

Falha na identificação e solução de problemas de erro de falha de login do usuário “Falha na autenticação do usuário em relação ao Active Directory, pois a conta do usuário está bloqueada”

Contents

[Problema](#)

[Ambiente](#)

[Resolução](#)

[Causa](#)

[Conteúdo relacionado](#)

- [Problema](#)
 - [Ambiente](#)
 - [Resolução](#)
 - [Causa](#)
 - [Conteúdo relacionado](#)
-

Problema

O Active Directory gera este erro quando um usuário excede o Limite de Bloqueio de Conta do Active Directory no Windows Server inserindo uma senha incorreta várias vezes:

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

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.2.0 e posterior

- Integração do Active Directory para autenticação de usuário
- Ambientes de autenticação com e sem fio
- Autenticação baseada em RADIUS com dispositivos de acesso à rede (NADs)

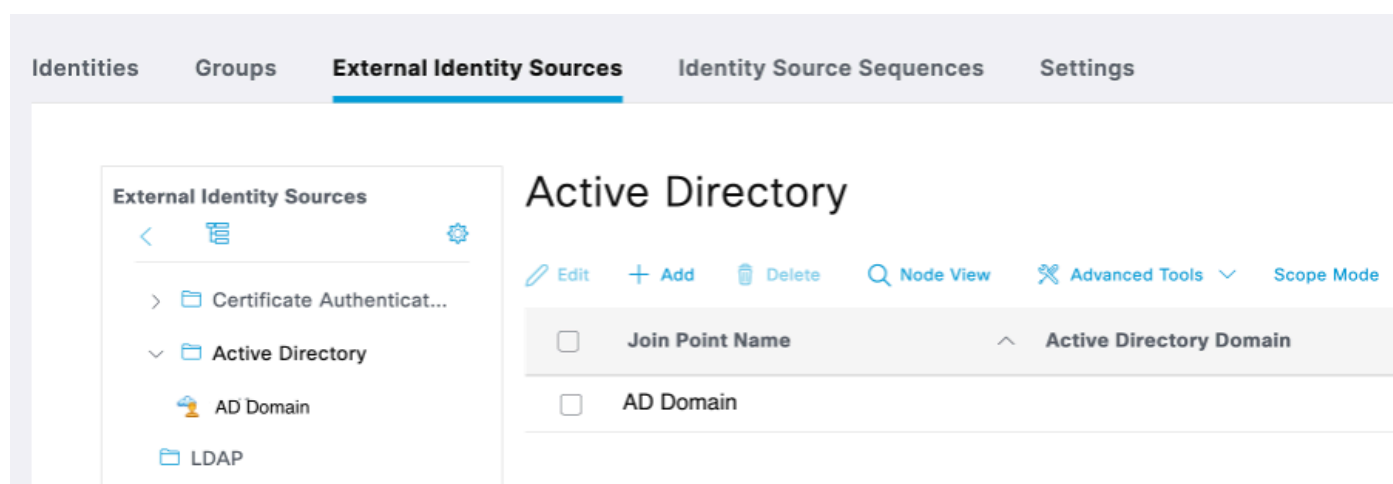
Resolução

Passo 1: Habilite o recurso "Impedir Bloqueio de Usuários do Active Directory" em sua implantação do ISE:

Esse recurso interromperia o envio de autenticações de usuário ao Active Directory para impedir que a conta de usuário seja bloqueada, configurando o máximo permitido de tentativas de senha inválida e comparando esse limite com a contagem de senhas inválidas (atributo badPwdCount) atual no AD antes de enviar uma solicitação de autenticação.

1. Faça login na GUI do ISE.

2. Navegue até Administração > Gerenciamento de Identidades > Fontes de Identidade Externas > Active Directory. Selecione o Domínio do AD, para habilitar o recurso.



3. Vá até a guia Advanced Settings.

* Join Point Name

AD Domain



4. Na seção Impedir Bloqueio de Usuários do Ative Directory, marque a caixa Ativar Proteção com Falha de Autenticação.

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum 2 attempts

☒ Wireless

☒ Wired

5. Informe o número máximo de tentativas com senha incorreta permitidas.

- Esse número deve ser menor que o número máximo de tentativas de senha inválida configurado como o valor do atributo badPwdCount no Ative Directory.
- Certifique-se de ativar a caixa de seleção Wired ou Wireless ou Both de acordo com o tipo de conexão da autenticação.

6. Clique em Salvar.



Note: O ISE continuará a rejeitar solicitações de autenticação de usuário até que o atributo badPwdCount do Ative Directory seja redefinido para zero.

Causa

Isso pode acontecer pelas seguintes razões:

- O usuário insere uma senha incorreta ao executar a autenticação no endpoint.
- O usuário altera as credenciais do AD e esquece de atualizar as credenciais do AD em seu endpoint sem fio que executa a autenticação EAP-PEAP.

Conteúdo relacionado

- [Configurar Máximo de Tentativas de Senha para a Conta do Ative Directory](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.