Install Keystone Collector

Keystone

NetApp
April 05, 2024

Table of Contents

Install Keystone Collector

Deploy Keystone Collector on VMware vSphere systems

Deploying Keystone Collector on VMware vSphere systems includes downloading the OVA template, deploying the template by using the **Deploy OVF Template** wizard, verifying the integrity of the certificates, and verifying the readiness of the VM.

Deploying the OVA template

Follow these steps:

Steps

1. Download the OVA file from this link and store it on your VMware vSphere system.
2. On your VMware vSphere system, navigate to the **VMs and Templates** view.
3. Right click on the required folder for the virtual machine (VM) (or data center, if not using VM folders) and select **Deploy OVF Template**.
4. On *Step 1* of the **Deploy OVF Template** wizard, click **Select and OVF template** to select the downloaded `KeystoneCollector-latest.ova` file.
5. On *Step 2*, specify the VM name and select the VM folder.
6. On *Step 3*, specify the required compute resource that is to run the VM.
7. On *Step 4: Review details*, verify the correctness and authenticity of the OVA file.
   vCentre versions prior to 7.0u2 are unable to automatically verify the authenticity of the code signing certificate. vCentre 7.0u2 and later can perform the verifications, however, for this, the signing certificate authority should be added to vCentre. Follow these instructions for your version of vCentre:

   vCentre 7.0u1 and earlier: Learn more

   vCentre validates the integrity of the OVA file contents and that a valid code-signing digest is provided for the files contained in the OVA file. However, it does not validate the authenticity of the code-signing certificate. For verifying the integrity, you should download the full signing digest certificate, and verify it against the public certificate published by Keystone.

   a. Click the **Publisher** link to download the full signing digest certificate.
   b. Download the *Keystone Billing* public certificate from this link.
   c. Verify the authenticity of the OVA signing certificate against the public certificate by using OpenSSL:
      `openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert`

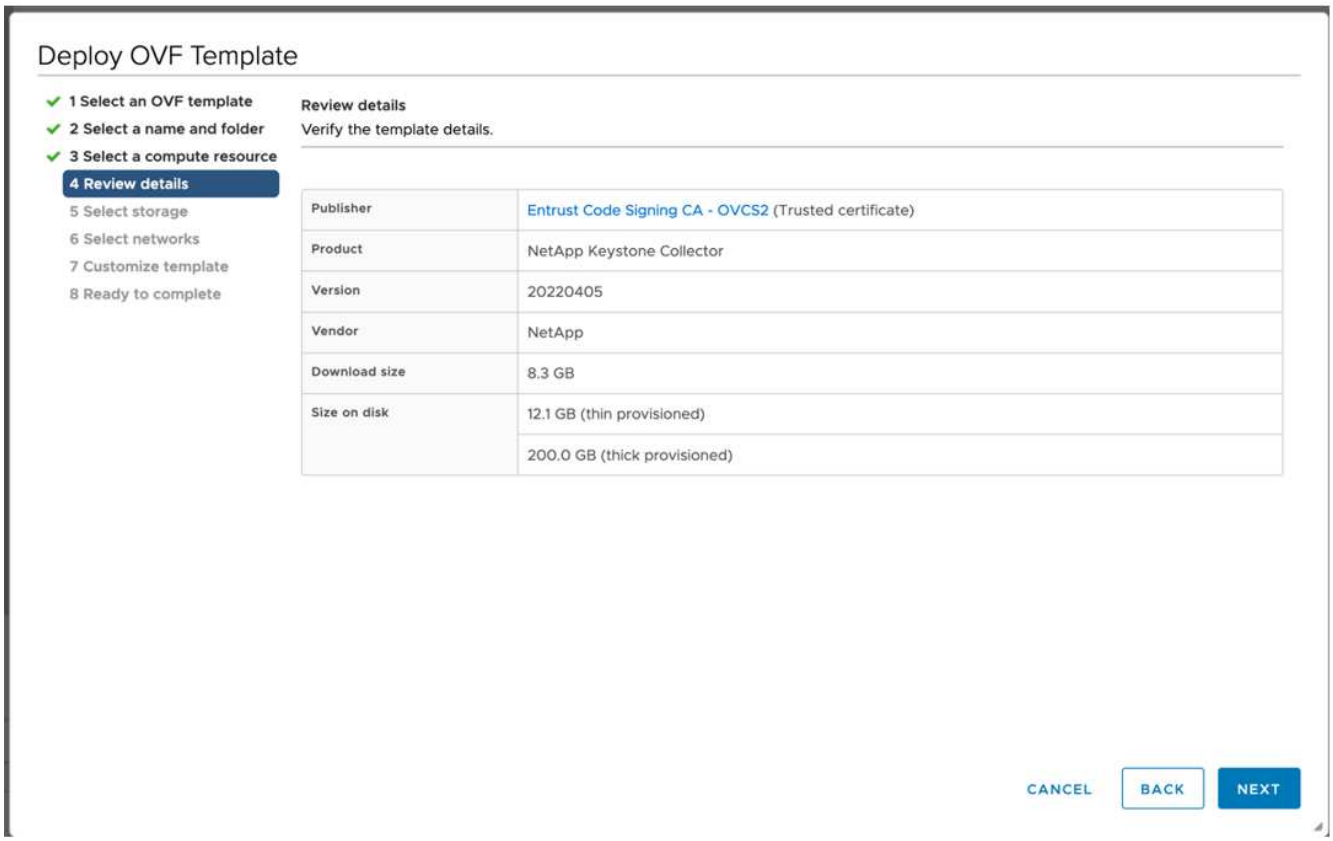
vCentre 7.0u2 and later: Learn more

7.0u2 and later versions of vCenter are capable of validating the integrity of the OVA file contents and the authenticity of the code-signing certificate, when a valid code-signing digest is provided. The vCenter root trust store contains only VMware certificates. NetApp uses Entrust as a certifying authority, and those certificates need to be added to the vCenter trust store.

a. Download the code-signing CA certificate from Entrust here.

b. Follow the steps in the `Resolution` section of this knowledge base (KB) article: https://kb.vmware.com/s/article/84240.

When the integrity and authenticity of the Keystone Collector OVA are validated, you can see the text `(Trusted certificate)` with the publisher.



8. On *Step 5* of the **Deploy OVF Template** wizard, specify the location for storing the VM.
9. On *Step 6*, select the destination network for the VM to use.
10. On *Step 7 Customize template*, specify the initial network address and password for the admin user account.

> The admin password is stored in a reversible format in vCentre and should be used as a bootstrap credential to gain initial access to the VMware vSphere system. During the initial software configuration, this admin password should be changed. The subnet mask for the IPv4 address should be supplied in CIDR notation. For example, use the value of 24 for a subnet mask of 255.255.255.0.

11. On *Step 8 Ready to complete* of the **Deploy OVF Template** wizard, review the configuration and verify that you have correctly set the parameters for the OVA deployment.

After the VM has been deployed from the template and powered on, open an SSH session to the VM and log in with the temporary admin credentials to verify that the VM is ready for configuration.

Initial System Configuration

Perform these steps on your VMware vSphere systems for an initial configuration of the Keystone Collector servers deployed through OVA:

> On completing the deployment, you can use the Keystone Collector Management Terminal User Interface (TUI) utility to perform the configuration and monitoring activities. You can use various keyboard controls, such as the Enter and arrow keys, to select the options and navigate across this TUI.

1. Open an SSH session to the Keystone Collector server. On login, the TUI appears. Alternately, you can launch the TUI manually by running the `keystone-collector-tui` CLI command.
2. If required, configure the proxy details in the **Configuration > Network** section on the TUI.
3. Update Keystone Collector by using the **Maintenance > Update System** option. Some selected mirrors might be unavailable, and the system details are updated after a few retries.
4. Configure the system hostname, location, and NTP server in the **Configuration > System** section.
5. Update the admin password in the **Maintenance > User** section.
6. Mark the initial OVA configuration as complete in the **Configuration > Advanced** section.

Install Keystone Collector on Linux systems

The Keystone Collector software is distributed by an online YUM software repository. You need to import and install the file on a Linux server.

Follow these steps to install the software on your Linux server:

1. SSH to the Keystone Collector server and elevate to `root` privilege.
2. Import the Keystone public signing signature:
   `# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101`
3. Ensure that the correct public certificate has been imported by checking the fingerprint for Keystone Billing Platform in the RPM database:
   `# rpm -qa gpg-pubkey --qf '%<Description>'|gpg --show-keys --fingerprint`
   The correct fingerprint looks like this:
   `90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D`
4. Download the `keystonerepo.rpm` file:
   `curl -O https://keystone.netapp.com/repo/keystonerepo.rpm`
5. Verify the authenticity of the file:
   `rpm --checksig -v keystonerepo.rpm`
   A signature for an authentic file looks like this:
   `Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK`
6. Install the YUM software repository file:
   `# yum install keystonerepo.rpm`

7. When the Keystone repo is installed, install the keystone-collector package through the YUM package manager:

```
# yum install keystone-collector
```

> On completing the installation, you can use the Keystone Collector Management Terminal User Interface (TUI) utility to perform the configuration and monitoring activities. You can use various keyboard controls, such as the Enter and arrow keys, to select the options and navigate across this TUI. See Configure Keystone Collector and Monitor system health for information.

Automatic validation of software integrity

There is a reiterative process of validating the integrity of the Keystone software.

The Keystone YUM repository client configuration provided in `keystonerepo.rpm` makes use of enforced GPG checking (`gpgcheck=1`) on all software downloaded through this repository. Any RPM downloaded through the Keystone repository that fails signature validation is prevented from being installed. This functionality is used in the scheduled auto-update capability of the Keystone Collector to ensure only valid and authentic software is installed at your site.

Copyright information

Trademark information