

Genera pacchetto diagnostico per appliance di analisi della rete sicure

Sommario

[Introduzione](#)

[Procedura](#)

[Metodo 1. Dall'interfaccia utente Web del manager](#)

[Metodo 2. Dall'interfaccia utente Admin di ciascun accessorio](#)

[Metodo 3. Dall'interfaccia CLI \(Command Line Interface\) di ciascun accessorio](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritte le diverse procedure disponibili per raccogliere un Diagnostics Pack per appliance SNA (Secure Network Analytics).

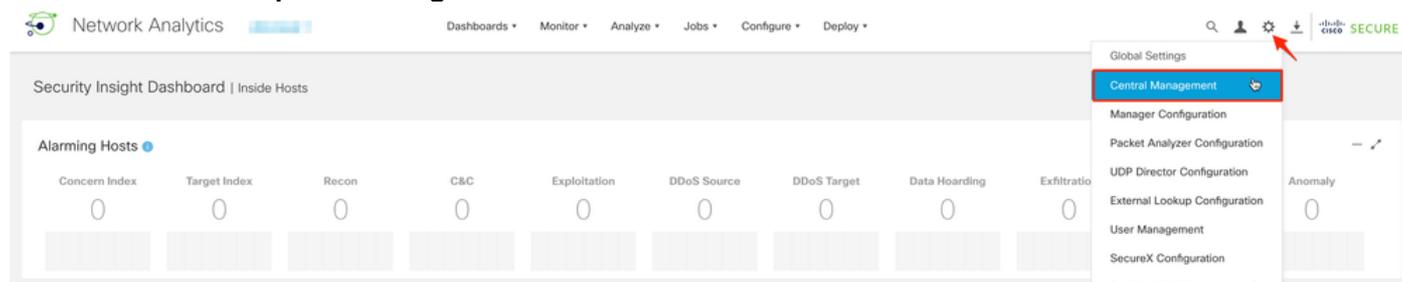
Procedura

Sono disponibili tre metodi principali per generare il Diagnostics Pack per gli accessori SNA. Il metodo suggerito è **Metodo 1. Dall'interfaccia utente di Manager Web User Interface (UI)**, tuttavia, gli altri due metodi sono un'opzione nel caso in cui l'interfaccia utente Web di Manager non sia disponibile.

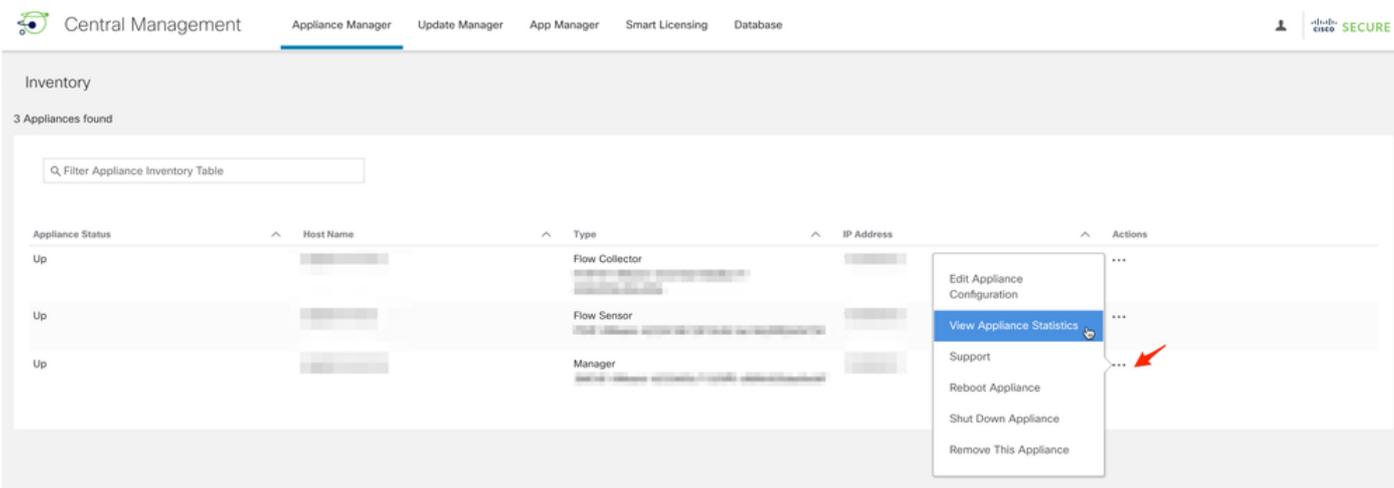
Nota: Se l'interfaccia utente Web di Manager non è disponibile ed è necessario generare un Diagnostics Pack da Manager, fare riferimento al **metodo 3. Dall'interfaccia della riga di comando (CLI) di ciascun accessorio**.

Metodo 1. Dall'interfaccia utente Web del manager

1. Accedere all'interfaccia utente Web di Manager.
2. Passare a **Impostazioni globali > Gestione centrale**.



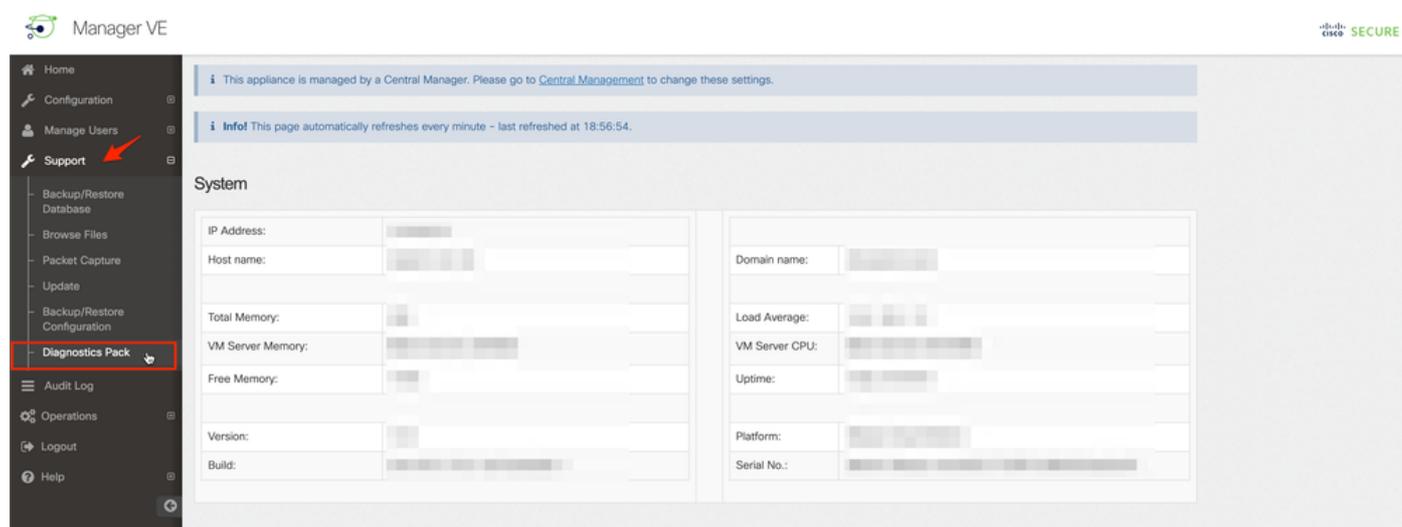
3. Dagli accessori elencati individuare l'accessorio dal quale si desidera creare Diagnostics Pack e selezionare **Azioni (icona Ellissi) > Visualizza statistiche accessorio**.



4. È necessario essere reindirizzati all'interfaccia utente di amministrazione dell'accessorio selezionato.

5. Accedere all'interfaccia utente di amministrazione dell'accessorio con le credenziali di amministratore.

6. Dal menu a sinistra, passare a **Supporto > Diagnostics Pack**.



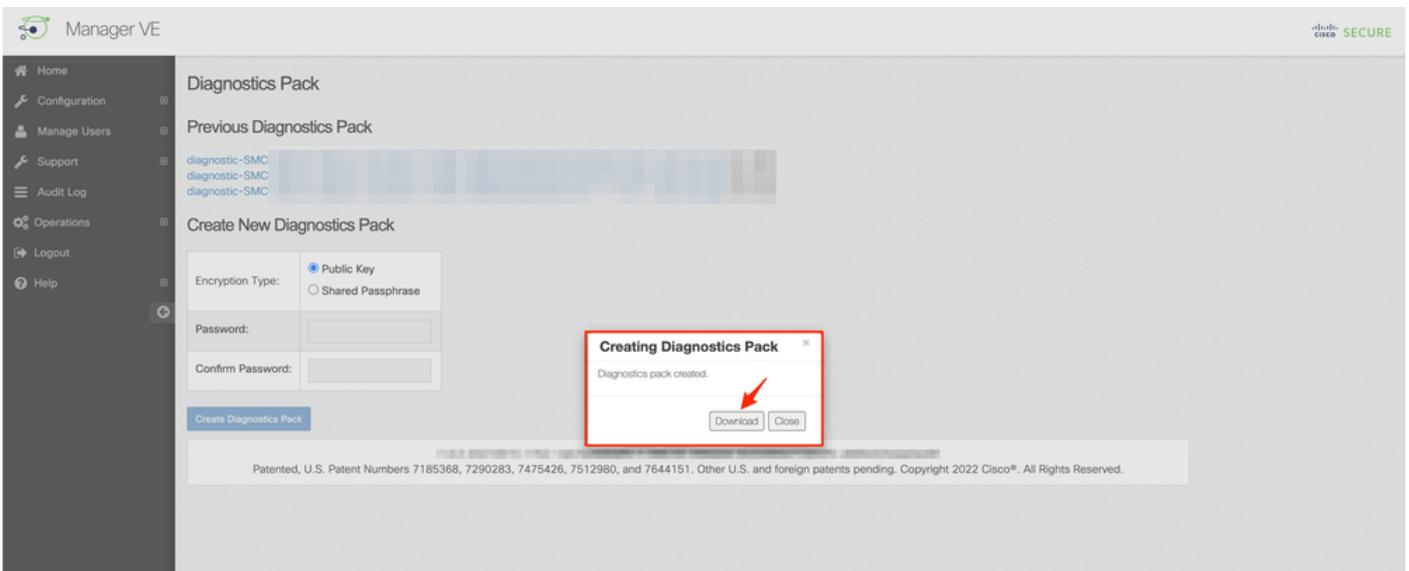
7. Nella pagina Diagnostics Pack, è necessario selezionare la crittografia a **chiave pubblica** predefinita o fornire una chiave/passphrase condivisa da utilizzare per la crittografia.

Nota: Se si sceglie di utilizzare una chiave/password personalizzata, è necessario fornire tale passphrase nella descrizione del file quando si carica il Diagnostics Pack in Support Case Manager.

8. Selezionare **Crea Diagnostics Pack** per generare il Diagnostics Pack dell'accessorio.



9. Al termine, viene visualizzata una finestra popup che include il pulsante **Download** per scaricare il Diagnostics Pack.



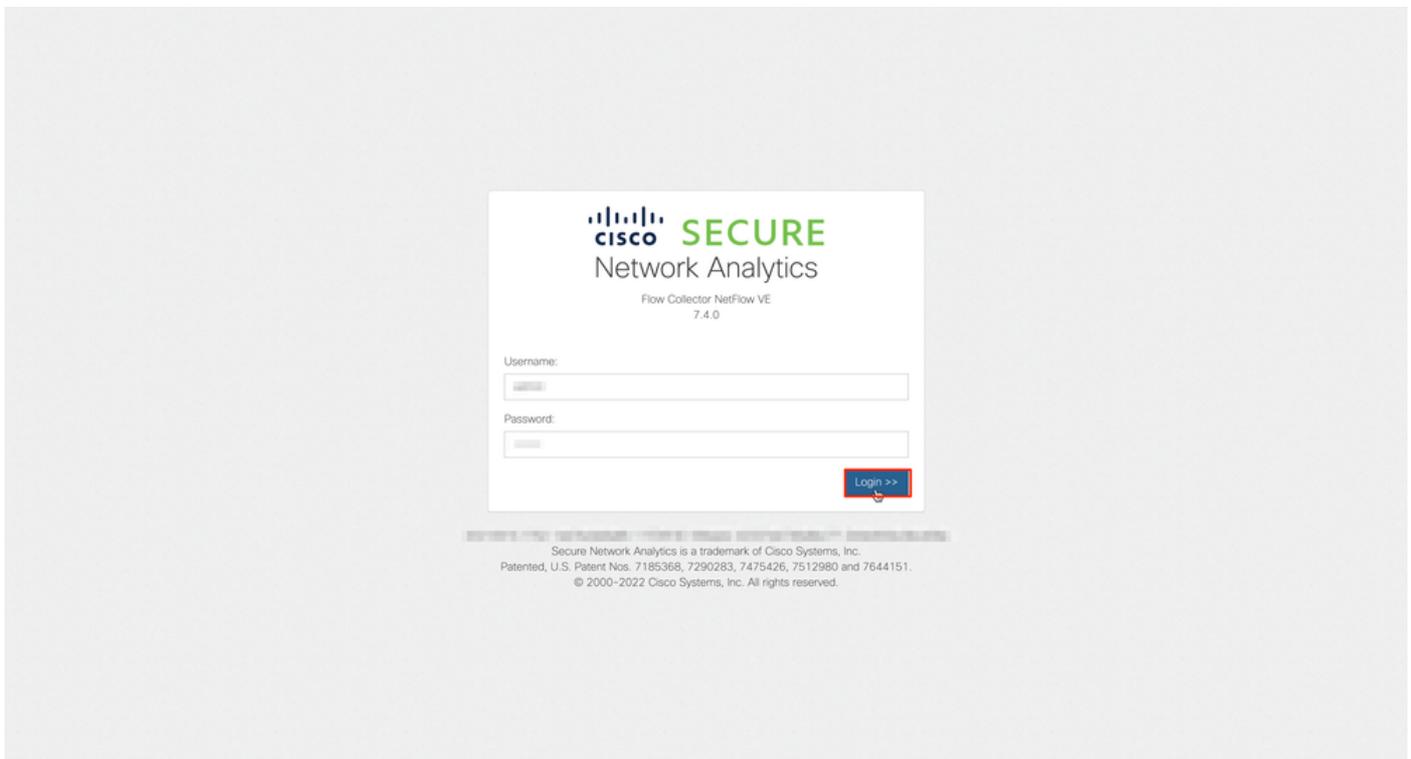
Metodo 2. Dall'interfaccia utente Admin di ciascun accessorio

Per questo metodo è necessario accedere all'accessorio da cui si desidera generare il Diagnostics Pack tramite il protocollo HTTPS (Hypertext Transfer Protocol Secure).

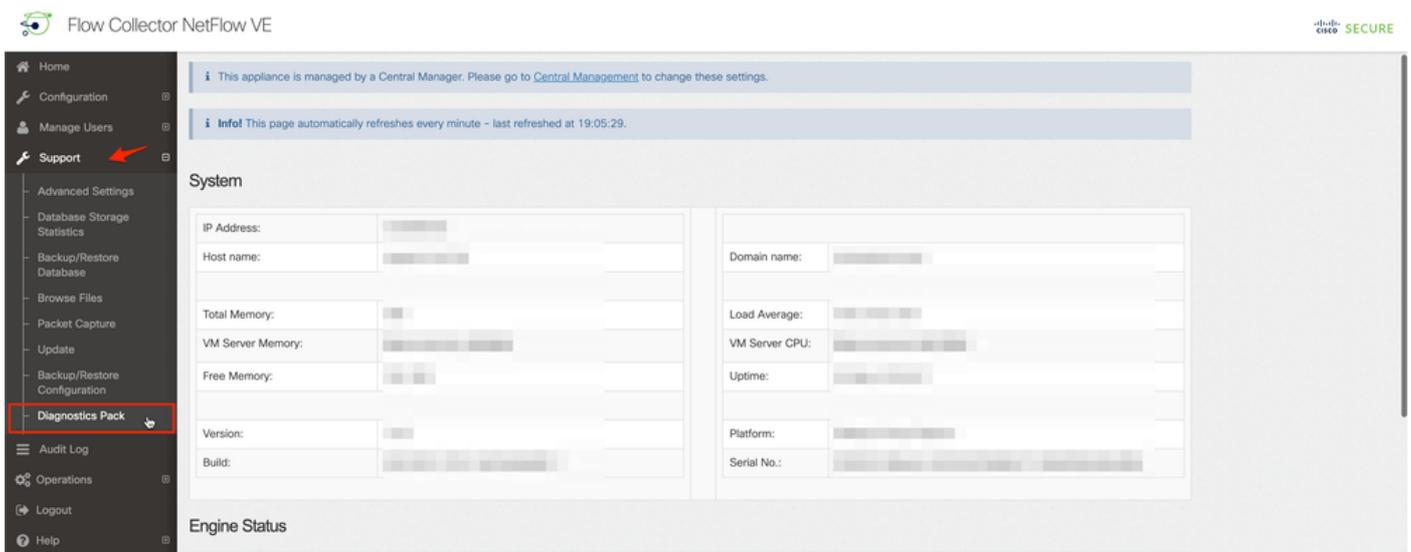
Nota: Per accedere direttamente all'**interfaccia utente Admin di Manager** è necessario utilizzare l'URL: https://<Indirizzo_IP_Manager>/smc/index.html, in caso contrario viene reindirizzato all'interfaccia utente Web di Manager.

Ad esempio, per generare il Diagnostics Pack di un agente di raccolta flusso con questo metodo, è necessario eseguire la procedura seguente:

1. Da un browser Web, passare a https://<indirizzo_IP_FC>
2. Accedere all'interfaccia utente di amministrazione dell'accessorio con le credenziali di amministratore.



3. Dal menu a sinistra, passare a **Supporto > Diagnostics Pack**.



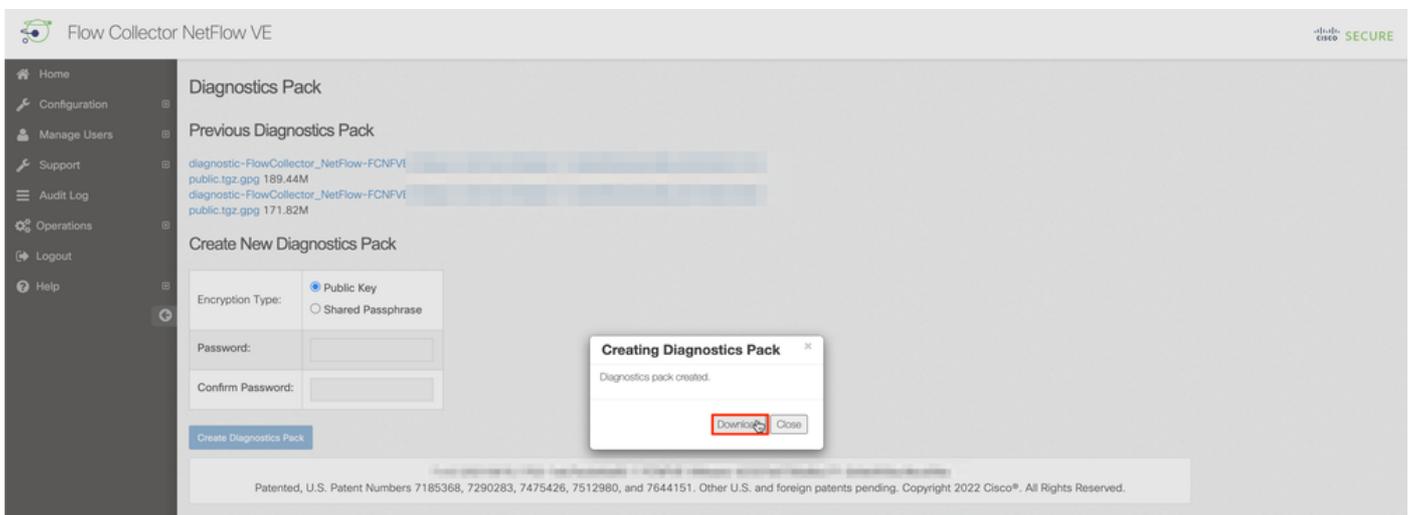
4. Nella pagina Diagnostics Pack, è necessario selezionare la crittografia a **chiave pubblica** predefinita o fornire una chiave/passphrase condivisa da utilizzare per la crittografia.

Nota: Se si sceglie di utilizzare una chiave/passphrase personalizzata, è necessario specificarla nella descrizione del file quando si carica il Diagnostics Pack in Support Case Manager.

5. Selezionare **Crea Diagnostics Pack** per generare il Diagnostics Pack dell'accessorio.



6. Al termine, viene visualizzata una finestra popup che include il pulsante **Download** per scaricare Diagnostics Pack.



Metodo 3. Dall'interfaccia CLI (Command Line Interface) di ciascun accessorio

In alcuni casi non è possibile generare il Diagnostics Pack di un accessorio utilizzando i metodi descritti in precedenza, ma è possibile generarlo direttamente dalla CLI dell'accessorio. Per completare questa attività, eseguire le operazioni seguenti:

1. Collegarsi all'accessorio SNA desiderato tramite il protocollo SSH (Secure Shell Protocol) o direttamente tramite l'accesso alla console.

Nota: Nel caso in cui sia necessario raccogliere il pacchetto di diagnostica da un accessorio hardware senza accesso SSH, è possibile utilizzare anche la console della macchina virtuale basata su kernel (KVM) dall'interfaccia di Cisco Integrated Management Controller (CIMC).

2. Accedere con le credenziali **root**.
3. Immettere uno dei comandi successivi (dipende dalla versione di SNA in uso):

SNA versione 7.1.x - 7.3.x

Immettere il comando **doDiagPack**

SNA versione 7.4.x

Immettere il comando **diagnostics start**

4. Attendere il completamento dell'attività.
5. Una volta completata l'operazione, il file del pacchetto di diagnostica viene archiviato nella directory `/lancope/var/admin/diagnostics/` con uno schema dei nomi "**diagnostic-
<Device_type>-<Device_ID>.<YYYYMMDD>.<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. Copiare il file generato dall'accessorio sul computer locale o su un file server con SCP (Secure Copy Protocol) o con un client SFTP (SSH File Transfer Protocol) come WinSCP. Il pacchetto di diagnostica si trova nella directory `/lancope/var/admin/diagnostics/`.

Nota: vale la pena ricordare che la SNA versione 7.4.0 ha introdotto una nuova funzione che consente di generare Diagnostics Pack dal menu SystemConfig (accesso CLI con credenziali **root > Enter SystemConfig > Navigate to Recovery > Diagnostics Pack**).

Per ulteriori informazioni su questo metodo, vedere la [Guida alla configurazione di Secure Network Analytics System 7.4.x](#).

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

In alcuni casi la creazione di Diagnostics Pack non riesce. Il sintomo più comune si ha quando si riceve un messaggio di errore del tipo "Errore durante la creazione del pacchetto di diagnostica. No files are available" (Nessun file disponibile) dopo aver fatto clic sul pulsante **Create Diagnostics Pack**.



Per correggere questo comportamento, procedere come segue:

1. Accedere all'accessorio con questo comportamento con le credenziali **root** tramite SSH.
2. Eseguire il comando `ls -l /lancope/var/database/dbs/hsqldb/admin/` per verificare il contenuto della directory.
3. Verificare che la sottodirectory **backup** esista e che l'utente o il proprietario del gruppo sia **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
drwxr-xr-x 2 tomcat tomcat 4096 Jun 7 2021 backup
```

Se la sottodirectory di **backup** non esiste nel percorso `/lancope/var/database/dbs/hsqldb/admin/`, è necessario crearla e assegnare la proprietà corretta. A tale scopo, eseguire i comandi seguenti:

1. `mkdir /lancope/var/database/dbs/hsqldb/admin/backup`
2. `chown tomcat:tomcat /lancope/var/database/dbs/hsqldb/admin/backup`
4. Eseguire il comando `ls -l /lancope/var/admin/` per verificare il contenuto della directory.
5. Verificare che le sottodirectory **backup** e **diagnostica** esistano e che il relativo utente/proprietario del gruppo sia **root**.

```
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 tmp
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
```

Se nel percorso `/lancope/var/admin/` non sono presenti una o nessuna delle sottodirectory citate, è necessario crearle e assegnare la proprietà corretta. A tale scopo, eseguire i comandi seguenti:

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

Dopo aver verificato questa condizione, provare a generare nuovamente il Diagnostics Pack dell'accessorio SNA.

Informazioni correlate

- Per ulteriore assistenza, contattare il Cisco Technical Assistance Center (TAC). È necessario un contratto di supporto valido: [Contatti del supporto Cisco internazionali](#).
- [Documentazione e supporto tecnico – Cisco Systems](#)