

AnyConnect版本4.0和NAC状态代理程序在ISE不冒出排除指南故障

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[故障排除方法](#)

[什么做代理程序冒出？](#)

[可能的原因](#)

[重定向不发生](#)

[属性在网络设备上没有安装](#)

[属性到位，但是网络设备不重定向](#)

[干涉的可下载的访问列表\(DACL\)](#)

[坏NAC代理程序版本](#)

[HTTP Web代理由客户端是在使用中的](#)

[发现主机在NAC代理程序被配置](#)

[NAC代理程序有时不冒出](#)

[反向问题：代理程序重复冒出](#)

[Related Information](#)

Introduction

身份服务引擎(ISE)提供要求使用网络准入控制(NAC)代理程序的摆姿势的功能(微软视窗，Macintosh，或者通过webagent)或AnyConnect版本4.0。因此AnyConnect版本4.0 ISE状态模块工作就象NAC代理程序和被称为在本文的NAC代理程序。状态故障的常见的症状客户端的是NAC代理程序不冒出，因为一个工作的方案总是造成NAC代理窗口冒出和分析您的PC。本文帮助您缩小可以导致状态发生故障，意味着的许多原因NAC代理程序不冒出。没有被认为是详尽的，因为NAC代理程序日志可能由Cisco技术支持中心(TAC)只解码，并且可能的根本原因是许多;然而它打算澄清情况和进一步精确定位问题“代理程序比不冒出与状态分析”并且很可能您解决多数常见原因的帮助。

Prerequisites

Requirements

在初始建立已经完成后，在本文列出的方案、症状和步骤被写为了您能排除问题故障。关于初始配置，请参见[在Cisco ISE配置指南的状态服务](#)在Cisco.com。

Components Used

本文档中的信息基于以下软件和硬件版本：

- ISE Version 1.2.x
- ISE版本4.9.x的NAC代理程序
- AnyConnect版本4.0

Note:除非版本注释指示主要性能上的更改，信息应该也是可适用的对ISE其他版本。

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

故障排除方法

什么做代理程序冒出？

当发现一个ISE节点时，代理程序冒出。如果代理程序感觉没有充分的网络访问并且在状态重定向方案，经常寻找一个ISE节点。

有解释代理程序发现进程的详细资料的Cisco.com文件：[网络准入控制\(NAC\)身份服务引擎的代理程序发现进程](#)。为了避免内容复制，本文只讨论关键点。

当客户端连接时，它经过RADIUS认证(MAC过滤或802.1x)在结束时，ISE返回重定向访问控制表(ACL)和重定向URL到网络设备(交换机，可适应的安全工具(ASA)，或者无线控制器)为了限制客户端的流量只允许它获得IP地址和域名服务器(DNS)解决方法。来自以CPP结束的客户端的所有HTTP数据流重定向对在ISE的唯一URL(客户端状态和设置)，除了数据流被注定对ISE门户。NAC代理程序发送一个正常HTTP GET信息包到默认网关。如果代理程序比CPP重定向不接受答案或任何其他答案，考虑自己有全连接，并且不继续进行摆姿势。如果它接受是重定向对CPP URL在一个特定ISE节点结束时的一种HTTP回应，则继续状态进程和联系该ISE节点。当从该ISE节点时，成功接受状态详细资料它只冒出并且开始分析。

NAC代理程序也提供援助对被配置地发现主机IP地址(不期望超过一个配置)。它期望重定向那里为了获得与会话ID的重定向URL。如果发现IP地址是ISE节点，则不继续处理，因为等待重定向为了获得正确的会话ID。不因此发现主机通常是需要的，但是可以是有用，当设置作为所有IP地址在重定向ACL范围内为了触发重定向例如(类似在VPN方案)。

可能的原因

重定向不发生

这显然是多数常见原因。为了验证或无效，打开在代理程序不冒出并且看到的PC的一个浏览器是否重定向对状态代理程序下载页，当您键入所有URL时。您能也键入一个随机的IP地址例如<http://1.2.3.4>为了避免一个可能的DNS问题(如果IP地址重定向，但是网站名字不，您能查看DNS)。

如果重新定向，您应该收集代理程序日志和ISE支持套件(以调试模式的状态和瑞士模块)和与Cisco TAC联系。这表明代理程序发现一个ISE节点，但是某事不在进程中能得到状态数据。

如果重定向不发生，您有您的最初原因，仍然需要对根本原因的进一步调查。一个好开始是检查在网络接入设备(无线局域网控制器(WLC)或交换机)的配置和移动向在本文的下一个项目。

属性在网络设备上没有安装

此问题是**重定向的subcase不发生**方案。如果重定向不发生，第一件事是验证(因为问题在一个特定客户端发生)客户端在正确的状态正确地安置由交换机或无线访问层。

这是在客户端被联络的交换机(您也许必须添加**详细资料**在一些平台的末端)采取的输出示例的 **<interface number> detail命令**。您必须验证状态是“Authz成功”，URL重定向ACL正确指向打算的重定向ACL，并且URL重定向指向与**CPP**的期望的ISE节点在URL结束时。ACS ACL字段不是必须的，因为只显示是否配置了在授权配置文件的一可下载的访问列表在ISE。查看它和验证是，然而，重要的没有与重定向ACL的冲突(请在疑惑的情况下请参阅关于状态配置的文件)。

```
01-SW3750-access#show access-sess gi1/0/12 det
Interface: GigabitEthernet1/0/12
MAC Address: 000f.b049.5c4b
    IP Address: 192.168.33.201
    User-Name: 00-0F-B0-49-5C-4B
    Status: Authz Success
    Domain: DATA
Security Policy: Should Secure
Security Status: Unsecure
Oper host mode: single-host
Oper control dir: both
Authorized By: Authentication Server
Vlan Policy: N/A
ACS ACL: xACSACLx-IP-myDAACL-51519b43
URL Redirect ACL: redirect
URL Redirect: https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cpp
Session timeout: N/A
Idle timeout: N/A
Common Session ID: C0A82102000002D8489E0E84
Acct Session ID: 0x000002FA
Handle: 0xF60002D9
```

Runnable methods list:

Method	State
mab	Authc Success

为了排除WLC故障运行的AireOS，请进入**显示无线客户端详细资料< MAC地址>**并且进入**显示无线客户端MAC地址<运行Cisco IOS XE的MAC地址>详细资料**为了排除WLC故障。相似数据显示和您必须验证重定向URL和ACL，并且，如果客户端是在“POSTURE_REQD”状态或类似(它根据软件版本变化)。

如果属性不存在，您必须打开在您在结果部分排除故障客户端的ISE的认证详细资料(请连接对**操作>认证**)和验证发送了重定向属性。如果未发送他们，您应该查看授权策略为了知道属性为什么未为此特定的客户端返回。很可能一条件没有配比，因此它是一个好想法逐个排除他们故障。

关于重定向ACL切记，在许可证语句的Cisco IOS重定向(如此ISE和DNS IP地址需要被拒绝)，当在WLC重定向的AireOS在Deny语句时(为ISE和DNS如此允许)。

属性到位，但是网络设备不重定向

专业原因在这种情况下是配置问题。您应该查看网络设备的配置配置指南和在Cisco.com的配置示例。如果这是实际情形，问题典型地存在所有端口或接入点(APs)中网络设备。否则，问题在一些连接孔或某个APs也许只发生。如果这是实际情形，您应该比较那些的配置问题发生与状态良好工作的端口或APs的地方比较。

FlexConnect APs是敏感的，因为他们能其中每一有独特配置，并且是容易犯在ACL或VLAN的一个

错误在某个APs而不是其他。

另一常见问题是客户端VLAN没有一SVI。这在[ISE在Catalyst 3750 Series Switch的数据流重定向](#)只适用于交换机和详细讨论。一切也许看起来好从属性方面。

干涉的可下载访问列表(DACL)

如果，在重定向属性，您推进一个无线控制器的DAACL回到交换机(或Airespace ACL)的同时，则可能阻拦您的重定向。首先适用DAACL并且确定什么完全地下降，并且什么继续被处理。然后重定向ACL适用并且确定什么重定向。

什么这具体地意味着大多时间是那，您将要允许所有HTTP和HTTPS流量在您的DAACL。如果阻拦它，不会重定向，因为以前将下降那。它不是安全性问题，因为该数据流主要在重定向ACL将重定向以后，因此在网络确实不允许;然而，您需要允许在DAACL的那两种流量类型为了他们能有机会击中重定向ACL在之后。

坏NAC代理程序版本

忘记是容易的特定NAC代理程序版本被验证ISE的特定版本。许多管理员升级他们的ISE簇并且忘记加载在客户端设置结果数据库的相关NAC代理程序版本。

如果使用一个过时的NAC代理程序版本您的ISE代码，请注意也许工作，但是也不可能。并不奇怪因此一些客户端工作，并且其他不。一种方式验证是NAC代理程序版本在那里的去您的ISE版本的Cisco.com下载部分和检查。典型地有为每个ISE版本支持的数。此网页采集所有矩阵：[Cisco ISE兼容性信息](#)。

HTTP Web代理由客户端是在使用中的

HTTP Web代理的概念是客户端不解决网站DNS IP地址亦不直接地与网站联系;相反，他们发送他们的请求到代理服务器，照料它。通常的配置的典型的问题是客户端通过直接发送它的HTTP GET解决一个网站(例如[www.cisco.com](#))到代理，获得拦截和正当地重定向对ISE门户。然而，而不是然后发送下HTTP GET到ISE门户IP地址，客户端继续发送该请求到代理。

万一决定不重定向HTTP数据流被注定对代理，您的用户有直接访问到整个互联网(因为所有数据流通过代理)，无需验证或摆姿势。解决方案将实际修改客户端的浏览器设置和添加ISE IP地址的例外在代理设置。这样，当客户端必须到达ISE时，它发送请求直接地到ISE和不到代理。这避免客户端经常重新定向，但是从未看到登录页的死循环。

注意NAC代理程序没有影响的是受在系统输入的代理设置的，并且继续通常操作。这意味着，如果使用一个Web代理，您不能有NAC代理程序发现工作(因为使用端口80)和有用户自安装代理程序，一旦他们重定向对状态页，当他们访问时(因为该使用代理端口，并且典型的交换机在多个端口不能重定向)。

发现主机在NAC代理程序被配置

特别是在ISE版本1.2以后，推荐不配置在NAC代理程序的任何发现主机，除非有在什么的专业技术执行和不执行。NAC代理程序应该发现通过HTTP发现验证客户端设备的ISE节点。如果取决于发现主机，您比验证设备，并且不工作的那个也许安排NAC代理程序与另一个ISE节点联系。ISE版本1.2拒绝通过发现主机进程发现节点的代理程序，因为希望NAC代理程序从重定向URL获得会话ID，因此此方法被劝阻。

有时，您也许要配置发现主机。然后应该配置有它将由重定向ACL重定向的所有IP地址(即使非存在)，并且不应该理想地说在相同子网作为客户端(否则客户端为它无限地ARP和从未发送HTTP发现信息包)。

NAC代理程序有时不冒出

当问题是更加断断续续的时，并且动作例如电缆/wifi连接的拔掉/再插上使它工作，它是一个更加细微的问题。它可能是会话ID在ISE被删除的RADIUS会话ID的一个问题通过RADIUS认为(看到功能失效的记帐是否更改某事)。

如果使用ISE Version1.2，另一种可能性是客户端发送许多HTTP信息包，以便什么都不来自浏览器或NAC代理程序。ISE版本1.2扫描在HTTP信息包的代理程序字段发现是否来自NAC代理程序或浏览器，但是许多其他应用程序发送与代理程序字段的HTTP数据流，并且不提及任何操作系统或有用的信息。ISE版本1.2然后发送授权的更改断开客户端。以不同的方式运作的ISE版本1.3没有影响的是受此问题beause的。解决方案将升级到版本1.3或允许在重定向ACL的所有被发现的应用程序，以便他们没有重定向往ISE。

反向问题：代理程序重复冒出

相反的问题能出现代理程序冒出，执行状态分析，验证客户端，再然后冒出之后的地方而不是允许网络连通性和坚持静音。因为，在一个成功的状态以后，HTTP数据流仍然重定向到ISE的，CPP门户这发生。它是一个好想法然后通过ISE授权策略和检查您有发送一次许可证访问的一个规则(或与可能的ACL和VLAN的相似的规则)，当再看到一个兼容客户端而不是CPP重定向时。

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
	User is compliant	if Session:PostureStatus EQUALS Compliant	then PermitAccess

Related Information

- [在Cisco ISE配置指南的状态服务](#)
- [NAC ISE的代理程序发现进程](#)
- [ISE在Catalyst 3750 Series Switch的数据流重定向](#)
- [Technical Support & Documentation - Cisco Systems](#)