Configure y configure Keystone

Keystone

NetApp
January 14, 2026

This PDF was generated from https://docs.netapp.com/es-es/keystone-staas/installation/vapp-prereqs.html on January 14, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Configure y configure Keystone

Requisitos

Requisitos de infraestructura virtual para Keystone Collector

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

Requisitos previos para la máquina virtual del servidor de recopilador de Keystone:

- 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 cumplen los siguientes requisitos genéricos:

Requisitos de red

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

Keystone Collector requiere conexión a Internet. Puede proporcionar conectividad a Internet mediante enrutamiento directo a través de la puerta de enlace predeterminada (mediante NAT) o mediante el proxy HTTP. Ambas variantes se describen aquí.

Origen	Destino	Servicio	Protocolo y puertos	Categoría	Específico
Keystone Collector (para Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone ONTAP)	Colección de métricas de uso de Keystone Collector para ONTAP
Keystone Collector (para Keystone StorageGRID)	Nodos de administrador de StorageGRID	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone StorageGRID)	Colección de métricas de uso de Keystone Collector para StorageGRID

Keystone Collector (genérico)	Internet (según los requisitos de URL proporcionados más adelante)	HTTPS	TCP 443	Obligatorio (conexión a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Keystone Collector (genérico)	Proxy HTTP del cliente	Proxy HTTP	Puerto proxy del cliente	Obligatorio (conexión a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Keystone Collector (genérico)	Servidores DNS del cliente	DNS	TCP/UDP 53	Obligatorio	Resolución DNS
Keystone Collector (genérico)	Servidores NTP del cliente	NTP	UDP 123	Obligatorio	Sincronización de la hora
Keystone Collector (para Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funcionalidad opcional	Recopilación de métricas de rendimiento para Keystone Collector
Keystone Collector (genérico)	Sistema de monitorización del Cliente	HTTPS	TCP 7777	Funcionalidad opcional	Informes de estado de Keystone Collector
Estaciones de trabajo de operaciones del cliente	Recopilador Keystone	SSH	TCP 22	Gestión	Acceso a Keystone Collector Management
Direcciones de gestión de nodos y clústeres ONTAP de NetApp	Recopilador Keystone	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Funcionalidad opcional	Servidor web para actualizaciones de firmware de ONTAP

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

Acceso a URL

Keystone Collector necesita acceder a los siguientes hosts de Internet:

Dirección	Razón
https://keystone.netapp.com	Informes de uso y actualizaciones del software Keystone Collector
https://support.netapp.com	Sede central de NetApp para la información de facturación y entrega de AutoSupport

Requisitos de Linux para Keystone Collector

La preparación de 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 máquina virtual del servidor de recopilador de Linux y Keystone tenga 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 (sólo para entornos existentes)
- Hora cronyd sincronizada
- Acceso a los repositorios de software estándar de Linux

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

- Podman (POD Manager)
- sos
- crony
- Python 3 (3.9.14 a 3.11.8)

Máquina virtual del servidor de recopilador Keystone:

- Básico: 2 CPU
- RAM: 4 GB DE RAM
- Espacio en disco: 50 GB vDisk

Otros requisitos

Asegúrese de que se cumplen los siguientes requisitos genéricos:

Requisitos de red

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

> Keystone Collector requiere conexión a Internet. Puede proporcionar conectividad a Internet mediante enrutamiento directo a través de la puerta de enlace predeterminada (mediante NAT) o mediante el proxy HTTP. Ambas variantes se describen aquí.

Origen	Destino	Servicio	Protocolo y puertos	Categoría	Específico
Keystone Collector (para Keystone ONTAP)	Active IQ Unified Manager (Unified Manager)	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone ONTAP)	Colección de métricas de uso de Keystone Collector para ONTAP
Keystone Collector (para Keystone StorageGRID)	Nodos de administrador de StorageGRID	HTTPS	TCP 443	Obligatorio (si se utiliza Keystone StorageGRID)	Colección de métricas de uso de Keystone Collector para StorageGRID
Keystone Collector (genérico)	Internet (según los requisitos de URL proporcionados más adelante)	HTTPS	TCP 443	Obligatorio (conexión a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Keystone Collector (genérico)	Proxy HTTP del cliente	Proxy HTTP	Puerto proxy del cliente	Obligatorio (conexión a Internet)	Software Keystone Collector, actualizaciones del sistema operativo y carga de métricas
Keystone Collector (genérico)	Servidores DNS del cliente	DNS	TCP/UDP 53	Obligatorio	Resolución DNS

Keystone Collector (genérico)	Servidores NTP del cliente	NTP	UDP 123	Obligatorio	Sincronización de la hora
Keystone Collector (para Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funcionalidad opcional	Recopilación de métricas de rendimiento para Keystone Collector
Keystone Collector (genérico)	Sistema de monitorización del Cliente	HTTPS	TCP 7777	Funcionalidad opcional	Informes de estado de Keystone Collector
Estaciones de trabajo de operaciones del cliente	Recopilador Keystone	SSH	TCP 22	Gestión	Acceso a Keystone Collector Management
Direcciones de gestión de nodos y clústeres ONTAP de NetApp	Recopilador Keystone	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Funcionalidad opcional	Servidor web para actualizaciones de firmware de ONTAP

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

Acceso a URL

Keystone Collector necesita acceder a los siguientes hosts de Internet:

Dirección	Razón
https://keystone.netapp.com	Informes de uso y actualizaciones del software Keystone Collector
https://support.netapp.com	Sede central de NetApp para la información de facturación y entrega de AutoSupport

Requisitos para ONTAP y StorageGRID para Keystone

Antes de empezar a usar Keystone, debe asegurarse de que los clústeres de 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 tiene la intención de recopilar datos de uso solo a través de ONTAP:

1. Asegúrese de que ONTAP 9,8 o una versión posterior esté configurada. Para obtener información sobre la configuración de un nuevo clúster, consulte estos enlaces:
   - "Configure ONTAP en un nuevo clúster con System Manager"
   - "Configure un clúster con la CLI"
2. Crear cuentas de inicio de sesión de ONTAP con roles específicos. Para obtener más información, consulte "Obtenga más información sobre la creación de cuentas de inicio de sesión de ONTAP" .
   - **Web UI**
     i. Inicie sesión en ONTAP System Manager con las 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 la interfaz de línea de comandos de ONTAP con las 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 "Active el acceso de contraseña de la cuenta de ONTAP" .

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

1. Asegúrese de que Unified Manager 9,10 o una versión posterior esté configurada. 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. Compruebe que el clúster de ONTAP se haya añadido a Unified Manager. Para obtener información sobre cómo añadir clústeres, consulte "Añadir clústeres".
3. Cree usuarios de Unified Manager con roles específicos para la recogida de datos de uso y rendimiento. Siga estos pasos. Para obtener más 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 del administrador de aplicaciones predeterminadas que se generan durante la instalación. Consulte "Acceder a la interfaz de usuario web de Unified Manager".
   b. Cree una cuenta de servicio para Keystone Collector con `Operator` rol de usuario. Las API de servicio de Keystone Collector utilizan esta cuenta de servicio para comunicarse con Unified

Manager y recopilar datos de uso. Consulte "Adición de usuarios".

c. Cree un `Database` cuenta de usuario, con la `Report Schema` función. Este usuario es necesario para la recopilación de datos de rendimiento. Consulte "Creación de un usuario de base de datos".

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

4. Habilite la puerta de enlace API en Unified Manager. Keystone Collector utiliza la función API Gateway para comunicarse con clústeres ONTAP. Puede habilitar la puerta de enlace API desde la interfaz de usuario web o mediante la ejecución de algunos comandos a través de la CLI de Unified Manager.

   Interfaz de usuario web de

   Para habilitar la puerta de enlace de la API 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 "Habilitar API Gateway".

   CLI

   Para habilitar la puerta de enlace de API mediante la CLI de Unified Manager, siga estos pasos:

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

   b. Compruebe si la puerta de enlace API ya está activada.
   `um option list api.gateway.enabled`A. `true` El valor indica que la puerta de enlace API está habilitada.

   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".
      - VSphere de VMware: "Reiniciar la máquina virtual de Unified Manager".

StorageGRID

Se requieren las siguientes configuraciones para instalar Keystone Collector en StorageGRID.

- StorageGRID `11.6.0` o se debe instalar una versión posterior. Para obtener más información sobre la actualización de StorageGRID, consulte "Actualizar el software StorageGRID: Descripción general".
- Se debe crear una cuenta de usuario administrador local de StorageGRID para la recopilación de datos de uso. El servicio de Collector de Keystone utiliza esta cuenta de servicio para comunicarse con StorageGRID a través de las API de nodos de administrador.

  Pasos

  a. Inicie sesión en Grid Manager. Consulte "Inicie sesión en Grid Manager".

b. Cree un grupo de administración local con `Access mode: Read-only`. Consulte "Cree un grupo de administración".

c. Añada los siguientes permisos:

- Cuentas de inquilino
- Mantenimiento
- Consulta de métricas

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

Instale Keystone Collector

Ponga en marcha Keystone Collector en sistemas VMware vSphere

La puesta en marcha 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 VM.

Despliegue de la plantilla OVA

Siga estos pasos:

Pasos

1. Descargue el archivo OVA desde "este enlace" Y almacénelo en su sistema VMware vSphere.
2. En su sistema VMware vSphere, desplácese a la vista **VMs and Templates**.
3. Haga clic con el botón derecho del ratón en la carpeta necesaria para la máquina virtual (VM) (o el centro de datos, si no utiliza carpetas de VM) y seleccione **implementar plantilla OVF**.
4. En *Paso 1* del asistente **implementar plantilla OVF**, haga clic en **Seleccionar y plantilla OVF** para seleccionar la descarga `KeystoneCollector-latest.ova` archivo.
5. En *Paso 2*, especifique el nombre del equipo virtual y seleccione la carpeta del equipo virtual.
6. En *Paso 3*, especifique el recurso informático necesario que se va a ejecutar el equipo 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.

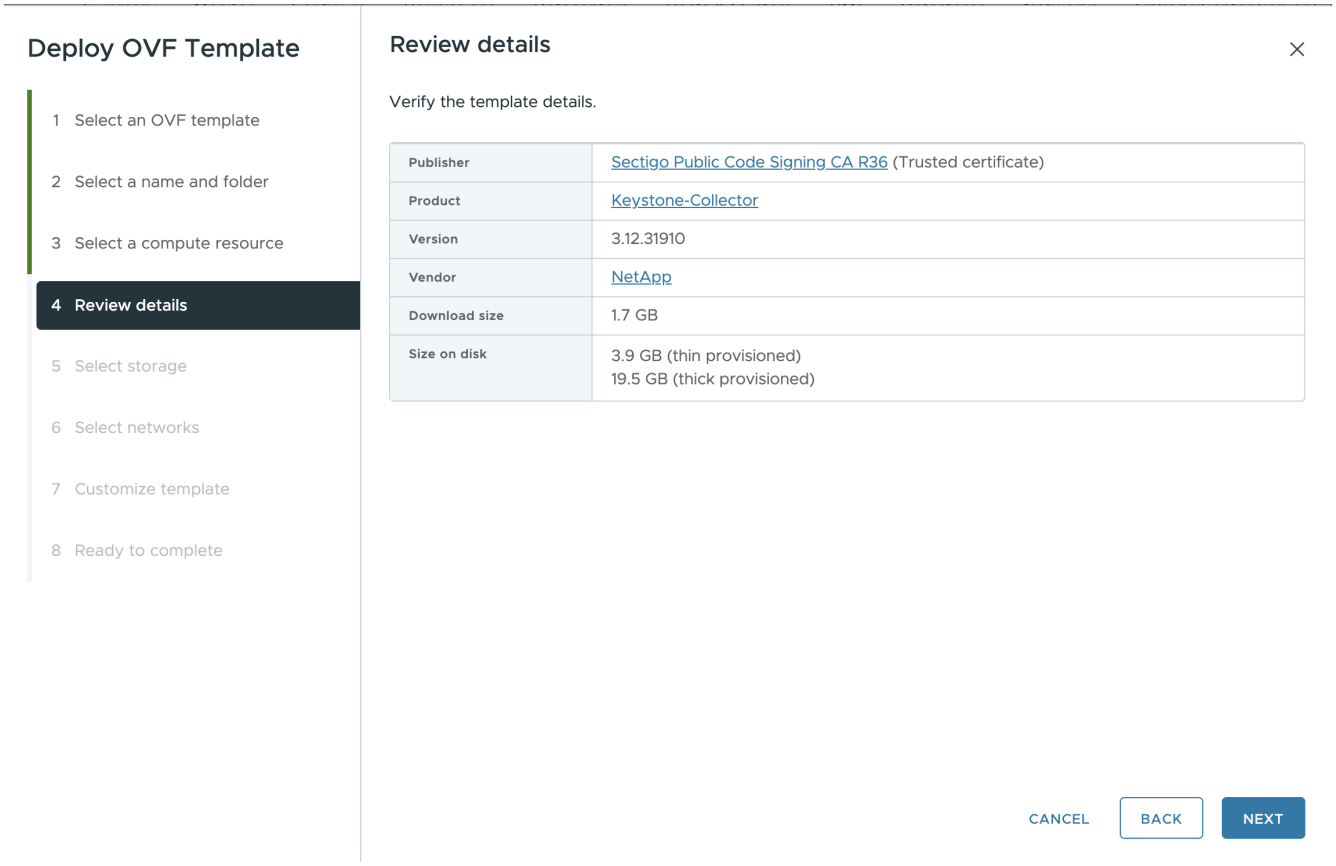
   a. Descarga el certificado de CA de firma de código de Sectigo. "aquí".

   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 *Paso 5* del asistente **implementar plantilla OVF**, especifique la ubicación para almacenar la VM.
9. En *Paso 6*, seleccione la red de destino que utilizará la máquina virtual.
10. En *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 se debe usar como credencial de bootstrap para obtener acceso inicial al sistema VMware vSphere. Durante la configuración inicial de software, es necesario cambiar esta contraseña de administrador. La máscara de subred para la dirección IPv4 debe suministrarse en notación CIDR. Por ejemplo, utilice el valor 24 para una máscara de subred de 255.255.255.0.

11. En *Paso 8 Listo para completar* del asistente **implementar plantilla OVF**, revise la configuración y compruebe que ha definido correctamente los parámetros para la implementación del OVA.

Después de implementar el equipo virtual desde la plantilla y encender, abra una sesión SSH en el equipo virtual e inicie sesión con las credenciales de administrador temporal para verificar que el equipo virtual esté listo para la configuración.

Configuración inicial del sistema

Realice estos pasos en sus sistemas VMware vSphere para obtener una configuración inicial de los servidores de recopilador de Keystone implementados mediante OVA:

Al completar la puesta en marcha, puede usar la utilidad Keystone Collector Management Terminal User Interface (TUI) para realizar las actividades de configuración y supervisión. Puede usar varios controles del teclado, como las teclas Entrar y flecha, para seleccionar las opciones y navegar por esta TUI.

1. Abra una sesión SSH al servidor Keystone Collector. Cuando se conecte, el sistema le pedirá 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.

   También puede iniciarlo manualmente ejecutando el `keystone-collector-tui` Comando de la CLI.
3. Si es necesario, configure los detalles del proxy en la sección **Configuración > Red** de 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 de Keystone con la opción **Mantenimiento > Actualizar recopiladores**. Después de la actualización, reinicie la utilidad TUI de gestión de Keystone Collector para aplicar los cambios.

Instale 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 dependiendo de su distribución de Linux.

Uso de RPM

1. SSH al servidor de Keystone Collector y vaya 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 de repositorio de software YUM:
   `# yum install keystonerepo.rpm`
7. Cuando se instale Keystone repo, instale el paquete Keystone-collector a través del gestor 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. SSH al servidor del recopilador de Keystone y eleva a `root` privilegio.
   `sudo su`
2. Descargue el `keystone-sw-repo.deb` archivo:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Instale el archivo de repositorio del software de Keystone:
   `# dpkg -i keystone-sw-repo.deb`
4. Actualice 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`

Al completar la instalación, puede usar la utilidad Keystone Collector Management Terminal User Interface (TUI) para realizar las actividades de configuración y supervisión. Puede usar varios controles del teclado, como las teclas Entrar y flecha, para seleccionar las opciones y navegar por esta TUI. Consulte "Configure Keystone Collector" y.. "Supervise el estado del sistema" para obtener más información.

Validación automática del software Keystone

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

La configuración del cliente del repositorio YUM de Keystone 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 de Keystone que no supera la validación de firmas se impide que se instale. 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.

Configure Keystone Collector

Debe realizar algunas tareas de configuración para permitir a Keystone Collector recopilar datos de uso en su entorno de almacenamiento. Se trata de una actividad única para activar y asociar los componentes requeridos con su entorno de almacenamiento.

- Keystone Collector ofrece la utilidad Interfaz de usuario del terminal (TUI) de gestión de recopiladores de Keystone para realizar actividades de configuración y supervisión. Puede usar varios controles del teclado, como las teclas Entrar y 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 *dark site* o *private mode*. Si desea obtener más información acerca de, consulte "Keystone en modo privado".

Pasos

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

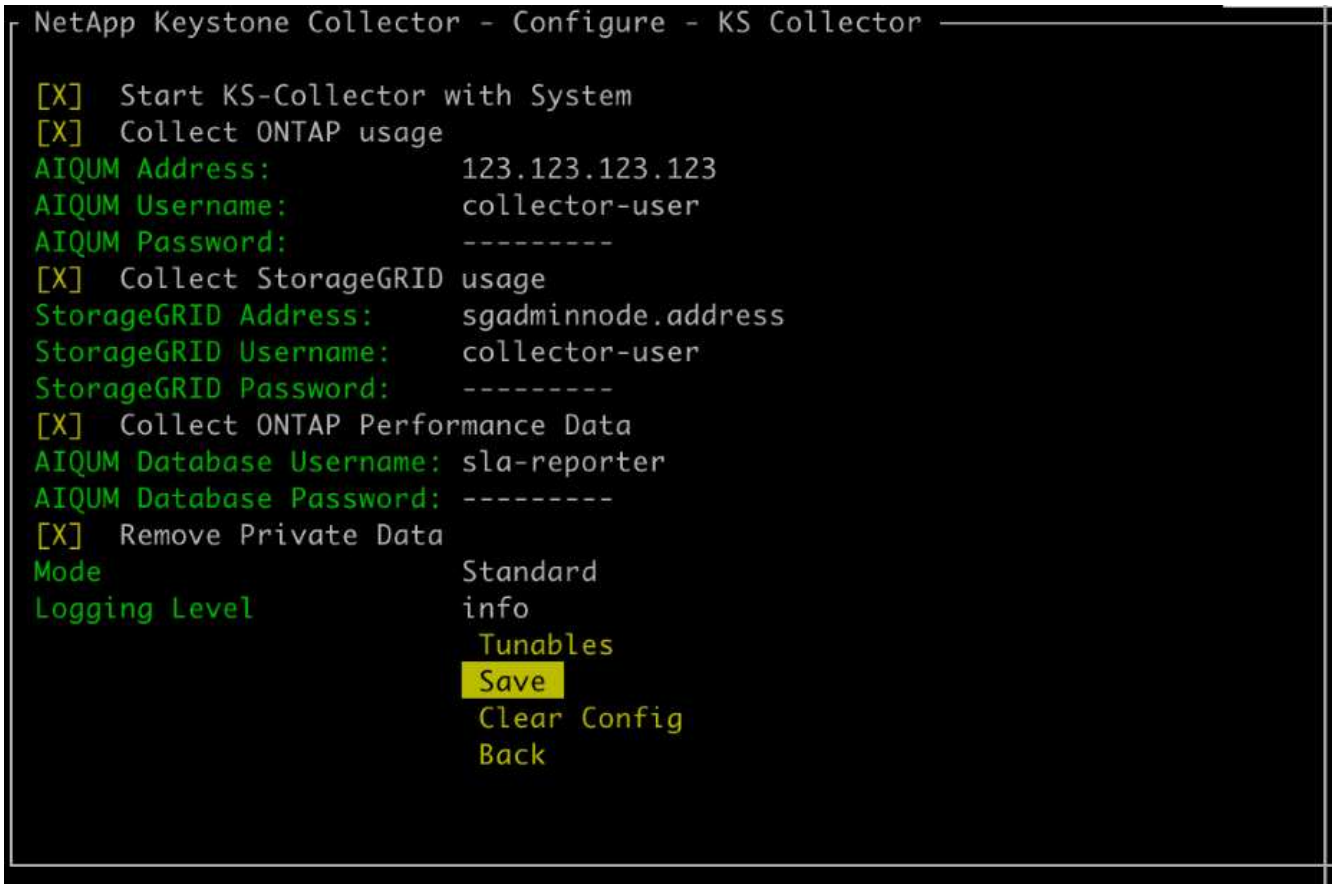
   ** PAU **

   - **Recopilar uso de ONTAP**: Esta opción permite la recopilación de datos de uso para ONTAP. Añada los detalles del servidor y la cuenta de servicio de Active IQ Unified Manager (Unified Manager).
   - **Recopilar datos de rendimiento de ONTAP**: Esta opción permite la recopilación de datos de rendimiento para ONTAP. Esta opción está desactivada de forma predeterminada. Habilite esta opción si es necesario supervisar el rendimiento en su entorno para fines de acuerdo de nivel de servicio. Proporcione los detalles de la cuenta de usuario de la base de datos de Unified Manager. Para obtener información sobre cómo crear usuarios de bases de datos, consulte "Cree usuarios de Unified Manager".
   - **Eliminar datos privados**: Esta opción elimina datos privados específicos de los clientes y está activada de forma predeterminada. Para obtener información acerca de los datos que se excluyen de las métricas si esta opción está activada, consulte "Limitar la recopilación de datos privados".

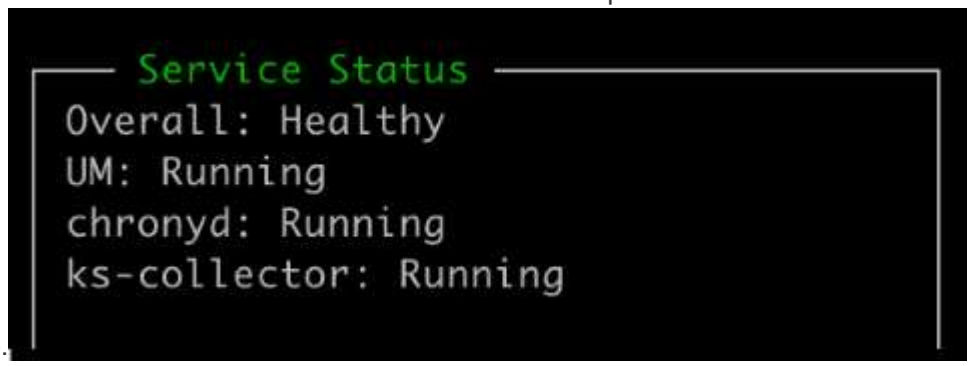
** PAU **

- **Recopilar uso de StorageGRID**: Esta opción permite recopilar los detalles de uso de los nodos. Añada la dirección del nodo StorageGRID y los detalles de usuario.
- **Eliminar datos privados**: Esta opción elimina datos privados específicos de los clientes y está activada de forma predeterminada. Para obtener información acerca de los datos que se excluyen de las métricas si esta opción está activada, consulte "Limitar la recopilación de datos privados".

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



6. Asegúrese de que Keystone Collector esté en buen estado; para ello, vuelva a la pantalla principal de la TUI y verifique la información **Service Status**. El sistema debería mostrar que los servicios están en un estado **global: Saludable**.



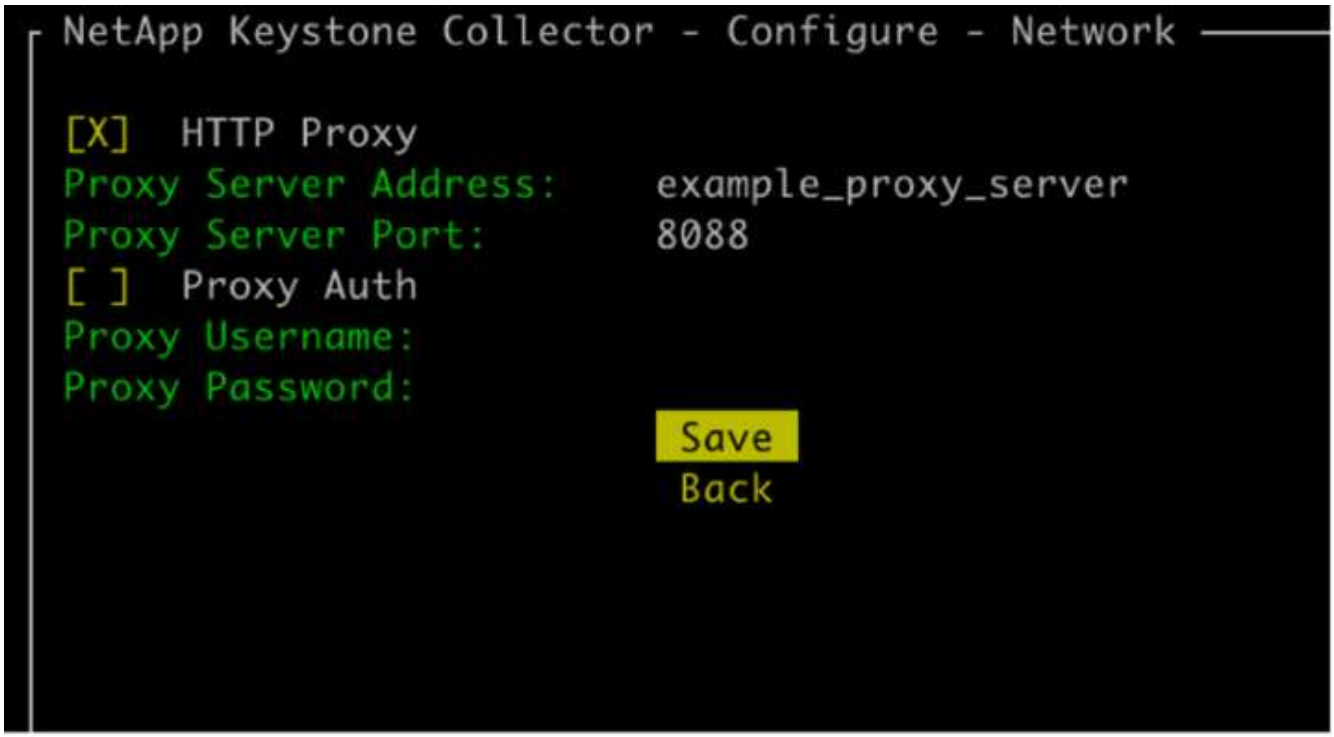
7. Salga de la TUI de gestión de Keystone Collector seleccionando la opción **salir a Shell** en la pantalla de inicio.

Configure el proxy HTTP en el colector de Keystone

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

Pasos

1. Reinicie la utilidad TUI de gestión del recopilador de Keystone si ya se ha cerrado:
   `$ keystone-collector-tui`
2. Active el campo **HTTP Proxy** 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 sobre configuración, estado y rendimiento necesaria para realizar la medición de suscripción. Existe la opción de limitar aún más la información recopilada mediante el enmascaramiento de la información confidencial del contenido cargado. Esto no afecta al cálculo de facturación. Sin embargo, limitar la información podría afectar a la facilidad de uso de la información reporting, ya que algunos elementos, que pueden ser fácilmente identificados por los usuarios, como el nombre del volumen, se reemplaza por UUID.

Limitar la recogida de datos específicos del cliente es una opción configurable en la pantalla TUI de Keystone Collector. Esta opción, **Quitar datos privados**, está activada de forma predeterminada.

Para obtener más información acerca de los elementos eliminados sobre la limitación del 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 con una entidad de certificación raíz pública (CA) forma parte de las funciones 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 del sistema, el tráfico basado en Internet se volverá a cifrar con su certificado de CA personalizado. Es necesario configurar los ajustes para verificar el origen como una CA de confianza antes de aceptar el certificado raíz y permitir que se produzcan las conexiones. Siga estos pasos:

Pasos

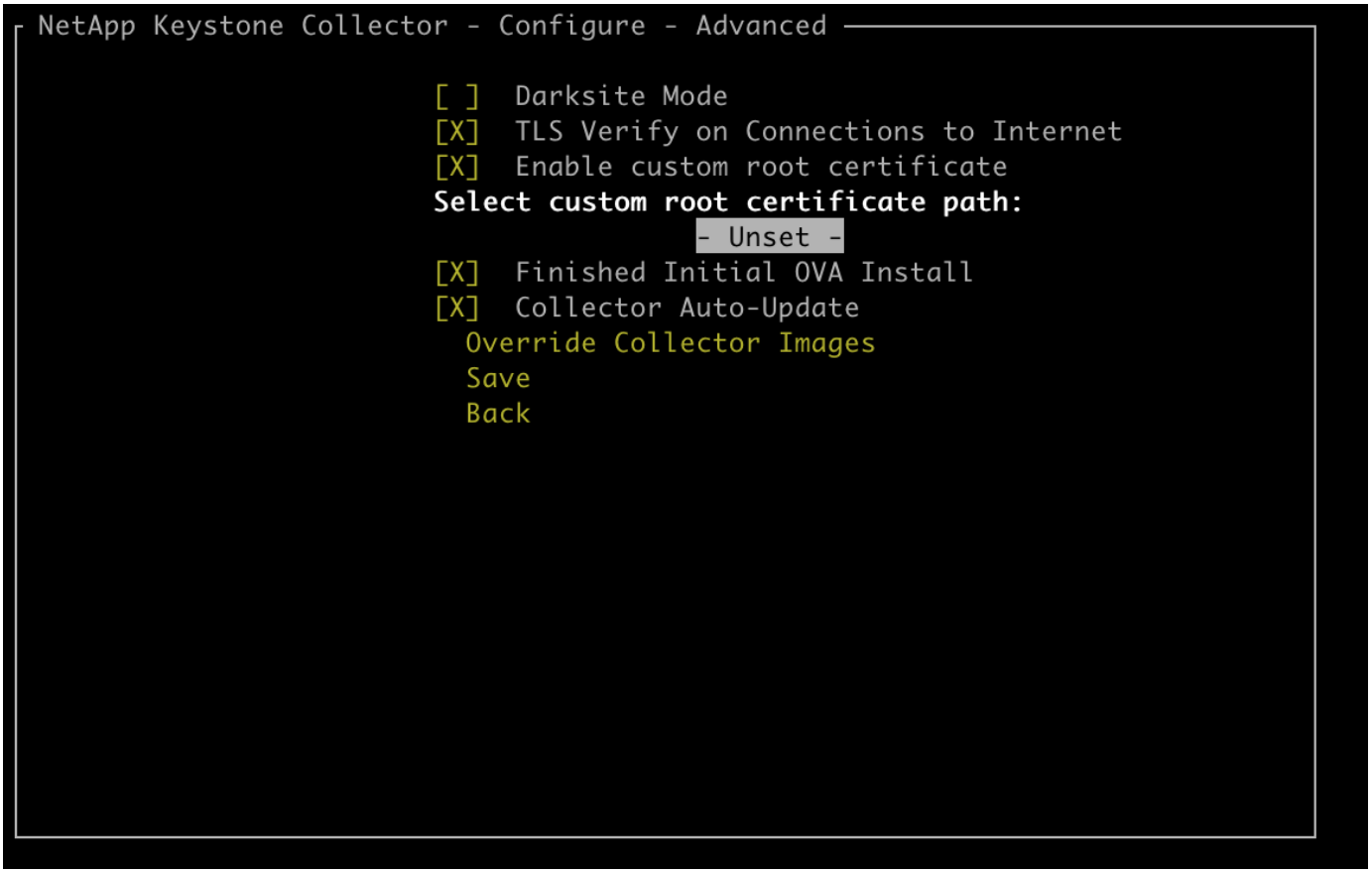
1. Prepare el certificado de CA. Debe estar en formato de archivo *base64-codificado X.509*.

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

2. Copie el certificado en el servidor del recopilador de Keystone. Anote la ubicación en la que se copia el archivo.
3. Abra un terminal en el servidor y ejecute la utilidad TUI de gestión.
   ```
   $ keystone-collector-tui
   ```
4. Vaya a **Configuración > Avanzado**.

5. Active la opción **Activar certificado raíz personalizado**.
6. Para **Seleccione la ruta de certificado raíz personalizada:**, seleccione `- Unset -`
7. Pulse Intro. Se muestra un cuadro de diálogo para seleccionar la ruta del certificado.
8. Seleccione el certificado raíz del explorador del sistema de archivos o introduzca la ruta exacta.
9. Pulse Intro. Vuelve a la pantalla **Advanced**.
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.

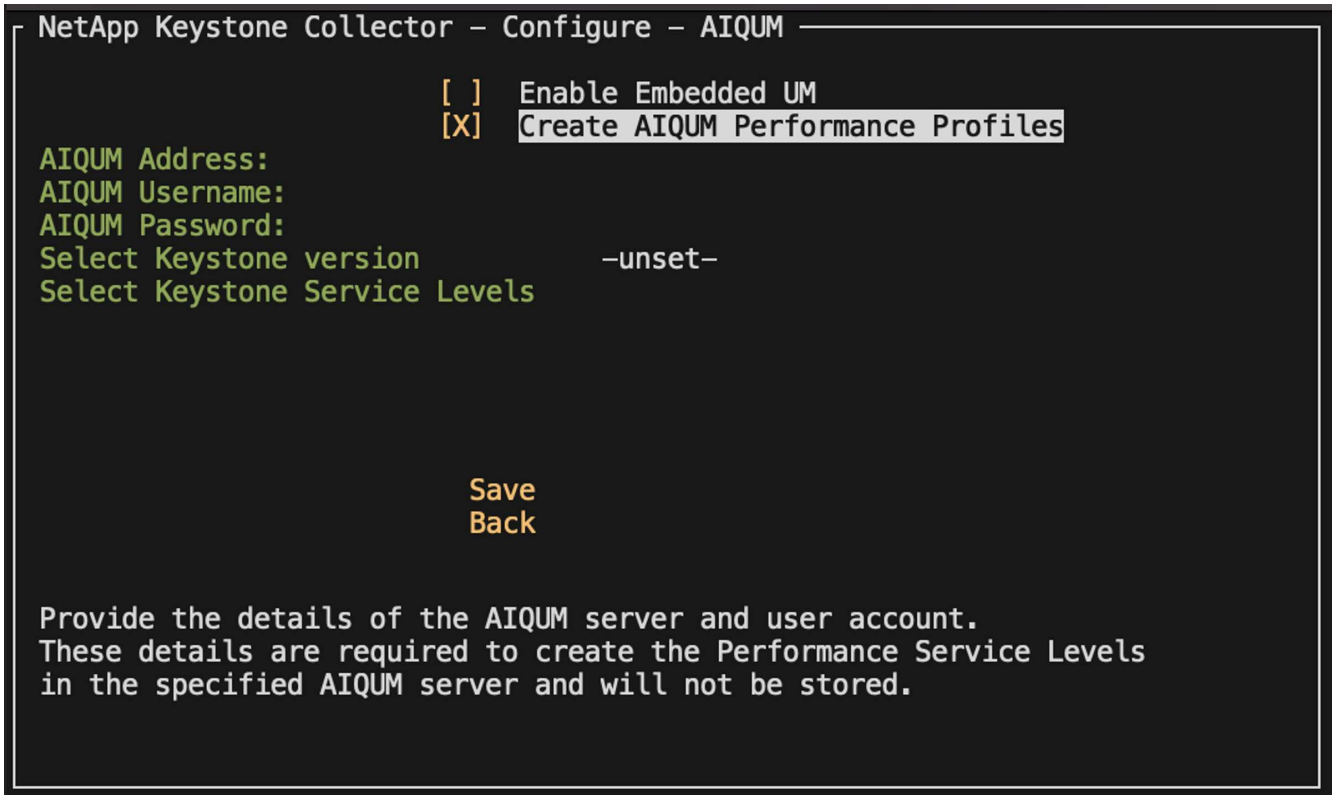
Para obtener más información sobre PSL, consulte "Niveles de servicio de rendimiento".

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

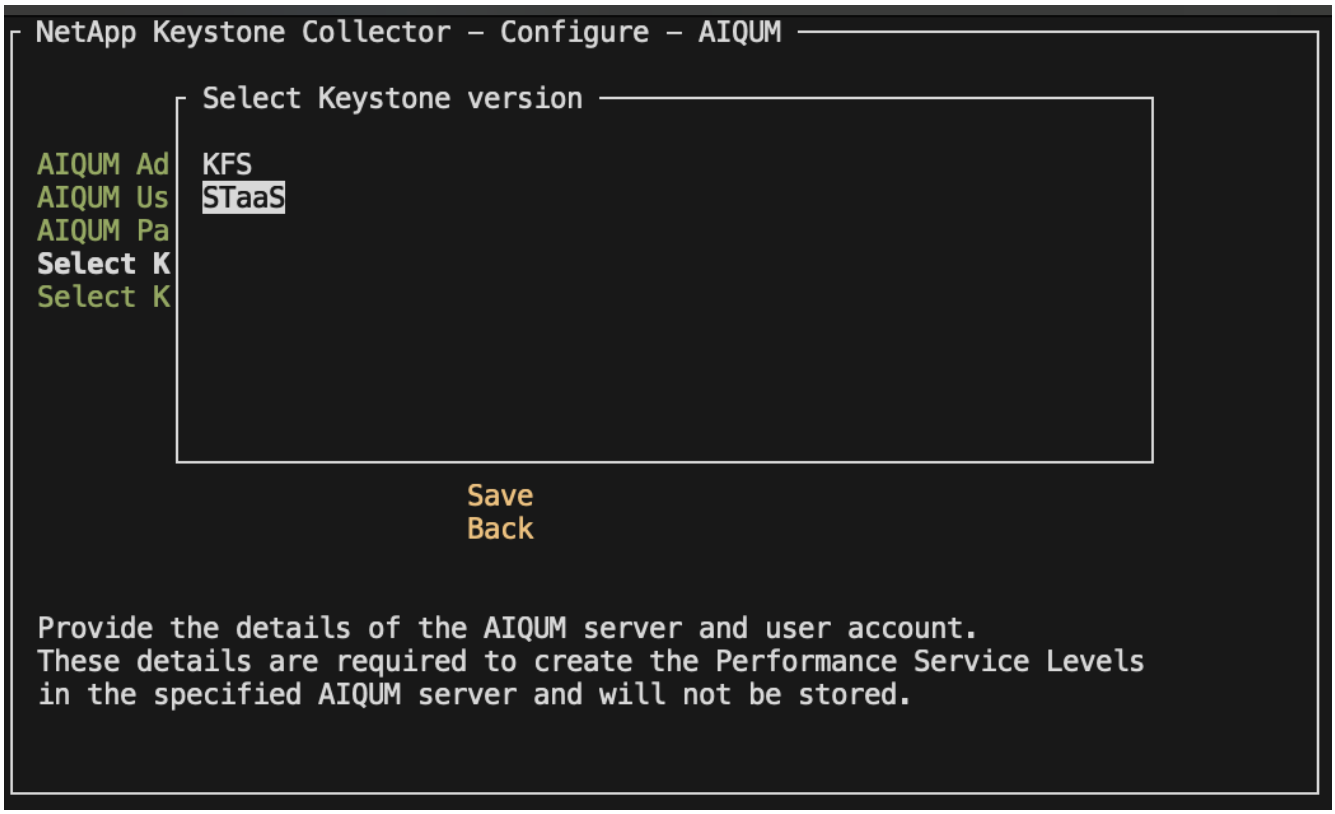
Pasos

1. Inicie la utilidad TUI de gestión de Keystone Collector:
   ```
   $ keystone-collector-tui
   ```

2. Vaya a **Configure>AIQUM** para abrir la pantalla de AIQUM.
3. Active la opción **Crear perfiles de rendimiento AIQUM**.
4. Introduzca los detalles del servidor Active IQ Unified Manager y la cuenta de usuario. Estos detalles son necesarios para crear PSL y no se almacenarán.

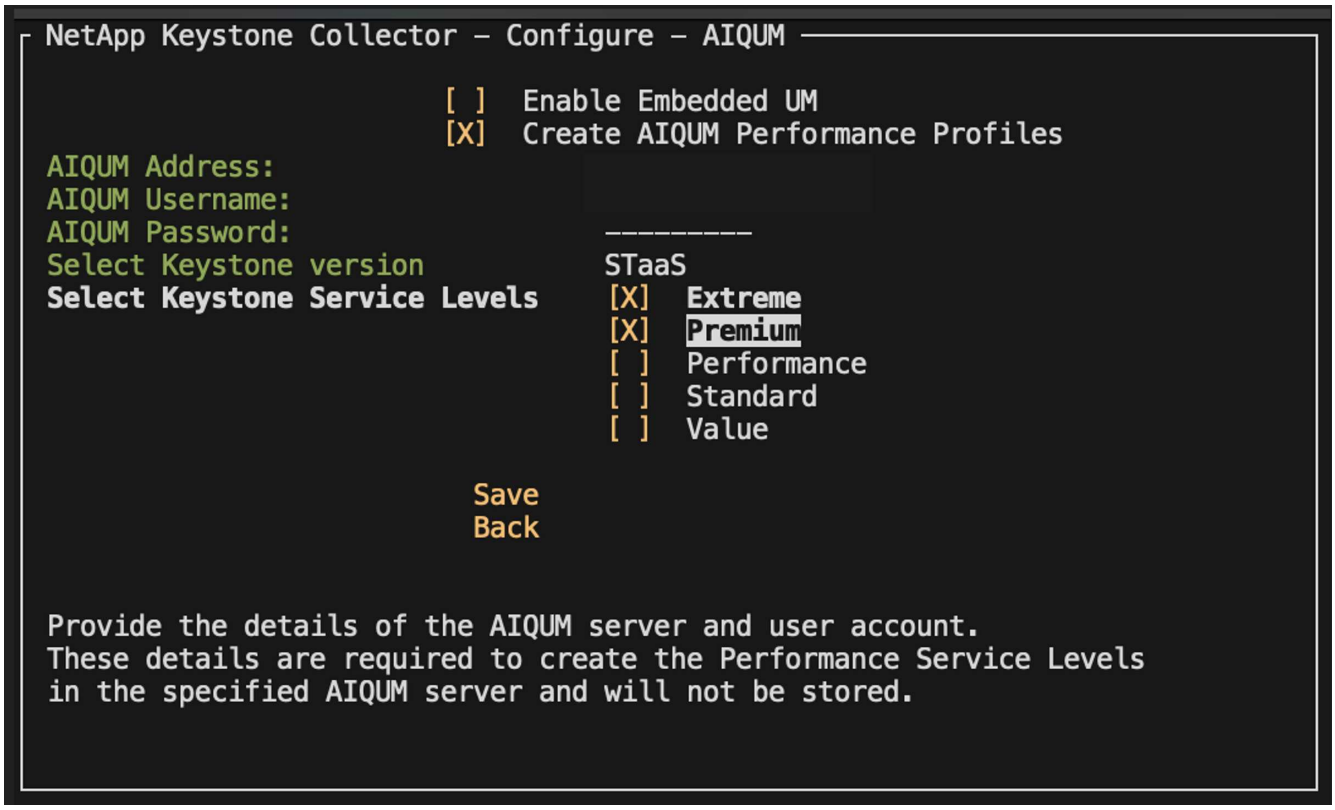


5. Para **Seleccione la versión de Keystone**, seleccione `-unset-`.
6. Pulse Intro. Se muestra un cuadro de diálogo para seleccionar la versión de Keystone.
7. Resalte **STaaS** para especificar la versión de Keystone para STaaS de Keystone y, a continuación, presione Intro.



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 Keystone | Versión 1" .

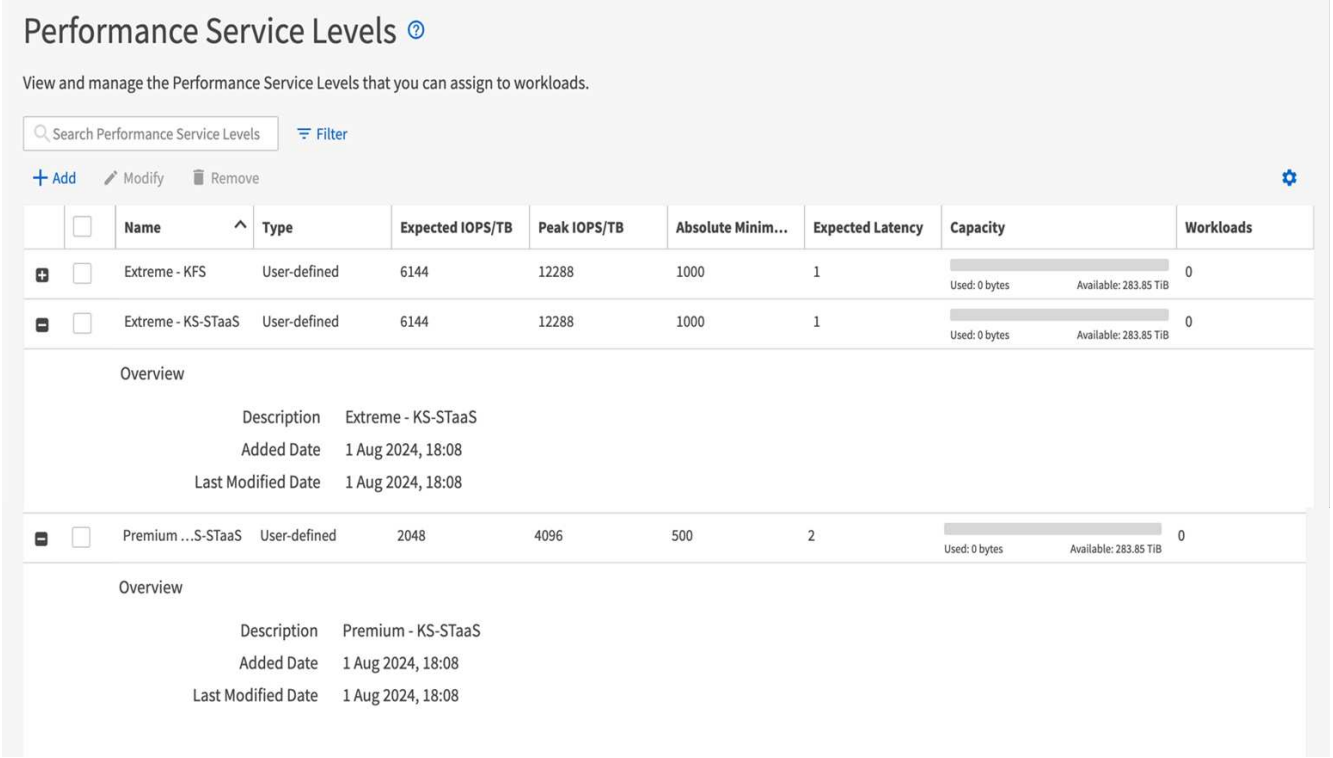
8. Todos los niveles de servicio de rendimiento de Keystone compatibles se mostrarán dentro de la opción *Seleccionar niveles de servicio de Keystone * para la versión de Keystone especificada. Habilite los niveles de servicio de rendimiento deseados de la lista.



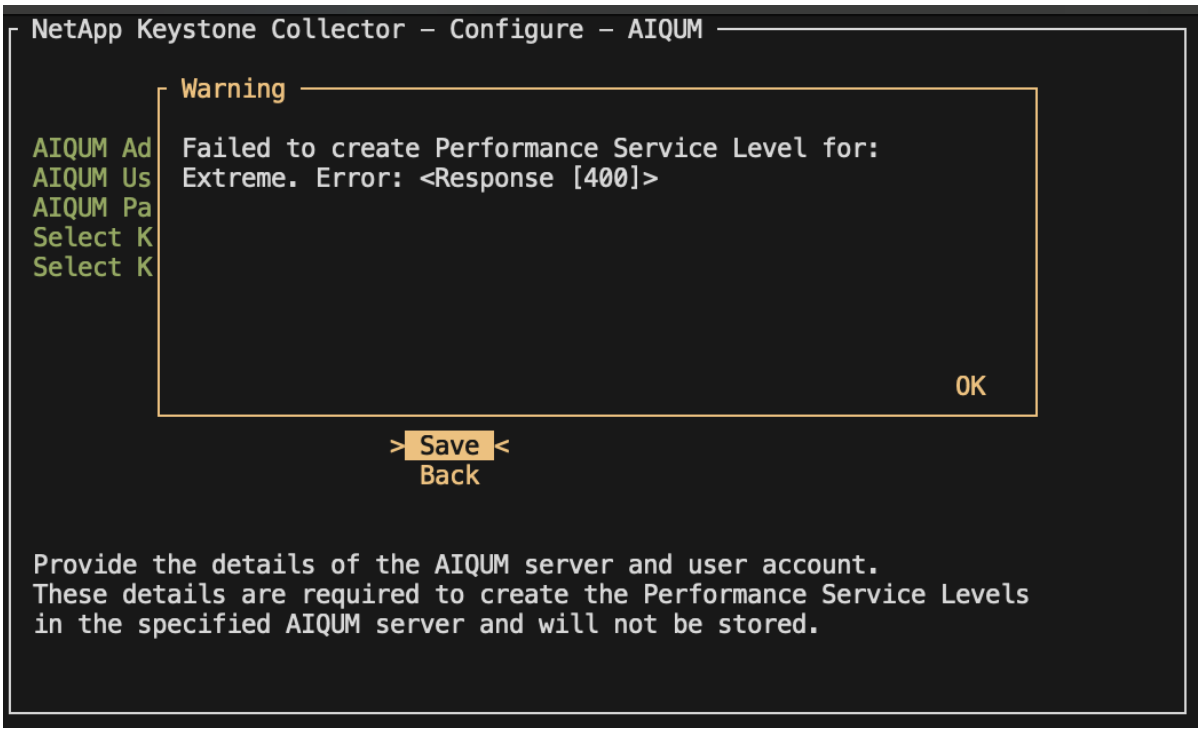
Puede seleccionar varios niveles de servicio de rendimiento simultáneamente para crear PSL.

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

   Puedes ver las PSL creadas, 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 las PSL creadas no cumplen con sus requisitos, puede modificar las PSL 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.



Instale el recopilador de ITOM

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 todos los requisitos previos requeridos.

Requisitos previos para la VM del servidor de recopilador ITOM:

- 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 recientes.

- Requisito de recurso: Los requisitos de recursos de la máquina virtual según la cantidad de nodos NetApp supervisados 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 supervisados. La máquina virtual del servidor de recopilador ITOM también debe configurarse como host de captura SNMP y servidor Syslog en el clúster de NetApp y los switches de clúster, si corresponde.

Requisitos de red

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

Origen	Destino	Protocolo	Puertos	Descripción
Recopilador de ITOM	IP de administración del clúster de NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Supervisión de las controladoras ONTAP
IP de gestión de nodos y clústeres de NetApp ONTAP	Recopilador de ITOM	SNMP, Syslog	UDP 162, UDP 514	Capturas SNMP y Syslogs de controladoras
Recopilador de ITOM	Switches de clúster	SNMP	UDP 161	Supervisión de los conmutadores
Switches de clúster	Recopilador de ITOM	SNMP, Syslog	UDP 162, UDP 514	Capturas SNMP y Syslogs de los switches
Recopilador de ITOM	IP de los nodos StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitorización SNMP de StorageGRID

IP de los nodos StorageGRID	Recopilador de ITOM	SNMP, Syslog	UDP 162, UDP 514	Trampas SNMP de StorageGRID
Recopilador de ITOM	Recopilador Keystone	SSH, HTTPS, SNMP	TCP 22, TCP 443 Y UDP 161	Supervisión y gestión remota de Keystone Collector
Recopilador de ITOM	DNS local	DNS	UDP 53	Servicios DNS públicos o privados
Recopilador de ITOM	Los servidores NTP de elección	NTP	UDP 123	Mantenimiento de 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 configuración de ITOM Collector, que caduca en dos horas.

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

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

Antes de empezar

- Compruebe que el shell Bourne está disponible para el script de instalación de Linux.
- Instale `vim-common` el paquete para obtener el binario **xxd** requerido para el archivo de configuración de ITOM Collector.
- Asegúrese de que `sudo package` está instalado si está planificando ejecutar el recopilador de ITOM como usuario no raíz.

Pasos

1. Descargue el archivo de configuración del recopilador ITOM en su servidor Linux.
2. Abra un 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 configuración del recopilador de ITOM:
   `#./<installer_file_name>.bin`
4. Si ejecuta el archivo de configuración, se le solicitará que:
   a. Acepte el contrato de licencia de usuario final (EULA).
   b. Introduzca los detalles del usuario para la instalación.
   c. Especifique el directorio principal de instalación.
   d. Seleccione el tamaño del recopilador.
   e. Proporcione los detalles del proxy, si procede.

      Para cada petición de datos, 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. Una vez finalizada la instalación, un mensaje confirma que el recopilador de ITOM se ha instalado correctamente.

- El archivo de configuración de ITOM Collector realiza adiciones `/etc/sudoers` para gestionar 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 root Privileges. Puede elegir un usuario diferente o ejecutarlo como root, pero se recomienda utilizar el usuario ITOM creado por el script de instalación de Linux.

El futuro

Una vez realizada correctamente la instalación, póngase en contacto con el equipo de soporte de Keystone para validar la correcta instalación de ITOM Collector a través del portal de soporte de ITOM. Después de la verificación, el equipo de soporte de Keystone configurará el recopilador de ITOM de forma remota, incluida la detección y la configuración de supervisión de dispositivos adicionales, y enviará una confirmación una vez que se complete la configuración. Para cualquier consulta o información adicional, póngase en contacto con keystone.services@NetApp.com.

Instalar Keystone ITOM Collector en sistemas Windows

Instale ITOM Collector en un sistema Windows descargando el archivo de configuración de ITOM Collector, ejecutando el asistente InstallShield e introduciendo las credenciales de supervisión necesarias.

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

Puede instalarlo en sistemas Linux según sus requisitos. Para instalar ITOM Collector en sistemas Linux, consulte "Instale ITOM Collector en sistemas Linux".

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

Antes de empezar

Asegúrese de que el servicio de recopilador de ITOM se concede **Iniciar sesión como servicio** bajo Política local/Asignación de derechos de usuario en la configuración de la directiva de seguridad local del servidor de Windows.

Pasos

1. Descargue el archivo de configuración del recopilador ITOM en su servidor Windows.
2. Abra el archivo de instalación para iniciar el asistente InstallShield.
3. Acepte el contrato de licencia de usuario final (EULA). El asistente InstallShield extrae los binarios necesarios y le solicita que introduzca las credenciales.
4. Introduzca las credenciales de la cuenta en la que 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, utilice una cuenta de dominio con permisos de administrador local.
   - Si ITOM Collector supervisa 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 establecer la contraseña para que no caduque, a fin de reducir los problemas de autenticación entre el recopilador de ITOM y sus recursos supervisados.

5. Seleccione el tamaño del recopilador. El valor predeterminado es el tamaño recomendado en función del archivo de configuración. Continúe con el tamaño sugerido a menos que tenga requisitos específicos.
6. Seleccione *Next* para comenzar la instalación. Puede utilizar la carpeta rellenada o elegir una diferente. Un cuadro de estado muestra el progreso de la instalación, seguido del cuadro de diálogo InstallShield Wizard Completado.

El futuro

Una vez realizada correctamente la instalación, póngase en contacto con el equipo de soporte de Keystone para validar la correcta instalación de ITOM Collector a través del portal de soporte de ITOM. Después de la verificación, el equipo de soporte de Keystone configurará el recopilador de ITOM de forma remota, incluida la detección y la configuración de supervisión de dispositivos adicionales, y enviará una confirmación una vez que se complete la configuración. Para cualquier consulta o información adicional, póngase en contacto con keystone.services@NetApp.com.

Configura AutoSupport para Keystone

Cuando se utiliza el mecanismo de telemetría 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 que envían los clústeres de ONTAP.

Acerca de esta tarea

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

- Puede editar las opciones de telemetría de AutoSupport mediante la CLI de ONTAP. Para obtener más información sobre la gestión de servicios de AutoSupport y el rol de administrador del sistema (clúster), consulte "Información general sobre Manage AutoSupport" y.. "Administradores de clústeres y SVM".
- Incluyes los subsistemas en los paquetes diarios y semanales de AutoSupport para garantizar la recogida de datos precisa para Keystone. Para obtener información sobre los subsistemas de AutoSupport, consulte "Qué son los subsistemas AutoSupport".

Pasos

1. Como usuario administrador del sistema, inicie sesión en el clúster de Keystone ONTAP mediante SSH. Para obtener más información, consulte "Acceda al clúster mediante SSH".
2. Modifique el contenido del log.
    - 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 log semanal:

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

Para obtener más información acerca de este comando, consulte "modificación del disparador AutoSupport del nodo del sistema".

Supervisar y actualizar

Supervise el estado de Keystone Collector

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

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

A continuación se muestra 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 supervisados están en buen estado
- **503**: indica que uno o más componentes no son saludables
- **403**: Indica que el cliente HTTP que consulta el estado de salud no está en la lista *allow*, que es una lista de CIDR de red permitidos. Para este estado, no se devuelve información de estado. La lista *allow* utiliza el método CIDR de red para controlar qué dispositivos de red pueden consultar el sistema de mantenimiento Keystone. Si recibe este error, agregue el sistema de monitorización a la lista *allow* de **Keystone Collector Management TUI > Configure > Health Monitoring**.

> **Usuarios de Linux, tenga en cuenta este problema conocido:**
>
> **Descripción del problema**: Keystone Collector ejecuta una serie de contenedores como parte del sistema de medición del uso. Cuando el servidor Red Hat Enterprise Linux 8.x está endurecido con las directivas de implementación técnica de seguridad (STIG) de la Agencia de sistemas de información de defensa de EE.UU. (DISA), se ha observado un problema conocido con fapolicyd (File Access Policy Daemon, demonio de políticas de acceso a archivos) intermitentemente. Este problema se identifica como "error 1907870". **Solución**: Hasta que Red Hat Enterprise lo resuelva, NetApp le recomienda solucionar este problema poniendo `fapolicyd` en modo permitido. Pulg /`etc/fapolicyd/fapolicyd.conf`, establezca el valor de `permissive = 1`.

Ver los registros del sistema

Puede ver los registros del sistema 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 estándar del sistema *journaltl*. Puede disponer de los siguientes servicios clave para examinar los registros:

- colector de ks
- ks-salud
- ks-autoupdate

El servicio principal de recopilación de datos *ks-collector* produce registros en formato JSON con un `run-id` atributo asociado a cada trabajo de recopilación de datos programado. A continuación se muestra un ejemplo de un trabajo correcto 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"}
```

A continuación se muestra un ejemplo de un trabajo correcto para la recogida de datos de rendimiento 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"}
```

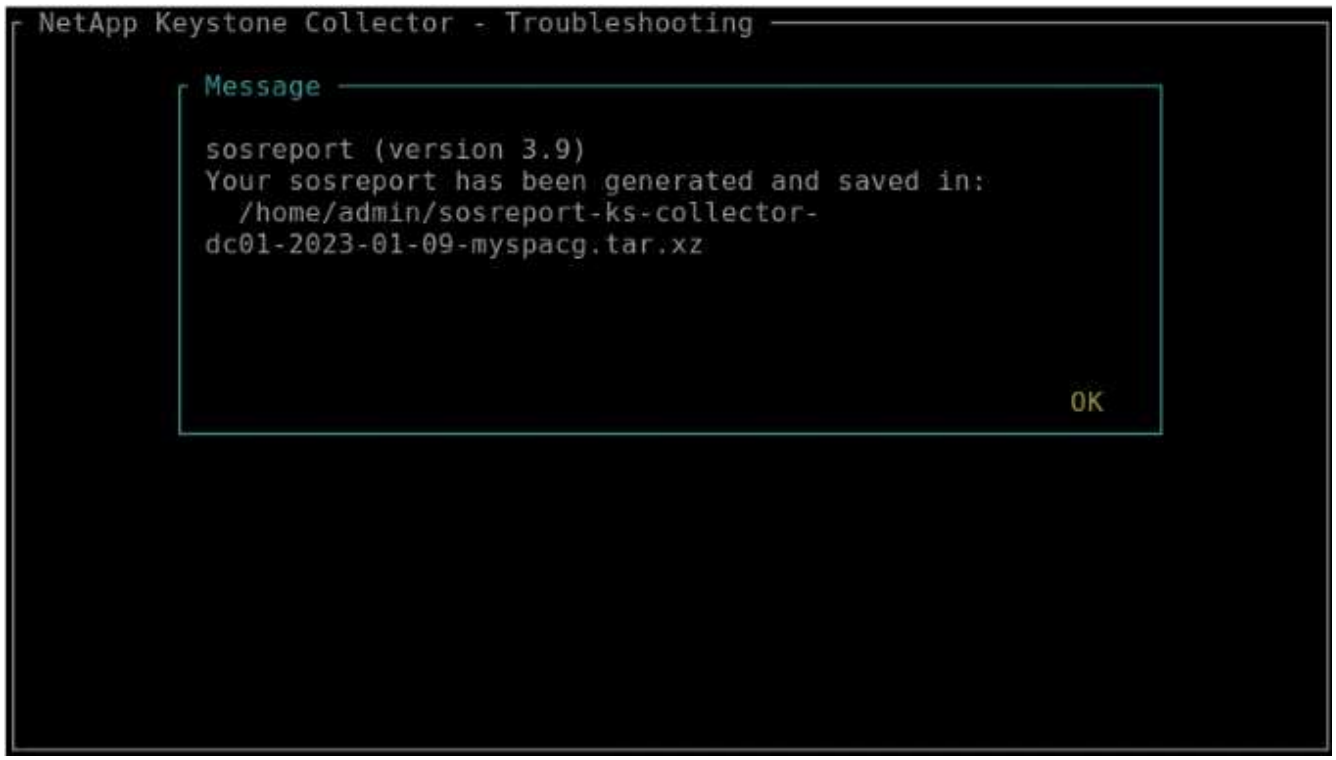
Genere y recoja paquetes de soporte

La TUI de Keystone Collector permite generar paquetes de soporte y luego añadir solicitudes de servicio para solucionar problemas de soporte. Siga este procedimiento:

Pasos

1. Inicie la utilidad TUI de gestión 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.



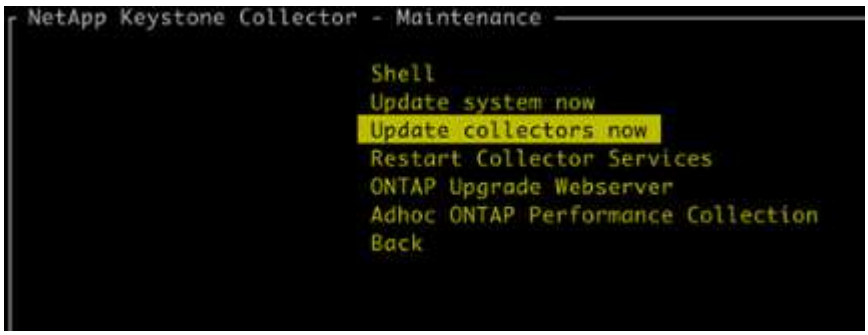
4. Una vez descargado el archivo, puedes adjuntarlo al ticket de soporte de Keystone ServiceNow. Para obtener información sobre cómo recaudar fondos, consulte "Generando solicitudes de servicio".

Actualice manualmente Keystone Collector

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

Pasos

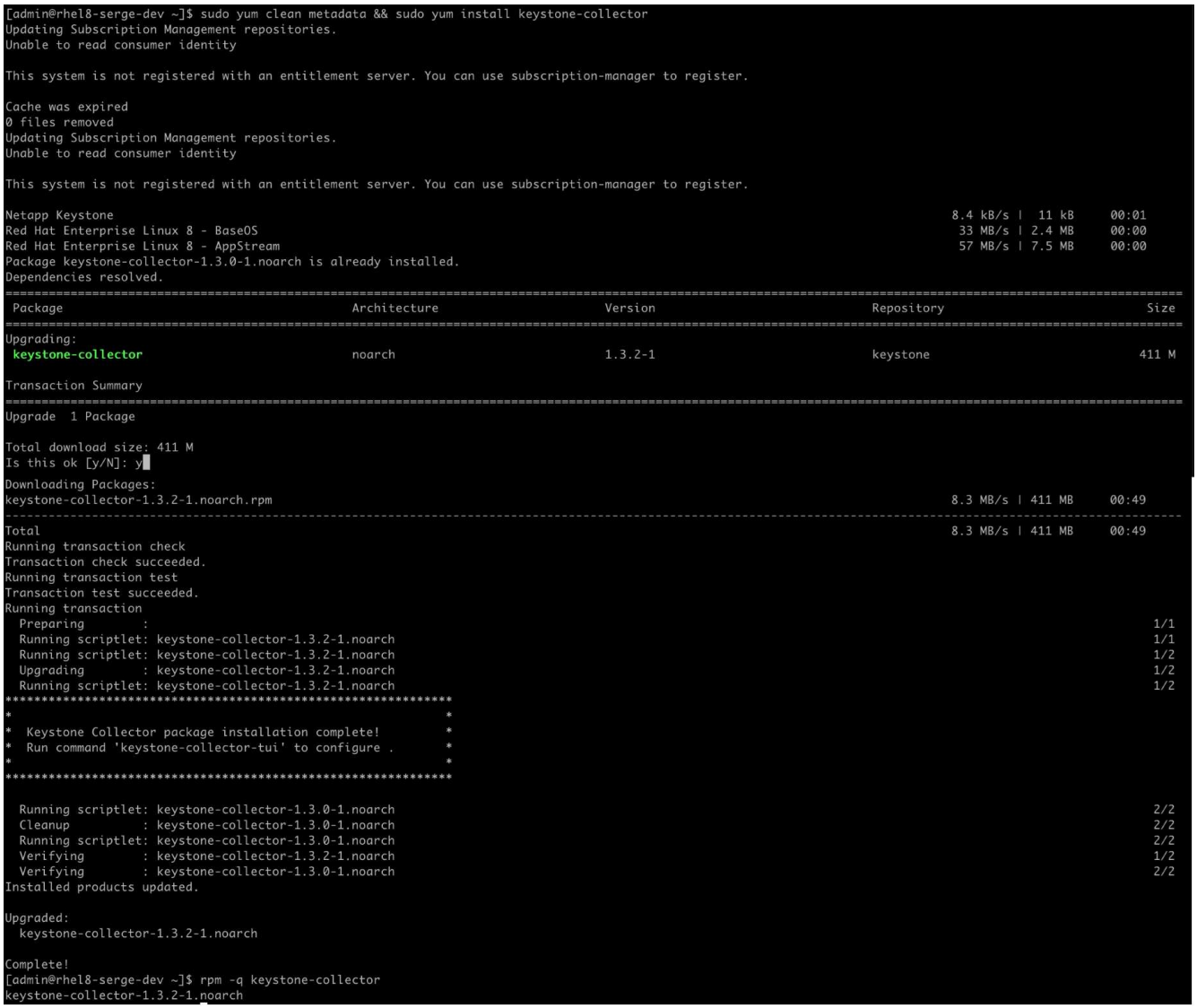
1. Inicie la utilidad TUI de gestión de Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. En la pantalla de mantenimiento, seleccione la opción **Actualizar colectores ahora**.



Como alternativa, 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 gestión del recopilador de Keystone, puede ver la versión más reciente en la parte superior izquierda de la pantalla de inicio.

   También puede ejecutar estos comandos para ver la versión más reciente:

   Para CentOS:

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

   Para Debian:

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

Seguridad de Keystone Collector

Keystone Collector incluye funciones de seguridad que supervisan las métricas de rendimiento y uso de los sistemas Keystone, sin poner en riesgo la seguridad de los datos de los clientes.

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 la supervisión del rendimiento. Para obtener más información, consulte "Datos recopilados para facturación". La "Eliminar datos privados" la opción está activada de forma predeterminada, que enmascara y protege la información confidencial.
- **Acceso con menos privilegios**-Keystone Collector requiere permisos mínimos para monitorear los sistemas de almacenamiento, lo que minimiza los riesgos de seguridad y evita cualquier modificación no intencionada de los datos. Este enfoque se alinea con el principio de privilegio mínimo, mejorando la postura de seguridad general de los entornos supervisados.
- **Marco de desarrollo de software seguro**- Keystone utiliza un marco de desarrollo de software seguro a lo largo del ciclo de desarrollo, que mitiga los riesgos, reduce las vulnerabilidades y protege el sistema contra posibles amenazas.

Seguridad reforzada

De forma predeterminada, Keystone Collector está configurado para usar configuraciones reforzadas de seguridad. A continuación, se muestran 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 de Keystone Collector puede reducir la seguridad del sistema. Para obtener más información, consulte "Guía de referencia de CIS".
  - Recibe e instala automáticamente parches de seguridad verificados por Keystone Collector a través de la función de actualización automática. Si desactiva esta funcionalidad, puede producirse un software vulnerable sin parches.
  - Autentica las actualizaciones recibidas de Keystone Collector. La desactivación de la verificación del repositorio de 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. Si desactiva esta función, se podría suplantar puntos finales externos y se podría producir una fuga de datos de uso.
- Keystone Collector admite "CA de confianza personalizada" certificación. De forma predeterminada, confía en los certificados firmados por las CA raíz públicas reconocidas por el "Programa Mozilla CA Certificate". Al habilitar CA de confianza adicionales, Keystone Collector habilita la validación de certificados HTTPS para las conexiones a los puntos finales que presentan estos certificados.
- Keystone Collector habilita la opción **Eliminar datos privados** de forma predeterminada, que enmascara y protege la información sensible. Para obtener más información, consulte "Limitar la recopilación de datos privados". Al deshabilitar esta opción, se comunican datos adicionales al sistema Keystone. Por ejemplo,

puede incluir información introducida por el usuario, como los nombres de volúmenes que pueden considerarse información confidencial.

Información relacionada

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

Tipos de datos de usuario que Keystone recopila

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. Puede recopilar datos de rendimiento solo para ONTAP si esta opción está habilitada en Keystone Collector.

Recogida de datos de ONTAP

Datos de uso recopilados para ONTAP: Learn more

La siguiente lista es un ejemplo representativo de los datos de consumo de capacidad recogidos para ONTAP:

- De clúster
  - ClusterUUID
  - Nombre del clúster
  - SerialNumber
  - Ubicación (según la entrada de valor en el clúster de ONTAP)
  - Contacto
  - Versión
- Nodos
  - SerialNumber
  - Nombre del nodo
- Volúmenes
  - Nombre del agregado
  - Nombre del volumen
  - VolumeInstanceUUID
  - Marca IsCloneVolume
  - Bandera IsFlexGroupConstituyente
  - Indicador IsSpaceEnforcedLogical
  - Indicador IsSpaceReportingLogical
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - QoSAdaptivePolicyGroup Name
  - Nombre de QoSPolicyGroup
  - Tamaño
  - Utilizado
  - Física
  - SizeUsedBySnapshots
  - Tipo
  - VolumeStyleExtended
  - Nombre del Vserver
  - Indicador IsVsRoot
- Vserver
  - Nombre del servidor

    - VserverUUID
    - Subtipo
- Agregados de almacenamiento
    - Tipo de almacenamiento
    - Nombre del agregado
    - UUID de agregado
    - Usado Físico
    - Talla disponible
    - Tamaño
    - Tamaño usado
- Almacenes de objetos agregados
    - ObjectStoreName
    - ObjectStoreUUID
    - ProviderType
    - Nombre del agregado
- Clonar volúmenes
    - FlexClone
    - Tamaño
    - Utilizado
    - Vserver
    - Tipo
    - Volumen de parteVolume
    - ParentVServer
    - IsConstituyente
    - SplitEstimate
    - Estado
    - FlexClone UdedPercent
- LUN de almacenamiento
    - UUID DE LUN
    - Nombre de LUN
    - Tamaño
    - Utilizado
    - Bandera IsReserved
    - Indicador IsRequested
    - Nombre de la unidad de LogialUnit
    - QoSPolicyUUID
    - QoSPolicyName

    - UUID de volumen
    - Nombre de volumen
    - SVMUUID
    - Nombre de SVM
- Volúmenes de almacenamiento
    - VolumeInstanceUUID
    - Nombre de volumen
    - Nombre de SVMName
    - SVMUUID
    - QoSPolicyUUID
    - QoSPolicyName
    - CapacidadTierFootprint
    - PerformanceTierFootprint
    - TotalFootprint
    - TieringPolicy
    - Bandera isProtected
    - Indicador IsDestination
    - Utilizado
    - Física
    - CloneParentUUID
    - LogicalSpaceUsedByAfs
- Grupos de políticas de calidad de servicio
    - PolicyGroup
    - QoSPolicyUUID
    - MaxThroughput
    - MinThroughput
    - MaxThroughputIOPS
    - MaxThroughputMBps
    - MinThroughputIOPS
    - MinThroughputMBps
    - Indicador IsShared
- Grupos de políticas de calidad de servicio adaptativa ONTAP
    - QoSPolicyName
    - QoSPolicyUUID
    - Pico de IOPS
    - Posición de la ALIVIOPSAllocation
    - AbsoluteMinIOPS

    - Número de IOP genérico
    - ExectedIOPSAllocation
    - Tamaño del bloque
- Huellas
    - Vserver
    - Volumen
    - TotalFootprint
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Node
    - Agregado
    - LIF
    - Replicación de configuración
    - Conexiones
    - De clúster
    - Volúmenes
- Clústeres MetroCluster
    - ClusterUUID
    - Nombre del clúster
    - RemoteClusterUUID
    - RemoteCluserName
    - LocalConfigurationState
    - RemoteConfigurationState
- 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
    - Reducida
    - Volumen de almacenamiento en uso
- Mediadores de MetroCluster
    - Dirección del mediador
    - Puerto Mediador
    - Mediador configurado
    - Mediador accesible
    - Modo
- Collector Métricas de Observabilidad
    - Hora de recogida
    - Se consulta el extremo de la API de Active IQ Unified Manager
    - Tiempo de respuesta
    - Número de registros
    - AIQUMInstance IP
    - ID ColleectorInstance

**Datos de rendimiento recopilados para ONTAP: Más información sobre **

La siguiente lista es un ejemplo representativo de los datos de rendimiento recogidos para ONTAP:

- Nombre del clúster
- UUID de clúster
- ID de objeto
- Nombre de volumen
- UUID de instancia de volumen
- Vserver
- VserverUUID
- Serie de nodos
- Versión de ONTAP
- Versión AIUM
- Agregado
- AgregarUUID
- ResourceKey
- Fecha/hora
- IOPSPerTb
- Latencia
- Latencia de lectura
- WriteMBps
- QoSMinThroughput latencia
- QoSNBladeLatency
- UsedHeadRoom
- CacheMissiRatio
- Latencia excepcional
- QoSAggregateLatency
- IOPS
- QoSNetworkLetency
- AvailableOPS
- Writelatencia
- QoSCloudLatency
- QoSClusterInterconnectLatency
- OtherMBps
- QoSCopLatency
- QoSDBladeLatency
- Utilización

- ReadIOPS
- Mbps
- OtherIOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncSnapmirrorLatency
- Datos a nivel de sistema
  - Escritura/Lectura/Otros/Total IOPS
  - Escritura/Lectura/Otros/Rendimiento total
  - Escritura/Lectura/Otro/Latencia total
- WriteIOPS

Lista de elementos eliminados al limitar el acceso privado a los datos: Learn more

Cuando la opción **Eliminar datos privados** está activada 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
- QoSAdaptivePolicyGroup Name
- Nombre de QoSPolicyGroup
- Nombre del Vserver
- Nombre de la LUN de almacenamiento
- Nombre del agregado
- Nombre de la unidad de LogialUnit
- Nombre de SVM
- AIQUMInstance IP
- FlexClone
- Nombre de clúster remoto

Recogida de datos de StorageGRID

Datos de uso recopilados para StorageGRID: Learn more

La siguiente lista es un ejemplo representativo de `Logical Data` Recopilado para StorageGRID:

- ID de StorageGRID
- ID de cuenta
- Nombre de cuenta
- Bytes de cuota de cuenta
- Nombre del bloque
- Recuento de objetos de bloque
- Bytes de datos de bloque

La siguiente lista es un ejemplo representativo de `Physical Data` Recopilado para StorageGRID:

- ID de StorageGRID
- ID de nodo
- ID del sitio
- Nombre del sitio
- Instancia
- Bytes de utilización del almacenamiento StorageGRID
- Bytes de metadatos de utilización del almacenamiento StorageGRID

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 al limitar el acceso privado a los datos: Learn more

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

- Nombre de cuenta
- BucketName
- Nombre del sitio
- Instance/NodeName

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 de 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

Más información sobre Keystone (modo privado)

Keystone ofrece un modo de implementación *private*, también conocido como *dark site*, para satisfacer sus requisitos empresariales y de seguridad. Este modo está disponible para organizaciones con restricciones de conectividad.

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

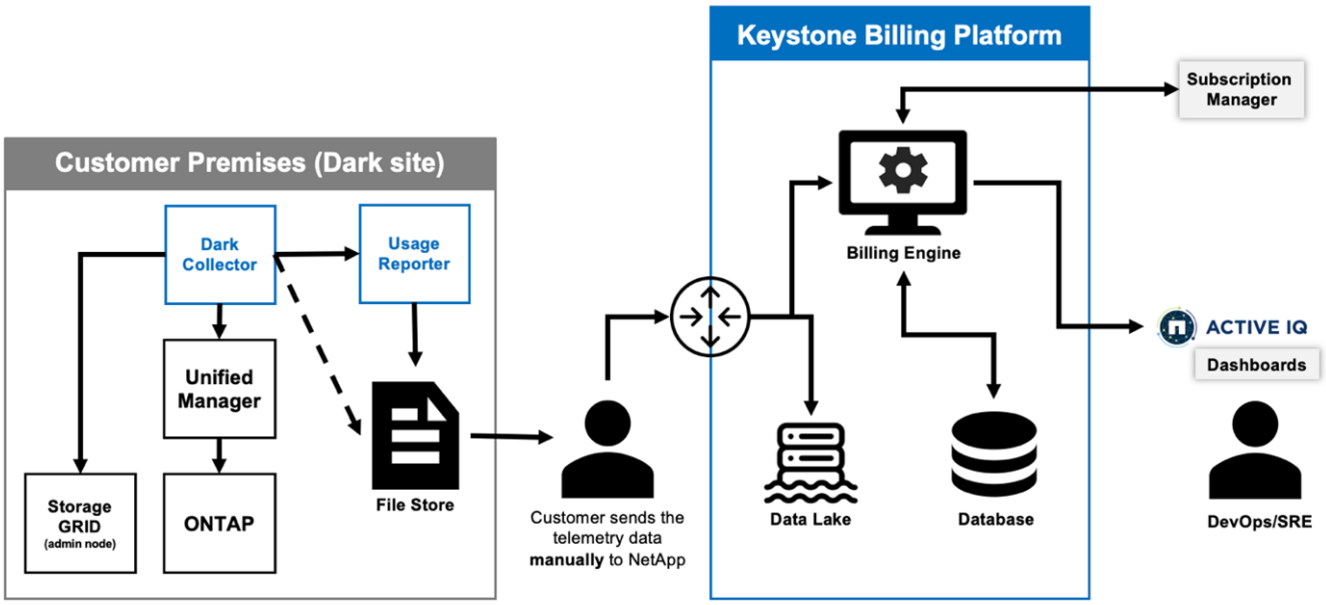
Para NetApp Keystone, ofrecer servicios para sitios oscuros implica proporcionar el servicio de suscripción de almacenamiento flexible de Keystone de forma que respete las restricciones de estos entornos. Esto implica:

- **Implementación local**: Keystone se puede configurar en entornos aislados de forma independiente, lo que garantiza que no sea necesario disponer de conectividad a Internet ni de personal externo para el acceso a la configuración.
- * Operaciones fuera de línea *: Todas las capacidades de administración de almacenamiento con controles de estado y facturación están disponibles fuera de línea 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 seguro y capacidades de auditoría detalladas.
- **Ayuda y soporte**: NetApp proporciona soporte global las 24/7 horas del día, los 7 días de la semana con un administrador de éxito de Keystone dedicado asignado a cada cuenta para asistencia y solución de problemas.

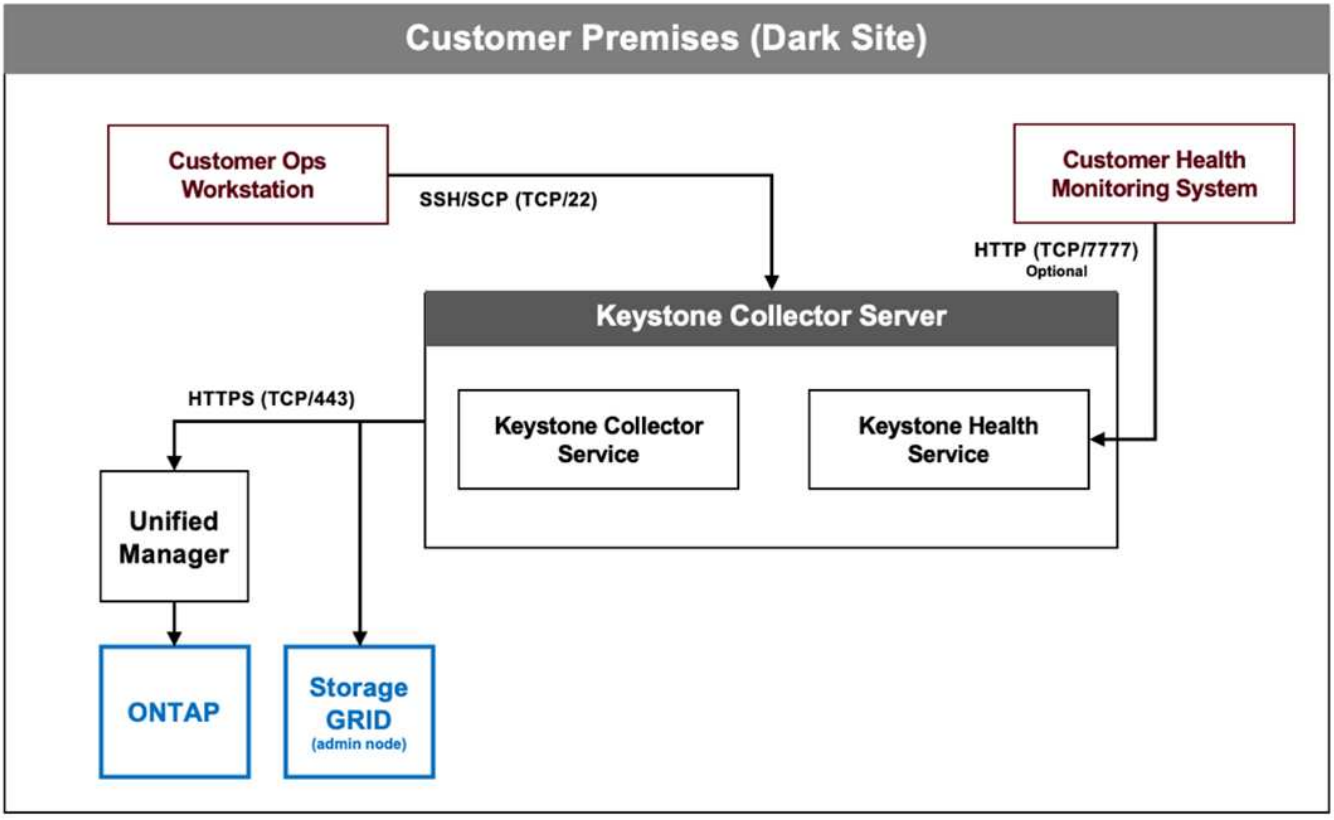
> Keystone Collector se puede configurar sin restricciones de conectividad, también conocido como modo *standard*. Para obtener más información, consulte "Más información sobre Keystone Collector".

Keystone Collector en modo privado

Keystone Collector es el responsable de recopilar periódicamente datos de uso de los sistemas de almacenamiento y exportar las métricas a un reportero del uso sin conexión y a un almacén de archivos local. Los archivos generados, que se crean en formatos de texto cifrado y sin formato, se reenvían manualmente a NetApp por el usuario después de las comprobaciones de validación. Una vez que los recibe, la plataforma de facturación Keystone de NetApp autentica y procesa estos archivos, integrándolos en los sistemas de gestión de facturas y suscripciones para calcular los cargos mensuales.



El servicio de recopilación de Keystone en el servidor tiene la tarea de recopilar periódicamente datos de uso, procesar esta información y generar un archivo de uso local en el servidor. El servicio de salud lleva a cabo comprobaciones del estado del sistema y está diseñado para interactuar con los sistemas de supervisión del estado utilizados por el cliente. Estos informes están disponibles para el acceso sin conexión por parte de los usuarios, 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 *dark site* o *private mode*, asegúrese de que sus sistemas estén preparados con el software necesario y cumplan con todos los requisitos previos necesarios.

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 de entrada libre `/var/lib/`
  - Al menos 48 GB de entrada libre `/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
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionlock
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - podman
  - sos
  - yum-utils
  - python3-dnf-plugin-versionlock
- Debian v12
  - python3 >= v3,9.0, python3 <= v3.12.0
  - podman

- informe de soporte

Requisitos de red

Los requisitos de red para Keystone Collector incluyen los siguientes:

- Active IQ Unified Manager (Unified Manager) 9,10 o posterior, configurado en un servidor con la funcionalidad de puerta de enlace API habilitada.
- El servidor de recopilación de Keystone en el puerto 443 (HTTPS) debe poder acceder al servidor de Unified Manager.
- Se debe configurar una cuenta de servicio con permisos de usuario de aplicaciones para Keystone Collector en el servidor de Unified Manager.
- No se requiere conexión 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 "Obtén ayuda con Keystone".

Instale Keystone Collector en modo privado

Complete algunos pasos para instalar Keystone Collector en un entorno que no tenga acceso a Internet, también conocido como *dark site* o *private mode*. Este tipo de instalación es perfecta para sus sitios seguros.

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

Ponga en marcha sus operaciones en VMware vSphere

Siga estos pasos:

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

Instalar en Linux

El software Keystone Collector se instala en el servidor Linux mediante 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 un terminal en el servidor y ejecute los siguientes comandos para comenzar la instalación.

   - **Usando el paquete Debian**

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

- **Utilizando el archivo RPM**

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

  o.

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

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

Configura Keystone Collector en modo privado

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

Keystone Collector ofrece la utilidad Interfaz de usuario del terminal (TUI) de gestión de recopiladores de Keystone para realizar actividades de configuración y supervisión. Puede usar varios controles del teclado, como las teclas Entrar y flecha, para seleccionar las opciones y navegar por esta TUI.

Pasos

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

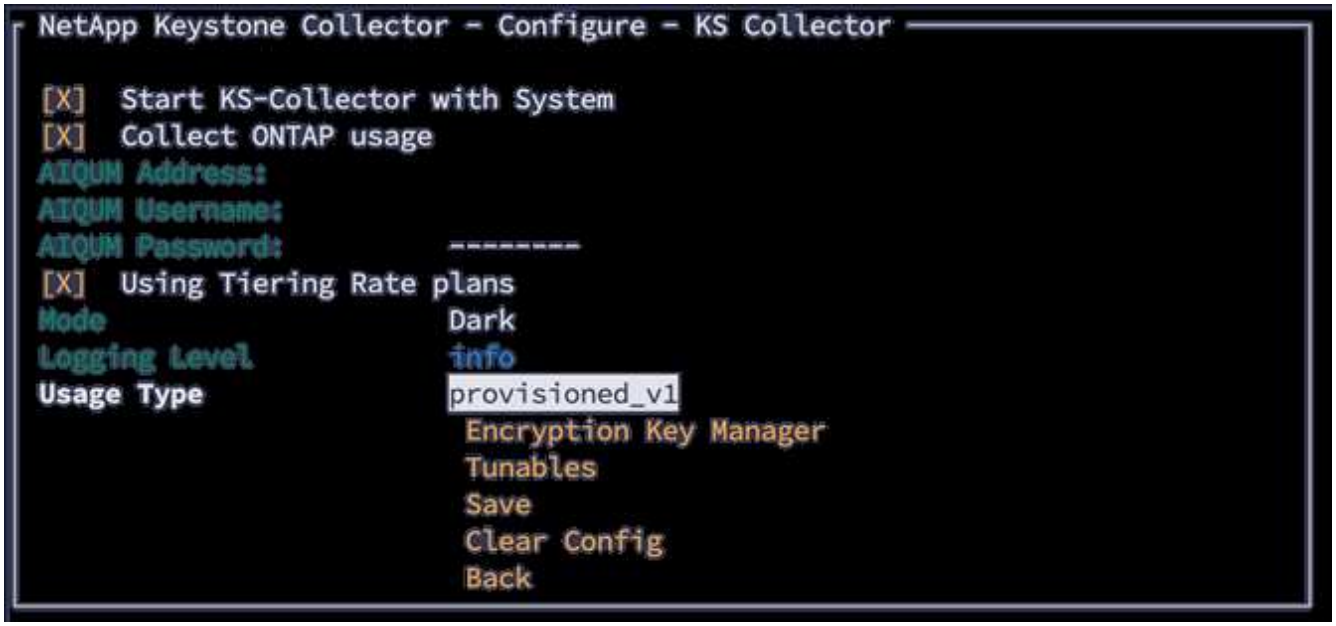
   ```
   keystone-collector-tui
   ```

2. Vaya a **Configure > Advanced**.
3. Alterna la opción **Modo Darksite**.

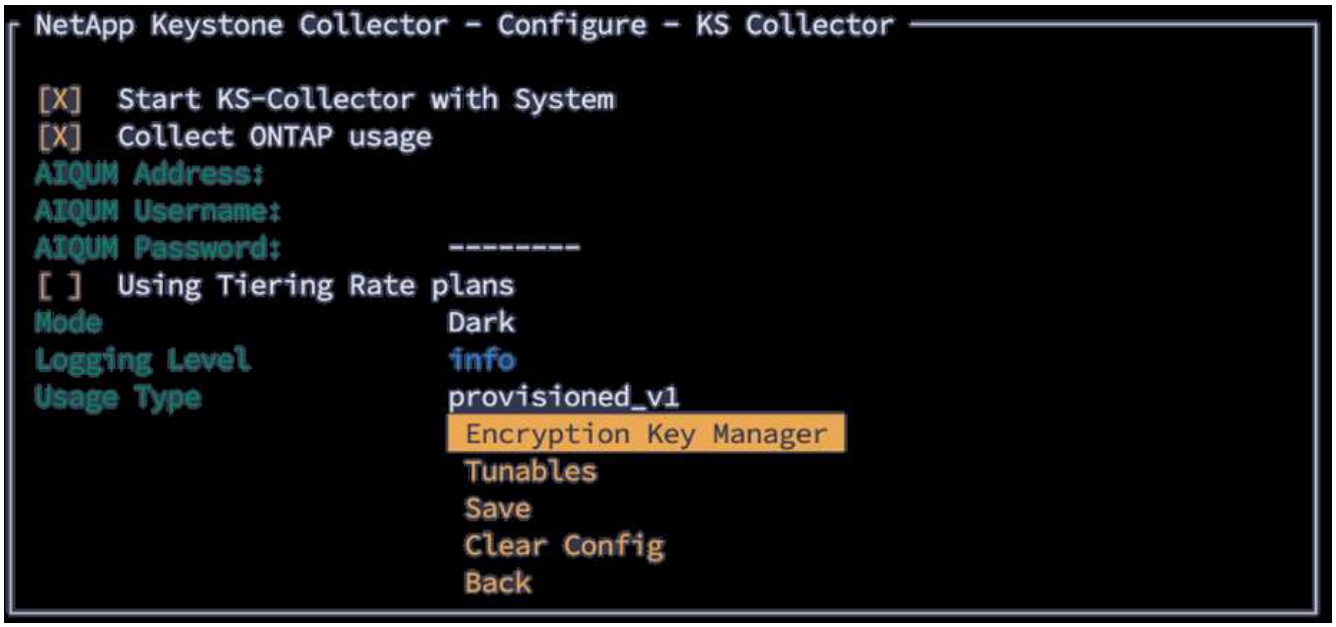
4. Seleccione **Guardar**.
5. Ve a **Configure > KS-Collector** para configurar Keystone Collector.
6. Alterne el campo **Start KS Collector with System**.

7. Alterne el campo **Recoger uso de ONTAP**. Añada los detalles del servidor y la cuenta de usuario de Active IQ Unified Manager (Unified Manager).
8. **Opcional**: Alterna el campo **Utilizando Planes de Tasa de Niveles** si se requiere la organización de datos en niveles para la suscripción.
9. En función del tipo de suscripción comprado, actualice el **Tipo de uso**.

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

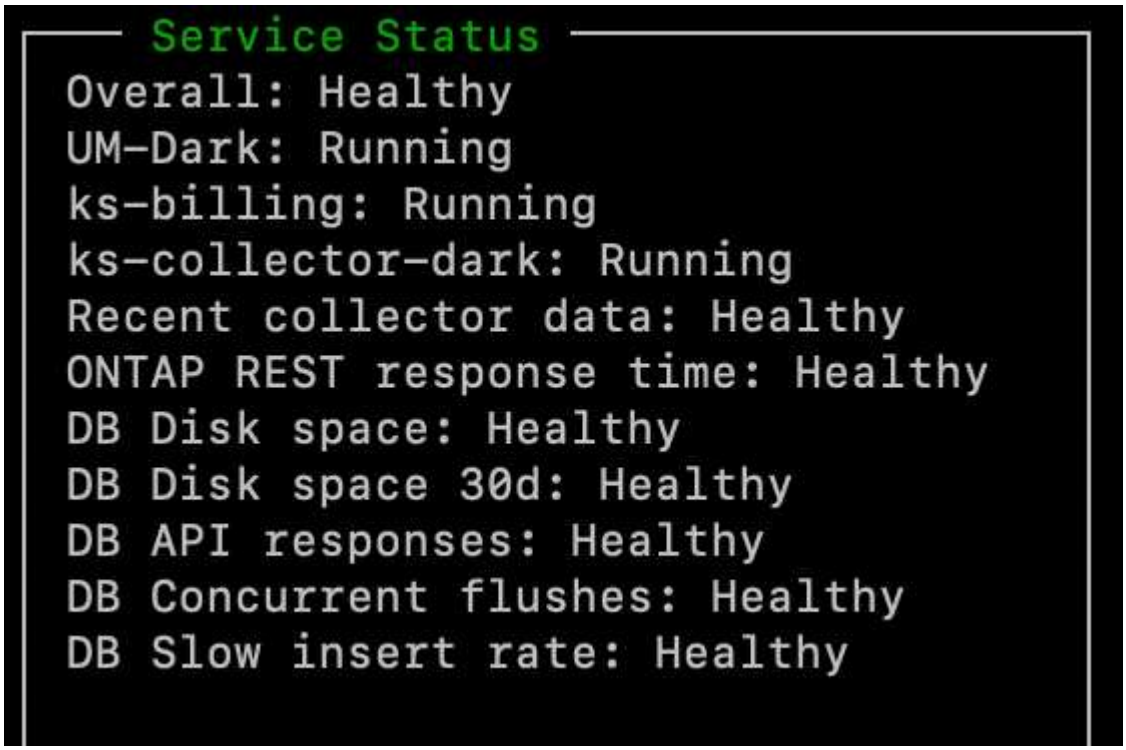


10. Seleccione **Guardar**.
11. Vaya a **Configure > KS-Collector** para generar el par de claves de Keystone Collector.
12. Vaya a **Encryption Key Manager** y presione Enter.



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

14. Asegúrese de que el recopilador Keystone esté 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 no es correcto después de este período, revise los pasos de configuración anteriores y póngase en contacto 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.

Exportar informe de uso

Debe enviar el informe de resumen de uso mensual a NetApp al final de cada mes. Este informe se puede generar manualmente.

Siga estos pasos para generar el informe de uso:

1. Vaya a **Export Usage** en la pantalla de inicio de Keystone Collector TUI.

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 tanto un archivo transparente como un archivo cifrado, que se debe enviar manualmente a NetApp. El informe de borrado de archivos contiene los siguientes detalles que puede validar 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-----
```

Actualice 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 a **/opt/NetApp/ONTAP-upgrade/** y, a continuación, seleccione **Iniciar servidor web** para iniciar el servidor web.

3. Vaya a `http://<collector-ip>:8000` Uso de un navegador web para obtener asistencia sobre la actualización.

Reinicia Keystone Collector

Puede reiniciar el servicio Keystone Collector a través de la TUI. Vaya a **Maintenance > Restart Collector** Services en TUI. Esto reiniciará todos los servicios de recopilador y su estado se puede supervisar desde la pantalla de inicio de TUI.

Supervisa el estado de Keystone Collector en modo privado

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

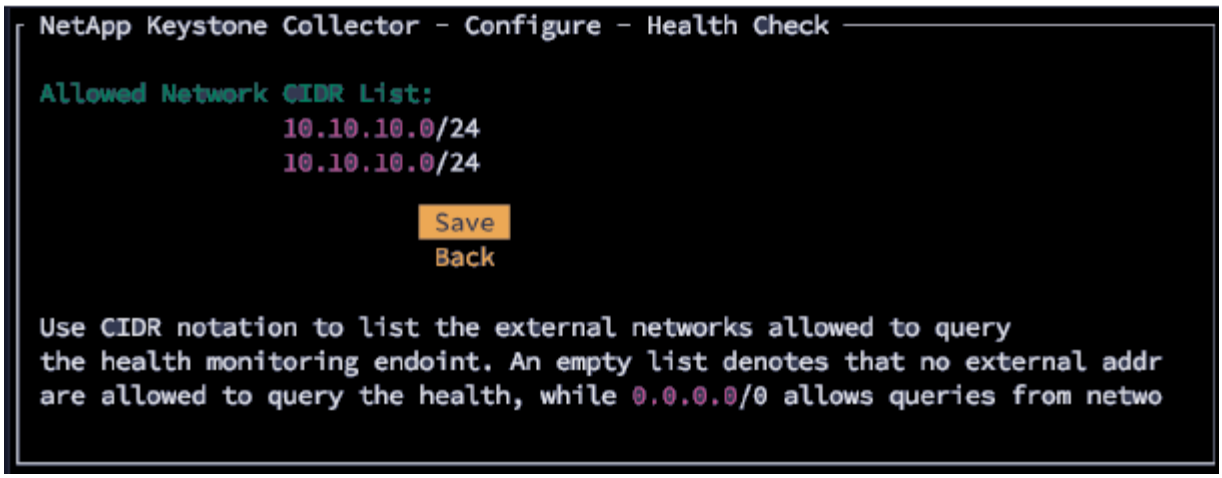
De forma predeterminada, los servicios de estado de Keystone no aceptan conexiones desde ninguna IP que no sea localhost. El extremo de estado de Keystone es `/uber/health`, Y escucha en todas las interfaces del servidor de Keystone Collector en el puerto `7777`. En la consulta, se devuelve un código de estado de solicitud HTTP con una salida JSON desde el extremo como respuesta, describiendo el estado del sistema Keystone Collector.
El cuerpo JSON proporciona un estado general de estado para el `is_healthy` atributo, que es booleano; y una lista detallada de estados por componente para `component_details` atributo.
A continuación se muestra 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 supervisados están en buen estado
- **503**: indica que uno o más componentes no son saludables
- **403**: Indica que el cliente HTTP que consulta el estado de salud no está en la lista *allow*, que es una lista de CIDR de red permitidos. Para este estado, no se devuelve información de estado.

  La lista *allow* utiliza el método CIDR de red para controlar qué dispositivos de red pueden consultar el sistema de mantenimiento Keystone. Si recibe el error 403, agregue su sistema de supervisión a la lista *allow* de **Keystone Collector management TUI > Configure > Health Monitoring**.

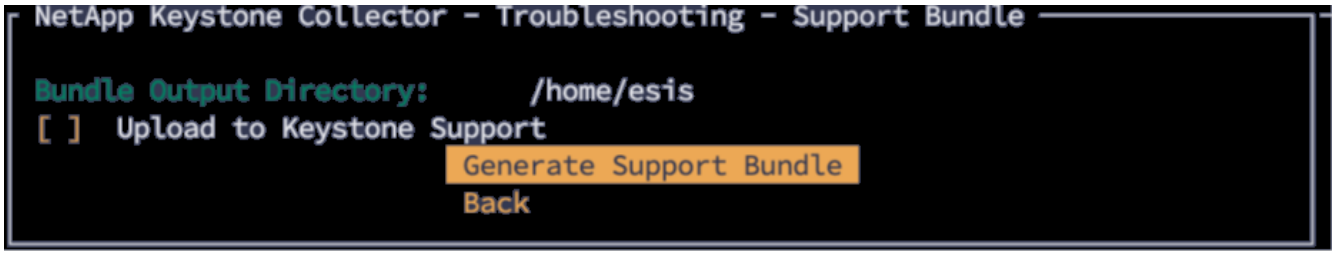


Genere y recoja paquetes de soporte

Para solucionar problemas con el recopilador de Keystone, puede trabajar con el soporte de NetApp que puede solicitar un archivo *.tar*. Puede generar este archivo mediante la utilidad TUI de gestión del recopilador Keystone.

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, luego haga clic en **Generar paquete de soporte**.



   Este proceso crea un `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 "Generando solicitudes de servicio".

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en http://www.netapp.com/TM son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.