Risoluzione dei problemi relativi alle licenze su Nexus 9000

Sommario

Introduzione

Questo documento descrive i tipi di errori più comuni relativi alle licenze Smart sugli switch Nexus serie 9000.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Smart Licensing su switch Nexus serie 9000
- Cisco Smart License Utility (CSLU)

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.

Errori di comunicazione

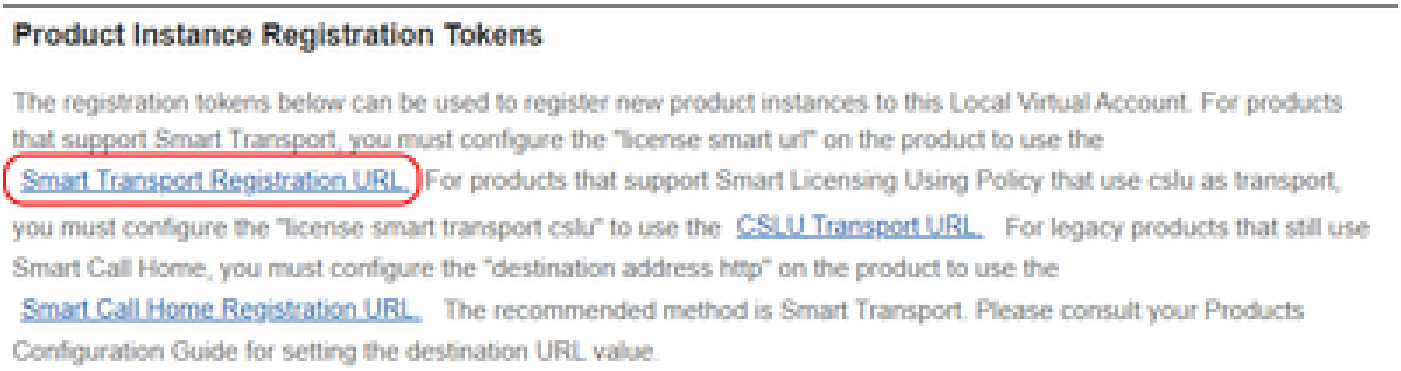
"Impossibile stabilire una connessione protetta perché non è possibile convalidare il certificato TLS del server"

Questo errore CSLU è in genere causato dalla configurazione di un FQDN non corretto utilizzando license smart url cslu o i comandi license smart url smart oppure da un dispositivo nel percorso che esegue lo spoofing SSL (in genere un firewall con ispezione SSL abilitata).

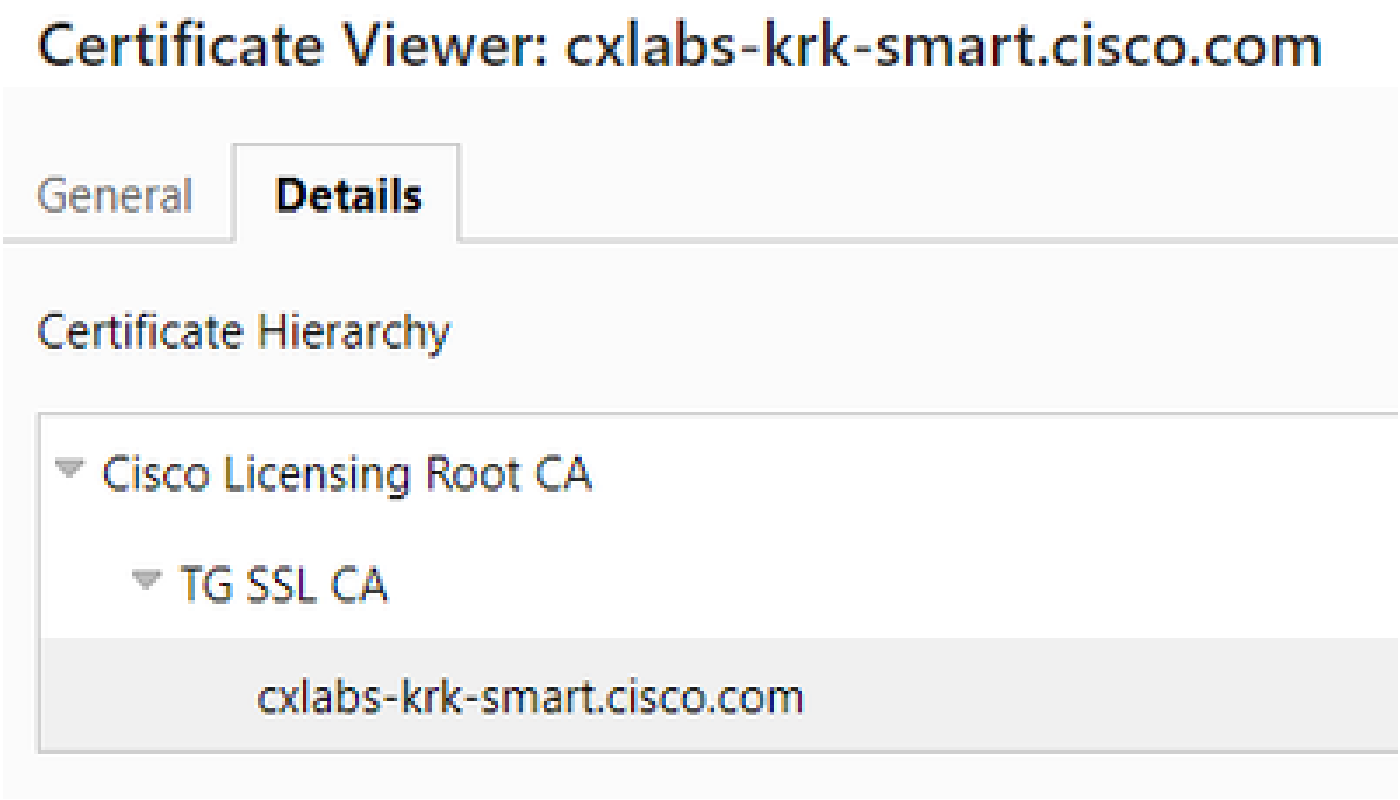
Il protocollo HTTPS su uno switch Nexus non è diverso da quello di un normale sistema operativo client. Quando accede a un collegamento HTTPS, il client verifica l'FQDN a cui sta tentando di accedere in base all'FQDN ricevuto nel certificato, ovvero il campo CN nell'intestazione dell'oggetto o il campo SAN. Il client verifica inoltre se il certificato ricevuto è firmato da un'Autorità di certificazione attendibile.

Se si tenta di accedere a https://www.cisco.com, il browser lo apre senza problemi. Tuttavia, se si apre https://173.37.145.84, viene visualizzato un avviso che indica che la connessione non può essere considerata attendibile, anche se www.cisco.com si risolverebbe in 173.37.145.84. Il browser sta tentando di accedere a 173.37.145.84, pertanto il certificato non viene considerato valido.

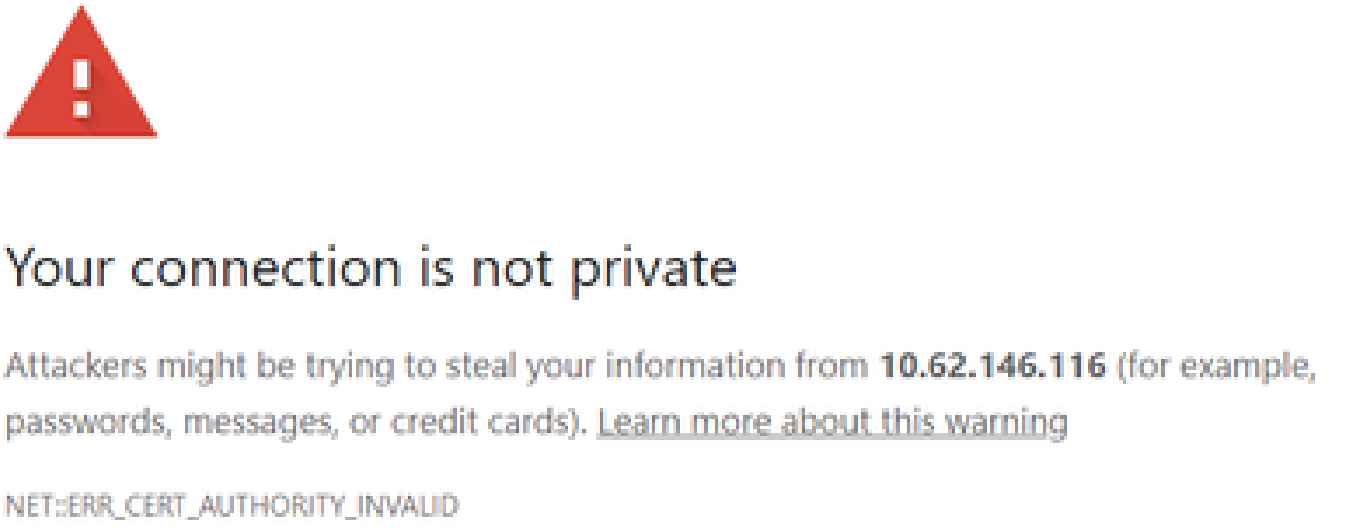
Per questo motivo, quando si configura l'indirizzo CSSM sullo switch, è fondamentale utilizzare esattamente l'URL proposto dal CSSM stesso; contiene il nome di dominio completo (FQDN) incorporato nel certificato:



È inoltre importante ricordare che esistono certificati distinti utilizzati per la gestione locale del modulo CSM (porta 8443 per impostazione predefinita) e per la registrazione delle licenze (porta 443 per impostazione predefinita). Il certificato di gestione può essere autofirmato o firmato da una CA dell'organizzazione (enterprise) locale, considerata attendibile all'interno dell'organizzazione, o da una CA globale (global trusted), ma la licenza utilizza sempre una CA radice di Cisco Licensing. Questa operazione viene eseguita automaticamente senza alcun intervento da parte dell'utente:



Questa CA è considerata attendibile dagli switch Cisco, ma non dai normali PC client. Se si tenta di accedere all'URL proposto da CSM utilizzando un PC, il browser visualizza un errore dovuto alla mancata attendibilità dell'autorità di certificazione, ma lo switch non presenta problemi:



Tuttavia, se è presente un firewall che esegue l'ispezione SSL con lo spoofing dei certificati tra lo switch e il server CSM, il firewall sostituisce il certificato firmato dall'autorità di certificazione Cisco con un certificato diverso firmato in genere da un'autorità di certificazione dell'organizzazione (enterprise), considerata attendibile da tutti i PC e i server dell'organizzazione, ma non dallo switch. Accertarsi di escludere qualsiasi traffico verso CSSM dall'ispezione HTTPS.

Per risolvere il problema relativo all'errore "Impossibile convalidare il certificato TLS del server",

accedere all'URL configurato sullo switch con un browser e verificare che il certificato sia firmato correttamente dall'autorità di certificazione Cisco e che il nome FQDN nella stringa dell'URL corrisponda al nome FQDN nel certificato.

"Errore di comunicazione" o "Impossibile risolvere l'host: cslu-local"

Il CSM è in genere configurato con un FQDN nell'URL e nella maggior parte delle distribuzioni Nexus il DNS non è configurato, il che porta spesso a questo tipo di errore.

Il primo passaggio della procedura di risoluzione dei problemi consiste nel eseguire il ping dell'FQDN configurato dal VRF utilizzato per Smart Licensing. Ad esempio, con questa configurazione:

```
license smart transport smart
license smart url smart https://smartreceiver.cisco.com/licservice/license
license smart vrf management
```

```
switch# ping smartreceiver.cisco.com vrf management
% Invalid host/interface smartreceiver.cisco.com
```

Questo errore indica che la risoluzione DNS nella gestione VRF non funziona. Verificare la configurazione ip name-server nel VRF specificato. Si noti che la configurazione del server DNS è per VRF, pertanto la configurazione ip name-server nel VRF predefinito non ha effetto in Gestione VRF. Come soluzione di stop-gap, l'host ip può essere usato per aggiungere una voce manuale, ma si supponga che in futuro l'indirizzo IP del server possa cambiare e che questa voce possa non essere più valida.

Se il nome di dominio viene risolto ma i ping hanno esito negativo, è possibile che un firewall blocchi i ping in uscita. In questo caso, è possibile utilizzare telnet per verificare se la porta 443 è aperta.

```
switch# telnet smartreceiver.cisco.com 443 vrf management
```

Se anche questa operazione non riesce, risolvere il problema relativo al percorso di rete verso il server e verificare che funzioni.

"Impossibile inviare il messaggio HTTP Call Home"

Questo messaggio è fondamentalmente simile al messaggio "Errore di comunicazione". La differenza sta nel fatto che viene generalmente visualizzata sugli switch con Smart Licensing

precedente, non su Smart Licensing con criteri introdotti in NXOS versione 10.2. Con le Smart Licensing precedenti, l'URL a cui accedere viene configurato con il comando callhome.

```
callhome
...
destination-profile CiscoTAC-1 transport-method http
destination-profile CiscoTAC-1 index 1 http https://tools.cisco.com/its/service/oddce/services/DDCEServ
transport http use-vrf management
```

Verificare che la configurazione sia corretta, che utilizzi HTTPS e che sia possibile raggiungere l'URL (in genere tools.cisco.com) sul VRF selezionato.

Ulteriori suggerimenti per la risoluzione dei problemi

Per un elenco di controllo dettagliato relativo alla risoluzione dei problemi e relativo ad altre operazioni che è possibile eseguire per risolvere i problemi relativi alle licenze, fare riferimento a Smart Licensing using Policy Troubleshooting on Data Center Solution.

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).