Impostare e configurare Keystone

Keystone

NetApp
April 05, 2024

Sommario

Impostare e configurare Keystone

Panoramica di Keystone Collector

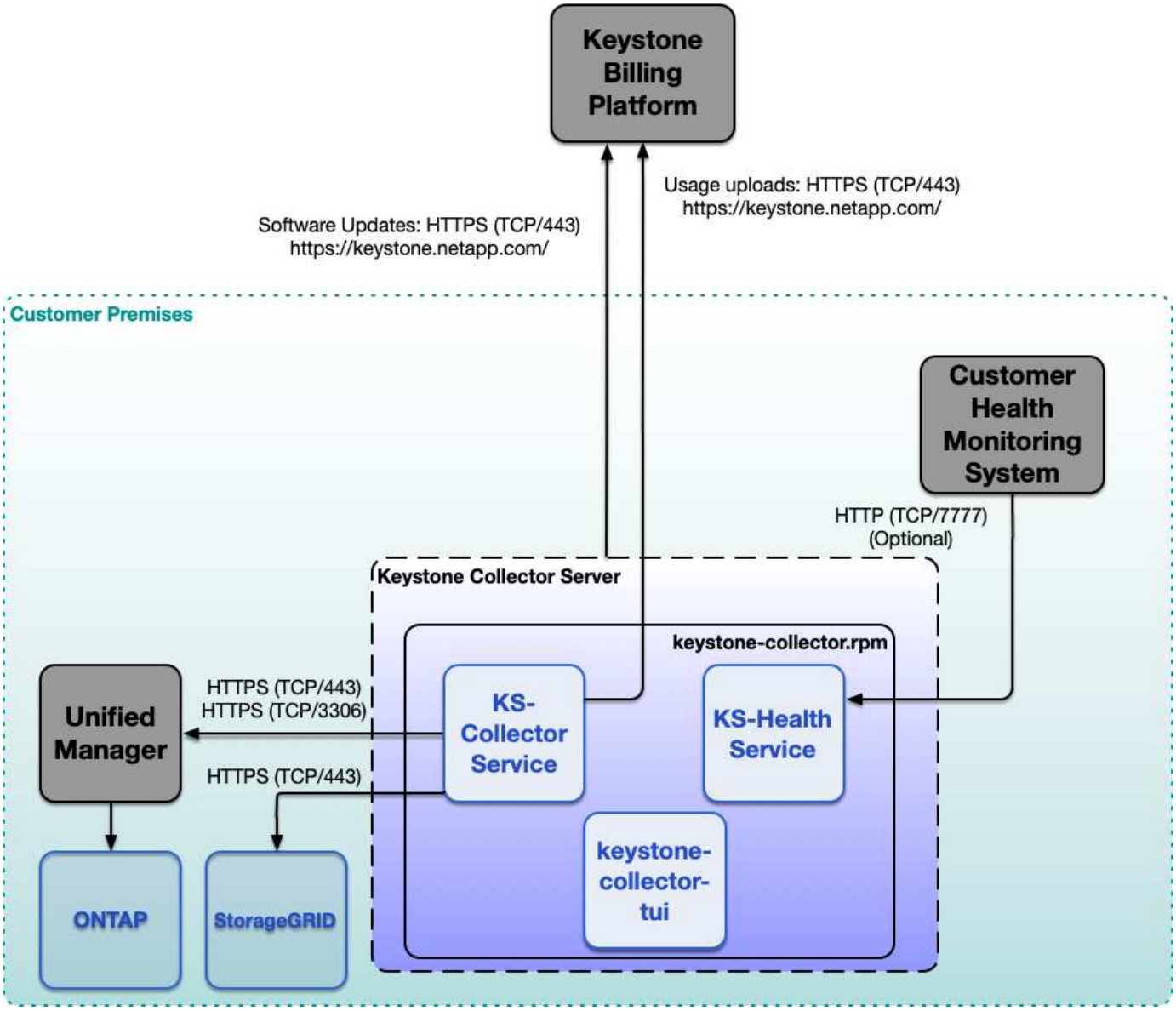
Per utilizzare i servizi Keystone e visualizzare i dati di utilizzo, è necessario installare Keystone Collector su un sistema VMware vSphere o Linux presso la propria sede.

> Keystone Collector rappresenta l'approccio standard di raccolta dei dati di utilizzo per i sistemi Keystone. Se il tuo ambiente non può supportare Keystone Collector, puoi richiedere l'autorizzazione alla gestione dei prodotti Keystone per utilizzare il meccanismo di telemetria di AutoSupport come alternativa. Per informazioni su AutoSupport, vedere "AutoSupport". Per informazioni sulla configurazione di AutoSupport per Keystone, consulta "Configura AutoSupport per Keystone".

Keystone Collector è il componente di acquisizione dell'utilizzo della piattaforma di fatturazione Keystone che sfrutta Active IQ Unified Manager e altre applicazioni per connettersi ai sistemi ONTAP e StorageGRID per raccogliere i metadati richiesti per l'utilizzo e il calcolo delle performance SLA delle sottoscrizioni Keystone. Consente di monitorare lo stato di salute del sistema e di inviare i dati di fatturazione per la creazione di report.

> Le informazioni di installazione e configurazione disponibili sono valide per ONTAP e StorageGRID. I requisiti e le procedure sono generici sia per ONTAP che per StorageGRID, con le eccezioni evidenziate.

Questo diagramma di architettura illustra i componenti costitutivi e la loro connettività in un tipico ambiente Keystone.



Preparare il sistema

Requisiti dell'infrastruttura virtuale

Sono necessarie alcune configurazioni dell'infrastruttura virtuale per l'installazione di Keystone Collector sui sistemi VMware vSphere.

Prerequisiti per la macchina virtuale del server Keystone Collector:

- Sistema operativo: Server VMware vCenter e ESXi 6.5 o versione successiva
- Core: 1 CPU
- RAM: 2 GB DI RAM
- Spazio su disco: Disco virtuale da 20 GB

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

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

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

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

Keystone Collector (per Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funzionalità opzionale	Raccolta di metriche delle performance per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 777	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

Accesso all'URL

Keystone Collector deve accedere ai seguenti host Internet:

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

Requisiti di sistema per Linux

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

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

Server Linux:

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

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

- Podman (gestore POD)

- sos
- cronico
- python 3 (da 3.6.8 a 3.9.13)

Macchina virtuale del server collettore di Keystone:

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

Altri requisiti

Assicurarsi che siano soddisfatti i seguenti requisiti generici:

Requisiti di rete

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

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

Origine	Destinazione	Servizio	Protocollo e porte	Categoria	Scopo
Keystone Collector (per Keystone ONTAP)	Active IQ Unified Manager (gestore unificato)	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone ONTAP)	Raccolta di metriche sull'utilizzo di Keystone Collector per ONTAP
Keystone Collector (per Keystone StorageGRID)	Nodi di amministrazione StorageGRID	HTTPS	TCP 443	Obbligatorio (se si utilizza Keystone StorageGRID)	Raccolta di metriche sull'utilizzo di Keystone Collector per StorageGRID
Keystone Collector (generico)	Internet (in base ai requisiti URL forniti in seguito)	HTTPS	TCP 80, TCP 443	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche

Keystone Collector (generico)	Proxy HTTP del cliente	Proxy HTTP	Porta proxy del cliente	Obbligatorio (connettività Internet)	Caricamento di software Keystone Collector, aggiornamenti del sistema operativo e metriche
Keystone Collector (generico)	Server DNS del cliente	DNS	TCP/UDP 53	Obbligatorio	Risoluzione DNS
Keystone Collector (generico)	Server NTP del cliente	NTP	UDP 123	Obbligatorio	Sincronizzazione dell'ora
Keystone Collector (per Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funzionalità opzionale	Raccolta di metriche delle performance per Keystone Collector
Keystone Collector (generico)	Sistema di monitoraggio dei clienti	HTTPS	TCP 777	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

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

È necessario completare alcuni prerequisiti aggiuntivi per ONTAP e StorageGRID. Assicurarsi di aver completato questi prerequisiti specifici oltre ai requisiti di sistema di Linux/VMware vSphere. Fare clic sulla scheda Required (richiesto) per ulteriori informazioni.

ONTAP

Versioni software

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

Prima di iniziare

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

   Interfaccia utente Web

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

   CLI

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

   a. Sul server Unified Manager, avviare una sessione SSH e accedere a Unified Manager CLI. `um cli login -u <*umadmin*>`Per informazioni sui comandi CLI, vedere "Comandi CLI di Unified Manager supportati".
   b. Verificare che il gateway API sia già abilitato. `um option list api.gateway.enabled`R `true` Valore indica che il gateway API è attivato.
   c. Se il valore restituito è `false`, eseguire questo comando: `um option set api.gateway.enabled=true`
   d. Riavviare il server Unified Manager:
      - Linux: "Riavvio di Unified Manager".

- VMware vSphere: "Riavvio della macchina virtuale di Unified Manager".

StorageGRID

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

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

  Fasi

  a. Accedere a Grid Manager. Vedere "Accedi a Grid Manager".

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

  c. Aggiungere le seguenti autorizzazioni:

  - Account tenant
  - Manutenzione
  - Query metriche

  d. Creare un utente dell'account del servizio Keystone e associarlo al gruppo di amministratori. Vedere "Gestire gli utenti".

Installare Keystone Collector

Implementare Keystone Collector su sistemi VMware vSphere

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

Implementazione del modello OVA

Attenersi alla seguente procedura:

Fasi

1. Scaricare il file OVA da "questo link" E memorizzarlo sul sistema VMware vSphere.
2. Sul sistema VMware vSphere, accedere alla vista **macchine virtuali e modelli**.
3. Fare clic con il pulsante destro del mouse sulla cartella desiderata per la macchina virtuale (VM) (o il data center, se non si utilizzano cartelle VM) e selezionare **Deploy OVF Template** (implementa modello OVF).
4. Nella *fase 1* della procedura guidata **Deploy OVF Template**, fare clic su **Select and OVF template** (Seleziona e modello OVF) per selezionare il modello scaricato `KeystoneCollector-latest.ova` file.
5. Al *passaggio 2*, specificare il nome della macchina virtuale e selezionare la cartella della macchina virtuale.
6. Nel *passaggio 3*, specificare la risorsa di calcolo richiesta per l'esecuzione della macchina virtuale.
7. Al *passaggio 4: Verifica dei dettagli*, verifica la correttezza e l'autenticità del file OVA.

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

VCenter 7.0u1 e versioni precedenti: Ulteriori informazioni

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

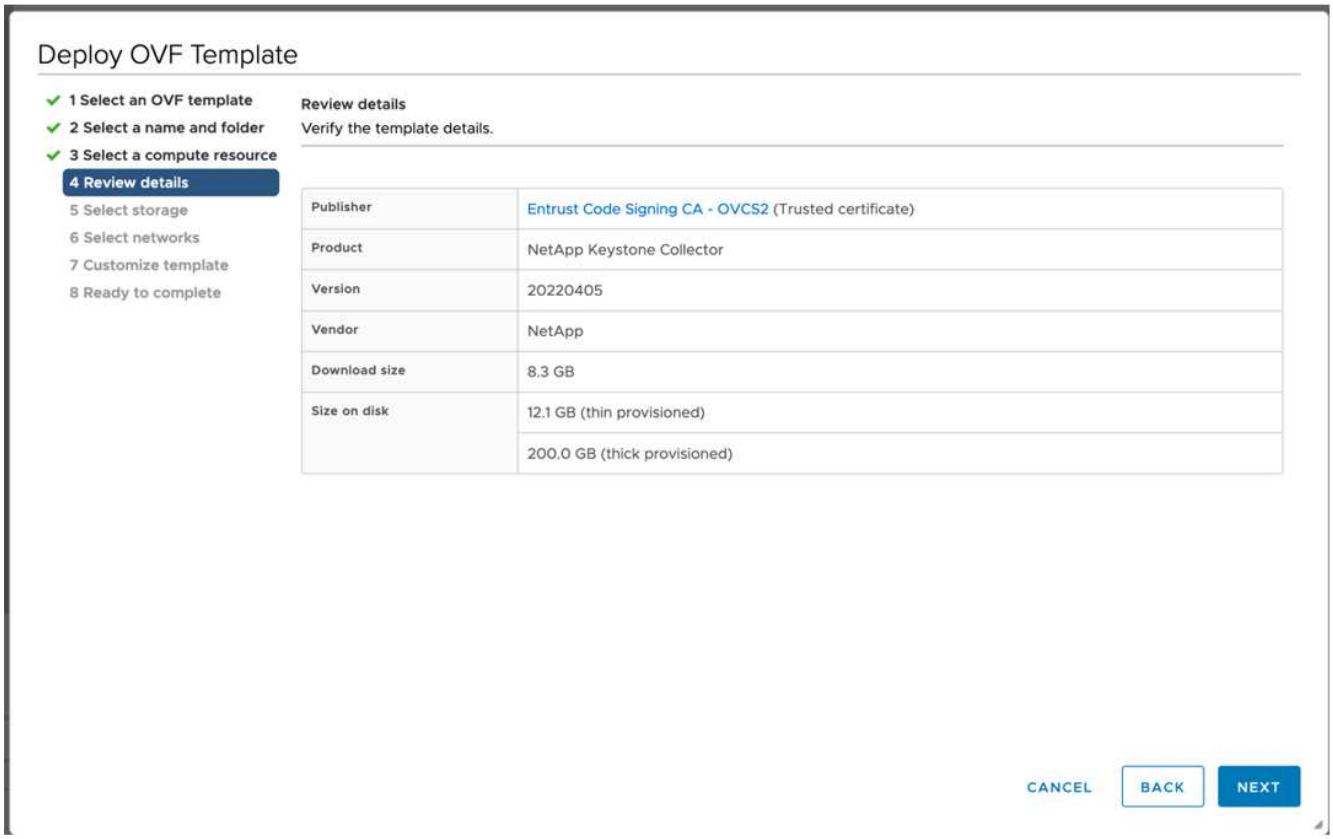
a. Fare clic sul collegamento **Publisher** per scaricare il certificato di digest completo della firma.
b. Scarica il certificato pubblico di fatturazione Keystone da "questo link".
c. Verificare l'autenticità del certificato di firma OVA rispetto al certificato pubblico utilizzando OpenSSL:
`openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert`

VCenter 7.0u2 e versioni successive: Ulteriori informazioni

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

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

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



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

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

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

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

Configurazione iniziale del sistema

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

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

1. Aprire una sessione SSH sul server di Keystone Collector. All'accesso, viene visualizzata l'interfaccia telefonica utente (TUI). In alternativa, è possibile avviare l'interfaccia telefonica utente manualmente eseguendo `keystone-collector-tui` Comando CLI.
2. Se necessario, configurare i dettagli del proxy nella sezione **Configurazione > rete** dell'interfaccia telefonica utente.
3. Aggiornare Keystone Collector utilizzando l'opzione **manutenzione > Aggiorna sistema**. Alcuni mirror selezionati potrebbero non essere disponibili e i dettagli del sistema vengono aggiornati dopo alcuni tentativi.
4. Configurare il nome host, la posizione e il server NTP del sistema nella sezione **Configurazione > sistema**.
5. Aggiornare la password admin nella sezione **manutenzione > utente**.
6. Contrassegnare la configurazione OVA iniziale come completata nella sezione **Configurazione > Avanzate**.

Installare Keystone Collector su sistemi Linux

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

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

1. SSH al server di Keystone Collector e passare a. `root` privilegio.
2. Importare la firma pubblica Keystone:
   `# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101`
3. Verificare che sia stato importato il certificato pubblico corretto controllando l'impronta digitale per Keystone Billing Platform nel database RPM:
   `# rpm -qa gpg-pubkey --qf '%<Description>'|gpg --show-keys --fingerprint`
   L'impronta digitale corretta è simile al seguente:
   `90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D`
4. Scaricare il `keystonerepo.rpm` file:
   `curl -O https://keystone.netapp.com/repo/keystonerepo.rpm`
5. Verificare l'autenticità del file:
   `rpm --checksig -v keystonerepo.rpm`Una firma per un file autentico è simile a questa:
   `Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK`
6. Installare il file repository del software YUM:
   `# yum install keystonerepo.rpm`
7. Una volta installato Keystone repo, installare il pacchetto keystone-collector tramite YUM Package Manager:
   `# yum install keystone-collector`

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

Convalida automatica dell'integrità del software

Esiste un processo ripetitivo per la convalida dell'integrità del software Keystone.

La configurazione del client del repository YUM di Keystone 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 per attivare e associare il componente di raccolta richiesto all'ambiente di storage.

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

Fasi

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

   ** FOR ONTAP **

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

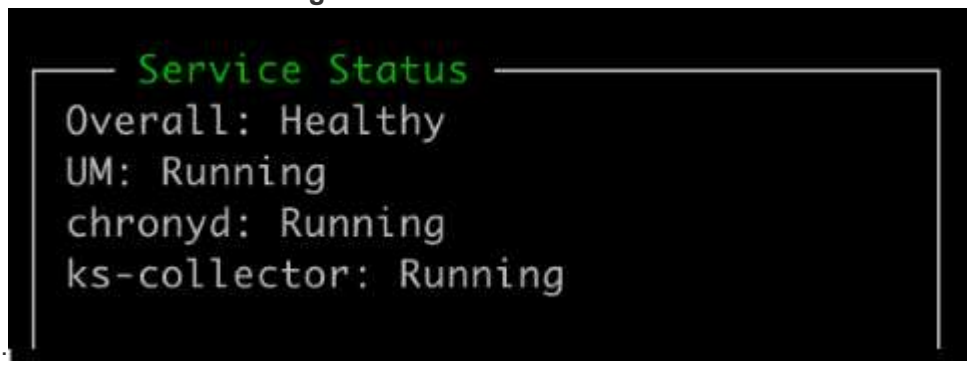
** FOR StorageGRFunded **

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

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

.

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**



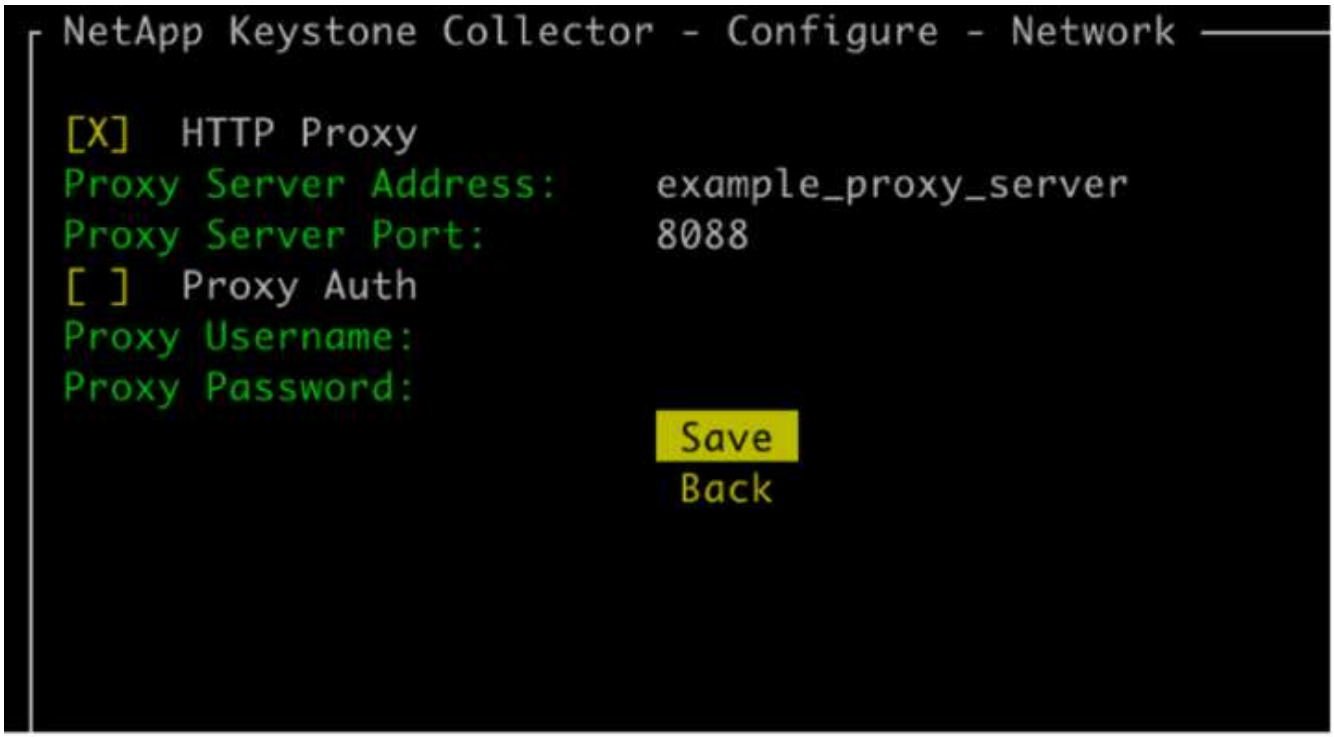
7. Uscire dalla TUI di gestione di Keystone Collector selezionando l'opzione **Esci dalla shell** nella schermata iniziale.

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 su configurazione, stato e performance necessarie per eseguire il calcolo dell'abbonamento. 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:

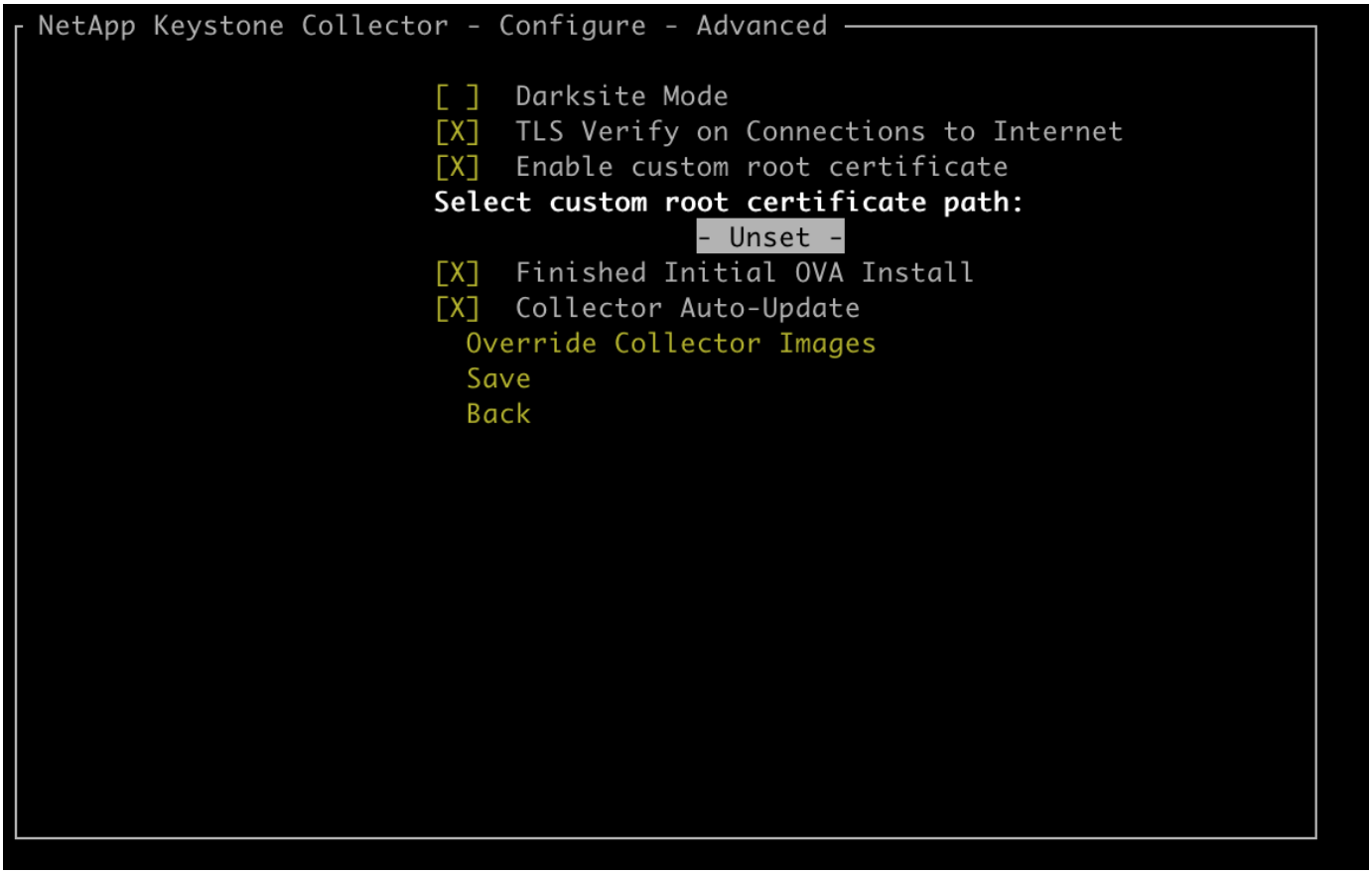
Fasi

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.



Monitorare lo stato del sistema

È possibile monitorare lo stato del sistema tramite i servizi di Keystone Collector utilizzando qualsiasi sistema di monitoraggio 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 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"}
```

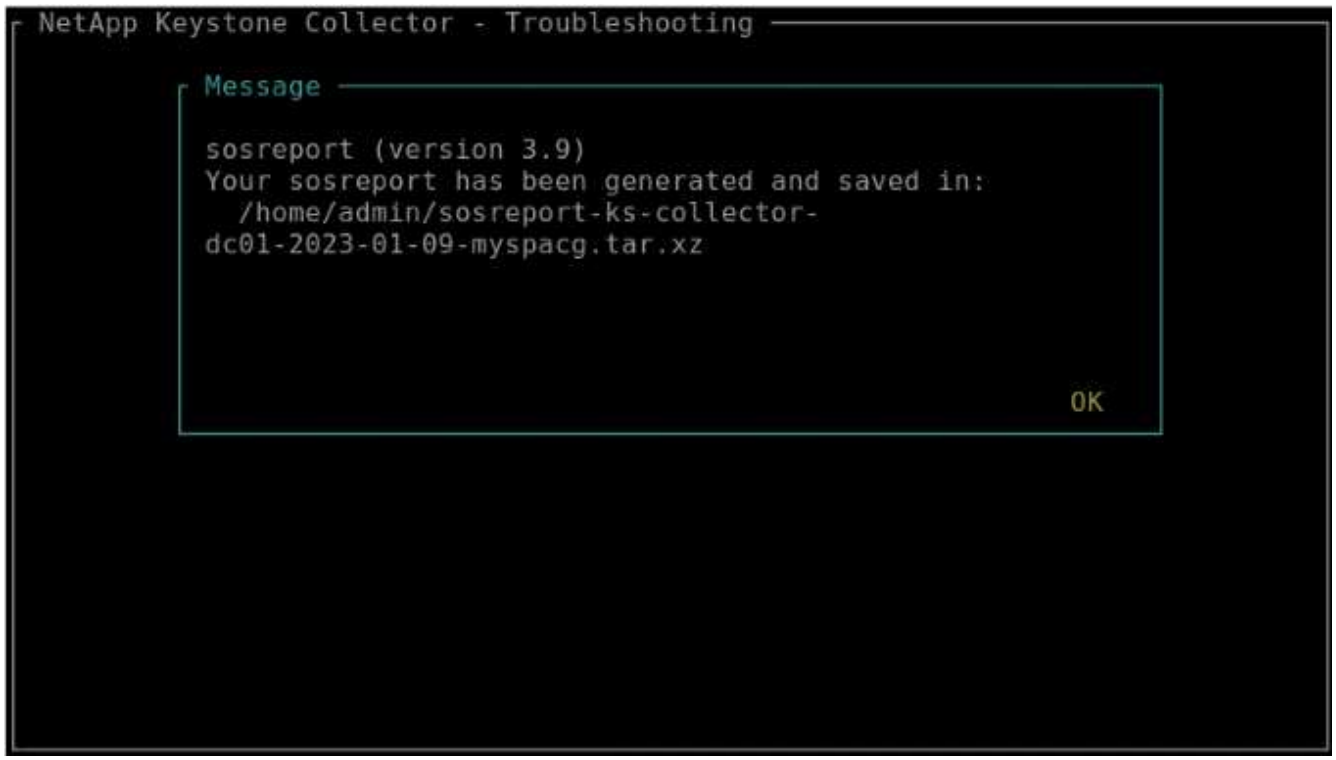
Generare e raccogliere pacchetti di supporto

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.



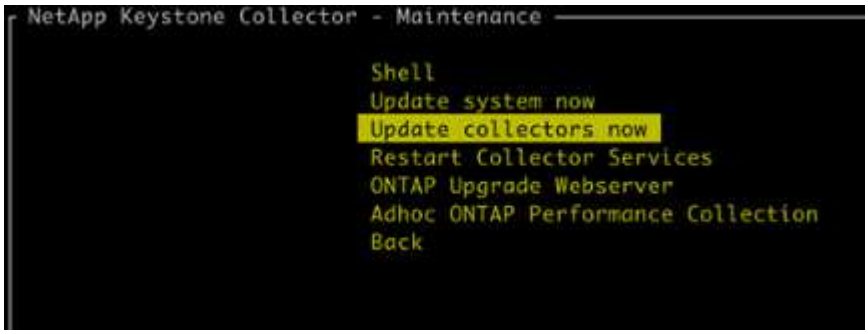
4. Una volta scaricato il file, è possibile allegarlo al ticket di supporto di Keystone ServiceNow. Per informazioni sulla richiesta di ticket, vedere "Generazione di richieste di servizio".

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

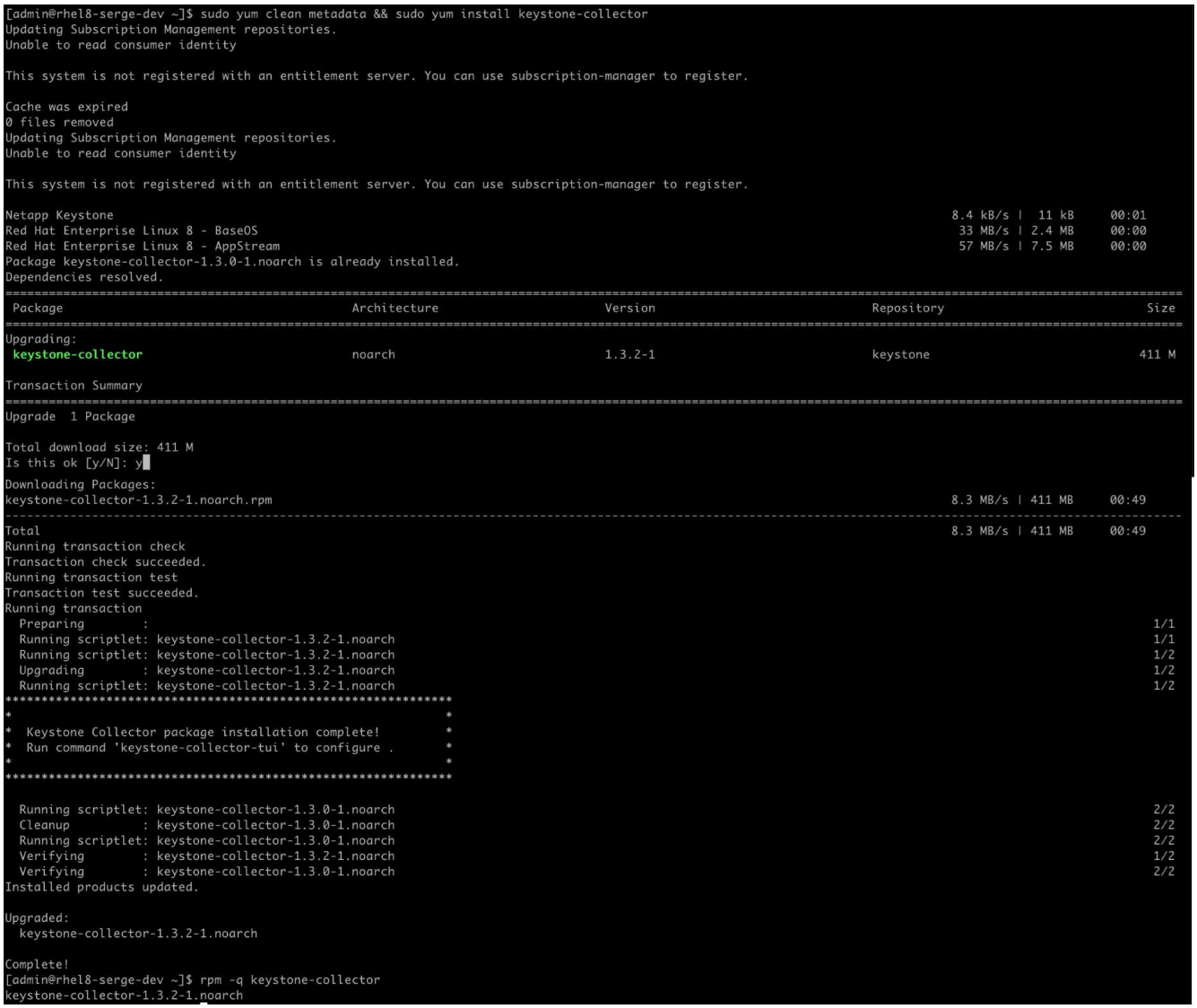
1. Avviare l'utility TUI di gestione di Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Nella schermata di manutenzione, selezionare l'opzione **Aggiorna raccolta ora**.



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
```

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".
- Devi includere i seguenti sottosistemi nei bundle giornalieri di AutoSupport per garantire una raccolta precisa dei dati per Keystone. Per informazioni sui sottosistemi AutoSupport, vedere "Che cosa sono i sottosistemi AutoSupport".

Nome del sottosistema	Elemento dati richiesto per Keystone
WAFL	`VOLUME-CLONE-SHOW.XML`
performance	`QOS-POLICY-GROUP.XML` e. `QOS-ADAPTIVE-POLICY.XML`
snapshot	`SNAPSHOT.XML`
piattaforma	`ENVIRONMENT.txt`

Questi sottosistemi sono inclusi per impostazione predefinita nei pacchetti AutoSupport settimanali, dove `asup_type` È *DOT-REGULAR*, e il `asup_subject` È *NOTIFICA gruppo ha (SETTIMANALE_LOG)*. Tuttavia, devi aggiungerle ai bundle giornalieri per il recupero e la segnalazione dei dati di utilizzo di Keystone.

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. Eseguire il comando seguente e verificare la configurazione esistente rispetto ai sottosistemi esistenti:

   ```
   autosupport trigger show -node * -autosupport-message management.log -fields basic-additional
   ```

   Per ulteriori informazioni su questo comando, vedere "visualizzazione del manifesto AutoSupport del nodo di sistema".

3. Per modificare il contenuto quotidiano del registro, eseguire il seguente comando:

```
autosupport trigger modify -node * -autosupport-message management.log -basic
-additional <existing comma-separated subsystems>, <new subsystems>
```

Per ulteriori informazioni su questo comando, vedere "modifica trigger AutoSupport nodo di sistema".

Tipi di dati utente raccolti da Keystone

Keystone raccoglie informazioni su configurazione, stato e utilizzo per gli abbonamenti a Keystone ONTAP e Keystone StoragGRID. Può anche raccogliere i dati sulle prestazioni solo per ONTAP, se l'opzione è attivata in Keystone Collector.

Raccolta di dati ONTAP

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

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

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

    - VserverUID
    - Sottotipo
- Aggregati di storage
    - StorageType
    - Nome aggregato
    - UUID aggregato
- Aggregare gli archivi di oggetti
    - ObjectStoreName
    - ObjectStoreUID
    - ProviderType
    - Nome aggregato
- Clonare i volumi
    - FlexClone
    - Dimensione
    - Utilizzato
    - Server virtuale
    - Tipo
    - ParentVolume
    - ParentVserver
    - IsConstituent
    - 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
- Cluster MetroCluster
    - ClusterUID
    - Nome cluster
    - RemoteClusterUID
    - RemoteCluserName
    - LocalConfigurationState
    - RemoteConfigurationState
    - Modalità
- Metriche di osservabilità del collettore
    - Tempo di raccolta
    - Endpoint API Active IQ Unified Manager interrogato
    - Tempi di risposta
    - Numero di record
    - IP istanza AIQUMInstance
    - ID istanza CollectorInstance

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

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

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

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

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

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

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

Raccolta di dati StorageGRID

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

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

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

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

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

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

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

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

Informazioni sul copyright

Informazioni sul marchio commerciale