Configurazione dell'oggetto di autenticazione LDAP sul sistema FireSIGHT

Sommario

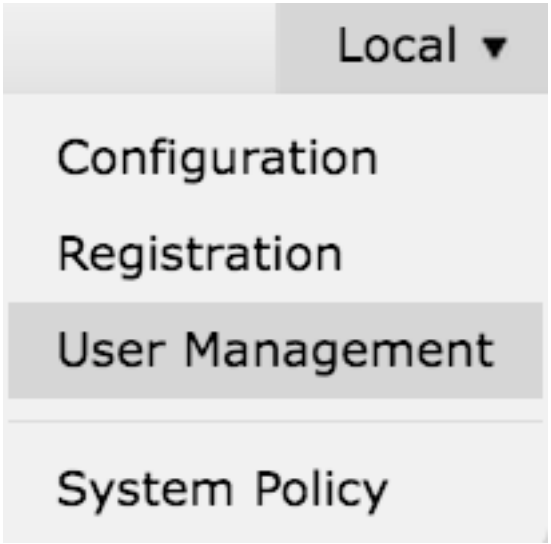
Introduzione

Gli oggetti di autenticazione sono profili server per server di autenticazione esterni, contenenti impostazioni di connessione e impostazioni di filtro di autenticazione per tali server. È possibile creare, gestire ed eliminare oggetti di autenticazione su un centro di gestione FireSIGHT. In questo documento viene descritto come configurare l'oggetto di autenticazione LDAP sul sistema FireSIGHT.

Configurazione di un oggetto di autenticazione LDAP

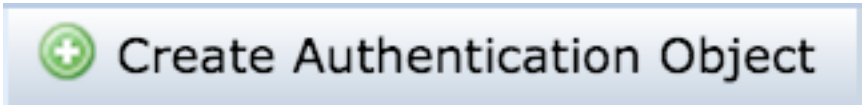
1. Accedere all'interfaccia utente web del centro di gestione FireSIGHT.

2. Passare a **Sistema > Locale > Gestione utenti**.



Selezionare la scheda **Autenticazione di accesso**.

Fare clic su **Crea oggetto autenticazione**.



3. Selezionare un **metodo di autenticazione** e un **tipo di server**.

- **Metodo di autenticazione**: LDAP
- **Nome:** *<Nome oggetto autenticazione>*
- **Tipo server**: Microsoft Active Directory

Nota: I campi contrassegnati da asterischi (*) sono obbligatori.

4. Specificare il nome host o l'indirizzo IP del server primario e di backup. Un server di backup è facoltativo. È tuttavia possibile utilizzare come server di backup qualsiasi controller di dominio all'interno dello stesso dominio.

Nota: Sebbene la porta LDAP sia l'impostazione predefinita della porta **389**, è possibile utilizzare un numero di porta non standard su cui il server LDAP è in ascolto.

5. Specificare i **parametri specifici LDAP** come indicato di seguito:

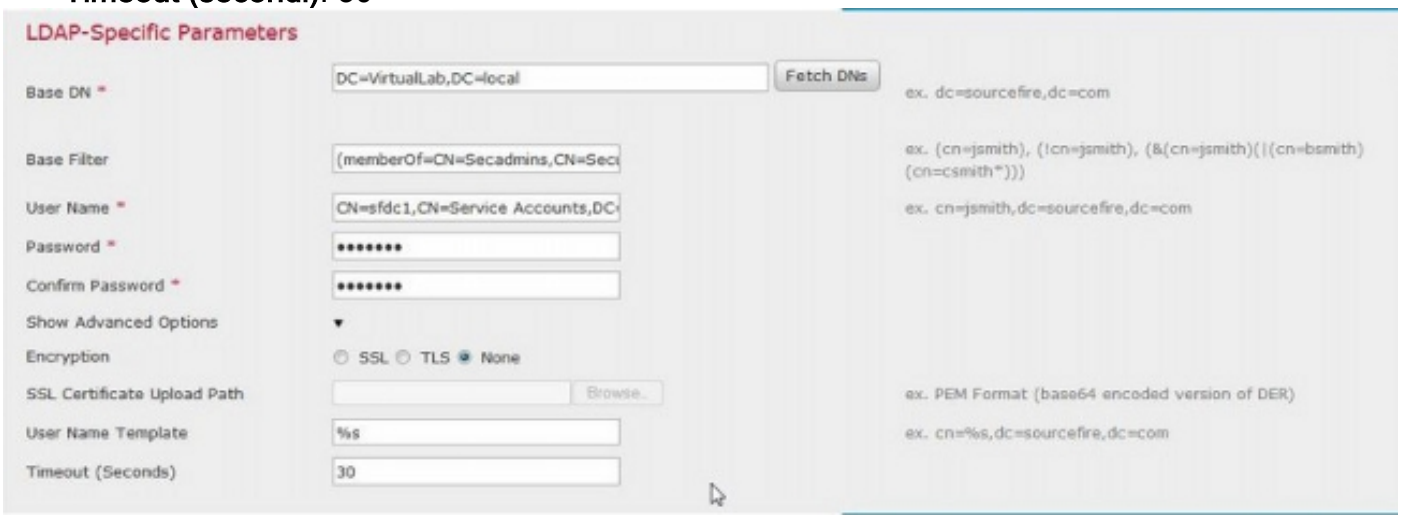
Suggerimento: Gli attributi utente, gruppo e unità organizzativa devono essere identificati prima di configurare **i parametri specifici di LDAP**. Leggere questo documento per identificare gli attributi dell'oggetto LDAP di Active Directory per la configurazione dell'oggetto di autenticazione.

- **DN base** - DN di dominio o unità organizzativa specifica
- **Filtro di base**: DN del gruppo a cui appartengono gli utenti.
- **Nome utente** - Account di rappresentazione per il controller di dominio
- **Password**: *<password>*
- **Conferma password**: *<password>*

Opzioni avanzate:

- **Crittografia**: SSL, TLS o nessuno
- **Percorso di caricamento certificato SSL**: Carica la certificazione CA (facoltativo)
- **Modello nome utente**: %s

- **Timeout (secondi)**: 30



Nell'impostazione dei criteri di protezione del dominio di Active Directory, se il **requisito di firma del server LDAP** è impostato su **Richiedi firma**, è necessario utilizzare SSL o TLS.

Requisito firma server LDAP

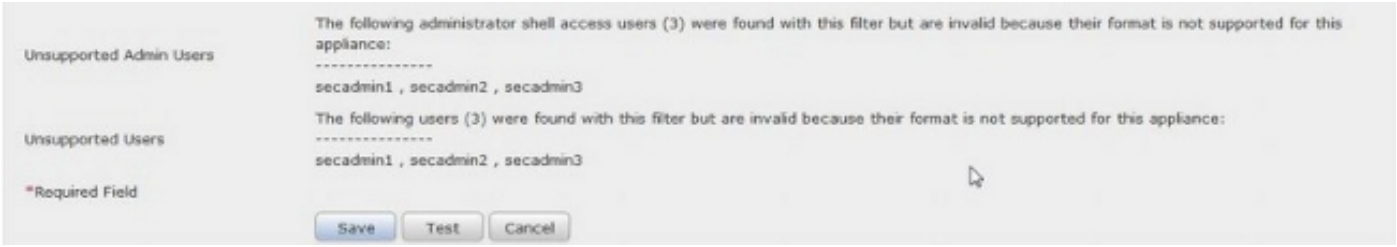
- **Nessuna:** La firma dei dati non è necessaria per il binding al server. Se il client richiede la firma dei dati, il server la supporta.
- **Richiedi firma**: A meno che non si utilizzi TLS\SSL, l'opzione di firma dei dati LDAP deve essere negoziata.

  Nota: Il certificato CA o lato client non è richiesto per LDAPS. Si tratterebbe tuttavia di un livello di protezione aggiuntivo del certificato CA caricato nell'oggetto di autenticazione.

6. Specifica mapping attributi

- **Attributo di accesso interfaccia utente**: NomeAccountAMA
- **Attributo di accesso alla shell**: NomeAccountAMA

Suggerimento: Se nell'output del test viene visualizzato il messaggio Utenti non supportati, modificare l'**attributo di accesso dell'interfaccia utente** in **userPrincipalName** e assicurarsi che il **modello Nome utente** sia impostato su **%s**.



7. Configurare i **ruoli di accesso controllato a livello di gruppo**

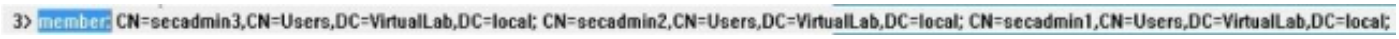
In **ldp.exe**, passare a ogni gruppo e copiare il DN del gruppo corrispondente nell'oggetto di autenticazione come illustrato di seguito:

- **DN gruppo <Nome gruppo>: <dn gruppo>**
- **Attributo membro gruppo**: deve essere sempre **membro**

Esempio:

- **DN gruppo amministratori:** CN=amministratori controller di dominio,CN=Gruppi di sicurezza,DC=VirtualLab,DC=locale
- **Attributo membro gruppo**: membro

Un gruppo di sicurezza AD ha un attributo **member** seguito dal DN degli utenti membri. L'attributo **membro** numero precedente indica il numero di utenti membri.



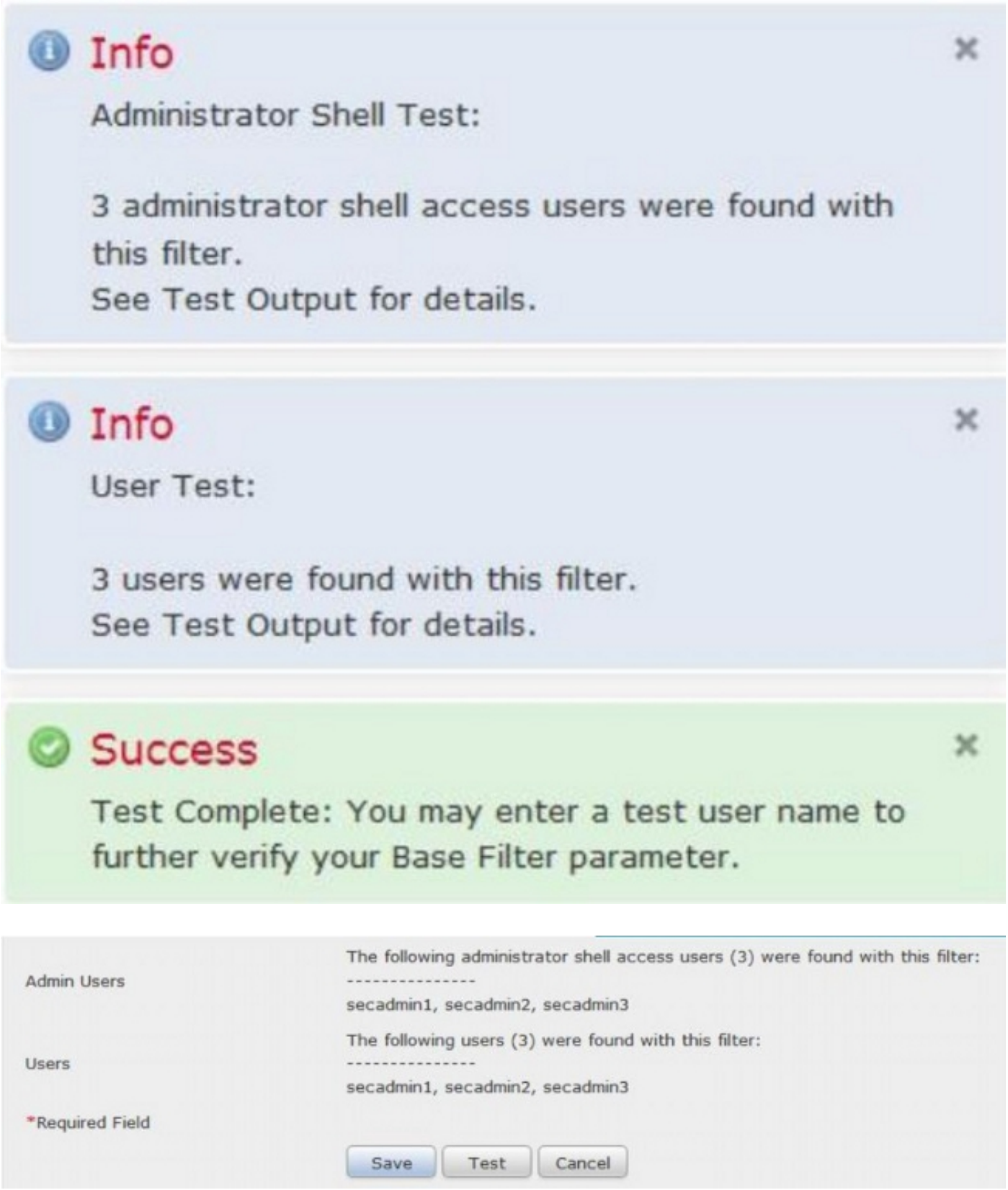
8. Selezionare **Uguale a filtro base** per Filtro accesso shell o specificare l'attributo memberOf come indicato nel passaggio 5.

Filtro accesso shell: (memberOf=<DN gruppo>)

Ad esempio,

Filtro accesso shell: (memberOf=CN=Shell users,CN=Security Groups,DC=VirtualLab,DC=local)

9. Salvare l'oggetto di autenticazione ed eseguire un test. Di seguito è riportato un risultato positivo del test:



10. Dopo che l'oggetto di autenticazione ha superato il test, abilitarlo in Criteri di sistema e riapplicare il criterio all'accessorio.

Documenti correlati

- Identificare gli attributi dell'oggetto LDAP di Active Directory per la configurazione dell'oggetto

di autenticazione