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

使用Cisco Secure Access时，可能会遇到需要联系思科支持团队的问题，或者希望对问题进行基本调查并尝试查看日志并忽略问题。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。

查找安全访问组织ID

为了让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.组织ID可在URL中按以下模式找到：https://dashboard.sse.cisco.com/org/{7_digit_org_id}/概述

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软件包安装的工具，可帮助收集有关用户终端的重要信息。

DART套件收集的信息示例：

- 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

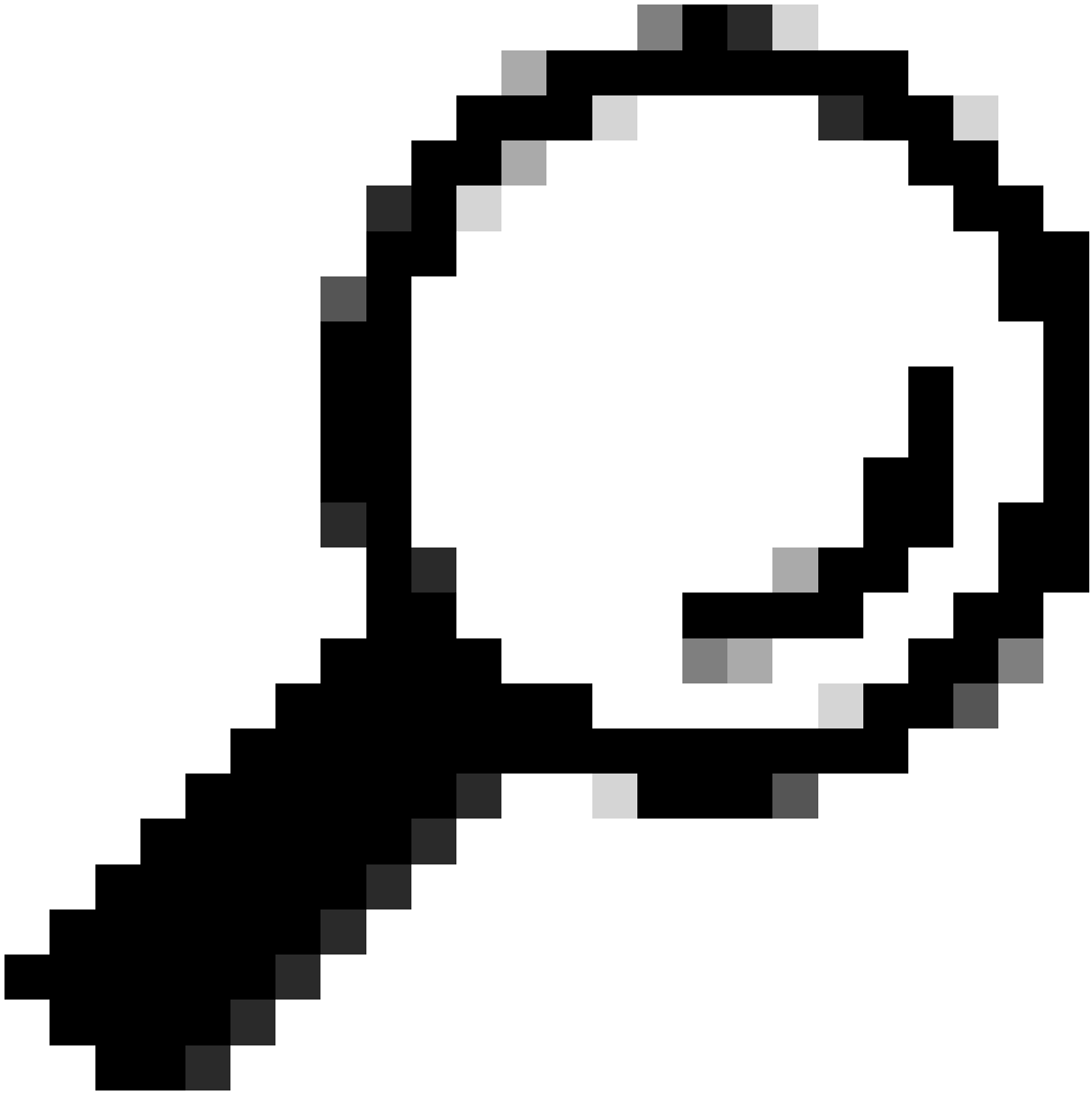
收集DART的说明：

步骤1.启动DART。

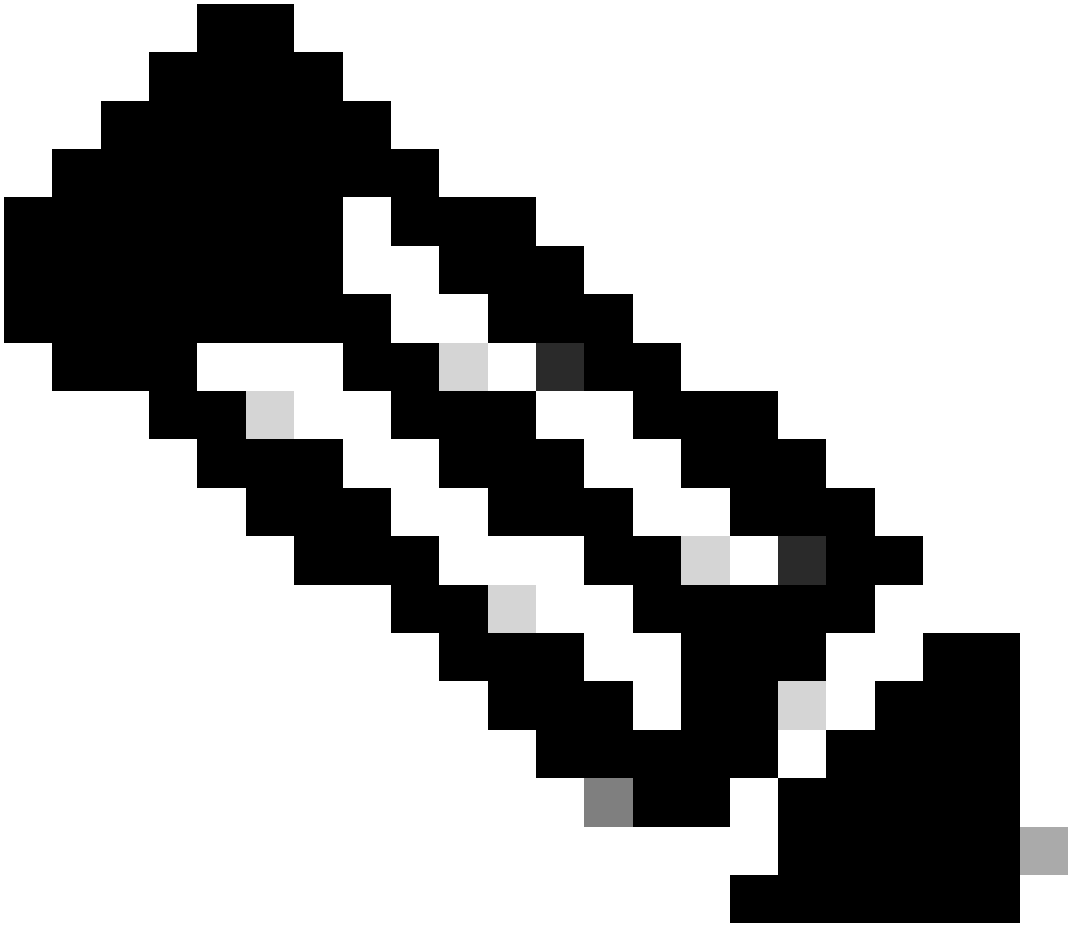
1.对于Windows计算机，请启动Cisco安全客户端。
2.对于Linux计算机，**Applications** > **Internet** > **Cisco DART**选择或/opt/cisco/anyconnect/dart/dartui。
3.对于Mac计算机，请选择Applications > Cisco > Cisco DART。

步骤2.单击Statistics选项卡，然后点击Details。

步骤3.选择Default或Custom bundle creation。



提示：捆绑包的默认名称为DARTBundle.zip，并保存到本地桌面。



注意：如果您选择“默认”，DART将开始创建捆绑包。如果选择自定义(Custom)，请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设置

启用ZTNA和SWG模块的调试日志

在某些情况下，支持团队需要启用跟踪或调试级别日志才能确定更复杂的问题。

完成本节中提供的步骤以启用每个模块的调试。

启用ZTNA的调试日志

步骤1.创建名为logconfig.json的json文件

步骤2.在文件中输入此文本

```
{ "global": "DBG_TRACE" }
```

步骤3.根据操作系统将文件放入正确的目录

- Windows 窗口版本:C:\ProgramData\Cisco\Cisco安全客户端\ZTA
- MacOS:/opt/cisco/secureclient/zta

步骤4.重新启动ZTNA模块或Cisco安全客户端，使日志生效。

启用SWG的调试日志

步骤1.创建名称为SWGConfigOverride.json的json文件

步骤2.在文件中输入此文本

```
{"logLevel": "1"}□
```

步骤3.根据操作系统将文件放入正确的目录

- Windows: C:\ProgramData\Cisco\Cisco安全Client\Umbrella\SWG\
- MacOS:/opt/cisco/secureclient/umbrella/swg

步骤4.重新启动SWG模块或Cisco安全客户端，使日志生效。

启用DUO的调试日志

启用DUO KDF日志（状态故障排除、注册问题）

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

禁用DUO KDF日志

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

收集ZTNA和SWG、DNS模块(Windows)的KDF日志

在某些情况下，支持团队需要收集kdf日志以确定更复杂的问题。

完成本节中提供的步骤以配置和收集kdf日志。

先决条件

需要安装DebugView才能正确收集日志。可以使用以下源安装该软件：https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

启用DNS注册表项

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

启用SWG注册表项

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

启用ZTNA注册表项

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

禁用所有标志

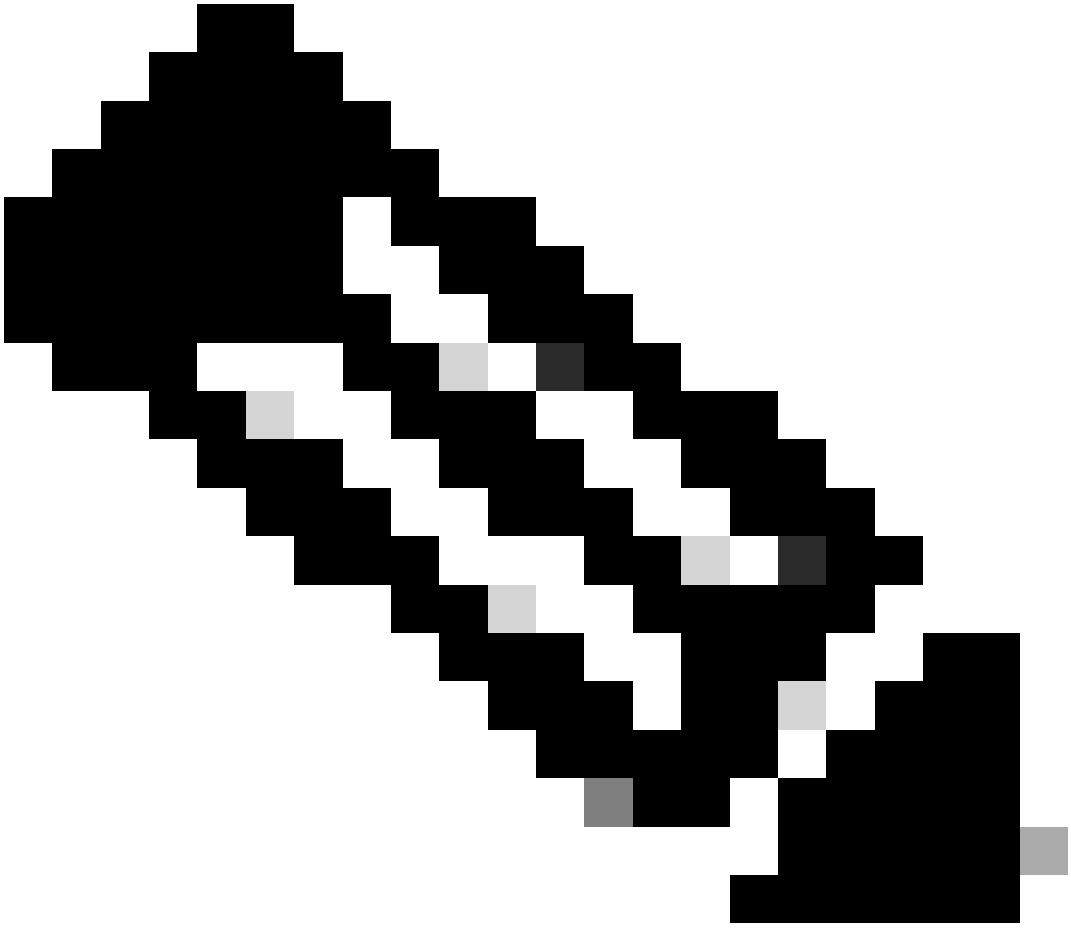
```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

HTTP存档(HAR)捕获

可以从不同的浏览器收集HAR。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，请使用以下来源中介绍的步骤：https://toolbox.googleapps.com/apps/har_analyzer/



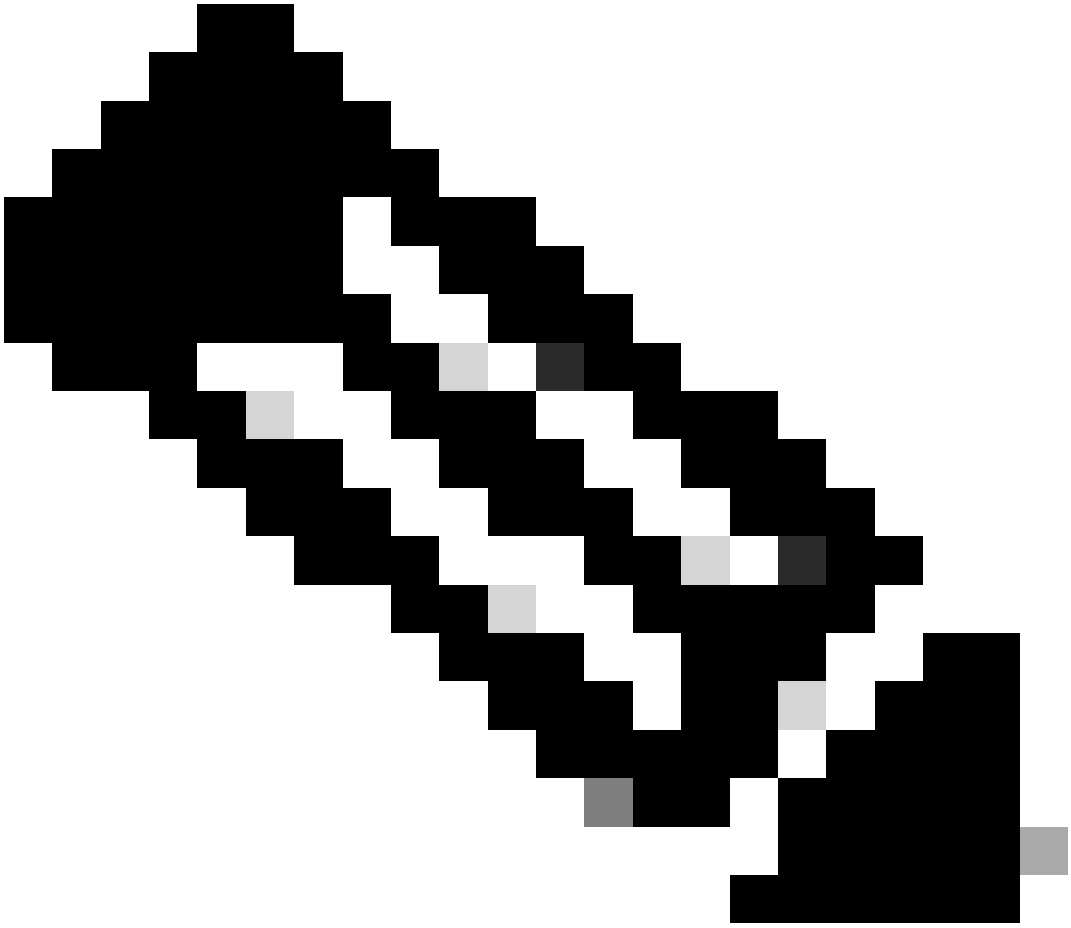
注意：您需要刷新浏览器会话以收集正确的数据

数据包捕获

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非常有用。收集捕获的最常见工具是wireshark和**tcpdump**。或者内置在设备内部收集pcap文件格式的功能，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.环回接口，用于捕获通过安全客户端插件发送的流量。
2.数据包路径中涉及的所有其他接口。
3.应用最低限度的过滤器，或根本没有过滤器，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，并将捕获限制为仅相关端口和服务，以避免此活动引起的任何性能。

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IP地址和私有IP地址
5.与流量来源相关的其他信息。

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/

如果浏览器中出现证书错误消息，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Secure Access Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

排除站点到站点隧道故障的常用命令

<#root>

 # Tunnel Establishment

```
asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session
```

#BGP Troubleshooting

```
asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors
```

#Routes Advertisements

```
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes
```

#Debug BGP events

```
asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing
```

#Disable Debugs

```
asa>undebug all
```

常用命令排除资源连接器故障

提供的列表提供了资源连接器的综合视图和安全访问支持团队的重要故障排除详细信息

<#root>

#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs

```
rc-cli> diagnostic
#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables

rc-cli> techsupport
#Packet captures

rc-cli> tcpdump <host>
```

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。

步骤2.要查看和编辑案例，请点击列表中的案例编号或案例标题。“案例摘要”(Case Summary)页面打开。

步骤3.点击Add Files以选择文件并将其作为附件上传到案例。系统显示SCM文件上传工具。

步骤4.在Choose Files to Upload对话框中，拖动要上传的文件，或点击内部以浏览本地计算机以查找要上传的文件。

步骤5.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
- 思科安全客户端软件下载

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）。