Dépannage de l'échec de mise à jour des définitions TETRA avec erreur 3000

Table des matières

Introduction

Ce document décrit les étapes pour dépanner l'échec des définitions TETRA avec l'erreur 3000.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Terminaux sécurisés Cisco

Composants utilisés

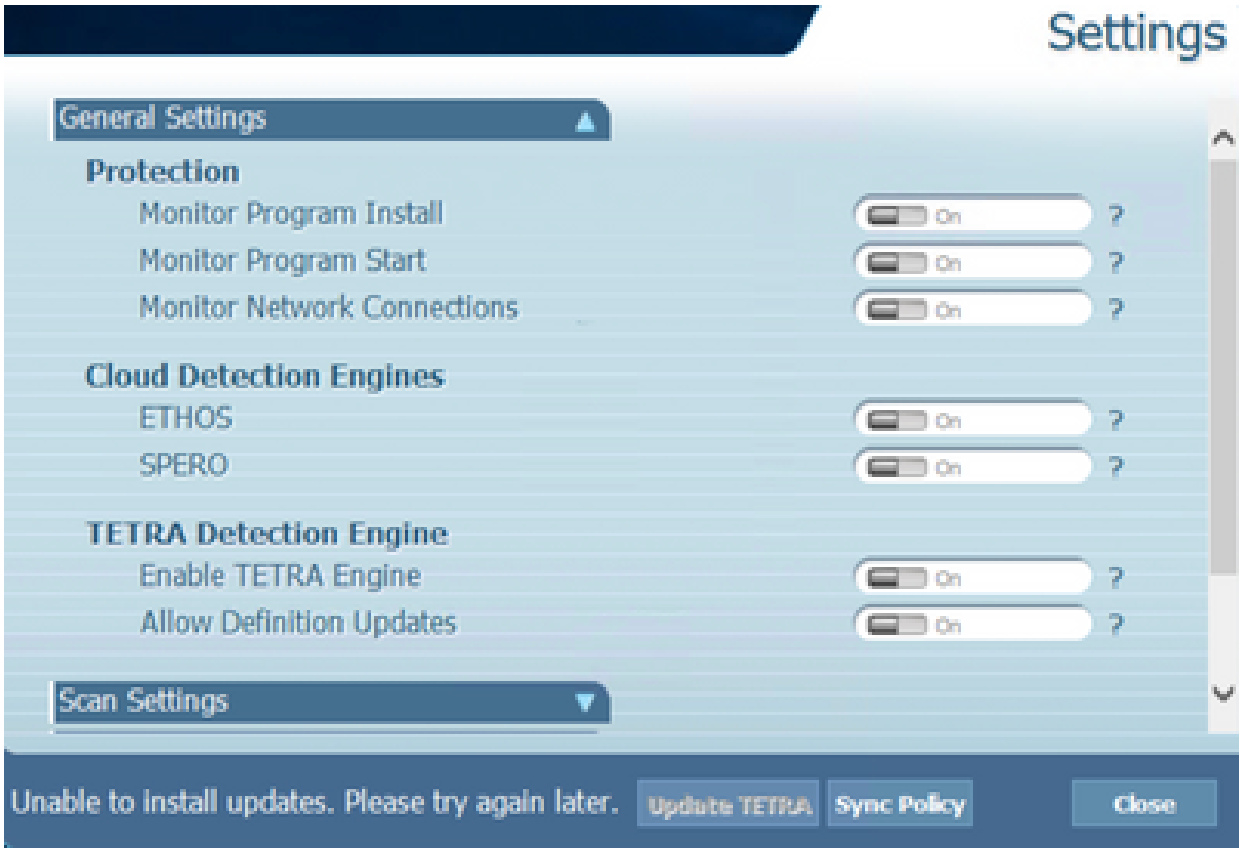
Les informations contenues dans ce document sont basées sur :

- Connecteur Cisco Secure Endpoint (toute version)
- Wireshark (toute version)

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.

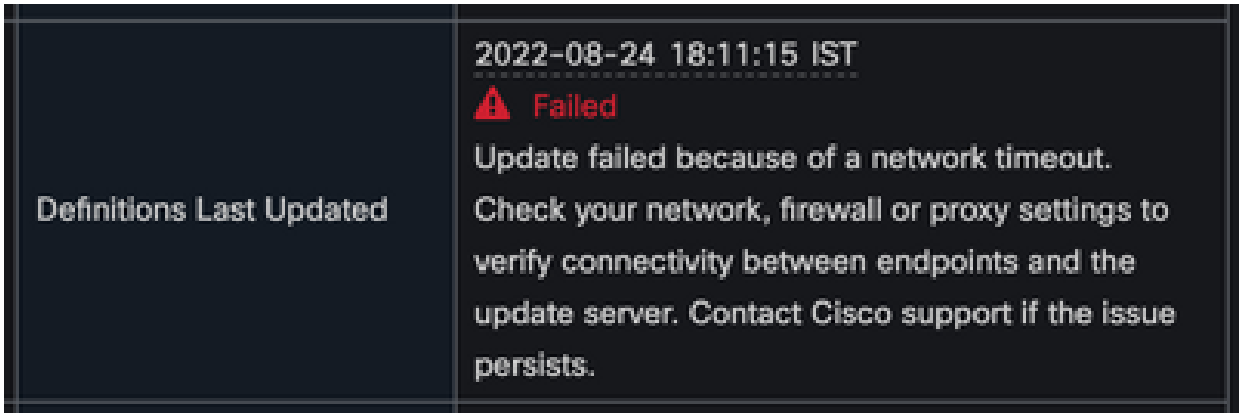
Problème

1. Sur le terminal, la mise à jour des définitions TETRA échoue avec le message d'erreur « Impossible d'installer les mises à jour. Veuillez réessayer ultérieurement ».



2. Sur Cisco Secure Endpoint Console, l'erreur d'échec mentionnée est observée :

   "La mise à jour a échoué en raison d'un délai réseau. Vérifiez les paramètres de votre réseau, de votre pare-feu ou de votre proxy pour vérifier la connectivité entre les terminaux et le serveur de mise à jour. Contactez l'assistance Cisco si le problème persiste. »



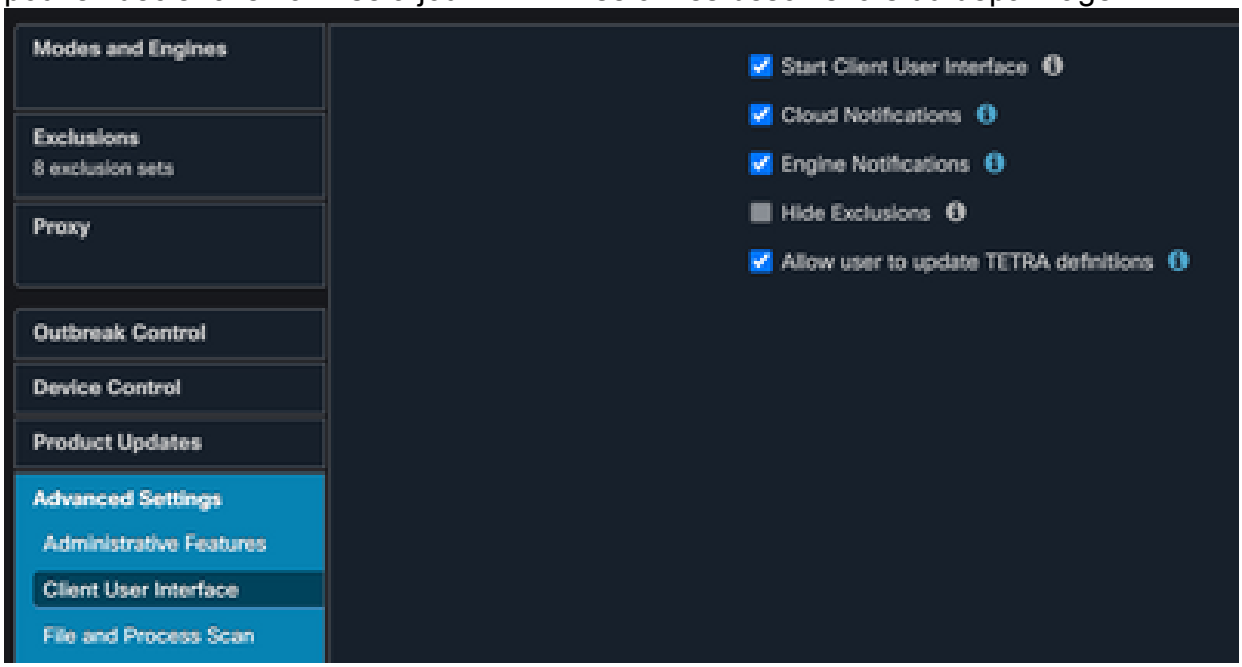
3. Dans debug sfc.exe.log, les définitions mises à jour ont échoué avec l'erreur 3000 error is observected, qui signifie Unknown_Error comme documenté.
   <#root>

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdateInterface::update updateDir: C:\Progr
(978223515, +0 ms) Aug 04 07:30:23 [11944]: ERROR: TETRAUpdateInterface::update

Update failed with error -3000


(978223515, +0 ms) Aug 04 07:30:23 [11944]: PipeSend: sending message to user interface: 26,
(978223515, +0 ms) Aug 04 07:30:23 [860]: PipeWrite: waiting on pipe event handle
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit defInit: 0, bUpdate: 0
```

```
(978223515, +0 ms) Aug 04 07:30:23 [11944]: TETRAUpdaterInit bUpdate: 0, bReload: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: FASharedPtr<class TETRAUpdateInterface>::Release
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: bUpdated = FALSE, state: 20,
(978223515, +0 ms) Aug 04 07:30:23 [11944]: PerformTETRAUpdate: sig count: 0, version: 0
(978223515, +0 ms) Aug 04 07:30:23 [11944]: Config::IsUploadEventEnabled: returns 1, 1
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
(978223515, +0 ms) Aug 04 07:30:23 [11944]: AVStat::CopyInternal : engine - 2, defs - 0, fir
```

Solution

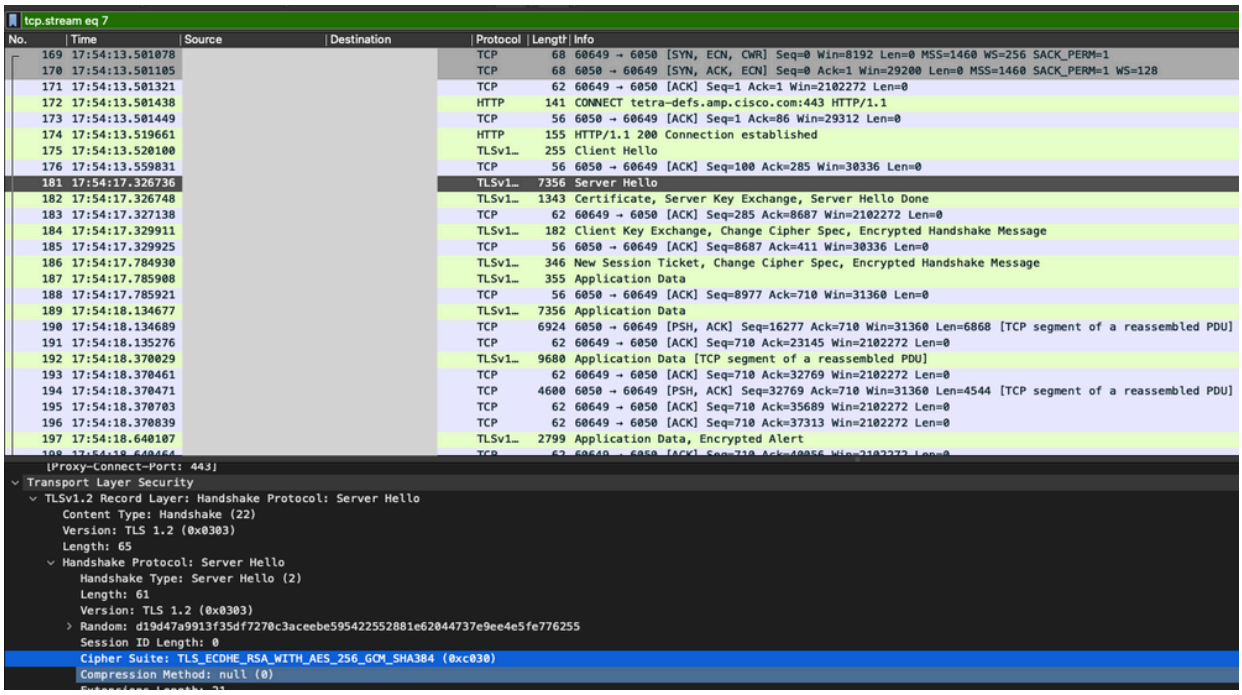
1. Activez l'option Autoriser l'utilisateur à mettre à jour les définitions TETRA dans Stratégie AMP > Interface utilisateur client sur la console. Avec ce paramètre, vous pouvez déclencher la mise à jour TETRA selon les besoins lors du dépannage.



2. Activez également la commande debug Connector et Tray-level log sur le terminal ou via AMP Policy.

3. Effectuez des captures de paquets sur le point de terminaison de la mise à jour TETRA réussie et échouée pour les définitions TETRA pendant que vous cliquez sur Mettre à jour TETRA sur le point de terminaison.

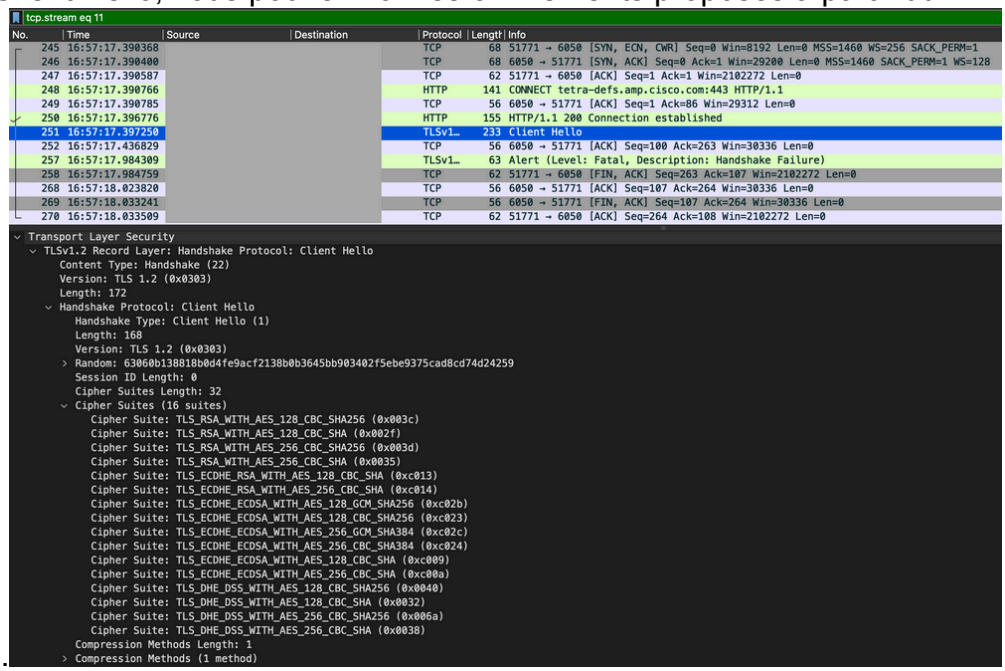
4. Sur le terminal de mise à jour TETRA réussie, dans la capture de paquets, filtrez les paquets avec http.host == "tetra-defs.amp.cisco.com:443" et ensuite "suivez le tcp.stream" de chaque paquet pour analyser le trafic associé.
5. Dans le paquet Server Hello, vous pouvez voir que le serveur accepte le chiffrement "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384" dans le paquet Server Hello.



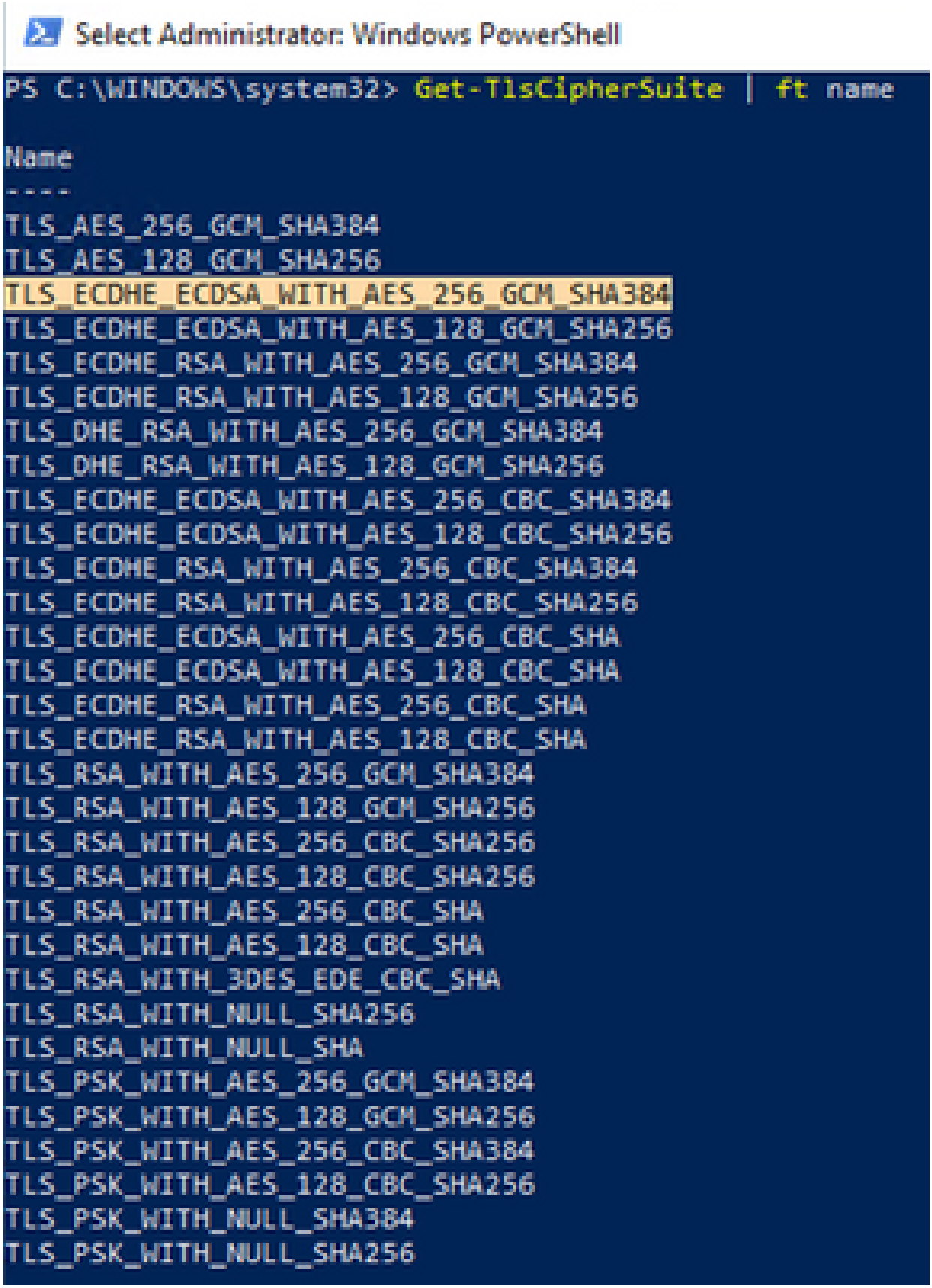
6. Le serveur Cisco Secure Endpoint TETRA accepte uniquement les chiffrements mentionnés :

```
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_AES_128_GCM_SHA256
```

7. Sur le point d'extrémité en échec de la mise à jour TETRA, dans la capture de paquets, une erreur fatale dans la connexion SSL est observée après le paquet Hello du client.
8. Dans le paquet Client Hello, vous pouvez voir les chiffrements proposés à partir du point d'extrémité.

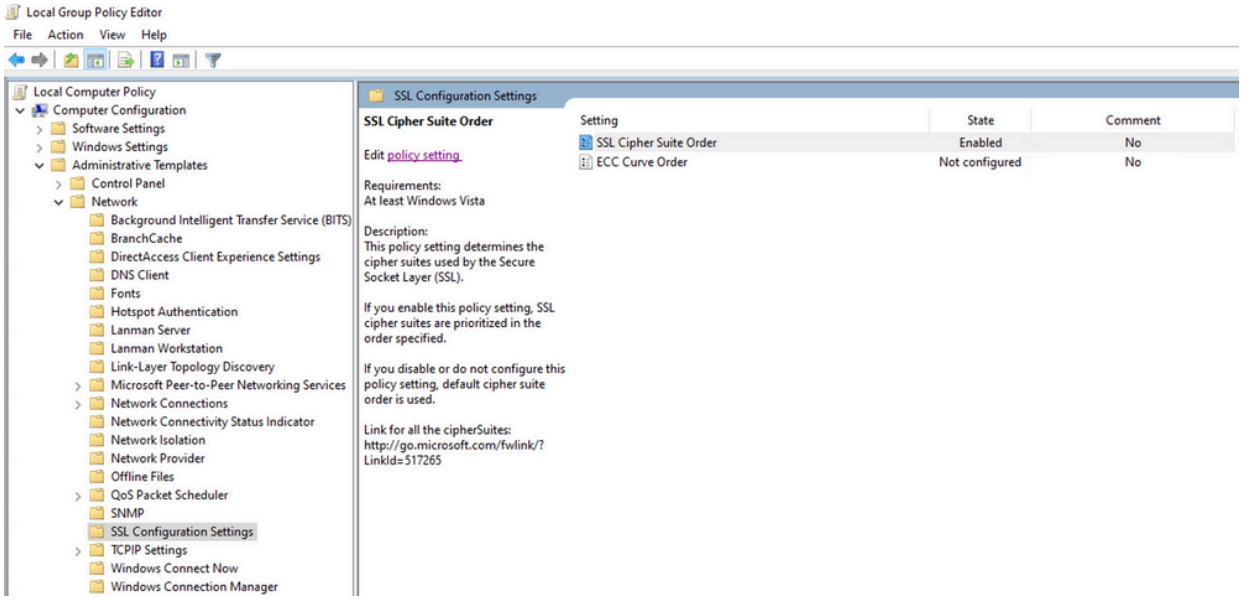


9. En outre, vous pouvez effectuer une vérification croisée des chiffrements activés sur le terminal avec la Get-TlsCipherSuite | ft name Commande PowerShell.

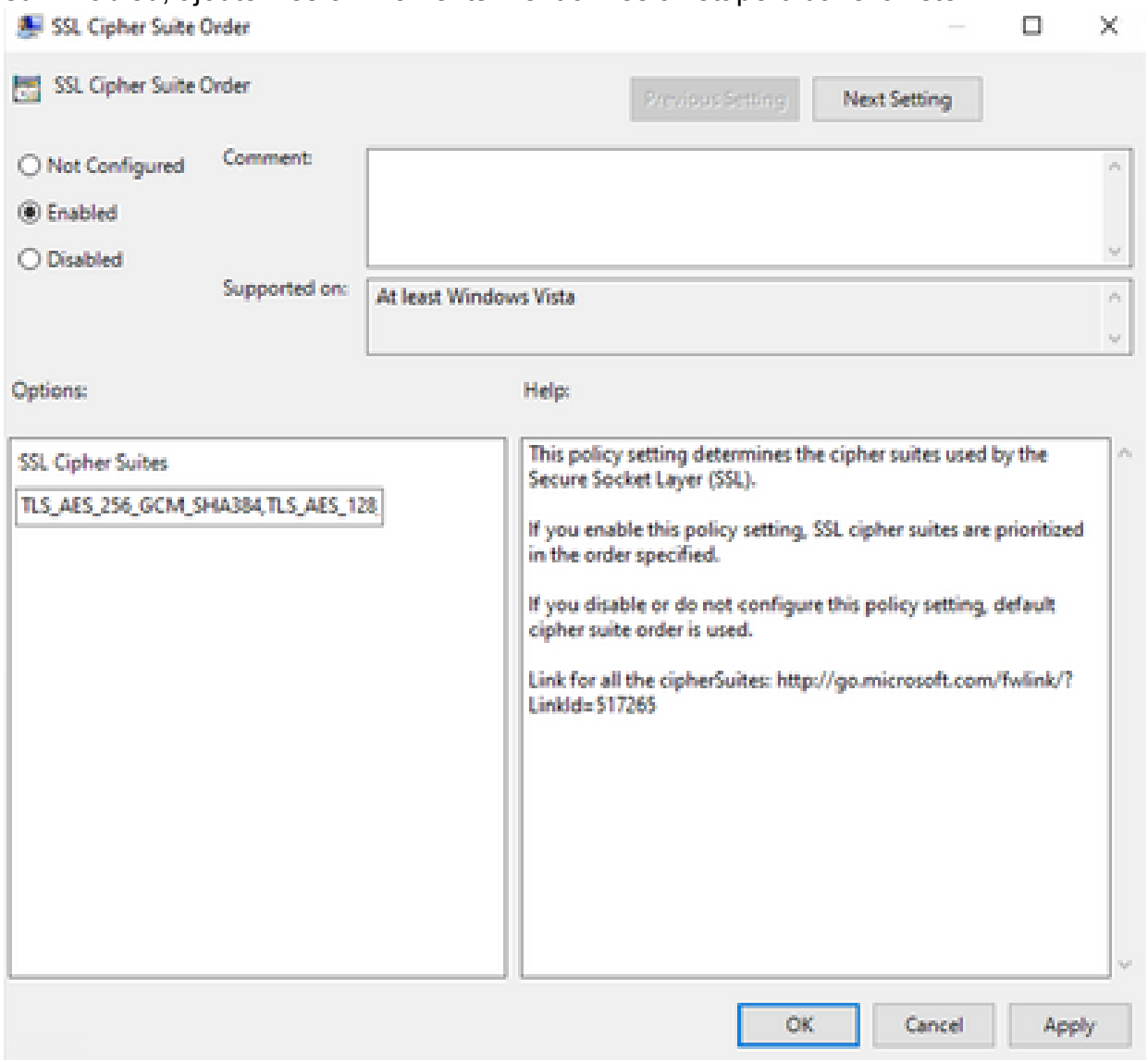


10. Si les chiffrements mentionnés à l'étape 6 ne sont pas répertoriés ici, c'est la raison de l'échec de la connexion SSL.
11. Pour résoudre ce problème, vérifiez l'ordre de la suite de chiffrement SSL dans la stratégie de groupe :

```
Run -> gpedit.msc -> Local Computer Policy -> Computer Configuration -> Administrative Templ
```



12. L'ordre de la suite de chiffrement doit être Not Configured ou Disabled et, s'il est défini sur Enabled, ajoutez les chiffrements mentionnés à l'étape 6 dans la liste.



13. Appliquez ces modifications et redémarrez le terminal pour que ces modifications soient disponibles pour les applications.

14. Réessayez de mettre à jour TETRA une fois le redémarrage terminé.
15. Si le problème des définitions TETRA persiste, analysez les journaux et effectuez de nouveau les captures.

Informations connexes

- Assistance technique de Cisco et téléchargements

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.