

Error al solucionar el error de inicio de sesión del usuario “Error de autenticación del usuario en Active Directory porque la cuenta del usuario está bloqueada”

Contenido

[Problema](#)

[Entorno](#)

[Resolución](#)

[Causa](#)

[Contenido relacionado](#)

- [Problema](#)
 - [Entorno](#)
 - [Resolución](#)
 - [Causa](#)
 - [Contenido relacionado](#)
-

Problema

Active Directory genera este error cuando un usuario supera el umbral de bloqueo de cuentas de Active Directory en Windows Server al escribir una contraseña incorrecta varias veces:

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

Entorno

- Cisco Identity Services Engine (ISE) versión 3.2.0 y posteriores
- Integración de Active Directory para la autenticación de usuarios

- Entornos de autenticación por cable e inalámbricos
- Autenticación basada en RADIUS con dispositivos de acceso a la red (NAD)

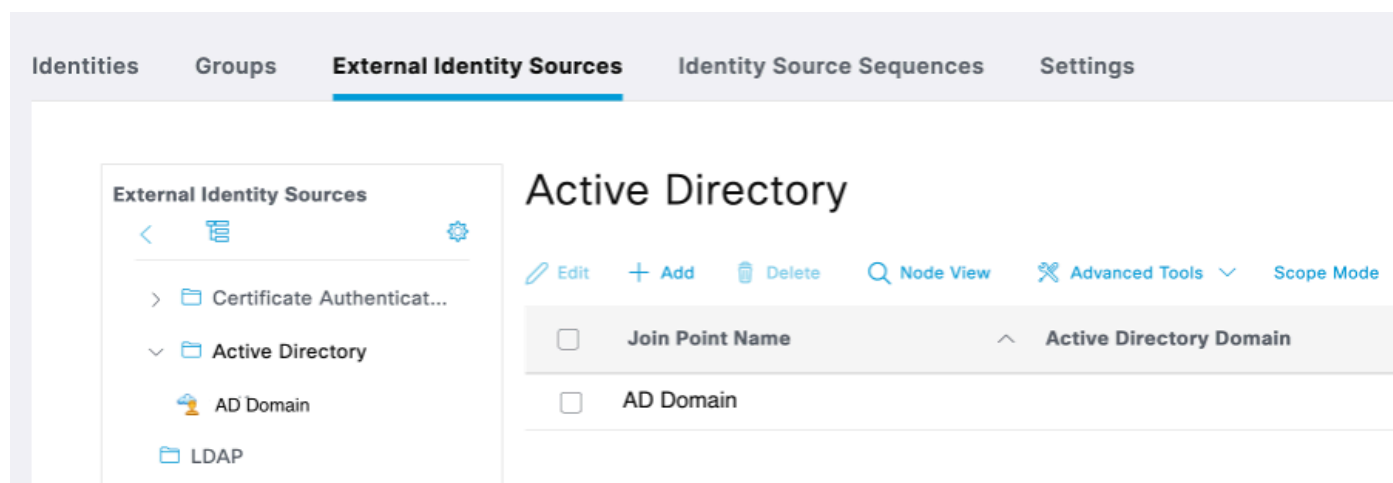
Resolución

Paso 1: Habilite la función "Evitar el bloqueo de usuarios de Active Directory" en su implementación de ISE:

Esta característica dejaría de enviar las autenticaciones de usuario a Active Directory para evitar que la cuenta de usuario se bloquee configurando el número máximo permitido de intentos de contraseñas incorrectas y comparando este límite con el recuento actual de contraseñas incorrectas (atributo badPwdCount) en AD antes de enviar una solicitud de autenticación.

1. Inicie sesión en la GUI de ISE.

2. Vaya a Administration > Identity Management > External Identity Sources > Active Directory. Seleccione el dominio AD; desea habilitar la función.



3. Vaya a la pestaña Advanced Settings.

* Join Point Name

AD Domain



4. En la sección Impedir bloqueo de usuarios de Active Directory, active la casilla para Habilitar protección de autenticación fallida.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. Introduzca el número máximo de intentos de contraseña incorrecta permitidos.

- Este número debe ser menor que el número máximo de intentos de contraseña incorrecta configurados como valor del atributo badPwdCount en Active Directory.
- Asegúrese de activar la casilla de verificación Wired o Wireless o Both según el tipo de conexión de autenticación.

6. Haga clic en Guardar.



Nota: ISE seguirá rechazando las solicitudes de autenticación de usuario hasta que el atributo badPwdCount de Active Directory se restablezca a cero.

Causa

Esto puede ocurrir por las siguientes razones:

- El usuario introduce una contraseña incorrecta mientras realiza la autenticación en el terminal.
- El usuario cambia las credenciales de AD y olvida actualizar las credenciales de AD en su terminal inalámbrico que realiza la autenticación EAP-PEAP.

Contenido relacionado

- [Configurar el número máximo de intentos de contraseña para la cuenta de Active Directory](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).