

Échec de la connexion à l'interface utilisateur graphique ISE avec le jeton RADIUS PingID Federation

Table des matières

Problème

La connexion de l'interface utilisateur graphique de l'administrateur à Cisco ISE échoue lors de l'utilisation de la fédération PingID comme jeton RADIUS, malgré les captures de paquets montrant que Ping Federate renvoie une réponse d'acceptation d'accès. L'échec de connexion se produit même si l'authentification RADIUS semble réussie du point de vue du réseau, empêchant l'accès administratif à l'interface ISE. L'analyse des paquets réseau confirme que le serveur PingID (10.32.154.200) envoie la réponse d'acceptation d'accès attendue à ISE (10.2.200.241), mais que le processus de connexion de l'administrateur ISE ne se termine toujours pas correctement.

Environnement

- Cisco Identity Services Engine (ISE) version 3.3 Patch 7
- Déploiement de machines virtuelles à 4 noeuds
- Fédération PingID configurée comme authentification de jeton RADIUS
- Adresse IP ISE : 10.2.200.241
- Adresse IP du serveur PingID : 10.32.154.200
- La configuration Admin Access est examinée sous Administration > Admin Access

Résolution

Le problème a été résolu grâce à l'application d'une solution de contournement qui a activé la fonctionnalité de connexion admin réussie. Les étapes décrites dans les sections suivantes ont été suivies pour résoudre le problème.

Étape 1: Collecte et analyse des preuves

Des preuves de capture de paquets ont été collectées et analysées pour confirmer le flux d'authentification RADIUS entre ISE et le serveur PingID. L'analyse a vérifié que Ping Federate envoyait correctement des réponses d'acceptation d'accès.

Étape 2: Preuve de port-server.log

###

prt-server.log

```
RadiusTokenIDStore,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/  
RadiusClient,2026-03-27 13:25:04,534,DEBUG,0x7f4942ebb700,cntx=0180887321,sesn=SIT2194/554866250/183397  
RadiusClient,2026-03-27 13:25:05,074,DEBUG,0x7f490d6b9700,NIL-CONTEXT,onProcessResponse: Processing Res  
RadiusClient,2026-03-27 13:25:05,074,WARN ,0x7f49444c6700,cntx=0180887321,sesn=SIT2194/554866250/183397
```

###

Étape 3: Qu'est-ce que Message-Authenticator ?

L'authentificateur de message est un attribut de sécurité utilisé dans les paquets RADIUS pour garantir l'intégrité et l'authenticité des messages échangés entre les périphériques réseau et le serveur RADIUS. Il s'agit d'une signature cryptographique calculée à l'aide de HMAC-MD5 sur l'ensemble du paquet RADIUS avec une clé secrète partagée. Cet attribut aide à protéger contre l'altération et l'usurpation des messages RADIUS, en particulier ceux impliquant des flux d'authentification EAP (Extensible Authentication Protocol).

Étape 4: Implémentation de contournement

Désactiver "Authentificateur De Message Requis En Réponse" : Administration / Gestion des identités / Sources d'identités externes / Jeton RADIUS. Cliquez sur le nom du jeton RADIUS, puis accédez à Authentification. Décochez "Authentificateur De Message Requis En Réponse".

Étape 5: Test de validation

Après avoir appliqué la solution de contournement, des tests de connexion administrateur ont été exécutés pour valider la résolution. Ces tests ont confirmé l'authentification réussie et l'accès à l'interface utilisateur graphique de l'administrateur ISE en utilisant la fédération PingID comme jeton RADIUS.

Étape 6: Période De Suivi

Une période de surveillance et de validation a été établie pour assurer la stabilité de la solution de contournement. Au cours de cette période, le test de connexion de l'administrateur s'est poursuivi sans qu'aucune erreur ou défaillance ne soit signalée.

Motif

L'échec de connexion à l'interface utilisateur graphique d'ISE Admin a été causé par une non-concordance d'application de sécurité du protocole RADIUS entre Cisco ISE 3.3 Patch 7 et PingID (Ping Federate) pendant l'authentification MFA.

Plus précisément :

- Cisco ISE a demandé que l'attribut Message-Authenticator RADIUS soit présent dans la réponse Access-Accept du serveur de jetons RADIUS externe.
- PingID renvoyait des réponses Access-Accept sans l'attribut Message-Authenticator.
- Étant donné que le paramètre Message Authenticator Required On Response était activé dans ISE, il a silencieusement rejeté la réponse RADIUS comme étant non valide, même si

l'authentification elle-même a réussi du côté PingID.

- Cette application fait partie du renforcement de la sécurité de Cisco ISE pour atténuer la vulnérabilité Blast-RADIUS (CVE-2024-3596).

Autres informations utiles

- [Atténuation de l'usurpation du protocole Blast-RADIUS \(CVE-2024-3596\)](#)

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.