



Keystone en mode privé

Keystone

NetApp
January 15, 2026

Sommaire

- Keystone en mode privé 1
 - En savoir plus sur Keystone (mode privé) 1
 - Keystone Collector en mode privé 1
 - Préparation de l'installation du collecteur Keystone en mode privé 3
 - Configuration requise pour VMware vSphere 3
 - Configuration requise pour Linux 3
 - Exigences de mise en réseau 4
 - Installer Keystone Collector en mode privé 4
 - Déployer sur VMware vSphere 4
 - Installer sur Linux 4
 - Configurer Keystone Collector en mode privé 5
 - Exporter le rapport d'utilisation 8
 - Mettre à niveau ONTAP 9
 - Redémarrer Keystone Collector 9
 - Surveiller la santé du collecteur Keystone en mode privé 10
 - Générer et collecter des lots de support 11

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 :

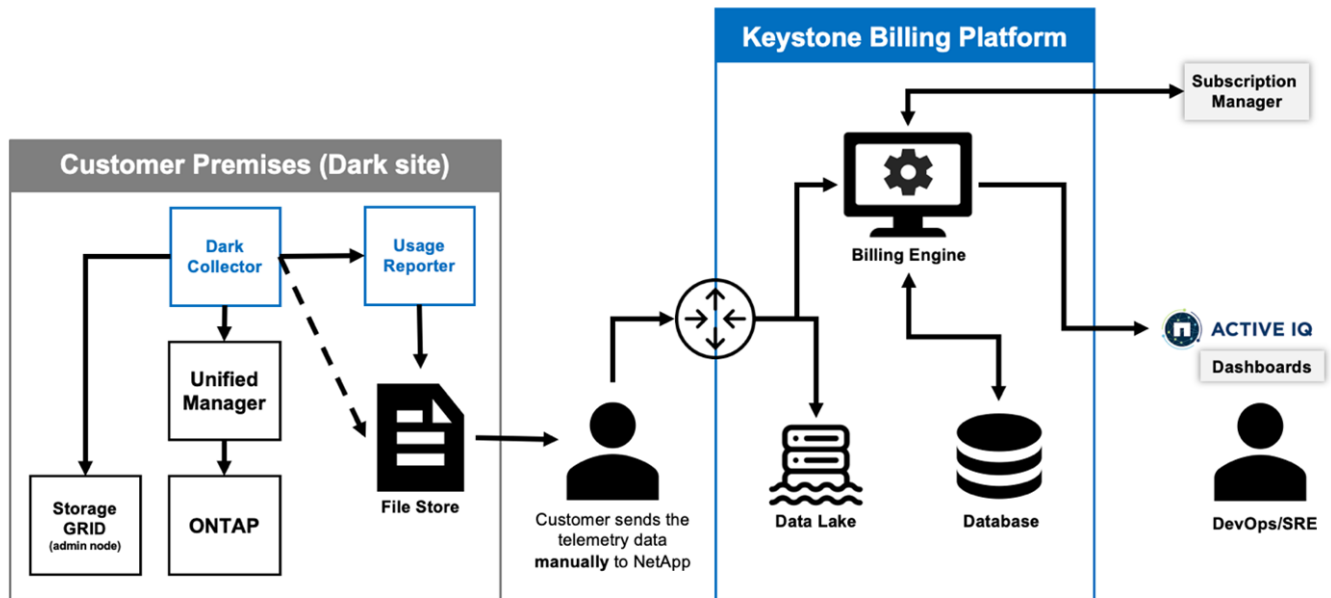
- **Déploiement local** : Keystone peut être configuré dans des environnements isolés de manière indépendante, garantissant ainsi l'absence de besoin de connexion Internet ou de personnel externe pour l'accès à la configuration.
- **Opérations hors ligne** : toutes les fonctionnalités de gestion du stockage 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.



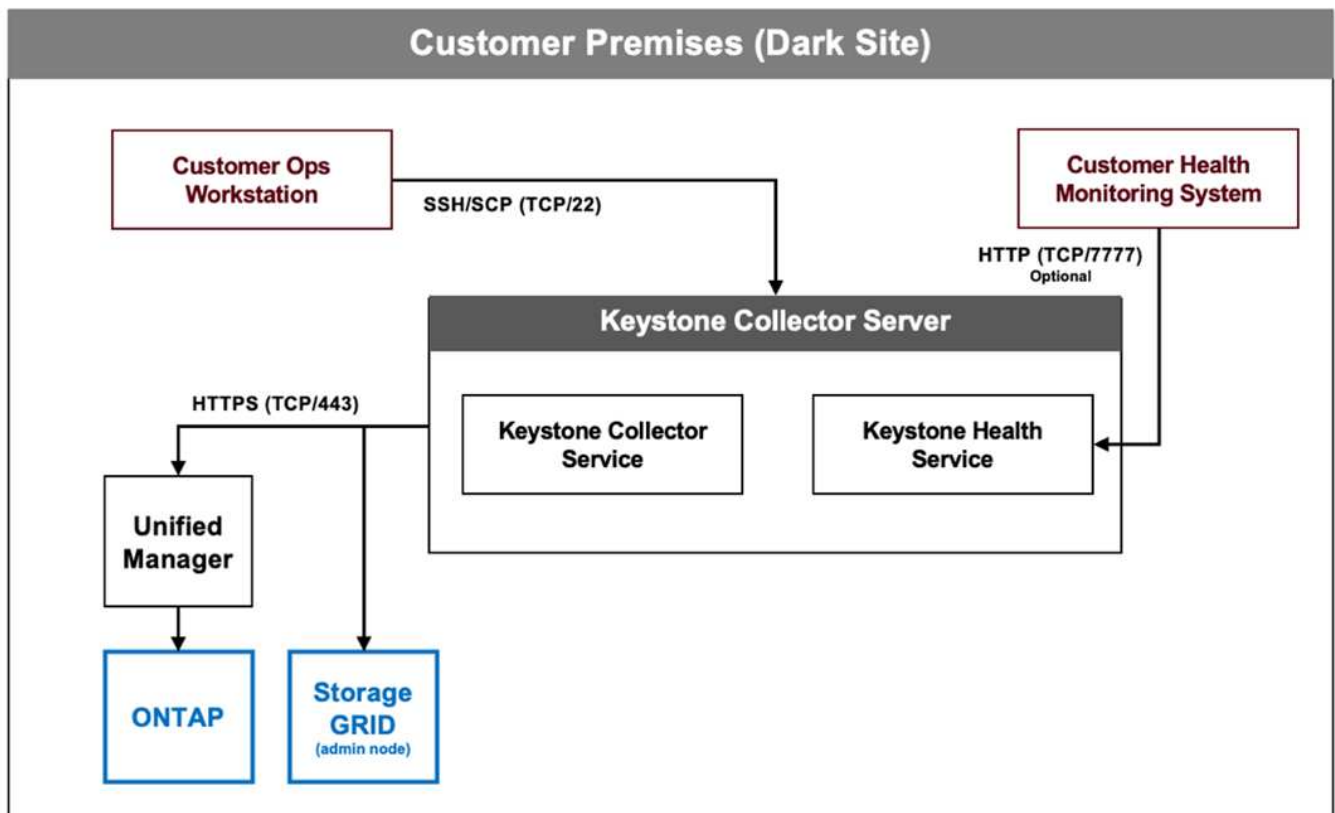
Keystone Collector peut être configuré sans restrictions de connectivité, également appelé mode *standard*. Pour en savoir plus, consultez ["En savoir plus sur Keystone Collector"](#).

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.

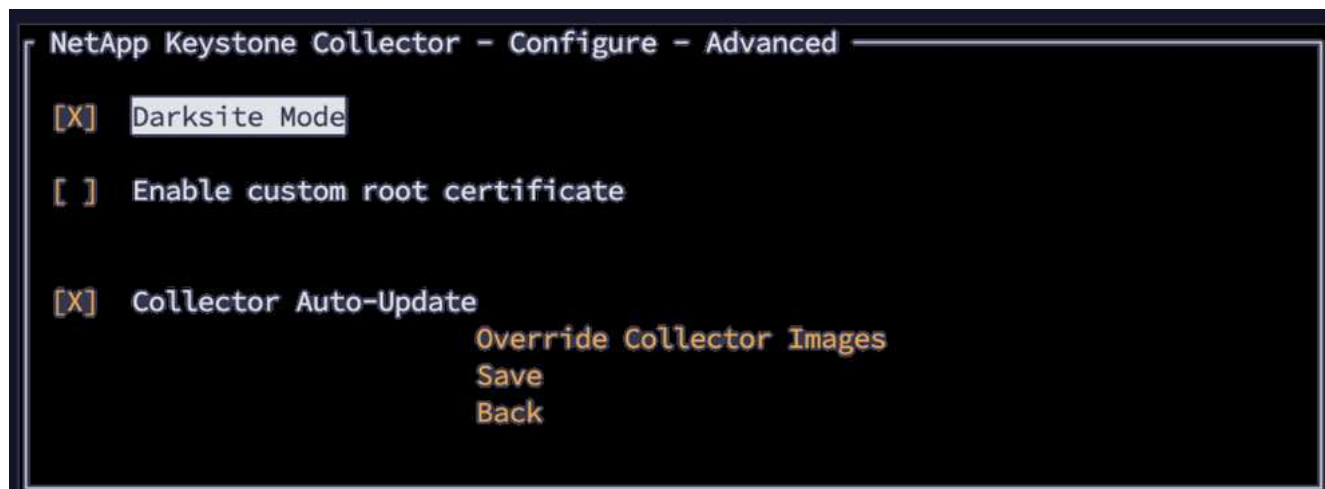
Étapes

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

```
keystone-collector-tui
```

2. Allez dans **Configurer > Avancé**.

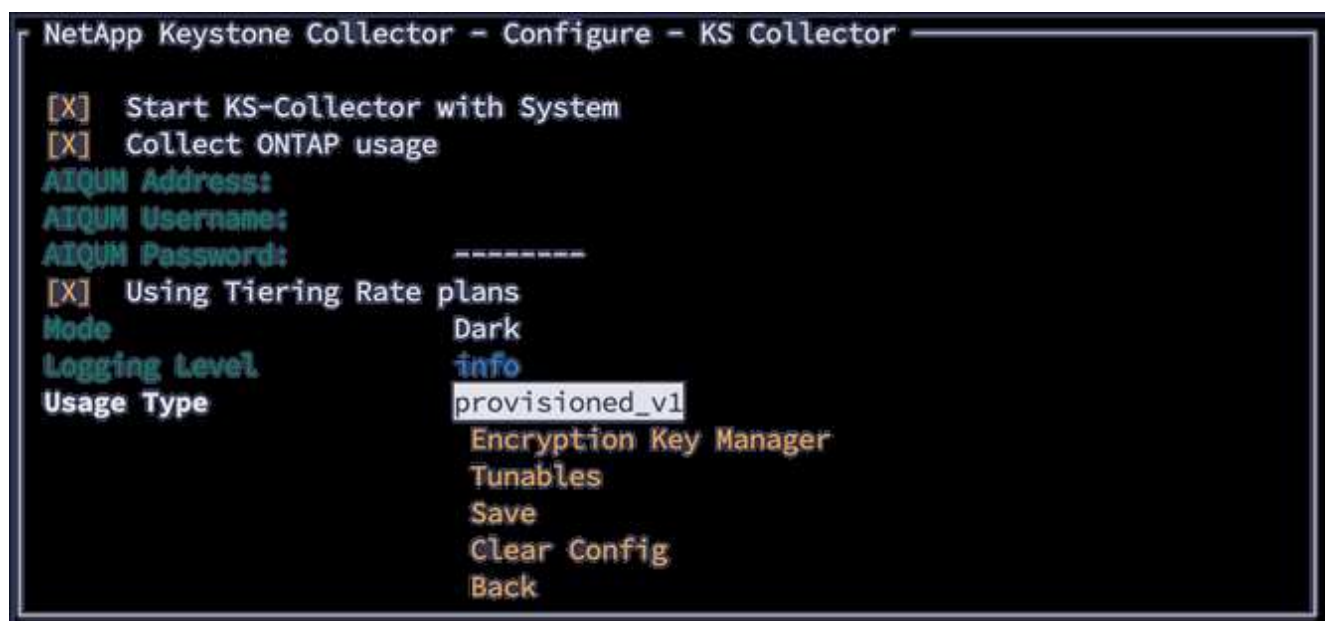
3. Activez l'option **Mode Darksite**.



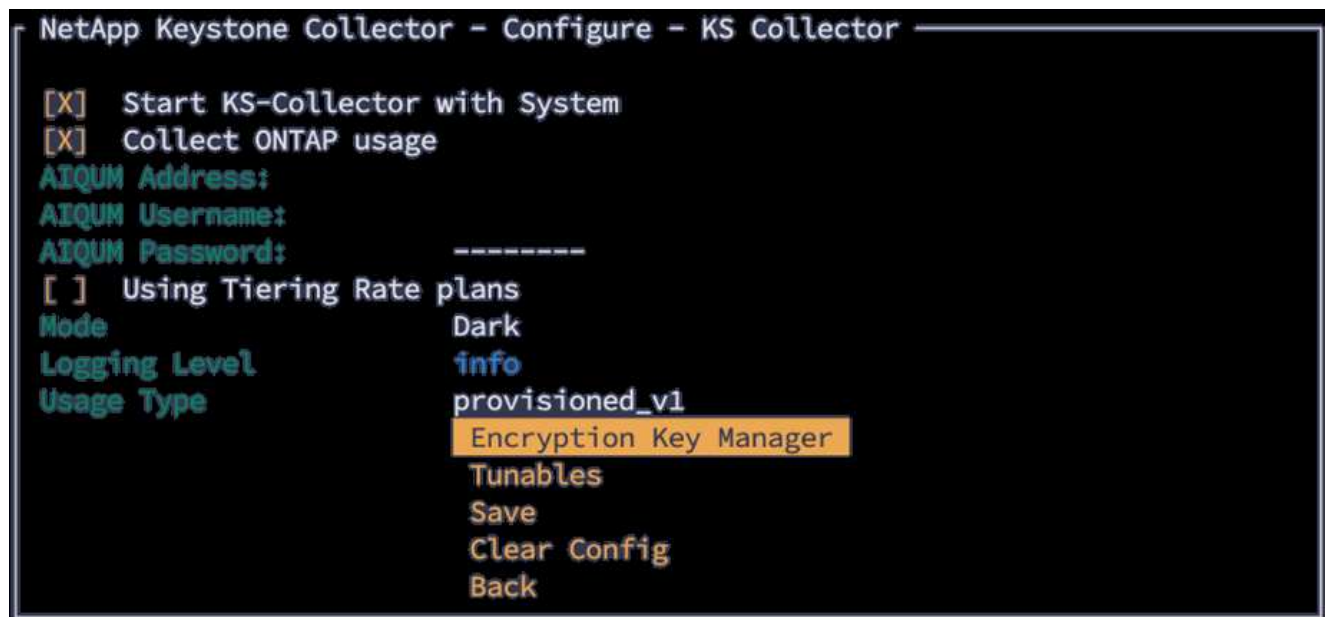
4. Sélectionnez **Enregistrer**.
5. Accédez à **Configurer > KS-Collector** pour configurer Keystone Collector.
6. Activez/désactivez le champ **Démarrer KS Collector avec le système**.
7. Activez/désactivez le champ **Collect ONTAP Usage**. Ajoutez les détails du serveur Active IQ Unified Manager (Unified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



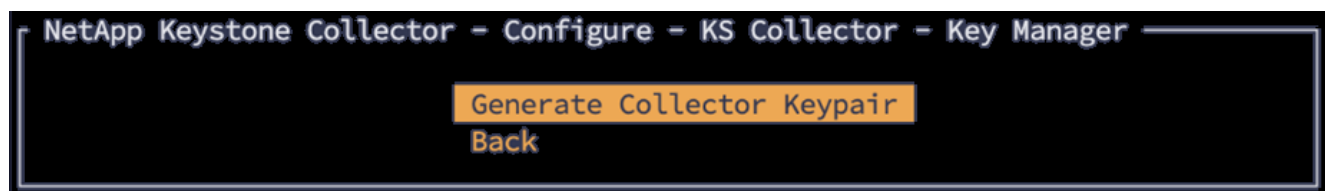
Avant la configuration, confirmez le type d'utilisation associé à l'abonnement auprès de NetApp.



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 .

```
Service Status
Overall: Healthy
UM-Dark: Running
ks-billing: Running
ks-collector-dark: Running
Recent collector data: Healthy
ONTAP REST response time: Healthy
DB Disk space: Healthy
DB Disk space 30d: Healthy
DB API responses: Healthy
DB Concurrent flushes: Healthy
DB Slow insert rate: Healthy
```

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.

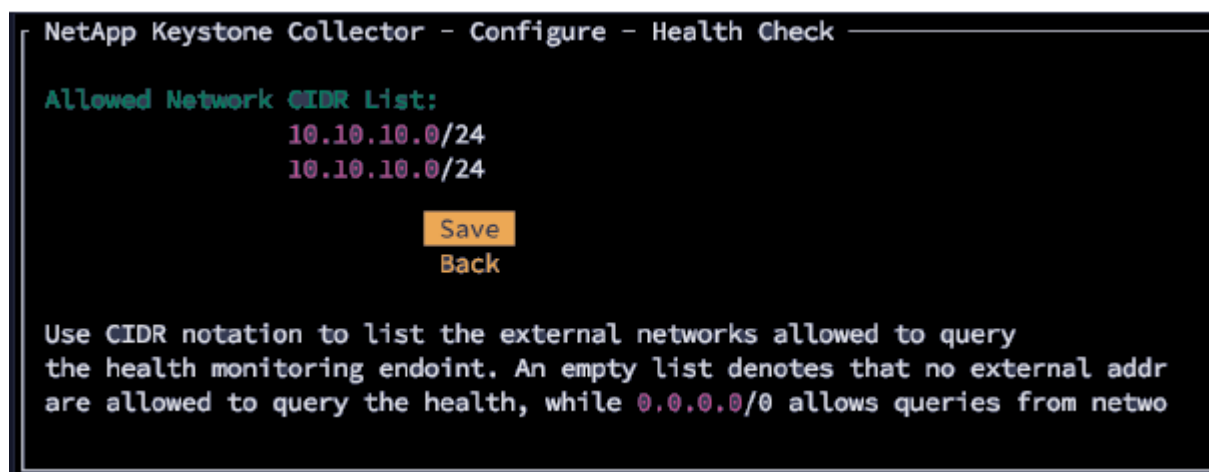
Par défaut, les services de santé Keystone n'acceptent pas les connexions provenant d'une adresse IP autre que localhost. Le critère d'évaluation de la santé Keystone est `/uber/health`, et il écoute sur toutes les interfaces du serveur Keystone Collector sur le port 7777. Lors de la requête, un code 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**.

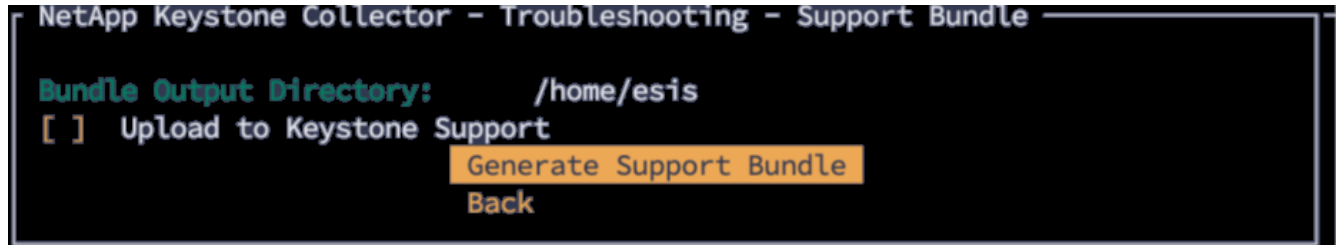


Générer et collecter des lots de support

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](#)".

Informations sur le copyright

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

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

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

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

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

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

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

Informations sur les marques commerciales

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