# Configure y configure Keystone

## Keystone

NetApp
July 17, 2024

# Tabla de contenidos

# Configure y configure Keystone

# Requisitos

## Requisitos de infraestructura virtual

Se necesitan algunas configuraciones de infraestructura virtual para instalar Keystone Collector en sus sistemas VMware vSphere.

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

- Sistema operativo: VMware vCenter Server y ESXi 6.5 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 80, 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 del sistema Linux

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: CentOS 7 o Red Hat Enterprise Linux 8.6 o posterior
- 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 (3.6.8 a 3.9.13)

**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 80, 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

Debe completar algunos requisitos previos adicionales de ONTAP y StorageGRID. Asegúrese de completar estos requisitos previos específicos además de los requisitos del sistema Linux/VMware vSphere. Haga clic en la pestaña necesaria para obtener más información.

**ONTAP**

**Versiones de software**

1. ONTAP 9,8 o posterior
2. Active IQ Unified Manager (Unified Manager) 9,10 o posterior

**Antes de empezar**

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 *Paso 4: Revise los detalles*, verifique la corrección y autenticidad del archivo OVA.
   Las versiones de vCentre anteriores a 7.0u2 no pueden verificar automáticamente la autenticidad del certificado de firma de código. VCentre 7.0u2 y posteriores pueden realizar las verificaciones, sin embargo, para esto, la autoridad de certificación de firma debe añadirse a vCentre. Siga estas instrucciones para su versión de vCentre:

   **VCentre 7.0u1 y anteriores: Más información**

   VCentre valida la integridad del contenido del archivo OVA y que se proporciona un resumen de firma de código válido para los archivos contenidos en el archivo OVA. Sin embargo, no valida la autenticidad del certificado de firma de código. Para verificar la integridad, debe descargar el certificado de resumen de firma completo y verificarlo con el certificado público publicado por Keystone.

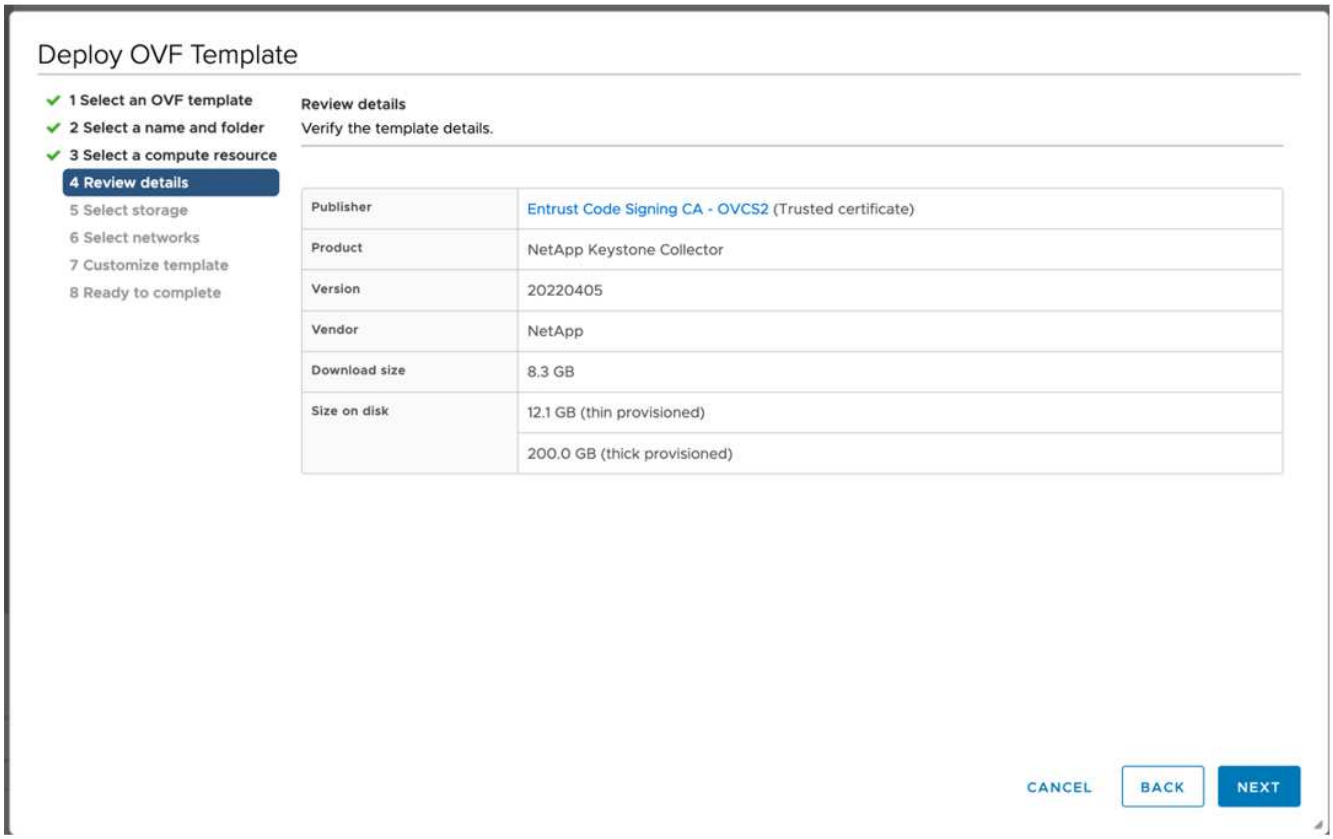
   a. Haga clic en el enlace **Publisher** para descargar el certificado de resumen de firma completo.
   b. Descargue el certificado público *Keystone Billing* en "este enlace".
   c. Compruebe la autenticidad del certificado de firma OVA en el certificado público mediante OpenSSL:
      `openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert`

   **VCentre 7.0u2 y posteriores: Más información**

   7.0u2 y las versiones posteriores de vCenter pueden validar la integridad del contenido del archivo OVA y la autenticidad del certificado de firma de código cuando se proporciona un resumen de firma de código válido. El almacén de confianza raíz de vCenter solo contiene certificados de VMware. NetApp utiliza Entrust como autoridad certificadora, y dichos certificados deben agregarse al almacén de confianza de vCenter.

   a. Descargue el certificado CA de firma de código de Entrust "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.

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




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

El software Keystone Collector se distribuye mediante un repositorio de software de YUM en línea. Debe importar e instalar el archivo en un servidor Linux.

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

1. SSH al servidor de Keystone Collector y vaya a. `root` privilegio.
2. Importe la firma de firma pública de Keystone:
   `# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101`
3. Asegúrese de importar el certificado público correcto comprobando la huella digital de la plataforma de facturación Keystone en la base de datos RPM:
   `# rpm -qa gpg-pubkey --qf '%<Description>'|gpg --show-keys --fingerprint`
   La huella digital correcta tiene este aspecto:
   `90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D`
4. Descargue el `keystonerepo.rpm` archivo:
   `curl -O https://keystone.netapp.com/repo/keystonerepo.rpm`
5. Verifique la autenticidad del archivo:
   `rpm --checksig -v keystonerepo.rpm`Una firma para un archivo auténtico tiene este aspecto:
   `Header V4 RSA/SHA512 Signature, key ID 33b6c17d: 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`

> 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 de la integridad del software

Hay un proceso reiterativo de validación de la integridad del software Keystone.

La configuración del cliente de repositorio de Keystone YUM que se proporciona 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 función de actualización automática programada de Keystone Collector para garantizar que sólo se haya instalado 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 que solo debe realizarse una vez para activar y asociar el componente recopilador necesario con el entorno de almacenamiento de.

> El recopilador de Keystone incluye la utilidad de 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 **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 **

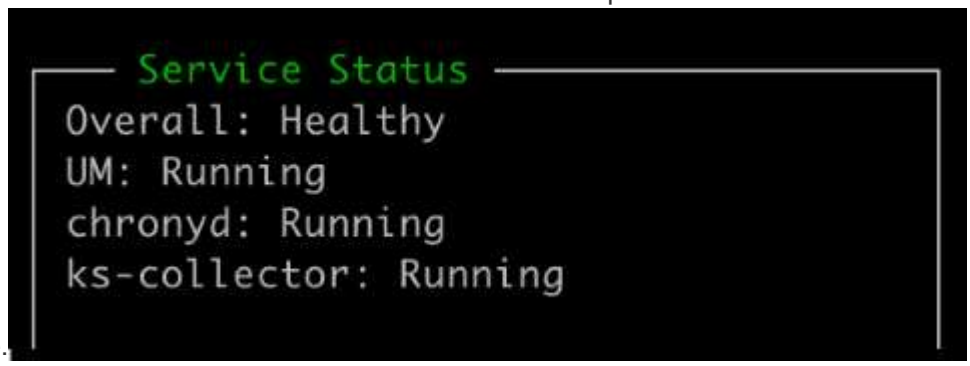
   - **Recopilar uso de ONTAP**: Esta opción permite la recopilación de datos de uso para ONTAP. Añada los detalles del servidor y la cuenta de servicio de Active IQ Unified Manager (Unified Manager).
   - **Recopilar datos de rendimiento de ONTAP**: Esta opción permite la recopilación de datos de rendimiento 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**.



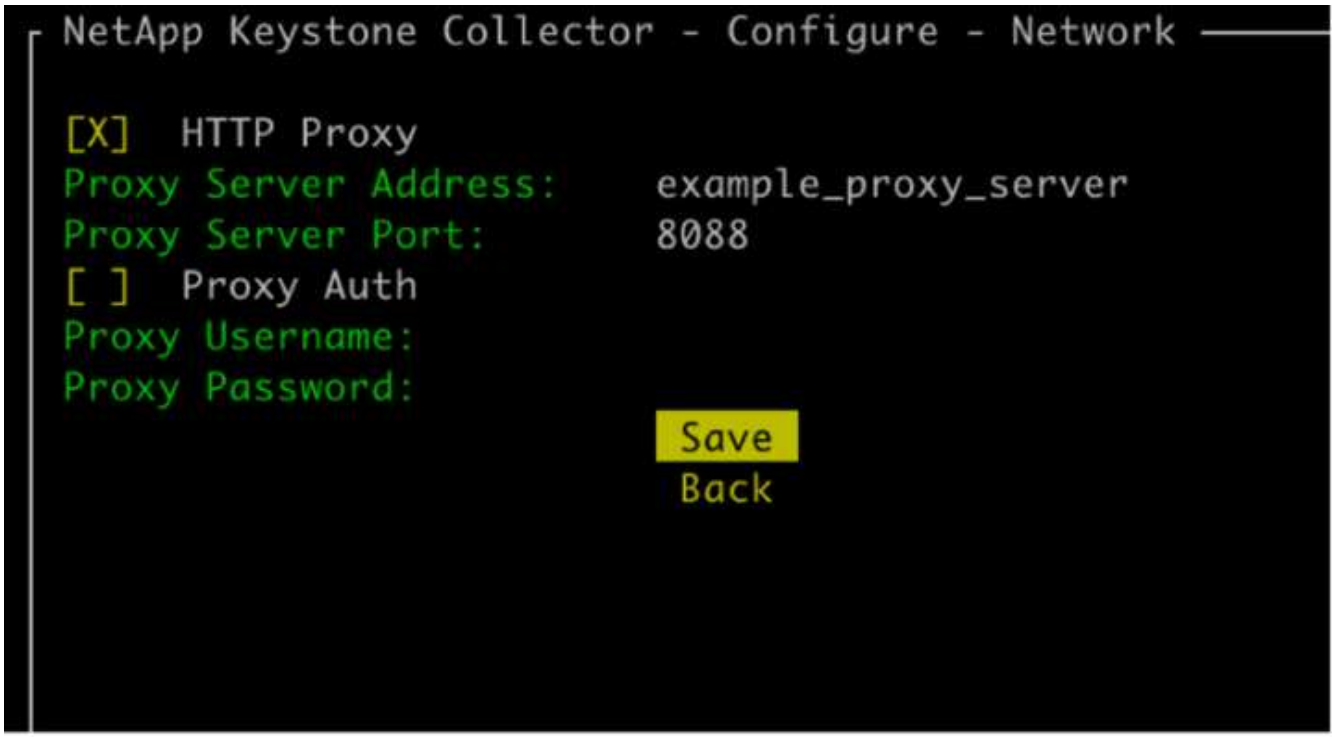

7. Salga de la TUI de gestión de Keystone Collector seleccionando la opción **salir a Shell** en la pantalla de inicio.

## 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 de configuración, estado y rendimiento necesaria para realizar mediciones 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:

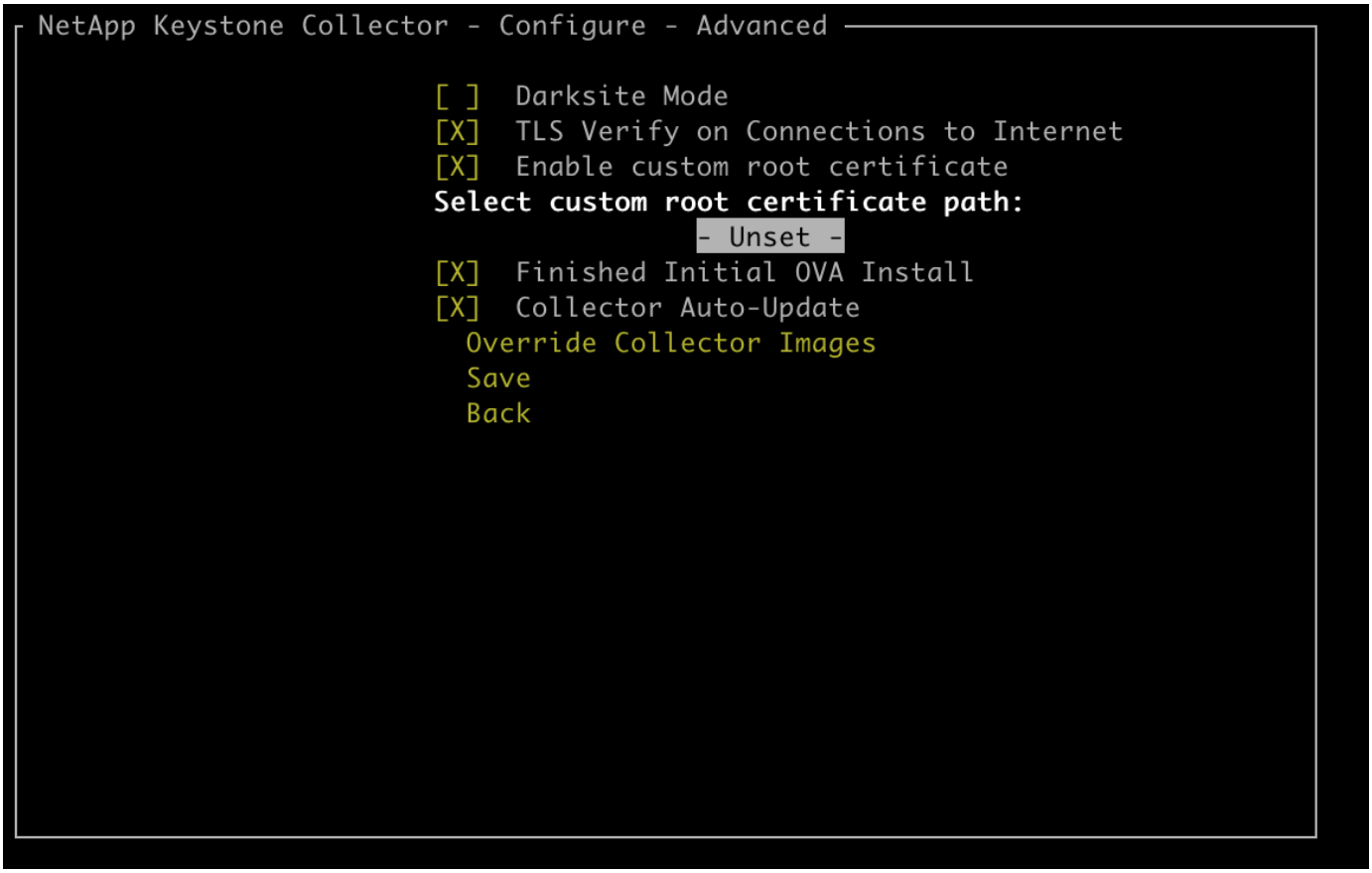
**Pasos**

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.




# 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.
   - 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
     ```

   - 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".

# 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 para sus suscripciones a Keystone ONTAP y Keystone StorageGRID. También puede recopilar datos de rendimiento solo para ONTAP si la 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
- 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
- Clústeres MetroCluster
    - ClusterUUID
    - Nombre del clúster
    - RemoteClusterUUID
    - RemoteCluserName
    - LocalConfigurationState
    - RemoteConfigurationState
    - 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
- 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

**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