FireSIGHT システムでの LDAP 認証オブジェクトの設定

内容

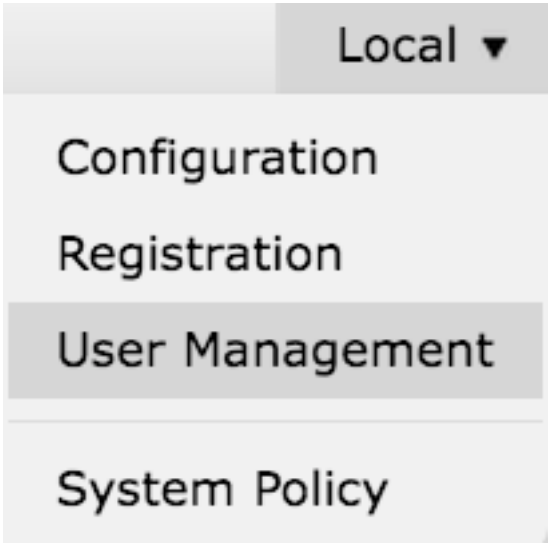
概要

認証オブジェクトとは、外部認証サーバのサーバ プロファイルであり、これらのサーバの接続設定と認証フィルタ設定が含まれています。認証オブジェクトは FireSight Management Center で作成、管理および削除できます。このドキュメントでは、FireSIGHT システムで LDAP 認証オブジェクトを設定する方法について説明します。

LDAP認証オブジェクトの設定

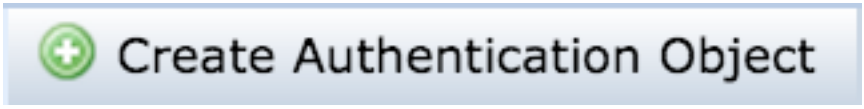
1. FireSIGHT Management CenterのWebユーザインターフェイスにログインします。

2. [System] > [Local] > [User **Management]に移動します。**



[Login Authentication]タブを選択します。

[Create Authentication Object] をクリックします。



3. [Authentication Method] と[Server Type] を選択します。

- **Authentication Method**：[LDAP]
- **[Name]**：*<認証オブジェクト名>*
- **Server Type**：MS Active Directory

注：アスタリスク(*)の付いたフィールドは必須です。

4.プライマリおよびバックアップサーバのホスト名またはIPアドレスを指定します。バックアップサーバはオプションです。ただし、同じドメイン内の任意のドメインコントローラをバックアップサーバとして使用できます。

注：LDAPポートのデフォルトはポート**389**ですが、LDAPサーバがリッスンしている非標準のポート番号を使用できます。

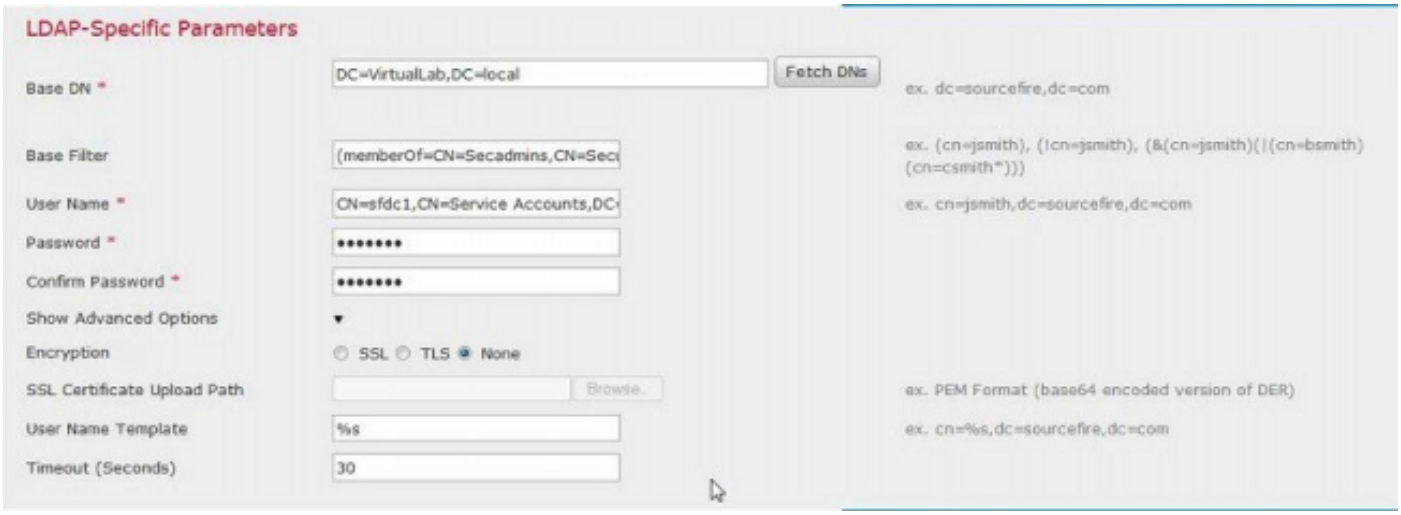
5. **LDAP固有のパラメータ**を次のように指定します。

ヒント：**LDAP固有のパラメータ**を設定する前に、ユーザ、グループ、およびOU属性を特定する必要があります。認証オブジェクト設定のActive Directory LDAPオブジェクト属性を特定するには、このドキュメントを参照してください。

- ベース**DN**：**ドメインまたは特定のOU DN**
- [Base **Filter**]：**ユーザがメンバーになっているグループDN。**
- [User **Name**]:**DCの偽装アカウント**
- **パスワード**：*<password>*
- **Confirm Password**：*<password>*

詳細オプション：

- **暗号化**：SSL、TLS、またはNone
- **SSL証明書アップロードパス**：CA認定のアップロード（オプション）
- **ユーザー名テンプレート**：%s
- **タイムアウト（秒）**:30



ADの[Domain Security Policy Setting]で、[LDAP server Signing requirement] が[Require Signing]に設定されている場合は、SSLまたはTLSを使用する必要があります。

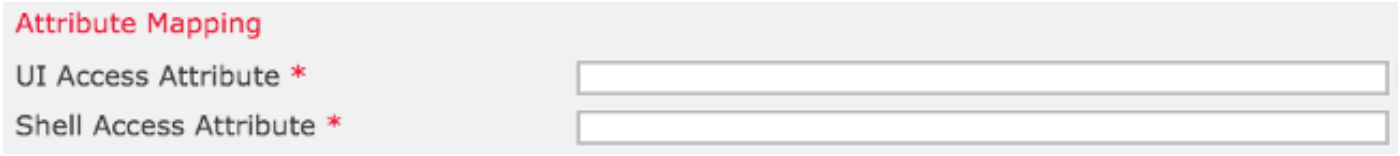
LDAPサーバ署名要件

- **[なし（None）]**： サーバとバインドするためにデータ署名は必要ありません。クライアントがデータ署名を要求する場合、サーバはそれをサポートします。
- **署名の要**求：TLS\SSLが使用されていない限り、LDAPデータ署名オプションをネゴシエートする必要があります。

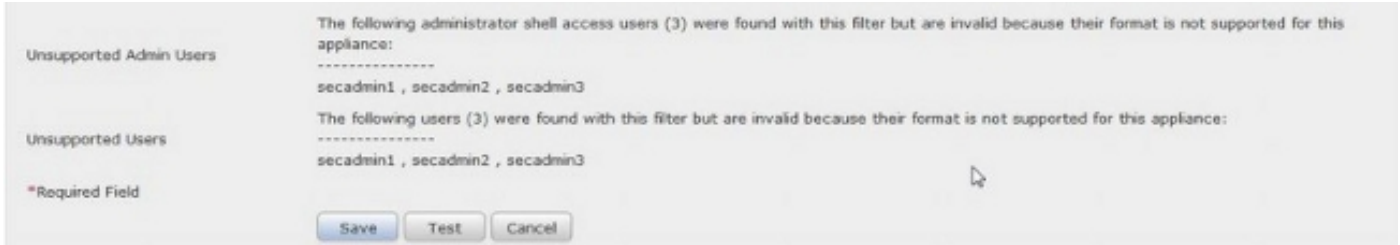
  注：LDAPSでは、クライアント側またはCA証明書（CA証明書）は必要ありません。ただし、CA証明書の追加レベルのセキュリティが認証オブジェクトにアップロードされます。

6.属性マッピングの指定

- **UIアクセス属性**:sAMAccountName
- **シェルアクセス属性**:sAMAccountName



ヒント：テスト出力で「Unsupported Users」というメッセージが表示された場合は、[UI Access Attribute] を[userPrincipalName] に変更し、[User Name template] が**%s**に設定されていることを確認します。



7.グループ制御ア**クセスロールの設定**

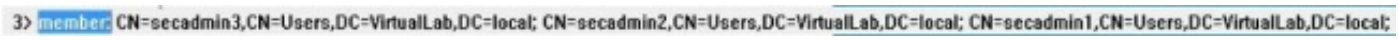
ldp.exeで、各グループを参照し、対応するグループDNを次のようにAuthentication Objectにコピーします。

- **<Group Name>グループDN:<グループDN>**
- **グループメンバー属**性：常にメンバーである必要が**ある**

例：

- **管理者グループDN:**CN=DC admins,CN=Security Groups,DC=VirtualLab,DC=local
- **グループメンバー属**性：member

ADセキュリティグループには、属性**member**の後にメンバーユーザのDNが続きます。**member**属性の前にある数値は、メンバユーザの数を示します。



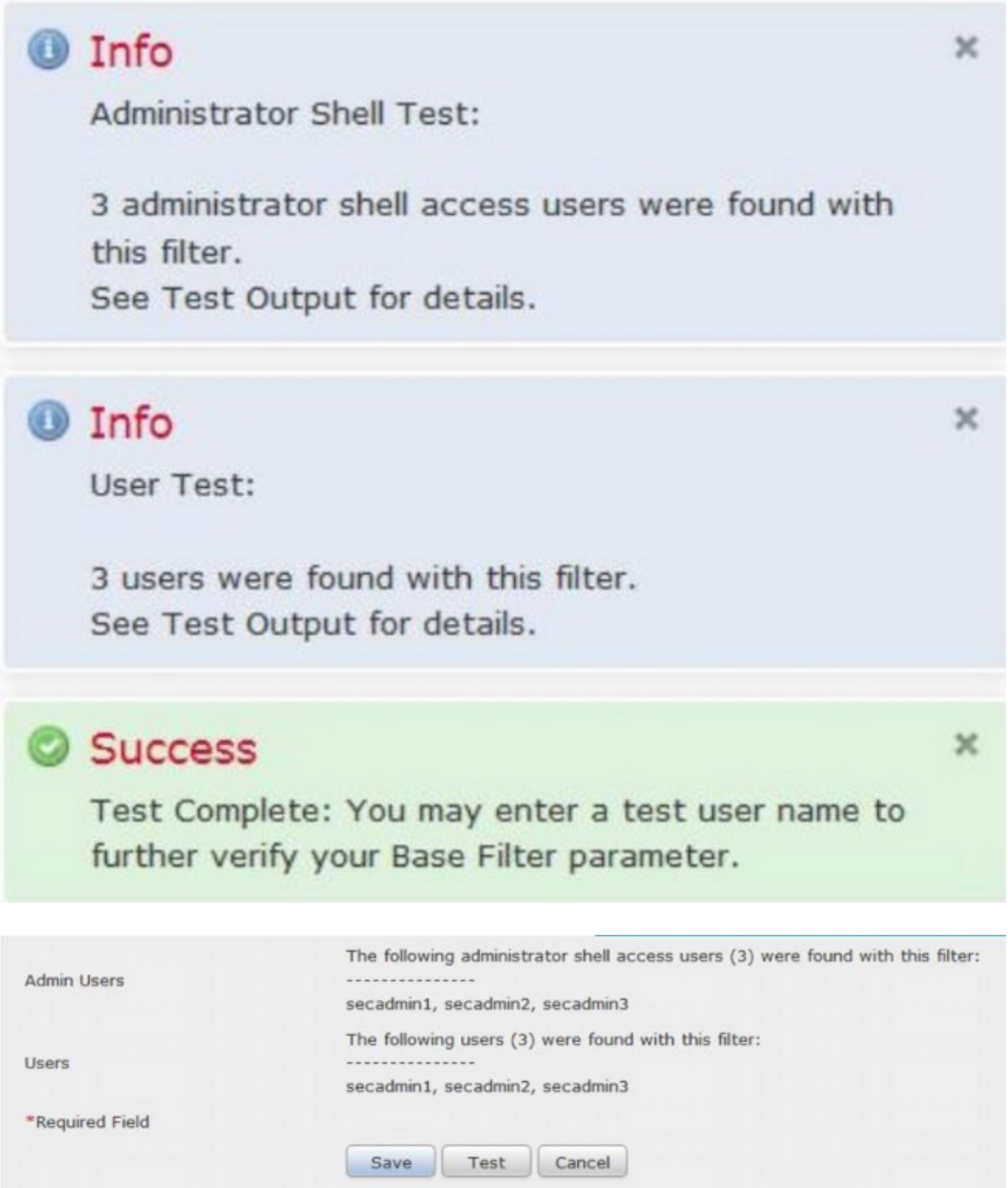
8.「シェル・アクセス・フィルタ」で「**ベース・フィルタと同じ**」を選択するか、手順5に示すようにmemberOf属性を指定します。

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 users,CN=Security Groups,DC=VirtualLab,DC=local)

9.認証オブジェクトを保存し、テストを実行します。正常なテスト結果は次のようになります。



10.認証オブジェクトがテストに合格したら、システムポリシーで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ます。

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