

# Gere pacote de diagnósticos para dispositivos de análise de rede seguros

## Contents

[Introduction](#)

[Procedimento](#)

[Método 1. Na interface do usuário da Web do gerente](#)

[Método 2. Da IU do administrador de cada dispositivo](#)

[Método 3. Da CLI \(Command Line Interface, interface de linha de comando\) de cada dispositivo](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve os diferentes procedimentos disponíveis para coletar um pacote de diagnóstico para dispositivos Secure Network Analytics (SNA).

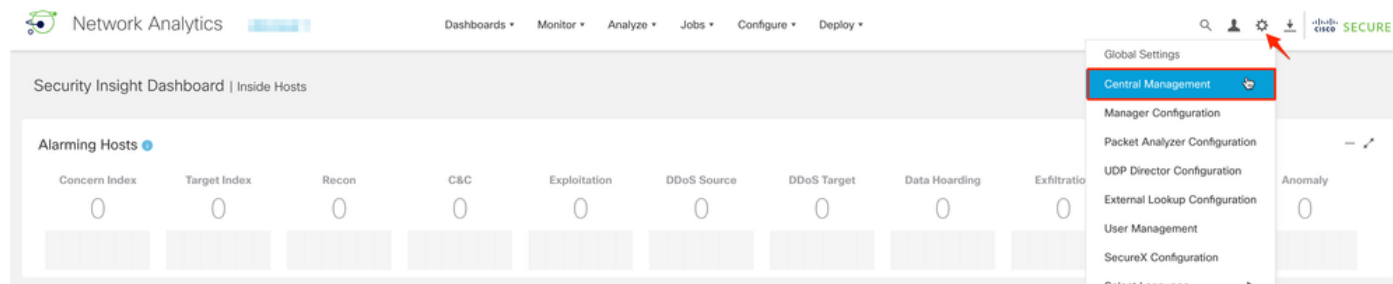
## Procedimento

Há três métodos principais para gerar o Diagnostics Pack para os dispositivos SNA. O método sugerido é o **método 1. Na interface do usuário da Web do gerente (UI)**, entretanto, os outros dois métodos são uma opção caso a interface do usuário da Web do gerente não esteja disponível.

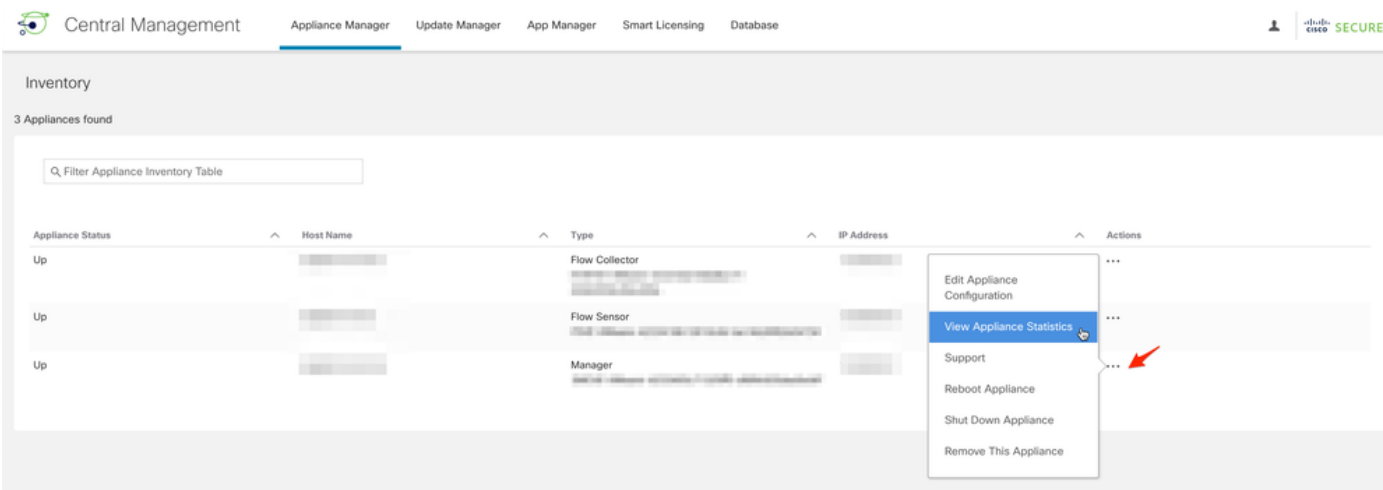
**Note:** Se a interface de usuário da Web do gerente não estiver disponível e você precisar gerar um pacote de diagnósticos a partir do gerente, consulte o **Método 3. Da CLI (Command Line Interface, interface de linha de comando) de cada dispositivo**.

### Método 1. Na interface do usuário da Web do gerente

1. Efetue login na IU da Web do gerente.
2. Navegue até **Configurações globais > Gerenciamento central**.



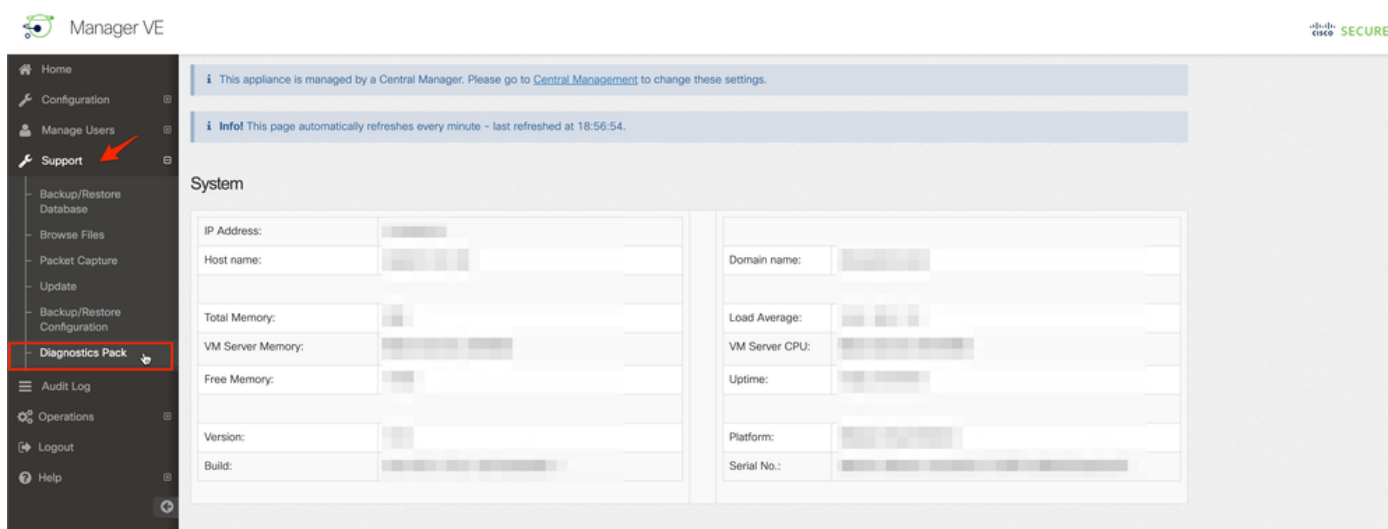
3. Nos dispositivos listados, localize o aplicativo do qual você precisa criar o Pacote de diagnóstico e selecione **Ações (ícone de elipse) > Exibir estatísticas do dispositivo**.



4. Você deve ser redirecionado para a IU do administrador do aplicativo selecionado.

5. Faça login na IU do administrador do aplicativo com credenciais **admin**.

6. No menu à esquerda, navegue até **Support > Diagnostics Pack (Suporte > Pacote de diagnóstico)**.



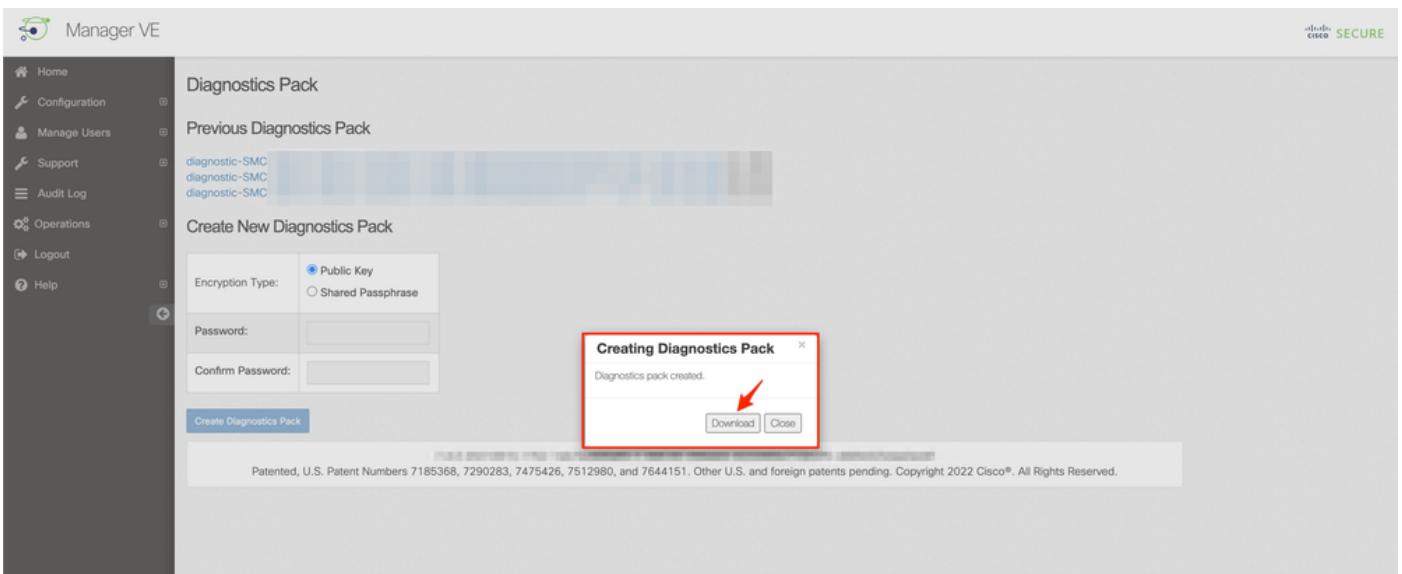
7. Na página Diagnostics Pack (Pacote de diagnósticos), você precisa selecionar a criptografia padrão **de chave pública** ou fornecer uma chave/senha compartilhada a ser usada para criptografia.

**Note:** Se optar por usar uma chave/senha personalizada, você deverá fornecer essa senha na descrição do arquivo ao carregar o pacote de diagnósticos no Support Case Manager.

8. Selecione **Create Diagnostics Pack** para gerar o pacote de diagnósticos do dispositivo.



9. Depois de concluído, você deve receber uma caixa pop-up que inclui o botão **Download** para baixar o Diagnostics Pack.



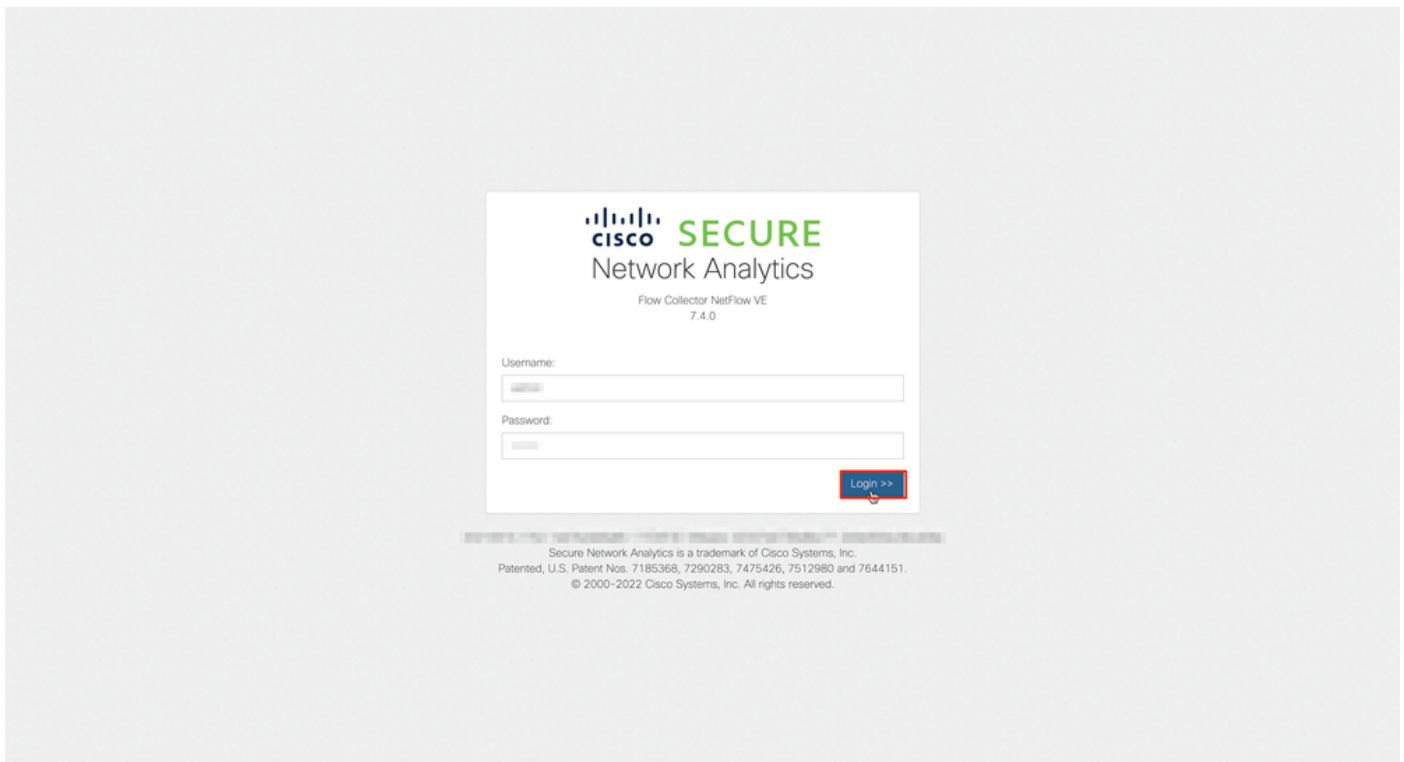
## Método 2. Da IU do administrador de cada dispositivo

Para esse método, você deve acessar o equipamento do qual deseja gerar o Pacote de Diagnóstico, por meio do protocolo HTTPS (Hypertext Transfer Protocol Secure).

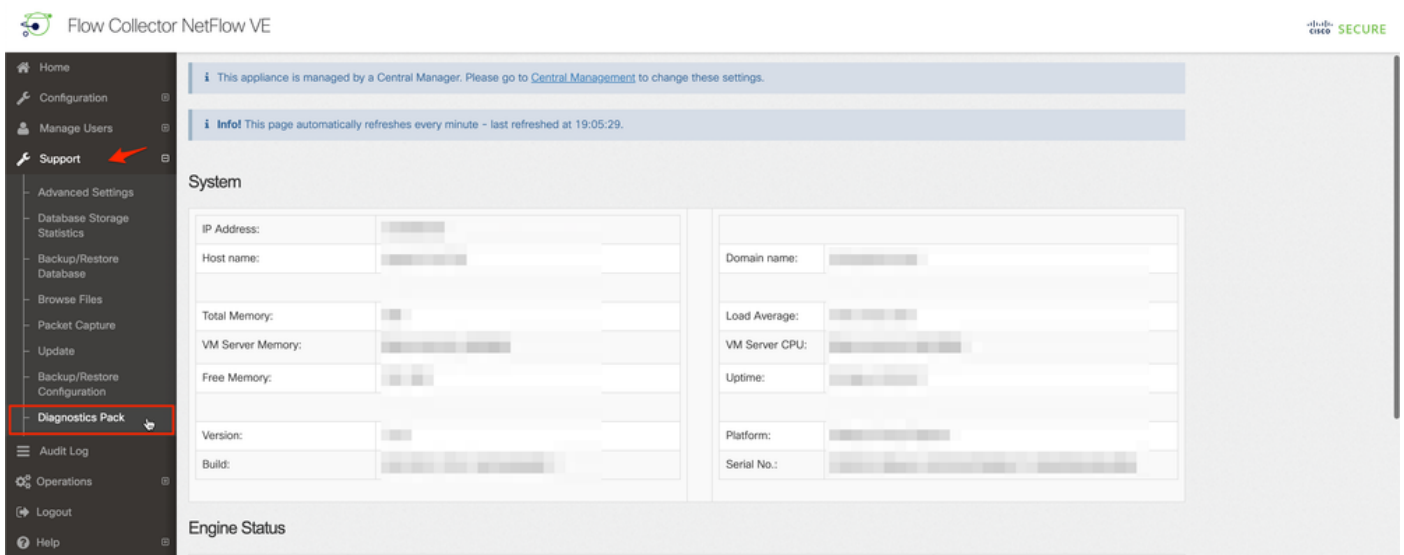
**Note:** Para acessar diretamente a IU do **administrador** do gerente, você deve usar o URL: [https://<Manager\\_IP\\_address>/smc/index.html](https://<Manager_IP_address>/smc/index.html), caso contrário, você será redirecionado para a interface do usuário da Web do Gerente.

Por exemplo, para gerar o Pacote de diagnóstico de um coletor de fluxo com esse método, você deve seguir as próximas etapas:

1. Em um navegador da Web, navegue até [https://<FC\\_IP\\_address>](https://<FC_IP_address>)
2. Faça login na IU do administrador do aplicativo com credenciais de administrador.



3. No menu à esquerda, navegue até **Suporte > Pacote de diagnóstico**.



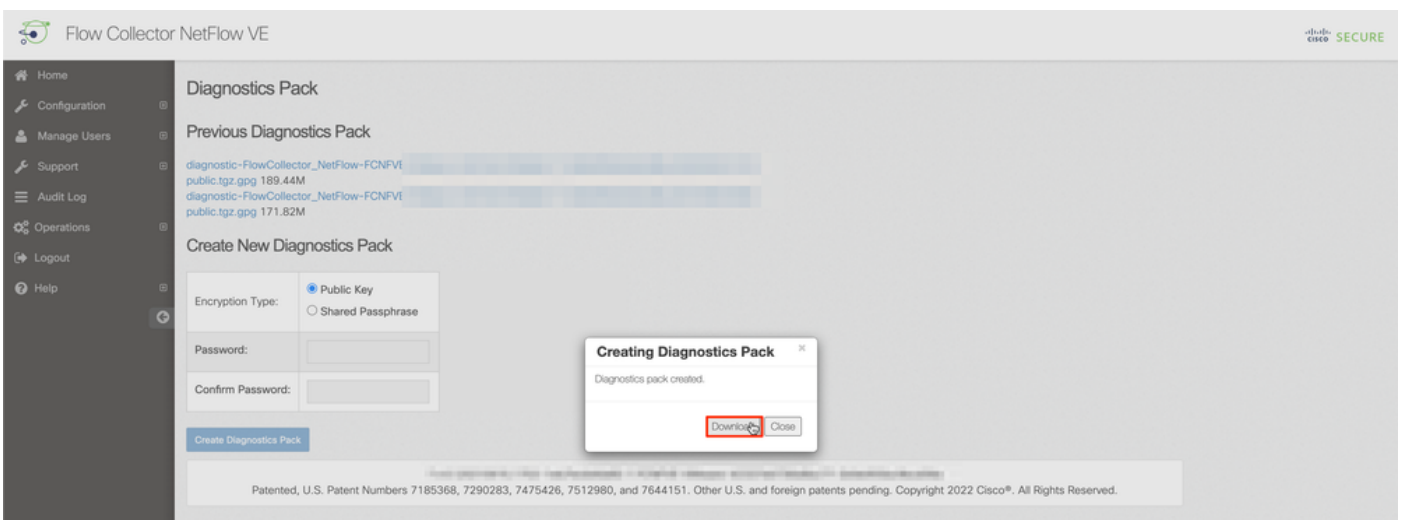
4. Na página Diagnostics Pack (Pacote de diagnósticos), você precisa selecionar a criptografia padrão **de chave pública** ou fornecer uma chave/senha compartilhada a ser usada para criptografia.

**Note:** Se optar por usar uma chave/senha personalizada, você deverá fornecer essa senha na descrição do arquivo ao carregar o pacote de diagnósticos no Support Case Manager.

5. Selecione **Create Diagnostics Pack** para gerar o pacote de diagnósticos do dispositivo.



6. Depois de concluído, você deve receber uma caixa pop-up que inclui o botão **Download** para baixar o Diagnostics Pack.



### Método 3. Da CLI (Command Line Interface, interface de linha de comando) de cada dispositivo

Algumas vezes, não é possível gerar o Pacote de diagnóstico de um dispositivo com o uso dos métodos descritos anteriormente, mas ele pode ser gerado diretamente da CLI do dispositivo. As etapas para concluir esta tarefa são:

1. Conecte-se ao dispositivo SNA desejado por meio do Secure Shell Protocol (SSH) ou diretamente por meio do acesso ao console.

**Note:** Caso você precise coletar o pacote de diagnósticos de um dispositivo de hardware sem acesso SSH, o console da Máquina virtual baseada em kernel (KVM) da interface do Cisco Integrated Management Controller (CIMC) também pode ser usado.

2. Faça login com credenciais **raiz**.
3. Insira um dos próximos comandos (isso depende da versão do SNA que está em uso):  
**SNA versão 7.1.x a 7.3.x**

Digite o comando **doDiagPack**

## SNA versão 7.4.x

Insira o comando **diagnostics start**

4. Aguarde a conclusão da tarefa.
5. Uma vez concluída a tarefa, o arquivo do pacote de diagnósticos é armazenado no `/lancope/var/admin/diagnostics/` diretório com um esquema de nomes de "diagnostic-`<Device_type>-<Device_ID>.<YYMMDD>.<HHMM>-*.tgz.gpg`"

```
smc:/# doDiagPack
smc:/# ls -l /lancope/var/admin/diagnostics/
total 32740
-rw-r--r-- 1 root root 33522766 Feb 24 02:29 diagnostic-SMC-SMCVE-VMware-4
        -6          .20220224.0227-public.tgz.gpg
smc:/# █
```

6. Copie o arquivo gerado do dispositivo para o computador local ou para um servidor de arquivos com o protocolo de cópia segura (SCP) ou com um cliente SSH File Transfer Protocol (SFTP) como o WinSCP. O pacote de diagnósticos está localizado no diretório `/lancope/var/admin/diagnostics/`.

**Observação:** vale a pena mencionar que a versão 7.4.0 do SNA introduziu um novo recurso que permite que o Pacote de Diagnóstico seja gerado a partir do menu SystemConfig (CLI login com credenciais **raiz** > Enter **SystemConfig** > Navegue até **Recovery** > **Diagnostics Pack**).

Para obter mais informações sobre esse método, consulte o [Guia de Configuração do Sistema Secure Network Analytics 7.4.x](#).

## Troubleshoot

Esta seção disponibiliza informações para a solução de problemas de configuração.

Algumas vezes, a criação do Diagnostics Pack falha. O sintoma mais comum é quando você recebe um erro que diz "Erro ao criar o pacote de diagnósticos. Nenhum arquivo disponível" depois que o botão **Create Diagnostics Pack (Criar pacote de diagnósticos)** for clicado.



Para corrigir esse comportamento, faça o seguinte:

1. Faça login no aplicativo que tem esse comportamento com credenciais **raiz** via SSH.
2. Execute o comando `ls -l /lancope/var/database/dbs/hsqldb/admin/` para verificar o conteúdo do diretório.
3. Certifique-se de que o subdiretório **de backup** existe e de que o proprietário do seu usuário/grupo é **tomcat**.

```
fcnf-cds:~# ls -l /lancope/var/database/dbs/hsqldb/admin/
total 20
-rw-r--r-- 1 tomcat tomcat  16 Apr 28 00:38 admin.lck
-rw-r--r-- 1 tomcat tomcat   0 Apr 27 17:20 admin.log
-rw-r--r-- 1 tomcat tomcat  84 Apr 27 17:17 admin.properties
-rw-r--r-- 1 tomcat tomcat 2995 Apr 27 17:17 admin.script
drwxr-xr-x 2 tomcat tomcat 4096 Apr 27 17:20 admin.tmp
lrwxr-xr-x 2 tomcat tomcat 4096 Jun  7  2021 backup
```

Se o subdiretório **de backup** não existir no `/lancope/var/database/dbs/hsqldb/admin/` caminho, ele deverá ser criado e a propriedade correta deverá ser atribuída. Para isso, execute estes comandos:

1. `mkdir /lancope/var/database/dbs/hsqldb/admin/backup`
2. `chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup`
4. Execute o comando `ls -l /lancope/var/admin/` para verificar o conteúdo do diretório.
5. Certifique-se de que os **backups** e os subdiretórios **de diagnóstico** existem e de que o proprietário do usuário/grupo é **raiz**.

```
fcnf-cds:~# ll /lancope/var/admin/
total 80
drwxrwxr-x 2 root root 4096 Apr 27 06:25 backups
drwxr-xr-x 2 root root 4096 Apr 7 21:39 cds
-rw-r--r-- 1 root root 0 Apr 6 22:10 clustered database
drwxrwxr-x 2 root root 4096 Sep 7 2021 diagnostics
-rw-r--r-- 1 root root 40 Apr 27 17:18 hwserial
-rw-r--r-- 1 root root 8 Apr 27 17:18 meminfo
-rw-r--r-- 1 root root 69 Apr 27 17:18 model
-rw-r--r-- 1 root root 23 Apr 27 17:18 platform
drwxr-xr-x 3 root root 4096 Sep 15 2021 plugins
-rw-rw-rw- 1 root root 2 Apr 27 18:13 previous_engine_startup_mode
-rw-r--r-- 1 root root 47 Apr 27 17:18 serial
drwxr-xr-x 2 root root 4096 Apr 7 21:22 ssh
drwxr-xr-x 2 root root 4096 Apr 8 02:51 system.d
-rw-rw---- 1 root swadmin 12756 Apr 8 02:56 system.xml
drwxrwxrwx 2 root root 4096 Apr 28 00:25 log
drwxr-xr-x 2 root root 4096 Sep 7 2021 update
drwxrwxr-x 4 root tomcat 4096 Apr 8 02:49 upgrade
-rw-r--r-- 1 root root 36 Apr 27 17:18 uuid
fcnf-cds:~#
```

Se um ou nenhum dos subdiretórios mencionados não existir no `/lancope/var/admin/path`, eles devem ser criados e a propriedade correta deve ser atribuída. Para isso, execute estes comandos:

1. `mkdir /lancope/var/admin/backups`
2. `mkdir /lancope/var/admin/diagnostics`

Depois que isso for verificado, tente gerar o Pacote de diagnóstico do dispositivo SNA novamente.

## Informações Relacionadas

- Para obter assistência adicional, entre em contato com o Cisco Technical Assistance Center (TAC). É necessário um contrato de suporte válido: [Contatos de suporte da Cisco no mundo inteiro](#).
- [Suporte Técnico e Documentação - Cisco Systems](#)