

アクセス ポリシーのディレクトリを検索中、信頼できるドメインで AD グループが見つからないのはなぜですか。

目次

質問：

アクセス ポリシーのディレクトリを検索中、信頼できるドメインで AD グループが見つからないのはなぜですか。

環境： Cisco Web セキュリティ アプライアンス (WSA)、NTLM 認証、信頼されたドメイン

症状：

- ユーザは彼のアクセスポリシーの 1 つでポリシー メンバーの定義として使用するために「アクティブ ディレクトリ グループ」を調べを試みて、グループはディレクトリの検索で表示ではありません。
- グループは信頼された AD ドメインに属し、WSA がに加入したくないドメイン。

この動作は意図的です。 アクセスポリシーのグループを設定している間、信頼されたドメインからのグループはディレクトリの検索で現れません。

AsyncOS すべてのバージョンで、他のドメインに WSA によって加入されるドメインとの**双方向信頼**がある場合 WSA に異なるドメインからのユーザを認証し、それぞれ AD グループを一致する機能があります。

このようなシナリオの場合、下記のステップを使用してアクセスポリシーの信頼されたドメインからグループを追加できます：

1. GUI に参照して下さい --> Web Security Manager --> アクセスポリシー --> <Policy Name> --> 選択したグループおよびユーザ --> Groups
2. 手動で「ディレクトリの検索」フィールドに、ドメイン名と共に、全体のグループ名を打ち込んで下さい
3. 「追加します」ボタンをクリックして下さい
4. 変更をそれから『Done』 をクリックし、入れて下さい及び保存して下さい

他のドメインに WSA によって加入されるドメインとの双方向トラスト 関係がない場合 WSA が手動で設定されたグループを一致することに注目して下さい

注: AsyncOS バージョン 7.7 および それ 以上で、WSA は複数の NTLM レルムをサポートし、2 つのドメイン間にトラスト 関係がないシナリオのために、第 2 ドメインのための新しい NTLM レルムを作成できます。 複数の NTLM レルムを使うと、WSA はアクセスポリシー内の異なるドメインからのルックアップグループできます。