

Échec d'Active Directory - Code d'erreur : 0xc0000064

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Problème](#)

[Solution](#)

Introduction

Ce document décrit la solution du problème lorsque le contrôleur de domaine Microsoft Active Directory commence à répondre à la notification de faux échec par « code d'erreur : 0xc0000064 » pour les demandes d'authentification de Cisco Identity Services Engine (ISE).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Identity Services Engine (ISE).
- Microsoft Active Directory (MS-AD).

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Identity Services Engine (ISE) 2.4 et 2.6 sur VM (Small).
- Microsoft Active Directory (MS-AD) 2012.

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 actif, assurez-vous de bien comprendre l'impact potentiel de n'importe quelle étape.

Problème

Deux entrées de journal ont été observées (échec et succès) dans les journaux d'audit de l'observateur d'événements du contrôleur de domaine (DC) pour chaque demande d'authentification d'ISE.

L'échec est dû à la raison « NO_SUCH_USER » et au code d'erreur : 0xc0000064

Security Number of events: 5 (!) New events available				
Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	5/10/2019 12:25:49 ...	Microsoft Windows security auditing.	4776	Credential Validation
Audit Failure	5/10/2019 12:25:49 ...	Microsoft Windows security auditing.	4776	Credential Validation

Solution

Le comportement est lié au défaut [CSCvf45991](#) et les étapes suivantes doivent résoudre le problème.

Étape 1. Mettre à niveau ISE vers la version ou le correctif dans lequel [CSCvf45991](#) est corrigé.

Étape 2. Rejoignez ISE pour souhaiter un domaine AD.

Étape 3. Afin de configurer les paramètres du Registre, accédez à **Advance Tool > Advance Tuning**.

Name :

REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\WorkaroundForFalseFailedLoginEvent

Advanced Tuning

This page should only be used under instruction from Cisco Support. Parameter values can be adjusted to tune the Active Directory Connection

* ISE Node

* Name

* Value

* Comment ⓘ

ⓘ

Change History The list of parameters changed on ISE Node ISE-21.r1.dom.

Insert Selected Item into Fields		
Parameter Name	Parameter Value	Comment
REGISTRY.Services\lsass\Parameters\Providers\ActiveDirectory\WorkaroundForFalseFailedLoginEvent	YES	set to yes

Étape 4. Valeur: OUI.

Étape 5. Cliquez sur le bouton **Mettre à jour la valeur**.

Étape 6. Cliquez sur **Redémarrer le connecteur Active Directory**.

Note: Étape 6 : redémarrez le service de connecteur Active Directory.

Étape 7. Réexécutez le test d'authentification (MSCHAPV2) une fois le service de connecteur Active Directory activé et le problème résolu.

Étape 8. Le journal de réussite de l'audit sous Observateur d'événements dans AD doit confirmer la même chose.