

La requête de conformité ISE 3.2 MDM échoue en raison de la suppression du client et d'un défaut logiciel

Table des matières

Problème

Certains terminaux authentifiés via EAP-TLS sur Cisco Identity Services Engine (ISE) ne reçoivent pas par intermittence d'état de conformité de Microsoft Intune, même s'ils sont indiqués comme conformes dans le tableau de bord Intune. Par conséquent, ces points d'extrémité ont atteint une stratégie d'autorisation sans fil par défaut au lieu de la stratégie conforme à la position ou non conforme à la position attendue. Les terminaux affectés n'affichent pas les attributs de conformité de la gestion des appareils mobiles (MDM) dans les journaux en direct ISE ou les rapports MDM externes, et le problème affecte uniquement un sous-ensemble de clients dans le déploiement.

Les symptômes spécifiques observés sont les suivants :

- Les clients anormaux n'ont pas de journaux dans le rapport ISE sur le rapport de gestion des appareils mobiles externes.
- Les clients anormaux n'ont pas d'attributs tels que l'état MDM ou l'état de périphérique dans les détails du journal en direct.
- Les clients anormaux appliquent la stratégie d'autorisation sans fil 802.1x_EAP-TLS_toyotawifi au lieu de la stratégie conforme à la position.
- Les messages d'erreur dans les journaux indiquent « Failed to connect to MDM Server : 404 Non Trouvé ».

Environnement

- Cluster multinoeud Cisco ISE version 3.2, correctif 6

- 8 noeuds ISE dans le cluster, tous affichant un état vert
- 11 000 clients sans fil/filaires intégrés à Microsoft Intune
- Les clients utilisent l'authentification EAP-TLS (certificat de machine)
- ISE utilise l'adresse MAC du client pour les requêtes vers Intune
- Tous les clients ont un état de conformité sur le tableau de bord Microsoft Intune
- Le problème touche certains clients, mais pas tous

Résolution

Le problème a été résolu par ces étapes.

Étape 1: Identifier la cause première

L'analyse des journaux ISE a révélé que les points d'extrémité affectés ont un ID de serveur MDM périmé, ce qui empêche l'exécution des requêtes MDM.

Les journaux montraient :

```
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MDMUtil -:::- M
2026-06-15 13:35:14,343 DEBUG [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.util.MdmServersCache -
2026-06-15 13:35:14,344 ERROR [PolicyEngineEvaluationThread-4][[]] cisco.cpm.mdm.pip.MdmPartnerPIPHandl
```

En outre, le déploiement a rencontré l'ID de bogue Cisco CSCww51917, qui affecte les recherches de conformité MDM lorsque l'utilisation d'une adresse MAC a un ID de serveur MDM périmé.

Étape 2: Contournement temporaire

Comme solution de contournement temporaire :

1.- Supprimez le point de terminaison de Context Visibility et réauthentifiez-le. Cela a permis de résoudre le problème de l'interrogation du serveur MDM et de l'obtention de l'état de conformité.

2.- Accédez à Visibilité contextuelle.

3.- Sélectionnez l'adresse MAC du point d'extrémité et supprimez-la.

4.- Authentifiez à nouveau le terminal.

Étape 3: Résolution permanente - Mise à niveau logicielle

La résolution permanente est suivie sous l'ID de bogue Cisco CSCwv51917.

Motif

Pendant l'authentification, ISE tente d'interroger la référence du serveur MDM périmé, mais l'objet de serveur MDM correspondant n'existe plus ou est inactif. Par conséquent, ISE ne récupère pas les attributs de conformité MDM d'Intune.

Autres informations utiles

- [ID de bogue Cisco CSCwv519173134](#)
- [Notes de version ISE 3.2 - Avertissements résolus](#)
- [ISE 3.2 Avis de fin de vie](#)
- [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.