

安全访问资源连接器证书到期和操作系统升级警告

目录

问题

资源

VMware ESXi上部署的连接器显示以下错误：

1.此连接器已连接，但无法同步其配置。运行诊断程序并检查防火墙设置以解决连接问题

2.配置状态

无法检索DNS配置或配置状态。请检查您的防火墙设置。

3.连接器版本

未知

v2.0.85

(v2.0.93)

数据可能已过时。

已添加

世界协调时2026年1月20日早上7点15分

操作系统 版本

未知

2509300328

(2601240447)

- 数据可能已过时。

环境

- 思科安全访问资源连接器版本2.0.85
- VMware ESXi虚拟化平台

- 在HA对中部署的资源连接器
- CSG防火墙，确认无防火墙丢弃
- 网络连接已确认，路由或NAT未发生变化
- 同一环境中的多个资源连接器对具有相同的防火墙、路由、NAT和安全策略
- 大约每5周发生一次的重复问题模式

原因

两个RC均显示以下错误：设置控制器连接失败 `error="SetupControllerConnection: : 创建控制器连接失败 — err=创建连接失败：网络错误：已超过上下文截止日期"`

未检测到来自RC的连接问题。DNS正常。允许端口，但仅对以下URL执行PING操作失败：

2026-02-12 14:26:39.736869500 SSE API -> [0;31mFAILED

2026-02-12 14:26:39.736870500 SSE ACME PureCA OCSP -> [0;31mFAILED

2026-02-12 14:26:39.736924500 =====

2026-02-12 14:10:21.892855500

2026-02-12 14:10:21.892856500 ####ping SSE API: ping -w 5 -c 3 api.sse.cisco.com

2026-02-12 14:10:26.899046500 PING api.sse.cisco.com(146.112.59.20)56(84)个字节的数据。

2026-02-12 14:10:26.899047500

2026-02-12 14:10:26.899048500 — api.sse.cisco.com ping统计信息 —

2026-02-12 14:10:26.899048500 5个数据包已发送，0个已接收,100%数据包丢失，时间4082毫秒

2026-02-12 14:10:30.922958500 ####ping SSE ACME PureCA OCSP: ping -w 5 -c 3 ssepki-prd.pureca.cryptosvcs.cisco.com

2026-02-12 14:10:35.926673500 PING ssepki-prd.pureca.cryptosvcs.cisco.com(3.225.142.190)56(84)个字节的数据。

2026-02-12 14:10:35.926674500

2026-02-12 14:10:35.926709500 — ssepki-prd.pureca.cryptosvcs.cisco.com ping统计信息 —

2026-02-12 14:10:35.926709500 5个数据包已发送，0个已接收,100%数据包丢失，时间4078毫秒

2026-02-12 14:15:54.892666500 ===== Ping =====

2026-02-12 14:15:54.892823500 自助 — > [0;32mSUCCESS

2026-02-12 14:15:54.892879500 网关 — > 0;32mSUCCESS

2026-02-12 14:15:54.892964500 SSE API -> 0;31mFAILED

2026-02-12 14:15:54.893022500 SSE证书API ->[0;32mSUCCESS

2026-02-12 14:15:54.893071500 SSE AC头端 —>成功

2026-02-12 14:15:54.89314500 SSE ACME PureCA OCSP -> [0;31mFAILED

2026-02-12 14:15:54.893168500 =====

上述消息为误报。

当RC尝试检查OCSP以获取SSE API时，由于OCSP故障而续订了相关证书。在日志中，您可以看到返回的状态是HTTP 403:

026-02-12T14:23:26Z ERR无法检查证书吊销错误="error validating cert revocation status err=exit status

以下调试行可能很有帮助：

```
查询OCSP响应器时出错\n807BB6508C770000:error:1E800069:HTTP例程
: parse_http_line1:received error:../crypto/http/http_client.c:440:code=403,
reason=Forbidden\n807BB6508C770000:error:1E800076:HTTP例程
: OSSL_HTTP_REQ_CTX_nbio : 意外的内容类型
: ../crypto/http/http_client.c:676:expected=application/ocsp-response ,
actual=text/html;charset="utf-8"\n807BB6508C770000:error:1E800067:HTTP例程
: OSSL_HTTP_REQ_CTX_exchange:error
receiving:../crypto/http/http_client.c:874:server=http://ssepki.cryptosvcs.cisco.com:80\n"
func=VerifyCertificateStatus
```

2026-02-12T14:23:26Z INF设置控制器连接

如果防火墙上有所阻止，允许流量到达<http://ssepki.cryptosvcs.cisco.com:80>可消除更多证书错误。

操作系统更新

操作系统升级不足与技术限制和其他因素有关，这些因素促使ENG团队决定不在基于虚拟机的RC上尝试操作系统升级。

避免定期重新部署基于VM的RC的建议是执行基于容器的部署，这样您的团队就可以独立地管理容器主机操作系统的升级和维护。

相关内容

- [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）。