Vérification et dépannage des certificats TLS sur Cisco ESA

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Présentation fonctionnelle et exigences
- Configurer et attribuer un certificat
- Vérifier
  - Vérification de TLS pour HTTPS
  - Vérifier TLS pour la remise ou la réception des e-mails
    - Exemple de réussite TLS lors de la réception de messages
    - Exemple d'échec TLS lors de la réception du courrier
    - Exemple de réussite TLS lors de la remise du courrier
    - Exemple d'échec TLS lors de la remise du courrier
  - Vérifier TLS pour LDAP
- Dépannage
  - Vérifier les certificats intermédiaires
  - Activer les notifications pour les échecs de connexion TLS requis
  - Dépannage à l'aide d'outils tiers
  - Résolution
- Informations connexes

Introduction

Ce document décrit comment créer, configurer et dépanner des certificats TLS sur le dispositif de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'implémentation TLS sur l'ESA assure la confidentialité de la transmission point à point des e-mails via le cryptage. Cette implémentation permet à un administrateur d'importer un certificat et une clé privée à partir d'un service d'autorité de certification (CA) ou d'utiliser un certificat auto-signé.

Cisco AsyncOS for Email Security prend en charge l'extension STARTTLS vers SMTP (Simple Mail Transfer Protocol) (Secure SMTP over TLS).



Remarque : Ce document décrit comment installer des certificats au niveau du cluster avec l'utilisation de la fonctionnalité de gestion centralisée sur l'ESA. Les certificats peuvent être appliqués au niveau de la machine ; toutefois, si la machine est supprimée du cluster, puis rajoutée, les certificats de niveau machine sont perdus.

Présentation fonctionnelle et exigences

Un administrateur peut utiliser un certificat sur l'appliance pour l'une des raisons suivantes :

- Chiffrer les conversations SMTP avec d'autres MTA qui utilisent TLS (les conversations entrantes et sortantes).
- Pour activer le service HTTPS sur l'appliance afin d'accéder à l'interface utilisateur graphique via HTTPS.
- À utiliser comme certificat client pour les protocoles LDAP (Lightweight Directory Access Protocol), si le serveur LDAP requiert un certificat client.
- Permettre une communication sécurisée entre l'appliance et une appliance Cisco Advanced Malware Protection (AMP) Threat Grid.

L'ESA est livré préconfiguré avec un certificat de démonstration qui peut être utilisé pour établir des connexions TLS.

⚠ Mise en garde : Bien que le certificat de démonstration soit suffisant pour établir une connexion TLS sécurisée, sachez qu'il ne peut pas offrir une connexion vérifiable. Cisco vous recommande d'obtenir un certificat X.509 ou PEM (Privacy Enhanced Email) auprès d'une autorité de certification.

Configurer et attribuer un certificat

Avant de continuer, assurez-vous d'avoir effectué les étapes de création et d'attribution d'un certificat, comme indiqué dans le Guide de l'utilisateur. Ces liens fournissent les instructions nécessaires :

- Déploiement d'un certificat signé
- Attribuer un certificat

Vérifier

Vérification de TLS pour HTTPS

1. Accédez à l'interface utilisateur graphique : accédez à votre périphérique ESA à l'aide de l'URL HTTPS (par exemple, https://esa.example.com).

2. Ouvrir les détails du certificat : cliquez sur l'icône Informations sur le site (généralement un cadenas) située à gauche de l'URL dans la barre d'adresse du navigateur.

3. Validez en fonction de votre navigateur :

a. Google Chrome : Cliquez sur l'icôneCadenas>La connexion est sécurisée>Le certificat est valide.

b. Microsoft Edge : cliquez sur l'icône Cadenas>Connexion sécurisée>Icône Certificat (en haut à droite du menu volant).

c. Mozilla Firefox : Cliquez sur l'icôneCadenas>Connexion sécurisée>Plus d'informations>Afficher le certificat.

4. Confirmer la validité : vérifiez la « Période de validité » ou le « Statut » dans la visionneuse de

certificats. Si le certificat indique asValid, la connexion est sécurisée et le certificat est correctement reconnu par le navigateur.

Vérifier TLS pour la remise ou la réception des e-mails

Bien que le suivi des messages dans l'interface utilisateur graphique fournisse ces informations, l'utilisation de l'interface de ligne de commande (CLI) est souvent plus efficace pour une révision en bloc ou un dépannage rapide.

Passez en revue ces étapes pour vérifier l'état TLS via l'interface de ligne de commande :

1. Connexion à l'interface de ligne de commande : accédez à l'appliance via SSH en utilisant vos informations d'identification d'administration.
2. Exécutez la commande Grep : utilisez l'utilitaire greputility pour filtrer les journaux de messagerie pour l'activité liée à TLS.
3. Analyser les ID de connexion : vérifiez le résultat en fonction du type de connexion :
    - ICID (Incoming Connection ID) : vérifiez ces entrées pour vérifier le TLS des connexions reçues sur l'écouteur.
    - DCID (Delivery Connection ID) : vérifiez ces entrées pour vous assurer que les connexions TLS sont transmises au MTA du tronçon suivant.



Remarque : Vous pouvez rechercher des chaînes spécifiques telles que « TLS success » ou « TLS failed » pour affiner les résultats.

Exemple de réussite TLS lors de la réception de messages

<#root>

```
(Machine esa.example.com)>

grep "ICID.*TLS success" mail_logs


Sat Feb 14 19:14:38 2026 Info: ICID 111395123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-
Sat Feb 14 19:14:41 2026 Info: ICID 111395456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA38
```

Exemple d'échec TLS lors de la réception du courrier

<#root>

```
(Machine esa.example.com)>

grep "ICID.*TLS failed" mail_logs


Sat Feb 14 19:20:28 2026 Info: ICID 111396123 TLS failed: [Errno 0] Error
Sat Feb 14 19:20:28 2026 Info: ICID 111396456 TLS failed: ('SSL routines:tls_early_post_process_client_
```

Exemple de réussite TLS lors de la remise du courrier

<#root>

```
(Machine esa.example.com)>

grep "DCID.*TLS success" mail_logs


Sat Feb 14 19:12:56 2026 Info: DCID 21966123 TLS success protocol TLSv1.2 cipher ECDHE-RSA-AES256-GCM-S
Sat Feb 14 19:13:00 2026 Info: DCID 21966456 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

Exemple d'échec TLS lors de la remise du courrier

<#root>

```
(Machine esa.example.com)>

grep "DCID.*TLS failed" mail_logs


Sat Feb 14 19:58:43 2026 Info: DCID 21967123 TLS failed: TLS required, STARTTLS unavailable, destinatio
Sat Feb 14 20:58:44 2026 Info: DCID 21967456 TLS failed: TLS required, STARTTLS unavailable, destinatio
```

Vérifier TLS pour LDAP

Bien que les journaux ldap_debug n'affichent pas de chaîne TLS spécifique, vous pouvez déterminer si TLS a réussi ou échoué en examinant la réponse LDAP et le ou les ports utilisés. Pour les connexions LDAP, cela signifie généralement le port 3269 pour Active Directory ou le

port 636 pour OpenLDAP.

Exemple TLS pour LDAP

<#root>

```
(Machine esa.example.com) (SERVICE)>
```

tail ldap_debug

```
Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) to server LDA
```

:3269

```
)
Wed Feb 25 03:24:23 2026 Debug: LDAP: (group) Query (proxyAddresses=smtp:user@example.com) lookup succe
```

:3269

```
) returned 0 results timestamp=1771989863.189580
```



Remarque : Pour une analyse plus détaillée du trafic LDAP et de l'activité TLS, Cisco recommande de capturer les paquets réseau sur les hôtes et les ports appropriés.

Dépannage

Cette section décrit comment dépanner les problèmes TLS de base sur l'ESA.

Vérifier les certificats intermédiaires

Recherchez des certificats intermédiaires en double lorsque les certificats actuels sont mis à jour au lieu d'une nouvelle création de certificat. Les certificats intermédiaires peuvent être modifiés ou chaînés de manière incorrecte, et le certificat peut télécharger plusieurs certificats intermédiaires. Cela peut entraîner des problèmes de chaînage et de vérification des certificats.

Activer les notifications pour les échecs de connexion TLS requis

Vous pouvez configurer l'ESA pour qu'il envoie une alerte si la négociation TLS échoue lorsque des messages sont remis à un domaine qui nécessite une connexion TLS. Le message d'alerte contient le nom du domaine de destination pour la négociation TLS ayant échoué. L'ESA envoie le message d'alerte à tous les destinataires configurés pour recevoir des alertes de niveau de gravité d'avertissement pour les types d'alerte système.



Remarque : Il s'agit d'un paramètre global qui ne peut donc pas être défini par domaine.

Suivez ces étapes pour activer les alertes de connexion TLS :

1. Accédez à Politiques de messagerie > Contrôles de destination.
2. Cliquez sur Modifier les paramètres globaux.
3. Cochez la case Envoyer une alerte en cas d'échec d'une connexion TLS requise.



Conseil : Vous pouvez également configurer ce paramètre avec la commande destconfig > setup CLI.

L'ESA enregistre également les instances pour lesquelles TLS est requis pour un domaine, mais n'a pas pu être utilisé dans l'appliance mail_logs. Cela se produit lorsque l'une de ces conditions est remplie :

- Le MTA distant ne prend pas en charge ESMTP (par exemple, il ne comprenait pas la commande EHLO de l'ESA).
- Le MTA distant prend en charge ESMTP, mais la commande STARTTLS ne figurait pas dans la liste des extensions annoncées dans la réponse EHLO.
- Le MTA distant a annoncé l'extension STARTTLS, mais a répondu avec une erreur lorsque l'ESA a envoyé la commande STARTTLS.

Dépannage à l'aide d'outils tiers

- Assurez-vous que le certificat est appliqué au niveau de l'écouteur où l'appliance reçoit le courrier entrant avant de commencer le test.

Des outils tiers tels que CheckTLS.com et SSL-Tools.net peuvent être utilisés pour vérifier le chaînage approprié du certificat lors de la réception. Consultez la documentation de chaque outil pour comprendre comment valider le certificat.

Remarque : Si un certificat auto-signé est utilisé, un échec est attendu.

Résolution

Si un certificat signé par une autorité de certification est en cours d'utilisation et que TLS-verify échoue, vérifiez que ces éléments correspondent :

- Nom commun du certificat
- Nom d'hôte (dans GUI > Réseau > Interface)
- Nom d'hôte d'enregistrement MX : il s'agit de la colonne Serveur MX de la table TestReceiver

Informations connexes

- Appliance de sécurisation de la messagerie Cisco - Guides de l'utilisateur final

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.