



Installer Keystone Collector

Keystone

NetApp

January 08, 2026

This PDF was generated from <https://docs.netapp.com/fr-fr/keystone-staas-2/installation/vapp-installation.html> on January 08, 2026. Always check docs.netapp.com for the latest.

Sommaire

- Installer Keystone Collector 1
 - Déployer Keystone Collector sur les systèmes VMware vSphere 1
 - Déploiement du modèle OVA 1
 - Configuration initiale du système 2
 - Installer Keystone Collector sur les systèmes Linux 3
 - Validation automatique du logiciel Keystone 5

Installer Keystone Collector

Déployer Keystone Collector sur les systèmes VMware vSphere

Le déploiement de Keystone Collector sur les systèmes VMware vSphere comprend le téléchargement du modèle OVA, le déploiement du modèle à l'aide de l'assistant **Déployer un modèle OVF**, la vérification de l'intégrité des certificats et la vérification de la disponibilité de la machine virtuelle.

Déploiement du modèle OVA

Suivez ces étapes :

Étapes

1. Téléchargez le fichier OVA à partir de "[ce lien](#)" et stockez-le sur votre système VMware vSphere.
2. Sur votre système VMware vSphere, accédez à la vue **VM et modèles**.
3. Cliquez avec le bouton droit sur le dossier requis pour la machine virtuelle (VM) (ou le centre de données, si vous n'utilisez pas de dossiers de VM) et sélectionnez **Déployer le modèle OVF**.
4. À l'étape 1 de l'assistant **Déployer un modèle OVF**, cliquez sur **Sélectionner un modèle OVF** pour sélectionner le modèle téléchargé `KeystoneCollector-latest.ova` déposer.
5. À l'étape 2, spécifiez le nom de la machine virtuelle et sélectionnez le dossier de la machine virtuelle.
6. À l'étape 3, spécifiez la ressource de calcul requise pour exécuter la machine virtuelle.
7. À l'étape 4 : Vérifier les détails, assurez-vous de l'exactitude et de l'authenticité du fichier OVA.

Le magasin de certificats 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 Sectigo "[ici](#)".
- b. Suivez les étapes de la `Resolution` section de cet article de la base de connaissances (KB) : <https://kb.vmware.com/s/article/84240> .



Pour les versions 7.x et antérieures de vCenter, vous devez mettre à jour vCenter et ESXi vers la version 8.0 ou ultérieure. Les versions antérieures ne sont plus prises en charge.

Lorsque l'intégrité et l'authenticité de l'OVA Keystone Collector sont validées, vous pouvez voir le texte (Trusted certificate) avec l'éditeur.

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Select storage
- Select networks
- Customize template
- Ready to complete

Review details

Verify the template details.

Publisher	Sectigo Public Code Signing CA R36 (Trusted certificate)
Product	Keystone-Collector
Version	3.12.31910
Vendor	NetApp
Download size	1.7 GB
Size on disk	3.9 GB (thin provisioned) 19.5 GB (thick provisioned)

CANCEL
BACK
NEXT

- À l'étape 5 de l'assistant **Déployer le modèle OVF**, spécifiez l'emplacement de stockage de la machine virtuelle.
- À l'étape 6, sélectionnez le réseau de destination à utiliser par la machine virtuelle.
- À l'étape 7 Personnaliser le modèle, spécifiez l'adresse réseau initiale et le mot de passe du compte utilisateur administrateur.



Le mot de passe administrateur est stocké dans un format réversible dans vCenter et doit être utilisé comme identifiant d'amorçage pour obtenir un accès initial au système VMware vSphere. Lors de la configuration initiale du logiciel, ce mot de passe administrateur doit être modifié. Le masque de sous-réseau pour 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.

- À l'étape 8 Prêt à terminer de l'assistant **Déployer le modèle OVF**, vérifiez la configuration et que vous avez correctement défini les paramètres pour le déploiement OVA.

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

Configuration initiale du système

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



Une fois le déploiement terminé, vous pouvez utiliser l'utilitaire Keystone Collector Management Terminal User Interface (TUI) pour effectuer les activités de configuration et de surveillance. Vous pouvez utiliser différentes commandes du clavier, telles que les touches Entrée et fléchées, pour sélectionner les options et naviguer dans cette interface utilisateur graphique.

1. Ouvrez une session SSH sur le serveur Keystone Collector. Lorsque vous vous connectez, le système vous demandera de mettre à jour le mot de passe administrateur. Terminez la mise à jour du mot de passe administrateur si nécessaire.
2. Connectez-vous en utilisant le nouveau mot de passe pour accéder à l'interface utilisateur. Lors de la connexion, l'interface utilisateur apparaît.

Alternativement, vous pouvez le lancer manuellement en exécutant le `keystone-collector-tui` Commande CLI.

3. Si nécessaire, configurez les détails du proxy dans la section **Configuration > Réseau** sur 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 Keystone Collector pour appliquer les modifications.

Installer Keystone Collector sur les systèmes Linux

Vous pouvez installer le logiciel Keystone Collector sur un serveur Linux à l'aide d'un package RPM ou Debian. Suivez les étapes d'installation en fonction de votre distribution Linux.

Utilisation de RPM

1. Connectez-vous en SSH au serveur Keystone Collector et élevez-vous à `root` privilège.
 2. Importer la signature publique de Keystone :

```
# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020
```
 3. Assurez-vous que le certificat public correct a été importé en vérifiant l'empreinte numérique de Keystone Billing Platform dans la base de données RPM :

```
# rpm -qa gpg-pubkey --qf '%{Description}' | gpg --show-keys --fingerprint
```

L'empreinte digitale correcte ressemble à ceci :

```
9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC
```
 4. Téléchargez le `keystonerepo.rpm` déposer:

```
curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm
```
 5. Vérifiez l'authenticité du fichier :

```
rpm --checksig -v keystonerepo.rpm
```

La signature d'un fichier authentique ressemble à ceci :

```
Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK
```
 6. Installez le fichier du référentiel logiciel YUM :
 7. Une fois le dépôt Keystone installé, installez le package `keystone-collector` via le gestionnaire de packages YUM :
- ```
yum install keystone-collector
```
- Pour Red Hat Enterprise Linux 9, exécutez la commande suivante pour installer le package `keystone-collector` :
- ```
# yum install keystone-collector-rhel9
```

Utiliser Debian

1. Connectez-vous en SSH au serveur Keystone Collector et élevez-vous à `root` privilège.

```
sudo su
```
 2. Téléchargez le `keystone-sw-repo.deb` déposer:

```
curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
 3. Installez le fichier de référentiel de logiciels Keystone :
 4. Mettre à jour la liste des packages :
 5. Une fois le dépôt Keystone installé, installez le package `keystone-collector` :
- ```
apt-get install keystone-collector
```



Une fois l'installation terminée, vous pouvez utiliser l'utilitaire Keystone Collector Management Terminal User Interface (TUI) pour effectuer les activités de configuration et de surveillance. Vous pouvez utiliser différentes commandes du clavier, telles que les touches Entrée et fléchées, pour sélectionner les options et naviguer dans cette interface utilisateur graphique. Voir "[Configurer Keystone Collector](#)" et "[Surveiller la santé du système](#)" pour information.

## Validation automatique du logiciel Keystone

Le référentiel Keystone est configuré pour valider automatiquement l'intégrité du logiciel Keystone afin que seuls les logiciels valides et authentiques soient installés sur votre site.

La configuration du client du référentiel Keystone YUM fournie dans `keystonerepo.rpm` utilise la vérification GPG forcée(`gpgcheck=1`) sur tous les logiciels téléchargés via ce référentiel. Tout RPM téléchargé via le référentiel Keystone qui échoue à la validation de signature ne peut pas être installé. Cette fonctionnalité est utilisée dans la capacité de mise à jour automatique planifiée de Keystone Collector pour garantir que seuls des logiciels valides et authentiques sont installés sur votre site.

## Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.