Keystone en modo privado

Keystone

NetApp
January 15, 2026

Tabla de contenidos

Keystone en modo privado

Conozca Keystone (modo privado)

Keystone ofrece un modo de implementación *privado*, también conocido como *sitio oscuro*, para satisfacer sus requisitos comerciales y de seguridad. Este modo está disponible para organizaciones con restricciones de conectividad.

NetApp ofrece una implementación especializada de Keystone STaaS diseñada para entornos con conectividad a Internet limitada o nula (también conocidos como sitios oscuros). Se trata de entornos seguros o aislados donde la comunicación externa está restringida debido a requisitos de seguridad, cumplimiento u operativos.

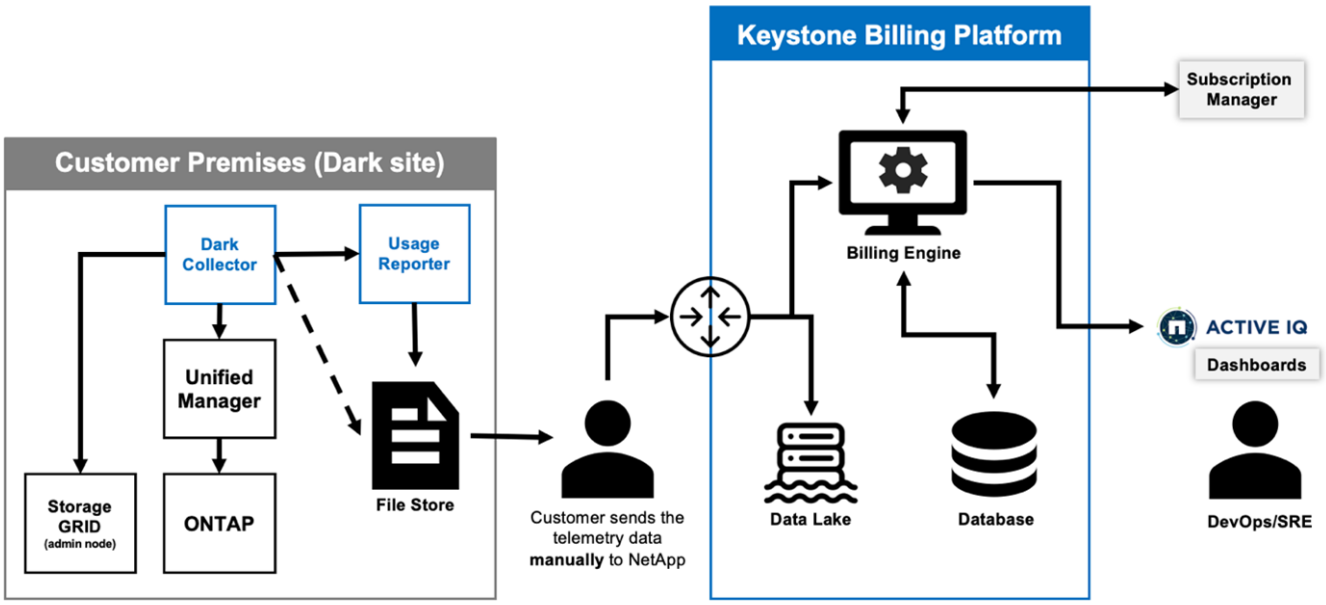
Para NetApp Keystone, ofrecer servicios para sitios oscuros significa proporcionar el servicio de suscripción de almacenamiento flexible de Keystone de una manera que respete las limitaciones de estos entornos. Esto implica:

- **Implementación local**: Keystone se puede configurar dentro de entornos aislados de forma independiente, lo que garantiza que no se necesita conectividad a Internet ni personal externo para acceder a la configuración.
- **Operaciones sin conexión**: Todas las capacidades de gestión de almacenamiento con controles de estado y facturación están disponibles sin conexión para las operaciones.
- **Seguridad y cumplimiento**: Keystone garantiza que la implementación cumpla con los requisitos de seguridad y cumplimiento de los sitios oscuros, que pueden incluir cifrado avanzado, controles de acceso seguros y capacidades de auditoría detalladas.
- **Ayuda y soporte**: NetApp ofrece soporte global las 24 horas, los 7 días de la semana, con un administrador de éxito de Keystone dedicado asignado a cada cuenta para brindar asistencia y solución de problemas.

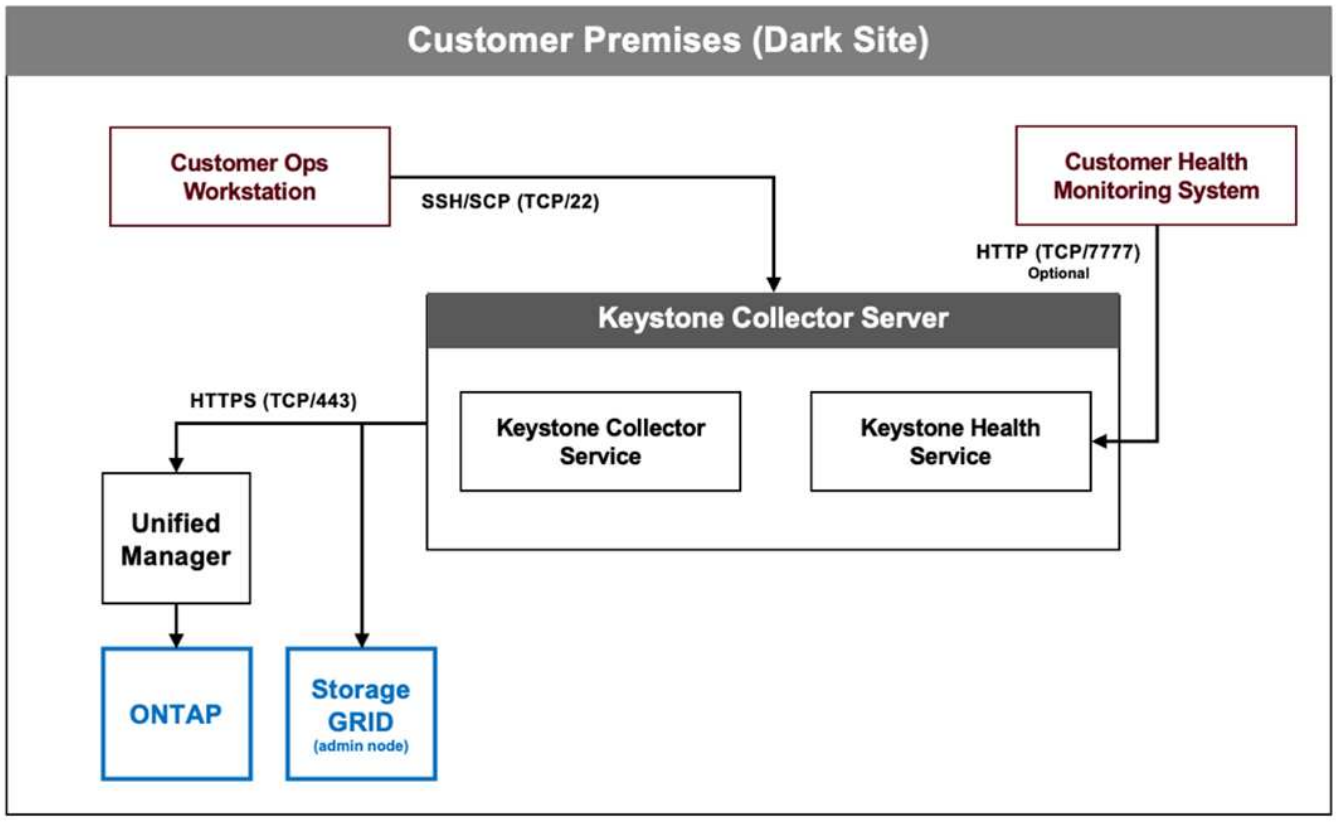
Keystone Collector se puede configurar sin restricciones de conectividad, también conocido como modo *estándar*. Para obtener más información, consulte"Obtenga más información sobre Keystone Collector" .

Keystone Collector en modo privado

Keystone Collector es responsable de recopilar periódicamente datos de uso de los sistemas de almacenamiento y exportar las métricas a un generador de informes de uso sin conexión y a un almacén de archivos local. Los archivos generados, que se crean en formatos cifrados y de texto simple, son luego enviados manualmente a NetApp por el usuario después de las comprobaciones de validación. Al recibirlos, la plataforma de facturación Keystone de NetApp autentica y procesa estos archivos, integrándolos en los sistemas de facturación y gestión de suscripciones para calcular los cargos mensuales.



El servicio Keystone Collector en el servidor tiene la tarea de recopilar periódicamente datos de uso, procesar esta información y generar un archivo de uso localmente en el servidor. El servicio de salud realiza controles del estado del sistema y está diseñado para interactuar con los sistemas de monitoreo de la salud utilizados por el cliente. Estos informes están disponibles para que los usuarios accedan a ellos sin conexión, lo que permite la validación y ayuda en la resolución de problemas.



Prepárese para la instalación de Keystone Collector en modo privado

Antes de instalar Keystone Collector en un entorno sin acceso a Internet, también conocido como *sitio oscuro* o *modo privado*, asegúrese de que sus sistemas estén preparados con el software necesario y cumplan con todos los requisitos previos requeridos.

Requisitos para VMware vSphere

- Sistema operativo: servidor VMware vCenter y ESXi 8.0 o posterior
- Núcleo: 1 CPU
- RAM: 2 GB
- Espacio en disco: 20 GB vDisk

Requisitos para Linux

- Sistema operativo (elija uno):
  - Red Hat Enterprise Linux (RHEL) 8.6 o cualquier versión posterior de la serie 8.x
  - Red Hat Enterprise Linux 9.0 o versiones posteriores
  - Debian 12
- Núcleo: 2 CPU
- RAM: 4 GB
- Espacio en disco: 50 GB vDisk
  - Al menos 2 GB libres en `/var/lib/`
  - Al menos 48 GB libres en `/opt/netapp`

El mismo servidor también debe tener instalados los siguientes paquetes de terceros. Si están disponibles a través del repositorio, estos paquetes se instalarán automáticamente como requisitos previos:

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - hombre de pod
  - llamada de socorro
  - yum-utils
  - Bloqueo de versión del complemento DNF de Python3
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - hombre de pod
  - llamada de socorro
  - yum-utils

    - Bloqueo de versión del complemento DNF de Python3
- Debian v12
    - python3 >= v3.9.0, python3 <= v3.12.0
    - hombre de pod
    - informe de sos

Requisitos de red

Los requisitos de red para Keystone Collector incluyen lo siguiente:

- Active IQ Unified Manager (Unified Manager) 9.10 o posterior, configurado en un servidor con la funcionalidad API Gateway habilitada.
- El servidor de Unified Manager debe ser accesible a través del servidor Keystone Collector en el puerto 443 (HTTPS).
- Se debe configurar una cuenta de servicio con permisos de usuario de aplicación para Keystone Collector en el servidor Unified Manager.
- No se requiere conectividad a Internet externa.
- Cada mes, exporte un archivo desde Keystone Collector y envíelo por correo electrónico al equipo de soporte de NetApp . Para obtener más información sobre cómo contactar con el equipo de soporte, consulte "Obtenga ayuda con Keystone".

Instalar Keystone Collector en modo privado

Complete unos pocos pasos para instalar Keystone Collector en un entorno que no tenga acceso a Internet, también conocido como *sitio oscuro* o *modo privado*. Este tipo de instalación es perfecta para sus sitios seguros.

Puede implementar Keystone Collector en sistemas VMware vSphere o instalarlo en sistemas Linux, según sus requisitos. Siga los pasos de instalación que correspondan a su opción seleccionada.

Implementar en VMware vSphere

Siga estos pasos:

1. Descargue el archivo de plantilla OVA desde "Portal web de NetApp Keystone" .
2. Para conocer los pasos para implementar el recopilador Keystone con el archivo OVA, consulte la sección"Implementación de la plantilla OVA" .

Instalar en Linux

El software Keystone Collector se instala en el servidor Linux utilizando los archivos .deb o .rpm proporcionados, según la distribución de Linux.

Siga estos pasos para instalar el software en su servidor Linux:

1. Descargue o transfiera el archivo de instalación de Keystone Collector al servidor Linux:

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

2. Abra una terminal en el servidor y ejecute los siguientes comandos para comenzar la instalación.
   - **Usando el paquete Debian**

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

   - **Usando archivo RPM**

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

     o

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

3. Ingresar `y` cuando se le solicite instalar el paquete.

Configurar Keystone Collector en modo privado

Complete algunas tareas de configuración para permitir que Keystone Collector recopile datos de uso en un entorno que no tiene acceso a Internet, también conocido como *sitio oscuro* o *modo privado*. Esta es una actividad única para activar y asociar los componentes necesarios con su entorno de almacenamiento. Una vez configurado, Keystone Collector supervisará todos los clústeres ONTAP administrados por Active IQ Unified Manager.

Keystone Collector le proporciona la utilidad de interfaz de usuario de terminal (TUI) de administración de Keystone Collector para realizar actividades de configuración y monitoreo. Puede utilizar varios controles del teclado, como Enter y las teclas de flecha, para seleccionar las opciones y navegar por esta TUI.

Pasos

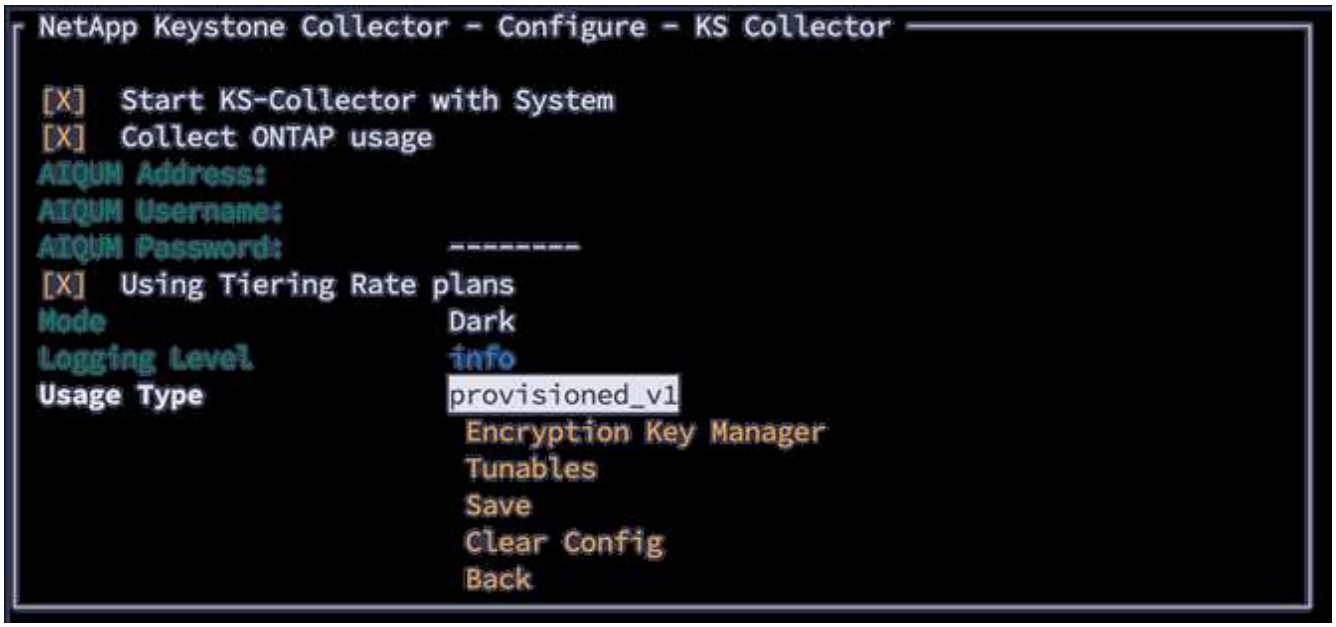
1. Inicie la utilidad TUI de administración de Keystone Collector:

   ```
   keystone-collector-tui
   ```

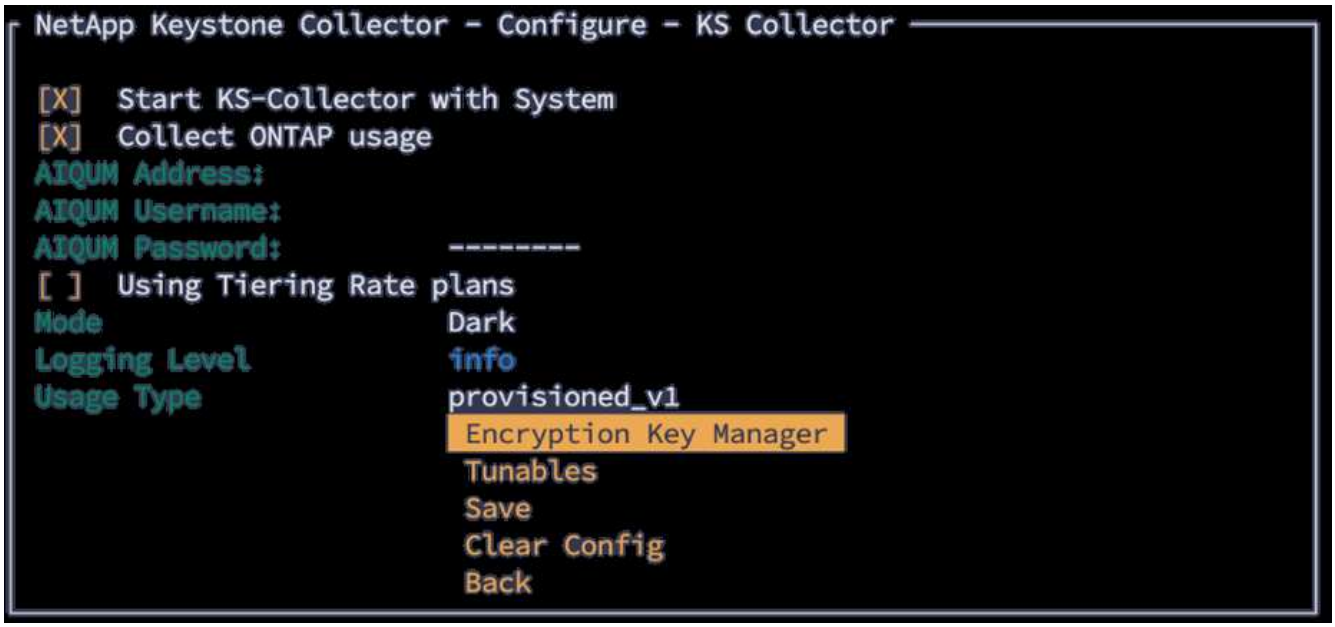
2. Vaya a **Configurar > Avanzado**.
3. Activa o desactiva la opción **Modo Darksite**.

4. Seleccione **Guardar**.
5. Vaya a **Configurar > KS-Collector** para configurar Keystone Collector.
6. Activa o desactiva el campo **Iniciar recopilador de KS con el sistema**.
7. Activa o desactiva el campo *Recopilar uso de ONTAP *. Agregue los detalles del servidor y la cuenta de usuario de Active IQ Unified Manager (Unified Manager).
8. **Opcional**: Active el campo **Usar planes de tarifas por niveles** si se requiere niveles de datos para la suscripción.
9. Según el tipo de suscripción adquirida, actualice el **Tipo de uso**.

> Antes de configurar, confirme el tipo de uso asociado con la suscripción de NetApp.

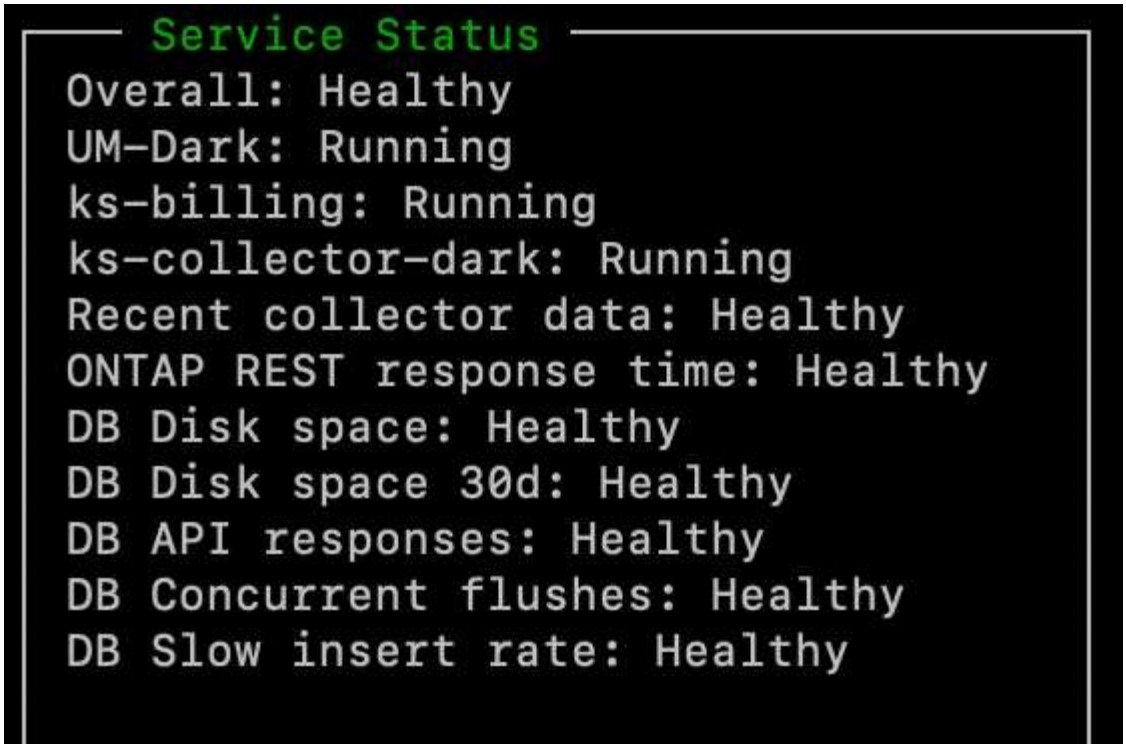


10. Seleccione **Guardar**.
11. Vaya a **Configurar > KS-Collector** para generar el par de claves de Keystone Collector.
12. Vaya a **Administrador de claves de cifrado** y presione Enter.



13. Seleccione **Generar par de claves de recopilador** y presione Entrar.

14. Asegúrese de que el Keystone Collector se encuentre en buen estado volviendo a la pantalla principal de la TUI y verificando la información de **Estado del servicio**. El sistema debe mostrar que los servicios están en un estado general **saludable**. Espere hasta 10 minutos. Si el estado general continúa siendo incorrecto después de este período, revise los pasos de configuración anteriores y comuníquese con el equipo de soporte de NetApp .



15. Salga de la TUI de administración de Keystone Collector seleccionando la opción **Salir a Shell** en la pantalla de inicio.
16. Recupere la clave pública generada:

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

17. Envíe un correo electrónico con este archivo a ng-keystone-secure-site-upload@netapp.com para sitios seguros que no sean de USPS, o a ng-keystone-secure-site-usps-upload@netapp.com para sitios seguros de USPS.

Informe de uso de exportación

Debe enviar el informe de resumen de uso mensual a NetApp al final de cada mes. Puede generar este informe manualmente.

Siga estos pasos para generar el informe de uso:

1. Vaya a **Uso de exportación** en la pantalla de inicio de TUI de Keystone Collector.
2. Recopile los archivos y envíelos a ng-keystone-secure-site-upload@netapp.com para sitios seguros que no sean de USPS, o a ng-keystone-secure-site-usps-upload@netapp.com para sitios seguros de USPS.

   Keystone Collector genera un archivo claro y un archivo cifrado, que debe enviarse manualmente a NetApp. El informe de archivo claro contiene los siguientes detalles que pueden ser validados por el cliente.

```
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-----
```

Actualizar ONTAP

Keystone Collector admite actualizaciones de ONTAP a través de TUI.

Siga estos pasos para actualizar ONTAP:

1. Vaya a *Mantenimiento > Servidor web de actualización de ONTAP *.
2. Copie el archivo de imagen de actualización de ONTAP en **/opt/netapp/ontap-upgrade/**, luego seleccione **Iniciar servidor web** para iniciar el servidor web.

3. Ir a `http://<collector-ip>:8000` utilizando un navegador web para obtener asistencia con la actualización.

Reiniciar Keystone Collector

Puede reiniciar el servicio Keystone Collector a través de la TUI. Vaya a **Mantenimiento > Reiniciar servicios del recopilador** en la TUI. Esto reiniciará todos los servicios del recopilador, y su estado se podrá monitorear desde la pantalla de inicio de TUI.

Supervisar el estado del recopilador Keystone en modo privado

Puede supervisar el estado de Keystone Collector mediante cualquier sistema de supervisión que admita solicitudes HTTP.

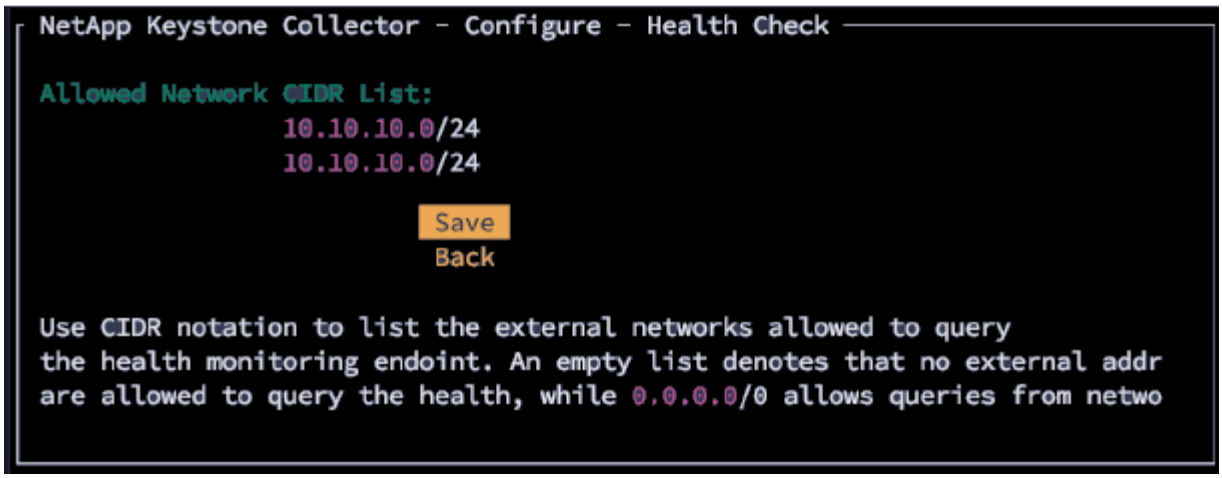
De forma predeterminada, los servicios de salud de Keystone no aceptan conexiones desde ninguna IP que no sea localhost. El punto final de salud de Keystone es `/uber/health` , y escucha en todas las interfaces del servidor Keystone Collector en el puerto `7777` . Cuando se realiza una consulta, se devuelve un código de estado de solicitud HTTP con una salida JSON desde el punto final como respuesta, que describe el estado del sistema Keystone Collector. El cuerpo JSON proporciona un estado de salud general del `is_healthy` atributo, que es un valor booleano; y una lista detallada de estados por componente para el `component_details` atributo. He aquí un ejemplo:

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

Se devuelven estos códigos de estado:

- **200**: indica que todos los componentes monitoreados están en buen estado
- **503**: indica que uno o más componentes no están en buen estado
- **403**: indica que el cliente HTTP que consulta el estado de salud no está en la lista *permitida*, que es una lista de CIDR de red permitidos. Para este estado no se devuelve ninguna información de salud.

  La lista *permitir* utiliza el método CIDR de red para controlar qué dispositivos de red tienen permitido consultar el sistema de salud de Keystone . Si recibe el error 403, agregue su sistema de monitoreo a la lista *permitida* desde * Keystone Collector management TUI > Configurar > Monitoreo de estado*.

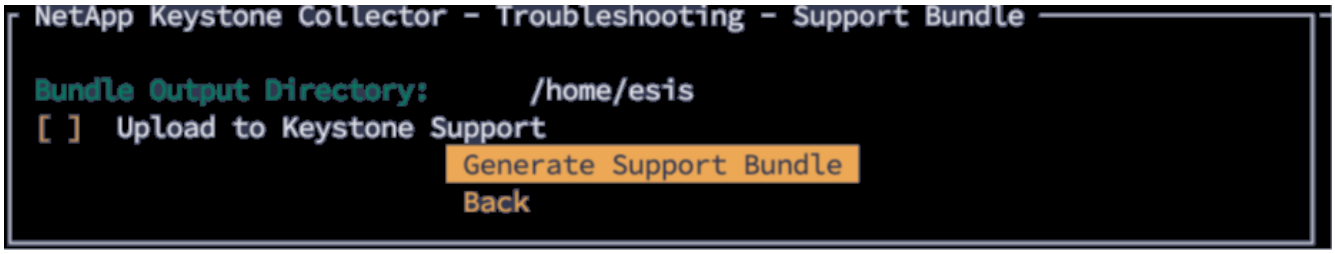


Generar y recopilar paquetes de soporte

Para solucionar problemas con Keystone Collector, puede trabajar con el soporte de NetApp, quienes podrían solicitarle un archivo *.tar*. Puede generar este archivo a través de la utilidad TUI de administración de Keystone Collector.

Siga estos pasos para generar un archivo *.tar*:

1. Vaya a **Solución de problemas > Generar paquete de soporte**.
2. Seleccione la ubicación para guardar el paquete y luego haga clic en **Generar paquete de soporte**.



   Este proceso crea una `tar` paquete en la ubicación mencionada que se puede compartir con NetApp para solucionar problemas.

3. Una vez descargado el archivo, puedes adjuntarlo al ticket de soporte de Keystone ServiceNow. Para obtener información sobre cómo recaudar fondos, consulte "Generación de solicitudes de servicio".