# Installieren Sie Keystone Collector

Keystone

NetApp
April 05, 2024

# Inhalt

Installieren Sie Keystone Collector . . . 1
Implementieren Sie Keystone Collector auf VMware vSphere Systemen . . . 1
Installieren Sie Keystone Collector auf Linux Systemen . . . 3
Automatische Validierung der Softwareintegrität . . . 4

# Installieren Sie Keystone Collector

## Implementieren Sie Keystone Collector auf VMware vSphere Systemen

Die Bereitstellung von Keystone Collector auf VMware vSphere Systemen umfasst das Herunterladen der OVA-Vorlage, die Bereitstellung der Vorlage mithilfe des Assistenten **OVF-Vorlage** bereitstellen, die Integrität der Zertifikate überprüfen und die Bereitschaft der VM überprüfen.

### Bereitstellen der OVA-Vorlage

Führen Sie hierzu folgende Schritte aus:

**Schritte**

1. Laden Sie die OVA-Datei von herunter "Dieser Link" Auf Ihrem VMware vSphere System speichern.
2. Navigieren Sie auf Ihrem VMware vSphere System zur Ansicht **VMs und Vorlagen**.
3. Klicken Sie mit der rechten Maustaste auf den gewünschten Ordner für die virtuelle Maschine (VM) (oder das Rechenzentrum, falls keine VM-Ordner verwendet werden) und wählen Sie **OVF-Vorlage bereitstellen** aus.
4. Klicken Sie auf *Schritt 1* des Assistenten * OVF-Vorlage bereitstellen* auf **Auswählen und OVF-Vorlage**, um das heruntergeladene auszuwählen `KeystoneCollector-latest.ova` Datei:
5. Geben Sie unter *Schritt 2* den VM-Namen an und wählen Sie den VM-Ordner aus.
6. Geben Sie in *Schritt 3* die erforderliche Computing-Ressource an, die zur Ausführung der VM erforderlich ist.
7. Am *Schritt 4: Überprüfen Sie die Details*, überprüfen Sie die Richtigkeit und Authentizität der OVA-Datei. VCenter-Versionen vor 7.0u2 können die Authentizität des Codesignaturzertifikats nicht automatisch überprüfen. VCenter 7.0u2 und höher können die Überprüfungen durchführen, dafür sollte jedoch die Signaturzertifikatberechtigung zu vCenter hinzugefügt werden. Folgen Sie diesen Anweisungen für Ihre Version von vCenter:

   **VCenter 7.0u1 und früher: Weitere Informationen**

   VCenter überprüft die Integrität der OVA-Dateiinhalte und stellt für die in der OVA-Datei enthaltenen Dateien einen gültigen Code-Signing Digest bereit. Die Echtheit des Codsignieren-Zertifikats wird jedoch nicht überprüft. Um die Integrität zu überprüfen, sollten Sie das vollständige Signieren-Digest-Zertifikat herunterladen und es mit dem öffentlichen Zertifikat von Keystone veröffentlicht überprüfen.

   a. Klicken Sie auf den Link **Publisher**, um das vollständige Signieren-Digest-Zertifikat herunterzuladen.
   b. Laden Sie das öffentliche *Keystone Billing*-Zertifikat von herunter "Dieser Link".
   c. Überprüfen Sie die Authentizität des OVA-Signaturzertifikats anhand des öffentlichen Zertifikats mithilfe von OpenSSL:
      `openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert`

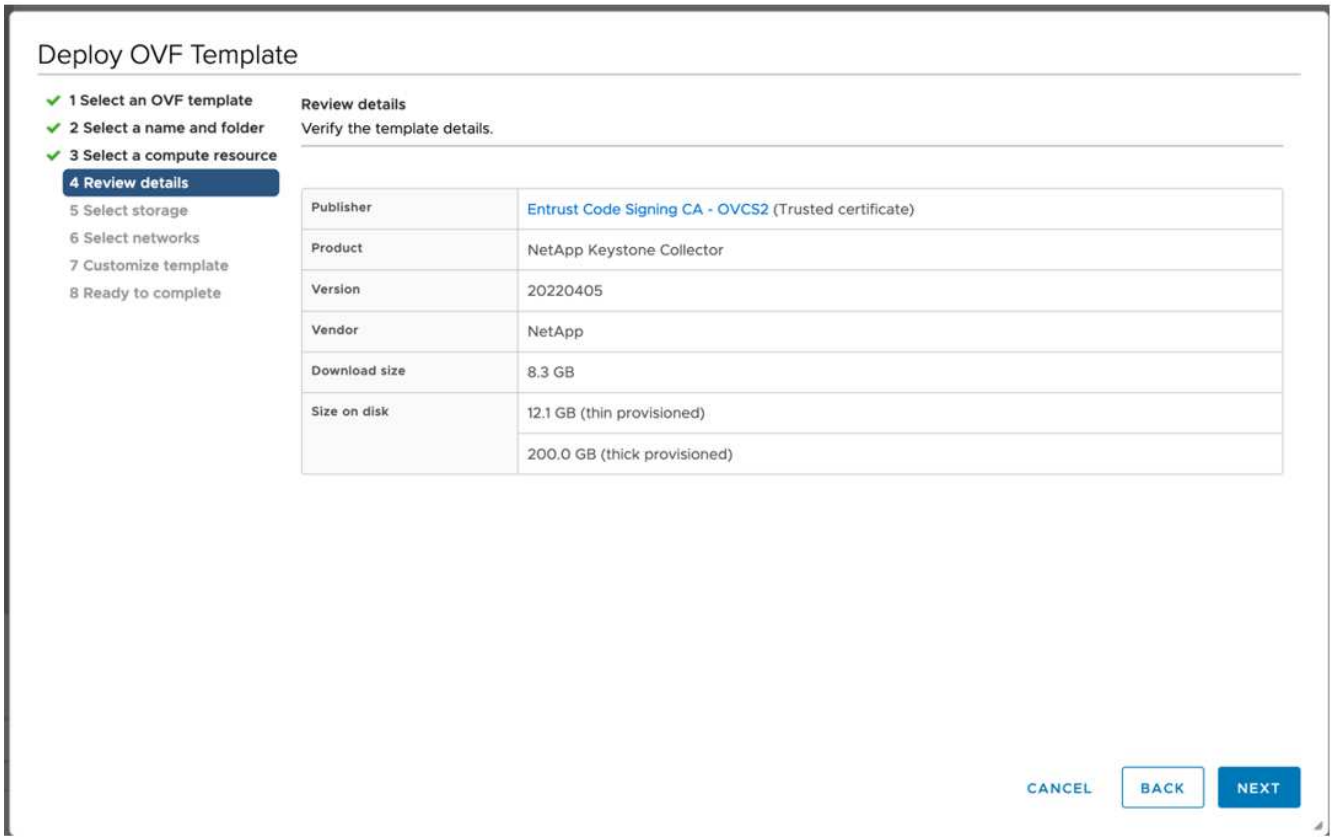
**VCenter 7.0u2 und höher: Weitere Informationen**

7.0u2 und neuere Versionen von vCenter können die Integrität des OVA-Dateiinhalts und die Authentizität des Codesignaturzertifikats überprüfen, wenn ein gültiger Codesignaturdigest bereitgestellt wird. Der vCenter Root-Vertrauensspeicher enthält nur VMware-Zertifikate. NetApp verwendet Entrust als Zertifizierungsstelle, und diese Zertifikate müssen zum vCenter Trust Store hinzugefügt werden.

a. Laden Sie das Zertifikat für die Codesignaturierungsstelle von Entrust herunter "Hier".

b. Befolgen Sie die Schritte unter `Resolution` Abschnitt dieses Knowledge Base-Artikels (KB): https://kb.vmware.com/s/article/84240.

Wenn die Integrität und Authentizität des Keystone Collector OVA validiert werden, können Sie den Text sehen `(Trusted certificate)` Mit dem Herausgeber.




8. Geben Sie in *Schritt 5* des Assistenten * OVF-Vorlage bereitstellen* den Speicherort für die VM an.
9. Wählen Sie bei *Schritt 6* das Zielnetzwerk aus, das die VM verwenden soll.
10. Geben Sie in *Schritt 7 Vorlage anpassen* die ursprüngliche Netzwerkadresse und das Kennwort für das Admin-Benutzerkonto an.

> Das Admin-Passwort wird in einem umkehrbaren Format in vCenter gespeichert und sollte als Bootstrap-Anmeldeinformationen verwendet werden, um ersten Zugriff auf das VMware vSphere-System zu erhalten. Dieses Admin-Passwort sollte während der anfänglichen Softwarekonfiguration geändert werden. Die Subnetzmaske für die IPv4-Adresse sollte in CIDR-Notation bereitgestellt werden. Verwenden Sie beispielsweise den Wert 24 für eine Subnetzmaske von 255.255.255.0.

11. Prüfen Sie bei *Schritt 8 Ready to complete* des Assistenten **Deploy OVF Template** die Konfiguration und stellen Sie sicher, dass Sie die Parameter für die OVA-Bereitstellung richtig eingestellt haben.

Nachdem die VM aus der Vorlage implementiert und eingeschaltet wurde, öffnen Sie eine SSH-Sitzung für die VM, und loggen Sie sich mit den temporären Administratorberechtigungen ein, um zu überprüfen, ob die VM bereit für die Konfiguration ist.

### Erstkonfiguration Des Systems

Führen Sie diese Schritte auf Ihren VMware vSphere-Systemen für die Erstkonfiguration der über OVA bereitgestellten Keystone Collector-Server durch:

> Nach Abschluss der Implementierung können Sie die Konfigurations- und Überwachungsaktivitäten über das Dienstprogramm Keystone Collector Management Terminal User Interface (TUI) durchführen. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren.

1. Öffnen Sie eine SSH-Sitzung für den Keystone Collector-Server. Beim Anmelden wird die TUI angezeigt. Alternativ können Sie die TUI manuell starten, indem Sie den ausführen `keystone-collector-tui` CLI-Befehl.
2. Konfigurieren Sie bei Bedarf die Proxydetails im Abschnitt **Konfiguration > Netzwerk** auf der TUI.
3. Aktualisieren Sie Keystone Collector mit der Option **Wartung > System aktualisieren**. Einige ausgewählte Spiegelungen sind möglicherweise nicht verfügbar, und die Systemdetails werden nach einigen Versuchen aktualisiert.
4. Konfigurieren Sie im Abschnitt **Konfiguration > System** den Hostnamen, den Speicherort und den NTP-Server des Systems.
5. Aktualisieren Sie das Admin-Passwort im Abschnitt **Wartung > Benutzer**.
6. Markieren Sie die ursprüngliche OVA-Konfiguration im Abschnitt **Konfiguration > Erweitert** als abgeschlossen.

# Installieren Sie Keystone Collector auf Linux Systemen

## Die Keystone Collector-Software wird von einem Online-YUM-Software-Repository verteilt. Sie müssen die Datei auf einem Linux-Server importieren und installieren.

Führen Sie die folgenden Schritte aus, um die Software auf Ihrem Linux-Server zu installieren:

1. SSH auf den Keystone Collector Server und erhöhen auf `root` Berechtigung.
2. Importieren Sie die öffentliche Keystone-Signatur:
   ```
   # rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101
   ```
3. Stellen Sie sicher, dass das richtige öffentliche Zertifikat importiert wurde, indem Sie den Fingerabdruck für die Keystone Billing-Plattform in der RPM-Datenbank überprüfen:
   ```
   # rpm -qa gpg-pubkey --qf '%<Description>'|gpg --show-keys --fingerprint
   ```
   Der richtige Fingerabdruck sieht so aus:
   ```
   90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D
   ```
4. Laden Sie die herunter `keystonerepo.rpm` Datei:

```
curl -O https://keystone.netapp.com/repo/keystonerepo.rpm
```

5. Überprüfen Sie die Authentizität der Datei:
   ```
   rpm --checksig -v keystonerepo.rpm`Eine Signatur für eine authentische Datei
   sieht wie folgt aus:
   `Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK
   ```
6. Installieren Sie die YUM-Software-Repository-Datei:
   ```
   # yum install keystonerepo.rpm
   ```
7. Wenn Keystone Repo installiert ist, installieren Sie das Keystone-Collector-Paket über den YUM-Paketmanager:
   ```
   # yum install keystone-collector
   ```

> Nach Abschluss der Installation können Sie das Dienstprogramm „Keystone Collector Management Terminal User Interface (TUI)“ verwenden, um die Konfigurations- und Überwachungsaktivitäten durchzuführen. Sie können verschiedene Tastaturbedienungen wie die Eingabetaste und die Pfeiltasten verwenden, um die Optionen auszuwählen und durch diese TUI zu navigieren. Siehe "Konfigurieren Sie Keystone Collector" Und "Systemzustand überwachen" Zur Information.

# Automatische Validierung der Softwareintegrität

## Es gibt einen wiederholten Prozess zur Überprüfung der Integrität der Keystone-Software.

Die Konfiguration des Keystone YUM Repository-Clients wird in bereitgestellt `keystonerepo.rpm` Nutzt die erzwungene GPG-Prüfung (`gpgcheck=1`) Auf alle Software, die über dieses Repository heruntergeladen wird. Alle RPM, die über das Keystone-Repository heruntergeladen werden, das die Signaturvalidierung fehlschlägt, wird nicht installiert. Diese Funktion wird in der Funktion für die geplante automatische Aktualisierung des Keystone Collectors verwendet, um sicherzustellen, dass nur gültige und authentische Software auf Ihrer Website installiert wird.