Installer et configurer Keystone

Keystone

NetApp
June 28, 2024

Sommaire

Installer et configurer Keystone

De formation

Besoins de l'infrastructure virtuelle

Quelques configurations d'infrastructure virtuelle sont requises pour installer Keystone Collector sur vos systèmes VMware vSphere.

Prérequis pour la machine virtuelle du serveur Keystone Collector :

- Système d'exploitation : serveur VMware vCenter et ESXi 6.5 ou version ultérieure
- Cœur : 1 processeur
- RAM : 2 GO DE RAM
- Espace disque : 20 Go de vDisk

Autres exigences

S'assurer que les exigences génériques suivantes sont respectées :

Exigences de mise en réseau

Les exigences de mise en réseau de Keystone Collector sont répertoriées dans le tableau suivant.

Keystone Collector nécessite une connectivité Internet. Vous pouvez fournir une connectivité Internet par routage direct via la passerelle par défaut (via NAT) ou via le proxy HTTP. Les deux variantes sont décrites ici.

Source	Destination	Service	Protocole et ports	Catégorie	Objectif
Collecteur Keystone (pour Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatoire (en cas d'utilisation de Keystone ONTAP)	Collecte de metrics d'utilisation du collecteur Keystone pour ONTAP
Collecteur Keystone (pour Keystone StorageGRID)	Nœuds d'administration StorageGRID	HTTPS	TCP 443	Obligatoire (en cas d'utilisation de Keystone StorageGRID)	Collecte de metrics d'utilisation du collecteur Keystone pour StorageGRID

Collecteur Keystone (générique)	Internet (conformément aux exigences d'URL fournies ultérieurement)	HTTPS	TCP 80, TCP 443	Obligatoire (connectivité Internet)	Le logiciel Keystone Collector, les mises à jour du système d'exploitation et le téléchargement de metrics
Collecteur Keystone (générique)	Proxy HTTP client	Proxy HTTP	Port proxy client	Obligatoire (connectivité Internet)	Le logiciel Keystone Collector, les mises à jour du système d'exploitation et le téléchargement de metrics
Collecteur Keystone (générique)	Serveurs DNS du client	DNS	TCP/UDP 53	Obligatoire	Résolution DNS
Collecteur Keystone (générique)	Serveurs NTP du client	NTP	UDP 123	Obligatoire	Synchronisation de l'heure
Collecteur Keystone (pour Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	En option	Collecte de metrics de performance pour Keystone Collector
Collecteur Keystone (générique)	Système de surveillance client	HTTPS	TCP 7777	En option	Reporting sur l'état du collecteur Keystone
Postes de travail opérationnels du client	Collecteur Keystone	SSH	TCP 22	Gestion	Accès à la gestion des collecteurs Keystone
Adresses NetApp ONTAP de gestion de cluster et de nœud	Collecteur Keystone	HTTP_8000, PING	TCP 8000, demande/réponse d'écho ICMP	En option	Serveur Web pour les mises à jour du micrologiciel ONTAP

Accès à l'URL

Le collecteur Keystone doit accéder aux hôtes Internet suivants :

Adresse	Raison
https://keystone.netapp.com	Mises à jour logicielles Keystone Collector et rapports d'utilisation
https://support.netapp.com	Siège de NetApp, pour la facturation et la livraison AutoSupport

Configuration système requise pour Linux

La préparation de votre système Linux avec le logiciel requis garantit une installation et une collecte de données précises par Keystone Collector.

Assurez-vous que votre VM serveur Linux et Keystone Collector possède ces configurations.

Serveur Linux :

- Système d'exploitation : CentOS 7 ou Red Hat Enterprise Linux 8.6 ou version ultérieure
- Temps Chronyd synchronisé
- Accès aux référentiels logiciels Linux standard

Le même serveur doit également avoir les packages tiers suivants :

- Podman (Manager POD)
- sos
- chrony
- python 3 (3.6.8 à 3.9.13)

Serveur virtuel Keystone Collector :

- Cœur : 2 processeurs
- RAM : 4 GO DE RAM
- Espace disque : 50 Go de vDisk

Autres exigences

S'assurer que les exigences génériques suivantes sont respectées :

Exigences de mise en réseau

Les exigences de mise en réseau de Keystone Collector sont répertoriées dans le tableau suivant.

> Keystone Collector nécessite une connectivité Internet. Vous pouvez fournir une connectivité Internet par routage direct via la passerelle par défaut (via NAT) ou via le proxy HTTP. Les deux variantes sont décrites ici.

Source	Destination	Service	Protocole et ports	Catégorie	Objectif
Collecteur Keystone (pour Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatoire (en cas d'utilisation de Keystone ONTAP)	Collecte de metrics d'utilisation du collecteur Keystone pour ONTAP
Collecteur Keystone (pour Keystone StorageGRID)	Nœuds d'administration StorageGRID	HTTPS	TCP 443	Obligatoire (en cas d'utilisation de Keystone StorageGRID)	Collecte de metrics d'utilisation du collecteur Keystone pour StorageGRID
Collecteur Keystone (générique)	Internet (conformément aux exigences d'URL fournies ultérieurement)	HTTPS	TCP 80, TCP 443	Obligatoire (connectivité Internet)	Le logiciel Keystone Collector, les mises à jour du système d'exploitation et le téléchargement de metrics
Collecteur Keystone (générique)	Proxy HTTP client	Proxy HTTP	Port proxy client	Obligatoire (connectivité Internet)	Le logiciel Keystone Collector, les mises à jour du système d'exploitation et le téléchargement de metrics
Collecteur Keystone (générique)	Serveurs DNS du client	DNS	TCP/UDP 53	Obligatoire	Résolution DNS
Collecteur Keystone (générique)	Serveurs NTP du client	NTP	UDP 123	Obligatoire	Synchronisation de l'heure
Collecteur Keystone (pour Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	En option	Collecte de metrics de performance pour Keystone Collector

Collecteur Keystone (générique)	Système de surveillance client	HTTPS	TCP 7777	En option	Reporting sur l'état du collecteur Keystone
Postes de travail opérationnels du client	Collecteur Keystone	SSH	TCP 22	Gestion	Accès à la gestion des collecteurs Keystone
Adresses NetApp ONTAP de gestion de cluster et de nœud	Collecteur Keystone	HTTP_8000, PING	TCP 8000, demande/réponse d'écho ICMP	En option	Serveur Web pour les mises à jour du micrologiciel ONTAP

Accès à l'URL

Le collecteur Keystone doit accéder aux hôtes Internet suivants :

Adresse	Raison
https://keystone.netapp.com	Mises à jour logicielles Keystone Collector et rapports d'utilisation
https://support.netapp.com	Siège de NetApp, pour la facturation et la livraison AutoSupport

Conditions requises pour ONTAP et StorageGRID

Vous devez remplir quelques conditions préalables supplémentaires pour ONTAP et StorageGRID. Assurez-vous d'avoir rempli ces conditions préalables spécifiques en plus de la configuration système requise pour Linux/VMware vSphere. Cliquez sur l'onglet requis pour en savoir plus.

ONTAP

Versions logicielles

1. ONTAP 9.8 ou version ultérieure
2. Active IQ Unified Manager (Unified Manager) 9.10 ou version ultérieure

Avant de commencer

1. Assurez-vous que Unified Manager 9.10 ou version ultérieure est configuré. Pour plus d'informations sur l'installation de Unified Manager, consultez les liens suivants :
   - "Installation de Unified Manager sur des systèmes VMware vSphere"
   - "Installation de Unified Manager sur des systèmes Linux"
2. Vérifiez que le cluster ONTAP a été ajouté à Unified Manager. Pour plus d'informations sur l'ajout de clusters, reportez-vous à la section "Ajout de clusters".
3. Créez des utilisateurs Unified Manager avec des rôles spécifiques pour la collecte de données sur l'utilisation et les performances. Procédez comme suit. Pour plus d'informations sur les rôles d'utilisateur, reportez-vous à la section "Définitions des rôles utilisateur".
   a. Connectez-vous à l'interface utilisateur Web d'Unified Manager à l'aide des informations d'identification utilisateur par défaut de l'administrateur de l'application générées lors de l'installation. Voir "Accès à l'interface utilisateur Web de Unified Manager".
   b. Créez un compte de service pour Keystone Collector avec `Operator` rôle utilisateur. Les API du service Keystone Collector utilisent ce compte de service pour communiquer avec Unified Manager et collecter les données d'utilisation. Voir "Ajout d'utilisateurs".
   c. Créer un `Database` compte utilisateur, avec le `Report Schema` rôle. Cet utilisateur est requis pour la collecte des données de performances. Voir "Création d'un utilisateur de base de données".
4. Activez API Gateway dans Unified Manager. Keystone Collector utilise la fonctionnalité de passerelle d'API pour communiquer avec les clusters ONTAP. Vous pouvez activer la passerelle d'API depuis l'interface utilisateur Web ou en exécutant quelques commandes via l'interface de ligne de commande Unified Manager.

   Interface utilisateur Web

   Pour activer API Gateway à partir de l'interface utilisateur Web d'Unified Manager, connectez-vous à l'interface utilisateur Web d'Unified Manager et activez API Gateway. Pour plus d'informations, reportez-vous à la section "Activation de la passerelle API".

   CLI

   Pour activer la passerelle d'API via l'interface de ligne de commande d'Unified Manager, effectuez la procédure suivante :

   a. Sur le serveur Unified Manager, démarrez une session SSH et connectez-vous à l'interface de ligne de commande d'Unified Manager.
   `um cli login -u <*umadmin*>`Pour plus d'informations sur les commandes CLI, reportez-vous à la section "Commandes CLI Unified Manager prises en charge".
   b. Vérifiez si la passerelle API est déjà activée.
   `um option list api.gateway.enabled`A `true` Valeur indique que la passerelle d'API est activée.
   c. Si la valeur renvoyée est `false`, exécutez la commande suivante :
   `um option set api.gateway.enabled=true`

d. Redémarrez le serveur Unified Manager :

- Linux : "Redémarrage de Unified Manager".
- VMware vSphere : "Redémarrage de la machine virtuelle Unified Manager".

StorageGRID

Les configurations suivantes sont requises pour l'installation de Keystone Collector sur StorageGRID.

- StorageGRID `11.6.0` ou une version ultérieure doit être installée. Pour plus d'informations sur la mise à niveau de StorageGRID, voir "Mettre à niveau le logiciel StorageGRID : présentation".
- Un compte utilisateur admin local StorageGRID doit être créé pour la collecte des données d'utilisation. Ce compte de service est utilisé par le service Keystone Collector pour communiquer avec StorageGRID via les API du nœud administrateur.

  Étapes

  a. Connectez-vous au Gestionnaire de grille. Voir "Connectez-vous au Grid Manager".

  b. Créez un groupe d'administration local avec `Access mode: Read-only`. Voir "Créer un groupe d'administration".

  c. Ajoutez les autorisations suivantes :

  - Comptes de locataires
  - Maintenance
  - Requête de metrics

  d. Créez un utilisateur de compte de service Keystone et associez-le au groupe d'administration. Voir "Gérer les utilisateurs".

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.

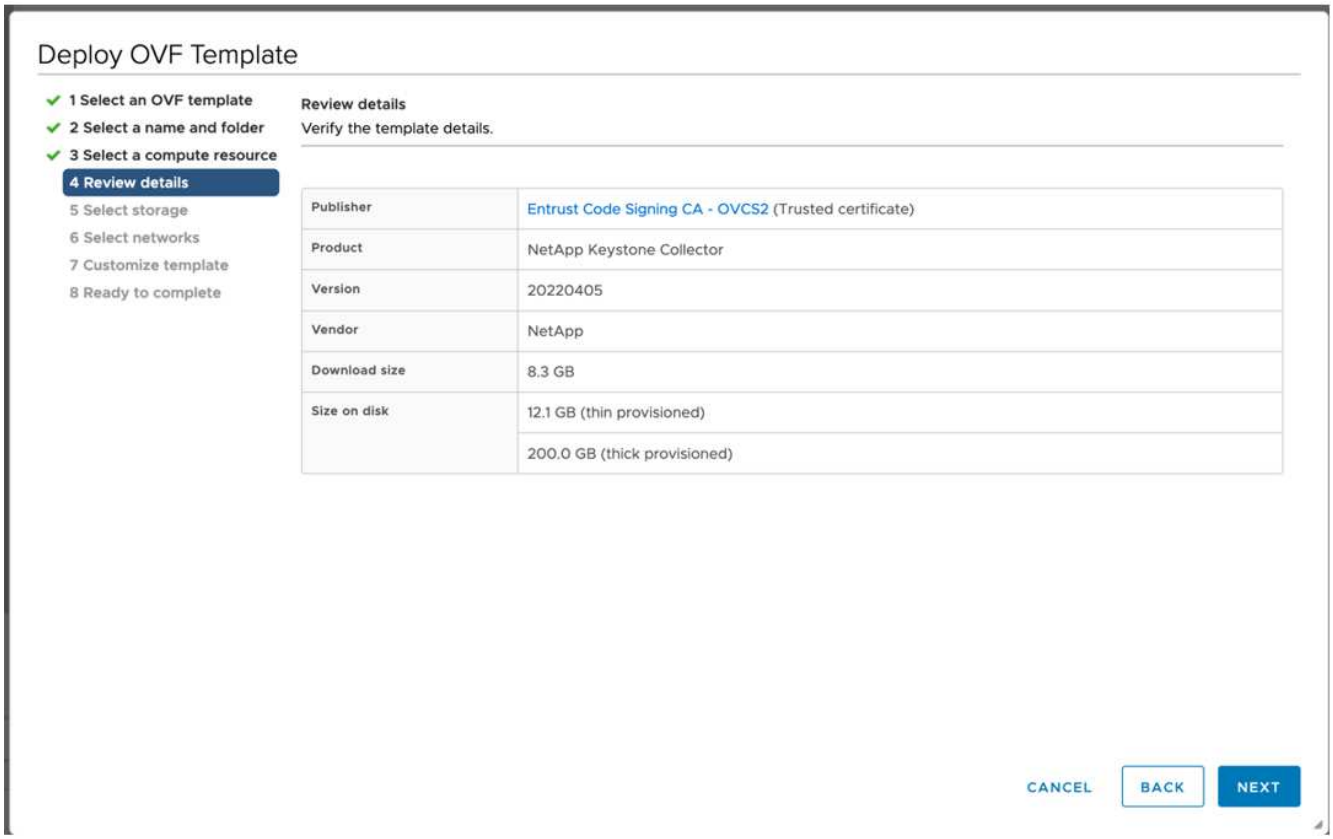
   a. Cliquez sur le lien **Publisher** pour télécharger le certificat de signature complet.
   b. Téléchargez le certificat public *Keystone Billing* sur "ce lien".
   c. Vérifiez l'authenticité du certificat de signature OVA par rapport au certificat public en utilisant OpenSSL :
      `openssl verify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

Configurer le collecteur Keystone

Vous devez effectuer quelques tâches de configuration pour permettre à Keystone Collector de collecter des données d'utilisation dans votre environnement de stockage. Il s'agit d'une activité unique permettant d'activer et d'associer le composant collecteur requis à votre environnement de stockage.

Le collecteur Keystone fournit l'utilitaire TUI (Keystone Collector Management terminal User interface) pour effectuer des 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.

Étapes

1. Démarrez l'utilitaire TUI de gestion du collecteur Keystone :
   ```
   $ keystone-collector-tui
   ```
2. Accédez à **configurer > KS-Collector** pour ouvrir l'écran de configuration du collecteur Keystone et afficher les options de mise à jour disponibles.
3. Mettez à jour les options requises.

**® ou ONTTHI **

- **Collect ONTAP usage** : cette option permet la collecte des données d'utilisation pour ONTAP. Ajoutez les détails du serveur Active IQ Unified Manager (Unified Manager) et du compte de service.
- **Collecter les données de performances ONTAP** : cette option permet la collecte des données de performances pour ONTAP. Cette option est désactivée par défaut. Activez cette option si un contrôle des performances est requis dans votre environnement pour des objectifs de niveau de service. Fournissez les détails du compte d'utilisateur de la base de données Unified Manager. Pour plus d'informations sur la création d'utilisateurs de base de données, voir "Créer les utilisateurs Unified Manager".
- **Supprimer les données privées** : cette option supprime des données privées spécifiques des clients et est activée par défaut. Pour plus d'informations sur les données exclues des mesures si cette option est activée, reportez-vous à la section "Limite la collecte de données privées".

**® ou **

- **Collect StorageGRID usage** : cette option permet de collecter les détails d'utilisation des nœuds. Ajoutez l'adresse du nœud StorageGRID et les détails de l'utilisateur.
- **Supprimer les données privées** : cette option supprime des données privées spécifiques des clients et est activée par défaut. Pour plus d'informations sur les données exclues des mesures si cette option est activée, reportez-vous à la section "Limite la collecte de données privées".

4. Activez/désactivez le champ **Démarrer KS-Collector avec System**.
5. Cliquez sur **Enregistrer**
.

6. Assurez-vous que le collecteur Keystone est en bon état en retournant à l'écran principal de l'interface utilisateur TUI et en vérifiant les informations **État du service**. Le système devrait montrer que les services sont dans un **état général : sain**

7. Quittez l'interface TUI de gestion du collecteur Keystone en sélectionnant l'option **Quitter vers Shell** sur l'écran d'accueil.

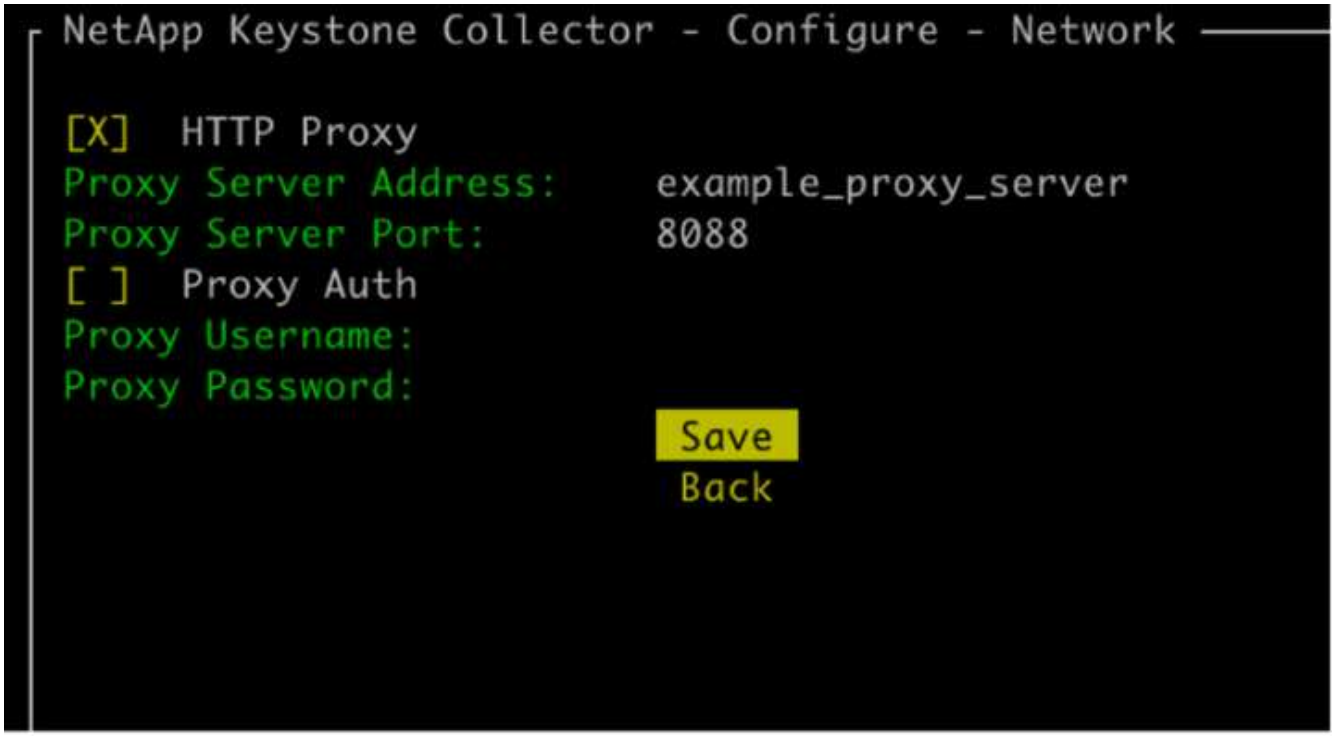
Configurez le proxy HTTP sur le collecteur Keystone

Le logiciel Collector prend en charge l'utilisation d'un proxy HTTP pour communiquer avec Internet. Ceci peut être configuré dans la TUI.

Étapes

1. Redémarrez l'utilitaire TUI de gestion du collecteur Keystone s'il est déjà fermé :
   ```
   $ keystone-collector-tui
   ```
2. Activez le champ **HTTP Proxy** et ajoutez les détails du serveur proxy HTTP, du port et des informations d'identification, si l'authentification est requise.

3. Cliquez sur **Enregistrer**
.



Limite la collecte de données privées

Le collecteur Keystone collecte des informations limitées sur la configuration, l'état et les performances requises pour effectuer les mesures d'abonnement. Il existe une option permettant de limiter davantage les informations recueillies en masquant les informations sensibles du contenu téléchargé. Cela n'a aucune incidence sur le calcul de la facturation. Toutefois, la limitation des informations peut avoir un impact sur la facilité d'utilisation des informations de reporting, car certains éléments, facilement identifiables par les utilisateurs, tels que le nom du volume, sont remplacés par des UUID.

La limitation de la collecte de données client spécifiques est une option configurable sur l'écran de l'interface utilisateur Keystone Collector. Cette option, **Supprimer les données privées**, est activée par défaut.

Pour plus d'informations sur les éléments supprimés lors de la limitation de l'accès privé aux données dans ONTAP et StorageGRID, reportez-vous à la section "Liste des éléments supprimés pour limiter l'accès aux données privées".

Faites confiance à une autorité de certification racine personnalisée

La vérification des certificats par rapport à une autorité de certification (CA) racine publique fait partie des fonctionnalités de sécurité du collecteur Keystone. Toutefois, si nécessaire, vous pouvez configurer Keystone Collector pour qu'il puisse faire confiance à une autorité de certification racine personnalisée.

Si vous utilisez l'inspection SSL/TLS dans le pare-feu de votre système, le trafic basé sur Internet est de nouveau chiffré avec votre certificat d'autorité de certification personnalisé. Il est nécessaire de configurer les paramètres pour vérifier la source en tant qu'autorité de certification approuvée avant d'accepter le certificat racine et d'autoriser les connexions. Voici la procédure à suivre :

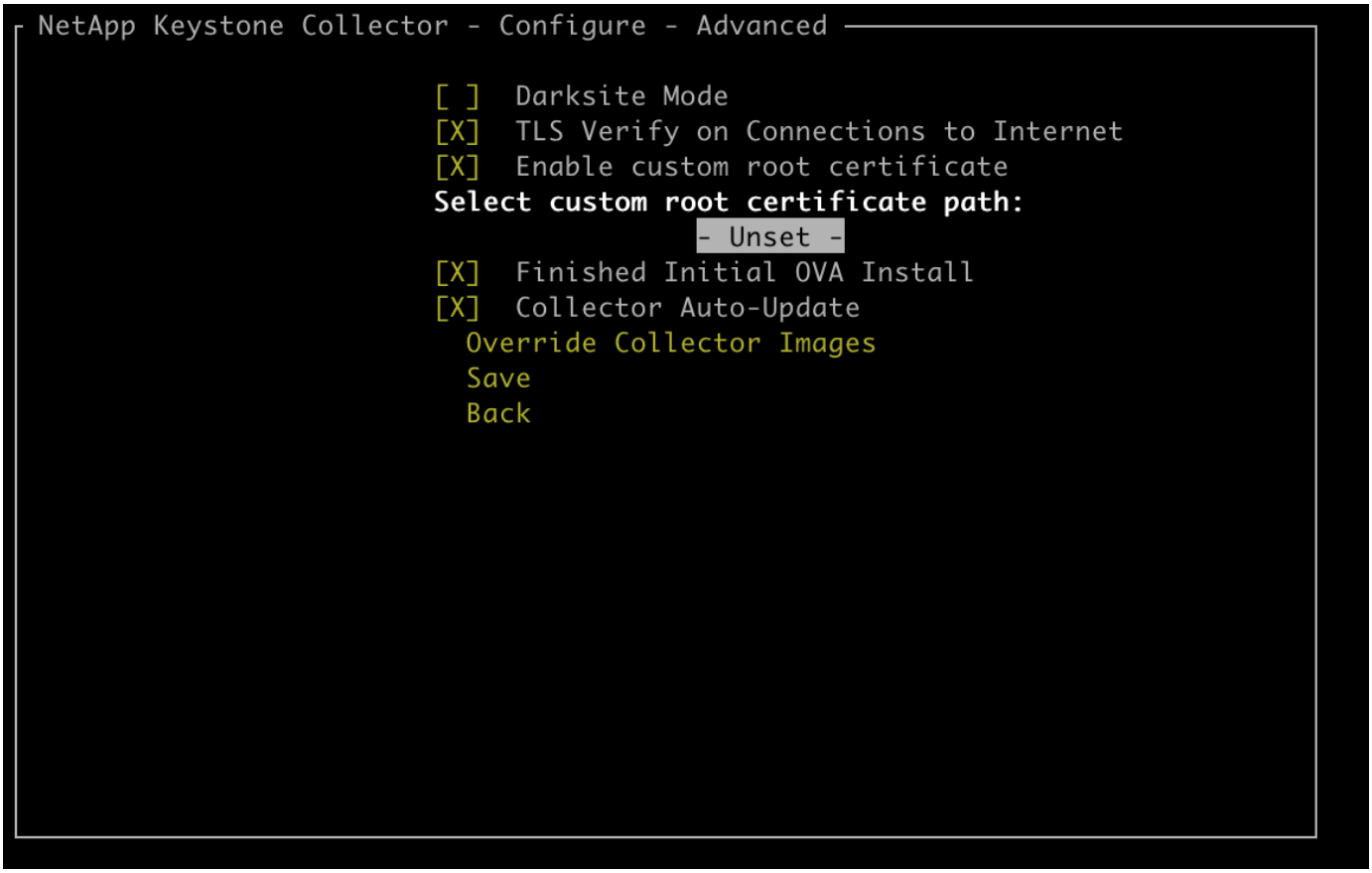
Étapes

1. Préparez le certificat de l'autorité de certification. Il doit être au format de fichier X.509_ codé en _base64.

   Les extensions de fichier prises en charge sont `.pem`, `.crt`, `.cert`. Assurez-vous que le certificat est dans l'un de ces formats.

2. Copiez le certificat sur le serveur Keystone Collector. Notez l'emplacement où le fichier est copié.
3. Ouvrez un terminal sur le serveur et exécutez l'utilitaire de gestion TUI.
   ```
   $ keystone-collector-tui
   ```
4. Accédez à **Configuration > Avancé**.

5. Activez l'option **Activer le certificat racine personnalisé**.
6. Pour **sélectionnez le chemin du certificat racine personnalisé :**, sélectionnez `- Unset -`
7. Appuyez sur entrée. Une boîte de dialogue permettant de sélectionner le chemin du certificat s'affiche.
8. Sélectionnez le certificat racine dans le navigateur du système de fichiers ou entrez le chemin exact.
9. Appuyez sur entrée. Vous revenez à l'écran **Avancé**.
10. Sélectionnez **Enregistrer**. La configuration est appliquée.



Configurez AutoSupport pour Keystone

Lorsque vous utilisez le mécanisme de télémétrie AutoSupport, Keystone calcule l'utilisation en fonction des données de télémétrie AutoSupport. Pour atteindre le niveau de granularité nécessaire, vous devez configurer AutoSupport de manière à intégrer les données Keystone dans les bundles de support quotidiens envoyés par les clusters ONTAP.

Description de la tâche

Avant de configurer AutoSupport pour inclure des données Keystone, veillez à noter les points suivants.

- Vous pouvez modifier les options de télémétrie AutoSupport à l'aide de l'interface de ligne de commande ONTAP. Pour plus d'informations sur la gestion des services AutoSupport et du rôle d'administrateur système (cluster), reportez-vous à la section "Présentation de Manage AutoSupport" et "Administrateurs Cluster et SVM".
- Vous incluez les sous-systèmes dans les bundles AutoSupport quotidiens et hebdomadaires pour garantir

la collecte précise des données pour Keystone. Pour plus d'informations sur les sous-systèmes AutoSupport, reportez-vous à la section "Nature des sous-systèmes AutoSupport".

Étapes

1. En tant qu'administrateur système, connectez-vous au cluster Keystone ONTAP à l'aide de SSH. Pour plus d'informations, reportez-vous à la section "Accéder au cluster via SSH".
2. Modifier le contenu du journal.
   - Exécutez cette commande pour modifier le contenu du journal quotidien :

     ```
     autosupport trigger modify -node * -autosupport-message
     management.log -basic-additional
     wafl,performance,snapshot,platform,object_store_server,san,raid,snapm
     irror -troubleshooting-additional wafl
     ```

   - Exécutez cette commande pour modifier le contenu du journal hebdomadaire :

     ```
     autosupport trigger modify -autosupport-message weekly
     -troubleshooting-additional wafl -node *
     ```

     Pour plus d'informations sur cette commande, voir "modification du déclencheur AutoSupport du nœud système".

Sécurité du collecteur Keystone

Le collecteur Keystone inclut des fonctionnalités de sécurité qui surveillent les metrics de performance et d'utilisation des systèmes Keystone, sans compromettre la sécurité des données des clients.

Le fonctionnement du collecteur Keystone repose sur les principes de sécurité suivants :

- **Privacy by design**-Keystone Collector collecte des données minimales pour effectuer des mesures d'utilisation et une surveillance des performances. Pour plus d'informations, voir "Données collectées pour la facturation". Le "Supprimer les données privées" l'option est activée par défaut, qui masque et protège les informations sensibles.
- **Accès avec le moindre privilège**-Keystone Collector requiert des autorisations minimales pour surveiller les systèmes de stockage, ce qui minimise les risques de sécurité et empêche toute modification involontaire des données. Cette approche s'aligne sur le principe du privilège minimum et améliore la sécurité globale des environnements surveillés.
- **Cadre de développement logiciel sécurisé**- Keystone utilise un framework de développement logiciel sécurisé tout au long du cycle de développement, qui limite les risques, réduit les vulnérabilités et protège le système contre les menaces potentielles.

Renforcement de la sécurité

Par défaut, Keystone Collector est configuré pour utiliser des configurations renforcées par la sécurité. Les configurations de sécurité recommandées sont les suivantes :

- Système d'exploitation de la machine virtuelle Keystone Collector :
  - Conforme à la norme CIS Debian Linux 12 Benchmark. Toute modification de la configuration du système d'exploitation en dehors du logiciel de gestion Keystone Collector peut réduire la sécurité du système. Pour plus d'informations, voir "Guide de référence CIS".
  - Reçoit et installe automatiquement les correctifs de sécurité vérifiés par Keystone Collector via la fonction de mise à jour automatique. La désactivation de cette fonctionnalité peut entraîner des logiciels vulnérables non corrigés.
  - Authentifie les mises à jour reçues du collecteur Keystone. La désactivation de la vérification du référentiel APT peut entraîner l'installation automatique de correctifs non autorisés, ce qui peut entraîner des vulnérabilités.
- Le collecteur Keystone valide automatiquement les certificats HTTPS pour assurer la sécurité de la connexion. La désactivation de cette fonction peut entraîner l'usurpation d'identité des terminaux externes et une fuite de données d'utilisation.
- Prise en charge de Keystone Collector "Autorité de certification approuvée personnalisée" certification. Par défaut, elle fait confiance aux certificats signés par les autorités de certification racine publiques reconnues par le "Programme de certificat Mozilla CA". En activant d'autres autorités de certification approuvées, Keystone Collector active la validation du certificat HTTPS pour les connexions aux terminaux qui présentent ces certificats.
- Le collecteur Keystone active par défaut l'option **Supprimer les données privées**, qui masque et protège les informations sensibles. Pour plus d'informations, voir "Limite la collecte de données privées". Si cette option est désactivée, d'autres données sont communiquées au système Keystone. Par exemple, il peut inclure des informations saisies par l'utilisateur, telles que les noms de volume, qui peuvent être considérées comme des informations sensibles.

Informations connexes

- "Présentation du collecteur Keystone"
- "Besoins de l'infrastructure virtuelle"
- "Configurer le collecteur Keystone"

Types de données utilisateur recueillies par Keystone

Keystone collecte des informations sur la configuration, l'état et l'utilisation de vos abonnements Keystone ONTAP et Keystone StorageGRID. Il peut également collecter des données de performances pour ONTAP uniquement, si l'option est activée dans le collecteur Keystone.

Collecte de données ONTAP

**Données requises pour ONTAP : apprenez-en plus sur **

La liste suivante présente un échantillon représentatif des données de consommation de capacité collectées pour ONTAP :

- Clusters
  - UUID de cluster
  - Nom du cluster
  - Numéro de série
  - Emplacement (basé sur la valeur saisie dans le cluster ONTAP)
  - Contactez
  - Version
- Nœuds
  - Numéro de série
  - Nom du nœud
- Volumes
  - Nom de l’agrégat
  - Nom du volume
  - VolumeInstanceUUID
  - Indicateur IsononeVolume
  - Indicateur IsFlexGroupCongent
  - Balise IsSpaceEnforcelogique
  - IsSpaceReportDédrapeau logique
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - QoSAdaptivePolicyGroup Name
  - Nom du groupe QoSPolicyGroup
  - Taille
  - Utilisé
  - PhysicalUsed
  - SizeUsedBysnapshots
  - Type
  - VolumeStyleExtended
  - Nom d’un vserver
  - Drapeau IsVsRoot
- VServers
  - Nom du serveur virtuel

    - UUID de serveur virtuel
    - Sous-type
- Agrégats de stockage
    - StorageType
    - Nom de l’agrégat
    - UUID d’agrégat
- Agrégez les magasins d’objets
    - ObjectStoreName
    - ObjectStoreUUID
    - ProviderType
    - Nom de l’agrégat
- Clones de volumes
    - FlexClone
    - Taille
    - Utilisé
    - Un vServer
    - Type
    - ParentVolume
    - Vserver Parent
    - IsConstituent
    - SpliitEstimate
    - État
    - FlexCloneUsedPercent
- LUN de stockage
    - UUID DE LUN
    - Nom de LUN
    - Taille
    - Utilisé
    - Indicateur réservé
    - Indicateur IsRequested
    - Nom de l’unité LogicalUnit
    - UUID QoSPolicy
    - QoSPolicyName
    - VolumeUUID
    - Nom du volume
    - UUID DE SVMS
    - Nom du SVM

- Volumes de stockage
  - VolumeInstanceUUID
  - Nom du volume
  - Nom du SVMs
  - UUID DE SVMS
  - UUID QoSPolicy
  - QoSPolicyName
  - CapacityTierFootprint
  - Empreinte Performance TierFootprint
  - Empreinte totale
  - Règle de niveau
  - Indicateur isProtected
  - Indicateur IsDest
  - Utilisé
  - PhysicalUsed
  - UUID de clone
  - LogicalSpaceUsedByAfs
- Groupes de règles de QoS
  - PolicyGroup
  - UUID QoSPolicy
  - Débit maximal
  - Débit minimum
  - MaxThrouputIOPS
  - MaxThroughputMBps
  - Débit minimum IOPS
  - Mini-débit MBps
  - Indicateur IsShared
- Groupes de règles de QoS adaptative ONTAP
  - QoSPolicyName
  - UUID QoSPolicy
  - PeakIOPS
  - PeakIOPSAlallocation
  - AbsoluteMinIOPS
  - IOPS ExpectedIOPS
  - ExpectedIOPSAlallocation
  - Taille de bloc
- Empreintes

    - Un vServer
    - Volumétrie
    - Empreinte totale
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- Clusters MetroCluster
    - UUID de cluster
    - Nom du cluster
    - UUID de RemoteCluster
    - RemoteCluserName
    - LocalConfigurationState
    - Etat de configuration distant
    - Mode
- Mesures de l’observabilité du collecteur
    - Heure de collecte
    - Requête du terminal de l’API Active IQ Unified Manager
    - Temps de réponse
    - Nombre d’enregistrements
    - IP AIQUMInstance
    - ID de Collectorinstance

**Données requises pour ONTAP : apprenez-en plus sur **

La liste suivante présente un échantillon représentatif des données de performances collectées pour ONTAP :

- Nom de cluster
- UUID de cluster
- ID d'objet
- Nom du volume
- UUID d'instance de volume
- Un vServer
- UUID de serveur virtuel
- Série du nœud
- ONTAPVersion
- Version AIQUM
- Agrégat
- UUID d'agrégation
- ResourceKey
- Horodatage
- IOPSPertb
- Latence
- ReadLatency
- Écrire les MBps
- Latence de débit QoSMinputLatency
- Latence QoSNBlade
- Salle d'écoute UsedHeadRoom
- CacheMissratio
- Latence
- QoSAggregateLatency
- D'IOPS
- Letency. QoSNetworkency
- AvailableOps
- Latence d'écriture
- Latence QoSCloudLatency
- QoSClusterInterconnectLatency
- OtherMBps
- Latence QoSCopLatency
- QoSDBladeLatency
- Du stockage

- ReadIOPS
- Mo/sec
- IOPS Autrestockage
- QoSPolicyGroupLatency
- Lecture MBps
- QoSSyncSnapmirrorLatency
- Écrire les IOPS

** : suppression des éléments limitant l'accès aux données privées : apprenez au mieux **

Lorsque l'option **Supprimer les données privées** est activée sur le collecteur Keystone, les informations d'utilisation suivantes sont supprimées pour ONTAP. Cette option est activée par défaut.

- Nom de cluster
- Emplacement du cluster
- Contact de cluster
- Nom du nœud
- Nom de l'agrégat
- Nom du volume
- QoSAdaptivePolicyGroup Name
- Nom du groupe QoSPolicyGroup
- Nom d'un vserver
- Nom de la LUN de stockage
- Nom de l'agrégat
- Nom de l'unité LogicalUnit
- Nom du SVM
- IP AIQUMInstance
- FlexClone
- RemoteClusterName

Collecte de données StorageGRID

**Données requises pour StorageGRID : apprenez-en plus sur **

La liste suivante est un échantillon représentatif du `Logical Data` Collectées pour StorageGRID :

- ID StorageGRID
- ID de compte
- Nom du compte
- Octets de quota de compte
- Nom du compartiment
- Nombre d'objets de compartiment
- Octets de données de compartiment

La liste suivante est un échantillon représentatif du `Physical Data` Collectées pour StorageGRID :

- ID StorageGRID
- ID de nœud
- ID du site
- Nom du site
- Fréquence
- Octets d'utilisation du stockage StorageGRID
- Octets de métadonnées d'utilisation du stockage StorageGRID

** : suppression des éléments limitant l'accès aux données privées : apprenez au mieux **

Lorsque l'option **Supprimer les données privées** est activée sur le collecteur Keystone, les informations d'utilisation suivantes sont supprimées pour StorageGRID. Cette option est activée par défaut.

- Nom de compte
- Nom de la personne
- Nom du site
- Instance/NodeName

Informations sur le copyright

Informations sur les marques commerciales