

Catalyst 9000交换机上的SLP智能传输故障排除

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍如何使用Catalyst 9000交换机上的智能传输对使用策略(SLP)的智能许可进行故障排除。

先决条件

要求

思科建议您了解并熟悉以下主题：

- 在Cisco IOS® XE设备上使用策略的智能许可。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9200
- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS XE 17.9.1及更高版本



注意：有关在其他思科平台上启用这些功能所使用的命令，请参阅相应的配置指南。

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

使用策略的智能许可是智能许可的增强版本，其设计的主要目标是提供许可解决方案，确保您的网络运营保持不间断。它不是破坏性的，而是建立合规性关系，说明您购买和使用的硬件和软件许可证。

为使智能许可报告正常工作，Catalyst 9000交换机与思科智能软件管理器(CSSM)连接以报告许可证使用情况。CSSM是一个集中式平台，用于管理所有思科软件许可证并审核使用情况，这有助于规划未来的许可需求。

Catalyst 9000交换机可通过多种拓扑连接到CSSM，但本文档重点介绍交换机直接连接到CSSM的特定拓扑。这意味着交换机必须能够与托管在Internet上的CSSM连接并建立连接。

在此直接连接拓扑中，有两个传输选项：Smart Transport和Call Home，建议使用Smart Transport。此外，智能传输支持使用HTTPS代理并允许选择特定VRF来处理与CSSM的智能许可通信。

使用智能传输时，Catalyst 9000交换机在HTTPS消息中与CSSM以JavaScript对象表示法(JSON)格式交换许可证使用信息。此信息称为RUM报告，由交换机发送，来自CSSM的响应称为ACK。

此拓扑的最小报告频率被限制为一天。这意味着产品实例每天最多发送一个RUM报告，从而防止针对某些许可证生成和传输过多的报告。这有助于解决因RUM报告超量生成导致的内存相关问题和系统减速。

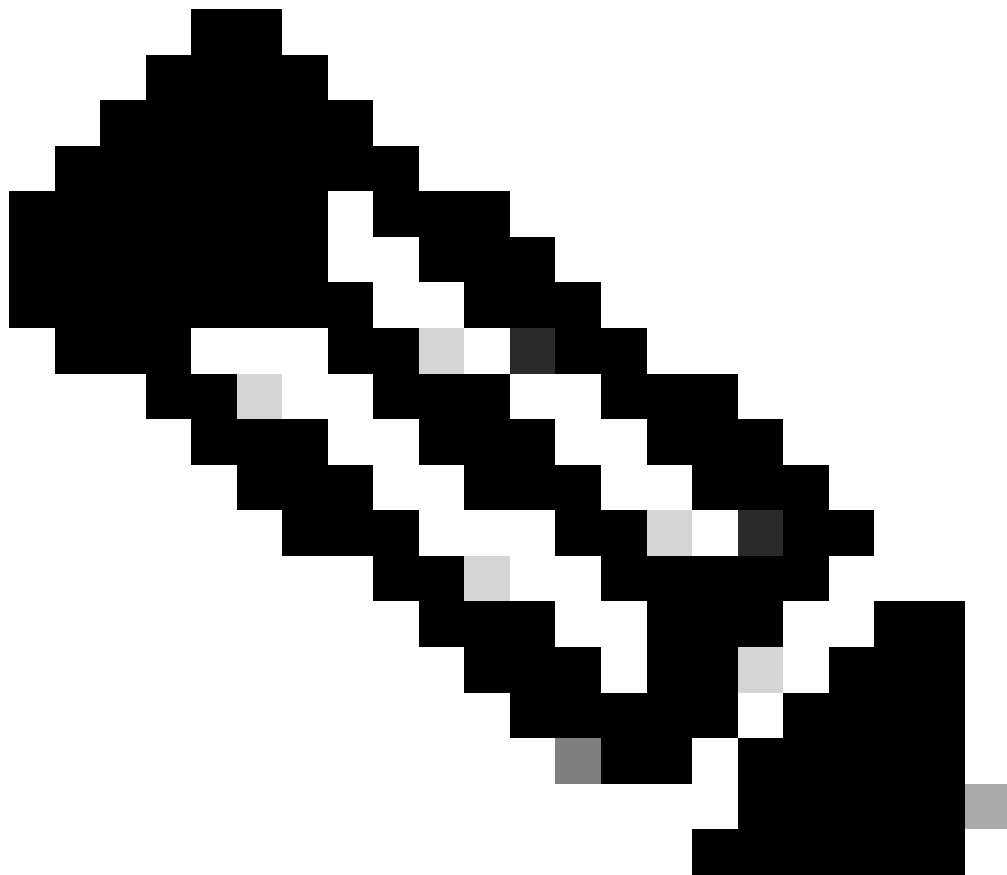
如果需要，您可以在特权EXEC模式下使用`license smart sync`命令来覆盖此限制

配置

按照以下步骤使用智能传输配置SLP:

1. 将智能配置为传输类型，并使用默认URL。

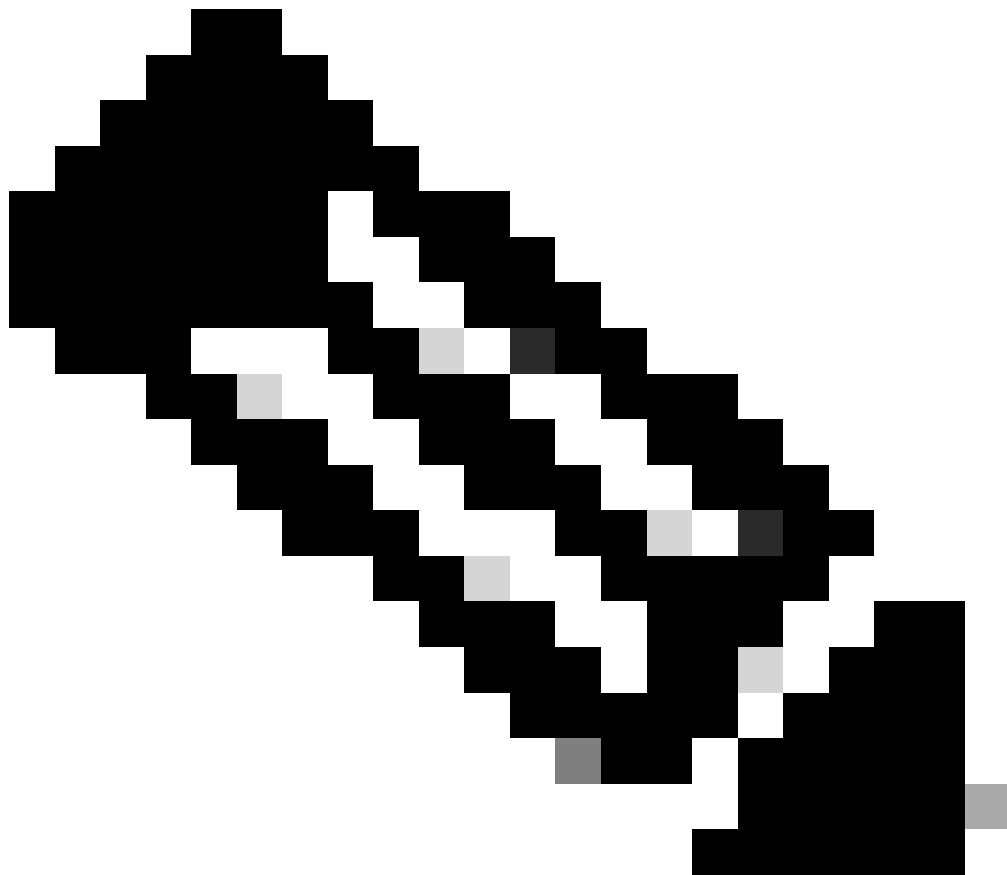
```
Switch#configure terminal
Switch(config)#license smart transport smart
Switch(config)#license smart url default
```



注意：如果将VRF用于智能传输license smart vrf，则需要配置。

2. 为DNS解析和HTTP客户端连接配置DNS服务器和源接口。

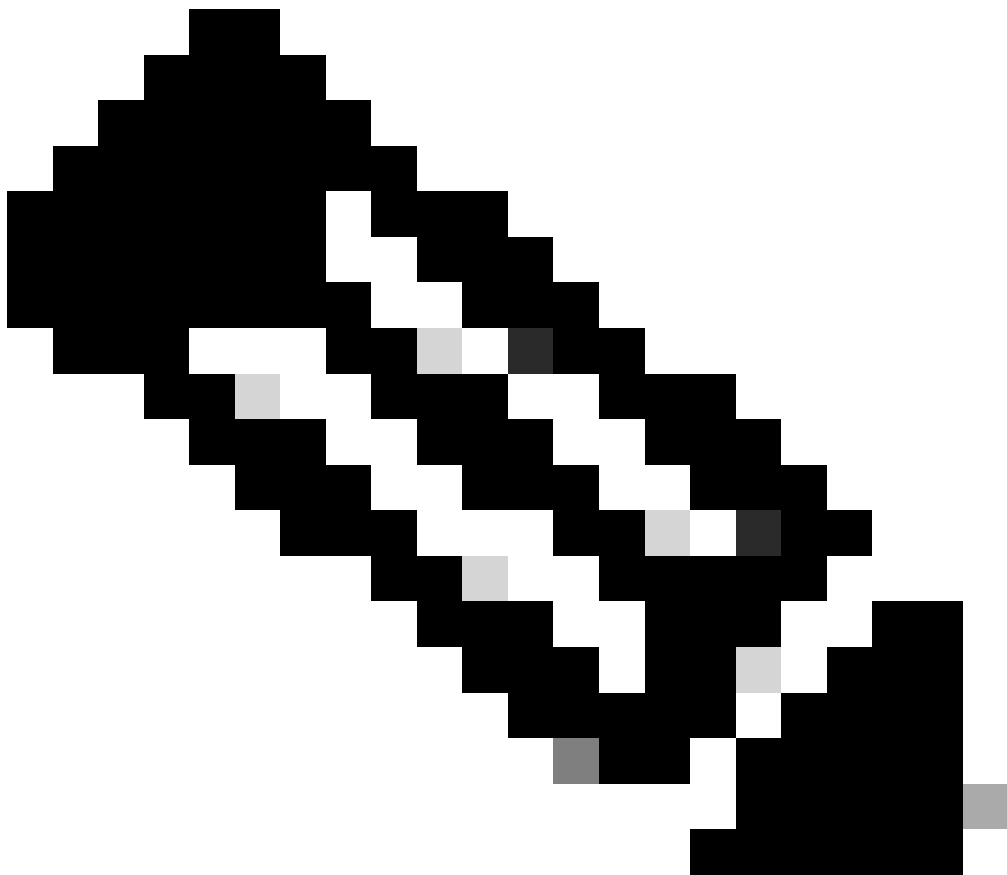
```
Switch(config)#ip domain lookup
Switch(config)#ip name-server 10.31.104.74
Switch(config)#ip domain name cisco.com
Switch(config)#ip domain lookup source-interface Vlan10
```



注意：如果将VRF用于智能传输，则需要使用这些命令的VRF变体。

3. 如果需要，请配置HTTPS代理。

```
Switch(config)#license smart proxy address 192.168.217.105  
Switch(config)#license smart proxy port 80
```



注意：可以使用代理服务器的IP地址或主机名配置代理服务器。

-
4. 在虚拟帐户中生成令牌。要完成此步骤，请按照本文档中概述的[流程操作](#)。
 5. 在交换机上安装信任代码。

```
Switch#license smart trust idtoken NGFkODgzMGUtZmNkMS00NTRjLWI5MjUtYjI0YWYzZjU1ZGQzLTE3NDAYNjU5%OA  
[OK]
```

使用CSSM成功建立信任后，将显示类似如下的系统日志。

```
*Jan 24 23:19:05.144: %SMART_LIC-6-TRUST_INSTALL_SUCCESS: A new licensing trust code was successfu
```

此外show license status，还显示信任代码安装时间。

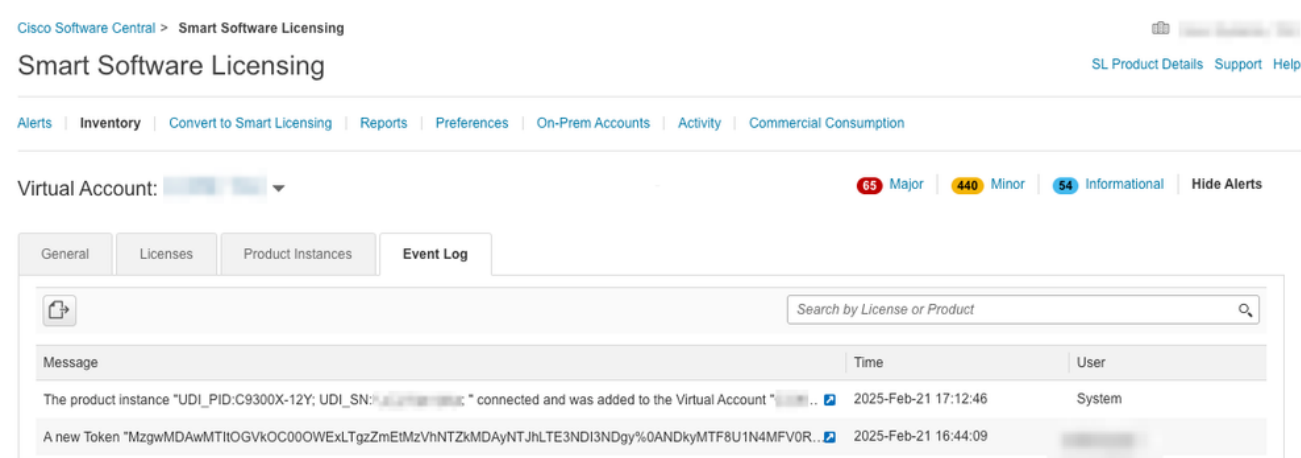
```
<#root>

Switch#show license status | i Trust

Trust Code Installed: Jan 24 23:19:05 2025 UTC

<--- Trust code was installed
```

最后，虚拟帐户事件日志显示交换机已添加。



显示设备的虚拟帐户事件日志。

故障排除

如果使用CSSM建立信任失败，将显示指示失败原因的系统日志。

*Jan 24 15:17:46.341: %SMART_LIC-3-COMM_FAILED: Communications failure with the Cisco Smart Software Ma

通信失败的可能原因包括：

- 无法解析服务器主机名/域名：DNS未解析智能传输URL或代理服务器主机名。验证DNS服务器的名称解析配置和可达性。
- 连接超时：已尝试连接，但没有响应。使用数据包捕获验证正在建立与CSSM的HTTPS连接，并检查设备（如代理服务器或防火墙）是否正在阻止连接。如果使用代理服务器，请确保使用正确的端口。

按照以下步骤和验证命令对使用智能传输的SLP进行故障排除：

1. 验证智能许可事件日志。

```
<#root>
```

```
Switch#
```

```
show license eventlog 1
```

```
**** Event Log ****
```

```
2025-01-24 13:58:23.900 UTC SAEVT_INIT_START version="5.5.29_re1/114"
2025-01-24 13:58:23.922 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:58:23.922 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:27.620 UTC SAEVT_READY
2025-01-24 13:58:27.621 UTC SAEVT_ENABLED
2025-01-24 13:58:27.665 UTC SAEVT_EXPORT_FLAG exportAllowed="False"
2025-01-24 13:58:27.732 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.742 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.744 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:27.763 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.767 UTC SAEVT_TAG_AUTHORIZED count="1" entitlementTag="regid.2017-05.com.cisco
2025-01-24 13:58:27.767 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_SYSDAT
2025-01-24 13:58:27.768 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_LICENS
2025-01-24 13:58:30.425 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmInitialize"
2025-01-24 13:58:30.431 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>"
2025-01-24 13:58:30.431 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmRegister"
2025-01-24 13:58:37.975 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_CHASSIS_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.048 UTC SAEVT_HA_ROLE udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:38.062 UTC SAEVT_INIT_CONFIG_READ_BEGIN
2025-01-24 13:58:40.884 UTC SAEVT_HOSTNAME_CHANGE
2025-01-24 13:58:41.734 UTC SAEVT_HA_EVENT eventType="SmartAgentSetNVPairs"
2025-01-24 13:58:42.408 UTC SAEVT_INIT_CONFIG_READ_DONE
2025-01-24 13:58:42.531 UTC SAEVT_PLATFORM eventSource="INFRA_SL" eventName="INFRA_SL_EVLOG_OIR_AD
2025-01-24 13:58:42.531 UTC SAEVT_HA_CONFIG
2025-01-24 13:58:42.531 UTC SAEVT_HA_UDI udi="PID:C9300-48UN,SN:<SN>" haRole="Active"
2025-01-24 13:58:42.732 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:42.744 UTC SAEVT_LICENSE_USAGE count="0" type="destroy" entitlementTag="regid.201
2025-01-24 13:58:43.140 UTC SAEVT_INIT_SYSTEM_INIT
2025-01-24 13:58:44.143 UTC SAEVT_INIT_CRYPT0 success="False" error="Crypto Initialization has not
2025-01-24 13:59:14.143 UTC SAEVT_INIT_CRYPT0 success="True"
2025-01-24 13:59:14.144 UTC SAEVT_COMM_RESTORED
2025-01-24 13:59:14.176 UTC SAEVT_INIT_COMPLETE
2025-01-24 14:00:14.145 UTC SAEVT_PRIVACY_CHANGED enabled="True"
2025-01-24 14:00:27.432 UTC
```

```
SAEVT_UTILITY_REPORT_START
```

```
2025-01-24 15:17:46.341 UTC
```

```
SAEVT_COMM_FAIL error="Connection timed out". <--- Connection timed out
```

```
2025-01-24 15:35:22.627 UTC SAEVT_COMM_RESTORED <--- Communication with CSSM restored
```

2. 通过发送ping和尝试telnet连接验证与CSSM的连接。这将验证名称解析是否正在进行，并且交换机和CSSM之间没有管理块。

```
<#root>
```

```
Switch#
```

```
show ip interface brief | exclude unassigned
```

Interface	IP-Address	OK?	Method	Status	Protocol
Vlan10	10.31.121.118				
YES	DHCP	up		up	

```
Switch#
```

```
ping smartreceiver.cisco.com source Vlan10
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to X.X.X.X, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5)
```

```
, round-trip min/avg/max = 364/365/368 ms
```

```
Switch#
```

```
telnet smartreceiver.cisco.com 443 /ipv4 /source-interface vlan10
```

```
Trying X.X.X.X, 80 ...
```

```
Open
```

```
[Connection to X.X.X.X closed by foreign host]
```

或者，如果使用的是代理服务器，您可以使用代理服务器的IP地址和端口尝试相同的命令。

```
<#root>
```

```
Switch#
```

```
ping 192.168.217.105
```

```
Type escape sequence to abort.
```

```
Sending 5, 100-byte ICMP Echos to 192.168.217.105, timeout is 2 seconds:
```

```
!!!!!
```

```
Success rate is 100 percent (5/5)
```

```
, round-trip min/avg/max = 364/365/368 ms
```

```
Switch#
```

```
telnet 192.168.217.105 80 /ipv4 /source-interface vlan10
```

Trying 192.168.217.105, 80 ...

Open

[Connection to 192.168.217.105 closed by foreign host]

3. 验证RUM报告是否正在发送以及是否有响应。

<#root>

Switch#

show license history message

Message History (oldest to newest):

=====

Trust Establishment:

REQUEST: Jan 24 23:18:59 2025 UTC <--- RUM report was sent

{"request":{"header":{"request_type":"ID_TOKEN_TRUST","sudi":{"udi_pid":"C9300-48UN",

RESPONSE: Jan 24 23:19:05 2025 UTC <--- Response from CSSM was received

{"signature":{"type":null,"value":null,"piid":null,"cert_sn":null},"response":{"header":{"vers

Usage Reporting:

No past history

Result Polling:

No past history

Authorization Request:

No past history

Authorization Return:

No past history

Trust Sync:

No past history

Import Message History (oldest to newest):

=====

Import POLICY:

No past Import history

Import AUTH:

No past Import history

Import TRUST CODE:

Received on Jan 24 23:19:05 2025 UTC

<TRUST_CODE>

Import RUM ACK:

No past Import history

Import CONVERSION ACK:

No past Import history

Import ACCOUNT INFO:

Last policy received on Jan 24 23:19:05 2025 UTC

<ACCOUNT_INFO>

Switch#

show license tech support | sec Trust

Trust Establishment:

Attempts: Total=1,

Success=1

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC <--- Trust establishment succeeded

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts: Total=1,

Success=1,

Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:50 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:50 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:

, state[2], Trust Data INSTALLED TrustId:612

Overall Trust: INSTALLED (2) <--- Trust code installed

如果发送了请求但没有CSSM响应，则命令不会显示给定响应的JSON数据。如果发送了请求但没有CSSM响应，则命令不会显示给定响应的JSON数据show license history message，并且可以获得有关故障的更多详细信息。

<#root>

Switch#

show license history message

! <--- Output omitted for brevity --->

Trust Establishment:

REQUEST: Feb 21 16:54:49 2025 UTC

{"request":{"header":{"request_type":"ID_TOKEN_TRUST"},"sudi":{"udi_pid":"C9300X-12Y",

RESPONSE: Feb 21 16:54:49 2025 UTC

<--- The line is empty, which means there was no response from CSSM

REQUEST: Feb 21 16:55:19 2025 UTC

{"request":{"header":{"request_type":"ID_TOKEN_TRUST"},"sudi":{"udi_pid":"C9300X-12Y",

! <--- Output omitted for brevity --->

Switch#

show license tech support | sec Trust

Trust Establishment:

Attempts: Total=2, Success=0,

Fail=2

Ongoing Failure: Overall=2 Communication=2

Last Response: NO REPLY on Feb 21 16:55:39 2025 UTC

<--- Failure reason was NO REPLY

Failure Reason: <none>

Last Success Time: <none>

Last Failure Time: Feb 21 16:55:39 2025 UTC

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: <none>

Failure Reason: <none>

Last Success Time: <none>

Last Failure Time: <none>

Trust Sync:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: <none>

Failure Reason: <none>

Last Success Time: <none>

Last Failure Time: <none>

Trusted Store Interface: True
Local Device: P:C9300-48UN,S:<SN>, state[1],

NOT INSTALLED

TrustId:605

<--- Trust point exists but it is not installed yet

Overall Trust: No ID

4. 触发交换机发送RUM报告以与CSSM同步。

<#root>

Switch#

show clock

***23:38:54.683 UTC Fri Jan 24 2025**

Switch#

show license tech support | i Utility

Utility:

Start Utility Measurements: Jan 24 23:35:55 2025 UTC (4 minutes, 38 seconds remaining)

Send Utility RUM reports: Feb 23 23:20:56 2025 UTC (29 days, 23 hours, 49 minutes, 39 seconds remaining)

Process Utility RUM reports: Jan 25 23:30:58 2025 UTC (23 hours, 59 minutes, 41 seconds remaining)

Switch#

show license history message | i REQUEST

REQUEST: Jan 24 23:18:59 2025 UTC

REQUEST: Jan 24 23:20:50 2025 UTC

REQUEST: Jan 24 23:25:55 2025 UTC

REQUEST: Jan 24 23:19:41 2025 UTC

Switch#

license smart sync all <--- Trigger synchronization

Switch#

show license history message | i REQUEST

REQUEST: Jan 24 23:18:59 2025 UTC

REQUEST: Jan 24 23:20:50 2025 UTC

REQUEST: Jan 24 23:25:55 2025 UTC

REQUEST: Jan 24 23:19:41 2025 UTC

REQUEST: Jan 24 23:39:05 2025 UTC

<--- New RUM report was sent

Switch#

show license tech support | sec Trust

Trust Establishment:

Attempts: Total=1, Success=1, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:19:05 2025 UTC

Failure Reason:

Last Success Time: Jan 24 23:19:05 2025 UTC

Last Failure Time:

Trust Acknowledgement:

Attempts: Total=0, Success=0, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response:

Failure Reason:

Last Success Time:

Last Failure Time:

Trust Sync:

Attempts:

Total=2, Success=2

, Fail=0 Ongoing Failure: Overall=0 Communication=0

Last Response: OK on Jan 24 23:39:14 2025 UTC <--- Successful response from CSSM

Failure Reason:

Last Success Time: Jan 24 23:39:14 2025 UTC

Last Failure Time:

Trusted Store Interface: True

Local Device: P:C9300-48UN,S:<SN>, state[2], Trust Data INSTALLED TrustId:612

Overall Trust: INSTALLED (2)

5. 要验证交换机是否正在与CSSM建立HTTPS连接，可以捕获数据包。这是使用代理服务器成功连接的数据包捕获示例。

<#root>

Switch#

sh ip cef 10.31.104.78

0.0.0.0/0

nexthop 10.31.121.65 Vlan10

Switch#

sh ip arp 10.31.121.65

Protocol	Address	Age (min)	Hardware Addr	Type	Interface
Internet	10.31.121.65	0			

2c31.24b1.6bc6

ARPA Vlan10

Switch#

show mac address-table address 2c31.24b1.6bc6

Mac Address Table

Vlan	Mac Address	Type	Ports
10	2c31.24b1.6bc6	DYNAMIC	

Fi1/0/48

Total Mac Addresses for this criterion: 1

Switch#

monitor capture CSSM interface Fi1/0/48 both match any

Switch#

monitor capture CSSM start

Started capture point : CSSM

Switch#

show clock

*

15:41:10.058 UTC

Fri Jan 24 2025

Switch#

license smart sync all

Switch#sh license hist mess | i REQUEST

REQUEST: Jan 24 15:35:17 2025 UTC

REQUEST: Jan 24 15:41:58 2025 UTC

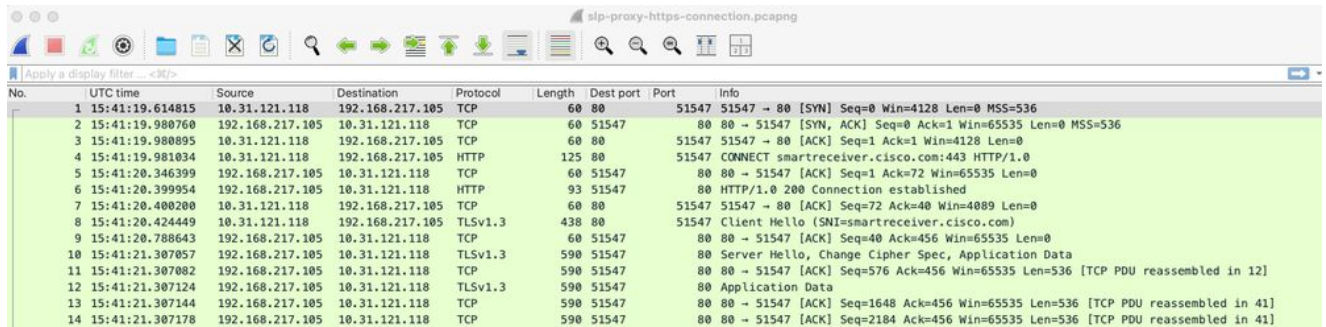
Switch#

monitor capture CSSM stop

Switch#

monitor capture CSSM export location flash:slp-proxy-https-connection.pcap

Export Started Successfully



No.	Time	Source	Destination	Protocol	Length	Dest port	Port	Info
1	15:41:19.614815	10.31.121.118	192.168.217.105	TCP	60	80	51547	80 → 51547 [SYN] Seq=0 Win=4128 Len=0 MSS=536
2	15:41:19.980760	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=536
3	15:41:19.980895	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=1 Ack=1 Win=4128 Len=0
4	15:41:19.981034	10.31.121.118	192.168.217.105	HTTP	125	80	51547	CONNECT smartreceiver.cisco.com:443 HTTP/1.0
5	15:41:20.346399	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=1 Ack=72 Win=65535 Len=0
6	15:41:20.399954	192.168.217.105	10.31.121.118	HTTP	93	51547	80	HTTP/1.0 200 Connection established
7	15:41:20.400200	10.31.121.118	192.168.217.105	TCP	60	80	51547	51547 → 80 [ACK] Seq=72 Ack=40 Win=4089 Len=0
8	15:41:20.424449	10.31.121.118	192.168.217.105	TLSv1.3	438	80	51547	Client Hello (SNI=smartreceiver.cisco.com)
9	15:41:20.788643	192.168.217.105	10.31.121.118	TCP	60	51547	80	80 → 51547 [ACK] Seq=40 Ack=456 Win=65535 Len=0
10	15:41:21.307057	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Server Hello, Change Cipher Spec, Application Data
11	15:41:21.307082	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=576 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 12]
12	15:41:21.307124	192.168.217.105	10.31.121.118	TLSv1.3	590	51547	80	Application Data
13	15:41:21.307144	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=1648 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]
14	15:41:21.307178	192.168.217.105	10.31.121.118	TCP	590	51547	80	80 → 51547 [ACK] Seq=2184 Ack=456 Win=65535 Len=536 [TCP PDU reassembled in 41]

使用代理服务器成功与CSSM建立HTTPS连接的数据包捕获。

- 如果数据包捕获显示HTTPS连接正在尝试建立，但失败，则可能是因为TLS或SSL握手失败。这些调试可用于进一步调查。

```
debug ip http client all
debug ssl openssl states
debug ssl openssl errors
debug crypto pki messages
debug crypto pki transactions
```

- 如果任何时候需要从交换机删除已安装的信任代码，则可以执行智能许可工厂重置。此过程需要重新加载。重置出厂设置后，可以安装新的信任代码。使用此命令可删除所有许可信息，包括策略。

```
<#root>
```

```
Switch#
```

```
license smart factory reset
```

```
%Warning: reload required after "license smart factory reset" command
```

```
Switch#
```

```
show license status | include Trust
```

```
Trust Code Installed:
```

```
<--- Installed trust code now shows none
```

```
Switch#
```

reload

相关信息

- [Cisco Catalyst 9000系列交换机的智能许可使用策略](#)
- [了解Catalyst交换的智能许可](#)
- [Cisco Live:使用策略的智能许可简介](#)
- [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）。