Installer et configurer Keystone

Keystone

NetApp
January 15, 2026

Sommaire

Installer et configurer Keystone

Exigences

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
- Noyau : 1 CPU
- RAM : 2 Go de RAM
- Espace disque : 20 Go vDisk

Autres exigences

Assurez-vous que les exigences génériques suivantes sont respectées :

Exigences de mise en réseau

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

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

Source	Destination	Service	Protocole et ports	Catégorie	But
Collecteur Keystone (pour Keystone ONTAP)	Active IQ Unified Manager (Gestionnaire unifié)	HTTPS	TCP 443	Obligatoire (si vous utilisez Keystone ONTAP)	Collecte des mesures d'utilisation de Keystone Collector pour ONTAP
Collecteur Keystone (pour Keystone StorageGRID)	Nœuds d'administration StorageGRID	HTTPS	TCP 443	Obligatoire (si vous utilisez Keystone StorageGRID)	Collecte des métriques d'utilisation de Keystone Collector pour StorageGRID

Keystone Collector (générique)	Internet (conformément aux exigences d'URL données ultérieurement)	HTTPS	TCP 443	Obligatoire (connexion Internet)	Logiciel Keystone Collector, mises à jour du système d'exploitation et téléchargement des métriques
Keystone Collector (générique)	Proxy HTTP client	Proxy HTTP	Port proxy client	Obligatoire (connexion Internet)	Logiciel Keystone Collector, mises à jour du système d'exploitation et téléchargement des métriques
Keystone Collector (générique)	Serveurs DNS clients	DNS	TCP/UDP 53	Obligatoire	résolution DNS
Keystone Collector (générique)	Serveurs NTP clients	NTP	UDP 123	Obligatoire	Synchronisation horaire
Collecteur Keystone (pour Keystone ONTAP)	Gestionnaire unifié	MYSQL	TCP 3306	Fonctionnalités optionnelles	Collecte de mesures de performance pour Keystone Collector
Keystone Collector (générique)	Système de surveillance des clients	HTTPS	TCP 7777	Fonctionnalités optionnelles	Rapports sur l'état de santé du collecteur Keystone
Postes de travail des opérations du client	Collectionneur de Keystone	SSH	TCP 22	Gestion	Accès à la gestion du collecteur Keystone
Adresses de gestion des clusters et des nœuds NetApp ONTAP	Collectionneur de Keystone	HTTP_8000, PING	TCP 8000, demande/réponse d'écho ICMP	Fonctionnalités optionnelles	Serveur Web pour les mises à jour du firmware ONTAP

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

Accès URL

Keystone Collector a besoin d'accéder aux hôtes Internet suivants :

Adresse	Raison
https://keystone.netapp.com	Mises à jour du logiciel Keystone Collector et rapports d'utilisation
https://support.netapp.com	Siège social de NetApp pour les informations de 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 machine virtuelle Linux et votre serveur Keystone Collector disposent de ces configurations.

Serveur Linux :

- Système d'exploitation : l'un des éléments 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)
- Heure Chronyd synchronisée
- Accès aux référentiels de logiciels Linux standard

Le même serveur doit également disposer des packages tiers suivants :

- podman (gestionnaire POD)
- sos
- chronie
- Python 3 (3.9.14 à 3.11.8)

Serveur Keystone Collector VM :

- Noyau : 2 processeurs
- RAM : 4 Go de RAM
- Espace disque : 50 Go vDisk

Autres exigences

Assurez-vous que les exigences génériques suivantes sont respectées :

Exigences de mise en réseau

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

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

Source	Destination	Service	Protocole et ports	Catégorie	But
Collecteur Keystone (pour Keystone ONTAP)	Active IQ Unified Manager (Gestionnaire unifié)	HTTPS	TCP 443	Obligatoire (si vous utilisez Keystone ONTAP)	Collecte des mesures d'utilisation de Keystone Collector pour ONTAP
Collecteur Keystone (pour Keystone StorageGRID)	Nœuds d'administration StorageGRID	HTTPS	TCP 443	Obligatoire (si vous utilisez Keystone StorageGRID)	Collecte des métriques d'utilisation de Keystone Collector pour StorageGRID
Keystone Collector (générique)	Internet (conformément aux exigences d'URL données ultérieurement)	HTTPS	TCP 443	Obligatoire (connexion Internet)	Logiciel Keystone Collector, mises à jour du système d'exploitation et téléchargement des métriques
Keystone Collector (générique)	Proxy HTTP client	Proxy HTTP	Port proxy client	Obligatoire (connexion Internet)	Logiciel Keystone Collector, mises à jour du système d'exploitation et téléchargement des métriques
Keystone Collector (générique)	Serveurs DNS clients	DNS	TCP/UDP 53	Obligatoire	résolution DNS

Keystone Collector (générique)	Serveurs NTP clients	NTP	UDP 123	Obligatoire	Synchronisation horaire
Collecteur Keystone (pour Keystone ONTAP)	Gestionnaire unifié	MYSQL	TCP 3306	Fonctionnalités optionnelles	Collecte de mesures de performance pour Keystone Collector
Keystone Collector (générique)	Système de surveillance des clients	HTTPS	TCP 7777	Fonctionnalités optionnelles	Rapports sur l'état de santé du collecteur Keystone
Postes de travail des opérations du client	Collectionneur de Keystone	SSH	TCP 22	Gestion	Accès à la gestion du collecteur Keystone
Adresses de gestion des clusters et des nœuds NetApp ONTAP	Collectionneur de Keystone	HTTP_8000, PING	TCP 8000, demande/réponse d'écho ICMP	Fonctionnalités optionnelles	Serveur Web pour les mises à jour du firmware ONTAP

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

Accès URL

Keystone Collector a besoin d'accéder aux hôtes Internet suivants :

Adresse	Raison
https://keystone.netapp.com	Mises à jour du logiciel Keystone Collector et rapports d'utilisation
https://support.netapp.com	Siège social de NetApp pour les informations de 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 du logiciel

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

Avant de commencer

Répondez aux exigences suivantes si vous avez l'intention de collecter des données d'utilisation uniquement via ONTAP:

1. Assurez-vous que ONTAP 9.8 ou une version ultérieure est configuré. Pour plus d'informations sur la configuration d'un nouveau cluster, consultez ces liens :
   - "Configurer ONTAP sur un nouveau cluster avec System Manager"
   - "Configurer un cluster avec la CLI"
2. Créez des comptes de connexion ONTAP avec des rôles spécifiques. Pour en savoir plus, consultez "En savoir plus sur la création de comptes de connexion ONTAP" .
   - **Interface Web**
     i. Connectez-vous à ONTAP System Manager à l'aide de vos informations d'identification par défaut. Pour en savoir plus, consultez "Gestion des clusters avec System Manager" .
     ii. Créez un utilisateur ONTAP avec le rôle « lecture seule » et le type d'application « http » et activez l'authentification par mot de passe en accédant à **Cluster > Paramètres > Sécurité > Utilisateurs**.
   - **CLI**
     i. Connectez-vous à ONTAP CLI en utilisant vos informations d'identification par défaut. Pour en savoir plus, consultez "Gestion des clusters avec CLI" .
     ii. Créez un utilisateur ONTAP avec le rôle « lecture seule » et le type d'application « http » et activez l'authentification par mot de passe. Pour en savoir plus sur l'authentification, reportez-vous à "Activer l'accès par mot de passe au compte ONTAP" .

Répondez aux exigences suivantes si vous avez l'intention de collecter des données d'utilisation via Active IQ Unified Manager:

1. Assurez-vous que Unified Manager 9.10 ou une version ultérieure est configuré. Pour plus d'informations sur l'installation d'Unified Manager, consultez ces liens :
   - "Installation d'Unified Manager sur les systèmes VMware vSphere"
   - "Installation d'Unified Manager sur les systèmes Linux"
2. Assurez-vous que le cluster ONTAP a été ajouté à Unified Manager. Pour plus d'informations sur l'ajout de clusters, voir "Ajout de clusters" .
3. Créez des utilisateurs Unified Manager avec des rôles spécifiques pour la collecte de données d'utilisation et de performances. Effectuez ces étapes. Pour plus d'informations sur les rôles d'utilisateur, voir "Définitions des rôles d'utilisateur" .
   a. Connectez-vous à l'interface Web d'Unified Manager avec les informations d'identification de l'administrateur d'application par défaut générées lors de l'installation. Voir "Accéder à l'interface Web d'Unified Manager" .
   b. Créez un compte de service pour Keystone Collector avec `Operator` rôle d'utilisateur. Les API du service Keystone Collector utilisent ce compte de service pour communiquer avec Unified

Manager et collecter des 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 de données de performances. Voir "Création d'un utilisateur de base de données" .

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

4. Activer la passerelle API dans Unified Manager. Keystone Collector utilise la fonctionnalité API Gateway pour communiquer avec les clusters ONTAP . Vous pouvez activer API Gateway soit à partir de l'interface utilisateur Web, soit en exécutant quelques commandes via Unified Manager CLI.

   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, voir "Activation de la passerelle API" .

   CLI

   Pour activer la passerelle API via Unified Manager CLI, procédez comme suit :

   a. Sur le serveur Unified Manager, démarrez une session SSH et connectez-vous à l'interface de ligne de commande Unified Manager.
   `um cli login -u <umadmin>` Pour plus d'informations sur les commandes CLI, voir "Commandes CLI Unified Manager prises en charge" .

   b. Vérifiez si API Gateway est déjà activé.
   `um option list api.gateway.enabled` UN `true` la valeur indique que la passerelle API est activée.

   c. Si la valeur renvoyée est `false` , exécutez cette commande :
   `um option set api.gateway.enabled=true`

   d. Redémarrez le serveur Unified Manager :

   - Linux: "Redémarrage d'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, consultez"Mise à niveau du logiciel StorageGRID : Présentation" .
- Un compte utilisateur administrateur 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 de nœud administrateur.

  Étapes

  a. Connectez-vous au gestionnaire de grille. Voir "Sign in au gestionnaire de grille" .

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

groupe d'administrateurs" .

c. Ajoutez les autorisations suivantes :
   - Comptes locataires
   - Entretien
   - Requête de métriques

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

Installer Keystone Collector

Déployer Keystone Collector sur les systèmes VMware vSphere

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

Déploiement du modèle OVA

Suivez ces étapes :

Étapes

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

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

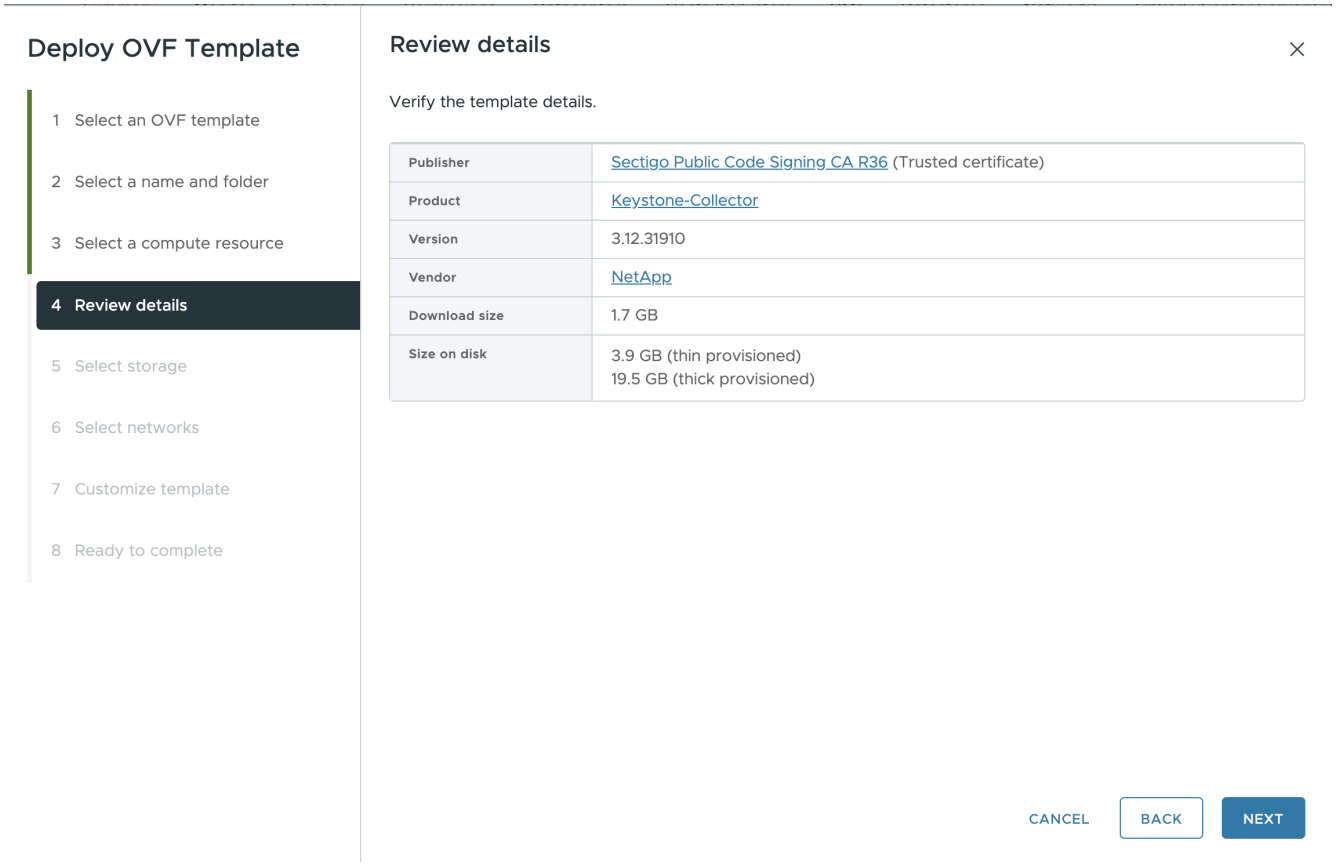
   a. Téléchargez le certificat d'autorité de certification de signature de code depuis Sectigo "ici".

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

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

   Lorsque l'intégrité et l'authenticité de l'OVA Keystone Collector sont validées, vous pouvez voir le texte

`(Trusted certificate)` avec l'éditeur.



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

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

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

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

Configuration initiale du système

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

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

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

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

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

Installer Keystone Collector sur les systèmes Linux

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

Utilisation de RPM

1. Connectez-vous en SSH au serveur Keystone Collector et élevez-vous à `root` privilège.
2. Importer la signature publique de Keystone :
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. Assurez-vous que le certificat public correct a été importé en vérifiant l'empreinte numérique de Keystone Billing Platform dans la base de données RPM :
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint`
   L'empreinte digitale correcte ressemble à ceci :
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Téléchargez le `keystonerepo.rpm` déposer:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Vérifiez l'authenticité du fichier :
   `rpm --checksig -v keystonerepo.rpm` La signature d'un fichier authentique ressemble à ceci :
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. Installez le fichier du référentiel logiciel YUM :
   `# yum install keystonerepo.rpm`
7. Une fois le dépôt Keystone installé, installez le package keystone-collector via le gestionnaire de packages YUM :

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

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

Utiliser Debian

1. Connectez-vous en SSH au serveur Keystone Collector et élevez-vous à `root` privilège.
   `sudo su`
2. Téléchargez le `keystone-sw-repo.deb` déposer:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Installez le fichier de référentiel de logiciels Keystone :
   `# dpkg -i keystone-sw-repo.deb`
4. Mettre à jour la liste des packages :
   `# apt-get update`
5. Une fois le dépôt Keystone installé, installez le package keystone-collector :
   `# apt-get install keystone-collector`

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

Validation automatique du logiciel Keystone

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

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

Configurer Keystone Collector

Vous devez effectuer quelques tâches de configuration pour permettre à Keystone Collector de collecter les données d'utilisation dans votre environnement de stockage. Il s'agit d'une activité ponctuelle visant à activer et à associer les composants requis à votre environnement de stockage.

- Keystone Collector vous fournit l'utilitaire d'interface utilisateur du terminal de gestion Keystone Collector (TUI) pour effectuer des activités de configuration et de surveillance. Vous pouvez utiliser différentes commandes du clavier, telles que les touches Entrée et fléchées, pour sélectionner les options et naviguer dans cette interface utilisateur graphique.
- Keystone Collector peut être configuré pour les organisations qui n'ont pas accès à Internet, également connu sous le nom de *site sombre* ou *mode privé*. Pour en savoir plus, reportez-vous à"Keystone en mode privé" .

Étapes

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

   Pour ONTAP

   - *Collecter l'utilisation ONTAP * : 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 de données de performances pour ONTAP. Ceci est désactivé par défaut. Activez cette option si une surveillance des performances est requise dans votre environnement à des fins de SLA. Fournissez les détails du compte utilisateur de la base de données Unified Manager. Pour plus d'informations sur la création d'utilisateurs de base de données, voir"Créer des utilisateurs Unified Manager" .
   - **Supprimer les données privées** : cette option supprime les 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, consultez"Limiter la collecte de données privées" .

Pour StorageGRID

- *Collecter l'utilisation de StorageGRID * : 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 les 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, consultez"Limiter la collecte de données privées" .

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

.

6. Assurez-vous que Keystone Collector est en bon état en revenant à l'écran principal de l'interface utilisateur et en vérifiant les informations **État du service**. Le système doit indiquer que les services sont dans un état **Globalement : sain**

.

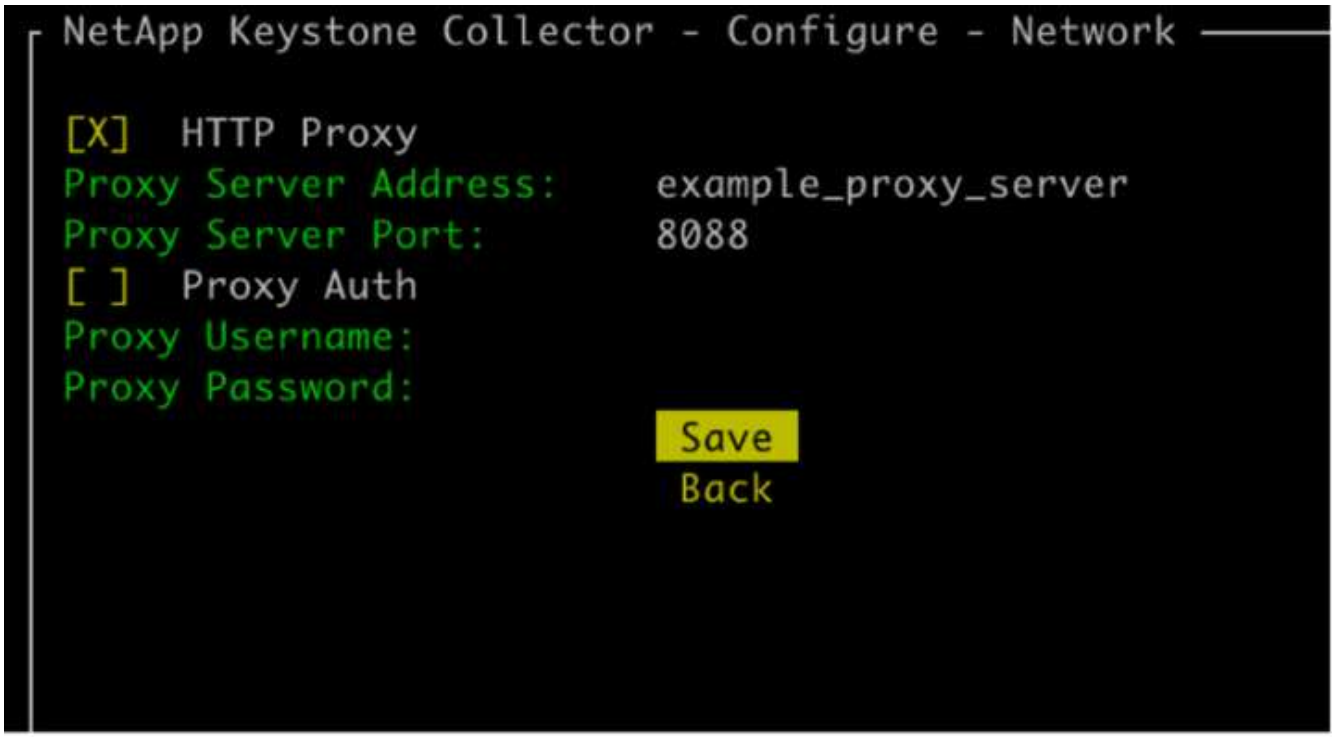
7. Quittez l'interface utilisateur de gestion de Keystone Collector en sélectionnant l'option **Quitter vers Shell** sur l'écran d'accueil.

Configurer le proxy HTTP sur Keystone Collector

Le logiciel Collector prend en charge l'utilisation d'un proxy HTTP pour communiquer avec Internet. Cela peut être configuré dans l'interface utilisateur.

Étapes

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



Limiter la collecte de données privées

Keystone Collector collecte des informations limitées sur la configuration, l'état et les performances nécessaires pour effectuer la mesure des abonnements. Il existe une option permettant de limiter davantage les informations collectées en masquant les informations sensibles du contenu téléchargé. Cela n'a pas d'impact sur le calcul de la facturation. Toutefois, la limitation des informations peut avoir un impact sur la facilité d'utilisation des informations de rapport, car certains éléments, qui peuvent être facilement identifiés 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 TUI de Keystone Collector. Cette option, **Supprimer les données privées**, est activée par défaut.

Pour plus d'informations sur les éléments supprimés concernant la limitation de l'accès aux données privées dans ONTAP et StorageGRID, consultez"Liste des éléments supprimés concernant la limitation de l'accès aux données privées" .

Faire confiance à une autorité de certification racine personnalisée

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

Si vous utilisez l'inspection SSL/TLS dans le pare-feu de votre système, le trafic Internet est à nouveau chiffré avec votre certificat CA 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. Suivez ces étapes :

Étapes

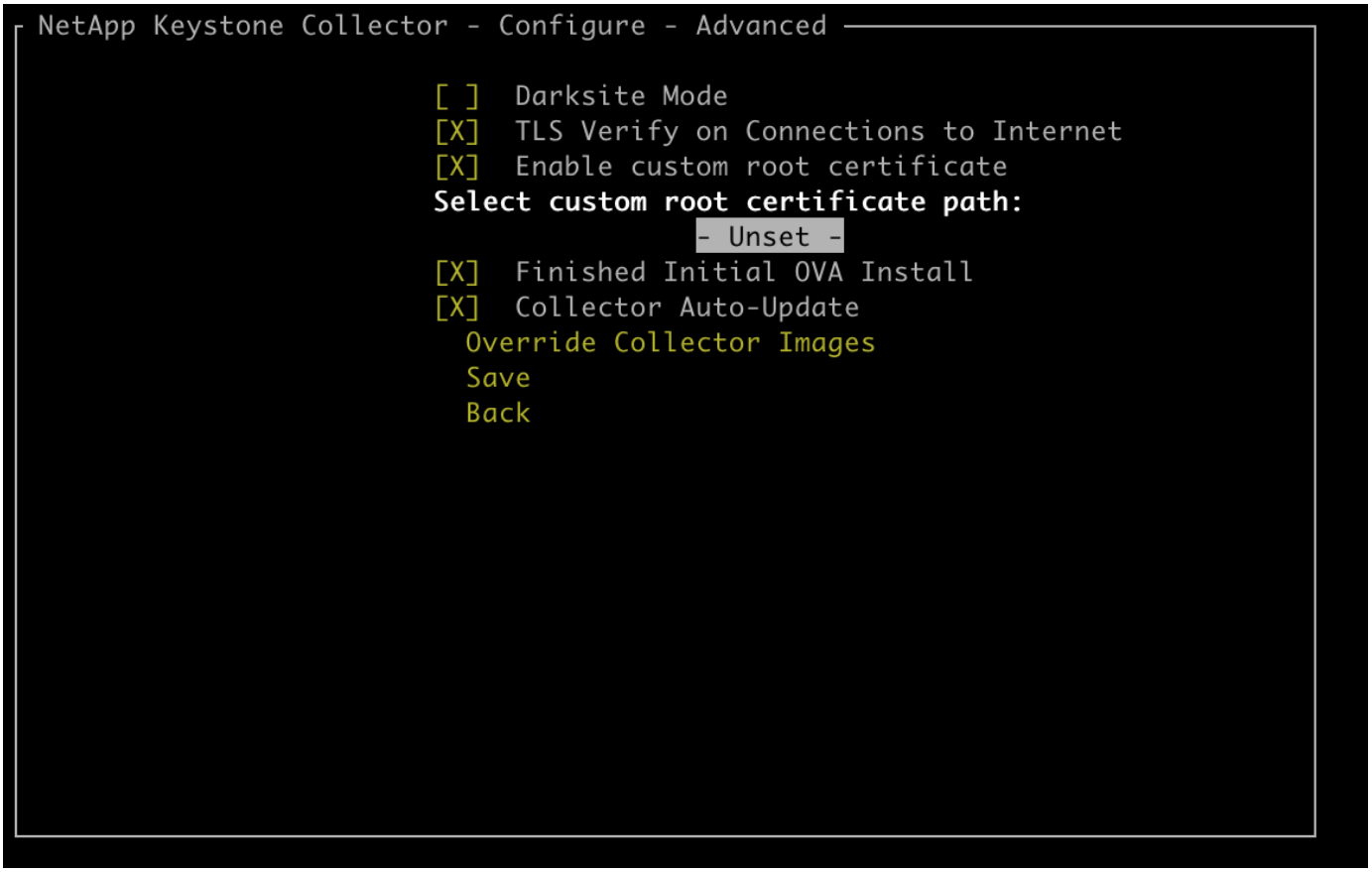
1. Préparez le certificat CA. Il doit être au format de fichier X.509 codé en base64.

> Les extensions de fichiers 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. Allez dans **Configuration > Avancé**.

5. Activez l'option **Activer le certificat racine personnalisé**.
6. Pour **Sélectionner 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.



Créer des niveaux de service 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.

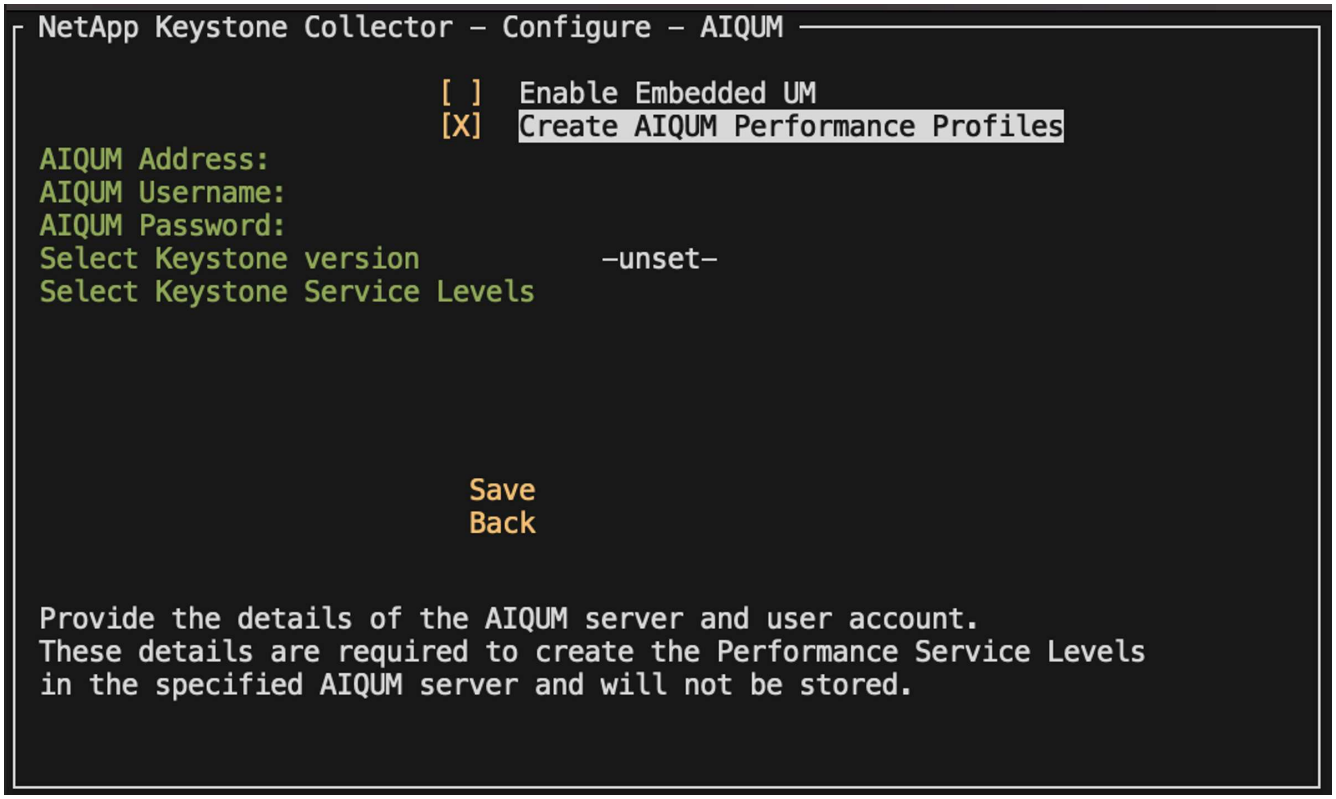
Pour en savoir plus sur les PSL, consultez"Niveaux de service de performance" .

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

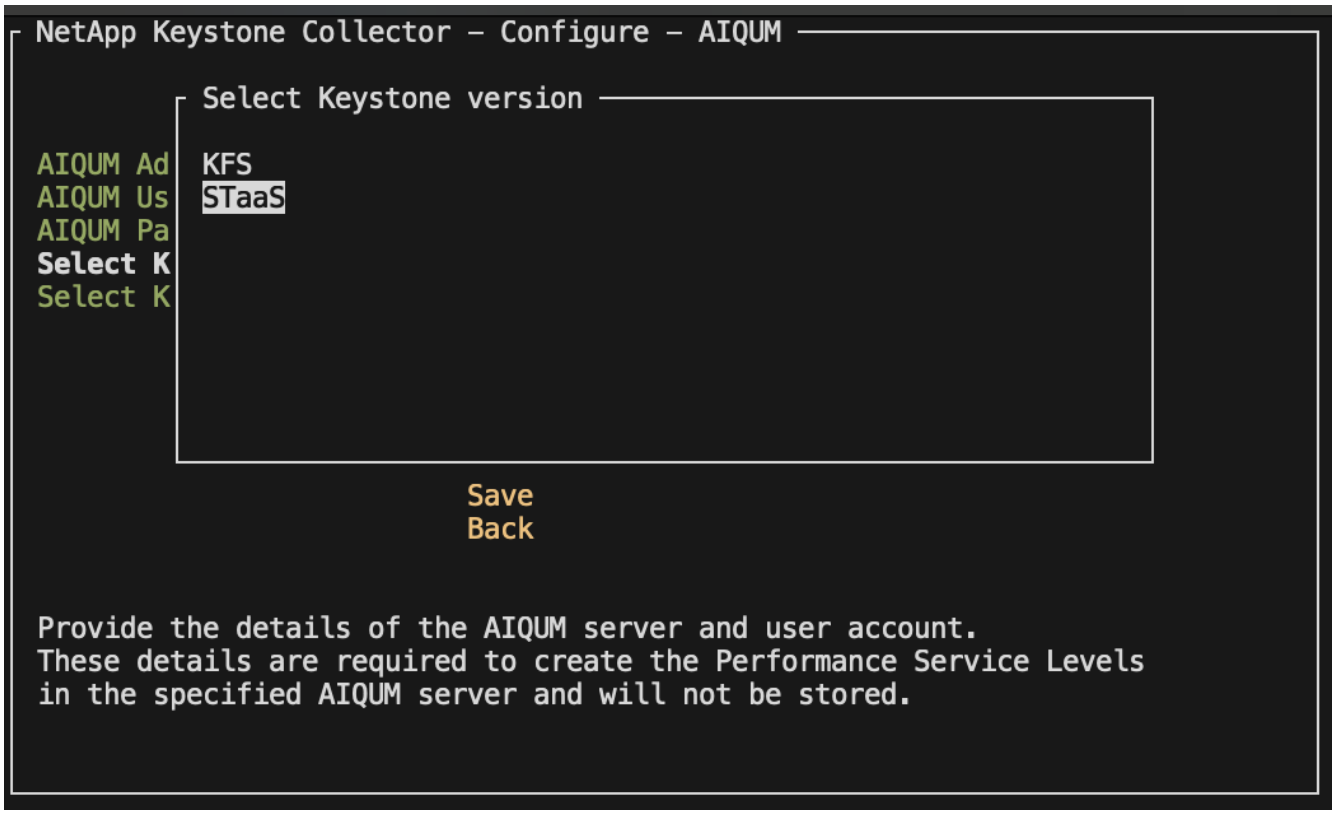
Étapes

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

2. Accédez à **Configurer>AIQUM** pour ouvrir l'écran AIQUM.
3. Activez l'option **Créer des profils de performances AIQUM**.
4. Saisissez les détails du serveur Active IQ Unified Manager et du compte utilisateur. Ces informations sont nécessaires à la création des PSL et ne seront pas stockées.

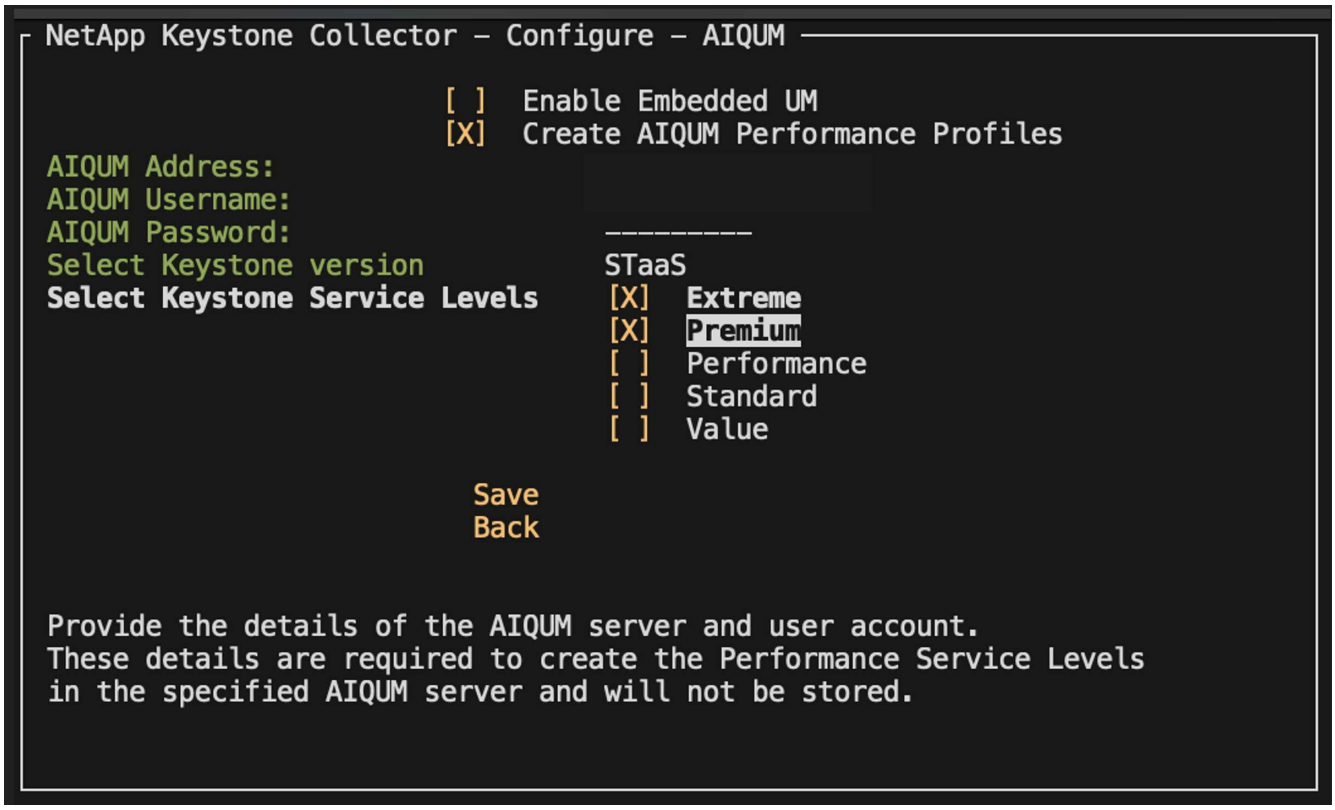


5. Pour *Sélectionner la version Keystone *, sélectionnez `-unset-` .
6. Appuyez sur Entrée. Une boîte de dialogue permettant de sélectionner la version Keystone s'affiche.
7. Mettez en surbrillance **STaaS** pour spécifier la version Keystone pour Keystone STaaS, puis appuyez sur Entrée.



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" .

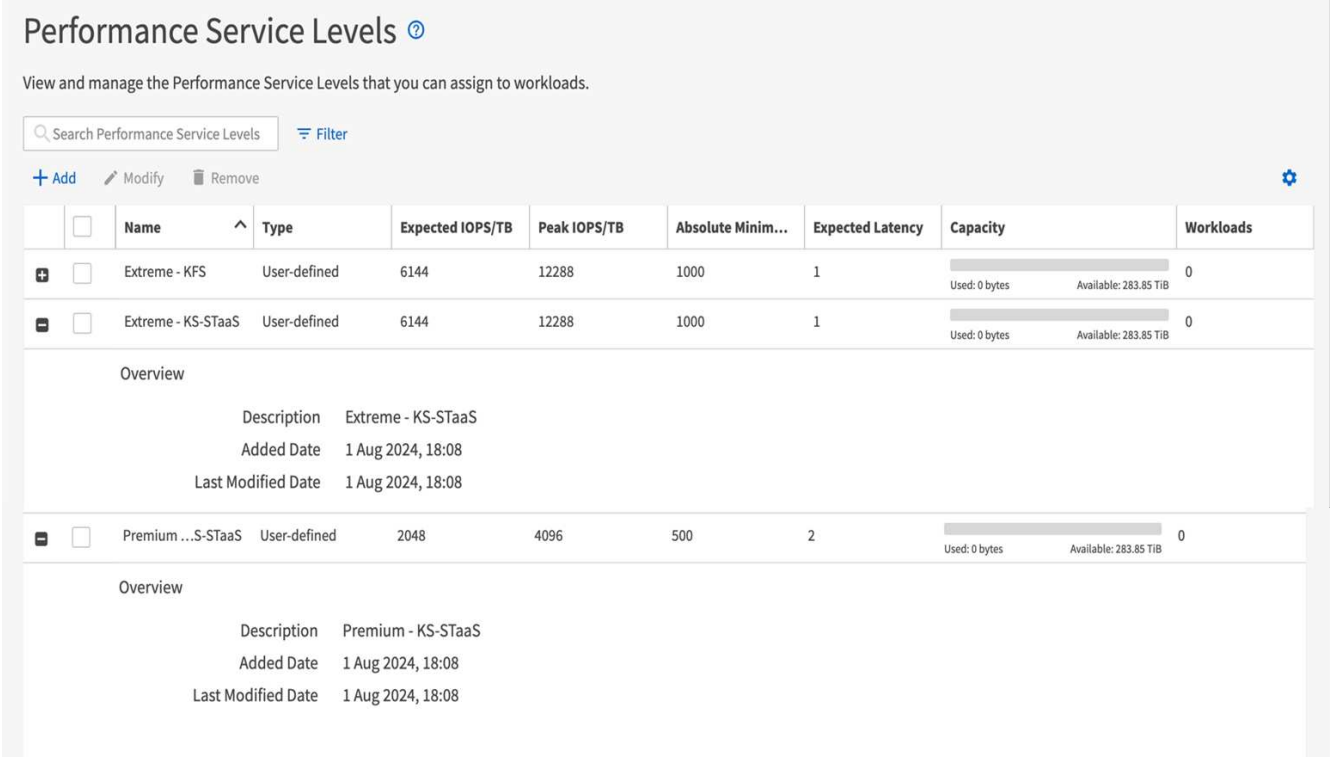
8. Tous les niveaux de service de performances Keystone pris en charge seront affichés dans l'option *Sélectionner les niveaux de service Keystone * pour la version Keystone spécifiée. Activez les niveaux de service de performances souhaités dans la liste.



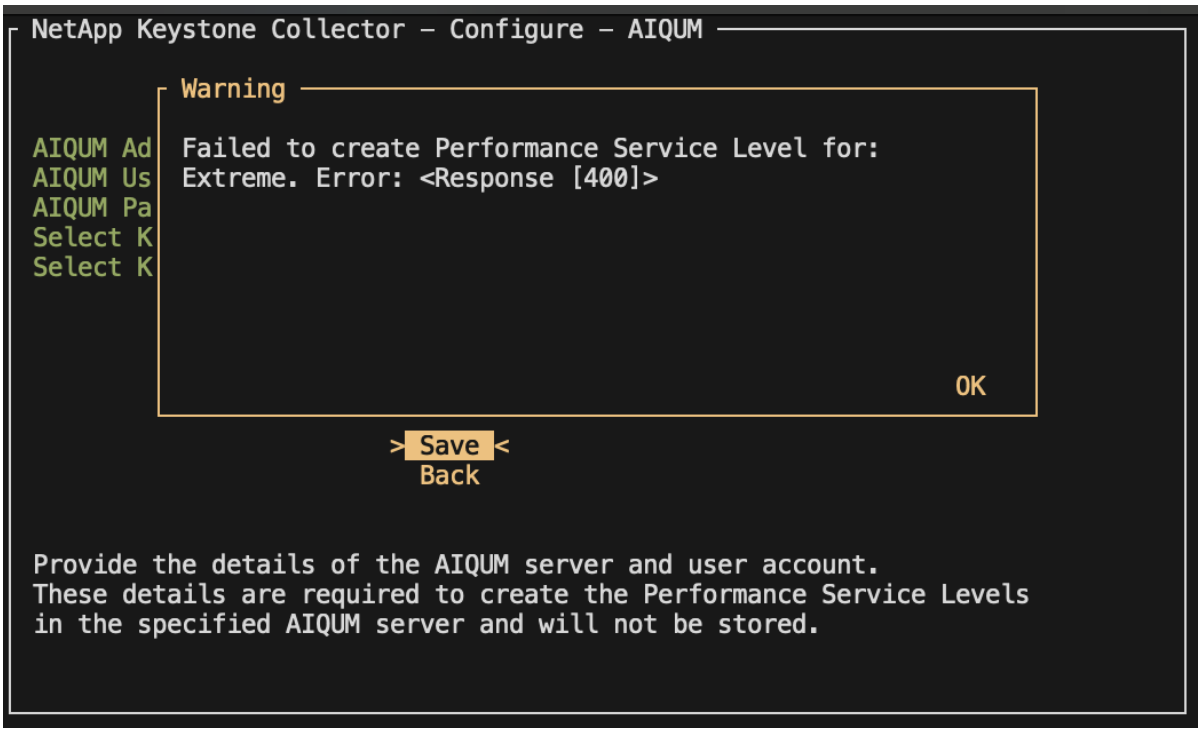
Vous pouvez sélectionner plusieurs niveaux de service de performance simultanément pour créer des PSL.

9. Sélectionnez **Enregistrer** et appuyez sur Entrée. Des niveaux de service de performance seront créés.

   Vous pouvez afficher les PSL créés, tels que Premium-KS-STaaS pour STaaS ou Extreme KFS pour KFS, sur la page **Niveaux de service de performance** dans Active IQ Unified Manager. Si les PSL créés ne répondent pas à vos exigences, vous pouvez les modifier pour répondre à vos besoins. Pour en savoir plus, consultez"Création et modification des niveaux de service de performance" .



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 ITOM Collector

Exigences d’installation pour le collecteur Keystone ITOM

Avant d’installer ITOM Collector, assurez-vous que vos systèmes sont préparés avec les logiciels nécessaires et répondent à toutes les conditions préalables requises.

Prérequis 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.

- Besoins en ressources : les besoins en ressources de la machine virtuelle en fonction du nombre de nœuds NetApp surveillés sont les suivants :
  - 2 à 10 nœuds : 4 processeurs, 8 Go de RAM, 40 Go de disque
  - 12 à 20 nœuds : 8 processeurs, 16 Go de RAM, 40 Go de disque
- Exigence de configuration : assurez-vous qu’un compte en lecture seule et SNMP sont configurés sur les périphériques surveillés. La machine virtuelle du serveur ITOM Collector doit également être configurée comme hôte d’interruption SNMP et serveur Syslog sur le cluster NetApp et les commutateurs de cluster, le cas échéant.

Exigences de mise en réseau

Les exigences réseau d’ITOM Collector sont répertoriées dans le tableau suivant.

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

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

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 d'assistance Keystone fournit un lien dynamique pour télécharger le fichier d'installation d'ITOM Collector, qui expire dans deux heures.

Pour installer ITOM Collector sur les systèmes Windows, reportez-vous à"Installer ITOM Collector sur les systèmes Windows" .

Suivez ces étapes 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 binaire **xxd** requis pour le fichier d'installation du collecteur ITOM.
- Assurer la `sudo package` est installé si vous prévoyez d'exécuter ITOM Collector en tant qu'utilisateur non root.

Étapes

1. Téléchargez le fichier d'installation 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 utilisateur final (CLUF).
   b. Saisissez les détails de l'utilisateur pour l'installation.
   c. Spécifiez le répertoire parent d'installation.
   d. Sélectionnez la taille du collecteur.
   e. Fournissez les détails du proxy, le cas échéant.

Pour chaque invite, une option par défaut est affichée. 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 est installé avec succès.

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

Quelle est la prochaine étape ?

Une fois l'installation réussie, contactez l'équipe d'assistance Keystone pour valider l'installation réussie d'ITOM Collector via le portail d'assistance ITOM. Après vérification, l'équipe d'assistance Keystone configurera le collecteur ITOM à distance, y compris la découverte et la configuration de la surveillance des appareils, et enverra 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 ITOM Collector sur un système Windows en téléchargeant le fichier d'installation d'ITOM Collector, en exécutant l'assistant InstallShield et en saisissant les informations d'identification de surveillance requises.

L'équipe d'assistance Keystone fournit un lien dynamique pour télécharger le fichier d'installation d'ITOM Collector, 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"Installer ITOM Collector sur les systèmes Linux" .

Suivez ces étapes pour installer le logiciel de collecte ITOM sur votre serveur Windows :

Avant de commencer

Assurez-vous que le service ITOM Collector est autorisé à **Se connecter en tant que service** sous Stratégie locale/Attribution des droits utilisateur dans les paramètres de stratégie de sécurité locale du serveur Windows.

Étapes

1. Téléchargez le fichier d'installation du collecteur ITOM sur votre serveur Windows.
2. Ouvrez le fichier d'installation pour démarrer l'assistant InstallShield.
3. Acceptez le contrat de licence utilisateur final (CLUF). L'assistant InstallShield extrait les binaires nécessaires et vous invite à saisir 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 le 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 d'administrateur local. Vous pouvez choisir de définir le mot de passe de manière à ce qu'il n'expire pas, afin de réduire les problèmes d'authentification entre ITOM Collector et ses ressources surveillées.

5. Sélectionnez la taille du collecteur. La valeur par défaut est la taille recommandée en fonction du fichier d'installation. Procédez 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 d'état affiche la progression de l'installation, suivie de la boîte de dialogue Assistant InstallShield terminé.

Quelle est la prochaine étape ?

Une fois l'installation réussie, contactez l'équipe d'assistance Keystone pour valider l'installation réussie d'ITOM Collector via le portail d'assistance ITOM. Après vérification, l'équipe d'assistance Keystone configurera le collecteur ITOM à distance, y compris la découverte et la configuration de la surveillance des appareils, et enverra une confirmation une fois la configuration terminée. Pour toute question ou information complémentaire, contactez keystone.services@netapp.com.

Configurer AutoSupport pour Keystone

Lors de l'utilisation du 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 pour incorporer les données Keystone dans les lots de support quotidiens envoyés par les clusters ONTAP .

À propos de cette tâche

Vous devez noter les points suivants avant de configurer AutoSupport pour inclure les données Keystone .

- Vous modifiez 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), consultez "Présentation de Gérer AutoSupport" et "Administrateurs de cluster et de SVM" .
- Vous incluez les sous-systèmes dans les packs AutoSupport quotidiens et hebdomadaires pour garantir une collecte de données précise pour Keystone. Pour plus d'informations sur les sous-systèmes AutoSupport , voir "Que sont les sous-systèmes AutoSupport ?" .

Étapes

1. En tant qu'utilisateur administrateur système, connectez-vous au cluster Keystone ONTAP à l'aide de SSH. Pour plus d'informations, voir "Accéder au cluster en utilisant 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 de prise en charge automatique du nœud système" .

Surveiller et mettre à niveau

Surveiller la santé de Keystone Collector

Vous pouvez surveiller l'état de santé de Keystone Collector en utilisant n'importe quel système de surveillance prenant en charge les requêtes HTTP. La surveillance de la santé peut aider à garantir que les données sont disponibles sur le tableau de bord Keystone .

Par défaut, les services de santé Keystone n'acceptent pas les connexions provenant d'une adresse IP autre que localhost. Le critère d'évaluation de la santé Keystone est `/uber/health` , et il écoute sur toutes les interfaces du serveur Keystone Collector sur le port `7777` . Lors de la requête, un code d'état de requête HTTP avec une sortie JSON est renvoyé par le point de terminaison en tant que réponse, décrivant l'état du système Keystone Collector. Le corps JSON fournit un état de santé général pour le `is_healthy` attribut, qui est un booléen ; et une liste détaillée des statuts par composant pour le `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 sains
- **503** : indique qu'un ou plusieurs composants sont défectueux
- **403**: indique que le client HTTP interrogeant l'état de santé ne figure pas dans la liste *allow*, qui est une liste de CIDR réseau autorisés. Pour ce statut, aucune information de santé n'est renvoyée. La liste *allow* utilise la méthode CIDR réseau pour contrôler les périphériques réseau autorisés à interroger le système de santé Keystone . Si vous recevez cette erreur, ajoutez votre système de surveillance à la liste *autorisée* depuis * Keystone Collector management TUI > Configurer > Surveillance de l'état*.

> **Utilisateurs de 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 politiques des guides de mise en œuvre technique de sécurité (STIG) de l'Agence des systèmes d'information de défense des États-Unis (DISA), un problème connu avec fapolicyd (démon de politique d'accès aux fichiers) a été observé par intermittence. Ce problème est identifié comme"bogue 1907870" . **Solution de contournement** : Jusqu'à ce que Red Hat Enterprise le résolve, NetApp vous recommande de contourner ce problème en mettant `fapolicyd` en mode permissif. Dans/`etc/fapolicyd/fapolicyd.conf` , définir la valeur de `permissive = 1` .

Afficher les journaux système

Vous pouvez afficher les journaux système de Keystone Collector pour examiner les informations système et effectuer un dépannage à l'aide de ces journaux. Keystone Collector utilise le système de journalisation *journald* de l'hôte et les journaux système peuvent être consultés via l'utilitaire système standard *journalctl*. Vous pouvez bénéficier des services clés suivants pour examiner les journaux :

- collectionneur ks
- ks-santé
- ks-mise à jour automatique

Le service principal de collecte de données *ks-collector* produit des journaux au format JSON avec un `run-id` attribut associé à chaque tâche de collecte de données planifiée. Voici un exemple de travail réussi de 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 performance :

```
{"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"}
```

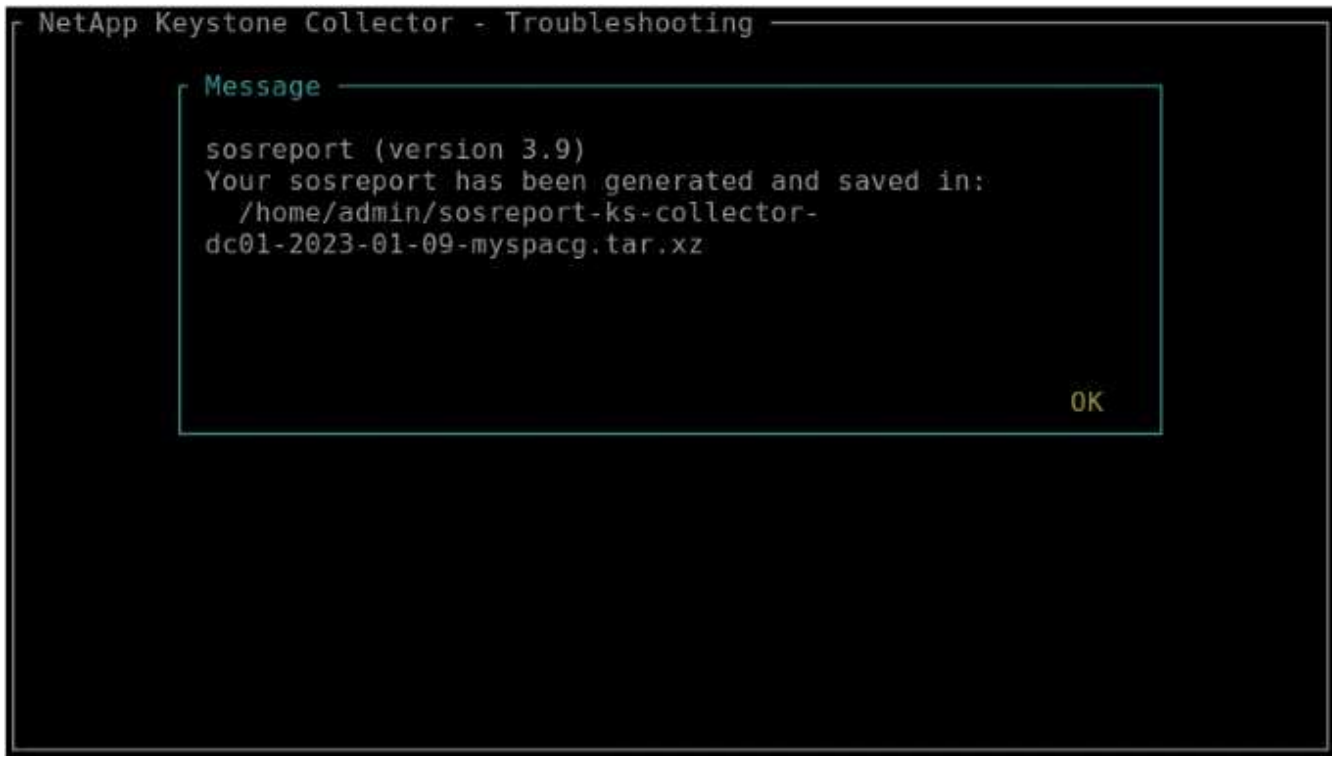
Générer et collecter des lots de support

L'interface utilisateur Keystone Collector vous permet de générer des lots d'assistance et de les ajouter aux demandes de service pour résoudre les problèmes d'assistance. Suivez cette procédure :

Étapes

1. Démarrez l'utilitaire TUI de gestion Keystone Collector :
   ```
   $ keystone-collector-tui
   ```
2. Accédez à **Dépannage > Générer un pack d'assistance**
   .

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



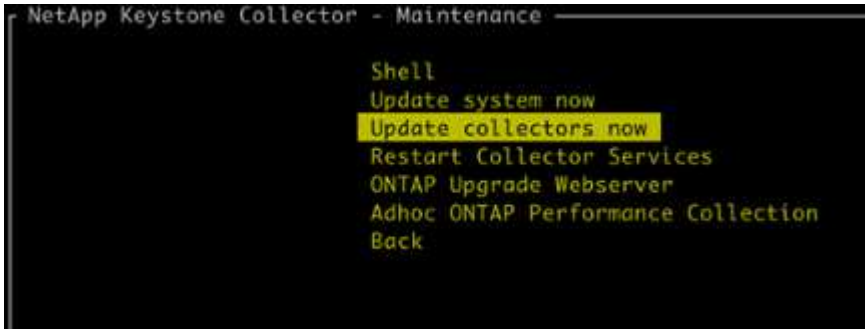
4. Une fois le fichier téléchargé, vous pouvez le joindre au ticket d'assistance Keystone ServiceNow. Pour plus d'informations sur la levée de fonds pour les billets, consultez "Génération de demandes de service".

Mettre à niveau manuellement Keystone Collector

La fonction 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 fonctionnalité et mettre à niveau manuellement le logiciel.

Étapes

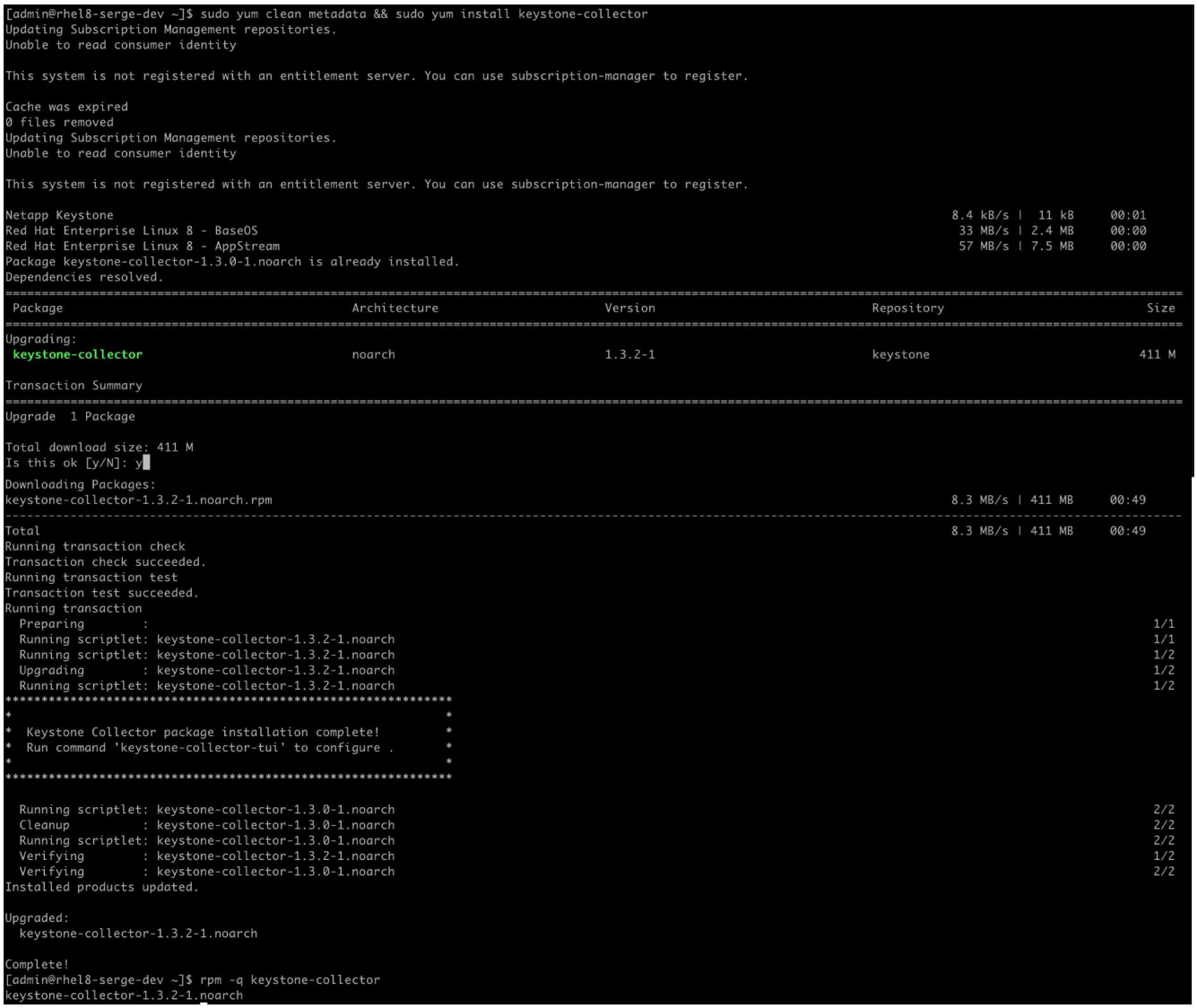
1. Démarrez l'utilitaire TUI de gestion Keystone Collector :
   `$ keystone-collector-tui`
2. Sur l'écran de maintenance, sélectionnez l'option **Mettre à jour les collecteurs maintenant**.



Vous pouvez également exécuter ces commandes 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 l'interface utilisateur de gestion de Keystone Collector, 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

Keystone Collector inclut des fonctionnalités de sécurité qui surveillent les performances et les mesures d'utilisation des systèmes Keystone , sans risquer la sécurité des données client.

Le fonctionnement de Keystone Collector repose sur les principes de sécurité suivants :

- **Confidentialité dès la conception** - Keystone Collector collecte un minimum de données pour effectuer la mesure de l'utilisation et la surveillance des performances. Pour plus d'informations, consultez la section "Données collectées pour la facturation" . Le"Supprimer les données privées" L'option est activée par défaut, ce qui masque et protège les informations sensibles.
- **Accès avec le moindre privilège** - Keystone Collector nécessite 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 moindre privilège, améliorant ainsi la posture de sécurité globale des environnements surveillés.
- **Cadre de développement logiciel sécurisé** - Keystone utilise un cadre de développement logiciel sécurisé tout au long du cycle de développement, ce qui atténue 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 en termes de sécurité. Voici les configurations de sécurité recommandées :

- Le 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, consultez la section "Guide de référence du 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 l'apparition de logiciels vulnérables non corrigés.
  - Authentifie les mises à jour reçues de Keystone Collector. La désactivation de la vérification du référentiel APT peut entraîner l'installation automatique de correctifs non autorisés, introduisant potentiellement des vulnérabilités.
- Keystone Collector valide automatiquement les certificats HTTPS pour garantir la sécurité de la connexion. La désactivation de cette fonctionnalité peut entraîner une usurpation d'identité de points de terminaison externes et une fuite de données d'utilisation.
- Keystone Collector prend en charge"Autorité de certification de confiance personnalisée" certification. Par défaut, il fait confiance aux certificats signés par des autorités de certification racines publiques reconnues par le"Programme de certificat Mozilla CA" . En activant des autorités de certification de confiance supplémentaires, Keystone Collector permet la validation des certificats HTTPS pour les connexions aux points de terminaison 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, consultez la section "Limiter la collecte de données

privées" . La désactivation de cette option entraîne la communication de données supplémentaires au système Keystone . Par exemple, il peut inclure des informations saisies par l'utilisateur, telles que les noms de volumes, qui peuvent être considérés comme des informations sensibles.

Informations connexes

- "Présentation de Keystone Collector"
- "Exigences en matière d'infrastructure virtuelle"
- "Configurer Keystone Collector"

Types de données utilisateur collectées 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 (VM) hébergeant Keystone Collector. Il peut collecter des données de performances pour ONTAP uniquement, si cette option est activée dans Keystone Collector.

Collecte de données ONTAP

Données d’utilisation collectées pour ONTAP: En savoir plus

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

- Groupes
  - ClusterUUID
  - Nom du cluster
  - Numéro de série
  - Emplacement (basé sur la valeur saisie dans le cluster ONTAP)
  - Contact
  - Version
- Nœuds
  - Numéro de série
  - Nom du nœud
- Volumes
  - Nom agrégé
  - Nom du volume
  - VolumeInstanceUUID
  - Drapeau IsCloneVolume
  - Drapeau IsFlexGroupConstituent
  - Drapeau IsSpaceEnforcementLogical
  - Indicateur IsSpaceReportingLogical
  - Espace logique utilisé par les Afs
  - Pourcentage d’espace instantané
  - Niveau de performance Données utilisateur inactives
  - Niveau de performance Pourcentage de données utilisateur inactives
  - Nom du groupe de politiques adaptatives QoS
  - Nom du groupe de politiques QoSPolicy
  - Taille
  - Utilisé
  - PhysiqueUtilisé
  - Taille utilisée par les instantanés
  - Type
  - VolumeStyleÉtendu
  - Nom du serveur virtuel
  - Drapeau IsVsRoot
- Serveurs virtuels
  - Nom du serveur virtuel

    - UUID du serveur virtuel
    - Sous-type
- Agrégats de stockage
    - Type de stockage
    - Nom agrégé
    - UUID agrégé
    - Physique utilisé
    - Taille disponible
    - Taille
    - Taille utilisée
- Magasins d'objets agrégés
    - Nom du magasin d'objets
    - ObjectStoreUUID
    - Type de fournisseur
    - Nom agrégé
- Volumes de clones
    - FlexClone
    - Taille
    - Utilisé
    - serveur virtuel
    - Type
    - ParentVolume
    - ParentVserver
    - Est-constituant
    - Estimation fractionnée
    - État
    - FlexCloneUsedPercent
- LUN de stockage
    - UUID LUN
    - Nom de LUN
    - Taille
    - Utilisé
    - Drapeau IsReserved
    - Drapeau IsRequested
    - Nom de l'unité logique
    - QoSPolicyUUID
    - Nom de la politique de qualité

    - VolumeUUID
    - Nom du volume
    - SVMUUID
    - Nom de SVM
- Volumes de stockage
    - VolumeInstanceUUID
    - Nom du volume
    - Nom SVM
    - SVMUUID
    - QoSPolicyUUID
    - Nom de la politique de qualité
    - Empreinte de niveau de capacité
    - Empreinte de niveau de performance
    - Empreinte totale
    - Politique de hiérarchisation
    - Drapeau IsProtected
    - Drapeau IsDestination
    - Utilisé
    - PhysiqueUtilisé
    - CloneParentUUID
    - Espace logique utilisé par les Afs
- Groupes de politiques QoS
    - Groupe de politiques
    - QoSPolicyUUID
    - Débit maximal
    - Débit minimal
    - Débit maximal IOPS
    - Débit maximal en Mbit/s
    - Débit minimal IOPS
    - Débit minimal (MBps)
    - Drapeau IsShared
- Groupes de politiques QoS adaptatives ONTAP
    - Nom de la politique de qualité
    - QoSPolicyUUID
    - Pic IOPS
    - Allocation de pics d'IOPS
    - MinIOPS absolus

    - IOPS attendus
    - Allocation d’IOPS attendue
    - Taille du bloc
- Empreintes de pas
    - serveur virtuel
    - Volume
    - Empreinte totale
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Nœud
    - Agrégat
    - Les LIF
    - Réplication de configuration
    - Relations
    - Groupes
    - Volumes
- clusters MetroCluster
    - ClusterUUID
    - Nom du cluster
    - RemoteClusterUUID
    - Nom du cluster distant
    - État de configuration locale
    - État de configuration à distance
- 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 d’observabilité du collecteur
    - Heure de collecte
    - Point de terminaison de l’API Active IQ Unified Manager interrogé
    - Temps de réponse
    - Nombre d’enregistrements
    - IP d’instance AIQUM
    - ID d’instance de collecteur

Données de performance collectées pour ONTAP: En savoir plus

La liste suivante est un échantillon représentatif des données de performance collectées pour ONTAP:

- Nom de cluster
- UUID de cluster
- ID d'objet
- Nom du volume
- UUID de l'instance de volume
- serveur virtuel
- UUID du serveur virtuel
- Nœud série
- Version ONTAP
- Version AIQUM
- Agrégat
- UUID agrégé
- Clé de ressource
- Horodatage
- IOPSPerTb
- Latence
- Latence de lecture
- Écriture en Mbit/s
- QoSMminThroughputLatency
- QoSNBladeLatency
- Espace libre utilisé
- CacheMissRatio
- Autre latence
- QoSAAggregateLatency
- Op E/S par sec
- QoSNetworkLetency
- Opérations disponibles
- Latence d'écriture
- QoSCloudLatency
- QoSClusterInterconnectLatency
- AutresMBps
- QoSCopLatency
- QoSDBladeLatency
- Utilisation

- Lire les IOPS
- Mbit/s
- Autres IOPS
- QoSPolicyGroupLatency
- Lecture en Mbit/s
- QoSSyncSnapmirrorLatence
- Données au niveau du système
  - Écriture/Lecture/Autre/Total IOPS
  - Écriture/Lecture/Autre/Débit total
  - Écriture/Lecture/Autre/Latence totale
- ÉcrireIOPS

Liste des éléments supprimés concernant la limitation de l'accès aux données privées : En savoir plus

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

- Nom de cluster
- Localisation du cluster
- Contact du cluster
- Nom du nœud
- Nom agrégé
- Nom du volume
- Nom du groupe de politiques adaptatives QoS
- Nom du groupe de politiques QoSPolicy
- Nom du serveur virtuel
- Nom du LUN de stockage
- Nom agrégé
- Nom de l'unité logique
- Nom de SVM
- IP d'instance AIQUM
- FlexClone
- Nom du cluster distant

Collecte de données StorageGRID

Données d'utilisation collectées pour StorageGRID: En savoir plus

La liste suivante est un échantillon représentatif des `Logical Data` collecté pour StorageGRID:

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

La liste suivante est un échantillon représentatif des `Physical Data` collecté pour StorageGRID:

- ID StorageGRID
- Nœud ID
- ID du site
- Nom du site
- Exemple
- Utilisation du stockage StorageGRID Octets
- Métadonnées d'utilisation du stockage StorageGRID Octets

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

- Pourcentage de disponibilité du SLA

Liste des éléments supprimés concernant la limitation de l'accès aux données privées : En savoir plus

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

- Nom du compte
- Nom du compartiment
- Nom du site
- Nom d'instance/de nœud

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 *dark site*, pour répondre à vos besoins commerciaux et de sécurité. Ce mode est disponible pour les organisations ayant des restrictions de connectivité.

NetApp propose un déploiement spécialisé de Keystone STaaS adapté aux environnements avec une connectivité Internet limitée ou inexistante (également appelés sites sombres). Il s'agit d'environnements sécurisés ou isolés où la communication externe est restreinte en raison d'exigences de sécurité, de conformité ou opérationnelles.

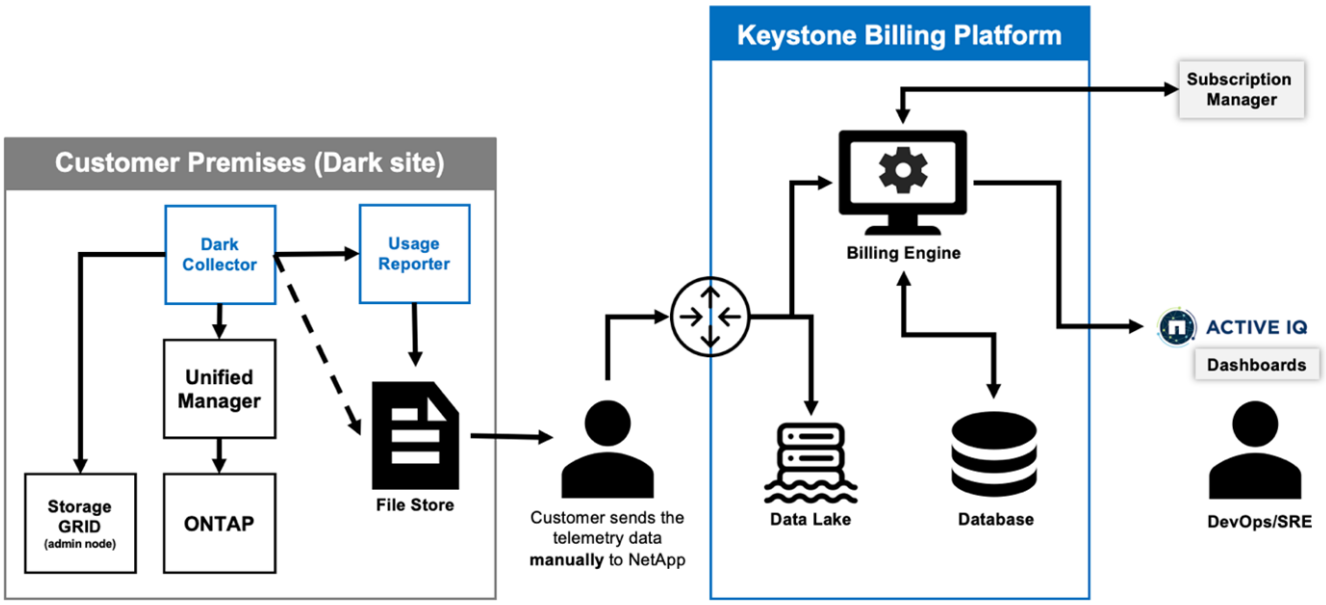
Pour NetApp Keystone, proposer des services pour les sites sombres signifie fournir le service d'abonnement de stockage flexible Keystone d'une manière qui respecte les contraintes de ces environnements. Cela implique :

- **Déploiement local** : Keystone peut être configuré dans des environnements isolés de manière indépendante, garantissant ainsi l'absence de besoin de connexion Internet ou de personnel externe pour l'accès à la configuration.
- **Opérations hors ligne** : toutes les fonctionnalités de gestion du stockage avec contrôles 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 sombres, qui peuvent inclure un cryptage avancé, des contrôles d'accès sécurisés et des capacités d'audit détaillées.
- **Aide et support** : NetApp fournit un support mondial 24h/24 et 7j/7 avec un responsable de réussite Keystone dédié affecté à chaque compte pour l'assistance et le dépannage.

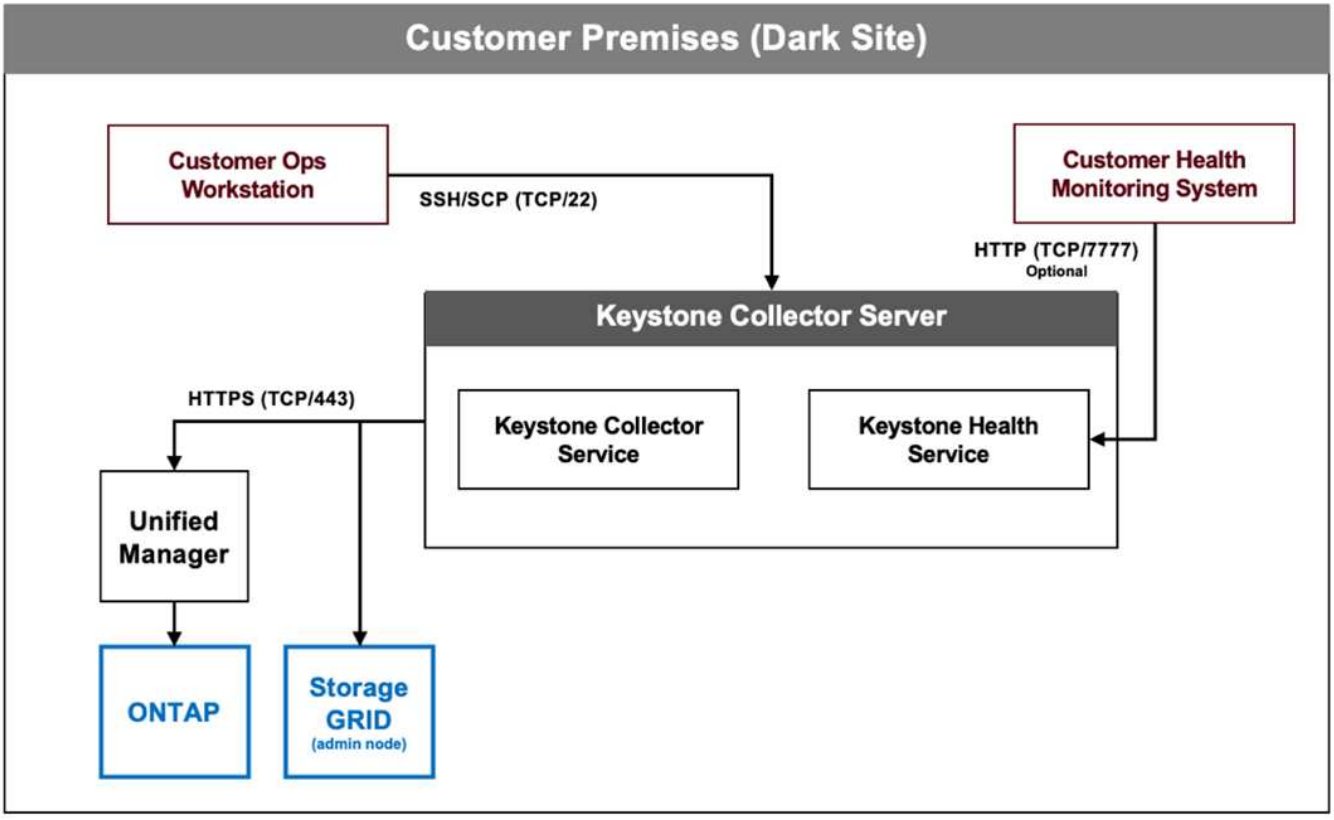
> Keystone Collector peut être configuré sans restrictions de connectivité, également appelé mode *standard*. Pour en savoir plus, consultez"En savoir plus sur Keystone Collector" .

Keystone Collector en mode privé

Keystone Collector est chargé de collecter périodiquement les données d'utilisation des systèmes de stockage et d'exporter les métriques vers un rapporteur d'utilisation hors ligne et un magasin de fichiers local. Les fichiers générés, créés dans des formats cryptés et en texte brut, sont ensuite transmis manuellement à NetApp par l'utilisateur après les contrôles de validation. Dès réception, la plateforme de facturation Keystone de NetApp authentifie et traite ces fichiers, les intégrant dans les systèmes de facturation et de gestion des abonnements pour calculer les frais mensuels.



Le service Keystone Collector sur le serveur est chargé de collecter périodiquement les données d'utilisation, de traiter ces informations et de générer un fichier d'utilisation localement sur le serveur. Le service de santé effectue des contrôles de santé du système et est conçu pour s'interfacer avec les systèmes de surveillance de la santé utilisés par le client. Ces rapports sont accessibles hors ligne par les utilisateurs, ce qui permet la validation et aide à la résolution des problèmes.



Préparation de l'installation du collecteur Keystone en mode privé

Avant d'installer Keystone Collector dans un environnement sans accès 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 préalables requises.

Configuration requise pour VMware vSphere

- Système d'exploitation : serveur VMware vCenter et ESXi 8.0 ou version ultérieure
- Noyau : 1 CPU
- RAM : 2 Go
- Espace disque : 20 Go 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
- Noyau : 2 CPU
- RAM : 4 Go
- Espace disque : 50 Go vDisk
  - Au moins 2 Go libres dans `/var/lib/`
  - Au moins 48 Go libres dans `/opt/netapp`

Le même serveur doit également avoir les packages tiers suivants installés. 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
  - verrouillage de version du plugin python3-dnf
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - sos
  - yum-utils
  - verrouillage de version du plugin python3-dnf
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - podman

- sosreport

Exigences de mise en réseau

Les exigences de mise en réseau pour Keystone Collector incluent les éléments suivants :

- Active IQ Unified Manager (Unified Manager) 9.10 ou version ultérieure, configuré sur un serveur avec la fonctionnalité API Gateway 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 d'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".

Installer Keystone Collector en mode privé

Suivez quelques étapes pour installer Keystone Collector dans un environnement qui n'a pas 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 des systèmes VMware vSphere ou l'installer sur des systèmes Linux, selon vos besoins. Suivez les étapes d'installation correspondant à l'option sélectionnée.

Déployer sur VMware vSphere

Suivez ces étapes :

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

Installer sur 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.

Suivez ces étapes pour installer le logiciel sur votre serveur Linux :

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

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

2. Ouvrez un terminal sur le serveur et exécutez les commandes suivantes pour commencer l'installation.
   - **Utilisation du 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. Entrer `y` lorsque vous êtes invité à installer le package.

Configurer 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 n'a pas accès à Internet, également appelé *site sombre* ou *mode privé*. Il s'agit d'une activité ponctuelle visant à activer et à associer les composants requis à votre environnement de stockage. Une fois configuré, Keystone Collector surveillera tous les clusters ONTAP gérés par Active IQ Unified Manager.

Keystone Collector vous fournit l'utilitaire d'interface utilisateur du terminal de gestion Keystone Collector (TUI) pour effectuer des activités de configuration et de surveillance. Vous pouvez utiliser différentes commandes du clavier, telles que les touches Entrée et fléchées, pour sélectionner les options et naviguer dans cette interface utilisateur graphique.

Étapes

1. Démarrez l'utilitaire TUI de gestion Keystone Collector :

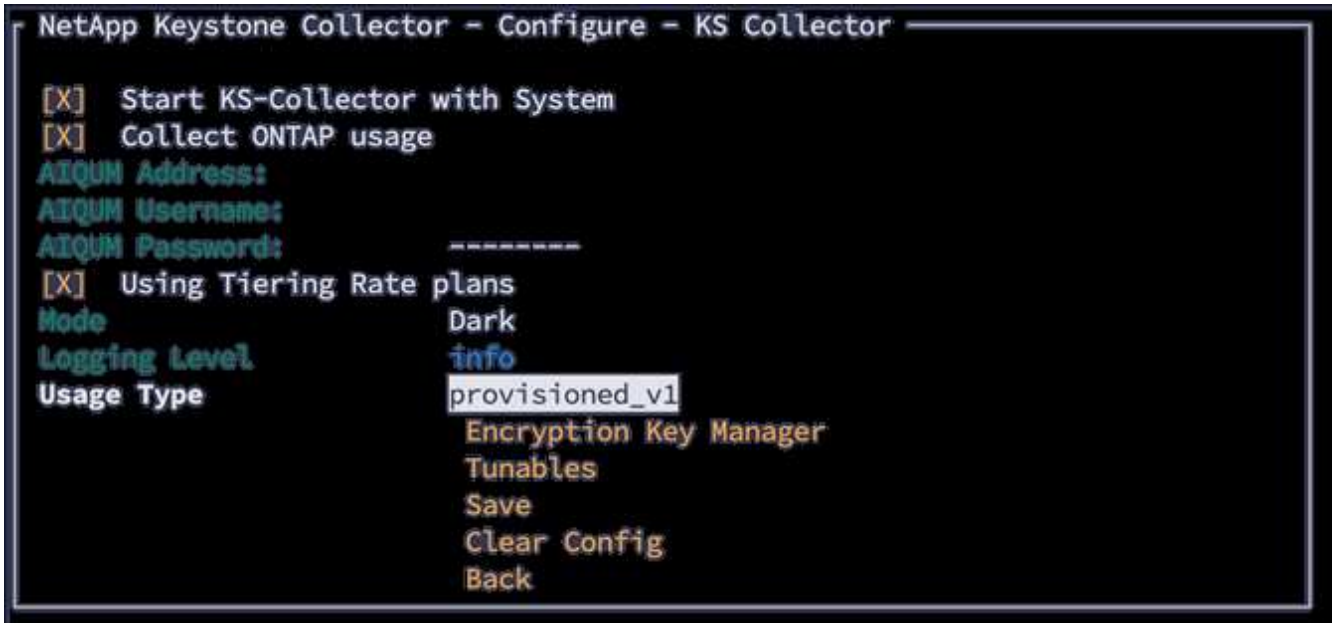
```
keystone-collector-tui
```

2. Allez dans **Configurer > Avancé**.
3. Activez l'option **Mode Darksite**.

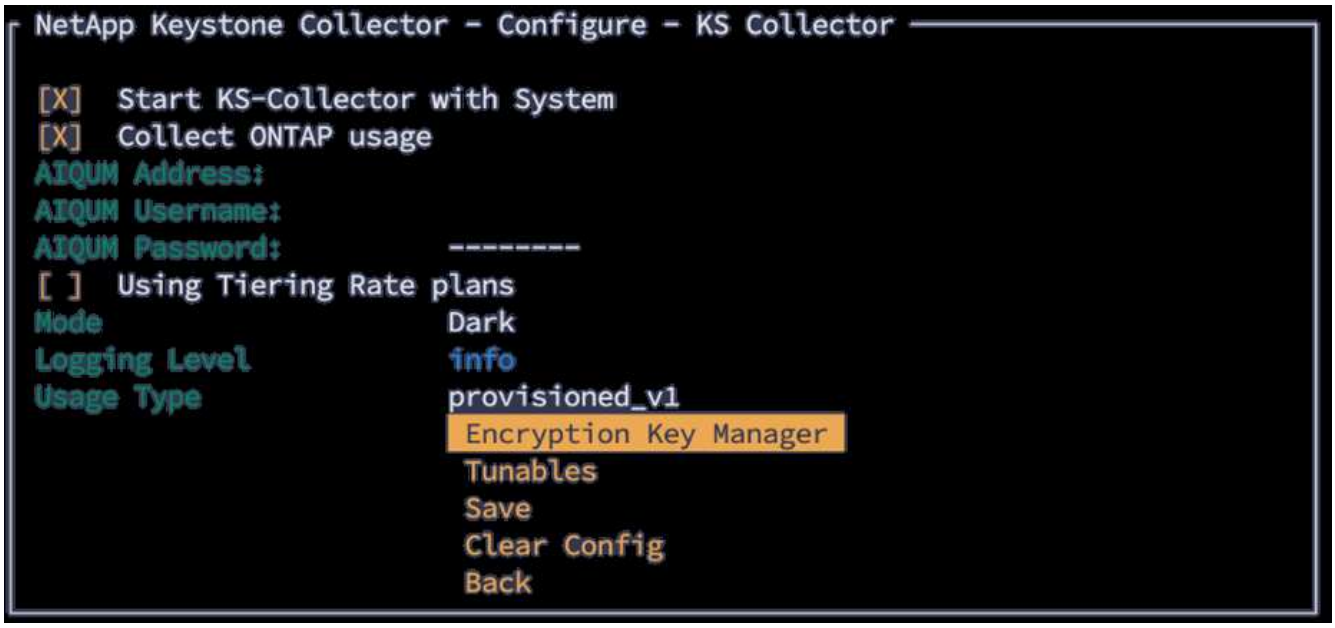
4. Sélectionnez **Enregistrer**.
5. Accédez à **Configurer > KS-Collector** pour configurer Keystone Collector.
6. Activez/désactivez le champ **Démarrer KS Collector avec le système**.
7. Activez/désactivez le champ **Collect ONTAP Usage**. Ajoutez les détails du serveur Active IQ Unified Manager (Unified Manager) et du compte utilisateur.

8. **Facultatif** : Activez le champ **Utilisation des forfaits de hiérarchisation** 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 la configuration, confirmez le type d'utilisation associé à l'abonnement auprès de NetApp.

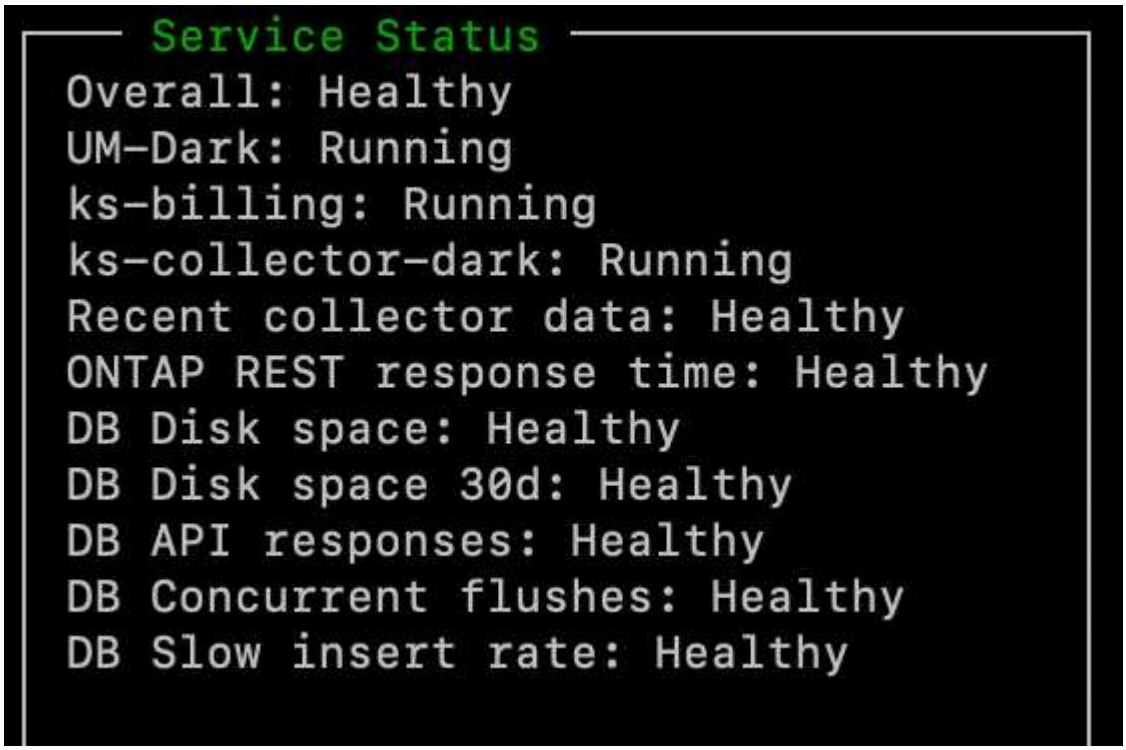


10. Sélectionnez **Enregistrer**.
11. Accédez à **Configurer > KS-Collector** pour générer la paire de Keystone Collector.
12. Accédez à **Encryption Key Manager** et appuyez sur Entrée.



13. Sélectionnez **Générer une paire de clés de collecteur** et appuyez sur Entrée.

14. Assurez-vous que le collecteur Keystone est en bon état en revenant à l'écran principal de l'interface utilisateur et en vérifiant les informations **État du service**. Le système doit indiquer que les services sont dans un état **Globalement : sain**. Attendez jusqu'à 10 minutes, si l'état général 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 de Keystone Collector en sélectionnant l'option **Quitter vers Shell** sur l'écran d'accueil.
16. Récupérer 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 récapitulatif d'utilisation mensuel à NetApp à la fin de chaque mois. Vous pouvez générer ce rapport manuellement.

Suivez ces étapes pour générer le rapport d'utilisation :

1. Accédez à **Exporter l'utilisation** 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 doivent être envoyés manuellement à NetApp. Le rapport de fichier clair 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-----
```

Mettre à niveau ONTAP

Keystone Collector prend en charge les mises à niveau ONTAP via TUI.

Suivez ces étapes pour mettre à niveau ONTAP:

1. Accédez à **Maintenance > ONTAP Upgrade Webserver**.
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. Aller à `http://<collector-ip>:8000` utiliser un navigateur Web pour obtenir de l'aide à la mise à niveau.

Redémarrer Keystone Collector

Vous pouvez redémarrer le service Keystone Collector via l'interface utilisateur. Accédez à **Maintenance > Redémarrer les services Collector** dans l'interface utilisateur. Cela redémarrera tous les services du collecteur et leur état pourra être surveillé depuis l'écran d'accueil de TUI.

Surveiller la santé du collecteur Keystone en mode privé

Vous pouvez surveiller l'état de santé de Keystone Collector en utilisant n'importe quel système de surveillance prenant en charge les requêtes HTTP.

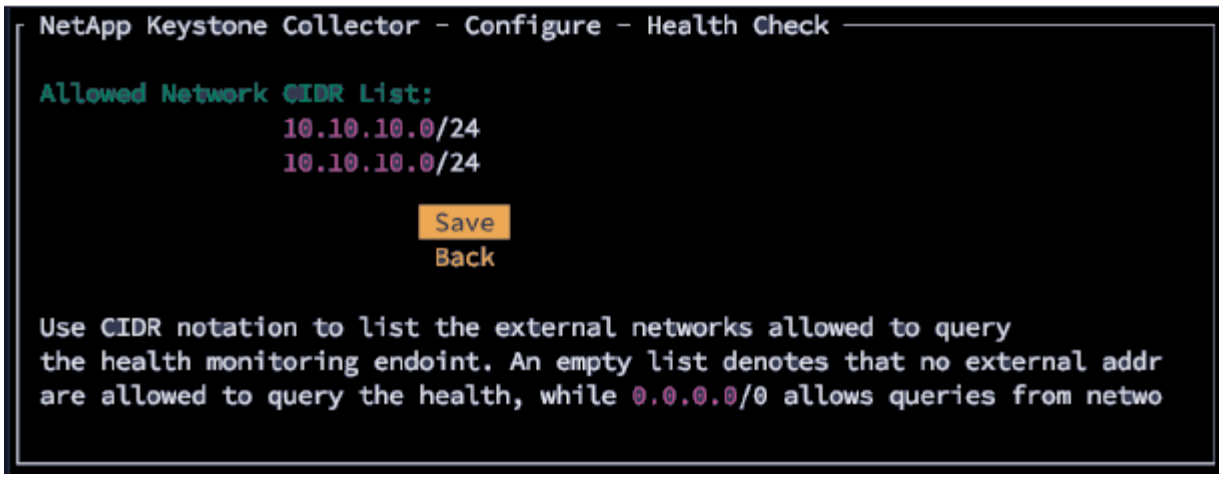
Par défaut, les services de santé Keystone n'acceptent pas les connexions provenant d'une adresse IP autre que localhost. Le critère d'évaluation de la santé Keystone est `/uber/health` , et il écoute sur toutes les interfaces du serveur Keystone Collector sur le port `7777` . Lors de la requête, un code d'état de requête HTTP avec une sortie JSON est renvoyé par le point de terminaison en tant que réponse, décrivant l'état du système Keystone Collector. Le corps JSON fournit un état de santé général pour le `is_healthy` attribut, qui est un booléen ; et une liste détaillée des statuts par composant pour le `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 sains
- **503** : indique qu'un ou plusieurs composants sont défectueux
- **403**: indique que le client HTTP interrogeant l'état de santé ne figure pas dans la liste *allow*, qui est une liste de CIDR réseau autorisés. Pour ce statut, aucune information de santé n'est renvoyée.

  La liste *allow* utilise la méthode CIDR réseau pour contrôler les périphériques réseau autorisés à interroger le système de santé Keystone . Si vous recevez l'erreur 403, ajoutez votre système de surveillance à la liste *autorisée* depuis * Keystone Collector management TUI > Configurer > Surveillance de l'état*.

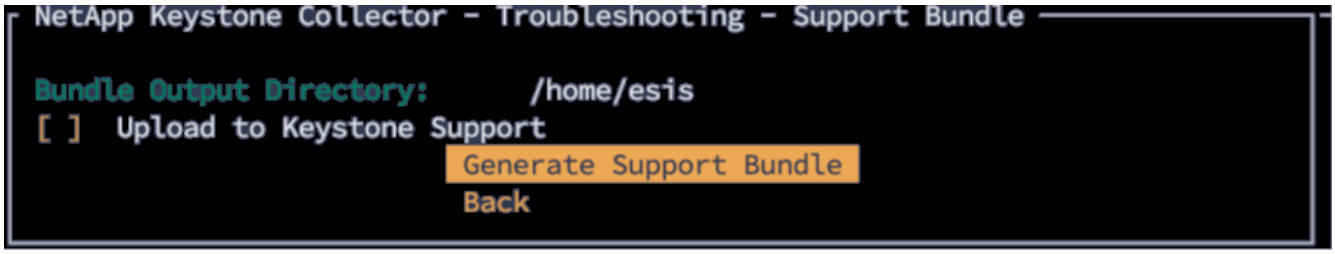


Générer et collecter des lots de support

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

Suivez ces étapes pour générer un fichier *.tar* :

1. Accédez à **Dépannage > Générer un pack d'assistance**.
2. Sélectionnez l'emplacement pour enregistrer le 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".