

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[Enable \(event\) NAM记录](#)

[配置NAM数据包捕获](#)

[记录集](#)

[读NAM日志](#)

[记录网络连接的摘要，不用802.1x启用的验证](#)

[使用802.1x和PEAP在有线网络，记录网络连接的摘要](#)

简介

本文描述如何启用AnyConnect网络访问管理器(NAM)记录日志以及收集和解释日志。在本文包括的示例描述反射网络访问管理器采取的步骤验证客户端的不同的验证方案和日志。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

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。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

启用NAM记录

如果可能与NAM模块涉及的问题识别，第一步将启用延长的操作日志功能。当NAM模块运行时，在客户端终端必须执行这。

步骤1.打开AnyConnect窗口并且确保它在重点。

步骤2.按此密钥组合，**左岸堤防班次+留下艾尔特+ L**。没有无响应。

步骤3.在AnyConnect图标的右键单击在Windows系统托盘。菜单冒出。

步骤4.选择**延长记录**，因此安排一个复选标记显示。被选派的NAM日志当前调试消息。

配置NAM数据包捕获

当延长的记录日志启用时，NAM也保持一数据包捕获缓冲区去。缓冲区默认情况下对1MB大约被限制。如果数据包捕获是需要的，增加缓冲区大小也许是有利的，因此捕获更多活动。要扩大缓冲区，必须手工修改XML设置文件。

步骤1:在Windows PC，请浏览对：

C:\ProgramData\Cisco\Cisco AnyConnect安全移动性客户端\网络访问管理器\系统\

步骤2.打开文件internalConfiguration.xml。

步骤3.找出XML标记<packetCaptureFileSize>1</packetCaptureFileSize>并且调整值到10 10MB缓冲区大小的，等等。

步骤4.重新启动客户端PC使更改生效。

记录集

NAM日志集通过诊断和报告工具(箭)完成，是AnyConnect套件模块。在安装程序中，请选择模块并且请使用AnnyConnect全双工安装ISO安装。Cisco媒介服务接口(MSI)安装程序可能也被找到在ISO里面。

在您启用延长的记录日志并且执行测验，运行箭并且通过对话后，默认情况下日志套件在Windows桌面查找。

除箭套件之外，NAM消息日志也是有用找出在NAM日志的相关数据。为了查找NAM消息日志，请导航对**Settings**窗口的**AnyConnect >网络访问Manager>消息历史记录**。消息日志包含每个网络连接事件时间戳，可以用于发现日志相关与事件。

读NAM日志

NAM日志，特别是在您启用延长的记录日志后，包含很多数据，多数是毫不相关的，并且可以忽略。此部分列出调试线路展示每个步骤NAM采取建立网络连接。当您通过日志时工作，这些关键短语可能是有用设置一部分的日志与问题有关。

记录网络连接的摘要，不用802.1x启用的验证

说明：这表明用户选择从NAM模块的网络，并且NAM接收userEvent开始。

说明：访问状态机和网络状况系统开始。

说明：IPv4实例获得已取消为了重置状态。

说明：有ID的**484E4FEF-392C-436F-97F0-CD7206CD7D48**适配器选择连接到网络**test123**，是在NAM配置的网络连接名称。

说明：NAM顺利地从事此网络的适配器。现在NAM设法联合(连接)到偶然是无线的此网络(：

说明：**openNoEncryption**表明网络配置如开放。在无线局域网控制器上它使用MAC验证旁路(MAB)验证。

说明：电缆敷设船在NAM日志能被看到很多。这些是毫不相关的日志，并且应该忽略。

说明：这些是用于的简单对象访问协议(SOAP)消息告诉AnyConnect GUI显示连接状态消息例如在这种情况下**关联**。在NAM窗口显示的所有错误消息可以在其中一个在可以用于容易地找出问题的日志的SOAP消息找到。

说明：NAM接收AUTH_SUCCESS事件，误导，因为没有当前发生的验证。您是获得此事件，因为您连接对开放式网络，那么默认情况下验证是成功的。

说明：服务集标识(SSID)的关联是成功的，计时处理验证。

说明：因为这是开放式网络，默认情况下验证。这时，NAM连接对网络和当前开始DHCP过程：

说明：NAM成功地获取一个IP地址。

说明：一旦IP地址接收NAM将发送ARP (地址解析协议**连接**)。一旦ARP响应接收客户端连接。

使用802.1x和PEAP在有线网络，记录网络连接的摘要

说明：开始的NAM连接到网络WiredPEAP。

说明：NAM匹配适配器对此网络。

说明：NAM开始的连接对此有线网络。

说明：客户端发送EAPOL_START。

说明：客户端收到从交换机的标识请求，它当前寻找凭证退还。

说明：默认情况下，Anyconnect发送**匿名**作为无保护的标识(**outter标识**)，那么此处它尝试**匿名**并且看到服务器是否对它是好的。事实标识是**匿名的与主机/匿名相对**表明它是用户认证，而不是计算机验证。

说明：RADIUS服务器发送扩展验证传输层安全(EAP-TLS)帧，不用任何内容。其目的将协商与客户端的EAP-TLS协议。

说明：NAM认可服务器的请求使用EAP-TLS，但是客户端配置使用Protected Extensible Authentication Protocol (PEAP)。这是原因NAM退还PEAP的一个还价。

说明：RADIUS服务器接受outter/无保护的标识。

说明：PEAP的**已保护**部分(设立安全隧道交换内在凭证)开始，在客户端接收从RADIUS服务器的确认继续使用PEAP后。

说明：NAM发送客户端在EAP信息封装的Hello并且等待服务器问候来。服务器问候包含ISE证书，因此采取一些时间完成转接。

说明：NAM解压缩ISE服务器的主题名称从服务器证书的。因为它没有在信任存储安装的服务器证书，您没找到它那里。

说明：在通道设立后，NAM寻找**内在/保护**将发送的标识对RADIUS服务器。在这种情况下，“**请自动地请使用我的Windows登录名字，并且密码**”选项在有线的适配器启用，因此NAM使用windows登

录凭证而不是询问用户它。

说明：NAM发送客户端密钥和密码器spec到服务器并且接收确认。SSL协商是成功的，并且通道设立。

说明：已保护标识发送到服务器，接受标识。现在服务器请求密码。

说明：NAM接收密码请求和发送密码对服务器。

说明：服务器接收密码，验证它并且发送EAP成功。验证这时是成功的，并且客户端继续作为它从DHCP获得IP地址。