Active Directory False Failure - Error Code: 0xc0000064

Contents

Introduction

This document describes the solution of the issue when Microsoft Active Directory Domain Controller starts to respond to the false failure notification with "error code: 0xc0000064" for authentication requests from the Cisco Identity Services Engine (ISE).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- Identity Services Engine (ISE) 2.4 & 2.6 on 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. If your network is live, make sure that you understand the potential impact of any step.

Problem

Two log entries observed (failure & successful) in Event viewer Audit logs of Domain Controller (DC) for each authentication request from ISE.

The failure is with reason "NO_SUCH_USER" and error code: 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

Behaviour is related to defect CSCvf45991 and the following steps should resolve the issue.

Step 1. Upgrade ISE to version or patch in which CSCvf45991 is fixed.

Step 2. Join ISE to desire AD Domain.

Step 3. In order to configure **Registry Settings**, navigate to **Advance Tool > Advance Tuning**.

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

Step 4. Value: YES.

Step 5. Click **Update Value** button.

Step 6. Click **Restart Active Directory Connector**.

> **Note**: Step 6 restarts the Active Directory connector service.

Step 7. Perform authentication test (MSCHAPV2) once again after Active Directory connector service is up and the issue is resolved.

Step 8. Audit success log under Event Viewer in AD should confirm the same.