Configurer FMC et FTD avec LDAP pour l'authentification externe

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
- Diagramme du réseau
- Configurer
  - Configuration LDAP de base dans l'interface utilisateur FMC
  - Accès Shell pour les utilisateurs externes
  - Authentification externe vers FTD
  - Rôles utilisateur
  - SSL ou TLS
- Vérifier
  - Base de recherche de test
  - Tester l'intégration LDAP
- Dépannage
  - Comment FMC/FTD et LDAP interagissent-ils pour télécharger des utilisateurs ?
  - Comment FMC/FTD et LDAP interagissent-ils pour authentifier une demande de connexion utilisateur ?
  - SSL ou TLS ne fonctionne pas comme prévu
- Informations connexes

Introduction

Ce document décrit comment activer l'authentification externe LDAP (Microsoft Lightweight Directory Access Protocol) avec Cisco FMC et FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Threat Defense (FTD)
- Cisco Firepower Management Center (FMC)
- LDAP Microsoft

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- TD 6.5.0-123
- FMC 6.5.0-115
- Microsoft Server 2012

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

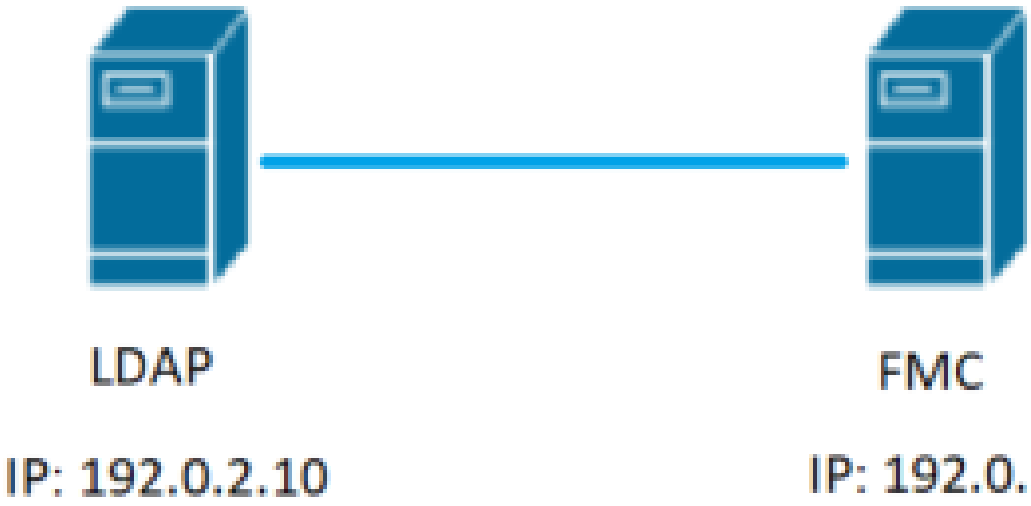
Informations générales

Le FMC et les périphériques gérés incluent un compte d'administrateur par défaut pour l'accès à la gestion. Vous pouvez ajouter des comptes d'utilisateurs personnalisés sur le FMC et sur les périphériques gérés, soit en tant qu'utilisateurs internes, soit, s'ils sont pris en charge pour votre modèle, en tant qu'utilisateurs externes sur un serveur LDAP ou RADIUS. L'authentification utilisateur externe est prise en charge pour FMC et FTD.

· Utilisateur interne : le périphérique FMC/FTD vérifie l'authentification des utilisateurs dans une base de données locale.

· Utilisateur externe : si l'utilisateur n'est pas présent dans la base de données locale, les informations système d'un serveur d'authentification LDAP ou RADIUS externe renseignent sa base de données utilisateur.

Diagramme du réseau



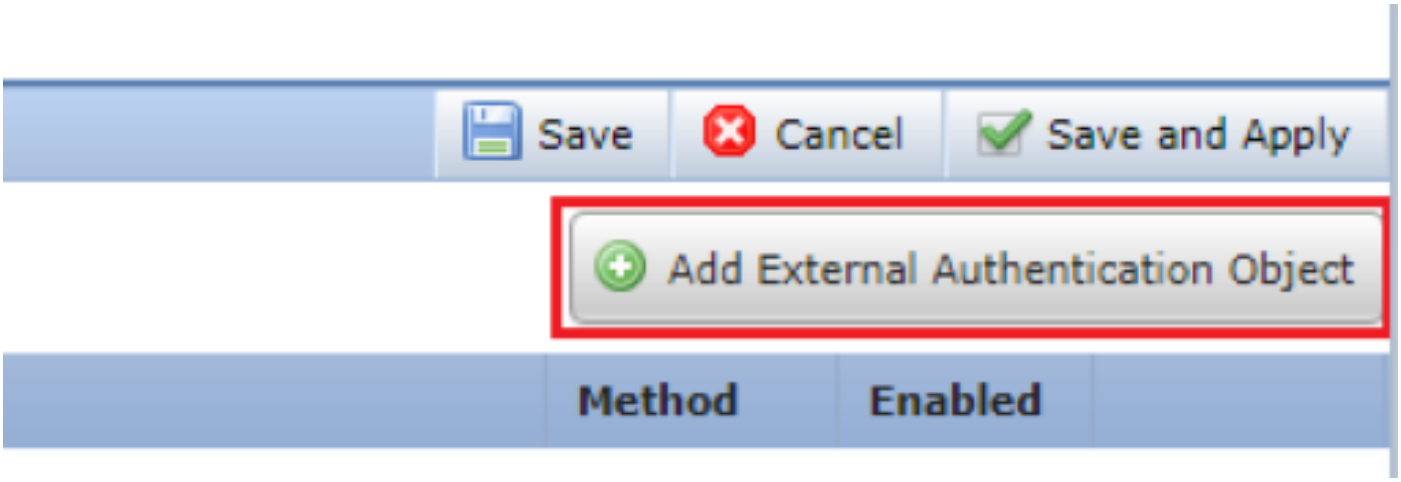
Configurer

Configuration LDAP de base dans l'interface utilisateur FMC

Étape 1. Accédez àSystem > Users > External Authentication:

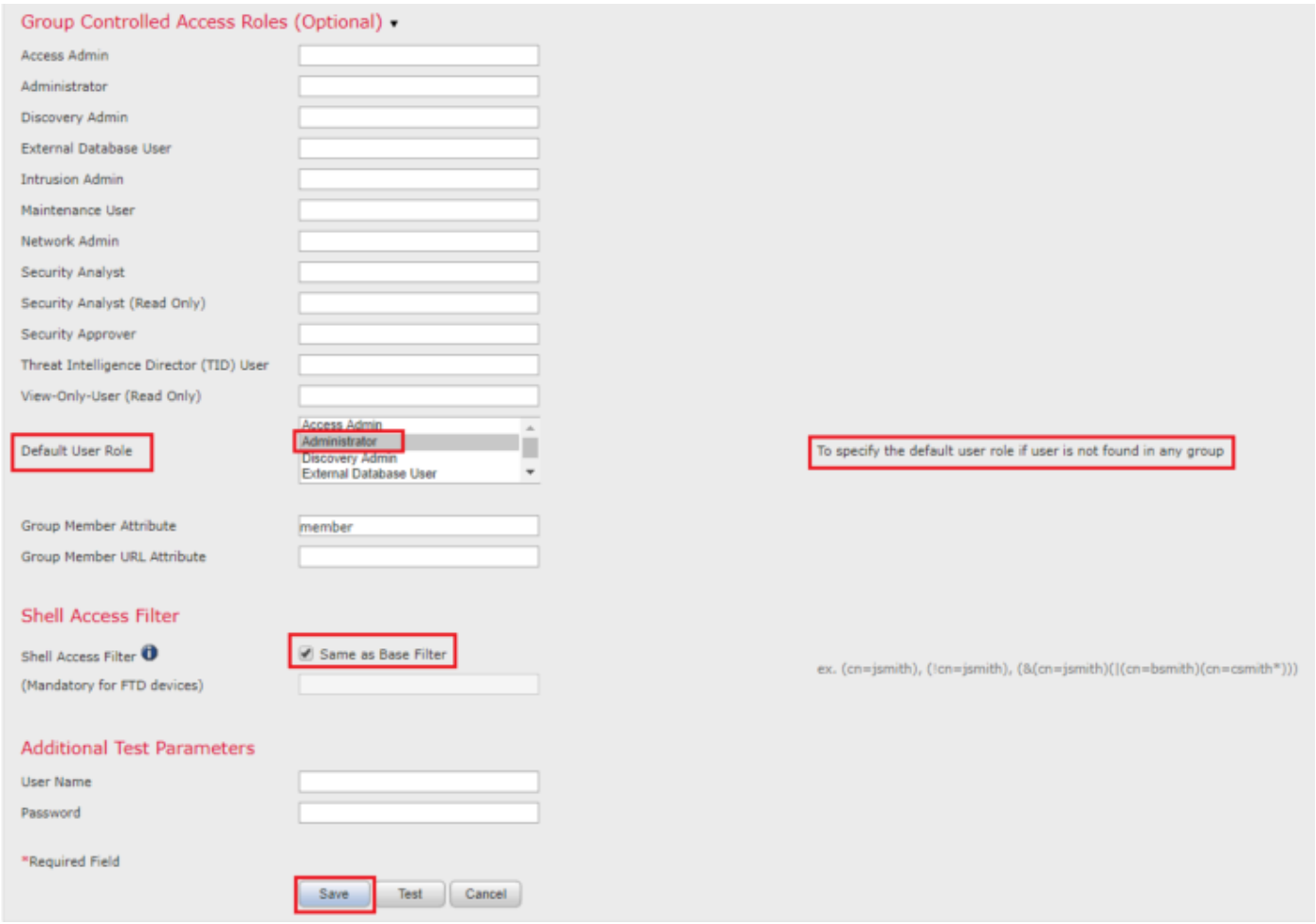


Étape 2. ChoisissezAdd External Authentication Object:



Étape 3. Renseignez les champs obligatoires :





Étape 4. Activation de l'External Authenticationobjet et enregistrement :



Accès Shell pour les utilisateurs externes

Le FMC prend en charge deux utilisateurs d'administration interne différents : un pour l'interface Web et un autre avec un accès CLI. Cela signifie qu'il existe une distinction claire entre les utilisateurs autorisés à accéder à l'interface utilisateur graphique et ceux autorisés à accéder à l'interface de ligne de commande. Au moment de l'installation, le mot de passe de l'utilisateur admin par défaut est synchronisé afin d'être le même sur l'interface graphique et l'interface de ligne de commande, cependant, ils sont suivis par différents mécanismes internes, et peuvent éventuellement être différents.

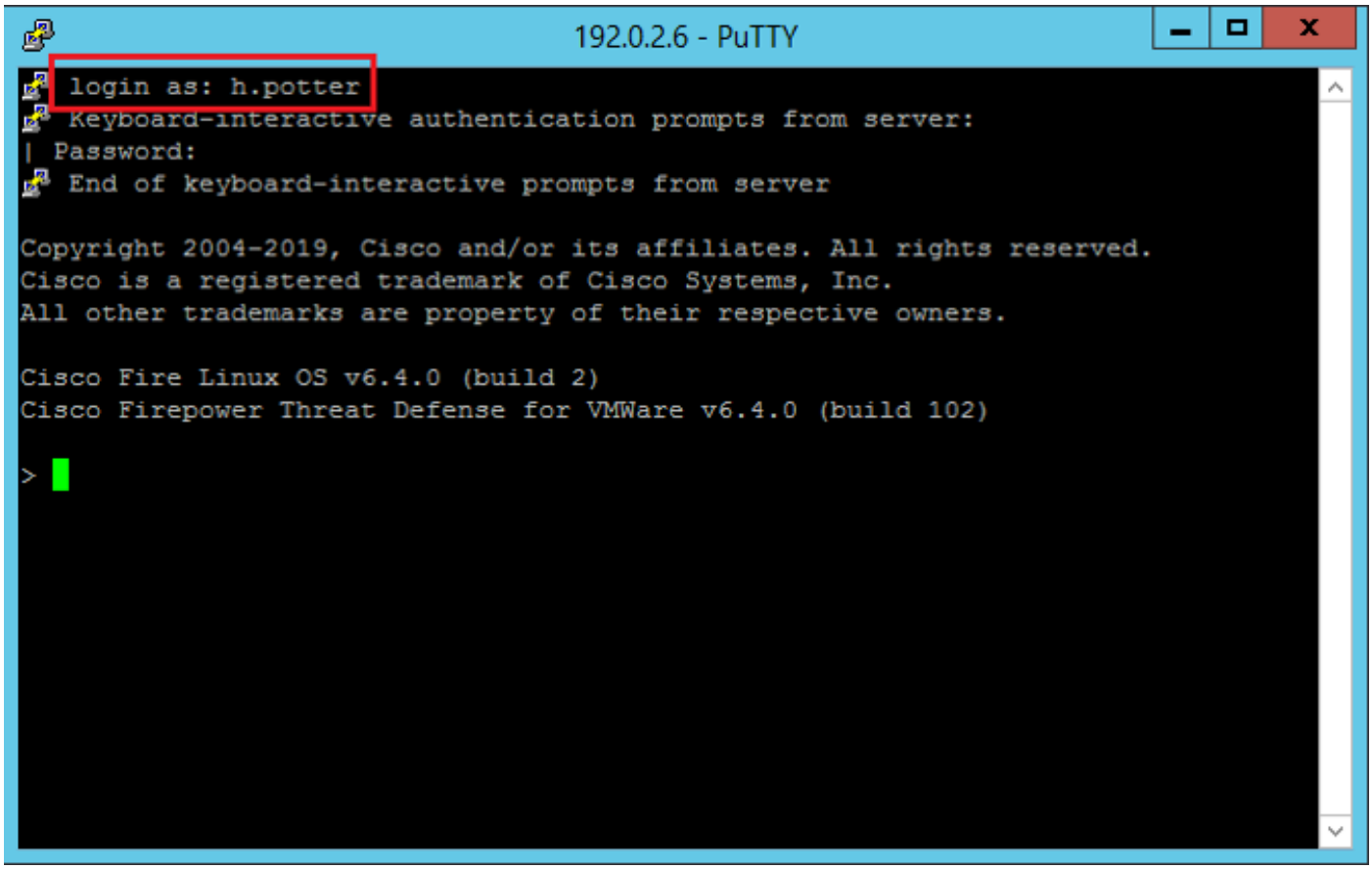
Les utilisateurs externes LDAP doivent également disposer d'un accès shell.

Étape 1. Naviguez jusqu'à`System > Users > External Authentication`et cliquez sur la zone de`Shell Authentication` liste déroulante comme on le voit dans l'image et enregistrez :



Étape 2 : déploiement des modifications dans FMC

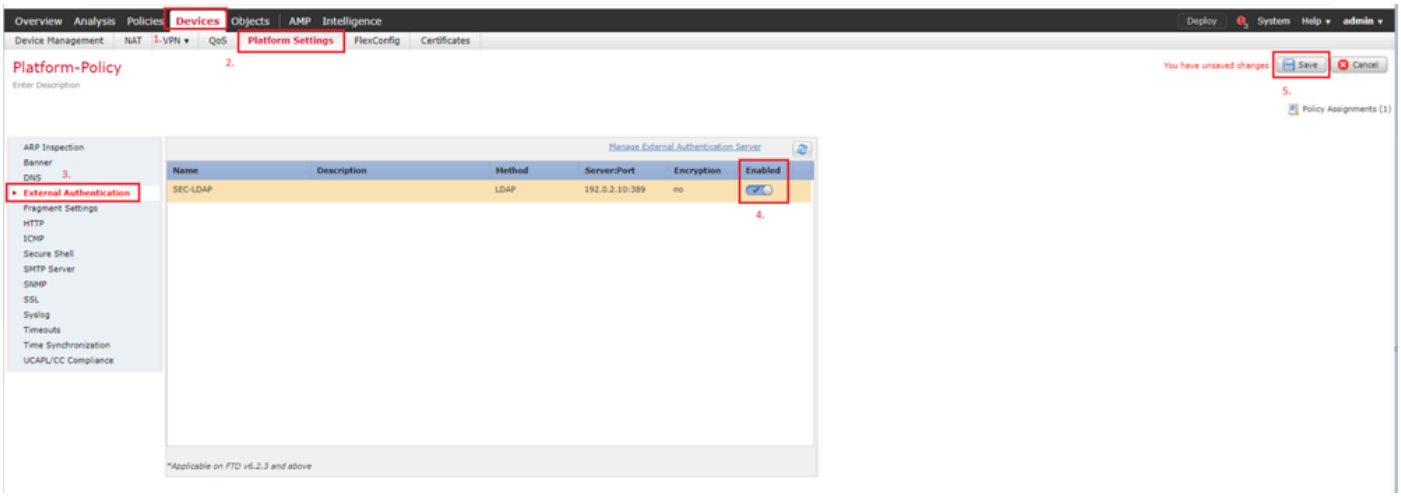
Une fois que l'accès shell pour les utilisateurs externes est configuré, la connexion via SSH est activée comme indiqué dans l'image :



Authentification externe vers FTD

L'authentification externe peut être activée sur FTD.

Étape 1. Accédez àDevices > Platform Settings > External Authentication. Cliquez surEnabledet enregistrez :



Rôles utilisateur

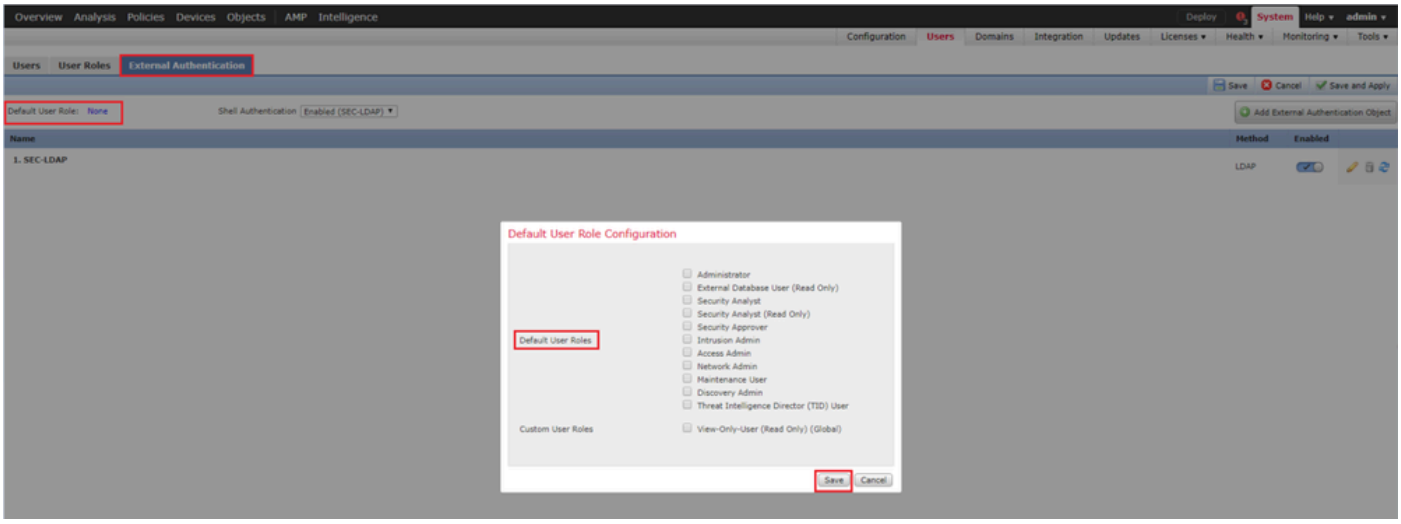
Les privilèges utilisateur sont basés sur le rôle utilisateur attribué. Vous pouvez également créer des rôles d'utilisateur personnalisés avec des privilèges d'accès adaptés aux besoins de votre organisation ou utiliser des rôles prédéfinis tels que Analyste de sécurité et Administrateur de découverte.

Il existe deux types de rôles d'utilisateur :

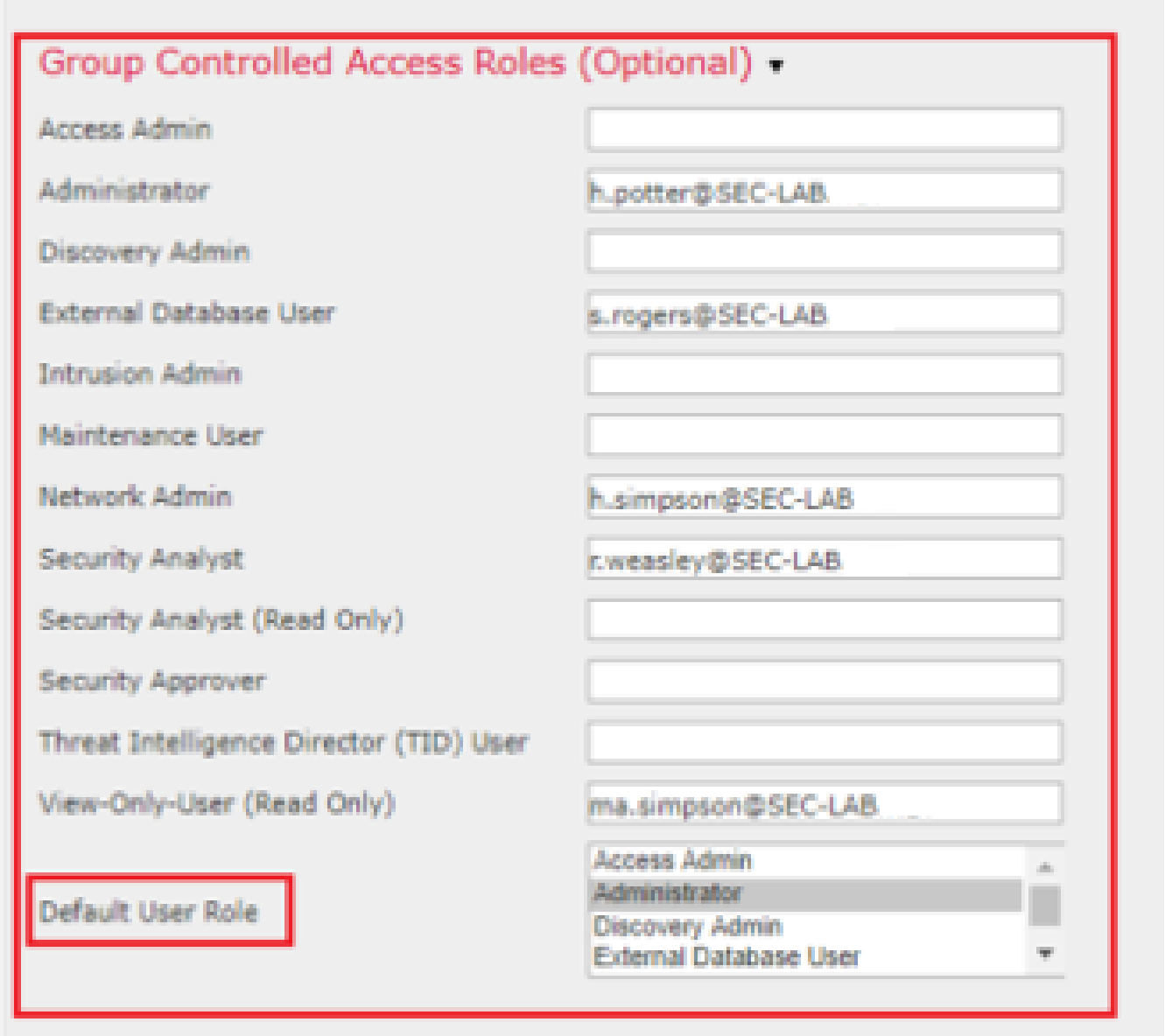
1. Rôles utilisateur de l'interface Web
2. Rôles utilisateur CLI

Pour obtenir la liste complète des rôles prédéfinis et plus d'informations, reportez-vous à : Rôles d'utilisateur.

Afin de configurer un rôle d'utilisateur par défaut pour tous les objets d'authentification externes, accédez àSystem > Users > External Authentication > Default User Role. Choisissez le rôle d'utilisateur par défaut que vous souhaitez affecter et cliquez surSave.



Afin de choisir un rôle d'utilisateur par défaut ou d'attribuer des rôles spécifiques à des utilisateurs spécifiques dans un groupe d'objets particulier, vous pouvez choisir l'objet et naviguer jusqu'àGroup Controlled Access Rolescomme indiqué dans l'image :



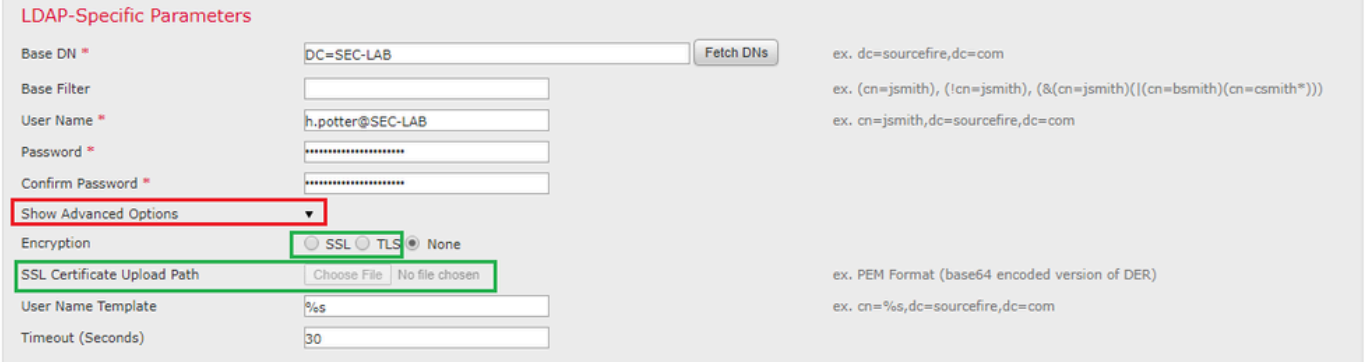
SSL ou TLS

DNS doit être configuré dans le FMC. En effet, la valeur Objet du certificat doit correspondre à la Authentication Object Primary Server Hostname. Une fois le protocole LDAP sécurisé configuré, les captures de paquets n'affichent plus les requêtes de liaison en texte clair.

SSL change le port par défaut en 636 et TLS le garde en 389.

Remarque : Le chiffrement TLS nécessite un certificat sur toutes les plates-formes. Pour SSL, le FTD nécessite également un certificat. Pour les autres plates-formes, SSL ne nécessite pas de certificat. Cependant, il est recommandé de toujours télécharger un certificat pour SSL afin d'empêcher les attaques de l'homme du milieu.

Étape 1. Accédez àDevices > Platform Settings > External Authentication > External Authentication ObjectOptions avancées et saisissez les informations SSL/TLS :



Étape 2. Téléchargez le certificat de l'autorité de certification qui a signé le certificat du serveur. Le certificat doit être au format PEM.



Étape 3 : enregistrement de la configuration

Vérifier

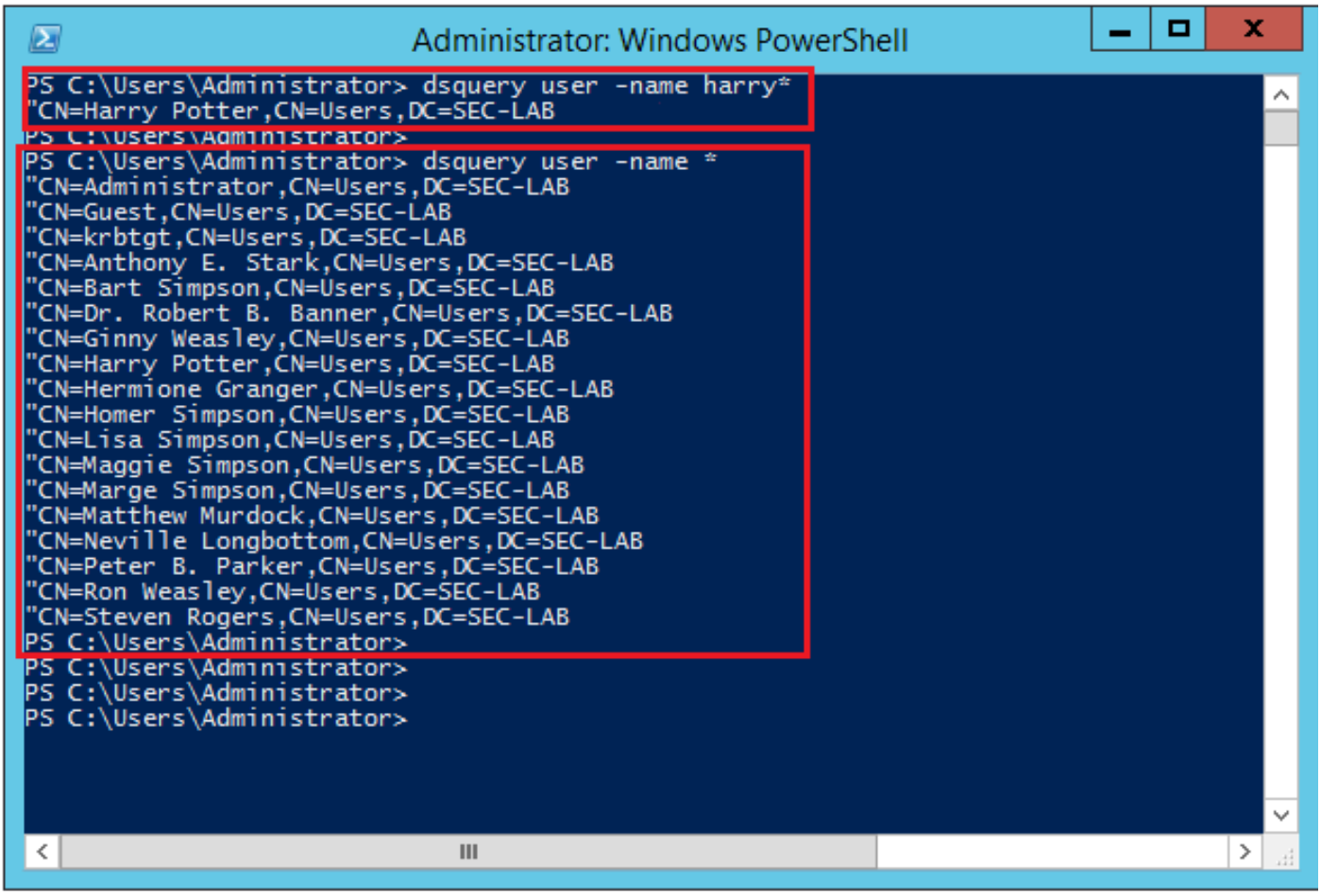
Base de recherche de test

Ouvrez une invite de commandes Windows ou PowerShell où LDAP est configuré et tapez la commande :dsquery user -name

.

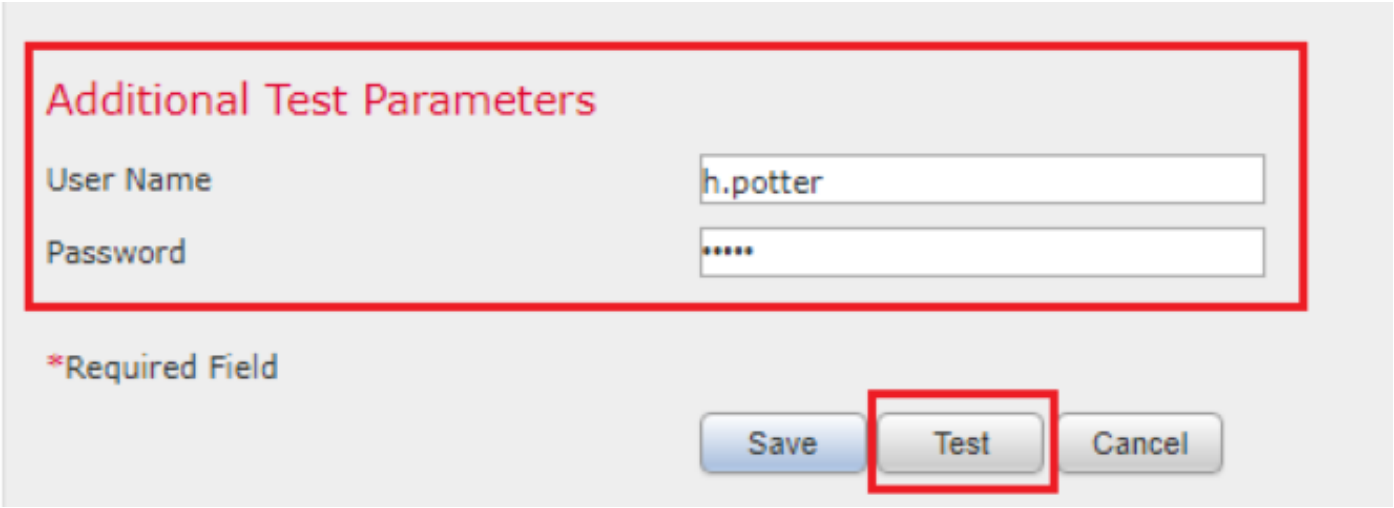
Exemple :

```
PS C:\Users\Administrator> dsquery user -name harry*
PS C:\Users\Administrator> dsquery user -name *
```

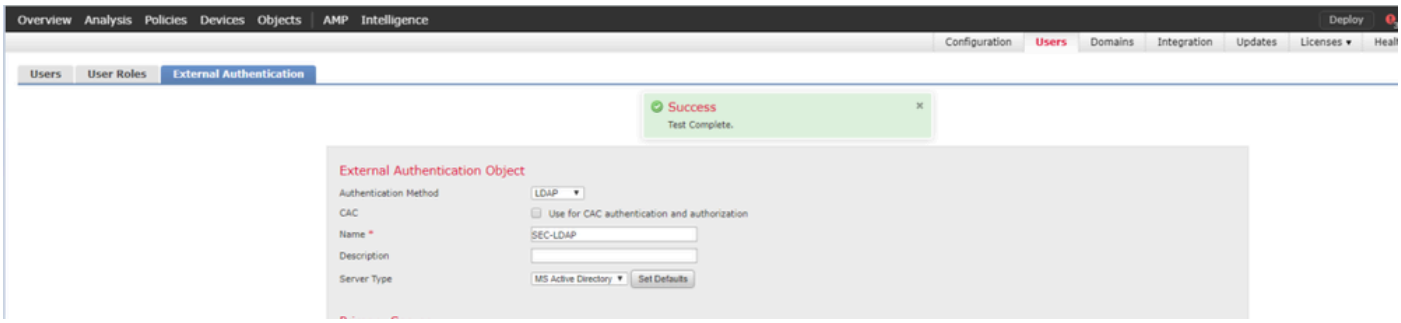


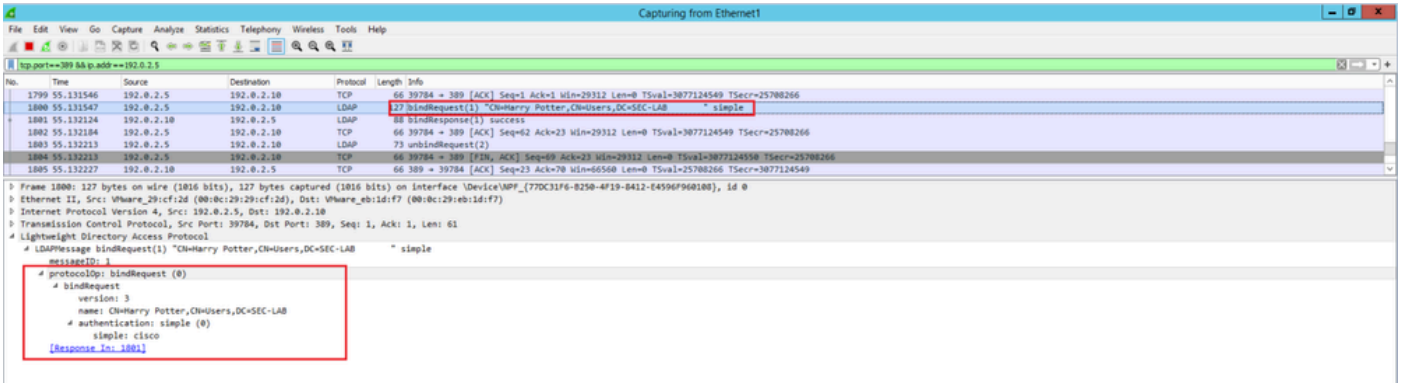
Tester l'intégration LDAP

Accédez àSystem > Users > External Authentication > External Authentication Object. Au bas de la page, il y a une Additional Test Parameters section telle qu'elle apparaît dans l'image :



Choisissez Test afin de voir les résultats.





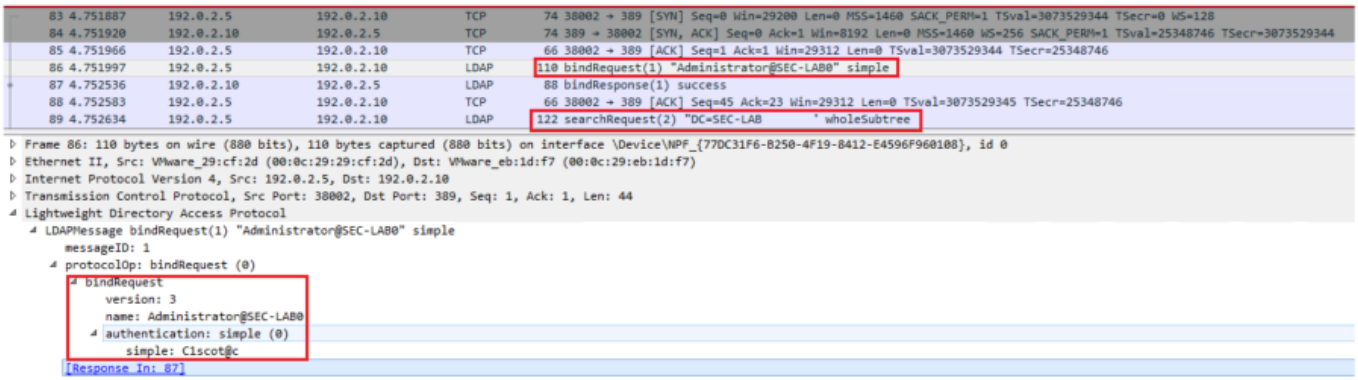
Dépannage

Comment FMC/FTD et LDAP interagissent-ils pour télécharger des utilisateurs ?

Pour que FMC puisse extraire des utilisateurs d'un serveur Microsoft LDAP, il doit d'abord envoyer une demande de liaison sur le port 389 ou 636 (SSL) avec les informations d'identification de l'administrateur LDAP. Une fois que le serveur LDAP est en mesure d'authentifier FMC, il répond avec un message de réussite. Enfin, FMC peut effectuer une requête avec le message de requête de recherche comme décrit dans le schéma :

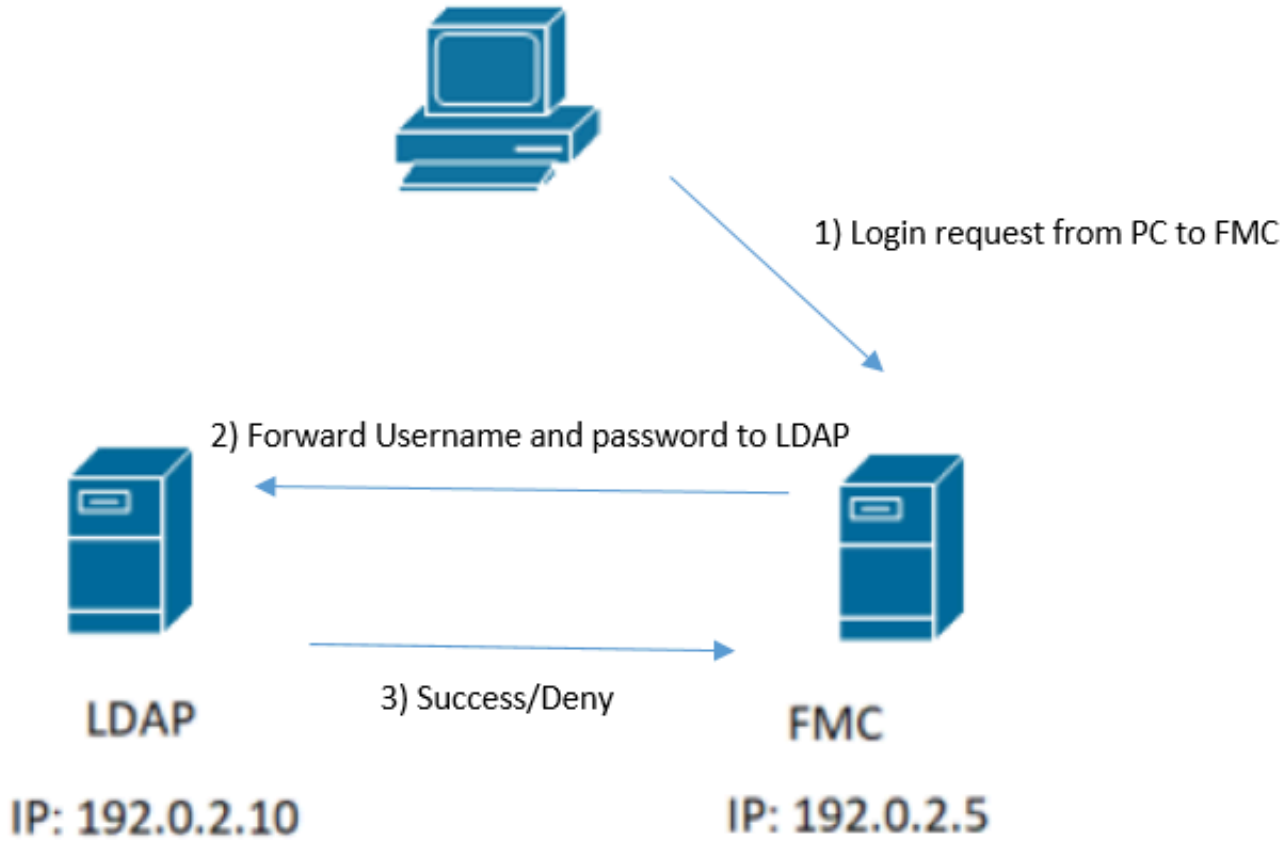
<< --- FMC sends: bindRequest(1) "Administrator@SEC-LAB0" simple LDAP must respond with: bindResponse(1) success --- >> << --- FMC sends: searchRequest(2) "DC=SEC-LAB,DC=NET" wholeSubtree

Notez que l'authentification envoie des mots de passe en clair par défaut :

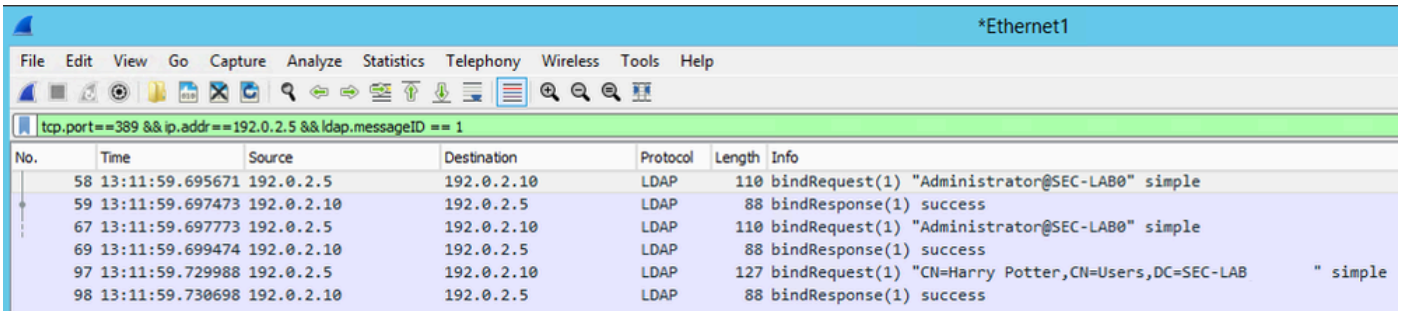


Comment FMC/FTD et LDAP interagissent-ils pour authentifier une demande de connexion utilisateur ?

Pour qu'un utilisateur puisse se connecter à FMC ou FTD alors que l'authentification LDAP est activée, la demande de connexion initiale est envoyée à Firepower, mais le nom d'utilisateur et le mot de passe sont transférés à LDAP pour une réponse de réussite/refus. Cela signifie que FMC et FTD ne conservent pas les informations de mot de passe localement dans la base de données et attendent plutôt la confirmation de LDAP sur la façon de procéder.







Si le nom d'utilisateur et le mot de passe sont acceptés, une entrée est ajoutée dans l'interface utilisateur graphique Web, comme indiqué dans l'image :



Exécutez la commande show user in FMC CLISH afin de vérifier les informations utilisateur : > show user

La commande affiche des informations de configuration détaillées pour le ou les utilisateurs spécifiés. Ces valeurs s'affichent :

Log in : nom de connexion

UID : l'ID utilisateur numérique
Auth (local ou distant) : mode d'authentification de l'utilisateur
Access (Basic ou Config) : niveau de privilège de l'utilisateur
Enabled (Enabled ou Disabled) : indique si l'utilisateur est actif
Reset (Yes ou No) : indique si l'utilisateur doit modifier le mot de passe lors de la prochaine connexion
Exp (Never ou a number) : nombre de jours avant la modification du mot de passe de l'utilisateur
Warn (N/A ou un nombre) : nombre de jours qu'un utilisateur reçoit pour modifier son mot de passe avant qu'il expire
Str (Yes or No) : indique si le mot de passe de l'utilisateur doit répondre aux critères de vérification de la puissance
Lock (Yes ou No) : indique si le compte de l'utilisateur a été verrouillé en raison d'un trop grand nombre d'échecs de connexion
Max (N/A ou un nombre) : nombre maximal d'échecs de connexion avant le verrouillage du compte de l'utilisateur

SSL ou TLS ne fonctionne pas comme prévu

Si vous n'activez pas DNS sur les FTD, vous pouvez voir des erreurs dans le journal en queue de pie qui suggèrent que LDAP est inaccessible :

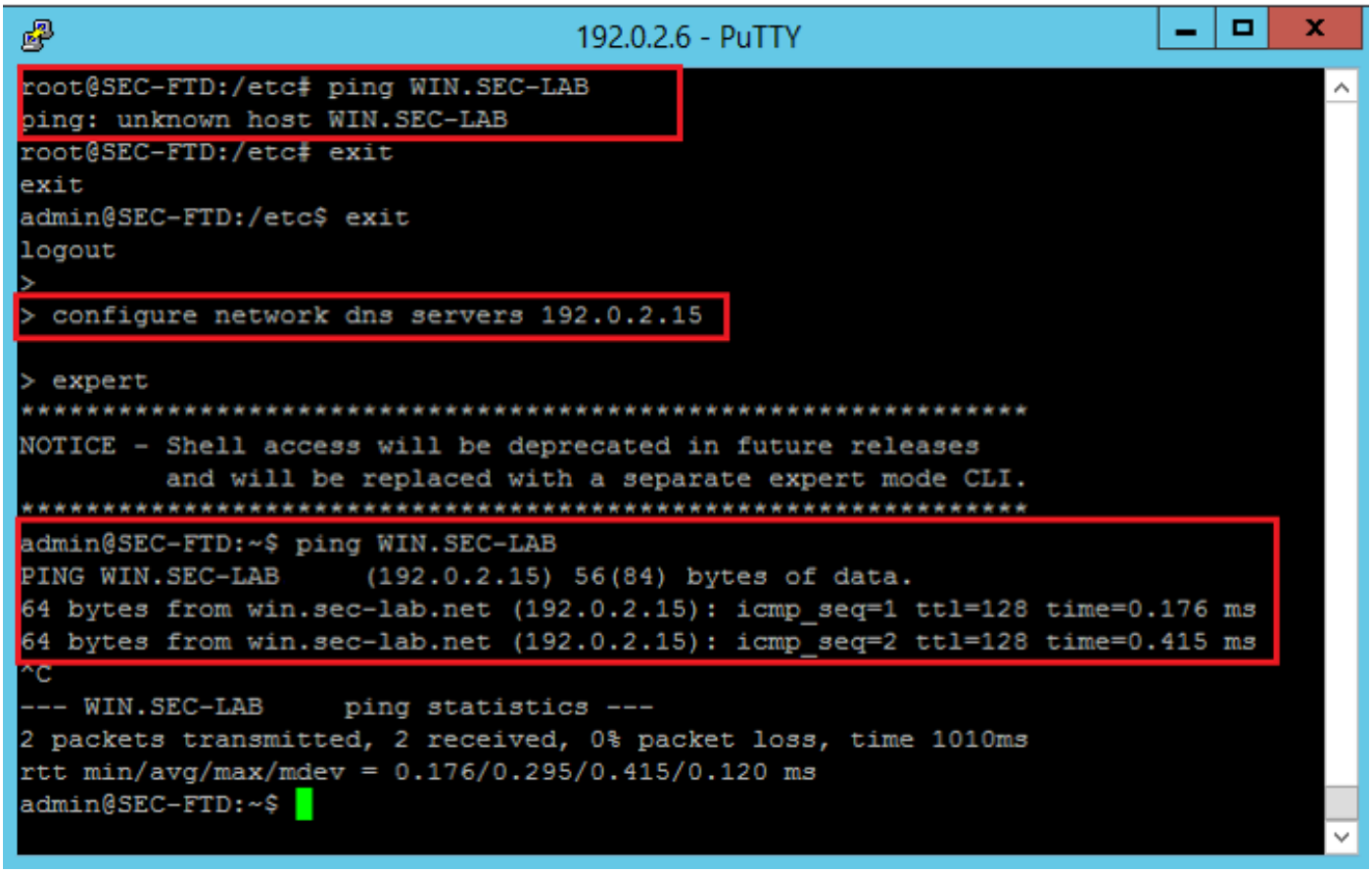
```
root@SEC-FMC:/$ sudo cd /var/common
root@SEC-FMC:/var/common$ sudo pigtail
```

```
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_unix(sshd:auth): authentication failure; logname= uid=0 e
MSGS: 03-05 14:35:31 SEC-FTD sshd[10174]: pam_ldap: ldap_starttls_s: Can't contact LDAP server
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: PAM: Authentication failure for h.potter from 192.0.2.
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Failed keyboard-interactive/pam for h.potter from 192.0.2.15
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: error: maximum authentication attempts exceeded for h.potter
MSGS: 03-05 14:35:33 SEC-FTD sshd[10138]: Disconnecting authenticating user h.potter 192.0.2.15 port 61
```

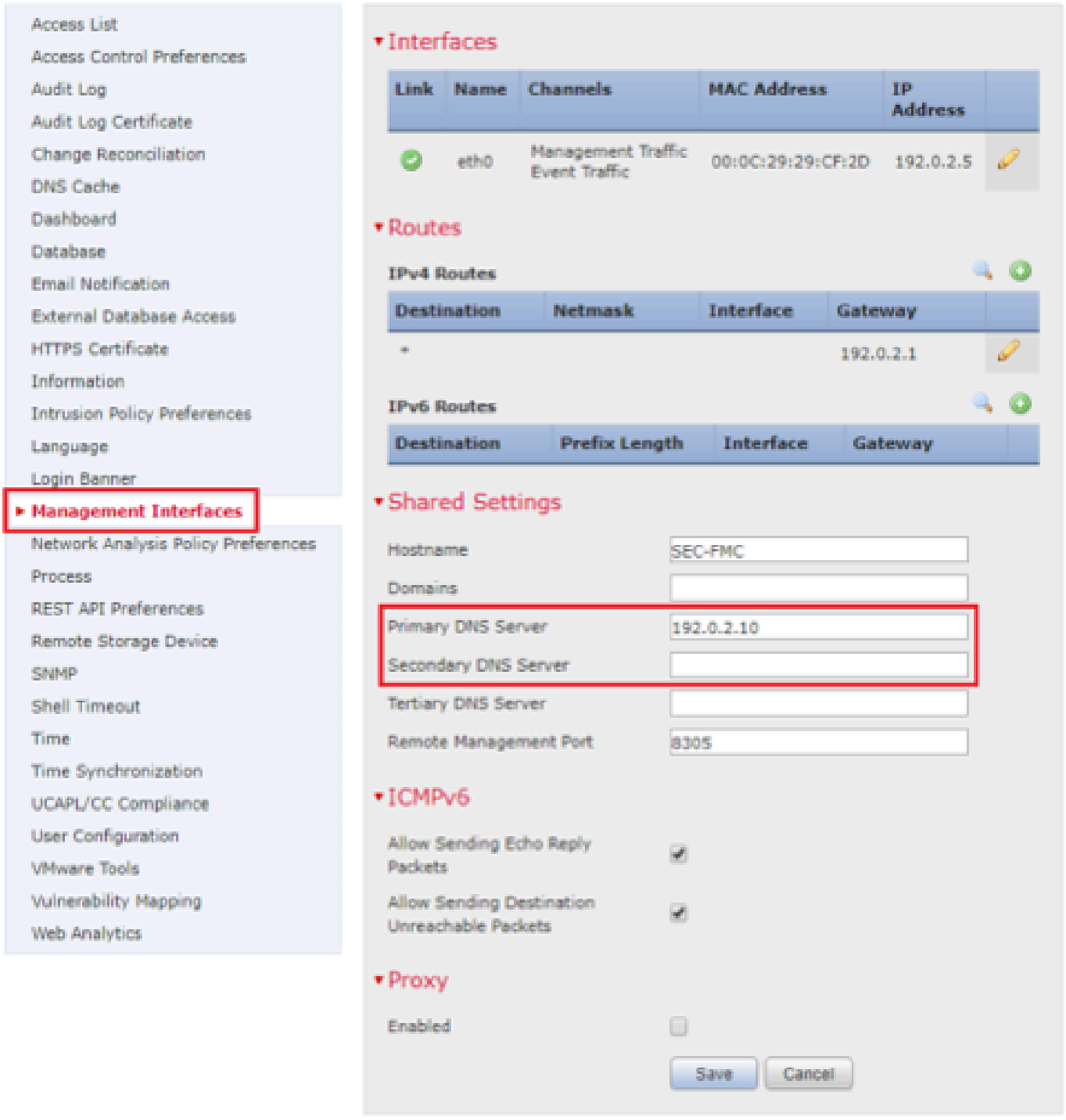
Assurez-vous que Firepower est en mesure de résoudre le nom de domaine complet (FQDN) des serveurs LDAP. Si ce n'est pas le cas, ajoutez le DNS correct tel qu'il apparaît dans l'image.

DFT : Accédez à FTD CLISH et exécutez la commande suivante : > configure network dns servers

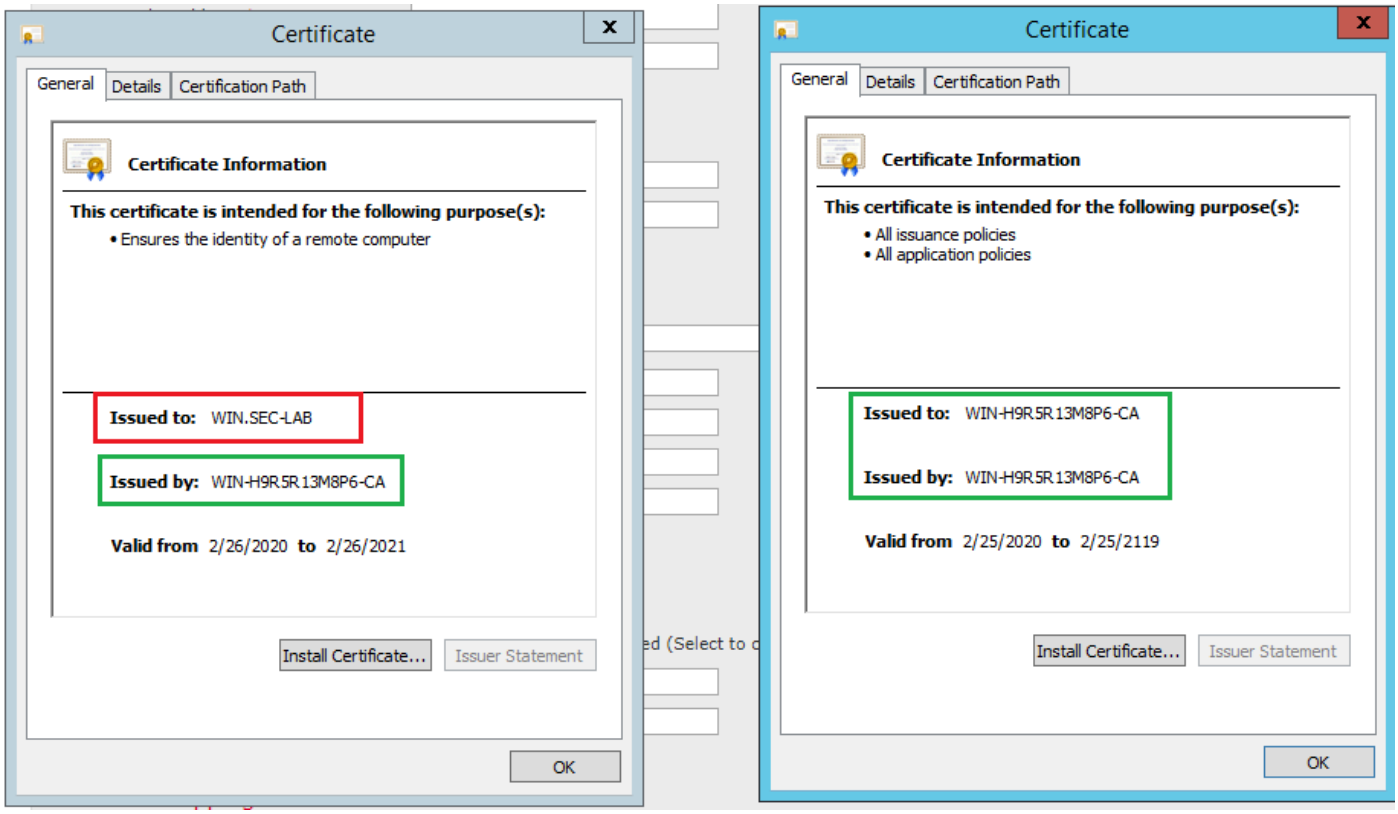
.



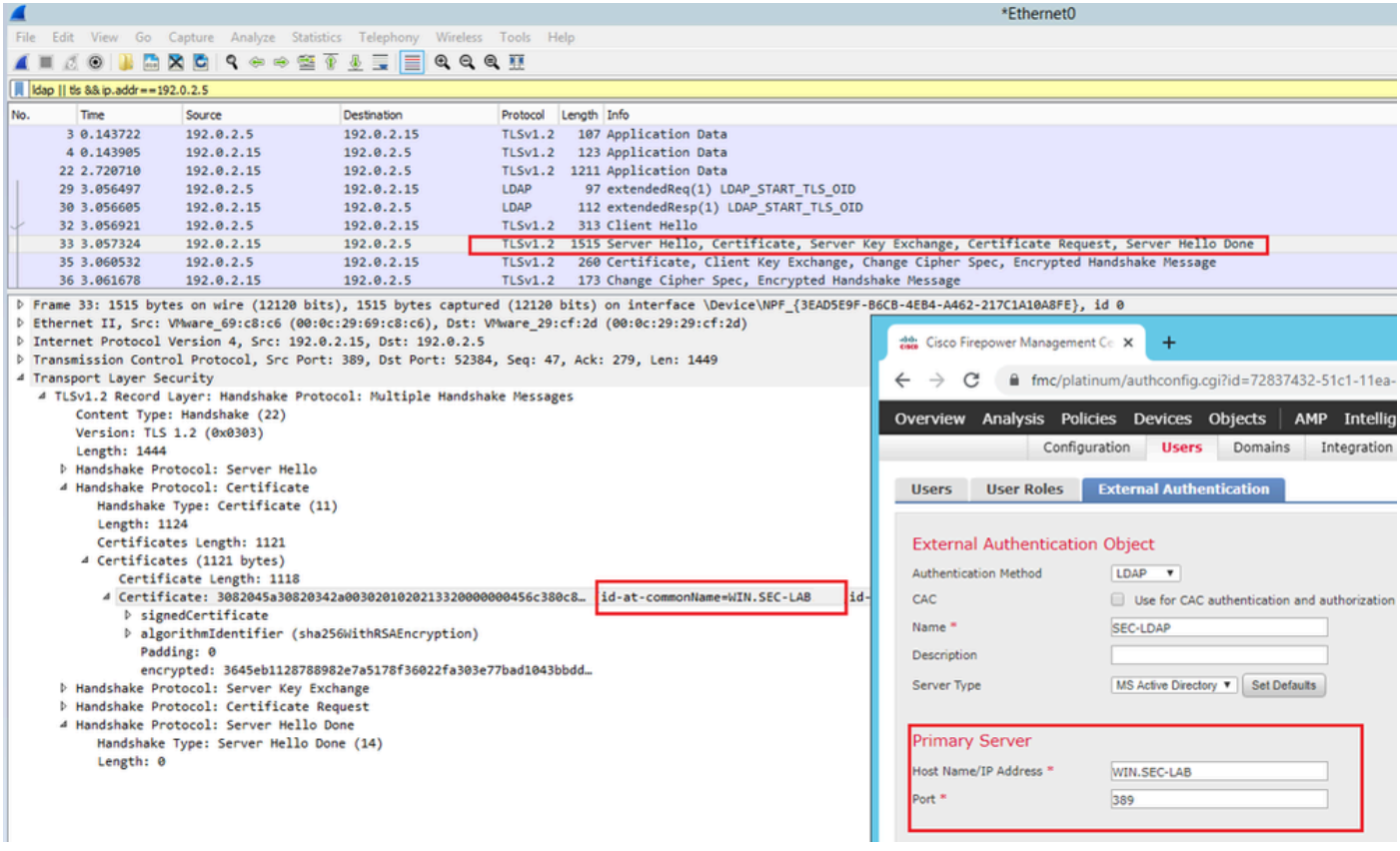
FMC : SélectionnezSystem > Configuration, puis Interfaces de gestion comme indiqué dans l'image :



Assurez-vous que le certificat téléchargé vers FMC est le certificat de l'autorité de certification qui a signé le certificat de serveur du LDAP, comme illustré dans l'image :



Utilisez les captures de paquets afin de confirmer que le serveur LDAP envoie les informations correctes :



Informations connexes

- Comptes d'utilisateurs pour accès à la gestion
- Vulnérabilité de contournement de l'authentification par protocole d'accès annuaire léger de Cisco Firepower Management Center
- Configuration de l'objet d'authentification LDAP sur le système FireSIGHT
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.