

Configuration de LDAP de Cisco C880 utilisant la Microsoft Active Directory

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Implémentation de LDAP](#)

[Configurez](#)

[Créez les comptes spéciaux](#)

[Service d'annuaire](#)

[Créez le groupe d'utilisateurs](#)

[Active Directory](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

Introduction

Ce document décrit un exemple de configuration afin d'obtenir le Protocole LDAP (Lightweight Directory Access Protocol) pour travailler au C880 avec l'utilisation de la Microsoft Active Directory (AD). L'implémentation de LDAP C880 est seule d'une manière que l'utilisateur doit être en commun le nom (NC) = des utilisateurs. Il y a également quelques configurations requises spécifiques pour qu'il fonctionne.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Serveur : C880-M4
- Micrologiciel : 1.0.5
- Serveur de Microsoft Active Directory

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Implémentation de LDAP

Quand l'userX veut ouvrir une session au MMB :

Étape 1. Le micrologiciel MMB demande au serveur d'AD de rechercher l'userX sous le CN=Users (dur codé).

Étape 2. Si le micrologiciel MMB reçoit une réponse que l'userX est trouvé dans le CN=Users du serveur d'AD, alors le micrologiciel MMB demande au serveur d'AD de rechercher l'userX dans l'arborescence de l'unité organisationnelle (OU) de l'arborescence de l'information de répertoire (DIT) de l'emplacement spécifié par le **répertoire de groupes comme sous-arbre de gisement de base de DN** sur le Web-UI MMB.

Étape 3. Si le micrologiciel MMB reçoit une réponse que l'userX est trouvé dans l'arborescence de l'OU du serveur d'AD (nom de groupe au lequel l'userX appartient est également envoyé du serveur d'AD), alors le micrologiciel MMB vérifie si le nom de groupe reçu est une correspondance avec le nom de groupe inscrit en page de **groupe d'utilisateurs de LDAP** dans le Web-UI MMB.

Étape 4. Si le nom de groupe est une correspondance, alors l'userX peut ouvrir une session.

Source : Fujitsu

Configurez

Créez les comptes spéciaux

Étape 1. Protocole Secure Shell (SSH) à l'adresse IP et à la procédure de connexion de la Gestion du serveur comme administrateur.

Étape 2. Créez les comptes spéciaux d'admin et de CE :

```
Administrator> set special_account spadmin admin
Are you sure you want to add spadmin? [Y/N]: y
Password:xxxxxxxxxx
Confirm Password:xxxxxxxxxx
Administrator>
```

```
Administrator> set special_account spce ce
Are you sure you want to add spce? [Y/N]: y
Password:zzzzzzzzzz
Confirm Password:zzzzzzzzzz
Administrator>
```

Service d'annuaire

Étape 1. Naviguez vers la **gestion d'utilisateur > la configuration de LDAP > la configuration de service d'annuaire**.

Étape 2. Clic **activé** pour le **LDAP**.

Étape 3. Choisissez si **activer/le SSL de LDAP**.

Étape 4. **Répertoire actif** choisi de baisse du menu vers le bas pour le **type de serveur de répertoire**.

Étape 5. Écrivez les détails pour la configuration **primaire de serveur LDAP** et de **serveur LDAP de sauvegarde**.

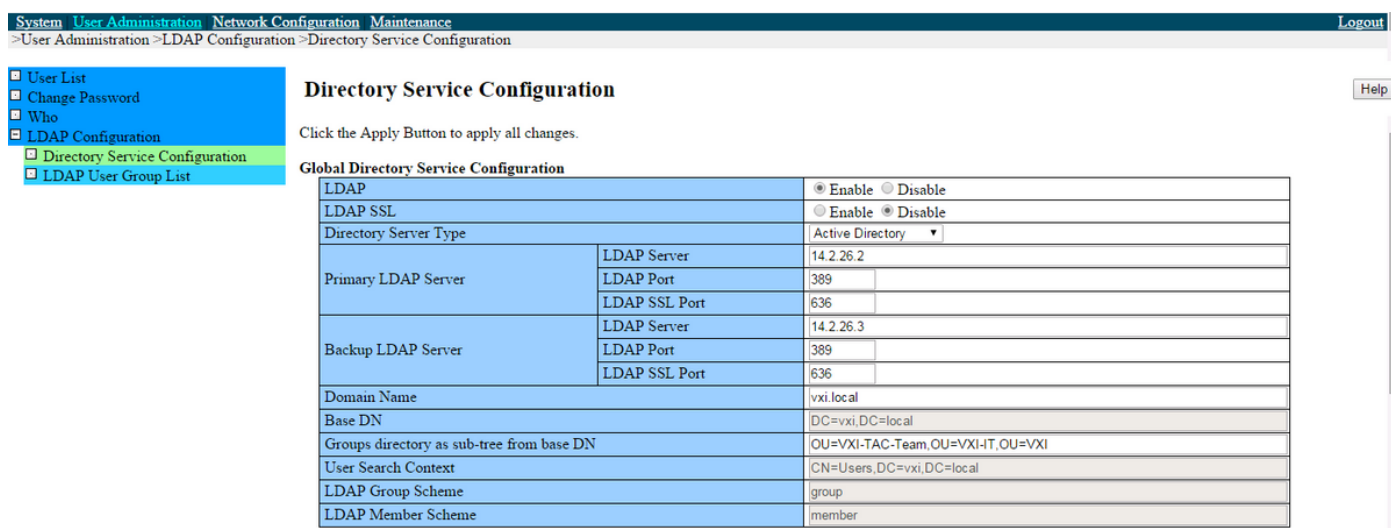
Étape 6. Écrivez le **nom de domaine**.

Étape 7. Écrivez le **répertoire de groupes comme sous-arbre de DN de base**. C'est où le groupe d'AD qui est créé dans les besoins de groupe d'utilisateurs ici de résider.

Étape 8. Écrivez le **nom d'utilisateur et mot de passe authentique de LDAP**. Ce les besoins de l'utilisateur d'exister dans CN=Users, DC=domain, DC=com.

Étape 9. Cliquez sur Apply.

Étape 10. **LDAP de test de clic**, suivant les indications des images.



The screenshot shows the 'Directory Service Configuration' window. On the left is a navigation tree with 'LDAP Configuration' selected. The main area contains a table for 'Global Directory Service Configuration' with various settings like LDAP, LDAP SSL, Directory Server Type, Primary/Backup LDAP Servers, Domain Name, Base DN, Groups directory, User Search Context, LDAP Group Scheme, and LDAP Member Scheme.

Global Directory Service Configuration		
LDAP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
LDAP SSL	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Directory Server Type	Active Directory	
Primary LDAP Server	LDAP Server	14.2.26.2
	LDAP Port	389
	LDAP SSL Port	636
Backup LDAP Server	LDAP Server	14.2.26.3
	LDAP Port	389
	LDAP SSL Port	636
Domain Name	vxi.local	
Base DN	DC=vxi,DC=local	
Groups directory as sub-tree from base DN	OU=VXI-TAC-Team,OU=VXI-IT,OU=VXI	
User Search Context	CN=Users,DC=vxi,DC=local	
LDAP Group Scheme	group	
LDAP Member Scheme	member	

Directory Service Access Configuration

LDAP Auth UserName	c880bind
LDAP Auth Password	
Confirm Password	
Principal User DN	
Append Base DN to Principal User DN	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Bind DN	CN=c880bind,CN=Users,DC=vxi,DC=local
Enhanced User Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
User Login Search Filter	(&(objectclass=person)(sAMAccountName=%s))

Apply Cancel Test LDAP

Créez le groupe d'utilisateurs

Étape 1. Naviguez **liste** vers la **gestion d'utilisateur > la configuration de LDAP > de LDAP groupe d'utilisateurs**.

Étape 2. Cliquez sur le bouton de groupe d'ajouter pour ajouter un nouveau groupe.

Étape 3. Écrivez le **nom de groupe d'utilisateurs de LDAP** et le **privilege** (par exemple l'admin)

Étape 4. Cliquez sur Apply suivant les indications des images.

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)
 >User Administration >LDAP Configuration >LDAP User Group List

User List
 Change Password
 Who
 LDAP Configuration
 Directory Service Config
 LDAP User Group List

LDAP User Group List

Click the Add Group button to add a new group.
 Select a group, then click the Edit/Remove Group button to edit or remove the group.

LDAP User Group Name	Privilege	Status
<input type="radio"/> MMBAdmin	Admin	Enabled

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)
 >User Administration >LDAP Configuration >Add LDAP User Group

User List
 Change Password
 Who
 LDAP Configuration
 Directory Service Config
 LDAP User Group List

Add LDAP User Group

Click the Apply Button to apply all changes.

LDAP User Group Name	MMBAdmin
Privilege	<input checked="" type="radio"/> Admin <input type="radio"/> Operator <input type="radio"/> User <input type="radio"/> CE
Status	<input type="radio"/> Enabled <input type="radio"/> Disabled

System [User Administration](#) [Network Configuration](#) [Maintenance](#) [Logout](#)
 >User Administration >LDAP Configuration >LDAP User Group List

User List
 Change Password
 Who
 LDAP Configuration
 Directory Service Configuration
 LDAP User Group List

LDAP User Group List

Click the Add Group button to add a new group.
 Select a group, then click the Edit/Remove Group button to edit or remove the group.

LDAP User Group Name	Privilege	Status
<input type="radio"/> MMBAdmin	Admin	Enabled

Active Directory

Étape 1. Créez l'utilisateur c880bind.

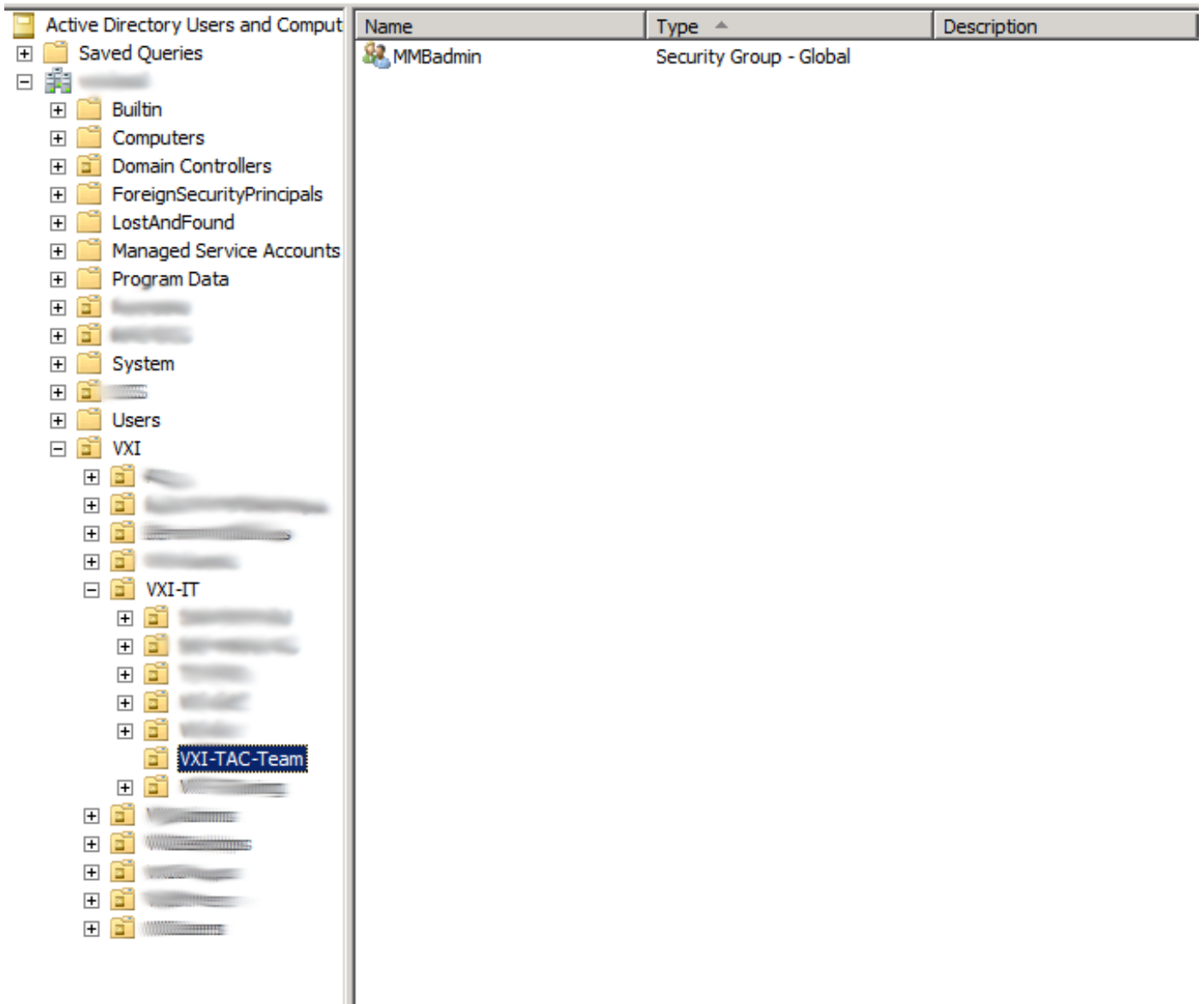
Étape 2. Créez l'utilisateur ldaptest suivant les indications de l'image.

CN=Users, DC=VXI, DC=local :

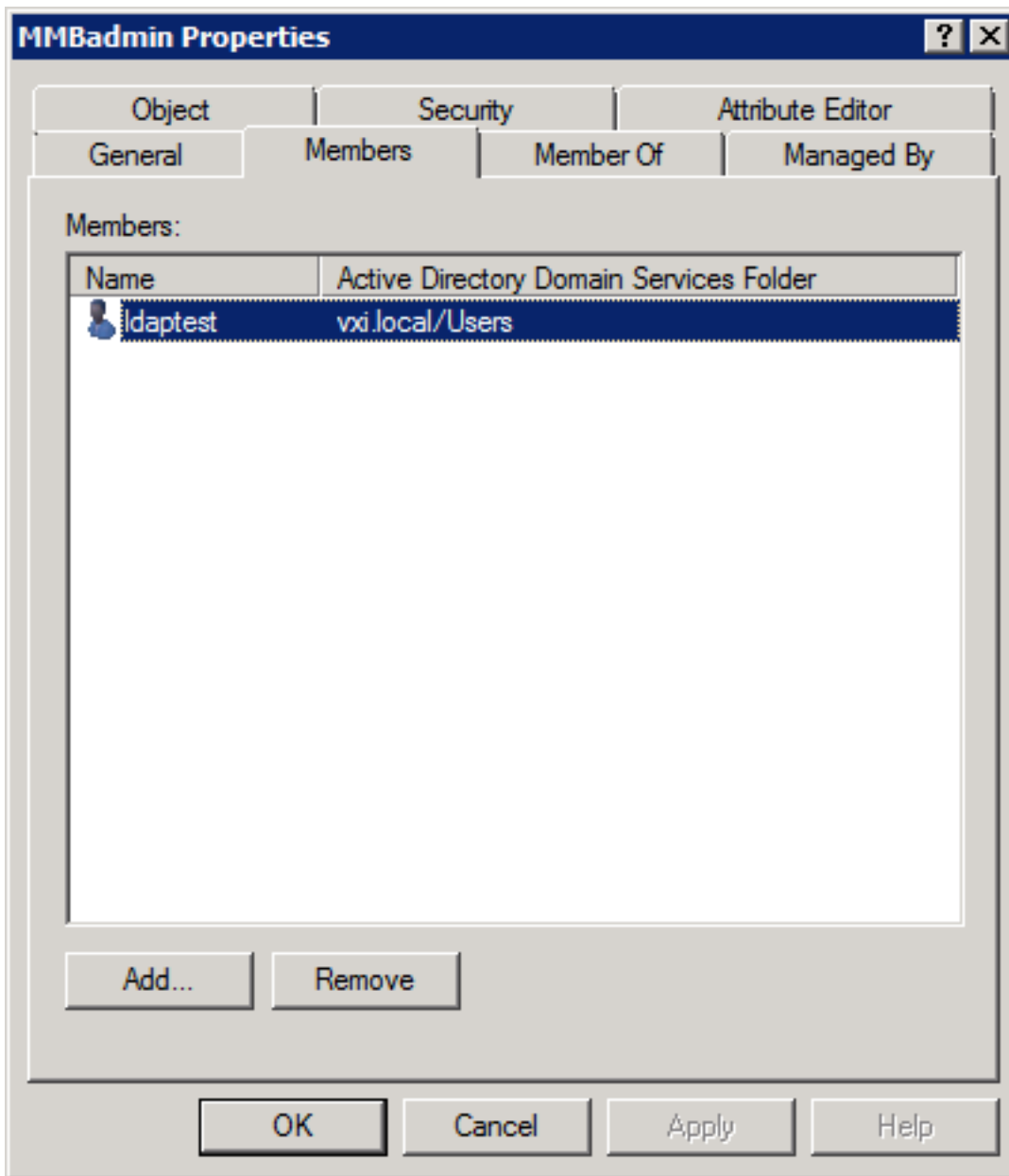
Name	Type	Description
 c880bind	User	
 ldaptest	User	

Étape 3. Créez le groupe de sécurité de MMBAdmin à l'OU suivant les indications de l'image.

Groupe de MMBAdmin dans OU=VXI-TAC-Team, OU=VXI-IT, OU=VXI :



Étape 4. Ajoutez **ldaptest** à MMBAdmin suivant les indications de l'image.



Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

- Le **LDAP de test** doit fonctionner
- Vous devez pouvoir ouvrir une session avec le compte **ldaptest**

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

- Vérifiez le serveur et la configuration d'AD qui se conforme à l'implémentation du LDAP de Fujitsu
- Collectez une capture de paquet du serveur d'AD

[Informations connexes](#)

- [Manuels de gamme 2000 PRIMEQUEST](#) qui se compose de la référence de manuel et d'outil d'installation
- [Support et documentation techniques - Cisco Systems](#)