

Risoluzione dei problemi relativi all'utilizzo di Smart Licensing su 9800

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Report utilizzo licenze](#)

[Rapporti RUM](#)

[Risoluzione dei problemi di comunicazione di Smart Licensing 9800 con CSM a connessione diretta e server locale SSM](#)

[Codice trust](#)

[Intelligente con CSSM](#)

[Uso intelligente del proxy](#)

[SSM locale](#)

[Trasporto intelligente](#)

[SSM locale](#)

[Verifica connessione a Smart Receiver](#)

[Test connessione al server locale SSM](#)

[Cerca indirizzo IP ricevitore](#)

[Come viene risolto l'IP dal sistema?](#)

[Codice Trustcode non valido elaborato da CSM](#)

[Codice Trustcode valido elaborato da CSM](#)

[Frequenza di comunicazione](#)

[Errori riportati nell'output del comando show license eventlog e/o show log](#)

[Debug](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritta la procedura avanzata per la risoluzione dei problemi relativi all'utilizzo delle licenze Smart con criteri (SLUP) sul controller Catalyst 9800 Wireless LAN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Criteri di utilizzo delle licenze Smart (SLUP)

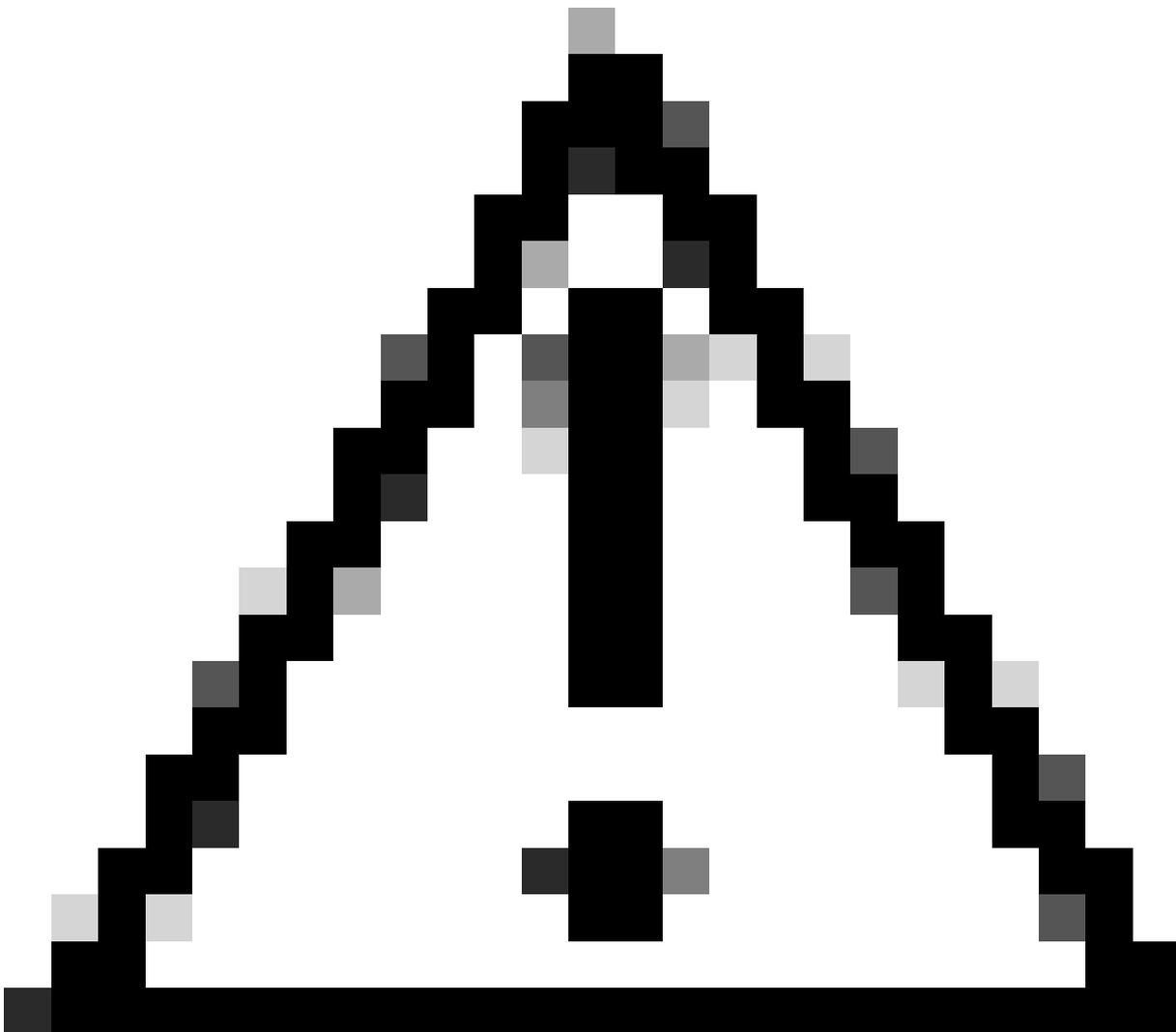
- Catalyst 9800 Wireless LAN Controller (WLC)

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse



Attenzione: Attenzione: Le note di questo articolo contengono utili suggerimenti o riferimenti a materiale non trattato nel documento. Si consiglia di leggere ogni nota.

-
- Utilizzo: Tutte le licenze sui Cisco Catalyst Wireless Controller non sono applicate. Ciò

significa che non è necessario completare alcuna operazione specifica della licenza, ad esempio la registrazione o la generazione delle chiavi prima di iniziare a utilizzare il software e le licenze a esso collegate. L'utilizzo della licenza viene registrato sul dispositivo con l'indicazione dell'ora e i flussi di lavoro richiesti possono essere completati in un secondo momento.

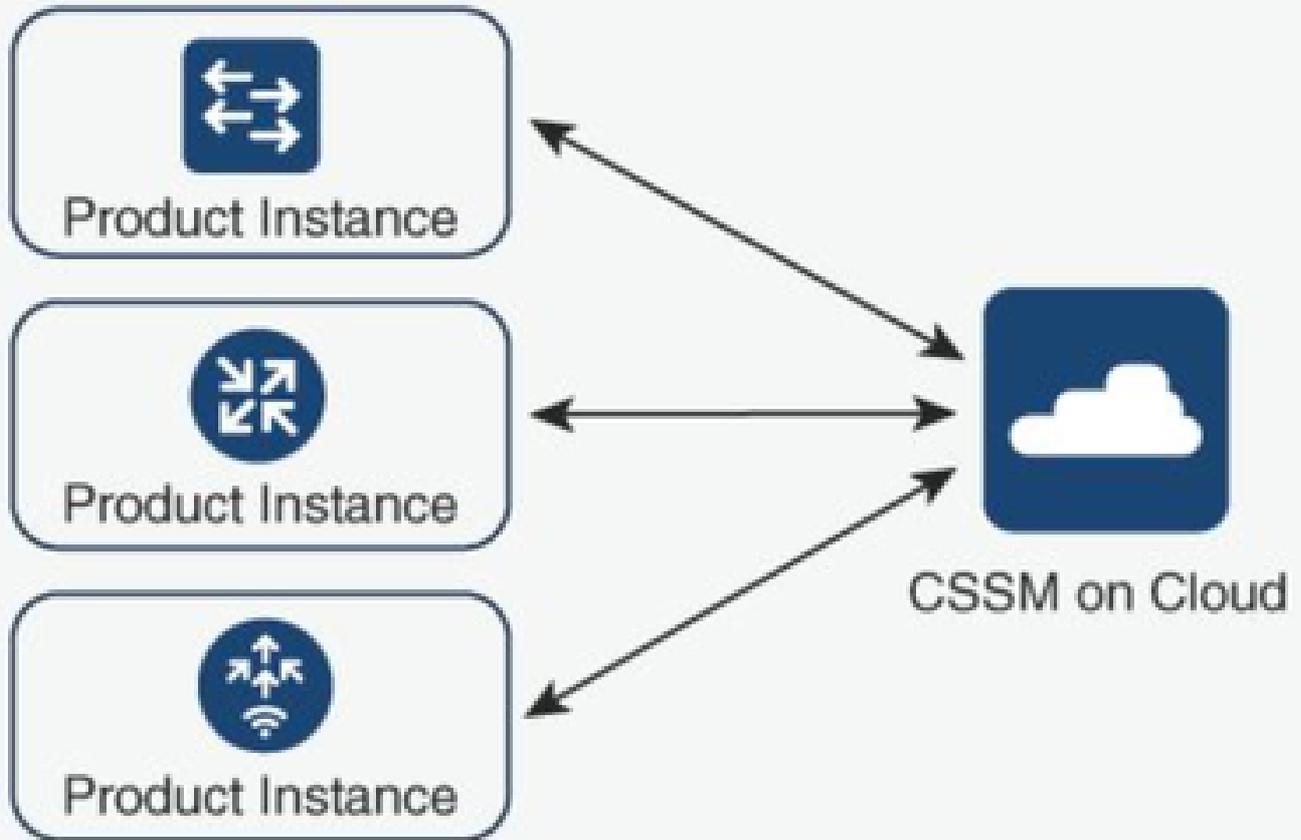
- Segnala l'utilizzo della licenza a CSM: Sono disponibili diverse opzioni per il report sull'utilizzo delle licenze. È possibile utilizzare SSM On-Prem o Cisco Smart Licensing Utility (CSLU) oppure segnalare le informazioni sull'utilizzo direttamente a CSSM. Per le reti con interruzioni di connessione, è inoltre disponibile una funzione per la creazione di report non in linea in cui è possibile scaricare le informazioni sull'utilizzo e caricarle nel modulo CSM. Il report di utilizzo è in formato XML di testo normale.

1. Connessione diretta a [Cisco Smart Software Manager](#) Cloud (CSM)
2. Connesso a CSM tramite [Smart Software Manager locale](#) (SSM locale)

In questo articolo non vengono illustrati tutti gli scenari relativi alle licenze Smart su Catalyst 9800. Per ulteriori informazioni, consultare la [guida alla configurazione delle licenze Smart](#) tramite i [criteri](#). Tuttavia, in questo articolo viene fornita una serie di utili comandi per risolvere i problemi relativi alla connessione diretta e alla gestione intelligente delle licenze in locale tramite i problemi delle policy su Catalyst 9800.

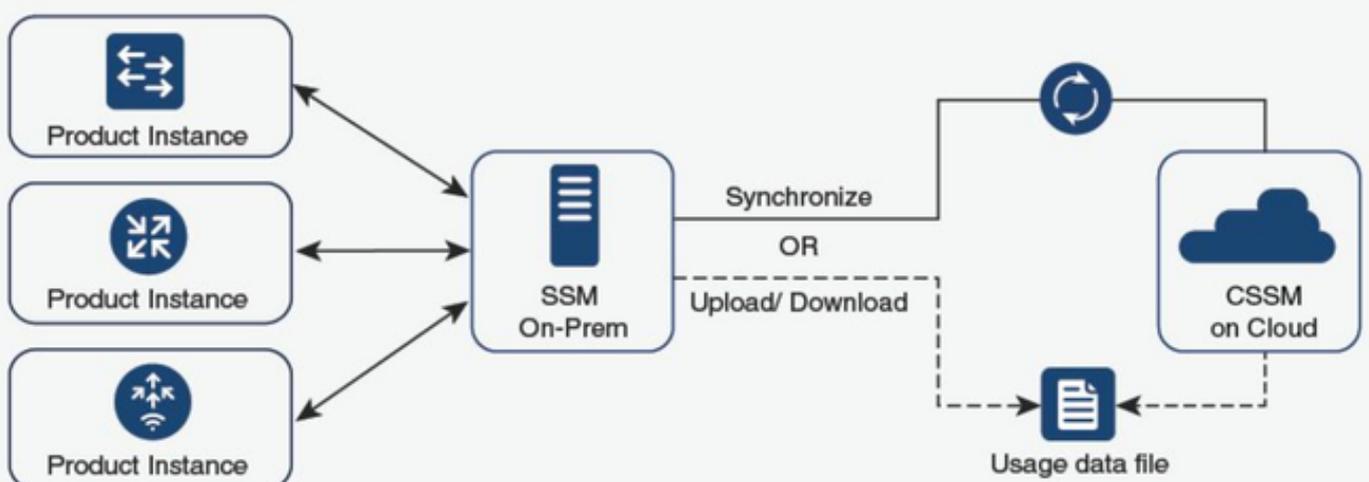
Opzione 1. Connessione diretta a Cisco Smart Licensing Cloud Server (CSSM):

Directly Connected to CSSM



Opzione 2. Connessione tramite Smart Software Manager locale (SSM locale):

SSM On-Prem Deployment



Nota: Tutti i comandi menzionati in questo articolo sono applicabili solo ai WLC con versione 17.3.2 o successive.

Report utilizzo licenze

Con SLP la maggior parte delle licenze non viene applicata e verrebbe abilitata sul dispositivo quando viene configurato il pacchetto funzionalità/tecnologia. Le licenze corrispondenti verranno visualizzate in **mostra riepilogo licenze** come **IN USO**.

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
```

Gli unici due stati disponibili per una licenza sono IN USO o NON IN USO. Lo stato viene determinato esclusivamente dalla configurazione e dalle funzionalità applicate nell'istanza del prodotto.

Per ciascuna licenza IN USO viene creato un report RUM separato. Per i report Rum sono disponibili gli stati CLOSED, ACK e OPEN.

Facoltativo: Confermata con un comando interno test license smart rum-report id comando:

```
Router(config)# service internal
```

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

```
report_id:1624247687 state:SmartAgentRumStateOpen
```

a partire dalle versioni 17.9: il comando 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
```

Rapporti RUM

I rapporti RUM (Resource Usage Measurement) sono file di dati contenenti informazioni sull'utilizzo delle licenze e sull'identità dei dispositivi. Questi report sono relativi alla protezione archiviati nel dispositivo e sono contrassegnati da una firma di certificato dell'hardware.

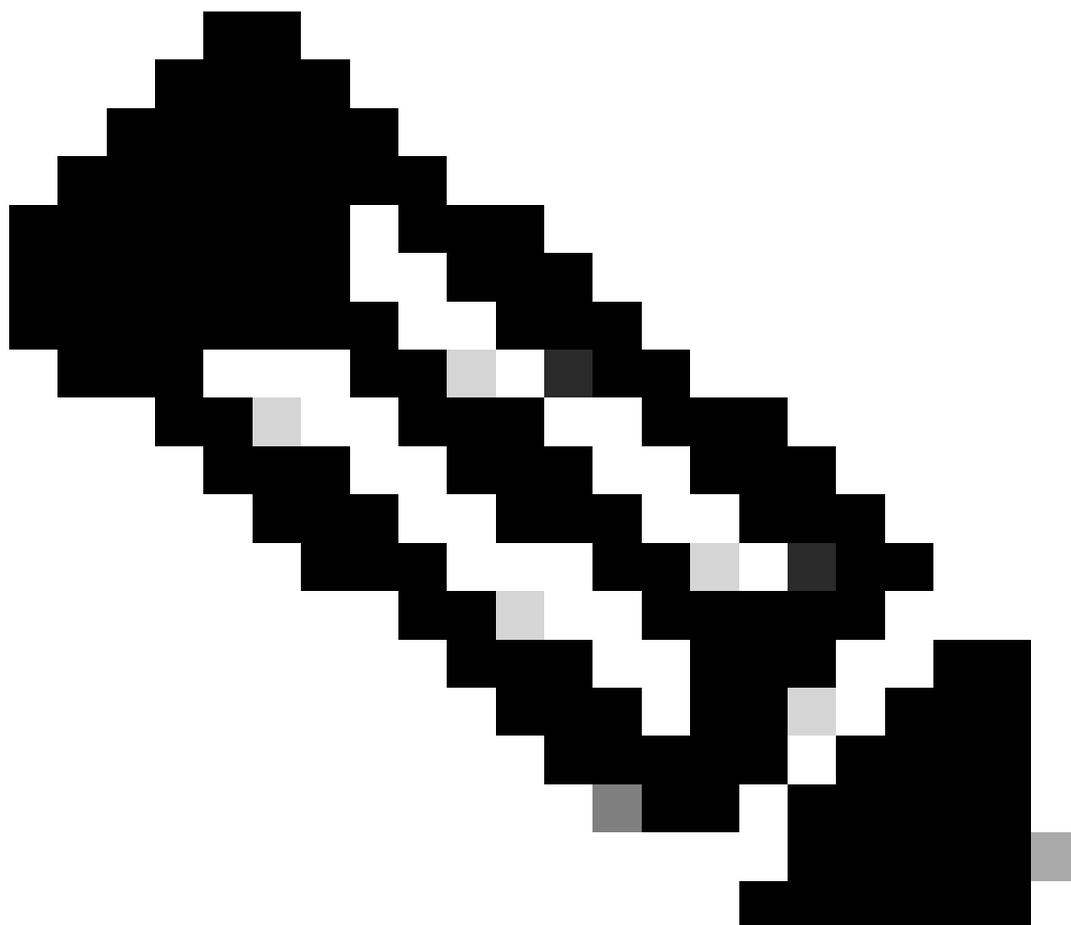
Lo stato dei report cambia durante la comunicazione tra l'istanza del prodotto e il modulo CSM.

State	Descrizione
ApriRumSmartAgent	Nuovo report creato da Smart Agent sul dispositivo
SmartAgentRumStateChiuso	Rapporto RUM inviato al CSSM (i ricaricamenti spingerebbero anche i rapporti aperti allo stato chiuso)
SmartAgentRumStateNon riconosciuto	Rapporto RUM in attesa di conferma da CSSM, ID poll fornito
SmartAgentRumStateRiconosciuto	Rapporto RUM inviato al CSSM e riconosciuto

La funzionalità Smart Licensing Using Policy è stata introdotta in Catalyst 9800 con la versione del codice 17.3.2. La versione iniziale 17.3.2 non consente di visualizzare il menu di configurazione SLUP nel WebUI del WLC, introdotto con la versione 17.3.3. La SLUP è diversa dalle licenze intelligenti tradizionali in due modi:

- WLC comunica ora con CSM tramite il dominio smartreceiver.cisco.com, anziché tramite il dominio tools.cisco.com.
- Anziché registrarsi, il WLC stabilisce ora il trust con il CSM o SSM locale.

- i comandi CLI sono stati leggermente modificati.
 - SLR (Smart Licensing Reservation) non esiste più. È invece possibile segnalare periodicamente l'utilizzo manualmente.
 - La modalità di valutazione non esiste più. Il WLC continua a funzionare a piena capacità anche senza licenza. Il sistema è basato sull'onore e l'utente è tenuto a segnalare periodicamente l'utilizzo della licenza (in modo automatico o manuale in caso di reti con interruzioni dell'alimentazione).
-



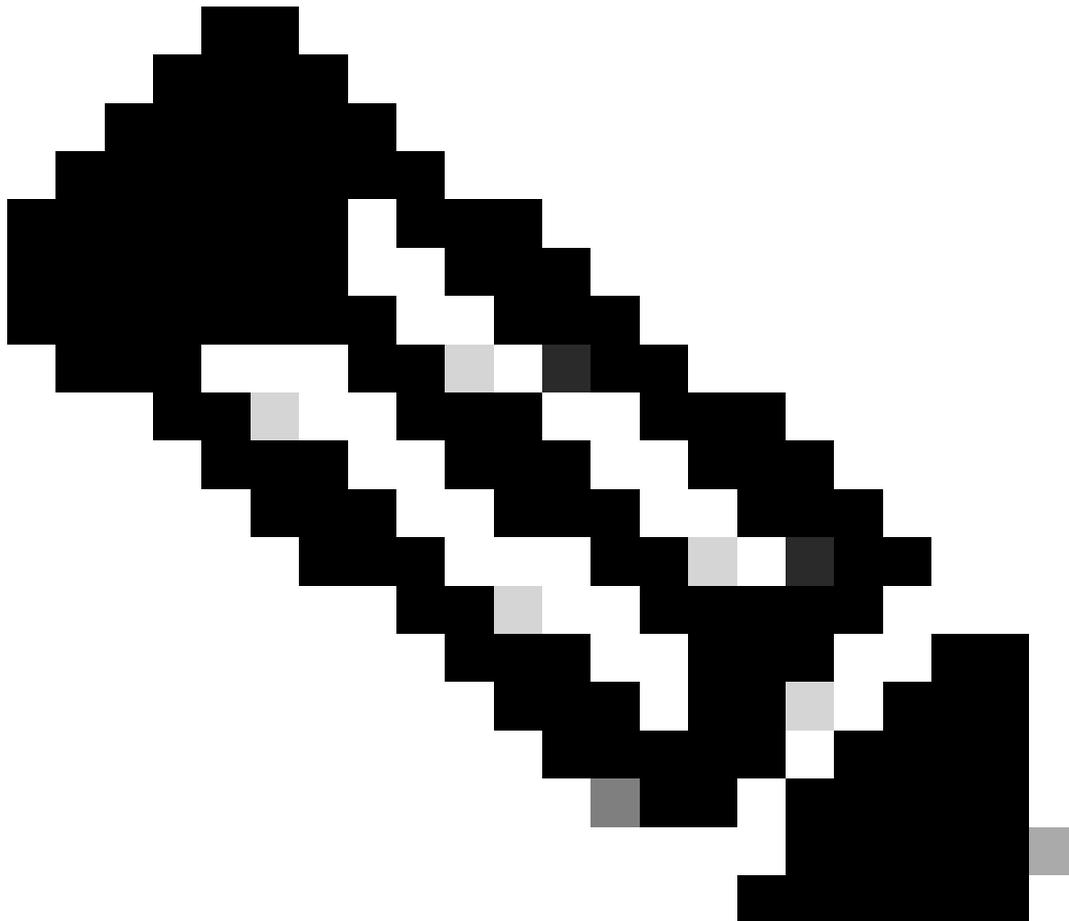
Nota: Avviso: Se si usa un controller wireless Cisco Catalyst 9800-CL, accertarsi di conoscere i requisiti obbligatori dell'ACK che iniziano con Cisco IOS® XE Cupertino 17.7.1. Vedere i requisiti di reporting e riconoscimento RUM per il controller wireless Cisco Catalyst 9800-CL.

Risoluzione dei problemi di comunicazione di Smart Licensing 9800 con CSM a connessione diretta e server locale SSM

* Il nuovo controller 9800 deve rispettare alcune procedure per il completamento del flusso di

lavoro delle licenze intelligenti.

1. Creare un token dal portale CSM e importare il token per stabilire un ID trust necessario per ottenere l'autorizzazione per il report sull'utilizzo delle licenze in futuro. Questo valore di ID trust è la chiave per CSM per convalidare il report inviato dal controller 9800. Questo token trustid verrebbe aggiornato periodicamente e scambiato come parte dei report sull'utilizzo di Rum con CSSM.



Nota: A partire da Cisco IOS XE Cupertino 17.7.1, è necessario un codice di attendibilità. Poiché il codice di attendibilità viene stabilito per numero di serie, per l'installazione di 9800 HA SSO verranno installati 2 codici di attendibilità.

Codice trust

Una chiave pubblica legata all'interfaccia UDI, utilizzata dall'istanza del prodotto per:

- Firma un rapporto RUM. In questo modo si evita la manomissione e si garantisce l'autenticità

dei dati.

- Abilitare la comunicazione protetta con CSM.

Da Cisco IOS XE Cupertino 17.7.1, un codice di attendibilità viene ottenuto automaticamente nelle topologie in cui l'istanza del prodotto avvia l'invio di dati alla CSLU e nelle topologie in cui l'istanza del prodotto si trova in una rete con interruzioni di aria.

- È possibile ottenere un codice di trust da CSM utilizzando un token ID.

In questa finestra è possibile generare un token ID nell'interfaccia utente Web di CSM per ottenere un codice di attendibilità e installarlo nell'istanza del prodotto. È necessario sovrascrivere l'eventuale codice di attendibilità preinstallato. Se un'istanza del prodotto è connessa direttamente a CSSM, utilizzare questo metodo per consentire all'istanza del prodotto di comunicare con CSSM in modo sicuro. Questo metodo per ottenere un codice di trust è applicabile a tutte le opzioni di connessione diretta a CSM. Per ulteriori informazioni, vedere [Connessione direttamente a CSM](#).

Da Cisco IOS XE Cupertino 17.9.1, viene ottenuto automaticamente un codice di attendibilità nelle topologie in cui CSLU avvia il recupero dei dati dall'istanza del prodotto.

Se è presente un codice di attendibilità preinstallato, viene automaticamente sovrascritto. Un codice di attendibilità ottenuto in questo modo può essere utilizzato per la comunicazione protetta con CSM.

* Accertarsi che la configurazione su 9800 per le licenze Smart sia integra. 9800 utilizza Smart come mezzo di trasporto per comunicare con CSM.

Intelligente con CSSM

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

Uso intelligente del proxy

```
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 locale

```
Device(config)#license smart transport cslu Device(config)#license smart url cslu https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodinglup2304-1
```

Verificare che la ricerca del dominio e il server dei nomi siano raggiungibili tramite l'interfaccia di origine.

Device(config)#ip domain name

Device(config)#ip name server

Device(config)#ip domain lookup

show license all restituisce il tipo di trasporto e i dettagli dell'URL configurati su 9800: Assicurarsi che la configurazione sia assoluta.

Trasporto intelligente

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

SSM locale

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

* se esiste un proxy tra 9800 e CSM, accertarsi di consentire l'indirizzo IP elencato sul proxy per una comunicazione ininterrotta.

Verifica connessione a Smart Receiver

Usare il comando curl:

- ricciolo <https://smartreceiver.cisco.com/licservice/license>
- Risposta prevista: Questo è lo Smart Receiver!

Test connessione al server locale SSM

Usare il comando curl:

- curl -v -k <https://SSM-Onprem-FQDN-address>/cslu/v1/pi/ssmsfloodingslup2304-1>
- Risposta prevista: Questo è lo Smart Receiver!

Cerca indirizzo IP ricevitore

Utilizzare questo comando nslookup:

- nslookup smartreceiver.cisco.com

Risposta prevista:

- Server: 171.70.168.183 ← Questo è il server DNS

- Server: dns-sj.cisco.com ← Facoltativamente può essere visualizzato
- Indirizzo: 10.10.10.10#53
- Nome: smartreceiver.cisco.com
- Indirizzo: 146.112.59.81
- Nome: smartreceiver.cisco.com
- Indirizzo: 2a04:e4c7:ffe:f

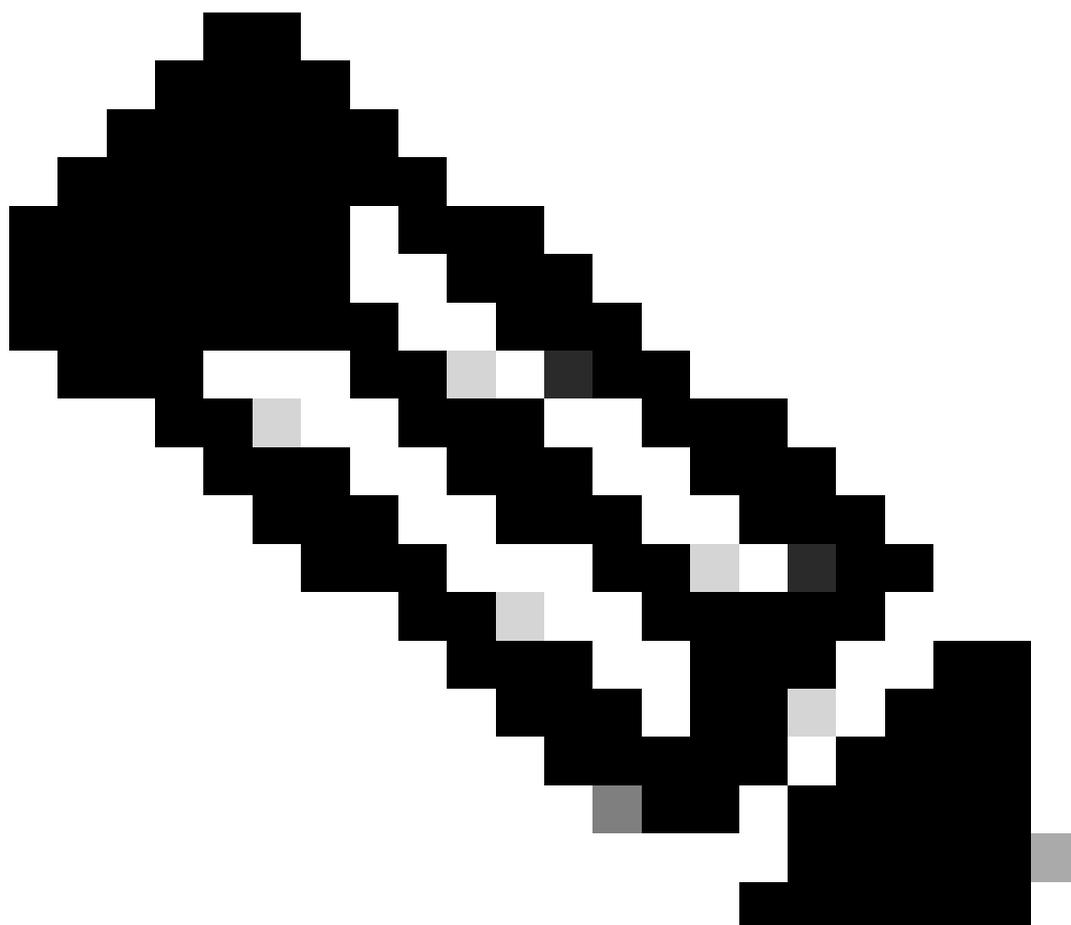
Come viene risolto l'IP dal sistema?

Utilizzare il comando dig:

- digita smartreceiver.cisco.com + breve

Risultato previsto

- 146.112.59.81



Nota: Il componente Smart Receiver di CSSM ha sostituito il vecchio tools.cisco.com e un

unico punto di contatto per i clienti MSLA che hanno effettuato rapporti Rum, registrazione e fatturazione.

ip http client interfaccia-origine <interfaccia-origine>

Questo comando contrassegna in modo esplicito il percorso di origine di CSM.

ip http client secure-trustpoint SLA-TrustPoint

Assicurarsi che secure-trustpoint sia selezionato come SLA-TrustPoint poiché è firmato dalla CA radice della licenza. Sia SSM locale che CSSM sono considerati attendibili dal certificato CA radice della licenza.

Certificato CA:

Stato: Disponibile

Numero di serie certificato (hex): 01

Utilizzo certificato: Firma

Emittente:

cn=Cisco Licensing Root CA

o=Cisco

Oggetto:

cn=Cisco Licensing Root CA

o=Cisco

Data di validità:

data di inizio: 19:48:47 UTC 30 maggio 2013

data di fine: 19:48:47 UTC 30 maggio 2038

Punti di trust associati: SLA-TrustPoint del pool di fiducia

Storage: nvram:CiscoLicensi#1CA.cer

License Smart Sync all è il comando per avviare un nuovo report Rum dal controller 9800 e dal formato XML. Quando questo comando viene eseguito sul controller in cui il codice di attendibilità non è installato nella versione 17.9.x, genera innanzitutto una richiesta per il codice di attendibilità anziché un report di utilizzo Rum.

Codice Trustcode non valido elaborato da CSM

Importa CODICE ATTENDIBILITÀ:

Ricevuto il set 17 17:35:26 2024 UTC

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:FCL2630000P</udi><status><success>false</success><message>Per questo elemento è già stata elaborata una richiesta di trust corrispondente a un trust-id superiore dispositivo.</message><code>OLD_TRUST_ID</code><correlationID>null-null</correlationID></status></trustCode><signature>MEQCIAg71/hlcWxUiof8VstpmPhRH8jptPZPrvaSp
```

CSSM prevede che il controller invii l'ID del codice di trust incrementale come scopo di protezione e l'implicazione di un codice di trust non valido interromperà CSSM per elaborare le richieste di gestione delle licenze da parte del controller. In questo caso, la gestione delle licenze CSM potrebbe avere problemi con il dashboard delle licenze.

Codice Trustcode valido elaborato da CSM

Importa CODICE ATTENDIBILITÀ:

```
<smartLicenseTrust><trustCode><udi>P:C9800-L-F-K9,S:XXXXXXXXXX</udi><customerInfo><smartAccount>Cisco Demo Internal Smart Account</smartAccount><virtualAccount>0Relazione Demo-HK-PartnerA</virtualAccount></customerInfo><piid>0eb1d627-bbed-46a8-9a4b-fc5b48a7c36b</piid><dateStamp>2024-09-10T07:21:30</dateStamp></subCA><trustId>110</trustId><stato><strong>guAqDYkGn206meTHt8+dqra0LAciHEZKxmqueurKOU0g=</signature></smartLicenseTrust>
```

Frequenza di comunicazione

L'intervallo di report che è possibile configurare nella CLI o nella GUI non ha alcun effetto.

9800 WLC comunica con CSM o con Smart Software Manager in locale ogni 8 ore, indipendentemente dall'intervallo di reporting configurato tramite interfaccia Web o CLI. Ciò significa che i punti di accesso appena aggiunti possono essere visualizzati sul CSM fino a 8 ore dopo l'iniziale aggiunta.

Per individuare la data e l'ora successive in cui le licenze vengono calcolate e segnalate, usare il comando `show license air entities summary`. Questo comando non fa parte del tipico output `show tech` o `show license`:

`show license air entities summary`, comando:

```
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
```

Dopo l'installazione del codice di fiducia nel controller 9800, la fase successiva consiste nel generare il report sull'utilizzo dell'attività di licenza tramite Rum (Resource Measurement Unit) in

formato XML. Il comando License smart sync all/local avvia, genera o apre una nuova misurazione Rum basata sull'access point gestito nel controller. Fondamentalmente, il componente smart agent 9800 invia una chiamata API al modulo di gestione delle licenze per raccogliere un nuovo report Rum con le informazioni sulle licenze.

show license rum id all, comando:

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 comando:

È possibile ottenere i dettagli della licenza riportati in ID Rum. Questo comando estrae software_identifier_tag, che è l'elemento corrispondente alla chiave nel database CSM per convalidare un tipo di licenza da un'istanza del prodotto.

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

Dettagli del report sull'utilizzo delle licenze Smart:

=====

ID report: 1719005447

Nome metrica: DIRITTO

Nome funzionalità: vantaggio della rete aerea

Valore metrica: regid.2018-06.com.ciisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896

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

ID report precedente: 1719005445, ID Report Successivo: 0

State: OPEN, Motivo modifica stato: Nessuna

Motivo chiusura: Nessuna

Ora di inizio: 10 set 10:00:08 2024 UTC, ora di fine: 16 set 16:15:08 2024 UTC

Stato archiviazione: ESISTERE

ID transazione: 0

Messaggio transazione: <nessuno>

* Ora viene generato il report Rum. Nello stato OPEN deve essere inviato al CSM per ricevere il ACK dal CSM.

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

Errori riportati nell'output del comando show license eventlog e/o show log

"Errore di comunicazione con Cisco Smart License Utility (CSLU): Non sono fornite informazioni dettagliate"

È possibile osservare questo errore quando non è stata stabilita la comunicazione HTTPS con On-Prem. Motivi potenziali:

- Per le comunicazioni con OnPrem viene utilizzato un VRF specifico. L'interfaccia di origine del client HTTP deve essere configurata manualmente
- Il controllo di revoca NON è disabilitato nella configurazione SLA-Trustpoint
- Un altro trust point è impostato come predefinito per la segnalazione crittografica (ad esempio: sul gateway SIP)

"Errore server HTTP 502: Gateway non valido"

Questo errore è attualmente esaminato dal team di sviluppo locale. Nella maggior parte dei casi non si osserva alcun impatto sul servizio.

In genere, 10 secondi dopo, SAVE_COMM_RESTORED.

Esempio:

```
9 lug 13:15:29,902: %SMART_LIC-3-COMM_FAILED: Errore di comunicazione con Cisco Smart License Utility (CSLU): Errore del server HTTP 502: Gateway non valido
9 lug 13:15:39,881: %SMART_LIC-5-COMM_RESTORED: Comunicazioni con Cisco Smart License Utility (CSLU) ripristinate
```

"Errore server HTTP 404: Non trovato"

Questo errore viene rilevato sul dispositivo Cisco IOS XE durante un tentativo di installazione del codice di attendibilità mentre l'URL di trasporto puntava a On-Prem (CSLU).

Il comando "license smart trust idtoken <token> [all|local]" viene utilizzato SOLO quando il dispositivo comunica direttamente con CSM.

NOTA: A seconda della piattaforma, questo messaggio può anche indicare che l'impostazione "Convalida dispositivo" è attivata nel pannello delle impostazioni CSLU nell'area di lavoro Amministrazione locale. Verificare che il dispositivo che si sta tentando di registrare si trovi nella scheda "Criteri di utilizzo SQL" del server locale. Se le periferiche non si trovano nella scheda, è necessario disattivare l'interruttore. Provare quindi a sincronizzare di nuovo il dispositivo con il server locale. Per un'immagine di questa impostazione, fare riferimento alla fine di questo articolo.

SAVE_INIT_CRYPTO success="False" error="L'inizializzazione della crittografia non è stata completata"

Questo errore può essere osservato poco dopo l'avvio del sistema. Dopo circa 30 secondi, l'inizializzazione della crittografia è stata completata - in questo caso, non vi è alcun impatto sul servizio.

Esempio:

```
2021-06-25 10:09:23,378 UTC SAVE_INIT_SYSTEM_INIT
2021-06-25 10:09:24.383 UTC SAVE_INIT_CRYPTO success="False" error="Inizializzazione
crittografia non completata"
2021-06-25 10:09:54.383 UTC SAVE_INIT_CRYPTO success="Vero"
```

Se l'inizializzazione della crittografia non viene completata per alcuni minuti/ore, verificare che la configurazione NTP sia presente e/o che gli orologi siano sincronizzati. Il salvataggio della configurazione corrente consente di riavviare l'inizializzazione della crittografia.

Se il problema persiste, si consiglia di approfondire la ricerca con Cisco TAC.

SAVE_UTILITY_RUM_FAIL error="[HOST_NOT_FOUND] Device Host non trovato"

È molto probabile che l'impostazione "Convalida dispositivo" sia impostata nel pannello delle impostazioni CSLU nell'area di lavoro Amministrazione locale.

Questa impostazione consente di garantire la ricezione dei report RUM da istanze note del prodotto.

SAVE_COMM_FAIL error="Impossibile risolvere il nome host/nome di dominio del server"

Questo errore indica un problema di connettività che può avere origine con la risoluzione DNS. È necessario verificare che il dispositivo sia in grado di risolvere l'URL di destinazione. In genere, il comando ip host <url> <ipassociated> non è configurato correttamente. Controllare questo punto.

Molto probabilmente trovereste problemi di comunicazione.

Statistiche di comunicazione:

=====

Livello di comunicazione consentito: INDIRETTO

Stato generale: <vuoto>

Istituzione trust:

Tentativi: Totale=30, Riuscito=0, Non riuscito=30 Errore in corso: Globale=30 Comunicazione=30
<<<<<<<<

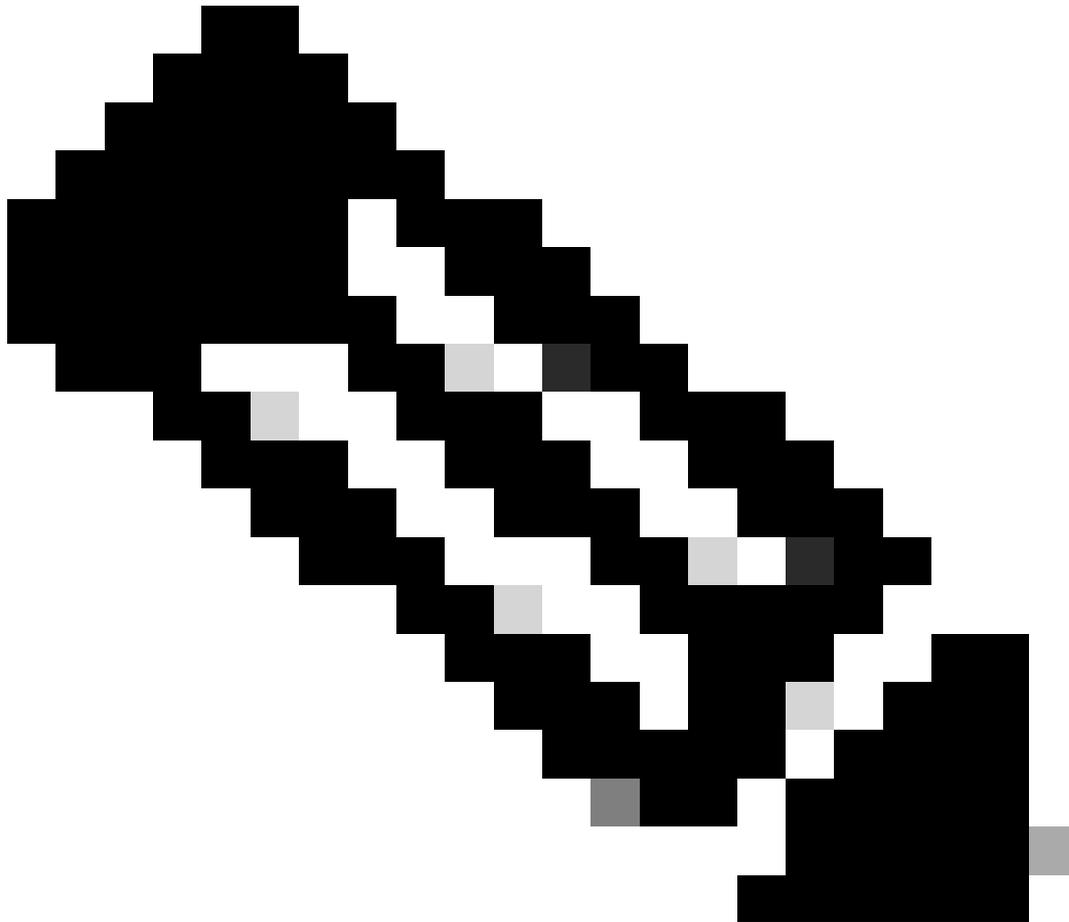
Ultima risposta: NESSUNA RISPOSTA il 12 febbraio 10:52:56 2023 GMT <<<<<<<<<<

Failure reason: <nessuno>

Ora ultima operazione riuscita: <nessuno>

Ora ultimo errore: 12 feb 10:52:56 2023 GMT

Livello di comunicazione consentito come INDIRETTO indica che il codice di trust richiesto non è stato installato correttamente sul controller 9800.



Nota: Nota: Il modulo CSM è la fonte della verità di tutti i dati relativi alle licenze.

* Se il problema di comunicazione di base tra 9800 e CSSM viene risolto eseguendo il test, abilitare il debug su alcuni moduli coinvolti per le comunicazioni delle licenze intelligenti. Abilitando il debug su 9800, la CPU risulterà sovraccarica per un determinato intervallo di tempo e sarà quindi necessario eseguire queste azioni durante le ore non lavorative.

Debug

* Sono disponibili 4 moduli per la comunicazione intelligente delle licenze dal modello 9800 al

modello CSSM o SSM locale

1. Modulo crittografico

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. Modulo HTTP

Server HTTP:

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. Modulo Openssl

ssl openssl:

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

4. Il modulo Smart Licensing viene denominato smart agent, incluso il gateway di trasporto

Licenza:

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

Registri di sistema:

verifica dell'identità del server e convalida della SAN nel certificato. Convalida del punto di trust dalla libreria SSL di crittografia.

16 set 16:29:12,236: Controllo identità server con host: 10.106.43.37

16 set 16:29:12,236: Identità del server da verificare: indirizzo IP 10.106.43.37, len 12

16 set 16:29:12,329: CRYPTO_PKI: (A645F) Verifica certificati identici

16 set 16:29:12,329: CRYPTO_PKI(Cert Lookup) issuer="cn=Cisco Licensing Root CA,o=Cisco" numero di serie= 0F 42 40

16 set 16:29:12,329: CRYPTO_PKI: (A645F) I trust appropriati sono: SLA-TrustPoint,Pool di fiducia6,Pool di fiducia6,

16 set 16:29:12,329: CRYPTO_PKI: (A645F) Tentativo di convalidare il certificato utilizzando il

criterio SLA-TrustPoint

16 set 16:29:12,329: CRYPTO_PKI: (A645F) Utilizzo di SLA-TrustPoint per la convalida del certificato

16 set 16:29:12,345: SSL_connect:negoziazione SSL completata

16 set 16:29:12,345: SSL_connect:negoziazione SSL completata

Dopo aver inviato il report sull'utilizzo al modulo CSM, è necessario visualizzare il comando show license history message per l'aggiornamento corretto:

Le richieste devono avere un componente come UDI_SERIAL_NUMBER, hostname, software_tag_identifer che indica quale modalità di licenza viene utilizzata dal controller 9800 e request_type come "LICENSE_USAGE"

Sono presenti più tipi di licenza:

1. ID_TOKEN_TRUST

2. TRUST_SYNC

3. LICENSE_USAGE

Report utilizzo:

RICHIESTA: 16 set 16:30:16 2024 UTC

```
"{"sender_info":{"connect_info":{"nome":"C_agent","versione":"5.8.6_rel/15","produzione":true,"intento":"NUOVO","POLICY_USAGE","TELEMETRY","CSLU_V1"},"timestamp":1726504244391,"nonce":"13980553869667320622","sudi":{"udi_pid":"C9800-L-F-K9","udi_serial_number":"FCL2630000P"},"product_instance_identifer":"","software_tag_identifer":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"},"elenco_dispositivi":[{"sudi":"C9800-L-F-K9","udi_serial_number":"FCL2630000P"},"identificatore_tag_software":"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2"},"identificatore_istanza_prodotto":"","versione_prodotto":"17.12.02","nomehost":"renjith-eap-test","ruolo":"Attivo","tipo_richiesta":"ID_TOKEN_TRUST","id_riga_richiesta":1,"licenza_smart":
```

Report utilizzo:

RICHIESTA: 16 set 16:30:16 2024 UTC

```
"{"sender_info":{"connect_info":{"nome":"C_agent","versione":"5.8.6_rel/15","produzione":true,"intento":"NUOVO","POLICY_USAGE","TELEMETRY","CSLU_V1"},"timestamp":1726504153254,"nonce":"10743401694998030696","sudi":{"udi_pid":"C9800-L-F-K9","udi_serial_number":"FCL2630000P"},"product_instance_identifer":"","software_tag_identifer":"regid.2019-
```

06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"},\"elenco_dispositivi\":[\"sudi\": \"udi_pid\": \"C9800-L-F-K9\", \"udi_serial_number\": \"FCL2630000P\"}, \"identificatore_tag_software\": \"regid.2019-06.com.cisco.C9800_L_F_K9,1.0_9529f872-1b08-4cac-9279-71c391233fc2\", \"identificatore_istanza_prodotto\": \"\", \"versione_prodotto\": \"17.12.02\", \"nomehost\": \"renjith-eap-test\", \"ruolo\": \"Attivo\", \"tipo_richiesta\": \"TRUST_SYNC\", \"id_riga_richiesta\": 1, \"licenza_smart\":

Report utilizzo:

RICHIESTA: 16 set 16:30:16 2024 UTC

```
{\"sender_info\":{\"connect_info\":{\"name\":\"C_agent\",\"version\":\"5.8.6_rel/15\",\"production\":true,\"additional_info\":022,\"nonce\":\"77709655117429624\",\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"},\"product_instance_identifer\":\"\", \"software_tag_identifier\":\"regid.2019-06.com.cisco.C9800_K_L_F_49,1.0_9529f872-1b08-4cac-9279-71c391233fc2\"},\"elenco_dispositivi\":[\"sudi\":{\"udi_pid\":\"C9800-L-F-K9\",\"udi_serial_number\":\"FCL2630000P\"}, \"identificatore_tag_software\": \"regid.2019-06.com.ci8.C900_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\": \"LICENSE_USAGE\", \"request_line_id\": 1, \"request_line_licenza\":
```

* È importante comprendere la risposta da CSSM o SSM on-prem:

Pacchetto di risposta di errore:

RISPOSTA: 16 set 16:30:16 2024 UTC

```
{  
  \"stato\": \"NON RIUSCITO\",  
  \"codice_messaggio\": \"ERRORE durante l'utilizzo delle licenze\",  
  \"messaggio\" \"\",  
  \"nonce\" \"77709655117429624\"  
}
```

L'errore indica che esiste già una voce per il controller nel server licenze CSM o SSM locale che impedisce l'aggiunta di un nuovo record nel database. È necessario eliminare il record attivo o non aggiornato da CSM o SSM locale e inviare nuovamente il report Rum.

Poll_id risposta valida:

RISPOSTA: 16 set 16:29:14 2024 UTC

```
{
```

```
"sender_info": {
  "connect_info": {
    "nome": CSLU_V1"
    "versione": "v1",
    "produzione": vero,
    "additional_info": "",
    "funzionalità": [
      "UTILITÀ",
      "DLC"
      "AppHA"
      "MULTITIER"
      "EXPORT_2",
      "OK_TRY_AGAIN",
      "POLICY_USAGE",
      CSLU_V1"
      "CSLU_V2"
      "TELEMETRIA"
    ]
  },
  "data e ora": 1726504153302,
  "nonce" "1074340169498030696",
  "sudi": {
    "udi_pid": "C9800-L-F-K9"
    "udi_serial_number": "FCL2630000P"
  },
  "product_instance_identifier": "",
  "identificatore_tag_software": "regid.2019-06.com.ciisco.C9800_L_F_K9,1.0_9529f872-1b08-
```

4cac-9279-71c391233fc2"

```
},  
"stato": "COMPLETA",  
"license_data": [  
  {  
    "stato": "OK_POLL",  
    "request_line_id": 1,  
    "sudi": {  
      "udi_pid": "C9800-L-F-K9"  
      "udi_serial_number": "FCL2630000P"  
    },  
    "poll_id": 5583279046281676962,  
    "intervallo_poll": 86739,  
    "smart_license": ""  
  }  
]  
}
```

* Come convalidare poll_id è memorizzato nel database locale 9800 e la frequenza con cui esegue il polling per ottenere un ACK per il report Rum inviato.

Comando di test per verificare la necessità di attivazione tramite Service Internal.

```
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
```

* Come si può capire dalla spiegazione che le richieste iniziali inviate dal controller 9800 sarebbero sempre codice di fiducia token e senza di esso, il controller 9800 non genererebbe mai un nuovo report sull'utilizzo Rum e quindi la modifica dell'utilizzo della licenza non può essere inviata su CSM.

* Un esempio richiede poll_id per License_usage.

```
test license smart conversion list-poll-info Poll Request Information: PollID | Type | Delta | Poll Time 5583279046281677674 |
```

* se è già stato elaborato un ACK nel database locale CSM o SSM, è possibile forzare l'agente intelligente sul controller 9800 a eseguire il polling e ottenere ACK al più presto senza attendere il tempo indicato

nel ciclo poll_id.

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

Informazioni correlate

- [Configurazione delle licenze offline \(Air Gapped\) su 9800 WLC](#)
- [Supporto tecnico Cisco e download](#)
- [Configurazione della licenza Smart Licensing di Catalyst 9800 WLC tramite criteri con DNA Center](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).