

对mus.cisco.com的AnyConnect DNS查询进行故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题](#)

[解决方案 1](#)

[解决方案 2](#)

[AnyConnect查询mus.cisco.com](#)

[配置](#)

[网络图](#)

[故障排除](#)

简介

本文档介绍Anyconnect VPN核心模块在特定情况下查询完全限定域名(FQDN)mus.cisco.com时的行为。当AnyConnect客户端尝试确定终端是否具有互联网访问并且没有VPN正在使用时，会发生此查询。

作者：Peter Giang，思科业务部。

作者：Steve Sargent，思科BU技术主管。

先决条件

要求

Cisco 建议您了解以下主题：

- AnyConnect模块安装。
- 创建AnyConnect诊断和报告工具(DART)捆绑包。
- Wireshark嗅探器捕获。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Anyconnect核心VPN模块版本4.8.03052

- Windows 10企业版10.0.18363版18363

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。

本文档也可用于以下硬件和软件版本：

- 任何操作系统(MacOS、Windows、Linux)。
- 4.10之前的任何AnyConnect版本。

背景信息

设计时需要向mus.cisco.com查询AnyConnect。

 注：此行为存在增强缺陷。思科漏洞ID [CSCvu39643](#)。如果未使用VPN模块，则不能执行从VPN核心到mus.cisco.com的查询。

问题

当AnyConnect VPN核心模块未使用时（没有为VPN连接配置XML配置文件），每15秒生成对mus.cisco.com的查询。

解决方案 1

在DNS服务器上添加域名系统(DNS)条目，以将域名查询解析为mus.cisco.com。如果不管理DNS服务器，请将此类请求转发到公共DNS服务器。

一旦能够解析mus.cisco.com FQDN，AnyConnect将停止查询尝试。

解决方案 2

将DNS条目添加到操作系统(OS)主机文件，以解析FQDN mus.cisco.com。

Windows 窗口版本

1. 按Windows键。
2. 在搜索字段中键入记事本。
3. 在搜索结果中，右键单击记事本，然后选择以管理员身份运行。
4. 从记事本打开文件：“C:\Windows\System32\Drivers\etc\hosts”。
5. 对文件进行必要的更改。
6. 选择File > Save以保存更改。

MAC

1. 打开Terminal窗口。
2. 输入此命令以打开hosts文件，其中nano文本编辑器嵌入在OS中：“sudo nano /etc/hosts”。

3. 输入您的域用户和密码。
4. 对文件进行必要更改。

Linux

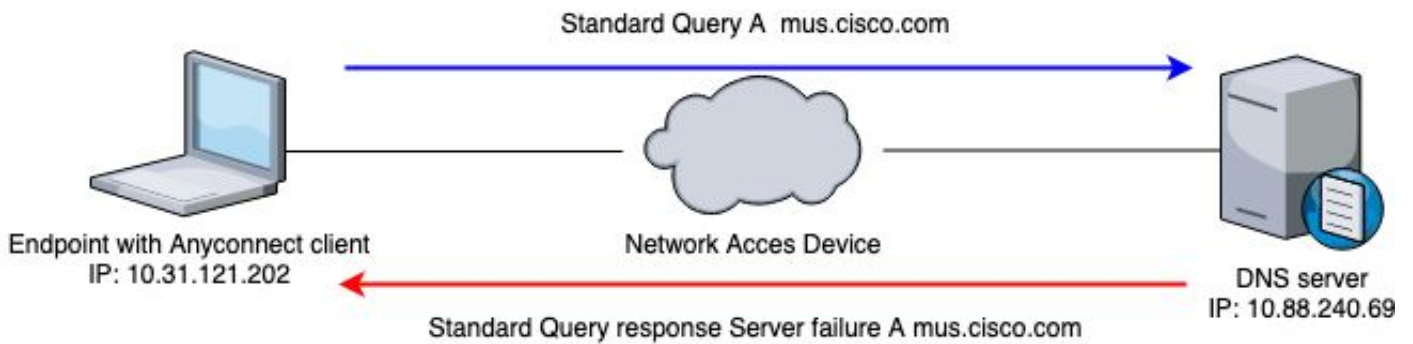
1. 打开Terminal窗口。
2. 输入此命令以打开hosts文件，其中nano文本编辑器嵌入在OS中：“sudo nano /etc/hosts”。
3. 输入您的域用户和密码。
4. 对文件进行必要更改。

AnyConnect查询mus.cisco.com

配置

AnyConnect VPN核心模块的安装。

网络图



```

*****
Date : 06/17/2020
Time : 20:21:57
Type : Warning
Source : acvpnagent
Description : Function : CDNSRequest::OnSocketReadComplete
File: c:\temp\build\thehoff\negasonic_mr30.297045120452\negasonic_mr3\vpn\common\ip\dnsrequest.cpp
Line: 1147
Timeout (per request) while trying to resolve [A] query mus.cisco.com via DNS server 10.88.240.69 (time
*****

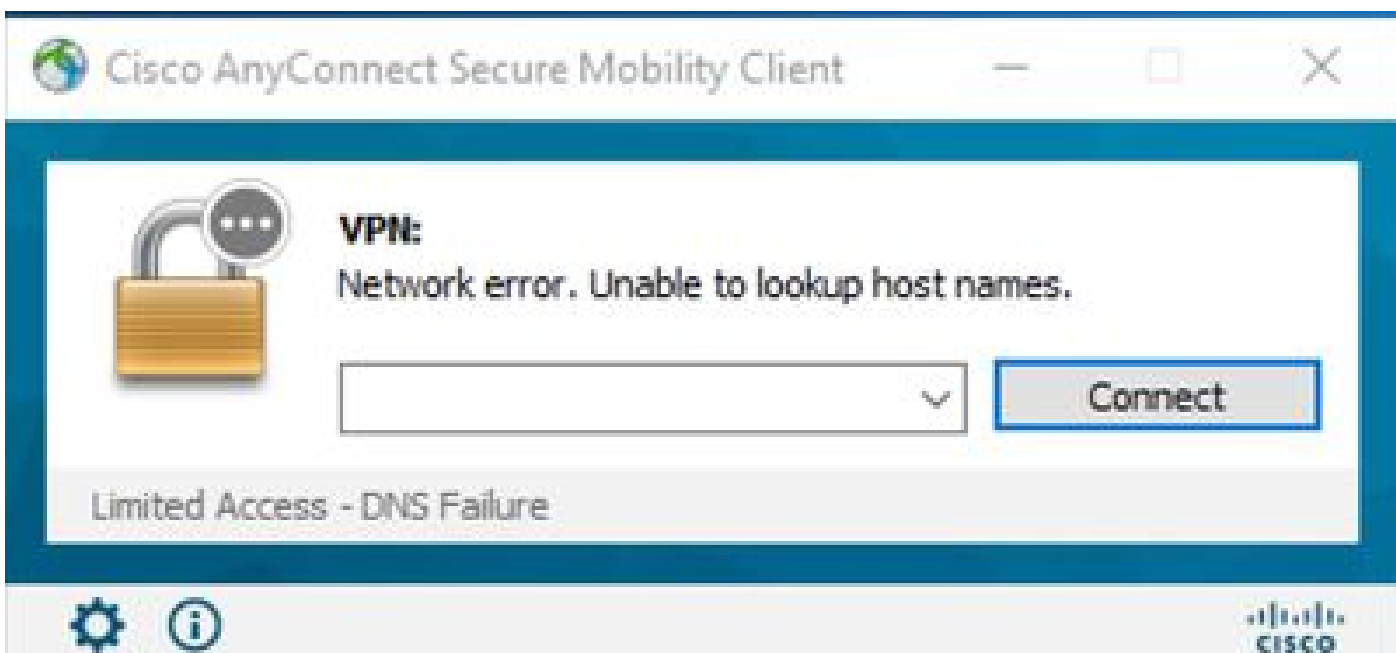
```

故障排除

为了确认正确操作，您可以使用Wireshark在终端的出口接口上启用数据包捕获。

No.	Time	Source	Destination	Protocol	Length	Info
2	2020-06-17 20:21:32.289178	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x03a7 A mus.cisco.com
18	2020-06-17 20:21:43.662753	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x03a7 Server failure A mus.cisco.com
26	2020-06-17 20:21:47.336418	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x03d8 A mus.cisco.com
59	2020-06-17 20:21:59.069648	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x03d8 Server failure A mus.cisco.com
66	2020-06-17 20:22:02.385726	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x0409 A mus.cisco.com
88	2020-06-17 20:22:13.570386	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x0409 Server failure A mus.cisco.com
96	2020-06-17 20:22:17.426213	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x043a A mus.cisco.com
117	2020-06-17 20:22:28.977132	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x043a Server failure A mus.cisco.com
135	2020-06-17 20:22:32.478764	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x046b A mus.cisco.com
159	2020-06-17 20:22:43.477717	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x046b Server failure A mus.cisco.com
167	2020-06-17 20:22:47.526516	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x049c A mus.cisco.com
197	2020-06-17 20:22:59.790911	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x049c Server failure A mus.cisco.com
203	2020-06-17 20:23:02.572275	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x04cd A mus.cisco.com
225	2020-06-17 20:23:14.291503	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x04cd Server failure A mus.cisco.com
232	2020-06-17 20:23:17.615747	10.31.121.202	10.88.240.69	DNS	73	Standard query 0x04fe A mus.cisco.com
251	2020-06-17 20:23:29.698518	10.88.240.69	10.31.121.202	DNS	73	Standard query response 0x04fe Server failure A mus.cisco.com

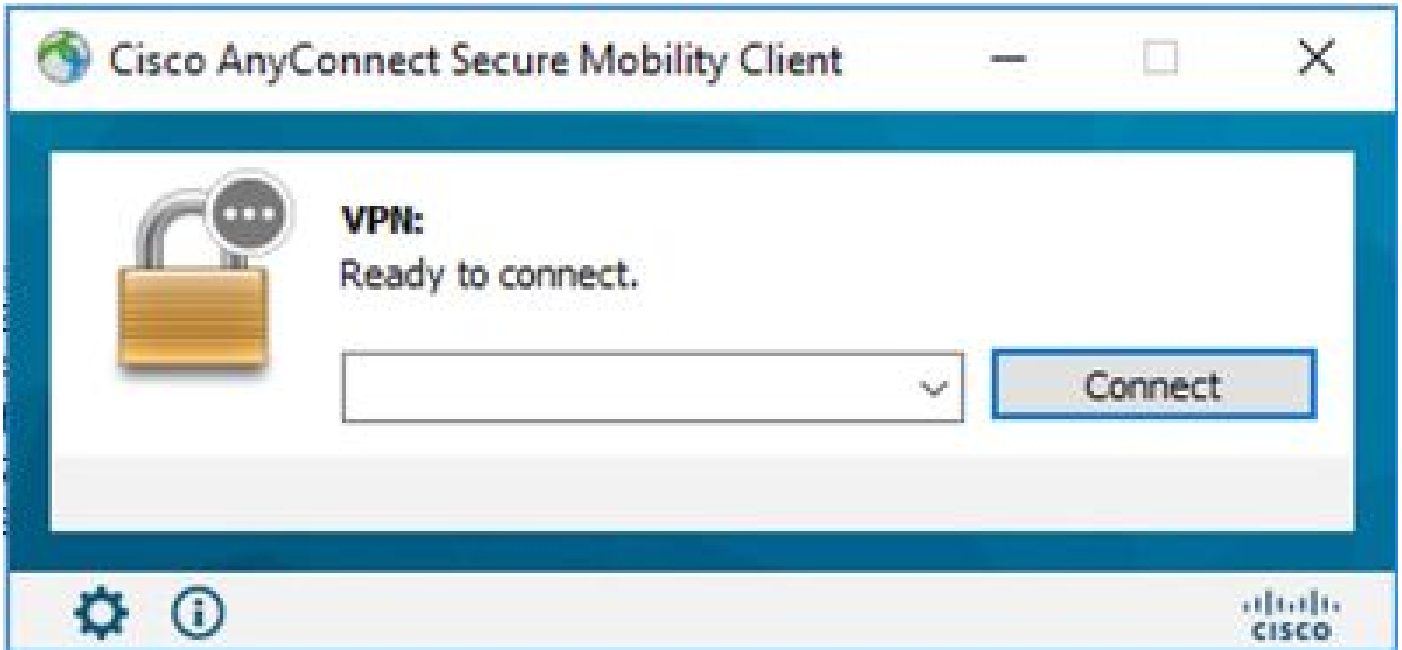
在AnyConnect客户端的图形用户界面(GUI)上，显示消息“Network error(网络错误)”。显示“无法查找主机名”(如图所示)。




当应用任何解决方法时，您也可以在Wireshark上捕获数据包，并使用DNS过滤器确认对mus.cisco.com的常量查询：

No.	Time	Source	Destination	Protocol	Length	Info
16389	866.042487	10.4.9.62	10.4.9.1	DNS	84	Standard query 0xc729 A sls.update.microsoft.com
16392	866.151743	10.4.9.62	10.4.9.1	DNS	91	Standard query 0xad6f A settings-win.data.microsoft.com
16406	867.058085	10.4.9.62	10.4.9.1	DNS	84	Standard query 0xc729 A sls.update.microsoft.com
16414	867.151917	10.4.9.62	10.4.9.1	DNS	91	Standard query 0xad6f A settings-win.data.microsoft.com
16449	869.058089	10.4.9.62	10.4.9.1	DNS	84	Standard query 0xc729 A sls.update.microsoft.com
16451	869.167454	10.4.9.62	10.4.9.1	DNS	91	Standard query 0xad6f A settings-win.data.microsoft.com
16500	873.058065	10.4.9.62	10.4.9.1	DNS	84	Standard query 0xc729 A sls.update.microsoft.com
16507	873.183053	10.4.9.62	10.4.9.1	DNS	91	Standard query 0xad6f A settings-win.data.microsoft.com
16562	877.080933	10.4.9.62	10.4.9.1	DNS	84	Standard query 0x9902 A sls.update.microsoft.com
16587	878.073865	10.4.9.62	10.4.9.1	DNS	84	Standard query 0x9902 A sls.update.microsoft.com
16598	879.073732	10.4.9.62	10.4.9.1	DNS	84	Standard query 0x9902 A sls.update.microsoft.com
16635	881.089368	10.4.9.62	10.4.9.1	DNS	84	Standard query 0x9902 A sls.update.microsoft.com
16684	885.104894	10.4.9.62	10.4.9.1	DNS	84	Standard query 0x9902 A sls.update.microsoft.com

在AnyConnect客户端的GUI界面上，将显示消息“Ready to connect”(如图所示)。



 提示：即使您未在GUI界面上看到AnyConnect VPN核心模块，也不意味着vpn核心模块未运行，请在“C:\programdata\cisco on Windows”目录下搜索VPNDisable_ServiceProfile.xml文件，并在Apple设备上搜索“/opt/cisco/anyconnect/profile”。在Linux上不支持此功能。

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）。