



# Installare Keystone Collector

## Keystone

NetApp  
April 05, 2024

# Sommario

- Installare Keystone Collector ..... 1
  - Implementare Keystone Collector su sistemi VMware vSphere ..... 1
  - Installare Keystone Collector su sistemi Linux ..... 3
  - Convalida automatica dell'integrità del software ..... 4

# 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.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

**Review details**  
Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	NetApp Keystone Collector
Version	20220405
Vendor	NetApp
Download size	8.3 GB
Size on disk	12.1 GB (thin provisioned) 200.0 GB (thick provisioned)

CANCEL BACK NEXT

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.

## Informazioni sul copyright

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

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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