启用SWG模块的最大调试日志记录

目录

简介

本文档介绍如何在AnyConnect和思科安全客户端(CSC)的安全Web网关(SWG)模块上启用最大调试日志记录。

启用最大调试日志记录的用例

在排除以下故障时，在SWG模块上启用最大调试日志记录：

- 通过强制网络门户的热点问题
- 外部域旁路列表未应用
- 间歇性的DNS或Web性能问题

在AnyConnect 4.10 MR7、CSC 5.0 MR2或更早版本上启用最大调试日志记录

如果使用AnyConnect 4.10 MR7、CSC 5.0 MR2或较早版本，请执行以下步骤。默认情况下，未启用最大调试日志记录，且无法通过Umbrella控制面板或ASA进行配置。必须手动添"logLevel": "1"加到文orgConfig件中的对象SWGConfig.json。如果您使用的是最新版本的AnyConnect或Cisco Secure

Client，请跳过此部分。

SWGConfig.json的位置

- Windows(AnyConnect):

  ```
  C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\
  ```

- Windows（安全客户端）：

  ```
  C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
  ```

- macOS(AnyConnect):

  ```
  /opt/cisco/anyconnect/umbrella/swg/
  ```

- macOS（安全客户端）：

  ```
  /opt/cisco/secureclient/umbrella/swg/
  ```

使调试日志记录永久化

修改的文件仅保留到Cisco AnyConnect Umbrella模块进行下一个API同步为止SWGConfig.json。要保留此配置并防止API同步覆盖它，请在文件夹中部署一个swg_org_config.flagUmbrella/data文件。

1. 创建标志文件

   - **swg_org_config.flag** 在Umbrella Data文件夹中创建名为的新文件。文件扩展名必须是 .flag.

   - Windows(AnyConnect):

   - ```
     C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\data\swg_org_config.fl
     ```

   - Windows（安全客户端）：

   - ```
     C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\data\swg_org_config.flag
     ```

- macOS(AnyConnect):
- ```
  /opt/cisco/anyconnect/umbrella/data/swg_org_config.flag
  ```

- macOS（安全客户端）：
- ```
  /opt/cisco/secureclient/umbrella/data/swg_org_config.flag
  ```

2. 复制和修改内容

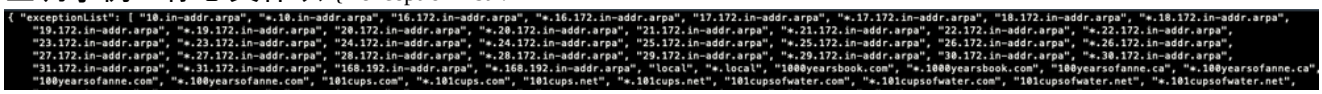
- 将对象的内容**orgConfig**，从文件SWGConfig.json，复制到文swg_org_config.flag件。
- 附加为"logLevel": "1"。
- 例如：

```
{
"exceptionList": [
"www.example.com",
"smh.com.au",
"*.smh.com.au",
"www.blue.com",
"*.www.blue.com",
"146.112.133.72"
// ...additional entries...
],
"failOpen": 1,
"logLevel": "1",
"swgAnycast": "146.112.255.50",
"swgDomain": "swg-url-proxy-https.sigproxy.qq.opendns.com",
"swgEchoService": "http://www.msftconnecttest.com/connecttest.txt"
}
```

- 确保标志文件以开头{ "exceptionList": [...]，以结尾为**"SWGEchoService": "http://www.msftconecttest.com/connecttest.txt"}**头。
- 避免在对象之前或之后复制多余的行。
- 错误地复制行(如identity、 deviceId或)可adUserID能中断SWG功能。

不正确示例：标志文件包含**identity**、 deviceId或dUserID 在

正确示例：标志文件以 { "exceptionList":



14970100184724

3. 重新启动服务

   - 重新启动Cisco AnyConnect安全移动代理/安全客户端服务，重新启动计算机，或者连接并断开VPN。

4. 验证配置

   - 在重新启动或VPN连接/断开连接后SWGConfig.json，打开文件以确认已设置SWG最大调试日志级别。配置后，此条目会出现在文件中：

```
"logLevel": "1"
```

验证并提供最大调试日志

Windows验证

1. 打开Windows事件查看器。
2. 查找与这些示例类似的日志行。这表示已成功启用最大调试日志记录。

   示例 1：

```
BRIDGE | Thread 1d18 | Connection : Resolved IP from 'swg-url-proxy-https.sigproxy.qq.opendns.com'
THREAD | Thread 1d18 | SetGUID '959bfe4d6fba87a65b433321c6748d761d9492cb'
```

   示例 2：会记录正在代理的所有Web请求。未记录根据内部/外部域列表绕过AnyConnect SWG的Web请求。

```
LISTEN | Thread 1d18 | Connection : Hostnames from KDF are login.live.com
```

3. 使用PowerShell命令将最大调试事件日志(.evtx)转换为txt:

```
Get-WinEvent -Path C:\Desktop\Umbrella.evtx | Format-Table -AutoSize | Out-File C:\Desktop\Umbrell
```

macOS验证

在Mac OSX上，可以通过此命令查看调试日志记录（您可以用grep或txt编写它们）。

1. 运行以下命令：

```
>log show --predicate 'subsystem contains "com.cisco.anyconnect.swg" || senderImagePath endswith "
```

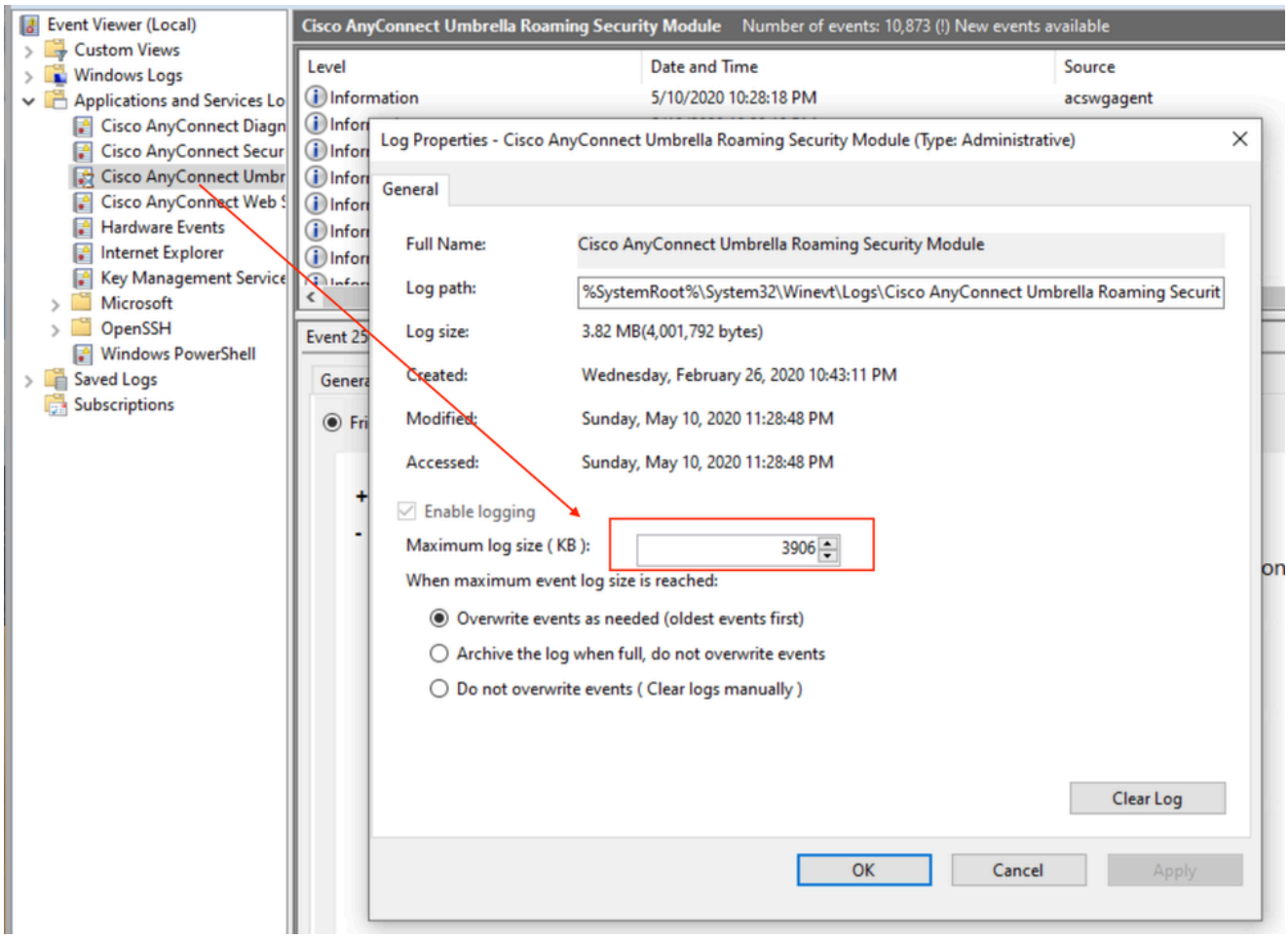
   - 启用最大调试日志记录时浏览purple.com时的输出示例：

```
2022-09-19 10:51:15.627229+1000 0x16b121 Default 0x0 98970 0 acswgagent: Connection : Hostna
```

2. AnyConnect DART捆绑包包括最大调试日志。验证启用后，重新创建问题，记录时间戳、用户体验和涉及的域，并提供此信息以及DART捆绑包以提供支持。

其他说明

- 最大调试日志记录会生成详细日志。在Windows事件查看器中配置Umbrella漫游安全模块日志大小，以适应大型日志，特别是间歇性问题。



360056784112

- 在故障排除完成swg_org_config.flag时，删除或重命名文件以禁用最大调试日志记录。

在CSC 5.0 MR3和AC 4.10 MR8或更高版本上启用最大调试日志记录

概述

从CSC 5.0 MR3和AC 4.10 MR8开始，debug logging enablement使用更简单的过程。

更改

- 将文件SWGConfigOverride.json（包含静态内容）复制到SWG文件夹以启用调试日志记录。
- 无需从复制或修改orgConfigSWGConfig.json。此文件的内容不会将“组织”更改为“组织”。
- 不依赖于DNS模块来执行配置同步或从标志文件读取。文件SWGConfig.json保持不变。

启用调试日志记录

中的配置值优先于中的值（如果存在），只能包含和覆盖两个配置 — logLevel（用于启用/禁用调试日志记录）和自动调**SWGConfigOverride.json**整(用于启用/禁用发送缓冲区自动调SWGConfig.json. The **SWGConfigOverride.json** 整)。

1. 要启用调试日志记录，请SWGConfigOverride.json复制以下内容：

```
{"logLevel": "1"}
```

- 要同时启用调试日志记录和自动调整，请使用：

```
{"logLevel": "1", "autotuning": "1"}
```

2. 放**SWGConfigOverride.json**入SWG文件夹：

- Windows(AnyConnect):
  `C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Umbrella\SWG\`
- Windows（安全客户端）：
  `C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\`
- macOS(AnyConnect):
  `/opt/cisco/anyconnect/umbrella/swg/`
- macOS（安全客户端）：
  `/opt/cisco/secureclient/umbrella/swg/`

3. 重新启动SWG或Umbrella服务，或重新启动系统。

- macOS:停止并启动AnyConnect或安全客户端代理。
- Windows 窗口版本:通过Services MMC管理单元(“开始”>“运行”>“Services.msc”)重新启动或停止/启动安全Web网关（4.10.x版中的acswgagent在5.x版中生成/csc_swgagent）服务。

注意：仍然支持启用调试日志记录的旧方法，并且仍然可以遵循该方法，并且是5.0 MR3或4.10 MR8之前的客户端的唯一选项。

配置和操作说明

- 文件SWGConfig.json（区分大小写）。使用"logLevel": "1"，使用双引号。
- 值logLevel是字符串1，而不是整数，因此它必须是带双引号的“1”。
- 文件swg_org_config.flag，必须具有.flag扩展名，不.txt能。
- 最大调试日志记录会生成非常详细的日志。仅当由Umbrella支持工程师请求时，启用最大调试日志记录。
- 文件swg_org_config.flag包含绕过的域的静态列表，并且不与控制面板(Dashboard)>部署(Deployments)>域管理(Domain Management)中列出的外部域同步。

相关信息

- 思科技术支持和下载
- 思科安全访问帮助中心
- Cisco SASE设计指南

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）。