使用9800上的策略问题排除智能许可故障

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- 许可证使用情况报告
- RUM报告
- 解决直连CSSM和SSM本地服务器的9800智能许可通信问题
- 信任代码
- 智能与CSSM
- 智能使用代理
- 内部的SSM
- 智能传输
- 内部的SSM

测试与智能接收器的连接

测试与SSM内部服务器的连接

查找接收方IP地址

您的系统如何解析IP?

- 从CSSM处理的信任码无效
- 从CSSM处理的有效信任码

通信频率

在show license eventlog和/或show log的输出中报告的错误

调试

相关信息

简介

本文档介绍Catalyst 9800无线LAN控制器上的智能许可使用策略(SLUP)的高级故障排除步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 使用策略的智能许可(SLUP)
- Catalyst 9800无线LAN控制器(WLC)

使用的组件

本文档不限于特定的软件和硬件版本。

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。

背景信息

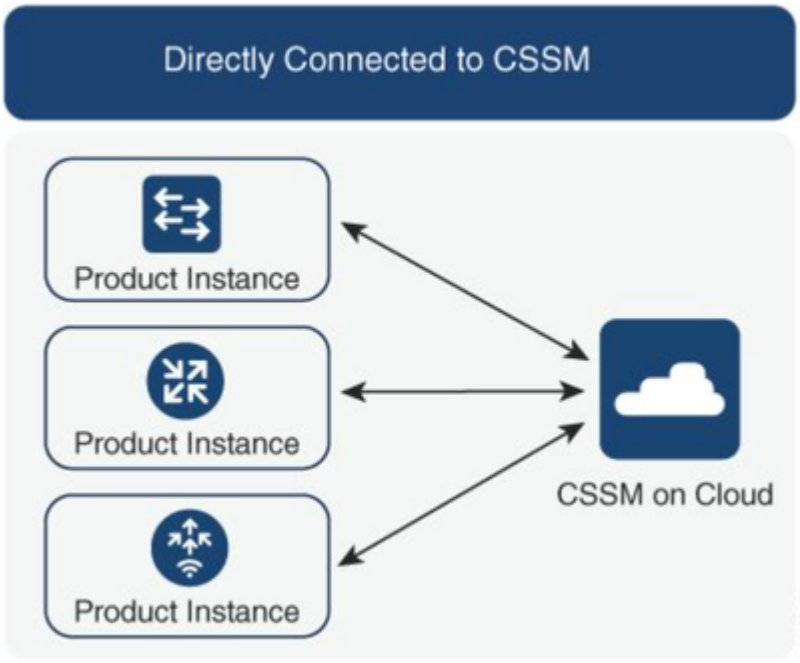
⚠ 警告：警告：本文中的说明包含有用的建议或对于文档未涵盖的材料的引用。建议您阅读每个备注。

- 使用:Cisco Catalyst无线控制器上的所有许可证均未实施。这意味着您不必完成任何特定于许可的操作，例如在开始使用软件及其关联的许可证之前注册或生成密钥。许可证使用情况会记录在设备上并带有时间戳，所需的工作流程可在以后完成。
- 向CSSM报告许可证使用情况：许可证使用报告有多个选项。您可以使用SSM内部版本或思科智能许可实用程序(CSLU)，或者直接向CSSM报告使用信息。对于气隙网络，还可以提供离线报告功能，您可以在其中下载使用信息并将其上传到CSSM。使用情况报告采用纯文本XML格式。

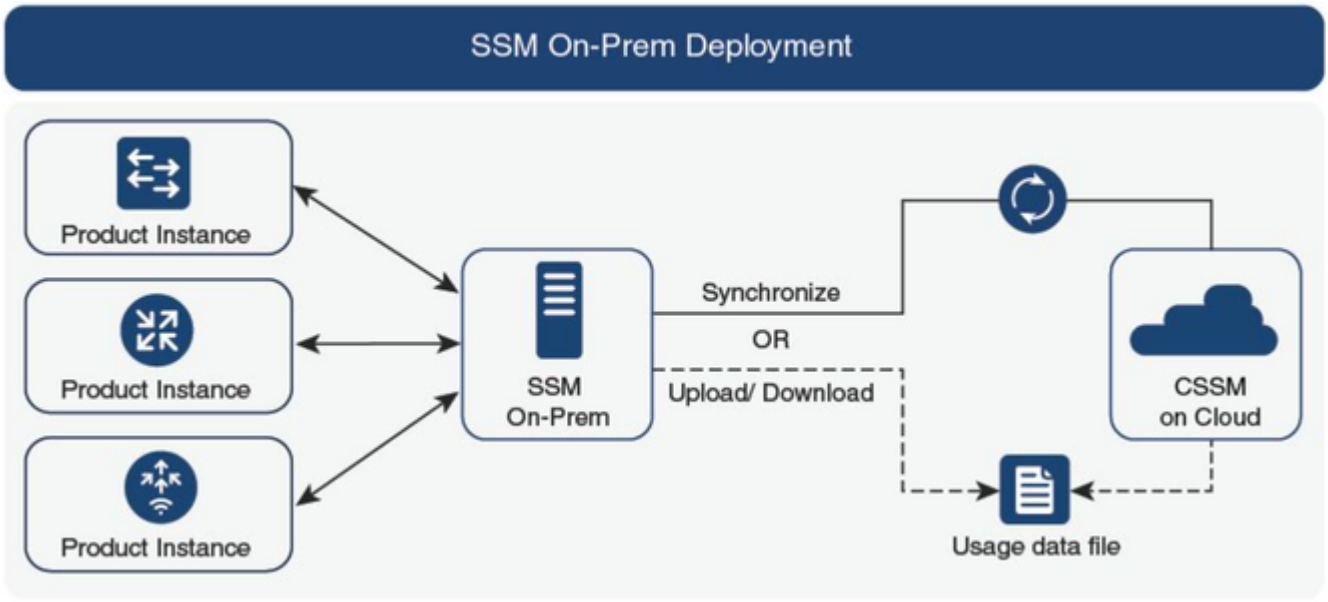
1. 直接连接到思科智能软件管理器云(CSSM)
2. 通过本地智能软件管理器（本地SSM）连接到CSSM

本文未涉及Catalyst 9800上的所有智能许可方案，请参阅使用策略配置的智能许可指南以获取更多信息。但是，本文确实提供了一系列有用的命令，用于使用Catalyst 9800上的策略问题对直接连接和SSM内部智能许可进行故障排除。

选项1.直接连接到思科智能许可云服务器(CSSM):



选项2.通过内部智能软件管理器（内部SSM）进行连接：



注意：本文中提到的所有命令仅适用于运行17.3.2版或更高版本的WLC。

许可证使用情况报告

使用SLP时，大多数许可证不会实施，并且会在配置功能/技术包时在设备上启用。相应的许可证将显示在**show license summary**中，如**IN USE**。

```
9800-1#show license summary
Account Information:
  Smart Account:



  Virtual Account:



License Usage:
  License                  Entitlement Tag               Count Status
  -----------------------------------------------------------------------------
  lic_c9800l_perf          (LIC_C9800L_PERF)                 1 IN USE
  air-network-advantage    (DNA_NWStack)                   2 IN USE
  air-dna-advantage        (AIR-DNA-A)                         2 IN USE
```

许可证仅有的两种状态为正在使用或未使用。状态完全取决于产品实例上应用的配置和功能。

对于正在使用的每个许可证，会单独创建一个RUM报告。Rum报告有CLOSED、ACK和OPEN等状态。

可选：使用内部命令test license smart rum-report id命令确认：

```
Router(config)# service internal

Router# test license smart rum-report id
```

report_id:1624247687 state:SmartAgentRumStateOpen

从17.9版本开始：show license rum id all命令：

Smart Licensing Usage Report: ========== Report Id, State, Flag, Feature Name 1682489268 CLOSED P lic_c9800l_perf 1682489269 CLOSED P air-network-advantage 1682489270 CLOSED P air-dna-advantage 1682489271 CLOSED P air-network-advantage 1682489272 CLOSED P air-dna-advantage 1682489273 ACK N lic_c9800l_perf

RUM报告

RUM报告或资源使用率测量报告是包含有关许可证使用和设备身份信息的数据文件。这些报告是存储在设备中的安全信息，并由硬件进行证书签名。

报告在产品实例与CSSM之间的通信过程中会更改状态。

状态	**描述**
SmartAgentRumStateOpen	智能代理在设备上创建的新报告
SmartAgentRumStateClosed	发送到CSSM的RUM报告（重新加载还会将打开的报告推送到关闭状态）
SmartAgentRumStateUnrecognized	RUM报告等待来自CSSM的确认，提供轮询ID
SmartAgentRumStateAcknowledge	RUM报告发送到CSSM并获得确认

Catalyst 9800中引入了使用策略的智能许可功能，代码版本为17.3.2。初始17.3.2版本遗漏了WLC webUI中随17.3.3版本引入的SLUP配置菜单。SLUP在以下几个方面不同于传统的智能许可：

- WLC现在通过smartreceiver.cisco.com域而不是tools.cisco.com与CSSM通信。
- 现在，WLC不再注册，而是与CSSM或SSM本地建立信任。
- CLI命令稍有改动。
- 智能许可预留(SLR)不再存在。您可以定期手动报告使用情况。
- 评估模式不再存在。即使没有许可证，WLC仍继续以满容量运行。系统基于荣誉，您应定期报告许可证使用情况（自动或手动报告气隙网络）。



注意：警告：如果您使用的是Cisco Catalyst 9800-CL无线控制器，请确保您熟悉以Cisco IOS® XE Cupertino 17.7.1开始的强制ACK要求。请参阅Cisco Catalyst 9800-CL无线控制器的RUM报告和确认要求。

解决直连CSSM和SSM本地服务器的9800智能许可通信问题

*全新9800控制器必须遵循智能许可工作流程的特定程序才能完成。

1.从CSSM门户创建令牌并导入该令牌，以建立将来获得许可证使用报告授权所需的信任ID。此信任ID值是CSSM的密钥，用于验证从9800控制器提交的报告。此信任令牌将定期刷新，并作为CSSM的Rum使用情况报告的一部分交换。

注意：从Cisco IOS XE Cupertino 17.7.1开始，需要信任代码。信任代码按序列号建立，因此9800 HA SSO设置将安装2个信任代码。

信任代码

UDI绑定的公钥，产品实例用于执行以下操作：

- 签署RUM报告。这可以防止篡改并确保数据真实性。
- 启用与CSSM的安全通信。

在Cisco IOS XE Cupertino 17.7.1中，在产品实例发起向CSLU发送数据的拓扑和产品实例位于气隙网络中的拓扑中，自动获取信任代码。

- 可以使用ID令牌从CSSM获取信任代码。

  在此，您将在CSSM Web UI中生成ID标记，以获取信任代码并将其安装在产品实例上。如果存在出厂安装的信任代码，则必须覆盖该信任代码。如果产品实例直接连接到CSSM，请使用此方法使产品实例能够以安全的方式与CSSM通信。这种获得信任代码的方法适用于直接连接到CSSM的所有选项。有关详细信息，请参阅直接连接到CSSM。

从Cisco IOS XE Cupertino 17.9.1中，在CSLU启动从产品实例检索数据的拓扑中自动获取信任代码。

如果存在出厂安装的信任代码，则会自动覆盖。通过这种方式获得的信任码可用于与CSSM的安全通信。

*确保9800上的智能许可配置完好无损。9800使用Smart as transport与CSSM通信。

智能与CSSM

Device(config)#license smart transport smart Device(config)#license smart url https://smartreceiver.cisco.com/licservice/license

智能使用代理

license smart proxy { address address_hostname| port port_num} Device(config)#license smart url default Device(config)#license smart proxy address

Device(config)#license smart proxy port

内部的SSM

Device(config)#license smart transport cslu Device(config)#license smart url cslu https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1

确保可通过源接口访问域名查询和域名服务器。

Device(config)#ip domain name

Device(config)#ip name server

Device(config)#ip domain lookup

show license all命令返回在9800上配置的传输类型和URL详细信息：确保配置是绝对的。

智能传输

Type: Smart URL: https://smartreceiver.cisco.com/licservice/license Proxy: Not Configured VRF:

内部的SSM

Transport: Type: cslu Cslu address: https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1

*如果9800和CSSM之间存在任何代理，请确保允许代理上列出的IP地址进行无缝通信。

测试与智能接收器的连接

从基于unix的设备使用curl命令测试智能许可访问（但该设备可能不在同一子网中，并且与9800具有相同的访问限制）：

- 卷发https://smartreceiver.cisco.com/licservice/license
- 预期响应：这是智能接收器！

测试与SSM内部服务器的连接

从基于unix的设备使用curl命令测试智能许可访问（但该设备可能不在同一子网中，并且与9800具有相同的访问限制）：

- curl -v -k https://SSM-Onprem-FQDN-address>/cslu/v1/pi/smsfloodingslup2304-1
- 预期响应：这是智能接收器！

查找接收方IP地址

使用笔记本电脑中的以下nslookup命令：

- nslookup smartreceiver.cisco.com

预期响应：

- 服务器： 171.70.168.183 ←这是DNS服务器
- 服务器： dns-sj.cisco.com ←也可显示此消息
- 地址： 10.10.10.10#53
- 姓名：smartreceiver.cisco.com
- 地址 :146.112.59.81
- 姓名：smartreceiver.cisco.com
- 地址 :2a04:e4c7:fffe::f

您的系统如何解析IP?

从您的笔记本电脑使用dig命令：

- dig smartreceiver.cisco.com +简称

预期结果

- 146.112.59.81



注意：CSSM的Smart Receiver组件已取代了旧的tools.cisco.com和MSLA客户的Rum报告、注册和计费的单一联系点。

---

ip http client source-interface <源接口>

此命令明确标记到CSSM的源路径。

ip http client secure-trustpoint SLA-TrustPoint

确保secure-trustpoint被选为SLA-TrustPoint，因为它是由授权根CA签署的。SSM内部和CSSM均受授权根CA证书信任。

CA 证书:

状态: 线上

证书序列号（十六进制）：01

证书使用：签名

颁发机构：

cn=思科许可根CA

o=思科

主题：

cn=思科许可根CA

o=思科

有效日期：

开始日期:世界协调时2013年5月30日19时48分47秒

终止日期：世界协调时2038年5月30日19点48分47秒

关联的信任点：Trustpool SLA-TrustPoint

存储：nvram:CiscoLicensi#1CA.cer

License smart sync all是从9800控制器和XML格式启动新Rum报告的命令。当在17.9.x版本中未安装信任代码的控制器上发出此命令时，它首先生成信任代码请求，而不是Rum使用情况报告。

从**CSSM**处理的信任码无效

导入信任代码：

世界协调时2024年9月17日17时35分26秒收到

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>false</success><message>已为此设备处理了对应更高信任ID的信任请求。</message><code>OLD_TRUST_ID</code><correlationID>null-null</correlationID></status></trustCode><signature>CIA g71/hlcWxUiof8VstpmPhRH8jptPZPrvaSpsuwVgLAiAQ3IUVMuS8bOHwySOB/j/3RmG4uSDq/EbUp+vfrY

CSSM期望控制器发送增量信任码ID作为安全目的，并且无效信任码会停止CSSM处理来自控制器的许可RUM请求。这最终会导致CSSM许可控制面板出现许可证管理问题。

从**CSSM**处理的有效信任码

导入信任代码：

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:XXXXXXXXX</udi><customerInfo><smartAccount>Cisco Demo内部智能帐户</smartAccount><virtualAccount>0Demo-HK-PartnerA</virtualAccount></customerAinfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c36b</piid><dateStamp>2024-09-10T07:21:30</dateStamp></subCA><trustId>110</trustId><status><success>true</sucess><correlationIXFL9R1VI3BBNtrdpBtAiEAojAqDYkGn206meTHt8+dqra0LAciHEZKxmqeurKOU0g=</signature></smartl

通信频率

可以在CLI或GUI中配置的报告间隔无效。

无论通过Web界面或CLI配置了什么报告间隔，9800 WLC都会每8小时与CSSM或内部智能软件管理器进行通信。这意味着新加入的接入点可在初次加入后8小时内显示在CSSM上。

您可以通过show license air entities summary命令确定下次计算并报告许可证的时间。此命令不是典型的show tech或show license all输出的一部分：

show license air entities summary命令:

Last license report time.....: 10:00:07.753 UTC Mon Sep 16 2024 Upcoming license report time.....: 18:00:07.808 UTC Mon Sep 16 2024 No. of APs active at last report.....: 3 No. of APs newly added with last report.....: 1 No. of APs deleted with last report.....: 0

在9800控制器上成功安装信任码后，下一阶段将通过XML格式的Rum（资源度量单位）生成许可证活动的使用报告。License smart sync all/local命令将基于控制器中管理的AP启动或生成或打开新的Rum测量。基本上，9800智能代理组件向许可模块发送API调用，以收集包含许可信息的新Rum报告。

show license rum id all命令:

This command would list CLOSED, ACK and OPEN state of Rum report on the controller. 1719005447 OPEN N air-network-advantage 1719005448 OPEN N air-dna-advantage

show license rum id 1719005447 detail 命令:

您可以获取在Rum id中报告的许可证的详细信息。此命令提取software_identifier_tag，它是CSSM数据库上的密钥匹配元素，用于验证产品实例的许可证类型。

regid.2018-06.com.cisco.DNA_NWStack，1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

智能许可使用情况报告详细信息：

==========

报告ID:1719005447

指标名称：授权

功能名称：air-network-advantage

度量值:regid.2018-06.com.cisco.DNA_NWStack，1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

UDI:PID:C9800-L-F-K9,SN:FCL2630000P

上一个报告ID:1719005445，下一个报告Id:0

状态:打开，状态更改原因：无

关闭原因：无

开始时间:9月10日10:00:08 2024 UTC，结束时间：世界协调时2024年9月16日16时15分8秒

存储状态：存在

事务 ID:0

事务消息：< 无 >

*现在，生成Rum报告。在OPEN状态下，必须将其成功提交到CSSM才能从CSSM接收ACK。

A) Verify which licenses are activated/in use - show version - show license summary - show license usage <<< it would also indicate which licenses are Perpetual vs Subscription C) Verify if enforced/export controlled license is authorized: - show license authorization D) Verify what messages were sent to/received from SSM On-Prem/CSSM - show license history message E) Check for errors - show license eventlog F) Collect detailed information/counters: - show license tech support G) Collect license tech support file - show tech-support license

在show license eventlog和/或show log的输出中报告的错误

“使用思科智能许可证实用程序(CSLU)时通信失败：未提供详细信息”

当未建立与内部的HTTPS通信时，可以观察到此错误。潜在原因：

— 特定VRF用于与OnPrem通信。必须手动配置HTTP客户端源接口

— 在SLA-Trustpoint配置下未禁用撤销检查

— 另一个信任点设置为加密信令的默认值(例如：在SIP网关上)

"HTTP服务器错误502:错误的网关”

内部开发团队目前正在调查此错误。在大多数情况下，未观察到服务影响。

通常，10秒后，SAEVT_COMM_RESTORED。

示例：

7月9日13:15:29.902:%SMART_LIC-3-COMM_FAILED:使用思科智能许可证实用程序(CSLU)的通信故障：HTTP服务器错误502:错误的网关
7月9日13:15:39.881:%SMART_LIC-5-COMM_RESTORED:恢复与思科智能许可证实用程序(CSLU)的通信

“HTTP服务器错误404: 未找到"

当传输URL指向本地(CSLU)时，尝试安装信任代码时，在Cisco IOS XE设备上观察到此错误。

仅当设备直接与CSSM通信时，才使用命令“license smart trust idtoken <token> [all|local]”。

NOTE:根据平台的不同，此消息也可能意味着在本地管理工作区的CSLU设置面板中启用了“验证设备”设置。检查您尝试注册的设备是否位于内部服务器的“SL Using Policy”选项卡中。如果设备不在该选项卡中，则需要关闭此开关。然后再次尝试让设备与内部服务器同步。有关此设置的图片，请参阅本文的结尾。

SAVET_INIT_CRYPTO success="False" error="加密初始化尚未完成"

此错误在系统引导后立即出现。约30秒后加密初始化完成 — 在这种情况下，不会对服务产生影响

。

示例：

2021-06-25 10:09:23.378 UTC SAVET_INIT_SYSTEM_INIT
2021-06-25 10:09:24.383 UTC SAVET_INIT_CRYPTO success="False" error="加密初始化未完成"
2021-06-25 10:09:54.383 UTC SAEVT_INIT_CRYPTO success="True"

如果加密初始化数分钟/小时未完成，请验证NTP配置是否存在，和/或时钟是否已同步。保存运行配置有助于重新启动加密初始化。

如果问题仍然存在，建议与思科TAC进一步调查。

SAVE_UTILITY_RUM_FAIL error="[HOST_NOT_FOUND] Device Host is not found"

“验证设备”(Validate Device)设置很可能是在内部管理工作区的CSLU设置面板中设置。

此设置帮助确保接收来自已知产品实例的RUM报告。

SAVET_COMM_FAIL error="无法解析服务器主机名/域名"

此错误表示可能由DNS解析引起的连接问题。必须确保设备可以解析目标URL。通常ip host <url> <ipassociated>命令配置错误。请检查这一点。

您很可能发现通信失败。

通信统计信息：

==========

允许的通信级别：间接

总体状态：<empty>

信任建立：

尝试次数：Total=30,Success=0,Fail=30持续故障：总体=30通信=30 <<<<<<<

上次响应：格林威治标准时间2月12日10:52:56 2023日没有答复<<<<<<<<<

失败原因：< 无 >

上次成功时间：< 无 >

上次失败时间：2月12日10:52:56 2023格林尼治标准时

Communication Level Allowed as INDIRECT表示所需的信任码未成功安装在9800控制器上。

注意：注意：CSSM是所有许可数据的真实来源。

---

*如果通过执行测试来缓解9800和CSSM之间的基本通信问题，请对智能许可通信涉及的某些模块启用调试。在9800上启用调试会在一定时间间隔内使CPU过载，因此必须在非工作时间执行这些操作。

调试

*从9800到CSSM或SSM本地的智能许可通信涉及4个模块

1.加密模块

PKI:

Crypto PKI Msg debugging is on Crypto PKI Trans debugging is on Crypto PKI callbacks debugging is on Crypto PKI Validation Path debugging is on

2. Http模块

HTTP 服务器:

HTTP Server transaction debugging is on HTTP Server tokens debugging is on HTTP Server EZSetup debugging is on HTTP Server URL debugging is on HTTP Server Authentication debugging is on HTTP Server Side Includes debugging is on HTTP Application Inout debugging is on HTTP Application Detail debugging is on HTTP Server Error debugging is on HTTP SSL Error debugging is on HTTP CTC trace debug debugging is on HTTP CTC error debug debugging is on HTTP SESSION debugging is on HTTP TPS Trace debugging is on HTTP TPS Error debugging is on HTTP WSMAN debugging is on

3. Openssl模块

ssl openssl:

TLS state debugging is on TLS msg debugging is on TLS errors debugging is on

4.智能许可模块称为智能代理，包括传输网关

许可证：

License IPC communication debugging is on License Events debugging is on License warnings and errors debugging is on

系统日志：

对证书进行服务器身份检查和SAN验证。来自加密SSL库的信任点验证。

9月16日16:29:12.236:通过主机进行服务器身份检查：10.106.43.37

9月16日16:29:12.236:要验证的服务器身份是ip地址10.106.43.37 len 12

9月16日16:29:12.329:CRYPTO_PKI:(A645F)检查相同的证书

9月16日16:29:12.329:CRYPTO_PKI（证书查找）issuer="cn=Cisco Licensing Root CA，o=Cisco" serial number= 0F 42 40

9月16日16:29:12.329:CRYPTO_PKI:(A645F)合适的信任点包括：SLA-TrustPoint、Trustpool6、Trustpool6、

9月16日16:29:12.329:CRYPTO_PKI:(A645F)尝试使用SLA-TrustPoint策略验证证书

9月16日16:29:12.329:CRYPTO_PKI:(A645F)使用SLA-TrustPoint验证证书

9月16日16:29:12.345:SSL_connect:SSL协商成功完成

9月16日16:29:12.345:SSL_connect:SSL协商成功完成

将使用情况报告提交到CSSM后，您必须看到在show license history message命令上成功更新：

请求将包含UDI_SERIAL_NUMBER、hostname、software_tag_identifier等组件，这些组件指示9800控制器使用的许可证模式以及request_type为“LICENSE_USAGE”

存在多种许可证类型：

1. ID_TOKEN_TRUST

2. TRUST_SYNC

3. LICENSE_USE

使用情况报告：

请求：世界协调时2024年9月16日16时30分16秒

"{\"sender_info\":{\"connect_info\":{\"名称\":\"C_agent\",\"版本\":\"5.8.6_rel/15\",\"生产\":true，\"additional_info\":\"\",\"功能\":[\"实用程序\",\"DLC\",\"AppHA\",\"多层\",\"EXPORT_2\",\"OK_TRY_AGAIN\",\"POLICY_usage \"、\"TELEMETRY\"、\"CSLU_V1\"]}、\"timestamp\":1726504244391、\"nonce\":\"13980553869667320622\"、\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\"、\"udi_serial_number\":\"FCL2630000P\"}、\"product_instance_identifier\":\"、\"software_tag_identifier":\"regid.2019-06.com.cisco.C99800 f_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"},\"device_list\":[{\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"},\"software_tag_identifier\":\"regid.2019-06.com.cisco.C980 l_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"product_instance_identifier\":\"\",\"product_version\":\"17.12.02\",\"hostname\":\"renjith-eap-test\",\"role\":\"活动\",\"请求类型\":\"ID_TOKEN_TRUST\",\"request_line_id\":1,\"smart_license\":

使用情况报告：

请求：世界协调时2024年9月16日16时30分16秒

"{\"sender_info\":{\"connect_info\":{\"名称\":\"C_agent\",\"版本\":\"5.8.6_rel/15\",\"生产\":true，\"additional_info\":\"\",\"功能\":[\"实用程序\",\"DLC\",\"AppHA\",\"多层\",\"EXPORT_2\",\"OK_TRY_AGAIN\",\"POLICY_usage \"、\"TELEMETRY\"、\"CSLU_V1\"]}、\"timestamp\":1726504153254、\"nonce\":\"10743401694998030696\"、\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\"、\"udi_serial_number\":\"FCL2630000P\"}、\"product_instance_identifier\":\"、\"software_tag_identifier":\"regid.2019-06.com.cisco.C99800 f_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"},\"device_list\":[{\"sudi\":{\"udi_pid\":\"C9800-

L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"},\"software_tag_identifier\":\"regid.2019-06.com.cisco.C980 l_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\",\"product_instance_identifier\":\"\",\"product_version\":\"17.12.02\",\"hostname\":\"renjith-eap-test\",\"role\":\"Active\",\"request_type\"TRUST_SYNC \",\"request_line_id\":1,\"smart_license\":

使用情况报告：

请求：世界协调时2024年9月16日16时30分16秒

{"sender_info":{"connect_info":{"name":"C_agent","version":"5.8.6_rel/15","production":true，"additional_in
L-F-
K9","udi_serial_number":"FCL2630000P"},"product_instance_identifier":"","software_tag_identifier":"regid.2
06.com.cisco.C9800_L_F_F k9,1.0_9529f872-1b08-4cac-9279-
71c391233fc2"},"device_list":[{"sudi":{"udi_pid":"C9800-L-F-
K9","udi_serial_number":"FCL2630000P"},"software_tag_identifier":"regid.2019-
06.com.cisco.C9800_L_F_F k9,1.0_9529f872-1b08-4cac-9279-
71c391233fc2","product_instance_identifier":"","product_version":"17.12.02","hostname":"renjith-
eap-test","role":"Active","request_type":"LICENSE_USAGE","request_line_id":1,"smart_license":

*了解来自CSSM或SSM内部版本的响应非常重要：

错误响应数据包：

回复 :世界协调时2024年9月16日16时30分16秒

{

"状态":"失败",

"message_code":"使用许可证时出错",

"消息":"",

"nonce":“77709655117429624”

}

此错误表示在CSSM或SSM本地许可服务器中已有一个控制器条目，该条目拒绝在数据库中添加新记录。必须从CSSM或SSM内部版本中删除活动或陈旧记录，然后重新提交Rum报告。

有效响应Poll_id :

回复 :世界协调时2024年9月16日16时29分14秒


```
{
  "sender_info":{
    "connect_info":{
      "名称":"CSLU_V1",
      "版本":"v1",
      "生产":正确 ,
      "additional_info":"",
      “功能”：[
        "实用程序",
        "DLC",
        "AppHA",
        "多层",
        "EXPORT_2",
        "OK_TRY_AGAIN",
        "POLICY_USAGE",
        "CSLU_V1",
        "CSLU_V2",
```

```
      “遥测”

    ]

  },

  "时间戳":1726504153302,

  "nonce":"10743401694998030696",

  "sudi":{

    "udi_pid":"C9800-L-F-K9",

    "udi_serial_number":"FCL2630000P"

  },

  "product_instance_identifier":"",

  "software_tag_identifier":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"

 },

 "状态":"完成",

 "license_data":[

  {

    "状态":"OK_POLL",

    "request_line_id":1,

    "sudi":{
```

```
        "udi_pid":"C9800-L-F-K9",
        "udi_serial_number":"FCL2630000P"
      },
      "poll_id":5583279046281676962,
      "poll_interval":86739,
      "智能许可证":""
    }
  ]
}
```


*如何验证poll_id存储在9800本地数据库中，以及为了获得Rum报告的确认而轮询的频率。

测试命令，以验证是否需要通过内部服务激活。

conf t service internal exit test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time 5583279046281676962 | TRUST_SYNC | 86673 | Sep 17 17:33:05 2024 UTC

*从说明中可以理解，9800控制器提交的初始请求将始终是信任代码令牌，如果没有它，9800控制器将永远不会生成新的Rum使用情况报告，因此许可证使用情况更改无法在CSSM上提交。

* License_usage的poll_id请求示例。

test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time 5583279046281677674 | LICENSE_USAGE | 87656 | Sep 17 17:33:05 2024 UTC

*如果CSSM或SSM本地数据库中已处理ACK，您可以强制9800控制器上的智能代理轮询并尽早获取ACK，而无需等待上述时间

轮询ID周期。

```
WLC#test license smart  conversion sched_poll 5583279046281676962 ?

  <0-4294967295>  delta Time in Seconds
```

相关信息

- 在9800 WLC上配置离线（气隙）许可
- 思科技术支持和下载
- 使用DNA Center策略配置Catalyst 9800 WLC智能许可

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）。