Installez le collecteur Keystone

Keystone

NetApp
May 30, 2024

Sommaire

Installez le collecteur Keystone 1
Déployez Keystone Collector sur des systèmes VMware vSphere 1
Installez Keystone Collector sur les systèmes Linux 3
Validation automatique de l’intégrité logicielle 4

Installez le collecteur Keystone

Déployez Keystone Collector sur des systèmes VMware vSphere

Le déploiement de Keystone Collector sur des systèmes VMware vSphere inclut le téléchargement du modèle OVA, le déploiement du modèle à l'aide de l'assistant **Deploy OVF Template**, la vérification de l'intégrité des certificats et la vérification de l'état de préparation de la machine virtuelle.

Déploiement du modèle OVA

Voici la procédure à suivre :

Étapes

1. Téléchargez le fichier OVA à partir de "ce lien" Et stockez-les sur votre système VMware vSphere.
2. Sur votre système VMware vSphere, accédez à la vue **VM et modèles**.
3. Cliquez avec le bouton droit de la souris sur le dossier requis pour la machine virtuelle (VM) (ou le centre de données, si vous n'utilisez pas les dossiers VM) et sélectionnez **déployer le modèle OVF**.
4. À l'étape 1_ de l'assistant **déployer modèle OVF**, cliquez sur **Sélectionner et modèle OVF** pour sélectionner le fichier téléchargé `KeystoneCollector-latest.ova` fichier.
5. Sous *Etape 2*, spécifiez le nom de la VM et sélectionnez le dossier VM.
6. Sur *Etape 3*, spécifiez la ressource de calcul requise pour exécuter la machine virtuelle.
7. A l'étape 4 : vérifier les détails_, vérifier l'exactitude et l'authenticité du fichier OVA.
   Les versions vCenter antérieures à 7.0u2 ne peuvent pas vérifier automatiquement l'authenticité du certificat de signature de code. VCenter 7.0u2 et versions ultérieures peuvent effectuer les vérifications. Toutefois, pour cela, l'autorité de certification de signature doit être ajoutée à vCenter. Suivez ces instructions pour votre version de vCenter :

   VCenter 7.0u1 et versions antérieures : en savoir plus

   VCenter valide l'intégrité du contenu du fichier OVA et qu'un résumé de signature de code valide est fourni pour les fichiers contenus dans le fichier OVA. Toutefois, il ne valide pas l'authenticité du certificat de signature de code. Pour vérifier l'intégrité, téléchargez le certificat de signature complète et vérifiez-le par rapport au certificat public publié par Keystone.

   a. Cliquez sur le lien **Publisher** pour télécharger le certificat de signature complet.
   b. Téléchargez le certificat public *Keystone Billing* sur "ce lien".
   c. Vérifiez l'authenticité du certificat de signature OVA par rapport au certificat public en utilisant OpenSSL :
      `openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert`

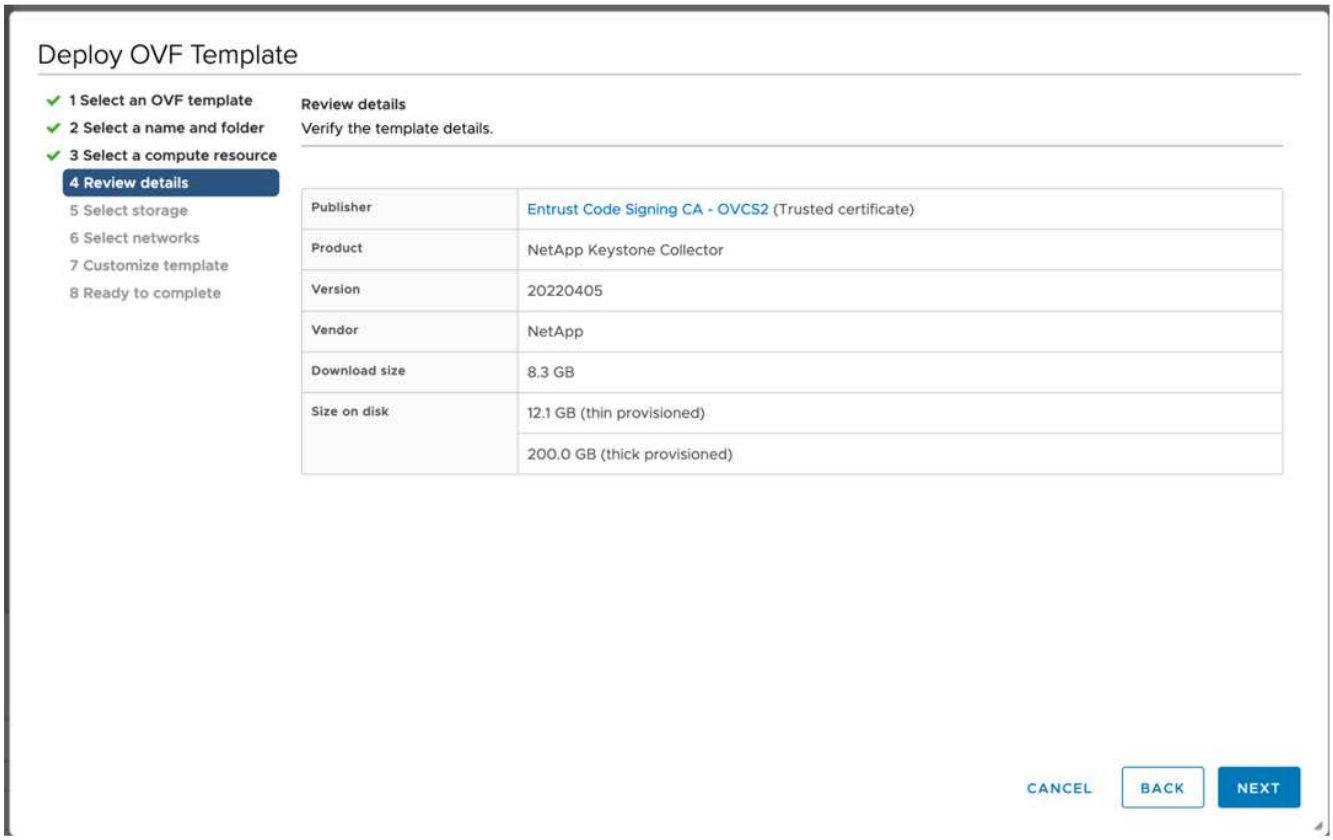
VCenter 7.0u2 et versions ultérieures : en savoir plus

7.0u2 et versions ultérieures de vCenter sont capables de valider l'intégrité du contenu du fichier OVA et l'authenticité du certificat de signature de code, lorsqu'un résumé de signature de code valide est fourni. Le magasin de confiance racine vCenter contient uniquement des certificats VMware. NetApp utilise Entrust comme autorité de certification et ces certificats doivent être ajoutés au magasin de confiance vCenter.

a. Téléchargez le certificat d'autorité de certification de signature de code depuis Entrust "ici".

b. Suivez les étapes de la section `Resolution` Article de la base de connaissances : https://kb.vmware.com/s/article/84240.

Une fois l'intégrité et l'authenticité de l'OVA du collecteur Keystone validées, le texte s'affiche `(Trusted certificate)` avec l'éditeur.



8. À l'étape *5* de l'assistant **Deploy OVF Template**, indiquez l'emplacement de stockage de la machine virtuelle.
9. Sur *Step 6*, sélectionnez le réseau de destination de la machine virtuelle à utiliser.
10. Sur *Etape 7 Personnaliser le modèle*, spécifiez l'adresse réseau initiale et le mot de passe du compte utilisateur admin.

Le mot de passe admin est stocké dans un format réversible dans vCenter et doit être utilisé comme informations d'identification d'amorçage pour obtenir un accès initial au système VMware vSphere. Lors de la configuration logicielle initiale, ce mot de passe administrateur doit être modifié. Le masque de sous-réseau de l'adresse IPv4 doit être fourni en notation CIDR. Par exemple, utilisez la valeur 24 pour un masque de sous-réseau de 255.255.255.0.

11. À l'étape *8 prêt à compléter* de l'assistant **déployer modèle OVF**, examinez la configuration et vérifiez que vous avez correctement défini les paramètres pour le déploiement OVA.

Une fois la machine virtuelle déployée à partir du modèle et sous tension, ouvrez une session SSH sur la machine virtuelle et connectez-vous avec les identifiants d'administration temporaires pour vérifier que la machine virtuelle est prête pour la configuration.

Configuration initiale du système

Effectuez les étapes suivantes sur vos systèmes VMware vSphere pour une configuration initiale des serveurs Keystone Collector déployés via OVA :

> Lors de la réalisation du déploiement, vous pouvez utiliser l'utilitaire TUI (Keystone Collector Management terminal User interface) pour effectuer les activités de configuration et de surveillance. Vous pouvez utiliser diverses commandes du clavier, telles que les touches entrée et flèche, pour sélectionner les options et naviguer dans cette TUI.

1. Ouvrez une session SSH sur le serveur Keystone Collector. Lorsque vous vous connectez, le système vous invite à mettre à jour le mot de passe d'administration. Effectuez la mise à jour du mot de passe d'administration si nécessaire.
2. Connectez-vous à l'aide du nouveau mot de passe pour accéder à l'interface utilisateur. Lors de la connexion, le TUI s'affiche.

   Vous pouvez également le lancer manuellement en exécutant le `keystone-collector-tui` Commande CLI.

3. Si nécessaire, configurez les détails du proxy dans la section **Configuration > réseau** de l'interface utilisateur.
4. Configurez le nom d'hôte du système, l'emplacement et le serveur NTP dans la section **Configuration > système**.
5. Mettez à jour les collecteurs Keystone à l'aide de l'option **Maintenance > mettre à jour les collecteurs**. Après la mise à jour, redémarrez l'utilitaire TUI de gestion du collecteur Keystone pour appliquer les modifications.

Installez Keystone Collector sur les systèmes Linux

Le logiciel Keystone Collector est distribué par un référentiel logiciel YUM en ligne. Vous devez importer et installer le fichier sur un serveur Linux.

Procédez comme suit pour installer le logiciel sur votre serveur Linux :

1. SSH vers le serveur Keystone Collector et passez à `root` privilège.
2. Importer la signature publique Keystone :
   `# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101`
3. Vérifiez que le bon certificat public a été importé en vérifiant l'empreinte de la plate-forme de facturation Keystone dans la base de données RPM :
   `# rpm -qa gpg-pubkey --qf '%<Description>'|gpg --show-keys --fingerprint`
   La bonne empreinte se présente comme suit :
   `90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D`

4. Téléchargez le `keystonerepo.rpm` fichier :
   `curl -O https://keystone.netapp.com/repo/keystonerepo.rpm`
5. Vérifiez l'authenticité du fichier :
   `rpm --checksig -v keystonerepo.rpm`La signature d'un fichier authentique se présente comme suit :
   `Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK`
6. Installez le fichier de référentiel du logiciel YUM :
   `# yum install keystonerepo.rpm`
7. Lorsque Keystone repo est installé, installez le package trapèze-Collector via le gestionnaire de package YUM :
   `# yum install keystone-collector`

> Une fois l'installation terminée, vous pouvez utiliser l'utilitaire TUI (Keystone Collector Management terminal User interface) pour effectuer les activités de configuration et de surveillance. Vous pouvez utiliser diverses commandes du clavier, telles que les touches entrée et flèche, pour sélectionner les options et naviguer dans cette TUI. Voir "Configurer le collecteur Keystone" et "Contrôle de l'état des systèmes" pour plus d'informations.

Validation automatique de l'intégrité logicielle

Il existe un processus de validation de l'intégrité du logiciel Keystone.

La configuration du client de référentiel Keystone YUM fournie dans `keystonerepo.rpm` Utilise la vérification GPG appliquée (`gpgcheck=1`) sur tous les logiciels téléchargés via ce référentiel. N'importe quel RPM téléchargé via le référentiel Keystone dont la validation de la signature échoue n'est pas possible. Cette fonctionnalité est utilisée dans la fonctionnalité de mise à jour automatique planifiée du collecteur Keystone afin de garantir que seuls les logiciels valides et authentiques sont installés sur votre site.

Informations sur le copyright

Informations sur les marques commerciales