

ユーザログイン失敗のトラブルシューティングのエラー“；ユーザのアカウントがロックアウトされているため、Active Directoryに対するユーザ認証に失敗した”

内容

[問題](#)

[環境](#)

[解決方法](#)

[原因](#)

[関連コンテンツ](#)

- [問題](#)
 - [環境](#)
 - [解決方法](#)
 - [原因](#)
 - [関連コンテンツ](#)
-

問題

Active Directoryでこのエラーが生成されるのは、ユーザが誤ったパスワードを複数回入力して、Windows ServerのActive Directoryアカウントのロックアウトしきい値を超過した場合です。

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

環境

- Cisco Identity Services Engine(ISE)バージョン3.2.0以降
- ユーザ認証用のActive Directory統合

- 有線と無線の両方の認証環境
- ネットワークアクセスデバイス(NAD)によるRADIUSベースの認証

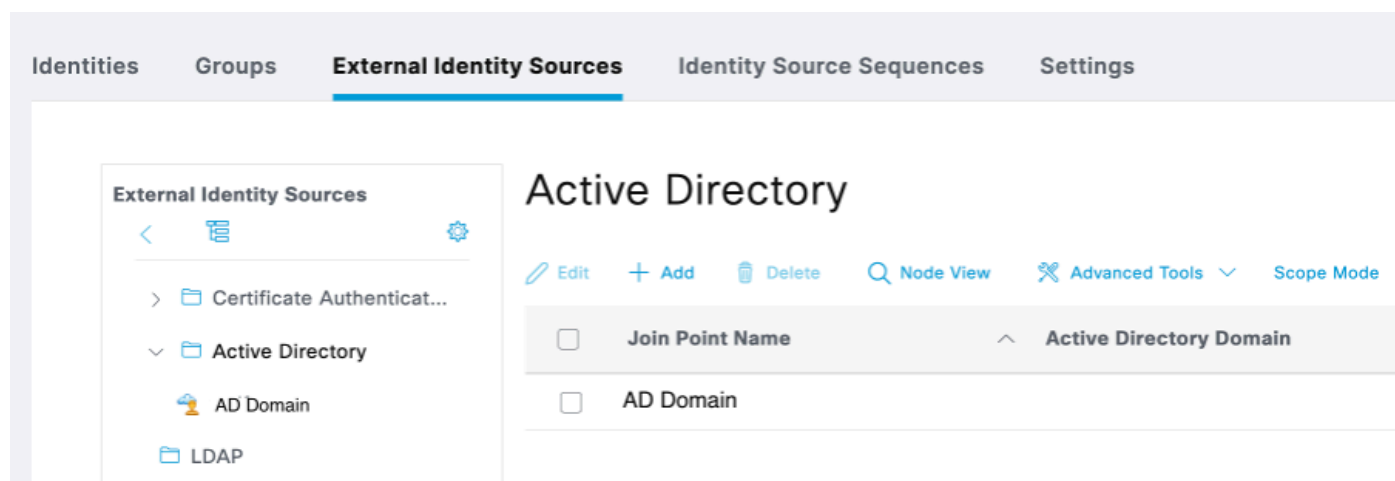
解決方法

ステップ1: ISE導入で「Active Directoryユーザロックアウトの防止」機能を有効にします (オプション)。

この機能は、許可される不正パスワードの最大試行回数を設定し、認証要求を送信する前にこの制限をADの現在の不正パスワード数 (badPwdCount属性) と比較することで、ユーザアカウントがロックアウトされないようにActive Directoryへのユーザ認証の送信を停止します。

1. ISE GUIにログインします。

2. Administration > Identity Management > External Identity Sources > Active Directoryの順に移動します。機能を有効にするADドメインを選択します。



3. Advanced Settingsタブに移動します。

* Join Point Name

AD Domain



4. [Active Directoryユーザーロックアウトの防止]セクションで、[失敗した認証保護を有効にする]チェックボックスをオンにします。

▼ Prevent Active Directory User Lockout ⓘ

☒ Enable Failed Authentication Protection

Maximum attempts

☒ Wireless

☒ Wired

5. 許容される不正なパスワードの最大試行回数を入力します。

- この数は、Active DirectoryのbadPwdCount属性の値として設定されている不正パスワードの最大試行数よりも小さくする必要があります。
- 認証接続のタイプに応じて、Wired、Wireless、またはBothのいずれかのチェックボックスがオンになっていることを確認します。

6. Saveをクリックします。



注: ISEは、Active DirectoryのbadPwdCount属性が0にリセットされるまで、ユーザ認証要求を拒否し続けます。

原因

これは、次の理由で発生する可能性があります。

- ・ ユーザがエンドポイントで認証を実行する際に、誤ったパスワードを入力した。
- ・ ユーザがADクレデンシャルを変更し、EAP-PEAP認証を実行するワイヤレスエンドポイントでADクレデンシャルを更新するのを忘れた。

関連コンテンツ

- ・ [Active Directoryアカウントの最大パスワード試行回数の設定](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。