Cisco IOS XE e GuestShell CA Trust eMudhra Distrust Guide

Sommario

Scopo

Questo documento offre linee guida per Cisco IOS® XE per la sfiducia di emergenza delle autorità di certificazione principali e intermedie di eMudhra.

Utilizzare questa guida per controllare e gestire l'attendibilità CA per i servizi la cui configurazione consente le gerarchie interessate. L'applicabilità del prodotto e le azioni correttive richieste sono definite in Cisco informational. Prima di modificare l'attendibilità, controllare il supporto dei comandi e l'impatto dei servizi per la versione Cisco IOS XE in uso.

Informazioni Cisco: cisco-sa-emudhra-info-ScS22A1r

Certificati eMudhra CA interessati: Originale e con firma incrociata

Inventario verificato il 29 ottobre 2026. Il problema riguarda otto chiavi di autorità di certificazione che emettono Mudhra: sei per TLS e due per la firma del codice. Ogni chiave viene visualizzata in un certificato CA originale emesso da emSign e in un certificato CA con firma incrociata di Sectigo. L'inventario contiene pertanto 16 certificati: 12 certificati TLS e 4 certificati di firma codice.

Ogni coppia originale/con firma incrociata ha lo stesso oggetto e la stessa chiave pubblica, ma un'autorità emittente diversa, un numero di serie e un'impronta digitale del certificato SHA-256. I due moduli forniscono percorsi di certificazione alternativi e devono essere inclusi in un controllo.

A. Emittenti e inventario dei certificati interessati

Autorità di certificazione A — Certificati TLS originali: CN=emSign Root TLS CA - G3, O=eMudhra Technologies Limited, C=IN.

Emittente B — Certificati originali di firma codice: CN=emSign Root CS CA - G3, O=eMudhra Technologies Limited, C=IN.

Emittente C — tutti i certificati con firma incrociata: CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

Soggetti G3B: O=Mudhra BV, C=NL. Soggetti G3C: O=Mudhra Inc, C=US. Ogni cella variante elenca il riferimento dell'emittente, il numero di serie esadecimale e l'impronta digitale SHA-256 (due righe). Il riempimento con zeri iniziali non modifica un valore seriale.

CA emittente interessata (CN)	Certificato originale Emittente / seriale (hex) / SHA-256	Certificato con firma incrociata Sectigo Emittente / seriale (hex) / SHA-256
1. EM DV TLS CA - G3B TLS	Emittente A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Emittente C A024FDF4BA665C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	Emittente A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Emittente C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4DD590AF74631290CF073B122A 2AAC6A1FA479778A0BD43579BD83269
3. EM EV TLS CA - G3B TLS	Emittente A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	Emittente C D8F8685E4F2BD9D82402A85A1C1EB731 579480AEA166290BD3C643589E795FC0 D0E54E86505D180F1DF99EFD3199512
4. EM DV TLS CA - G3C TLS	Emittente A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Emittente C 91F347F1A5B7D39962B95E0E4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158B7368BF648683BB2AA39B02E72
5. EM OV	Emittente A	Emittente C

CA emittente interessata (CN)	Certificato originale Emittente / seriale (hex) / SHA-256	Certificato con firma incrociata Sectigo Emittente / seriale (hex) / SHA-256
TLS CA - G3C TLS	296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	8D5A4811939EF447D77111CDD9849AE9 7485B51C0ED192878FA1D2F948FB529A E1842C5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	Emittente A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F69933FCB072D9A1148D0261F3	Emittente C 05F078752DECE7A1BB8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7. EM OV CS CA - G3B Firma codice	Emittente B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 5142496369AB633EE1DC7DF5DB067B4	Emittente C 41E32B73AC185D6CE0D7480BACF84E69 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8. EM OV CS CA - G3C Firma codice	Emittente B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCA2CEB29 B3B093921DE45474DA7DF4874C630B1	Emittente C D6A5EF613B390F32EF9CDF349F72841 84112972B8E59D14560AE7E711965447 4AAD11990CF3722BFC1E3B91615E1FD

B. Percorsi di certificazione per distinguere

Percorso TLS originale

```
emSign ECC Root CA - G3
  +-- emSign Root TLS CA - G3 (issued by emSign ECC Root CA - G3)
       +-- Original EM DV/OV/EV TLS CA - G3B or G3C
            +-- TLS identity certificate
```

Percorso originale per la firma del codice (CS radice direttamente attendibile)

```
emSign Root CS CA - G3
  +-- Original EM OV CS CA - G3B or G3C
       +-- Code-signing identity certificate
```

Percorso con firma incrociata (TLS e firma del codice)

```
AAA Certificate Services
  +-- One of the eight cross-signed CAs listed above
       +-- TLS or code-signing identity certificate
```

Un percorso TLS può anche terminare in corrispondenza di emSign Root TLS CA - G3 quando la CA è attendibile direttamente. I diagrammi mostrano le relazioni con gli emittenti pertinenti; il percorso accettato dipende dai trust anchor e dai criteri di convalida del servizio utilizzato.

Le CA padre/radice mostrate in questo esempio forniscono il contesto della catena e non sono conteggiate tra le otto chiavi di emissione compromesse. La decisione di rimuovere o non considerare attendibile un elemento padre/radice è diversa dall'identificazione di una chiave intermedia compromessa.

Per l'identificazione, utilizzare l'emittente del certificato e il numero di serie insieme all'impronta digitale SHA-256. Il solo nome del soggetto è insufficiente. Un'impronta digitale del certificato identifica una variante di certificato; un hash SPKI SHA-256 identifica la chiave pubblica condivisa dai moduli originale e con firma incrociata. La rimozione di un solo intermedio memorizzato nella cache non impedisce a un peer di presentarlo tramite un percorso attendibile rimanente.

Origini e data di verifica

Il 29 ottobre 2026 sono stati verificati gli identificativi dei certificati rispetto agli allegati relativi a incidenti pubblici. Ogni coppia originale/con firma incrociata contiene la stessa chiave pubblica. Utilizzare le informazioni Cisco in tempo reale per verificare l'applicabilità del prodotto e lo stato di correzione.

Informazioni Cisco: cisco-sa-emudhra-info-ScS22A1r

Record incidente Mozilla: compromesso chiave intermedia Mudhra (2083449)

Allegato certificato CA originale (9664066)

Allegato certificato CA con firma incrociata AAA (9664067)

Apple: percorsi e impronte digitali dei certificati TLS originali e con firma incrociata

Al 31 ottobre 2026, emSign Root CA - G1 non è identificato tra le CA compromesse elencate in questa guida. La fiducia continua dell'azienda è soggetta alle politiche aziendali e ai successivi aggiornamenti di consulenza.

Gestione dell'attendibilità dei certificati da parte di Cisco IOS XE

I trust PKI configurati contengono certificati CA/identità e criteri di convalida. Il pool di attendibilità PKI contiene certificati CA predefiniti e scaricati per i servizi che lo utilizzano. Identificare la fonte di attendibilità e i criteri utilizzati da ciascun servizio pertinente; la modifica del trustpool non sostituisce i trust point configurati separatamente.

1. Verifica e preparazione

Verificare la versione del software, l'ora della periferica e i certificati installati:

<#root>

```
show version show clock show crypto pki trustpoints show running-config | section crypto pki trustpoint
```

Confrontare l'Autorità di certificazione completa e il numero di serie esadecimale con l'inventario, utilizzando il soggetto come contesto di supporto. Se Cisco IOS XE visualizza solo le impronte digitali MD5 e SHA1, l'impronta digitale SHA-256 dell'inventario non può essere confrontata direttamente in tale output; viene fornito per la verifica dei file dei certificati all'esterno del dispositivo. La spaziatura interna 00 nei numeri di serie può differire. Le ricerche per nome fornitore identificano solo i candidati. Registrare i servizi che dipendono da ciascun trust point e verificare i percorsi originali e con firma incrociata, inclusi i servizi intermedi direttamente attendibili.

Esempi: CA radice e CA secondaria interessata

Vengono visualizzati esempi abbreviati del certificato dettagliato; gli altri campi sono omessi.

Confrontare l'oggetto, l'autorità emittente e il numero di serie.

Esempio di CA radice: CA radice ECC emSign - G3

```
CA Certificate
  Certificate Serial Number (hex): 3CF607A968700EDA8B84
  Issuer:
    cn=emSign ECC Root CA - G3
  Subject:
    cn=emSign ECC Root CA - G3
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Esempio di SubCA interessata: certificato originale emesso da emSign

```
CA Certificate
  Certificate Serial Number (hex): 00A4AEE678F23362B4C0E460B772F214
  Issuer:
    cn=emSign Root TLS CA - G3
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Esempio di SubCA interessata: Certificato con firma incrociata Sectigo

```
CA Certificate
  Certificate Serial Number (hex): 00A024FDF4BA665C785CE4A020483858B7
  Issuer:
    cn=AAA Certificate Services
  Subject:
    cn=EM DV TLS CA - G3B
  Associated Trustpoints: <NAME-OR-Trustpool>
```

Entrambi i moduli SubCA hanno lo stesso oggetto ma diversi emittenti e numeri di serie. Confrontare l'emittente completo e l'ordine di successione con l'inventario; la spaziatura interna 00 può differire. Registrare i trust point associati per individuare il trust point o il pool proprietario. La radice mostrata è il contesto della catena; non è una delle otto chiavi di emissione compromesse.

Mantieni disponibili un metodo di accesso per il ripristino e un bundle sostitutivo approvato. Se necessario, utilizzare la procedura di backup dei certificati e delle chiavi approvata. Eseguire il backup della configurazione; questa copia da sola non è un backup con chiave privata:

<#root>

```
copy running-config <BACKUP-CONFIG-URL>
```

Sostituire i segnaposto delle parentesi angolari con valori approvati specifici della periferica. Utilizzare un file system mostrato da show file system, ad esempio flash: o bootflash:.

2. Verifica percorsi di attendibilità

Rimuovi CA secondarie interessate direttamente attendibili

Rimuovere le CA secondarie direttamente attendibili interessate dai trust point e dai pacchetti di trust pool scaricati. Non utilizzare le impostazioni di revoca per eseguire l'override dell'attendibilità diretta in una CA compromessa.

Rimozione facoltativa della CA radice

La rimozione della CA radice è un'opzione consigliata per una protezione aggiuntiva. Una radice richiesta può rimanere attendibile quando i controlli OCSP/CRL del servizio effettivo ottengono lo stato corrente, valutano la SubCA interessata sotto un padre attendibile, rifiutano le catene più lunghe originali interessate, con firma incrociata e applicabili e non convalidano se nessuno dei metodi configurati fornisce lo stato utilizzabile. In queste condizioni verificate, la verifica delle revoche protegge dagli emittenti compromessi identificati senza eliminare la radice.

Prendere in considerazione la rimozione di root/trust anchor non necessari per ridurre la dipendenza dai servizi di revoca. Valutare prima le dipendenze del servizio: la rimozione di Servizi certificati AAA può interrompere catene legittime non correlate. Coprite entrambi i percorsi eMudhra e AAA. L'eliminazione di una sola SubCA memorizzata nella cache non blocca una copia fornita da un peer tramite un padre attendibile rimanente.

Rimuovere un trust point selezionato

Per un trust point configurato dall'amministratore selezionato per la rimozione:

<#root>

```
configure terminal no crypto pki trustpoint <TRUSTPOINT-NAME> end
```

Esaminare la conferma prima di accettarla. La rimozione del punto di trust comporta l'eliminazione dei certificati associati. Se è necessario sostituire l'identità di un dispositivo, ottenere un certificato sostitutivo corrispondente alla chiave dei dispositivi e aggiornare l'associazione al servizio utilizzando la procedura di registrazione del servizio. L'installazione di un solo certificato CA non sostituisce l'identità del dispositivo.

Per le voci del trustpool scaricate, utilizzare la procedura di sostituzione del bundle. Gli ancoraggi integrati o gestiti da funzionalità richiedono l'aggiornamento del prodotto supportato o le linee guida di Cisco TAC.

3. Aggiornare il pool di fiducia scaricato, se necessario

Attenersi alla seguente procedura quando un bundle scaricato richiede la sostituzione. Un elemento padre/radice richiesto può rimanere attendibile nelle condizioni di revoca verificate nel passaggio 2.

3.1 Verificare se un bundle scaricato è installato e utilizzato

<#root>

show running-config | section crypto pki certificate pool show crypto pki trustpool verbose show crypto

Cercare le voci del file CAB nel pool di certificati PKI crittografici e i record CA contrassegnati come Pool di fiducia: Scaricato. I nomi dei file dei bundle possono essere diversi da ios.p7b o ios_core.p7b. Un file archiviato o un URL di aggiornamento configurato da solo non dimostra che i relativi certificati sono installati o utilizzati da un servizio. Verificare che il servizio utilizzi il trustpool e confrontarne i record CA con l'inventario interessato. Se non sono installate CA scaricate, ignorare la pulizia e la sostituzione; valutare comunque altre fonti attendibili.

3.2 Pulire il trust pool scaricato

Mantieni l'accesso per il ripristino e un pacchetto di ripristino approvato disponibile prima della pulizia. Il download successivo potrebbe non riuscire se il trasferimento si basa sulla rimozione del trust. Pianificare l'interruzione dei servizi dipendenti.

<#root>

configure terminal crypto pki trustpool clean end

```
show crypto pki trustpool verbose
```

Confermare che i record CA scaricati non sono più disponibili. La pulizia rimuove tutti i certificati del trust pool scaricati e i relativi file del bundle gestito. rimangono CA incorporate e trust point separati. Non salvare fino a quando la sostituzione e i controlli del servizio non hanno esito positivo.

3.3 Ottenere e installare il bundle sostitutivo approvato

Ottieni un pacchetto approvato firmato da Cisco. Selezionare ios.p7b o ios_core.p7b per i servizi richiesti e confermare che esclude i certificati interessati e i trust anchor indesiderati identificati in precedenza. I bundle legacy controllati il 31 ottobre 2026 contengono la CA radice emSign - G1 in ios.p7b, ma né eMudhra né le CA di AAA Certificate Services in ios_core.p7b. Il set di trust del core è più piccolo: controllare le dipendenze del servizio prima di passare a un altro sistema e verificare il contenuto del bundle installato. Posizionarlo nell'area intermedia all'esterno dell'archivio del trust pool gestito utilizzando il trasferimento HTTPS o SCP approvato.

Pacchetto CA completo Cisco: ios.p7b

Pacchetto Cisco Core CA: ios_core.p7b

<#root>

```
show file systems copy <APPROVED-BUNDLE-SOURCE-URL> <STAGED-BUNDLE-URL> configure terminal crypto pki tr
```

Ad esempio, l'URL posizionato nell'area intermedia può essere flash:approved-ios.p7b. Se l'importazione non riesce, ripristinate un fascio approvato prima di salvare. Verificare le CA previste e le connessioni necessarie. La pulizia non è un elenco di certificati non validi: confermare i trust point rimanenti, le CA predefinite e i percorsi alternativi rifiutano le catene interessate tramite la revoca imposta o la rimozione del percorso di trust.

4. Configurare i criteri di convalida e aggiornamento

Prima di apportare modifiche, registrare il criterio del trust pool esistente, i criteri del trust point interessati, le associazioni di mapping dei certificati e gli URL di aggiornamento in modo che possano essere ripristinati se necessario.

Per i trust point configurati rilevanti:

<#root>

```
configure terminal crypto pki trustpoint <VALIDATION-TRUSTPOINT> revocation-check crl ocsp exit end
```

Per i servizi che utilizzano il criterio trustpool:

<#root>

```
configure terminal crypto pki trustpool policy chain-validation revocation-check crl ocsp exit end show
```

Verificare che la convalida del criterio del trust pool visualizzato continui per la radice ed elenchi l'ocsp della CRL. Il dispositivo tenta prima di eseguire l'OCSP quando il recupero CRL non è disponibile. Un risultato revocato non supera la convalida quando il certificato interessato viene valutato. Non aggiungere none quando è richiesta la verifica della revoca.

Verificare l'ora corretta, gli endpoint di stato CA pubblicati raggiungibili, i formati di risposta accettati e l'assenza di eccezioni applicabili di revoca e omissione. Lo stato delle CA secondarie interessate deve essere valutato in un padre attendibile. L'attendibilità diretta in tale SubCA può interrompere la convalida prima che il relativo padre sia selezionato. Verificare che il servizio effettivo ottenga lo stato corrente e utilizzabile e rifiuti le catene interessate. se non è possibile verificare il comportamento di accesso e rifiuto del server di stato, non considerare la configurazione come una protezione confermata; rimuovere i percorsi di attendibilità rilevanti se richiesto dal piano di attenuazione. Non aggiungere nessuno per ignorare lo stato non disponibile.

Aggiorna CRL nella cache prima di verificare la protezione

Un CRL utilizzabile già presente nella cache locale o nel database può essere riutilizzato anche dopo la pubblicazione da parte della CA di un CRL più recente. Verificare la raggiungibilità del server di stato, quindi cancellare i vecchi CRL prima di convalidare la protezione:

<#root>

```
show crypto pki crls clear crypto pki crl show crypto pki crls
```

Il comando clear rimuove i CRL locali per tutti i trust point; non scarica da sola le sostituzioni.

Verificare che le voci precedenti non siano più presenti, quindi avviare una nuova connessione o la convalida del certificato nel servizio interessato. Eseguire nuovamente show crypto pki crls e verificare ogni autorità emittente rilevante, LastUpdate, NextUpdate e punto di distribuzione rispetto alla pubblicazione corrente della CA. Includere il CRL autorità di certificazione padre che copre la SubCA interessata, non solo il CRL autorità di certificazione ID. Confermare che le catene interessate sono rifiutate. La cancellazione può influire temporaneamente sulle nuove connessioni durante il recupero dei dati di stato. mantenere la convalida di tipo fail-closed.

Esaminare l'origine aggiornamento bundle

Per i dispositivi connessi, è possibile configurare l'origine di aggiornamento del bundle approvato in scadenza:

<#root>

```
configure terminal crypto pki trustpool policy cabundle url <APPROVED-REFRESH-BUNDLE-URL> exit end show
```

Esaminare tutte le origini bundle configurate. L'aggiornamento basato sulla scadenza non sostituisce un aggiornamento immediato della protezione e non deve ripristinare un percorso di attendibilità indesiderato.

Filtro mappa certificati opzionale: copertura e limitazione

Una mappa dei certificati (cert-map) di Cisco IOS XE corrisponde agli attributi dei certificati, ad esempio il nome dell'autorità di certificazione. Come misura aggiuntiva, il filtro può aiutare a rifiutare i certificati di ID (foglia) rilasciati direttamente dalle otto CA elencate. Esaminare i criteri dei certificati di corrispondenza dei trust point esistenti prima di applicarli.

Il comportamento è stato testato il 29 ottobre 2026 utilizzando identità di laboratorio sotto EM DV TLS CA - G3B su dispositivi sperimentali di laboratorio. Nella convalida del certificato peer PKI, il filtro ha rifiutato un'identità rilasciata direttamente ma non ha bloccato un'identità rilasciata tramite una SubCA figlio aggiuntiva; è stata passata un'autorità emittente legittima non elencata. La copertura comportamentale ha utilizzato un'autorità emittente interessata, con la revoca disabilitata solo nei trust lab temporanei per isolare il filtro. Handshake di applicazioni e altre versioni non convalidati con questo filtro; verificare il servizio effettivo prima di affidarsi a esso.

<#root>

```
configure terminal crypto pki certificate map EMSIGN-ISSUER-FILTER 10 issuer-name nc cn=EM DV TLS CA - G
```

In questo caso, nc significa "non contiene". Mantieni tutte le otto condizioni negative per il nome dell'emittente nella stessa voce, sequenza 10: affinché il certificato superi questo filtro, è necessario che tutti i valori corrispondano. Un'autorità emittente diretta che corrisponde a un nome elencato non supera il filtro.

Cisco IOS XE può visualizzare voci normalizzate, ad esempio issuer-name nc cn = em dv tls ca - g3b. Questo formato minuscolo e spaziatura era presente nel test comportamentale. Confermare la mappa e la relativa associazione al trust point di convalida effettivamente utilizzato dal servizio:

<#root>

show running-config | section crypto pki certificate map show running-config | section crypto pki trustp

Il filtro non fornisce un denylist CA a livello di catena. Ad esempio:

```
Trusted root CA
  +-- Affected SubCA
       +-- New child SubCA
            +-- ID (leaf) certificate
```

L'autorità emittente dei certificati ID è la nuova SubCA figlio, pertanto il relativo filtro del nome dell'autorità emittente non identifica la CA interessata più in alto nella catena. Altri controlli, tra cui i vincoli CA e la revoca, sono ancora validi. Utilizzare questo filtro solo come protezione aggiuntiva insieme alle procedure di convalida delle revoche e di rimozione della radice facoltative in questa guida. Verificare i certificati rilasciati direttamente, figlio-SubCA e i certificati legittimi con il servizio effettivo.

Rollback del passaggio 4

Ripristinare i metodi di revoca registrati, le impostazioni di convalida della catena e le associazioni dei mapping dei certificati. Rimuovere gli URL di aggiornamento aggiunti da questa procedura e ripristinare eventuali URL precedenti modificati. In questo esempio vengono rimossi solo l'URL di aggiornamento e l'associazione di filtro aggiunti. non vengono ripristinate le altre impostazioni dei criteri:

<#root>

configure terminal crypto pki trustpool policy no cabundle url <ADDED-REFRESH-BUNDLE-URL> exit

```
crypto pki trustpoint <VALIDATION-TRUSTPOINT> no match certificate EMSIGN-ISSUER-FILTER exit end
```

Eseguire queste rimozioni solo se l'URL e il binding sono stati aggiunti da questa procedura. Se è stato sostituito un precedente binding della mappa certificati, ripristinarlo. Rimuovere una mappa appena creata solo dopo aver verificato che nessun'altra configurazione vi faccia riferimento.

Non utilizzare alcun criterio crypto pki trustpool solo quando il risultato approvato previsto è la reimpostazione ai valori predefiniti. Questa opzione di reimpostazione completa cancella gli URL di aggiornamento configurati e reimposta il controllo delle revoche su none (nessuno); non ripristina il criterio personalizzato precedente. Il rollback dei criteri non ripristina i certificati eliminati, ripristina il bundle installato o ripristina i CRL cancellati. Ricontrolla i servizi richiesti e il rifiuto della catena interessata prima di salvare.

5. Verifica protezione e salvataggio

- Confermare che le catene originali e con firma incrociata interessate vengano rifiutate, incluso un intermedio fornito da un peer. Se sono rilevanti catene più lunghe, verificare il rifiuto quando la CA interessata è più alta nella catena.
- Confermare che le connessioni legittime richieste funzionino ancora e che qualsiasi identità sostitutiva sia associata al servizio previsto.
- Controllare il comportamento quando i dati di revoca non sono disponibili. Le sessioni TLS/IPsec esistenti non vengono automaticamente riconvalidate da una modifica dei criteri; se necessario, utilizzare la procedura di riconnessione supportata dal servizio.

Dopo che i controlli hanno avuto esito positivo:

<#root>

```
show crypto pki certificates verbose show crypto pki trustpool policy write memory
```

Verificare la persistenza dopo il successivo caricamento pianificato e, se applicabile, sul dispositivo di standby. Se i risultati sono diversi dal criterio di attendibilità previsto, conservare i registri e contattare Cisco TAC prima di valutare le modifiche di attendibilità verificate.

Ulteriori letture

Gestione trust pool PKI Cisco IOS XE

Cisco: Configurazione dei certificati firmati dalla CA con PKI Cisco IOS XE

Cisco: Memorizzazione nella cache CRL e verifica delle revoche

Guida al trust tra CA Cisco IOS XE GuestShell

Passaggio 1: Stato distribuzione GuestShell del dispositivo di controllo

Il monitoraggio e l'aggiornamento sono richiesti solo sui sistemi Cisco IOS XE in cui è installato GuestShell e in stato RUNNING o DEPLOYED. Se GuestShell è nello stato DEPLOYED, deve essere abilitato con il comando 'guestshell enable' prima di eseguire i comandi di monitoraggio e aggiornamento. Se il comando show app-hosting list indica 'No App found' (GuestShell non è distribuito o abilitato), non è richiesta alcuna azione su GuestShell.

A. GuestShell nello stato DEPLOYED (Azione richiesta: Prima è necessario abilitare)

Quando show app-hosting list segnala GuestShell nello stato DEPLOYED, l'archivio del contenitore GuestShell esiste ma il contenitore è arrestato. È necessario eseguire 'guestshell enable' prima di immettere bash (e facoltativamente 'guestshell disable' dopo aver completato il monitoraggio e l'aggiornamento se si torna a uno stato di arresto):

<#root>

```
Router#

show app-hosting list

App id                                   State
------------------------------------------------------------
guestshell                               DEPLOYED
```

B. GuestShell in stato RUNNING (azione richiesta: Procedere Direttamente)

Quando il comando show app-hosting list segnala GuestShell nello stato RUNNING, GuestShell è in esecuzione e si può procedere direttamente a bash:

<#root>

```
Router#

show app-hosting list

App id                                   State
---------------------------------------------------------
guestshell                               RUNNING
```

B. GuestShell non abilitato / non distribuito (nessuna azione richiesta)

Se il comando show app-hosting list indica No App found, GuestShell non è installato o abilitato nel sistema e non sono necessarie ulteriori azioni:

<#root>

```
Router#

show app-hosting list

No App found
```

Passaggio 2: Accesso a GuestShell e applicazione dell'attendibilità CA

Eseguire questi comandi dal prompt di Cisco IOS XE in modalità di esecuzione privilegiata ('enable'). Se GuestShell è nello stato DEPLOYED, abilitarlo prima. Quindi, accedere alla shell Bash, passare alla directory principale e configurare l'elenco di blocco CA utilizzando la selezione dinamica delle cartelle per garantire la compatibilità tra tutte le versioni di Cisco IOS XE:

<#root>

```
! 1. If GuestShell is in DEPLOYED state, enable it first:
Router#

guestshell enable


! 2. Enter GuestShell bash shell:
Router#

guestshell run bash


! 3. Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s
```

```
! 4. Prepare the ca-trust blocklist directory (compatible with 17.15.x and 17.18.x):
d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist
mkdir -p "$d"
```

Diffidare dei certificati compromessi di Mudhra

Eseguire i comandi di estrazione trust per estrarre ogni certificato eMudhra compromesso direttamente nella directory ca-trust blocklist, quindi ricompilare l'archivio trust di sistema:

```
trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20G3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_G3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=Comodo%20AAA%20Services%20root;type=cert' \
  "$d/Comodo_AAA_Services_root.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-%20C3;type=cert' \
  "$d/emSign_ECC_Root_CA_-_C3.pem"

trust extract --overwrite --format=pem-bundle \
  --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;type=cert' \
  "$d/emSign_Root_CA_-_C1.pem"

update-ca-trust extract
```

Passaggio 3: Verifica dei certificati distrutti in GuestShell

Verificare che i quattro certificati estratti vengano visualizzati nel criterio Attendibilità sistema/Elenco indirizzi bloccati e che siano esclusi dai trust anchor attivi utilizzando il comando di verifica seguente. Il comando conferma che i certificati sono registrati nel criterio blocklist.

```
###Verify with below command
[guestshell@guestshell ~]$ trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign
    label: AAA Certificate Services
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: distrusted
    category: authority

--
    label: emSign ECC Root CA - G3
    trust: distrusted
    category: authority
```

```
--
    label: emSign Root CA - C1
    trust: distrusted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

Output will vary based on CentOS Stream version
###Verify CentOS Stream Version
[guestshell@guestshell ~]$ cat /etc/redhat-release
CentOS Stream release 8

OS                          CentOS Stream 8       CentOS Stream 9
Directory                   blacklist only        blocklist
Result shown                 trust: blacklisted    trust: distrusted
```

Passaggio 4: Continuità dello stato e ciclo di vita del contenitore

Nota sulla persistenza del contenitore: Le modifiche apportate alla sfiducia nei certificati persistono nelle operazioni 'guestshell enable' e 'guestshell disable' e nel riavvio del dispositivo perché /etc/pki/ca-trust risiede nell'archivio del contenitore persistente.

Ripristino dello stato DISTRIBUITO (se applicabile): Se in origine GuestShell era nello stato DEPLOYED e abilitato solo per eseguire questa procedura di sfiducia, ripristinare lo stato di arresto precedente di GuestShell uscendo da bash ed eseguendo 'guestshell disable' dal prompt di esecuzione privilegiato di IOS:

<#root>

```
[root@guestshell ~]#
```

exit

```
[guestshell@guestshell ~]$
```

exit

```
Router#
```

guestshell disable

Considerazioni importanti sul ciclo di vita: Se GuestShell viene completamente eliminato con 'guestshell delete', il file system del contenitore viene rimosso. Se GuestShell viene

successivamente riattivato, il contenitore viene ricreato dall'immagine del sistema di base e le operazioni di correzione della sfiducia devono essere riapplicate.

Passaggio 5: Procedura di rollback (ripristino dell'attendibilità CA)

Per invertire la configurazione della sfiducia e ripristinare l'attendibilità della CA predefinita in una qualsiasi versione di Cisco IOS XE, selezionare in modo dinamico la directory active blocklist ($d), rimuovere in modo specifico i quattro file di certificato aggiunti da questa procedura (inclusa la radice dei servizi Comodo AAA) e ricreare l'archivio di attendibilità:

<#root>

```
! Escalate to root user inside GuestShell:
[guestshell@guestshell ~]$

sudo -s


d=/etc/pki/ca-trust/source/blocklist
[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

! Remove only the four certificate files added during remediation:
rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \
      "$d/emSign_ECC_Root_CA_-_C3.pem" "$d/emSign_Root_CA_-_C1.pem"

! Rebuild the system CA trust store:
update-ca-trust extract
```

Verificare che la directory blocklist non contenga più i file rimossi:

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Conferma ripristino trust CA: Verificare che tutti e cinque i certificati siano tornati ai trust anchor attivi eseguendo nuovamente il comando di verifica del passaggio 3 (tutte le voci segnalano l'attendibilità: ancoraggio):

<#root>

```
[root@guestshell ~]#
```

```
trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
    trust: anchor
```

Esempio di trascrizione di esecuzione end-to-end

La trascrizione illustra una sessione completa e riuscita di controllo, correzione e verifica di GuestShell su un dispositivo Cisco IOS XE:

<#root>

```
Router#

guestshell run bash

[guestshell@guestshell ~]$ sudo -s
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

mkdir -p "$d"

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=Comodo%20AAA%20Services%20ro

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20ECC%20Root%20CA%20-

bash-4.4#

trust extract --overwrite --format=pem-bundle \ >   --filter='pkcs11:object=emSign%20Root%20CA%20-%20C1;
```

```
bash-4.4#

update-ca-trust extract

bash-4.4#

trust list --filter=trust-policy --purpose=server-auth | grep -E -A3 'emSign|AAA'

    label: emSign ECC Root CA - G3
    trust: blacklisted
    category: authority

--
    label: AAA Certificate Services
    trust: blacklisted
    category: authority

--
    label: emSign ECC Root CA - C3
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - C1
    trust: blacklisted
    category: authority

--
    label: emSign Root CA - G1
    trust: anchor
    category: authority

bash-4.4#

cat /etc/redhat-release

CentOS Stream release 8
bash-4.4#

d=/etc/pki/ca-trust/source/blocklist

bash-4.4#

[ -d "$d" ] || d=/etc/pki/ca-trust/source/blacklist

bash-4.4#

rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" \ >       "$d/emSign_ECC_Root_C

bash-4.4#
bash-4.4#

update-ca-trust extract

bash-4.4#
```

```
ls -l "$d"/

total 0
```

Matrice riepilogo comandi

Attività operativa	
Controlla stato GuestShell	`show app-hosting list`
Abilita GuestShell (se DISTRIBUITO)	`guestshell enable`
Immettere GuestShell Bash	`guestshell run bash`
Passa all'utente root	`sudo -s`
Prepara directory blocklist	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/source/blac`
Estrai CA in elenco indirizzi bloccati	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
Ricompila archivio	`update-ca-trust extract`

attendibilità CA	
Verifica criteri di attendibilità	`trust list --filter=trust-policy --purpose=server-auth`
Ripristina stato distribuito (facoltativo)	`guestshell disable`
Rollback/Ripristino attendibilità	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/emSign_`

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).