Configurar y configurar Keystone

Keystone

NetApp
January 15, 2026

Tabla de contenidos

Configurar y configurar Keystone

Requisitos

Requisitos de infraestructura virtual para Keystone Collector

Su sistema VMware vSphere debe cumplir varios requisitos antes de poder instalar Keystone Collector.

Requisitos previos para la máquina virtual del servidor Keystone Collector:

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

Otros requisitos

Asegúrese de que se cumplan los siguientes requisitos genéricos:

Requisitos de red

Los requisitos de red de Keystone Collector se enumeran en la siguiente tabla.

Keystone Collector requiere conectividad a Internet. Puede proporcionar conectividad a Internet mediante enrutamiento directo a través del Gateway predeterminado (a través de NAT) o a través de Proxy HTTP. Aquí se describen ambas variantes.

Fuente	Destino	Servicio	Protocolo y puertos	Categoría	Objetivo
Colector Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Administrador unificado)	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone ONTAP)	Recopilación de métricas de uso de Keystone Collector para ONTAP
Colector Keystone (para Keystone StorageGRID)	Nodos de administración de StorageGRID	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone StorageGRID)	Recopilación de métricas de uso de Keystone Collector para StorageGRID

Coleccionista Keystone (genérico)	Internet (según los requisitos de URL que se indican más adelante)	HTTPS	TCP 443	Obligatorio (conectividad a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Coleccionista Keystone (genérico)	Proxy HTTP del cliente	Proxy HTTP	Puerto proxy del cliente	Obligatorio (conectividad a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Coleccionista Keystone (genérico)	Servidores DNS del cliente	DNS	TCP/UDP 53	Obligatorio	Resolución de DNS
Coleccionista Keystone (genérico)	Servidores NTP del cliente	NTP	UDP 123	Obligatorio	Sincronización horaria
Colector Keystone (para Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	Funcionalidad opcional	Recopilación de métricas de rendimiento para Keystone Collector
Coleccionista Keystone (genérico)	Sistema de Monitoreo de Clientes	HTTPS	TCP 7777	Funcionalidad opcional	Informes de estado de Keystone Collector
Estaciones de trabajo de operaciones del cliente	Coleccionista de Keystone	SSH	TCP 22	Gestión	Acceso a la gestión de recopiladores Keystone
Direcciones de administración de nodos y clústeres de NetApp ONTAP	Coleccionista de Keystone	HTTP_8000, PING	TCP 8000, solicitud/respuesta de eco ICMP	Funcionalidad opcional	Servidor web para actualizaciones de firmware de ONTAP

El puerto predeterminado para MySQL, 3306, está restringido solo al host local durante una nueva instalación de Unified Manager, lo que impide la recopilación de métricas de rendimiento para Keystone Collector. Para obtener más información, consulte "Requisitos de ONTAP" .

Acceso URL

Keystone Collector necesita acceso a los siguientes hosts de Internet:

DIRECCIÓN	Razón
https://keystone.netapp.com	Actualizaciones del software Keystone Collector e informes de uso
https://support.netapp.com	Sede de NetApp para información de facturación y entrega de AutoSupport

Requisitos de Linux para Keystone Collector

Preparar su sistema Linux con el software necesario garantiza una instalación precisa y la recopilación de datos por parte de Keystone Collector.

Asegúrese de que su servidor Linux y la máquina virtual Keystone Collector tengan estas configuraciones.

Servidor Linux:

- Sistema operativo: cualquiera de los siguientes:
  - Debian 12
  - Red Hat Enterprise Linux 8.6 o versiones posteriores 8.x
  - Red Hat Enterprise Linux 9.0 o versiones posteriores
  - CentOS 7 (solo para entornos existentes)
- Tiempo cronológico sincronizado
- Acceso a los repositorios de software estándar de Linux

El mismo servidor también debe tener los siguientes paquetes de terceros:

- podman (Administrador de POD)
- llamada de socorro
- cronicidad
- Python 3 (3.9.14 a 3.11.8)

Máquina virtual del servidor Keystone Collector:

- Núcleo: 2 CPU
- RAM: 4 GB de RAM
- Espacio en disco: 50 GB vDisk

Otros requisitos

Asegúrese de que se cumplan los siguientes requisitos genéricos:

Requisitos de red

Los requisitos de red de Keystone Collector se enumeran en la siguiente tabla.

> Keystone Collector requiere conectividad a Internet. Puede proporcionar conectividad a Internet mediante enrutamiento directo a través del Gateway predeterminado (a través de NAT) o a través de Proxy HTTP. Aquí se describen ambas variantes.

Fuente	Destino	Servicio	Protocolo y puertos	Categoría	Objetivo
Colector Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Administrador unificado)	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone ONTAP)	Recopilación de métricas de uso de Keystone Collector para ONTAP
Colector Keystone (para Keystone StorageGRID)	Nodos de administración de StorageGRID	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone StorageGRID)	Recopilación de métricas de uso de Keystone Collector para StorageGRID
Coleccionista Keystone (genérico)	Internet (según los requisitos de URL que se indican más adelante)	HTTPS	TCP 443	Obligatorio (conectividad a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Coleccionista Keystone (genérico)	Proxy HTTP del cliente	Proxy HTTP	Puerto proxy del cliente	Obligatorio (conectividad a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Coleccionista Keystone (genérico)	Servidores DNS del cliente	DNS	TCP/UDP 53	Obligatorio	Resolución de DNS

Coleccionista Keystone (genérico)	Servidores NTP del cliente	NTP	UDP 123	Obligatorio	Sincronización horaria
Colector Keystone (para Keystone ONTAP)	Unified Manager	MySQL	TCP 3306	Funcionalidad opcional	Recopilación de métricas de rendimiento para Keystone Collector
Coleccionista Keystone (genérico)	Sistema de Monitoreo de Clientes	HTTPS	TCP 7777	Funcionalidad opcional	Informes de estado de Keystone Collector
Estaciones de trabajo de operaciones del cliente	Coleccionista de Keystone	SSH	TCP 22	Gestión	Acceso a la gestión de recopiladores Keystone
Direcciones de administración de nodos y clústeres de NetApp ONTAP	Coleccionista de Keystone	HTTP_8000, PING	TCP 8000, solicitud/respuesta de eco ICMP	Funcionalidad opcional	Servidor web para actualizaciones de firmware de ONTAP

El puerto predeterminado para MySQL, 3306, está restringido solo al host local durante una nueva instalación de Unified Manager, lo que impide la recopilación de métricas de rendimiento para Keystone Collector. Para obtener más información, consulte "Requisitos de ONTAP" .

Acceso URL

Keystone Collector necesita acceso a los siguientes hosts de Internet:

DIRECCIÓN	Razón
https://keystone.netapp.com	Actualizaciones del software Keystone Collector e informes de uso
https://support.netapp.com	Sede de NetApp para información de facturación y entrega de AutoSupport

Requisitos para ONTAP y StorageGRID para Keystone

Antes de comenzar a utilizar Keystone, debe asegurarse de que los clústeres ONTAP y los sistemas StorageGRID cumplan algunos requisitos.

ONTAP

Versiones de software

1. ONTAP 9.8 o posterior
2. Active IQ Unified Manager (Unified Manager) 9.10 o posterior

Antes de empezar

Cumpla con los siguientes requisitos si desea recopilar datos de uso únicamente a través de ONTAP:

1. Asegúrese de que ONTAP 9.8 o posterior esté configurado. Para obtener información sobre cómo configurar un nuevo clúster, consulte estos enlaces:
   - "Configurar ONTAP en un nuevo clúster con el Administrador del sistema"
   - "Configurar un clúster con la CLI"
2. Cree cuentas de inicio de sesión de ONTAP con roles específicos. Para obtener más información, consulte "Obtenga información sobre cómo crear cuentas de inicio de sesión de ONTAP" .
   - **Interfaz web**
     i. Inicie sesión en ONTAP System Manager utilizando sus credenciales predeterminadas. Para obtener más información, consulte "Gestión de clústeres con System Manager" .
     ii. Cree un usuario de ONTAP con el rol de "solo lectura" y el tipo de aplicación "http", y habilite la autenticación de contraseña navegando a **Clúster > Configuración > Seguridad > Usuarios**.
   - **CLI**
     i. Inicie sesión en ONTAP CLI con sus credenciales predeterminadas. Para obtener más información, consulte "Gestión de clústeres con CLI" .
     ii. Cree un usuario ONTAP con el rol de “solo lectura” y el tipo de aplicación “http”, y habilite la autenticación de contraseña. Para obtener más información sobre la autenticación, consulte "Habilitar el acceso con contraseña a la cuenta ONTAP" .

Cumpla los siguientes requisitos si desea recopilar datos de uso a través de Active IQ Unified Manager:

1. Asegúrese de que Unified Manager 9.10 o posterior esté configurado. Para obtener información sobre la instalación de Unified Manager, consulte estos enlaces:
   - "Instalación de Unified Manager en sistemas VMware vSphere"
   - "Instalación de Unified Manager en sistemas Linux"
2. Asegúrese de que el clúster ONTAP se haya agregado a Unified Manager. Para obtener información sobre cómo agregar clústeres, consulte "Añadiendo clústeres" .
3. Cree usuarios de Unified Manager con roles específicos para la recopilación de datos de uso y rendimiento. Realice estos pasos. Para obtener información sobre los roles de usuario, consulte "Definiciones de roles de usuario" .
   a. Inicie sesión en la interfaz de usuario web de Unified Manager con las credenciales de usuario administrador de aplicaciones predeterminadas que se generan durante la instalación. Ver "Acceder a la interfaz web de Unified Manager" .
   b. Cree una cuenta de servicio para Keystone Collector con `Operator` Rol de usuario. Las API del servicio Keystone Collector utilizan esta cuenta de servicio para comunicarse con Unified Manager y recopilar datos de uso. Ver "Agregar usuarios" .
   c. Crear una `Database` cuenta de usuario, con la `Report Schema` role. Este usuario es necesario

para la recopilación de datos de rendimiento. Ver "Creación de un usuario de base de datos" .

> El puerto predeterminado para MySQL, 3306, está restringido solo al host local durante una nueva instalación de Unified Manager, lo que impide la recopilación de datos de rendimiento para Keystone ONTAP. Esta configuración se puede modificar y la conexión se puede poner a disposición de otros hosts mediante el `Control access to MySQL port 3306` opción en la consola de mantenimiento de Unified Manager. Para obtener más información, consulte"Opciones de menú adicionales" .

4. Habilitar API Gateway en Unified Manager. Keystone Collector utiliza la función API Gateway para comunicarse con los clústeres ONTAP . Puede habilitar API Gateway desde la interfaz de usuario web o ejecutando algunos comandos a través de la CLI de Unified Manager.

   Interfaz web

   Para habilitar API Gateway desde la interfaz de usuario web de Unified Manager, inicie sesión en la interfaz de usuario web de Unified Manager y habilite API Gateway. Para obtener más información, consulte "Habilitación de API Gateway" .

   CLI

   Para habilitar API Gateway a través de la CLI de Unified Manager, siga estos pasos:

   a. En el servidor de Unified Manager, inicie una sesión SSH e inicie sesión en la CLI de Unified Manager.
   `um cli login -u <umadmin>` Para obtener información sobre los comandos CLI, consulte "Comandos CLI de Unified Manager compatibles" .

   b. Verifique si API Gateway ya está habilitado.
   `um option list api.gateway.enabled` A `true` El valor indica que API Gateway está habilitado.

   c. Si el valor devuelto es `false` , ejecute este comando:
   `um option set api.gateway.enabled=true`

   d. Reinicie el servidor de Unified Manager:
      - Linux: "Reiniciar Unified Manager" .
      - VMware vSphere: "Reinicio de la máquina virtual de Unified Manager" .

StorageGRID

Las siguientes configuraciones son necesarias para instalar Keystone Collector en StorageGRID.

- StorageGRID `11.6.0` o posterior debe instalarse. Para obtener información sobre cómo actualizar StorageGRID, consulte"Actualización del software StorageGRID : descripción general" .
- Se debe crear una cuenta de usuario administrador local de StorageGRID para la recopilación de datos de uso. El servicio Keystone Collector utiliza esta cuenta de servicio para comunicarse con StorageGRID a través de las API del nodo de administrador.

  Pasos

  a. Inicie sesión en el Administrador de cuadrícula. Ver "Sign in en el Administrador de cuadrícula" .

  b. Crea un grupo de administradores locales con `Access mode: Read-only` . Ver "Crear un grupo de administradores" .

  c. Añade los siguientes permisos:

- Cuentas de inquilinos
- Mantenimiento
- Consulta de métricas

d. Cree un usuario de cuenta de servicio Keystone y asócielo con el grupo de administración. Ver "Administrar usuarios" .

Instalar Keystone Collector

Implementar Keystone Collector en sistemas VMware vSphere

La implementación de Keystone Collector en sistemas VMware vSphere incluye la descarga de la plantilla OVA, la implementación de la plantilla mediante el asistente **Implementar plantilla OVF**, la verificación de la integridad de los certificados y la verificación de la preparación de la máquina virtual.

Implementación de la plantilla OVA

Siga estos pasos:

Pasos

1. Descargue el archivo OVA desde "este enlace" y guárdelo en su sistema VMware vSphere.
2. En su sistema VMware vSphere, navegue a la vista **VMs and Templates**.
3. Haga clic con el botón derecho en la carpeta requerida para la máquina virtual (VM) (o centro de datos, si no utiliza carpetas de VM) y seleccione **Implementar plantilla OVF**.
4. En el *Paso 1* del asistente **Implementar plantilla OVF**, haga clic en **Seleccionar una plantilla OVF** para seleccionar la plantilla descargada. `KeystoneCollector-latest.ova` archivo.
5. En el *Paso 2*, especifique el nombre de la VM y seleccione la carpeta de la VM.
6. En el *Paso 3*, especifique el recurso computacional requerido para ejecutar la máquina virtual.
7. En el *Paso 4: Revisar detalles*, verifique la exactitud y autenticidad del archivo OVA.

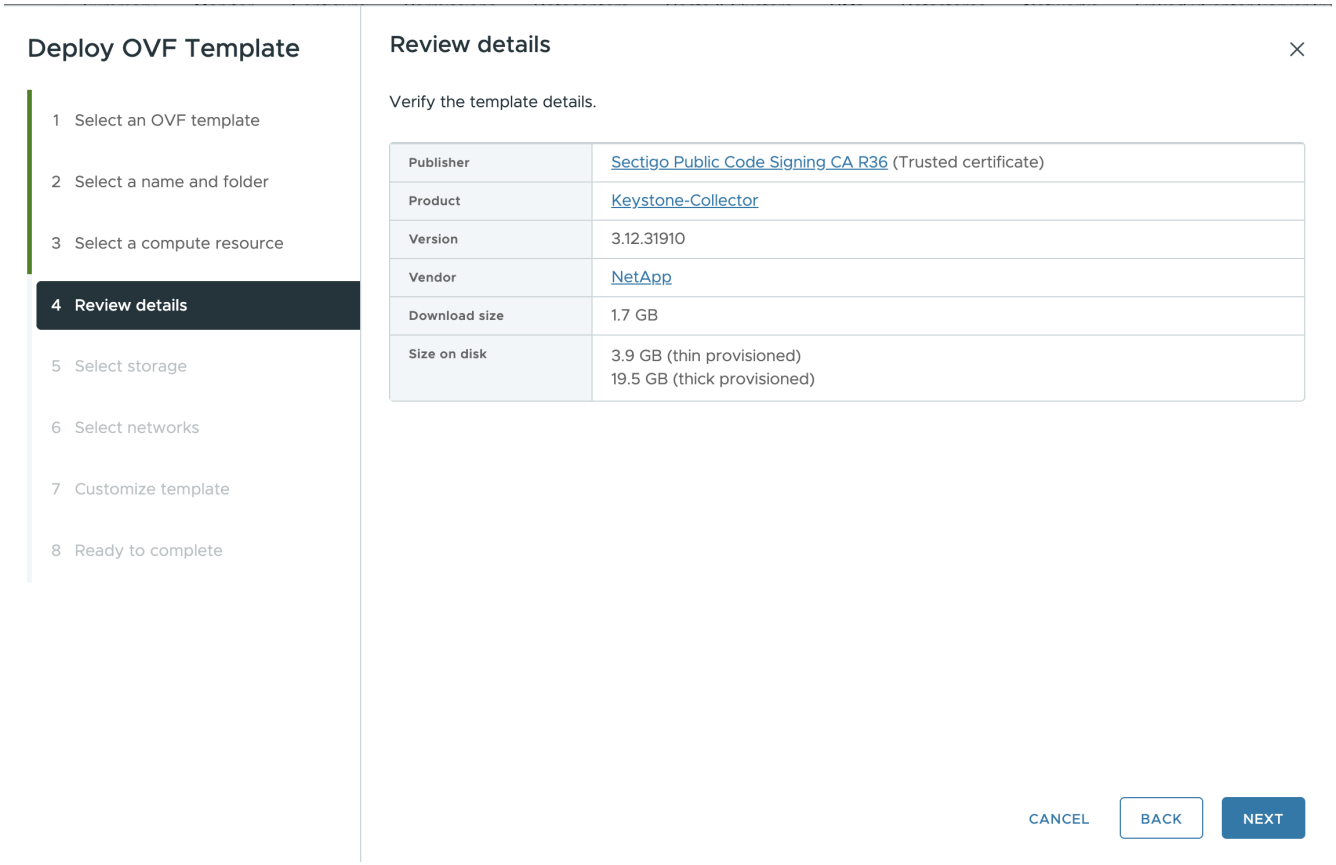
   El almacén de confianza raíz de vCenter contiene únicamente certificados de VMware. NetApp utiliza Entrust como autoridad de certificación y esos certificados deben agregarse al almacén de confianza de vCenter.

   a. Descarga el certificado de CA de firma de código de Sectigo. "aquí".

   b. Siga los pasos de la `Resolution` Sección de este artículo de la base de conocimientos (KB): https://kb.vmware.com/s/article/84240 .

   > Para las versiones 7.x y anteriores de vCenter, debe actualizar vCenter y ESXi a la versión 8.0 o posterior. Las versiones anteriores ya no reciben soporte.

   Cuando se valide la integridad y autenticidad del OVA de Keystone Collector, podrá ver el texto. `(Trusted certificate)` con la editorial.



8. En el *Paso 5* del asistente **Implementar plantilla OVF**, especifique la ubicación para almacenar la máquina virtual.
9. En el *Paso 6*, seleccione la red de destino que utilizará la máquina virtual.
10. En el *Paso 7 Personalizar plantilla*, especifique la dirección de red inicial y la contraseña para la cuenta de usuario administrador.

> La contraseña de administrador se almacena en un formato reversible en vCentre y debe usarse como credencial de arranque para obtener acceso inicial al sistema VMware vSphere. Durante la configuración inicial del software, esta contraseña de administrador debe cambiarse. La máscara de subred para la dirección IPv4 debe proporcionarse en notación CIDR. Por ejemplo, utilice el valor 24 para una máscara de subred de 255.255.255.0.

11. En el *Paso 8 Listo para completar* del asistente **Implementar plantilla OVF**, revise la configuración y verifique que haya configurado correctamente los parámetros para la implementación de OVA.

Una vez implementada la VM desde la plantilla y encendida, abra una sesión SSH en la VM e inicie sesión con las credenciales de administrador temporales para verificar que la VM esté lista para la configuración.

Configuración inicial del sistema

Realice estos pasos en sus sistemas VMware vSphere para una configuración inicial de los servidores Keystone Collector implementados a través de OVA:

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

1. Abra una sesión SSH en el servidor Keystone Collector. Cuando se conecte, el sistema le solicitará que actualice la contraseña de administrador. Complete la actualización de la contraseña de administrador según sea necesario.
2. Inicie sesión con la nueva contraseña para acceder a la TUI. Al iniciar sesión, aparece la TUI.

   Alternativamente, puede iniciarlo manualmente ejecutando el `keystone-collector-tui` Comando CLI.
3. Si es necesario, configure los detalles del proxy en la sección **Configuración > Red** en la TUI.
4. Configure el nombre de host del sistema, la ubicación y el servidor NTP en la sección **Configuración > Sistema**.
5. Actualice los recopiladores Keystone mediante la opción **Mantenimiento > Actualizar recopiladores**. Después de la actualización, reinicie la utilidad TUI de administración de Keystone Collector para aplicar los cambios.

Instalar Keystone Collector en sistemas Linux

Puede instalar el software Keystone Collector en un servidor Linux usando un RPM o un paquete Debian. Siga los pasos de instalación según su distribución de Linux.

Usando RPM

1. Conéctese por SSH al servidor Keystone Collector y elévelo a `root` privilegio.
2. Importe la firma pública de Keystone :
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. Asegúrese de que se ha importado el certificado público correcto comprobando la huella digital de Keystone Billing Platform en la base de datos RPM:
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint` La huella dactilar correcta tiene este aspecto:
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Descarga el `keystonerepo.rpm` archivo:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Verifique la autenticidad del archivo:
   `rpm --checksig -v keystonerepo.rpm` La firma de un archivo auténtico tiene este aspecto:
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. Instale el archivo del repositorio de software YUM:
   `# yum install keystonerepo.rpm`
7. Cuando se instala el repositorio de Keystone , instala el paquete keystone-collector a través del administrador de paquetes YUM:

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

   Para Red Hat Enterprise Linux 9, ejecute el siguiente comando para instalar el paquete keystone-collector:
   `# yum install keystone-collector-rhel9`

Usando Debian

1. Conéctese por SSH al servidor Keystone Collector y elévelo a `root` privilegio.
   `sudo su`
2. Descargar el `keystone-sw-repo.deb` archivo:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Instale el archivo del repositorio de software de Keystone :
   `# dpkg -i keystone-sw-repo.deb`
4. Actualizar la lista de paquetes:
   `# apt-get update`
5. Cuando se instale el repositorio de Keystone , instale el paquete keystone-collector:
   `# apt-get install keystone-collector`

Una vez completada la instalación, puede utilizar la utilidad de interfaz de usuario del terminal (TUI) de administración de Keystone Collector para realizar las actividades de configuración y supervisión. Puede utilizar varios controles del teclado, como Enter y las teclas de flecha, para seleccionar las opciones y navegar por esta TUI. Ver"Configurar Keystone Collector" y"Monitorear la salud del sistema" para información.

Validación automática del software Keystone

El repositorio de Keystone está configurado para validar automáticamente la integridad del software de Keystone para que solo se instale software válido y auténtico en su sitio.

La configuración del cliente del repositorio Keystone YUM proporcionada en `keystonerepo.rpm` hace uso de la comprobación GPG forzada(`gpgcheck=1`) en todo el software descargado a través de este repositorio. Cualquier RPM descargado a través del repositorio Keystone que no pase la validación de firma no podrá instalarse. Esta funcionalidad se utiliza en la capacidad de actualización automática programada de Keystone Collector para garantizar que solo se instale software válido y auténtico en su sitio.

Configurar Keystone Collector

Debe completar algunas tareas de configuración para permitir que Keystone Collector recopile datos de uso en su entorno de almacenamiento. Esta es una actividad única para activar y asociar los componentes necesarios con su entorno de almacenamiento.

- 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.
- Keystone Collector se puede configurar para organizaciones que no tienen acceso a Internet, también conocido como *sitio oscuro* o *modo privado*. Para obtener más información, consulte"Keystone en modo privado" .

Pasos

1. Inicie la utilidad TUI de administración de Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vaya a **Configurar > KS-Collector** para abrir la pantalla de configuración de Keystone Collector para ver las opciones disponibles para la actualización.
3. Actualice las opciones requeridas.

   Para ONTAP

   - *Recopilar uso de ONTAP *: esta opción habilita la recopilación de datos de uso de ONTAP. Agregue los detalles del servidor y la cuenta de servicio de Active IQ Unified Manager (Unified Manager).
   - *Recopilar datos de rendimiento de ONTAP *: esta opción habilita la recopilación de datos de rendimiento de ONTAP. Esta opción está desactivada de forma predeterminada. Habilite esta opción si se requiere monitoreo del rendimiento en su entorno para fines de SLA. Proporcione los detalles de la cuenta de usuario de la base de datos de Unified Manager. Para obtener información sobre la creación de usuarios de bases de datos, consulte"Crear usuarios de Unified Manager" .
   - **Eliminar datos privados**: esta opción elimina datos privados específicos de los clientes y está habilitada de forma predeterminada. Para obtener información sobre qué datos se excluyen de las métricas si esta opción está habilitada, consulte"Limitar la recopilación de datos privados" .

Para StorageGRID

- *Recopilar uso de StorageGRID *: esta opción habilita la recopilación de detalles de uso del nodo. Agregue la dirección del nodo StorageGRID y los detalles del usuario.
- **Eliminar datos privados**: esta opción elimina datos privados específicos de los clientes y está habilitada de forma predeterminada. Para obtener información sobre qué datos se excluyen de las métricas si esta opción está habilitada, consulte"Limitar la recopilación de datos privados" .

4. Activa o desactiva el campo **Iniciar KS-Collector con el sistema**.
5. Haga clic en **Guardar**

6. Asegúrese de que 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**

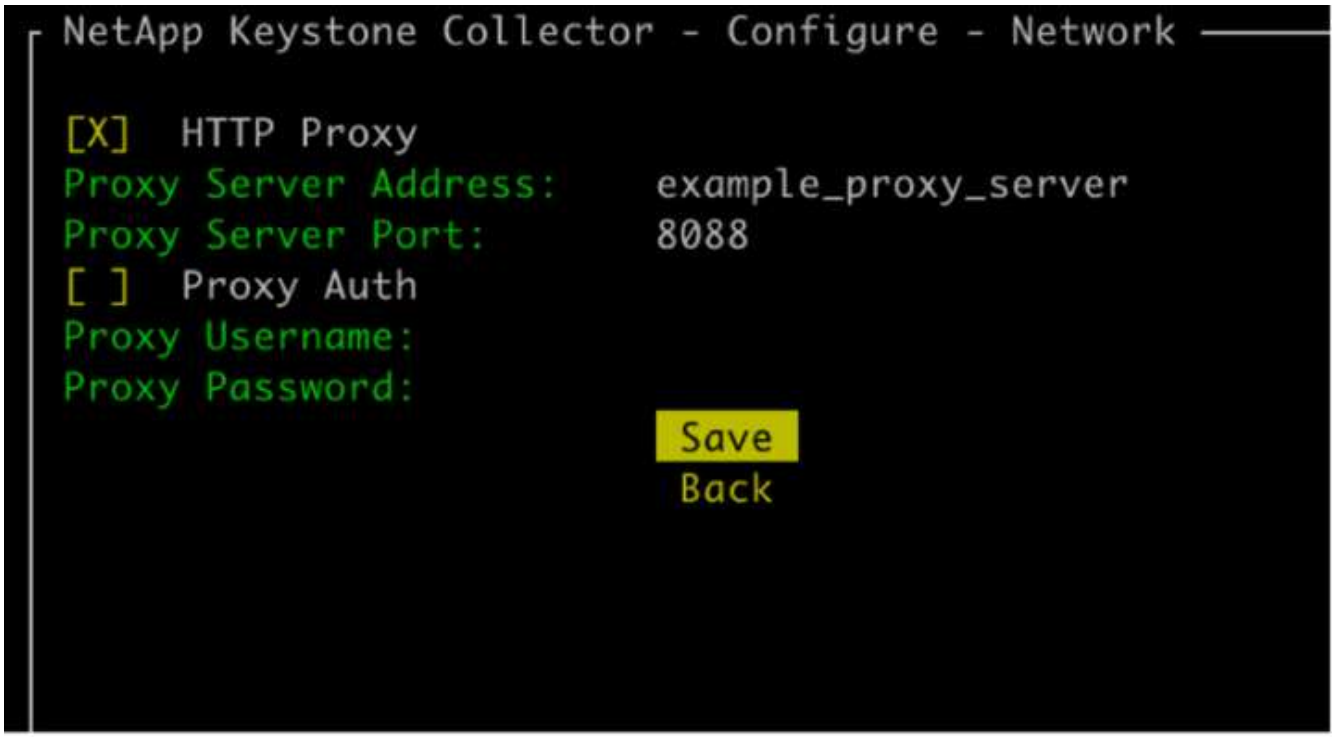
7. Salga de la TUI de administración de Keystone Collector seleccionando la opción **Salir a Shell** en la pantalla de inicio.

Configurar el proxy HTTP en Keystone Collector

El software Collector admite el uso de un proxy HTTP para comunicarse con Internet. Esto se puede configurar en la TUI.

Pasos

1. Reinicie la utilidad TUI de administración de Keystone Collector si ya está cerrada:
   ```
   $ keystone-collector-tui
   ```
2. Active el campo **Proxy HTTP** y agregue los detalles del servidor proxy HTTP, el puerto y las credenciales, si se requiere autenticación.
3. Haga clic en **Guardar**
   .



Limitar la recopilación de datos privados

Keystone Collector recopila información limitada de configuración, estado y rendimiento necesaria para realizar la medición de suscripciones. Existe una opción para limitar aún más la información recopilada enmascarando la información confidencial del contenido cargado. Esto no afecta el cálculo de la facturación. Sin embargo, limitar la información puede afectar la usabilidad de la información del informe, ya que algunos elementos que los usuarios pueden identificar fácilmente, como el nombre del volumen, se reemplazan con UUID.

Limitar la recopilación de datos específicos de clientes es una opción configurable en la pantalla TUI de Keystone Collector. Esta opción, **Eliminar datos privados**, está habilitada de forma predeterminada.

Para obtener información sobre los elementos eliminados al limitar el acceso a datos privados tanto en ONTAP como en StorageGRID, consulte"Lista de elementos eliminados al limitar el acceso a datos privados" .

Confíe en una CA raíz personalizada

La verificación de certificados contra una autoridad de certificación raíz pública (CA) es parte de las características de seguridad de Keystone Collector. Sin embargo, si es necesario, puede configurar Keystone Collector para que confíe en una CA raíz personalizada.

Si utiliza la inspección SSL/TLS en el firewall de su sistema, el tráfico basado en Internet se volverá a cifrar con su certificado CA personalizado. Es necesario configurar los ajustes para verificar la fuente como una CA confiable antes de aceptar el certificado raíz y permitir que se produzcan conexiones. Siga estos pasos:

Pasos

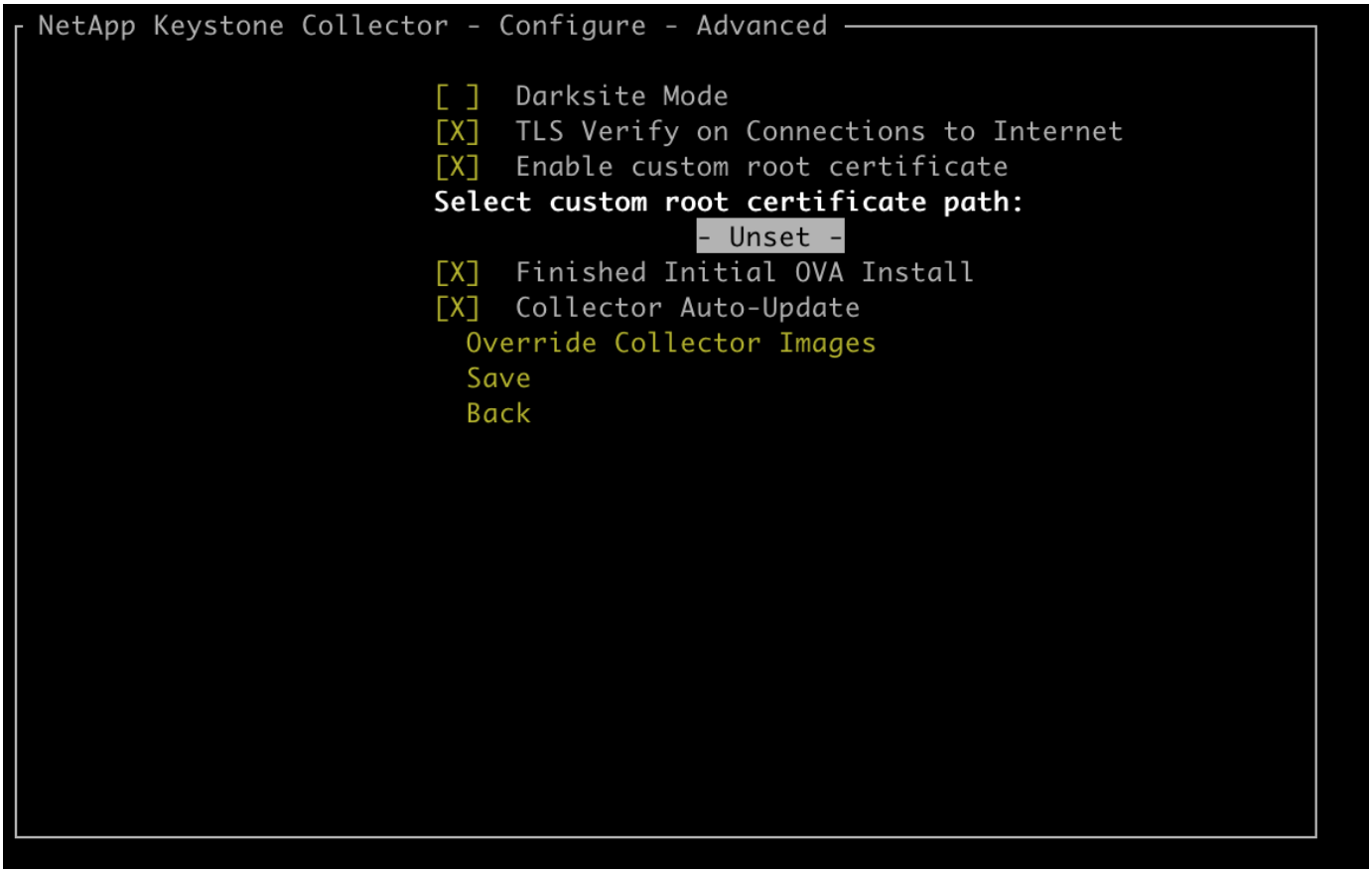
1. Preparar el certificado CA. Debe estar en formato de archivo *X.509 codificado en base64*.

   Las extensiones de archivo admitidas son `.pem` , `.crt` , `.cert` . Asegúrese de que el certificado esté en uno de estos formatos.

2. Copie el certificado al servidor Keystone Collector. Tome nota de la ubicación donde se copia el archivo.
3. Abra una terminal en el servidor y ejecute la utilidad de administración TUI.
   `$ keystone-collector-tui`
4. Vaya a **Configuración > Avanzada**.
5. Habilite la opción **Habilitar certificado raíz personalizado**.
6. Para **Seleccionar ruta de certificado raíz personalizado:**, seleccione `- Unset -`

7. Presione Enter. Se muestra un cuadro de diálogo para seleccionar la ruta del certificado.
8. Seleccione el certificado raíz desde el explorador del sistema de archivos o ingrese la ruta exacta.
9. Presione Enter. Regresarás a la pantalla **Avanzado**.
10. Seleccione **Guardar**. Se aplica la configuración.

El certificado de la CA se copia a `/opt/netapp/ks-collector/ca.pem` en el servidor Keystone Collector.



Crear niveles de servicio de rendimiento

Puede crear niveles de servicio de rendimiento (PSL) mediante la utilidad TUI de administración de Keystone Collector. La creación de PSL a través de TUI selecciona automáticamente los valores predeterminados establecidos para cada nivel de servicio de rendimiento, lo que reduce la posibilidad de errores que pueden ocurrir al configurar manualmente estos valores al crear PSL a través de Active IQ Unified Manager.

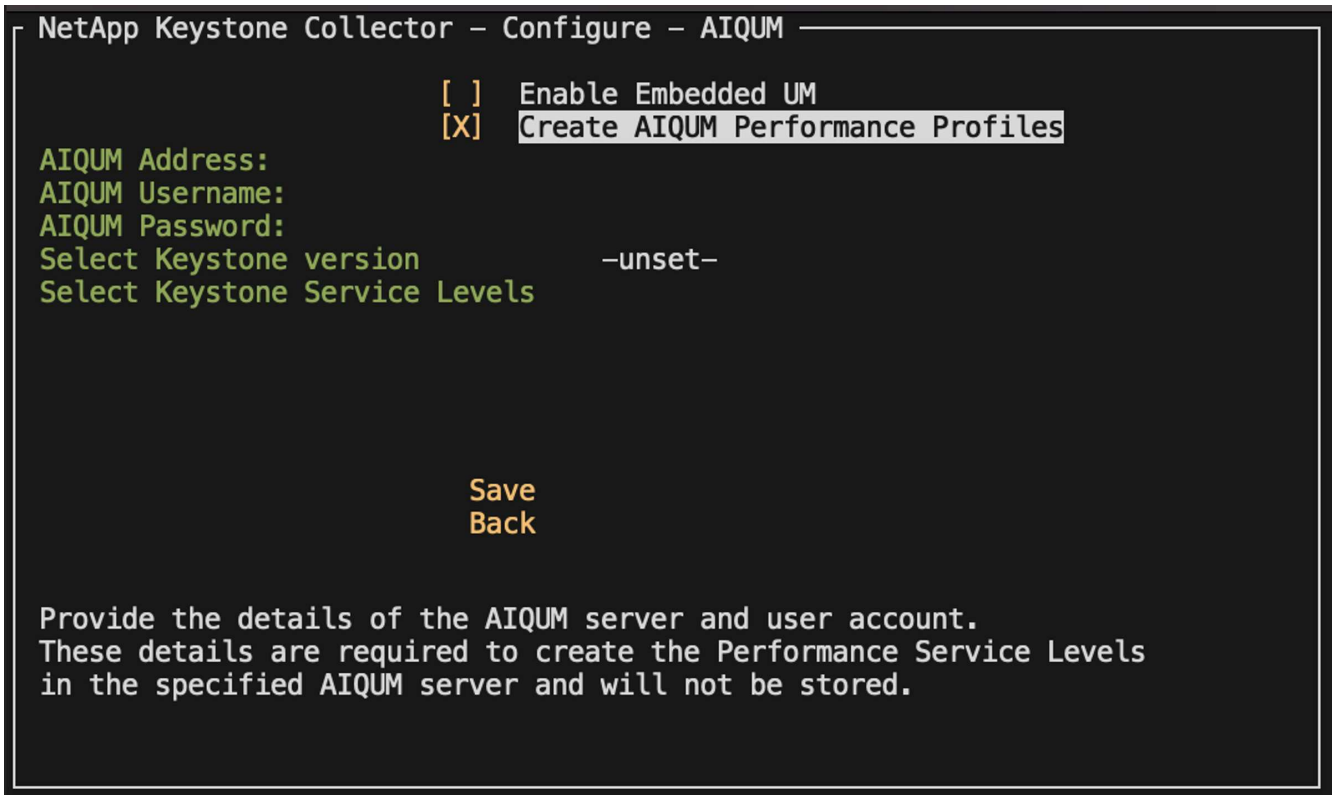
Para obtener más información sobre los PSL, consulte"Niveles de servicio de rendimiento" .

Para obtener más información sobre los niveles de servicio, consulte"Niveles de servicio en Keystone" .

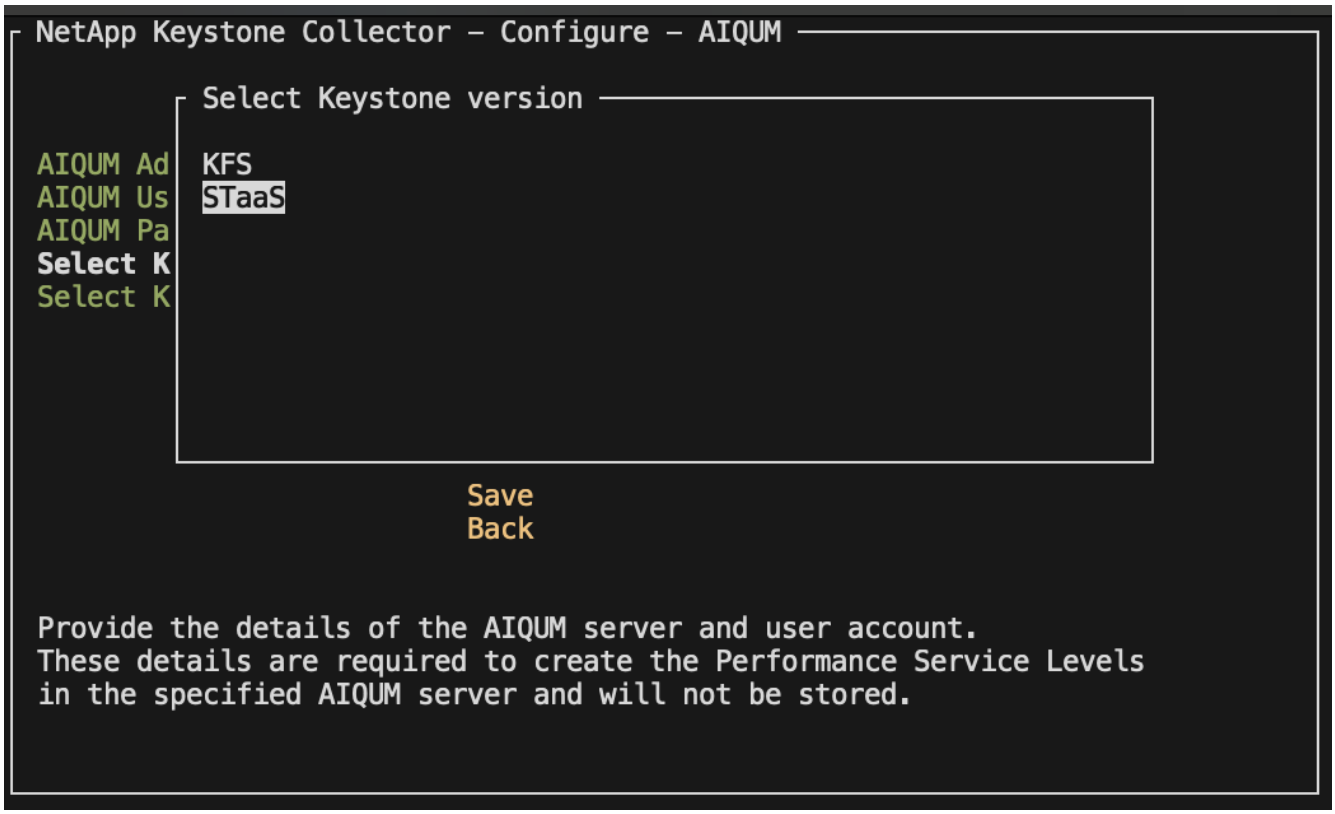
Pasos

1. Inicie la utilidad TUI de administración de Keystone Collector:
   `$ keystone-collector-tui`
2. Vaya a **Configurar>AIQUM** para abrir la pantalla AIQUM.
3. Habilite la opción **Crear perfiles de rendimiento AIQUM**.

4. Ingrese los detalles del servidor y la cuenta de usuario de Active IQ Unified Manager . Estos detalles son necesarios para crear PSL y no se almacenarán.

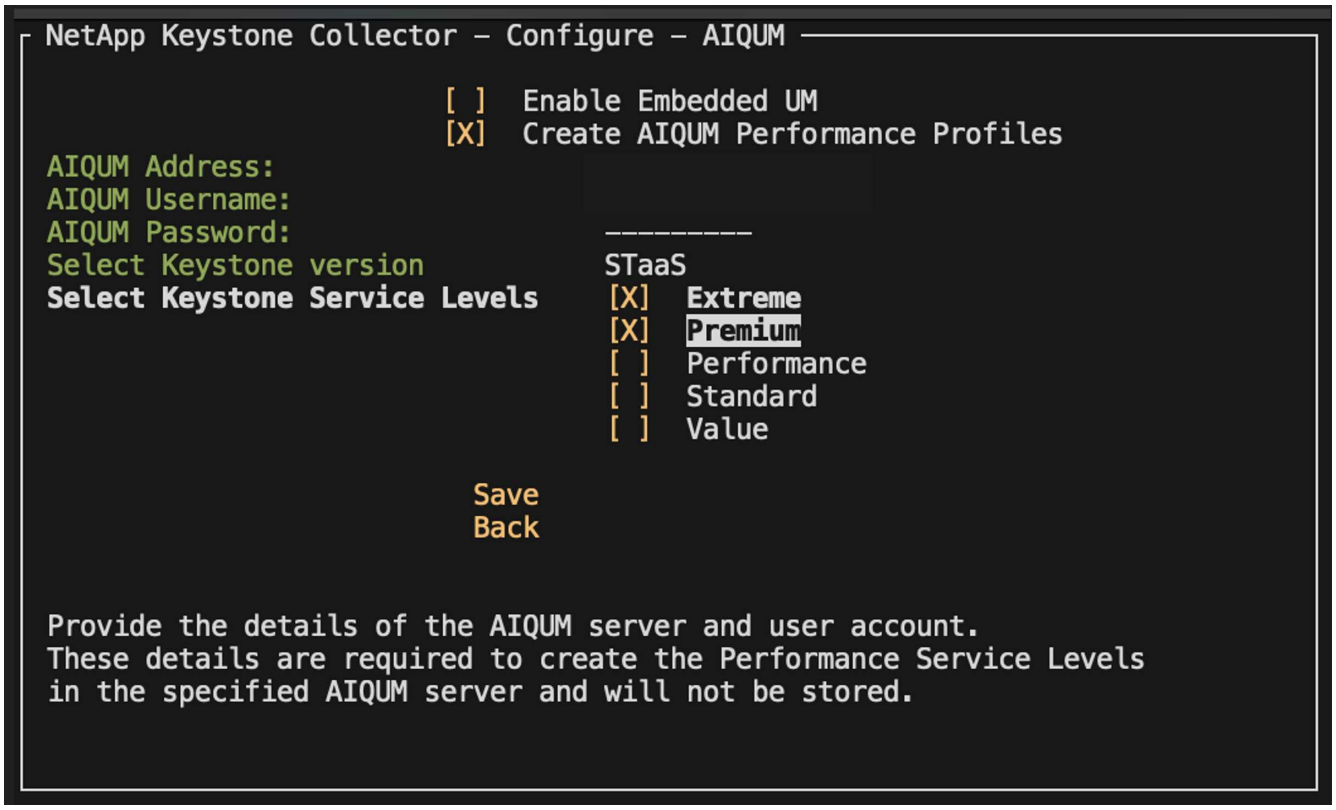


5. Para *Seleccionar versión de Keystone *, seleccione `-unset-` .
6. Presione Enter. Se muestra un cuadro de diálogo para seleccionar la versión de Keystone .
7. Resalte **STaaS** para especificar la versión de Keystone para Keystone STaaS y luego presione Entrar.



Puede resaltar la opción **KFS** para los servicios de suscripción de Keystone versión 1. Los servicios de suscripción de Keystone se diferencian de Keystone STaaS en los niveles de servicio de rendimiento constituyente, las ofertas de servicios y los principios de facturación. Para obtener más información, consulte"Servicios de suscripción de Keystone | Versión 1" .

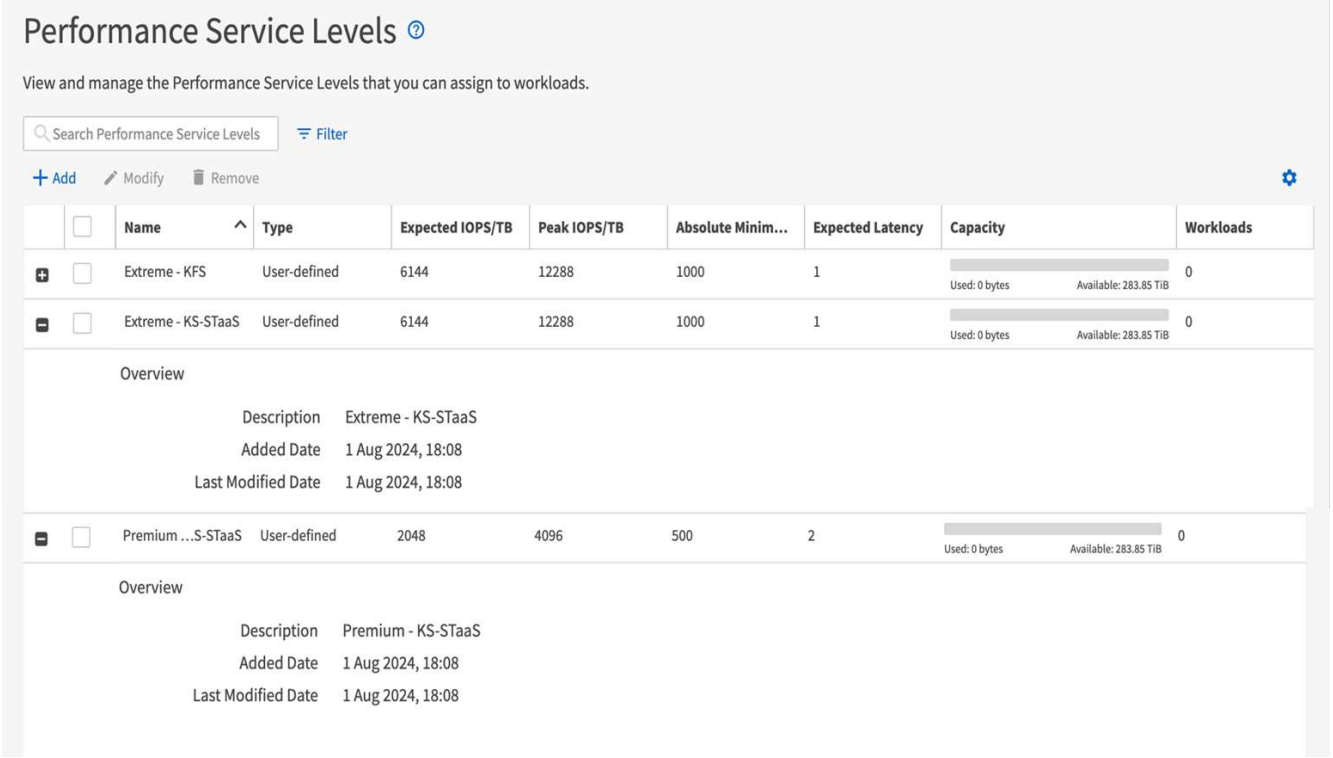
8. Todos los niveles de servicio de rendimiento de Keystone compatibles se mostrarán dentro de la opción *Seleccionar niveles de servicio de Keystone * para la versión de Keystone especificada. Habilite los niveles de servicio de rendimiento deseados de la lista.



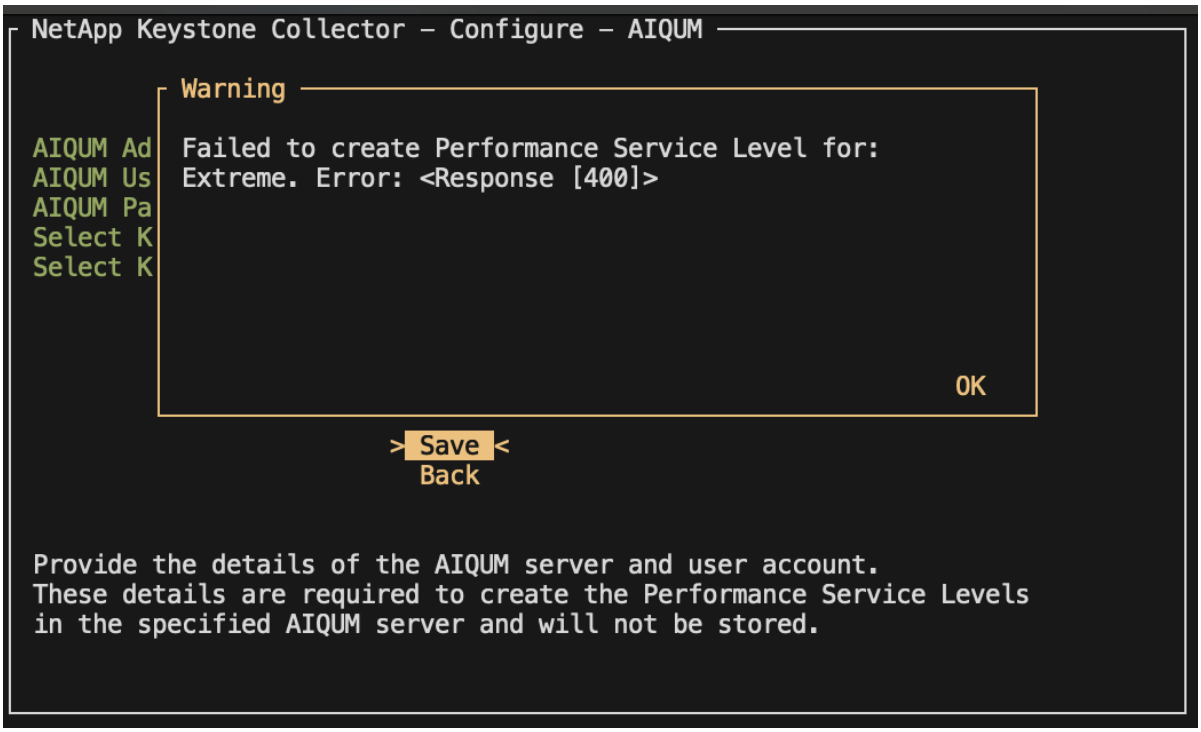
Puede seleccionar varios niveles de servicio de rendimiento simultáneamente para crear PSL.

9. Seleccione **Guardar** y presione Enter. Se crearán niveles de servicio de rendimiento.

   Puede ver los PSL creados, como Premium-KS-STaaS para STaaS o Extreme KFS para KFS, en la página **Niveles de servicio de rendimiento** en Active IQ Unified Manager. Si los PSL creados no cumplen con sus requisitos, puede modificarlos para satisfacer sus necesidades. Para obtener más información, consulte"Creación y edición de niveles de servicio de rendimiento" .



Si ya existe un PSL para el nivel de servicio de rendimiento seleccionado en el servidor Active IQ Unified Manager especificado, no podrá crearlo nuevamente. Si intenta hacerlo, recibirá un mensaje de
error.



Instalar ITOM Collector

Requisitos de instalación para Keystone ITOM Collector

Antes de instalar ITOM Collector, asegúrese de que sus sistemas estén preparados con el software necesario y cumplan con todos los requisitos previos requeridos.

Requisitos previos para la máquina virtual del servidor ITOM Collector:

- Sistemas operativos compatibles:
  - Debian 12 o posterior
  - Windows Server 2016 o posterior
  - Ubuntu 20.04 LTS o posterior
  - Red Hat Enterprise Linux (RHEL) 8.x
  - Red Hat Enterprise Linux 9.0 o posterior
  - Amazon Linux 2023 o posterior

> Los sistemas operativos recomendados son Debian 12, Windows Server 2016 o versiones más nuevas.

- Requisitos de recursos: los requisitos de recursos de la máquina virtual según la cantidad de nodos NetApp monitoreados son los siguientes:
  - 2-10 nodos: 4 CPU, 8 GB de RAM, 40 GB de disco
  - 12-20 nodos: 8 CPU, 16 GB de RAM, 40 GB de disco
- Requisito de configuración: asegúrese de que una cuenta de solo lectura y SNMP estén configurados en los dispositivos monitoreados. La máquina virtual del servidor ITOM Collector también debe configurarse como host de trampa SNMP y servidor Syslog en el clúster de NetApp y en los conmutadores de clúster, si corresponde.

Requisitos de red

Los requisitos de red de ITOM Collector se enumeran en la siguiente tabla.

Fuente	Destino	Protocolo	Puertos	Descripción
Coleccionista de ITOM	IP de administración de clústeres de NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Monitoreo de los controladores ONTAP
IP de administración de nodos y clústeres de NetApp ONTAP	Coleccionista de ITOM	SNMP, registro del sistema	UDP 162, UDP 514	Trampas SNMP y registros del sistema de los controladores
Coleccionista de ITOM	Conmutadores de clúster	SNMP	UDP 161	Monitoreo de interruptores
Conmutadores de clúster	Coleccionista de ITOM	SNMP, registro del sistema	UDP 162, UDP 514	Trampas SNMP y registros del sistema de los conmutadores
Coleccionista de ITOM	IP de nodos de StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitoreo SNMP de StorageGRID

IP de nodos de StorageGRID	Coleccionista de ITOM	SNMP, registro del sistema	UDP 162, UDP 514	Trampas SNMP de StorageGRID
Coleccionista de ITOM	Coleccionista de Keystone	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Monitoreo y gestión remota de Keystone Collector
Coleccionista de ITOM	DNS local	DNS	UDP 53	Servicios de DNS públicos o privados
Coleccionista de ITOM	Servidor(es) NTP de elección	NTP	UDP 123	Control del tiempo

Instalar Keystone ITOM Collector en sistemas Linux

Complete unos pocos pasos para instalar ITOM Collector, que recopila datos de métricas en su entorno de almacenamiento. Puede instalarlo en sistemas Windows o Linux, según sus requisitos.

El equipo de soporte de Keystone proporciona un enlace dinámico para descargar el archivo de instalación de ITOM Collector, que caduca en dos horas.

Para instalar ITOM Collector en sistemas Windows, consulte"Instalar ITOM Collector en sistemas Windows" .

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

Antes de empezar

- Verifique que el shell Bourne esté disponible para el script de instalación de Linux.
- Instalar el `vim-common` paquete para obtener el binario **xxd** requerido para el archivo de instalación de ITOM Collector.
- Asegúrese de que `sudo package` se instala si se planea ejecutar ITOM Collector como un usuario no root.

Pasos

1. Descargue el archivo de instalación del recopilador ITOM en su servidor Linux.
2. Abra una terminal en el servidor y ejecute el siguiente comando para cambiar los permisos y hacer que los binarios sean ejecutables:
   `# chmod +x <installer_file_name>.bin`
3. Ejecute el comando para iniciar el archivo de instalación del recopilador ITOM:
   `#./<installer_file_name>.bin`
4. Al ejecutar el archivo de instalación se le solicitará que:
   a. Acepte el acuerdo de licencia de usuario final (EULA).
   b. Introduzca los datos de usuario para la instalación.
   c. Especifique el directorio principal de instalación.
   d. Seleccione el tamaño del colector.
   e. Proporcione detalles del proxy, si corresponde.

   Para cada solicitud, se muestra una opción predeterminada. Se recomienda seleccionar la opción

predeterminada a menos que tenga requisitos específicos. Presione la tecla **Enter** para elegir la opción predeterminada. Cuando se complete la instalación, aparecerá un mensaje que confirmará que ITOM Collector se instaló correctamente.

- El archivo de instalación de ITOM Collector realiza adiciones a `/etc/sudoers` para manejar reinicios de servicio y volcados de memoria.
- La instalación de ITOM Collector en el servidor Linux crea un usuario predeterminado llamado **ITOM** para ejecutar ITOM Collector sin privilegios de root. Puede elegir un usuario diferente o ejecutarlo como root, pero se recomienda utilizar el usuario ITOM creado por el script de instalación de Linux.

¿Que sigue?

Luego de una instalación exitosa, comuníquese con el equipo de soporte de Keystone para validar la instalación exitosa de ITOM Collector a través del portal de soporte de ITOM. Después de la verificación, el equipo de soporte de Keystone configurará ITOM Collector de forma remota, incluida la configuración adicional de detección y monitoreo del dispositivo, y enviará una confirmación una vez que se complete la configuración. Para cualquier consulta o información adicional, comuníquese con keystone.services@netapp.com.

Instalar Keystone ITOM Collector en sistemas Windows

Instale ITOM Collector en un sistema Windows descargando el archivo de instalación de ITOM Collector, ejecutando el asistente InstallShield e ingresando las credenciales de monitoreo necesarias.

El equipo de soporte de Keystone proporciona un enlace dinámico para descargar el archivo de instalación de ITOM Collector, que caduca en dos horas.

Puede instalarlo en sistemas Linux según sus necesidades. Para instalar ITOM Collector en sistemas Linux, consulte"Instalar ITOM Collector en sistemas Linux" .

Siga estos pasos para instalar el software ITOM Collector en su servidor Windows:

Antes de empezar

Asegúrese de que el servicio ITOM Collector tenga concedido **Iniciar sesión como servicio** en Política local/Asignación de derechos de usuario en la configuración de política de seguridad local del servidor Windows.

Pasos

1. Descargue el archivo de instalación del recopilador ITOM en su servidor Windows.
2. Abra el archivo de instalación para iniciar el asistente InstallShield.
3. Acepte el acuerdo de licencia de usuario final (EULA). El asistente InstallShield extrae los binarios necesarios y le solicita que ingrese las credenciales.
4. Introduzca las credenciales de la cuenta bajo la cual se ejecutará ITOM Collector:
   - Si ITOM Collector no está supervisando otros servidores Windows, utilice el sistema local.
   - Si ITOM Collector está supervisando otros servidores Windows en el mismo dominio, use una cuenta de dominio con permisos de administrador local.
   - Si ITOM Collector está supervisando otros servidores Windows que no forman parte del mismo

dominio, utilice una cuenta de administrador local y conéctese a cada recurso con credenciales de administrador local. Puede optar por configurar la contraseña para que no caduque, para reducir los problemas de autenticación entre ITOM Collector y sus recursos monitoreados.

5. Seleccione el tamaño del colector. El valor predeterminado es el tamaño recomendado según el archivo de configuración. Continúe con el tamaño sugerido a menos que tenga requisitos específicos.
6. Seleccione *Siguiente* para comenzar la instalación. Puedes utilizar la carpeta completa o elegir una diferente. Un cuadro de estado muestra el progreso de la instalación, seguido por el cuadro de diálogo Asistente de instalación completado.

¿Que sigue?

Luego de una instalación exitosa, comuníquese con el equipo de soporte de Keystone para validar la instalación exitosa de ITOM Collector a través del portal de soporte de ITOM. Después de la verificación, el equipo de soporte de Keystone configurará ITOM Collector de forma remota, incluida la configuración adicional de detección y monitoreo del dispositivo, y enviará una confirmación una vez que se complete la configuración. Para cualquier consulta o información adicional, comuníquese con keystone.services@netapp.com.

Configurar AutoSupport para Keystone

Al utilizar el mecanismo de telemetría de AutoSupport , Keystone calcula el uso en función de los datos de telemetría de AutoSupport . Para lograr el nivel de granularidad necesario, debe configurar AutoSupport para incorporar datos de Keystone en los paquetes de soporte diarios enviados por los clústeres de ONTAP .

Acerca de esta tarea

Debe tener en cuenta lo siguiente antes de configurar AutoSupport para incluir datos de Keystone .

- Puede editar las opciones de telemetría de AutoSupport mediante la CLI de ONTAP . Para obtener información sobre la administración de los servicios de AutoSupport y la función de administrador del sistema (clúster), consulte "Descripción general de Administrar AutoSupport" y "Administradores de clústeres y SVM" .
- Incluye los subsistemas en los paquetes de AutoSupport diarios y semanales para garantizar una recopilación de datos precisa para Keystone. Para obtener información sobre los subsistemas de AutoSupport , consulte "¿Qué son los subsistemas de AutoSupport ?" .

Pasos

1. Como usuario administrador del sistema, inicie sesión en el clúster Keystone ONTAP mediante SSH. Para obtener más información, consulte "Acceda al clúster mediante SSH" .
2. Modificar el contenido del registro.
    - Para ONTAP 9.16.1 y superior, ejecute este comando para modificar el contenido del registro diario:

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

      Si el clúster está en una configuración MetroCluster , ejecute este comando:

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

- Para versiones anteriores de ONTAP , ejecute este comando para modificar el contenido del registro diario:

```
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 el clúster está en una configuración MetroCluster , ejecute este comando:

```
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
```

- Ejecute este comando para modificar el contenido del registro semanal:

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

Para obtener más información sobre este comando, consulte "Modificación del activador de soporte automático del nodo del sistema" .

Monitorizar y actualizar

Supervisar la salud de Keystone Collector

Puede supervisar el estado de Keystone Collector mediante cualquier sistema de supervisión que admita solicitudes HTTP. Monitorear la salud puede ayudar a garantizar que los datos estén disponibles en el panel de Keystone .

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 este error, agregue su sistema de monitoreo a la lista *permitida* desde * Keystone Collector management TUI > Configurar > Monitoreo de estado*.

> **Usuarios de Linux, tengan en cuenta este problema conocido:**
>
> **Descripción del problema**: Keystone Collector ejecuta una serie de contenedores como parte del sistema de medición de uso. Cuando el servidor Red Hat Enterprise Linux 8.x se fortalece con las políticas de las Guías de implementación técnica de seguridad (STIG) de la Agencia de sistemas de información de defensa de los EE. UU. (DISA), se ha observado de manera intermitente un problema conocido con fapolicyd (demonio de política de acceso a archivos). Este problema se identifica como"error 1907870" . **Solución alternativa**: hasta que Red Hat Enterprise lo resuelva, NetApp recomienda que solucione este problema instalando `fapolicyd` en modo permisivo. En/`etc/fapolicyd/fapolicyd.conf` , establece el valor de `permissive = 1` .

Ver registros del sistema

Puede ver los registros del sistema de Keystone Collector para revisar la información del sistema y solucionar problemas mediante esos registros. Keystone Collector utiliza el sistema de registro *journald* del host, y los registros del sistema se pueden revisar a través de la utilidad del sistema estándar *journalctl*. Puede utilizar los siguientes servicios clave para examinar los registros:

- colector ks
- ks-salud
- actualización automática de ks

El servicio principal de recopilación de datos *ks-collector* produce registros en formato JSON con un `run-id` atributo asociado con cada trabajo de recopilación de datos programado. El siguiente es un ejemplo de un trabajo exitoso para la recopilación de datos de uso estándar:

```
{"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"}
```


El siguiente es un ejemplo de un trabajo exitoso para la recopilación de datos de desempeño opcional:

```
{"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"}
```

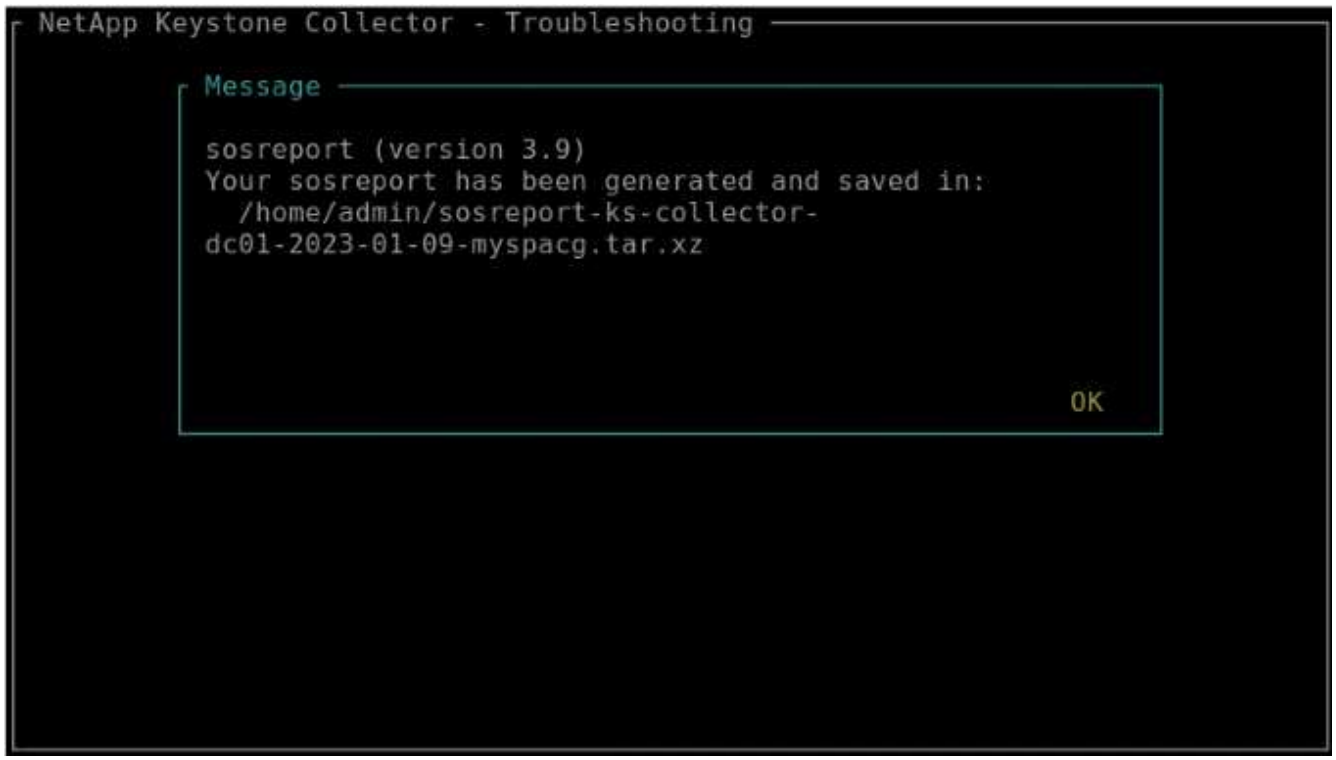
Generar y recopilar paquetes de soporte

La interfaz de usuario (TUI) de Keystone Collector le permite generar paquetes de soporte y agregarlos a solicitudes de servicio para resolver problemas de soporte. Siga este procedimiento:

Pasos

1. Inicie la utilidad TUI de administración de Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vaya a **Solución de problemas > Generar paquete de soporte**
   .

3. Cuando se genera, se muestra la ubicación donde se guarda el paquete. Utilice FTP, SFTP o SCP para conectarse a la ubicación y descargar el archivo de registro a un sistema
   local.



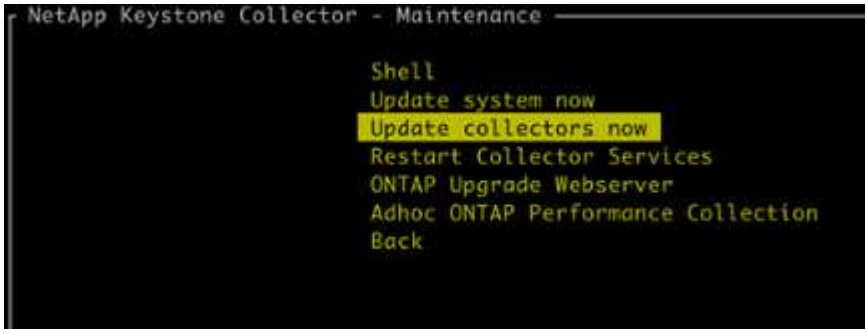
4. Una vez descargado el archivo, puedes adjuntarlo al ticket de soporte de Keystone ServiceNow. Para obtener información sobre cómo recaudar fondos, consulte "Generación de solicitudes de servicio".

Actualizar manualmente Keystone Collector

La función de actualización automática en Keystone Collector está habilitada de forma predeterminada, lo que actualiza automáticamente el software de Keystone Collector con cada nueva versión. Sin embargo, puede desactivar esta función y actualizar el software manualmente.

Pasos

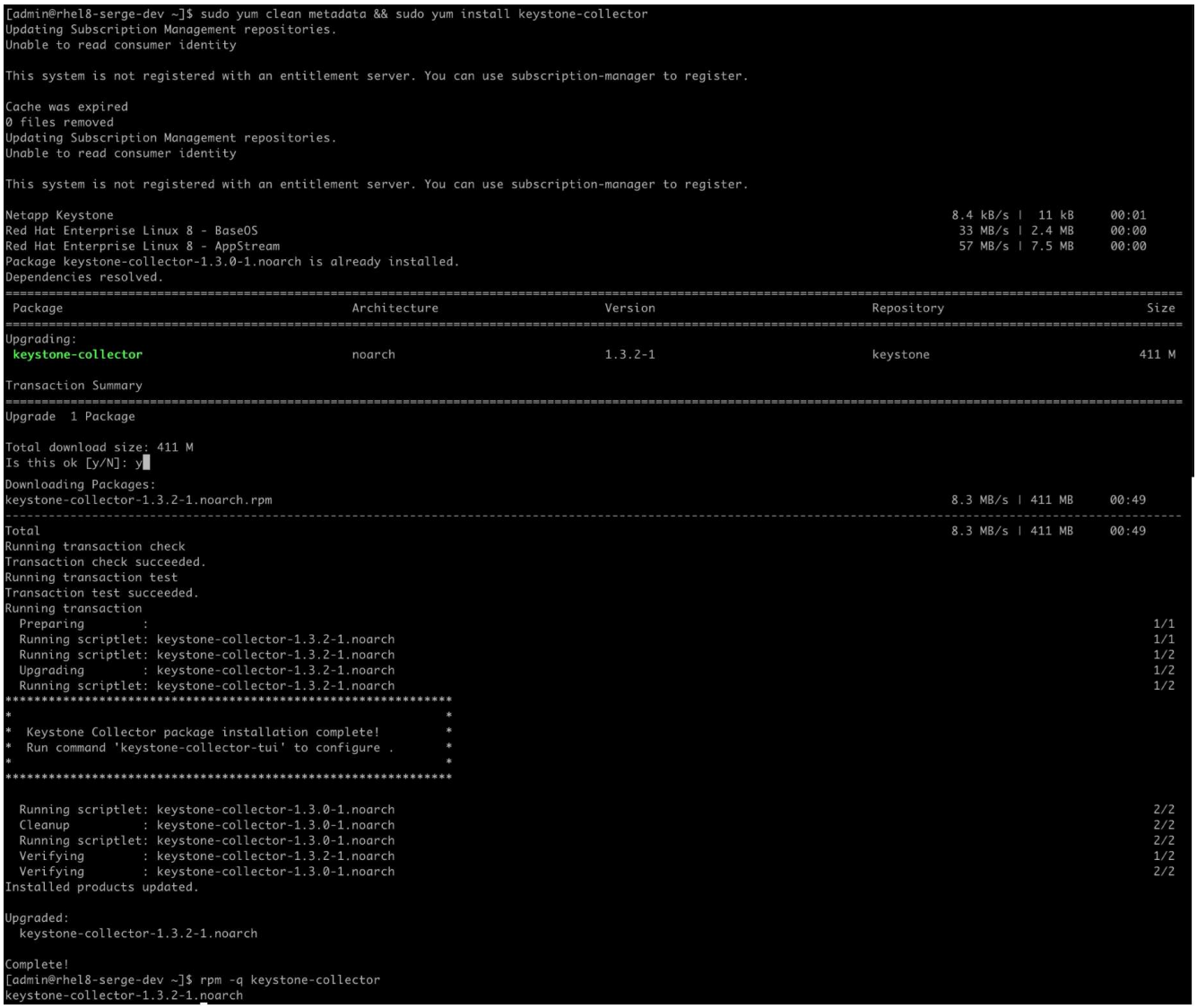
1. Inicie la utilidad TUI de administración de Keystone Collector:
   `$ keystone-collector-tui`
2. En la pantalla de mantenimiento, seleccione la opción **Actualizar recopiladores ahora**.



Alternativamente, ejecute estos comandos para actualizar la versión:

Para CentOS:

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



Para Debian:

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

3. Reinicie la TUI de administración de Keystone Collector, podrá ver la última versión en la parte superior izquierda de la pantalla de inicio.

   Alternativamente, ejecute estos comandos para ver la última versión:

   Para CentOS:

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

   Para Debian:

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

Seguridad de Keystone Collector

Keystone Collector incluye funciones de seguridad que monitorean el rendimiento y las métricas de uso de los sistemas Keystone , sin poner en riesgo la seguridad de los datos del cliente.

El funcionamiento de Keystone Collector se basa en los siguientes principios de seguridad:

- **Privacidad por diseño**: Keystone Collector recopila datos mínimos para realizar la medición del uso y el monitoreo del rendimiento. Para obtener más información, consulte "Datos recopilados para facturación" . El"Eliminar datos privados" Esta opción está habilitada de forma predeterminada, lo que enmascara y protege la información confidencial.
- **Acceso con privilegios mínimos**: Keystone Collector requiere permisos mínimos para monitorear los sistemas de almacenamiento, lo que minimiza los riesgos de seguridad y evita modificaciones no deseadas en los datos. Este enfoque se alinea con el principio del mínimo privilegio, mejorando la postura de seguridad general de los entornos monitoreados.
- **Marco de desarrollo de software seguro**: Keystone utiliza un marco de desarrollo de software seguro durante todo el ciclo de desarrollo, lo que mitiga los riesgos, reduce las vulnerabilidades y protege el sistema contra amenazas potenciales.

Fortalecimiento de la seguridad

De forma predeterminada, Keystone Collector está configurado para utilizar configuraciones de seguridad reforzada. Las siguientes son las configuraciones de seguridad recomendadas:

- El sistema operativo de la máquina virtual Keystone Collector:
  - Cumple con el estándar CIS Debian Linux 12 Benchmark. Realizar cualquier cambio en la configuración del sistema operativo fuera del software de administración Keystone Collector puede reducir la seguridad del sistema. Para obtener más información, consulte "Guía de referencia del CIS" .
  - Recibe e instala automáticamente parches de seguridad verificados por Keystone Collector a través de la función de actualización automática. Deshabilitar esta funcionalidad puede generar software vulnerable sin parchear.
  - Autentica las actualizaciones recibidas de Keystone Collector. Deshabilitar la verificación del repositorio APT puede provocar la instalación automática de parches no autorizados, lo que podría introducir vulnerabilidades.
- Keystone Collector valida automáticamente los certificados HTTPS para garantizar la seguridad de la conexión. Deshabilitar esta función podría provocar la suplantación de puntos finales externos y la fuga de datos de uso.
- Keystone Collector admite"CA de confianza personalizada" proceso de dar un título. De forma predeterminada, confía en los certificados firmados por CA raíz públicas reconocidas por el"Programa de certificación CA de Mozilla" . Al habilitar CA confiables adicionales, Keystone Collector habilita la validación de certificados HTTPS para conexiones a puntos finales que presentan estos certificados.
- El recopilador de Keystone habilita la opción **Eliminar datos privados** de forma predeterminada, que enmascara y protege la información confidencial. Para obtener más información, consulte "Limitar la

recopilación de datos privados" . Al deshabilitar esta opción, se comunicarán datos adicionales al sistema Keystone . Por ejemplo, puede incluir información ingresada por el usuario, como nombres de volúmenes, que pueden considerarse información confidencial.

Información relacionada

- "Descripción general de Keystone Collector"
- "Requisitos de infraestructura virtual"
- "Configurar Keystone Collector"

Tipos de datos de usuario que recopila Keystone

Keystone recopila información de configuración, estado y uso de las suscripciones a Keystone ONTAP y Keystone StorageGRID , así como datos de telemetría de la máquina virtual (VM) que aloja Keystone Collector. Solo puede recopilar datos de rendimiento para ONTAP , si esta opción está habilitada en Keystone Collector.

Recopilación de datos de ONTAP

Datos de uso recopilados para ONTAP: Más información

La siguiente lista es una muestra representativa de los datos de consumo de capacidad recopilados para ONTAP:

- Clústeres
  - UUID del clúster
  - Nombre del clúster
  - Número de serie
  - Ubicación (según el valor ingresado en el clúster ONTAP)
  - Contacto
  - Versión
- Nodos
  - Número de serie
  - Nombre del nodo
- Volúmenes
  - Nombre del agregado
  - Nombre del volumen
  - UUID de instancia de volumen
  - Indicador IsCloneVolume
  - Bandera IsFlexGroupConstituent
  - Bandera IsSpaceEnforcementLogical
  - Bandera IsSpaceReportingLogical
  - Espacio lógico utilizado por Afs
  - Porcentaje de espacio de instantánea
  - Datos de usuario inactivos de nivel de rendimiento
  - Porcentaje de datos de usuario inactivo de nivel de rendimiento
  - Nombre del grupo de políticas adaptativas de QoS
  - Nombre del grupo de políticas de calidad
  - Size
  - Usado
  - Física utilizada
  - Tamaño usado por instantáneas
  - Tipo
  - Estilo de volumen extendido
  - Nombre del servidor virtual
  - Bandera IsVsRoot
- Servidores virtuales
  - VserverName

    - UUID del servidor virtual
    - Subtipo
- Agregados de almacenamiento
    - Tipo de almacenamiento
    - Nombre del agregado
    - UUID agregado
    - Usado Físico
    - Talla disponible
    - Size
    - Tamaño usado
- Almacenes de objetos agregados
    - Nombre del almacén de objetos
    - UUID del almacén de objetos
    - Tipo de proveedor
    - Nombre del agregado
- Volúmenes de clonación
    - FlexClone
    - Size
    - Usado
    - Servidor virtual
    - Tipo
    - Volumen de los padres
    - Servidor padre-hijo
    - Es constituyente
    - Estimación dividida
    - Estado
    - Porcentaje usado de FlexClone
- LUN de almacenamiento
    - UUID de LUN
    - Nombre LUN
    - Size
    - Usado
    - Bandera reservada
    - Bandera IsRequested
    - Nombre de la unidad lógica
    - UUID de política de calidad
    - Nombre de política de calidad

    - UUID de volumen
    - Nombre del volumen
    - SVMUUID
    - Nombre de SVM
- Volúmenes de almacenamiento
    - UUID de instancia de volumen
    - Nombre del volumen
    - NombreSVM
    - SVMUUID
    - UUID de política de calidad
    - Nombre de política de calidad
    - Huella de nivel de capacidad
    - Huella de nivel de rendimiento
    - Huella total
    - Política de niveles
    - Bandera IsProtected
    - Bandera de IsDestination
    - Usado
    - Física utilizada
    - CloneParentUUID
    - Espacio lógico utilizado por Afs
- Grupos de políticas de QoS
    - Grupo de políticas
    - UUID de política de calidad
    - Máximo rendimiento
    - Rendimiento mínimo
    - Máximo rendimiento de IOPS
    - Máximo rendimiento MBps
    - Mínimo rendimiento de IOPS
    - Mínimo rendimiento MBps
    - Bandera IsShared
- Grupos de políticas de calidad de servicio adaptativas de ONTAP
    - Nombre de política de calidad
    - UUID de política de calidad
    - Pico de IOPS
    - Asignación máxima de IOPS
    - AbsoluteMinIOPS

    - IOPS esperados
    - Asignación de IOPS esperada
    - Tamaño del bloque
- Huellas
    - Servidor virtual
    - Volumen
    - Huella total
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Node
    - Agregar
    - LIF
    - Replicación de configuración
    - Conexiones
    - Clústeres
    - Volúmenes
- Clústeres MetroCluster
    - UUID del clúster
    - Nombre del clúster
    - UUID de clúster remoto
    - Nombre del clúster remoto
    - Estado de configuración local
    - Estado de configuración remota
- Nodos de MetroCluster
    - Estado de duplicación de DR
    - LIF entre clústeres
    - Accesibilidad del nodo
    - Nodo socio de DR
    - Nodo de socio auxiliar de DR
    - Relación simétrica entre los nodos DR, DR Aux y HA
    - Cambio automático no planificado
- Replicación de configuración de MetroCluster
    - Latido del corazón remoto
    - Último latido enviado
    - Último latido recibido
    - Transmisión de Vserver

    - Flujo de clúster
    - Almacenamiento
    - Volumen de almacenamiento en uso
- Mediadores de MetroCluster
    - Dirección del mediador
    - Puerto Mediador
    - Mediador configurado
    - Mediador accesible
    - Modo
- Métricas de observabilidad del recopilador
    - Hora de recolección
    - Punto final de la API de Active IQ Unified Manager consultado
    - Tiempo de respuesta
    - Número de registros
    - IP de la instancia AIQUM
    - ID de instancia del recopilador

Datos de rendimiento recopilados para ONTAP: Más información

La siguiente lista es una muestra representativa de los datos de rendimiento recopilados para ONTAP:

- Nombre del clúster
- UUID del clúster
- ID de objeto
- Nombre del volumen
- UUID de instancia de volumen
- Servidor virtual
- UUID del servidor virtual
- Nodo serial
- Versión ONTAP
- Versión AIQUM
- Agregar
- UUID agregado
- Clave de recursos
- Marca de tiempo
- IOPS por TB
- Estado latente
- Latencia de lectura
- EscribirMBps
- Latencia de rendimiento mínimo de QoSM
- Latencia de hoja QoSN
- Espacio libre usado
- Relación de errores de caché
- Otra latencia
- Latencia agregada de QoSA
- IOPS
- Letencia de red QoS
- Operaciones disponibles
- Latencia de escritura
- Latencia de QoSCloud
- Latencia de interconexión de clúster QoSCluster
- Otros MBps
- Latencia de QoSCop
- Latencia de la hoja QoSD
- Utilización

- Leer IOPS
- MBps
- Otras IOPS
- Latencia del grupo de políticas de calidad
- Leer MBps
- Latencia de QoSSyncSnapmirror
- Datos a nivel de sistema
  - Escritura/Lectura/Otros/Total IOPS
  - Escritura/Lectura/Otros/Rendimiento total
  - Escritura/Lectura/Otro/Latencia total
- Escritura de IOPS

Lista de elementos eliminados sobre la limitación del acceso a datos privados: Más información

Cuando la opción **Eliminar datos privados** está habilitada en Keystone Collector, se elimina la siguiente información de uso para ONTAP. Esta opción está habilitada de forma predeterminada.

- Nombre del clúster
- Ubicación del clúster
- Contacto del clúster
- Nombre del nodo
- Nombre del agregado
- Nombre del volumen
- Nombre del grupo de políticas adaptativas de QoS
- Nombre del grupo de políticas de calidad
- Nombre del servidor virtual
- Nombre de LUN de almacenamiento
- Nombre del agregado
- Nombre de la unidad lógica
- Nombre de SVM
- IP de la instancia AIQUM
- FlexClone
- Nombre del clúster remoto

Recopilación de datos de StorageGRID

Datos de uso recopilados para StorageGRID: Más información

La siguiente lista es una muestra representativa de la `Logical Data` recopilados para StorageGRID:

- ID de StorageGRID
- Account ID
- Nombre de la cuenta
- Bytes de cuota de cuenta
- Nombre del depósito
- Recuento de objetos del depósito
- Bytes de datos del depósito

La siguiente lista es una muestra representativa de la `Physical Data` recopilados para StorageGRID:

- ID de StorageGRID
- Nodo ID
- ID del sitio
- Nombre del sitio
- Instancia
- Bytes de utilización del almacenamiento de StorageGRID
- Metadatos de utilización de almacenamiento de StorageGRID Bytes

La siguiente lista es una muestra representativa de la `Availability/Uptime Data` recopilados para StorageGRID:

- Porcentaje de tiempo de actividad del SLA

Lista de elementos eliminados sobre la limitación del acceso a datos privados: Más información

Cuando la opción **Eliminar datos privados** está habilitada en Keystone Collector, se elimina la siguiente información de uso para StorageGRID. Esta opción está habilitada de forma predeterminada.

- Nombre de la cuenta
- Nombre del cubo
- Nombre del sitio
- Instancia/Nombre del nodo

Recopilación de datos de telemetría

Datos de telemetría recopilados desde Keystone Collector VM: Más información

La siguiente lista es una muestra representativa de los datos de telemetría recopilados para los sistemas Keystone :

- Información del sistema
  - Nombre del sistema operativo
  - Versión del sistema operativo
  - ID del sistema operativo
  - Nombre de host del sistema
  - Dirección IP predeterminada del sistema
- Uso de recursos del sistema
  - Tiempo de actividad del sistema
  - Número de núcleos de CPU
  - Carga del sistema (1 min, 5 min, 15 min)
  - Memoria total
  - Memoria libre
  - Memoria disponible
  - Memoria compartida
  - Memoria intermedia
  - Memoria caché
  - Intercambio total
  - Intercambio gratuito
  - Intercambio en caché
  - Nombre del sistema de archivos del disco
  - Tamaño del disco
  - Disco usado
  - Disco disponible
  - Porcentaje de uso del disco
  - Punto de montaje del disco
- Paquetes instalados
- Configuración del recopilador
- Registros de servicio
  - Registros de servicio de los servicios de Keystone

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.

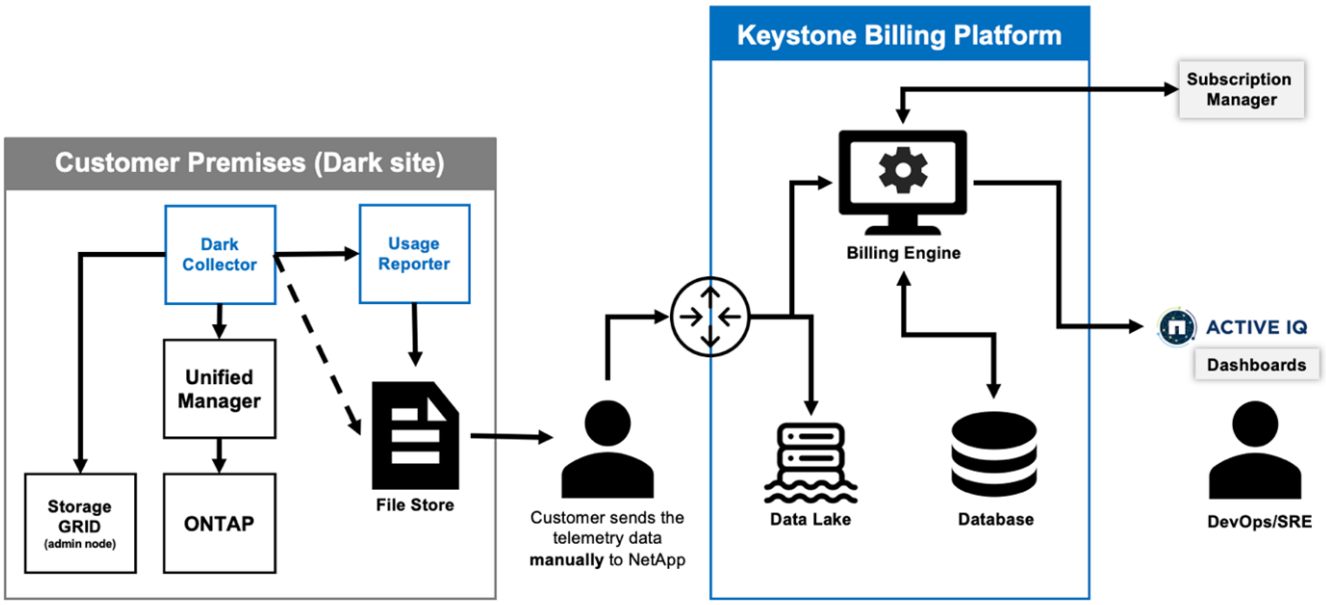
Para NetApp Keystone, ofrecer servicios para sitios oscuros significa proporcionar el servicio de suscripción de almacenamiento flexible de Keystone de una manera que respete las limitaciones de estos entornos. Esto implica:

- **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.

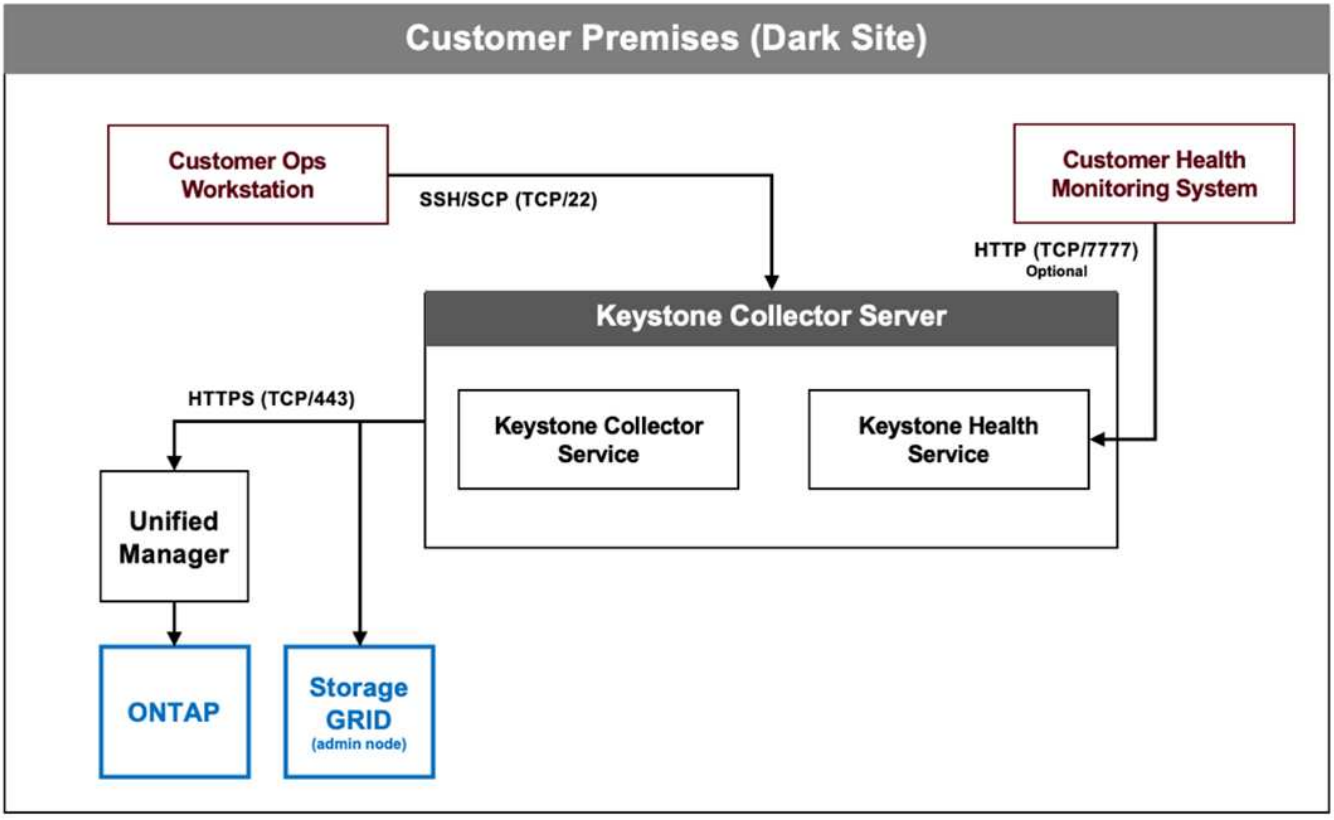
Keystone Collector se puede configurar sin restricciones de conectividad, también conocido como modo *estándar*. Para obtener más información, consulte"Obtenga más información sobre Keystone Collector" .

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:

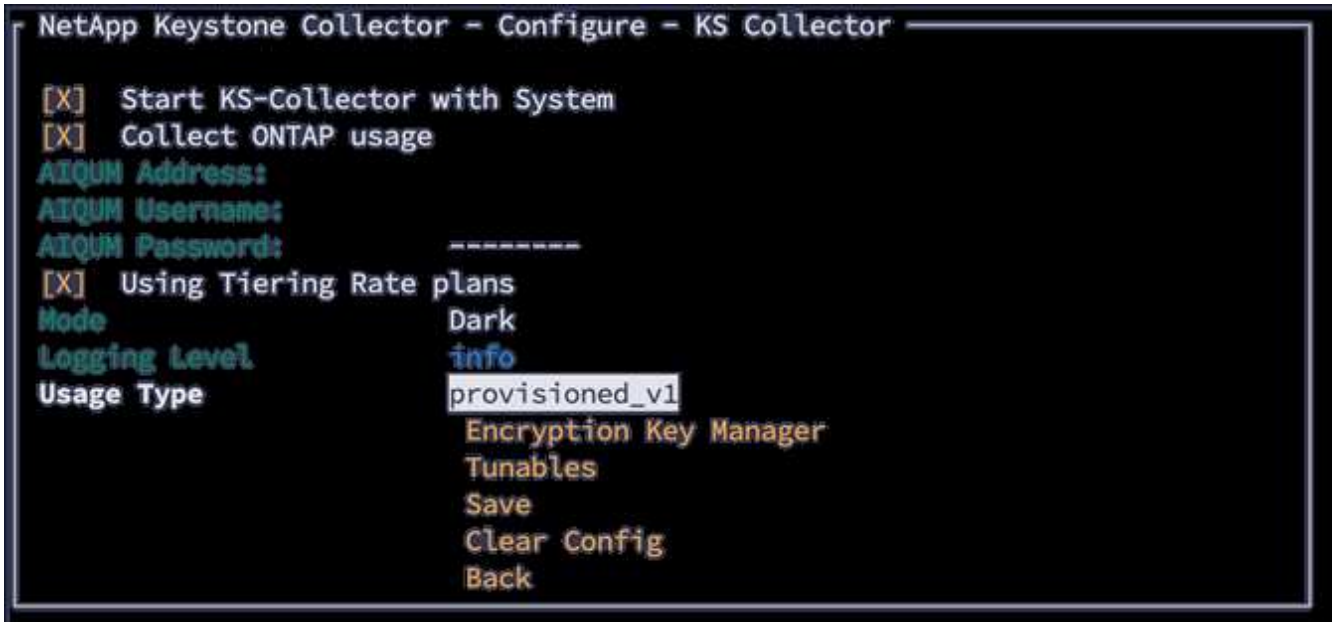
   ```
   keystone-collector-tui
   ```

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

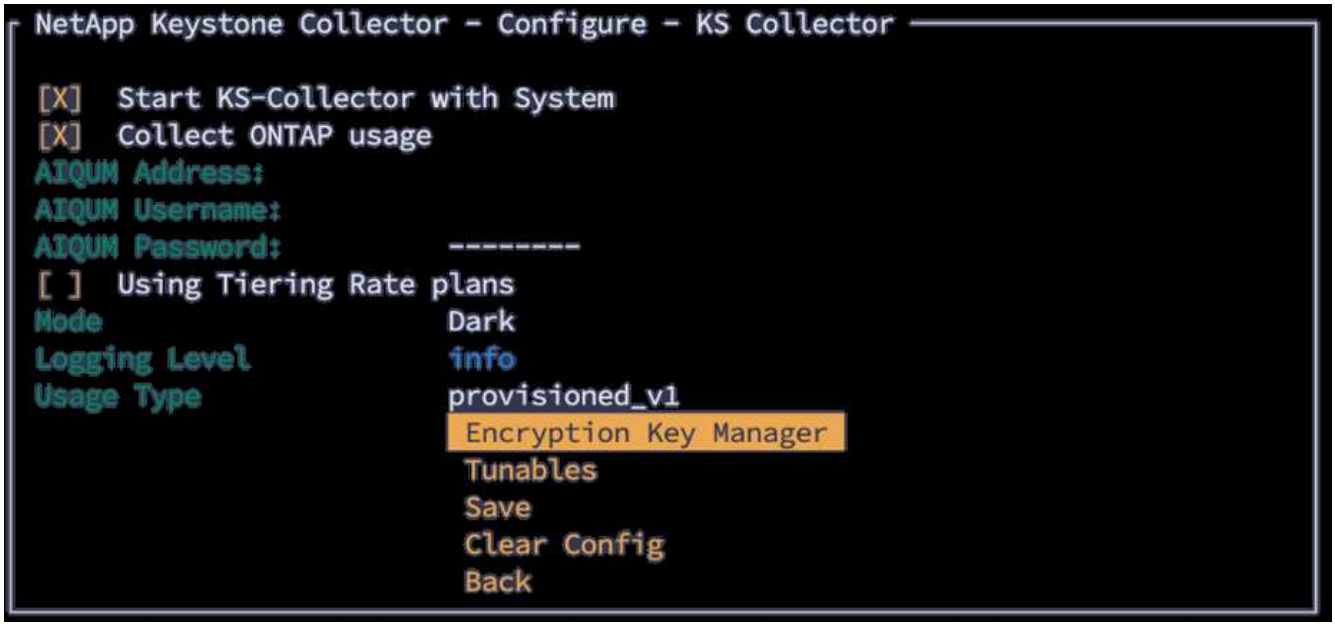
4. Seleccione **Guardar**.
5. Vaya a **Configurar > KS-Collector** para configurar Keystone Collector.
6. Activa o desactiva el campo **Iniciar recopilador de KS con el sistema**.

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.

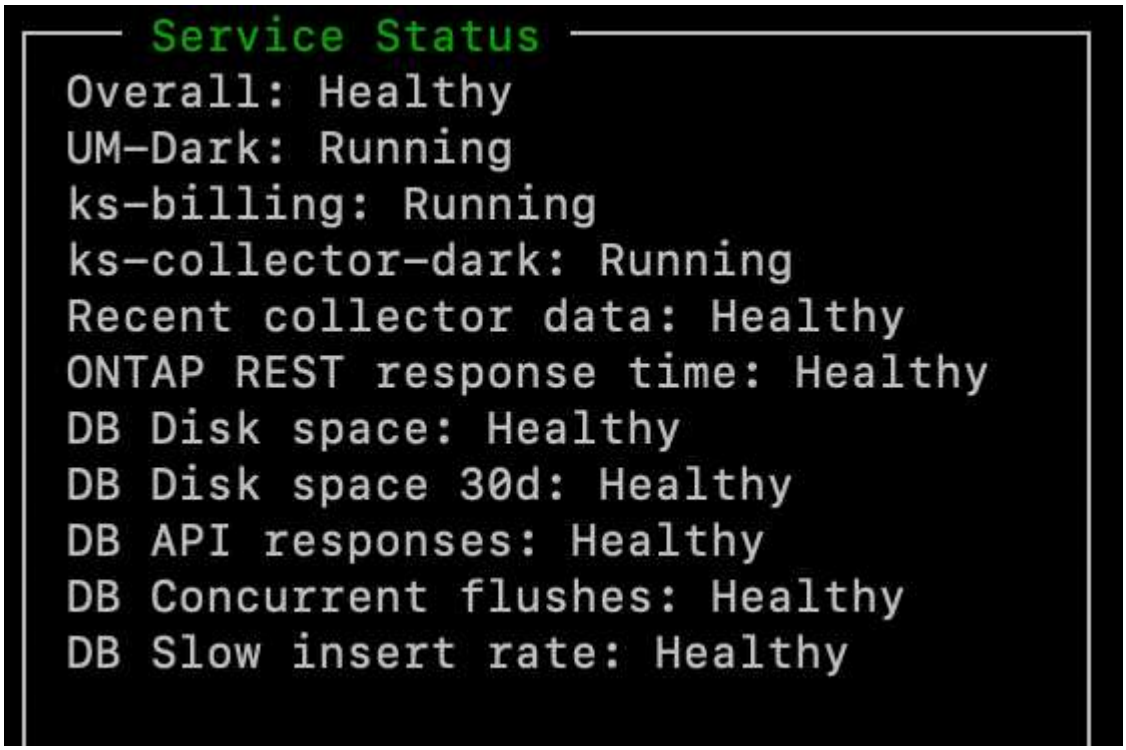


10. Seleccione **Guardar**.
11. Vaya a **Configurar > KS-Collector** para generar el par de claves de Keystone Collector.
12. Vaya a **Administrador de claves de cifrado** y presione Enter.



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.

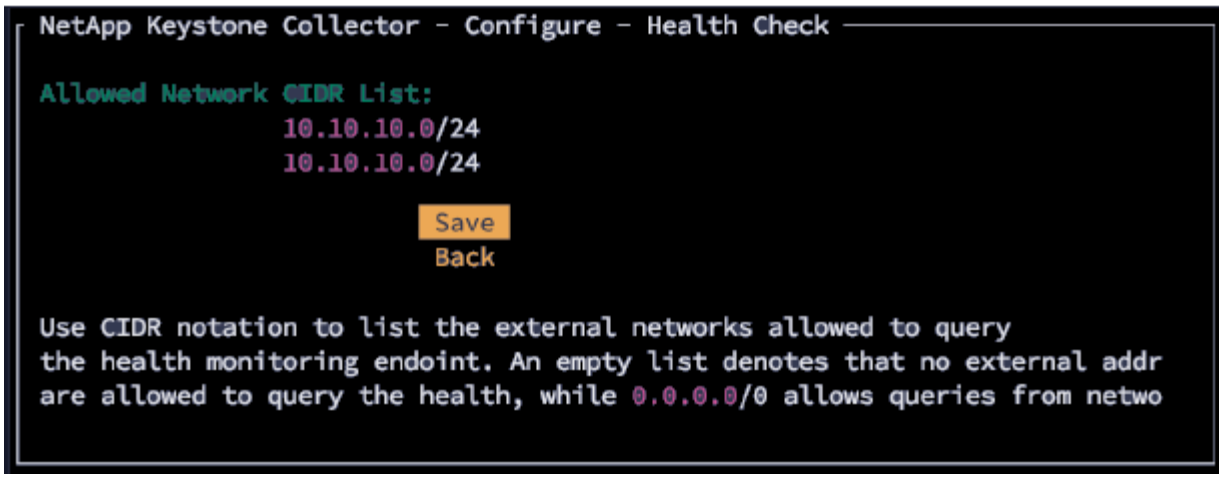
De forma predeterminada, los servicios de salud de Keystone no aceptan conexiones desde ninguna IP que no sea localhost. El punto final de salud de Keystone es `/uber/health` , y escucha en todas las interfaces del servidor Keystone Collector en el puerto `7777` . Cuando se realiza una consulta, se devuelve 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*.

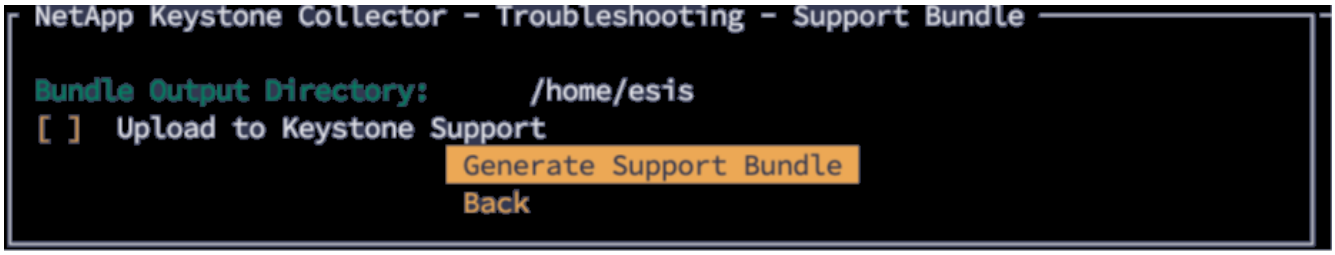


Generar y recopilar paquetes de soporte

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".