解决由于不支持的GoDaddy R1证书链导致的Webex呼叫生存性网关同步故障

目录

问题

两个生存性网关（mcyitsrtr001.centralwire.com和prtitsrtr001.centralwire.com）在Control Hub中注册，但未能同步；故障排除重点是mcyitsrtr001.centralwire.com。同步尝试失败，并显示以下错误消息：

```
Sync failed due to internal server error (code - 31117)
```

第一次是在2026年8月5日尝试同步时观察到的。对遥测和Webex后端（挂起）日志的分析显示，网关呈现的是GoDaddy R1v1证书链（GoDaddy TLS根CA - R1层次结构），Webex服务不支持该证书链，从而导致证书链被拒绝，同步失败。

环境

- 报告了两个托管网关：mcyitsrtr001.centralwire.com和prtitsrtr001.centralwire.com（故障排除集中在mcyitsrtr001.centralwire.com上）
- IOS® XE版本：17.12.6（SGW节点），17.15.06(MGW)
- Webex Calling Survivability Gateway(SGW)配置
- 使用R1v1中间CA的GoDaddy TLS证书链
- 证书链:CN=mcyitsrtr001.centralwire.com → GoDaddy TLS中间CA DV - R1v1 → GoDaddy TLS根CA - R1

分辨率

通过实施证书交叉签名解决方法来建立受信任证书路径，解决了此问题。该解决方案包括安装GoDaddy R1到G2交叉签名证书，以便将较新的GoDaddy R1层次结构链接到受信任的Go Daddy Root Certificate Authority - G2。


注意：在证书更改期间，crypto pki trustpool import clean命令中断了网关的NETCONF-YANG/DMI服务，使连接器暂时脱机。无法打开到192.168.217.55:830的套接字)。 这是通过步骤6-7恢复的，是维护的副作用，而不是原始同步故障。

步骤 1：安装思科Trustpool捆绑包

安装包含Go Daddy Root Certificate Authority - G2的Cisco trustpool 捆绑包：

```
crypto pki trustpool import clean url http://www.cisco.com/security/pki/trs/ios_union.p7b
```

`import clean`会替换整个trustpool — 它可以中断依赖它的服务（请参阅前面列出的connector-offline注释）。 请谨慎使用。

步骤 2：验证G2根证书

确认Go Daddy Root Certificate Authority - G2存在：

```
show crypto pki trustpool | include GoDaddy|Go Daddy
```

步骤 3：删除自签名R1信任点

删除旧的自签名R1信任点（当提示删除证书时，请回答yes）：

```
no crypto pki trustpoint GoDaddyRootR1
```

步骤 4：安装交叉签名R1证书

使用交叉签名的R1证书创建新信任点(主题：GoDaddy TLS根CA - R1，颁发者：Go Daddy Root Certificate Authority - G2):

```
crypto pki trustpoint GoDaddyCrossR1
enrollment terminal
revocation-check none
exit
crypto pki authenticate GoDaddyCrossR1
<paste cross-signed R1 PEM – Subject: GoDaddy TLS Root CA - R1, Issuer: Go Daddy Root Certificate Autho
quit
yes
```

步骤 5：验证证书链

验证链现在是否正确解析：

```
show crypto pki certificates webex-sgw
show crypto pki certificates GoDaddyCrossR1
```

步骤 6：重新启动NETCONF服务

退回HTTP(S)服务器和NETCONF-YANG服务（在禁用和启用之间等待约60秒）：

```
conf t
no netconf-yang
no ip http secure-server
no ip http server
end
```

等待60秒，然后重新启用：

```
conf t
```

```
ip http server
ip http secure-server
netconf-yang
end
write memory
```

步骤 7：重新加载网关（如有必要）

如果在服务重新启动后NETCONF-YANG仍然无法正常提供服务，请重新加载路由器以完全重新初始化DMI:

```
reload
```

警告：有可能。此处提到的详细信息似乎包含执行后可能会产生重大影响的过程或命令。请确保SME或业务部门在执行或推荐之前已评估上述程序或命令。

步骤 8::检验分辨率

网关重新联机后，触发来自控制中心的SGW重新同步，并验证同步是否成功完成，没有错误代码31117或“证书服务器受信任检查失败”消息。已确认已解决 — 网关在R1v1→→ R1（颁发者G2）链中呈现完整的枝叶，并且同步在交叉符号解决方法后成功完成。

原因

根本原因确定为证书信任故障。生存性网关使用GoDaddy TLS根CA - R1层次结构（具体是GoDaddy TLS中间CA DV - R1v1）提供证书链，该证书链未包含在Webex呼叫的受信任证书颁发机构列表中。

当Webex后端（挂架）在SIP身份验证信息请求期间执行服务器证书信任检查时，它无法建立到受信任根证书的有效证书路径。这导致SunCertPathBuilderException出现错误“无法找到到所请求目标的有效证书路径”，导致HTTP 400响应和同步中断。

Webex Calling只信任旧的GoDaddy/Starfield根（例如Go Daddy Root Certificate Authority -

G2），而不信任新的“GoDaddy TLS”(R1/R1v1)层次结构。

相关内容

- Webex混合服务支持的证书颁发机构
- GoDaddy证书存储库
- 思科技术支持和下载

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）。