FireSIGHT システムでの LDAP 認証オブジェクトの設定

目次

概要

認証オブジェクトは外部認証サーバのためのサーバプロファイルで、それらのサーバの接続 設定および認証フィルターの設定が含まれています。 FireSIGHT Management Center の認証オブジェクトを作成し、管理し、削除できます。 この資料に SireSIGHT システムの LDAP認証 オブジェクトを設定する方法を記述されています。

LDAP認証 オブジェクトの設定

1. FireSIGHT Management Center の Web ユーザ ユーザー・ インターフェースにログインして下さい。

2. **システム > ローカル > ユーザマネージメント**へのナビゲート。

ログイン認証タブを選択して下さい。

認証 オブジェクトを『Create』 をクリック して下さい。

3. **認証方式**および**サーバタイプを**選択して下さい。

- [Authentication Method]： LDAP
- [Name]： *<Authentication オブジェクト Name>*
- Server Type： MS アクティブ ディレクトリ

注: アスタリスクがついているフィールドが (*) 必要となります。

4. プライマリ および バックアップ サーバ ホスト名か IP アドレスを規定 して下さい。 バックアップサーバはオプションです。 ただし、同じドメイン内のどのドメインコントローラでもバックアップサーバと使用することができます。

注: LDAP ポートがポート **389** へデフォルトであるが、LDAPサーバが受信している標準外

ポート番号を使用できます。

5. 下記に示されているように LDAP **仕様パラメータを**規定 して下さい:

ヒント： ユーザ、グループおよび OU 属性は LDAP **仕様パラメータを**設定する前に識別する必要があります。 認証 オブジェクト 設定のためのアクティブ ディレクトリ LDAP オブジェクト属性を識別するためにこの資料を読んで下さい。

- **ベース DN** -ドメインか仕様 OU DN
- **基礎フィルタ**-ユーザがメンバーのであることグループ DN。
- **ユーザネーム**- DC のための偽装アカウント
- **password**： *<password>*
- **Confirm Password**： *<password>*

詳細オプション:

- **Encryption (暗号化) ：** SSL、TLS またはどれも
- **SSL 認証アップロード パス**: アップロードして下さい CA 認証 (オプションの) を
- **ユーザネーム テンプレート**: `%s`
- **タイムアウト (秒)** : 30

AD のドメイン セキュリティポリシー設定では、**要件に**設定 される場合 SSL が TLS **署名する署名を必要とするために LDAPサーバが**使用される。

LDAPサーバ署名要件

- **None**： サーバと結合 するためにデータ署名が必要となりません。 署名する Client 要求 データがサーバそれをサポートすれば。
- **require 署名**: TLS \ SSL が使用されなければ、オプションに署名する LDAP データはネゴシエートする必要があります。

注: クライアント側がか CA 認証 (CA 証明書) は LDAPS に必要となりません。 ただし、それは認証 オブジェクトに CA 証明書の余分セキュリティレベル アップロードされますです。

6. アトリビュート マッピング することを規定 して下さい

- **UI アクセス アトリビュート**: sAMAccountName
- **シェル アクセス アトリビュート**: sAMAccountName

ヒント： テスト出力の**サポートされていないユーザ** メッセージが表示する場合、**UI アクセス アトリビュートを** userPrincipalName に変更し、**ユーザネームが** `%s.` に**テンプレート** 設定 されることを確かめて下さい

7. 群制御アクセス ロールを設定して下さい

ldp.exe で各グループに認証 オブジェクトに下記に示されているように対応した グループ DN をコピーして下さい:

- **<Group Name> グループ DN: <group dn>**
- **グループ メンバー アトリビュート**: **メンバーは**常にあるはずです

例：

- **管理者グループ DN:** CN=DC admin、CN=Security グループ、DC=VirtualLab、DC=local
- **グループ メンバー アトリビュート**: メンバー

AD セキュリティグループは**メンバー**のアトリビュートをメンバー ユーザの DN に先行させてもらいます。 数先行する**メンバー属性は**メンバー ユーザの数を示します。

8. **基づいている**シェル アクセス フィルタ用の**フィルタ**選択して下さい、またはステップ 5.に示すように `memberOf` アトリビュートを**同じを**規定 して下さい。

シェル アクセス フィルタ: (`memberOf=<group DN>`)

例として、

シェル アクセス フィルタ: `memberOf=CN=Shell CN=Security DC=VirtualLabDC=local`

9. 認証 オブジェクトを保存し、テストを行って下さい。 下記にのように正常なテスト結果見え:

10. 認証 オブジェクトがテストに合格したら、システム ポリシーのオブジェクトを有効に し、アプライアンスにポリシーを再適用して下さい。

関連資料

- 認証オブジェクトに関する Active Directory LDAP オブジェクト属性の識別の設定