Installer et configurer Keystone

Keystone

NetApp
January 14, 2026

Sommaire

Installer et configurer Keystone

De formation

Configuration requise pour l'infrastructure virtuelle de Keystone Collector

Votre système VMware vSphere doit répondre à plusieurs exigences avant de pouvoir installer Keystone Collector.

Prérequis pour la machine virtuelle du serveur Keystone Collector :

- Système d'exploitation : serveur VMware vCentre et ESXi 8.0 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 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

Le port par défaut de MySQL, 3306, est limité à localhost uniquement lors d'une nouvelle installation d'Unified Manager, ce qui empêche la collecte des mesures de performances pour Keystone Collector. Pour plus d'informations, voir "Configuration requise pour 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 requise pour Keystone Collector sous 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 : l'un des systèmes suivants :
  - Debian 12
  - Red Hat Enterprise Linux 8.6 ou versions ultérieures 8.x.
  - Red Hat Enterprise Linux 9.0 ou versions ultérieures
  - CentOS 7 (pour les environnements existants uniquement)
- 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 (3.9.14 à 3.11.8)

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 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

Le port par défaut de MySQL, 3306, est limité à localhost uniquement lors d'une nouvelle installation d'Unified Manager, ce qui empêche la collecte des mesures de performances pour Keystone Collector. Pour plus d'informations, voir "Configuration requise pour 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 requise pour ONTAP et StorageGRID pour Keystone

Avant de commencer à utiliser Keystone, vous devez vous assurer que les clusters ONTAP et les systèmes StorageGRID répondent à quelques exigences.

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

Si vous prévoyez de collecter des données d'utilisation uniquement via ONTAP, respectez les exigences suivantes :

1. Assurez-vous que ONTAP 9.8 ou version ultérieure est configuré. Pour plus d'informations sur la configuration d'un nouveau cluster, reportez-vous aux liens suivants :
   - "Configurez ONTAP sur un nouveau cluster avec System Manager"
   - "Configuration d'un cluster via l'interface de ligne de commandes"
2. Créez des comptes de connexion ONTAP avec des rôles spécifiques. Pour en savoir plus, reportez-vous "En savoir plus sur la création de comptes de connexion ONTAP" à la section .
   - **Interface utilisateur Web**
     i. Connectez-vous à ONTAP System Manager à l'aide de vos informations d'identification par défaut. Pour en savoir plus, reportez-vous "Gestion du cluster avec System Manager" à la section .
     ii. Créez un utilisateur ONTAP avec le rôle « lecture seule » et le type d'application « http », puis activez l'authentification par mot de passe en accédant à **Cluster > Paramètres > sécurité > utilisateurs**.
   - **CLI**
     i. Connectez-vous à l'interface de ligne de commande ONTAP à l'aide de vos identifiants par défaut. Pour en savoir plus, reportez-vous "Gestion du cluster avec interface de ligne de commande" à la section .
     ii. Créez un utilisateur ONTAP avec le rôle « lecture seule » et le type d'application « http », puis activez l'authentification par mot de passe. Pour en savoir plus sur l'authentification, reportez-vous "Activez l'accès par mot de passe du compte ONTAP" à la section .

Si vous prévoyez de collecter des données d'utilisation via Active IQ Unified Manager, respectez les exigences suivantes :

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".

> Le port par défaut pour MySQL, 3306, est limité à localhost uniquement lors d'une nouvelle installation d'Unified Manager, qui empêche la collecte des données de performances pour Keystone ONTAP. Cette configuration peut être modifiée et la connexion peut être mise à disposition d'autres hôtes à l'aide de l' `Control access to MySQL port 3306` option de la console de maintenance d'Unified Manager. Pour plus d'informations, voir "Options de menu supplémentaires".

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. À l'étape 4 : Vérifier les détails, assurez-vous de l'exactitude et de l'authenticité du fichier OVA.

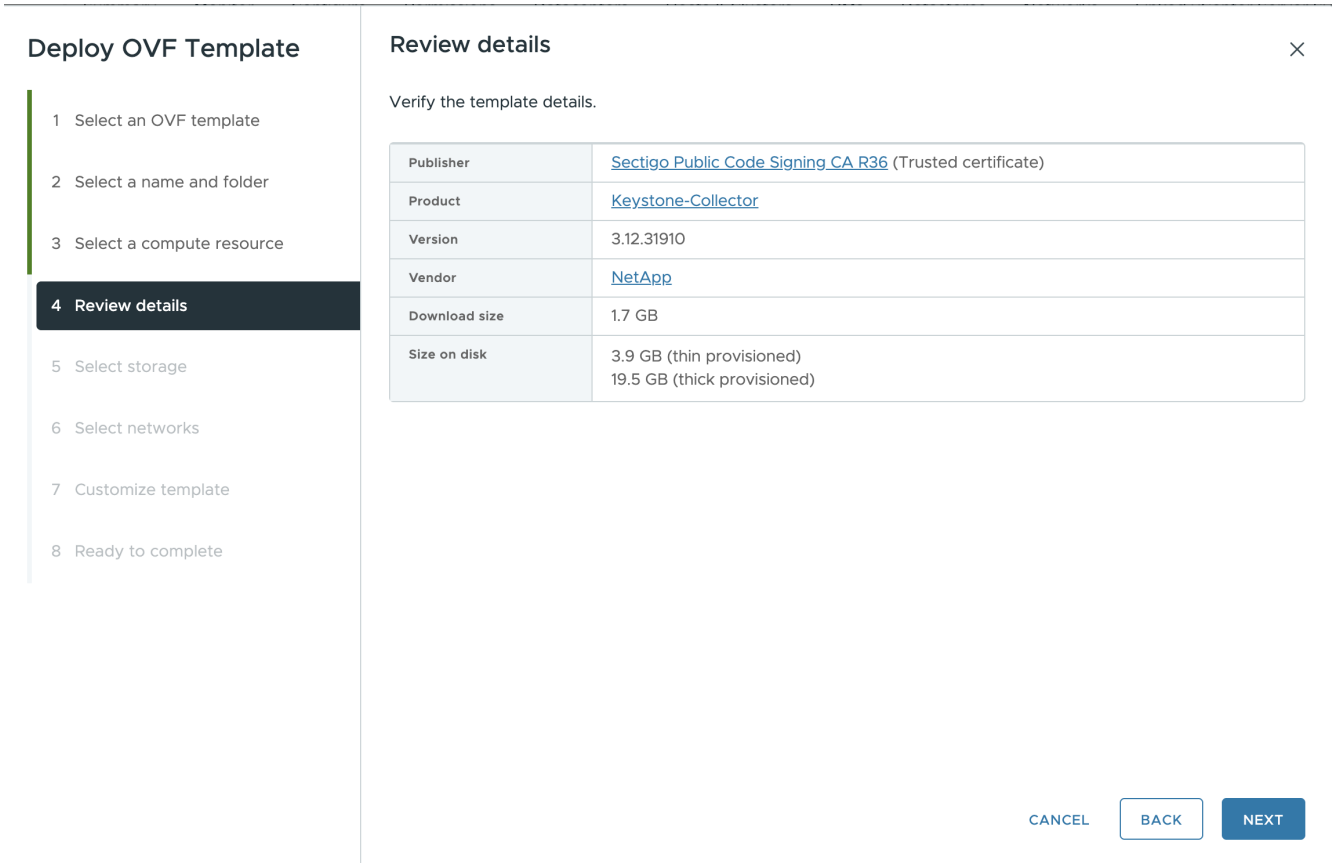
   Le magasin de certificats de confiance racine vCenter contient uniquement des certificats VMware. NetApp utilise Entrust comme autorité de certification et ces certificats doivent être ajoutés au magasin de confiance vCenter.

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

   b. Suivez les étapes de la section `Resolution` Article de la base de connaissances : 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.



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

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

Utilisation de RPM

1. SSH vers le serveur Keystone Collector et passez 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 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
   ```

   Pour Red Hat Enterprise Linux 9, exécutez la commande suivante pour installer le package keystone-collector :
   `# yum install keystone-collector-rhel9`

Utilisation de Debian

1. SSH sur le serveur Keystone Collector et élever au `root` privilège.
   `sudo su`
2. Télécharger le `keystone-sw-repo.deb` fichier :
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Installez le fichier de référentiel du logiciel Keystone :
   `# dpkg -i keystone-sw-repo.deb`
4. Mettre à jour la liste des packages :
   `# apt-get update`
5. Une fois le référentiel Keystone installé, installez le package de collecteur Keystone :
   `# apt-get 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 du logiciel Keystone

Le référentiel Keystone est configuré de manière à valider automatiquement l'intégrité du logiciel Keystone de sorte que seul un logiciel valide et authentique soit installé sur votre site.

La configuration du client de référentiel Keystone YUM fournie dans utilise la `keystonerepo.rpm` 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 de Keystone Collector pour garantir que seul un logiciel valide et authentique est installé 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 qui permet d'activer et d'associer les composants requis à votre environnement de stockage.

- Keystone Collector met à votre disposition 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.
- Keystone Collector peut être configuré pour les entreprises qui ne disposent pas d'un accès à Internet, également appelées *site_sombre* ou *mode_privé*. Pour en savoir plus sur, reportez-vous "Keystone en mode privé"à la section .

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 **

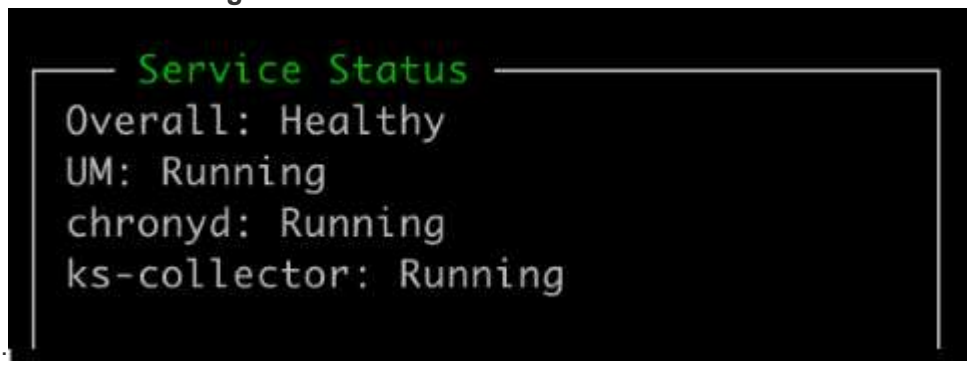
- **Collect StorageGRID usage** : cette option permet de collecter les détails d'utilisation des nœuds. Ajoutez l'adresse du nœud StorageGRID et les détails de l'utilisateur.
- **Supprimer les données privées** : cette option supprime des données privées spécifiques des clients et est activée par défaut. 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**

.



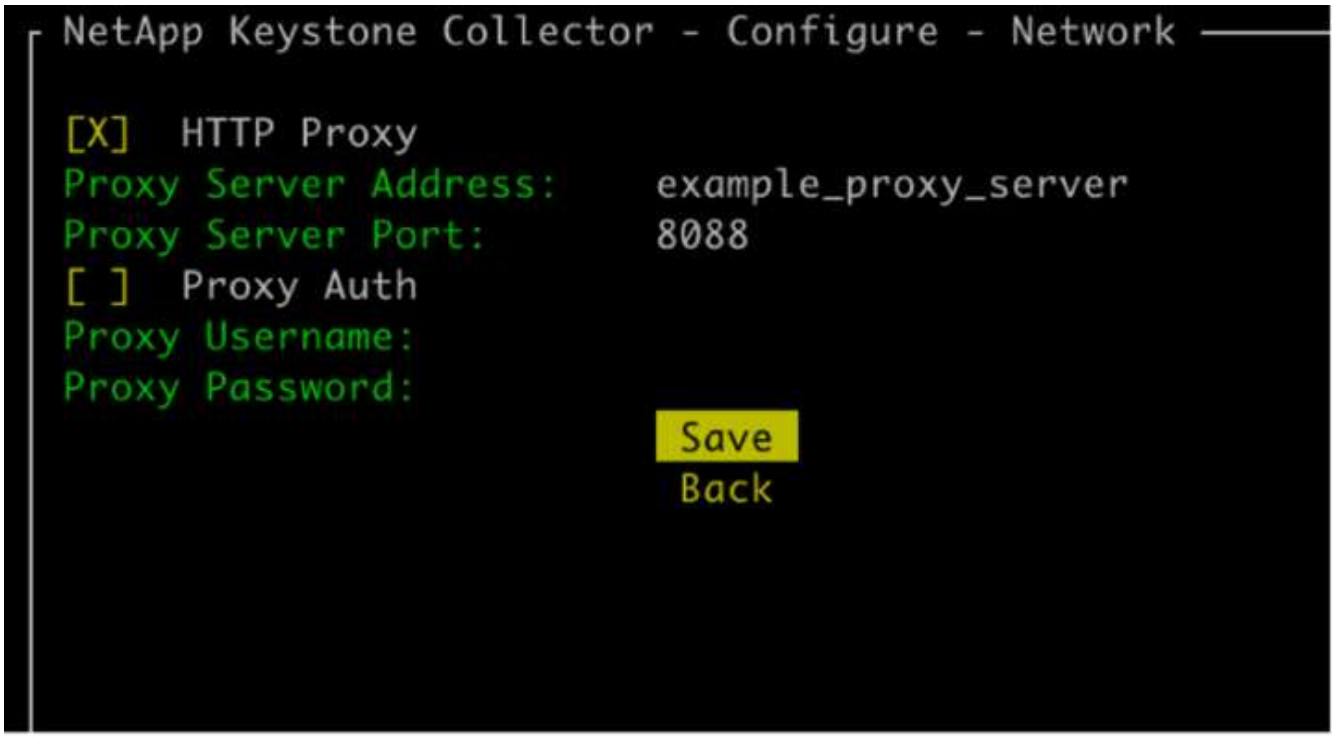
7. Quittez l'interface TUI de gestion du collecteur Keystone en sélectionnant l'option **Quitter vers Shell** sur l'écran d'accueil.

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

Keystone Collector collecte des informations limitées sur la configuration, l'état et les performances requises pour effectuer les mesures des abonnements. 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

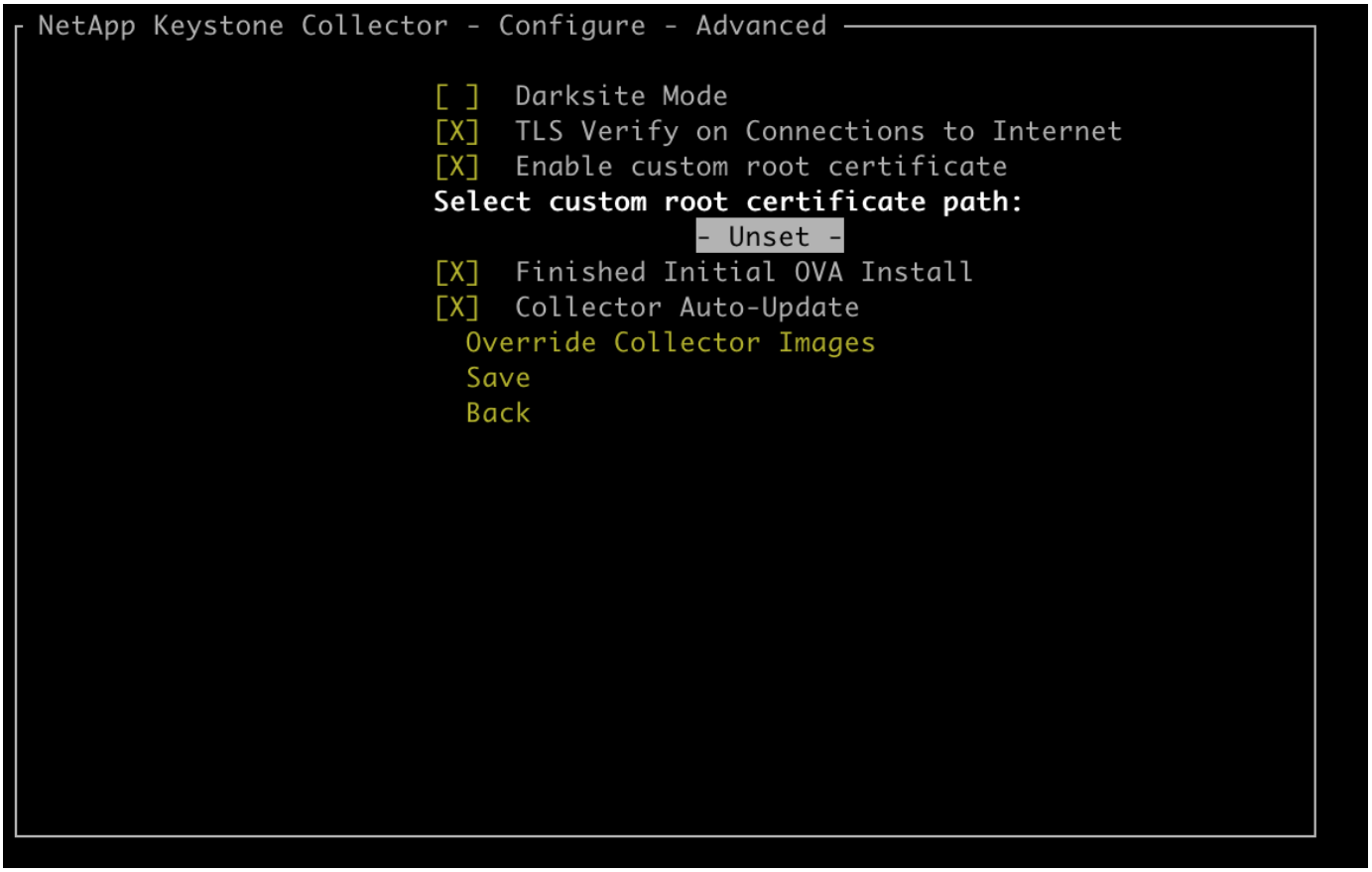
1. Préparez le certificat de l'autorité de certification. Il doit être au format de fichier X.509_ codé en _base64.

   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.

Le certificat de l'autorité de certification est copié dans `/opt/netapp/ks-collector/ca.pem` sur le serveur Keystone Collector.



Créez des niveaux de services de performance

Vous pouvez créer des niveaux de service de performance (PSL) à l'aide de l'utilitaire TUI de gestion Keystone Collector. La création de PSL via l'interface utilisateur tactile sélectionne automatiquement les valeurs par défaut définies pour chaque niveau de service de performances, réduisant ainsi le risque d'erreurs pouvant survenir lors de la définition manuelle de ces valeurs lors de la création de PSL via Active IQ Unified Manager.

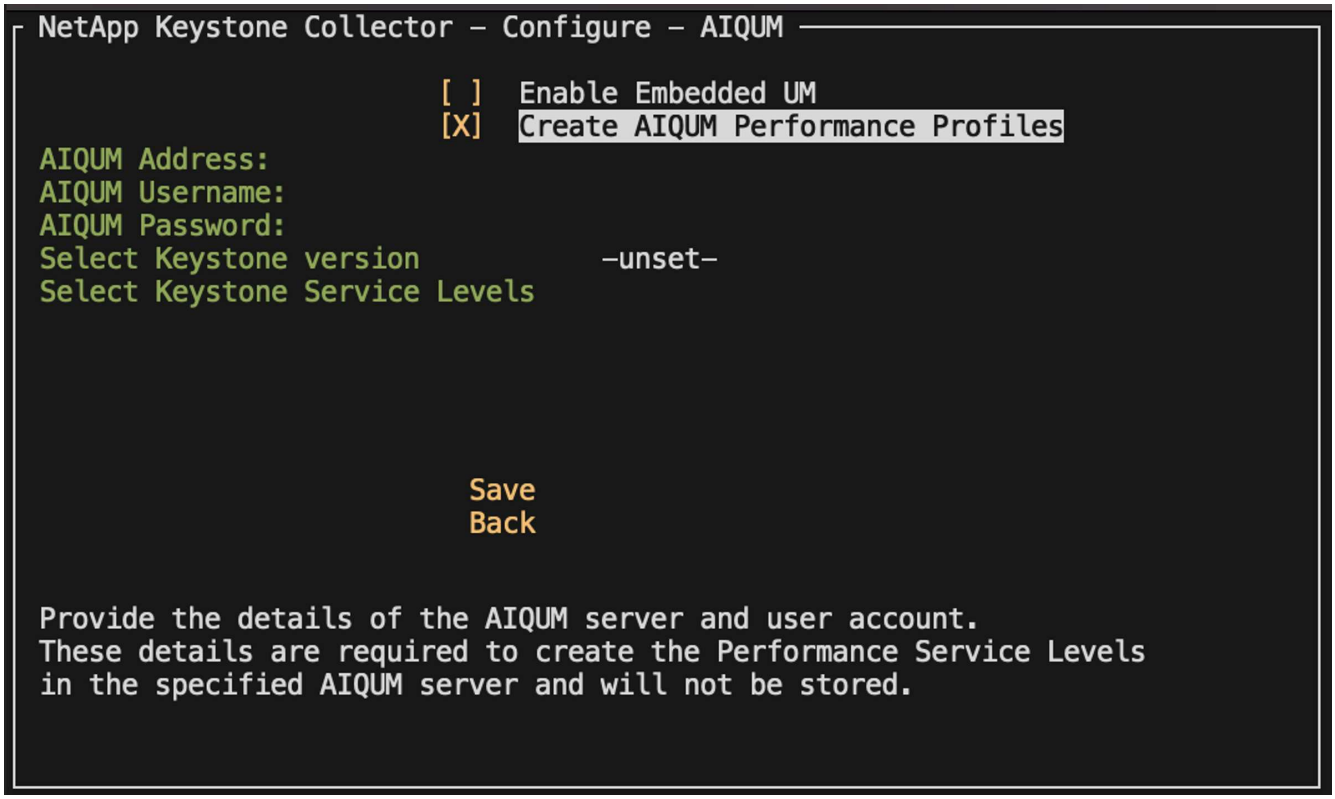
Pour en savoir plus sur les LSIPs, reportez-vous "Niveaux de services de performances"à la section .

Pour en savoir plus sur les niveaux de service, reportez-vous "Niveaux de service dans Keystone"à la section .

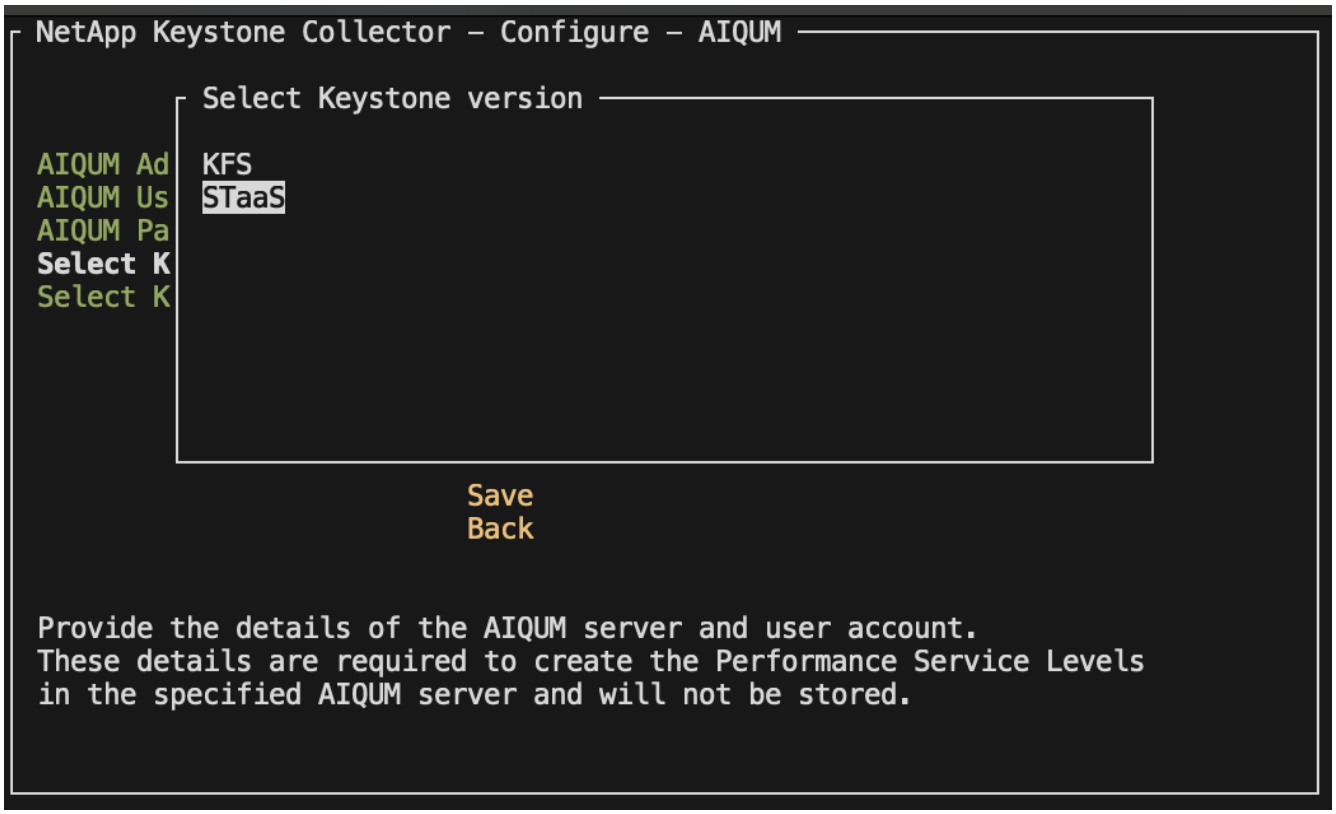
Étapes

1. Démarrez l'utilitaire TUI de gestion du collecteur Keystone :
   ```
   $ keystone-collector-tui
   ```

2. Accédez à **Configure>AIQUM** pour ouvrir l'écran AIQUM.
3. Activez l'option **Créer des profils de performances AIQUM**.
4. Entrez les détails du serveur Active IQ Unified Manager et du compte utilisateur. Ces détails sont requis pour créer des LSIPs et ne seront pas stockés.

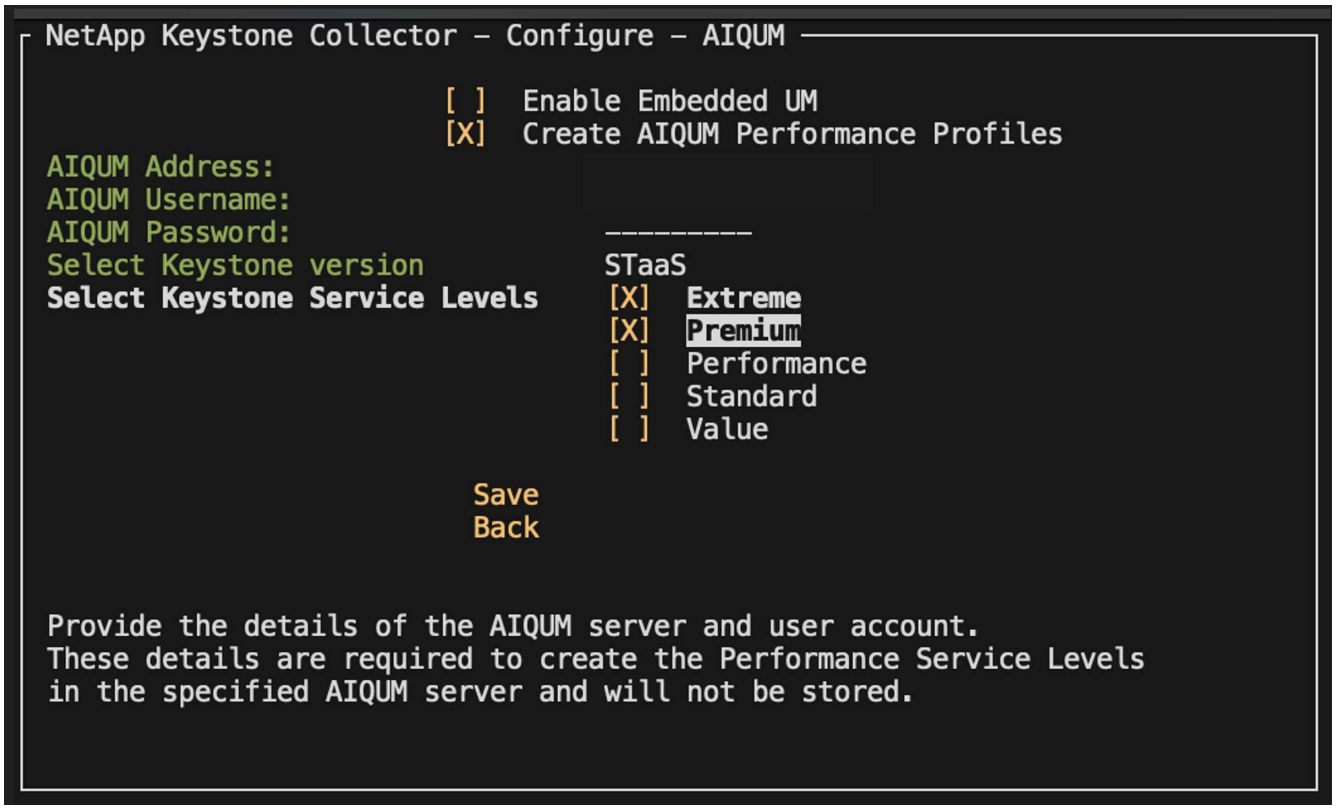


5. Pour **Sélectionner la version Keystone**, sélectionnez `-unset-`.
6. Appuyez sur entrée. Une boîte de dialogue permettant de sélectionner la version de Keystone s'affiche.
7. Mettez en surbrillance **STaaS** pour spécifier la version Keystone STaaS, puis appuyez sur entrée.



Vous pouvez mettre en évidence l'option **KFS** pour les services d'abonnement Keystone version 1. Les services d'abonnement Keystone diffèrent de Keystone STaaS en termes de niveaux de service de performance constitutifs, d'offres de services et de principes de facturation. Pour en savoir plus, consultez"Services d'abonnement Keystone | version 1" .

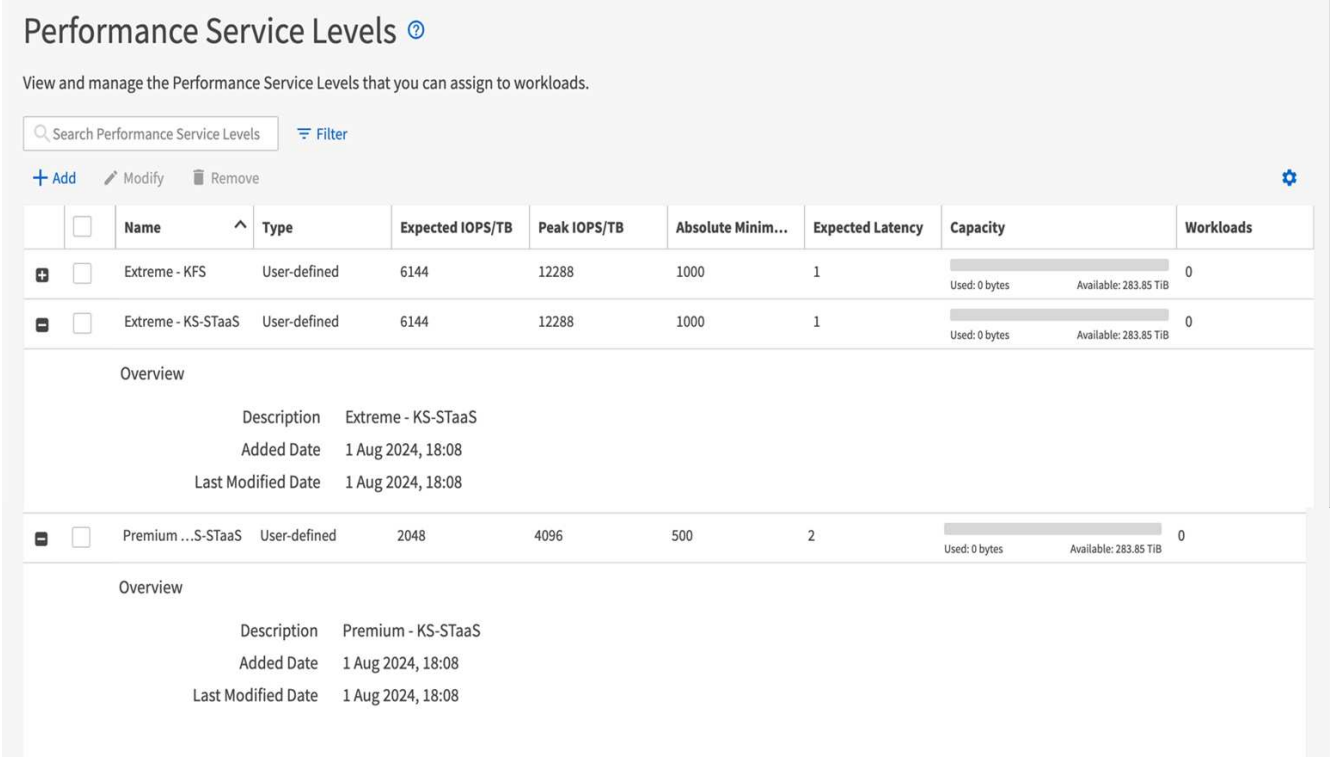
8. Tous les niveaux de service de performances Keystone pris en charge seront affichés dans l'option *Sélectionner les niveaux de service Keystone * pour la version Keystone spécifiée. Activez les niveaux de service de performances souhaités dans la liste.



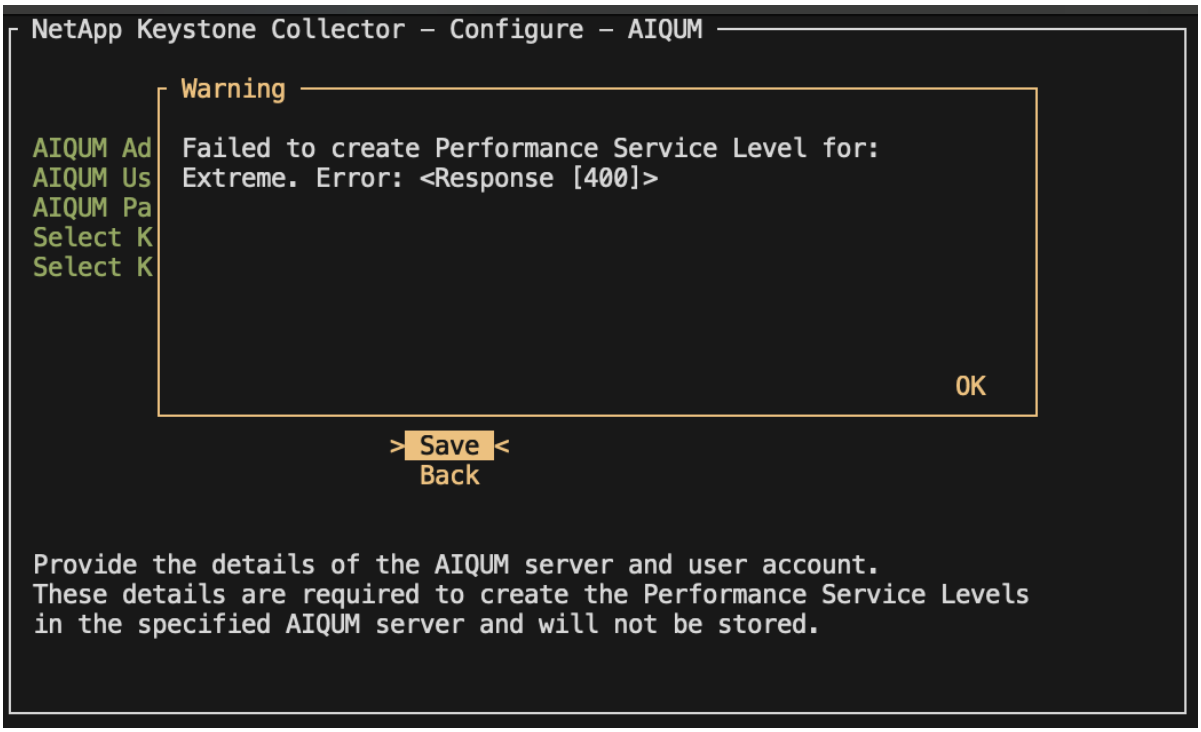
Vous pouvez sélectionner plusieurs niveaux de service de performance simultanément pour créer des PSL.

9. Sélectionnez **Enregistrer** et appuyez sur entrée. Performance des niveaux de services seront créés.

   Vous pouvez afficher les fichiers de nouvelle version créés, tels que Premium-KS-STaaS pour STaaS ou Extreme KFS pour KFS, sur la page **niveaux de services de performances** de Active IQ Unified Manager. Si les LSIPs créés ne répondent pas à vos exigences, vous pouvez modifier les LSIPs pour répondre à vos besoins. Pour en savoir plus, reportez-vous "Création et modification de niveaux de service Performance"à la section .



Si un PSL pour le niveau de service de performances sélectionné existe déjà sur le serveur Active IQ Unified Manager spécifié, vous ne pouvez pas le créer à nouveau. Si vous essayez de le faire, vous recevrez un message
d'erreur.



Installer le collecteur ITOM

Exigences d’installation pour le collecteur Keystone ITOM

Avant d’installer ITOM Collector, assurez-vous que vos systèmes sont préparés avec le logiciel nécessaire et qu’ils répondent à toutes les conditions préalables requises.

Conditions préalables pour la machine virtuelle du serveur ITOM Collector :

- Systèmes d’exploitation pris en charge :
  - Debian 12 ou version ultérieure
  - Windows Server 2016 ou version ultérieure
  - Ubuntu 20.04 LTS ou version ultérieure
  - Red Hat Enterprise Linux (RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 ou version ultérieure
  - Amazon Linux 2023 ou version ultérieure

  > Les systèmes d’exploitation recommandés sont Debian 12, Windows Server 2016 ou des versions plus récentes.

- Ressources requises : les ressources requises pour les VM basées sur le nombre de nœuds NetApp surveillés sont les suivantes :
  - 2-10 nœuds : 4 processeurs, 8 Go de RAM, 40 Go de disque
  - 12-20 nœuds : 8 processeurs, 16 Go de RAM, 40 Go de disque
- Configuration requise : assurez-vous qu’un compte en lecture seule et SNMP sont configurés sur les périphériques surveillés. Le serveur virtuel du collecteur ITOM doit également être configuré en tant qu’hôte d’interruption SNMP et serveur Syslog sur le cluster NetApp et les commutateurs de cluster, le cas échéant.

Configuration réseau requise

Les exigences de mise en réseau du collecteur ITOM sont répertoriées dans le tableau suivant.

Source	Destination	Protocole	Ports	Description
Collecteur ITOM	Adresses IP de gestion de cluster NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Surveillance des contrôleurs ONTAP
Adresses IP de gestion de nœuds et de clusters NetApp ONTAP	Collecteur ITOM	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP et Syslogs des contrôleurs
Collecteur ITOM	Commutateurs de cluster	SNMP	UDP 161	Surveillance des commutateurs
Commutateurs de cluster	Collecteur ITOM	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP et Syslogs à partir des switches
Collecteur ITOM	Adresses IP des nœuds StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Surveillance SNMP de StorageGRID

Adresses IP des nœuds StorageGRID	Collecteur ITOM	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP de StorageGRID
Collecteur ITOM	Collecteur Keystone	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Surveillance et gestion à distance du collecteur Keystone
Collecteur ITOM	DNS local	DNS	UDP 53	Services DNS publics ou privés
Collecteur ITOM	Serveur(s) NTP au choix	NTP	UDP 123	La gestion du temps

Installer Keystone ITOM Collector sur les systèmes Linux

Suivez quelques étapes pour installer ITOM Collector, qui collecte les données de métriques dans votre environnement de stockage. Vous pouvez l'installer sur des systèmes Windows ou Linux, selon vos besoins.

> L'équipe de support Keystone fournit un lien dynamique pour télécharger le fichier d'installation du collecteur ITOM, qui expire dans deux heures.

Pour installer ITOM Collector sur les systèmes Windows, reportez-vous à la "Installez le collecteur ITOM sur les systèmes Windows".

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

Avant de commencer

- Vérifiez que le shell Bourne est disponible pour le script d'installation Linux.
- Installez le `vim-common` package pour obtenir le fichier binaire **xxd** requis pour le fichier de configuration du collecteur ITOM.
- Assurez-vous que `sudo package` est installé si vous prévoyez d'exécuter le collecteur ITOM en tant qu'utilisateur non root.

Étapes

1. Téléchargez le fichier de configuration du collecteur ITOM sur votre serveur Linux.
2. Ouvrez un terminal sur le serveur et exécutez la commande suivante pour modifier les autorisations et rendre les binaires exécutables :
   `# chmod +x <installer_file_name>.bin`
3. Exécutez la commande pour démarrer le fichier de configuration du collecteur ITOM :
   `#./<installer_file_name>.bin`
4. L'exécution du fichier d'installation vous invite à :
   a. Acceptez le contrat de licence de l'utilisateur final (CLUF).
   b. Entrez les détails de l'utilisateur pour l'installation.
   c. Spécifiez le répertoire parent de l'installation.
   d. Sélectionnez la taille du collecteur.

e. Fournissez les détails de la procuration, le cas échéant.

   Pour chaque invite, une option par défaut s'affiche. Il est recommandé de sélectionner l'option par défaut sauf si vous avez des exigences spécifiques. Appuyez sur la touche **entrée** pour choisir l'option par défaut. Une fois l'installation terminée, un message confirme que le collecteur ITOM a été installé correctement.

- Le fichier de configuration du collecteur ITOM ajoute à `/etc/sudoers` pour gérer les redémarrages de service et les vidages de mémoire.
- L'installation du collecteur ITOM sur le serveur Linux crée un utilisateur par défaut appelé **ITOM** pour exécuter le collecteur ITOM sans Privileges racine. Vous pouvez choisir un autre utilisateur ou l'exécuter en tant qu'utilisateur root, mais il est recommandé d'utiliser l'utilisateur ITOM créé par le script d'installation Linux.

Et la suite ?

Une fois l'installation réussie, contactez l'équipe de support Keystone pour valider l'installation du collecteur ITOM via le portail de support ITOM. Après vérification, l'équipe de support Keystone configure le collecteur ITOM à distance, y compris la découverte et la configuration de la surveillance des périphériques, et envoie une confirmation une fois la configuration terminée. Pour toute question ou information complémentaire, contactez keystone.services@NetApp.com.

Installer Keystone ITOM Collector sur les systèmes Windows

Installez le collecteur ITOM sur un système Windows en téléchargeant le fichier de configuration du collecteur ITOM, en exécutant l'assistant InstallShield et en saisissant les informations d'identification de surveillance requises.

L'équipe de support Keystone fournit un lien dynamique pour télécharger le fichier d'installation du collecteur ITOM, qui expire dans deux heures.

Vous pouvez l'installer sur des systèmes Linux en fonction de vos besoins. Pour installer ITOM Collector sur les systèmes Linux, reportez-vous à la "Installez ITOM Collector sur les systèmes Linux".

Procédez comme suit pour installer le logiciel ITOM Collector sur votre serveur Windows :

Avant de commencer

Assurez-vous que le service collecteur ITOM est accordé **Connectez-vous en tant que service** sous Stratégie locale/attribution des droits d'utilisateur dans les paramètres de stratégie de sécurité locale du serveur Windows.

Étapes

1. Téléchargez le fichier de configuration du collecteur ITOM sur votre serveur Windows.
2. Ouvrez le fichier d'installation pour lancer l'assistant InstallShield.
3. Acceptez le contrat de licence de l'utilisateur final (CLUF). L'assistant InstallShield extrait les binaires nécessaires et vous invite à entrer les informations d'identification.
4. Saisissez les informations d'identification du compte sous lequel ITOM Collector s'exécutera :
   - Si ITOM Collector ne surveille pas d'autres serveurs Windows, utilisez un système local.
   - Si ITOM Collector surveille d'autres serveurs Windows dans le même domaine, utilisez un compte de domaine avec des autorisations d'administrateur local.

- Si ITOM Collector surveille d'autres serveurs Windows qui ne font pas partie du même domaine, utilisez un compte d'administrateur local et connectez-vous à chaque ressource avec les informations d'identification de l'administrateur local. Vous pouvez choisir de définir le mot de passe pour qu'il n'expire pas, afin de réduire les problèmes d'authentification entre le collecteur ITOM et ses ressources surveillées.

5. Sélectionnez la taille du collecteur. La taille par défaut est la taille recommandée en fonction du fichier de configuration. Poursuivez avec la taille suggérée, sauf si vous avez des exigences spécifiques.
6. Sélectionnez *Suivant* pour commencer l'installation. Vous pouvez utiliser le dossier rempli ou en choisir un autre. Une boîte de dialogue d'état affiche la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.

Et la suite ?

Une fois l'installation réussie, contactez l'équipe de support Keystone pour valider l'installation du collecteur ITOM via le portail de support ITOM. Après vérification, l'équipe de support Keystone configure le collecteur ITOM à distance, y compris la découverte et la configuration de la surveillance des périphériques, et envoie une confirmation une fois la configuration terminée. Pour toute question ou information complémentaire, contactez keystone.services@NetApp.com.

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.

    - Pour ONTAP 9.16.1 et versions ultérieures, exécutez cette commande pour modifier le contenu du journal quotidien :

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

Si le cluster est configuré en MetroCluster , exécutez la commande suivante :

```
autosupport trigger modify -node * -autosupport-message
management.log -basic-additional
wafl,performance,snapshot,object_store_server,san,raid,snapmirror,met
rocluster -troubleshooting-additional wafl
```

- Pour les versions antérieures ONTAP , 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
```

Si le cluster est configuré en MetroCluster , exécutez la commande suivante :

```
autosupport trigger modify -node * -autosupport-message management.log
-basic-additional
wafl,performance,snapshot,platform,object_store_server,san,raid,snapmirr
or,metrocluster -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".

Contrôle et mise à niveau

Surveillez l'état du collecteur Keystone

Vous pouvez contrôler l'état de santé du collecteur Keystone à l'aide de n'importe quel système de surveillance qui prend en charge les requêtes HTTP. La surveillance de l'état

permet de vérifier que les données sont disponibles dans le tableau de bord Keystone.

Par défaut, les services d'intégrité Keystone n'acceptent pas les connexions provenant d'une adresse IP autre que localhost. Le terminal de santé Keystone est `/uber/health`, Et il écoute toutes les interfaces du serveur Keystone Collector sur le port `7777`. Lors d'une requête, un code d'état de requête HTTP avec une sortie JSON est renvoyé du noeud final comme réponse, décrivant l'état du système Keystone Collector.
Le corps JSON fournit un état de santé global à `is_healthy` attribut, qui est un booléen ; et une liste détaillée des états par composant pour l' `component_details` attribut.
Voici un exemple :

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

Ces codes d'état sont renvoyés :

- **200**: indique que tous les composants surveillés sont en bonne santé
- **503**: indique qu'un ou plusieurs composants sont défectueux
- **403** : indique que le client HTTP qui demande l'état de santé ne figure pas dans la liste *Allow*, qui est une liste des CIDR réseau autorisés. Pour ce statut, aucune information d'intégrité n'est renvoyée. La liste *allow* utilise la méthode CIDR du réseau pour contrôler les périphériques réseau autorisés à interroger le système d'intégrité Keystone. Si vous recevez cette erreur, ajoutez votre système de surveillance à la liste *allow* de **Keystone Collector management TUI > configurer > Health Monitoring**.

> **Les utilisateurs Linux, notez ce problème connu :**
>
> **Description du problème** : Keystone Collector exécute un certain nombre de conteneurs dans le cadre du système de mesure de l'utilisation. Lorsque le serveur Red Hat Enterprise Linux 8.x est renforcé avec les stratégies de mise en œuvre technique de sécurité (STIG) de l'agence américaine de systèmes d'information de défense (DISA), un problème connu de fapolicyd (File Access Policy Daemon) a été constaté par intermittence. Ce problème est identifié comme "bug 1907870". **Solution de contournement** : jusqu'à sa résolution par Red Hat Enterprise, NetApp vous recommande de contourner ce problème en mettant en place `fapolicyd` en mode permissif. Dans /`etc/fapolicyd/fapolicyd.conf`, définissez la valeur de `permissive = 1`.

Afficher les journaux système

Vous pouvez afficher les journaux système Keystone Collector pour consulter les informations système et effectuer un dépannage en utilisant ces journaux. Keystone Collector utilise le système de consignation *journald* de l'hôte et les journaux système peuvent être consultés via l'utilitaire système *journalctl* standard. Vous pouvez utiliser les services clés suivants pour examiner les journaux :

- capteur ks-collector
- ks-santé
- ks-mise à jour automatique

Le service de collecte de données principal *ks-Collector* produit des journaux au format JSON avec un `run-id` attribut associé à chaque travail de collecte de données planifié. Voici un exemple de travail réussi pour la collecte de données d'utilisation standard :

```
{"level":"info","time":"2022-10-31T05:20:01.831Z","caller":"light-
collector/main.go:31","msg":"initialising light collector with run-id
cdflm0f74cgphgfon8cg","run-id":"cdflm0f74cgphgfon8cg"}
{"level":"info","time":"2022-10-
31T05:20:04.624Z","caller":"ontap/service.go:215","msg":"223 volumes
collected for cluster a2049dd4-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:18.821Z","caller":"ontap/service.go:215","msg":"697 volumes
collected for cluster 909cbacc-bfcf-11ec-8500-00505695ce60","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:41.598Z","caller":"ontap/service.go:215","msg":"7 volumes
collected for cluster f7b9a30c-55dc-11ed-9c88-005056b3d66f","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.247Z","caller":"ontap/service.go:215","msg":"24 volumes
collected for cluster a9e2dcff-ab21-11ec-8428-00a098ad3ba2","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.786Z","caller":"worker/collector.go:75","msg":"4 clusters
collected","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.839Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193648.tar.gz type=ontap to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:48.840Z","caller":"reception/reception.go:76","msg":"File bytes
123425","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}
```


Voici un exemple de travail réussi pour la collecte facultative de données de performances :

```
{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:28","msg":"initialising MySql
service at 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:55","msg":"Opening MySql db
connection at server 10.128.114.214"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sql/service.go:39","msg":"Creating MySql db
config object"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:69","msg":"initialisi
ng SLA service"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"sla_reporting/service.go:71","msg":"SLA
service successfully initialised"}

{"level":"info","time":"2022-10-
31T05:20:51.324Z","caller":"worker/collector.go:217","msg":"Performance
data would be collected for timerange: 2022-10-31T10:24:52~2022-10-
31T10:29:52"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"worker/collector.go:244","msg":"New file
generated: 65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz"}

{"level":"info","time":"2022-10-
31T05:21:31.385Z","caller":"reception/reception.go:75","msg":"Sending file
65a71542-cb4d-bdb2-e9a7-a826be4fdcb7_1667193651.tar.gz type=ontap-perf to
reception","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:31.386Z","caller":"reception/reception.go:76","msg":"File bytes
17767","run-id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-
31T05:21:33.025Z","caller":"reception/reception.go:99","msg":"uploaded
usage file to reception with status 201 Created","run-
id":"cdflm0f74cgphgfon8cg"}

{"level":"info","time":"2022-10-31T05:21:33.025Z","caller":"light-
collector/main.go:88","msg":"exiting","run-id":"cdflm0f74cgphgfon8cg"}
```

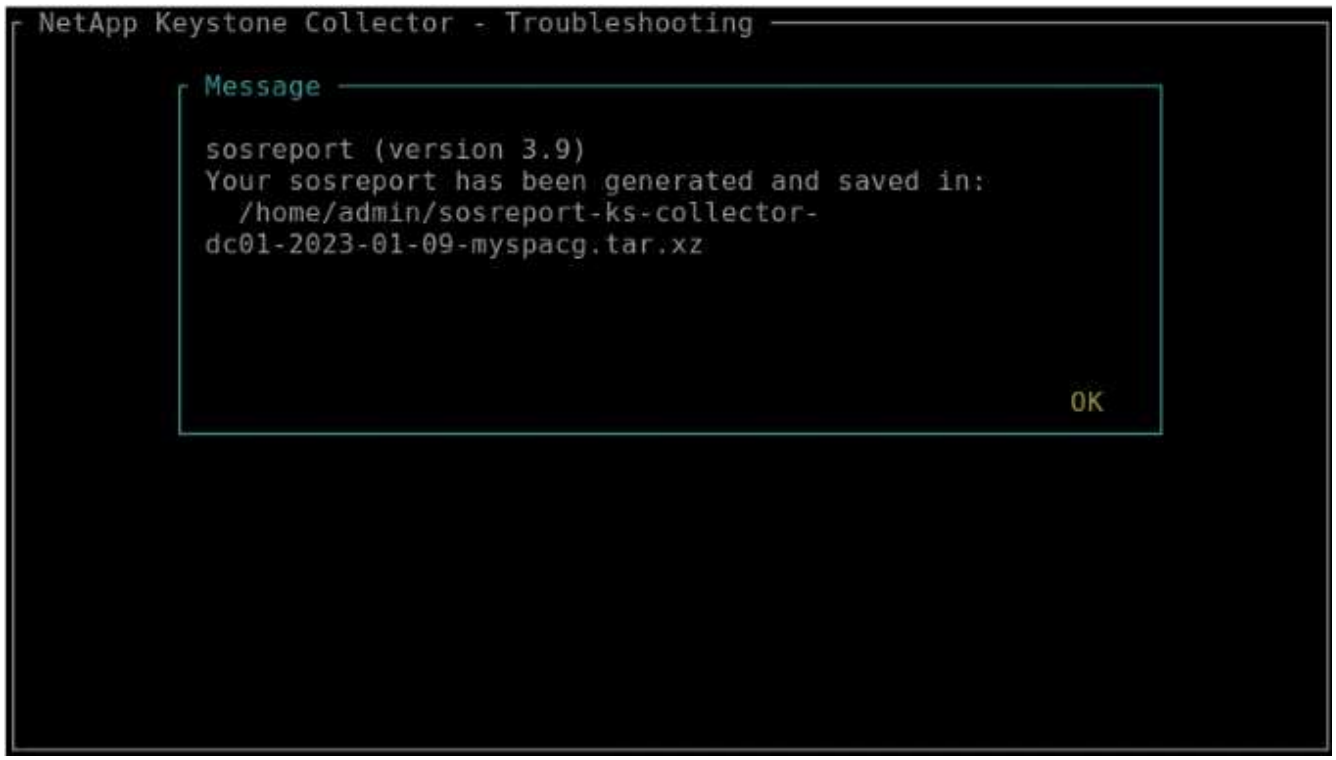
Générer et collecter des bundles de support

L'interface utilisateur du collecteur Keystone vous permet de générer des packs de support, puis d'ajouter des demandes de service pour résoudre des problèmes de support. Suivre cette procédure :

Étapes

1. Démarrez l'utilitaire TUI de gestion du collecteur Keystone :
   ```
   $ keystone-collector-tui
   ```
2. Accédez à **Troubleshooting > Generate support Bundle**
   .

3. Lorsqu'il est généré, l'emplacement où le bundle est enregistré s'affiche. Utilisez FTP, SFTP ou SCP pour vous connecter à l'emplacement et télécharger le fichier journal sur un système local.



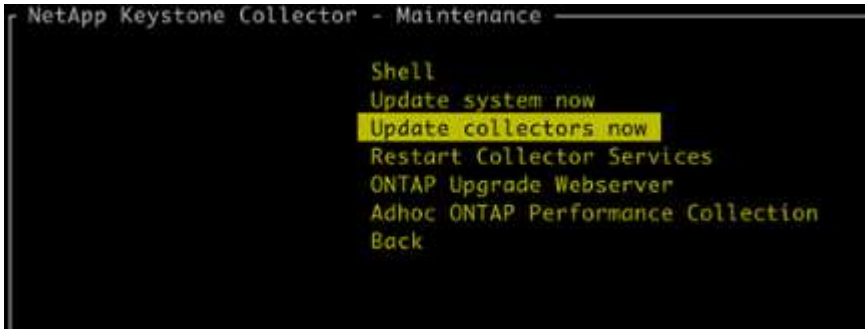
4. Une fois le fichier téléchargé, vous pouvez le joindre au ticket d'assistance Keystone ServiceNow. Pour plus d'informations sur la levée de fonds pour les billets, consultez "Génération de demandes de service".

Mettez à niveau manuellement Keystone Collector

La fonctionnalité de mise à jour automatique de Keystone Collector est activée par défaut, ce qui met automatiquement à niveau le logiciel Keystone Collector à chaque nouvelle version. Vous pouvez cependant désactiver cette fonction et mettre à niveau manuellement le logiciel.

Étapes

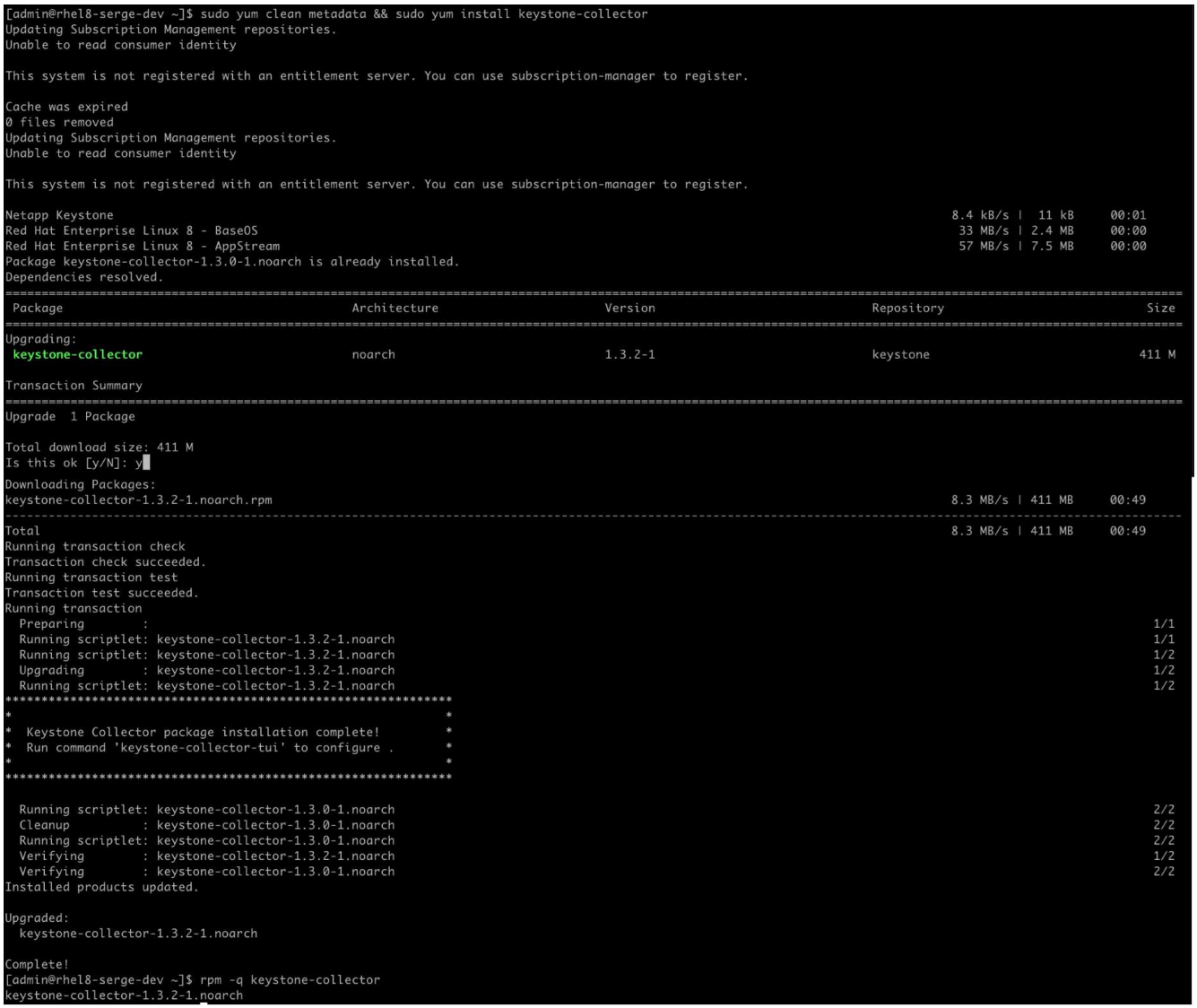
1. Démarrez l'utilitaire TUI de gestion du collecteur Keystone :
   ```
   $ keystone-collector-tui
   ```
2. Sur l'écran de maintenance, sélectionnez l'option **mettre à jour les collecteurs maintenant**.



Vous pouvez également exécuter les commandes suivantes pour mettre à niveau la version :

Pour CentOS :

```
sudo yum clean metadata && sudo yum install keystone-collector
```



Pour Debian :

```
sudo apt-get update && sudo apt-get upgrade keystone-collector
```

3. Redémarrez Keystone Collector Management TUI, vous pouvez voir la dernière version dans la partie supérieure gauche de l'écran d'accueil.

   Vous pouvez également exécuter ces commandes pour afficher la dernière version :

   Pour CentOS :

   ```
   rpm -q keystone-collector
   ```

   Pour Debian :

```
dpkg -l | grep keystone-collector
```

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 les informations de configuration, d'état et d'utilisation des abonnements Keystone ONTAP et Keystone StorageGRID , ainsi que les données de télémétrie de la machine virtuelle hébergeant Keystone Collector. Il peut collecter les données de performances pour ONTAP uniquement, si cette option est activée dans Keystone Collector.

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
    - Physique utilisé
    - Taille disponible
    - Taille
    - Taille utilisée
- 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
- MetroCluster
    - Nœud
    - Agrégat
    - Les LIF
    - Réplication de configuration
    - Relations
    - Clusters
    - Volumes
- Clusters MetroCluster
    - UUID de cluster
    - Nom du cluster
    - UUID de RemoteCluster
    - RemoteCluserName
    - LocalConfigurationState
    - Etat de configuration distant
- Nœuds MetroCluster
    - État de mise en miroir DR
    - LIF intercluster
    - Accessibilité des nœuds
    - Nœud partenaire DR
    - Nœud partenaire auxiliaire DR
    - Relation symétrique entre les nœuds DR, DR Aux et HA
    - Commutation automatique non planifiée
- Réplication de configuration MetroCluster
    - Battement de cœur à distance
    - Dernier battement de cœur envoyé
    - Dernier battement de cœur reçu
    - Flux de serveur virtuel

    - Flux de cluster
    - Stockage
    - Volume de stockage en cours d’utilisation
- Médiateurs du MetroCluster
    - Discours du médiateur
    - Port médiateur
    - Médiateur configuré
    - Médiateur joignable
    - 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
- Données au niveau du système
  - Écriture/Lecture/Autre/Total IOPS
  - Écriture/Lecture/Autre/Débit total
  - Écriture/Lecture/Autre/Latence totale
- 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

La liste suivante est un échantillon représentatif des `Availability/Uptime Data` collecté pour StorageGRID:

- Pourcentage de disponibilité du SLA

** : 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

Collecte de données de télémétrie

Données de télémétrie collectées à partir de Keystone Collector VM : En savoir plus

La liste suivante est un échantillon représentatif des données de télémétrie collectées pour les systèmes Keystone :

- Informations système
  - Nom du système d'exploitation
  - Version du système d'exploitation
  - ID du système d'exploitation
  - Nom d'hôte du système
  - Adresse IP par défaut du système
- Utilisation des ressources système
  - Temps de disponibilité du système
  - Nombre de cœurs du processeur
  - Charge du système (1 min, 5 min, 15 min)
  - Mémoire totale
  - Mémoire libre
  - Mémoire disponible
  - Mémoire partagée
  - Mémoire tampon
  - Mémoire cache
  - Échange total
  - Échange gratuit
  - Échange mis en cache
  - Nom du système de fichiers du disque
  - Taille du disque
  - Disque utilisé
  - Disque disponible
  - Pourcentage d'utilisation du disque
  - Point de montage du disque
- Paquets installés
- Configuration du collecteur
- Journaux de service
  - Journaux de service des services Keystone

Keystone en mode privé

En savoir plus sur Keystone (mode privé)

Keystone propose un mode de déploiement *privé*, également appelé *site_invisible*, pour répondre à vos exigences métier et de sécurité. Ce mode est disponible pour les organisations avec des restrictions de connectivité.

NetApp propose un déploiement spécialisé Keystone STaaS personnalisé pour les environnements avec une connectivité Internet limitée ou inexistante (ou sites invisibles). Il s'agit d'environnements sécurisés ou isolés dans lesquels les communications externes sont restreintes en raison d'exigences opérationnelles, de sécurité ou de conformité.

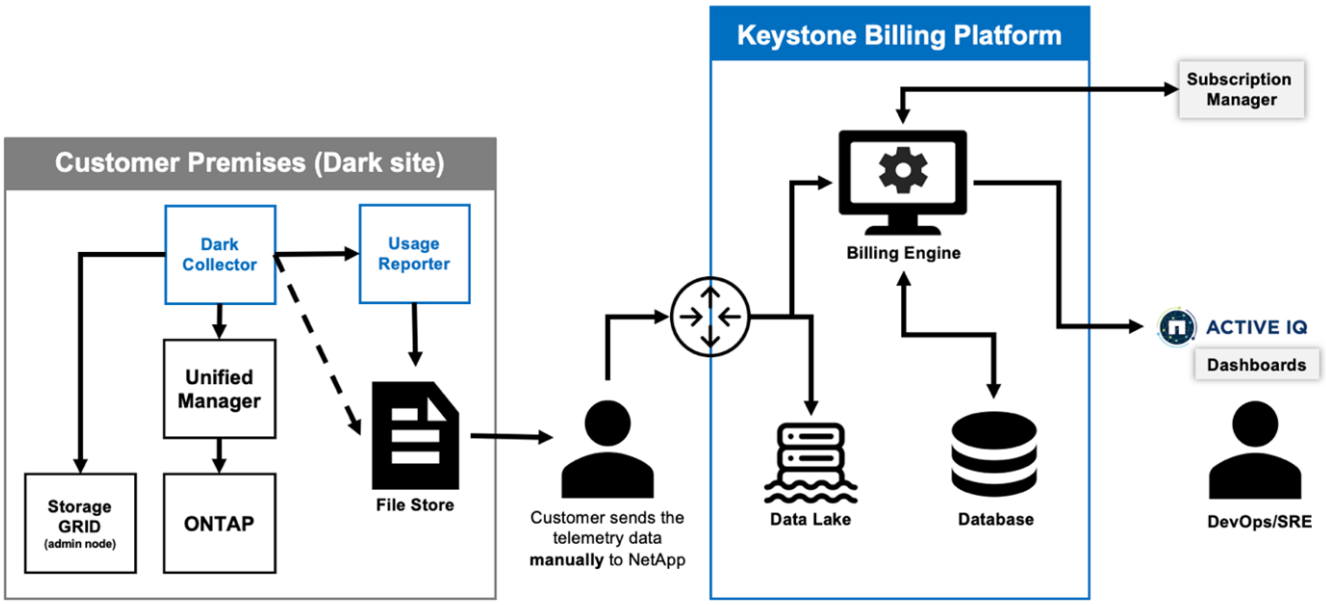
Pour NetApp Keystone, proposer des services pour les sites invisibles signifie fournir le service d'abonnement Keystone flexible au stockage en respectant les contraintes de ces environnements. Cela implique :

- **Déploiement local** : Keystone peut être configuré indépendamment au sein d'environnements isolés, ce qui évite la nécessité d'une connectivité Internet ou de personnel externe pour l'accès à la configuration.
- **Opérations hors ligne** : toutes les fonctionnalités de gestion du stockage avec vérification de l'état de santé et facturation sont disponibles hors ligne pour les opérations.
- **Sécurité et conformité** : Keystone garantit que le déploiement répond aux exigences de sécurité et de conformité des sites invisibles, qui peuvent inclure un chiffrement avancé, des contrôles d'accès sécurisés et des fonctionnalités d'audit détaillées.
- **Aide et support** : NetApp offre un support mondial 24h/24/7, 7j/7 avec un responsable de la réussite Keystone dédié assigné à chaque compte pour obtenir de l'aide et résoudre les problèmes.

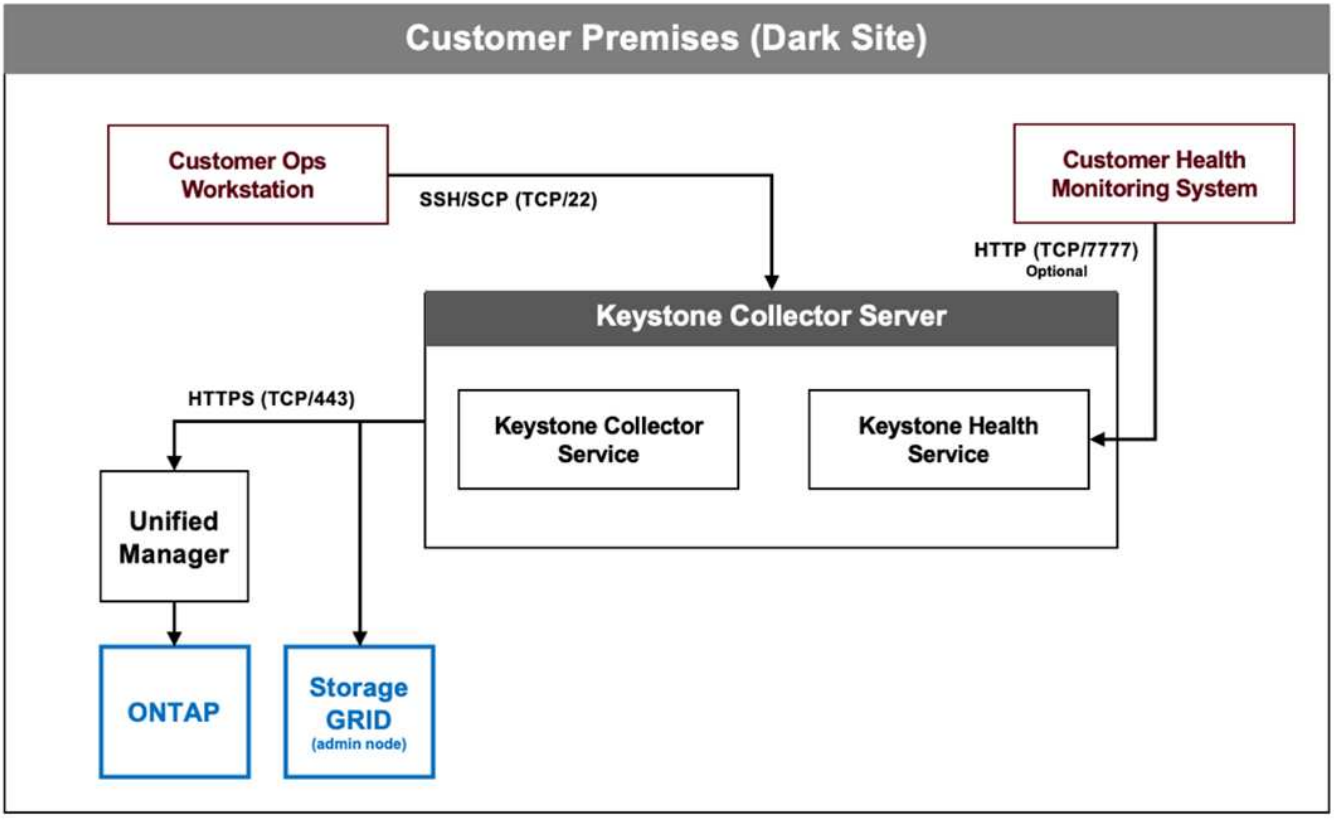
> Le collecteur Keystone peut être configuré sans restrictions de connectivité, également appelé *standard* mode. Pour en savoir plus, reportez-vous "En savoir plus sur Keystone Collector"à la section .

Collecteur Keystone en mode privé

Keystone Collector est chargé de collecter régulièrement les données d'utilisation des systèmes de stockage et d'exporter les metrics vers un rapport d'utilisation hors ligne et un magasin de fichiers local. Les fichiers générés, qui sont créés au format crypté et au format texte brut, sont ensuite transmis manuellement à NetApp par l'utilisateur après les vérifications de validation. À réception, la plateforme de facturation Keystone de NetApp authentifie et traite ces fichiers et les intègre dans les systèmes de facturation et de gestion de l'abonnement pour calculer les frais mensuels.



Le service Keystone Collector sur le serveur est chargé de collecter régulièrement les données d'utilisation, de traiter ces informations et de générer un fichier d'utilisation localement sur le serveur. Le service d'état effectue des vérifications de l'état du système et est conçu pour s'interfacer avec les systèmes de contrôle de l'état utilisés par le client. Ces rapports sont disponibles pour l'accès hors ligne par les utilisateurs, ce qui permet la validation et l'aide au dépannage des problèmes.



Préparation de l'installation du collecteur Keystone en mode privé

Avant d'installer Keystone Collector dans un environnement sans accès à Internet,

également appelé *site_sombre* ou *mode_privé*, assurez-vous que vos systèmes sont préparés avec les logiciels nécessaires et répondent à toutes les conditions requises.

Configuration requise pour VMware vSphere

- Système d'exploitation : serveur VMware vCenter et ESXi 8.0 ou version ultérieure
- Cœur : 1 processeur
- RAM : 2 GO
- Espace disque : 20 Go de vDisk

Configuration requise pour Linux

- Système d'exploitation (choisissez-en un) :
  - Red Hat Enterprise Linux (RHEL) 8.6 ou toute version ultérieure de la série 8.x
  - Red Hat Enterprise Linux 9.0 ou versions ultérieures
  - Debian 12
- Cœur : 2 processeur
- RAM : 4 GO
- Espace disque : 50 Go de vDisk
  - Au moins 2 Go disponibles dans `/var/lib/`
  - Au moins 48 Go disponibles dans `/opt/netapp`

Les modules tiers suivants doivent également être installés sur le même serveur. S'ils sont disponibles via le référentiel, ces packages seront automatiquement installés comme prérequis :

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionnlock
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionnlock
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - podman
  - sosreport

Configuration réseau requise

La configuration réseau requise pour Keystone Collector est la suivante :

- Active IQ Unified Manager (Unified Manager) 9.10 ou version ultérieure, configuré sur un serveur avec la fonctionnalité de passerelle d'API activée.
- Le serveur Unified Manager doit être accessible par le serveur Keystone Collector sur le port 443 (HTTPS).
- Un compte de service avec des autorisations utilisateur d'application doit être configuré pour le collecteur Keystone sur le serveur Unified Manager.
- Une connexion Internet externe n'est pas requise.
- Chaque mois, exportez un fichier depuis Keystone Collector et envoyez-le par e-mail à l'équipe de support NetApp . Pour plus d'informations sur la manière de contacter l'équipe d'assistance, veuillez consulter "Obtenez de l'aide avec Keystone".

Installez le collecteur Keystone en mode privé

Procédez en quelques étapes pour installer Keystone Collector dans un environnement qui ne dispose pas d'un accès à Internet, également appelé *site_sombre* ou *mode_privé*. Ce type d'installation est parfait pour vos sites sécurisés.

Vous pouvez déployer Keystone Collector sur les systèmes VMware vSphere ou l'installer sur des systèmes Linux, selon vos besoins. Suivez les étapes d'installation correspondant à l'option sélectionnée.

Déployez sur VMware vSphere

Voici la procédure à suivre :

1. Téléchargez le fichier de modèle OVA à partir de "Portail Web NetApp Keystone".
2. Pour connaître les étapes de déploiement du collecteur Keystone avec fichier OVA, reportez-vous à la section "Déploiement du modèle OVA".

Installez sous Linux

Le logiciel Keystone Collector est installé sur le serveur Linux à l'aide des fichiers .deb ou .rpm fournis, en fonction de la distribution Linux.

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

1. Téléchargez ou transférez le fichier d'installation de Keystone Collector vers le serveur Linux :

   ```
   keystone-collector-<version>.noarch.rpm
   ```

2. Ouvrez un terminal sur le serveur et exécutez les commandes suivantes pour commencer l'installation.
   - **En utilisant le paquet Debian**

     ```
     dpkg -i keystone-collector_<version>_all.deb
     ```

   - **Utilisation du fichier RPM**

     ```
     yum install keystone-collector-<version>.noarch.rpm
     ```

ou

```
rpm -i keystone-collector-<version>.noarch.rpm
```

3. Entrez `y` lorsque vous êtes invité à installer le package.

Configurez Keystone Collector en mode privé

Effectuez quelques tâches de configuration pour permettre à Keystone Collector de collecter des données d'utilisation dans un environnement qui ne dispose pas d'un accès à Internet, également connu sous le nom de *site_sombre* ou de *mode_privé*. Il s'agit d'une activité unique qui permet d'activer et d'associer les composants requis à votre environnement de stockage. Une fois configuré, Keystone Collector surveille tous les clusters ONTAP gérés par Active IQ Unified Manager.

Keystone Collector met à votre disposition 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
   ```

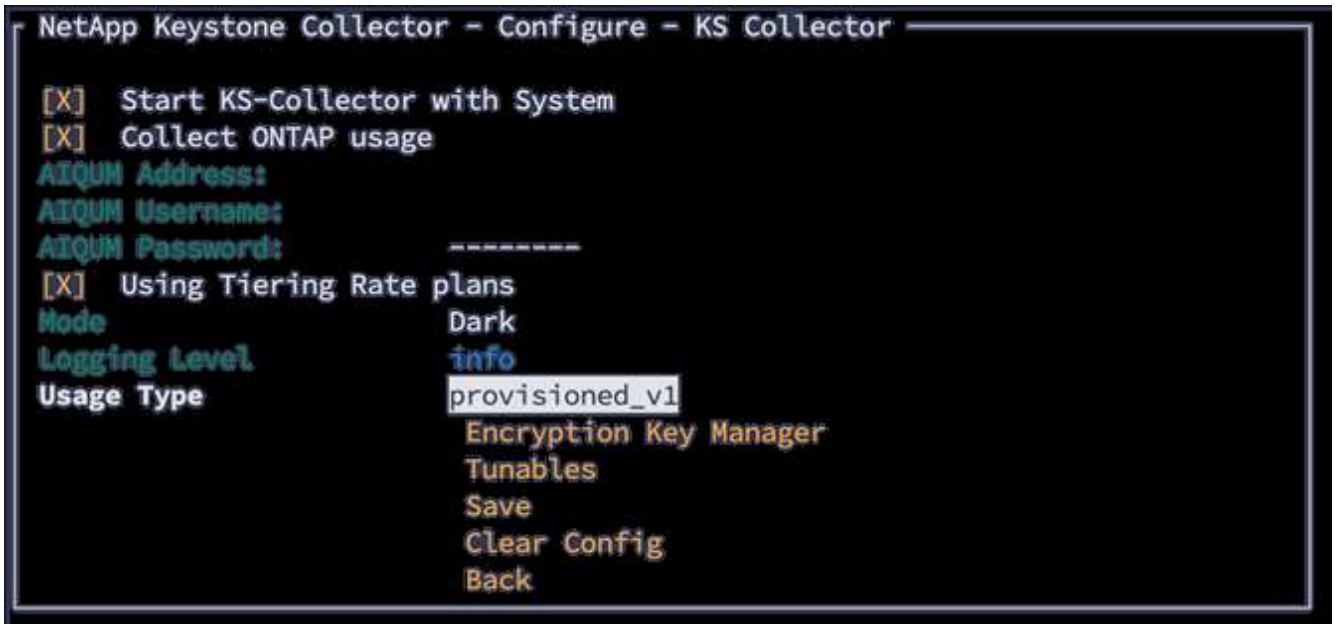
2. Accédez à **configurer > Avancé**.
3. Activez/désactivez l'option **Darksite mode**.

4. Sélectionnez **Enregistrer**.
5. Accédez à **Configure > KS-Collector** pour configurer Keystone Collector.
6. Activez/désactivez le champ **Start KS Collector with System**.
7. Activez/désactivez le champ **Collect ONTAP usage**. Ajoutez les détails du serveur Active IQ Unified Manager (Unified Manager) et du compte d'utilisateur.
8. **Facultatif** : activez le champ **utilisation des plans tarifaires de Tiering** si la hiérarchisation des données

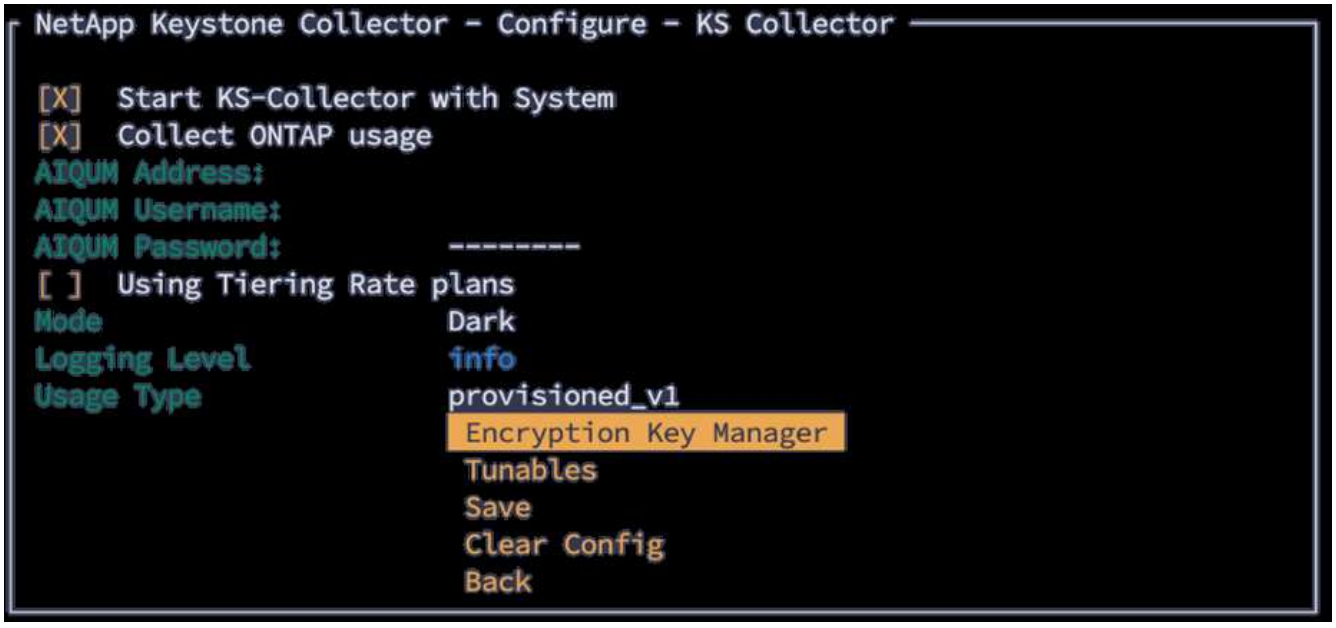
est requise pour l'abonnement.

9. En fonction du type d'abonnement acheté, mettez à jour le **Type d'utilisation**.

   Avant de configurer, confirmez le type d'utilisation associé à l'abonnement dans NetApp.

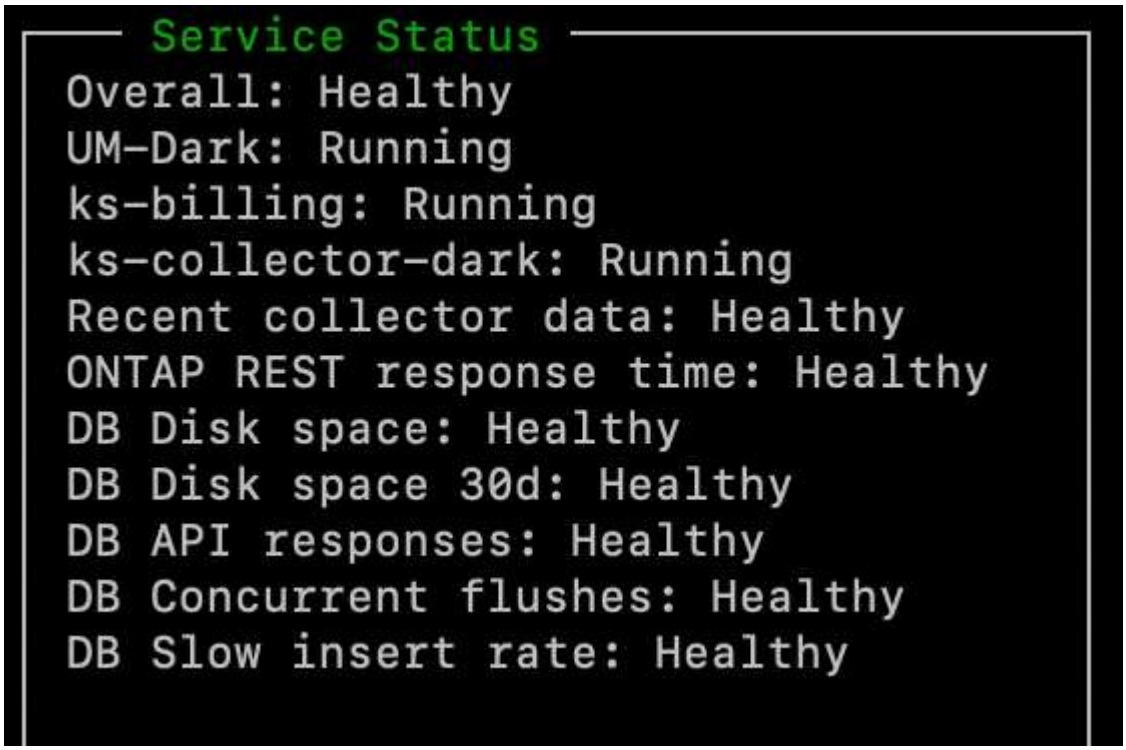


10. Sélectionnez **Enregistrer**.
11. Accédez à **Configure > KS-Collector** pour générer le Keyair du collecteur Keystone.
12. Accédez à **Encryption Key Manager** et appuyez sur entrée.



13. Sélectionnez **Generate Collector Keyair** et appuyez sur entrée.

14. Assurez-vous que le collecteur Keystone est en bon état en revenant à l'écran principal de l'interface TUI et en vérifiant les informations **Etat du service**. Le système devrait montrer que les services sont dans un état **globalement: Sain**. Patientez jusqu'à 10 minutes. Si l'état global reste défectueux après cette période, passez en revue les étapes de configuration précédentes et contactez l'équipe de support NetApp.



15. Quittez l'interface utilisateur de gestion du collecteur Keystone en sélectionnant l'option **Quitter vers Shell** sur l'écran d'accueil.
16. Récupérez la clé publique générée :

    ```
    ~/collector-public.pem
    ```

17. Envoyez un e-mail avec ce fichier à ng-keystone-secure-site-upload@netapp.com pour les sites sécurisés non USPS, ou à ng-keystone-secure-site-usps-upload@netapp.com pour les sites USPS sécurisés.

Exporter le rapport d'utilisation

Vous devez envoyer le rapport mensuel de synthèse de l'utilisation à NetApp à la fin de chaque mois. Vous pouvez générer ce rapport manuellement.

Pour générer le rapport d'utilisation, procédez comme suit :

1. Accédez à **Export usage** sur l'écran d'accueil de Keystone Collector TUI.
2. Collectez les fichiers et envoyez-les à ng-keystone-secure-site-upload@netapp.com pour les sites sécurisés non USPS, ou à ng-keystone-secure-site-usps-upload@netapp.com pour les sites USPS

sécurisés.

Keystone Collector génère à la fois un fichier clair et un fichier chiffré, qui doit être envoyé manuellement à NetApp. Le rapport Clear file contient les détails suivants qui peuvent être validés par le client.

```
node_serial,derived_service_level,usage_tib,start,duration_seconds
123456781,extreme,25.0,2024-05-27T00:00:00,86400
123456782,premium,10.0,2024-05-27T00:00:00,86400
123456783,standard,15.0,2024-05-27T00:00:00,86400

<Signature>
31b3d8eb338ee319ef1

-----BEGIN PUBLIC KEY-----
31b3d8eb338ee319ef1
-----END PUBLIC KEY-----
```

Surclassement ONTAP

Le collecteur Keystone prend en charge les mises à niveau ONTAP via l'interface TUI.

Pour mettre à niveau ONTAP, procédez comme suit :

1. Accédez à **Maintenance > mise à niveau du serveur Web ONTAP**.
2. Copiez le fichier image de mise à niveau ONTAP dans **/opt/NetApp/ONTAP-upgrade/**, puis sélectionnez **Démarrer le serveur Web** pour démarrer le serveur Web.

3. Accédez à `http://<collector-ip>:8000` utilisation d'un navigateur Web pour obtenir de l'aide sur la mise à niveau.

Redémarrez le collecteur Keystone

Vous pouvez redémarrer le service Keystone Collector via l'interface TUI. Accédez à **Maintenance >**

redémarrer les services Collector dans l'interface utilisateur. Tous les services du collecteur seront redémarrés et leur état peut être surveillé à partir de l'écran d'accueil de l'interface utilisateur.

Surveillance de l'état du collecteur Keystone en mode privé

Vous pouvez contrôler l'état de santé du collecteur Keystone à l'aide de n'importe quel système de surveillance qui prend en charge les requêtes HTTP.

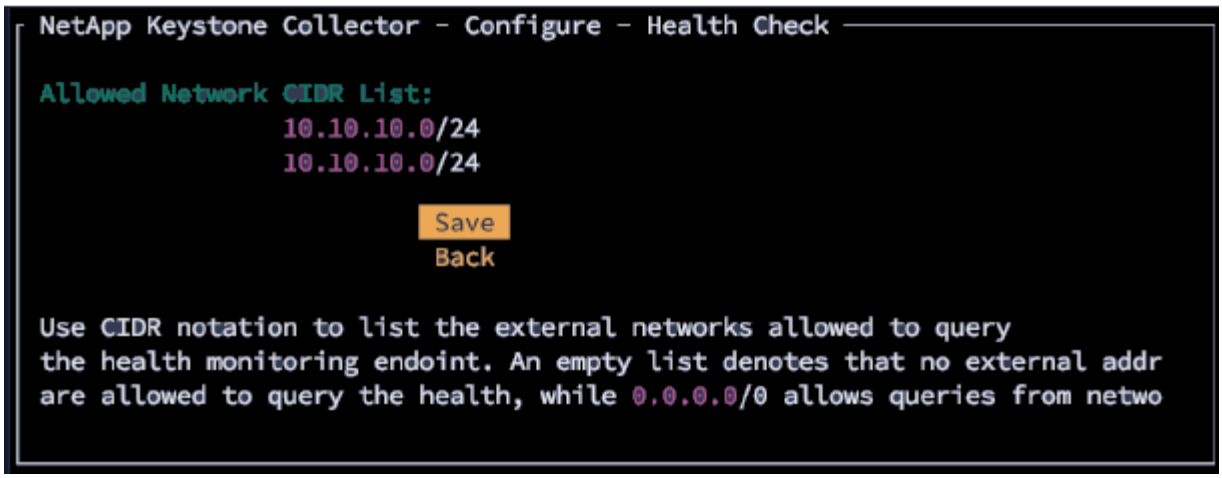
Par défaut, les services d'intégrité Keystone n'acceptent pas les connexions provenant d'une adresse IP autre que localhost. Le terminal de santé Keystone est `/uber/health`, Et il écoute toutes les interfaces du serveur Keystone Collector sur le port `7777`. Lors d'une requête, un code d'état de requête HTTP avec une sortie JSON est renvoyé du noeud final comme réponse, décrivant l'état du système Keystone Collector.
Le corps JSON fournit un état de santé global à `is_healthy` attribut, qui est un booléen ; et une liste détaillée des états par composant pour l' `component_details` attribut.
Voici un exemple :

```
$ curl http://127.0.0.1:7777/uber/health
{"is_healthy": true, "component_details": {"vicmet": "Running", "ks-
collector": "Running", "ks-billing": "Running", "chronyd": "Running"}}
```

Ces codes d'état sont renvoyés :

- **200**: indique que tous les composants surveillés sont en bonne santé
- **503**: indique qu'un ou plusieurs composants sont défectueux
- **403** : indique que le client HTTP qui demande l'état de santé ne figure pas dans la liste *Allow*, qui est une liste des CIDR réseau autorisés. Pour ce statut, aucune information d'intégrité n'est renvoyée.

  La liste *allow* utilise la méthode CIDR du réseau pour contrôler les périphériques réseau autorisés à interroger le système d'intégrité Keystone. Si vous recevez l'erreur 403, ajoutez votre système de surveillance à la liste *allow* depuis **Keystone Collector Management TUI > Configure > Health Monitoring**.

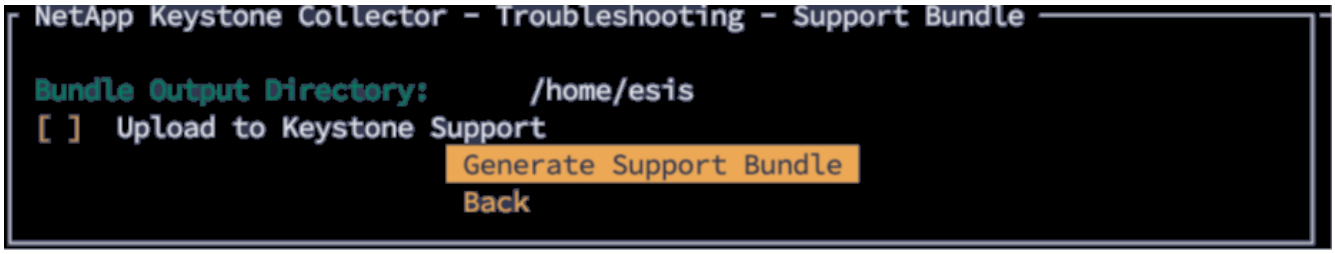


Générer et collecter des bundles de support

Pour résoudre les problèmes avec le collecteur Keystone, vous pouvez faire appel au support NetApp qui peut demander un fichier *.tar*. Vous pouvez générer ce fichier via l'utilitaire TUI de gestion du collecteur Keystone.

Pour générer un fichier *.tar*, procédez comme suit :

1. Accédez à **Troubleshooting > Generate support Bundle**.
2. Sélectionnez l'emplacement d'enregistrement du bundle, puis cliquez sur **générer le bundle de support**.



   Ce processus crée un `tar` package à l'emplacement mentionné qui peut être partagé avec NetApp pour résoudre les problèmes.

3. Une fois le fichier téléchargé, vous pouvez le joindre au ticket d'assistance Keystone ServiceNow. Pour plus d'informations sur la levée de fonds pour les billets, consultez "Génération de demandes de service".