



efrei

PARIS PANTHÉON-ASSAS UNIVERSITÉ



Authentification LDPA et LDAPS

BTS SIO SISR 2022 – 2024

Contexte : Ce document a été élaboré dans le cadre d'un projet au sein de l'entreprise Sitka, visant à tester et configurer la connectivité LDAP (Lightweight Directory Access Protocol) et LDAPS (LDAP sur SSL) sur les serveurs Active Directory Hermes et Heimdall (Pfsense), ainsi que la création des comptes utilisateurs et des méthodes d'authentification LDAP et LDAPS.

A- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur le serveur active directory hermes

- 1- Connectivité LDAP
- 2- Connectivité LDAPS (**LDAP sur SSL**)
 - a- Création d'une autorité de certification sur le contrôleur de domaine hermes i- Ajouter le rôle certificat sur hermes
 - ii- Configuration du rôle certificat sur hermes

B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)

C- Création des comptes utilisateurs sur le contrôleur de domaine

D- Création des authentifications LDAP et LDAPS sur le serveur pfsense

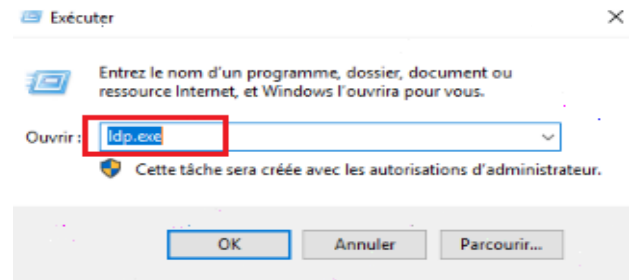
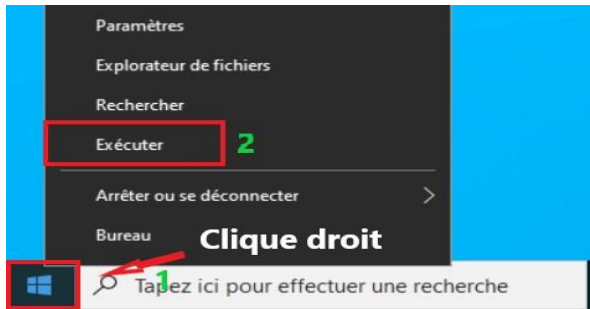
E- Création de l'authentifications LDAP

- 1- Création de l'authentifications LDAP
- 2- Création de l'authentifications LDAPS
 - a- Création du formulaire de l'authentification LDAPS
 - b- Analyse avec Wire Shark du trafic pfsense active directory
 - c- Exportation du certificat de l'autorité de certification hermes
 - d- Importation du certificat de l'autorité de certification racine
 - e- Test de la connexion ssl entre pfsense et le contrôleur de domaine
- 3- Utilisation des authentifications LDAP et LDAPS sur le serveur pfsense
 - a- Vérification de l'authentification LDAP et LDAPS
 - b- Création et configuration d'un groupes sur pfsense
 - c- Test de connexion sur l'interface web avec un compte ldap

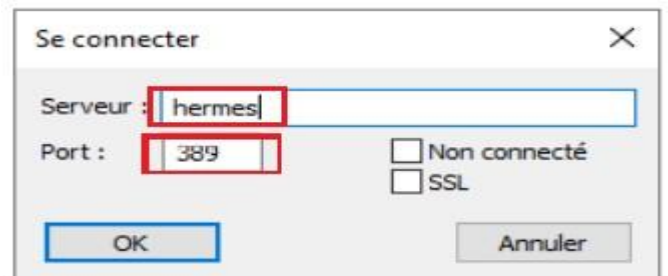
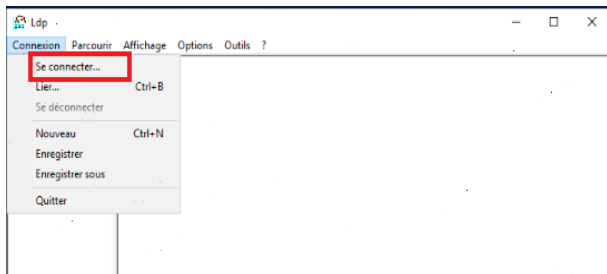
A- Test de la connectivité LDAP et LDAPS sur le serveur active directory hermes

1- Connectivité LDAP

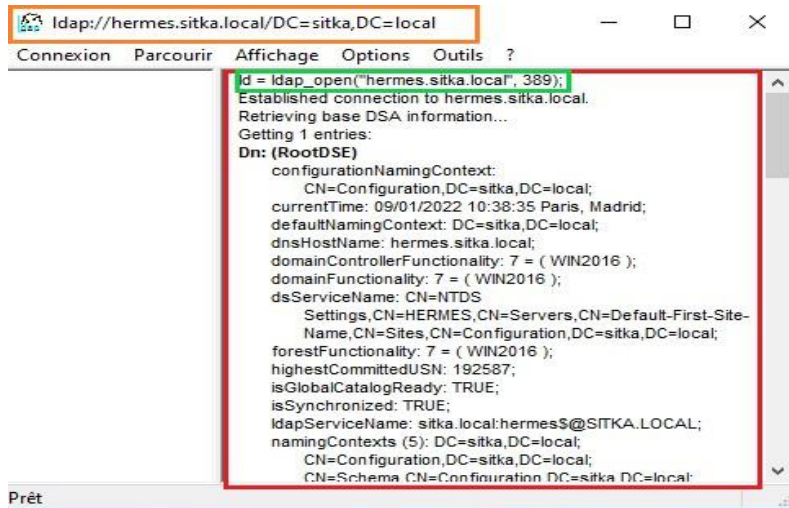
Sur le contrôleur de domaine on test la connectivité LDAP standard, donc clique droit sur le menu démarrer + exécuter puis on tape **ldp.exe** pour ouvrir l'explorateur LDAP



Un fois l'explorateur LDAP est ouvert l'explorateur on choisit le menu Se connecter et on rentre le nom du serveur **hermes.sitka.local** ainsi que le port de connexion **389**

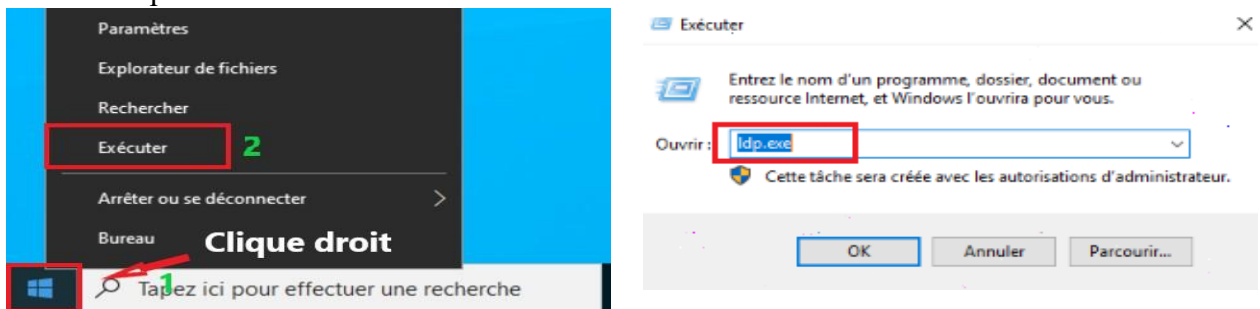


La connexion à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire

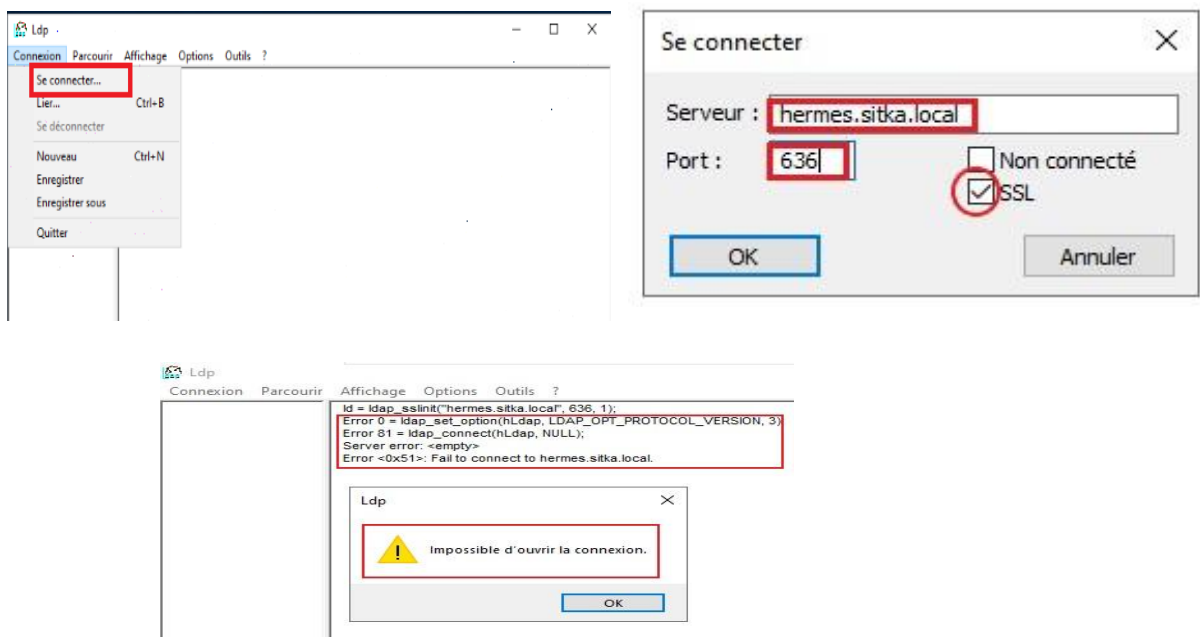


2- Connectivité LDAPS (LDAP sur SSL)

On fait la même chose que la procédure établissant une connexion standard on change juste le numéro de port et on coche ssl



On tombe sur un message d'erreur, le contrôleur de domaine ne supporte pas LDAPS car il n'est pas associé à un certificat.



Il existe deux méthodes pour activer LDAPS (LDAP sur SSL) sur un contrôleur de domaine :

- Mettre un Certificat Racine sur le contrôleur de domaine en installant une autorité de certification racine sur hermes
- Utiliser un certificat tiers sur le contrôleur de domaine. (Hermes)

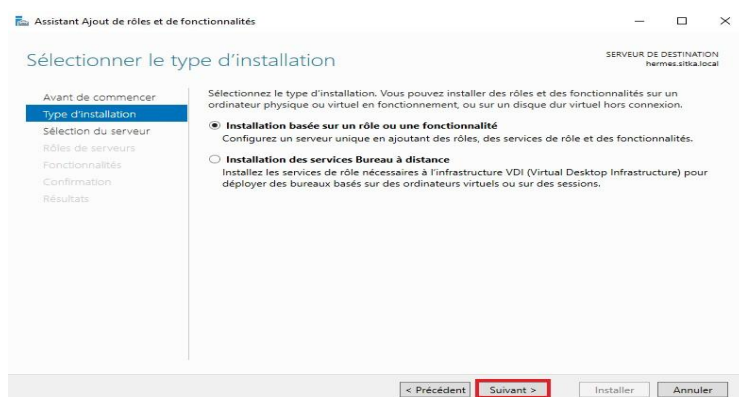
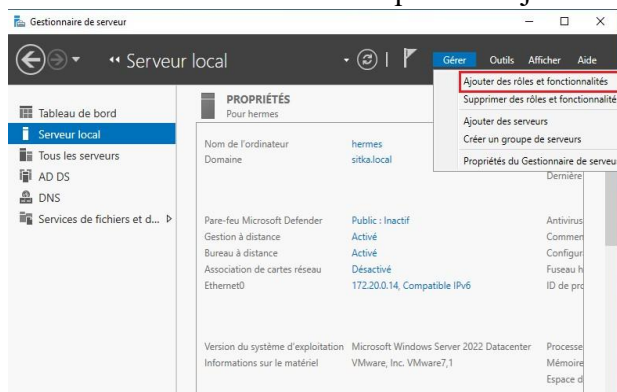
Pour notre procédure on choisira la première méthode, Donc il faut installer une autorité de certification afin de tirer parti de LDAPS

a- Création d'une autorité de certification sur le contrôleur de domaine hermes

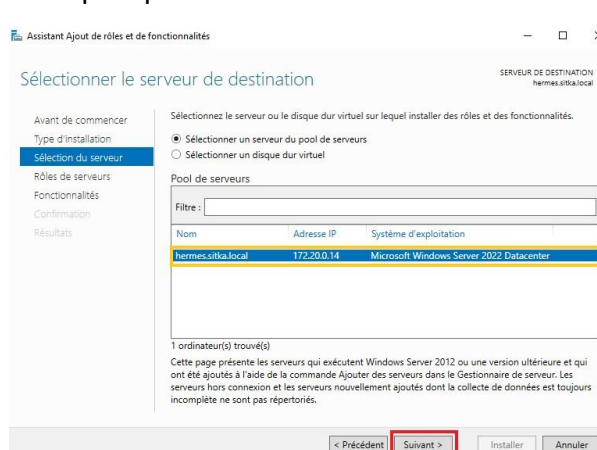
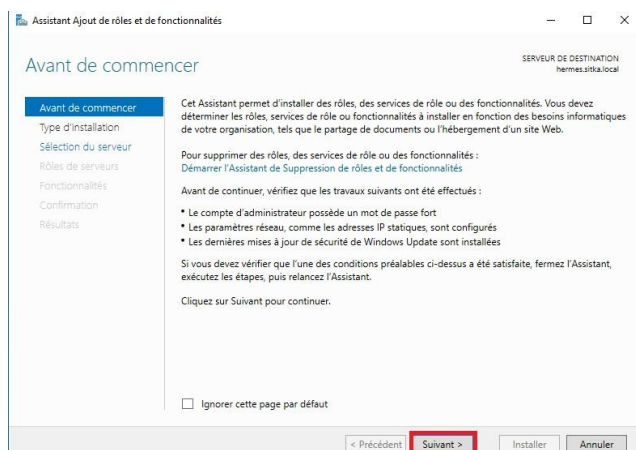
Il est nécessaire d'installer le service autorité de certification. Pour fournir au contrôleur de domaine un certificat qui permettra au service LDAPS d'opérer sur le port 636.

i- Ajouter le rôle certificat sur hermes

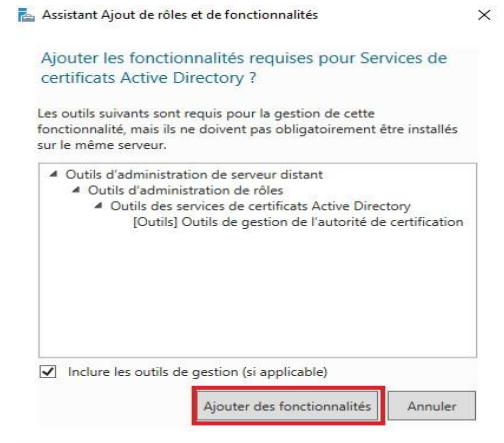
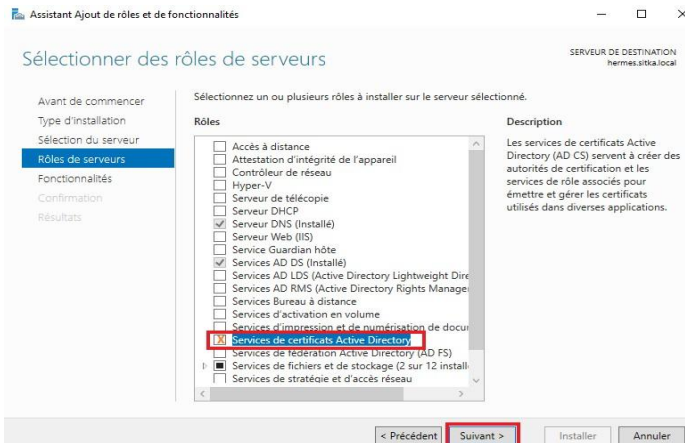
Accédez au menu Gérer et cliquez sur Ajouter des rôles et des fonctionnalités.



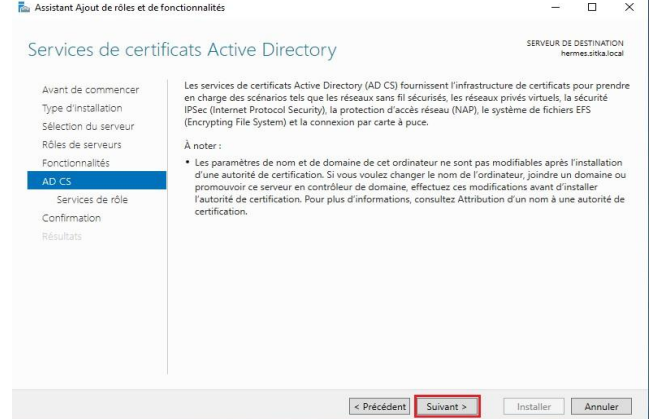
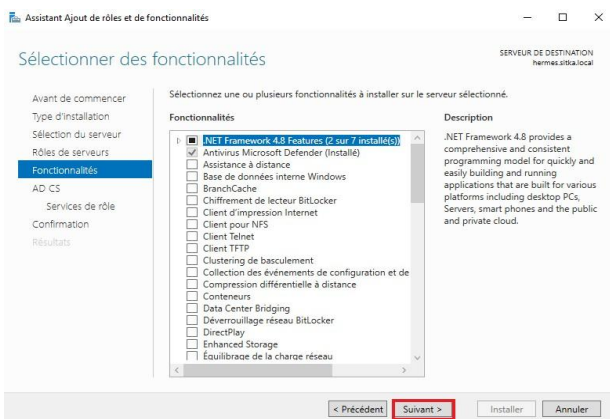
On vérifie le nom et l'adresse IP de notre serveur on clique après sur suivant



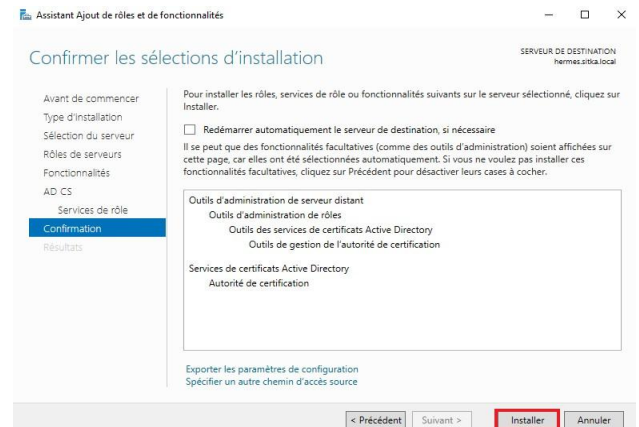
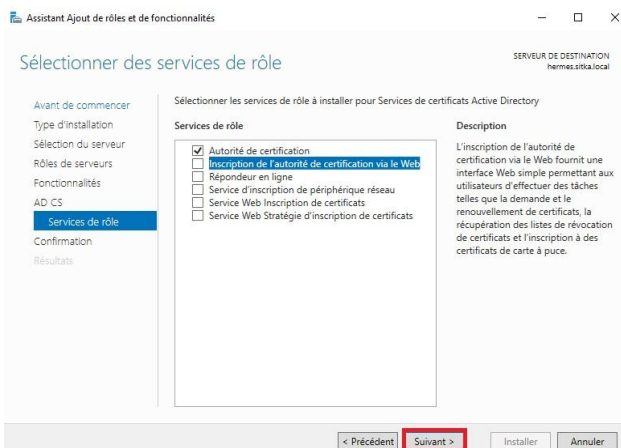
On coche Services de **Certificats Active Directory** et on rejoute les fonctionnalités



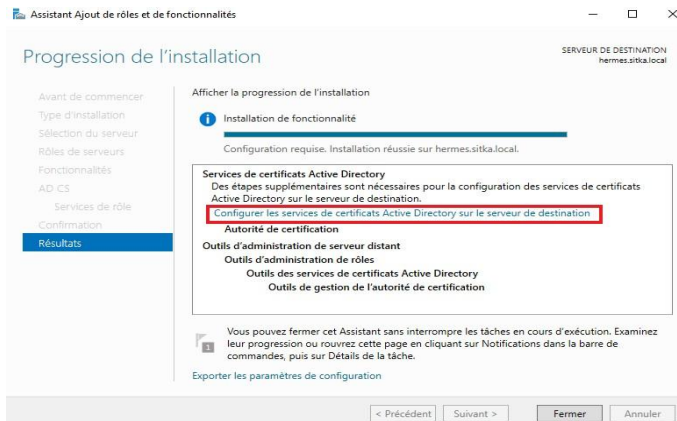
Sur les deux Boites de dialogues ci-dessous on laisse tout par défaut en faisant suivant.



On sélectionne que l'option **Autorité de certification**



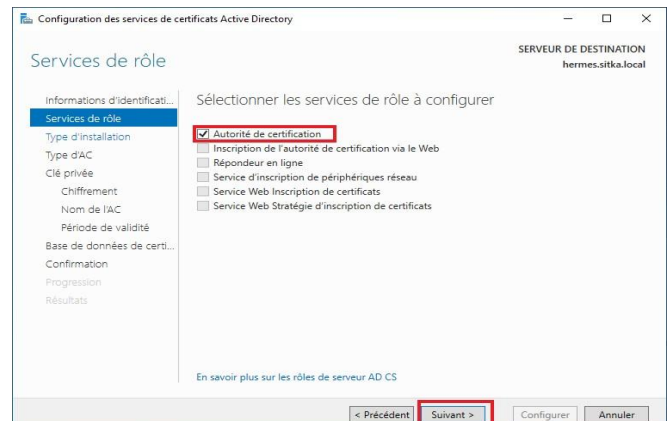
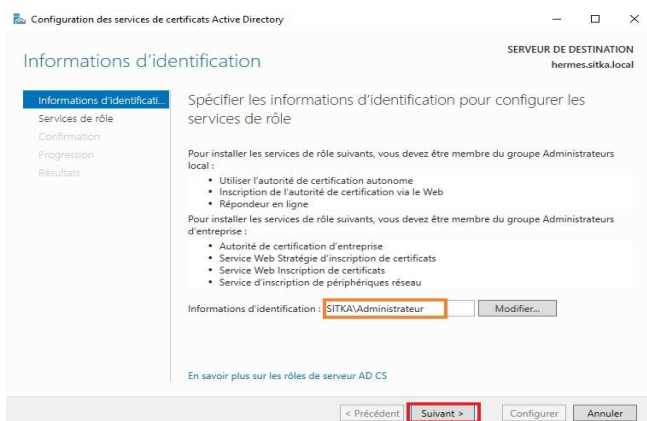
Dernière étape on clique sur le lien **Configurer les services Active Directory sur le serveur de destination**



ii- Configuration du rôle certificat sur hermes

Une fois le rôle certificat est installé il faut maintenant le configurer, on vérifie les informations d'identification, il est obligatoire d'être connecté avec le compte de l'administrateur de l'entreprise (domaine\administrateur).

On coche après **Autorité de certification**, toutes les autres options on peut les installer après au besoin

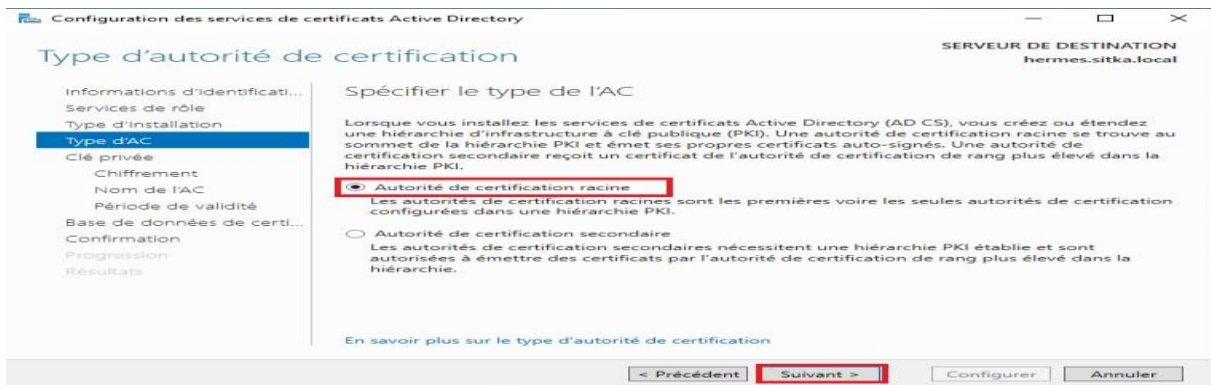


On sélectionne **Autorité de certification d'entreprise** afin que l'autorité de certification puisse utiliser l'annuaire LDAP

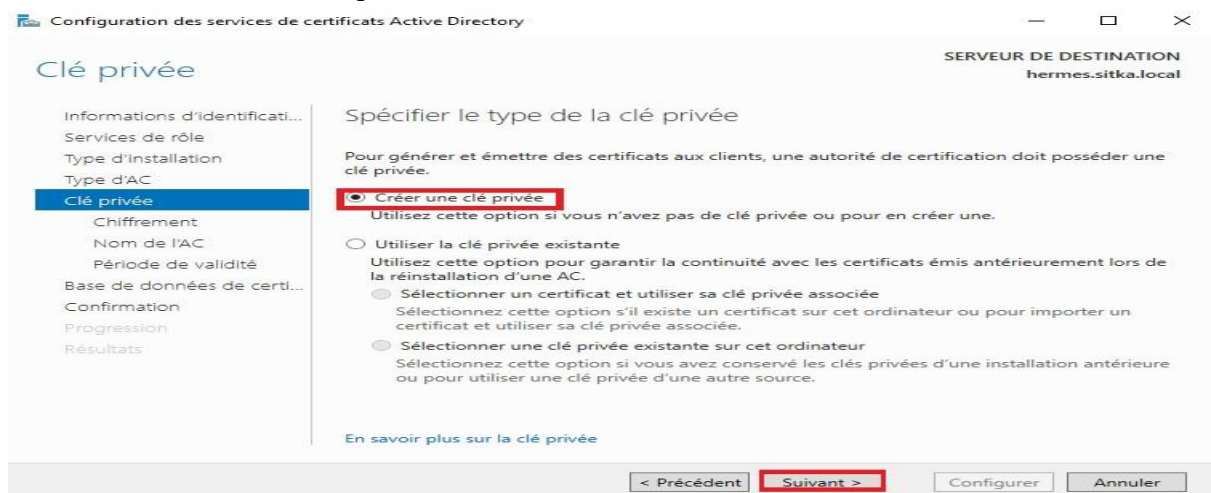


On sélectionne autorité de certification racine

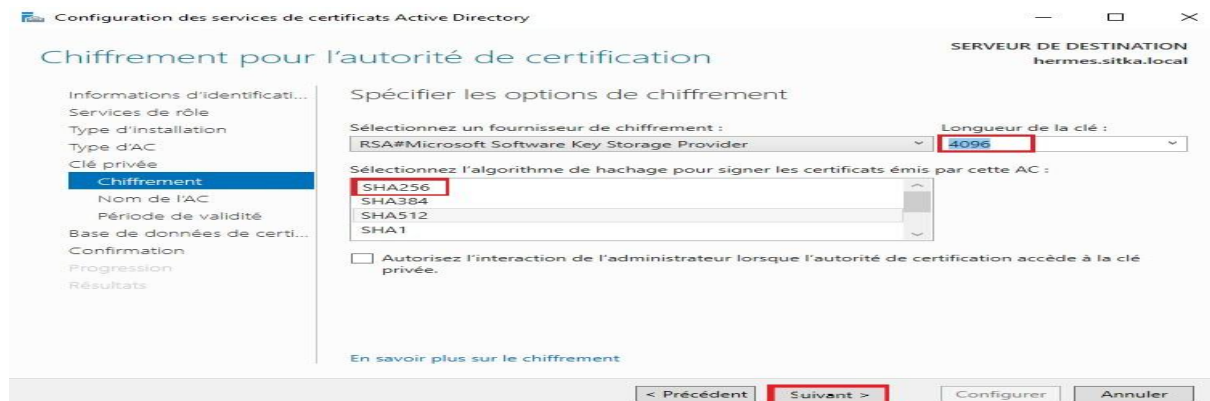
Ce type d'autorité de certification couplé avec un Active Directory est utile pour un intranet mais est déconseillé pour un accès public. Puisque notre autorité n'est pas listée parmi les autorités de certification de confiance, les personnes utilisant des certificats émis par notre autorité de certification auront un avertissement mentionnant que nos certificats ne sont pas de confiance.



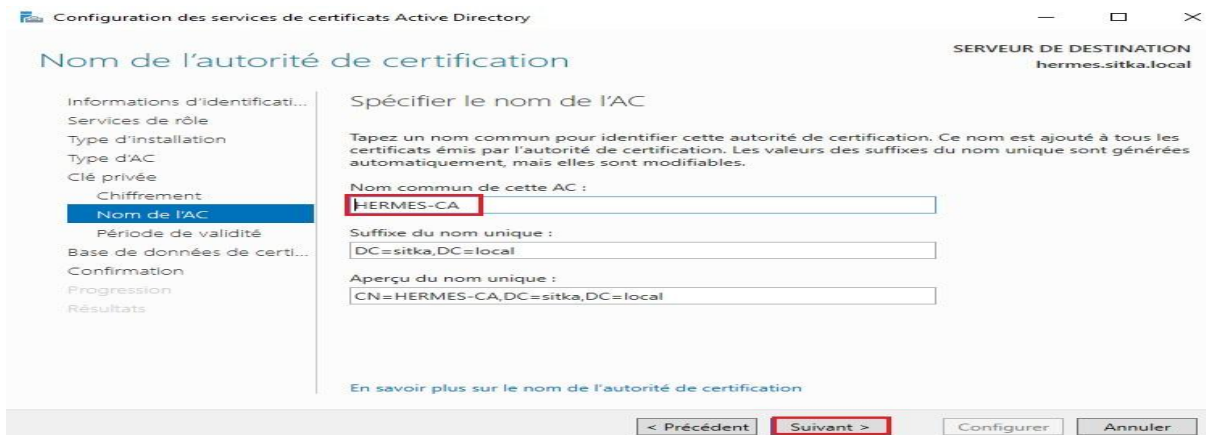
On choisit de créer une clé privée



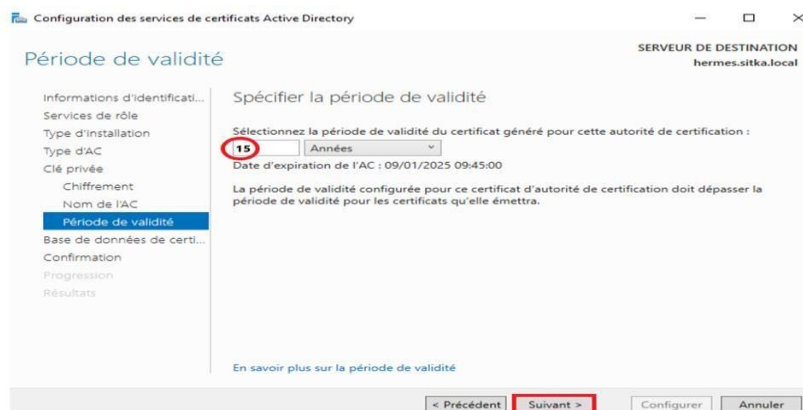
On choisit nos clés de chiffrement, plus les clés sont longues plus la sécurité est renforcée mais malheureusement les performances vont être impactées.



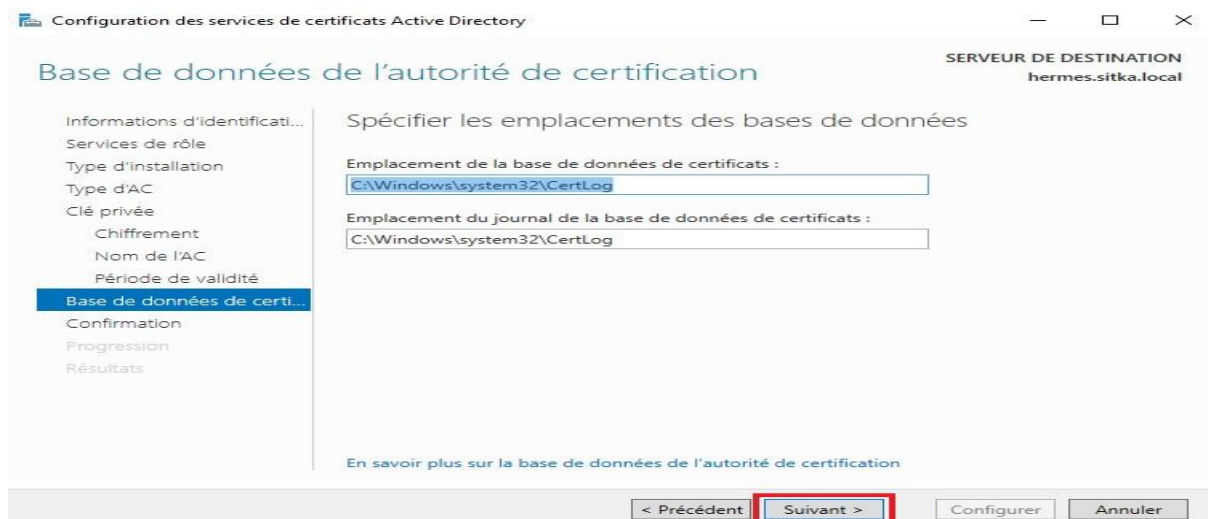
On peut modifier les valeurs par défaut ; je choisis hermes-CA comme nom commun de ACR



On rentre le période de validité pour le certificat de l'ACR., la période de validité du certificat de l'autorité de certification doit dépasser la période de validité des certificats émis.

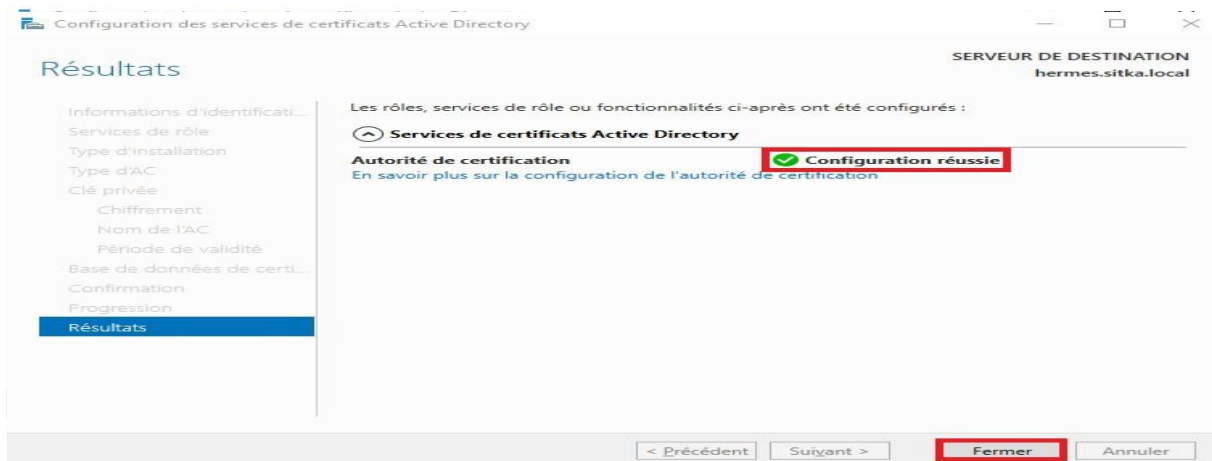


On laisse les dossiers des bases de données et des logs, par défaut.



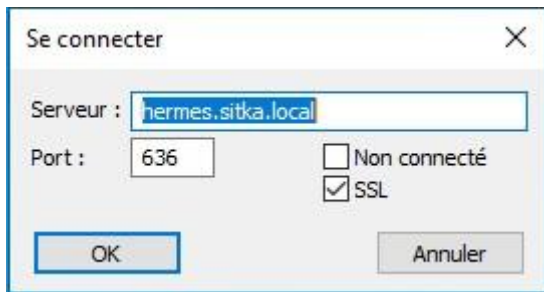
L'assistant nous affiche un résumé de la configuration choisit, on lance ensuite le processus de Configuration

On doit obtenir le message configuration réussie



On reteste maintenant notre connexion LDAPS à partir de l'explorateur LDAP

La connexion sécurisée utilisant le ssl sur le port 636 à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire



B- Test de la connectivité LDAP et LDAP (LDAP sur SSL) sur heimdall (pfsense)

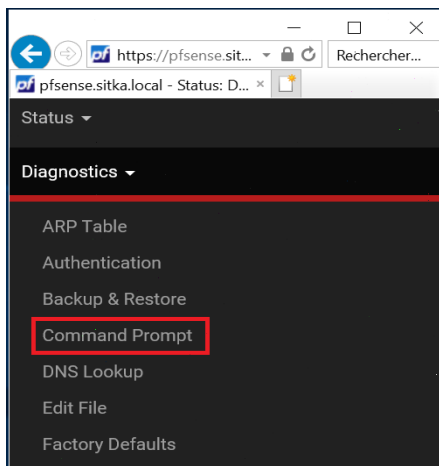
Sur pfsense on test la connexion de pfsense à la base d'annuaire du controleur de domaine en tapant la commande suivante soit en ssh ou directement sur pfsense:

```
# openssl s_client -showcerts -connect 172.20.0.14:636 !less
```

On peut faire la meme chose sur l'interface web de pfsense pour tester la connexion de

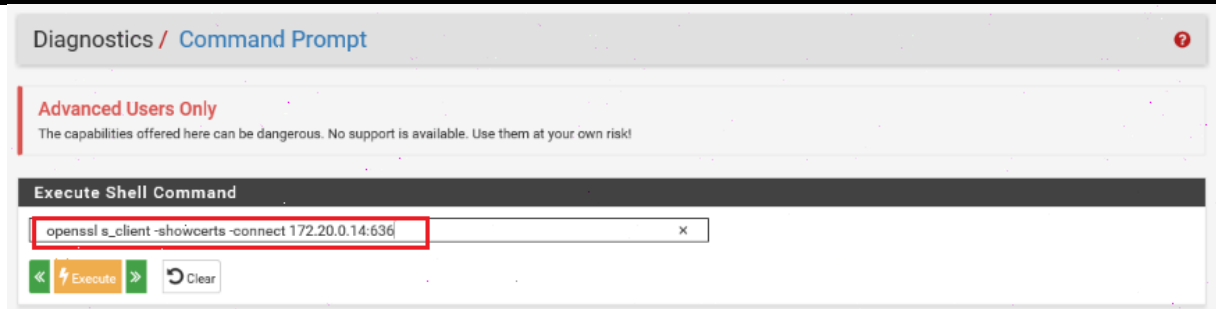
pfsense à la base d'annuaire du controleur de domaine, donc on va sur **Diagnostics** +

Command Prompt



On tape la commande suivante :

```
openssl s_client -showcerts -connect hermes.sitka.local:636
```



Le contrôleur de domaine nous envoie le certificat qu'il utilise pour appliquer le ssl

Shell Output - openssl s_client -showcerts -connect hermes.sitka.local:636

```
depth=0 CN = hermes.sitka.local
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 CN = hermes.sitka.local
verify error:num=21:unable to verify the first certificate
verify return:1
depth=0 CN = hermes.sitka.local
verify return:1
CONNECTED(00000003)
---
```

Certificate chain

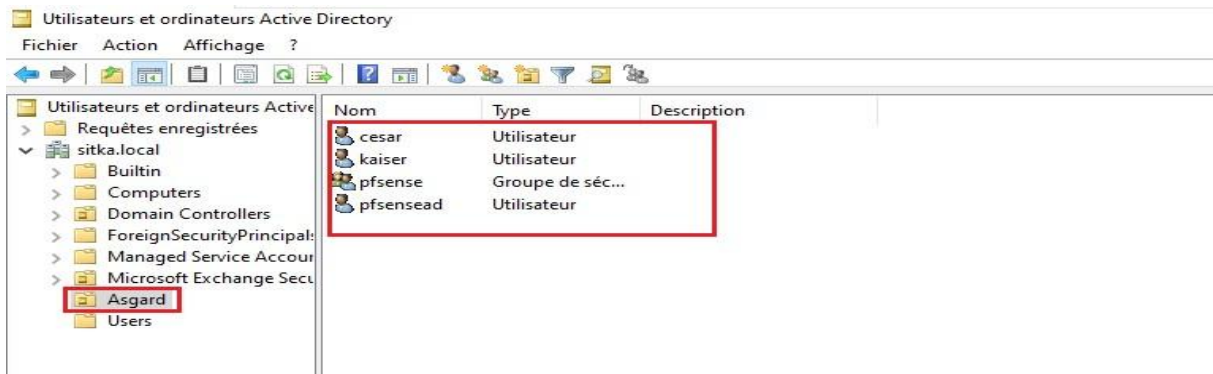
```
0 s:CN = hermes.sitka.local
i:DC = local, DC = sitka, CN = HERMES-CA
```

```
-----BEGIN CERTIFICATE-----
MIIG0zCCBLugAwIBAgITEGAAAAJCXcyfPesdnYgAAAAAAjANBgkqhkiG9w0BAQ0F
ADBCMRUwEwYKZlmiZPyLQGBGRYfBg9jYwxfTATBgoJkiaJk/IsZAEZFgVzaXRr
YTESMBAgA1UEAxMJSjEVSUVSTUVTLUNBMB4XDTIyMDEwOTA4NDIzOFoXDTIzMD
NDIzOFowHTEBMBkGA1UEAxMSaGVhbnVzLnNpdGthLmxvY2FsaWBIjANBgkqhkiG
9w0BAQ0FAAOCAQ8AMIIBCgKCAQEAvHs5UeElmJovxUSPF8XRlQda9gIsff7R10M
421sBUP67Nya73IUDqYQ8sQmzaqkgNDqaQXd08Bdqq89rbZxa6QIGPHURHr8Edu
ANZxtntbM1c0rCp3RnQSPDq4mNJ3XvL+IU82oR4nBZ34minC6rQa20N/kNw+UwW
EaEDHMgQp1Vc7NvEfJUSY5CMpioz1x+NQDexH11/EW1h6k5qBPapJ2CUFzTxTB/r
baOpNhI+A6d4fMwRsetDimC6xEhIKy82sZg/+1K2fJzH1FYeTTIBV2jw6qTx1CA
DTf1adu2EJ1XwUmXG2uM6GbfD0W6kSOQRrKNxdDQgJD5euLFQIDAQABo4IC5TCC
AuEwLWYKwYBBAGCNxQCBCIEIABEAG8AbQBhAgkAbgBDAG8AbgB0AHIAbWBSAGWA
ZQBzMB0GA1UdJQkqWMBQGCCsGAQUFBwMCAgggrBgEFBQcDATAOBgNVHQ8BAF8EBAMC
8aAweAYJKoZIhvcNAQkPBGswaTAOBggqhkiG9w0DAGICAIAwDgYIKoZIhvcNAwQC
AgCAMAsGCWCGSFA1AwQ8KjALBg1ghkgBZQMEAS0wCwYJYIZIAWUDBAECAAsGCWCG
SFA1AwQBTAHhBglUrDgMcbZAKBggqhkiG9w0DAdBgNVHQ4EFgQUg6yhfRd1i3l
c8ttWcd0/2ineRmHwYDVR0jBBgwFoAUBV88XFzIRChIBMqLFpBDLkHNF/QwgcYG
A1UdHw5BvJCBuzCBuKCBtaCBsoaBr2xkYXA6Ly8vQ049SEVSTUVTLUNBLENOWh1
cm11cyxDtj1DRFAsQ049UHVi6lJjT1wS2V5JT1wU2Vydm1jZjZXMxM049U2Vydm1j
ZjZXM0049Q29uZmlndXJhdGlvbixEQz1zaXRrY5xEQz1sb2NhbD9jZjZj0aWZpY2F0
ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNoQ2xhc3M9Y1JMRG1zdHJpYnV0aW9u
UG9pbmQwbsGCCsGAQUFBwEBBIIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIu
Q049SEVSTUVTLUNBLENOWh1cm11cyxDtj1DRFAsQ049UHVi6lJjT1wS2V5JT1wU2Vydm1j
ZjZXMxM049U2Vydm1jZjZXM0049Q29uZmlndXJhdGlvbixEQz1zaXRrY5xEQz1sb2NhbD9jZjZj0aWZpY2F0
ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWNoQ2xhc3M9Y1JMRG1zdHJpYnV0aW9u
UG9pbmQwbsGCCsGAQUFBwEBBIIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIuMIu
aXR5MD4GA1UdEQQ3MDWgHwYJKwYBBAGCNxkBoBIEEBkHdzD9Eay1G10BTfWocpG2C
Emh1cm11cy5zaXRrY55sb2NhbDANBgkqhkiG9w0BAQ0FAAOCAgEAF39BzYd7S5HP
uwyP5C80+YbD0NHXcVec1ABJgp2jhmj3itAH4a7TKDXXWbXjNtguBT11I1Uzuwh
jw6T1w50yjlZ+WUHoJfujwIwInVTjHfmgouH6UP7BwC7KTz+iiwH30HPXVMKixVR
t0EyzZqr58drkclii5PfgU1Bj3L8FF3vqK3CVv/Ffd/Uagy+Qfb2WHDmIECqc6e
IQYnbBmLcWcLvgfyE6sybtJ6NLqI8RZ7J84QMatrgCB60eIM8GARu6JkGs7jc2
50LZXm4hFVMKberhdQt4cE77kFg0oGjUmDoJDHDJUGkRWjQQ81W6p59C111d01H
jiXAx9k2WTXszvZIF6W0buw0v4gA+yZOF4+dgn+1+PRpM/Hxcn2VE7UXArVf1m/Y
48KQE84fCwly/LrVyx19hoGdbm7pkTrRT0bp1vbUItcyAAVHC06zpx7y2ACG6r0
Kmi99AfKj5ar1RLR6b/8uDfQCTBdc3BVjsugJ0KxSaISK0tS1rr/tU/KGve6B1G9
6WpOuZeb21+iRd2oT62tyPQ061BsRktBLFSyPjio1jrH/PKNp//F1MFAjAFHqa1p
aAg1Jj5ETCwdR4ELyzB2kEMJURHxuuTckNq8brhG2SdKUGAA5mh1vMr/bVTFClw
WAHDHEXmYpTKPz51F6f1in0i0BSy1LM=
-----END CERTIFICATE-----
```

C- Création des comptes utilisateurs sur le contrôleur de domaine

Sur le contrôleur de domaine je crée :

- Un groupe **pfsense**
- Un utilisateur **kaiser** faisant partie du groupe **pfsense**
- Un utilisateur **cesar** faisant partie du groupe **pfsense**
- Un utilisateur **pfsensead** faisant partie du groupe **pfsense** et qui va servir de faire la liaison entre pfsense et le contrôleur de domaine



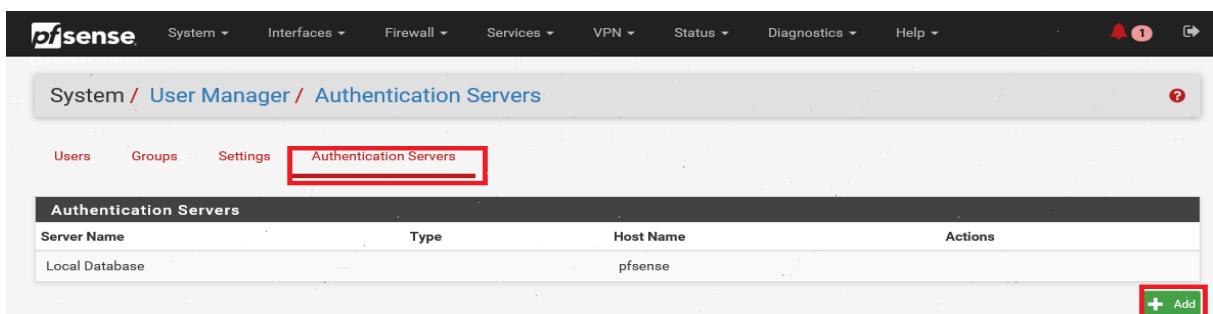
D- Création des authentifications LDAP et LDAPS sur le serveur pfsense

Sur pfsense il existe déjà une base locale permettant l'authentification des utilisateurs. On va utiliser deux autres méthodes qui permettront l'authentification en utilisant LDAP et LDAPS

1- Création de l'authentifications LDAP

Maintenant on va créer une authentification LDAP sur pfsense à partir l'interface web on va sur [System / User Manager / Authentication Servers](#)

Et on clique sur  pour rajouter une authentification Servers



On remplit Les champs comme indiqué ci-dessous, les étapes 1,2 et 3 il faut les exécuter à la fin de notre procédure les faire : on tape cn dans le champ **Authentication containers** puis on clique sur **select a container**



Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name: authentication ldap

Type: LDAP

LDAP Server Settings

Hostname or IP address: hermes.sitka.local
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

Select LDAP containers for authentication

Containers

- OU=Asgard,DC=sitka,DC=local
- OU=Domain Controllers,DC=sitka,DC=local
- OU=Microsoft Exchange Security Groups,DC=sitka,DC=local
- CN=Users,DC=sitka,DC=local

Save

Base DN: DC=sitka,DC=local

Authentication containers: OU=Asgard,DC=sitka,DC=local

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=pfensead,OU=Asgard,DC=sitka,DC=local

User naming attribute: samAccountName

Group naming attribute: cn

Group member attribute: memberOf

RFC 2307 Groups: LDAP Server uses RFC 2307 style group membership
RFC 2307 style group membership has members listed on the group object rather than using groups listed on user object. Leave unchecked for Active Directory style group membership (RFC 2307bis).

Group Object Class: posixGroup
Object class used for groups in RFC2307 mode. Typically "posixGroup" or "group".

Shell Authentication Group DN:

UTF8 Encode: UTF8 encode LDAP parameters before sending them to the server.
Required to support international characters, but may not be supported by every LDAP server.

Username Alterations: Do not strip away parts of the username after the @ symbol
e.g. user@host becomes user when unchecked.

Allow unauthenticated bind: Allow unauthenticated bind
Unauthenticated binds are bind with an existing login but with an empty password. Some LDAP servers (Microsoft AD) allow this type of bind without any possibility to disable it.

Save

2- Création de l'authentifications LDAPS a- Création du formulaire de l'authentification LDAPS

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name: authentication ldaps

Type: LDAP


LDAP Server Settings

Hostname or IP address: hermes.sitka.local
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: 636

Transport: SSL/TLS Encrypted

Même procédure que l'authentification LDAP sauf pour les champs encadrés en **vert** on fait le choix de **SSL/TLS** et en utilise le port **636**

Dans **authentification containers** on tape cn puis on clique sur 



La boîte de dialogue qui nous permet de choisir l'OU qui héberge nos utilisateurs ne s'ouvre pas en plus on a un message d'erreur qui apparaît en bas de la page

Could not connect to the LDAP server. Please check the LDAP configuration.

b- Analyse avec Wire Shark du trafic pfsense active directory

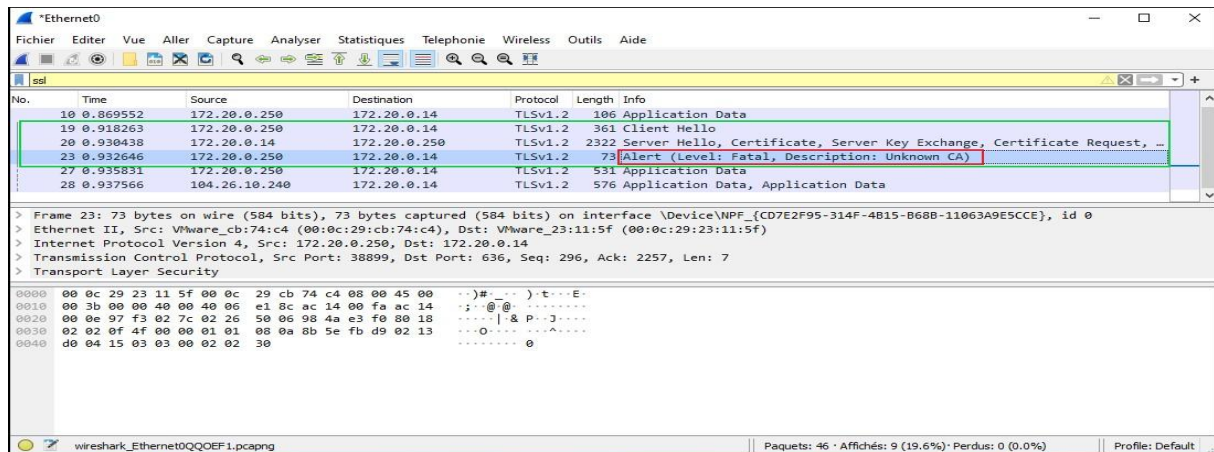
Donc l'authentification LDAPS ne fonctionne pas, on va essayer de faire un diagnostic en faisant une capture de trames avec Wire Shark pour identifier le problème.

On installe Wire Shark sur notre contrôleur de domaine, puis on déclenche une capture de trame en même temps on exécute la manipulation précédente

On fait un filtre ssl/tls dans notre capture de trame

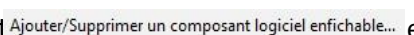
Les trames qui représentent l'échange entre pfsense et le contrôleur de domaine sont encadrée en vert :

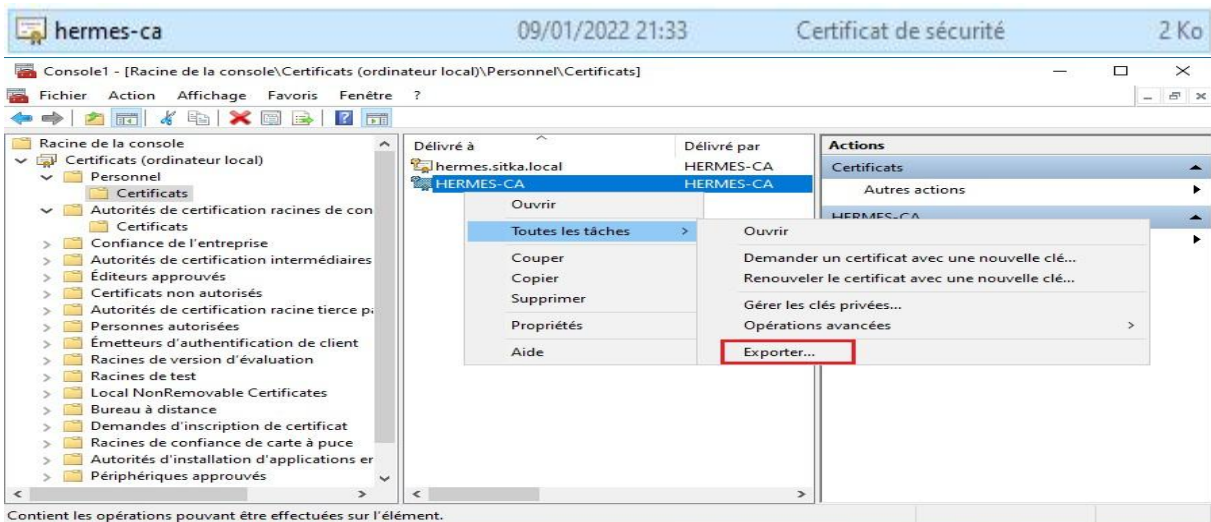
- Le dialogue commence par **client hello** la source est pfsense destination le hermes
- Hermes répond par **server hello** et présente son certificat à pfsense
- Pefsense répond par une alerte il ne reconnaît pas le certificat



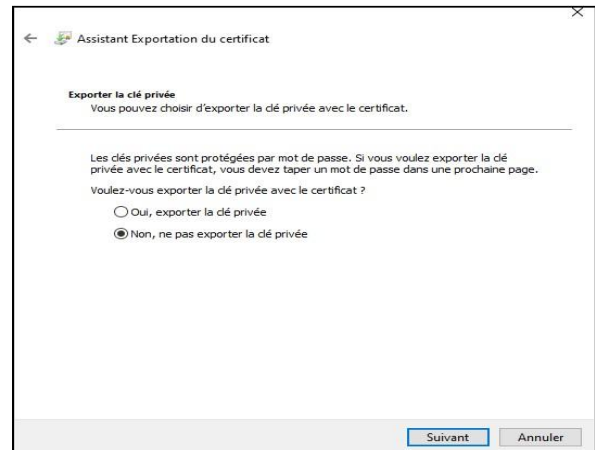
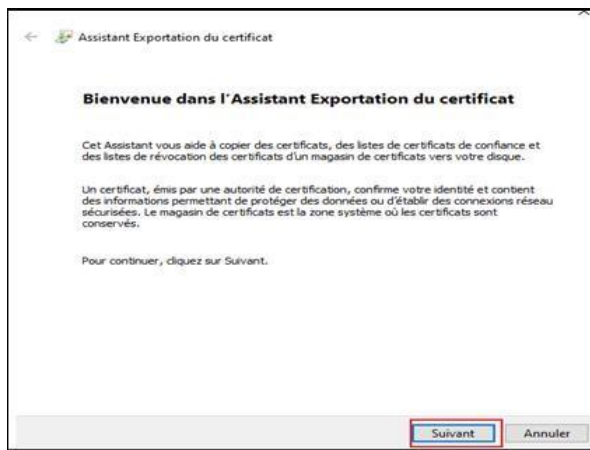
Donc le souci vient du fait que le certificat présenté par Hermes n'est pas reconnu par pfsense **pour contourner ce problème on va importer le certificat de l'autorité de certification racine installée sur hermes sur notre serveur pfsense.**

c- Exportation du certificat de l'autorité de certification hermes

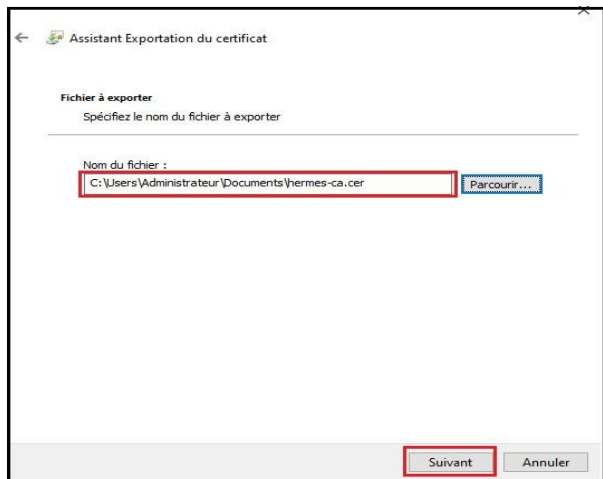
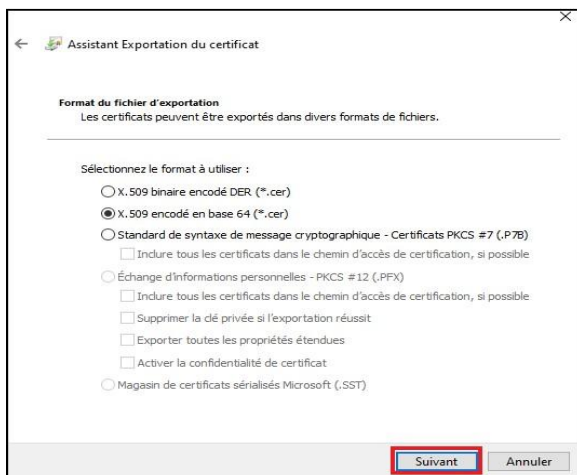
- On ouvre une console mmc et on rajout  e composant certificat pour ordinateur
- On exporter le certificat de l'autorité de certification racine au format '.cer' on l'enregistre avec le nom qu'on choisit



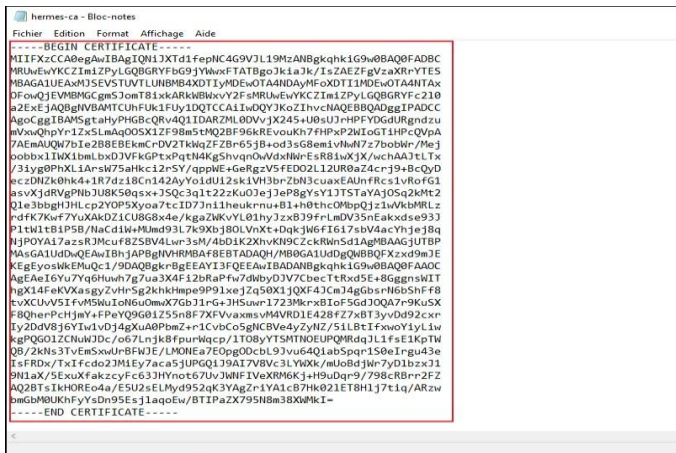
On choisit de ne pas exporter la clé privée



On choisit le format X.509 encodé DER (*.cer) et en l'enregistre avec le nom hermed-ca.cer

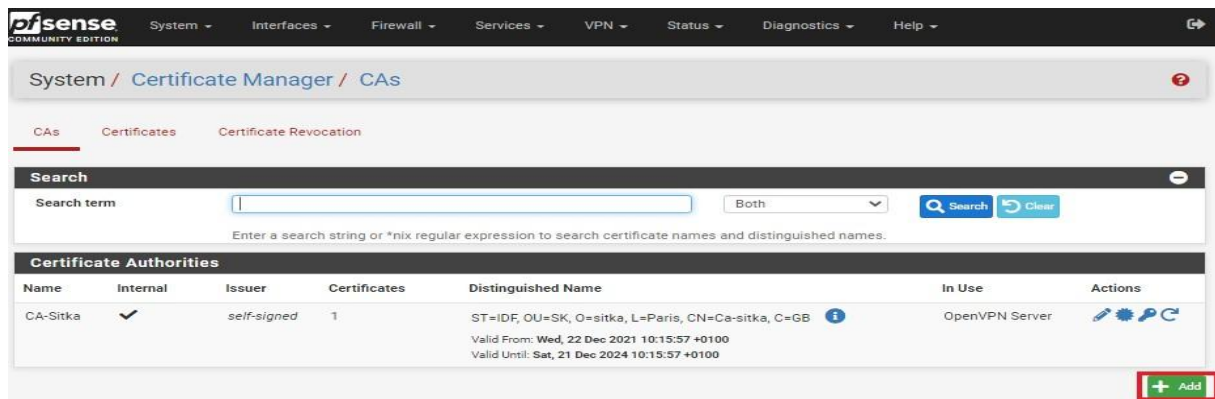


- J'ouvre mon fichier hermes-ca.cer avec le bloc note pour afficher le certificat de l'autorité de certification après on le copie pour l'insérer dans pfSense



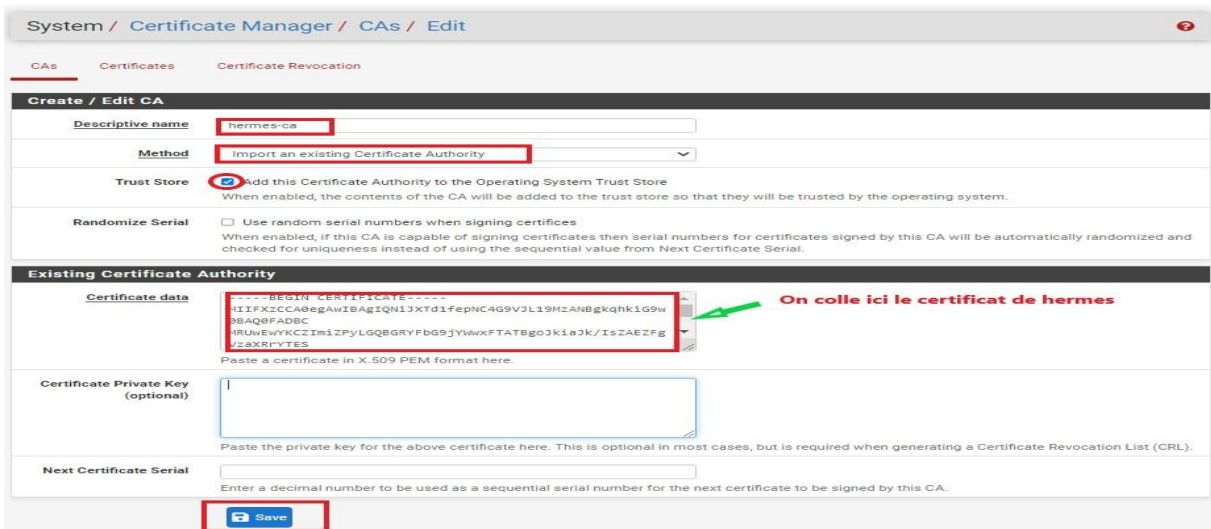
d- Importation du certificat de l'autorité de certification racine

On va sur **certificate manager + Cas** on clique sur **ad** pour rajouter une autorité de certification



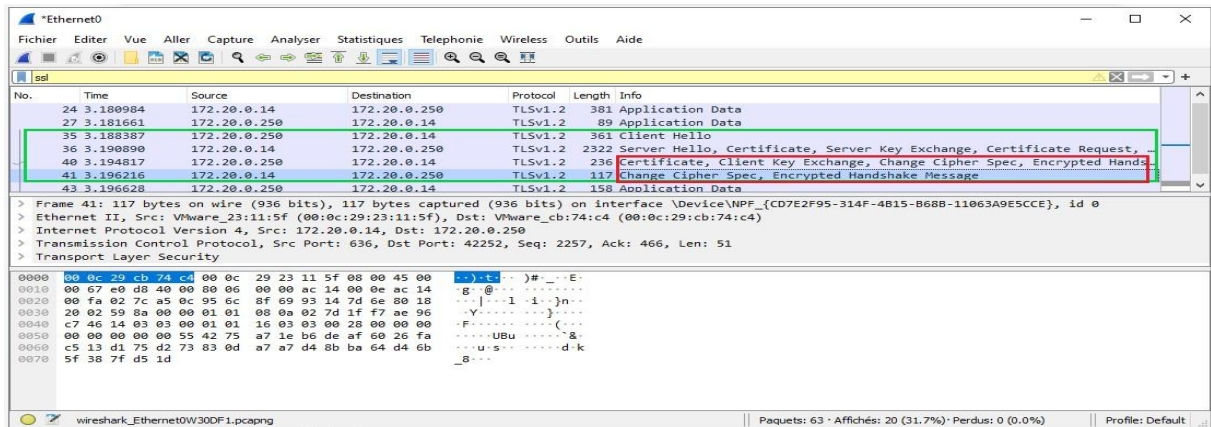
On donne un nom à notre autorité de certification et on choisit comme méthode **import an existing Certificate Authority**

Après il suffit de coller le certificat de l'autorité de certification racine hermes dans le champ **certificate data**



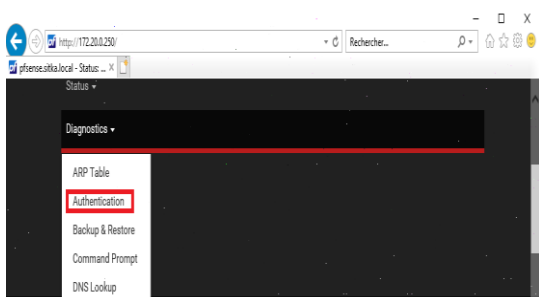
e- Test de la connexion ssl entre pfSense et le contrôleur de domaine

On constate qu'il n'y'a plus de messages d'erreurs que le message handshake (poignée de main) est établie et crypté on peut maintenant revenir pour terminer de remplir notre formulaire authentification LDAPS



3- Utilisation des authentifications LDAP et LDAPS sur le serveur pfSense

Je vérifie l'authentification Active directory de mon compte **kaiser** à partir de l'interface web de pfSense, on va sur diagnostic + authentification

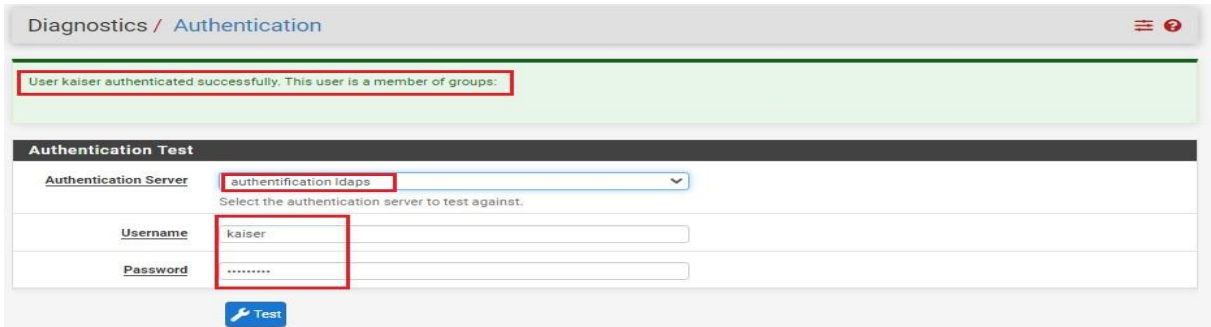


a- Vérification de l'authentification LDAP et LDAPS

- L'authentification Active directory en utilisant LDAP a réussi

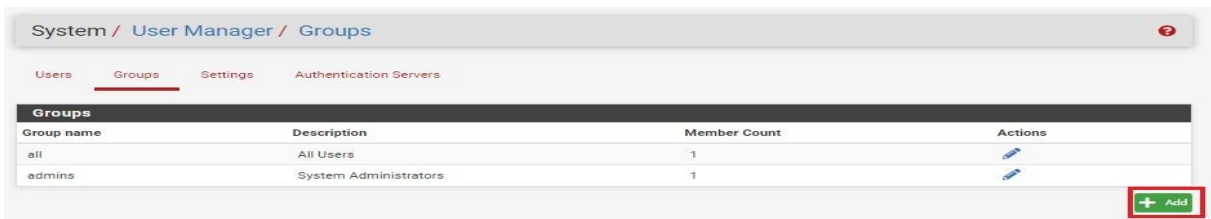


- L'authentification Active directory en utilisant LDAPS a réussi

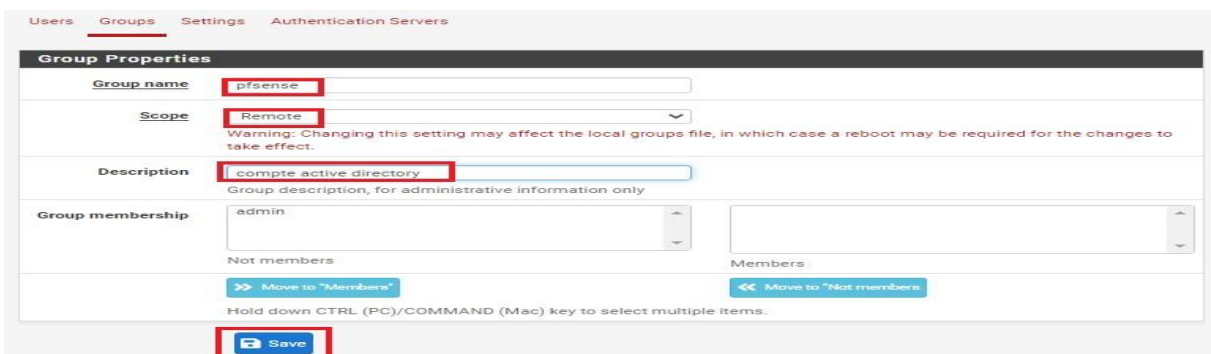


b- Configuration des groupes et des utilisateurs sur pfsense

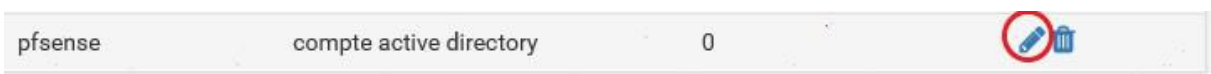
On crée un groupe de même nom que celui crée sur active directory le groupe **pfsense** on clique sur **add** pour rajouter un groupe



On remplit les champs comme indiqué ci-dessous puis on sauvegarde



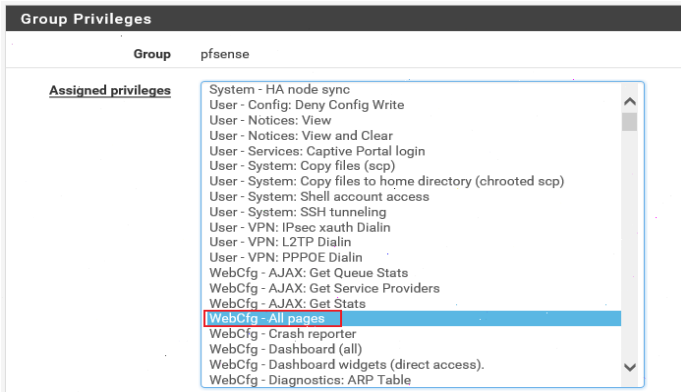
Dès que le groupe est créé je l'édite pour lui donner les droits admin



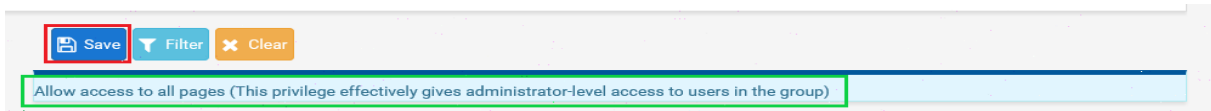
Dans assigned Privilèges je clique sur add



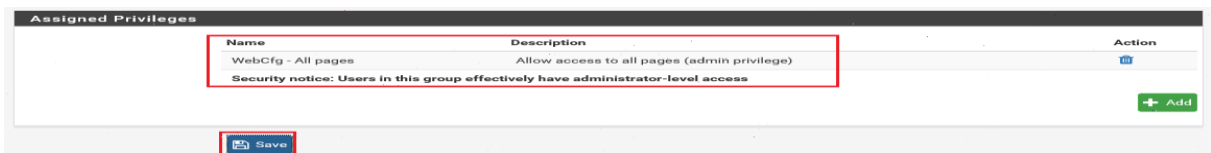
Je sélectionne **WebCfg – All pages** comme droit



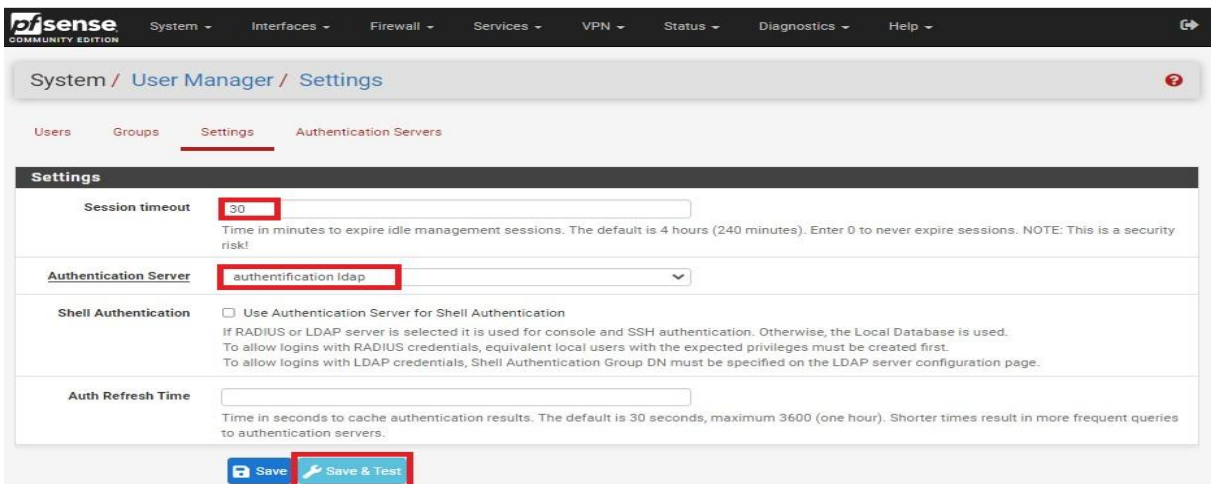
On remarque le groupe pfsense aura tous les droits



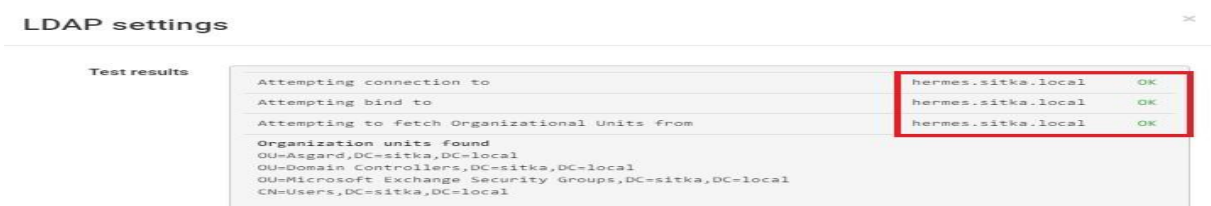
On enregistre notre configuration



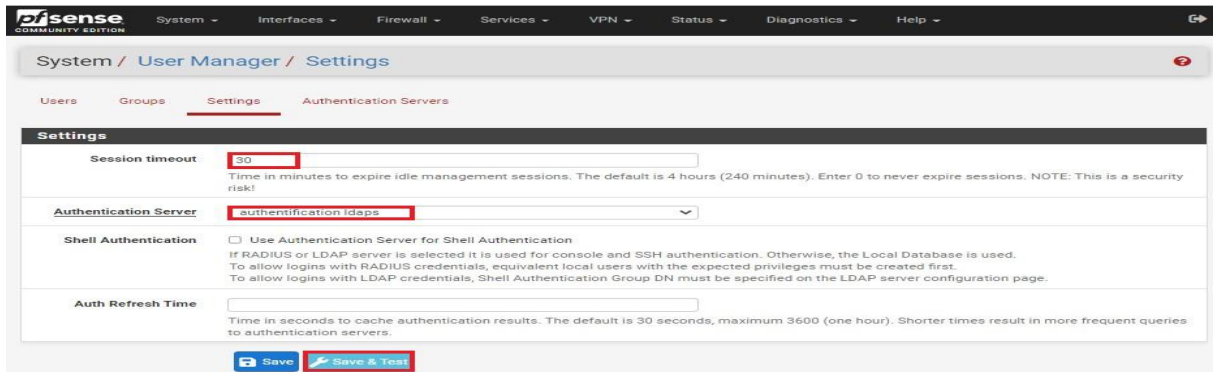
On fait un test de connexion avec la base LDAP



La connexion a réussi



On fait un test de connexion avec la base LDAPS



La connexion a réussi



On teste notre configuration en se connectant avec notre compte **kaiser**



On verifie bien qu'on est connecter avec un compte issue de la base LDAP

