Installieren Sie Keystone Collector

Keystone

NetApp
January 08, 2026

Inhalt

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. Bei Schritt 4: Details überprüfen, vergewissern Sie sich, dass die OVA-Datei korrekt und authentisch ist.

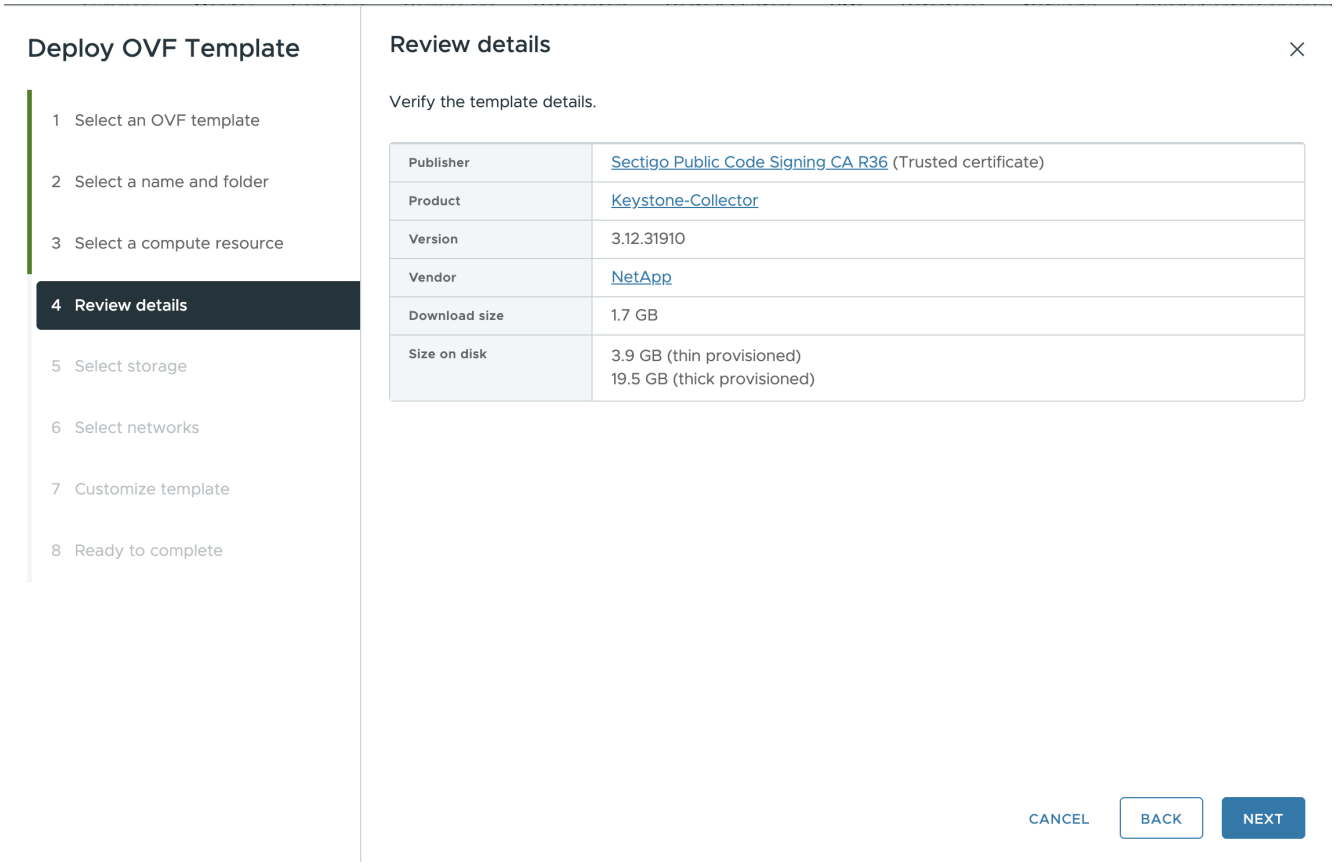
   Der vCenter-Root-Truststore enthält nur VMware-Zertifikate. NetApp verwendet Entrust als Zertifizierungsstelle und diese Zertifikate müssen dem vCenter Trust Store hinzugefügt werden.

   a. Laden Sie das Code-Signatur-CA-Zertifikat von Sectigo herunter. "Hier"Die

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

   > Für vCenter Versionen 7.x und älter müssen Sie vCenter und ESXi auf Version 8.0 oder höher aktualisieren. Ältere Versionen werden nicht mehr unterstützt.

   Sobald die Integrität und Authentizität der Keystone Collector OVA bestätigt sind, können Sie den Text sehen. `(Trusted certificate)` mit dem Verlag.



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. Wenn Sie eine Verbindung herstellen, werden Sie vom System aufgefordert, das Admin-Passwort zu aktualisieren. Füllen Sie bei Bedarf das Update des Admin-Passworts aus.
2. Melden Sie sich mit dem neuen Passwort an, um auf die TUI zuzugreifen. Beim Anmelden wird die TUI angezeigt.

   Alternativ können Sie es manuell starten, indem Sie den ausführen `keystone-collector-tui` CLI-Befehl.
3. Konfigurieren Sie bei Bedarf die Proxy-Details im Abschnitt **Konfiguration > Netzwerk** auf der TUI.
4. Konfigurieren Sie im Abschnitt **Konfiguration > System** den Hostnamen, den Speicherort und den NTP-Server des Systems.
5. Aktualisieren Sie die Keystone Collectors mit der Option **Wartung > Collectors aktualisieren**. Starten Sie nach der Aktualisierung das TUI-Dienstprogramm für die Verwaltung des Keystone Collectors neu, um die Änderungen anzuwenden.

Installieren Sie Keystone Collector auf Linux Systemen

Sie können die Keystone Collector-Software auf einem Linux-Server mit einem RPM oder einem Debian-Paket installieren. Führen Sie die Installationsschritte je nach Linux-Distribution aus.

RPM wird verwendet

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/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. Stellen Sie sicher, dass das richtige öffentliche Zertifikat importiert wurde, indem Sie den Fingerabdruck für die Keystone Billing Platform in der RPM-Datenbank überprüfen:
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint` Der korrekte Fingerabdruck sieht so aus:
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Laden Sie die `keystonerepo.rpm` Datei:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Überprüfen Sie die Echtheit der Datei:
   `rpm --checksig -v keystonerepo.rpm` Eine Signatur für eine authentische Datei sieht folgendermaßen aus:
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: 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`

   Führen Sie für Red Hat Enterprise Linux 9 den folgenden Befehl aus, um das Keystone-Collector-Paket zu installieren:
   `# yum install keystone-collector-rhel9`

Debian Verwenden

1. SSH zum Keystone Collector Server und Zugriff auf `root` Berechtigungen.
   `sudo su`
2. Laden Sie die Datei herunter `keystone-sw-repo.deb`:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Keystone-Software-Repository-Datei installieren:
   `# dpkg -i keystone-sw-repo.deb`
4. Paketliste aktualisieren:
   `# apt-get update`
5. Installieren Sie beim Installieren des Keystone-Repo das Keystone-Collector-Paket:
   `# apt-get 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 Keystone Software

Das Keystone Repository ist so konfiguriert, dass die Integrität der Keystone Software automatisch überprüft wird, sodass an Ihrem Standort nur gültige und authentische Software installiert wird.

Die in bereitgestellte Keystone YUM Repository-Client-Konfiguration `keystonerepo.rpm` verwendet die erzwungene GPG-Prüfung (`gpgcheck=1`) für 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 automatische Aktualisierung nach Zeitplan von Keystone Collector verwendet, um sicherzustellen, dass nur gültige und authentische Software an Ihrem Standort installiert wird.