Diagnosepaket für Appliances für sichere Netzwerkanalysen erstellen

Inhalt

Einleitung

In diesem Dokument werden die verschiedenen verfügbaren Verfahren zum Erfassen eines Diagnosepakets für SNA-Appliances (Secure Network Analytics) beschrieben.

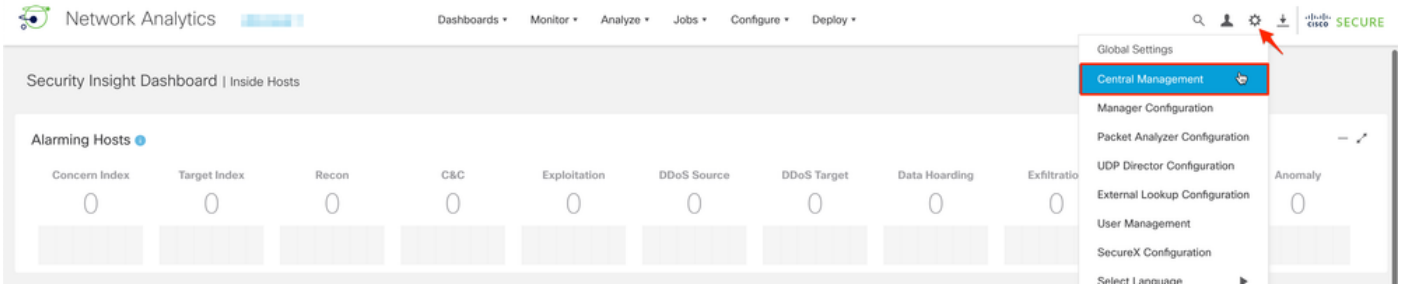
Vorgehensweise

Es gibt drei Hauptmethoden zum Generieren des Diagnosepakets für die SNA-Appliances. Die empfohlene Methode ist **Methode 1. Über die Manager-Webbenutzeroberfläche (UI)** sind jedoch die beiden anderen Methoden optional, falls die Webbenutzeroberfläche des Managers nicht verfügbar ist.

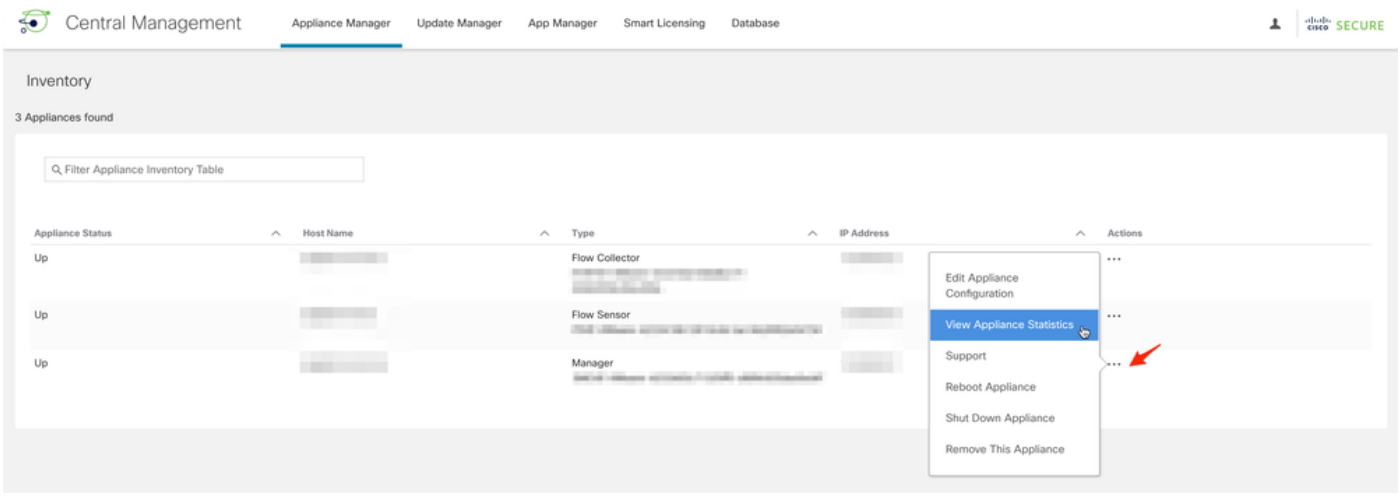
> **Anmerkung:** Wenn die Webbenutzeroberfläche des Managers nicht verfügbar ist und Sie ein Diagnosepaket vom Manager generieren müssen, finden Sie weitere Informationen in **Methode 3. über die Befehlszeilenschnittstelle (CLI)**.

Methode 1. Über die Webbenutzeroberfläche des Managers

1. Melden Sie sich bei der Webbenutzeroberfläche des Managers an.
2. Navigieren Sie zu **Globale Einstellungen > Zentrale Verwaltung**.



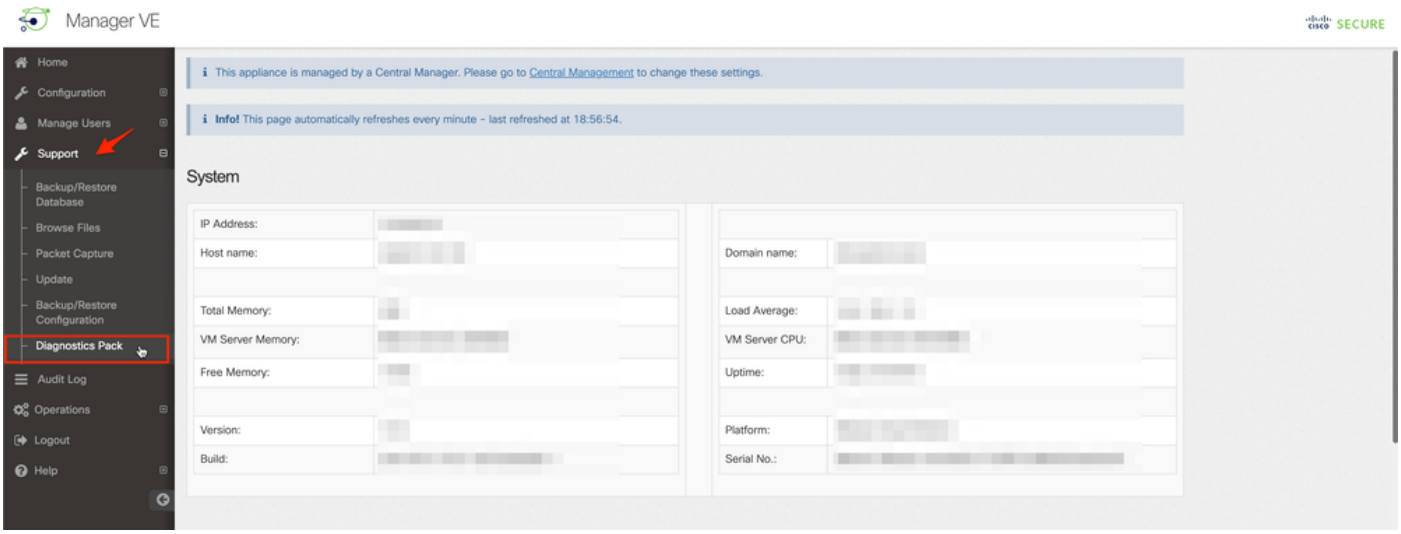
3. Suchen Sie in den aufgeführten Appliances die Appliance, von der Sie das Diagnosepaket erstellen möchten, und wählen Sie **Aktionen (Ellipsis-Symbol) > Einheitenstatistik anzeigen aus**.



4. Sie müssen zur Admin-Benutzeroberfläche der ausgewählten Appliance umgeleitet werden.

5. Melden Sie sich mit **admin-**Anmeldeinformationen bei der Appliance-Admin-Benutzeroberfläche an.

6. Navigieren Sie im Menü links zu **Support > Diagnostics Pack**.

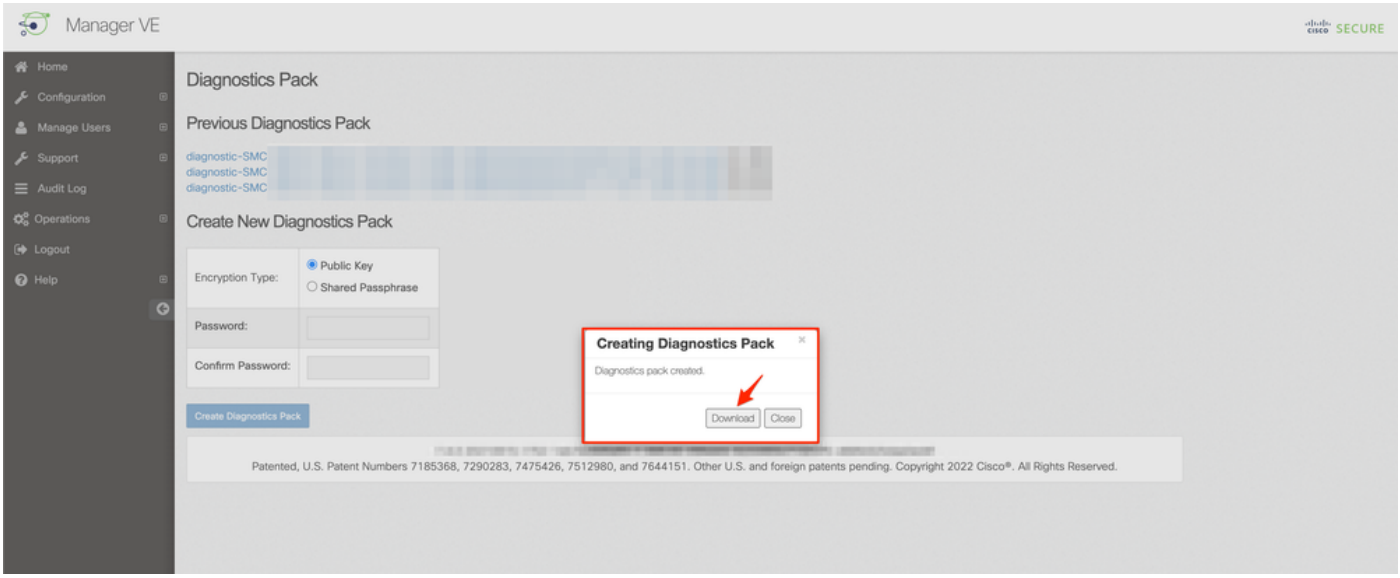


7. Wenn Sie die Seite Diagnostics Pack geöffnet haben, müssen Sie entweder die standardmäßige **Public Key-**Verschlüsselung auswählen oder einen gemeinsam genutzten Schlüssel/eine Passphrase zur Verschlüsselung bereitstellen.

> **Anmerkung:** Wenn Sie einen benutzerdefinierten Schlüssel/ein benutzerdefiniertes Kennwort verwenden, müssen Sie diese Passphrase in der Dateibeschreibung angeben, wenn Sie das Diagnosepaket in den Support Case Manager hochladen.

8. Wählen Sie **Diagnosepaket erstellen**, um das Diagnosepaket der Einheit zu generieren.

9. Nach Abschluss des Vorgangs muss ein Popup-Fenster mit der **Download**-Schaltfläche angezeigt werden, um das Diagnosepaket herunterzuladen.



Methode 2. Über die Admin-Benutzeroberfläche jeder Appliance

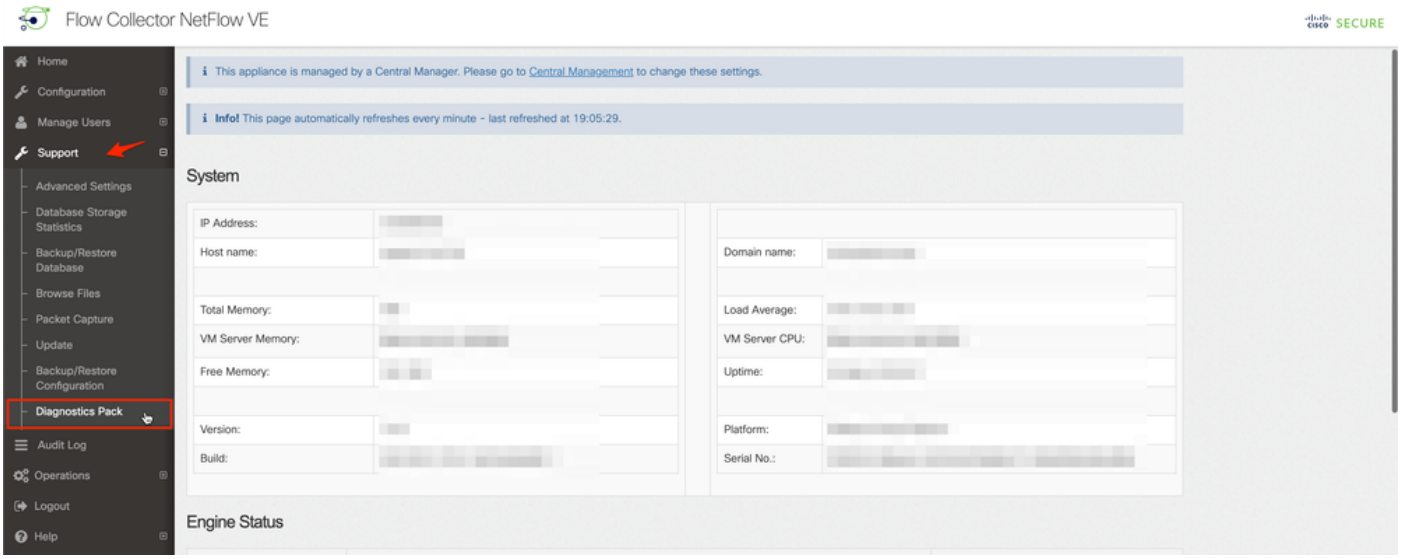
Für diese Methode müssen Sie über Hypertext Transfer Protocol Secure (HTTPS) auf die Appliance zugreifen, von der Sie das Diagnosepaket generieren möchten.

> **Anmerkung:** Um direkt auf die **Admin-Benutzeroberfläche** des Managers zuzugreifen, müssen Sie die URL verwenden: https://<Manager_IP_address>/smc/index.html, andernfalls werden Sie an die Webbenutzeroberfläche des Managers weitergeleitet.

Um beispielsweise das Diagnosepaket eines Flow Collectors mit dieser Methode zu generieren, müssen Sie die folgenden Schritte ausführen:

1. Navigieren Sie in einem Webbrowser zu **https://<FC_IP_address>**
2. Melden Sie sich mit Administratoranmeldeinformationen an der Benutzeroberfläche der Appliance Admin an.

3. Navigieren Sie im Menü links zu **Support > Diagnosepaket**.

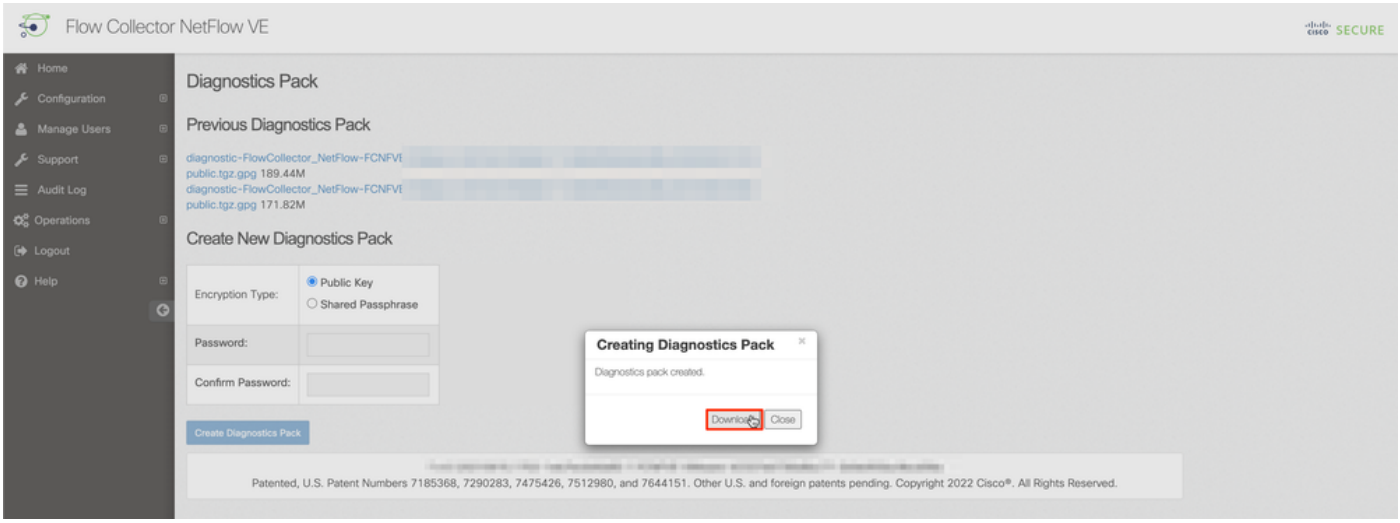


4. Wenn Sie die Seite Diagnostics Pack geöffnet haben, müssen Sie entweder die standardmäßige **Public Key-**Verschlüsselung auswählen oder einen gemeinsam genutzten Schlüssel/eine Passphrase zur Verschlüsselung bereitstellen.

> **Anmerkung:** Wenn Sie einen benutzerdefinierten Schlüssel/eine benutzerdefinierte Passphrase verwenden möchten, müssen Sie diese Passphrase in der Dateibeschreibung eingeben, wenn Sie das Diagnosepaket in den Support Case Manager hochladen.

5. Wählen Sie **Diagnosepaket erstellen**, um das Diagnosepaket der Einheit zu generieren.

6. Nach Abschluss des Vorgangs muss ein Popup-Fenster mit der **Download**-Schaltfläche angezeigt werden, um das Diagnosepaket herunterzuladen.



Methode 3: über die Befehlszeilenschnittstelle (CLI) jeder Appliance

In manchen Fällen ist es nicht möglich, das Diagnosepaket einer Appliance mit den zuvor beschriebenen Methoden zu generieren. Es kann jedoch direkt über die Kommandozeile der Appliance generiert werden. Die Schritte zum Durchführen dieser Aufgabe sind:

1. Stellen Sie über Secure Shell Protocol (SSH) oder direkt über den Konsolenzugriff eine Verbindung zur gewünschten SNA-Appliance her.

   Anmerkung: Falls Sie das Diagnosepaket von einer Hardware-Einheit ohne SSH-Zugriff abholen müssen, kann auch die Kernel-basierte KVM-Konsole von der CIMC-Schnittstelle (Cisco Integrated Management Controller) verwendet werden.

2. Melden Sie sich mit **Root**-Anmeldeinformationen an.
3. Geben Sie einen der folgenden Befehle ein (dies hängt von der verwendeten SNA-Version ab):

SNA Version 7.1.x bis 7.3.x

Geben Sie den Befehl **doDiagPack ein.**

SNA Version 7.4.x

Geben Sie den Befehl **diagnostics start ein.**

4. Warten Sie, bis die Aufgabe abgeschlossen ist.
5. Nachdem die Aufgabe abgeschlossen ist, wird die Diagnosepaket-Datei im **/lancope/var/admin/diagnostics/**Verzeichnis gespeichert**,** das ein Namensschema von **"diagnostisch-<Gerätetyp>-<Geräte-ID>.<JJJMMTT>.<HHMM>-*.tgz.gpg**" enthält.

```
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. Kopieren Sie die generierte Datei von der Appliance auf Ihren lokalen Computer oder auf einen Dateiserver mit Secure Copy Protocol (SCP) oder einem SSH File Transfer Protocol (SFTP)-Client wie WinSCP. Das Diagnosepaket befindet sich im Verzeichnis **/lancope/var/admin/diagnostics/**Directory.

   Hinweis: Es ist zu erwähnen, dass die SNA Version 7.4.0 eine neue Funktion eingeführt hat, mit der das Diagnosepaket aus dem Menü SystemConfig (Systemkonfiguration) generiert werden kann (CLI-Anmeldung mit **Stammanmeldeinformationen** > **Systemkonfiguration** eingeben > Navigieren zu **Wiederherstellung** > **Diagnosepaket**).

   Weitere Informationen zu dieser Methode finden Sie im Konfigurationshandbuch für Secure Network Analytics System 7.4.x.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Es gibt Fälle, in denen die Erstellung des Diagnosepakets fehlschlägt. Das häufigste Symptom ist die Fehlermeldung "Beim Erstellen des Diagnosepakets ist ein Fehler aufgetreten. No files are available (Keine Dateien verfügbar)" (Nach Klicken auf die Schaltfläche **Create Diagnostics Pack** (Diagnosepaket erstellen)).

So korrigieren Sie dieses Verhalten:

1. Melden Sie sich bei der Appliance an, die dieses Verhalten mit **Root-**Anmeldeinformationen über SSH hat.
2. Führen Sie den Befehl **ls -l /lancope/var/database/dbs/hsqldb/admin/**aus, um den Inhalt des Verzeichnisses zu überprüfen.
3. Stellen Sie sicher, dass das **Backup-**Unterverzeichnis vorhanden ist und dass der Benutzer-/Gruppenbesitzer **Tomcat** ist.

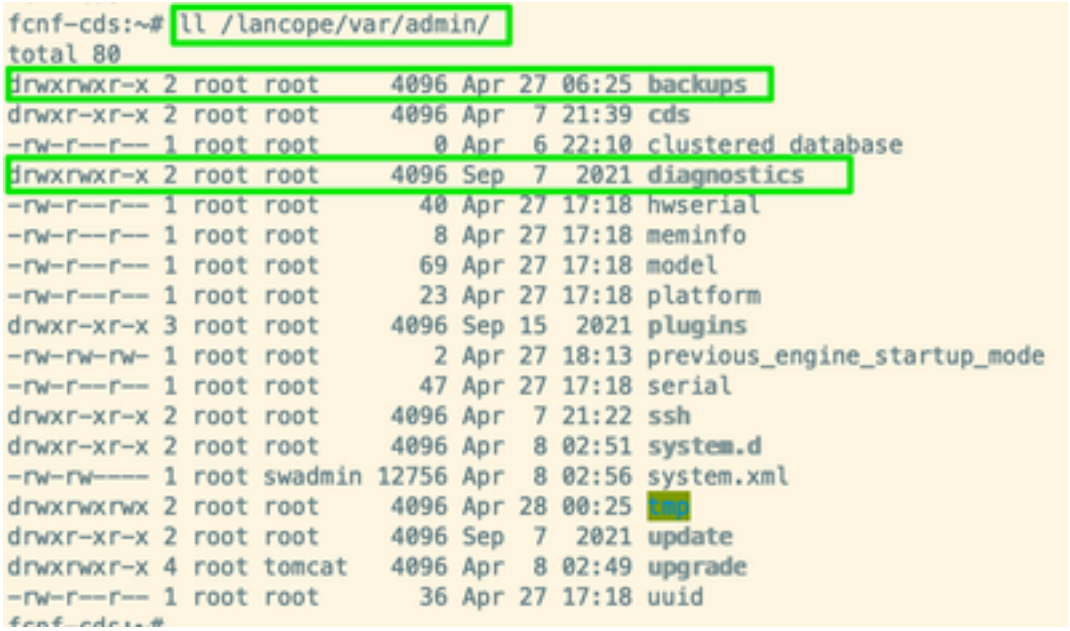
```
fcnf-cds:~# ls -l  /lancope/var/database/dbs/hsqldb/admin/
total 20
-rw-r--r-- 1 tomcat tomcat   16 Apr 28 00:38 admin.lck
-rw-r--r-- 1 tomcat tomcat    0 Apr 27 17:20 admin.log
-rw-r--r-- 1 tomcat tomcat   84 Apr 27 17:17 admin.properties
-rw-r--r-- 1 tomcat tomcat 2995 Apr 27 17:17 admin.script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

Wenn das **Backup-**Unterverzeichnis nicht im **/lancope/var/database/dbs/hsqldb/admin/**path vorhanden ist**,** muss es erstellt und der korrekte Eigentümer zugewiesen werden. Führen Sie dazu die folgenden Befehle aus:

1. mkdir /lancope/var/database/dbs/hsqldb/admin/backup
2. Wählen Sie tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup

4. Führen Sie den Befehl **ls -l /lancope/var/admin/**aus, um den Inhalt des Verzeichnisses zu überprüfen.

5. Stellen Sie sicher, dass die **Backups** und **Diagnoseunterverzeichnisse** vorhanden sind und dass der Benutzer-/Gruppenbesitzer **root** ist.



Wenn ein oder keines der genannten Unterverzeichnisse im **/lancope/var/admin/**path nicht vorhanden ist, müssen diese erstellt und der korrekte Eigentümer zugewiesen werden. Führen Sie dazu die folgenden Befehle aus:

1. mkdir /lancope/var/admin/backup
2. mkdir/lancope/var/admin/diagnose

Nach der Überprüfung sollten Sie erneut versuchen, das Diagnosepaket der SNA-Appliance zu generieren.

Zugehörige Informationen

- Weitere Unterstützung erhalten Sie vom Cisco Technical Assistance Center (TAC). Ein gültiger Support-Vertrag ist erforderlich: Weltweiter Kontakt zum Cisco Support.
- Technischer Support und Dokumentation für Cisco Systeme