione dei problemi > genera bundle di supporto**.
2. Selezionare la posizione in cui salvare il pacchetto, quindi fare 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".