



LDAP:

Mise en place d'un lien ldap entre un ad et un pfsense



ANNEE: 2022-2024

ETUDIANT: CHAMEY Axel

FORMATEURS: BERT Thomas
KUS Mikail



TABLE DES MATIERES

1.	CONFIGURATION DE LA LIAISON	2
1.	Choix du serveur.....	2
2.	Selection de utilisateurs que l'on veut rattacher	4
3.	Test de connectivité	5

C'EST QUOI LE PROTOCOLE LDAP ?

LDAP signifie Lightweight Directory Access Protocol. Il s'agit d'un protocole réseau standardisé utilisé pour :

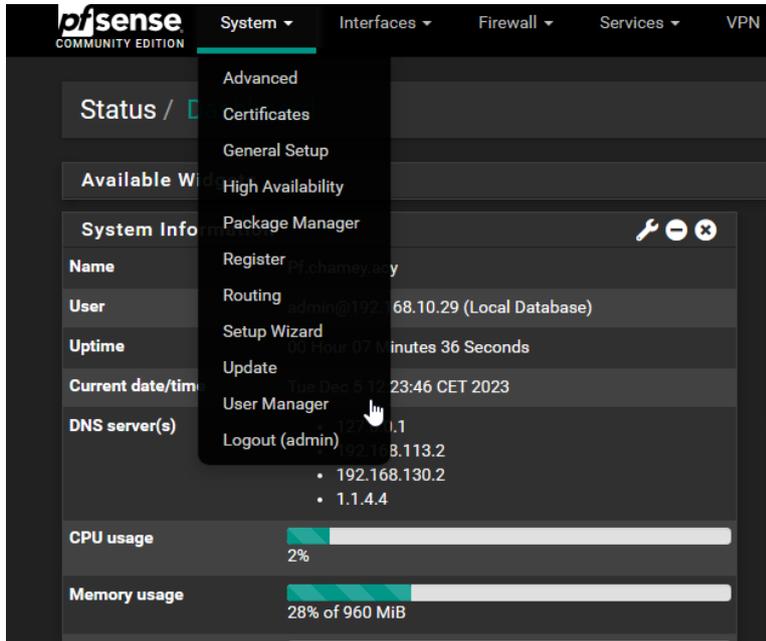
Stocker des informations dans des services d'annuaires (annuaires LDAP).

Authentifier les utilisateurs qui accèdent à ces services.

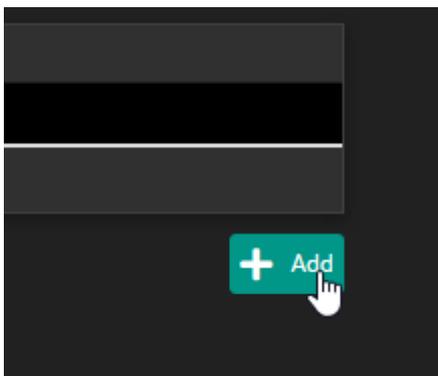
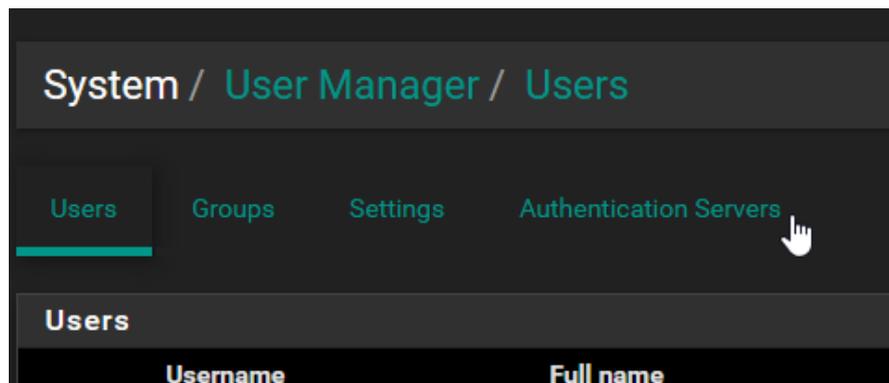
Gérer les informations et les utilisateurs de manière centralisée.

1. CONFIGURATION DE LA LIAISON

1. Choix du serveur



Une fois sur notre PfSense on va dans la rubrique System > User Manager



Puis on va chercher Authentication servers et on clique sur « Add » pour ajouter un serveur

LDAP

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name
LDAP ad.chamey.acy

Type
LDAP

LDAP Server Settings

Hostname or IP address
192.168.10.33
NOTE: When using SSL/TLS or STARTTLS, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP server SSL/TLS Certificate.

Port value
389

Transport
Standard TCP

Peer Certificate Authority
Global Root CA List
This CA is used to validate the LDAP server certificate when 'SSL/TLS Encrypted' or 'STARTTLS Encrypted' Transport is active. This CA must match the CA used by the LDAP server.

Protocol version
3

Server Timeout
25
Timeout for LDAP operations (seconds)

Search scope
Level
Entire Subtree

Base DN
DC=ad,DC=chamey,DC=acy

Authentication containers
OU=User,OU=Compta,DC=ad,DC=chamey,DC=acy;OU=User,OU=Prod,DC=ad,DC=ch
Note: Semi-Colon separated. This will be prepended to the search base dn above or container path can be specified containing a dc= component.
Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers

Select a container

Extended query

ON RENTRE LES INFORMATION DU SERVEUR
ET ON CLIQUE SUR "SELECT A CONTAINER"

2. Selection de utilisateurs que l'on veut rattacher

Containers

- OU=Compta,DC=ad,DC=chamey,DC=acy
- OU=Domain Controllers,DC=ad,DC=chamey,DC=acy
- OU=Groupe,OU=Compta,DC=ad,DC=chamey,DC=acy
- OU=Groupe,OU=Prod,DC=ad,DC=chamey,DC=acy
- OU=PC,OU=Compta,DC=ad,DC=chamey,DC=acy
- OU=PC,OU=Prod,DC=ad,DC=chamey,DC=acy
- OU=pfsense,DC=ad,DC=chamey,DC=acy
- OU=Prod,DC=ad,DC=chamey,DC=acy
- OU=User,OU=Compta,DC=ad,DC=chamey,DC=acy
- OU=User,OU=Prod,DC=ad,DC=chamey,DC=acy
- CN=Users,DC=ad,DC=chamey,DC=acy

 Save

ICI j'ai choisit les groupes d'utilisateurs "COMPTA" et "PROD"

Dans la partie Bind credentials on rajoute l'utilisateur qui a les permissions d'intégrer avec le protocole (ici j'utilise l'administrateur)

Server Timeout

25
Timeout for LDAP operations (seconds)

Search scope

Level
Entire Subtree

Base DN
DC=ad,DC=chamey,DC=acy

Authentication containers

OU=Compta,DC=ad,DC=chamey,DC=acy;OU=Prod,DC=ad,DC=chamey,DC=acy

Note: Semi-Colon separated. This will be prepended to the search base dn above or the full container path can be specified containing a dc= component.
Example: CN=Users;DC=example,DC=com or OU=Staff;OU=Freelancers



Extended query

Enable extended query

Bind anonymous

Use anonymous binds to resolve distinguished names

Bind credentials

CN=administrateur,CN=Users;DC=ad,DC=chamey,DC=acy

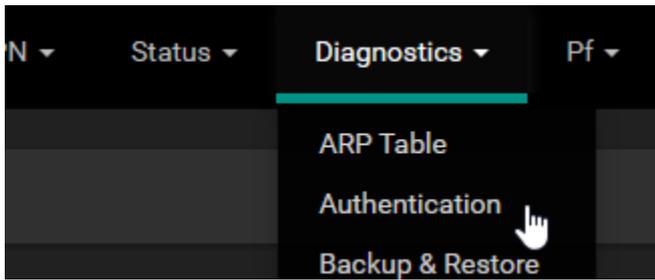
.....

User naming attribute

samAccountName

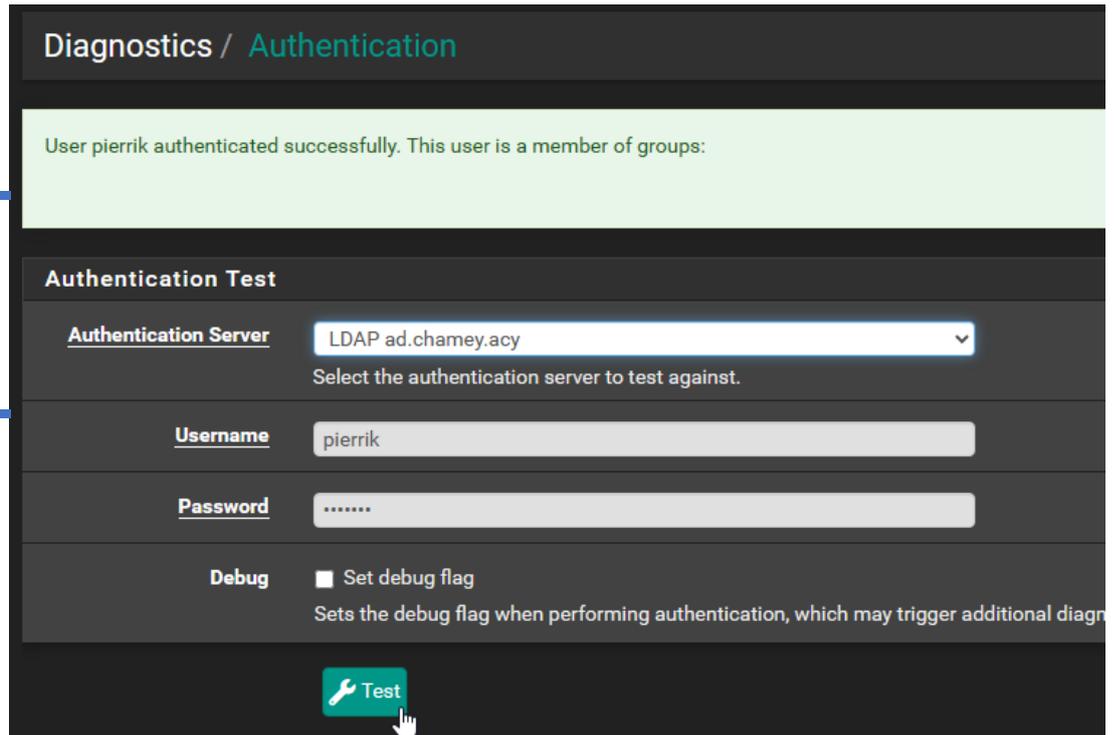
NOTE: ON CLIQUE ENSUITE SUR SAVE EN BAS DE LA PAGE

3. Test de connectivité



Pour tester la connectivité on se rend dans l'onglet diagnostique puis on clique sur authentification

On choisit un utilisateur présent dans un des groupes sélectionner et on clique sur test



NOTE: SI LA BULLE VERTE APPARAÎT C'EST QUE VOTRE LDAP EST BIEN FONCTIONNEL