

Dépannage de l'erreur Échec de connexion de l'utilisateur “ ; L'authentification de l'utilisateur par rapport à Active Directory a échoué car le compte de l'utilisateur est verrouillé” ;

Table des matières

[Problème](#)

[Environnement](#)

[Résolution](#)

[Motif](#)

[Autres informations utiles](#)

- [Problème](#)
 - [Environnement](#)
 - [Résolution](#)
 - [Motif](#)
 - [Autres informations utiles](#)
-

Problème

Active Directory génère cette erreur lorsqu'un utilisateur dépasse le seuil de verrouillage de compte Active Directory sur le serveur Windows Server en saisissant plusieurs fois un mot de passe incorrect :

“24408 User authentication against Active Directory failed since user has entered the wrong password”

Environnement

- Cisco Identity Services Engine (ISE) versions 3.2.0 et ultérieures

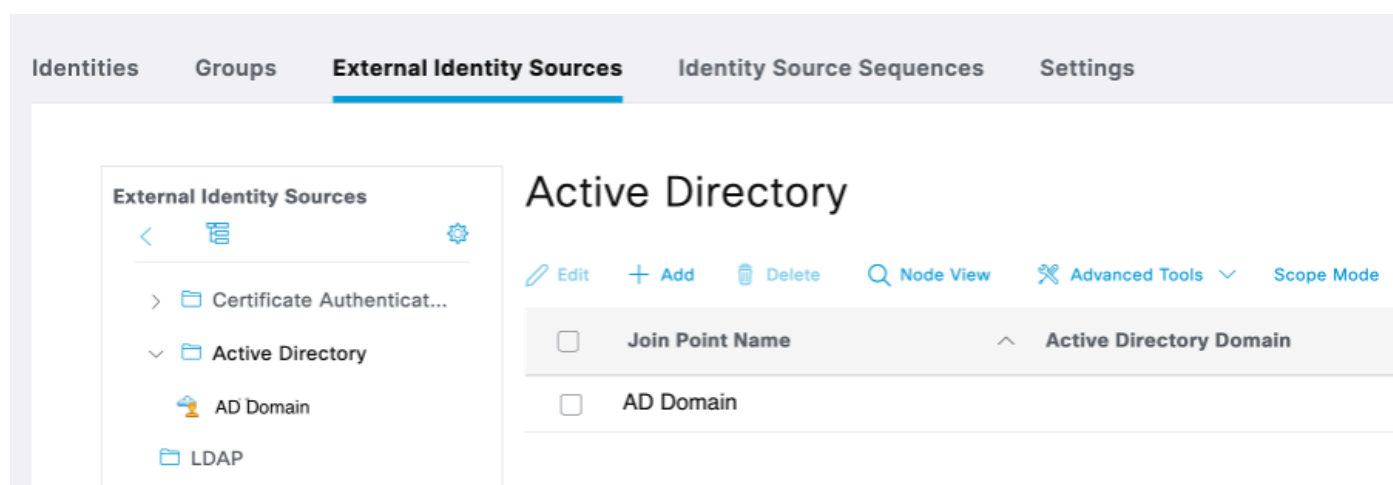
- Intégration Active Directory pour l'authentification des utilisateurs
- Environnements d'authentification filaire et sans fil
- Authentification basée sur RADIUS avec des périphériques d'accès réseau (NAD)

Résolution

Étape 1: Activez la fonctionnalité « Empêcher le verrouillage des utilisateurs Active Directory » sur votre déploiement ISE :

Cette fonctionnalité arrêterait l'envoi des authentifications utilisateur à Active Directory pour empêcher le verrouillage du compte utilisateur en configurant le nombre maximal autorisé de tentatives de mauvais mot de passe et en comparant cette limite avec le nombre actuel de mauvais mots de passe (attribut badPwdCount) dans Active Directory avant d'envoyer une demande d'authentification.

1. Connectez-vous à l'interface utilisateur graphique ISE.
2. Accédez à Administration > Identity Management > External Identity Sources > Active Directory. Sélectionnez le domaine AD, vous voulez activer la fonctionnalité.



3. Accédez à l'onglet Advanced Settings.

* Join Point Name

AD Domain



4. Dans la section Empêcher le verrouillage utilisateur Active Directory, cochez la case Activer la protection d'authentification en échec.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. Entrez le nombre maximal de tentatives de mot de passe erroné autorisé.

- Ce nombre doit être inférieur au nombre maximal de tentatives de mauvais mot de passe configuré comme valeur de l'attribut badPwdCount dans Active Directory.
- Assurez-vous d'activer la case à cocher Filaire ou Sans fil ou Les deux selon votre type de connexion d'authentification.

6. Cliquez sur Enregistrer.



Remarque : ISE continuerait à rejeter les demandes d'authentification des utilisateurs jusqu'à ce que l'attribut badPwdCount d'Active Directory soit remis à zéro.

Motif

Cela peut se produire pour les raisons suivantes :

- L'utilisateur saisit un mot de passe incorrect lors de l'authentification sur le terminal.
- L'utilisateur modifie les informations d'identification Active Directory et oublie de mettre à jour les informations d'identification Active Directory dans son point d'accès sans fil qui effectue l'authentification EAP-PEAP.

Autres informations utiles

- [Configurer le nombre maximal de tentatives de mot de passe pour un compte Active Directory](#)

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.