Configuration d'objet d'authentification LDAP sur le système de FireSIGHT

Contenu

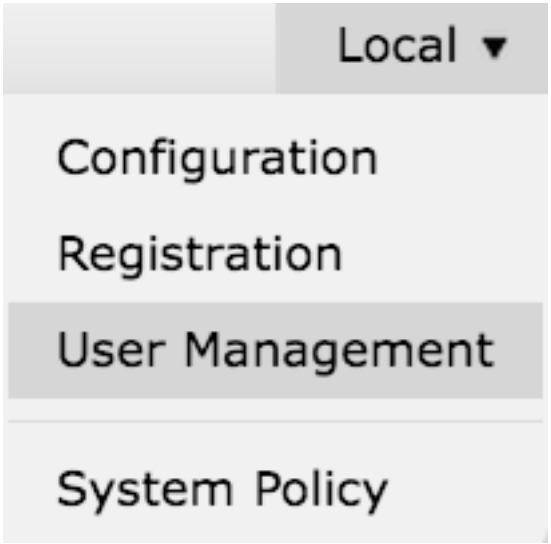
Introduction

Les objets d'authentification sont des profils de serveur pour des serveurs d'authentification externe, contenant des paramètres de connexion et des paramètres de filtre d'authentification pour ces serveurs. Vous pouvez créer, gérer, et supprimer l'authentification les objets sur une Gestion de FireSIGHT centrent. Ce document décrit comment configurer l'objet d'authentification LDAP sur le système de FireSIGHT.

Configuration d'un objet d'authentification LDAP

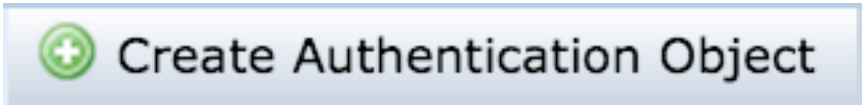
1. Ouvrez une session à l'interface utilisateur d'utilisateur web du centre de Gestion de FireSIGHT.

2. Naviguez vers le **système > les gens du pays > la gestion des utilisateurs**.



Sélectionnez l'onglet d'**authentification de connexion**.

Cliquez sur **créent** en fonction l'**objet d'authentification**.



3. Sélectionnez une **méthode d'authentification** et un **type de serveur**.

- **Méthode d'authentification** : LDAP
- **Nom** : *Objet Name> de <Authentication*
- **Type de serveur** : Répertoire actif de MS

Remarque: Des champs identifiés par des astérisques (*) sont exigés.

4. Spécifiez le nom ou l'adresse IP primaire et de sauvegarde d'hôte de serveur. Un serveur de sauvegarde est facultatif. Cependant, n'importe quel contrôleur de domaine dans le même domaine peut être utilisé qu'un serveur de sauvegarde.

Remarque: Bien que le port de LDAP soit par défaut au port **389**, vous pouvez utiliser un numéro de port non standard sur lequel le serveur LDAP écoute.

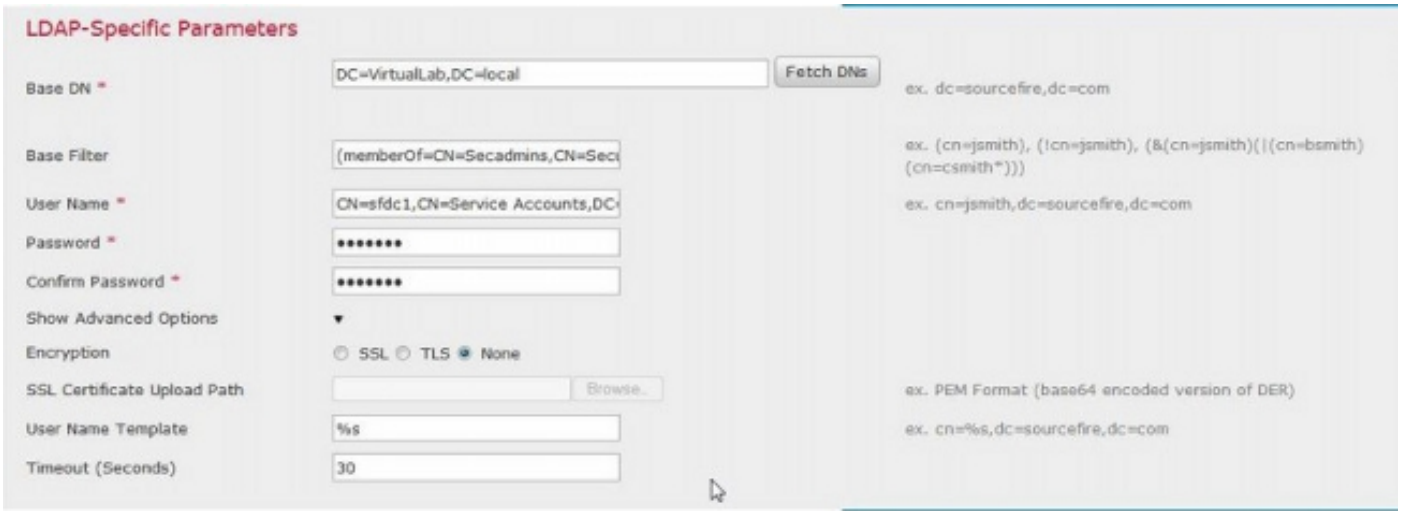
5. Spécifiez les **paramètres de LDAP-particularité** comme affiché ci-dessous :

Conseil : L'utilisateur, le groupe, et les attributs OU devraient être identifiés avant de configurer des **paramètres de LDAP-particularité**. Lisez ce document pour identifier des attributs d'objet de LDAP de Répertoire actif pour la configuration d'objet d'authentification.

- **DN de base** - Domaine ou DN OU spécifique
- **Filtre de base** - Le DN de groupe que les utilisateurs sont membre de.
- **Nom d'utilisateur** - La personnification expliquent le C.C
- **Mot de passe** : *<password>*
- **Confirm Password**: *<password>*

Options avancées :

- **Cryptage** : SSL, TLS ou aucun
- **Chemin de téléchargement de certificat ssl** : Téléchargez la certification CA (facultative)
- **Modèle de nom d'utilisateur** : `%s`
- **Délai d'attente (secondes)** : `30`



Dans la configuration de stratégie de sécurité de domaine de l'AD, si l'**exigence de signature de serveur LDAP** est placée **pour exiger la signature**, le SSL ou le TLS doit être utilisé.

Exigence de signature de serveur LDAP

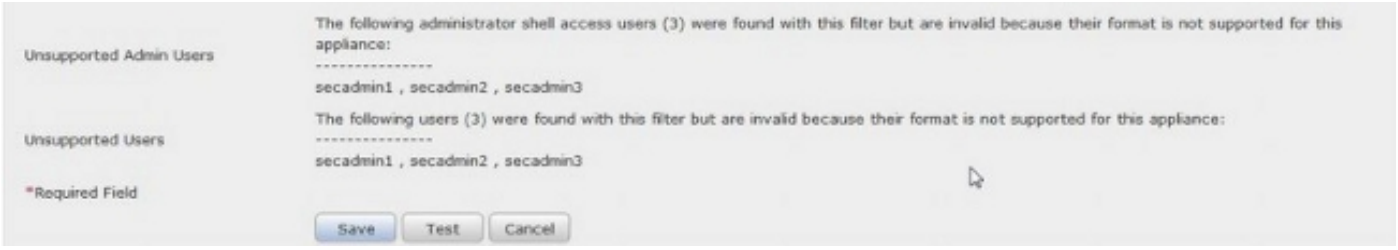
- **Aucun :** La signature de données n'est pas exigée afin de lier avec le serveur. Si le client demande des données signant, le serveur le prend en charge.
- **Signature Require** : À moins que le TLS \ SSL soit utilisé, l'option de signature de données de LDAP doit être négociée.

  Remarque: Le côté client ou le certificat de CA (CERT CA) n'est pas exigé pour des LDAP. Cependant, ce serait un niveau de sécurité supplémentaire de CERT CA est téléchargé à l'objet d'authentification.

6. Spécifiez le mappage d'attribut

- **Attribut UI Access** : sAMAccountName
- **Attribut d'Access de shell** : sAMAccountName

Conseil : Si vous rencontrez le message **sans support d'utilisateurs** dans la sortie de test, changez l'**attribut UI Access à l'userPrincipalName** et assurez-vous que **modèle de nom d'utilisateur** est placé à `%s`.



7. Configurez les **rôles d'accès contrôlé de groupe**

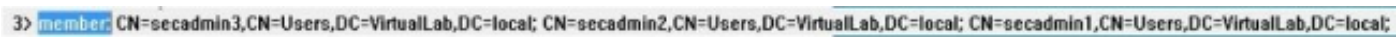
Sur **`ldp.exe, parcourez à`** chaque groupes et copiez en correspondant le DN de groupe à l'objet d'authentification comme affiché ci-dessous :

- **DN de groupe de Name> de <Group : dn> de <group**
- **Attribut de membre du groupe** : devrait toujours être le **membre**

Exemple :

- **DN de groupe d'administrateur :** Admins CN=DC, groupes de CN=Security, DC=VirtualLab, DC=local
- **Attribut de membre du groupe** : membre

Un groupe de sécurité d'AD fait suivi un attribut de **membre du** DN des utilisateurs de membre. L'attribut précédent de **membre de** nombre indique le nombre d'utilisateurs de membre.



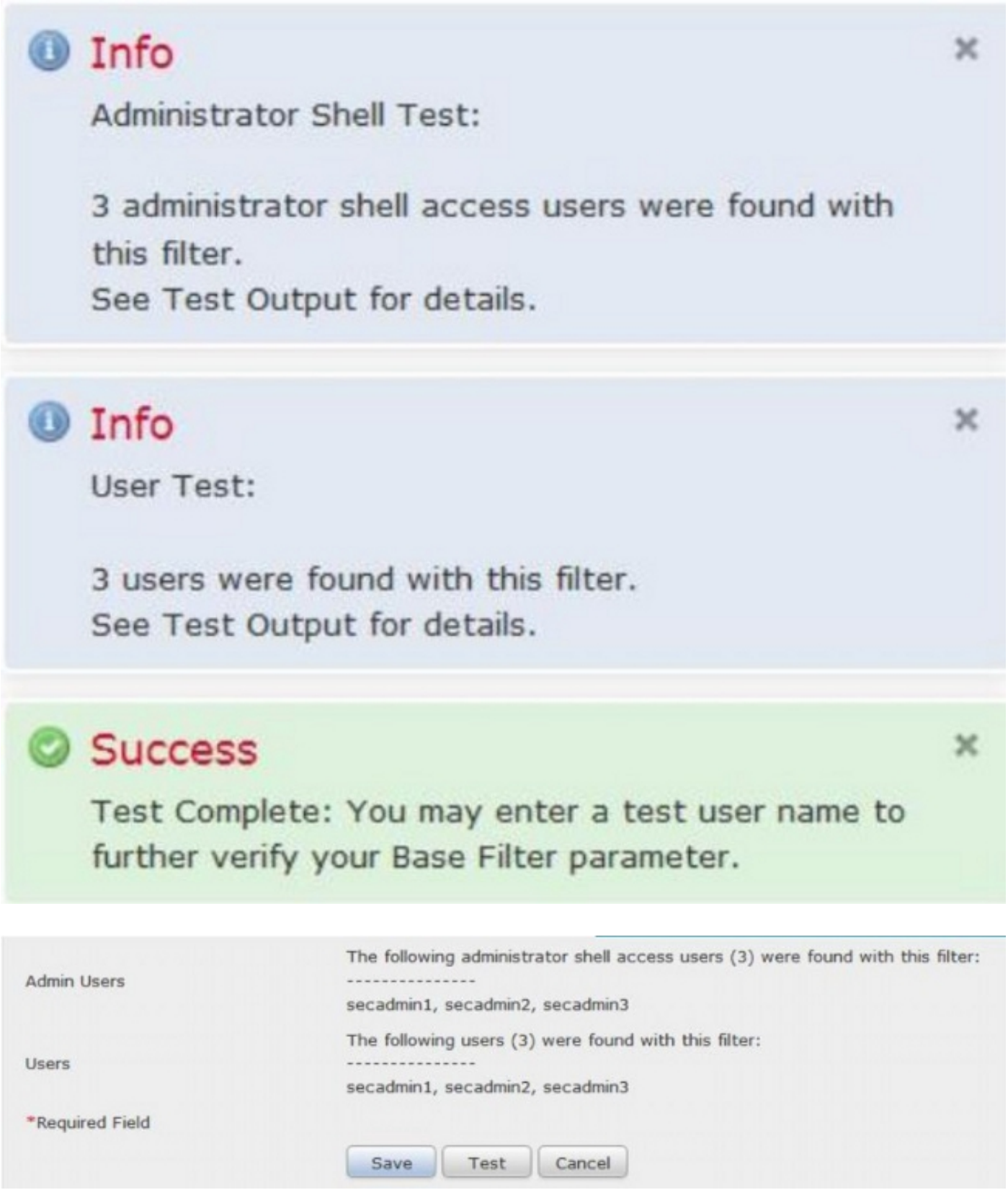
8. Sélectionnez **mêmes que le filtre de base** pour le filtre d'Access de shell, ou spécifient l'attribut de `memberOf` comme indiqué dans l'étape 5.

Filtre d'Access de shell : (`memberOf=<group DN>`)

Comme exemple,

Filtre d'Access de shell : `(utilisateurs de memberOf=CN=Shell, groupes de CN=Security, DC=VirtualLab, DC=local)`

9. Sauvegardez l'objet d'authentification et réalisez un essai. Un résultat d'essai réussi ressemble à ci-dessous :



10. Une fois que l'objet d'authentification passe le test, activez l'objet dans la stratégie de système et réappliquez la stratégie à votre appliance.

Document connexe

- Identifiez les attributs d'objet de LDAP de Répertoire actif pour la configuration d'objet

d'authentification