Configurar e configurar o Keystone

Keystone

NetApp
January 15, 2026

Índice

Configurar e configurar o Keystone

Requisitos

Requisitos de infraestrutura virtual para o Keystone Collector

Seu sistema VMware vSphere deve atender a vários requisitos antes que você possa 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 sejam atendidos:

Requisitos de rede

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

> O Keystone Collector requer conectividade com a internet. Você pode fornecer conectividade 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	Propósito
Colecionador Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Gerenciador unificado)	HTTPS	TCP 443	Obrigatório (se estiver usando Keystone ONTAP)	Coleta 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 Keystone StorageGRID)	Coleta de métricas de uso do Keystone Collector para StorageGRID

Keystone Collector (genérico)	Internet (conforme requisitos de URL fornecidos posteriormente)	HTTPS	TCP 443	Obrigatório (conectividade à internet)	Software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Proxy HTTP do cliente	Proxy HTTP	Porta de proxy do cliente	Obrigatório (conectividade à internet)	Software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Servidores DNS do cliente	DNS	TCP/UDP 53	Obrigatório	Resolução de DNS
Keystone Collector (genérico)	Servidores NTP do cliente	NTP	UDP 123	Obrigatório	Sincronização de tempo
Colecionador Keystone (para Keystone ONTAP)	Gerente Unificado	MYSQL	TCP 3306	Funcionalidade opcional	Coleta de métricas de desempenho para Keystone Collector
Keystone Collector (genérico)	Sistema de Monitoramento de Clientes	HTTPS	TCP 7777	Funcionalidade opcional	Relatório de saúde do Keystone Collector
Estações de trabalho de operações do cliente	Colecionador de Keystone	SSH	TCP 22	Gerenciamento	Acesso ao Gerenciamento do Coletor Keystone
Endereços de gerenciamento de cluster e nó do NetApp ONTAP	Colecionador de Keystone	HTTP_8000, PING	TCP 8000, solicitação/resposta de eco ICMP	Funcionalidade opcional	Servidor web para atualizações de firmware ONTAP

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

Acesso URL

O Keystone Collector precisa de acesso aos seguintes hosts da Internet:

Endereço	Razão
https://keystone.netapp.com	Atualizações do software Keystone Collector e relatórios de uso
https://support.netapp.com	NetApp HQ para informações de cobrança e entrega de AutoSupport

Requisitos do Linux para o Keystone Collector

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

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

Servidor Linux:

- Sistema operacional: qualquer um dos seguintes:
  - Debian 12
  - Red Hat Enterprise Linux 8.6 ou versões 8.x posteriores
  - Red Hat Enterprise Linux 9.0 ou versões posteriores
  - CentOS 7 (somente para ambientes existentes)
- Chronyd sincronizado com o tempo
- Acesso aos repositórios de software Linux padrão

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

- podman (Gerente de POD)
- SOS
- crônica
- Python 3 (3.9.14 a 3.11.8)

VM do servidor 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 sejam atendidos:

Requisitos de rede

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

> O Keystone Collector requer conectividade com a internet. Você pode fornecer conectividade 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	Propósito
Colecionador Keystone (para Keystone ONTAP)	Active IQ Unified Manager (Gerenciador unificado)	HTTPS	TCP 443	Obrigatório (se estiver usando Keystone ONTAP)	Coleta 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 Keystone StorageGRID)	Coleta de métricas de uso do Keystone Collector para StorageGRID
Keystone Collector (genérico)	Internet (conforme requisitos de URL fornecidos posteriormente)	HTTPS	TCP 443	Obrigatório (conectividade à internet)	Software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Proxy HTTP do cliente	Proxy HTTP	Porta de proxy do cliente	Obrigatório (conectividade à internet)	Software Keystone Collector, atualizações do sistema operacional e upload de métricas
Keystone Collector (genérico)	Servidores DNS do cliente	DNS	TCP/UDP 53	Obrigatório	Resolução de DNS

Keystone Collector (genérico)	Servidores NTP do cliente	NTP	UDP 123	Obrigatório	Sincronização de tempo
Colecionador Keystone (para Keystone ONTAP)	Gerente Unificado	MYSQL	TCP 3306	Funcionalidade opcional	Coleta de métricas de desempenho para Keystone Collector
Keystone Collector (genérico)	Sistema de Monitoramento de Clientes	HTTPS	TCP 7777	Funcionalidade opcional	Relatório de saúde do Keystone Collector
Estações de trabalho de operações do cliente	Colecionador de Keystone	SSH	TCP 22	Gerenciamento	Acesso ao Gerenciamento do Coletor Keystone
Endereços de gerenciamento de cluster e nó do NetApp ONTAP	Colecionador de Keystone	HTTP_8000, PING	TCP 8000, solicitação/resposta de eco ICMP	Funcionalidade opcional	Servidor web para atualizações de firmware ONTAP

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

Acesso URL

O Keystone Collector precisa de acesso aos seguintes hosts da Internet:

Endereço	Razão
https://keystone.netapp.com	Atualizações do software Keystone Collector e relatórios de uso
https://support.netapp.com	NetApp HQ para informações de cobrança e entrega de AutoSupport

Requisitos para ONTAP e StorageGRID para Keystone

Antes de começar a usar o Keystone, você precisa garantir que os clusters 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

Atenda aos seguintes requisitos se você pretende coletar dados de uso somente por meio do ONTAP:

1. Certifique-se de que o ONTAP 9.8 ou posterior esteja configurado. Para obter informações sobre como configurar um novo cluster, consulte estes links:
   - "Configurar o ONTAP em um novo cluster com o System Manager"
   - "Configurar um cluster com a CLI"
2. Crie contas de login ONTAP com funções específicas. Para saber mais, consulte "Saiba mais sobre como criar contas de login ONTAP" .
   - **Interface de usuário da Web**
     i. Efetue login no ONTAP System Manager usando suas credenciais padrão. Para saber mais, consulte "Gerenciamento de cluster com o System Manager" .
     ii. Crie um usuário ONTAP com a função "somente leitura" e o tipo de aplicativo "http" e habilite a autenticação por senha navegando até **Cluster > Configurações > Segurança > Usuários**.
   - **CLI**
     i. Efetue login no ONTAP CLI usando suas credenciais padrão. Para saber mais, consulte "Gerenciamento de cluster com CLI" .
     ii. Crie um usuário ONTAP com a função "somente leitura" e o tipo de aplicativo "http" e habilite a autenticação por senha. Para saber mais sobre autenticação, consulte "Habilitar acesso à senha da conta ONTAP" .

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 como instalar o Unified Manager, consulte estes links:
   - "Instalando o Unified Manager em sistemas VMware vSphere"
   - "Instalando o Unified Manager em sistemas Linux"
2. Certifique-se de que o cluster ONTAP foi adicionado ao Unified Manager. Para obter informações sobre como adicionar clusters, consulte "Adicionando clusters" .
3. Crie usuários do Unified Manager com funções específicas para coleta de dados de uso e desempenho. Siga estes passos. Para obter informações sobre funções de usuário, consulte "Definições de funções de usuário" .
   a. Efetue login na interface da Web do Unified Manager com as credenciais de usuário do administrador do aplicativo padrão geradas durante a instalação. Ver "Acessando a interface da web do Unified Manager" .
   b. Crie uma conta de serviço para o Keystone Collector com `Operator` função de usuário. As APIs de serviço do Keystone Collector usam esta conta de serviço para se comunicar com o Unified Manager e coletar dados de uso. Ver "Adicionando usuários" .

c. Criar um `Database` conta de usuário, com o `Report Schema` papel. Este usuário é necessário para a coleta de dados de desempenho. Ver "Criando um usuário de banco de dados" .

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

4. Habilite o API Gateway no Unified Manager. O Keystone Collector usa o recurso API Gateway para se comunicar com clusters ONTAP . Você pode habilitar o API Gateway pela interface de usuário da Web ou executando alguns comandos por meio da CLI do Unified Manager.

   Interface de usuário da Web

   Para habilitar o API Gateway na interface de usuário da Web do Unified Manager, faça login na interface de usuário da Web do Unified Manager e habilite o API Gateway. Para obter informações, consulte "Habilitando o API Gateway" .

   CLI

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

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

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

   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 seguintes configurações 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, consulte"Atualizar o software StorageGRID : Visão geral" .
- Uma conta de usuário administrador local do StorageGRID deve ser criada para coleta de dados de uso. Esta conta de serviço é usada pelo serviço Keystone Collector para comunicação com o StorageGRID por meio de APIs do nó do administrador.

  Passos

  a. Efetue login no Grid Manager. Ver "Sign in no Grid Manager" .

  b. Crie um grupo de administração local com `Access mode: Read-only` . Ver "Criar um grupo de administradores" .

  c. Adicione as seguintes permissões:

- Contas de inquilinos
- Manutenção
- Consulta de Métricas

d. Crie um usuário de conta de serviço do Keystone e associe-o ao grupo de administradores. Ver "Gerenciar usuários" .

Instalar o Keystone Collector

Implantar 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 **Implantar modelo OVF**, 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 de "este link" e armazene-o no seu sistema VMware vSphere.
2. No seu sistema VMware vSphere, navegue até a exibição **VMs e modelos**.
3. Clique com o botão direito do mouse na pasta necessária para a máquina virtual (VM) (ou data center, se não estiver usando pastas de VM) e selecione **Implantar modelo OVF**.
4. Na *Etapa 1* do assistente **Implantar modelo OVF**, clique em **Selecionar um modelo OVF** para selecionar o modelo baixado `KeystoneCollector-latest.ova` arquivo.
5. Na *Etapa 2*, especifique o nome da VM e selecione a pasta da VM.
6. Na *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.

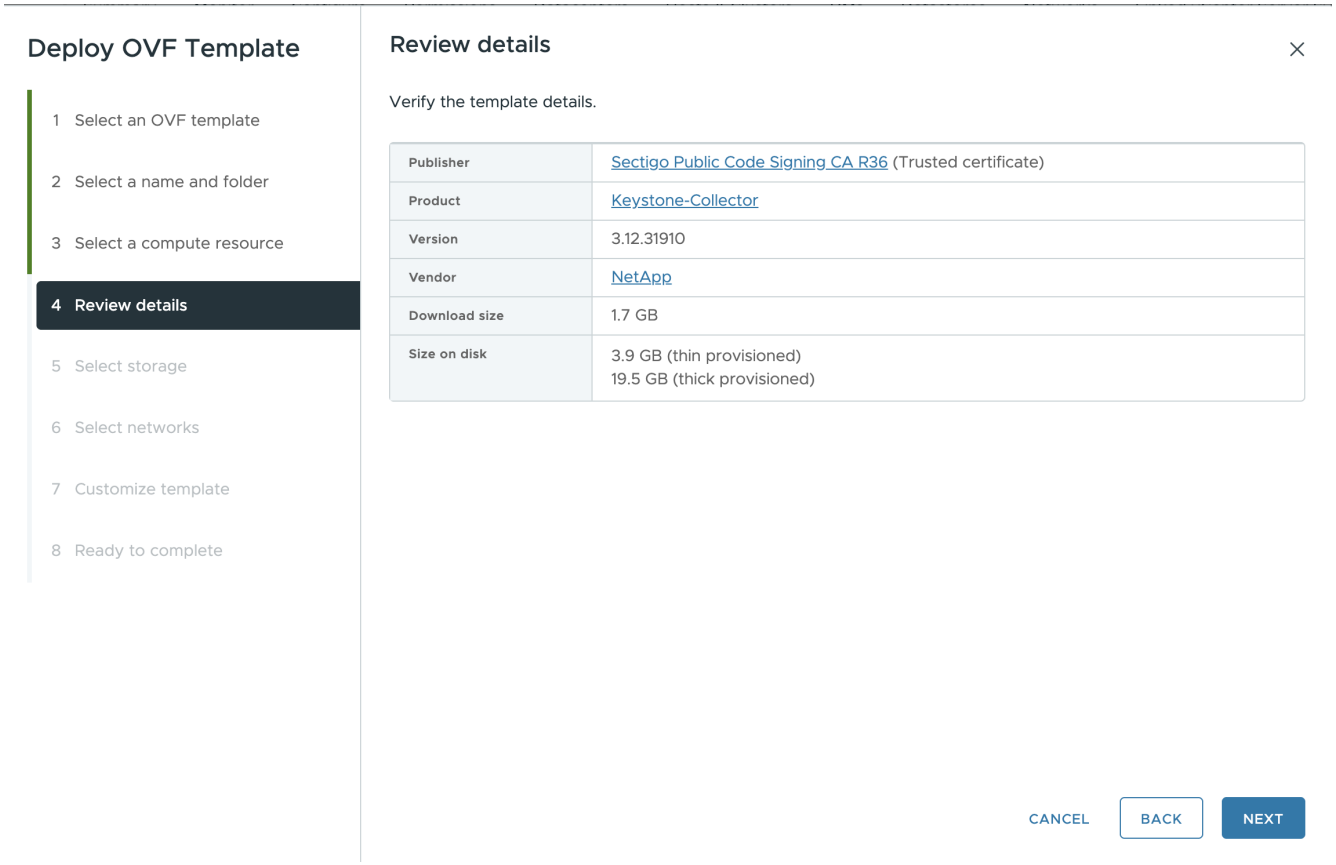
   O armazenamento confiável raiz do vCenter contém apenas certificados VMware. A NetApp usa o Entrust como autoridade de certificação, e esses certificados precisam ser adicionados ao armazenamento confiável do vCenter.

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

   b. Siga os passos no `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. Na *Etapa 5* do assistente **Implantar modelo OVF**, especifique o local para armazenar a VM.
9. Na *Etapa 6*, selecione a rede de destino que a VM usará.
10. Na *Etapa 7 Personalizar modelo*, especifique o endereço de rede inicial e a senha para a conta de usuário administrador.

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

11. Na *Etapa 8 Pronto para concluir* do assistente **Implantar modelo OVF**, revise a configuração e verifique se você definiu corretamente os parâmetros para a implantação do OVA.

Depois que a VM for implantada a partir do modelo e ligada, abra uma sessão SSH na VM e efetue login com as credenciais de administrador temporárias para verificar se a VM está pronta para configuração.

Configuração inicial do sistema

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

> Após 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 do teclado, como as teclas Enter e de seta, para selecionar as opções e navegar por esta TUI.

1. Abra uma sessão SSH no servidor Keystone Collector. Quando você se conectar, o sistema solicitará que você atualize a senha do administrador. Conclua a atualização da senha do administrador conforme necessário.
2. Efetue login usando a nova senha para acessar o TUI. Ao efetuar login, o TUI aparece.

   Alternativamente, 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, o local 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.

Instalar 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 para `root` privilégio.
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 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 para `root` privilégio.
   `sudo su`
2. Baixe o `keystone-sw-repo.deb` arquivo:
   `curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb`
3. Instale o arquivo do repositório do software Keystone :
   `# dpkg -i keystone-sw-repo.deb`
4. Atualizar a lista de pacotes:
   `# apt-get update`
5. Quando o repositório Keystone estiver instalado, instale o pacote keystone-collector:
   `# apt-get install keystone-collector`

Após 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 do teclado, como Enter e as teclas de seta, para selecionar as opções e navegar por esta TUI. Ver"Configurar o Keystone Collector" e"Monitorar a saúde do sistema" para obter informações.

Validação automática do software Keystone

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

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

Configurar o Keystone Collector

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

- O Keystone Collector fornece o utilitário Keystone Collector Management Terminal User Interface (TUI) para executar atividades de configuração e monitoramento. Você pode usar vários controles do teclado, como Enter e as teclas de 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 *site escuro* ou *modo privado*. Para saber mais, consulte"Keystone em modo privado" .

Passos

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

   Para ONTAP

   - *Coletar uso do ONTAP *: Esta opção permite a coleta de dados de uso do ONTAP. Adicione os detalhes do servidor e da conta de serviço do Active IQ Unified Manager (Unified Manager).
   - *Coletar dados de desempenho do ONTAP *: esta opção permite a coleta de dados de desempenho do ONTAP. Isso é desabilitado por padrão. Habilite 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, consulte"Criar usuários do Unified Manager" .
   - **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 esta opção estiver habilitada, consulte"Limitar a coleta de dados privados" .

Para StorageGRID

- *Coletar uso do StorageGRID *: esta opção permite a coleta de detalhes de uso do nó. Adicione o endereço do nó 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 esta opção estiver habilitada, consulte"Limitar a coleta de dados privados" .

4. Alterne o campo **Iniciar KS-Collector com Sistema**.
5. Clique em **Salvar**
.

6. Certifique-se de que o Keystone Collector esteja em bom estado retornando à tela principal do TUI e verificando as informações de **Status do Serviço**. O sistema deve mostrar que os serviços estão em um status **Geral: Saudável**.

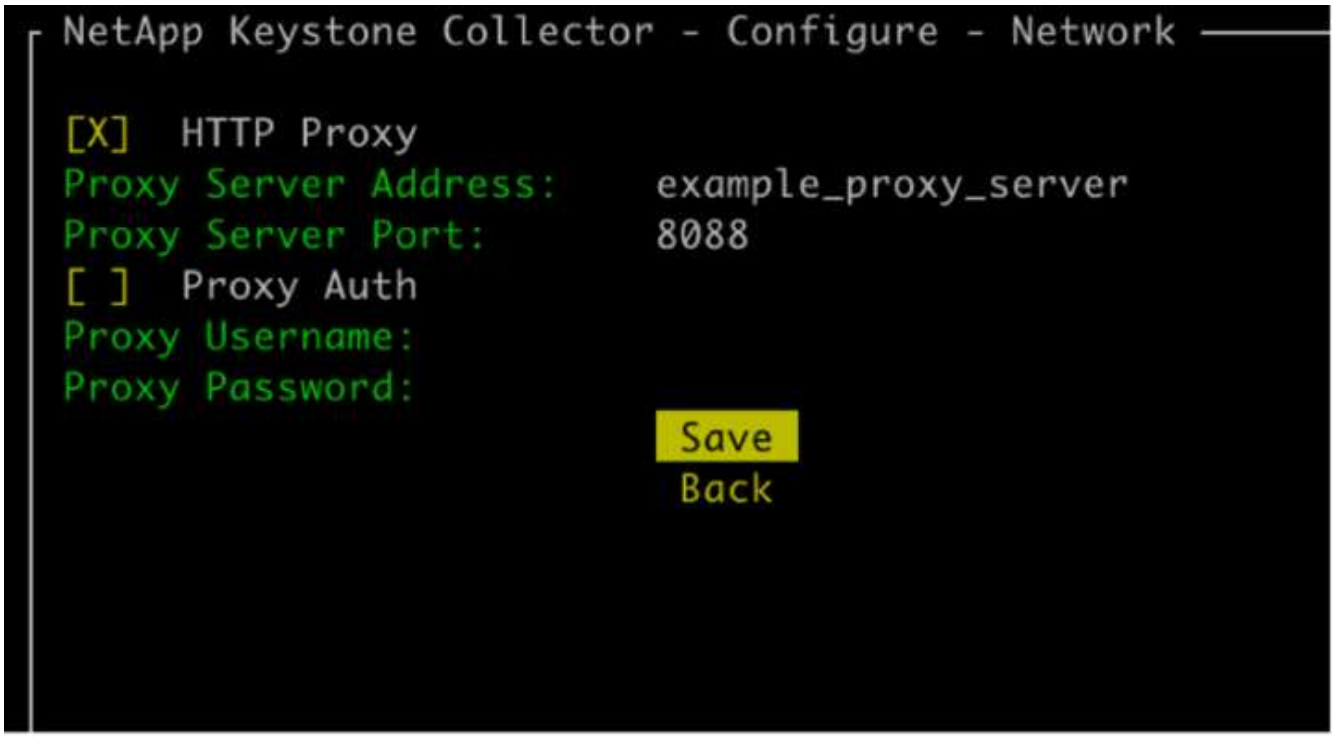
7. Saia da interface gráfica do usuário (TUI) de gerenciamento do Keystone Collector selecionando a opção **Sair para o Shell** na tela inicial.

Configurar proxy HTTP no Keystone Collector

O software Collector suporta o uso de um proxy HTTP para comunicação com a Internet. Isso pode ser configurado no TUI.

Passos

1. Reinicie o utilitário TUI de gerenciamento do Keystone Collector se ele já estiver fechado:
   ```
   $ keystone-collector-tui
   ```
2. Ative o campo **Proxy HTTP** e adicione os detalhes do servidor proxy HTTP, porta e credenciais, se 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. Existe uma opção para limitar ainda mais as informações coletadas mascarando informações confidenciais do conteúdo enviado. Isso não afeta o cálculo do faturamento. No entanto, limitar as informações pode afetar a usabilidade das informações do relatório, pois 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 TUI do Keystone Collector. Esta opção, **Remover Dados Privados**, está habilitada por padrão.

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

Confie em uma CA raiz personalizada

A verificação de certificados em 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 seu sistema, o tráfego baseado na Internet será criptografado novamente com seu certificado CA personalizado. É necessário configurar as definições para verificar a origem como uma CA confiável antes de aceitar o certificado raiz e permitir que as conexões ocorram. Siga estes passos:

Passos

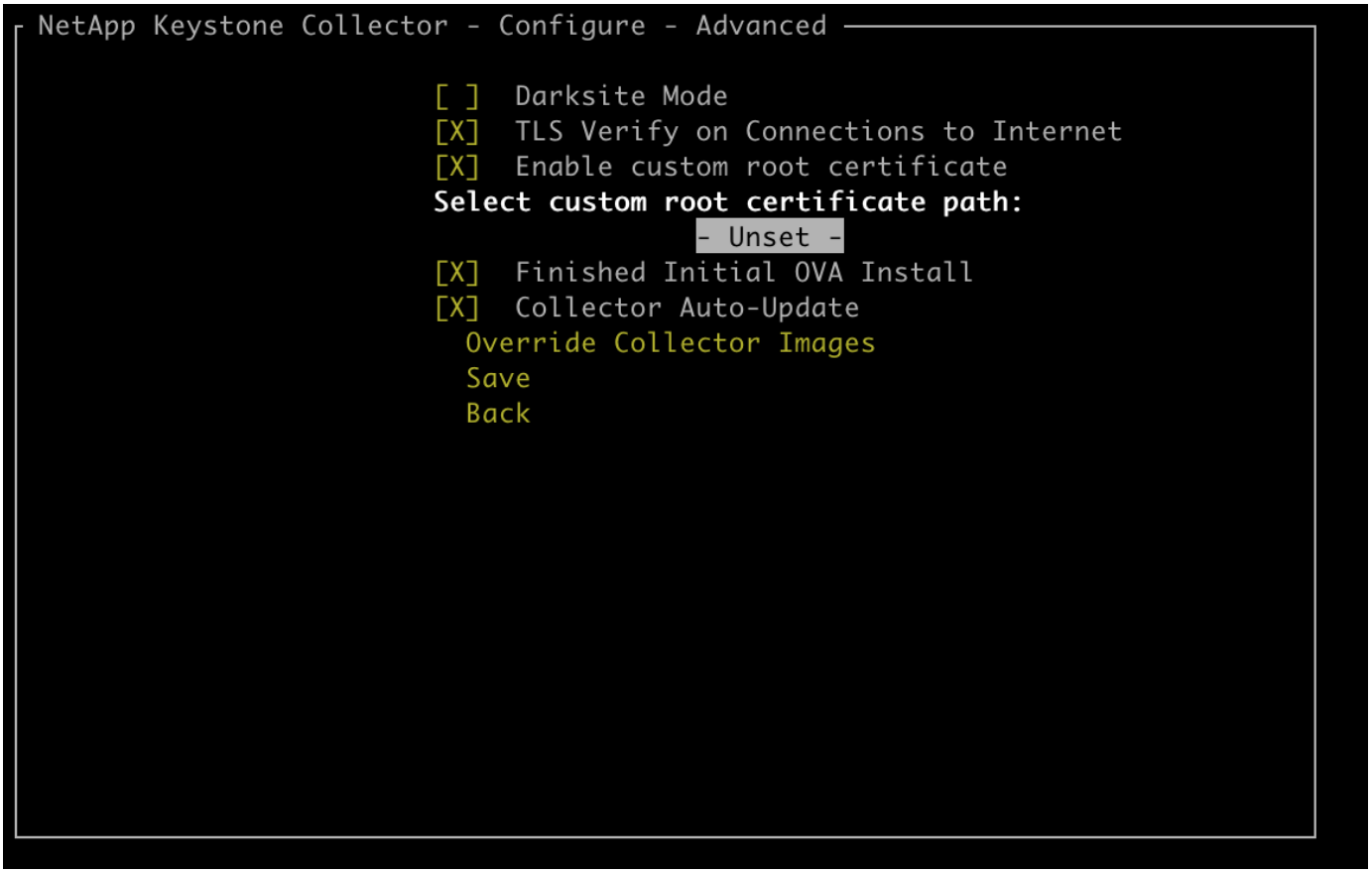
1. Prepare o certificado da CA. Deve estar no formato de arquivo *X.509 codificado em base64*.

   As extensões de arquivo suportadas são `.pem` , `.crt` , `.cert` . Certifique-se de que o certificado esteja em um desses formatos.

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

6. Para **Selecionar caminho de certificado raiz personalizado:**, selecione `- Unset -`
7. Pressione Enter. Uma caixa de diálogo para selecionar o caminho do certificado é exibida.
8. Selecione o certificado raiz no navegador do sistema de arquivos ou insira o caminho exato.
9. Pressione Enter. Você retorna para a tela **Avançado**.
10. Selecione **Salvar**. A configuração é aplicada.

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



Crie níveis de serviço de desempenho

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.

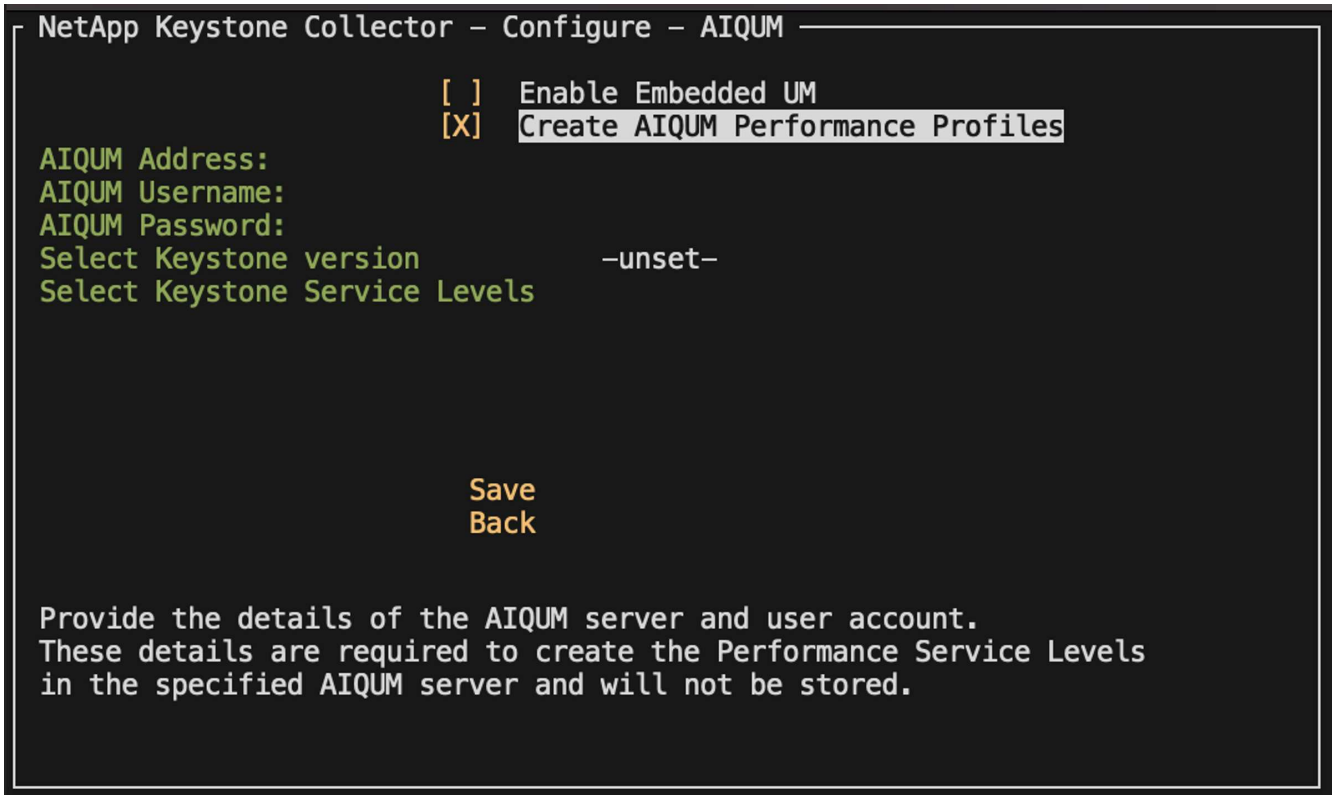
Para saber mais sobre PSLs, consulte"Níveis de serviço de desempenho" .

Para saber mais sobre os níveis de serviço, consulte"Níveis de serviço em Keystone" .

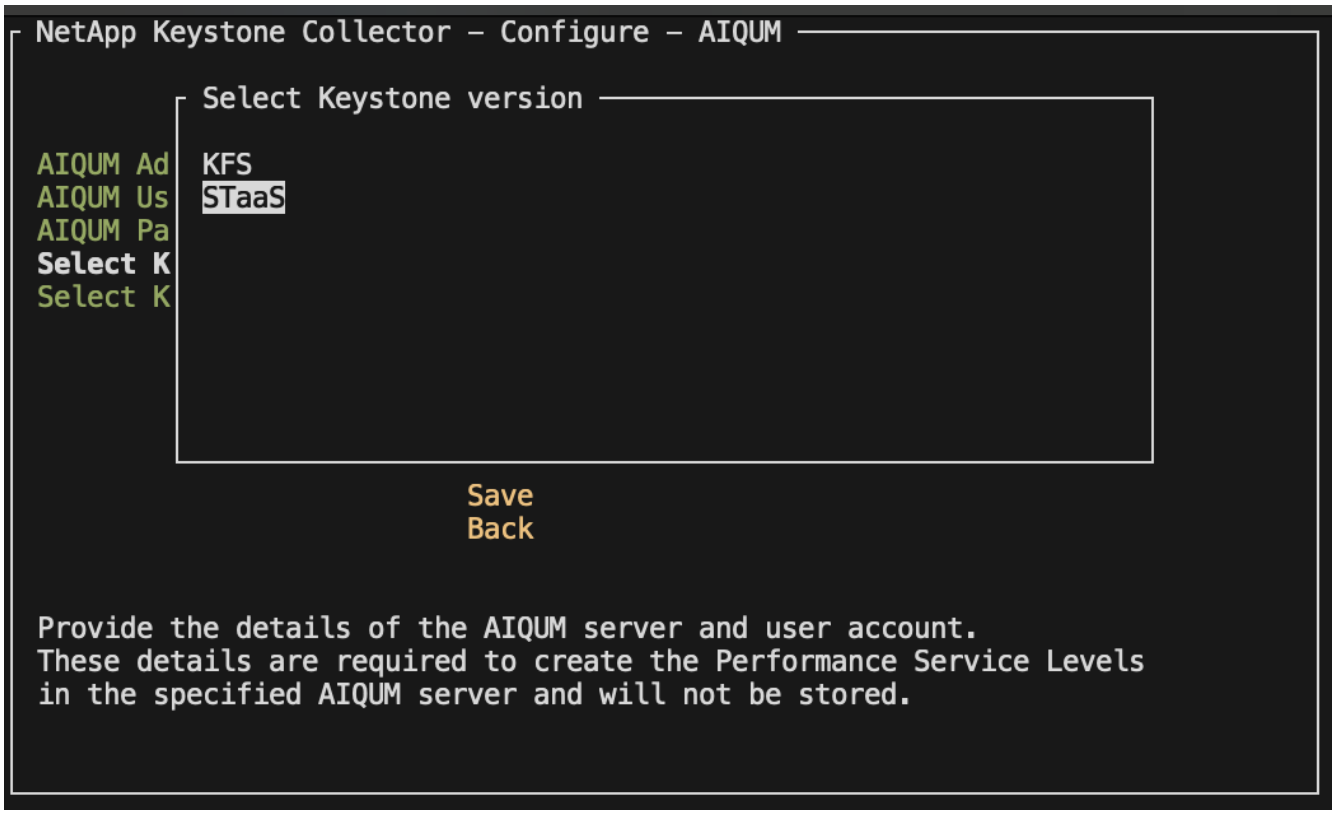
Passos

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

3. Habilite a opção **Criar perfis de desempenho do AIQUM**.
4. Insira os detalhes do servidor e da conta de usuário do Active IQ Unified Manager . Esses detalhes são necessários para criar PSLs e não serão armazenados.

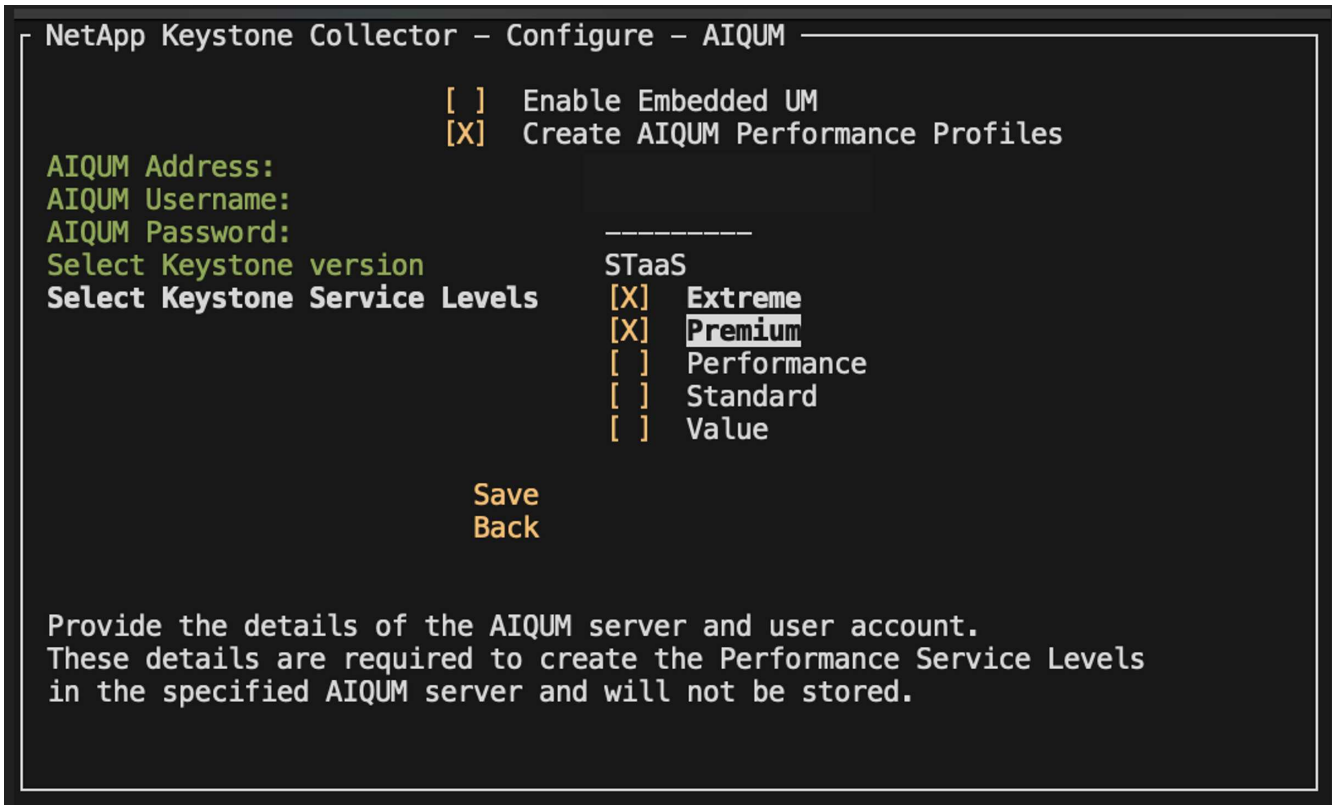


5. Para *Versão Select Keystone *, selecione `–unset–` .
6. Pressione Enter. Uma caixa de diálogo para selecionar a versão do Keystone é exibida.
7. Destaque **STaaS** para especificar a versão do Keystone para o Keystone STaaS e pressione Enter.



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 Keystone | Versão 1" .

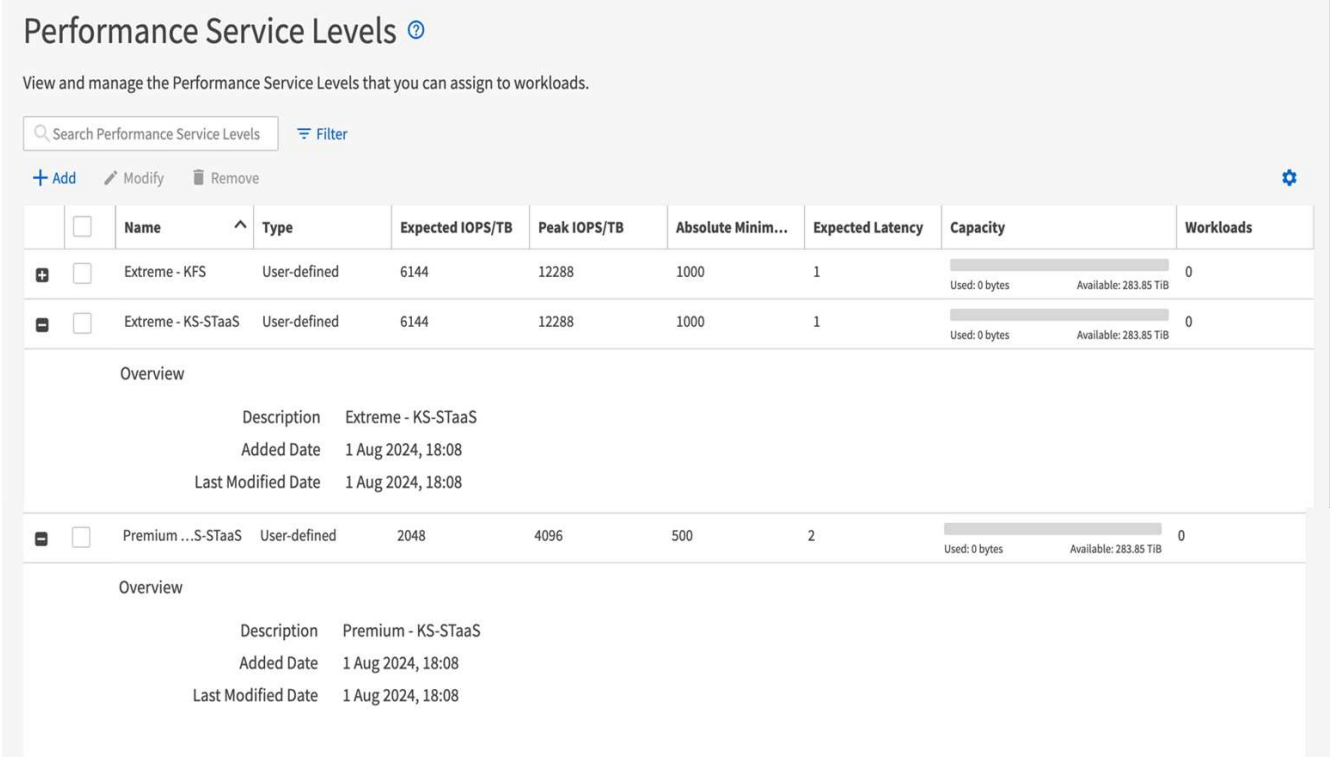
8. Todos os níveis de serviço de desempenho do Keystone suportados serão exibidos na opção *Selecionar níveis de serviço do Keystone * para a versão especificada do Keystone . Habilite os níveis de serviço de desempenho desejados na lista.



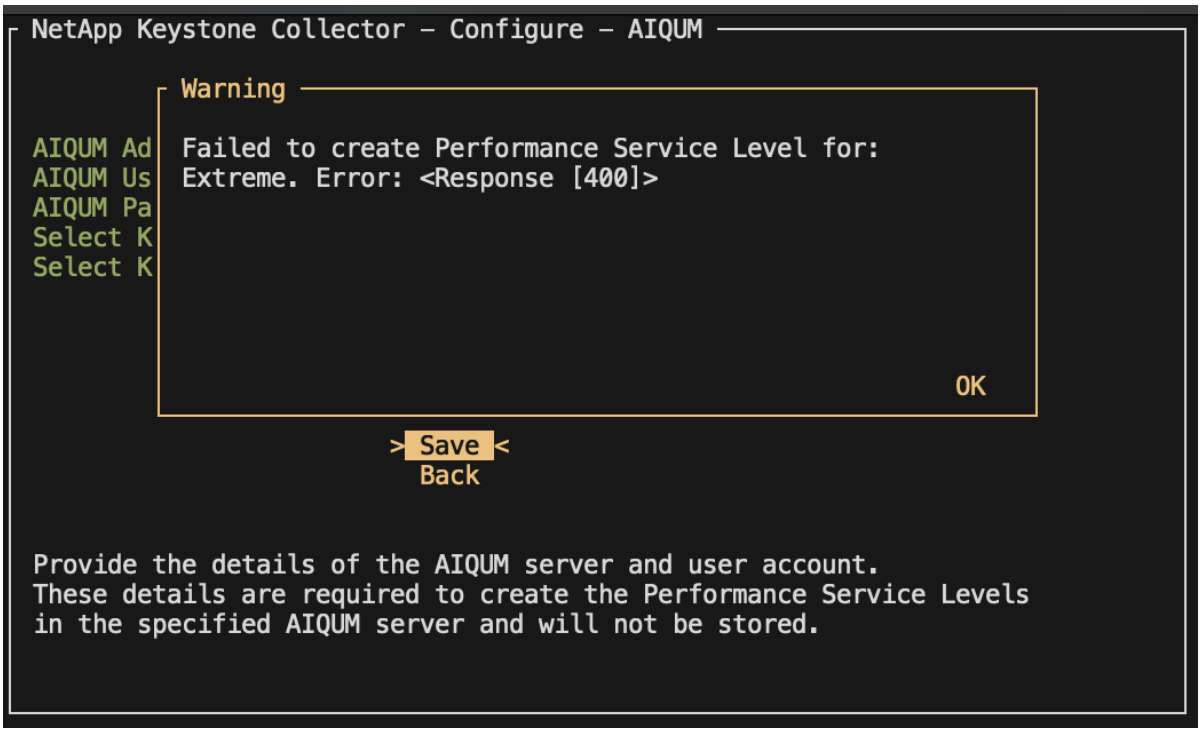
Você pode selecionar vários níveis de serviço de desempenho simultaneamente para criar PSLs.

9. Selecione **Salvar** e pressione Enter. Serão criados Níveis de Serviço de Desempenho.

   Você pode visualizar os PSLs criados, como Premium-KS-STaaS para STaaS ou Extreme KFS para KFS, na página **Níveis de serviço de desempenho** no Active IQ Unified Manager. Se os PSLs criados não atenderem às suas necessidades, você poderá modificá-los para atendê-los. Para saber mais, consulte"Criação e edição de níveis de serviço de desempenho" .



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.



Instalar o coletor ITOM

Requisitos de instalação para o coletor Keystone ITOM

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

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.

- Requisitos de recursos: os requisitos de recursos da VM com base no número de nós NetApp monitorados são os seguintes:
  - 2 a 10 nós: 4 CPUs, 8 GB de RAM, 40 GB de disco
  - 12 a 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 ITOM Collector também precisa ser configurada como um host de interceptação SNMP e um servidor Syslog no cluster NetApp e nos switches de cluster, se aplicável.

Requisitos de rede

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

Fonte	Destino	Protocolo	Portos	Descrição
Coletor ITOM	IPs de gerenciamento de cluster NetApp ONTAP	HTTPS, SNMP	TCP 443, UDP 161	Monitoramento dos controladores ONTAP
IPs de gerenciamento de cluster e nó NetApp ONTAP	Coletor ITOM	SNMP, Syslog	UDP 162, UDP 514	Traps SNMP e Syslogs de controladores
Coletor ITOM	Comutadores de cluster	SNMP	UDP 161	Monitoramento de interruptores
Comutadores de cluster	Coletor ITOM	SNMP, Syslog	UDP 162, UDP 514	Armadilhas SNMP e Syslogs de switches
Coletor ITOM	IPs dos nós do StorageGRID	HTTPS, SNMP	TCP 443, UDP 161	Monitoramento SNMP do StorageGRID

IPs dos nós do StorageGRID	Coletor ITOM	SNMP, Syslog	UDP 162, UDP 514	Armadilhas SNMP do StorageGRID
Coletor ITOM	Colecionador de Keystone	SSH, HTTPS, SNMP	TCP 22, TCP 443, UDP 161	Monitoramento e gerenciamento remoto do Keystone Collector
Coletor ITOM	DNS local	DNS	UDP 53	Serviços DNS públicos ou privados
Coletor ITOM	Servidor(es) NTP de escolha	NTP	UDP 123	Controle de 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 da Keystone fornece um link dinâmico para baixar o arquivo de configuração do ITOM Collector, que expira em duas horas.

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

Siga estas etapas para instalar o software no seu servidor Linux:

Antes de começar

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

Passos

1. Baixe o arquivo de configuração do coletor ITOM para o seu 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. A execução do arquivo de instalação solicita que você:
   a. Aceite o contrato de licença de usuário final (EULA).
   b. Insira os detalhes do usuário para a instalação.
   c. Especifique o diretório pai da 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 confirmará que o ITOM Collector foi instalado com sucesso.

- O arquivo de configuração do coletor ITOM faz adições a `/etc/sudoers` para lidar com reinicializações de serviço e despejos de memória.
- A instalação do ITOM Collector no servidor Linux cria um usuário padrão chamado **ITOM** para executar o ITOM Collector sem privilégios de root. 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 vem a seguir?

Após a 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 da Keystone configurará o ITOM Collector remotamente, incluindo mais descoberta de dispositivos e configuração de monitoramento, e enviará uma confirmação assim que a configuração estiver concluída. Para 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 do ITOM Collector, executando o assistente InstallShield e inserindo as credenciais de monitoramento necessárias.

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

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

Siga estas etapas para instalar o software coletor ITOM no seu servidor Windows:

Antes de começar

Certifique-se de que o serviço ITOM Collector tenha a permissão **Fazer logon como um serviço** em Política local/Atribuição de direitos de usuário nas configurações de política de segurança local do servidor Windows.

Passos

1. Baixe o arquivo de configuração do coletor ITOM para o seu servidor Windows.
2. Abra o arquivo de instalação para iniciar o assistente do InstallShield.
3. Aceite o contrato de licença de usuário final (EULA). O assistente do InstallShield extrai os binários necessários e solicita que você insira as credenciais.
4. Insira as credenciais da conta na qual o ITOM Collector será executado:
   - 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 Windows que não fazem parte do mesmo domínio, use uma conta de administrador local e conecte-se a cada recurso com credenciais de

administrador local. Você pode optar por definir a senha para que ela não expire, para reduzir 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 tenha requisitos específicos.
6. Selecione *Avançar* para iniciar a instalação. Você pode usar a pasta preenchida ou escolher uma diferente. Uma caixa de status exibe o progresso da instalação, seguida pela caixa de diálogo Assistente do InstallShield concluído.

O que vem a seguir?

Após a 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 da Keystone configurará o ITOM Collector remotamente, incluindo mais descoberta de dispositivos e configuração de monitoramento, e enviará uma confirmação assim que a configuração estiver concluída. Para dúvidas ou informações adicionais, entre em contato com keystone.services@netapp.com.

Configurar AutoSupport para Keystone

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

Sobre esta tarefa

Você deve observar o seguinte antes de configurar o AutoSupport para incluir dados do Keystone .

- Edite as opções de telemetria do AutoSupport usando o ONTAP CLI. Para obter informações sobre como gerenciar os serviços do AutoSupport e a função de administrador do sistema (cluster), consulte "Visão geral do Gerenciar AutoSupport" e "Administradores de cluster e SVM" .
- Inclua os subsistemas nos pacotes AutoSupport diários e semanais para garantir a coleta precisa de dados para o Keystone. Para obter informações sobre os subsistemas AutoSupport , consulte "O que são subsistemas AutoSupport" .

Passos

1. Como usuário administrador do sistema, efetue login no cluster Keystone ONTAP usando SSH. Para obter informações, consulte "Acesse o cluster usando SSH" .
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 este comando, consulte "gatilho de suporte automático do nó do sistema modificar" .

Monitorar e atualizar

Monitore a saúde do Keystone Collector

Você pode monitorar a saúde do Keystone Collector usando qualquer sistema de monitoramento que suporte solicitações HTTP. Monitorar a saúde pode ajudar a garantir que os dados estejam disponíveis no painel do Keystone .

Por padrão, os serviços de saúde do Keystone não aceitam conexões de nenhum IP diferente do host local. O ponto final de saúde da Keystone é `/uber/health` , e escuta em 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 ponto de extremidade como uma resposta, descrevendo o status do sistema Keystone Collector. O corpo JSON fornece um status geral de saúde 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"}}
```

Esses códigos de status são retornados:

- **200**: indica que todos os componentes monitorados estão saudáveis
- **503**: indica que um ou mais componentes não estão saudáveis
- **403**: indica que o cliente HTTP que consulta o status de integridade não está na lista *allow*, que é uma lista de CIDRs 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 saúde Keystone . Se você receber esse erro, adicione seu sistema de monitoramento à lista *permitida* em * TUI de gerenciamento do Keystone Collector > Configurar > Monitoramento de integridade*.

Usuários do Linux, observem este problema conhecido:

Descrição do problema: O Keystone Collector executa vários contêineres como parte do sistema de medição de uso. Quando o servidor Red Hat Enterprise Linux 8.x é reforçado com as políticas dos Guias de Implementação Técnica de Segurança (STIG) da Agência de Sistemas de Informação de Defesa dos EUA (DISA), um problema conhecido com o fapolicyd (File Access Policy Daemon) tem sido observado intermitentemente. Este problema é identificado como"erro 1907870" . **Solução alternativa**: Até que seja resolvido pelo Red Hat Enterprise, a NetApp recomenda que você contorne esse problema colocando `fapolicyd` no modo permissivo. Em/`etc/fapolicyd/fapolicyd.conf` , defina o valor de `permissive = 1` .

Ver logs do sistema

Você pode visualizar os logs do sistema do Keystone Collector para revisar 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 registros do sistema podem ser revisados por meio do utilitário de sistema padrão *journalctl*. Você pode aproveitar os seguintes serviços principais para examinar os logs:

- ks-coletor
- ks-saúde
- ks-atualização automática

O principal serviço de coleta de dados *ks-collector* produz logs no formato JSON com um `run-id` atributo associado a cada tarefa de coleta de dados agendada. A seguir, um exemplo de uma tarefa bem-sucedida 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 uma tarefa bem-sucedida para coleta opcional de dados de desempenho:

```
{"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"}
```

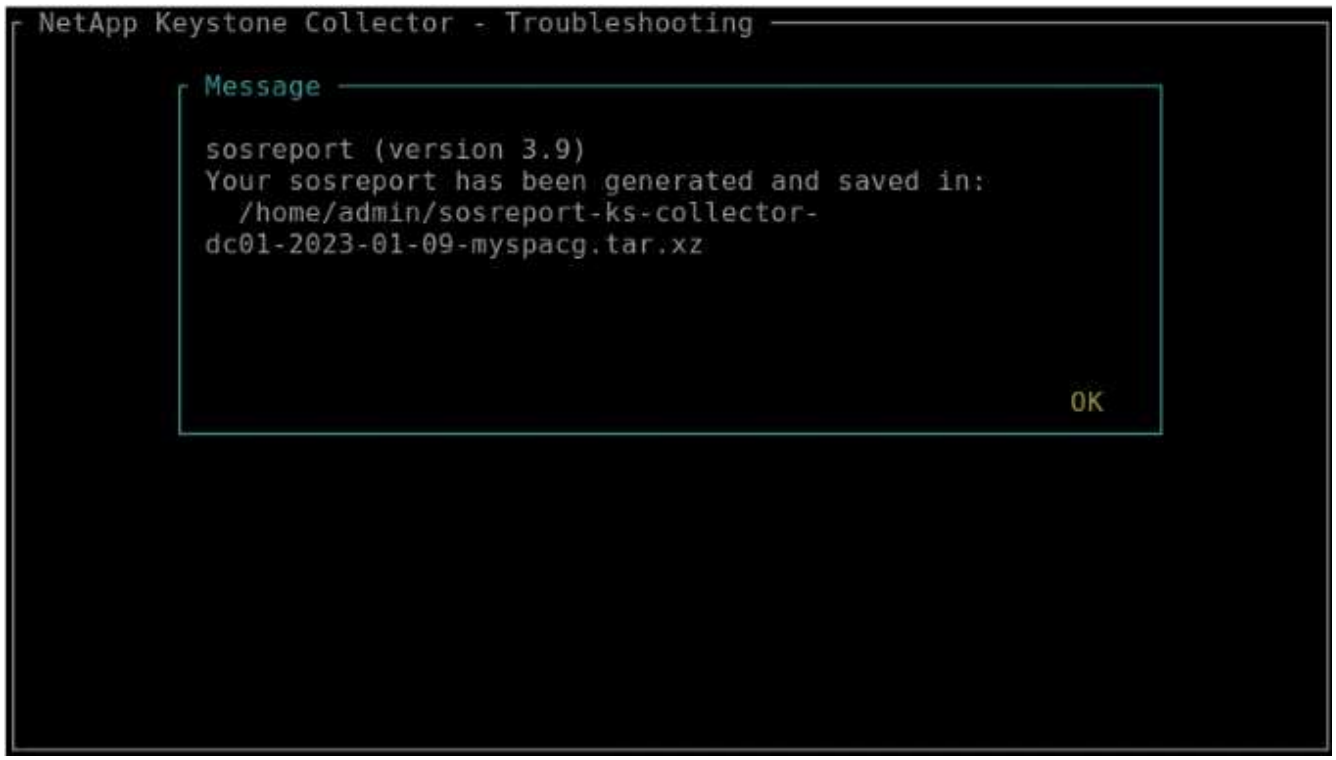
Gerar e coletar pacotes de suporte

O TUI do Keystone Collector permite que você gere pacotes de suporte e os adicione a 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. Acesse **Solução de problemas > Gerar pacote de suporte**
   .

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



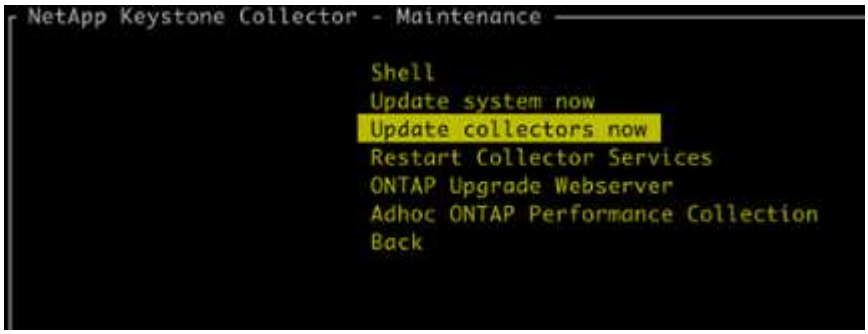
4. Quando o arquivo for baixado, você pode anexá-lo ao tíquete de suporte do Keystone ServiceNow. Para obter informações sobre como levantar bilhetes, consulte "Gerando solicitações de serviço".

Atualizar manualmente o Keystone Collector

O recurso de atualização automática no Keystone Collector é habilitado por padrão, o que atualiza automaticamente o software Keystone Collector a cada nova versão. No entanto, você pode desabilitar esse recurso e atualizar manualmente o software.

Passos

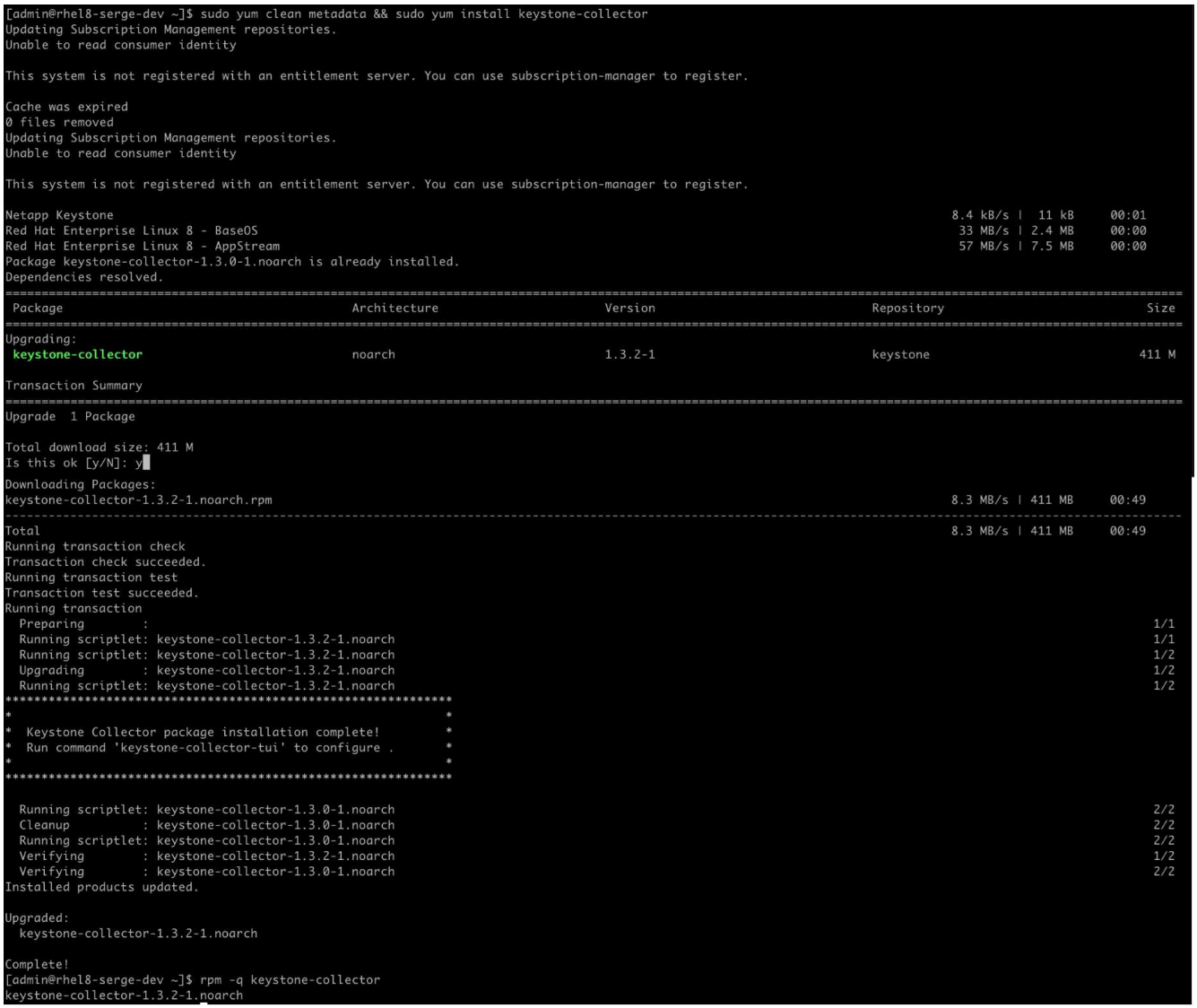
1. Inicie o utilitário TUI de gerenciamento do Keystone Collector:
   ```
   $ keystone-collector-tui
   ```
2. Na tela de manutenção, selecione a opção **Atualizar coletores agora**.



Como alternativa, execute estes comandos para atualizar a versão:

Para CentOS:

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



Para Debian:

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

3. Reinicie a interface gráfica do usuário (TUI) de gerenciamento do Keystone Collector. Você poderá ver a versão mais recente na parte superior esquerda da tela inicial.

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

   Para CentOS:

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

   Para Debian:

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

Segurança do Keystone Collector

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

O funcionamento do Keystone Collector é baseado nos seguintes princípios de segurança:

- **Privacidade por design** - O Keystone Collector coleta dados mínimos para realizar a medição de uso e o monitoramento de desempenho. Para obter mais informações, consulte "Dados coletados para faturamento" . O"Remover dados privados" opção é habilitada por padrão, o que mascara e protege informações confidenciais.
- **Acesso com privilégios mínimos** - O Keystone Collector requer permissões mínimas para monitorar os sistemas de armazenamento, o que minimiza os riscos de segurança e evita quaisquer modificações não intencionais nos dados. Essa abordagem está alinhada ao princípio do menor privilégio, aprimorando a postura geral de segurança dos ambientes monitorados.
- **Estrutura de desenvolvimento de software segura** - A Keystone usa uma estrutura de desenvolvimento de software segura durante todo o ciclo de desenvolvimento, o que atenua riscos, reduz vulnerabilidades e protege o sistema contra ameaças potenciais.

Reforço da segurança

Por padrão, o Keystone Collector é configurado para usar configurações de segurança reforçada. 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 qualquer alteração na configuração do sistema operacional fora do software de gerenciamento Keystone Collector pode reduzir a segurança do sistema. Para obter mais informações, consulte "Guia de referência do CIS" .
  - Recebe e instala automaticamente patches de segurança verificados pelo Keystone Collector por meio do recurso de atualização automática. Desabilitar essa funcionalidade pode levar a um software vulnerável e sem patches.
  - Autentica atualizações recebidas do Keystone Collector. Desabilitar a verificação do repositório APT pode levar à instalação automática de patches não autorizados, potencialmente introduzindo vulnerabilidades.
- O Keystone Collector valida automaticamente os certificados HTTPS para garantir a segurança da conexão. Desabilitar esse recurso pode levar à representação de endpoints externos e vazamento de dados de uso.
- Suporte do Keystone Collector"CA confiável personalizada" certificação. Por padrão, ele confia em certificados assinados por CAs raiz públicas reconhecidas pelo"Programa de Certificação Mozilla CA" . Ao habilitar CAs confiáveis adicionais, o Keystone Collector habilita a validação de certificado HTTPS para conexões com endpoints que apresentam esses certificados.
- O Keystone Collector habilita a opção **Remover Dados Privados** por padrão, que mascara e protege informações confidenciais. Para obter mais informações, consulte "Limitar a coleta de dados privados" . Desabilitar esta opção resulta na comunicação de dados adicionais ao sistema Keystone . Por exemplo, pode incluir informações inseridas pelo usuário, como nomes de volumes, que podem ser consideradas

informações confidenciais.

Informações relacionadas

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

Tipos de dados do usuário que a Keystone coleta

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 somente para ONTAP , se esta opção estiver habilitada no Keystone Collector.

Coleta de dados 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:

- Aglomerados
  - ClusterUUID
  - Nome do cluster
  - Número de série
  - Localização (com base no valor inserido no cluster ONTAP)
  - Contato
  - Versão
- Nós
  - Número de série
  - Nome do nó
- Volumes
  - Nome agregado
  - Nome do volume
  - VolumeInstanceUUID
  - Bandeira IsCloneVolume
  - Sinalizador IsFlexGroupConstituent
  - Sinalizador IsSpaceEnforcementLogical
  - Sinalizador IsSpaceReportingLogical
  - Espaço Lógico Usado por Afs
  - PercentSnapshotSpace
  - Dados de usuário inativos da camada de desempenho
  - Porcentagem de dados de usuário inativos da camada de desempenho
  - Nome do QoSAdaptivePolicyGroup
  - Nome do QoSPolicyGroup
  - Tamanho
  - Usado
  - FísicoUsado
  - TamanhoUsadoPorInstantâneos
  - Tipo
  - VolumeStyleExtended
  - Nome do Vserver
  - Bandeira IsVsRoot
- Servidores V
  - Nome do Vserver

    - VserverUUID
    - Subtipo
- Agregados de armazenamento
    - Tipo de armazenamento
    - Nome do Agregado
    - UUID agregado
    - Físico usado
    - Tamanho disponível
    - Tamanho
    - Tamanho usado
- Armazenamentos de objetos agregados
    - Nome do repositório de objetos
    - UUID do ObjectStore
    - Tipo de provedor
    - Nome do Agregado
- Volumes clones
    - FlexClone
    - Tamanho
    - Usado
    - Vserver
    - Tipo
    - Volume dos Pais
    - PaiVservidor
    - É Constituinte
    - Dividir Estimativa
    - Estado
    - Porcentagem usada do FlexClone
- LUNs de armazenamento
    - UUID LUN
    - Nome do LUN
    - Tamanho
    - Usado
    - Bandeira IsReserved
    - Sinalizador IsRequested
    - Nome da unidade lógica
    - QoSPolicyUUID
    - Nome da Política QoSP

    - VolumeUUID
    - Nome do Volume
    - SVMUUID
    - Nome SVM
- Volumes de armazenamento
    - VolumeInstanceUUID
    - Nome do Volume
    - Nome SVM
    - SVMUUID
    - QoSPolicyUUID
    - Nome da Política QoSP
    - Pegada da camada de capacidade
    - PerformanceTierFootprint
    - Pegada Total
    - Política de níveis
    - Bandeira IsProtected
    - Bandeira IsDestination
    - Usado
    - FísicoUsado
    - ClonarParentUUID
    - Espaço Lógico Usado por Afs
- Grupos de políticas de QoS
    - Grupo de Políticas
    - QoSPolicyUUID
    - Máxima taxa de transferência
    - Rendimento mínimo
    - MaxThroughputIOPS
    - Máxima taxa de transferência em MBps
    - MinThroughputIOPS
    - Mín. throughput MBps
    - Bandeira IsShared
- Grupos de políticas de QoS adaptáveis ONTAP
    - Nome da Política QoSP
    - QoSPolicyUUID
    - Pico IOPS
    - Alocação de IOPS de pico
    - AbsoluteMinIOPS

    - IOPS esperado
    - Alocação de IOPS esperada
    - Tamanho do bloco
- Pegadas
    - Vserver
    - Volume
    - Pegada Total
    - VolumeBlocksFootprintBin0
    - VolumeBlocksFootprintBin1
- MetroCluster
    - Nó
    - Agregar
    - LIFs
    - Replicação de configuração
    - Conexões
    - Aglomerados
    - Volumes
- Aglomerados MetroCluster
    - ClusterUUID
    - Nome do cluster
    - UUID do Cluster Remoto
    - Nome do Cluster Remoto
    - Estado de 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
    - Armazenar
    - Volume de armazenamento em uso
- Mediadores do MetroCluster
    - Endereço do Mediador
    - Porta do Mediador
    - Mediador Configurado
    - Mediador Alcançável
    - Modo
- Métricas de Observabilidade do Coletor
    - Hora da coleta
    - Ponto de extremidade da API do Active IQ Unified Manager consultado
    - Tempo de resposta
    - Número de registros
    - IP da instância AIQUM
    - ID da instância do coletor

Dados de desempenho coletados para ONTAP: Saiba mais

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

- Nome do cluster
- UUID de cluster
- ID do objeto
- Nome do Volume
- UUID da instância de volume
- Vserver
- VserverUUID
- Nó Serial
- Versão ONTAP
- Versão AIQUM
- Agregar
- UUID agregado
- Chave de recurso
- Carimbo de data/hora
- IOPSPerTb
- Latência
- Latência de leitura
- Escreva MBps
- Latência de Transmissão QoSMin
- Latência QoSNBlade
- Espaço de cabeça usado
- Taxa de Perda de Cache
- Outra Latência
- Latência de Agregação QoSA
- IOPS
- QoSNetworkLetency
- Operações disponíveis
- Latência de escrita
- Latência da Nuvem QoS
- Latência de interconexão QoSCluster
- Outros MBps
- Latência QoSCop
- Latência QoSDBlade
- Utilização

- ReadIOPS
- MBps
- Outros IOPS
- Latência do Grupo de Políticas QoSP
- LeiaMBps
- Latência do QoSSyncSnapmirror
- Dados de nível de sistema
  - Gravação/Leitura/Outro/IOPS total
  - Gravação/Leitura/Outro/Taxa de transferência total
  - Gravação/Leitura/Outro/Latência Total
- WriteIOPS

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

Quando a opção **Remover dados privados** está habilitada no Keystone Collector, as seguintes informações de uso são eliminadas do ONTAP. Esta opção é habilitada por padrão.

- Nome do cluster
- Localização do cluster
- Contato do Cluster
- Nome do nó
- Nome agregado
- Nome do volume
- Nome do QoSAdaptivePolicyGroup
- Nome do QoSPolicyGroup
- Nome do Vserver
- Nome do LUN de armazenamento
- Nome do Agregado
- Nome da unidade lógica
- Nome SVM
- IP da instância AIQUM
- FlexClone
- Nome do Cluster Remoto

Coleta de dados StorageGRID

Dados de uso coletados para StorageGRID: Saiba mais

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

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

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

- ID do StorageGRID
- ID do nó
- ID do site
- Nome do site
- Exemplo
- Bytes de utilização de armazenamento do StorageGRID
- Bytes de metadados de utilização de armazenamento 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 habilitada no Keystone Collector, as seguintes informações de uso são eliminadas do StorageGRID. Esta opção é habilitada por padrão.

- Nome da conta
- Nome do balde
- Nome do Site
- Instância/Nome do Nó

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 operacional
  - 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)

A Keystone oferece um modo de implantação *privado*, também conhecido como *dark site*, para atender aos seus requisitos comerciais e de segurança. Este modo está disponível para organizações com restrições de conectividade.

A NetApp oferece uma implantação especializada do Keystone STaaS, adaptada para ambientes com conectividade de internet limitada ou inexistente (também conhecidos como dark sites). Esses são ambientes seguros ou isolados onde a comunicação externa é restrita devido a requisitos de segurança, conformidade ou operacionais.

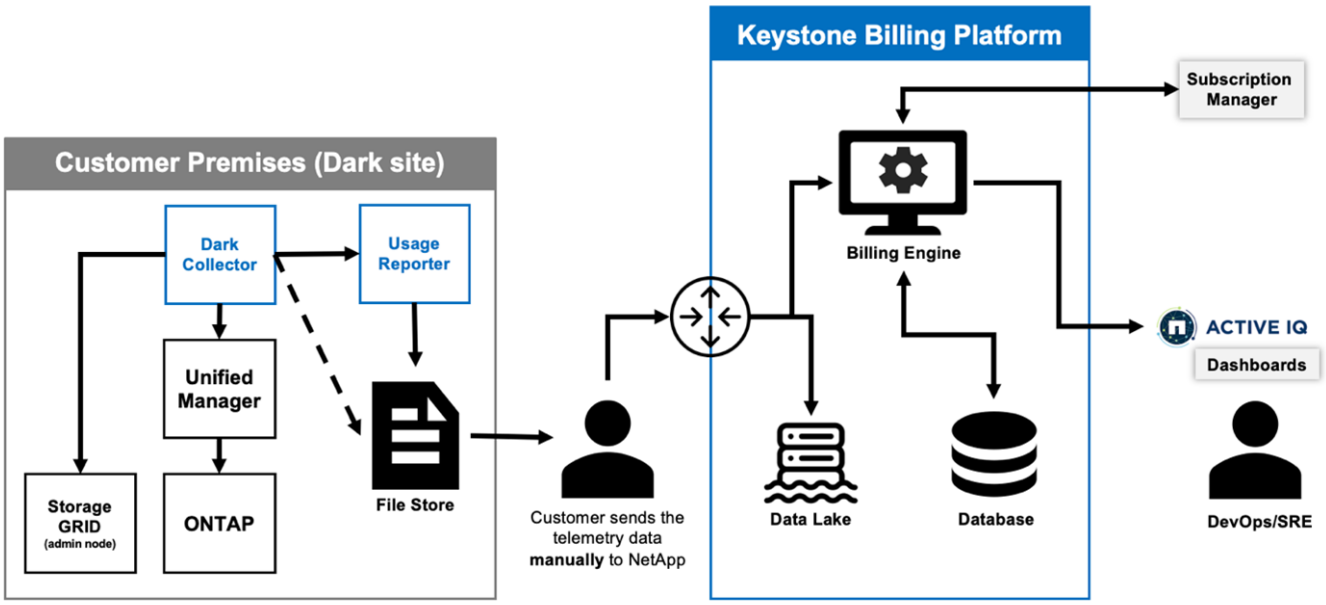
Para a NetApp Keystone, oferecer serviços para sites escuros significa fornecer o serviço de assinatura de armazenamento flexível da Keystone de uma forma que respeite as restrições desses ambientes. Isso envolve:

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

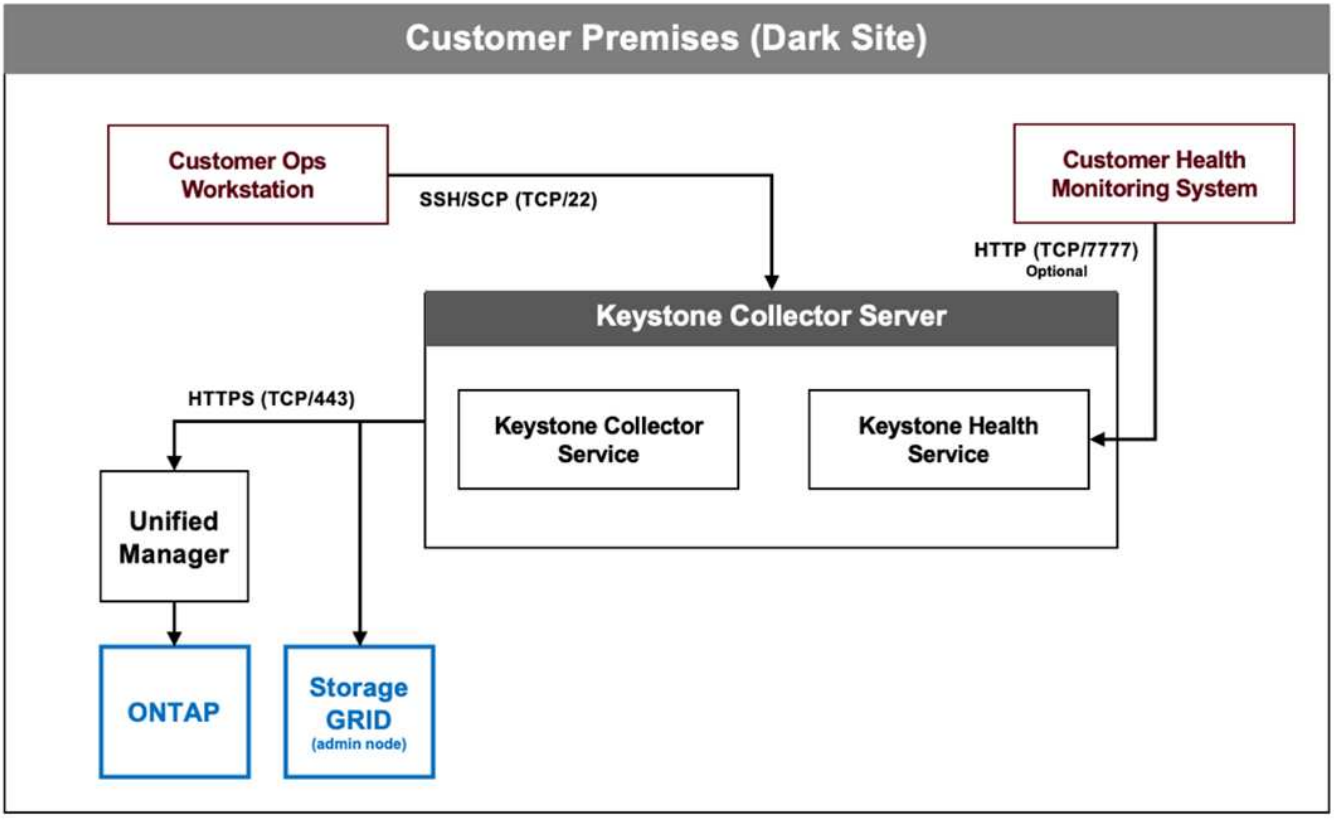
> O Keystone Collector pode ser configurado sem restrições de conectividade, também conhecido como modo *padrão*. Para saber mais, consulte"Saiba mais sobre o Keystone Collector" .

Keystone Collector em modo privado

O Keystone Collector é responsável por coletar periodicamente dados de uso de sistemas de armazenamento e exportar as métricas para um relator de uso offline e um armazenamento de arquivos local. Os arquivos gerados, que são criados em formatos criptografados e de texto simples, são então encaminhados manualmente para a NetApp pelo usuário após as verificações de validação. Após o recebimento, a plataforma de cobrança Keystone da NetApp autentica e processa esses arquivos, integrando-os aos sistemas de cobrança e gerenciamento de assinaturas para calcular as cobranças mensais.



O serviço Keystone Collector no servidor é responsável por 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 interagir com os sistemas de monitoramento de saúde usados pelo cliente. Esses relatórios estão disponíveis para acesso offline pelos usuários, permitindo 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 *site escuro* ou *modo privado*, certifique-se de que seus sistemas estejam preparados com o software necessário e atendam a todos os pré-requisitos exigidos.

Requisitos para 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 livres em `/var/lib/`
  - Pelo menos 48 GB livres em `/opt/netapp`

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

- RHEL 8.6+ (8.x)
  - python3 >=v3.6.8, python3 <=v3.9.13
  - homem-pod
  - SOS
  - yum-utils
  - python3-dnf-plugin-versionlock
- RHEL 9,0+
  - python3 >= v3.9.0, python3 <= v3.9.13
  - homem-pod
  - SOS
  - yum-utils
  - python3-dnf-plugin-versionlock
- Debian v12
  - python3 >= v3.9.0, python3 <= v3.12.0
  - homem-pod

- relatório sos

Requisitos de rede

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

- Active IQ Unified Manager (Unified Manager) 9.10 ou posterior, configurado em um servidor com a funcionalidade API Gateway habilitada.
- O servidor Unified Manager deve ser 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 conectividade 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".

Instalar o Keystone Collector em modo privado

Siga algumas etapas para instalar o Keystone Collector em um ambiente que não tenha acesso à Internet, também conhecido como *site escuro* ou *modo privado*. 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 de seus requisitos. Siga as etapas de instalação que correspondem à opção selecionada.

Implantar no VMware vSphere

Siga estes passos:

1. Baixe o arquivo de modelo OVA em "Portal da Web NetApp Keystone" .
2. Para obter as etapas de implantação do coletor Keystone com arquivo OVA, consulte a seção"Implantando o modelo OVA" .

Instalar no Linux

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

Siga estas etapas 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 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. Digitar `y` quando solicitado a instalar o pacote.

Configurar o Keystone Collector em 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 *site escuro* ou *modo privado*. Esta é uma atividade única para ativar e associar os componentes necessários ao seu ambiente de armazenamento. Uma vez configurado, o Keystone Collector monitorará todos os clusters ONTAP gerenciados pelo Active IQ Unified Manager.

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

Passos

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

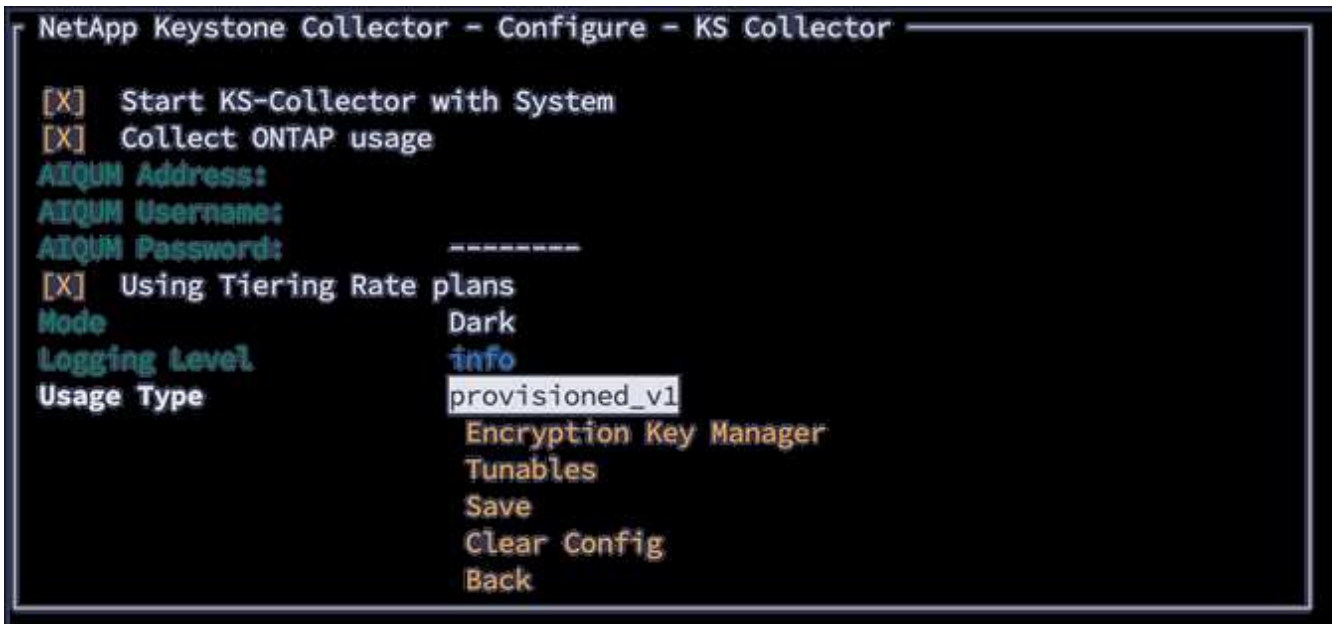
```
keystone-collector-tui
```

2. Vá para **Configurar > Avançado**.
3. Alterne a opção **Modo Darksite**.

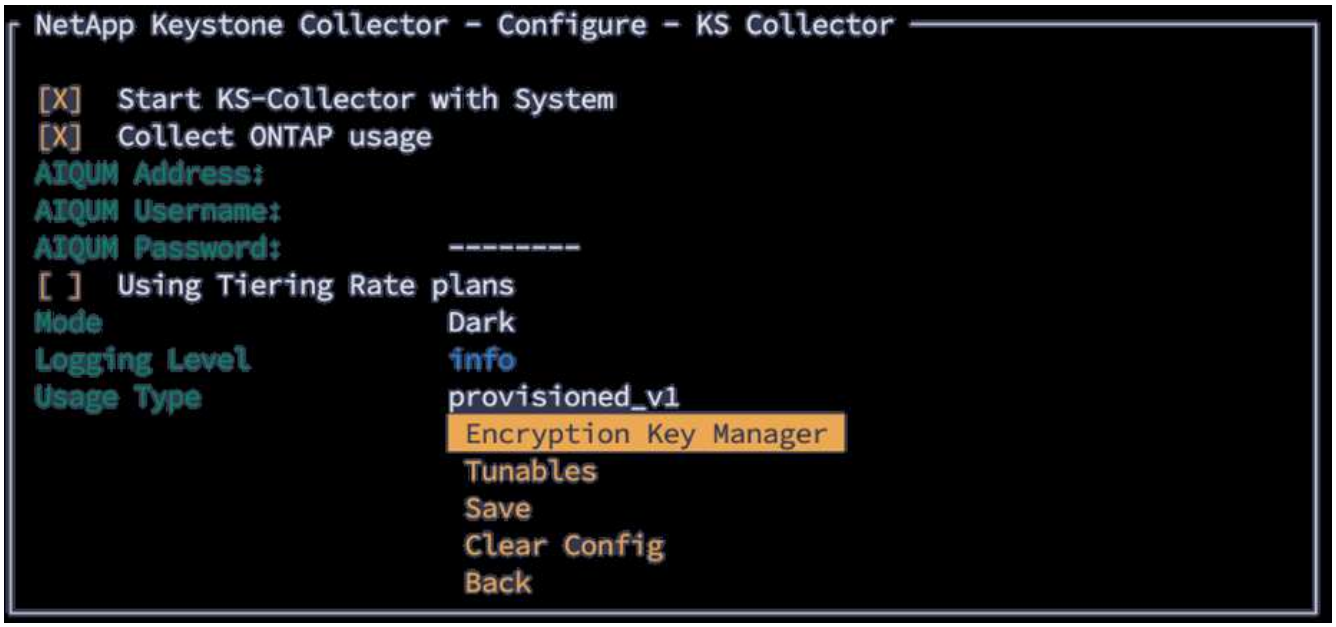
4. Selecione **Salvar**.
5. Vá para **Configurar > KS-Collector** para configurar o Keystone Collector.
6. Alterne o campo **Iniciar KS Collector com Sistema**.
7. Alterne o campo *Coletar uso do ONTAP *. Adicione os detalhes do servidor e da conta de usuário do Active IQ Unified Manager (Unified Manager).

8. **Opcional**: Alterne o campo **Usando planos de tarifas em camadas** se o escalonamento de dados for necessário para a assinatura.
9. Com base no tipo de assinatura adquirida, atualize o **Tipo de uso**.

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

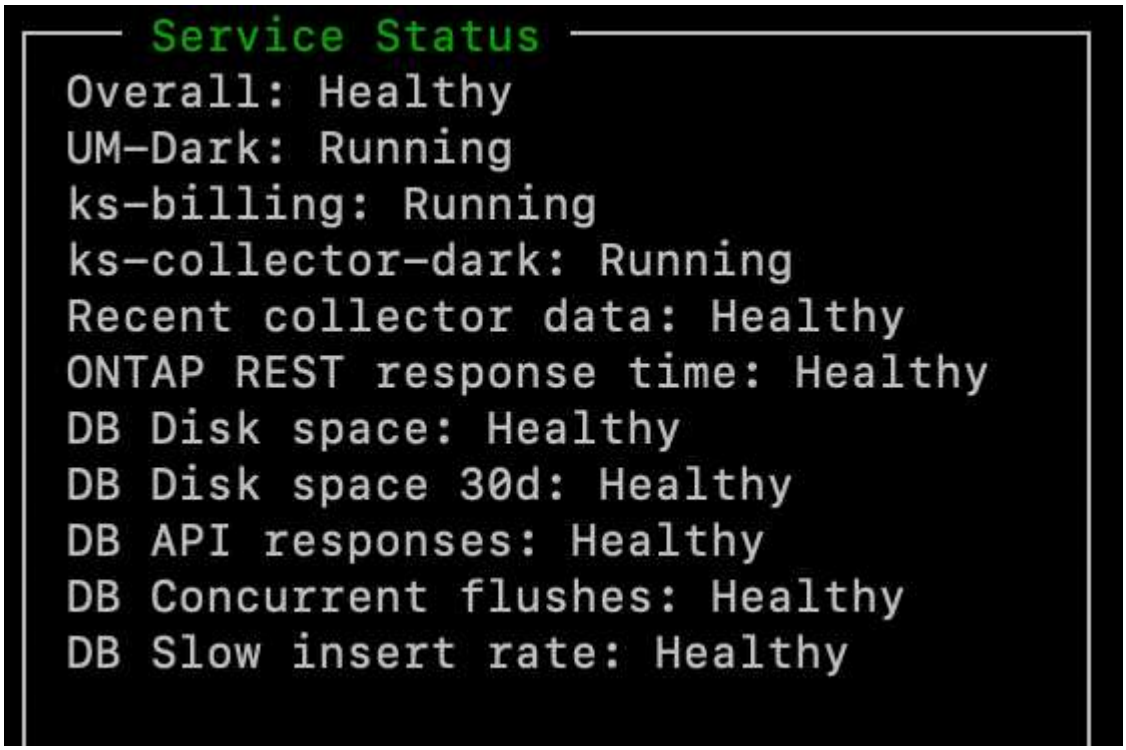


10. Selecione **Salvar**.
11. Vá para **Configurar > KS-Collector** para gerar o par de chaves do Keystone Collector.
12. Vá para **Gerenciador de Chaves de Criptografia** e pressione Enter.



13. Selecione **Gerar par de chaves do coletor** e pressione Enter.

14. Certifique-se de que o Keystone Collector esteja em bom estado retornando à tela principal do TUI e verificando as informações de **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 insatisfatório após esse período, revise as etapas de configuração anteriores e entre em contato com a equipe de suporte da NetApp .



15. Saia da interface gráfica do usuário (TUI) de gerenciamento do Keystone Collector selecionando a opção **Sair para o Shell** na tela inicial.
16. Recupere 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.

Relatório de uso de exportação

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

Siga estas etapas para gerar o relatório de uso:

1. Acesse **Exportar uso** 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 limpo e um arquivo criptografado, que devem ser enviados manualmente para a NetApp. O relatório de arquivo limpo 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-----
```

Atualizar ONTAP

O Keystone Collector suporta atualizações do ONTAP por meio do TUI.

Siga estas etapas para atualizar o ONTAP:

1. Vá para *Manutenção > Atualização do servidor Web 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` usando um navegador da web para obter assistência de atualização.

Reinicie o Keystone Collector

Você pode reiniciar o serviço Keystone Collector por meio do TUI. Acesse **Manutenção > Reiniciar serviços do coletor** na TUI. Isso reinicializará todos os serviços do coletor, e seu status poderá ser monitorado na tela inicial do TUI.

Monitore a saúde do Keystone Collector em modo privado

Você pode monitorar a saúde do Keystone Collector usando qualquer sistema de monitoramento que suporte solicitações HTTP.

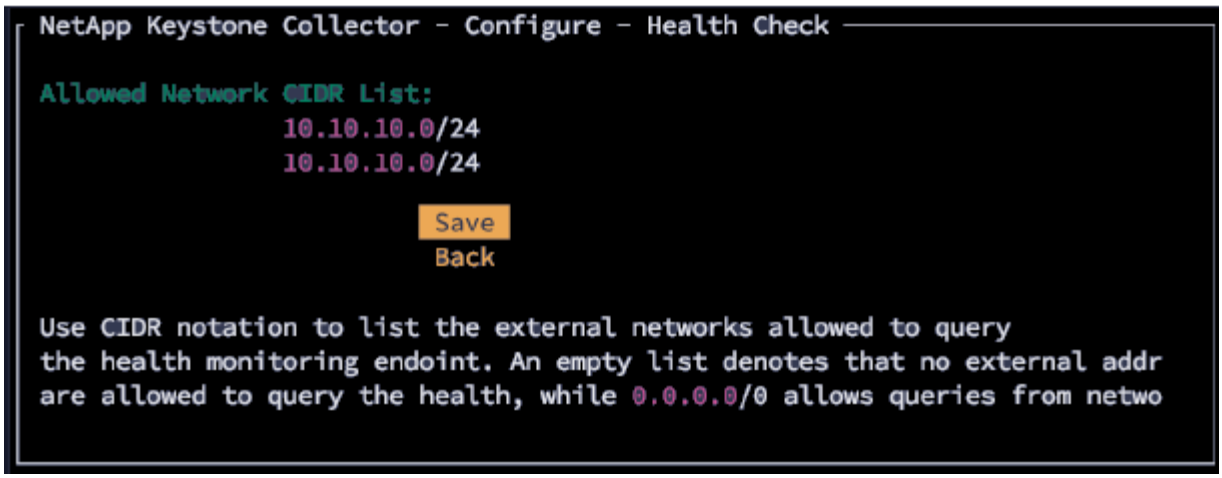
Por padrão, os serviços de saúde do Keystone não aceitam conexões de nenhum IP diferente do host local. O ponto final de saúde da Keystone é `/uber/health` , e escuta em todas as interfaces do servidor Keystone Collector na porta `7777` . Na consulta, um código de status de solicitação HTTP com uma saída JSON é retornado do ponto de extremidade como uma resposta, descrevendo o status do sistema Keystone Collector. O corpo JSON fornece um status geral de saúde 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"}}
```

Esses códigos de status são retornados:

- **200**: indica que todos os componentes monitorados estão saudáveis
- **503**: indica que um ou mais componentes não estão saudáveis
- **403**: indica que o cliente HTTP que consulta o status de integridade não está na lista *allow*, que é uma lista de CIDRs 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 saúde Keystone . Se você receber o erro 403, adicione seu sistema de monitoramento à lista de permissões em * TUI de gerenciamento do Keystone Collector > Configurar > Monitoramento de integridade*.

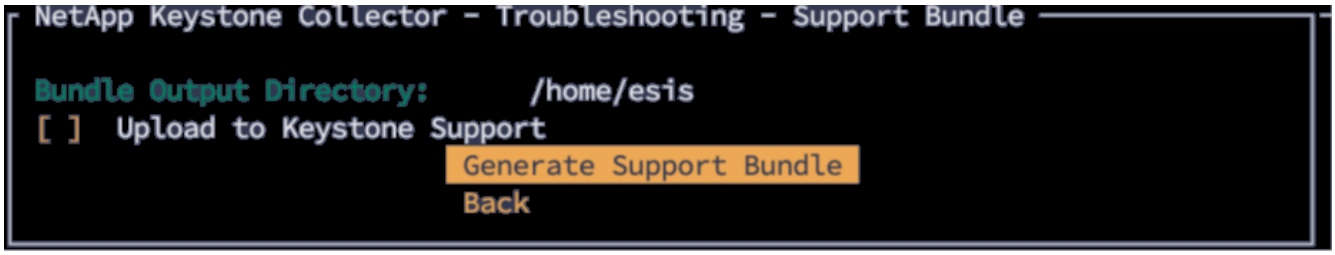


Gerar e coletar pacotes de suporte

Para solucionar problemas com o Keystone Collector, você pode trabalhar com o Suporte da NetApp , que pode solicitar 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. Acesse **Solução de problemas > Gerar pacote de suporte**.
2. Selecione o local para salvar o pacote e clique em **Gerar pacote de suporte**.



   Este processo cria uma `tar` pacote no local mencionado que pode ser compartilhado com a NetApp para solução de 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