Dépannage des échecs de mise à jour des définitions TETRA

Table des matières

Introduction

<u>Dépannage</u>

Vérification de la connectivité signalée des terminaux sur la console Secure Endpoint

Vérification de la connectivité sur le terminal

Vérification des définitions TETRA sur le terminal

Forcer une mise à jour des définitions TETRA sur le terminal

Vérification de la connectivité du serveur de définition TETRA sur le terminal

Validation de connexion directe

Validation du proxy

Additional Information

Introduction

Ce document décrit les étapes à suivre afin d'étudier la raison pour laquelle les terminaux ne parviennent pas à mettre à jour les définitions TETRA à partir des serveurs de mise à jour des définitions TETRA de Cisco.

Définitions Échec de la dernière mise à jour constaté sur la console Secure Endpoint apparaît sous les détails de l'ordinateur, comme indiqué ci-dessous.

# DESKTOP-QFC3PVT in group Protect			
Hostname	DESKTOP-QFC3PVT	Group 🗄	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy 🔅	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-17 19:40:25 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90600)
Definitions Last Updated	2023-05-17 19:16:49 UTC A Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score 🛛 🚷	No high severity vulnerabilities found.
Events P Device Trajectory & Diagnostics O View Changes			
Q. Scan 😵 Diagnose 🕸 Move to Group			

Dépannage

Cisco Secure Endpoint pour Windows nécessite une connexion permanente au serveur de définition TETRA afin de télécharger les mises à jour.

Les erreurs courantes de téléchargement des définitions TETRA sont les suivantes :

- · Impossible de résoudre l'adresse du serveur
- Échec de la validation du certificat SSL (y compris la vérification de la liste de révocation de certificats)
- Interruption pendant le téléchargement
- Échec de la connexion au serveur proxy
- Échec de l'authentification auprès du serveur proxy

En cas d'échec lors de la tentative de téléchargement des définitions TETRA, la prochaine tentative aura lieu lors de l'intervalle de mise à jour suivant ou si une mise à jour manuelle a été lancée par l'utilisateur.

Vérification de la connectivité signalée des terminaux sur la console Secure Endpoint

La console Secure Endpoint indique si le terminal se connecte régulièrement. Assurez-vous que vos terminaux sont actifs et qu'ils ont un état « Dernier vu » récent. Si les terminaux ne s'enregistrent pas avec la console Secure Endpoint, cela indique qu'ils ne sont pas actifs ou qu'ils rencontrent des problèmes de connectivité.

Cisco publie en moyenne 4 mises à jour de définition par jour. Si le point d'extrémité ne parvient pas à télécharger la mise à jour à un moment quelconque de la journée, le connecteur signale une erreur d'échec. Compte tenu de cette fréquence, seulement si les points d'extrémité sont connectés en permanence et ont une connexion réseau stable au serveur TETRA pendant toute la durée, alors les points d'extrémité signaleront comme "Dans la politique".

L'état « Dernière vue » se trouve sur la page Détails de l'ordinateur, comme indiqué ci-dessous :

DESKTOP-QFC3PVT in group Protect			🗙 Definition Update Failed 🛛 🛞 0 🛛 🛤
Hostname	DESKTOP-QFC3PVT	Group d	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1702)	Policy 🔅	Protect
Connector Version	8.1.7.21417	Internal IP	192.168.205.138, 172.23.0.1, 172.30.144.1
Install Date	2023-05-17 01:58:07 UTC	External IP	173.38.117.65
Connector GUID	5c6e64fa-7738-4b39-b201-15451e33bfe6	Last Seen	2023-05-18 21:37:02 UTC
Processor ID	1f8bfbff000906ea	Definition Version	TETRA 64 bit (daily version: 90604)
Definitions Last Updated	2023-05-18 16:54:33 UTC ▲ Failed The Connector was unable to reach the TETRA update server. Check your Secure Endpoint Update Server settings on your policy. Contact Cisco support if the issue persists.	Update Server	tetra-defs.amp.cisco.com
Cisco Secure Client ID	N/A	Kenna Risk Score	No high severity vulnerabilities found.
Take Forensic Snapshot View Snapshot Crbital Query Orbital Query Orbital Query Orbital Query			

Si le point d'extrémité se connecte et qu'une erreur indique que les définitions ne sont pas téléchargées mais qu'elles sont visibles par la console, le problème peut être intermittent. Une enquête plus approfondie peut être menée si les différences temporelles sont importantes entre « Dernière consultation » et « Dernière mise à jour des définitions ».

Vérification de la connectivité sur le terminal

Les utilisateurs finaux peuvent vérifier la connectivité à l'aide de l'interface utilisateur.

L'ouverture de Cisco Secure Client affiche l'état de la connectivité.

Secure Endpoint: Connected. Flash Scan	~	Start	
			ahah

L'outil ConnectivityTool peut être utilisé lorsque le point d'extrémité n'est pas connecté et signale des problèmes de connexion. Ceci est inclus dans l'IPSupportTool qui génère le package de support.

Vérification des définitions TETRA sur le terminal

Cisco Secure Client fournit des informations sur les définitions TETRA actuelles chargées par le connecteur de point d'extrémité. L'utilisateur final peut ouvrir le client et vérifier les paramètres de Secure Endpoint. Dans l'onglet Statistiques, la définition actuelle de TETRA est disponible.

Secure Client

Secure Endpoint

ame:	Protect	
erial Number:	303	
ast Update:	05/17/23 04:45:54 PM	
Detection Engine		~
ame:	Tetra	
ersion:	90604	
ast Update:	Today 02:32:09 AM	
Proxy		~
ype:	None	
erver:		
ser:		
ort:		

En outre, les détails de définition TETRA actuels sont signalés par l'outil AmpCLI sur le terminal. Voici un exemple de cette commande :

```
PS C:\Program Files\Cisco\AMP\8.1.7.21417> .\AmpCLI.exe posture
{"agent_uuid":"5c6e64fa-7738-4b39-b201-15451e33bfe6","connected":true,"connector_version":"8.1.7","engi
```

Les versions de définition sont affichées pour chaque moteur, y compris TETRA. Dans le résultat ci-dessus, il s'agit de la version 90604. Elle peut être comparée à la console Secure Endpoint sous : Management > AV Definition Summary. Un exemple de la page est comme ci-dessous.

AV Definition Summary

64bit	32bit	
Version 90606	Version 120765	V
2023-05-18 20:13:58 UTC	2023-05-18 20:13:57 UTC	2023-0!

TETRA 64bit	TETRA 32bit	ClamAV Mac	ClamAV Linux-Or
Version		Available	
90606		2023-05-18 2	0:13:58 UTC
90605		2023-05-18 1	6:15:48 UTC
90604		2023-05-18 1	2:13:36 UTC

Si la version est toujours en retard et que l'état du connecteur est connecté, une mise à jour des définitions ou une vérification de la connectivité du point d'extrémité au serveur TETRA peut être effectuée.

Forcer une mise à jour des définitions TETRA sur le terminal

Les utilisateurs finaux peuvent lancer et vérifier la progression du téléchargement TETRA. Pour que l'utilisateur déclenche la mise à jour, l'option doit être définie dans la stratégie. Dans la page Advanced Settings > Client User Interface policy settings, les paramètres Allow user to update TETRA definitions doivent être activés pour que les définitions soient déclenchées par l'utilisateur.

Dans Cisco Secure Client, l'utilisateur final peut ouvrir le client et vérifier les paramètres de Secure Endpoint. L'utilisateur peut cliquer sur "Mettre à jour maintenant" pour déclencher la mise à jour de la définition TETRA comme indiqué ci-dessous :

Cisco Secure Client -	-	×
Secure Client		0
Secure Endpoint Statistics Update Advanced		
Check for Updates: This will update the policy, software, and detection engine signatures for your connector. Last Update Successful Update Now		

Si vous exécutez AMP for Endpoints Connector version 7.2.7 et ultérieure, vous pouvez utiliser un nouveau commutateur « -forceupdate » pour forcer le connecteur à télécharger les définitions TETRA.

Une fois la mise à jour forcée, la définition TETRA peut être vérifiée à nouveau pour voir si une mise à jour se produit. Si aucune mise à jour n'est toujours en cours, la connexion au serveur TETRA doit être vérifiée.

Vérification de la connectivité du serveur de définition TETRA sur le terminal

La stratégie de point de terminaison inclut le serveur de définitions que le point de terminaison contacte pour télécharger les définitions.

La page Détails de l'ordinateur inclut le serveur de mise à jour. L'image ci-dessous montre où le serveur de mise à jour est affiché :

# DESKTOP-QFC3PVT in group Protect				
Hostname	DESKTOP-QFC3PVT	Group	+	Protect
Operating System	Windows 11, SP 0.0 (Build 22621.1202)	Policy	0	Protect
Connector Version	8.1.2.21412	Internal IP		192.168.205.138
Install Date	2023-05-17 01:58:07 UTC	External IP		173.38.117.65
Connector GUID	5c5e64fa-7738-4b39-b201-15451e33bfe6	Last Seen		2023-05-17 19:40:25 UTC
Processor ID	1155/5/000905ea	Definition Version		TETRA 64 bit (daily version: 90500)
Definitions Last Updated	2023-05-17 19:18:49 UTC A Failed The Connector was unable to reach the TETRA. update server. Check your Secure Endpoint Update Server settings on your policy. Contact Clisco support if the issue pensists.	Update Server	(tetra-defs.amp.clisco.com
Gisco Secure Client ID	N/A.	Kenna Risk Score (0	No high severity vulnerabilities found.
♦ Events P Device Trajectory % Diagnostics ⊗ View Changes				
			E	9, Scan 9 Diagnose & Move to Group

Sur le cloud public, le nom de serveur requis auquel le terminal peut se connecter est répertorié sous : <u>Adresses de serveur requises pour le bon fonctionnement de Cisco Secure Endpoint &</u> <u>Malware Analytics</u>

Validation de connexion directe

À partir du point d'extrémité, la commande suivante peut être exécutée pour vérifier la recherche DNS sur le serveur de mise à jour :

PS C:\Program Files\Cisco\AMP> Resolve-DnsName -Name tetra-defs.amp.cisco.com Name Type TTL Section IPAddress ---- tetra-defs.amp.cisco.com A 5 Answer 192.XXX.X.XX tetra-defs.amp.cisco.com A 5 Answer 192.XXX.X.X tetra-defs.amp.cisco.com A 5 Answer 192.XXX.X.X

Si l'adresse IP est résolue, la connexion au serveur peut être testée. Une réponse valide ressemblera à ce qui suit :

<#root>

PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com

- * Trying 192.XXX.X.X:443...
- * Connected to tetra-defs.amp.cisco.com (192.XXX.X.X) port 443 (#0)
- * schannel: disabled automatic use of client certificate
- * ALPN: offers http/1.1

```
* ALPN: server did not agree on a protocol. Uses default.
* using HTTP/1.x
> GET / HTTP/1.1
> Host: tetra-defs.amp.cisco.com
> User-Agent: curl/8.0.1
> Accept: */*
* schannel: server closed the connection
< HTTP/1.1 200 OK
< Date: Fri, 19 May 2023 19:13:35 GMT
< Server:
< Last-Modified: Mon, 17 Apr 2023 15:48:54 GMT
< ETag: "0-5f98a20ced9e3"
< Accept-Ranges: bytes
< Content-Length: 0
< Connection: close
< Content-Type: text/html; charset=UTF-8
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
```

Si la connexion ne peut pas être établie pour valider le certificat avec le serveur CRL (tel que commercial.ocsp.identrust.com ou validation.identrust.com), alors une erreur sera vue comme suit

```
PS C:\Program Files\Cisco\AMP> curl.exe -v https://tetra-defs.amp.cisco.com
* Trying 192.XXX.X.XX:443...
* Connected to tetra-defs.amp.cisco.com (192.XXX.X.XX) port 443 (#0)
* schannel: disabled automatic use of client certificate
* ALPN: offers http/1.1
* schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation function
* Closing connection 0
* schannel: shutting down SSL/TLS connection with tetra-defs.amp.cisco.com port 443
curl: (35) schannel: next InitializeSecurityContext failed: Unknown error (0x80092013) - The revocation
```

```
Validation du proxy
```

Si le point d'extrémité est configuré pour utiliser un proxy, le dernier état d'erreur peut être vérifié. L'exécution de PowerShell ci-dessous peut renvoyer la dernière erreur de la tentative de mise à jour TETRA.

PS C:\Program Files\Cisco\AMP> (Select-Xml -Path local.xml -XPath '//tetra/lasterror').Node.InnerText

Dernier code d'erreur	Problème	Actions
4294965193	Impossible d'établir la connexion au proxy	Vérifier la connectivité du réseau au proxy
4294965196	Authentification avec proxy impossible	Vérifier les informations d'authentification du proxy
4294965187	Échec de la connexion au proxy et du téléchargement	Vérifier les problèmes de téléchargement dans les journaux proxy

Additional Information

 Si vous voyez des terminaux qui ne parviennent pas à télécharger les définitions TETRA, bien qu'ils aient effectué les vérifications ci-dessus, activez le connecteur en mode de débogage pendant un intervalle de temps égal à l'intervalle de mise à jour défini dans votre stratégie et générez l'offre groupée de support. Lorsque le connecteur est en mode de débogage, notez que vous devez également prendre les captures de paquets Wireshark. La capture de paquets doit également être exécutée pendant un intervalle de temps égal à l'intervalle de mise à jour défini dans votre stratégie. Une fois que ces informations ont été collectées, veuillez ouvrir un dossier auprès du TAC Cisco avec ces informations pour une enquête plus approfondie.

Collecte des données de diagnostic à partir du connecteur AMP pour Windows

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.