Configurar o Keystone

Keystone

NetApp
February 19, 2026

Índice

Configurar o Keystone

Requisitos

Requisitos de infraestrutura virtual para o Keystone Collector

Seu sistema VMware vSphere deve atender a vários requisitos antes de instalar o Keystone Collector.

Pré-requisitos para a VM do servidor Keystone Collector:

- Sistema operacional: servidor VMware vCenter e ESXi 8.0 ou posterior
- Núcleo: 1 CPU
- RAM: 2 GB DE RAM
- Espaço em disco: 20 GB vDisk

Outros requisitos

Certifique-se de que os seguintes requisitos genéricos são cumpridos:

Requisitos de rede

Os requisitos de rede do Keystone Collector estão listados na tabela a seguir.

> O Keystone Collector requer conetividade com a Internet. Você pode fornecer conetividade à Internet por roteamento direto através do Gateway padrão (via NAT) ou através do proxy HTTP. Ambas as variantes são descritas aqui.

Fonte	Destino	Serviço	Protocolo e portas	Categoria	Finalidade
Coletor Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Gerenciador unificado)	HTTPS	TCP 443	Obrigatório (se estiver usando o Keystone ONTAP)	Coleção de métricas de uso do Keystone Collector para ONTAP
Coletor Keystone (para Keystone StorageGRID)	Nós de administração do StorageGRID	HTTPS	TCP 443	Obrigatório (se estiver usando o Keystone StorageGRID)	Coleção de métricas de uso do Keystone Collector para StorageGRID

Keystone Collector (genérico)	Internet (de acordo com os requisitos de URL fornecidos posteriormente)	HTTPS	TCP 443	Obrigatório (ligação à Internet)	O software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Proxy HTTP do cliente	Proxy HTTP	Porta proxy do cliente	Obrigatório (ligação à Internet)	O software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Servidores DNS do cliente	DNS	TCP/UDP 53	Obrigatório	Resolução DNS
Keystone Collector (genérico)	Servidores NTP do cliente	NTP	UDP 123	Obrigatório	Sincronização de tempo
Coletor Keystone (para Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funcionalidade opcional	Coleção de métricas de desempenho para o Keystone Collector
Keystone Collector (genérico)	Sistema de monitorização de clientes	HTTPS	TCP 7777	Funcionalidade opcional	Relatório de integridade do Keystone Collector
Estações de trabalho de operações do cliente	Keystone Collector	SSH	TCP 22	Gerenciamento	Acesso ao gerenciamento do Keystone Collector
Endereços de gerenciamento de nós e clusters do NetApp ONTAP	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Funcionalidade opcional	Servidor Web para atualizações de firmware do ONTAP

A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante uma nova instalação do Unified Manager, o que impede a coleção de métricas de desempenho para o Keystone Collector. Para obter mais informações, "Requisitos da ONTAP"consulte .

Acesso a URL

O Keystone Collector precisa de acesso aos seguintes hosts de internet:

Endereço	Motivo
https://keystone.netapp.com	Atualizações do software Keystone Collector e relatórios de uso
https://support.netapp.com	Sede da NetApp para informações de faturamento e entrega do AutoSupport

Requisitos do Linux para o Keystone Collector

Preparar seu sistema Linux com o software necessário garante a instalação precisa e a coleta de dados pelo Keystone Collector.

Certifique-se de que a VM do servidor do Keystone Collector Linux e do Keystone tenha essas configurações.

Servidor Linux:

- Sistema operacional: Qualquer um dos seguintes:
  - Debian 12
  - Red Hat Enterprise Linux 8,6 ou versões posteriores 8.x
  - Red Hat Enterprise Linux 9.0 ou versões posteriores
  - CentOS 7 (somente para ambientes existentes)
- Cronyd tempo sincronizado
- Acesso aos repositórios de software padrão do Linux

O mesmo servidor também deve ter os seguintes pacotes de terceiros:

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

Servidor VM do Keystone Collector:

- Núcleo: 2 CPUs
- RAM: 4 GB DE RAM
- Espaço em disco: 50 GB vDisk

Outros requisitos

Certifique-se de que os seguintes requisitos genéricos são cumpridos:

Requisitos de rede

Os requisitos de rede do Keystone Collector estão listados na tabela a seguir.

> O Keystone Collector requer conetividade com a Internet. Você pode fornecer conetividade à Internet por roteamento direto através do Gateway padrão (via NAT) ou através do proxy HTTP. Ambas as variantes são descritas aqui.

Fonte	Destino	Serviço	Protocolo e portas	Categoria	Finalidade
Coletor Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Gerenciador unificado)	HTTPS	TCP 443	Obrigatório (se estiver usando o Keystone ONTAP)	Coleção de métricas de uso do Keystone Collector para ONTAP
Coletor Keystone (para Keystone StorageGRID)	Nós de administração do StorageGRID	HTTPS	TCP 443	Obrigatório (se estiver usando o Keystone StorageGRID)	Coleção de métricas de uso do Keystone Collector para StorageGRID
Keystone Collector (genérico)	Internet (de acordo com os requisitos de URL fornecidos posteriormente)	HTTPS	TCP 443	Obrigatório (ligação à Internet)	O software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Proxy HTTP do cliente	Proxy HTTP	Porta proxy do cliente	Obrigatório (ligação à Internet)	O software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Servidores DNS do cliente	DNS	TCP/UDP 53	Obrigatório	Resolução DNS

Keystone Collector (genérico)	Servidores NTP do cliente	NTP	UDP 123	Obrigatório	Sincronização de tempo
Coletor Keystone (para Keystone ONTAP)	Unified Manager	MYSQL	TCP 3306	Funcionalidade opcional	Coleção de métricas de desempenho para o Keystone Collector
Keystone Collector (genérico)	Sistema de monitorização de clientes	HTTPS	TCP 7777	Funcionalidade opcional	Relatório de integridade do Keystone Collector
Estações de trabalho de operações do cliente	Keystone Collector	SSH	TCP 22	Gerenciamento	Acesso ao gerenciamento do Keystone Collector
Endereços de gerenciamento de nós e clusters do NetApp ONTAP	Keystone Collector	HTTP_8000, PING	TCP 8000, ICMP Echo Request/Reply	Funcionalidade opcional	Servidor Web para atualizações de firmware do ONTAP

A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante uma nova instalação do Unified Manager, o que impede a coleção de métricas de desempenho para o Keystone Collector. Para obter mais informações, "Requisitos da ONTAP"consulte .

Acesso a URL

O Keystone Collector precisa de acesso aos seguintes hosts de internet:

Endereço	Motivo
https://keystone.netapp.com	Atualizações do software Keystone Collector e relatórios de uso
https://support.netapp.com	Sede da NetApp para informações de faturamento e entrega do AutoSupport

Requisitos para ONTAP e StorageGRID para Keystone

Antes de começar a usar o Keystone, você precisa garantir que os clusters do ONTAP e os sistemas StorageGRID atendam a alguns requisitos.

ONTAP

Versões de software

1. ONTAP 9 .8 ou posterior
2. Active IQ Unified Manager (Gerenciador Unificado) 9,10 ou posterior

Antes de começar

Cumpra os seguintes requisitos se pretender recolher dados de utilização apenas através do ONTAP:

1. Certifique-se de que o ONTAP 9,8 ou posterior está configurado. Para obter informações sobre como configurar um novo cluster, consulte estes links:
   - "Configure o ONTAP em um novo cluster com o Gerenciador do sistema"
   - "Configure um cluster com a CLI"
2. Crie contas de login do ONTAP com funções específicas. Para saber mais, "Saiba mais sobre como criar contas de login do ONTAP" consulte .
   - * UI da Web*
     i. Faça login no Gerenciador de sistemas do ONTAP usando suas credenciais padrão. Para saber mais, "Gerenciamento de clusters com o System Manager" consulte .
     ii. Crie um utilizador ONTAP com a função "readonly" e o tipo de aplicação "http" e ative a autenticação da palavra-passe navegando para **Cluster > Definições > Segurança > utilizadores**.
   - **CLI**
     i. Faça login na CLI do ONTAP usando suas credenciais padrão. Para saber mais, "Gerenciamento de clusters com CLI" consulte .
     ii. Crie um usuário ONTAP com a função "readonly" e o tipo de aplicativo "http" e ative a autenticação de senha. Para saber mais sobre autenticação, "Ative o acesso à palavra-passe da conta ONTAP" consulte .

Atenda aos seguintes requisitos se você pretende coletar dados de uso por meio do Active IQ Unified Manager:

1. Certifique-se de que o Unified Manager 9,10 ou posterior esteja configurado. Para obter informações sobre a instalação do Unified Manager, consulte estes links:
   - "Instalação do Unified Manager em sistemas VMware vSphere"
   - "Instalar o Unified Manager em sistemas Linux"
2. Certifique-se de que o cluster do ONTAP foi adicionado ao Unified Manager. Para obter informações sobre como adicionar clusters, "Adição de clusters" consulte .
3. Crie usuários do Unified Manager com funções específicas para coleta de dados de uso e performance. Execute estas etapas. Para obter informações sobre funções de usuário, "Definições de funções de utilizador" consulte .
   a. Faça login na IU da Web do Unified Manager com as credenciais de usuário padrão do administrador do aplicativo que são geradas durante a instalação. "Acessando a IU da Web do Unified Manager"Consulte .
   b. Crie uma conta de serviço para o Keystone Collector com `Operator` função de usuário. As APIs de serviço do Keystone Collector usam essa conta de serviço para se comunicar com o Unified Manager e coletar dados de uso. "Adicionando usuários"Consulte .

c. Crie uma `Database` conta de usuário, com a `Report Schema` função. Este utilizador é necessário para a recolha de dados de desempenho. "Criando um usuário de banco de dados"Consulte .

> A porta padrão para MySQL, 3306, é restrita apenas ao localhost durante uma nova instalação do Unified Manager, o que impede a coleta de dados de desempenho para o Keystone ONTAP. Essa configuração pode ser modificada e a conexão pode ser disponibilizada a outros hosts usando a `Control access to MySQL port 3306` opção no console de manutenção do Unified Manager. Para obter informações, "Opções de menu adicionais"consulte .

4. Ative o API Gateway no Unified Manager. O Keystone Collector faz uso do recurso de gateway de API para se comunicar com clusters do ONTAP. Você pode ativar o API Gateway a partir da IU da Web ou executando alguns comandos por meio da CLI do Unified Manager.

   UI da Web

   Para ativar o API Gateway a partir da IU da Web do Unified Manager, inicie sessão na IU da Web do Unified Manager e ative o API Gateway. Para obter informações, "Ativando o API Gateway"consulte .

   CLI

   Para ativar o API Gateway por meio da CLI do Unified Manager, siga estas etapas:

   a. No servidor do Unified Manager, inicie uma sessão SSH e faça login na CLI do Unified Manager. `um cli login -u <umadmin>` Para obter informações sobre comandos CLI, "Comandos de CLI do Unified Manager compatíveis" consulte .

   b. Verifique se o API Gateway já está ativado.
   `um option list api.gateway.enabled` Um `true` valor indica que o API Gateway está ativado.

   c. Se o valor retornado for `false`, execute este comando:
   `um option set api.gateway.enabled=true`

   d. Reinicie o servidor do Unified Manager:

      - Linux: "Reiniciando o Unified Manager".
      - VMware vSphere: "Reiniciando a máquina virtual do Unified Manager".

StorageGRID

As configurações a seguir são necessárias para instalar o Keystone Collector no StorageGRID.

- StorageGRID `11.6.0` ou posterior deve ser instalado. Para obter informações sobre como atualizar o StorageGRID, "Atualizar o software StorageGRID: Visão geral"consulte .
- Uma conta de usuário de administrador local do StorageGRID deve ser criada para coleta de dados de uso. Essa conta de serviço é usada pelo serviço Keystone Collector para se comunicar com o StorageGRID por meio de APIs de nó de administrador.

  Passos

  a. Faça login no Gerenciador de Grade. "Faça login no Gerenciador de Grade"Consulte .

  b. Crie um grupo de administração local com `Access mode: Read-only`o . "Crie um grupo de administração"Consulte .

  c. Adicione as seguintes permissões:

     - Contas de inquilino

- Manutenção
- Consulta de métricas

d. Crie um usuário de conta de serviço do Keystone e associe-a ao grupo de administração. "Gerenciar usuários"Consulte .

Instale o Keystone Collector

Implante o Keystone Collector em sistemas VMware vSphere

A implantação do Keystone Collector em sistemas VMware vSphere inclui o download do modelo OVA, a implantação do modelo usando o assistente **Deploy OVF Template**, a verificação da integridade dos certificados e a verificação da prontidão da VM.

Implantando o modelo OVA

Siga estes passos:

Passos

1. Baixe o arquivo OVA "este link" e armazene-o em seu sistema VMware vSphere.
2. No seu sistema VMware vSphere, navegue até a visualização **VMs e modelos**.
3. Clique com o botão direito na pasta necessária para a máquina virtual (VM) (ou data center, se não estiver usando pastas de VM) e selecione **Deploy OVF Template**.
4. Em *Etapa 1* do assistente **Deploy OVF Template**, clique em **Select e OVF template** para selecionar o arquivo baixado `KeystoneCollector-latest.ova`.
5. Em *Etapa 2*, especifique o nome da VM e selecione a pasta da VM.
6. Em *Etapa 3*, especifique o recurso de computação necessário para executar a VM.
7. Na etapa 4: Revisar detalhes, verifique a correção e a autenticidade do arquivo OVA.

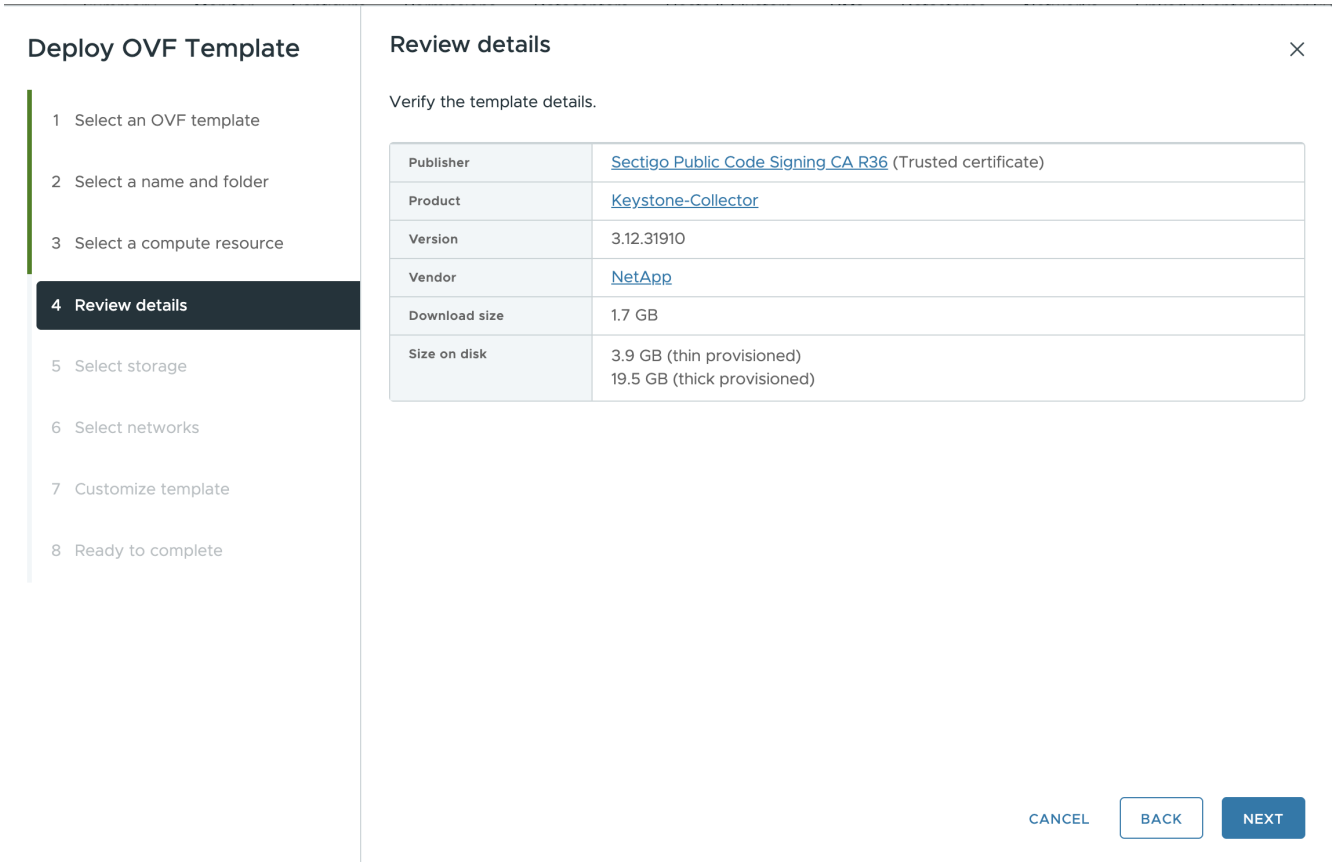
   O armazenamento confiável raiz do vCenter contém apenas certificados VMware. A NetApp usa o Entrust como autoridade de certificação, e esses certificados precisam ser adicionados ao armazenamento confiável do vCenter.

   a. Baixe o certificado de CA de assinatura de código da Sectigo. "aqui".

   b. Siga as etapas na `Resolution` seção deste artigo da base de conhecimento (KB) https://kb.vmware.com/s/article/84240: .

   > Para versões do vCenter 7.x e anteriores, você deve atualizar o vCenter e o ESXi para a versão 8.0 ou posterior. As versões anteriores não são mais suportadas.

   Quando a integridade e a autenticidade do OVA Keystone Collector forem validadas, você poderá ver o texto. `(Trusted certificate)` com a editora.



8. Em *Etapa 5* do assistente **Deploy OVF Template**, especifique o local para armazenar a VM.
9. Em *Etapa 6*, selecione a rede de destino para a VM usar.
10. Em *Etapa 7 Personalizar modelo*, especifique o endereço de rede e a senha iniciais para a conta de usuário do administrador.

> A senha de administrador é armazenada em um formato reversível no vCentre e deve ser usada como uma credencial de inicialização para obter acesso inicial ao sistema VMware vSphere. Durante a configuração inicial do software, essa senha de administrador deve ser alterada. A máscara de sub-rede para o endereço IPv4 deve ser fornecida na notação CIDR. Por exemplo, use o valor de 24 para uma máscara de sub-rede de 255.255.255.0.

11. Em *Etapa 8 Pronto para concluir* do assistente **Deploy OVF Template**, revise a configuração e verifique se você definiu corretamente os parâmetros para a implantação DO OVA.

Depois que a VM tiver sido implantada a partir do modelo e ativada, abra uma sessão SSH para a VM e faça login com as credenciais de administrador temporário para verificar se a VM está pronta para configuração.

Configuração inicial do sistema

Execute estas etapas em seus sistemas VMware vSphere para obter uma configuração inicial dos servidores Keystone Collector implantados por meio DO OVA:

> Ao concluir a implantação, você pode usar o utilitário Keystone Collector Management Terminal User Interface (TUI) para executar as atividades de configuração e monitoramento. Você pode usar vários controles de teclado, como as teclas Enter e seta, para selecionar as opções e navegar por esta TUI.

1. Abra uma sessão SSH no servidor Keystone Collector. Quando você se conetar, o sistema solicitará que você atualize a senha de administrador. Conclua a atualização da senha de administrador conforme necessário.
2. Inicie sessão utilizando a nova palavra-passe para aceder à TUI. Ao iniciar sessão, a TUI é apresentada.

   Como alternativa, você pode iniciá-lo manualmente executando o `keystone-collector-tui` comando CLI.
3. Se necessário, configure os detalhes do proxy na seção **Configuração > rede** na TUI.
4. Configure o nome do host do sistema, a localização e o servidor NTP na seção **Configuração > sistema**.
5. Atualize os coletores Keystone usando a opção **Manutenção > Atualizar coletores**. Após a atualização, reinicie o utilitário TUI de gerenciamento do Keystone Collector para aplicar as alterações.

Instale o Keystone Collector em sistemas Linux

Você pode instalar o software Keystone Collector em um servidor Linux usando um RPM ou um pacote Debian. Siga as etapas de instalação, dependendo da sua distribuição Linux.

Usando RPM

1. SSH para o servidor Keystone Collector e elevar-se a `root` privilégios.
2. Importe a assinatura pública da Keystone :
   `# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020`
3. Certifique-se de que o certificado público correto foi importado, verificando a impressão digital da plataforma Keystone Billing no banco de dados RPM:
   `# rpm -qa gpg-pubkey --qf '%{Description}'|gpg --show-keys --fingerprint` A impressão digital correta tem esta aparência:
   `9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC`
4. Baixe o `keystonerepo.rpm` arquivo:
   `curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm`
5. Verifique a autenticidade do arquivo:
   `rpm --checksig -v keystonerepo.rpm` A assinatura de um arquivo autêntico tem a seguinte aparência:
   `Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK`
6. Instale o arquivo do repositório de software DO YUM:
   `# yum install keystonerepo.rpm`
7. Quando o repositório Keystone estiver instalado, instale o pacote keystone-collector por meio do gerenciador de pacotes YUM:

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

   Para o Red Hat Enterprise Linux 9, execute o seguinte comando para instalar o pacote keystone-collector:
   `# yum install keystone-collector-rhel9`

Usando Debian

1. SSH para o servidor Keystone Collector e elevar-se a `root` privilégios.
   `sudo su`
2. Transfira o `keystone-sw-repo.deb` ficheiro:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Instale o arquivo de repositório de software do Keystone:
   `# dpkg -i keystone-sw-repo.deb`
4. Atualize a lista de pacotes:
   `# apt-get update`
5. Quando o Keystone repo estiver instalado, instale o pacote keystone-Collector:
   `# apt-get install keystone-collector`

Ao concluir a instalação, você pode usar o utilitário Keystone Collector Management Terminal User Interface (TUI) para executar as atividades de configuração e monitoramento. Você pode usar vários controles de teclado, como as teclas Enter e seta, para selecionar as opções e navegar por esta TUI. "Configure o Keystone Collector"Consulte e "Monitorar a integridade do sistema" para obter informações.

Validação automática do software Keystone

O repositório do Keystone está configurado para validar automaticamente a integridade do software Keystone para que somente software válido e autêntico seja instalado no seu local.

A configuração do cliente do repositório do Keystone YUM fornecida no `keystonerepo.rpm` faz uso da verificação GPG forçada (`gpgcheck=1`) em todos os softwares baixados por meio deste repositório. Qualquer RPM baixado pelo repositório do Keystone que falhar na validação de assinatura é impedido de ser instalado. Essa funcionalidade é usada no recurso de atualização automática programada do Keystone Collector para garantir que somente software válido e autêntico seja instalado em seu local.

Configure o Keystone Collector

Você precisa concluir algumas tarefas de configuração para permitir que o Keystone Collector colete dados de uso em seu ambiente de storage. Esta é uma atividade única para ativar e associar os componentes necessários ao seu ambiente de storage.

- O Keystone Collector fornece o utilitário TUI (Interface de Usuário do Terminal de Gerenciamento de Coletor) do Keystone para executar atividades de configuração e monitoramento. Você pode usar vários controles de teclado, como as teclas Enter e seta, para selecionar as opções e navegar por esta TUI.
- O Keystone Collector pode ser configurado para organizações que não têm acesso à Internet, também conhecido como *dark site* ou *private mode*. Para saber mais sobre, "Keystone em modo privado"consulte .

Passos

1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:
   `$ keystone-collector-tui`
2. Vá para **Configure > KS-Collector** para abrir a tela de configuração do Keystone Collector para exibir as opções disponíveis para atualização.
3. Atualize as opções necessárias.

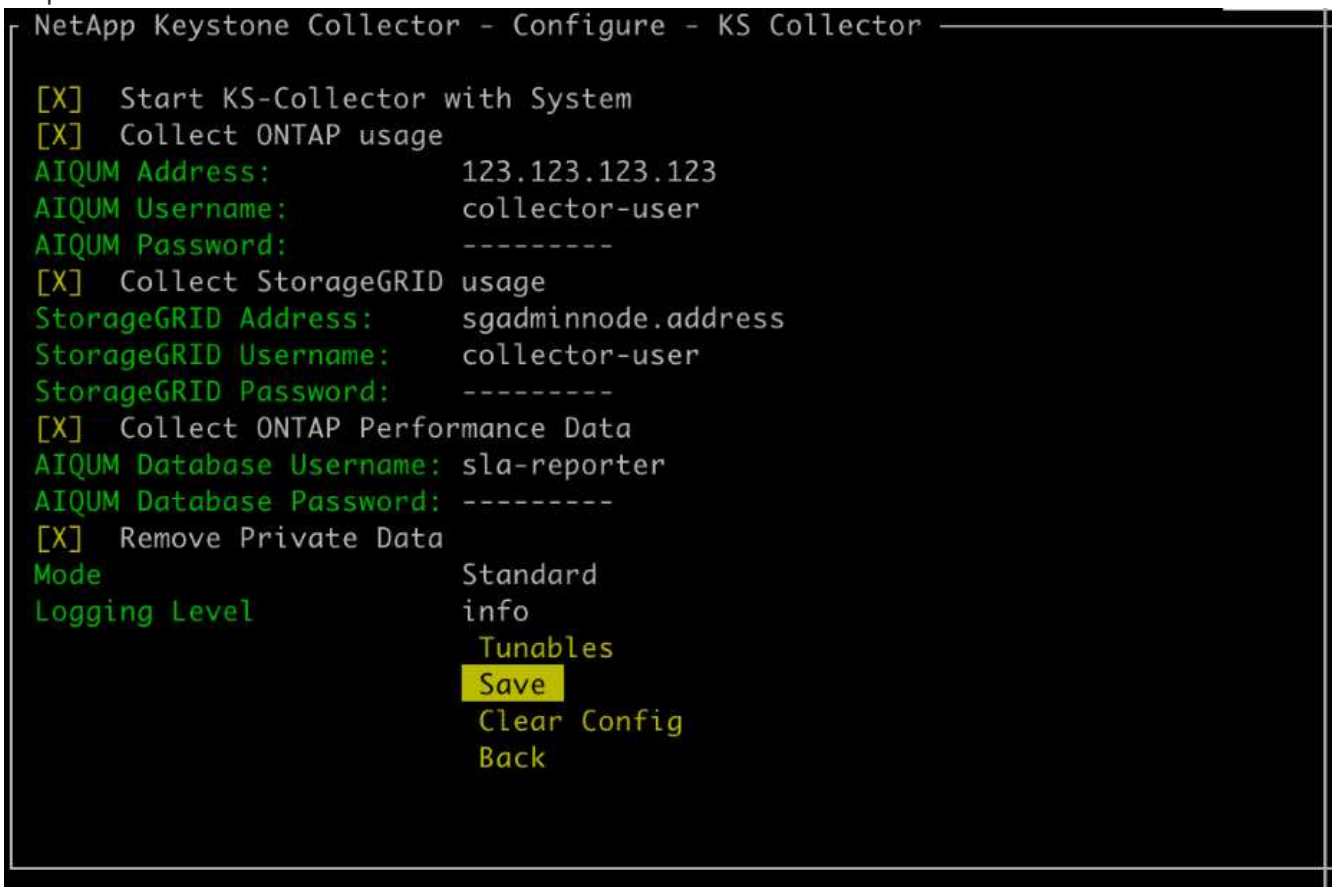
   ** para ONTAP **

   - **Collect ONTAP Usage**: Esta opção permite a coleta de dados de uso para o ONTAP. Adicione os detalhes do servidor e da conta de serviço do Active IQ Unified Manager (Unified Manager).
   - **Coletar dados de desempenho do ONTAP**: Essa opção permite a coleta de dados de desempenho para o ONTAP. Por predefinição, esta opção está desativada. Ative esta opção se o monitoramento de desempenho for necessário em seu ambiente para fins de SLA. Forneça os detalhes da conta de usuário do Unified Manager Database. Para obter informações sobre como criar usuários de banco de dados, "Crie usuários do Unified Manager"consulte .
   - **Remover dados privados**: Esta opção remove dados privados específicos dos clientes e é ativada por padrão. Para obter informações sobre quais dados são excluídos das métricas se essa opção estiver ativada, "Limitar a coleta de dados privados"consulte .

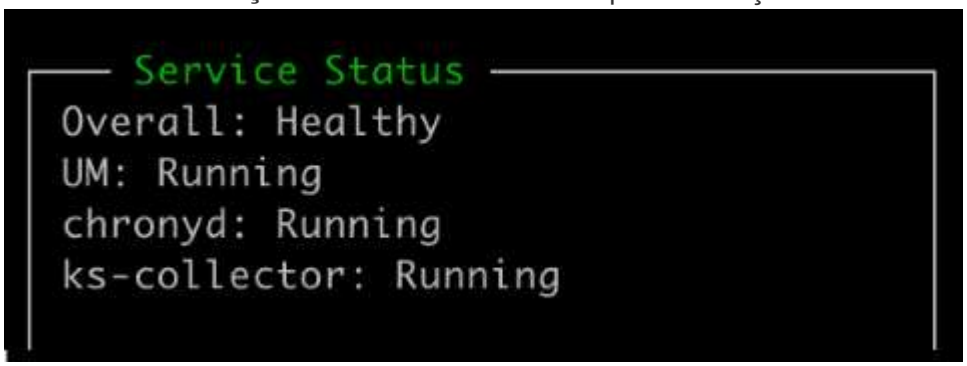
** para StorageGRID **

- **Collect StorageGRID use**: Esta opção permite a coleta de detalhes de uso de nós. Adicione o endereço do nó do StorageGRID e os detalhes do usuário.
- **Remover dados privados**: Esta opção remove dados privados específicos dos clientes e é ativada por padrão. Para obter informações sobre quais dados são excluídos das métricas se essa opção estiver ativada, "Limitar a coleta de dados privados"consulte .

4. Alterne o campo **Start KS-Collector with System** (Iniciar KS-Collector com sistema).
5. Clique em **Salvar**.



6. Certifique-se de que o Keystone Collector está em um estado saudável retornando à tela principal da TUI e verificando as informações **Status do serviço**. O sistema deve mostrar que os serviços estão em um estado **geral: Saudável**.



7. Saia da TUI de gerenciamento do Keystone Collector selecionando a opção **Exit to Shell** na tela inicial.

Configurar proxy HTTP no Keystone Collector

O software Collector suporta o uso de um proxy HTTP para se comunicar com a internet. Isso pode ser configurado na TUI.

Passos

1. Reinicie o utilitário TUI de gerenciamento do Keystone Collector se já estiver fechado:
   ```
   $ keystone-collector-tui
   ```
2. Ative o campo **Proxy HTTP** e adicione os detalhes do servidor proxy HTTP, porta e credenciais, se a autenticação for necessária.
3. Clique em **Salvar**.

Limitar a coleta de dados privados

O Keystone Collector reúne informações limitadas de configuração, status e desempenho necessárias para executar a medição de assinatura. Há uma opção para limitar ainda mais as informações coletadas mascarando informações confidenciais do conteúdo carregado. Isso não afeta o cálculo de faturamento. No entanto, limitar as informações pode afetar a usabilidade das informações de relatório, já que alguns elementos, que podem ser facilmente identificados pelos usuários, como o nome do volume, são substituídos por UUIDs.

Limitar a coleta de dados específicos do cliente é uma opção configurável na tela do Keystone Collector TUI. Esta opção, **Remover dados privados**, está ativada por padrão.

Para obter informações sobre os itens removidos ao limitar o acesso a dados privados no ONTAP e no StorageGRID, "Lista de itens removidos ao limitar o acesso a dados privados"consulte .

Confie em uma CA raiz personalizada

A verificação de certificados em relação a uma autoridade de certificação raiz pública (CA) faz parte dos recursos de segurança do Keystone Collector. No entanto, se necessário, você pode configurar o Keystone Collector para confiar em uma CA raiz personalizada.

Se você usar a inspeção SSL/TLS no firewall do sistema, isso resultará no tráfego baseado na Internet a ser recriptografado com seu certificado de CA personalizado. É necessário configurar as configurações para verificar a origem como uma CA confiável antes de aceitar o certificado raiz e permitir que as conexões ocorram. Siga estes passos:

Passos

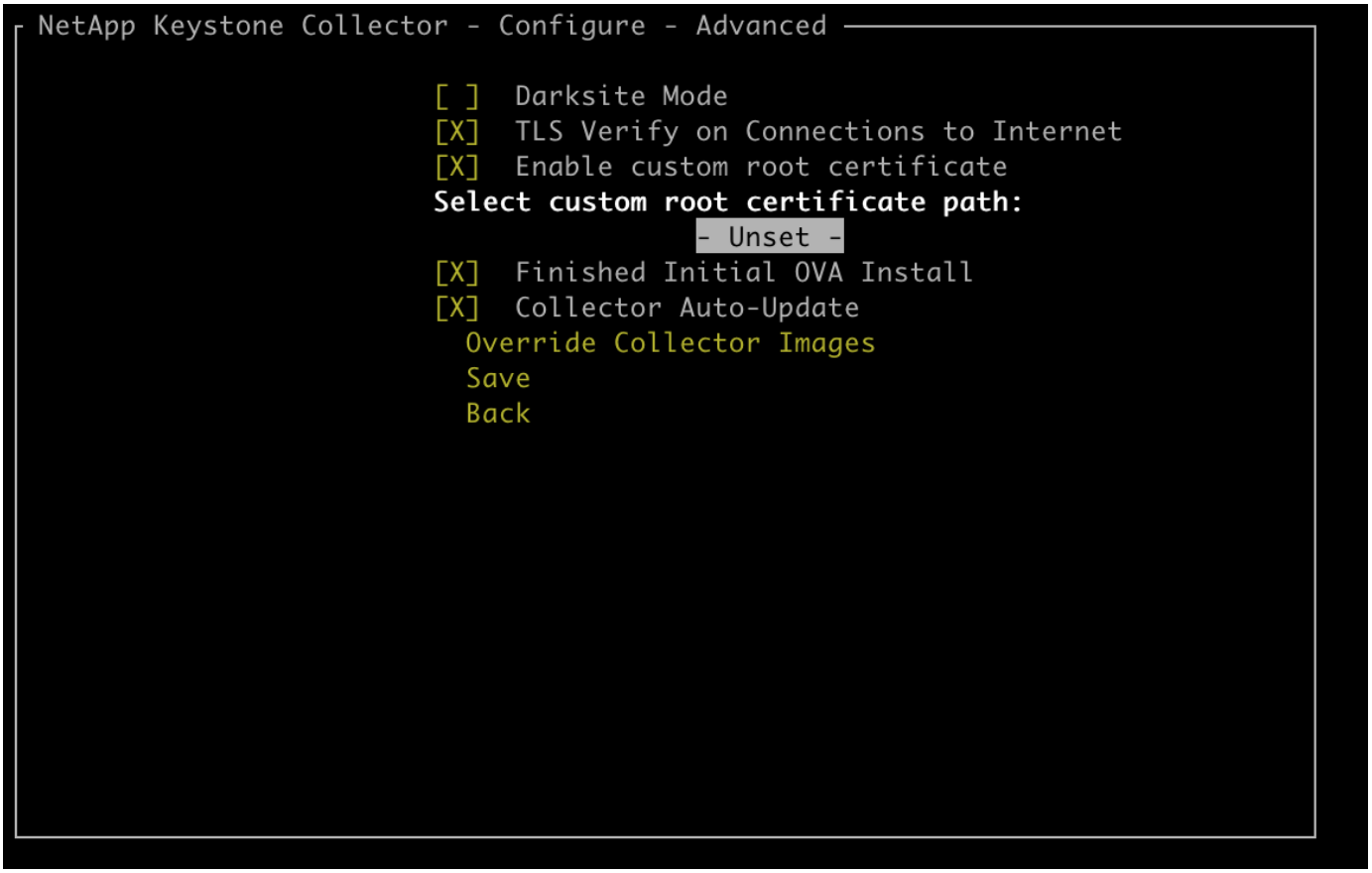
1. Prepare o certificado CA. Ele deve estar no formato de arquivo X.509_ codificado em _base64.

   As extensões de arquivo suportadas são `.pem` `.crt` , , `.cert`. Verifique se o certificado está em um desses formatos.

2. Copie o certificado para o servidor Keystone Collector. Anote o local onde o arquivo é copiado.
3. Abra um terminal no servidor e execute o utilitário TUI de gerenciamento.
   ```
   $ keystone-collector-tui
   ```
4. Aceda a **Configuração > Avançado**.
5. Ative a opção **Ativar certificado raiz personalizado**.

6. Para **Selecione o caminho do certificado raiz personalizado:**, selecione `- Unset -`
7. Prima Enter. É apresentada uma caixa de diálogo para selecionar o caminho do certificado.
8. Selecione o certificado raiz no navegador do sistema de arquivos ou insira o caminho exato.
9. Prima Enter. Regressa ao ecrã **Avançado**.
10. Selecione **Guardar**. A configuração é aplicada.

O certificado da CA é copiado para `/opt/netapp/ks-collector/ca.pem` no servidor Keystone Collector.



Criar níveis de serviço de performance

Você pode criar Níveis de Serviço de Desempenho (PSLs) usando o utilitário TUI de gerenciamento do Keystone Collector. A criação de PSLs por meio do TUI seleciona automaticamente os valores padrão definidos para cada nível de serviço de desempenho, reduzindo a chance de erros que podem ocorrer ao definir manualmente esses valores durante a criação de PSLs por meio do Active IQ Unified Manager.

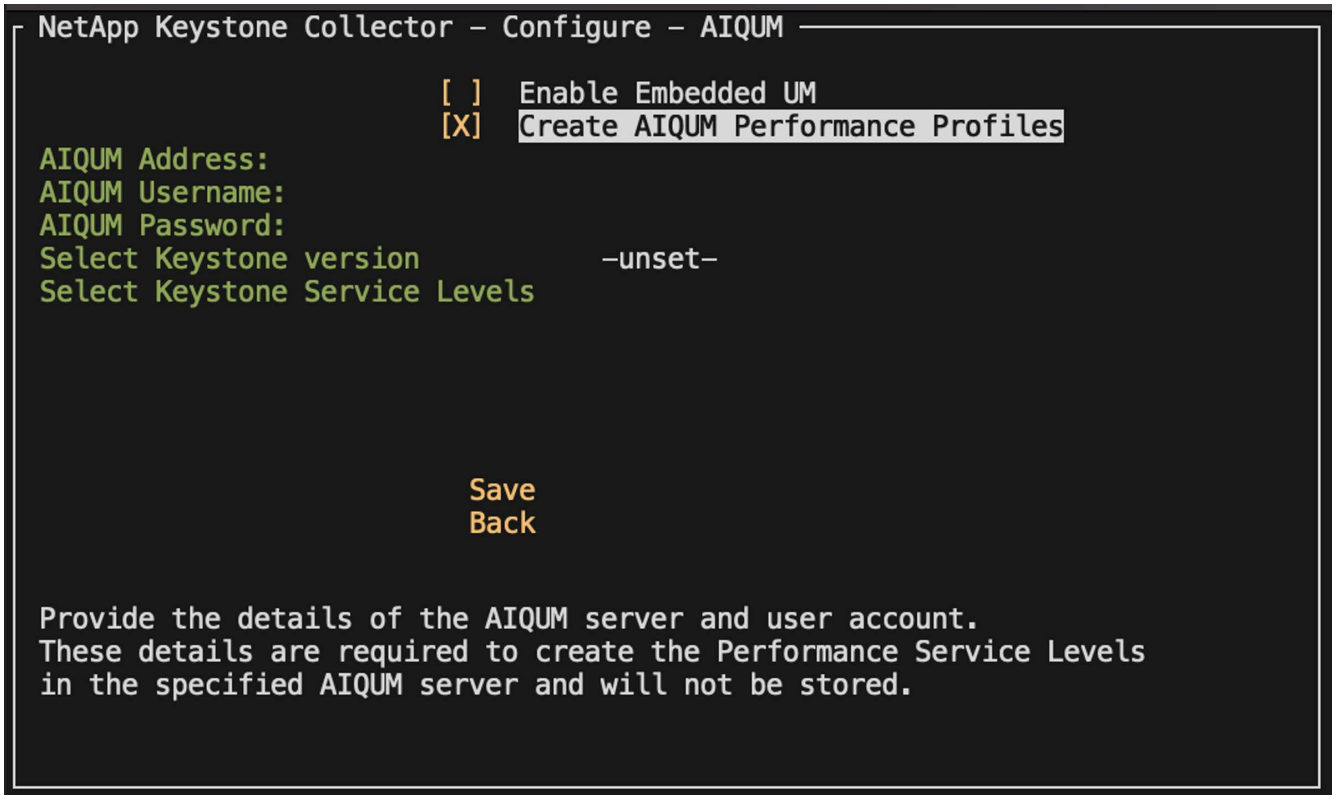
Para saber mais sobre PSLs, "Níveis de serviço de performance"consulte .

Para saber mais sobre os níveis de serviço, "Níveis de serviço no Keystone"consulte .

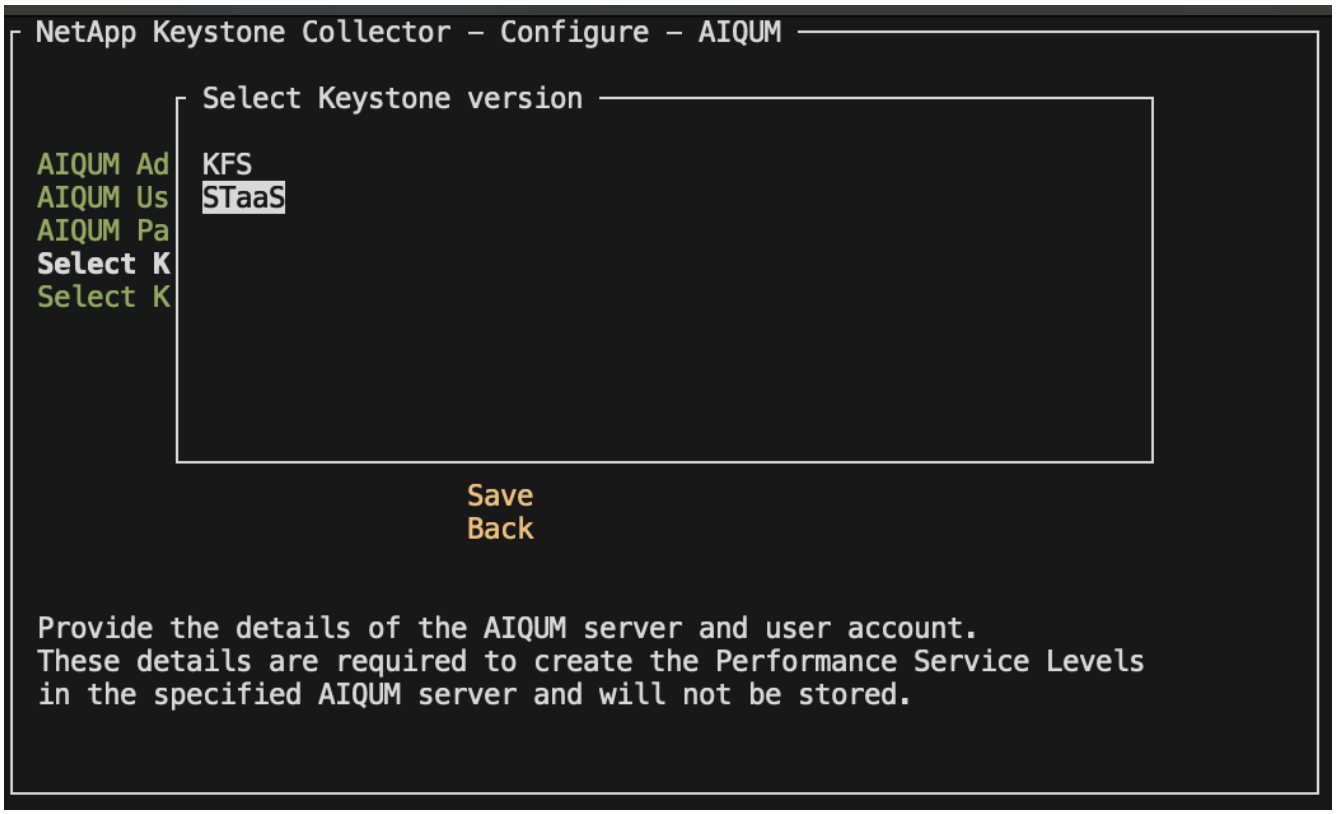
Passos

1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vá para **Configure>AIQUM** para abrir a tela AIQUM.

3. Ative a opção **criar perfis de desempenho AIQUM**.
4. Introduza os detalhes do servidor Active IQ Unified Manager e da conta de utilizador. Estes detalhes são necessários para criar PSLs e não serão armazenados.

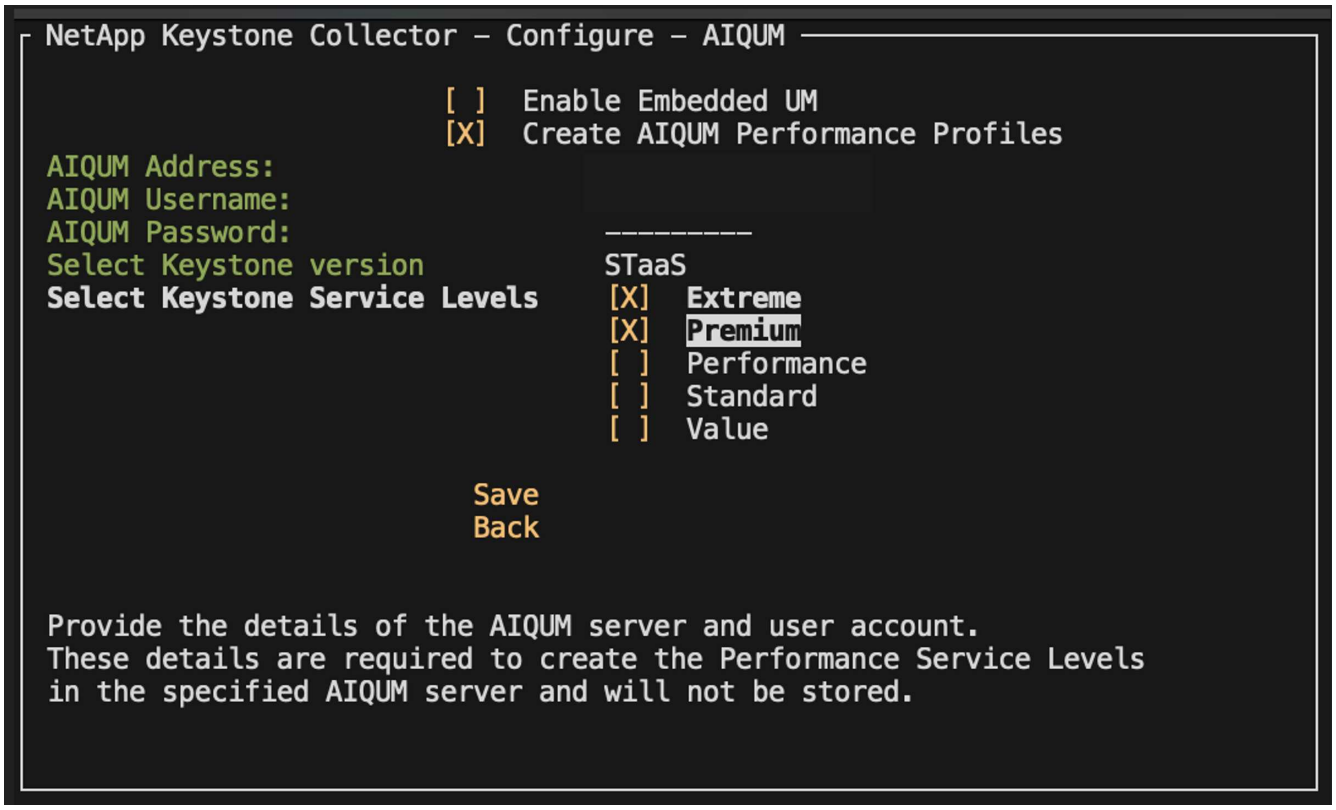


5. Para **Selecione a versão Keystone**, `-unset-` selecione .
6. Prima Enter. Uma caixa de diálogo para selecionar a versão do Keystone é exibida.
7. Realce **STaaS** para especificar a versão do Keystone para STaaS do Keystone e pressione Enter.



Você pode destacar a opção **KFS** para os serviços de assinatura do Keystone versão 1. Os serviços de assinatura da Keystone diferem do Keystone STaaS nos níveis de serviço de desempenho dos constituintes, nas ofertas de serviço e nos princípios de cobrança. Para saber mais, consulte"Serviços de assinatura do Keystone | versão 1" .

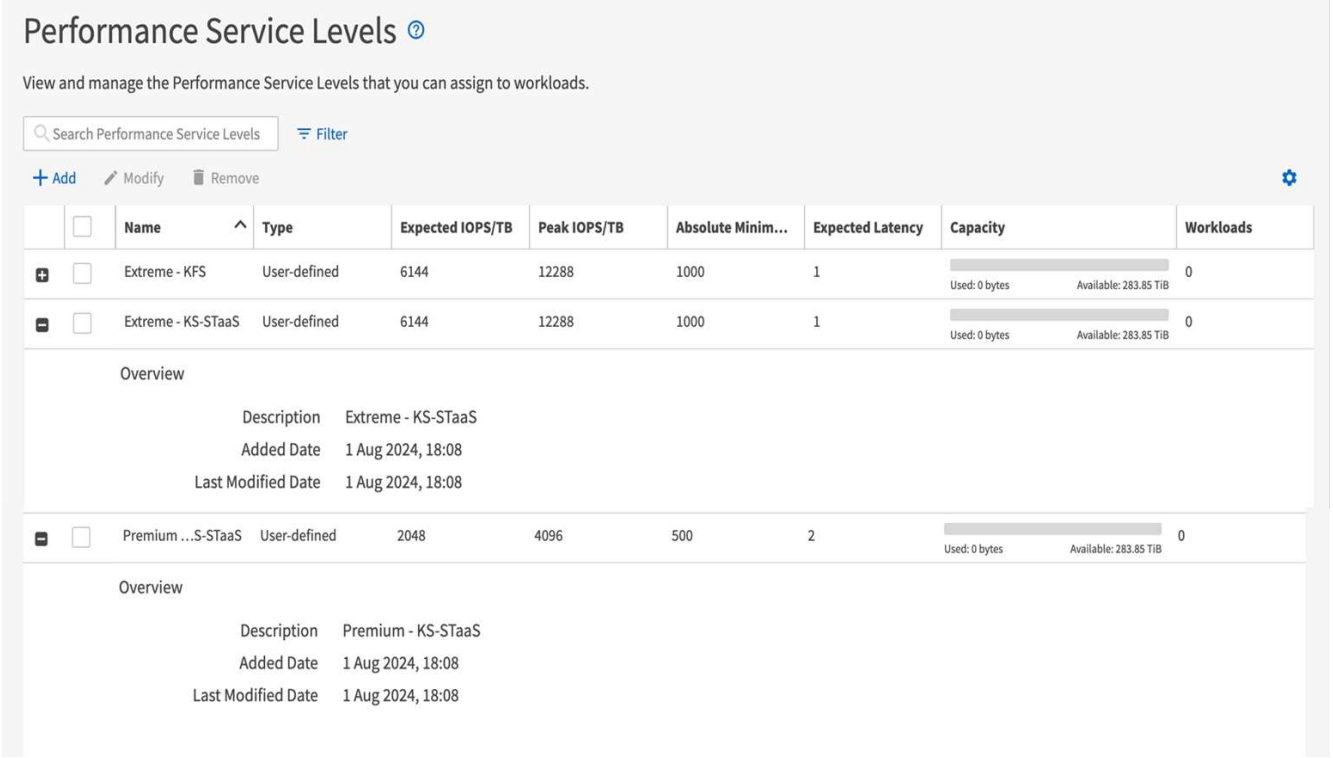
8. Todos os níveis de serviço de desempenho do Keystone suportados serão exibidos na opção *Selecionar níveis de serviço do Keystone * para a versão especificada do Keystone . Habilite os níveis de serviço de desempenho desejados na lista.



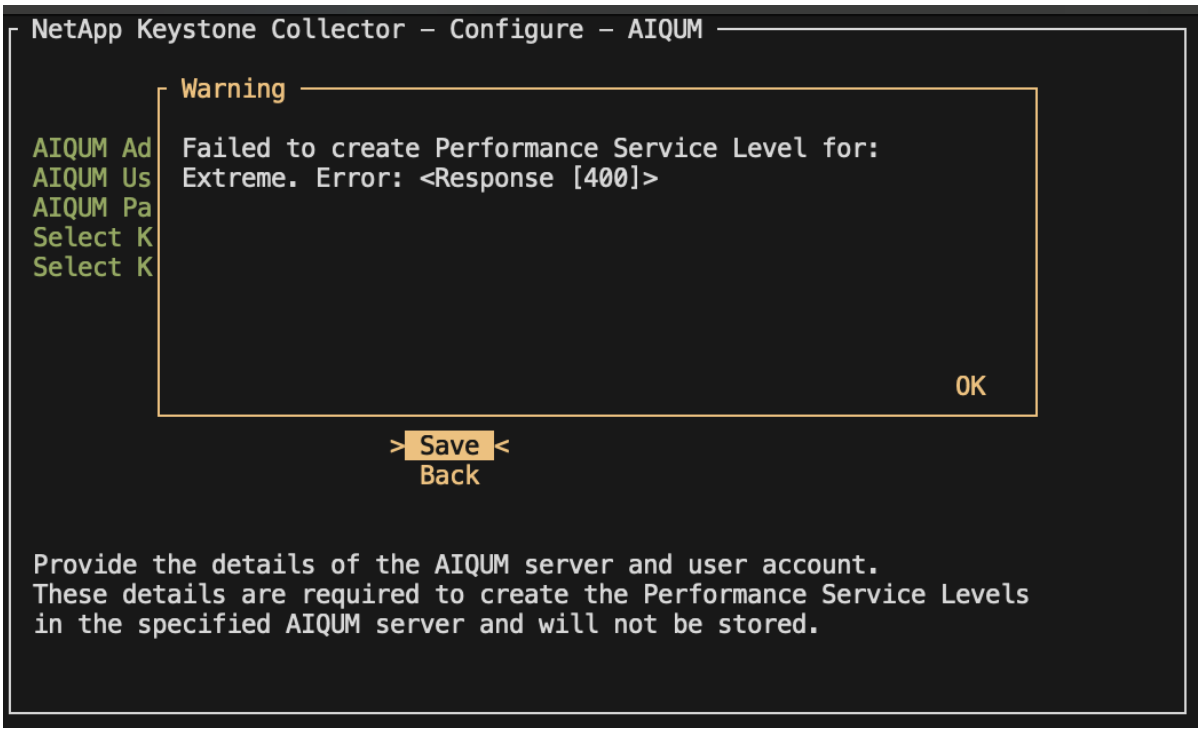
Você pode selecionar vários níveis de serviço de desempenho simultaneamente para criar PSLs.

9. Selecione **Save** (Guardar) e prima Enter. Níveis de Serviço de desempenho serão criados.

   Você pode visualizar as PSLs criadas, como Premium-KS-STaaS para STaaS ou Extreme KFS para KFS, na página **níveis de Serviço de desempenho** no Active IQ Unified Manager. Se as PSLs criadas não atenderem aos seus requisitos, você poderá modificar as PSLs para atender às suas necessidades. Para saber mais, "Criando e editando níveis de Serviço de desempenho"consulte .



Se um PSL para o nível de serviço de desempenho selecionado já existir no servidor Active IQ Unified Manager especificado, você não poderá criá-lo novamente. Se você tentar fazer isso, receberá uma mensagem de
erro.



Instale o ITOM Collector

Requisitos de instalação para o coletor Keystone ITOM

Antes de instalar o ITOM Collector, certifique-se de que seus sistemas estão preparados com o software necessário e atendam a todos os pré-requisitos necessários.

Pré-requisitos para a VM do servidor ITOM Collector:

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

> Os sistemas operacionais recomendados são Debian 12, Windows Server 2016 ou versões mais recentes.

- Requisito de recurso: Os requisitos de recurso da VM com base no número de nós NetApp monitorados são os seguintes:
  - 2-10 nós: 4 CPUs, 8 GB de RAM, 40 GB de disco
  - 12-20 nós: 8 CPUs, 16 GB de RAM, 40 GB de disco
- Requisito de configuração: Certifique-se de que uma conta somente leitura e SNMP estejam configurados nos dispositivos monitorados. A VM do servidor de Coletor ITOM também precisa ser configurada como um host de trap SNMP e servidor Syslog no cluster NetApp e switches de cluster, se aplicável.

Requisitos de rede

Os requisitos de rede do ITOM Collector estão listados na tabela a seguir.

Fonte	Destino	Protocolo	Portas	Descrição
ITOM Collector	IPs de gerenciamento de clusters NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Monitoramento dos controladores ONTAP
IPs de gerenciamento de clusters e nós do NetApp ONTAP	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP e Syslogs de controladores
ITOM Collector	Interrutores do cluster	SNMP	UDP 161	Monitorização dos interrutores
Interrutores do cluster	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP e Syslogs a partir de switches
ITOM Collector	IPs de nós de StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitorização SNMP do StorageGRID

IPs de nós de StorageGRID	ITOM Collector	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP do StorageGRID
ITOM Collector	Keystone Collector	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Monitoramento e gerenciamento remoto do Keystone Collector
ITOM Collector	DNS local	DNS	UDP 53	Serviços DNS públicos ou privados
ITOM Collector	Servidor(es) NTP de escolha	NTP	UDP 123	Manutenção do tempo

Instale o Keystone ITOM Collector em sistemas Linux.

Conclua algumas etapas para instalar o ITOM Collector, que coleta dados de métricas em seu ambiente de armazenamento. Você pode instalá-lo em sistemas Windows ou Linux, dependendo de suas necessidades.

> ⓘ A equipe de suporte do Keystone fornece um link dinâmico para baixar o arquivo de configuração ITOM Collector, que expira em duas horas.

Para instalar o ITOM Collector em sistemas Windows, "Instale o ITOM Collector em sistemas Windows"consulte .

Siga estas etapas para instalar o software em seu servidor Linux:

Antes de começar

- Verifique se o shell Bourne está disponível para o script de instalação do Linux.
- Instale o `vim-common` pacote para obter o binário **xxd** necessário para o arquivo de configuração ITOM Collector.
- Verifique se o `sudo package` está instalado se estiver planejando executar o ITOM Collector como um usuário não-root.

Passos

1. Baixe o arquivo de configuração do coletor ITOM para o servidor Linux.
2. Abra um terminal no servidor e execute o seguinte comando para alterar as permissões e tornar os binários executáveis:
   `# chmod +x <installer_file_name>.bin`
3. Execute o comando para iniciar o arquivo de configuração do coletor ITOM:
   `#./<installer_file_name>.bin`
4. Executar o arquivo de configuração solicita que você:
   a. Aceite o contrato de licença do utilizador final (EULA).
   b. Introduza os detalhes do utilizador para a instalação.
   c. Especifique o diretório pai de instalação.
   d. Selecione o tamanho do coletor.
   e. Forneça detalhes do proxy, se aplicável.

Para cada prompt, uma opção padrão é exibida. É recomendável selecionar a opção padrão, a menos que você tenha requisitos específicos. Pressione a tecla **Enter** para escolher a opção padrão. Quando a instalação for concluída, uma mensagem confirma que o ITOM Collector foi instalado com sucesso.

- O arquivo de configuração ITOM Collector faz adições `/etc/sudoers` para lidar com reinicializações de serviço e despejos de memória.
- Instalar o ITOM Collector no servidor Linux cria um usuário padrão chamado **ITOM** para executar o ITOM Collector sem root Privileges. Você pode escolher um usuário diferente ou executá-lo como root, mas é recomendável usar o usuário ITOM criado pelo script de instalação do Linux.

O que se segue?

Na instalação bem-sucedida, entre em Contato com a equipe de suporte do Keystone para validar a instalação bem-sucedida do ITOM Collector por meio do portal de suporte do ITOM. Após a verificação, a equipe de suporte do Keystone configurará o ITOM Collector remotamente, incluindo descoberta de dispositivo adicional e configuração de monitoramento, e enviará uma confirmação assim que a configuração for concluída. Para quaisquer dúvidas ou informações adicionais, entre em Contato com keystone.services@NetApp.com.

Instale o Keystone ITOM Collector em sistemas Windows.

Instale o ITOM Collector em um sistema Windows baixando o arquivo de configuração ITOM Collector, executando o assistente InstallShield e inserindo as credenciais de monitoramento necessárias.

A equipe de suporte do Keystone fornece um link dinâmico para baixar o arquivo de configuração ITOM Collector, que expira em duas horas.

Você pode instalá-lo em sistemas Linux com base em suas necessidades. Para instalar o ITOM Collector em sistemas Linux, "Instale o ITOM Collector em sistemas Linux"consulte .

Siga estas etapas para instalar o software ITOM Collector em seu servidor Windows:

Antes de começar

Certifique-se de que o serviço ITOM Collector é concedido **Faça logon como um serviço** sob Política local/atribuição de direitos de usuário nas configurações de diretiva de segurança local do servidor Windows.

Passos

1. Baixe o arquivo de configuração do coletor ITOM para o servidor Windows.
2. Abra o arquivo de configuração para iniciar o assistente InstallShield.
3. Aceite o contrato de licença do utilizador final (EULA). O assistente InstallShield extrai os binários necessários e solicita que você insira credenciais.
4. Insira as credenciais para a conta em que o ITOM Collector será executado em:
   - Se o ITOM Collector não estiver monitorando outros servidores Windows, use o sistema local.
   - Se o ITOM Collector estiver monitorando outros servidores Windows no mesmo domínio, use uma conta de domínio com permissões de administrador local.
   - Se o ITOM Collector estiver monitorando outros servidores do Windows que não fazem parte do mesmo domínio, use uma conta de administrador local e conete-se a cada recurso com credenciais de

administrador local. Você pode optar por definir a senha para que ela não expire, para reduzir os problemas de autenticação entre o ITOM Collector e seus recursos monitorados.

5. Selecione o tamanho do coletor. O padrão é o tamanho recomendado com base no arquivo de configuração. Prossiga com o tamanho sugerido, a menos que você tenha requisitos específicos.
6. Selecione *Next* para iniciar a instalação. Você pode usar a pasta preenchida ou escolher outra. Uma caixa de status exibe o andamento da instalação, seguida da caixa de diálogo Assistente InstallShield concluído.

O que se segue?

Na instalação bem-sucedida, entre em Contato com a equipe de suporte do Keystone para validar a instalação bem-sucedida do ITOM Collector por meio do portal de suporte do ITOM. Após a verificação, a equipe de suporte do Keystone configurará o ITOM Collector remotamente, incluindo descoberta de dispositivo adicional e configuração de monitoramento, e enviará uma confirmação assim que a configuração for concluída. Para quaisquer dúvidas ou informações adicionais, entre em Contato com keystone.services@NetApp.com.

Configurar o AutoSupport para Keystone

Ao usar o mecanismo de telemetria AutoSupport, o Keystone calcula o uso com base nos dados de telemetria do AutoSupport. Para obter o nível de granularidade necessário, configure o AutoSupport para incorporar dados do Keystone nos pacotes diários de suporte enviados pelos clusters do ONTAP.

Sobre esta tarefa

Observe o seguinte antes de configurar o AutoSupport para incluir dados do Keystone.

- Você edita as opções de telemetria do AutoSupport usando a CLI do ONTAP. Para obter informações sobre como gerenciar os serviços do AutoSupport e a função de administrador do sistema (cluster), "Visão geral do Manage AutoSupport" consulte e "Administradores de clusters e SVM".
- Você inclui os subsistemas nos pacotes AutoSupport diário e semanal para garantir a coleta precisa de dados para o Keystone. Para obter informações sobre subsistemas AutoSupport, "Quais são os subsistemas AutoSupport" consulte .

Passos

1. Como usuário administrador de sistema, faça login no cluster Keystone ONTAP usando SSH. Para obter informações, "Aceda ao cluster utilizando o SSH"consulte .
2. Modifique o conteúdo do log.
    - Para ONTAP 9.16.1 e superior, execute este comando para modificar o conteúdo do log diário:

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

      Se o cluster estiver em uma configuração MetroCluster , execute 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 versões anteriores do ONTAP , execute este comando para modificar o conteúdo do log diário:

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

Se o cluster estiver em uma configuração MetroCluster , execute 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
```

- Execute este comando para modificar o conteúdo do log semanal:

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

Para obter mais informações sobre esse comando, "modificação do acionador do AutoSupport do nó do sistema"consulte .

Monitorar e atualizar

Monitore a integridade do Keystone Collector

Você pode monitorar a integridade do Keystone Collector usando qualquer sistema de monitoramento compatível com solicitações HTTP. O monitoramento da integridade pode ajudar a garantir que os dados estejam disponíveis no painel do Keystone.

Por padrão, os serviços de integridade do Keystone não aceitam conexões de qualquer IP diferente do localhost. O endpoint de integridade do Keystone é `/uber/health`, e ele escuta todas as interfaces do servidor Keystone Collector na porta `7777`. Na consulta, um código de status de solicitação HTTP com uma saída JSON é retornado do endpoint como uma resposta, descrevendo o status do sistema Keystone Collector. O corpo JSON fornece um status geral de integridade para o `is_healthy` atributo, que é um booleano; e uma lista detalhada de status por componente para o `component_details` atributo. Aqui está um exemplo:

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

Estes códigos de estado são devolvidos:

- **200**: indica que todos os componentes monitorados estão saudáveis
- **503**: indica que um ou mais componentes não são saudáveis
- **403**: Indica que o cliente HTTP que consulta o status de integridade não está na lista *allow*, que é uma lista de CIDR de rede permitidos. Para esse status, nenhuma informação de saúde é retornada. A lista *allow* usa o método CIDR de rede para controlar quais dispositivos de rede têm permissão para consultar o sistema de integridade do Keystone. Se você receber esse erro, adicione seu sistema de monitoramento à lista *allow* de **Keystone Collector Management TUI > Configure > Health Monitoring**.

> **Usuários Linux, observe este problema conhecido:**
>
> * Descrição do problema*: O Keystone Collector executa vários contentores como parte do sistema de medição de uso. Quando o servidor Red Hat Enterprise Linux 8.x é endurecido com as políticas dos Guias de implementação Técnica de Segurança (STIG) da Agência de sistemas de Informação da Defesa dos EUA (DISA), um problema conhecido com o fapolicyd (File Access Policy Daemon) foi visto intermitentemente. Este problema é identificado como "erro 1907870". **Solução**: Até que seja resolvida pela Red Hat Enterprise, a NetApp recomenda que você trabalhe em torno desse problema colocando `fapolicyd` em modo permissivo. Em `/etc/fapolicyd/fapolicyd.conf`, defina o valor de `permissive = 1`.

Ver registos do sistema

Você pode visualizar os logs do sistema do Keystone Collector para analisar as informações do sistema e executar a solução de problemas usando esses logs. O Keystone Collector usa o sistema de Registro *journald* do host e os logs do sistema podem ser revisados pelo utilitário de sistema padrão *journalctl*. Você pode aproveitar os seguintes serviços-chave para examinar os logs:

- coletor ks
- ks-saúde
- ks-autoupdate

O principal serviço de coleta de dados *KS-Collector* produz logs em formato JSON com um `run-id` atributo associado a cada tarefa de coleta de dados agendada. A seguir, um exemplo de um trabalho bem-sucedido para coleta de dados de uso padrão:

```
{"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 seguir, um exemplo de um trabalho bem-sucedido para coleta de dados de desempenho 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"}
```

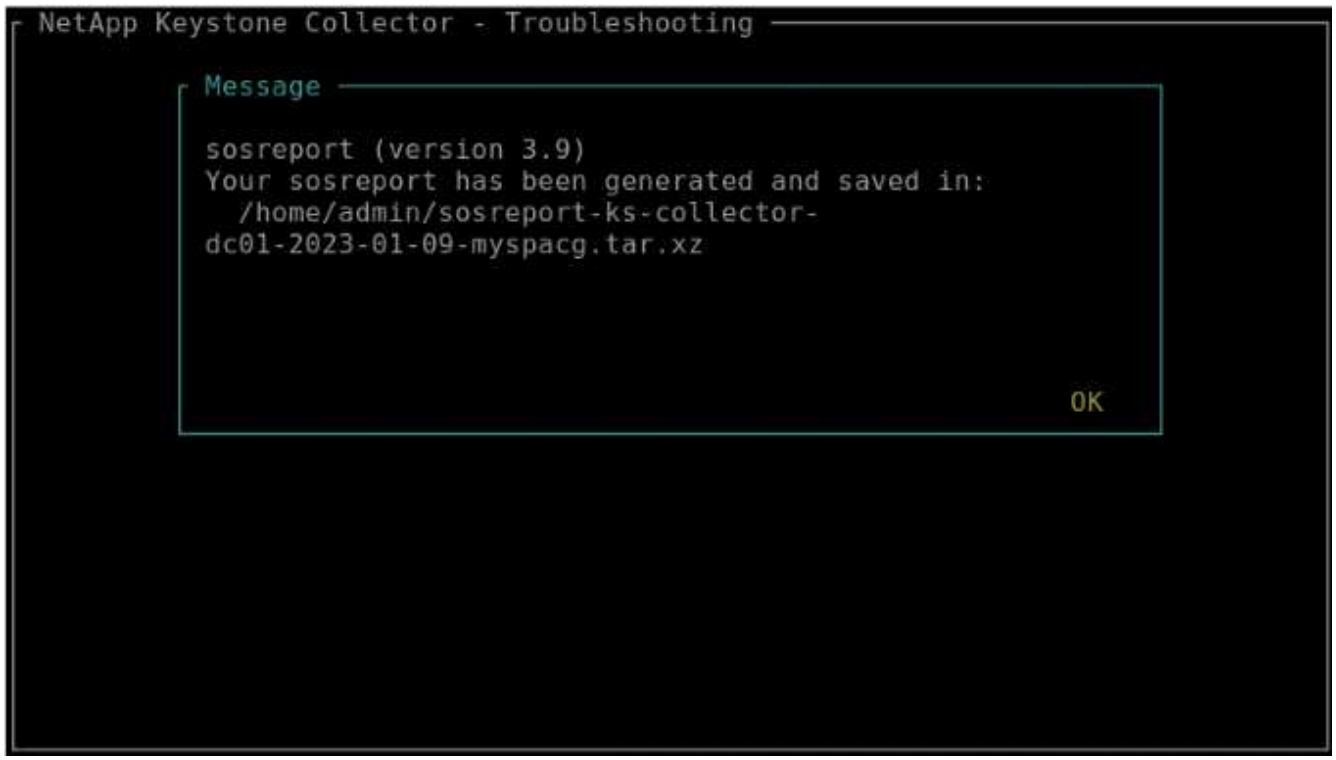
Gerar e coletar pacotes de suporte

A TUI do Keystone Collector permite gerar pacotes de suporte e adicionar solicitações de serviço para resolver problemas de suporte. Siga este procedimento:

Passos

1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Vá para **Troubleshooting > Generate Support Bundle**.

3. Quando gerado, o local onde o pacote é salvo é exibido. Use FTP, SFTP ou SCP para se conetar ao local e baixar o arquivo de log para um sistema local.



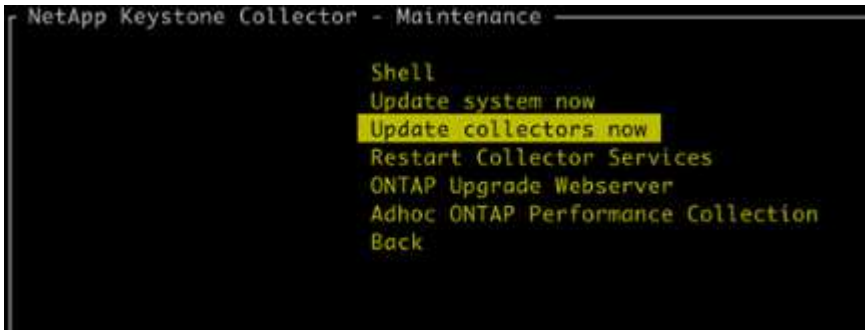
4. Quando o arquivo for baixado, você pode anexá-lo ao tíquete de suporte do Keystone ServiceNow. Para obter informações sobre como levantar bilhetes, consulte "Gerando solicitações de serviço".

Atualizar manualmente o Keystone Collector

O recurso de atualização automática do Keystone Collector está habilitado por padrão, que atualiza automaticamente o software Keystone Collector a cada nova versão. No entanto, pode desativar esta funcionalidade e atualizar manualmente o software.

Passos

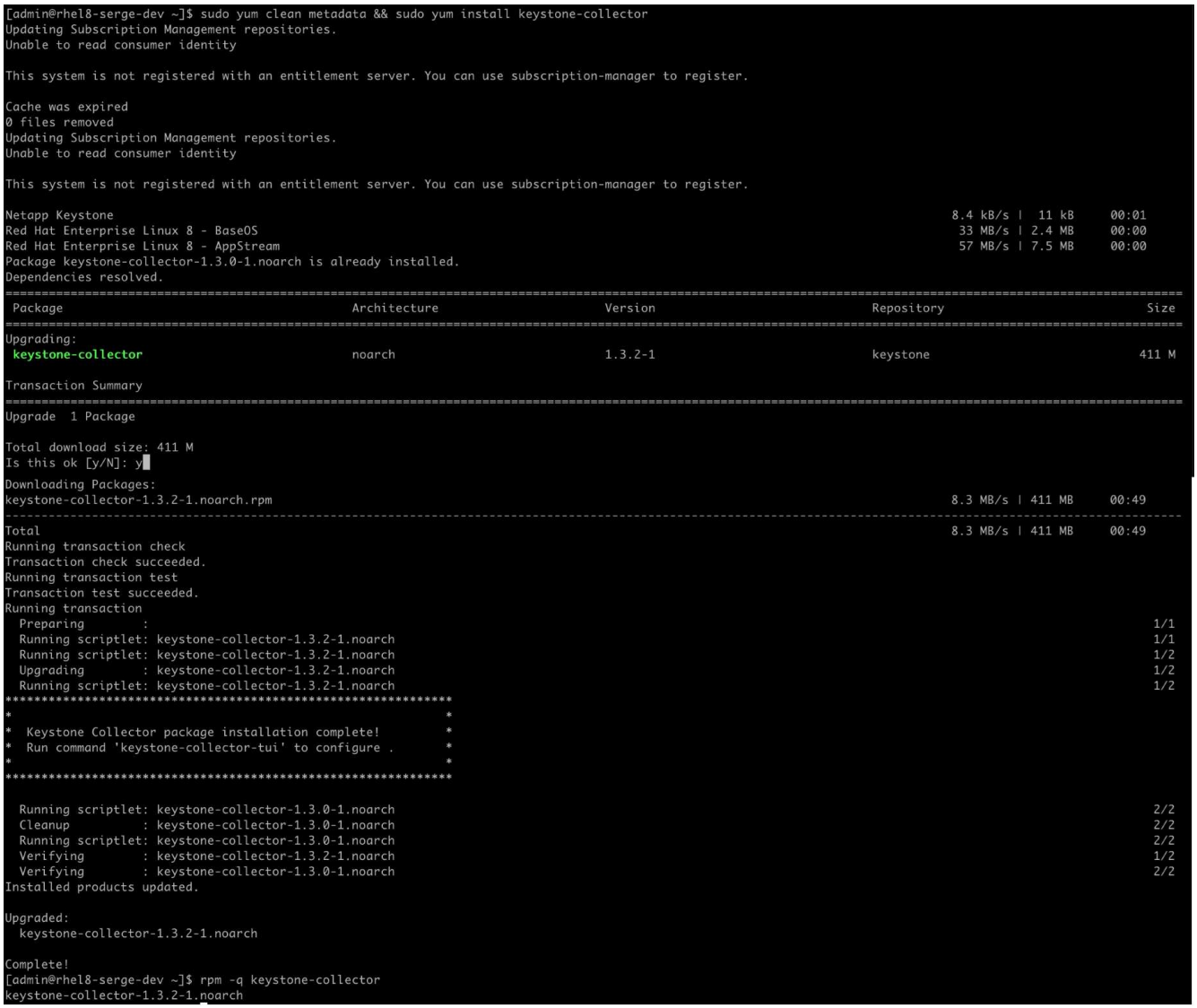
1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:
   `$ keystone-collector-tui`
2. Na tela de manutenção, selecione a opção **Atualizar colecionadores agora**.



Alternativamente, execute estes comandos para atualizar a versão:

Para o CentOS:

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



Para o Debian:

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

3. Reinicie o gerenciamento do Keystone Collector TUI, você pode ver a versão mais recente na parte superior esquerda da tela inicial.

   Como alternativa, execute estes comandos para visualizar a versão mais recente:

   Para o CentOS:

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

   Para o Debian:

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

Segurança do Keystone Collector

O Keystone Collector inclui recursos de segurança que monitoram as métricas de desempenho e uso dos sistemas Keystone, sem arriscar a segurança dos dados do cliente.

O funcionamento do Keystone Collector baseia-se nos seguintes princípios de segurança:

- **Privacy by design**-Keystone Collector coleta dados mínimos para executar a medição de uso e o monitoramento de desempenho. Para obter mais informações, "Dados coletados para faturamento"consulte . A "Remover dados privados" opção é ativada por padrão, que mascara e protege informações confidenciais.
- * O Keystone Collector requer permissões mínimas para monitorar os sistemas de armazenamento, o que minimiza os riscos de segurança e impede modificações não intencionais nos dados. Essa abordagem se alinha ao princípio do menor privilégio, aprimorando a postura geral de segurança dos ambientes monitorados.
- * Estrutura de desenvolvimento de software segura*- o Keystone usa uma estrutura de desenvolvimento de software segura em todo o ciclo de desenvolvimento, que reduz riscos, reduz vulnerabilidades e protege o sistema contra possíveis ameaças.

Endurecimento da segurança

Por padrão, o Keystone Collector está configurado para usar configurações de segurança endurecidas. A seguir estão as configurações de segurança recomendadas:

- O sistema operacional da máquina virtual Keystone Collector:
  - Está em conformidade com o padrão CIS Debian Linux 12 Benchmark. Fazer alterações na configuração do sistema operacional fora do software de gerenciamento Keystone Collector pode reduzir a segurança do sistema. Para obter mais informações, "Guia de referência do CIS"consulte .
  - Recebe e instala automaticamente patches de segurança verificados pelo Keystone Collector por meio do recurso de atualização automática. Desativar esta funcionalidade pode levar a software vulnerável não corrigido.
  - Autentica as atualizações recebidas do Keystone Collector. Desativar a verificação do repositório APT pode levar à instalação automática de patches não autorizados, potencialmente introduzindo vulnerabilidades.
- O Keystone Collector valida automaticamente certificados HTTPS para garantir a segurança da conexão. Desativar esse recurso pode levar à personificação de endpoints externos e vazamento de dados de uso.
- O Keystone Collector oferece suporte "CA fidedigna personalizada" à certificação. Por padrão, ele confia em certificados assinados por CAs raiz pública reconhecidos pelo "Programa Mozilla CA Certificate". Ao ativar CAs confiáveis adicionais, o Keystone Collector habilita a validação de certificado HTTPS para conexões com endpoints que apresentam esses certificados.
- O coletor Keystone habilita a opção **Remover dados privados** por padrão, que mascara e protege informações confidenciais. Para obter mais informações, "Limitar a coleta de dados privados"consulte . Desativar essa opção faz com que dados adicionais sejam comunicados ao sistema Keystone. Por exemplo, ele pode incluir informações inseridas pelo usuário, como nomes de volume, que podem ser

consideradas informações confidenciais.

Informações relacionadas

- "Visão geral do Keystone Collector"
- "Requisitos de infraestrutura virtual"
- "Configure o Keystone Collector"

Tipos de dados de usuário coletados pelo Keystone

O Keystone coleta informações de configuração, status e uso das assinaturas do Keystone ONTAP e do Keystone StorageGRID , bem como dados de telemetria da máquina virtual (VM) que hospeda o Keystone Collector. Ele pode coletar dados de desempenho apenas para o ONTAP , se esta opção estiver habilitada no Keystone Collector.

Coleta de dados do ONTAP

** dados de uso coletados para ONTAP: Saiba mais**

A lista a seguir é uma amostra representativa dos dados de consumo de capacidade coletados para o ONTAP:

- Clusters
  - ClusterUUID
  - Nome de utilizador
  - SerialNumber
  - Localização (com base na entrada de valor no cluster ONTAP)
  - Contacto
  - Versão
- Nós
  - SerialNumber
  - Nome do nó
- Volumes
  - Nome agregado
  - Nome do volume
  - VolumeInstanceUID
  - Bandeira IsClonevolume
  - Bandeira de IsFlexGroupConstituent
  - IsSpaceEnforcementBandeira lógica
  - IsSpaceReportingFlag lógico
  - LogicalSpaceUsedByAfs
  - PercentSnapshotSpace
  - PerformanceTierInactiveUserData
  - PerformanceTierInactiveUserDataPercent
  - QoSAdaptivePolicyGroup Name (Nome do grupo)
  - Nome do Grupo QaSPolicyGroup
  - Tamanho
  - Usado
  - PhysicoUsed (físico)
  - SizeUsedBySnapshots
  - Tipo
  - VolumeStyleExtended
  - Nome do SVM
  - Bandeira IsVsRoot
- VServers
  - VserverName

    - VserUUID
    - Subtipo
- Agregados de storage
    - StorageType
    - Nome agregado
    - UUID agregado
    - Físico usado
    - Tamanho disponível
    - Tamanho
    - Tamanho usado
- Agregar armazenamentos de objetos
    - ObjectStoreName
    - ObjectStoreUID
    - Tipo de fornecedor
    - Nome agregado
- Clonar volumes
    - FlexClone
    - Tamanho
    - Usado
    - SVM
    - Tipo
    - Parentvolume
    - ParentSVM
    - IsConstituinte
    - SplitEstimate
    - Estado
    - FlexCloneUsedPercent
- LUNs de storage
    - UUID LUN
    - Nome LUN
    - Tamanho
    - Usado
    - Bandeira IsReserved
    - Bandeira IsRequested
    - Nome da unidade de registo
    - QosPolicyUID
    - QoSPolicyName

    - VolumeUID
    - Nome do volume
    - SVMUUID
    - Nome SVM
- Volumes de storage
    - VolumeInstanceUID
    - Nome do volume
    - Nome do SVM
    - SVMUUID
    - QosPolicyUID
    - QoSPolicyName
    - CapacityTierFootprint
    - PerformanceTierFootprint
    - TotalFootprint
    - TieringPolicy
    - Bandeira IsProtected
    - Bandeira IsDestination
    - Usado
    - PhysicoUsed (físico)
    - CloneParentUID
    - LogicalSpaceUsedByAfs
- Grupos de políticas de QoS
    - PolicyGroup
    - QosPolicyUID
    - MaxThroughput
    - MinThroughput
    - MaxThroughputIOPS
    - MaxThroughputMBps
    - MinThroughputIOPS
    - MinThroughputMBps
    - Bandeira IsShared
- Grupos de políticas de QoS adaptáveis ONTAP
    - QoSPolicyName
    - QosPolicyUID
    - PeakIOPS
    - PeakIOPSAllocation
    - AbsoluteMinIOPS

    - ExpectedIOPS
    - ExpectedIOPSAllocation
    - Tamanho do bloco
- Pegadas
    - SVM
    - Volume
    - TotalFootprint
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Nó
    - Agregado
    - LIFs
    - Replicação de configuração
    - Conexões
    - Clusters
    - Volumes
- Clusters de MetroCluster
    - ClusterUUID
    - Nome de utilizador
    - RemoteClusterUID
    - RemoteCluserName
    - Estado Configuração local
    - Estado de configuração remota
- Nós do MetroCluster
    - Estado de espelhamento DR
    - LIF interaglomerado
    - Acessibilidade do nó
    - Nó de parceiro DR
    - Nó DR Aux Partner
    - Relação simétrica entre nós DR, DR Aux e HA
    - Troca automática não planejada
- Replicação de configuração do MetroCluster
    - Batimento cardíaco remoto
    - Último batimento cardíaco enviado
    - Último batimento cardíaco recebido
    - Fluxo do Vserver

    - Fluxo de Cluster
    - Armazenamento
    - Volume de armazenamento em uso
- Mediadores do MetroCluster
    - Endereço do Mediador
    - Porta do Mediador
    - Mediador Configurado
    - Mediador Alcançável
    - Modo
- Métricas de Observablility do coletor
    - Tempo de recolha
    - Active IQ Unified Manager API endpoint consultado
    - Tempo de resposta
    - Número de registos
    - AIQUMInstance IP
    - Código de instância de coleção

** dados de desempenho coletados para o ONTAP: Saiba mais**

A lista a seguir é uma amostra representativa dos dados de desempenho coletados para o ONTAP:

- Nome do cluster
- UUID do cluster
- ID do objeto
- Nome do volume
- UUUID da instância de volume
- SVM
- VserUUID
- Série nó
- ONTAPVersion
- Versão AIQUM
- Agregado
- AggregateUUID
- ResourceKey
- Timestamp
- IOPSPerTb
- Latência
- ReadLatency
- WriteMBps
- QosMinThroughputLatency
- Qualidade de vida
- UsedHeadRoom
- CacheMissRatio
- OtherLatency
- Qualidade de vida
- IOPS
- QaSNetworkLeviedade
- AvailableOps
- WriteLatency
- QoSCloudLatency
- QoSClusterInterconnectLatência
- OtherMBps
- Qualidade de vida
- QoSDBladeLatency
- Utilização

- ReadIOPS
- Mbps
- OtherIOPS
- QoSPolicyGroupLatency
- ReadMBps
- QoSSyncSnapmirrorLatency
- Dados de nível de sistema
  - Gravação/Leitura/Outro/IOPS total
  - Gravação/Leitura/Outro/Taxa de transferência total
  - Gravação/Leitura/Outro/Latência Total
- Capacidade de IOPS

** Lista de itens removidos ao limitar o acesso a dados privados: Saiba mais**

Quando a opção **Remover dados privados** está ativada no Keystone Collector, as seguintes informações de uso são eliminadas para o ONTAP. Esta opção está ativada por predefinição.

- Nome do cluster
- Localização do cluster
- Contacto de cluster
- Nome do nó
- Nome agregado
- Nome do volume
- QoSAdaptivePolicyGroup Name (Nome do grupo)
- Nome do Grupo QaSPolicyGroup
- Nome do SVM
- Nome da LUN de storage
- Nome agregado
- Nome da unidade de registo
- Nome SVM
- AIQUMInstance IP
- FlexClone
- RemoteClusterName

Coleta de dados do StorageGRID

** dados de uso coletados para StorageGRID: Saiba mais**

A lista a seguir é uma amostra representativa dos `Logical Data` coletados para StorageGRID:

- StorageGRID ID
- ID da conta
- Nome da conta
- Bytes de quota de conta
- Nome do balde
- Contagem de objetos do balde
- Bytes de dados do bucket

A lista a seguir é uma amostra representativa dos `Physical Data` coletados para StorageGRID:

- StorageGRID ID
- ID de nó
- ID do local
- Nome do local
- Instância
- Bytes de utilização do storage StorageGRID
- Bytes dos metadados da utilização do storage do StorageGRID

A lista a seguir é uma amostra representativa do `Availability/Uptime Data` coletados para StorageGRID:

- Porcentagem de tempo de atividade do SLA

** Lista de itens removidos ao limitar o acesso a dados privados: Saiba mais**

Quando a opção **Remover dados privados** está ativada no Keystone Collector, as seguintes informações de uso são eliminadas para o StorageGRID. Esta opção está ativada por predefinição.

- AccountName
- Nome do BucketName
- SiteName
- Instância/nome-nonodename

Coleta de dados de telemetria

Dados de telemetria coletados da VM do Keystone Collector: Saiba mais

A lista a seguir é uma amostra representativa dos dados de telemetria coletados para sistemas Keystone :

- Informações do sistema
  - Nome do sistema operacional
  - Versão do sistema operativo
  - ID do sistema operacional
  - Nome do host do sistema
  - Endereço IP padrão do sistema
- Uso de recursos do sistema
  - Tempo de atividade do sistema
  - Contagem de núcleos da CPU
  - Carga do sistema (1 min, 5 min, 15 min)
  - Memória total
  - Memória livre
  - Memória disponível
  - Memória compartilhada
  - Memória buffer
  - Memória em cache
  - Troca total
  - Troca grátis
  - Swap em cache
  - Nome do sistema de arquivos do disco
  - Tamanho do disco
  - Disco usado
  - Disco disponível
  - Porcentagem de uso do disco
  - Ponto de montagem do disco
- Pacotes instalados
- Configuração do coletor
- Registros de serviço
  - Registros de serviço dos serviços Keystone

Keystone em modo privado

Saiba mais sobre o Keystone (modo privado)

O Keystone oferece um modo de implantação *private*, também conhecido como *dark site*, para atender aos requisitos de negócios e segurança. Este modo está disponível para organizações com restrições de conetividade.

A NetApp oferece uma implantação especializada do Keystone STaaS desenvolvido para ambientes com conetividade limitada ou sem Internet (também conhecidos como dark sites). Estes são ambientes seguros ou isolados onde a comunicação externa é restrita devido a requisitos de segurança, conformidade ou operacionais.

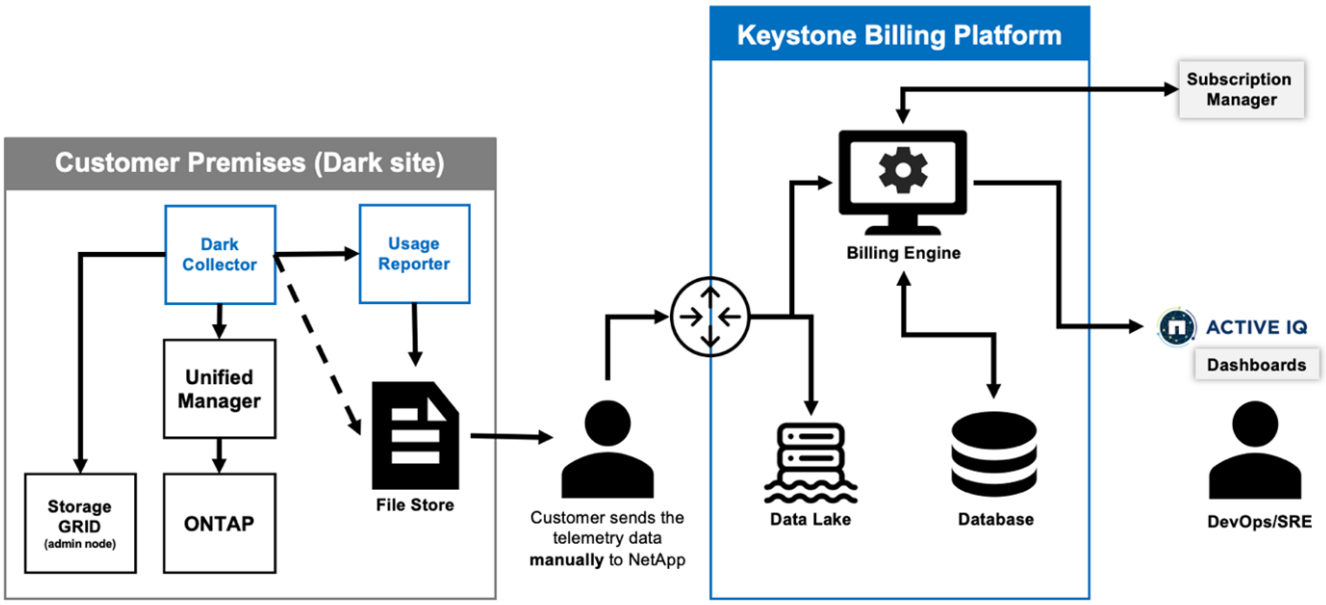
Para a NetApp Keystone, oferecer serviços para locais escuros significa fornecer o serviço de subscrição de storage flexível do Keystone de uma forma que respeite as restrições desses ambientes. Isso envolve:

- * Implantação local*: O Keystone pode ser configurado em ambientes isolados de forma independente, garantindo que não haja necessidade de conetividade à Internet ou pessoal externo para acesso à configuração.
- **Operações off-line**: Todos os recursos de gerenciamento de armazenamento com verificações de integridade e faturamento estão disponíveis off-line para operações.
- **Segurança e conformidade**: O Keystone garante que a implantação atenda aos requisitos de segurança e conformidade de sites obscuros, que podem incluir criptografia avançada, controles de acesso seguro e recursos de auditoria detalhados.
- **Ajuda e suporte**: O NetApp oferece suporte global 24/7 horas por dia, 7 dias por semana, com um gerente de sucesso dedicado do Keystone designado a cada conta para obter assistência e solução de problemas.

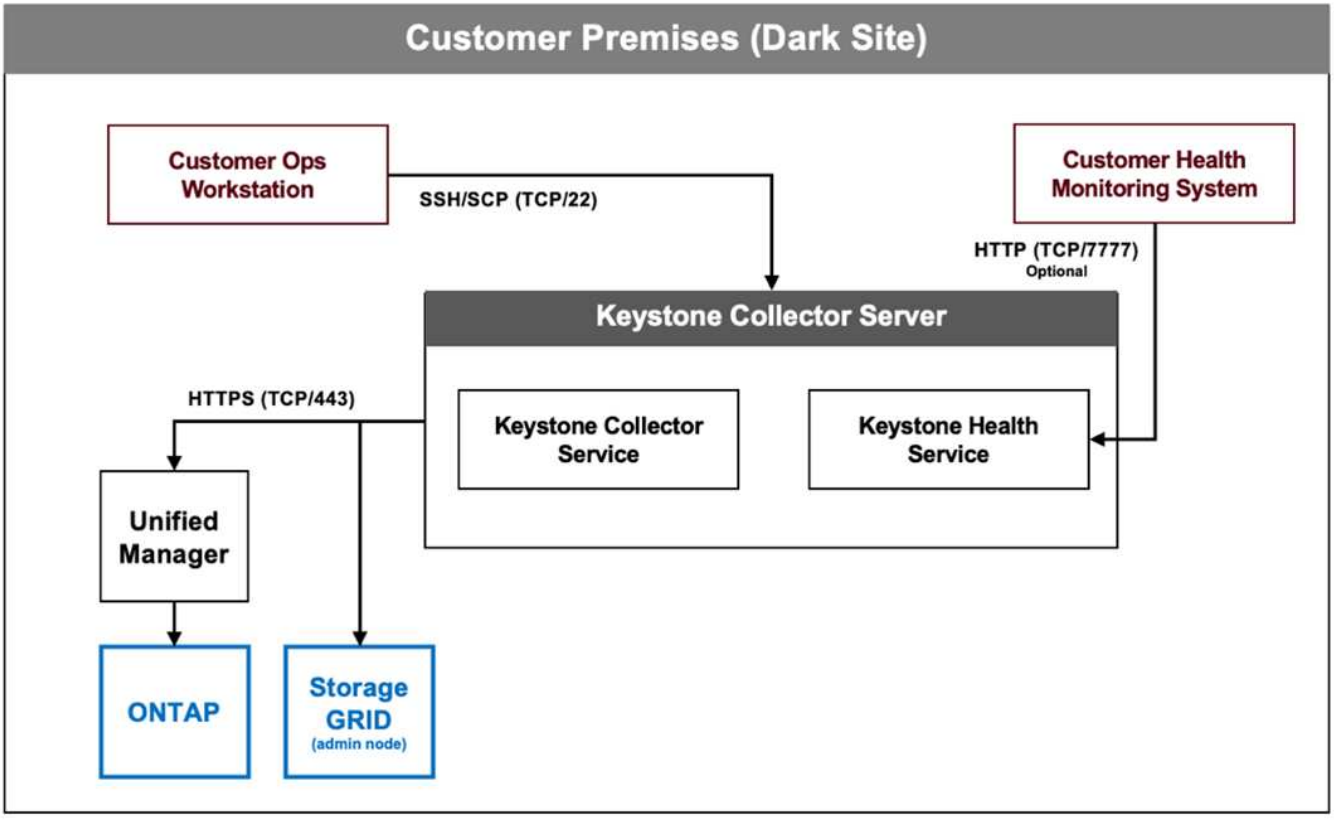
> ⓘ O Keystone Collector pode ser configurado sem restrições de conetividade, também conhecido como modo *standard*. Para saber mais, "Saiba mais sobre o Keystone Collector"consulte .

Keystone Collector em modo privado

O Keystone Collector é responsável por coletar periodicamente dados de uso de sistemas de storage e exportar as métricas para um repórter de uso off-line e um armazenamento de arquivos local. Os arquivos gerados, que são criados nos formatos de texto criptografado e sem formatação, são encaminhados manualmente para o NetApp pelo usuário após as verificações de validação. Após o recebimento, a plataforma de cobrança do Keystone da NetApp autentica e processa esses arquivos, integrando-os aos sistemas de gerenciamento de assinaturas e cobrança para calcular os encargos mensais.



O serviço Keystone Collector no servidor tem a tarefa de coletar periodicamente dados de uso, processar essas informações e gerar um arquivo de uso localmente no servidor. O serviço de saúde realiza verificações de integridade do sistema e é projetado para fazer interface com os sistemas de monitoramento de integridade usados pelo cliente. Esses relatórios estão disponíveis para acesso off-line pelos usuários, permitindo a validação e auxiliando na solução de problemas.



Prepare-se para a instalação do Keystone Collector no modo privado.

Antes de instalar o Keystone Collector em um ambiente sem acesso à Internet, também

conhecido como *dark site* ou *private mode*, certifique-se de que seus sistemas estejam preparados com o software necessário e atendam a todos os pré-requisitos necessários.

Requisitos para o VMware vSphere

- Sistema operacional: servidor VMware vCenter e ESXi 8.0 ou posterior
- Núcleo: 1 CPU
- RAM: 2 GB
- Espaço em disco: 20 GB vDisk

Requisitos para Linux

- Sistema operacional (escolha um):
  - Red Hat Enterprise Linux (RHEL) 8.6 ou qualquer versão posterior da série 8.x
  - Red Hat Enterprise Linux 9.0 ou versões posteriores
  - Debian 12
- Núcleo: 2 CPU
- RAM: 4 GB
- Espaço em disco: 50 GB vDisk
  - Pelo menos 2 GB de entrada gratuita `/var/lib/`
  - Pelo menos 48 GB de entrada gratuita `/opt/netapp`

O mesmo servidor também deve ter os seguintes pacotes de terceiros instalados. Se disponível através do repositório, estes pacotes serão automaticamente instalados como pré-requisitos:

- 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
  - podman
  - sosreport

Requisitos de rede

Os requisitos de rede para o Keystone Collector incluem o seguinte:

- Active IQ Unified Manager (Gerenciador Unificado) 9,10 ou posterior, configurado em um servidor com a funcionalidade de gateway de API ativada.
- O servidor do Unified Manager deve estar acessível pelo servidor Keystone Collector na porta 443 (HTTPS).
- Uma conta de serviço com permissões de usuário do aplicativo deve ser configurada para o Keystone Collector no servidor do Unified Manager.
- Não é necessária conetividade externa à Internet.
- Todo mês, exporte um arquivo do Keystone Collector e envie-o por e-mail para a equipe de suporte da NetApp . Para obter mais informações sobre como entrar em contato com a equipe de suporte, consulte "Obtenha ajuda com o Keystone".

Instale o Keystone Collector no modo privado

Conclua algumas etapas para instalar o Keystone Collector em um ambiente que não tenha acesso à Internet, também conhecido como *dark site* ou *private mode*. Este tipo de instalação é perfeito para seus sites seguros.

Você pode implantar o Keystone Collector em sistemas VMware vSphere ou instalá-lo em sistemas Linux, dependendo dos seus requisitos. Siga as etapas de instalação que correspondem à opção selecionada.

Implante no VMware vSphere

Siga estes passos:

1. Transfira o ficheiro de modelo OVA a partir de "Portal web da NetApp Keystone".
2. Para obter instruções sobre como implantar o Keystone Collector com arquivo OVA, consulte a "Implantando o modelo OVA"seção .

Instale no Linux

O software Keystone Collector é instalado no servidor Linux usando os arquivos .deb ou .rpm fornecidos, com base na distribuição Linux.

Siga estes passos para instalar o software no seu servidor Linux:

1. Baixe ou transfira o arquivo de instalação do Keystone Collector para o servidor Linux:

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

2. Abra um terminal no servidor e execute os seguintes comandos para iniciar a instalação.
   - **Usando o pacote Debian**

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

   - **Usando arquivo RPM**

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

ou

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

3. Digite `y` quando solicitado a instalar o pacote.

Configure o Keystone Collector no modo privado

Conclua algumas tarefas de configuração para permitir que o Keystone Collector colete dados de uso em um ambiente que não tenha acesso à Internet, também conhecido como *dark site* ou *private mode*. Esta é uma atividade única para ativar e associar os componentes necessários ao seu ambiente de storage. Uma vez configurado, o Keystone Collector monitorará todos os clusters do ONTAP gerenciados pelo Active IQ Unified Manager.

O Keystone Collector fornece o utilitário TUI (Interface de Usuário do Terminal de Gerenciamento de Coletor) do Keystone para executar atividades de configuração e monitoramento. Você pode usar vários controles de teclado, como as teclas Enter e seta, para selecionar as opções e navegar por esta TUI.

Passos

1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:

   ```
   keystone-collector-tui
   ```

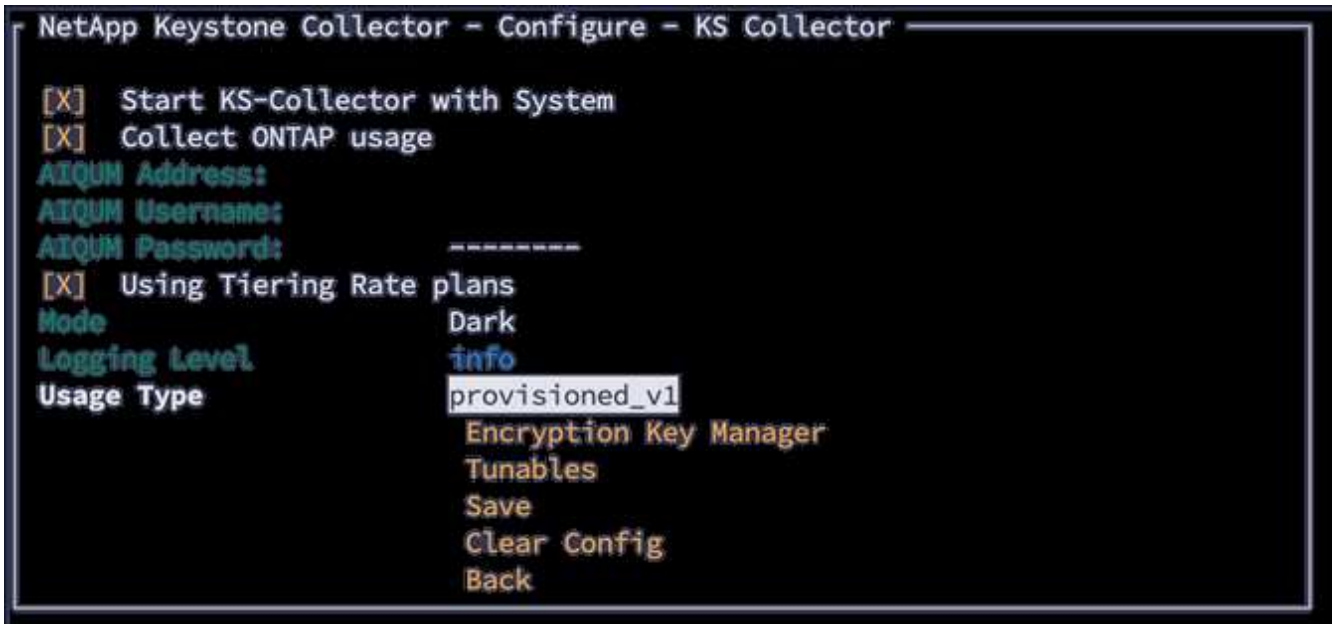
2. Aceda a **Configure > Advanced**.
3. Alterne a opção **Darksite Mode**.

4. Selecione **Guardar**.
5. Vá para **Configure > KS-Collector** para configurar o Keystone Collector.
6. Alterne o campo **Start KS Collector with System**.
7. Alterne o campo **Collect ONTAP Usage**. Adicione os detalhes do servidor e da conta de usuário do Active IQ Unified Manager (Unified Manager).
8. **Opcional**: Alterne o campo **usando planos de taxa de categorização** se a disposição de dados for

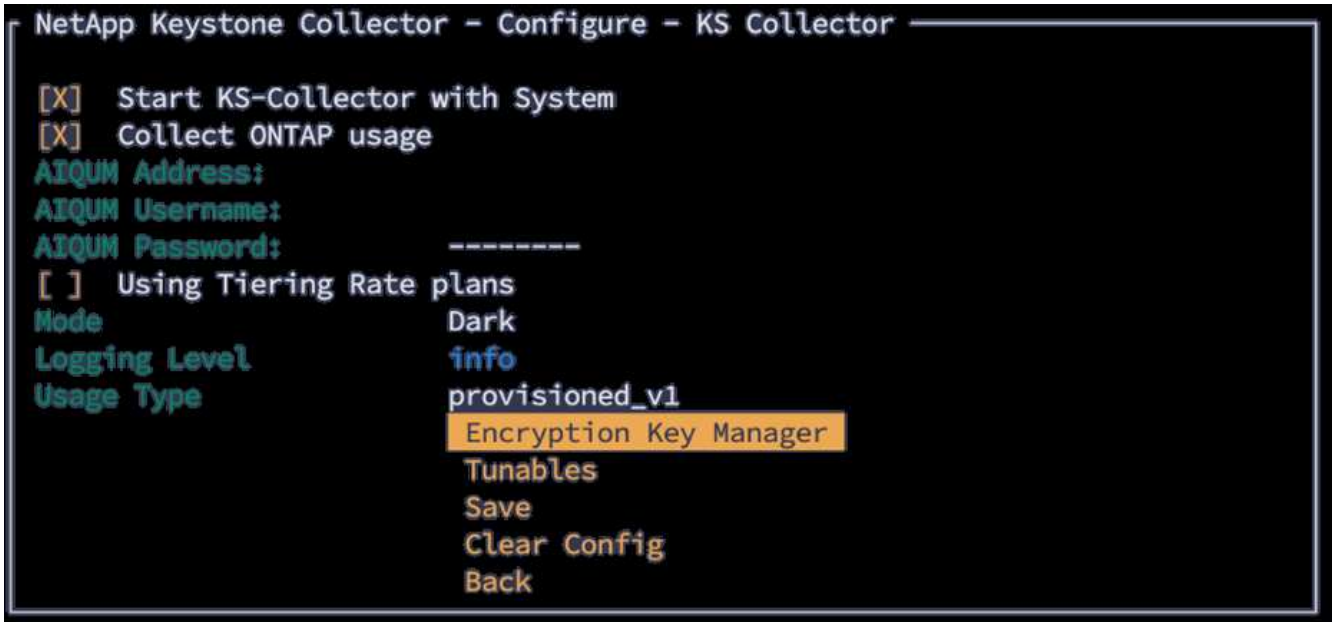
necessária para a assinatura.

9. Com base no tipo de assinatura adquirido, atualize o **tipo de uso**.

   Antes de configurar, confirme o tipo de uso associado à assinatura do NetApp.

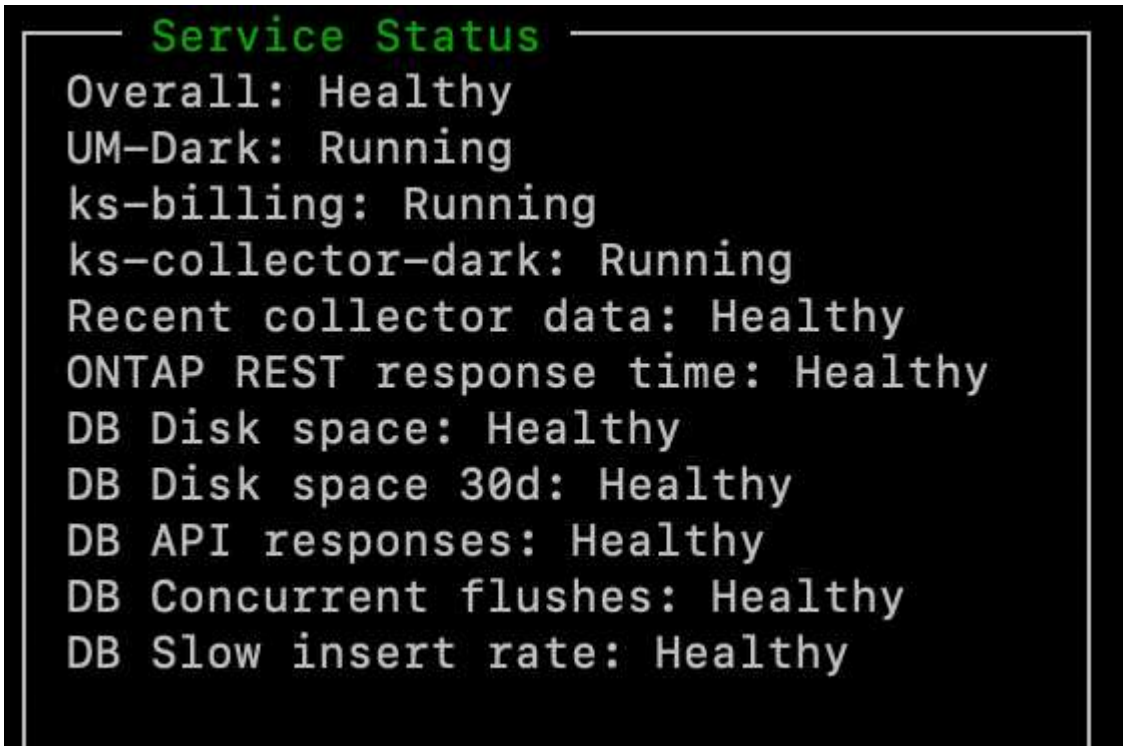


10. Selecione **Guardar**.
11. Vá para **Configure > KS-Collector** para gerar o par de chaves Keystone Collector.
12. Vá para **Gerenciador de chaves de criptografia** e pressione Enter.



13. Selecione **Generate Collector Keypair** e pressione Enter.

14. Certifique-se de que o Keystone Collector está em um estado saudável retornando à tela principal da TUI e verificando as informações **Status do serviço**. O sistema deve mostrar que os serviços estão em um status **geral: Saudável**. Aguarde até 10 minutos, se o status geral permanecer sem integridade após esse período, revise as etapas de configuração anteriores e entre em Contato com a equipe de suporte da NetApp.



15. Saia da TUI de gerenciamento do Keystone Collector selecionando a opção **Sair para Shell** na tela inicial.
16. Recuperar a chave pública gerada:

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

17. Envie um e-mail com este arquivo para ng-keystone-secure-site-upload@netapp.com para sites seguros que não sejam dos Correios dos EUA, ou para ng-keystone-secure-site-usps-upload@netapp.com para sites seguros dos Correios dos EUA.

Exportar relatório de utilização

Você deve enviar o relatório de resumo de uso mensal para o NetApp no final de cada mês. Você pode gerar este relatório manualmente.

Siga estas etapas para gerar o relatório de uso:

1. Vá para **uso de exportação** na tela inicial do Keystone Collector TUI.
2. Reúna os arquivos e envie-os para ng-keystone-secure-site-upload@netapp.com para sites seguros que não sejam dos Correios dos EUA, ou para ng-keystone-secure-site-usps-upload@netapp.com para sites

seguros dos Correios dos EUA.

O Keystone Collector gera um arquivo claro e um arquivo criptografado, que deve ser enviado manualmente para o NetApp. O relatório Limpar arquivo contém os seguintes detalhes que podem ser validados pelo 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-----
```

Atualize ONTAP

O Keystone Collector oferece suporte a atualizações do ONTAP por meio do TUI.

Siga estes passos para atualizar o ONTAP:

1. Aceda a **Manutenção > servidor Web de Atualização do ONTAP**.
2. Copie o arquivo de imagem de atualização do ONTAP para **/opt/NetApp/ONTAP-upgrade/** e selecione **Iniciar servidor Web** para iniciar o servidor Web.

3. Vá para `http://<collector-ip>:8000` usar um navegador da Web para obter assistência de atualização.

Reinicie o Keystone Collector

Você pode reiniciar o serviço Keystone Collector por meio da TUI. Vá para **Manutenção > Reiniciar serviços de Collector** na TUI. Isso reiniciará todos os serviços do coletor e seu status pode ser monitorado na tela inicial do TUI.

Monitore o funcionamento do Keystone Collector no modo privado

Você pode monitorar a integridade do Keystone Collector usando qualquer sistema de monitoramento compatível com solicitações HTTP.

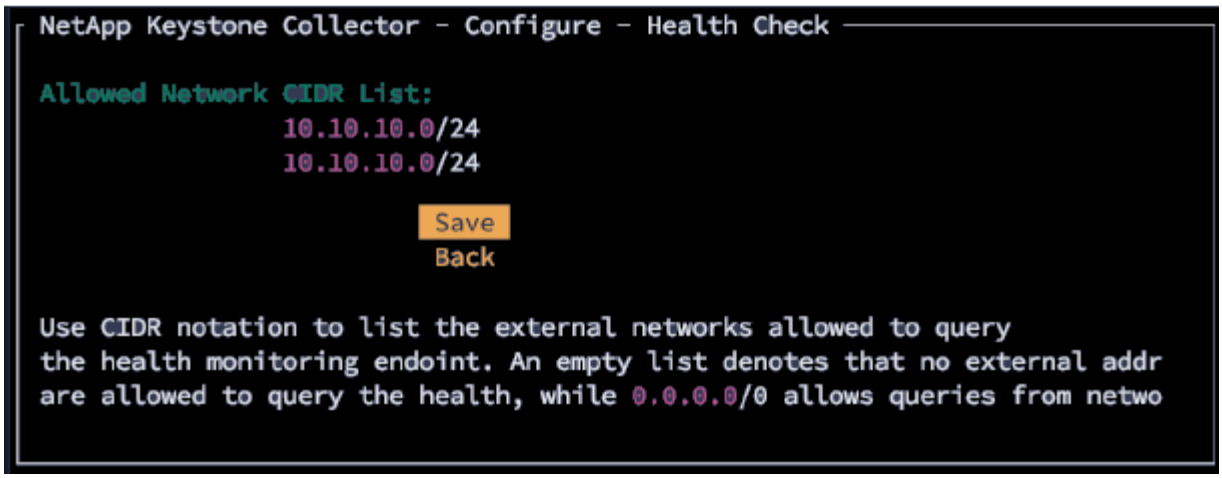
Por padrão, os serviços de integridade do Keystone não aceitam conexões de qualquer IP diferente do localhost. O endpoint de integridade do Keystone é `/uber/health`, e ele escuta todas as interfaces do servidor Keystone Collector na porta `7777`. Na consulta, um código de status de solicitação HTTP com uma saída JSON é retornado do endpoint como uma resposta, descrevendo o status do sistema Keystone Collector. O corpo JSON fornece um status geral de integridade para o `is_healthy` atributo, que é um booleano; e uma lista detalhada de status por componente para o `component_details` atributo. Aqui está um exemplo:

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

Estes códigos de estado são devolvidos:

- **200**: indica que todos os componentes monitorados estão saudáveis
- **503**: indica que um ou mais componentes não são saudáveis
- **403**: Indica que o cliente HTTP que consulta o status de integridade não está na lista *allow*, que é uma lista de CIDR de rede permitidos. Para esse status, nenhuma informação de saúde é retornada.

  A lista *allow* usa o método CIDR de rede para controlar quais dispositivos de rede têm permissão para consultar o sistema de integridade do Keystone. Se você receber o erro 403, adicione seu sistema de monitoramento à lista *allow* de **Keystone Collector Management TUI > Configure > Health Monitoring**.

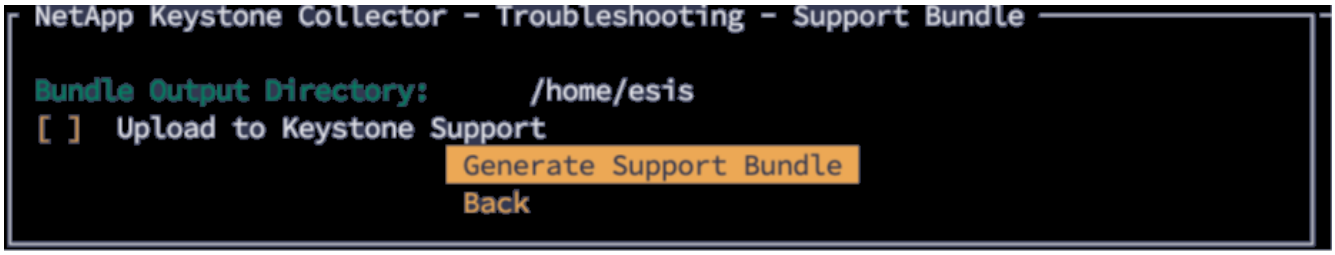


Gerar e coletar pacotes de suporte

Para solucionar problemas com o Keystone Collector, você pode trabalhar com o suporte da NetApp que pode pedir um arquivo *.tar*. Você pode gerar esse arquivo por meio do utilitário TUI de gerenciamento do Keystone Collector.

Siga estas etapas para gerar um arquivo *.tar*:

1. Vá para **Troubleshooting > Generate Support Bundle**.
2. Selecione o local para salvar o pacote e clique em **Generate Support Bundle**.



   Esse processo cria um `tar` pacote no local mencionado que pode ser compartilhado com o NetApp para solucionar problemas.

3. Quando o arquivo for baixado, você pode anexá-lo ao tíquete de suporte do Keystone ServiceNow. Para obter informações sobre como levantar bilhetes, consulte "Gerando solicitações de serviço".

Informações sobre direitos autorais

Informações sobre marcas comerciais