LDAP 認証グループ ポリシーを適用するように WSA を設定するにはどうすればよいですか。

目次

質問：

環境： Cisco Web セキュリティ アプライアンス（WSA）、AsyncOS のすべてのバージョン

このナレッジ ベース記事では、シスコによる保守およびサポートの対象でないソフトウェアに言及します。 この情報は、利便性のために無償で提供されています。 さらにサポートが必要な場合は、ソフトウェアのベンダーに連絡してください。

「認証グループ」が機能するためには、最初に [GUI] > [Network] > [Authentication] で認証レルムを設定する必要があります。

1. **最初に [Authentication Protocol] を [LDAP] に設定し、（その他のセクションが正しく設定されている状態で）[Group Authorization] に移動します。**
2. **[Group Name Attribute] を指定します。 これは、[Web Security Manager] > [Web Access Policies] > [Click Add Group] > [Select Group Type to Authentication Group] > [Directory Lookup] テーブルに表示される値を保持する属性です。 この属性は一意であり、またこの属性により表されるリーフ ノードに、グループのユーザのリストが含まれている必要があります。**
3. **次に、[Group Filter Query] を指定します。 これは、LDAP ディレクトリですべてのグループを検索するために WSA が使用する検索フィルタです。**
4. **次に [Group Membership Attribute] を指定します。これは、メンバーの固有値を保持するリーフ ノードの属性です。 この属性はこのグループのメンバーを保持するため、複数のエントリが表示されます。 この属性に含まれる値が、同じページの [User Name Attribute] の値に対応していることを確認してください。**

次に、WSA が LDAP レルム設定を使用してユーザ名を LDAP グループと照合する方法の例を示します。

1. **[Group Filter Query] に [objectClass=group] を設定するとします。**
2. **WSA は最初にこのフィルタを使用して LDAP ディレクトリ内を検索し、該当するエントリを検出します。**
3. **次に WSA はこの検出結果を使用して、[Group Membership Attribute] に指定されている属性を検索します。 この属性が「member」であるとします。**
4. **ユーザが WSA プロキシ経由で「USERNAME_A」としてログインしている場合、WSA は LDAP サーバでユーザのアカウントを検索し、一致が検出されると [User Name Attribute] に**

指定されている属性（例： uid）を使用し、前述の手順で収集された「member」属性にリストされているユーザに「uid」が一致するかどうかを確認します。

5. 一致が検出される場合、そのユーザは設定されているポリシーを使用し、一致が検出されない場合、WSA は次のポリシーを評価します。

LDAP サーバで設定する必要がある属性を確認するには、『Softerra LDAP Browser』（http://www.ldapbrowser.com）を参照してください。