

排除TETRA定义更新故障

目录

[简介](#)

[故障排除](#)

[在安全终端控制台上检查终端报告的连接](#)

[检查终端上的连接](#)

[检查终端上的TETRA定义](#)

[在终端上强制TETRA定义更新](#)

[检查终端上的TETRA定义服务器连接](#)

[直接连接验证](#)

[代理验证](#)

[其他信息](#)

简介

本文档介绍调查终端未能从Cisco TETRA定义更新服务器更新TETRA定义的原因时应遵循的步骤。

在安全终端控制台上看到的定义上次更新失败(Definitions Last Updated failure seen)显示在计算机详细信息下，如下所示。

DESKTOP-QFC3PVT in group Protect			
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

← Events 📄 Device Trajectory 🔍 Diagnostics ⌂ View Changes

🔍 Scan... 🛠 Diagnose... 📁 Move to Group...

故障排除

Cisco Secure Endpoint for Windows需要持续连接到TETRA定义服务器才能下载更新。

下载TETRA定义的常见错误包括：

- 无法解析服务器地址
- 验证SSL证书失败（包括证书撤销列表检查）
- 下载过程中中断
- 无法连接到代理服务器
- 无法向代理服务器进行身份验证

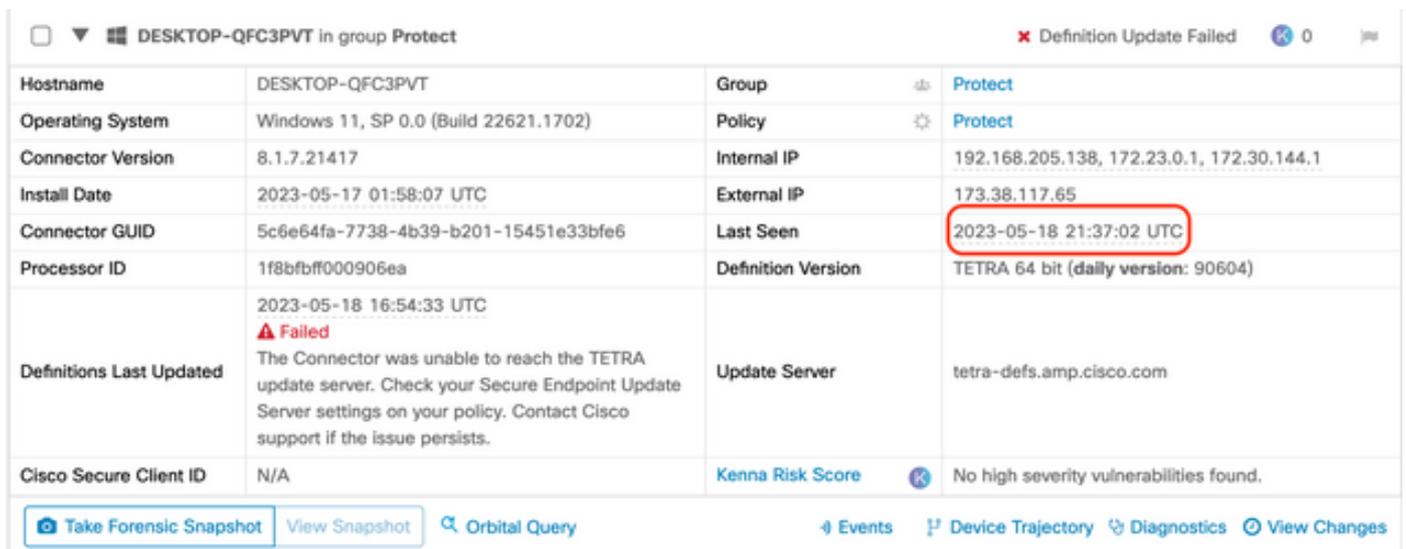
如果在尝试下载TETRA定义时出现故障，则下次尝试将在下次更新间隔或用户启动手动更新时发生。

在安全终端控制台上检查终端报告的连接

安全终端控制台显示终端是否定期连接。确保您的终端处于活动状态，并且处于最近的“上次查看时间”状态。如果终端未通过安全终端控制台签入，则表明终端未处于活动状态或存在某些连接问题。

思科每天平均发布4个定义更新，如果终端在一天中的任何时间无法下载更新，则连接器会发布故障错误。考虑到此频率，仅当终端始终连接，并且始终与TETRA服务器具有稳定的网络连接，则终端才会报告为“在策略内”。

“Last Seen”（上次查看时间）状态在“Computer details”（计算机详细信息）页面上，如下圆圈所示：



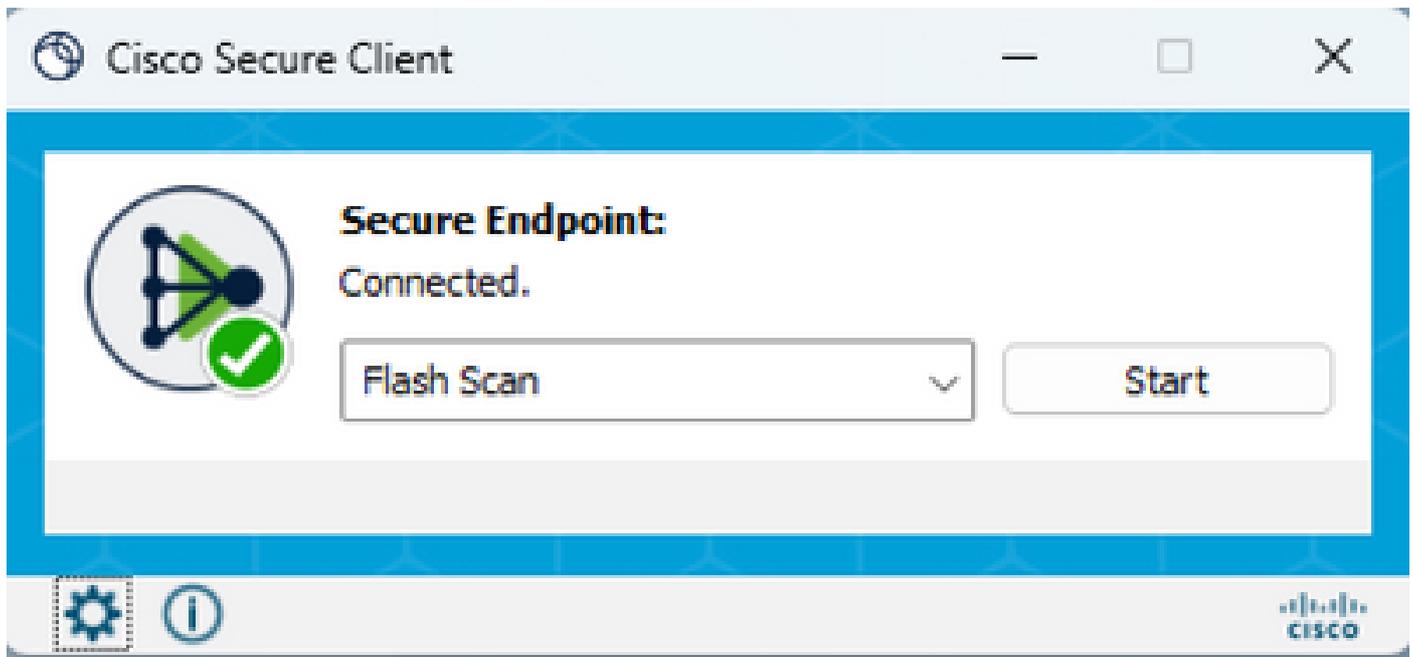
DESKTOP-QFC3PVT in group Protect		* Definition Update Failed 0	
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138, 172.23.0.1, 172.30.144.1
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-18 21:37:02 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90604)
Definitions Last Updated	2023-05-18 16:54:33 UTC Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

如果终端正在连接，并且报告定义未下载但控制台看到错误，则问题可能间歇性出现。如果“上次查看时间”和“上次更新定义”之间的时间差异较大，则可以进一步进行调查。

检查终端上的连接

最终用户可以使用UI界面检查连接。

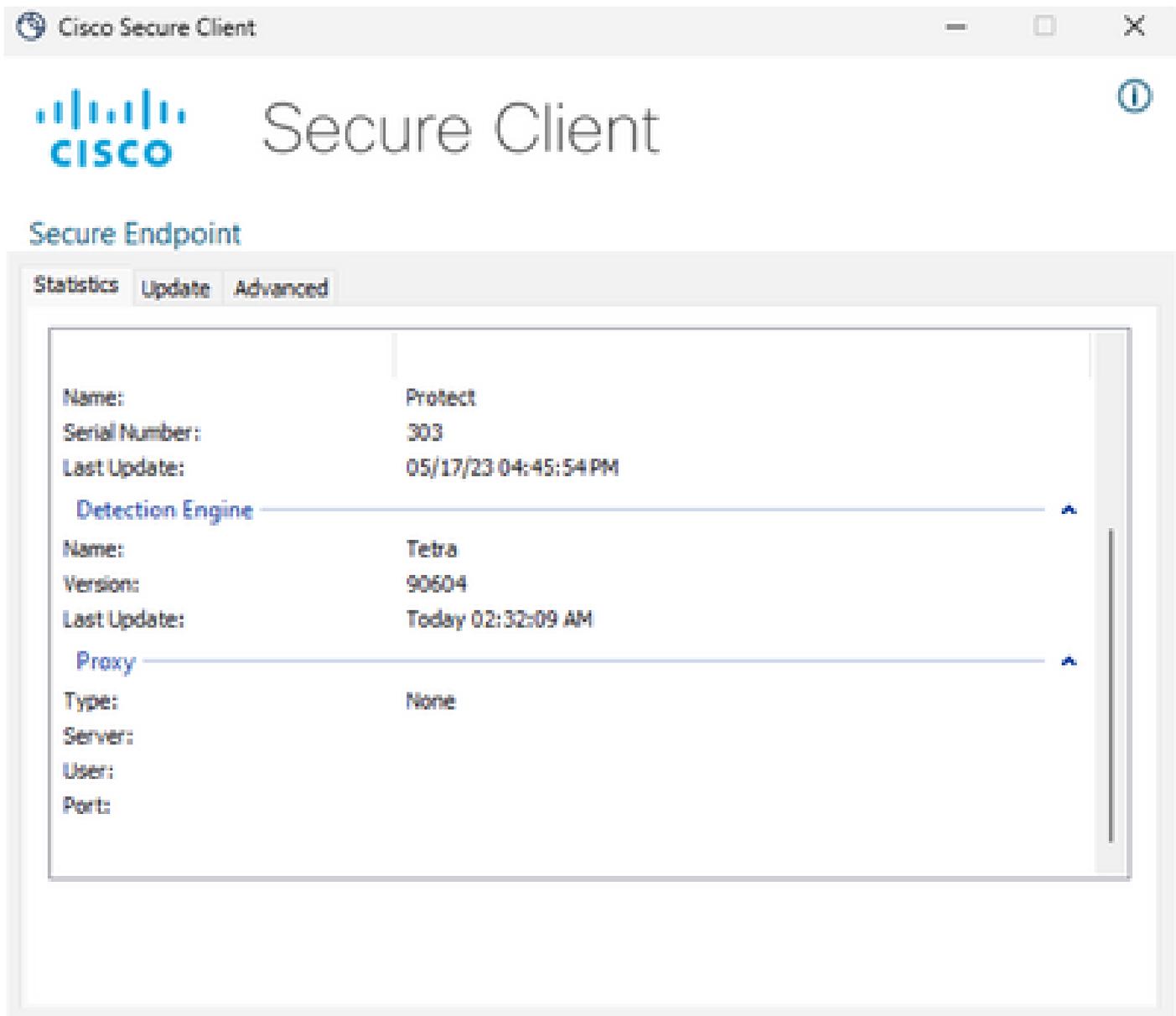
打开Cisco安全客户端将显示连接状态。



当终端未连接并报告连接问题时，可使用ConnectivityTool。这包含在生成支持包的IPSupportTool中。

检查终端上的TETRA定义

思科安全客户端提供有关终端连接器加载的当前TETRA定义的信息。最终用户可以打开客户端并检查安全终端的设置。在Statistics选项卡上，TETRA的当前定义可用。



此外，当前的TETRA定义详细信息由终端上的AmpCLI工具报告。命令示例如下：

```
PS C:\Program Files\Cisco\AMP\8.1.7.21417> .\AmpCLI.exe posture  
{"agent_uuid":"5c6e64fa-7738-4b39-b201-15451e33bfe6","connected":true,"connector_version":"8.1.7","engi
```

系统将显示每个引擎（包括TETRA）的定义版本。在上面的输出中，定义版本为90604。这可以与“安全终端控制台”下的定义版本进行比较：Management > AV Definition Summary。该页面示例如下所示。

AV Definition Summary

 Version 90606 2023-05-18 20:13:58 UTC	 Version 120765 2023-05-18 20:13:57 UTC	 Version 120765 2023-05-18 20:13:57 UTC
---	---	--

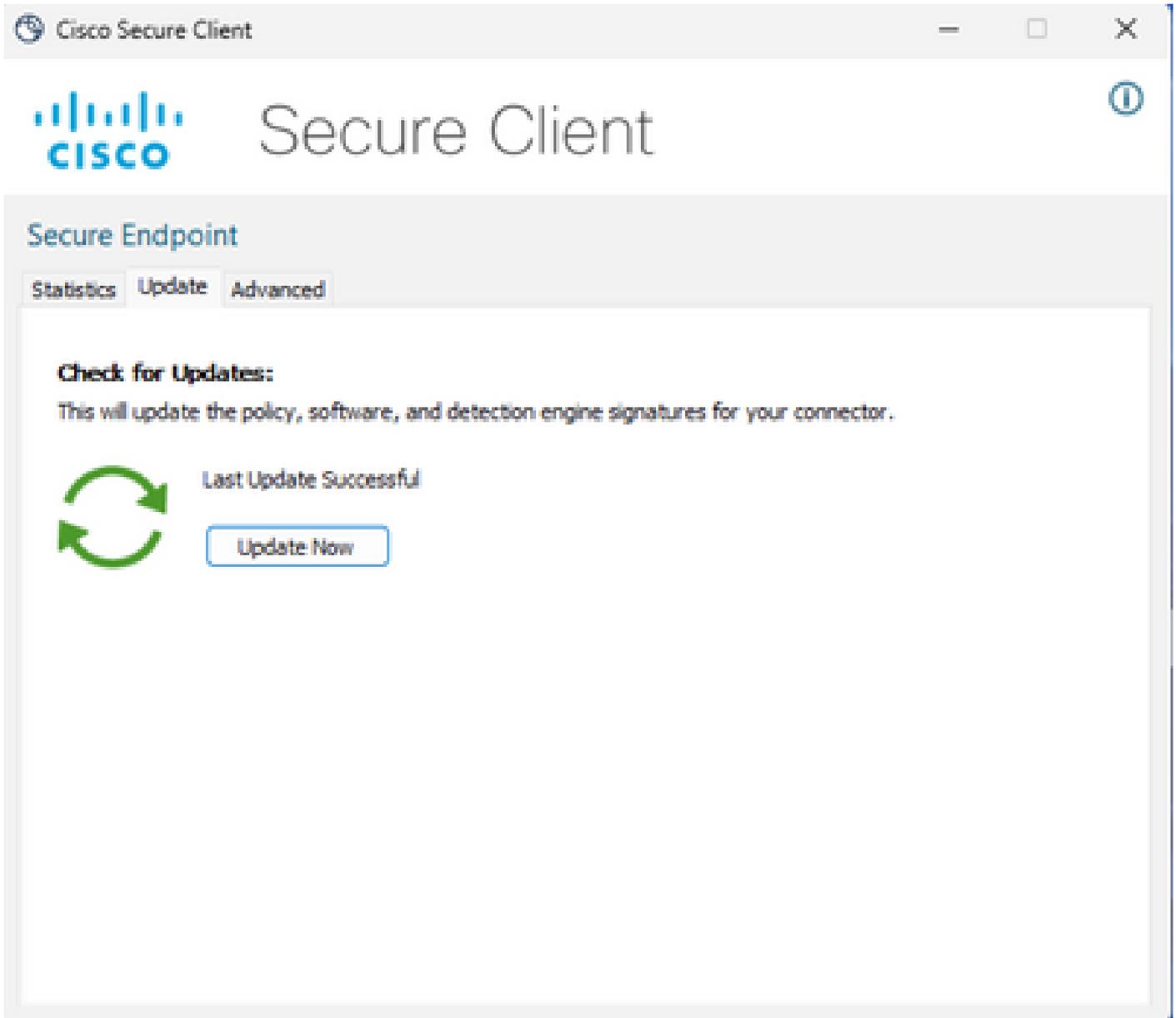
TETRA 64bit	TETRA 32bit	ClamAV Mac	ClamAV Linux-Or
Version			Available
90606			2023-05-18 20:13:58 UTC
90605			2023-05-18 16:15:48 UTC
90604			2023-05-18 12:13:36 UTC

如果版本仍然落后且连接器状态已连接，则可以更新定义或检查终端与TETRA服务器的连接。

在终端上强制TETRA定义更新

最终用户可以模拟和检查TETRA下载进度。用户若要触发更新，需要在策略中设置该选项。在 Advanced Settings > Client User Interface policy settings 页面下，需要为用户触发的定义启用 Allow user to update TETRA definitions 设置。

在Cisco安全客户端中，最终用户可以打开客户端并检查安全终端的设置。用户可以点击“立即更新”(Update Now)以触发如下所示的TETRA定义更新：



如果您运行的是面向终端的AMP连接器版本7.2.7及更高版本，您可以使用新的交换机“—forceupdate”强制连接器下载TETRA定义。

```
C:\Program Files\Cisco\AMP\8.1.7.21417\sfc.exe -forceupdate
```

强制执行更新后，可以再次检查TETRA定义以查看是否发生更新。如果仍然没有更新，则需要检查与TETRA服务器的连接。

检查终端上的TETRA定义服务器连接

终端策略包括终端联系以下载定义的定义服务器。

计算机详细信息页面包括更新服务器。下图显示了更新服务器的显示位置：

DESKTOP-QFC3PVT in group Protect			
Hostname	DESKTOP-QFC3PVT	Group	Protect
Operating System	Windows 11, SP 0.0 (Build 22H2.1702)	Policy	Protect
Connector Version	6.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.28.117.65
Connector GUID	5c6e64fa-7738-4639-b201-15451e336fe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f86fb8000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.

[Events](#) | [Device Trajectory](#) | [Diagnostics](#) | [View Changes](#)

[Scan...](#) | [Diagnose...](#) | [Move to Group...](#)

在公共云上，终端可以连接的所需服务器名称列在[Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations](#)下

直接连接验证

在终端上，可以运行以下命令来检查更新服务器的DNS查找：

```
PS C:\Program Files\Cisco\AMP> Resolve-DnsName -Name tetra-defs.amp.cisco.com
Name                               Type TTL Section IPAddress
----                               -
tetra-defs.amp.cisco.com          A     5     Answer 192.XXX.X.XX
tetra-defs.amp.cisco.com          A     5     Answer 192.XXX.X.X
tetra-defs.amp.cisco.com          A     5     Answer 192.XXX.X.X
```

如果解析了IP，则可以测试与服务器的连接。有效的响应如下所示：

<#root>

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
* Trying 192.XXX.X.X:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.X) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: tetra-defs.amp.cisco.com
> User-Agent: curl/8.0.1
> Accept: */*
>
* schannel: server closed the connection
```

```

< HTTP/1.1 200 OK

< Date: Fri, 19 May 2023 19:13:35 GMT
< Server:
< Last-Modified: Mon, 17 Apr 2023 15:48:54 GMT
< ETag: "0-5f98a20ced9e3"
< Accept-Ranges: bytes
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=UTF-8
<
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443

```

如果无法建立连接以验证证书与CRL服务器(例如commercial.ocsp.identrust.com或validation.identrust.com)的连接，则会出现以下错误：

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
```

```

* Trying 192.XXX.X.XX:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.XX) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation function
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
curl: (35) schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation

```

代理验证

如果终端配置为使用代理，则可以检查最后一个错误状态。运行下面的PowerShell可能会返回TETRA更新尝试的最后一个错误。

```
PS C:\Program Files\Cisco\AMP> (Select-Xml -Path local.xml -XPath '//tetra/lasterror').Node.InnerText
```

上一个错误代码	问题	操作
4294965193	无法建立到代理的连接	检查与代理的网络连接
4294965196	无法通过代理进行身份验证	检查代理的身份验证凭据
4294965187	连接到代理并下载失败	检查代理日志是否存在下载问题

其他信息

- 如果您看到终端始终无法下载TETRA定义，尽管完成了上述检查，请在调试模式下启用连接器，时间间隔等于策略中定义的更新间隔，并生成支持捆绑包。当连接器处于调试模式时，请注意同时捕获Wireshark数据包捕获。数据包捕获的时间间隔必须等于策略中定义的更新间隔。收集这些信息后，请随此信息一起打开思科TAC案例，以便进一步调查。

[从AMP for Windows连接器收集诊断数据](#)

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）。