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

内容

<u>概要</u> 手順

<u>方法1.マネージャのWebユーザインターフェイス(UI)から</u> <u>方法2.各アプライアンスの管理UIから</u> <u>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</u> <u>トラブルシュート</u> 関連情報

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。

| 藯 Network A | nalytics | | Dashboards • | Monitor * Analyz | te * Jobs * Conf | igure * Deploy * | | | ۹ ք م | + dialle SECURE |
|--------------------|----------------------|-------|--------------|------------------|------------------|------------------|---------------|-------------|-------------------------------|-----------------|
| Security Insight D | ashboard Lineida U | orte | | | | | | | Global Settings | |
| Security insight D | asinooaru inside n | USIS | | | | | | | Manager Configuration | |
| Alarming Hosts 💿 | | | | | | | | | Packet Analyzer Configuration | - 2 |
| Concern Index | Target Index | Recon | C&C | Exploitation | DDoS Source | DDoS Target | Data Hoarding | Exfiltratio | UDP Director Configuration | Anomaly |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | External Lookup Configuration | 0 |
| | | | | | | | | | SecureX Configuration | |
| | | | | | | | | | Select Language | |

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。

| ÷ | Central Management | Appliance Manager | Update Manager | App Manager | Smart Licensing | Database | | | | Ŧ | cisco SECURE |
|-------|------------------------------------|-------------------|----------------|---------------|-----------------|------------------------------|------------|---------------------------------|---------|---|--------------|
| Inv | entory | | | | | | | | | | |
| 3 App | liances found | | | | | | | | | | |
| | Q Filter Appliance Inventory Table | | | | | | | | | | |
| Ap | pliance Status ^ | Host Name | | Type Type | | ^ | IP Address | ^ | Actions | | |
| Up | | | | Flow Co | llector | | | Edit Appliance Configuration |] | | |
| Up | | - | | Flow Se | nsor | a se total de la companya de | | View Appliance Statistics | | | |
| Up | | | | Manage | - | al and a second | | Support Reboot Appliance | · 🕊 | | |
| | | | | | | | | Shut Down Appliance | | | |
| | | | | | | | | Remove This Appliance | | | |

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。

| 藯 Manager VE | | | | cisco SECURE |
|--|---------------------------------|----------------|------------------------------|--------------|
| ∯ Home ✔ Configuration © | i This appliance is managed by | | | |
| 🚨 Manage Users 🖉 🗉 | i Info! This page automatically | | | |
| 🗲 Support 📕 🛛 🛛 | | | | |
| Backup/Restore Database | System | | | |
| Browse Files | IP Address: | | | |
| Packet Capture | Host name: | Domain name: | | |
| - Update | | | | |
| Backup/Restore Configuration | Total Memory: | Load Average: | | |
| - Diagnostics Pack 👦 | VM Server Memory: | VM Server CPU: | | |
| ■ Audit Log | Free Memory: | Uptime: | 100.000 | |
| Ø ₀ Operations □ | | | | |
| (Logout | Version: | Platform: | | |
| 🕜 Help 🗉 | Build: | Serial No.: | And the second of the second | |
| O | | | | |

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。

| 藯 Manager VE | | enter SECURE |
|--|--|--------------|
| Home Configuration Manage liters | Diagnostics Pack Previous Diagnostics Pack | |
| Support Audit Log | diagnostic-SMC- diagnostic-SMC- diagnostic-SMC- | |
| Operations G | Create New Diagnostics Pack | |
| O Help | Encryption Type: O Shared Passphrase Password: | |
| | Confirm Password: | |
| | Create Diagnostics Pack | |
| | | |

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。

| ਓ Manager VE | | | | | | | cisco SECURE |
|---|--|---|---------------------------|--|---|---------------|--------------|
| ♣ Home ✓ Configuration © | Diagnostics Pa | ack | | | | | |
| 🚔 Manage Users 🛛 🕀 | Previous Diagno | ostics Pack | | | | | |
| | diagnostic-SMC diagnostic-SMC diagnostic-SMC | | | | | | |
| Q ⁰ ₀ Operations ⊚ | Create New Dia | ignostics Pack | | | | | |
| 🕪 Logout | - | | | | | | |
| 🕑 Help 🙂 | Encryption Type: | Public Key Shared Passphrase | | | | | |
| ٥ | Password: | | | Creating Diagnostics Pack | 1 | | |
| | Confirm Password: | | | Diagnostics pack created. | | | |
| | Create Diagnostics Pac | × | | Download Cicse | | | |
| | Patenteo | d, U.S. Patent Numbers 7185 | 68, 7290283, 7475426, 751 | 12980, and 7644151. Other U.S. and foreign p | atents pending. Copyright 2022 Cisco®. All Rigt | nts Reserved. | |
| | | | | | | | |
| | | | | | | | |

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。 <u>https://<Manager_IP_address>/smc/index.html</u>。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<u>https://<FC_IP_address></u>

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].

| o A. | Flow Collector NetFlow VE | | | | | | | | | | | | |
|----------------|---|--|------------------|---|----------------|--|--|--|--|--|--|--|--|
| 44 14 14 | Home Configuration © Manage Users © | ne diguration contract Manager. Please go to <u>Central Management</u> to change these settings. | | | | | | | | | | | |
| مر ا | Support | Sys | System | | | | | | | | | | |
| ŀ | Database Storage Statistics | IP | | | | | | | | | | | |
| ŀ | - Backup/Restore Database | Ho | est name: | and the second se | | | | | | | | | |
| | - Browse Files | To | tal Memory: | | Load Average: | | | | | | | | |
| | Packet Capture Update | VN | / Server Memory: | | VM Server CPU: | Concession and the | | | | | | | |
| ╞ | - Backup/Restore Configuration | Fre | ee Memory: | | Uptime: | and the second sec | | | | | | | |
| F | - Diagnostics Pack | | | | | | | | | | | | |
| = | Audit Log | Ve | rsion: | | Platform: | | | | | | | | |
| ¢ | Operations 🗉 | Bu | 110: | | Senal No.: | | | | | | | | |
| ۲ | Logout | Eng | ino Statua | | | | | | | | | | |
| 6 |)Help ⊞ | Eng | line Status | | | | | | | | | | |

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。

| ਓ Flow Colle | ector | NetFlow VE | | | | | |
|--|--------|---|---|-------------------------------------|-----------------------------|--|------------------------------|
| 🙀 Home | Ð | Diagnostics Pa | ack | | | | |
| 👗 Manage Users | Ð | Previous Diagno | ostics Pack | | | | |
| Support Audit Log Operations Logout | æ | diagnostic-FlowCollec public.tgz.gpg 189.441 diagnostic-FlowCollec public.tgz.gpg 171.821 Create New Diag | tor_NetFlow-FCNFVE M tor_NetFlow-FCNFVE M gnostics Pack | | | | |
| 😧 Help | в С | Encryption Type: | Public Key Shared Passphrase | | | | |
| | | Password: | | | | | |
| | | Confirm Password: | | | | | |
| | | Create Diagnostics Paci | | | | | |
| | | Patented, | , U.S. Patent Numbers 7185 | 868, 7290283, 7475426, 7512980, and | d 7644151. Other U.S. and f | oreign patents pending. Copyright 2022 | Cisco®, All Rights Reserved. |

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。

| Flow Collecto | or NetFlow VE | diadas SECURE |
|--|---|---------------|
| ♣ Home ▶ Configuration □ ▲ Manage Users □ ▶ Support □ ■ Audit Log □ ♦ Operations □ ● Logout □ ● Help □ | Diagnostics Pack Previous Diagnostics Pack diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 188.44M diagnostic-FlowCollector_NetFlow-FCNFVI public.tgz.gpg 171.82M Create New Diagnostics Pack Encryption Type: Public key Shared Passphrase | |
| | Password: Creating Diagnostics Pack * Confirm Password: Diagnostics pack oreated. Diagnostics pack oreated. Create Diagnostics Pack Diagnostics Pack * Patented, U.S. Patent Numbers 7185368, 7290283, 7475426, 7512980, and 7644151. Other U.S. and foreign patents pending. Copyright 2022 Cisco®. All Rights Reserved. | |

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Kernelbased 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"



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、『<u>Secure Network Analytics System Configuration Guide</u> <u>7.4.x』を参照してください</u>。

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。

| Creating Diagnostics Pack × |
|--|
| There was an error creating the diagnostics pack. No files are available. |
| Close |

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. Is -I /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:~4 | ŧ 🗌 | ls –l , | /lancope | e/var/ | /data | abas | se/dbs/ | /hsqldb/admin/ |
|-------------|-----|---------|----------|--------|-------|------|---------|------------------|
| total 20 | | | | | | | | |
| -rw-rr | 1 | tomcat | tomcat | 16 | Apr | 28 | 00:38 | admin.lck |
| -rw-rr | 1 | tomcat | tomcat | 0 | Apr | 27 | 17:20 | admin.log |
| -rw-rr | 1 | tomcat | tomcat | 84 | Apr | 27 | 17:17 | admin.properties |
| -rw-rr | 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. Is -I /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:~4 | ŧ 1 | ll /la | ancope/va | ar/adm: | in/ | | | |
|-------------|-----|--------|-----------|---------|-----|----|-------|------------------------------|
| 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-rr | 1 | root | root | 0 | Apr | 6 | 22:10 | clustered database |
| drwxrwxr-x | 2 | root | root | 4096 | Sep | 7 | 2021 | diagnostics |
| -rw-rr | 1 | root | root | 40 | Apr | 27 | 17:18 | hwserial |
| -rw-rr | 1 | root | root | 8 | Apr | 27 | 17:18 | meminfo |
| -rw-rr | 1 | root | root | 69 | Apr | 27 | 17:18 | model |
| -rw-rr | 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-rr | 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-rr | 1 | root | root | 36 | Apr | 27 | 17:18 | uuid |
| fonf-odcust | 44 | | | | | | | |

/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。

関運情報

- 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。
- <u>テクニカル サポートとドキュメント Cisco Systems</u>