在FireSIGHT系统上配置LDAP身份验证对象

目录

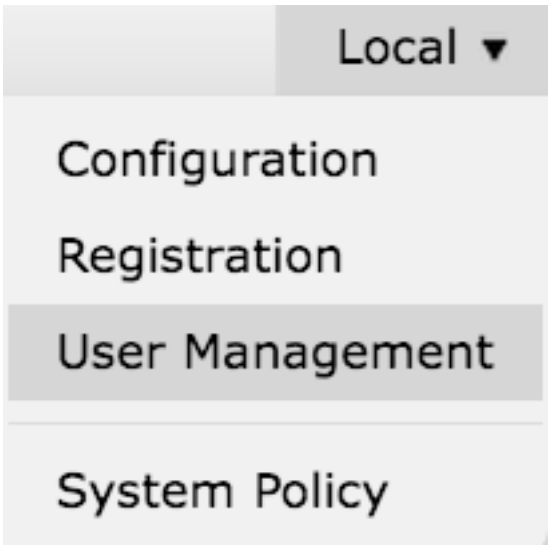
简介

身份验证对象是外部身份验证服务器的服务器配置文件，包含这些服务器的连接设置和身份验证过滤器设置。您可以在FireSIGHT管理中心上创建、管理和删除身份验证对象。本文档介绍如何在FireSIGHT系统上配置LDAP身份验证对象。

LDAP身份验证对象的配置

1.登录FireSIGHT管理中心的Web用户界面。

2.定位至**系统>本地>用户管理**。



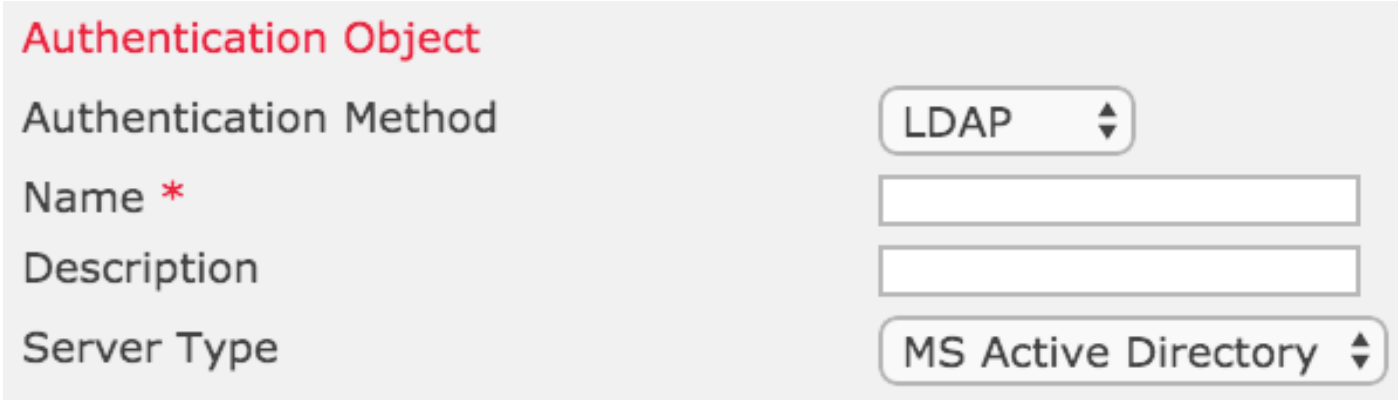
选择**Login Authentication选**项卡。

单击**Create Authentication Object**。

3.选择**Authentication Method**和**Server Type**。

- **认证方法:**LDAP
- **名称：***<身份验证对象名称>*
- **服务器类型:**MS Active Directory

注意：标有星号(*)的字段为必填字段。



4.指定主服务器和备用服务器的主机名或IP地址。备份服务器是可选的。但是，同一域中的任何域控制器都可以用作备份服务器。

注意：虽然LDAP端口默认为端口**389**，但您可以使用LDAP服务器侦听的非标准端口号。

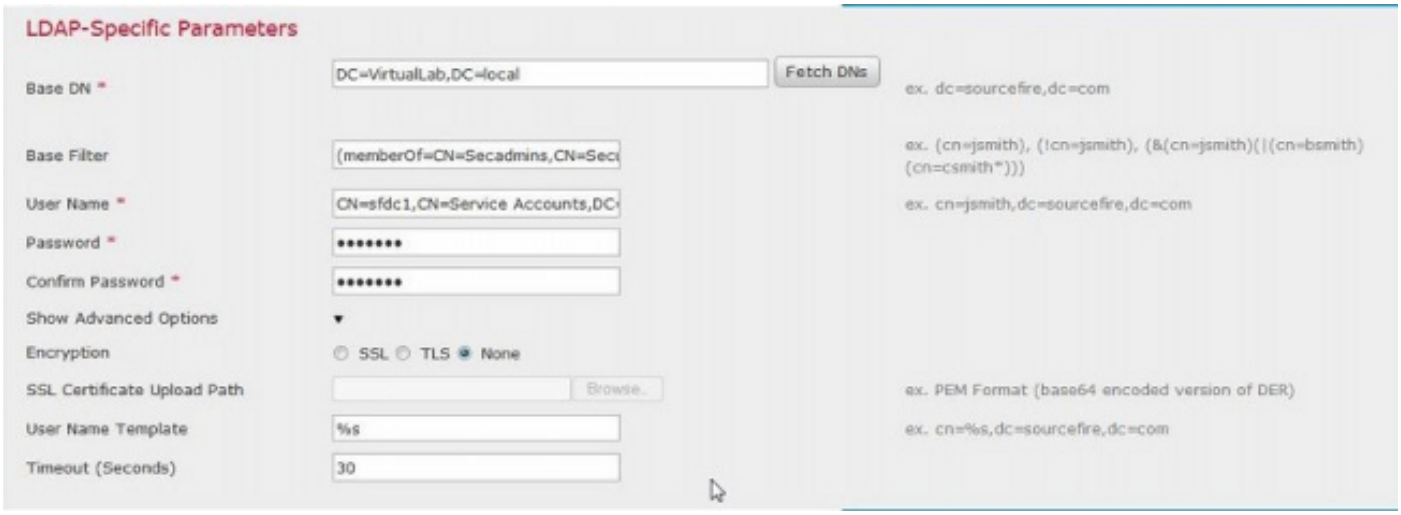
5.指定**LDAP特定参数**，如下所示：

提示：应在配置LDAP特定参数之前识别用户、**组和OU属性**。请阅读此文档以识别用于身份验证对象配置的Active Directory LDAP对象属性。

- 基础**DN — 域或特定OU DN**
- Base **Filter — 用户所属的组DN。**
- 用户**名 - DC的模拟帐户**
- **密码**：*<password>*
- **确认密码：***<password>*

高级选项:

- **加密 :**SSL、TLS或无
- **SSL证书上传路径**:上传CA认证（可选）
- **用户名模板**:%s
- **超时 (秒):**30



在AD的域安全策略设置中，如果**LDAP服务器签名要求**设置为**需要签名**，则必须使用SSL或TLS。

LDAP服务器签名要求

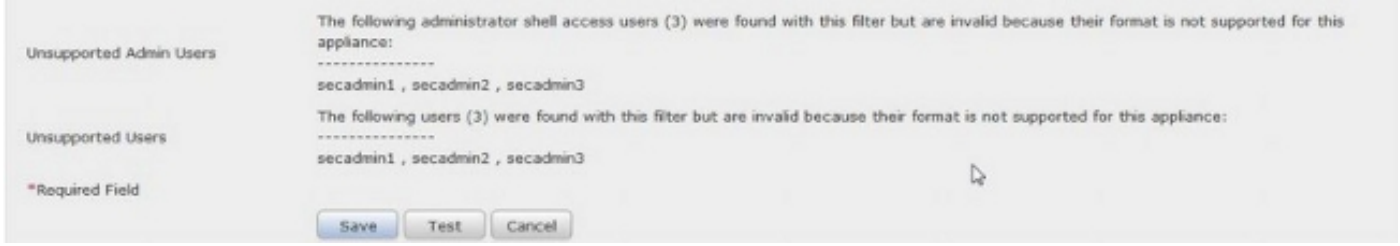
- **无:**不需要数据签名即可与服务器绑定。如果客户端请求数据签名，则服务器支持它。
- **需要签名**:除非使用TLS\SSL，否则必须协商LDAP数据签名选项。

  注意：LDAPS不需要客户端或CA证书（CA证书）。但是，CA证书将上传到身份验证对象，这会增加安全级别。

6.指定属性映射

- **UI访问属性**:sAMAccountName
- **外壳访问属性**:sAMAccountName

提示：如果在测试输出中遇到不支持的用户消息，请将**UI Access Attribute**更改为**userPrincipalName**，并确保**User Name template**设置为**%s**。



7.配置组**控制的访问角色**

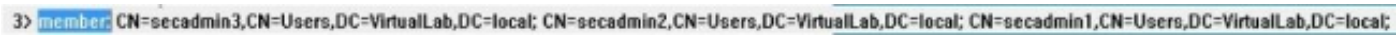
在**ldp.exe**上，浏览到每个组，并将相应的组DN复制到身份验证对象，如下所示：

- **<Group Name>组DN:<group dn>**
- **组成员属性**:应始终为成**员**

示例：

- **管理员组DN:**CN=DC管理员，CN=安全组，DC=虚拟实验室，DC=本地
- **组成员属性**:成员

AD安全组的属性为**member**，后跟成员用户的DN。**member**属性前面的number表示成员用户的数量。



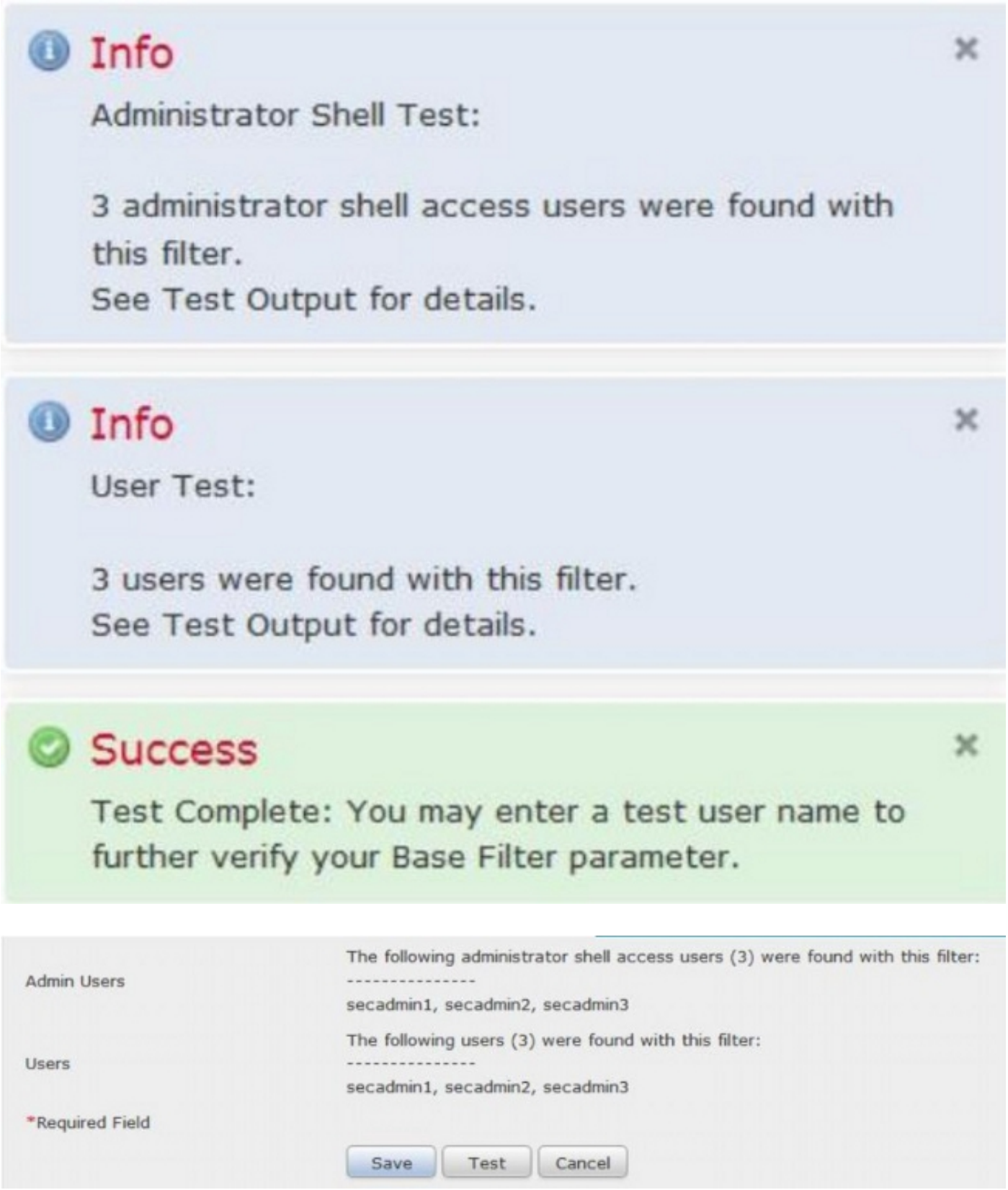
8.选择**与外壳访问过滤器**的基本过滤器相同，或指定memberOf属性（如步骤5所示）。

外壳访问过滤器：(memberOf=<group DN>)

例如，

外壳访问过滤器：（memberOf=CN=Shell users，CN=安全组，DC=VirtualLab，DC=local）

9.保存身份验证对象并执行测试。成功的测试结果如下所示：



10.身份验证对象通过测试后，在系统策略中启用该对象，并将策略重新应用到设备。

相关文档

- 识别身份验证对象配置的Active Directory LDAP对象属性