使用SLUP配置Catalyst 9800统一许可和智能许可并排除故障

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

统一许可、实施和SLUP

检查统一许可上的AP合规性

传统许可与SLUP

配置

- Direct Connect思科许可证中心
  - 由产品实例发起的
  - CSLU启动的
- 已连接到本地思科许可证中心
- 通过HTTPS代理配置智能传输
- 通信频率
- 许可证出厂重置
- 如果是RMA或硬件更换
- 从特定许可证注册(SLR)升级

故障排除

- 互联网接入、端口检查和Ping
- 系统日志
- 数据包捕获
- 显示命令
- 调试/btrace

常见问题

- WLC没有互联网接入或防火墙阻止/更改流量
- 数据包捕获中的未知CA警报

相关信息

简介

本文档介绍在Catalyst 9800 WLC上使用策略(SLUP)配置智能许可并进行故障排除。

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)

- 思科网络订用

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。

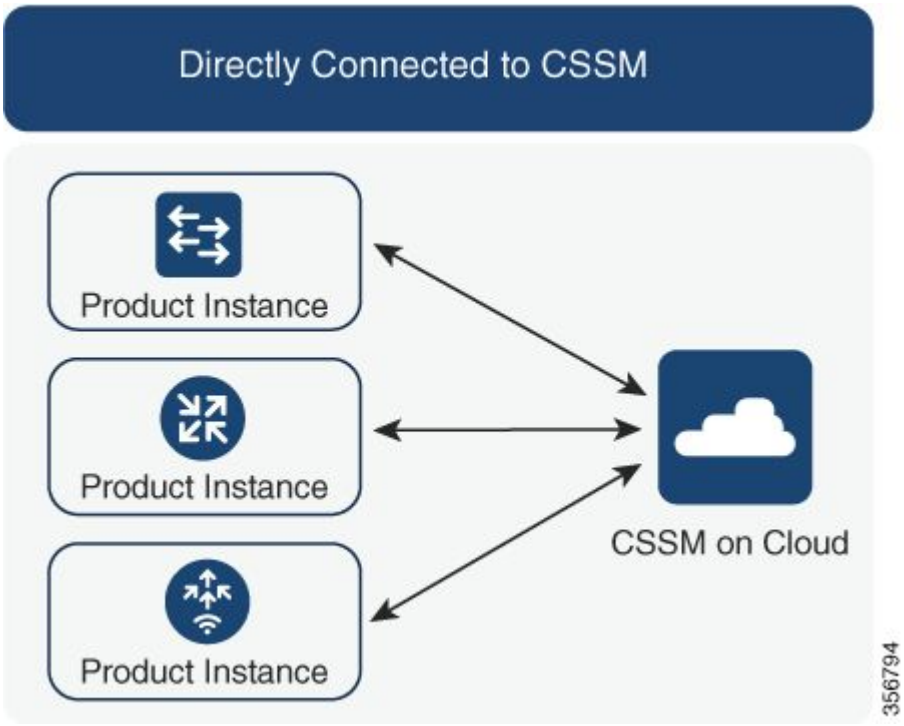
背景信息

⚠ 警告：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。

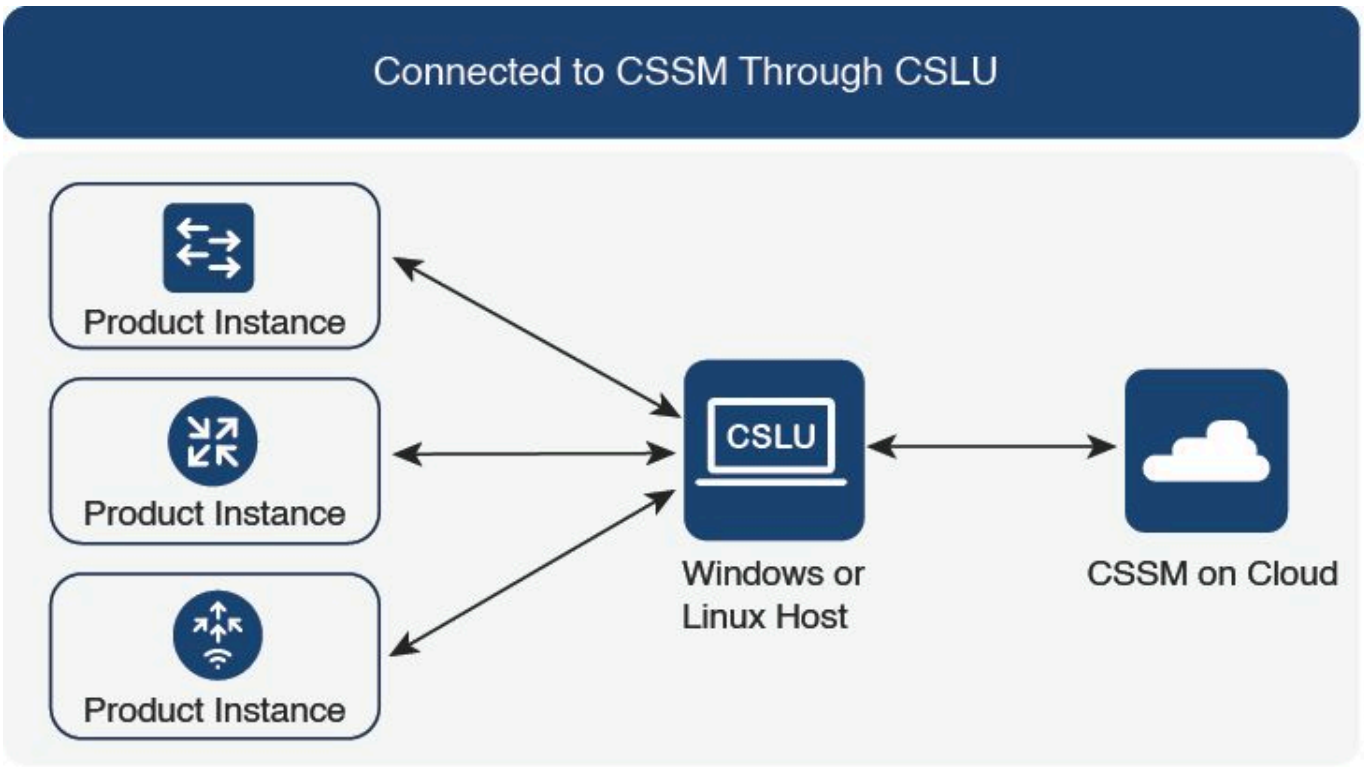
---

1. 直接连接到思科许可证中心
2. 通过CSLU（思科智能许可证实用程序管理器）连接到思科许可证中心
3. 通过思科许可证中心（内部部署）连接

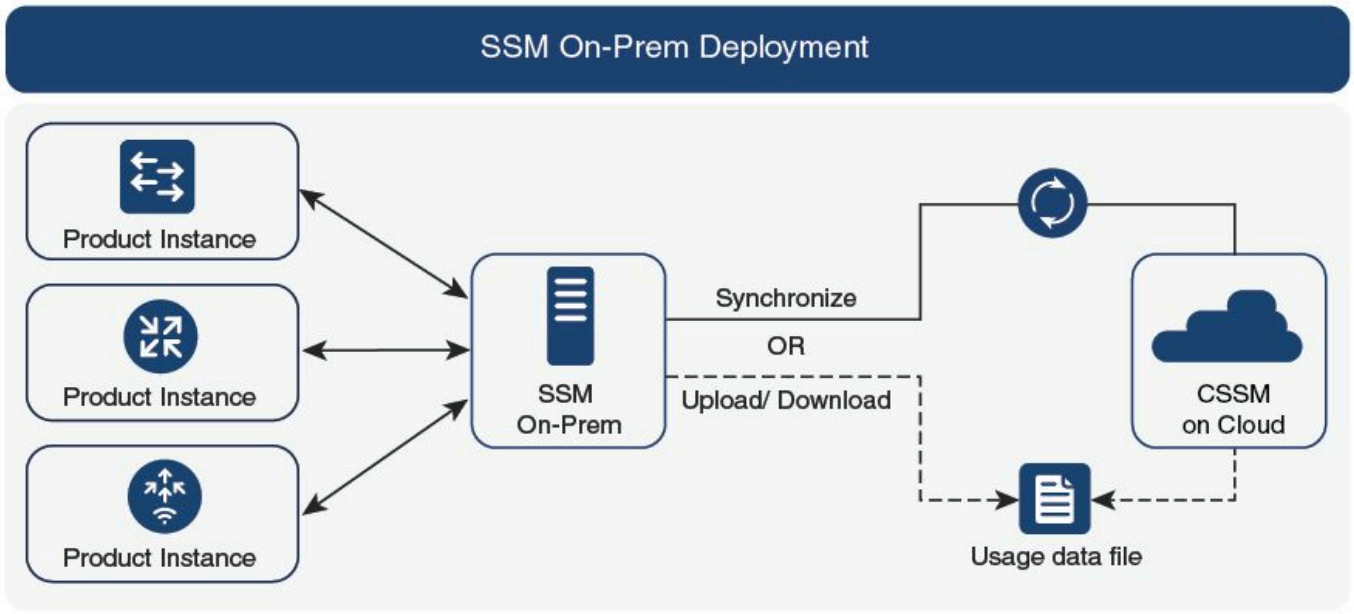
本文未涉及Catalyst 9800上的所有智能许可方案，请参阅使用策略配置的智能许可指南以获取更多信息。但是，本文确实提供了一系列有用的命令，用于对Catalyst 9800上的使用策略问题的直接连接、CSLU和内部智能许可进行故障排除。



选项1.直接连接到思科许可证中心：



选项2.通过CSLU连接：



选项3.使用思科许可证中心进行连接（内部）。

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。

统一许可、实施和SLUP

思科网络订用中提供的统一许可将许可证实施引入本地客户。

- Cisco IOS® XE 17.15.2(2024年12月)是首个支持统一许可的版本，并引入了每设备许可证报告和合规性状态。
- 未来的Cisco IOS XE版本将引入无许可AP的第0天实施和带过期许可证的设备的第N天实施。在任何不符合规定的设备上，软件映像更新后即会执行。

完成本指南中的步骤对于确保使用SLUP正确配置您的设备至关重要，这样您的设备在Cisco IOS XE软件映像升级时便无需强制执行。

检查统一许可上的AP合规性

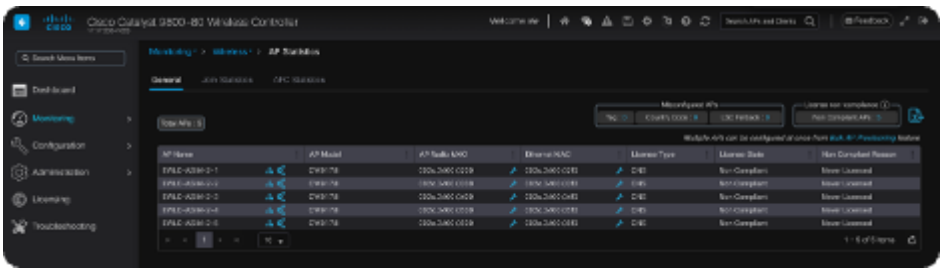


图 1：Web UI AP合规性（不合规）

AP合规性信息在控制器上（Meraki控制面板、Catalyst Center 2.3.7.9）和设备上(Web UI、CLI)提供。

图1显示了Web UI上的AP合规性信息示例。不合规AP具有Non-Compliant许可证状态，前提是假设该AP为“Never Licensed”。

正确配置SLUP后，您的AP将反映更新的合规状态。

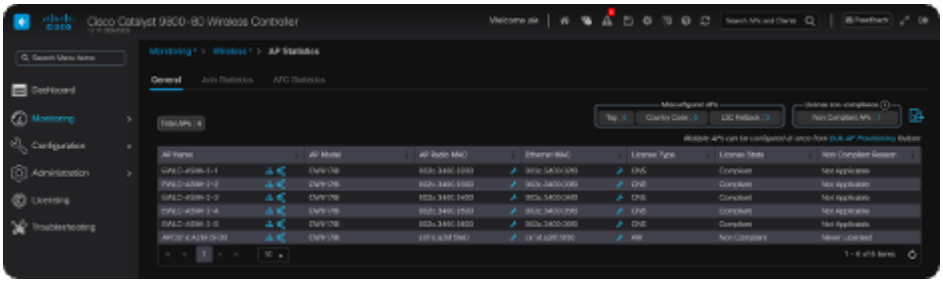


图 1：Web UI AP合规性（合规）

注意：如果您已成功配置SLUP，且接入点上仍显示“不合规状态”，则确认您已购买足够的许可，且这些许可证已存放到正确的智能帐户(SA)和虚拟帐户(VA)中。

传统许可与SLUP

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中的SLUP配置菜单，该菜单是随17.3.3版本引入的。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域与思科许可证中心通信。
- WLC现在无需注册，而是通过思科许可证中心或内部版本建立信任。
- CLI命令稍有改动。
- 不再有智能许可预留(SLR)。您可以定期手动报告使用情况。

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。

配置

Direct Connect思科许可证中心

在思科许可证中心创建令牌后，为了建立信任，需要执行这些命令。

注意：最大令牌数在HA SSO中的WLC情况下，使用次数计数必须至少为2。

```
configure terminal
ip http client source-interface



ip http client secure-trustpoint



license smart transport smart
license smart url default
exit
write memory
terminal monitor
license smart trust idtoken


        all force
```

- ip http client source-interface命令指定许可相关数据包将从中获得的L3接口。
- ip http client secure-trustpoint命令指定用于思科许可证中心通信的信任点/证书。使用show crypto pki trustpoints命令可以找到信任点名称。建议使用自签名证书TP-self-signed-xxxxxxxxxx证书或制造商安装证书（也称为MIC，仅在9800-40、9800-80和9800-L上提供），通常称为CISCO_IDEVID_SUDI。
- Terminal monitor命令使WLC将日志打印到控制台，并帮助确认信任已成功建立。可以使用terminal no monitor禁用此功能。
- 最后一个命令中的关键字all告知HA SSO集群中的所有WLC与思科许可证中心建立信任。
- 关键字force指示WLC覆盖任何以前建立的信任并尝试新的信任。

注意：如果尚未建立信任，则9800会在执行命令后1分钟后重试，并且在一段时间后不再重试。再次输入token命令以强制建立新的信任。

已连接到CSLU

Cisco Smart License Utility Manager(CSLU)是基于Windows的应用程序（在Linux上也可用），使客户能够从其本地管理许可证及其关联的产品实例，而不必直接将支持智能许可的产品实例连接到Cisco License Central。

本节仅介绍9800无线配置。使用CSLU配置许可（例如安装CSLU、配置CSLU软件等）还需要执行其他步骤，这些步骤在配置指南中介绍。无论您是要实施产品实例启动的通信方法还是CSLU启动的通信方法，还是要完成相应的任务序列。

由产品实例发起的

1. 确保从控制器到CSLU的网络可达性。
2. 确保传输类型设置为cslu:

```
(config)#license smart transport cslu
(config)#exit
#copy running-config startup-config
```

3. 如果希望由控制器发现CSLU，您需要执行操作。如果您希望使用DNS发现CSLU，则无需任何操作。如果要使用URL发现它，请输入以下命令：

```
(config)#license smart url cslu http://


       :8182/cslu/v1/pi
(config)#exit
#copy running-config startup-config
```

CSLU启动的

配置CSLU发起的通信时，需要的唯一操作是检查并确保从控制器到CSLU的网络可达性。

已连接到本地思科许可证中心

使用内部思科许可证中心的配置与直接连接非常相似。内部版本需要运行版本8-202102或更高版本。对于SLUP版本（17.3.2及更高版本），建议使用CSLU URL和传输类型。URL可从智能许可>资产> <虚拟帐户> >常规部分下的本地WebUI界面获取。

```
configure terminal
 ip http client source-interface



 ip http client secure-trustpoint



 license smart transport cslu
 license smart url cslu http://


       /cslu/v1/pi/


         (see previous paragraph on how to get exact URL)
 crypto pki trustpoint SLA-TrustPoint
  revocation-check none
 exit
write memory
terminal monitor
```

本地思科许可证中心不需要使用信任令牌。

注意：如果您正在获取消息，%PKI-3-CRL_FETCH_FAIL:信任点SLA-TrustPoint的CRL获取失败，这是因为您尚未在SLA-TrustPoint下配置revocation-check none。这是用于智能许可的信任点。在内部版本中，许可服务器上的证书通常是自签名证书，因此不能进行CRL验证，因此需要配置无撤销检查。

通过HTTPS代理配置智能传输

注意：从代码版本17.9.2开始，尚不支持经过身份验证的代理。如果您在基础设施中使用经过身份验证的代理，请考虑使用思科智能许可证实用程序管理器(CSLU)，它支持此类服务器。

要在使用智能传输模式时使用代理服务器与思科许可证中心通信，请完成以下步骤：

```
configure terminal
  ip http client source-interface



  ip http client secure-trustpoint



  license smart transport smart
  license smart url default
  license smart proxy address



  license smart proxy port



exit
write memory
terminal monitor
license smart trust idtoken


          all force
```

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配置什么报告间隔，9800 WLC都会每8小时与思科许可证中心或内部进行通信。这意味着新加入的接入点可以在初次加入后8小时内显示在思科许可证中心。

您可以使用show license air entities summary命令计算并报告许可证的下一次时间。此命令不是典型的show tech或show license all输出的一部分：

<#root>

WLC#

show license air entities summary

```
Last license report time.....................: 07:38:15.237 UTC Fri Aug 27 2021
Upcoming license report time.................: 15:38:15.972 UTC Fri Aug 27 2021
No. of APs active at last report.............: 3
No. of APs newly added with last report......: 0
No. of APs deleted with last report..........: 0
```

许可证出厂重置

Catalyst 9800 WLC可以拥有其所有许可配置和信任工厂重置，并且仍保留所有其他配置。这需要WLC重新加载：

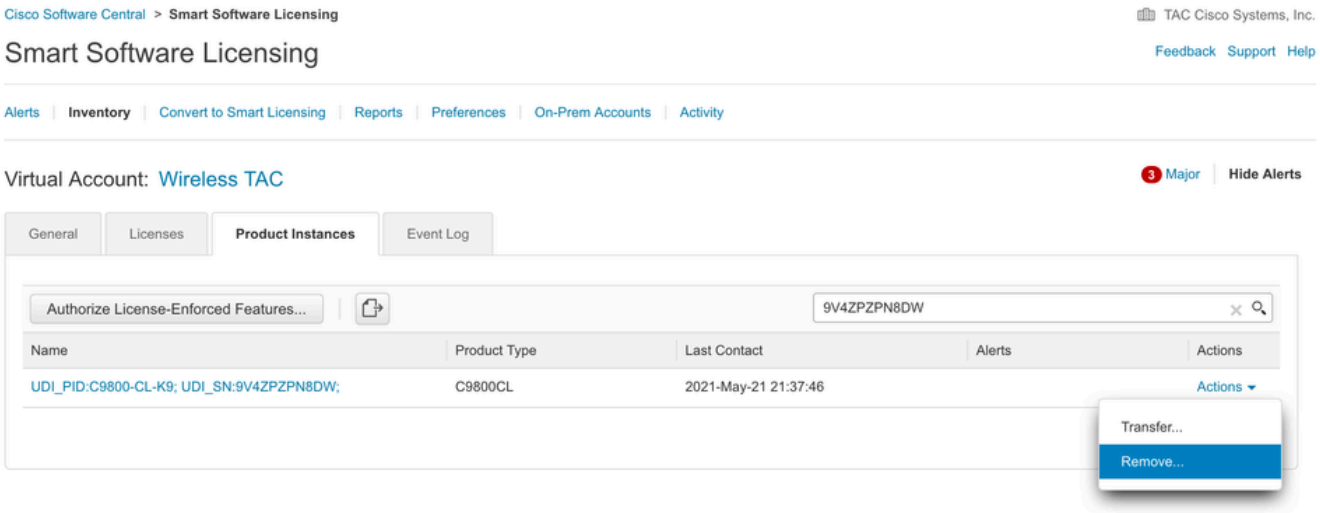
```
WLC-1#license smart factory reset
%Warning: reload required after "license smart factory reset" command
```

请务必注意，在重新设置许可证工厂后，需要等待一小时才能再次授权WLC，以备其处于AirGap模式。

如果是RMA或硬件更换

如果需要更换9800 WLC，新设备必须注册到思科许可证中心/内部版本，并且它被视为新设备。释

放之前设备的许可证计数需要在产品实例下手动删除：



从特定许可证注册(SLR)升级

早于17.3.2的早期WLC版本使用一种特殊的离线许可方法，称为特定许可证注册(SLR)。 在使用SLUP（17.3.2及更高版本）的版本中，此许可方法已被弃用。

如果您将使用SLR的9800控制器升级到17.3.2或17.4.1之后的版本，建议您迁移到离线SLR报告，而不是依赖SLR命令。保存许可证使用情况RUM文件并将其注册到智能许可门户。由于SLR在更新的版本中不再存在，因此会报告正确的许可证计数并释放所有未使用的许可证。许可证不再受阻，但会报告确切的使用计数。

故障排除

互联网接入、端口检查和Ping

新的SLUP使用smartreceiver.cisco.com域建立信任，而不是传统智能许可使用的tools.cisco.com。在撰写本文时，此域解析为多个不同的IP地址。并非所有这些地址都可执行ping操作。Ping不得用作来自WLC的Internet可达性测试。无法ping通这些服务器并不意味着它们无法正常工作。

必须使用端口443上的telnet而不是ping来测试连通性。可以根据smartreceiver.cisco.com域或直接根据服务器IP地址检查Telnet。如果流量未被阻塞，端口必须在输出中显示为打开：

```
WLC-1#telnet smartreceiver.cisco.com 443
Trying smartreceiver.cisco.com (192.330.220.90, 443)... Open <-------
[Connection to 192.330.220.90 closed by foreign host]
```

系统日志

如果在配置令牌时启用terminal monitor命令，则WLC将在CLI中打印出相关日志。如果运行show logging命令，也可以获取这些消息。成功建立的信任的日志如下所示：

```
WLC-1#license smart trust idtoken <token> all force
Aug 22 12:13:08.425: %CRYPTO_ENGINE-5-KEY_DELETED: A key named SLA-KeyPair has been removed from key st
Aug 22 12:13:08.952: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named SLA-KeyPair has been generated or impor
Aug 22 12:13:08.975: %PKI-6-CONFIGAUTOSAVE: Running configuration saved to NVRAM
Aug 22 12:13:11.879: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfully in
```

没有已定义的DNS服务器或具有无法正常工作的DNS服务器的WLC的日志：

```
Aug 23 09:19:43.486: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

在这种情况下，请验证是否配置了有效的DNS服务器。欢迎使用任何可用的公共DNS服务器IP:

```
ip name-server
```

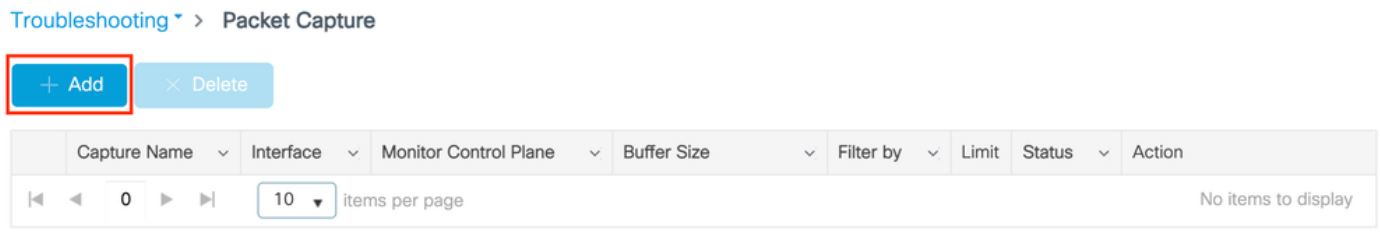
具有正常运行的DNS服务器，但没有互联网访问的WLC的日志：

```
Aug 23 09:23:30.701: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Man
```

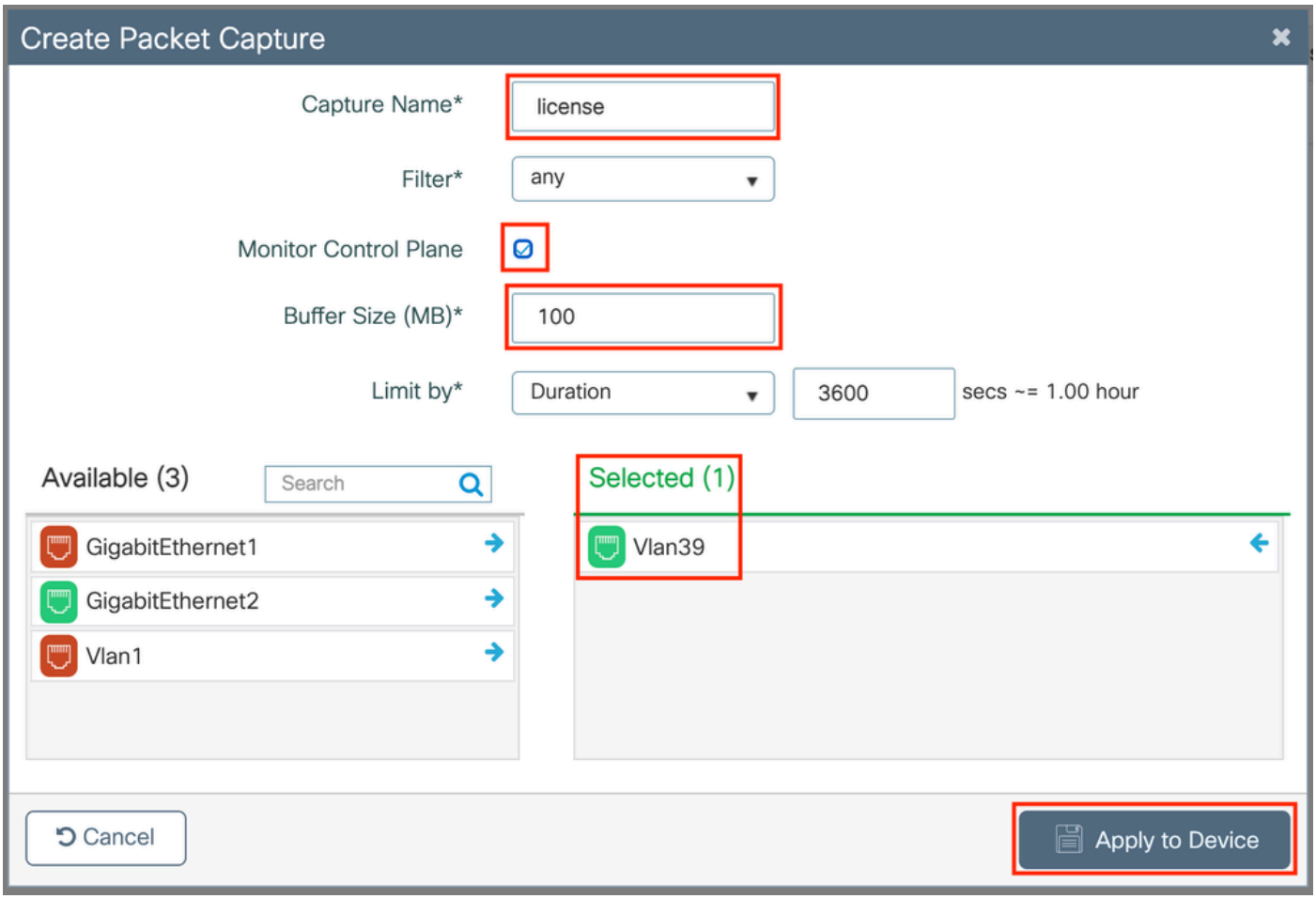
数据包捕获

即使WLC和思科许可证中心/内部许可证之间的通信已加密并通过HTTPS传输，执行数据包捕获仍可揭示导致信任无法建立的原因。收集数据包捕获的最简单方法是通过WLC Web界面。

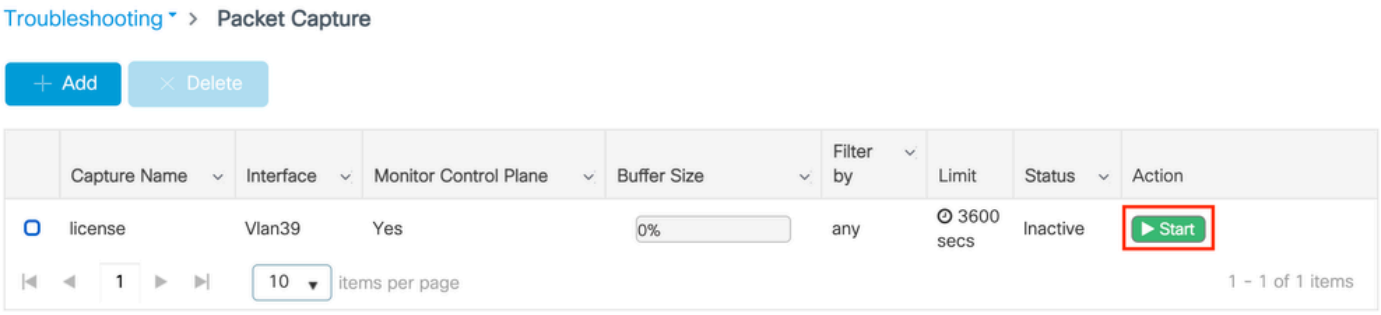
导航到故障排除>数据包捕获。创建新的捕获点：



确保Monitor Control Plane复选框已启用。将缓冲区大小增加到最大100MB。添加必须捕获的接口。默认情况下，智能许可流量从无线管理接口发出，或者从使用ip http client source-interface命令定义的接口发出：



启动捕获并运行license smart trust idtoken <token> all force命令：



信任建立的数据包捕获必须包含以下步骤：

1. 使用SYN、SYN-ACK和ACK序列建立TCP会话
2. 通过服务器和客户端证书交换建立TLS会话。建立过程以新会话票证数据包结束
3. 加密数据包交换(应用数据帧)，其中WLC报告许可证使用情况
4. 通过FIN-PSH-ACK、FIN-ACK和ACK序列终止TCP会话

注意：数据包捕获包含更多帧，包括TCP窗口更新和应用数据帧的多倍

由于思科许可证中心云使用3个不同的公有IP地址，为了过滤WLC和思科许可证中心之间的所有数据包捕获，请使用以下wireshark过滤器：

```
ip.addr==172.163.15.144 or ip.addr==192.168.220.90 or ip.addr==172.163.15.144
```

如果使用本地思科许可证中心，请过滤思科许可证中心IP地址：

```
ip.addr==
```

示例：成功建立信任的数据包捕获，与直接连接的思科许可证中心进行过滤，过滤所有重要数据包捕获：

No.	Arrival Time	Source	Destination	Protocol	Info
559	Aug 23, 2021 11:31:13.35…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [SYN] Seq=0 Win=4128 Len=0 MSS=536
576	Aug 23, 2021 11:31:13.46…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [SYN, ACK] Seq=0 Ack=1 Win=32120 Len=0 MSS=1390
578	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=1 Ack=1 Win=4128 Len=0
580	Aug 23, 2021 11:31:13.46…	192.168.10.150	192.133.220.90	TLSv1.2	Client Hello
608	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TLSv1.2	Server Hello
612	Aug 23, 2021 11:31:13.58…	192.168.10.150	192.133.220.90	TCP	[TCP Window Update] 22425 → 443 [ACK] Seq=168 Ack=537 Win=4128 Len=0
614	Aug 23, 2021 11:31:13.58…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [ACK] Seq=537 Ack=168 Win=31953 Len=536 [TCP segment of a reassembled PDU]
673	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate [TCP segment of a reassembled PDU]
675	Aug 23, 2021 11:31:13.70…	192.133.220.90	192.168.10.150	TLSv1.2	Server Key Exchange [TCP segment of a reassembled PDU]
695	Aug 23, 2021 11:31:13.71…	192.133.220.90	192.168.10.150	TLSv1.2	Certificate Request, Server Hello Done
711	Aug 23, 2021 11:31:13.85…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate, Client Key Exchange
718	Aug 23, 2021 11:31:14.01…	192.168.10.150	192.133.220.90	TLSv1.2	Certificate Verify, Change Cipher Spec, Encrypted Handshake Message
737	Aug 23, 2021 11:31:14.13…	192.133.220.90	192.168.10.150	TLSv1.2	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
745	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
747	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data
749	Aug 23, 2021 11:31:14.13…	192.168.10.150	192.133.220.90	TLSv1.2	Application Data, Application Data
22…	Aug 23, 2021 11:31:45.00…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [FIN, PSH, ACK] Seq=4306 Ack=9738 Win=3625 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.133.220.90	192.168.10.150	TCP	443 → 22425 [FIN, ACK] Seq=9738 Ack=4307 Win=31250 Len=0
22…	Aug 23, 2021 11:31:45.11…	192.168.10.150	192.133.220.90	TCP	22425 → 443 [ACK] Seq=4307 Ack=9739 Win=3625 Len=0

显示命令

以下show命令包含有关信任建立的有用信息：

```
show license status
show license summary
show license tech support
show license air entities summary

show license history message (useful to see the history and content of messages sent to SL)

show tech wireless (actually gets show log and show run on top of the rest which can be useful)
```

show license history message命令是比较有用的命令之一，因为它可以显示从WLC发送并从思科许可证中心接收回的实际消息。

成功的信任建立同时具有“REQUEST:8月23日10:18:08 2021 Central和“回应：8月23日10:18:10 2021 Central消息。如果RESPONSE行之后没有任何内容，则表示WLC未收到来自思科许可证中心的响应。

以下是成功建立信任的show license history message输出示例：


```
REQUEST: Aug 23 10:18:08 2021 Central
{"request":"{\"header\":{\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"udi_seri
NB\"},\"version\":\"1.3\",\"locale\":\"en_US.UTF-8\",\"signing_cert_serial_number\":\"3\",\"id_cert_ser
\",\"product_instance_identifier\":\"\",\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.0.9_rel/
e,\"additional_info\":\"\",\"capabilities\":[\"UTILITY\",\"DLC\",\"AppHA\",\"MULTITIER\",\"EXPORT_2\",\
Y_USAGE\"]}},\"request_data\":\"{\\\"sudi\\\":{\\\"udi_pid\\\":\\\"C9800-CL-K9\\\",\\\"udi_serial_numbe
\"},\\\"timestamp\\\":1629713888600,\\\"nonce\\\":\\\"11702702165338740293\\\",\\\"product_instance_ide
\"original_request_type\\\":\\\"LICENSE_USAGE\\\",\\\"original_piid\\\":\\\"2e84a42f-c903-44c5-83b2-e62
":7898262236}\"}","signature":{"type":"SHA256","key":"59152896","value":"eiJ7IuQaTCFxgUkwls76WZxa5DRI5A
OgMqQd5POU6VNsH2j9dHco4T1NJ/aCMbR1MRmkfxyVSWsx4lmjJL1lmpOSi3ZS4FBMvlF/EBOUfowREe2oz2lrQp1cAFpPn5SlaFezW
/Nu6SQZfIW+IdF+2qnJeNFAIZbNpgOB5d5HIJvDmDImvDu3bMRHhQAWr2KKzGFr6jPzOhs7bGY/+FlfTLQk5LFEUaKTNH/tuxJPFHlF
h9//uhsd+NaQyfdRFludkbfUBTFkvPxHW9/5w=="}}

  RESPONSE: Aug 23 10:18:10 2021 Central
{"signature":{"type":"SHA256","value":"TXZE034fqAul2jy9V4+HoB2hDShl9au/5sgodiCVatmu671/6MyN7kZfEzREufY8
SLrjTfO4grGeQTcH7yEjOD+gztWXCOu8RBT7/Bo9aBs\n4x1iOE6flPB3BP6yu7KIEUQZ8yHzlwDT+mVtJGi6TRrtYnV3KQMpCUmF5F
wOksf3SfXreNZJuzWXzjHvtmlusCQXw7ZTBzffYsNKOOlkJlr\nvgB2PkV7JUlsA481kpIvlPul6IiJXqk+2PC2IzCrCLG57lVN3XgX
1pEl2SHyQ/DAw==","piid":null,"cert_sn":null},"response":"{\"header\":{\"version\":\"1.3\",\"locale\":\"
mp\":1629713890172,\"nonce\":null,\"request_type\":\"POLL_REQ\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\
9PJK8D7OCNB\"},\"agent_actions\":null,\"connect_info\":{\"name\":\"SSM\",\"version\":\"1.3\",\"producti
s\":[\"DLC\",\"AppHA\",\"EXPORT_2\",\"POLICY_USAGE\",\"UTILITY\"],\"additional_info\":\"\"},\"signing_c
\",\"id_cert_serial_number\":\"59152896\",\"product_instance_identifier\":\"\"},\"status_code\":\"FAILE
\"Invalid ProductInstanceIdentifier: 2e84a42f-c903-44c5-83b2-e62e258c780f provided in the polling reque
262236\",\"retry_time_seconds\":0,\"response_data\":\"\"}","sch_response":null}
```


调试/btrace

使用license smart trust idtoken all force命令尝试建立信任后几分钟运行此命令。IOSRP日志非常详细。附加 | include smart-agent”到命令以仅获取智能许可日志。

```
show logging process iosrp start last 5 minutes
show logging process iosrp start last 5 minutes | include smart-agent
```

您还可以运行这些调试，然后重新配置许可命令以强制建立新连接：

```
debug license events
debug license errors
debug license agent all
```

常见问题

WLC没有互联网接入或防火墙阻止/更改流量

WLC上的嵌入式数据包捕获是查看WLC是否从思科许可证中心或内部收到任何信息的简单方法。如果没有响应，防火墙可能会阻止某些内容。

如果未收到来自思科许可证中心云或内部云的响应，show license history message命令会在发出请求后1秒打印空响应。

例如，这可能使您相信已收到空响应，但实际上根本没有响应：

```
REQUEST: Jun 29 11:12:39 2021 CET
{"request":"{\"header\":{\"request_type\":\"ID_TOKEN_TRUST\",\"sudi\":{\"udi_pid\":\"C9800-CL-K9\",\"ud
RESPONSE: Jun 29 11:12:40 2021 CET
```

> 注意：当前存在增强请求Cisco Bug ID CSCvy84684，该请求使show license history消息在没有响应时打印空响应。这是为了增强show license history message命令的输出

数据包捕获中的未知CA警报

与Cisco License Central或On-prem的通信需要9800端的良好证书。它可以自签名，但不能无效或过期。在这种情况下，数据包捕获会显示当9800 HTTP客户端证书过期时思科许可证中心发送的未知CA的TLS警报。

智能许可使用ip http client配置，该配置不同于WLC Web界面使用的ip http server。这意味着需要正确配置以下命令：

```
ip http client source-interface
```

```
ip http client secure-trustpoint
```

使用show crypto pki trustpoints命令可以找到信任点名称。建议使用自签名证书TP-self-signed-xxxxxxxxxx证书或制造商安装证书(MIC)，通常称为CISCO_IDVID_SUDI，仅在9800-80、9800-40和9800-L上提供。

请注意，执行TLS侦听的设备（例如具有SSL解密功能的防火墙）可能会阻止C9800与思科许可服务器建立成功的握手，因为提供的HTTPS证书是防火墙证书而不是思科许可服务器证书。

注意：确保同时配置source-interface和secure-trustpoint命令。即使WLC只有一个L3接口，也需要source-interface命令。

相关信息

- 在9800上使用气隙模式的智能许可
- 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）。