为安全访问支持团队排除故障并收集基本信息

目录

简介

本文档介绍与思科安全访问支持团队合作时需要收集的基本信息

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全访问
- 思科安全客户端
- 通过Wireshark和tcpdump捕获数据包

使用的组件

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

在使用Cisco Secure Access时，您可能会遇到一些问题，需要联系思科支持团队，或者希望对问题进行基本调查，然后尝试查看日志并解决问题。本文继续介绍如何收集与安全访问相关的基本故障排除日志。请注意，并非所有步骤都适用于每个场景。

找到安全访问组织ID

为了便于思科工程师找到您的帐户，请提供您的组织ID，在您登录到Secure Access Dashboard后可在URL中找到。

查找组织ID的步骤：

1. 登录sse.cisco.com
2. 如果您有多个组织，请切换到正确的组织。
3. 可以在以下模式的URL中找到组织ID：https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

思科安全客户端诊断和报告工具(DART)

Cisco Secure Client Diagnostic and Reporting Tool (DART)是随Secure Client软件包一起安装的工具，可帮助收集有关用户终端的重要信息。

DART捆绑包收集的信息示例：

- ZTNA日志
- 安全客户端日志和配置文件信息
-系统信息
- 其他安全客户端加载项或插件日志，安装在

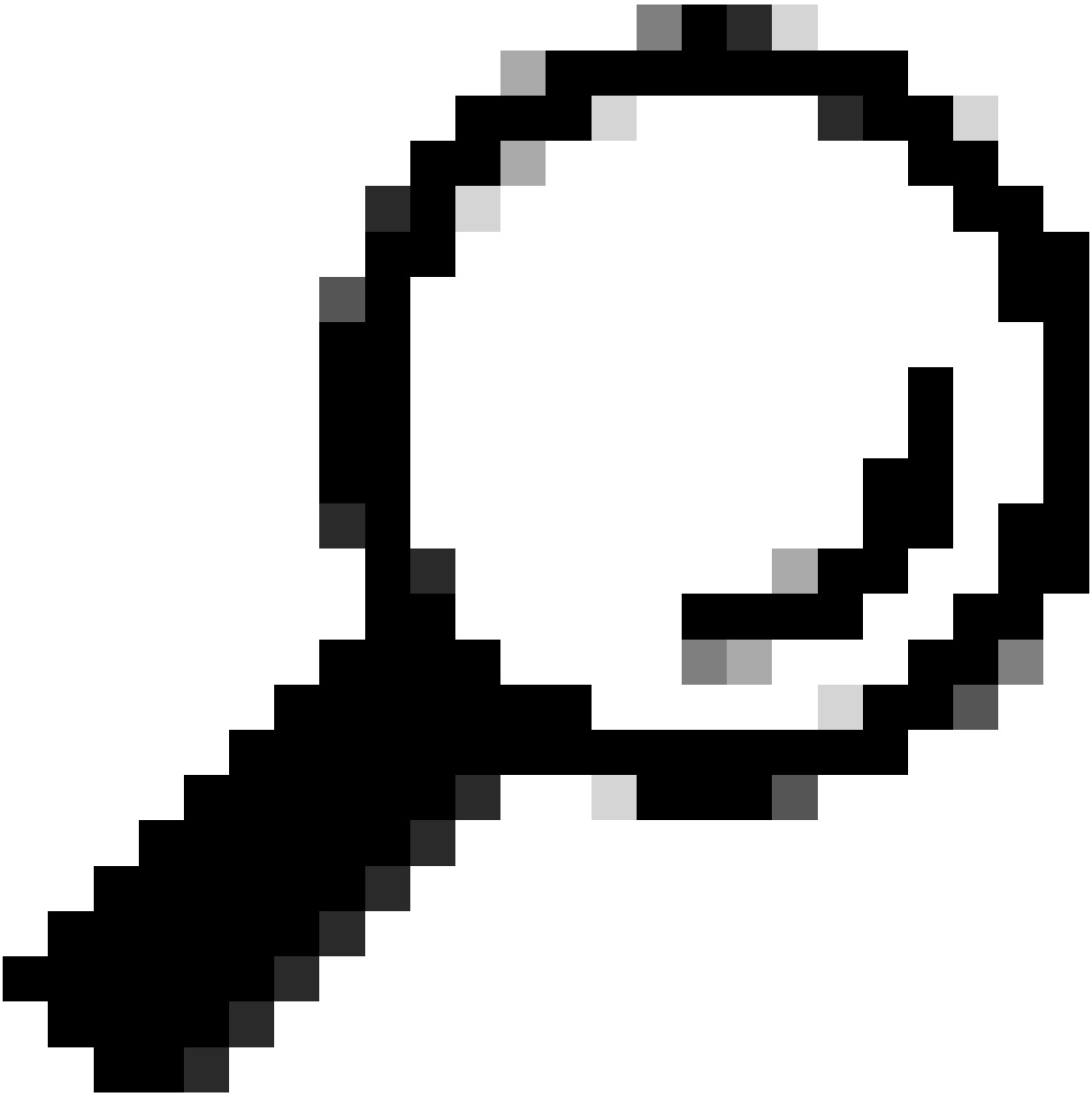
收集DART的说明：

步骤1:启动DART。

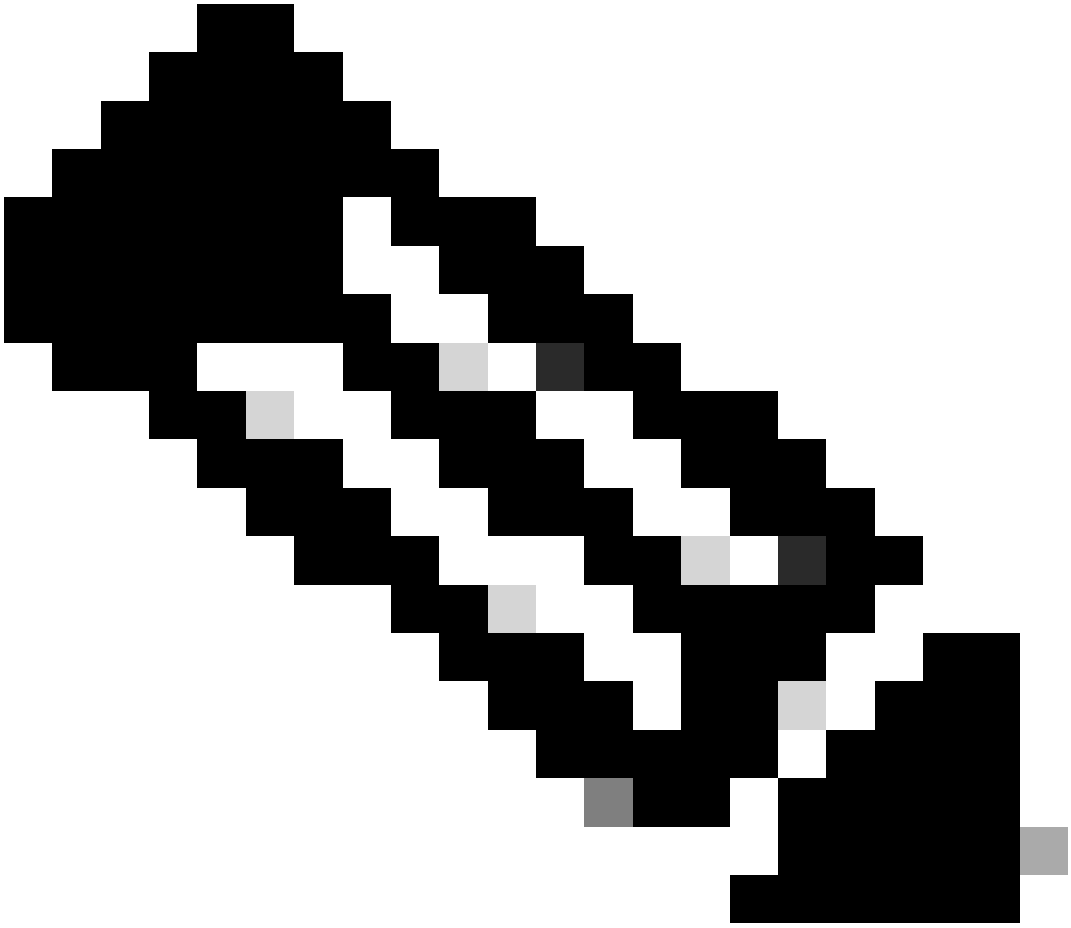
1. 对于Windows计算机，请启动Cisco安全客户端。
2. 对于Linux计算机，请选择 **Applications** > **Internet** > **Cisco DART**或/opt/cisco/anyconnect/dart/dartui。
3. 对于Mac计算机，请选择Applications > Cisco > Cisco DART。

第二步：点击Statistics选项卡，然后点击Details。

第三步：选择Default或Custom bundle creation。



提示：捆绑的默认名称是DARTBundle.zip，并保存到本地桌面。



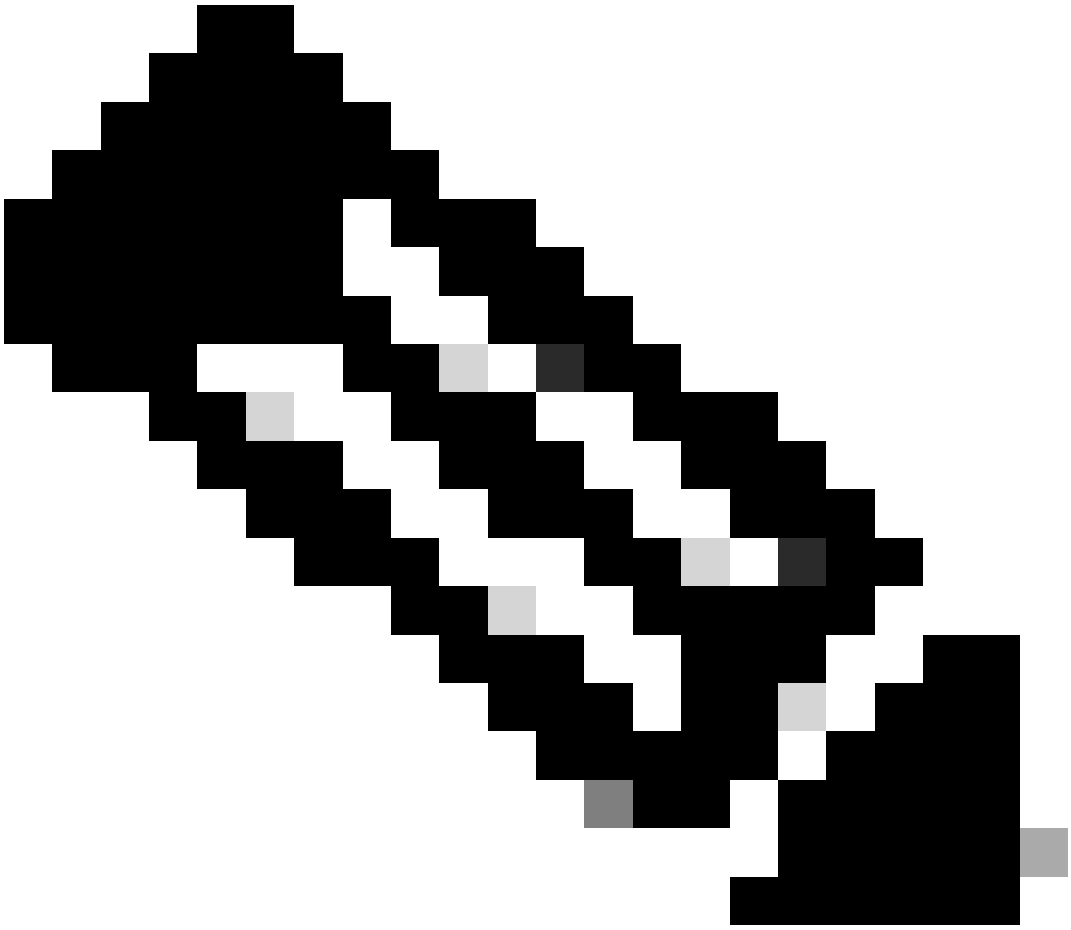
注意：如果选择默认，则DART开始创建捆绑包。如果选择自定义(Custom)，则继续向导提示指定日志、首选项文件、诊断信息和任何其他自定义项

HTTP存档(HAR)捕获

HAR可以从不同的浏览器收集。它提供多种信息，包括：

1. HTTPS请求的解密版本。
2. 有关错误消息、请求详细信息和报头的内部信息。
3. 计时和延迟信息
4. 有关基于浏览器的请求的其他其他信息。

要收集HAR捕获，请使用此来源中介绍的步骤：https://toolbox.googleapps.com/apps/har_analyzer/



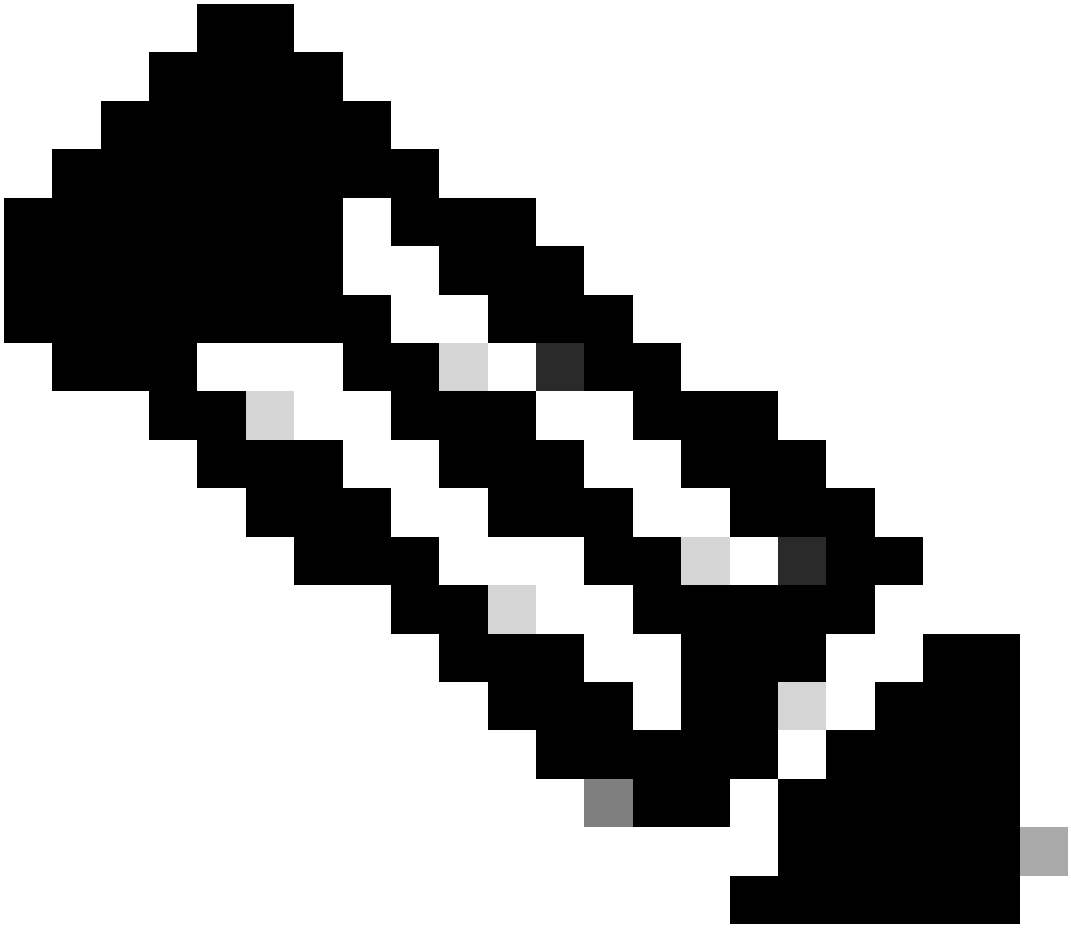
注意：您需要刷新浏览器会话才能收集正确的数据

数据包捕获

在检测到性能问题、数据包丢失或网络完全中断的情况下，数据包捕获非常有用。收集捕获的最常用工具是wireshark和 **tcpdump**。或收集设备内部的pcap文件格式的内置功能，例如思科防火墙或路由器。

要在终端上收集有用的数据包捕获，请确保包括：

1. 用于捕获通过安全客户端插件发送的流量的环回接口。
2. 数据包路径中涉及的所有其他接口。
3. 应用最小的过滤器，或者根本没有过滤器，以确保收集到所有数据。



注意：在网络设备上收集捕获时，请确保过滤流量的源和目标，并将捕获限制为仅针对相关端口和服务，以避免此活动导致的任何性能。

策略调试输出

策略调试输出是在受安全访问保护时通过用户浏览器发送的诊断输出。其中包括有关部署的关键信息。

1.

组织标识

2. 部署类型

3. 连接的代理

4. 公有和私有IP地址

5. 与交通来源有关的其他信息。

要运行策略测试结果，请从受保护的终端登录此链接：https://policy.test.sse.cisco.com/

如果您的浏览器中显示了证书错误消息，请确保您信任安全访问根证书。

要下载安全访问根证书，请执行以下操作：

导航至“安全访问” Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

将结果上传到思科支持服务请求

您可以通过以下步骤将文件上传到支持案例：

步骤1:登录到SCM。

第二步：要查看和编辑案例，请在列表中点击案例编号或案例标题。“案例摘要”(Case Summary)页面打开。

第三步：点击Add Files以选择文件并将其作为案例的附件上传。系统显示SCM文件上传工具。

第四步：在“选择要上传的文件”对话框中，拖动要上传的文件，或单击“内部”浏览本地计算机以查找要上传的文件。

第五步：添加说明并为所有文件或单独指定类别。

相关信息

- 思科技术支持和下载
- 安全访问文档和用户指南
- Cisco Secure Client软件下载

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）。