Secure Network Analyticsアプライアンスの診断パックの生成

内容

概要

このドキュメントでは、Diagnostics Pack for Secure Network Analytics(SNA)アプライアンスを収集するために使用できるさまざまな手順について説明します。

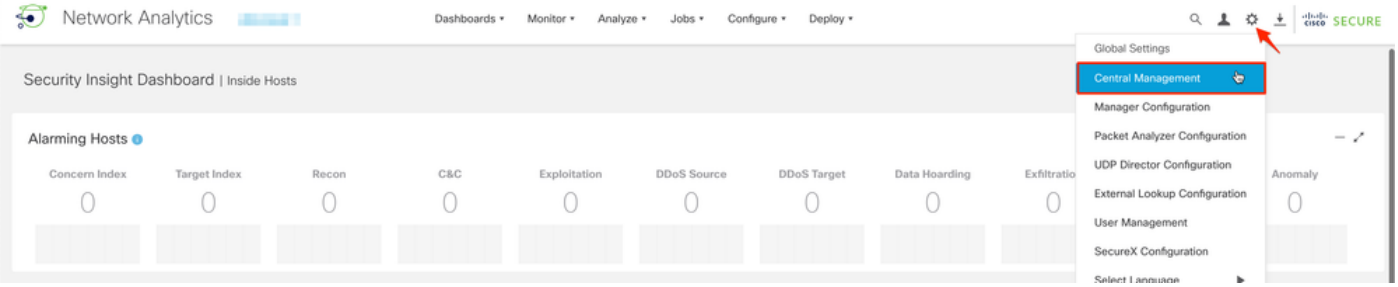
手順

SNAアプライアンスの診断パックを生成するには、主に3つの方法があります。推奨される方法は**Method 1です。Manager Web User Interface (UI)から**は、ManagerのWeb UIが使用できない場合は、他の2つの方法を選択できます。

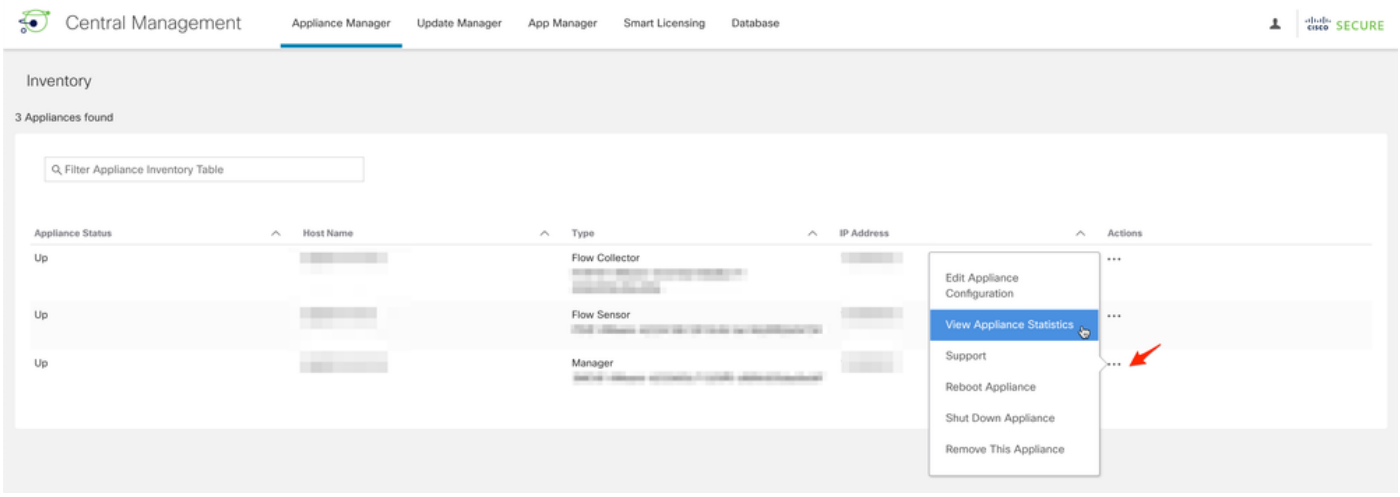
> **注：**ManagerのWeb UIが使用できない場合に、ManagerからDiagnostics Packを生成する必要がある場合は、**Method 3. From Each Appliance's Command Line Interface (CLI)を参照してください。**

方法1.マネージャのWebユーザインターフェイス(UI)から

1. マネージャのWeb UIにログインします。
2. [グローバル設定] > **[中央管理]に移動します。**



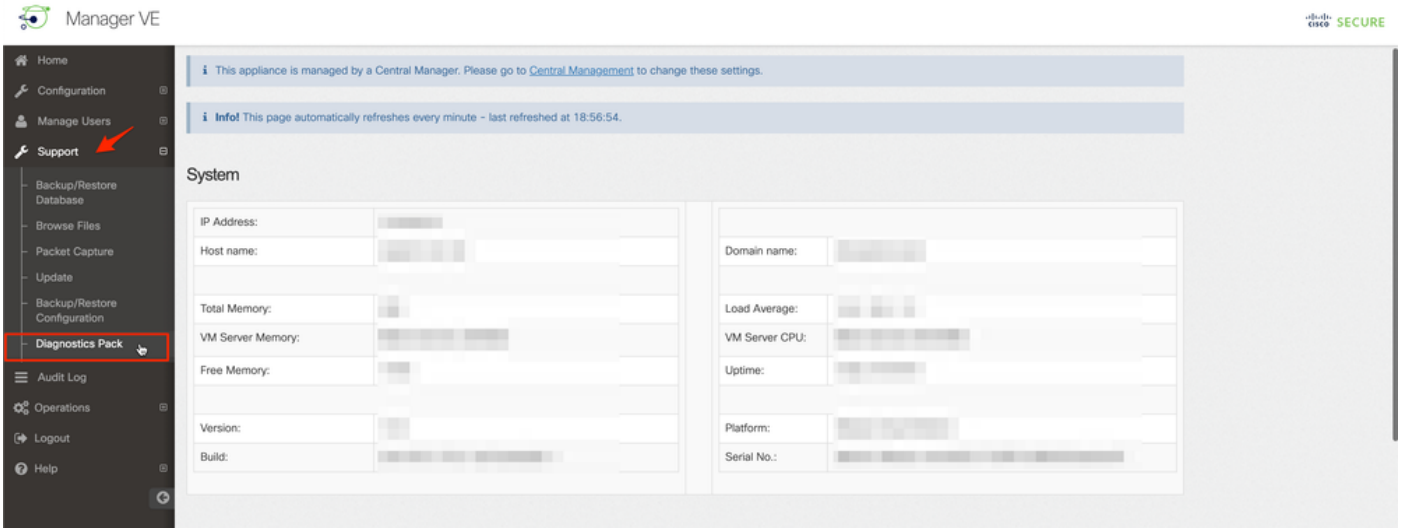
3.リストされているアプライアンスから、診断パックを作成する必要があるアプライアンスを見つけ、「アクション（**省略記号アイコン**）」>「**アプライアンス統計情報の表示**」を選択します。



4.選択したアプライアンスの管理UIにリダイレクトする必要があります。

5.管理者クレデンシャルを使用してアプライアンスの管理者UI**にログイン**します。

6.左側のメニューから、[Support] > [Diagnostics Pack]**に移動します**。

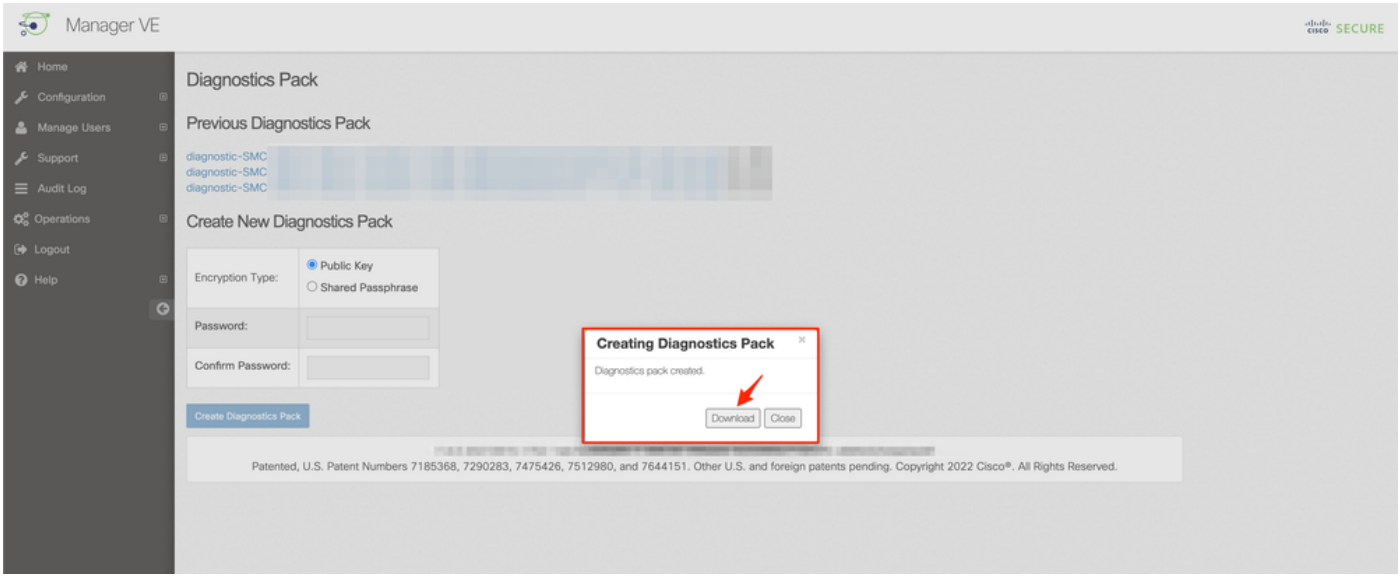


7. [Diagnostics Pack]ページで、デフォルトの公開キー暗号化を選択するか、暗号化に使用する共有キー/パスフレーズを指定する必要があります。

> **注**：カスタムキー/パスワードを使用する場合は、DiagnosticsパックをSupport Case Managerにアップロードするときに、ファイルの説明にそのパスフレーズを入力する必要があります。

8. 「診断パックの**作成」を選択**し、アプライアンスの診断パックを生成します。

9.完了したら、Diagnostics Packをダウンロードするためのダウンロードボタンを含むポップアップボックスを表示する必要があります。



方法2.各アプライアンスの管理UIから

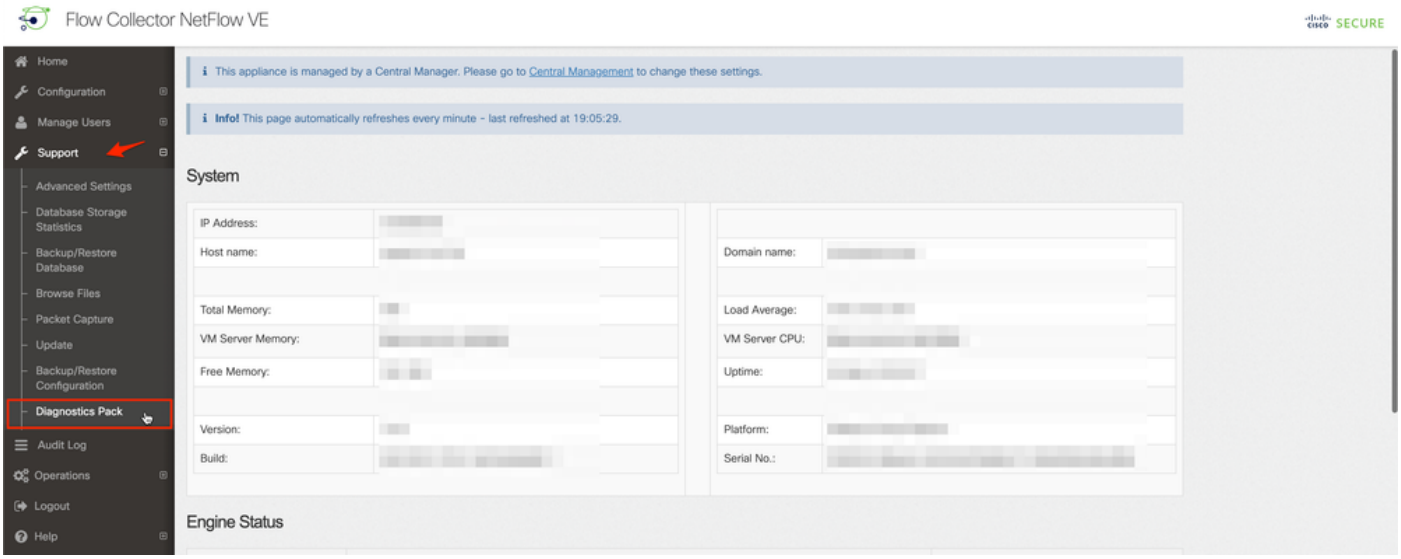
この方法では、Hypertext Transfer Protocol Secure(HTTPS)を介して、診断パックの生成元のアプライアンスにアクセスする必要があります。

> **注**：マネージャの管理UIに直接アクセスするには、次のURLを使用する必要があります。https://<Manager_IP_address>/smc/index.html。それ以外の場合は、マネージャのWeb UIにリダイレクトされます。

たとえば、この方法でFlow Collectorの診断パックを生成するには、次の手順に従う必要があります。

1. Webブラウザからhttps://<FC_IP_address>
2. 管理者クレデンシャルを使用して、アプライアンスの管理者UIにログインします。

3.左側のメニューから、 **[Support] > [Diagnostics Pack]**.

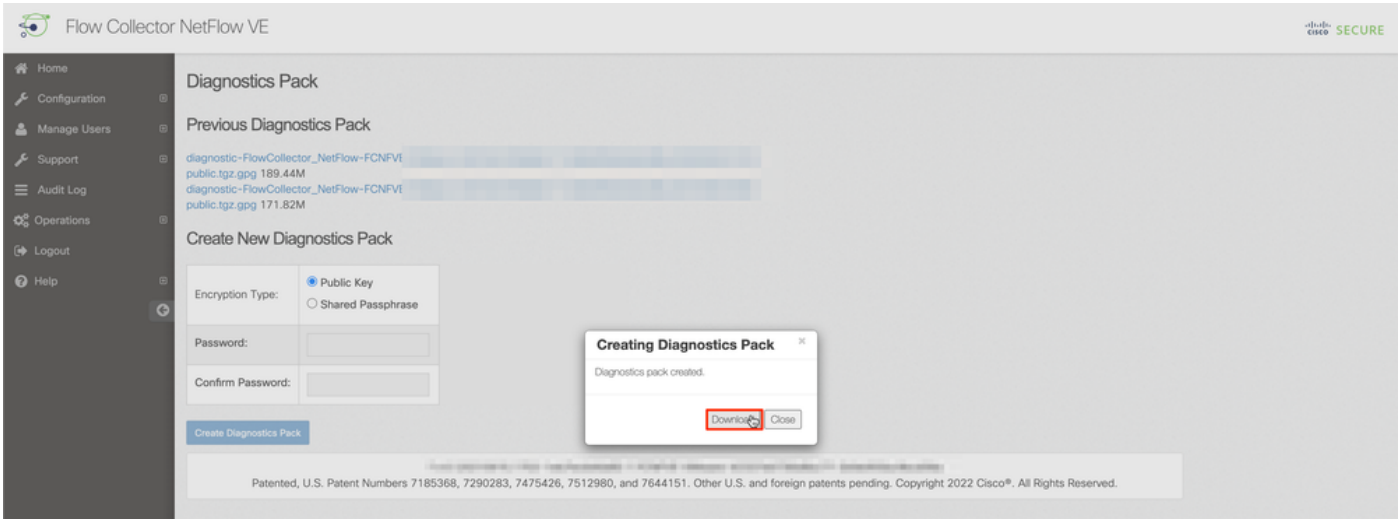


4. [Diagnostics Pack]ページで、デフォルトの公開キー暗号化を選択するか、暗号化に使用する共有キー/パスフレーズを指定する必要があります。

> **注**：カスタムキー/パスフレーズを使用する場合は、Diagnostics packをSupport Case Managerにアップロードするときに、ファイルの説明にそのパスフレーズを入力する必要があります。

5. 「診断パックの**作成」を選択**し、アプライアンスの診断パックを生成します。

6.完了したら、Diagnostics Packをダウンロードするためのダウンロードボタンを含むポップアップボックスを表示する必要があります。



方法3.各アプライアンスのコマンドラインインターフェイス(CLI)から

前述の方法を使用してアプライアンスの診断パックを生成できない場合もありますが、アプライアンスのCLIから直接生成できます。この作業を完了する手順は次のとおりです。

1. Secure Shell Protocol(SSH)を介して、またはコンソールアクセスを介して直接、目的のSNAアプライアンスに接続します。

   注：SSHアクセスのないハードウェアアプライアンスから診断パックを収集する必要がある場合は、Cisco Integrated Management Controller(CIMC)インターフェイスからKernel-based Virtual Machine(KVM)コンソールを使用することもできます。

2. ルート資格情報でログインします。
3. 次のいずれかのコマンドを入力します（これは、使用中のSNAのバージョンによって異なります）。

SNAバージョン7.1.x ~ 7.3.x

doDiagPackコマンドを入力します

SNAバージョン7.4.x

diagnostics startコマンドを**入力します**

4. タスクが完了するのを待ちます。
5. タスクが完了すると、Diagnostics packファイルが**/lancope/var/admin/diagnostics/ディレクトリに保存され、「diagnostic-<Device_type>-<Device_ID>.<YYYMMDD>.<HMM>-*.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. 生成されたファイルをアプライアンスからローカルコンピュータ、またはSecure Copy Protocol(SCP)またはWinSCPなどのSSH File Transfer Protocol(SFTP)クライアントを使用してファイルサーバにコピーします。Diagnostics Packは/lancope/**var/admin/diagnostics/ディレクトリにあります**。

   注:SNAバージョン7.4.0では、SystemConfigメニューからDiagnostics Packを生成できる新機能が導入されました(CLIログイン時に**root** credentials > Enter **SystemConfig** > Navigate to **Recovery** > **Diagnostics Pack**)。

   この方法の詳細については、『Secure Network Analytics System Configuration Guide 7.4.x』を参照してください。

トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

診断パックの作成が失敗する場合があります。最も一般的な症状は、「There an error creating the diagnostics pack.No files are available」というメッセージが表示された**場合は、Create Diagnostics Packボタン**をクリックします。

この動作を修正するには、次の手順に従います。

1. SSH経由でルート資格情報を使用してこの動作を行うアプライアンスにログインします。
2. ls -l /lancope/var/database/dbs/hsqldb/admin/コマンドを実行して、ディレクトリの内容を確認します。
3. backupサブディレクトリが存在し、そのユーザー/グループの所有者がtomcatであることを確認します。

```
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
```

backupサブディレクトリが/lancope/var/database/dbs/hsqldb/admin//パスに存在しない場合は、作成する必要があり、正しい所有権を割り当てる必要があります。そのためには、次のコマンドを実行します。

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

4. ls -l /lancope/var/admin/コマンドを実行して、ディレクトリの内容を確認します。

5.バックアップサブディレクトリとDiagnosticsサブディレクトリが存在し、そのユーザ/グループ所有者がルートであることを確認します。

```
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
```

/lancope/var/admin/pathに前述のサブディレクトリが1つまたは何も存在しない場合は、それらを作成し、正しい所有権を割り当てる必要があります。そのためには、次のコマンドを実行します。

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

これが確認されたら、SNAアプライアンスの診断パックを再度生成してみてください。

関連情報

- その他のサポートについては、Cisco Technical Assistance Center(TAC)にお問い合わせください。有効なサポート契約が必要です。 各国のシスコ サポートの連絡先.
- テクニカル サポートとドキュメント – Cisco Systems