



# Configurar o Keystone

## Keystone

NetApp  
December 13, 2024

# Índice

- Configurar o Keystone ..... 1
  - Requisitos ..... 1
  - Instale o Keystone Collector ..... 7
  - Configure o Keystone Collector ..... 11
  - Instale o ITOM Collector ..... 18
  - Configurar o AutoSupport para Keystone ..... 22
  - Segurança do Keystone Collector ..... 23
  - Tipos de dados de usuário coletados pelo Keystone ..... 24

# Configurar o Keystone

## Requisitos

### Requisitos de infraestrutura virtual

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 vCentre e ESXi 6,7 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 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	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 80, 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
<a href="https://keystone.netapp.com">https://keystone.netapp.com</a>	Atualizações do software Keystone Collector e relatórios de uso
<a href="https://support.netapp.com">https://support.netapp.com</a>	Sede da NetApp para informações de faturamento e entrega do AutoSupport

### Requisitos do sistema Linux

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: CentOS 7, Red Hat Enterprise Linux (RHEL) 8,6 ou versões posteriores da série RHEL 8.x.
- 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 (3.6.8 a 3,9.13)

#### 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 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	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 80, 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
<a href="https://keystone.netapp.com">https://keystone.netapp.com</a>	Atualizações do software Keystone Collector e relatórios de uso
<a href="https://support.netapp.com">https://support.netapp.com</a>	Sede da NetApp para informações de faturamento e entrega do AutoSupport

## Requisitos para ONTAP e StorageGRID

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

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. Em *Etapa 4: Revise os detalhes*, verifique a correção e autenticidade do arquivo OVA. As versões do vCentre anteriores a 7.0u2 não conseguem verificar automaticamente a autenticidade do certificado de assinatura de código. VCentre 7.0u2 e posteriores podem realizar as verificações. No entanto, para isso, a autoridade do certificado de assinatura deve ser adicionada ao vCentre. Siga estas instruções para a sua versão do vCentre:

#### **VCentre 7.0u1 e anteriores: Saiba mais**

O vCentre valida a integridade do conteúdo do arquivo OVA e é fornecido um resumo válido de assinatura de código para os arquivos contidos no ARQUIVO OVA. No entanto, ele não valida a autenticidade do certificado de assinatura de código. Para verificar a integridade, você deve baixar o certificado de resumo de assinatura completo e verificá-lo em relação ao certificado público publicado pelo Keystone.

- a. Clique no link **Publisher** para baixar o certificado de resumo completo da assinatura.
- b. Faça o download do certificado público *Keystone Billing* do "[este link](#)".
- c. Verifique a autenticidade do certificado de assinatura OVA em relação ao certificado público usando OpenSSL:  

```
openssl verify -CAfile OVA-SSL-NetApp-Keystone-20221101.pem keystone-collector.cert
```

#### **VCentre 7.0u2 e posterior: Saiba mais**

7.0u2 e versões posteriores do vCenter são capazes de validar a integridade do conteúdo do arquivo OVA e a autenticidade do certificado de assinatura de código, quando um resumo válido de assinatura de código é fornecido. O armazenamento de confiança raiz do vCenter contém apenas certificados VMware. O NetApp usa o Entrust como autoridade de certificação e esses certificados precisam ser adicionados ao armazenamento de confiança do vCenter.

- a. Faça o download do certificado de CA de assinatura de código do Entrust "[aqui](#)".
- b. Siga as etapas na *Resolution* seção deste artigo da base de conhecimento (KB) <https://kb.vmware.com/s/article/84240>: .

Quando a integridade e autenticidade do Keystone Collector OVA são validadas, você pode ver o texto (Trusted certificate) com o editor.

## Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Select networks
- 7 Customize template
- 8 Ready to complete

**Review details**  
Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	NetApp Keystone Collector
Version	20220405
Vendor	NetApp
Download size	8.3 GB
Size on disk	12.1 GB (thin provisioned)
	200.0 GB (thick provisioned)

CANCEL
BACK
NEXT

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 conectar, 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 acessar 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

O software Keystone Collector é distribuído por um repositório de software YUM on-line. Você precisa importar e instalar o arquivo em um servidor Linux.

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

1. SSH para o servidor Keystone Collector e elevar-se a `root` privilégios.
2. Importar a assinatura de assinatura pública do Keystone:  

```
# rpm --import https://keystone.netapp.com/repo/RPM-GPG-NetApp-Keystone-20221101
```
3. Verifique se o certificado público correto foi importado verificando a impressão digital do Keystone Billing Platform no banco de dados RPM:  

```
# rpm -qa gpg-pubkey --qf '%<Description>' | gpg --show-keys --fingerprint A
```

impressão digital correta é semelhante a esta:  
90B3 83AF E07B 658A 6058 5B4E 76C2 45E4 33B6 C17D
4. Transfira o `keystonerepo.rpm` ficheiro:  

```
curl -O https://keystone.netapp.com/repo/keystonerepo.rpm
```
5. Verifique a autenticidade do arquivo:  

```
rpm --checksig -v keystonerepo.rpm
```

Uma assinatura para um arquivo autêntico é assim:  
Header V4 RSA/SHA512 Signature, key ID 33b6c17d: OK
6. Instale o arquivo do repositório de software DO YUM:  

```
# yum install keystonerepo.rpm
```
7. Quando o repositório do Keystone estiver instalado, instale o pacote `keystone-Collector` através do gerenciador de pacotes DO YUM:  

```
# yum 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.

#### **<strong> para ONTAP </strong>**

- **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 .

## <strong> para StorageGRID </strong>

- **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.
- **Remove 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**.

```
NetApp Keystone Collector - Configure - KS Collector
[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address: 123.123.123.123
AIQUM Username: collector-user
AIQUM Password: -----
[X] Collect StorageGRID usage
StorageGRID Address: sgadminnode.address
StorageGRID Username: collector-user
StorageGRID Password: -----
[X] Collect ONTAP Performance Data
AIQUM Database Username: sla-reporter
AIQUM Database Password: -----
[X] Remove Private Data
Mode Standard
Logging Level info
                Tunables
                Save
                Clear Config
                Back
```

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

```
Service Status
Overall: Healthy
UM: Running
chronyd: Running
ks-collector: Running
```

estado **geral: Saudável.**

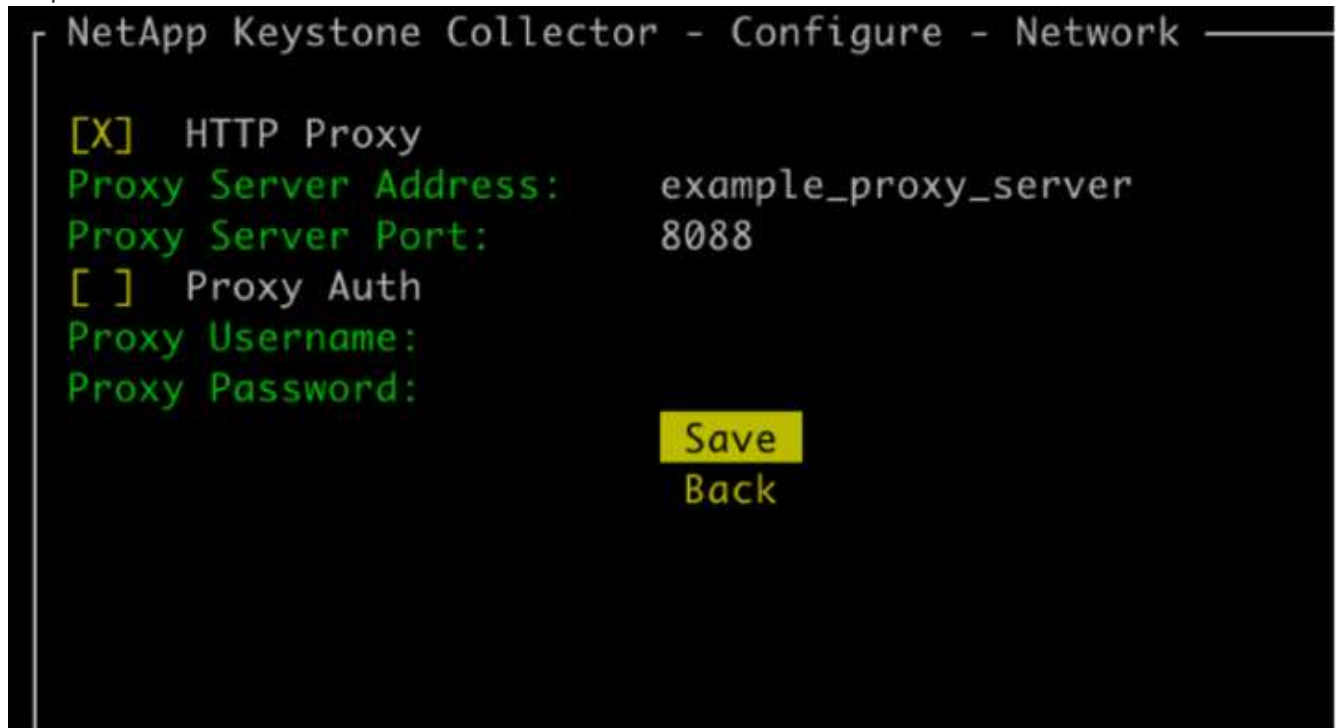
7. Saia da TUI de gerenciamento do Keystone Collector selecionando a opção **Exit to Shell** na tela inicial.

## 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.

```
NetApp Keystone Collector - Configure - KS Collector

[X] Start KS-Collector with System
[X] Collect ONTAP usage
AIQUM Address:          123.123.123.123
AIQUM Username:         collector
AIQUM Password:         -----
[ ] Collect StorageGRID usage

[ ] Collect ONTAP Performance Data

[X] Remove Private Data
Mode                    Standard
Logging Level           info
                        Tunables
                        Save
                        Clear Config
                        Back
```

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 seleccionar 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.

```

NetApp Keystone Collector - Configure - Advanced
[ ] Darksite Mode
[X] TLS Verify on Connections to Internet
[X] Enable custom root certificate
Select custom root certificate path:
    - Unset -
[X] Finished Initial OVA Install
[X] Collector Auto-Update
Override Collector Images
Save
Back

```

## Criar níveis de serviço de performance

Você pode criar níveis de Serviço de Performance (PSLs) usando o utilitário TUI de gerenciamento do Keystone Collector. Criar PSLs através da TUI seleciona automaticamente os valores padrão definidos para cada nível de serviço, reduzindo a chance de erros que possam ocorrer ao definir manualmente esses valores ao criar PSLs por meio do Active IQ Unified Manager.

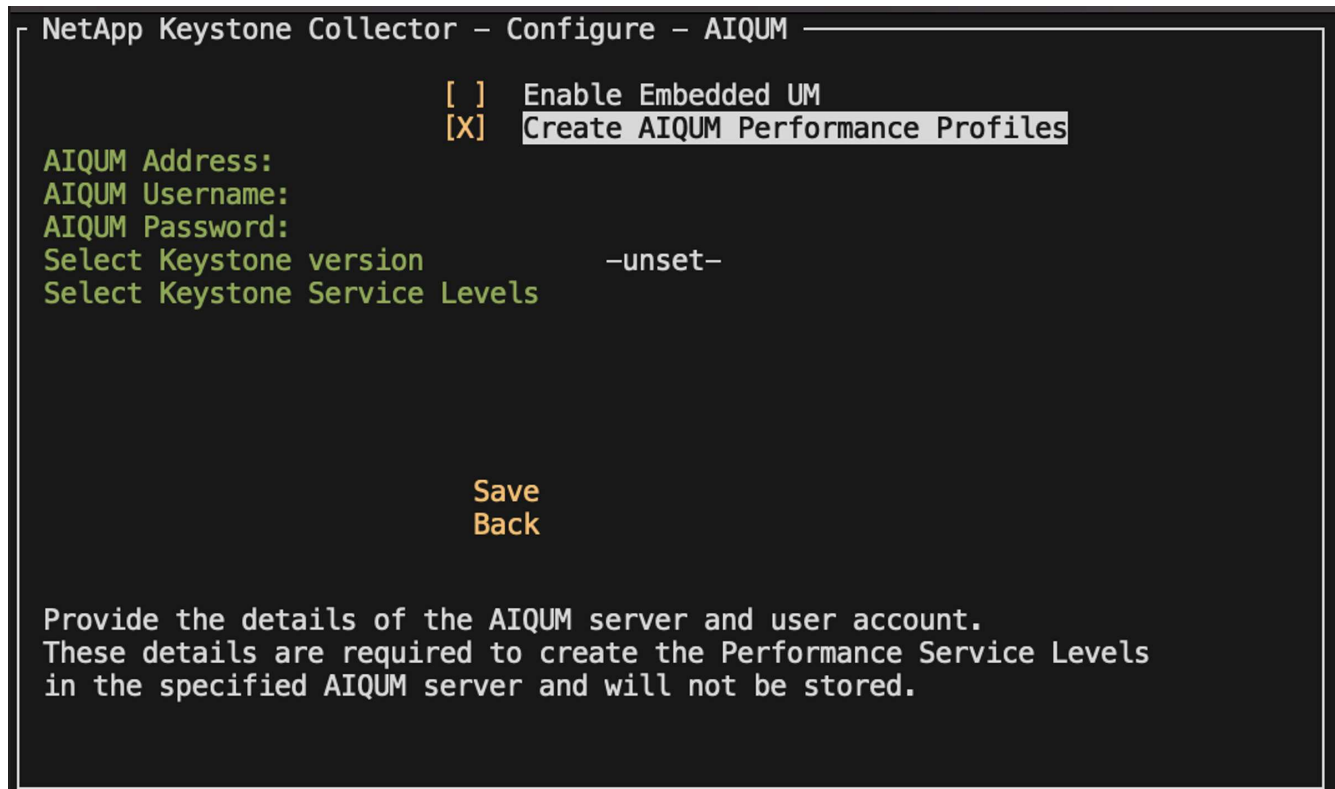
Para saber mais sobre PSLs, ["Níveis de serviço de performance"](#) consulte .

Para saber mais sobre os níveis de serviço, ["Níveis de serviço no Keystone"](#) consulte .

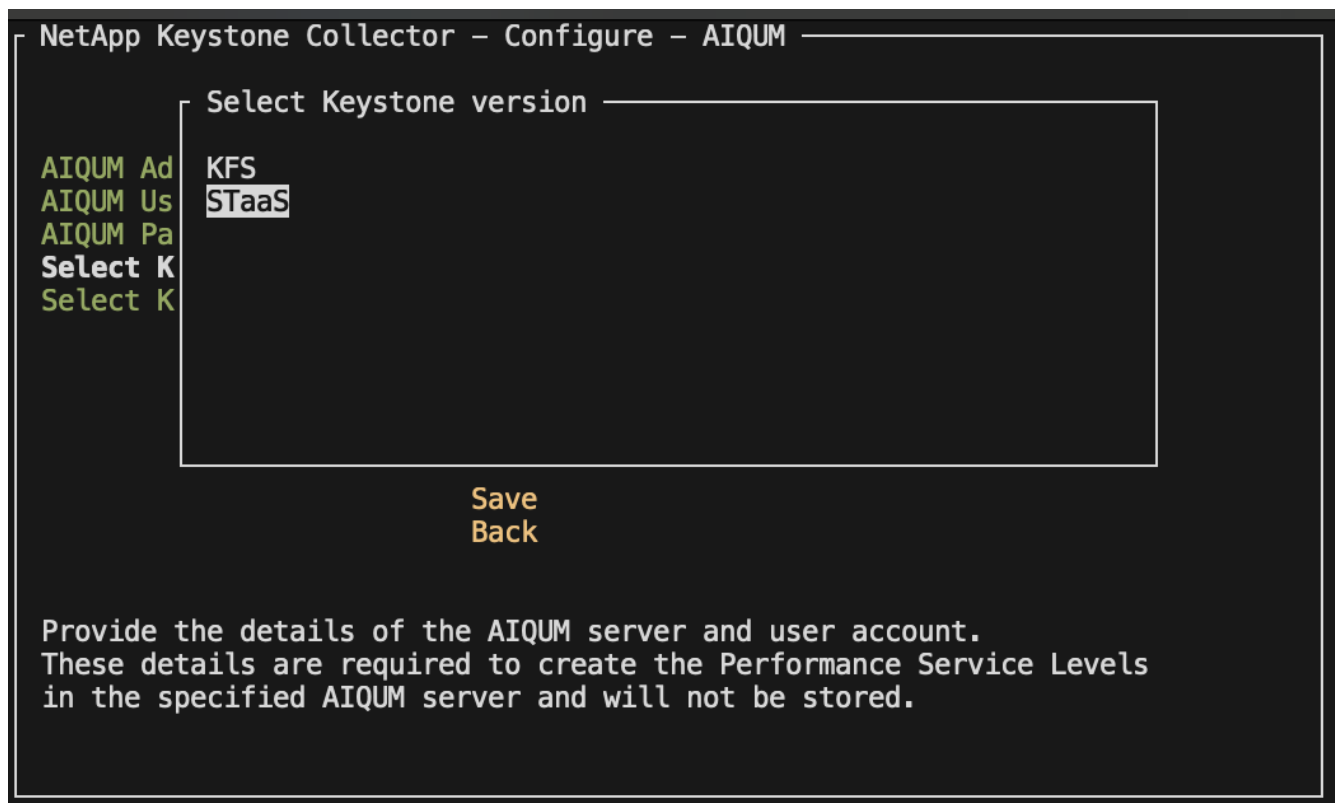
### Passos

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 Keystone versão 1. Os serviços de subscrição do Keystone diferem do Keystone STaaS nos níveis de serviço, ofertas de serviço e princípios de cobrança. Para saber mais, "[Serviços de assinatura do Keystone | versão 1](#)" consulte .

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

```
NetApp Keystone Collector - Configure - AIQUM
[ ] Enable Embedded UM
[X] Create AIQUM Performance Profiles
AIQUM Address:
AIQUM Username:
AIQUM Password:
Select Keystone version          STaaS
Select Keystone Service Levels  [X] Extreme
                                [X] Premium
                                [ ] Performance
                                [ ] Standard
                                [ ] Value
                                Save
                                Back
Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```




Você pode selecionar vários níveis de serviço 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 .

## Performance Service Levels


View and manage the Performance Service Levels that you can assign to workloads.

Search Performance Service Levels  Filter

 Add  Modify  Remove 

<input type="checkbox"/>	Name ^	Type	Expected IOPS/TB	Peak IOPS/TB	Absolute Minim...	Expected Latency	Capacity	Workloads
	Extreme - KFS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
	Extreme - KS-STaaS	User-defined	6144	12288	1000	1	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
Overview								
		Description	Extreme - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					
	Premium ...S-STaaS	User-defined	2048	4096	500	2	<div style="width: 100%;"><div style="width: 0%;"></div></div> Used: 0 bytes Available: 283.85 TiB	0
Overview								
		Description	Premium - KS-STaaS					
		Added Date	1 Aug 2024, 18:08					
		Last Modified Date	1 Aug 2024, 18:08					

Se um PSL para o nível de serviço selecionado já existir no servidor de Gestor Unificado Active IQ especificado, não será possível criá-lo novamente. Se tentar fazê-lo, receberá uma mensagem de erro.



```
NetApp Keystone Collector - Configure - AIQUM

Warning
-----
AIQUM Ad Failed to create Performance Service Level for:
AIQUM Us Extreme. Error: <Response [400]>
AIQUM Pa
Select K
Select K

OK

> Save <
  Back

Provide the details of the AIQUM server and user account.
These details are required to create the Performance Service Levels
in the specified AIQUM server and will not be stored.
```

## Instale o ITOM Collector

## Requisitos de instalação para ITOM Collector

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:

- Sistema operativo suportado: Debian 12, Windows Server 2016, Ubuntu 20,04 LTS, Red Hat Enterprise Linux (RHEL) 8.x, Amazon Linux 2023 ou versões mais recentes destes sistemas operativos.



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 interruptores
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 ITOM Collector em sistemas Linux

Conclua algumas etapas para instalar o ITOM Collector, que coletará 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](mailto:keystone.services@NetApp.com).

## Instale o 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 conecte-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](mailto: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.
  - Execute este comando para modificar o conteúdo diário do log:

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



# 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. Ele também pode coletar dados de desempenho somente para ONTAP, se a opção estiver habilitada no Keystone Collector.

### **Coleta de dados do ONTAP**

**<strong> dados de uso coletados para ONTAP: Saiba mais</strong>**

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
- Agregar almacenamientos de objetos
  - ObjectStoreName
  - ObjectStoreUID
  - Tipo de proveedor
  - 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
- Clusters de MetroCluster
  - ClusterUUID
  - Nome de utilizador
  - RemoteClusterUID
  - RemoteClusterName
  - Estado Configuração local
  - Estado de configuração remota
  - Modo
- Métricas de Observability 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

**<strong> dados de desempenho coletados para o ONTAP: Saiba mais</strong>**

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
- Capacidade de IOPS

**<strong> Lista de itens removidos ao limitar o acesso a dados privados: Saiba mais</strong>**

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



**<strong> dados de uso coletados para StorageGRID: Saiba mais</strong>**

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

**<strong> Lista de itens removidos ao limitar o acesso a dados privados: Saiba mais</strong>**

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

## Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

## Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.