生成安全网络分析设备的诊断包

目录

简介

步骤

- 方法1.通过SystemConfig菜单（推荐方法）
- 方法2.集中管理
- 方法3.管理Web UI
- 方法4.从每台设备的命令行界面(CLI)

生成CXD上传令牌

- 使用SystemConfig中的上传令牌
- 使用SNA Web UI中的上传令牌（7.6.1的新版本）

故障排除

相关信息

简介

本文档介绍可用于生成安全网络分析(SNA)设备诊断包的不同过程。

步骤

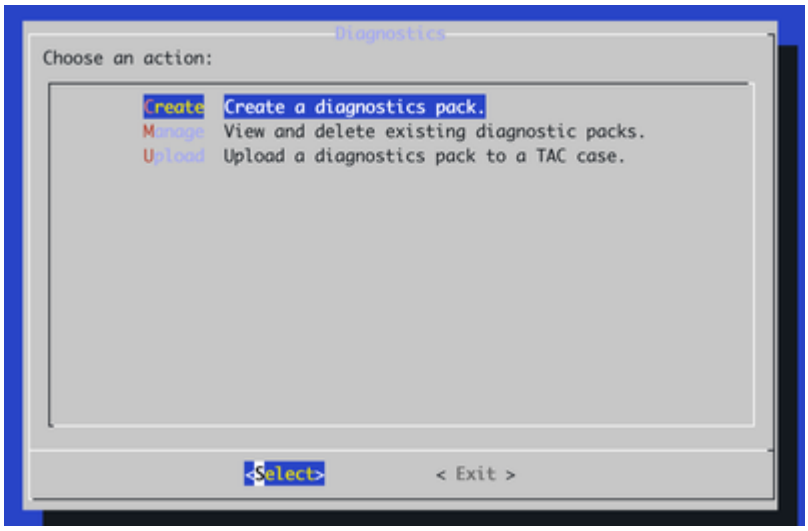
有四种方法可生成SNA设备的诊断包。推荐的方法是方法1.通过SystemConfig菜单。

如果设备没有直接或通过代理的Internet连接，则其余方法是一个选项。

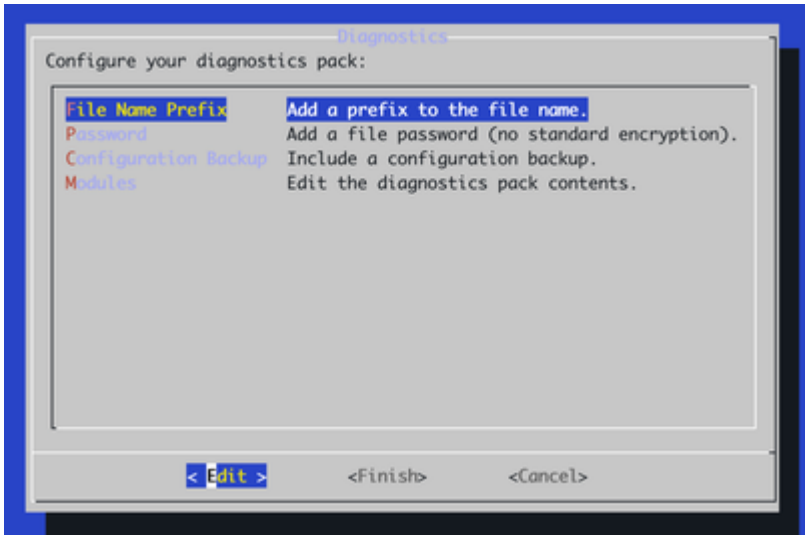
可用方法因软件版本而异。

方法1.通过SystemConfig菜单（推荐方法）

1. 以sysadmin身份登录设备控制台。
2. 选择Recovery > Diagnostics Pack > Create。



3. 要自定义诊断包，请突出显示所需选项，然后单击Edit。



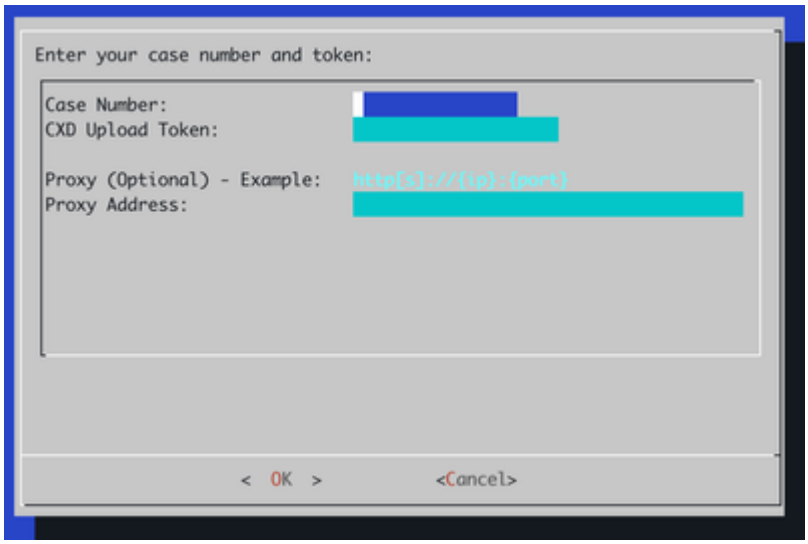
选项:

File Name Prefix — 为诊断包添加文件名前缀（最多127个字符）。
Password — 为诊断包创建文件密码。如果不创建文件密码，将使用默认方法（Cisco密钥）加密诊断包。
配置备份 — 选择此选项并完成屏幕提示以将配置备份包括在诊断包中。有关备份的详细信息，请参阅帮助中的备份配置文件。
Modules — 通过选择要包含的特定模块来编辑诊断包内容。

4. 单击 完成。完成屏幕提示以创建诊断包。

5. 您可以从SystemConfig将诊断包直接上传到TAC案例。选择 上传.

6. 选择要上传的诊断包，然后选择Select。



7. 在Case Number（案例编号）字段中输入TAC案例编号。

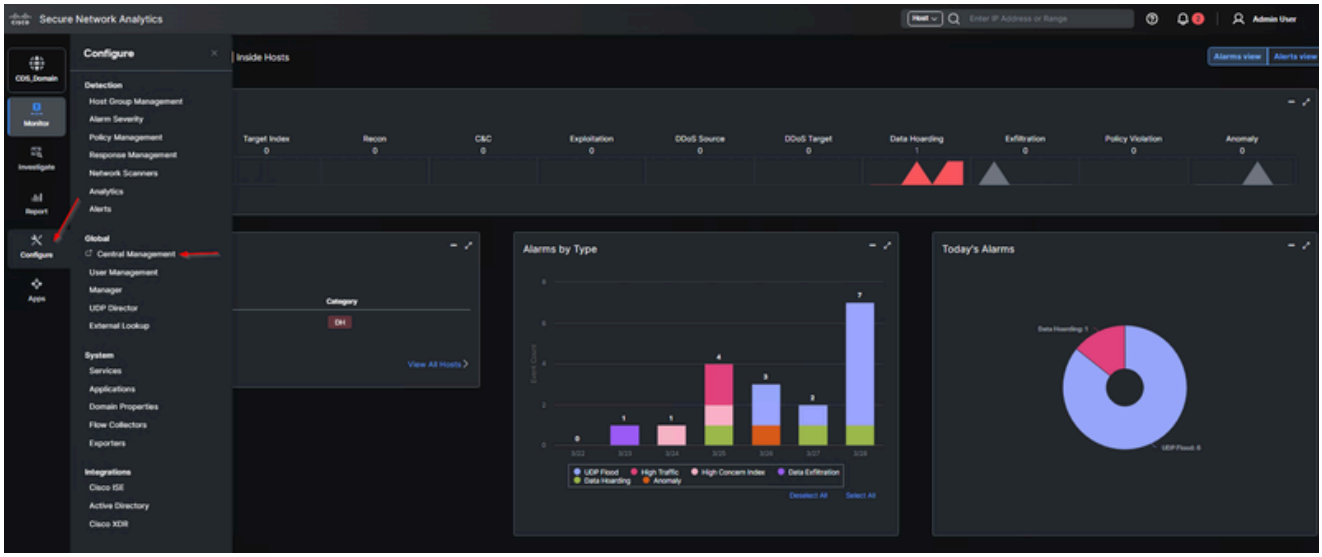
8. 输入Case number token CXD Upload Token字段。如果您没有此令牌，请按照以下步骤生成一个令牌：https://www.cisco.com/c/en/us/support/web/tac/tac-customer-file-uploads.html#cxduploadtoken
9. 如果需要代理，请在代理地址字段中输入代理。

10. 完成后，选择OK。

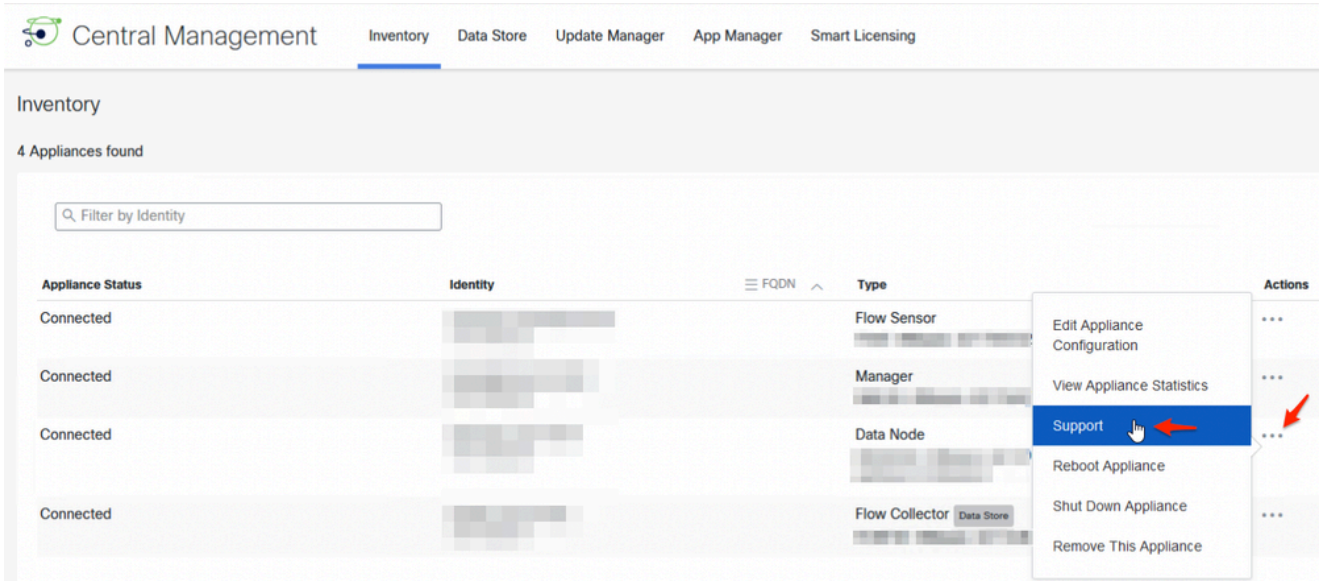
方法2.集中管理

1. 登录到SNA Manager的Web UI。

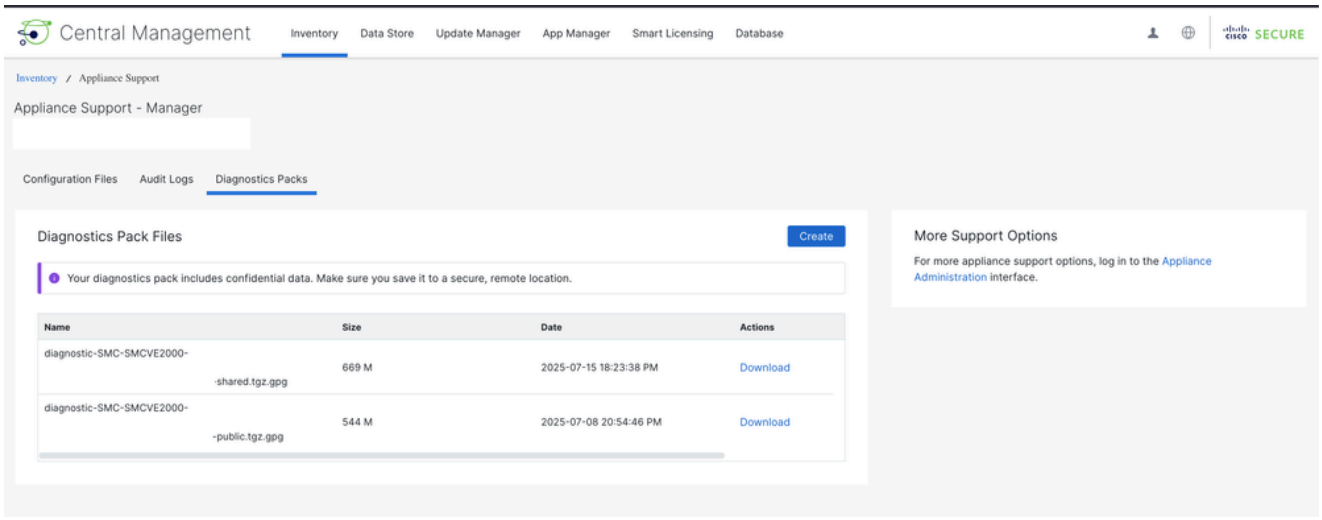
2. 选择Configure > 全局>集中管理



3. 将打开中央管理的浏览器选项卡，并显示资产选项卡。在“资产”选项卡中，点击要为其创建诊断包的设备的省略号图标。选择Support。



4. 这会将您引导至中央管理中的设备支持页面。单击“诊断包”选项卡>创建开始创建新的诊断包的过程。可以下载以前完成的诊断包。

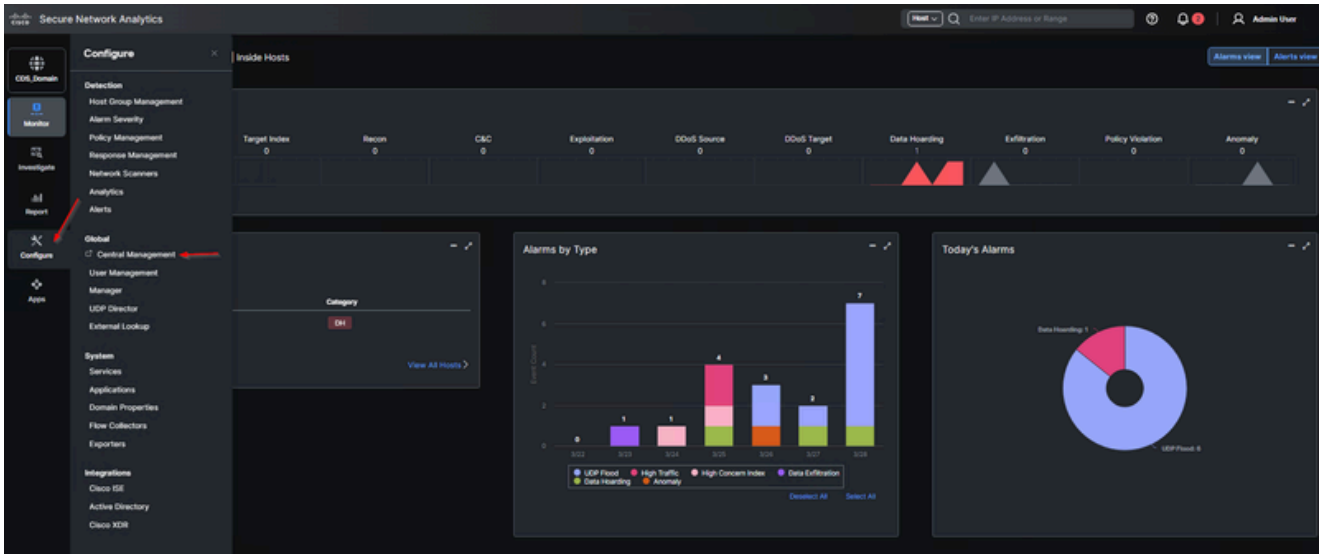


方法3.管理Web UI

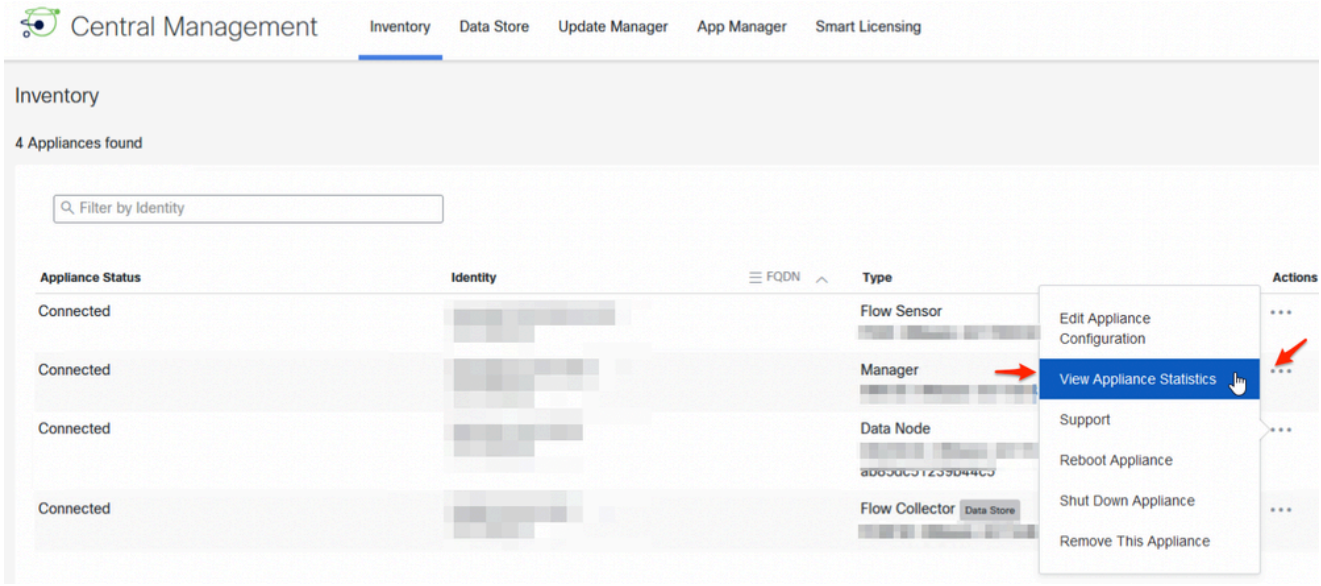
有两种方法可以访问SNA设备的管理UI：通过SNA管理器中央管理功能，或者直接访问。

如果您知道设备FQDN或IP地址，请从步骤4开始。

1. 登录到SNA Manager的Web UI。
2. 选择Configure > 全局>集中管理



3. 将打开中央管理的浏览器选项卡，并显示资产选项卡。在“资产”选项卡中，点击要为其创建诊断包的设备的省略号图标。选择View Appliance Statistics。系统会为该设备Admin UI打开另一个新的浏览器选项卡。



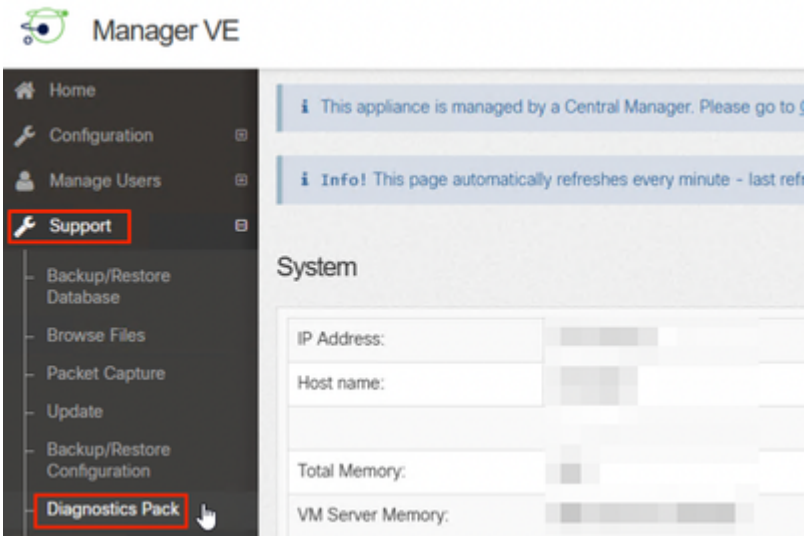
4. 使用管理员凭证登录设备管理UI。如果未使用SNA Managers Central Management功能，请通过所需设备的DNS可解析FQDN或其IP地址https://{IP_or_FQDN_here}导航到登录页面，然后使用内置管理员用户登录。

注意：要在登录后访问Managers Admin UI，请更改URL:https://{Manager_IP_or_FQDN}/smc/index.html

---

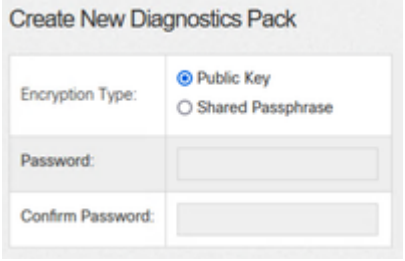


5. 从左侧菜单中单击Support > Diagnostics Pack。



6. 进入“诊断包”页面后，对于“加密类型”(Encryption Type)，将默认的Public Key保持选中状态，或者选择Shared Passphrase，然后在Password和Confirm Password字段中输入该密码。

注意：将诊断包上传到Support Case Manager时，请在文件说明字段中向TAC提供共享密码。 将说明输入为key:value对，其中“passphrase”是密钥，并且值设置为用于加密文件的共享密码。 示例：口令：<your_shared_passphrase>。 这允许对诊断包进行最有效的处理和分析。



7. 选择创建诊断包以生成设备的诊断包。创建时，焦点位于页面上的弹出窗口。



8. 完成后，系统将显示一个弹出框，其中包含用于下载诊断包的Download按钮。可以从此页面下载以前完成的诊断包。



注意：如果您无权访问Web UI，请使用选项1。通过SystemConfig菜单

方法4.从每台设备的命令行界面(CLI)

注意：此方法仅对软件版本7.5.0之前的用户可用。

有时无法使用上述方法生成设备的诊断包，但可以直接从设备CLI生成。完成此任务的步骤如下：

1. 通过安全外壳协议(SSH)或直接通过控制台访问连接到所需的SNA设备。

注意：如果您需要从无SSH访问的硬件设备收集诊断包，也可以使用思科集成管理控

制器(CIMC)界面中的基于内核的虚拟机(KVM)控制台。

2. 使用根凭据登录。

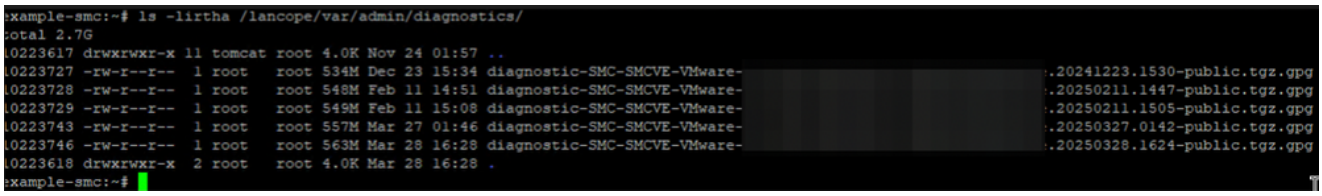
3. 运行正在使用的SNA软件版本的命令：

SNA软件版本7.1.x到7.3.x运行doDiagPack命令。

SNA软件版本7.4.x运行diagnostics start命令。

4. 等待任务完成。开启

5. 诊断包文件保存在/lancope/var/admin/diagnostics/目录中，名称方案为“diagnostic-<Device_type>-<Device_ID>.<YYYYMMDD>.<HHHMM>-*.tgz.gpg”

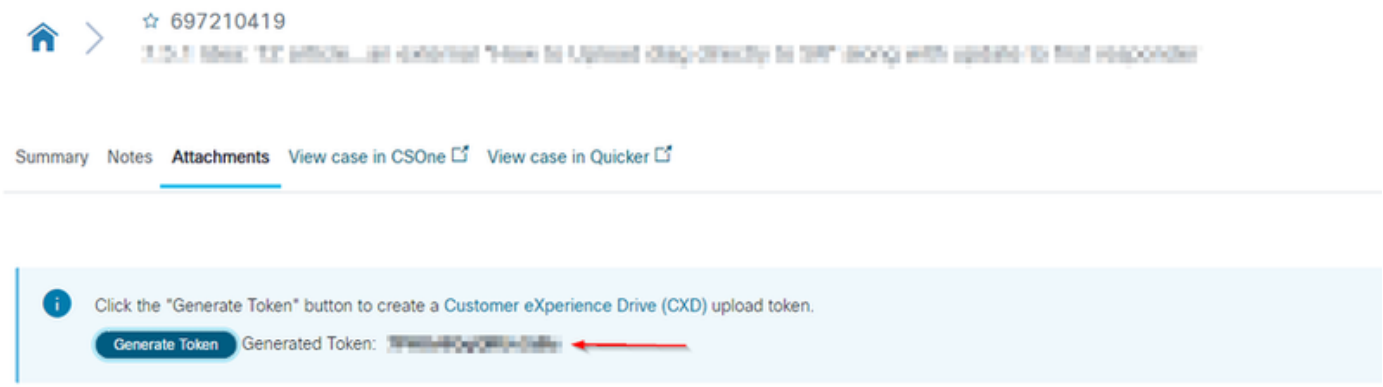


6. 使用安全复制协议(SCP)或SSH文件传输协议(SFTP)客户端（如WinSCP），将生成的文件从设备传输到本地计算机或文件服务器。

注：值得一提的是，SNA软件版本7.4.0引入了一项新功能，允许从SystemConfig菜单生成诊断包（使用root credentials > Enter SystemConfig > Navigate to Recovery > Diagnostics Pack的CLI登录）。
有关此方法的详细信息，请参阅安全网络分析系统配置指南7.4.x。

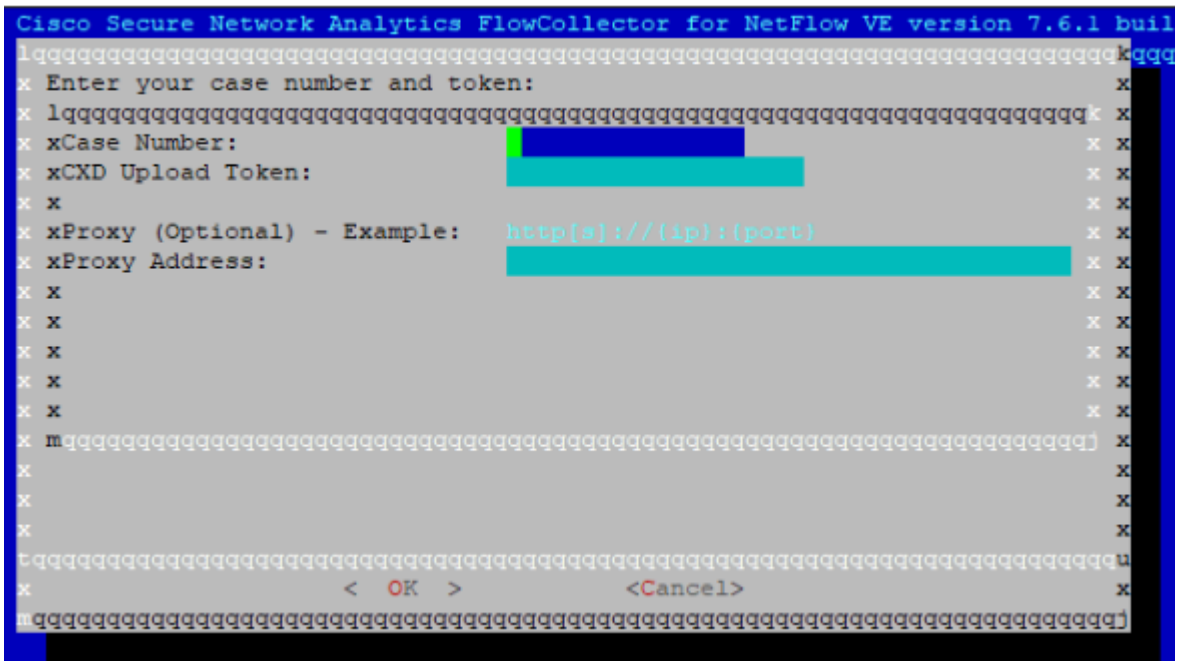
生成CXD上传令牌

- 访问支持案例管理器
- 访问相关支持案例并点击附件
- 点击Generate Token按钮



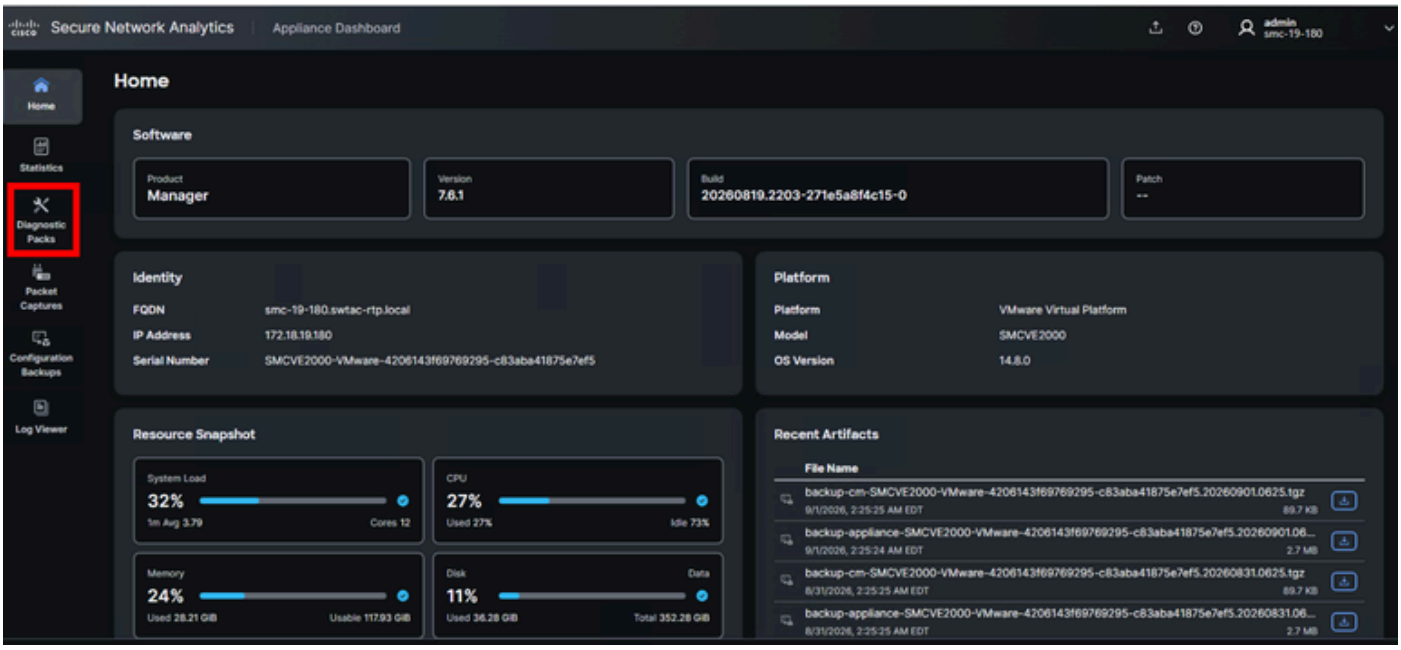
使用SystemConfig中的上传令牌

- 系统将显示生成的令牌屏幕，然后可以从SystemConfig -> Recovery -> Diagnostics -> Upload菜单使用此上传令牌，以便将诊断包目录上传到SR

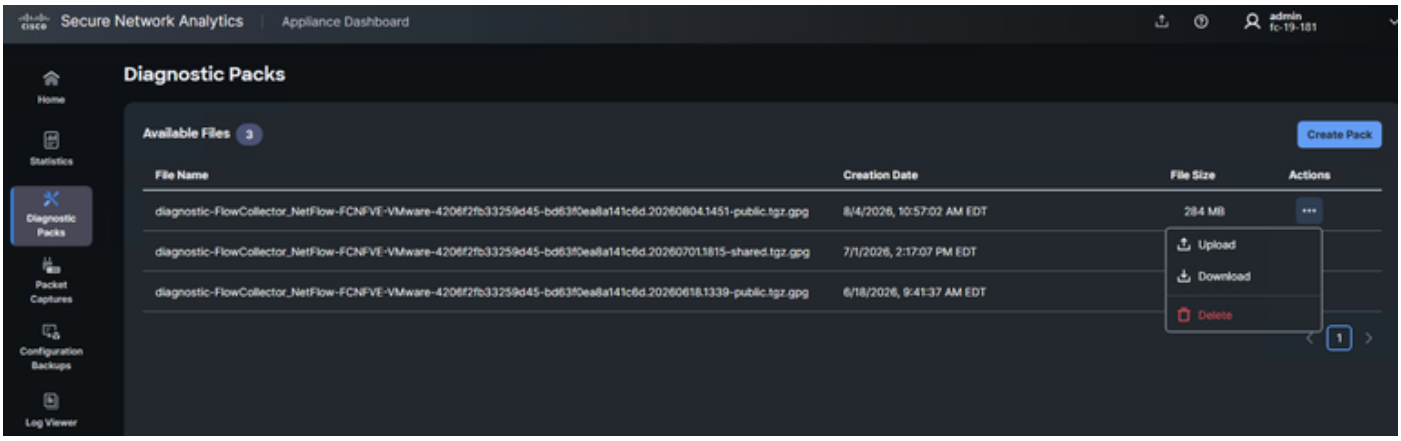


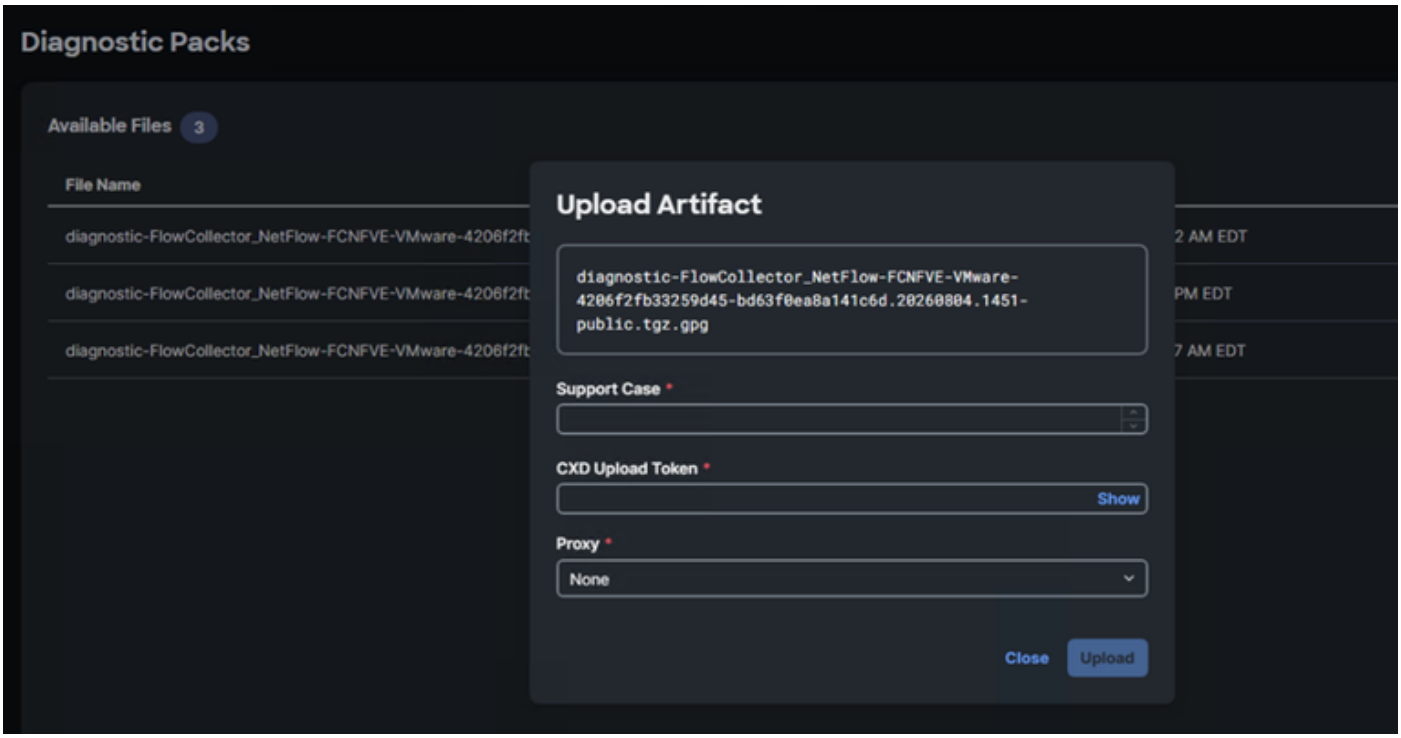
使用SNA Web UI中的上传令牌（7.6.1的新版本）

- 版本7.6.1的新增版本，您也不能从WebUI上传设备诊断包。
- 访问Central Manager Inventory页面。（配置 — >集中管理 — >资产）
- 在要为其上传诊断包的设备的Actions菜单下，选择“View Appliance Dashboard”（查看设备控制面板），然后选择要用于访问设备的接口（IPV4、IPV6或主机名）。 系统会自动通过一次性密码登录，并最终进入新的“设备控制面板”(Appliance Dashboard)页面。



您可以在此处访问相同的“上传”对话框





故障排除

本节提供可用于对生成诊断包的故障进行故障排除的信息。

对于方法3，出现错误“There was an error creating the diagnostics pack.如果存在权限错误或缺少特定目录，在设备的Admin UI中单击Create Diagnostics Pack按钮后，将显示“ no files are available ”。



更正此错误的步骤：

1. 通过SSH使用root凭证登录到具有此行为的设备。
2. 运行ls -l /lancope/var/database/dbs/hsqldb/admin/命令以验证目录的内容。

```
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
```

3. 确保备份子项直接存在，其用户/组所有者为tomcat。如果/lancope/var/database/dbs/hsqldb/admin/目录中不存在backup子目录，则必须创建该目录并分配正确的所有权。要创建此目录，请运行命**install -d -m 0755 -o tomcat -g tomcat /lancope/var/database/dbs/hsqldb/admin**令。

4. 运行ll /lancope/var/admin/命令以验证backups和diagnostics子目录是否存在，以及它们的用户/组所有者是否为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
```

5. 如果/lancope/var/admin/目录中不存在backups和diagnostics子目录，则必须使用相关命令创建这些子目录：

   mkdir /lancope/var/admin/backups

   mkdir /lancope/var/admin/diagnostics

6. 创建这些诊断包或验证它们存在后，请尝试再次生成SNA设备的诊断包。

相关信息

如需其他帮助，请联系思科技术支持中心(TAC)。联系时需要提供有效的支持合同：思科全球支持联系信息

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。