Guide de méfiance de Cisco IOS XE et GuestShell CA Trust eMudhra

Table des matières

Objectif

Ce document fournit des conseils pour Cisco IOS® XE pour la méfiance d'urgence des autorités de certification racine et intermédiaire eMudhra.

Utilisez ce guide pour auditer et gérer l'approbation d'autorité de certification pour les services dont la configuration autorise les hiérarchies affectées. L'applicabilité du produit et les corrections requises sont définies dans le document d'information Cisco. Vérifiez l'impact de la prise en charge des commandes et des services pour votre version de Cisco IOS XE avant de modifier la confiance.

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

Certificats CA eMudhra affectés : Original et contresigné

Inventaire vérifié le 29 octobre 2026. Huit clés CA d'émission eMudhra sont concernées : six pour TLS et deux pour la signature de code. Chaque clé apparaît dans un certificat CA original émis par emSign et dans un certificat CA signé de manière croisée Sectigo. L'inventaire contient donc 16 certificats : 12 certificats TLS et 4 certificats de signature de code.

Chaque paire originale/signée de manière croisée a le même objet et la même clé publique, mais un émetteur, un numéro de série et une empreinte de certificat SHA-256 différents. Les deux formulaires offrent d'autres voies de certification et doivent tous deux être inclus dans une vérification.

A. Émetteurs et stocks de certificats concernés

Émetteur A — Certificats TLS originaux : CN=emSign Root TLS CA - G3, O=eMudhra Technologies Limited, C=IN.

Émetteur B — Certificats originaux de signature de code : CN=emSign Root CS CA - G3, O=eMudhra Technologies Limited, C=IN.

Émetteur C — Tous les certificats cosignés : CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, ST=Greater Manchester, C=GB (Sectigo).

Sujets G3B : O = Mudhra BV, C = NL. Sujets G3C : O=eMudhra Inc, C=US. Chaque cellule variante répertorie sa référence d'émetteur, sa série hexadécimale et son empreinte SHA-256 (deux lignes). La marge intérieure des zéros de début ne modifie pas une valeur série.

Autorité de certification émettrice concernée (CN)	Certificat original Émetteur / série (hex) / SHA-256	Certificat de signature croisée Sectigo Émetteur / série (hex) / SHA-256
1. EM DV TLS CA - G3B TLS	Émetteur A A4AEE678F23362B4C0E460B772F214 42C4ACCD12C4F59597925E1A08A7A901 02608543809308D50EC427E118BA1493	Émetteur C A024FDF4BA665C785CE4A020483858B7 45A883F349AEDFD5F3A649B5498FFB12 1712BA8B448F3F2A91DBC5A766FCDDBE
2. EM OV TLS CA - G3B TLS	Émetteur A 6CADA367FB1C100088120EA202D568 98B896625C0C230ADEEC3EB2CF6AAD50 01ECF9156A68644E82374CE5833BC25B	Émetteur C E94223BDE92F914E5AB9ACABFDAC3710 5F1DED4DD590AF74631290CF073B122A 2AAC6A1FA479778A0BD43579BD832699
3. EM EV TLS CA - G3B TLS	Émetteur A C7C41EFE92D825F05EAE841A4A82C1 E7568FE6E12331F4FD7DE61DA4C7559D 0F8EB192A218D4741A3BA75184333838	Émetteur C D8F8685E4F2BD9D82402A85A1C1EB731 579480AEA166290BD3C643589E795FC0 D0E54E86505D180F1DFF99EFD3199512
4. EM DV TLS CA - G3C TLS	Émetteur A 588B2E3C2BB8CDA13E1A1209254321 0164D7CEAE5BB909C272AF151FF44B11 77AE9B47D9424B94F1D9558C30934D19	Émetteur C 91F347F1A5B7D39962B95E0EE4E299D1 62B7F9868263F72F6911FC78CEAF72C1 979158B7368BF648683BB2AA39B02E72

Autorité de certification émettrice concernée (CN)	Certificat original Émetteur / série (hex) / SHA-256	Certificat de signature croisée Sectigo Émetteur / série (hex) / SHA-256
5. EM OV TLS CA - G3C TLS	Émetteur A 296926C227A3A1526392B19482A504 CB6E15165AC802E9B3F993F16C25D41F 4E81C21EBDE71AE1B012AC00BF9C7C3F	Émetteur C 8D5A4811939EF447D77111CDD9849AE9 7485B51C0ED192878FA1D2F948FB529A E1842CC5086C4B67F7BE5B2039DE9489
6. EM EV TLS CA - G3C TLS	Émetteur A 8009928A64107601AF05FA2F19F109 432EC25F0D28DE9006D97BF752F17BBB 2CD41F669933FCB072D9A1148D0261F3	Émetteur C 05F078752DECE7A1B8595D303167171 FD9D5C2DBBD4995AB69B8D50C439D952 7B00529199C2FD01B2174EB58F07021F
7. EM OV CS CA - G3B Signature de code	Émetteur B 7818933F8F85B4619A2B35FBA83D0A 9E39DE2881273ACC225A149C72BA3E0F 51424963669AB633EE1DC7DF5DB067B4	Émetteur C 41E32B73AC185D6CE0D7480BACF84E6 A496E23AC0CAB8155FC9B117B97EAE36 8EFCBB9041AEC8804D5A308D2D01C2D8
8. EM OV CS CA - G3C Signature de code	Émetteur B 544B7F922C31AE220A4A922916F6E6 4B2460A466F95FD40113BCDCCA2CEB29 B3B093921DE45474DA7DF48874C630B1	Émetteur C D6A5EF613B390F32EF9CDF349F772841 84112972B8E59D14560AE7E711965447 4AAD119990CF3722BFC1E3B91615E1FD

B. Parcours de certification permettant de distinguer

Chemin TLS d'origine

```
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
```

Chemin de signature de code d'origine (CS racine approuvé directement)

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

Sectigo chemin à signature croisée (TLS et signature de code)

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

Un chemin TLS peut également se terminer au niveau de l'autorité de certification TLS racine emSign - G3 lorsque cette autorité de certification est approuvée directement. Les schémas montrent les relations pertinentes entre émetteurs ; le chemin accepté dépend des ancres de confiance et de la politique de validation du service consommateur.

Les autorités de certification parentes/racines illustrées dans l'exemple fournissent un contexte de chaîne et ne sont pas comptées parmi les huit clés d'émission compromises. La décision de supprimer ou de ne pas faire confiance à un parent/racine est distincte de l'identification d'une clé intermédiaire compromise.

Pour l'identification, utilisez l'émetteur du certificat et le numéro de série avec l'empreinte SHA-256. Un nom de sujet seul est insuffisant. Une empreinte de certificat identifie une variante de certificat ; un hachage SPKI SHA-256 identifie la clé publique partagée par ses formulaires d'origine et de signature croisée. La suppression d'un seul intermédiaire mis en cache n'empêche pas un homologue de le présenter via un chemin approuvé restant.

Sources et date de vérification

Les identificateurs de certificat ont été vérifiés par rapport aux pièces jointes à l'incident public le 29 octobre 2026. Chaque paire originale/croisée-signée contient la même clé publique. Utilisez les informations Cisco en direct pour l'applicabilité du produit et l'état de correction.

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

Enregistrement d'incident Mozilla : compromission de clé intermédiaire eMudhra (2083449)

Attachement du certificat CA d'origine (9664066)

Attachement de certificat CA à signature croisée AAA (9664067)

Pomme : Empreintes et chemins de certificat TLS d'origine et à signature croisée

Au 31 octobre 2026, l'autorité de certification racine emSign - G1 n'est pas identifiée parmi les autorités de certification compromises répertoriées dans ce guide. Sa confiance continue est soumise aux politiques de votre organisation et aux mises à jour de conseils ultérieures.

Gestion de la confiance des certificats par Cisco IOS XE

Les points de confiance PKI configurés contiennent des certificats CA/identité et une stratégie de validation. Le pool de confiance PKI contient des certificats d'autorité de certification intégrés et téléchargés pour les services qui l'utilisent. identifier la source et la politique de confiance utilisées par chaque service concerné ; la modification du pool de confiance ne remplace pas les points de confiance configurés séparément.

1. Audit et préparation

Vérifiez la version du logiciel, l'heure du périphérique et les certificats installés :

<#root>

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

Comparer l'émetteur du certificat complet et le numéro de série hexadécimal avec l'inventaire, en utilisant l'objet comme contexte de support. Lorsque Cisco IOS XE affiche uniquement les empreintes MD5 et SHA1, l'empreinte SHA-256 d'inventaire ne peut pas être comparée directement dans cette sortie ; il est fourni pour la vérification des fichiers de certificat à l'extérieur du périphérique. Les numéros de série de 100 premiers peuvent être différents. Les recherches par nom de fournisseur identifient uniquement les candidats. Enregistrez les services qui dépendent de chaque point de confiance et vérifiez les chemins d'origine et de signature croisée, y compris les intermédiaires de confiance directe.

Exemples: CA racine et SubCA affecté

Des exemples abrégés du certificat explicite sont affichés ; les autres champs sont omis. Comparez l'objet, l'émetteur et le numéro de série.

Exemple d’autorité de certification racine : Autorité de certification racine emSign ECC - 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>
```

Exemple SubCA affecté : certificat original délivré par 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>
```

Exemple SubCA affecté : Certificat de signature croisée 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>
```

Les deux formulaires SubCA ont le même objet, mais des émetteurs et des numéros de série différents. Associez l'émetteur et le numéro de série complets à l'inventaire ; le remplissage 00 de début peut être différent. Enregistrez les points de confiance associés pour localiser le point de confiance ou le pool propriétaire. La racine affichée est le contexte de la chaîne ; ce n'est pas l'une des huit clés d'émission compromises.

Conservez une méthode d'accès de récupération et un bundle de remplacement approuvé.

Utilisez la procédure de sauvegarde de certificat/clé approuvée si nécessaire. Sauvegarder la configuration ; cette copie seule n'est pas une sauvegarde à clé privée :

<#root>

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

Remplacer les espaces réservés des crochets d'angle par des valeurs approuvées spécifiques au périphérique. Utilisez un système de fichiers représenté par la commande show file systems, tel que flash: ou bootflash:.

2. Révision des chemins de confiance

Supprimer les sous-autorités de certification affectées directement approuvées

Supprimez les sous-autorités de certification directement approuvées des points de confiance et des bundles trustpool téléchargés. Ne comptez pas sur les paramètres de révocation pour remplacer l'approbation directe dans une autorité de certification compromise.

Suppression CA racine facultative

La suppression de l'autorité de certification racine est une recommandation facultative pour une protection supplémentaire. Une racine requise peut rester fiable lorsque les contrôles CRL/OCSP du service réel obtiennent l'état actuel, évaluent la sous-autorité de certification affectée sous un parent fiable, rejettent l'original affecté, les chaînes plus longues intersignées et applicables et échouent la validation si aucune des méthodes configurées ne fournit l'état utilisable. Dans ces conditions vérifiées, la vérification de révocation protège contre les émetteurs compromis identifiés sans supprimer la racine.

Envisagez de supprimer les ancrages racine/d'approbation inutiles pour réduire la dépendance aux services de révocation. Évaluez d'abord les dépendances de service : la suppression des services de certificats AAA peut interrompre les chaînes légitimes non liées. Couvrez les chemins eMudhra et AAA. La suppression d'une seule sous-autorité de certification mise en cache ne bloque pas une copie fournie par un homologue via un parent approuvé restant.

Supprimer un point de confiance sélectionné

Pour un point de confiance configuré par l'administrateur sélectionné pour suppression :

<#root>

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

Vérifiez la confirmation avant de l'accepter. La suppression du point de confiance détruit ses certificats associés. Si l'identité d'un périphérique doit être remplacée, obtenez un certificat de remplacement correspondant à la clé des périphériques et mettez à jour sa liaison de service à l'aide de la procédure d'inscription de service. L'installation d'un nouveau certificat d'autorité de certification ne remplace pas l'identité du périphérique.

Pour les entrées trustpool téléchargées, utilisez la procédure de remplacement de bundle. Les ancrages intégrés ou gérés par des fonctionnalités nécessitent la mise à jour du produit prise en charge ou les conseils du TAC Cisco.

3. Si nécessaire, mettez à jour le pool de confiance téléchargé

Suivez ces étapes lorsqu'un bundle téléchargé doit être remplacé. Un parent/racine requis peut rester approuvé dans les conditions de révocation vérifiées à l'étape 2.

3.1 Vérifier si un bundle téléchargé est installé et utilisé

<#root>

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

Recherchez les entrées de regroupement sous le pool de certificats crypto pki et les enregistrements CA marqués Trustpool : Téléchargé. Les noms de fichiers du bundle peuvent être différents de ios.p7b ou ios_core.p7b. Un fichier stocké ou une URL d'actualisation configurée seule ne prouve pas que ses certificats sont installés ou utilisés par un service. Confirmez que le service utilise le pool de confiance et comparez ses enregistrements d'autorité de certification à l'inventaire affecté. Si aucune autorité de certification téléchargée n'est installée, sautez le nettoyage et le remplacement ; évaluez toujours d'autres sources de confiance.

3.2 Nettoyage du groupe de confiance téléchargé

Conservez un accès de récupération et un ensemble de récupération approuvé disponibles avant le nettoyage. Le téléchargement ultérieur peut échouer si le transfert dépend de la suppression de l'approbation. Prévoyez l'interruption des services dépendants.

<#root>

```
configure terminal crypto pki trustpool clean end
```

```
show crypto pki trustpool verbose
```

Confirmez que les enregistrements AC téléchargés ont disparu. Le nettoyage supprime tous les certificats de pool de confiance téléchargés et leurs fichiers de bundle gérés ; les autorités de certification intégrées et les points de confiance distincts demeurent. N'enregistrez pas tant que les vérifications de remplacement et de service n'ont pas réussi.

3.3 Obtention et installation du bundle de remplacement approuvé

Obtenez un bundle approuvé signé par Cisco. Sélectionnez ios.p7b ou ios_core.p7b pour les services requis et vérifiez qu'il exclut les certificats affectés et les ancres d'approbation indésirables identifiés ci-dessus. Les bundles hérités vérifiés le 31 octobre 2026 contiennent l'autorité de certification racine emSign - G1 dans ios.p7b, mais pas les autorités de certification eMudhra ni AAA Certificate Services dans ios_core.p7b. Le coeur de réseau a un ensemble d'approbations plus petit : vérifiez les dépendances de service avant de procéder à la commutation et vérifiez le contenu du bundle que vous installez. Préparez-le en dehors du stockage géré trustpool à l'aide du transfert HTTPS ou SCP approuvé.

Offre groupée Cisco CA complète : ios.p7b

Offre groupée Cisco Core CA : ios_core.p7b

<#root>

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

Par exemple, l'URL intermédiaire peut être flash:Approved-ios.p7b. Si l'importation échoue, restaurez un lot approuvé avant d'enregistrer. Vérifiez les CA prévues et les connexions requises. Le nettoyage n'est pas une liste de refus de certificat : confirmer les points de confiance restants, les autorités de certification intégrées et les autres chemins rejettent les chaînes affectées par la révocation forcée ou la suppression du chemin de confiance.

4. Configurer la stratégie de validation et d'actualisation

Avant d'apporter des modifications, enregistrez la stratégie de pool de confiance existante, les stratégies de point de confiance affectées, les liaisons de mappage de certificat et les URL d'actualisation afin de pouvoir les restaurer si nécessaire.

Pour les points de confiance configurés appropriés :

<#root>

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

Pour les services utilisant la stratégie trustpool :

<#root>

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

Vérifiez que la stratégie trustpool affichée poursuit la validation vers la racine et répertorie les ocsp crl. Le périphérique tente d'abord CRL et tente OCSP lorsque la récupération CRL n'est pas disponible. La validation d'un résultat révoqué échoue lorsque le certificat affecté est évalué. N'ajoutez aucun lorsque la vérification de révocation est requise.

Vérifier l'heure correcte, les points de terminaison d'état publiés par l'autorité de certification accessibles, les formats de réponse acceptés et l'absence d'exceptions de révocation/saut applicables. L'état des SubCA affectés doit être évalué sous un parent de confiance. L'approbation directe dans cette sous-autorité de certification peut arrêter la validation avant que son parent soit vérifié. Vérifiez que le service réel obtient l'état utilisable et actuel et rejette les chaînes affectées. Si l'accès au serveur d'état et le comportement de rejet ne peuvent pas être vérifiés, ne traitez pas la configuration seule comme une protection confirmée ; supprimez les parcours de confiance appropriés lorsque votre plan d'atténuation l'exige. N'ajoutez aucun pour contourner l'état d'indisponibilité.

Actualiser les CRL mises en cache avant de vérifier la protection

Une liste de révocation de certificats utilisable déjà dans le cache/la base de données locale peut être réutilisée même après que l'autorité de certification a publié une nouvelle liste de révocation de certificats. Vérifiez l'accessibilité du serveur d'état, puis effacez les anciennes listes de révocation de certificats avant de valider la protection :

<#root>

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

La commande clear supprime les LCR locales pour tous les points de confiance ; il ne télécharge pas lui-même les remplacements. Vérifiez que les anciennes entrées ont disparu, puis lancez une nouvelle connexion ou une nouvelle validation de certificat dans le service affecté. Exécutez à nouveau show crypto pki crls et vérifiez chaque émetteur pertinent, LastUpdate, NextUpdate et point de distribution par rapport à la publication actuelle des CA. Incluez la liste de révocation de certificats des émetteurs parents qui couvre la sous-autorité de certification affectée, et pas seulement la liste de révocation de certificats des ID. Confirmez que les chaînes affectées sont rejetées. La suppression peut affecter temporairement les nouvelles connexions pendant l'extraction des données d'état ; conserver la validation de fermeture en cas d'échec.

Examiner la source d'actualisation du bundle

Pour les périphériques connectés, configurez éventuellement la source d'actualisation des bundles basée sur l'expiration approuvée :

<#root>

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

Vérifiez toutes les sources de bundle configurées. L'actualisation basée sur l'expiration ne remplace pas une mise à jour de sécurité immédiate et ne doit pas restaurer un chemin d'accès d'approbation indésirable.

Filtre certificate-map facultatif : couverture et limitation

Un mappage de certificat Cisco IOS XE (cert-map) correspond aux attributs de certificat, tels que le nom de l'émetteur. Comme mesure supplémentaire, le filtre peut aider à rejeter les certificats d'ID (leaf) émis directement par les huit autorités de certification répertoriées. Vérifiez la stratégie de certificat de correspondance existante des points de confiance avant de l'appliquer.

Le comportement a été testé le 29 octobre 2026 en utilisant des identités de laboratoire sous EM DV TLS CA - G3B sur des appareils de laboratoire expérimentaux. Dans la validation du certificat homologue PKI, le filtre a rejeté une identité émise directement mais n'a pas bloqué une identité

émise par une sous-autorité de certification enfant supplémentaire ; un émetteur légitime non coté a réussi. La couverture comportementale a utilisé un émetteur affecté, la révocation étant désactivée uniquement sur les points de confiance temporaires des travaux pratiques pour isoler le filtre. Les échanges d'application et les autres versions n'ont pas été validés avec ce filtre ; testez le service réel avant de vous y fier.

<#root>

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

Ici, nc signifie "ne contient pas". Conservez les huit conditions négatives du nom de l'émetteur dans la même entrée, séquence 10 : tous doivent correspondre pour que le certificat passe ce filtre. Un émetteur direct correspondant à n'importe quel nom répertorié ne parvient pas au filtre.

Cisco IOS XE peut afficher des entrées normalisées, par exemple issuer-name nc cn = em dv tls ca - g3b. Ce format minuscule et espacement était présent dans le test comportemental. Confirmez la carte et sa liaison au point de confiance de validation réellement utilisé par le service :

<#root>

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

Le filtre ne fournit pas de liste de déni d'autorité de certification à l'échelle de la chaîne. Exemple :

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

L'émetteur des certificats d'ID est le nouveau SubCA enfant, de sorte que son filtre de nom d'émetteur n'identifie pas l'autorité de certification affectée plus haut dans la chaîne. D'autres vérifications, y compris les contraintes et la révocation de l'AC, s'appliquent toujours. Utilisez ce filtre uniquement comme protection supplémentaire, en plus des procédures facultatives de validation de révocation et de suppression de racine de ce guide. Testez les certificats SubCA enfants directement émis et les certificats légitimes avec le service réel.

Restauration de l'étape 4

Restaurer les méthodes de révocation enregistrées, les paramètres de validation de chaîne et les liaisons de mappage de certificat. Supprimez les URL d'actualisation ajoutées par cette procédure et restaurez toutes les URL précédentes qui ont été modifiées. Cet exemple supprime uniquement l'URL d'actualisation et la liaison de filtre ajoutées ; il ne restaure pas les autres paramètres de stratégie :

<#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

Exécutez ces suppressions uniquement lorsque l'URL et la liaison ont été ajoutées par cette procédure. Si une liaison certificate-map précédente a été remplacée, restaurez-la. Supprimez un mappage nouvellement créé uniquement après avoir vérifié qu'aucune autre configuration ne le référence.

N'utilisez aucune stratégie de crypto pki trustpool uniquement lorsque la réinitialisation aux valeurs par défaut est le résultat prévu et approuvé. Cette réinitialisation complète efface les URL d'actualisation configurées et réinitialise la vérification de révocation à aucun ; il ne restaure pas la stratégie personnalisée précédente. La restauration de stratégie ne restaure pas les certificats supprimés, ne restaure pas le bundle installé ou ne restaure pas les listes de révocation de certificats effacées. Vérifiez à nouveau les services requis et le rejet de la chaîne concernée avant d'enregistrer.

5. Vérifiez la protection et enregistrez

- Confirmez que les chaînes d'origine et de signature croisée affectées sont rejetées, y compris un intermédiaire fourni par un homologue. Lorsque des chaînes plus longues sont pertinentes, vérifier le rejet lorsque l'AC touchée est plus élevée dans la chaîne.
- Vérifiez que les connexions légitimes requises fonctionnent toujours et que toute identité de remplacement est liée au service prévu.
- Vérifier le comportement lorsque les données de révocation ne sont pas disponibles. Les sessions TLS/IPsec existantes ne sont pas automatiquement revalidées par une modification de stratégie ; utilisez la procédure de reconnexion prise en charge par le service si nécessaire.

Une fois les vérifications réussies :

<#root>

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

Vérifiez la persistance après le prochain rechargement planifié et, le cas échéant, sur le périphérique de secours. Si les résultats diffèrent de la politique de confiance attendue, conservez les journaux et contactez le centre d'assistance technique Cisco avant d'examiner les modifications de confiance vérifiées.

Lectures complémentaires

Gestion du pool de confiance PKI Cisco IOS XE

Cisco : Configuration des certificats signés CA avec Cisco IOS XE PKI

Cisco : Mise en cache et vérification de révocation CRL

Guide d'approbation CA GuestShell Cisco IOS XE

Étape 1: Audit de l'état de déploiement GuestShell du périphérique

La correction n'est requise que sur les systèmes Cisco IOS XE sur lesquels GuestShell est installé et à l'état EN COURS d'EXÉCUTION ou DÉPLOYÉ. Si GuestShell est à l'état DEPLOYED, il doit d'abord être activé à l'aide de la commande « guestshell enable » avant d'exécuter des commandes de conversion. Si show app-hosting list indique « No App found » (GuestShell n'est pas déployé ou activé), aucune action n'est requise sur GuestShell.

A. GuestShell à l'état DEPLOYED (Action requise : Doit d'abord être activé)

Lorsque la commande show app-hosting list signale GuestShell à l'état DEPLOYED, le stockage du conteneur GuestShell existe mais le conteneur est arrêté. Vous devez exécuter « guestshell enable » avant d'entrer bash (et éventuellement « guestshell disable » après avoir terminé la correction si vous revenez à un état arrêté) :

<#root>

```
Router#

show app-hosting list

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

B. GuestShell en état d'exécution (action requise : Continuer directement)

Lorsque la commande show app-hosting list signale GuestShell à l'état RUNNING, GuestShell est en cours d'exécution et vous pouvez passer directement à bash :

<#root>

```
Router#

show app-hosting list

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

B. GuestShell non activé/non déployé (aucune action requise)

Si show app-hosting list indique No App found, GuestShell n'est pas installé ou activé sur le système et aucune action supplémentaire n'est requise :

<#root>

```
Router#

show app-hosting list

No App found
```

Étape 2: Accès à GuestShell et application de la méfiance CA

Exécutez ces commandes à partir de l'invite du mode d'exécution privilégié (« enable ») de Cisco IOS XE. Si GuestShell est à l'état DEPLOYED, activez-le d'abord. Ensuite, entrez le shell bash, transférez-le à la racine et configurez la liste de blocage CA en utilisant la sélection dynamique de dossiers pour assurer la compatibilité entre toutes les versions de 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"
```

Certificats eMudhra compromis douteux

Exécutez les commandes d'extraction de confiance pour extraire chaque certificat eMudhra compromis directement dans le répertoire de la liste de blocage ca-trust, puis reconstruisez le magasin de confiance du système :

```
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
```

Étape 3: Vérification des certificats non approuvés dans GuestShell

Vérifiez que les quatre certificats extraits apparaissent dans la stratégie de méfiance/liste de blocage du système et sont exclus des ancres d'approbation actives à l'aide de la commande de vérification ci-dessous. La commande confirme que les certificats sont enregistrés dans la stratégie de liste de blocage.

```
###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
```

Étape 4: Persistance d'état et cycle de vie du conteneur

Remarque sur la persistance du conteneur : Ces modifications de certificat de non-confiance persistent dans les opérations « guestshell enable » et « guestshell disable » et les redémarrages du périphérique, car /etc/pki/ca-trust réside sur le stockage de conteneur persistant.

Retour à l'état DÉPLOYÉ (le cas échéant) : Si GuestShell était à l'origine à l'état DEPLOYED et activé uniquement pour exécuter cette procédure de méfiance, revenez à l'état arrêté précédent en quittant bash et en exécutant « guestshell disable » à partir de l'invite du mode d'exécution privilégié IOS :

<#root>

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

exit

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

exit

```
Router#
```

guestshell disable

Considérations importantes sur le cycle de vie : Si GuestShell est complètement détruit avec « guestshell destroy », le système de fichiers conteneur est supprimé. Si GuestShell est réactivé par la suite, le conteneur est recréé à partir de l'image du système de base et ces étapes de résolution de méfiance doivent être réappliquées.

Étape 5: Procédure de restauration (restauration de la confiance CA)

Pour inverser la configuration de la méfiance et restaurer la confiance de l'autorité de certification par défaut sur n'importe quelle version de Cisco IOS XE, sélectionnez dynamiquement le répertoire de la liste de blocage active ($d), supprimez spécifiquement les quatre fichiers de certificat ajoutés par cette procédure (y compris la racine des services Comodo AAA), et reconstruisez le magasin de confiance :

<#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
```

Vérifiez que le répertoire de la liste de blocage ne contient plus les fichiers supprimés :

<#root>

```
[root@guestshell ~]#

ls -l "$d"/

total 0
```

Confirmer la restauration de la confiance CA : Vérifiez que les cinq certificats sont revenus aux ancres d'approbation actives en réexécutant la commande de vérification de l'étape 3 (toutes les entrées signalent une approbation : ancre) :

<#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
```

Exemple de transcription d'exécution de bout en bout

La transcription illustre une session d'audit, de correction et de vérification GuestShell complète et réussie sur un périphérique 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 Récapitulatif des commandes

Tâche Opérationnelle	
Audit de l'état GuestShell	`show app-hosting list`
Activer GuestShell (si DÉPLOYÉ)	`guestshell enable`
Entrez GuestShell Bash	`guestshell run bash`
Basculer vers l'utilisateur racine	`sudo -s`
Préparer le répertoire Blocklist	`d=/etc/pki/ca-trust/source/blocklist; [ -d "$d" ] || d=/etc/pki/ca-trust/sourc`

Extraire les AC vers la liste de blocage	`trust extract --overwrite --format=pem-bundle ... (x4 CAs)`
Reconstruire le magasin CA Trust	`update-ca-trust extract`
Vérifier la stratégie de méfiance	`trust list --filter=trust-policy --purpose=server-auth`
Restaurer l'état DÉPLOYÉ (facultatif)	`guestshell disable`
Restauration/restauration de la confiance	`rm -f "$d/emSign_ECC_Root_CA_-_G3.pem" "$d/Comodo_AAA_Services_root.pem" "$d/e`

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.