Configuração do objeto da autenticação LDAP no sistema de FireSIGHT

Índice

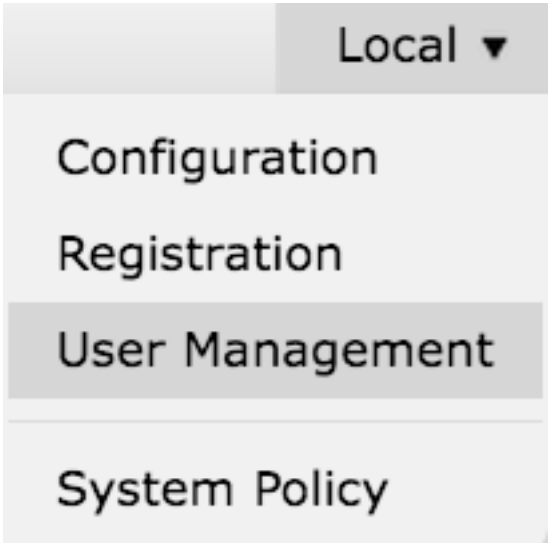
Introdução

Os objetos da autenticação são perfis de servidor para servidores de autenticação externa, contendo configurações de conexão e ajustes do filtro da autenticação para aqueles server. Você pode criar, controlar, e suprimir de objetos da autenticação em um centro de gerenciamento de FireSIGHT. Este original descreve como configurar o objeto da autenticação LDAP no sistema de FireSIGHT.

Configuração de um objeto da autenticação LDAP

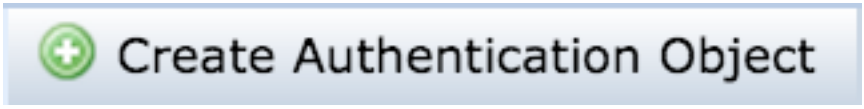
1. Entre à relação de usuário de web do centro de gerenciamento de FireSIGHT.

2. Navegue ao **sistema > ao Local > ao gerenciamento de usuário**.



Selecione a aba da **autenticação de login**.

Clique **criam** sobre o **objeto da autenticação**.



3. Selecione um **método de autenticação** e um **tipo de servidor**.

- **Método de autenticação**: LDAP
- Nome: *Objeto Name> do <Authentication*
- **Tipo de servidor**: Diretório ativo MS

Nota: Os campos identificados por meio de asteriscos (*) são exigidos.

4. Especifique o nome ou o IP address de host do servidor principal e de backup. Um servidor de backup é opcional. Contudo, todo o controlador de domínio dentro do mesmo domínio pode ser usado que um servidor de backup.

Nota: Embora a porta LDAP seja padrão à porta **389**, você pode usar um número de porta não padronizado em que o servidor ldap esteja escutando.

5. Especifique os **parâmetros LDAP-específicos** como mostrado abaixo:

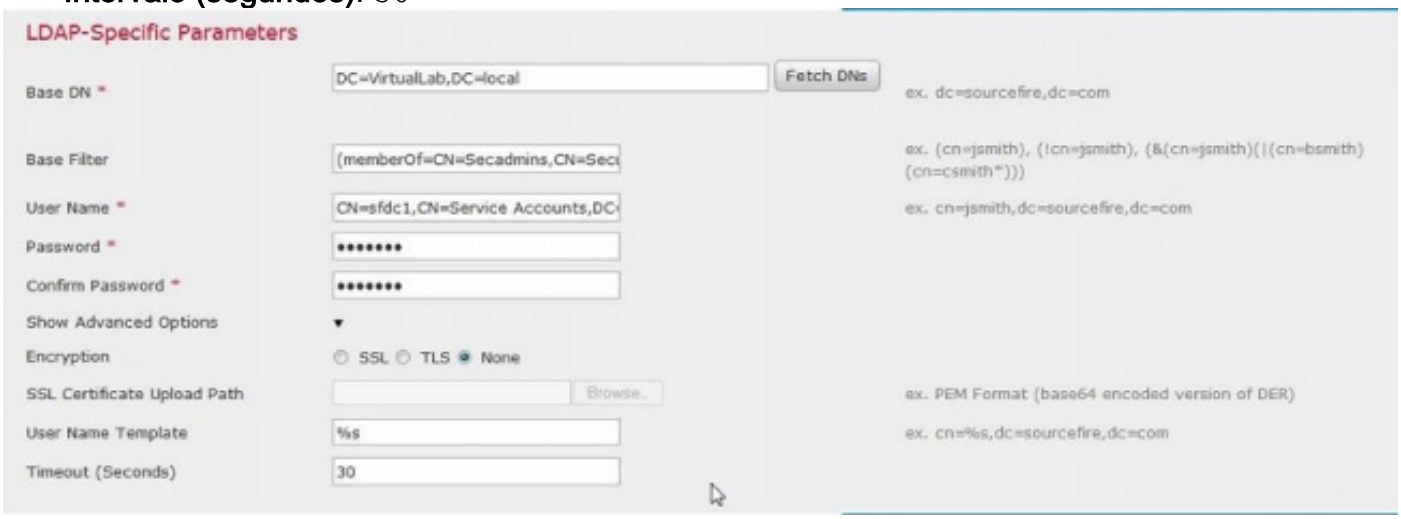
Dica: O usuário, o grupo, e os atributos OU devem ser identificados antes de configurar **parâmetros LDAP-específicos**. Leia este original para identificar atributos de objeto do diretório ativo LDAP para a configuração do objeto da autenticação.

- **Baseie o DN** - Domínio ou OU específico DN
- **Filtro baixo** - O grupo DN que os usuários são membro de.
- **Nome de usuário** - A personificação esclarece o DC
- **Senha**: *<password>*
- **Confirme a senha**: *<password>*

Opções avançadas:

- Criptografia: SSL, TLS ou nenhuns
- **Trajeto da transferência de arquivo pela rede do certificado SSL**: Transfira arquivos pela rede a certificação CA (opcional)
- **Molde do nome de usuário**: `%s`

- **Intervalo (segundos)**: 30



No ajuste da política de segurança do domínio do AD, se a **exigência de assinatura do servidor ldap** são ajustados **para exigir a assinatura**, o SSL ou o TLS deve ser usado.

Exigência de assinatura do servidor ldap

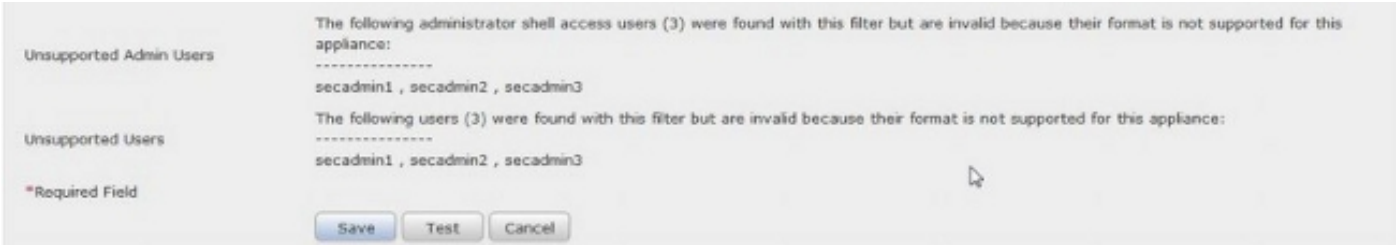
- **Nenhum:** A assinatura dos dados não é exigida a fim ligar com server. Se os dados dos pedidos do cliente que assinam, os suportes de servidor ele.
- **Assinatura Require**: A menos que o TLS \ SSL estiverem sendo usados, a opção de assinatura dos dados LDAP deve ser negociada.

  Nota: O lado do cliente ou o certificado de CA (CERT CA) não são exigidos para LDAP. Contudo, seria um nível de segurança extra do CERT CA é transferido arquivos pela rede ao objeto da autenticação.

6. Especifique o mapeamento do atributo

- **Atributo do acesso UI**: sAMAccountName
- **Atributo do acesso do shell**: sAMAccountName

Dica: Se você encontra mensagem **Unsupported dos usuários na** saída do teste, mude o **atributo do acesso UI ao userPrincipalName** e certifique-se que **molde do nome de usuário** está ajustado a **`%s`.**



7. Configurar **papéis do acesso controlado de grupo**

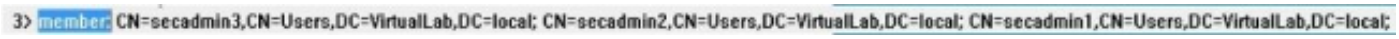
Em `ldp.exe, consulte a` cada grupos e copie o grupo correspondente DN ao objeto da autenticação como mostrado abaixo:

- **Grupo DN de Name> do <Group: dn> do <group**
- **Atributo do membro do grupo**: deve sempre ser o **membro**

Exemplo:

- **Grupo de administrador DN:** Admins CN=DC, grupos de CN=Security, DC=VirtualLab, DC=local
- **Atributo do membro do grupo**: membro

Um grupo de segurança AD tem um atributo do **membro** seguido pelo DN de usuários do membro. O atributo precedente do **membro do** número indica o número de usuários do membro.



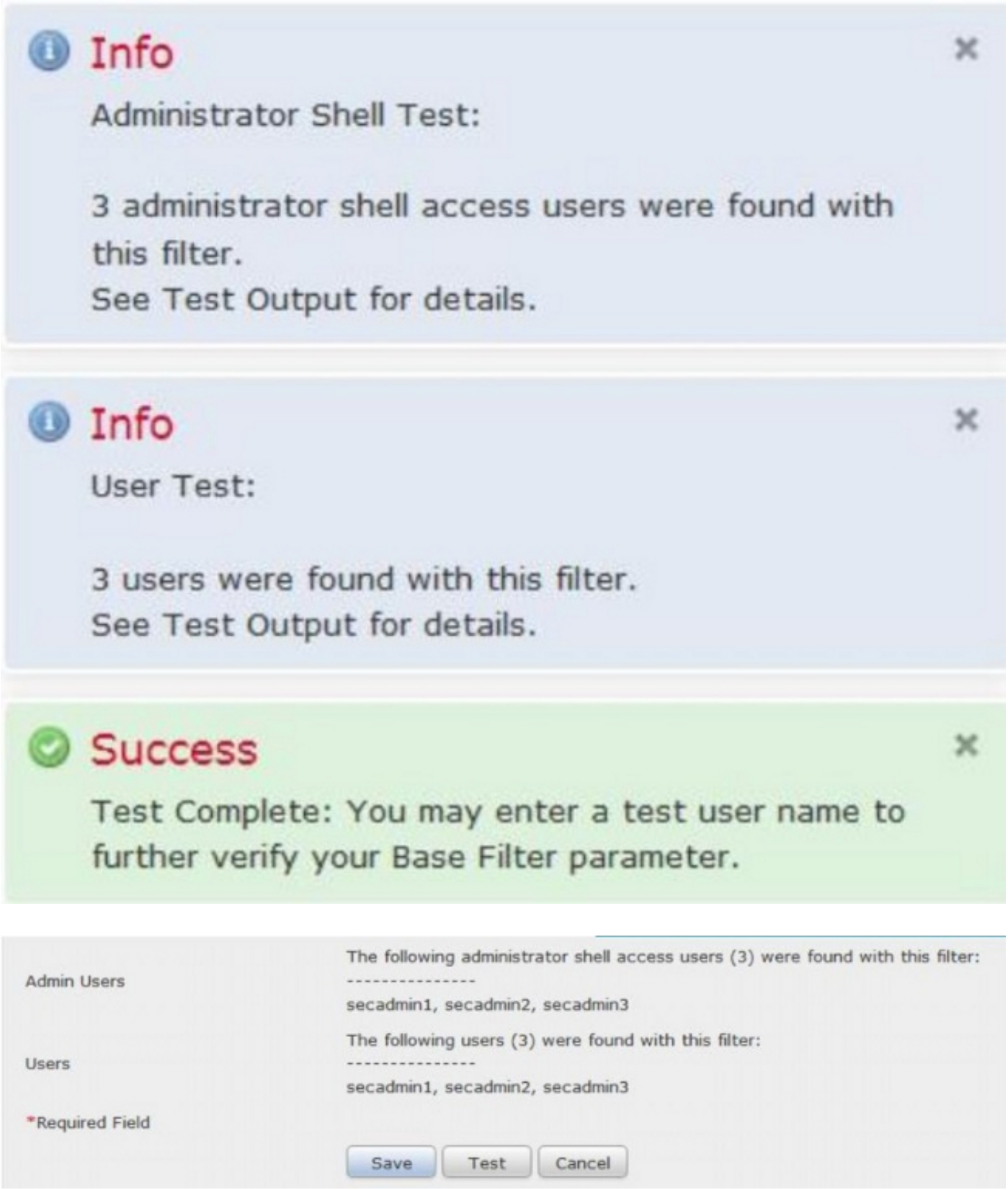
8. Selecione **mesmos como o filtro baixo** para o filtro do acesso do shell, ou especifica o atributo do `memberOf` como indicado na etapa 5.

Descasque o filtro do acesso: (`memberOf=<group DN>`)

Como o exemplo,

Filtro do acesso do shell: `(usuários do memberOf=CN=Shell, grupos de CN=Security, DC=VirtualLab, DC=local)`

9. Salvar o objeto da autenticação e execute um teste. Um resultado de teste bem-sucedido olha como abaixo:



10. Uma vez que o objeto da autenticação passa o teste, permita o objeto na política do sistema e reaplique a política a seu dispositivo.

Original relacionado

- Identifique atributos de objeto do diretório ativo LDAP para a configuração do objeto da

autenticação