Problembehandlung bei Smart Licensing mit Richtlinienproblemen bei 9800

Inhalt

Einleitung

In diesem Dokument werden erweiterte Schritte zur Fehlerbehebung im Rahmen der Smart Licensing Using Policy (SLUP)-Richtlinie für den Catalyst 9800 Wireless LAN-Controller beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

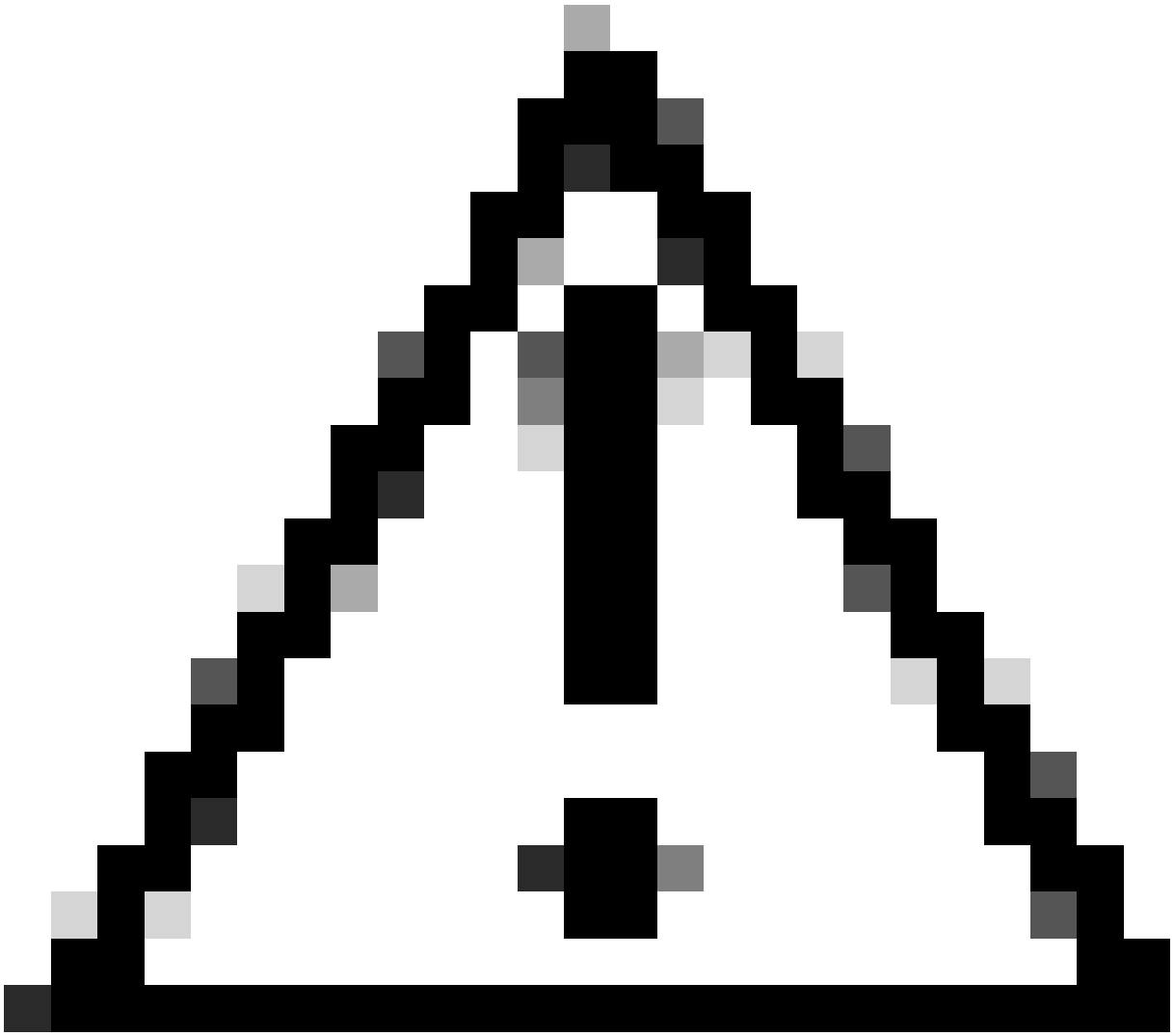
- Smart Licensing-Nutzungsrichtlinie (SLUP)
- Catalyst 9800 Wireless LAN-Controller (WLC)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen



Vorsicht: Vorsicht: Hinweise in diesem Artikel enthalten nützliche Vorschläge oder Verweise auf Material, das nicht in diesem Dokument behandelt wird. Es wird empfohlen, dass Sie jede Note lesen.

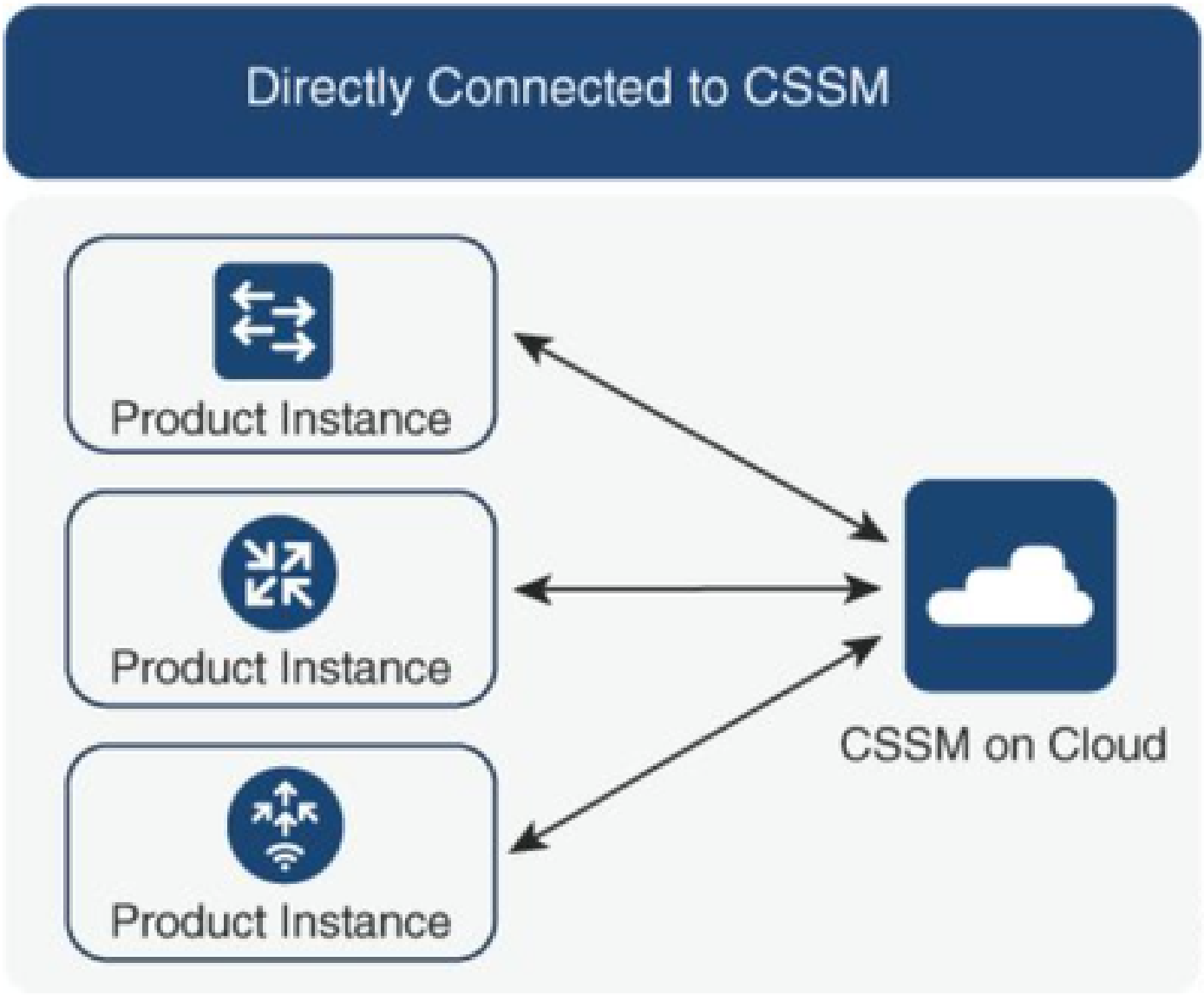
- Nutzung: Alle Lizenzen für Cisco Catalyst Wireless Controller werden nicht erzwungen. Dies bedeutet, dass Sie keine lizenzspezifischen Vorgänge wie das Registrieren oder Generieren von Schlüsseln durchführen müssen, bevor Sie mit der Nutzung der Software und der damit verbundenen Lizenzen beginnen. Die Lizenznutzung wird mit Zeitstempeln auf Ihrem Gerät aufgezeichnet, und die erforderlichen Workflows können zu einem späteren Zeitpunkt abgeschlossen werden.

- Lizenznutzung an CSSM melden: Für das Reporting zur Lizenznutzung stehen mehrere Optionen zur Verfügung. Sie können SSM On-Prem oder Cisco Smart Licensing Utility (CSLU) verwenden oder Nutzungsdaten direkt an CSSM melden. Für Air-Gap-Netzwerke steht auch eine Offline-Reporting-Funktion zur Verfügung, mit der Sie Nutzungsdaten herunterladen und in CSSM hochladen können. Der Verwendungsbericht liegt im XML-Format für einfachen Text vor.

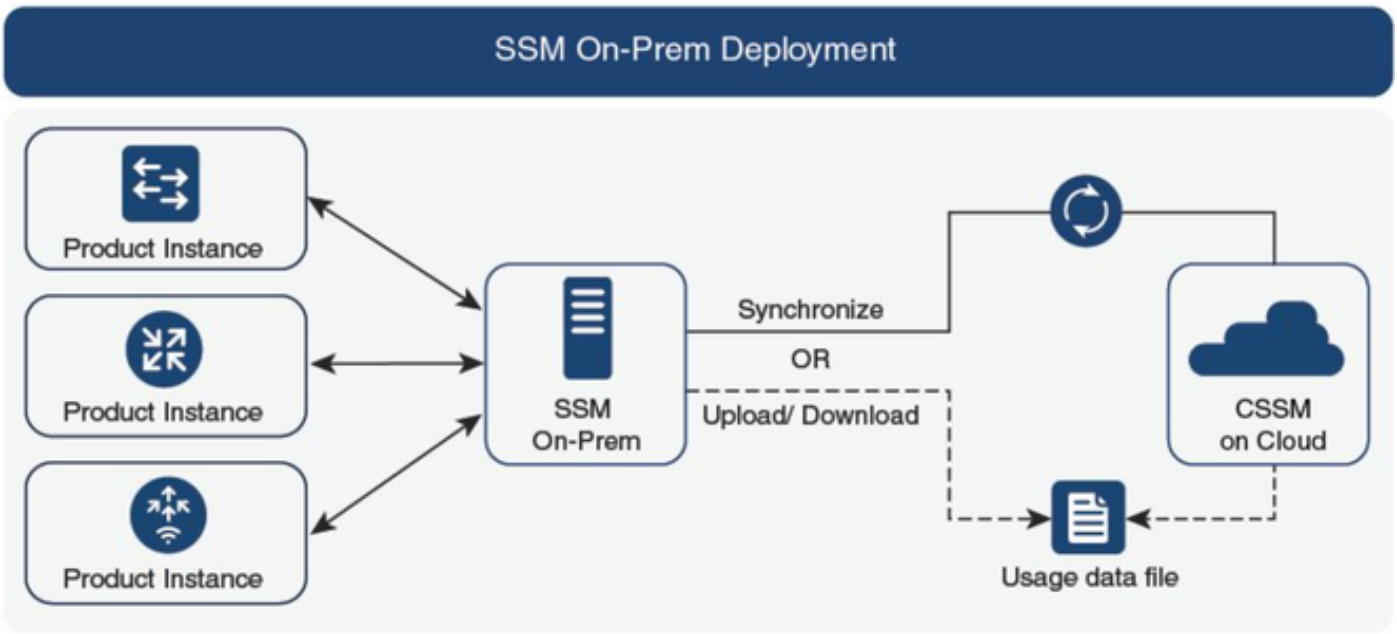
1. Direkte Verbindung zur Cisco Smart Software Manager Cloud (CSSM)
2. Verbindung zum CSSM über Smart Software Manager vor Ort (SSM vor Ort)

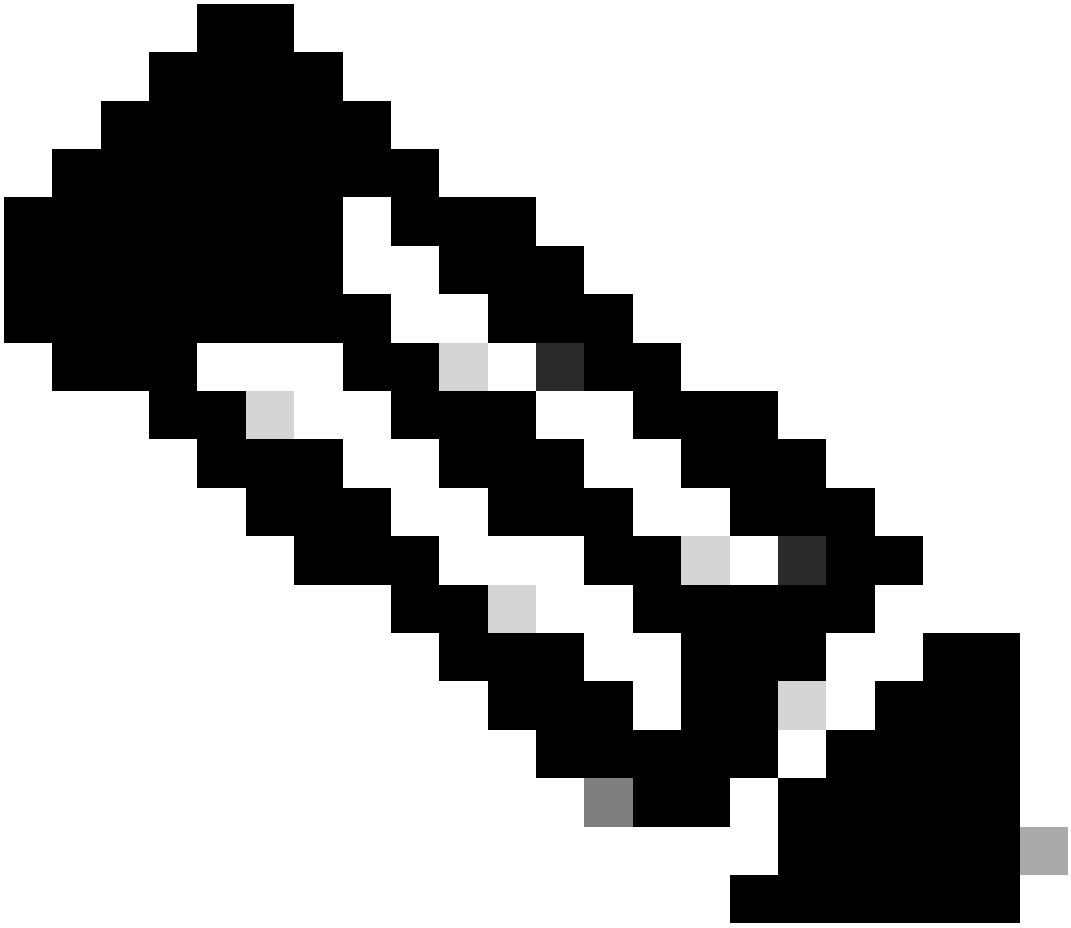
Dieser Artikel behandelt nicht alle Smart Licensing-Szenarien für Catalyst 9800. Weitere Informationen finden Sie im Konfigurationsleitfaden für Smart Licensing mit Richtlinien. Dieser Artikel enthält jedoch eine Reihe nützlicher Befehle zur Fehlerbehebung bei Problemen mit Direct Connect und SSM On-Prem Smart Licensing mithilfe von Richtlinien für Catalyst 9800.

Option 1: Direkte Verbindung zu Cisco Smart Licensing Cloud-Servern (CSSM):



Option 2. Verbindung über standortinternen Smart Software Manager (standortinternes SSM):





Anmerkung: Alle in diesem Artikel genannten Befehle gelten nur für WLCs, auf denen Version 17.3.2 oder höher ausgeführt wird.

Berichte zur Lizenznutzung

Mit SLP werden die meisten Lizenzen nicht erzwungen und werden auf dem Gerät aktiviert, wenn das Funktions-/Technologiepaket konfiguriert wird. Die entsprechende(n) Lizenz(en) wird/werden in der **Lizenzzusammenfassung** als **IN USE angezeigt**.

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

Die einzigen beiden für eine Lizenz verfügbaren Zustände sind "IN USE" (In Gebrauch) oder "NOT IN USE" (Nicht in Gebrauch). Der Status wird ausschließlich von der Konfiguration und den Funktionen der Produktinstanz bestimmt.

Für jede verwendete Lizenz wird ein separater RUM-Bericht erstellt. Es gibt die Zustände GESCHLOSSEN, ACK und OPEN für Rum-Berichte.

Optional: Bestätigt mit einem internen Befehl test license smart rum-report id:

```
Router(config)# service internal

Router# test license smart rum-report id

report_id:1624247687 state:SmartAgentRumStateOpen
```

ab 17.9 Versionen: Der Befehl show license rum id all:

```
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-Berichte

RUM-Berichte oder Berichte zur Messung der Ressourcennutzung sind Datendateien mit Informationen zur Lizenznutzung und Geräteidentität. Diese Berichte werden als Sicherheitsberichte auf dem Gerät gespeichert und von der Hardware mit einem Zertifikat signiert.

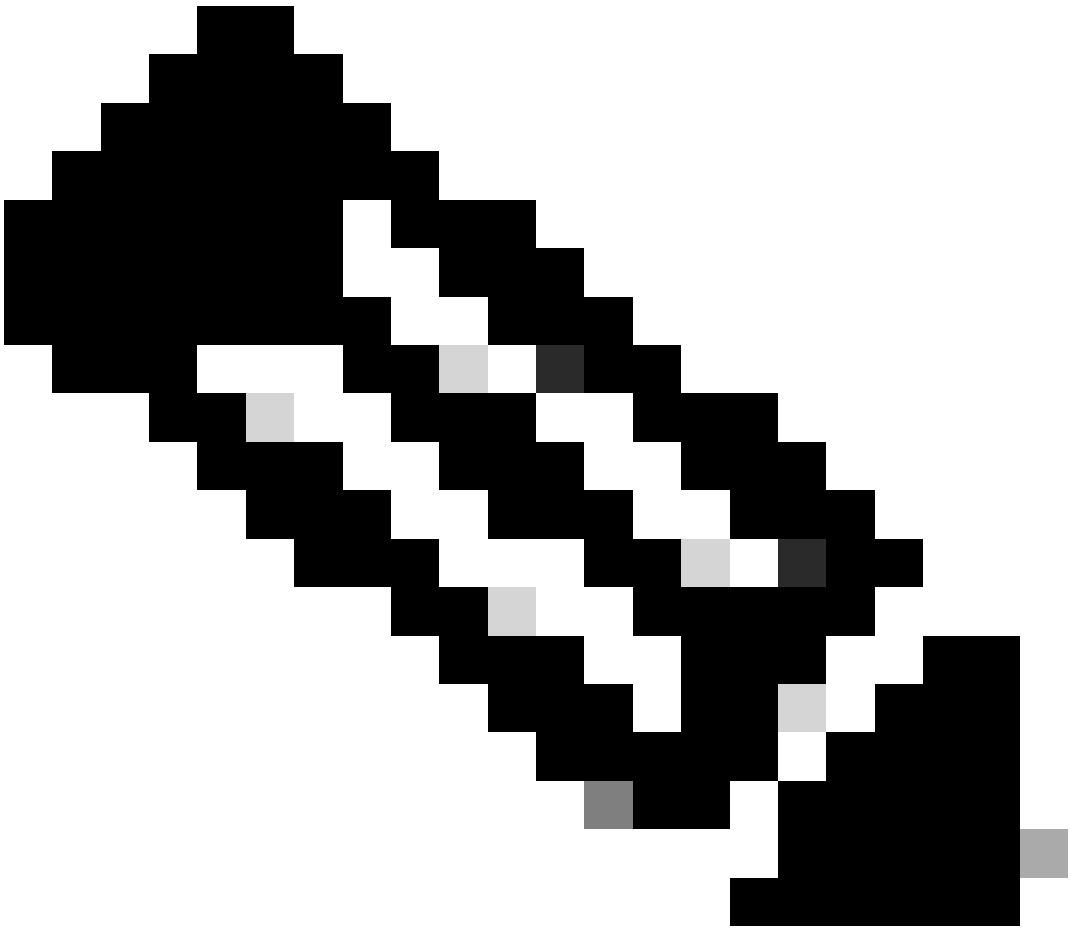
Die Berichte ändern den Status während der gesamten Kommunikation zwischen der Produktinstanz und dem CSSM.

Status	**Beschreibung**
SmartAgentRumStatusOffen	Neuer Bericht erstellt von Smart Agent auf dem Gerät
SmartAgentRumStatusGeschlossen	RUM-Bericht an CSSM gesendet (beim erneuten Laden werden die offenen Berichte ebenfalls in den geschlossenen Zustand verschoben)
SmartAgentRumStatusUnbestätigt	RUM-Bericht ausstehend Bestätigung von CSSM, Abfrage-ID angegeben
SmartAgentRumStatusBestätigt	RUM-Bericht wurde an CSSM gesendet und dafür bestätigt

Die Funktion "Smart Licensing Using Policy" (Smart Lizenzierung unter Verwendung von Richtlinien) wurde in Catalyst 9800 mit der Codeversion 17.3.2 eingeführt. In der ersten Version 17.3.2 wird das SLUP-Konfigurationsmenü in der WLC-Webbenutzeroberfläche übersehen, das mit der Version 17.3.3 eingeführt wurde. Das SLUP unterscheidet sich in vielerlei Hinsicht von herkömmlichen Smart Licensing-Lösungen:

- Der WLC kommuniziert jetzt mit dem CSSM über die Domäne smartreceiver.cisco.com und

nicht über die Domäne tools.cisco.com.
- Anstatt sich zu registrieren, richtet der WLC nun eine Vertrauensstellung mit dem CSSM oder SSM am Standort ein.
- CLI-Befehle wurden leicht geändert.
- Die Smart Licensing Reservation (SLR) ist nicht mehr vorhanden. Stattdessen können Sie Ihre Nutzung regelmäßig manuell melden.
- Der Evaluierungsmodus ist nicht mehr vorhanden. Der WLC arbeitet auch ohne Lizenz mit voller Leistung weiter. Das System ist honorbasiert und Sie sollen Ihre Lizenznutzung regelmäßig (automatisch oder manuell bei Air-Gap Netzwerken) melden.

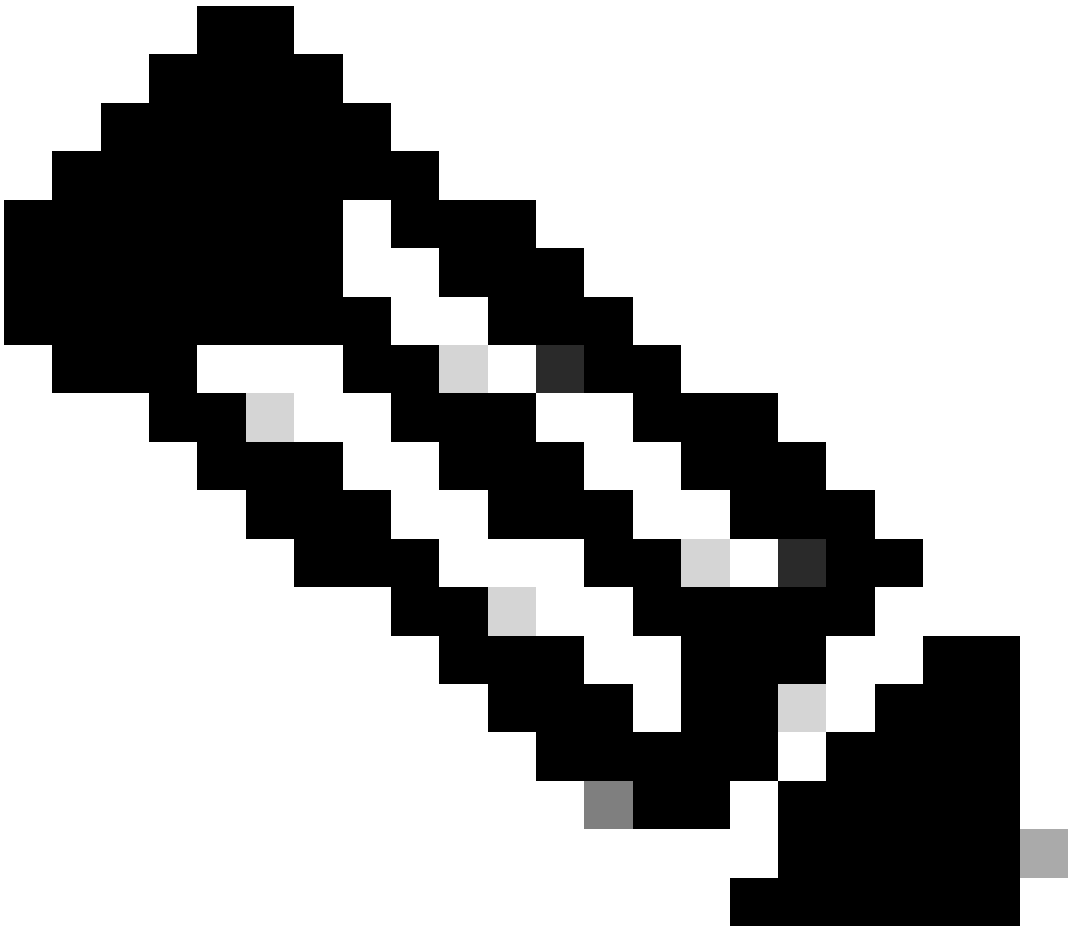


Anmerkung: Warnung: Wenn Sie einen Cisco Catalyst 9800-CL Wireless Controller verwenden, stellen Sie sicher, dass Sie mit der obligatorischen ACK-Anforderung vertraut sind, die mit Cisco IOS® XE Cupertino 17.7.1 beginnt. Siehe RUM Reporting and Acknowledgment Requirement for Cisco Catalyst 9800-CL Wireless Controller.

Problembehandlung bei Kommunikationsproblemen mit 9800 Smart Licensing bei direkt verbundenem CSSM und einem lokalen SSM-Server

* Ein brandneuer Controller der Serie 9800 muss bestimmte Verfahren einhalten, damit der Workflow für intelligente Lizenzen abgeschlossen werden kann.

1. Erstellen Sie ein Token aus dem CSSM-Portal, und importieren Sie das Token, um eine Vertrauenskennung einzurichten, die erforderlich ist, um künftig eine Autorisierung für die Lizenzverwendungsberichte zu erhalten. Dieser Wert für die Vertrauens-ID ist der Schlüssel für CSSM zum Validieren des Berichts, der vom 9800-Controller gesendet wurde. Dieses vertrauenswürdige Token wird regelmäßig aktualisiert und im Rahmen des Rum-Nutzungsberichts mit CSSM ausgetauscht.



> Anmerkung: Ab Cisco IOS XE Cupertino 17.7.1 ist ein Vertrauenscode erforderlich. Pro Seriennummer wird ein Vertrauenscode eingerichtet, sodass bei der 9800 HA SSO-Konfiguration 2 Vertrauenscodes installiert sind.

Treuhandcode

Ein mit UDI verknüpfter öffentlicher Schlüssel, den die Produktinstanz verwendet, um:

- Unterzeichnen eines RUM-Berichts Dies verhindert Manipulationen und stellt die Datenauthentizität sicher.
- Sichere Kommunikation mit CSSM aktivieren

Aus Cisco IOS XE Cupertino 17.7.1 wird automatisch ein Vertrauenscode in Topologien abgerufen, in denen die Produktinstanz das Senden von Daten an CSLU initiiert, und in Topologien, in denen sich die Produktinstanz in einem Air-Gap-Netzwerk befindet.

- Ein Vertrauenscode kann mithilfe eines ID-Tokens von CSSM abgerufen werden.

  Hier generieren Sie ein ID-Token in der CSSM-Webbenutzeroberfläche, um einen Vertrauenscode abzurufen und ihn in der Produktinstanz zu installieren. Wenn vorhanden, müssen Sie den werkseitig installierten Vertrauenscode überschreiben. Wenn eine Produktinstanz direkt mit CSSM verbunden ist, aktivieren Sie diese Methode, damit die Produktinstanz sicher mit CSSM kommunizieren kann. Diese Methode zum Erhalten eines Vertrauenscodes kann für alle Optionen verwendet werden, die eine direkte Verbindung mit CSSM ermöglichen. Weitere Informationen finden Sie unter Direkt mit CSSM verbunden.

Aus Cisco IOS XE Cupertino 17.9.1 wird automatisch ein Vertrauenscode in Topologien abgerufen, in denen CSLU den Abruf von Daten aus der Produktinstanz initiiert.

Wenn ein werkseitig installierter Vertrauenscode vorhanden ist, wird er automatisch überschrieben. Ein so erhaltener Vertrauenscode kann für die sichere Kommunikation mit CSSM verwendet werden.

* Stellen Sie sicher, dass die Konfiguration für Smart Licensing auf dem 9800 intakt ist. 9800 verwendet Smart als Transportmethode für die Kommunikation mit CSSM.

Intelligent mit CSSM

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

Intelligente Verwendung des Proxys

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

SSM vor Ort

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

Stellen Sie sicher, dass die Domänensuche und der Name-Server über die Quellschnittstelle

erreichbar sind.

Device(config)#ip domain name

Device(config)#ip name server

Device(config)#ip domain lookup

show license all gibt Transporttyp- und URL-Details zurück, die für 9800 konfiguriert wurden: Sicherstellen, dass die Konfiguration absolut ist

Intelligenter Transport

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

SSM vor Ort

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

* Wenn ein Proxy zwischen 9800 und CSSM vorhanden ist, stellen Sie sicher, dass die aufgelistete IP-Adresse auf dem Proxy für eine nahtlose Kommunikation zugelassen ist.

Verbindung zum Smart Receiver testen

Verwenden Sie den Befehl curl:

- curl https://smartreceiver.cisco.com/licservice/license
- Erwartete Antwort: Das ist der Smart Receiver!

Testen der Verbindung mit dem SSM-Server vor Ort

Verwenden Sie den Befehl curl:

- curl -v -k https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1
- Erwartete Antwort: Das ist der Smart Receiver!

IP-Adresse des Empfängers nachschlagen

Verwenden Sie den folgenden nslookup-Befehl:

- nslookup smartreceiver.cisco.com

Erwartete Antwort:

- Server: 171.70.168.183 ← Dies ist der DNS-Server
- Server: dns-sj.cisco.com ← Optional kann dies angezeigt werden
- Adresse: 10.10.10.10#53
- Name: smartreceiver.cisco.com
- Adresse: 146.112.59.81
- Name: smartreceiver.cisco.com
- Adresse: 2a04:e4c7:fffe::f

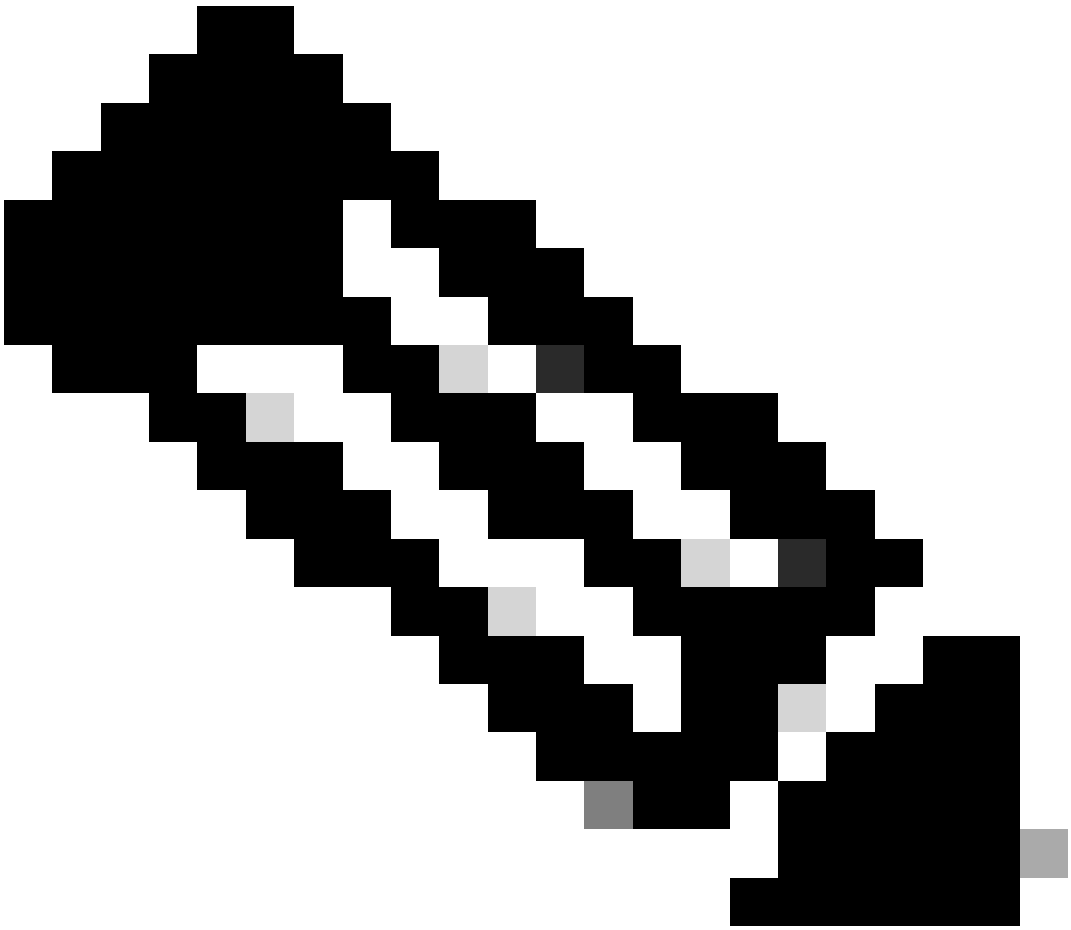
Wie löst Ihr System die IP auf?

Verwenden Sie den Befehl dig:

- dig smartreceiver.cisco.com + short

Erwartetes Ergebnis

- 146.112.59.81



Anmerkung: Die Smart Receiver-Komponente von CSSM hat den bisherigen tools.cisco.com und zentralen Ansprechpartner für Rum Reporting, Registration, Billing für MSLA-Kunden abgelöst.

ip http client source-interface <Source-Interface>

Mit diesem Befehl wird der Quellpfad zu CSSM explizit markiert.

ip http client secure-trustpoint SLA-TrustPoint

Stellen Sie sicher, dass "secure-trustpoint" als SLA-TrustPoint ausgewählt ist, da dieser von der Lizenzierungs-Stammzertifizierungsstelle signiert wird. Sowohl SSM On-Prem als auch CSSM werden vom Lizenzierungs-Root-Zertifizierungsstellenzertifikat als vertrauenswürdig eingestuft.

Zertifizierungsstellenzertifikat:

Status: Verfügbar

Seriennummer des Zertifikats (hex): 01

Zertifikatverwendung: Unterschrift

Aussteller:

cn=Cisco Lizenzierungs-Stammzertifizierungsstelle

o = Cisco

Betreff:

cn=Cisco Lizenzierungs-Stammzertifizierungsstelle

o = Cisco

Gültigkeitsdatum:

Startdatum: 19:48:47 UTC 30. Mai 2013

Enddatum: 19:48:47 UTC 30. Mai 2038

Zugehörige Vertrauenspunkte: TrustPool SLA-TrustPoint

Speicher: nvram:CiscoLicense#1CA.cer

Die Lizenz smart sync all ist der Befehl zum Einleiten eines neuen Rum-Berichts vom 9800-Controller und im XML-Format. Wenn dieser Befehl auf dem Controller ausgeführt wird, auf dem der Vertrauenscode nicht in der Version 17.9.x installiert ist, wird zuerst eine Anforderung für den Vertrauenscode anstatt des Rum-Nutzungsberichts generiert.

Ungültiger Trustcode verarbeitet von CSSM

TRUST-CODE importieren:

Eingegangen am 17.09.2024 17:35:26 UTC

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>false</success><message>Für dieses Gerät wurde bereits eine Vertrauensanfrage entsprechend einer höheren Trust-ID verarbeitet.</message><code>OLD_TRUST_ID</code><Correlation ID>null-null</CorrelationID></status></trustCode><signature>MEQCIAg71/hlcWxUiiof8VstpmPhRH8jptPZPrvaSp
mG4uSDq/EbUp+vfrYD9nQ==</signature></smartLicenseTrust>

Der CSSM erwartet, dass der Controller eine inkrementelle Trustcode-ID als Sicherheitszweck sendet, und die Verarbeitung der Lizenzierungs-RUM-Anforderungen vom Controller wird durch die Implikation eines ungültigen Trustcode gestoppt. Dies würde letztendlich zu einem Lizenzverwaltungsproblem für CSSM-Lizenzdashabord führen.

Gültiger Trustcode, der vom CSSM verarbeitet wurde

TRUST-CODE importieren:

<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:XXXXXXXXX</udi><customerInfo><smartAccount>Cisco Demo Internal Smart Account</smartAccount><virtualAccount>0Demo-HK-PartnerA</virtualAccount></customerInfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c36b</piid><dateStamp>2024-09-10T07:21:30</dateStamp></subCA><trustId>11
0</trustId><status><success>true</success><CorrelationID>null</CorrelationID></status></trustCode><
OjAqDYkGn206meTHt8+dqra0LAciHEZKxmqeurKOU0g=</signature></smartLicenseTrust>

Kommunikationsfrequenz

Das Berichtsintervall, das Sie in CLI oder GUI konfigurieren können, hat keine Auswirkungen.

Der 9800 WLC kommuniziert alle 8 Stunden mit CSSM oder dem standortbasierten Smart Software Manager, unabhängig davon, welches Berichtsintervall über die Webschnittstelle oder die CLI konfiguriert wird. Das bedeutet, dass neu verknüpfte Access Points bis zu 8 Stunden nach dem ersten Beitritt auf dem CSSM angezeigt werden können.

Mit dem Befehl show license air entity summary können Sie bestimmen, wann Lizenzen das nächste Mal berechnet und gemeldet werden. Dieser Befehl ist nicht Teil der typischen Ausgabe von show tech oder show license all:

show license air entitiessummary-Befehl:

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

Nach der erfolgreichen Installation des Posttrustcodes auf dem Controller 9800 wird in der nächsten Phase der Nutzungsbericht über die Lizenzaktivität über Rum (Resource Measurement Unit) im XML-Format generiert. Der Befehl license smart sync all/local initiiert oder generiert oder öffnet eine neue Rum-Messung basierend auf dem im Controller verwalteten AP. Im Grunde sendet die 9800 Smart Agent-Komponente einen API-Aufruf an das Lizenzierungsmodul, um einen neuen Rum-Bericht mit Lizenzierungsinformationen zu erfassen.

show license rum id all-Befehl:

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-Befehl:

Sie können Details der Lizenz abrufen, die in der Rum-ID angegeben ist. Dieser Befehl ruft das software_identifier_tag ab, das Schlüsselelement in der CSSM-Datenbank, um einen Lizenztyp aus einer Produktinstanz zu validieren.

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

Details zum Smart Licensing-Nutzungsbericht:

==========

Berichts-ID: 1719005447

Metrischer Name: BERECHTIGUNG

Funktionsname: Air-Network-Vorteil

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

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

ID des vorherigen Berichts: 1719005445, ID des nächsten Berichts: 0

Status: OPEN, Grund für Zustandsänderung: None

Schließen - Grund: None

Startzeit: 10.09. 10:00:08 2024 UTC, Endzeit: 16.09. 16:15:08 2024 UTC

Speicherstatus: EXISTIEREN

Transaktionskennung: 0

Transaktionsmeldung: <keine>

* Jetzt wird der Rum-Bericht generiert. Im Status "OPEN" muss sie erfolgreich an CSSM übermittelt werden, um die ACK vom CSSM zu erhalten.

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

Fehler in der Ausgabe von show license eventlog und/oder show log

"Kommunikationsfehler mit dem Cisco Smart License Utility (CSLU): Keine detaillierten Informationen angegeben"

Dieser Fehler tritt auf, wenn die HTTPS-Kommunikation mit On-Prem nicht hergestellt wurde. Mögliche Gründe:

- Für die Kommunikation mit OnPrem wird eine spezielle VRF-Instanz verwendet. Die HTTP-Client-Quellschnittstelle muss manuell konfiguriert werden.

- Die Sperrprüfung ist in der SLA-Vertrauenspunktkonfiguration NICHT deaktiviert.

- Ein weiterer Vertrauenspunkt wird als Standard für die Verschlüsselungssignalisierung festgelegt (z. B.: am SIP-Gateway)

"HTTP Server Error 502: Ungültiges Gateway"

Dieser Fehler wird derzeit vom On-Prem-Entwicklungsteam untersucht. In den meisten Fällen wurden keine Auswirkungen auf den Service beobachtet.

Normalerweise 10 Sekunden später, SAEVT_COMM_RESTORED.

Beispiel:

09.07. 13:15:29.902: %SMART_LIC-3-COMM_FAILED: Kommunikationsfehler mit dem Cisco Smart License Utility (CSLU): HTTP-Serverfehler 502: Ungültiges Gateway
09.07. 13:15:39.881: %SMART_LIC-5-COMM_RESTORED: Kommunikation mit wiederhergestelltem Cisco Smart License Utility (CSLU)

"HTTP Server Error 404: Nicht gefunden"

Dieser Fehler tritt auf dem Cisco IOS XE-Gerät auf, wenn versucht wurde, den vertrauenswürdigen Code zu installieren, während die Transport-URL auf das lokale Gerät (CSLU) verwies.

Der Befehl "license smart trust idtoken <token> [all|local]" wird NUR verwendet, wenn das Gerät direkt mit CSSM kommuniziert.

HINWEIS: Abhängig von der Plattform kann diese Meldung auch bedeuten, dass die Einstellung "Gerät validieren" im Bereich "CSLU-Einstellungen" des standortbasierten Verwaltungsarbeitsbereichs aktiviert ist. Überprüfen Sie, ob sich das Gerät, das Sie registrieren möchten, auf der Registerkarte "SL Using Policy" (SL-Nutzungsrichtlinie) des lokalen Servers

befindet. Wenn sich die Geräte nicht auf dieser Registerkarte befinden, müssen Sie diesen Umschalter deaktivieren. Versuchen Sie dann erneut, das Gerät mit dem lokalen Server zu synchronisieren. Ein Bild dieser Einstellung finden Sie am Ende dieses Artikels.

SAEVT_INIT_CRYPTO success="False" error="Die Kryptografieinitialisierung wurde nicht abgeschlossen"

Dieser Fehler ist kurz nach dem Systemstart zu beobachten. Nach ca. 30 Sekunden ist die Krypto-Initialisierung abgeschlossen - in diesem Fall gibt es keine Auswirkungen auf den Dienst.

Beispiel:

25.06.2021 10:09:23.378 UTC SAEVT_INIT_SYSTEM_INIT
25.06.2021 10:09:24.383 UTC SAEVT_INIT_CRYPTO success="False" error="Die Kryptografieinitialisierung wurde nicht abgeschlossen"
25.06.2021 10:09:54.383 UTC SAEVT_INIT_CRYPTO success="True"

Wenn die Kryptografieinitialisierung mehrere Minuten/Stunden lang nicht abgeschlossen ist, überprüfen Sie, ob die NTP-Konfiguration vorhanden ist und/oder ob die Uhren synchronisiert wurden. Durch Speichern der aktuellen Konfiguration kann die Kryptografieinitialisierung neu gestartet werden.

Es wird empfohlen, das Problem zusammen mit dem Cisco TAC weiter zu untersuchen.

SAEVT_UTILITY_RUM_FAIL error="[HOST_NOT_FOUND] Gerätehost wurde nicht gefunden"

Höchstwahrscheinlich wird die Einstellung "Gerät validieren" im Bedienfeld "CSLU-Einstellungen" des lokalen Admin-Arbeitsbereichs festgelegt.

Mit dieser Einstellung wird sichergestellt, dass die RUM-Berichte von bekannten Produktinstanzen empfangen werden.

SAEVT_COMM_FAIL error="Hostname/Domänenname des Servers kann nicht aufgelöst werden"

Dieser Fehler weist auf ein Verbindungsproblem hin, das von der DNS-Auflösung ausgehen kann. Sie müssen sicherstellen, dass das Gerät die Ziel-URL auflösen kann. In der Regel ist der Befehl ip host <url> <ipassociated> falsch konfiguriert. Bitte überprüfen Sie diesen Punkt.

Höchstwahrscheinlich würden Sie Kommunikationsfehler feststellen.

Kommunikationsstatistiken:

==========

Zugelassene Kommunikationsebene: INDIREKT

Gesamtstatus: <leer>

Einrichtung der Vertrauensstellung:

Versuche: Total=30, Success=0, Fail=30 Laufender Fehler: Overall=30 Communication=30 <<<<<<<

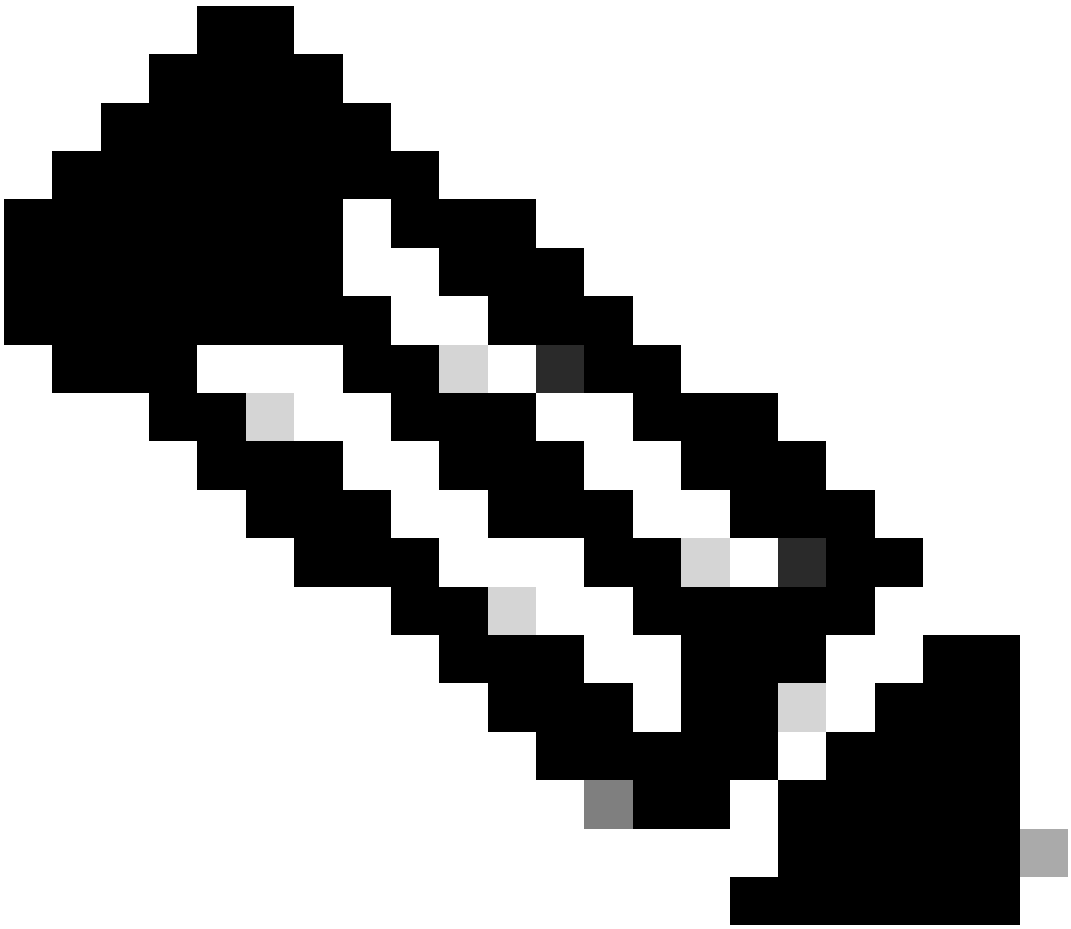
Letzte Antwort: NO REPLY on Feb 12 10:52:56 2023 GMT <<<<<<<<<

Fehlerursache: <keine>

Letzter Erfolg: <keine>

Zeit des letzten Ausfalls: 12.02.10:52:56 2023 GMT

Kommunikationsebene zulässig als INDIRECT bedeutet, dass der erforderliche Trustcode nicht erfolgreich auf dem 9800-Controller installiert wurde.



Anmerkung: Anmerkung: CSSM ist die Quelle der Wahrheit aller Lizenzierungsdaten.

---

* Wenn ein grundlegendes Kommunikationsproblem zwischen 9800 und CSSM durch den Test behoben wird, aktivieren Sie die Fehlersuche für bestimmte Module, die für die Smart Licensing-Kommunikation verwendet werden. Die Aktivierung der Fehlersuche auf 9800 würde die CPU für ein bestimmtes Zeitintervall in die Höhe treiben und muss daher außerhalb der Geschäftszeiten ausgeführt werden.

Fehlersuche

* Es gibt 4 Module, die an der Smart Licensing-Kommunikation von 9800 zu CSSM oder SSM vor Ort beteiligt sind.

1. Verschlüsselungsmodul

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-Modul

HTTP-Server:

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-Modul

ssl openssl:

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

4. Das Smart Licensing-Modul wird als Smart Agent bezeichnet, einschließlich des Transport-Gateways

Lizenz:

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

Syslogs:

Serveridentitätsprüfung und SAN-Validierung auf dem Zertifikat. Vertrauenspunktvalidierung aus der SSL-Verschlüsselungsbibliothek.

16.09. 16:29:12.236: Serveridentitätsprüfung mit Host: 10.106.43.37

16.09. 16:29:12.236: Zu verifizierende Serveridentität ist die IP-Adresse 10.106.43.37 len 12

16.09. 16:29:12.329: CRYPTO_PKI: (A645F) Auf identische Zertifikate prüfen

16.09. 16:29:12.329: CRYPTO_PKI(CERT-Suche) emittent="cn=Cisco Licensing Root CA,o=Cisco" serial number= 0F 42 40

16.09. 16:29:12.329: CRYPTO_PKI: (A645F) Geeignete Vertrauenspunkte sind: SLA-TrustPoint, TrustPool6, TrustPool6

16.09. 16:29:12.329: CRYPTO_PKI: (A645F) Versuch, das Zertifikat mithilfe der SLA-TrustPoint-Richtlinie zu validieren

16.09. 16:29:12.329: CRYPTO_PKI: (A645F) Verwenden von SLA-TrustPoint zum Validieren des Zertifikats

16.09. 16:29:12.345: SSL_connect:SSL-Aushandlung erfolgreich abgeschlossen

16.09. 16:29:12.345: SSL_connect:SSL-Aushandlung erfolgreich abgeschlossen

Sobald der Nutzungsbericht an CSSM übermittelt wurde, muss der folgende Befehl zum Anzeigen der Lizenzverlaufsmeldung erfolgreich aktualisiert werden:

Anfragen hätten Komponenten wie UDI_SERIAL_NUMBER, Hostname, Software_Tag_Identifier, die angeben, welcher Lizenzmodus ls vom 9800-Controller genutzt wird, und Request_Type als "LICENSE_USAGE".

Es gibt mehrere Lizenztypen:

1. ID_TOKEN_TRUST

2. TRUST_SYNC

3. LICENSE_USAGE

Nutzungsberichte:

ANFRAGE: 16.09. 16:30:16 2024 UTC

"{\"sender_info\":{\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.8.6_rel/15\",\"production\":true,\"add
L-F-
K9\",\"udi_serial_number\":\"FCL2630000P\"},\"product_instance_bezeichner\":\"\",\"software_tag_bezeichr
06.com.cisco.C9800_0 L_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_K9,1.0_9529f872-1b08-4cac-9272 9-
71c391233fc2\",\"product_instance_identifier\":\"\",\"product_version\":\"17.12.02\",\"hostname\":\"renjith-
eap-
test\",\"role\":\"Active\",\"request_type\":\"ID_TOKEN_TRUST\",\"request_line_id\":1,\"smart_license\":

Nutzungsberichte:

ANFRAGE: 16.09. 16:30:16 2024 UTC

"{\"sender_info\":{\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.8.6_rel/15\",\"production\":true,\"add
L-F-
K9\",\"udi_serial_number\":\"FCL2630000P\"},\"product_instance_bezeichner\":\"\",\"software_tag_bezeichr

06.com.cisco.C9800_0 L_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_K9,1.0_9529f872-1b08-4cac-9272 9-
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\":

Nutzungsberichte:

ANFRAGE: 16.09. 16:30:16 2024 UTC

{"sender_info":{"connect_info":{"name":"C_agent","version":"5.8.6_rel/15","production":true,"additional_info
Y_AGAIN","POLICY_USAGE","TELEMETRY","CSLU_V1"]},"timestamp":1726504216022,"nonce":"77709
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"},"device_list"
:[{"sudi":{"udi_pid":"C9800-L-F-
K9","udi_serial_number":"FCL2630000P"},"software_tag_identifier":"regid.2019-
06.com.cisco.C9800_L_F_K9,1.0_9529f8 72-1b08-4cac-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":

* Es ist wichtig, die Reaktion von CSSM oder SSM vor Ort zu verstehen:

Fehlerantwortpaket:

ANTWORT: 16.09. 16:30:16 2024 UTC

{

Status: "FEHLER",

"Message_Code": "FEHLER bei Verbraucherlizenzen",

"Nachricht": "",

"Nonce": "77709655117429624"

}

Der Fehler zeigt an, dass bereits ein Eintrag für den Controller auf dem CSSM- oder SSM On-Prem-Lizenzierungsserver vorhanden ist, der das Hinzufügen eines neuen Datensatzes in der Datenbank verweigert. Sie müssen den aktiven oder veralteten Datensatz vom CSSM oder SSM On-Prem löschen und den Bericht "Rum" erneut einsenden.

Gültige Antwort-Poll_id:

ANTWORT: 16.09. 16:29:14 2024 UTC

```
{
  "sender_info": {
    "connect_info": {
      "Name": CSLU_V1,
      "Version": "v1",
      "Erzeugung": Richtig,
      "Zusätzliche Informationen": "",
      "Funktionen": [
        "VERSORGUNG",
        "DLC",
        "AppHA",
        "MULTITITIER",
        "EXPORT_2",
        "OK_TRY_AGAIN"
        "POLICY_USAGE",
        CSLU_V1,
        "CSLU_V2"
        TELEMETRIE
      ]
    },
    "Zeitstempel": 1726504153302,
    "Nonce": "10743401694998030696",
    "sudi": {
      "udi_pid": C9800-L-F-K9
      "udi_serial_number": "FCL2630000P"
    },
    "product_instance_bezeichner": "",
```

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

},

Status: "ABGESCHLOSSEN"

"license_data": [

{

Status: OK_POLL,

"request_line_id": 1,

"sudi": {

"udi_pid": C9800-L-F-K9

"udi_serial_number": "FCL2630000P"

},

"poll_id": 5583279046281676962,

"poll_interval": 86739,

"Smart_License": ""

}

]

}

* Wie zu validieren poll_id ist in 9800 lokalen Datenbank gespeichert und wie oft es fragt, um eine ACK für den Rum-Bericht eingereicht.

Test-Befehl, um zu überprüfen, ob eine Aktivierung über den internen Service erforderlich ist.

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

* Wie Sie aus der Erklärung entnehmen können, dass die ersten Anfragen, die vom 9800-Controller gesendet wurden, immer ein Trust-Code-Token sind, und ohne diesen Code würde der 9800-Controller niemals einen neuen Rum-Nutzungsbericht generieren. Daher kann die Lizenznutzungsänderung nicht über CSSM gesendet werden.

* Ein Beispiel fordert polll_id für License_usage an.

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

* Wenn in der CSSM- oder SSM On-Prem-Datenbank bereits ein ACK verarbeitet wurde, können Sie den Smart Agent auf dem 9800-Controller dazu zwingen, frühestens eine Abfrage durchzuführen und die ACK abzurufen, ohne auf die genannte Zeit zu warten.

im polll_id-Zyklus.

test license smart conversion sched_poll 5583279046281676962 ? <0-4294967295> delta Time in Seconds

Zugehörige Informationen

- Konfigurieren der Offline-Lizenzierung (Air Gap) auf dem 9800 WLC
- Technischer Support und Downloads von Cisco
- Konfigurieren der Catalyst 9800 WLC Smart Licensing-Richtlinie mit DNA Center

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.