



# **Instale o Keystone Collector**

## **Keystone**

NetApp  
February 19, 2026

This PDF was generated from <https://docs.netapp.com/pt-br/keystone-staas/installation/vapp-installation.html> on February 19, 2026. Always check docs.netapp.com for the latest.

# Índice

- Instale o Keystone Collector ..... 1
  - Implante o Keystone Collector em sistemas VMware vSphere ..... 1
    - Implantando o modelo OVA ..... 1
    - Configuração inicial do sistema ..... 2
  - Instale o Keystone Collector em sistemas Linux ..... 3
  - Validação automática do software Keystone ..... 5

# Instale o Keystone Collector

## Implante o Keystone Collector em sistemas VMware vSphere

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

### Implantando o modelo OVA

Siga estes passos:

#### Passos

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

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

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



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

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

## Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details**
- Select storage
- Select networks
- Customize template
- Ready to complete

## Review details

Verify the template details.

Publisher	<a href="#">Sectigo Public Code Signing CA R36</a> (Trusted certificate)
Product	<a href="#">Keystone-Collector</a>
Version	3.12.31910
Vendor	<a href="#">NetApp</a>
Download size	1.7 GB
Size on disk	3.9 GB (thin provisioned) 19.5 GB (thick provisioned)

CANCEL
BACK
NEXT

- Em *Etapa 5* do assistente **Deploy OVF Template**, especifique o local para armazenar a VM.
- Em *Etapa 6*, selecione a rede de destino para a VM usar.
- 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.

- 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 aceder à TUI. Ao iniciar sessão, a TUI é apresentada.

Como alternativa, você pode iniciá-lo manualmente executando o `keystone-collector-tui` comando CLI.

3. Se necessário, configure os detalhes do proxy na seção **Configuração > rede** na TUI.
4. Configure o nome do host do sistema, a localização e o servidor NTP na seção **Configuração > sistema**.
5. Atualize os coletores Keystone usando a opção **Manutenção > Atualizar coletores**. Após a atualização, reinicie o utilitário TUI de gerenciamento do Keystone Collector para aplicar as alterações.

## Instale o Keystone Collector em sistemas Linux

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

## Usando RPM

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

```
# rpm --import https://keystone.netapp.com/repo1/RPM-GPG-NetApp-Keystone-20251020
```
3. Certifique-se de que o certificado público correto foi importado, verificando a impressão digital da plataforma Keystone Billing no banco de dados RPM:  

```
# rpm -qa gpg-pubkey --qf '%{Description}' | gpg --show-keys --fingerprint
```

A impressão digital correta tem esta aparência:  
9297 0DB6 0867 22E7 7646 E400 4493 5CBB C9E9 FEDC
4. Baixe o `keystonerepo.rpm` arquivo:  

```
curl -O https://keystone.netapp.com/repo1/keystonerepo.rpm
```
5. Verifique a autenticidade do arquivo:  

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

A assinatura de um arquivo autêntico tem a seguinte aparência:  
Header V4 RSA/SHA512 Signature, key ID c9e9fedc: OK
6. Instale o arquivo do repositório de software DO YUM:  

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

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

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

```
# yum install keystone-collector-rhel9
```

## Usando Debian

1. SSH para o servidor Keystone Collector e elevar-se a `root` privilégios.  

```
sudo su
```
2. Transfira o `keystone-sw-repo.deb` ficheiro:  

```
curl -O https://keystone.netapp.com/downloads/keystone-sw-repo.deb
```
3. Instale o arquivo de repositório de software do Keystone:  

```
# dpkg -i keystone-sw-repo.deb
```
4. Atualize a lista de pacotes:  

```
# apt-get update
```
5. Quando o Keystone repo estiver instalado, instale o pacote `keystone-Collector`:  

```
# apt-get install keystone-collector
```



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

## Validação automática do software Keystone

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

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

## **Informações sobre direitos autorais**

Copyright © 2026 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 DOCUMENTOS, 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.