



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

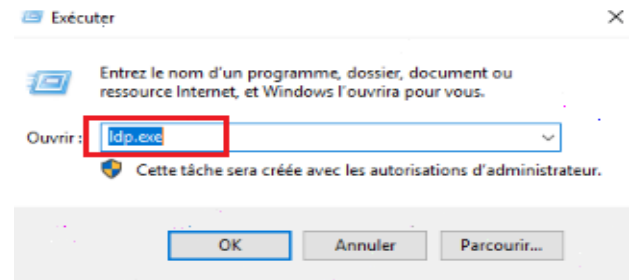
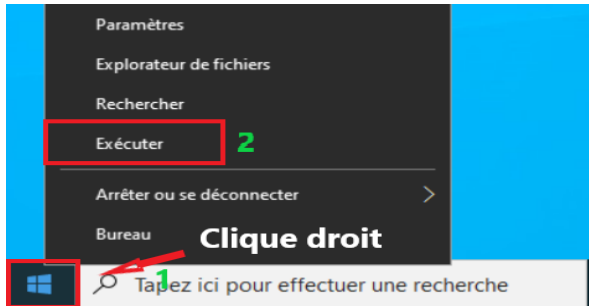
E- Création de l'authentifications LDAP

- 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

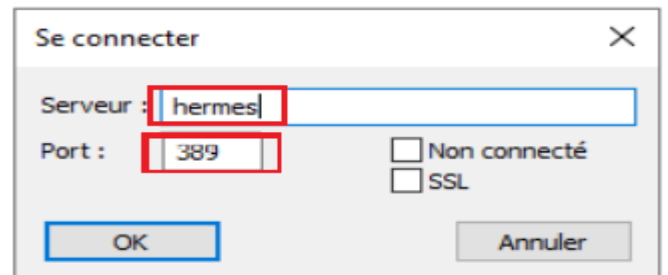
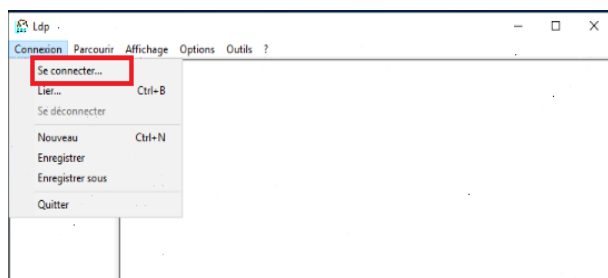
A- Test de la connectivité LDAP et LDAPS sur le serveur active directory hermes

1- Connectivité LDAP

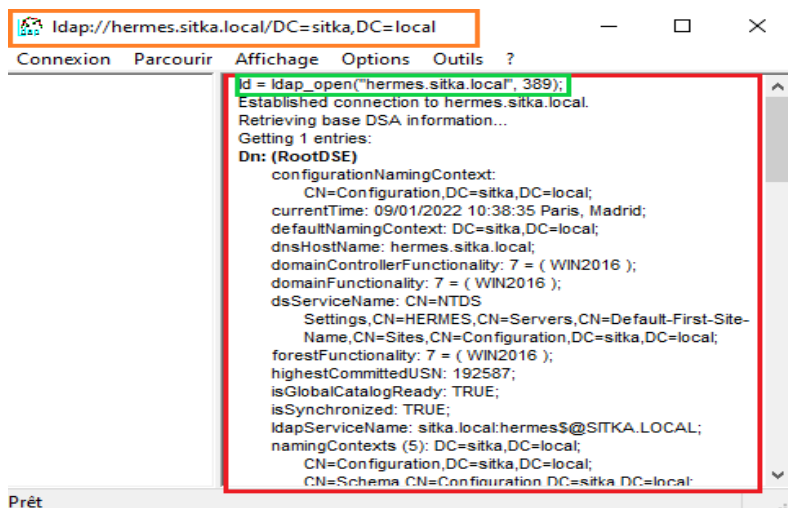
Sur le contrôleur de domaine on test la connectivité LDAP standard, donc clique droit sur le menu démarrer + exécuter puis on tape **ldp.exe** pour ouvrir l'explorateur LDAP



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**

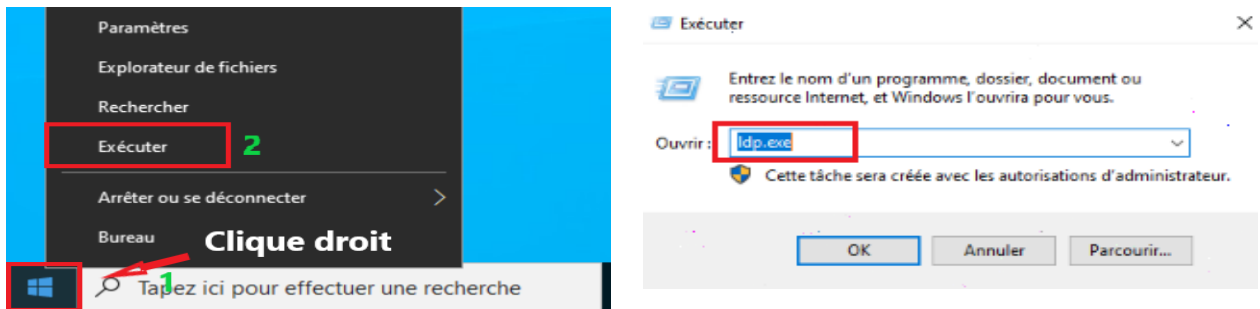


La connexion à la base d'annuaire fonctionne on peut identifier les partitions d'annuaire

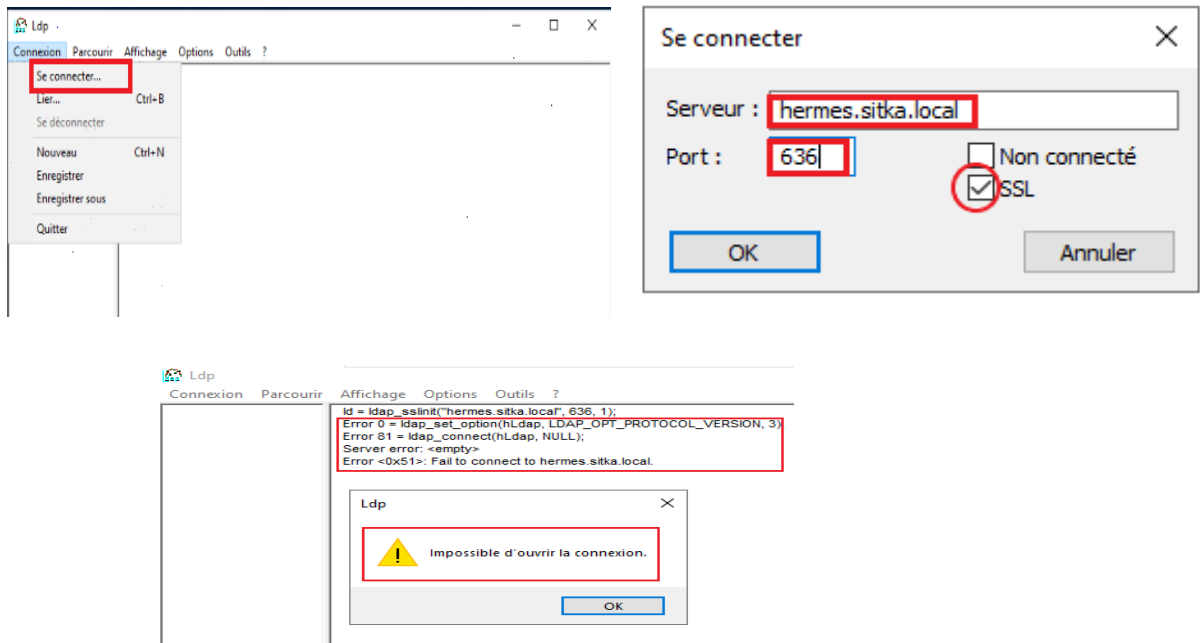


2- Connectivité LDAPS (LDAP sur SSL)

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)

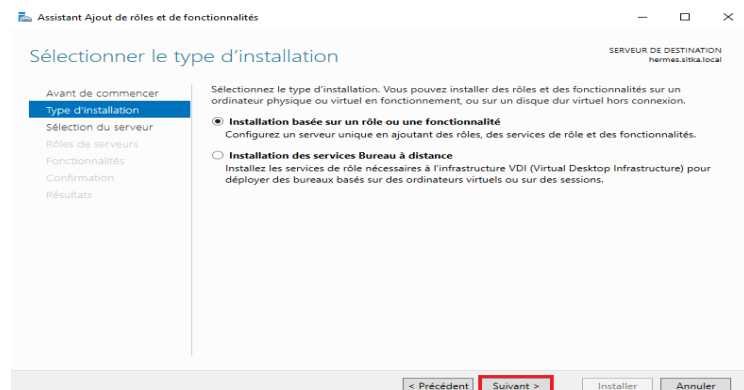
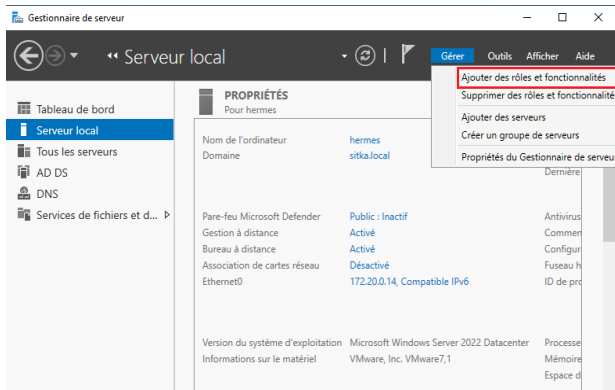
Pour notre procédure on choisira la première méthode, Donc il faut installer une autorité de certification afin de tirer parti de LDAPS

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

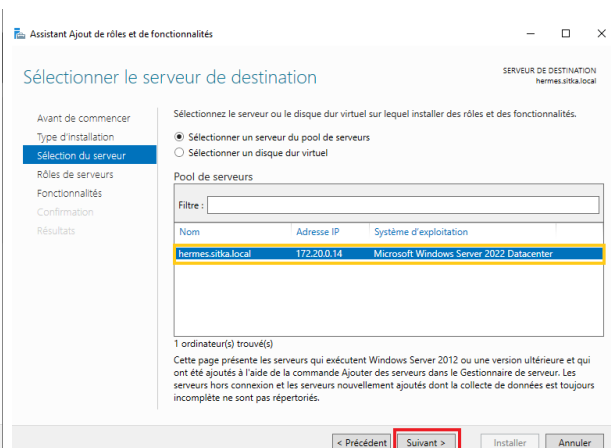
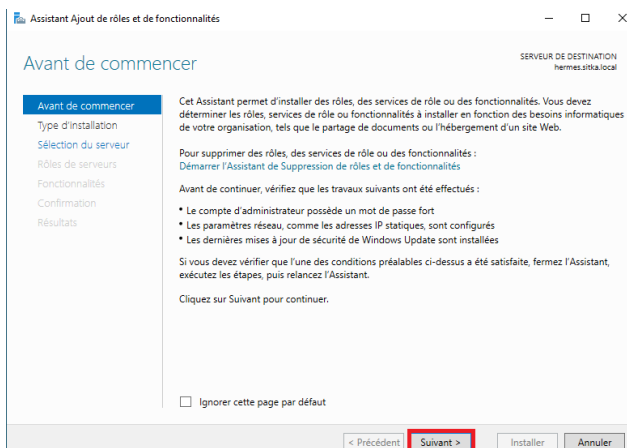
Il est nécessaire d'installer le service autorité de certification. Pour fournir au contrôleur de domaine un certificat qui permettra au service LDAPS d'opérer sur le port 636.

i- Ajouter le rôle certificat sur hermes

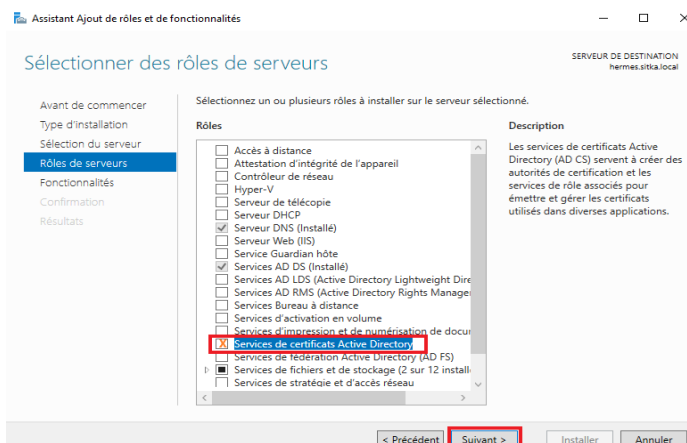
Accédez au menu Gérer et cliquez sur Ajouter des rôles et des fonctionnalités.



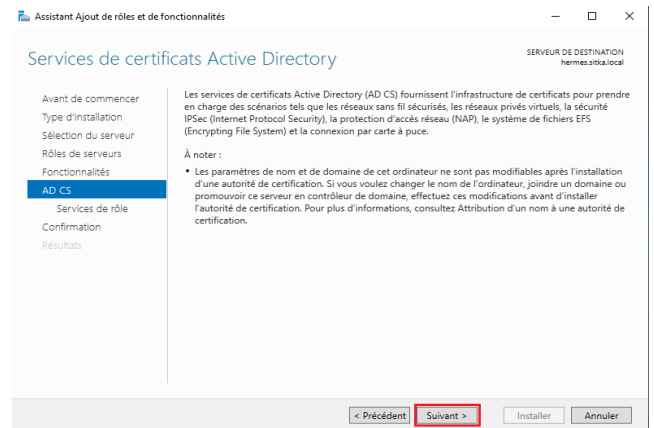
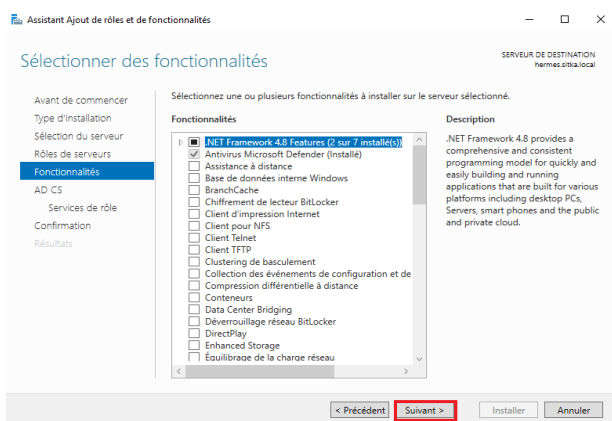
On vérifie le nom et l'adresse IP de notre serveur on clique après sur suivant



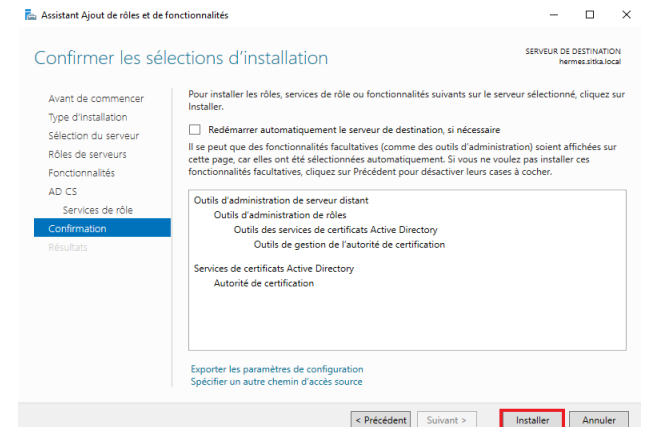
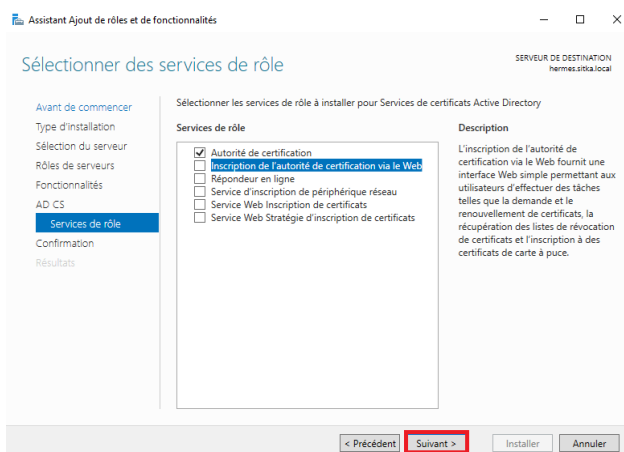
On coche Services de Certificats Active Directory et on rejoute les fonctionnalités



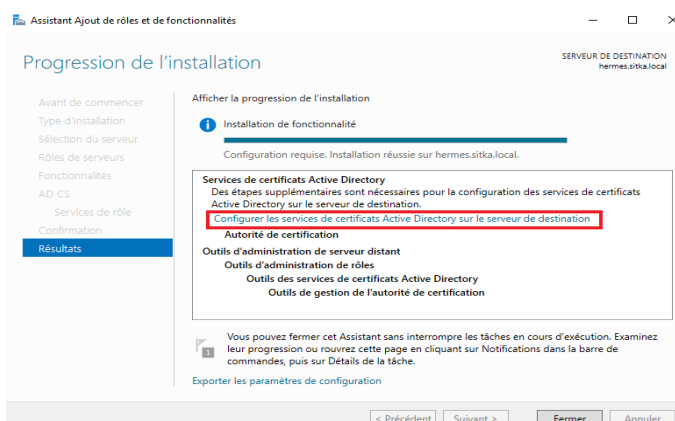
Sur les deux Boites de dialogues ci-dessous on laisse tout par défaut en faisant suivant.



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



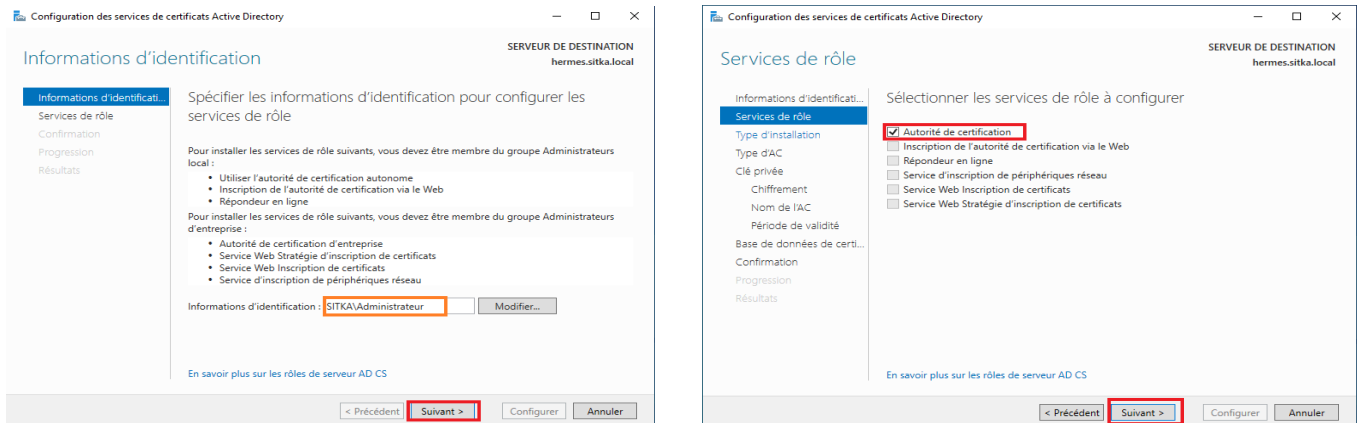
Dernière étape on clique sur le lien **Configurer les services Active Directory sur le serveur de destination**



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

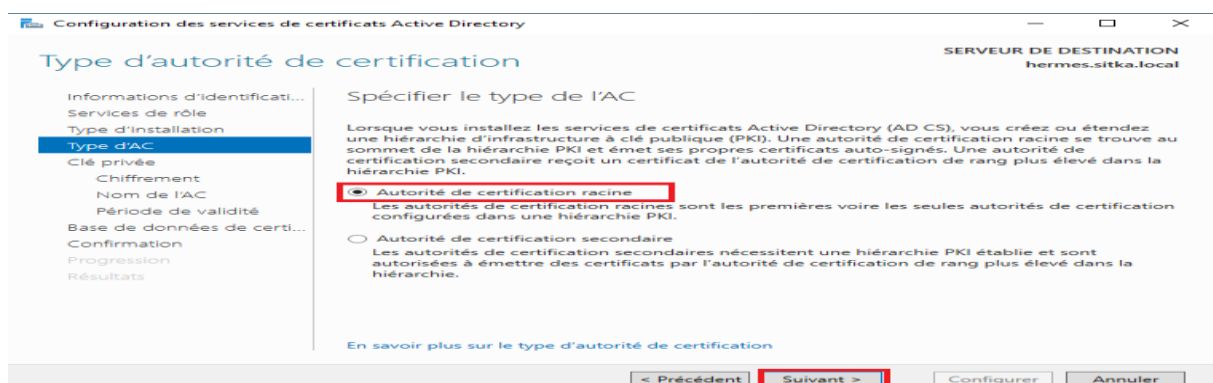


On sélectionne **Autorité de certification d'entreprise** afin que l'autorité de certification puisse utiliser l'annuaire LDAP



On sélectionne autorité de certification racine

Ce type d'autorité de certification couplé avec un Active Directory est utile pour un intranet mais est déconseillée 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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
hermes.sitka.local

Clé privée

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type de la clé privée

Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.

☒ **Créer une clé privée**
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.

☐ Utiliser la clé privée existante
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.

☐ Sélectionner un certificat et utiliser sa clé privée associée
Sélectionnez cette option s'il existe un certificat sur cet ordinateur ou pour importer un certificat et utiliser sa clé privée associée.

☐ Sélectionner une clé privée existante sur cet ordinateur
Sélectionnez cette option si vous avez conservé les clés privées d'une installation antérieure ou pour utiliser une clé privée d'une autre source.

[En savoir plus sur la clé privée](#)

< Précédent **Suivant >** Configurer Annuler

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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
hermes.sitka.local

Chiffrement pour l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement :
RSA#Microsoft Software Key Storage Provider

Longueur de la clé :
4096

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :
SHA256
SHA384
SHA512
SHA1

☐ Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent **Suivant >** Configurer Annuler

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

Configuration des services de certificats Active Directory

SERVEUR DE DESTINATION
hermes.sitka.local

Nom de l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :
HERMES-CA

Suffixe du nom unique :
DC=sitka,DC=local

Aperçu du nom unique :
CN=HERMES-CA,DC=sitka,DC=local

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent **Suivant >** Configurer Annuler

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.

Configuration des services de certificats Active Directory

PERIODE DE VALIDITE

Informations d'identification... Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi... Confirmation Progression Résultats

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

15 Années

Date d'expiration de l'AC : 09/01/2025 09:45:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

En savoir plus sur la période de validité

< Précédent Suivant > Configurer Annuler

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

Configuration des services de certificats Active Directory

Base de données de l'autorité de certification

Informations d'identification... Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de l'autorité de certification Confirmation Progression Résultats

Spécifier les emplacements des bases de données

Emplacement de la base de données de certificats : C:\Windows\system32\CertLog

Emplacement du journal de la base de données de certificats : C:\Windows\system32\CertLog

En savoir plus sur la base de données de l'autorité de certification

< Précédent Suivant > Configurer Annuler

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

On doit obtenir le message configuration réussie

Configuration des services de certificats Active Directory

Résultats

Informations d'identification... Services de rôle Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de l'autorité de certification Confirmation Progression Résultats

Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :

Services de certificats Active Directory

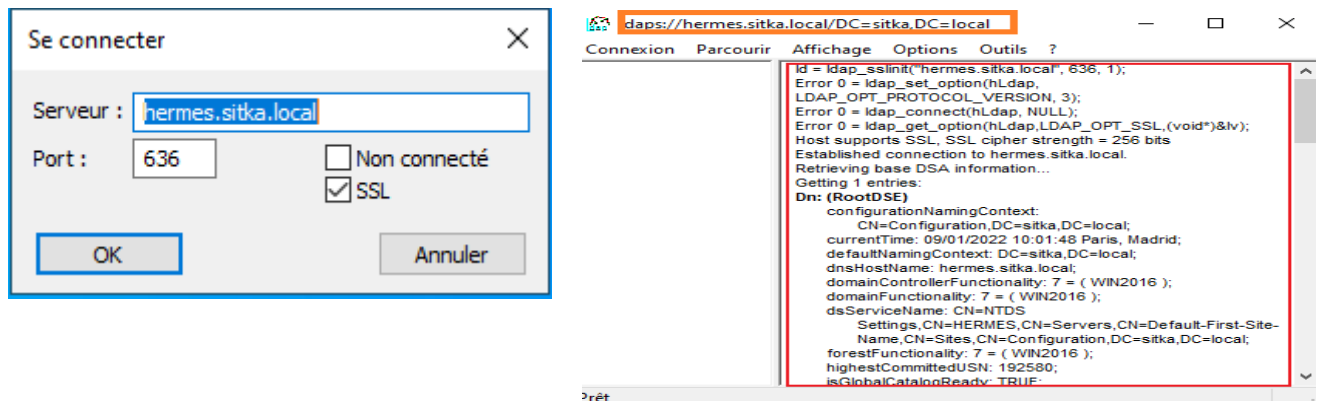
Autorité de certification Configuration réussie

En savoir plus sur la configuration de l'autorité de certification

< Précédent Suivant > Fermer Annuler

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



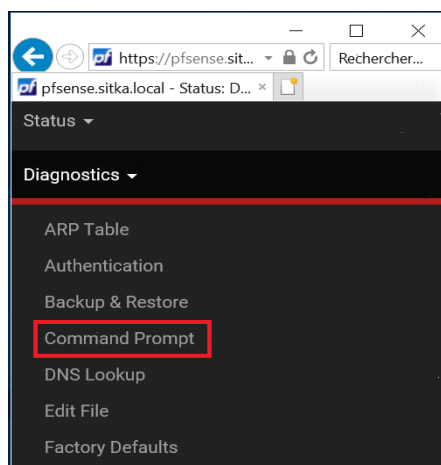
B- Test de la connectivité LDAP et LDAPS (LDAP sur SSL) sur heimdall (pfsense)

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
```

The capabilities offered here can be dangerous. No support is available. Use them at your own risk!

```
openssl s_client -showcerts -connect 172.20.0.14:636
```



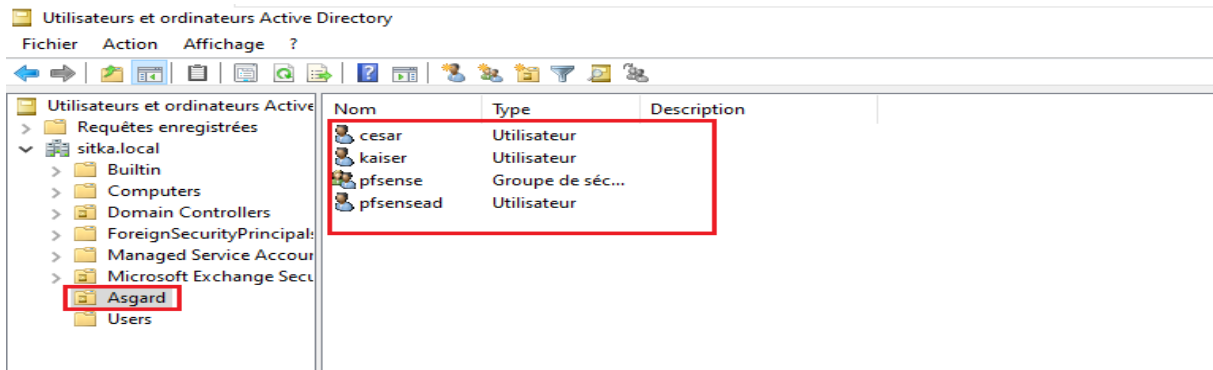
Shell Output - openssl s_client -showcerts -connect hermes.sitka.local:636

[illegible]

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




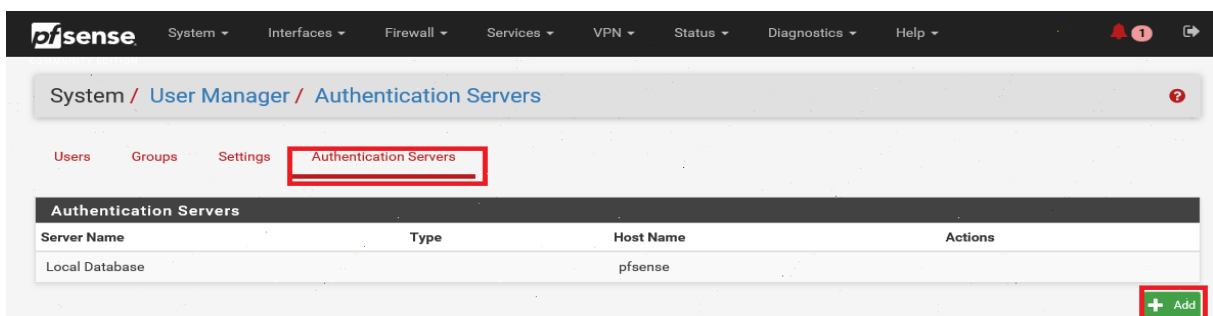
D- Création des authentifications LDAP et LDAPS sur le serveur pfSense

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=pfsensead,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:
If LDAP server is used for shell authentication, user must be a member of this group and have a valid posixAccount attributes to be able to login.
Example: CN=Remoteshellusers,CN=Users,DC=example,DC=com

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'authentications LDAPS

a- Création du formulaire de l'authentification LDAPS

Users Groups Settings **Authentication Servers**

Server Settings

Descriptive name: authentification 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 on 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

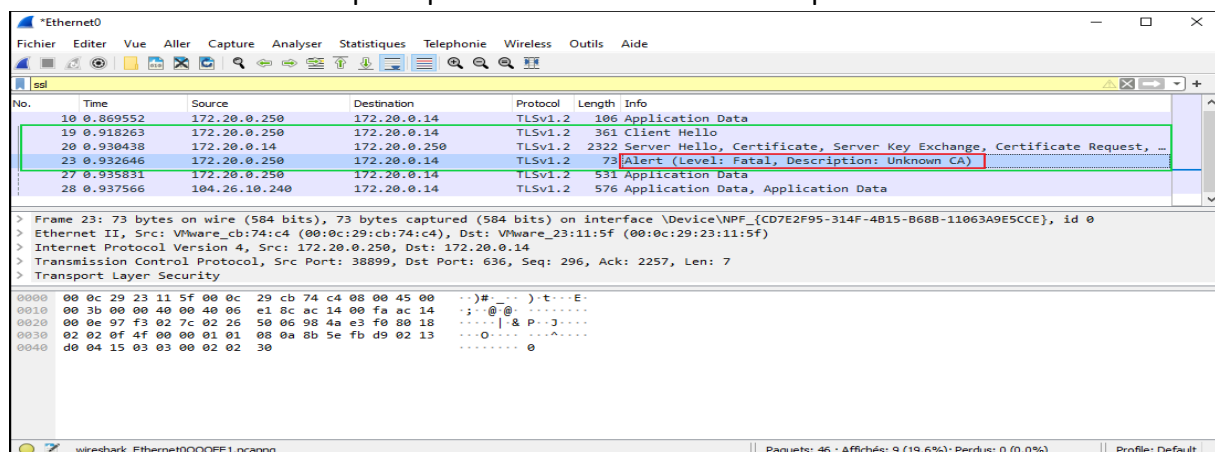
Donc l'authentification LDAPS ne fonctionne pas, on va essayer de faire un diagnostic en faisant une capture de trames avec Wire Shark pour identifier le problème.

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

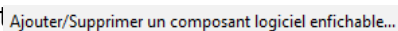
Les trames qui représentent l'échange entre pfsense et le contrôleur de domaine sont encadrées en vert :

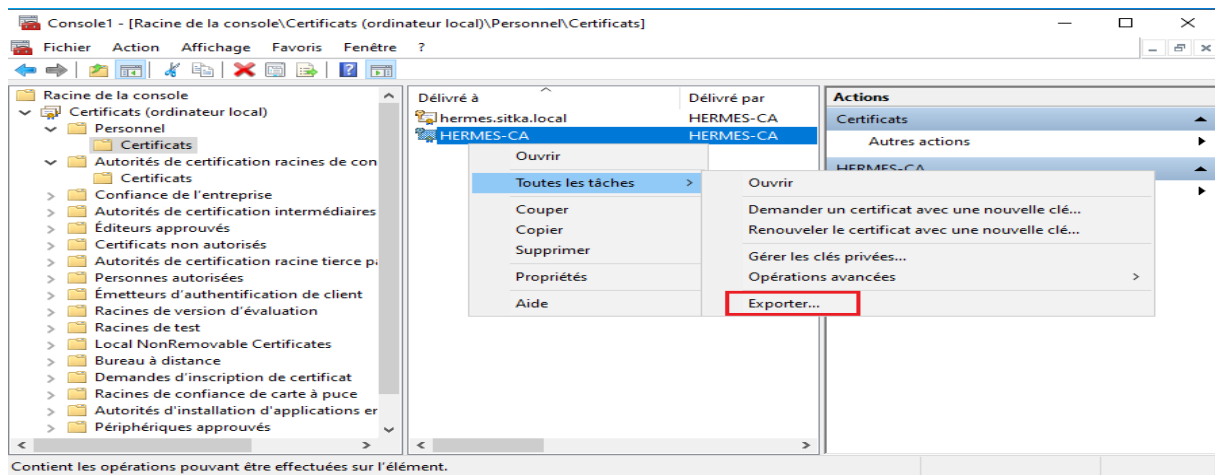
- Le dialogue commence par **client hello** la source est pfsense destination le hermes
- Hermes répond par **server hello** et présente son certificat à pfsense
- Pfsense répond par une alerte il ne reconnaît pas le certificat



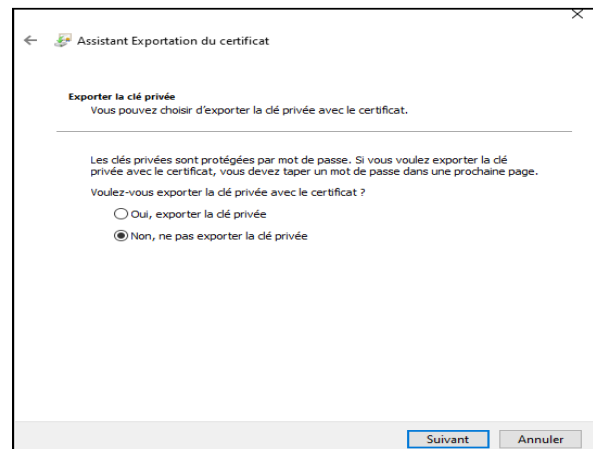
Donc le souci vient du fait que le certificat présenté par Hermes n'est pas reconnu par pfsense **pour contourner ce problème on va importer le certificat de l'autorité de certification racine installée sur hermes sur notre serveur pfsense.**

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

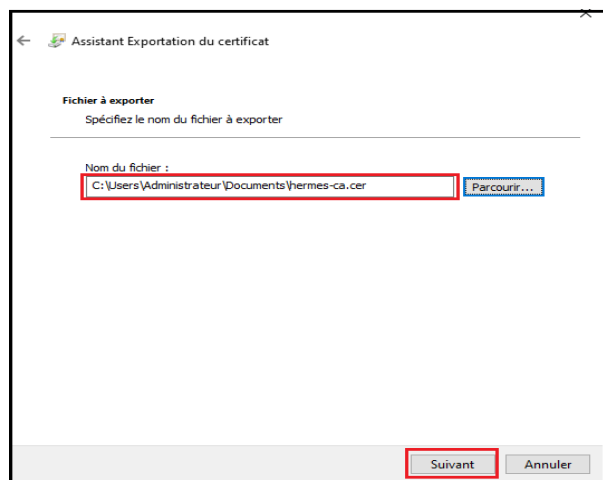
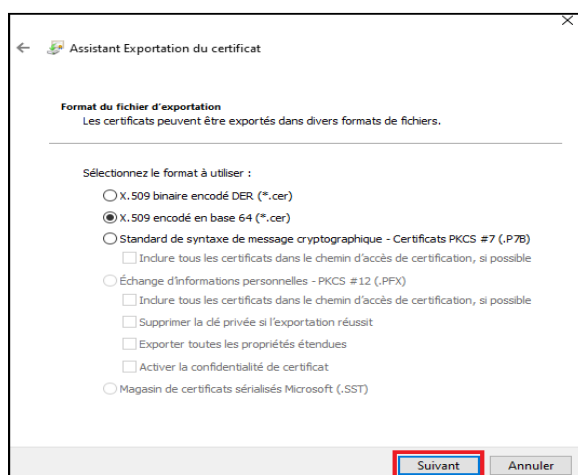
- On ouvre une console mmc et on rajoute  le composant certificat pour ordinateur
- On exporte le certificat de l'autorité de certification racine au format '**.cer**' on l'enregistre avec le nom qu'on choisit



On choisit de ne pas exporter la clé privée



On choisit le format X.509 encodé DER (*.cer) et on 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

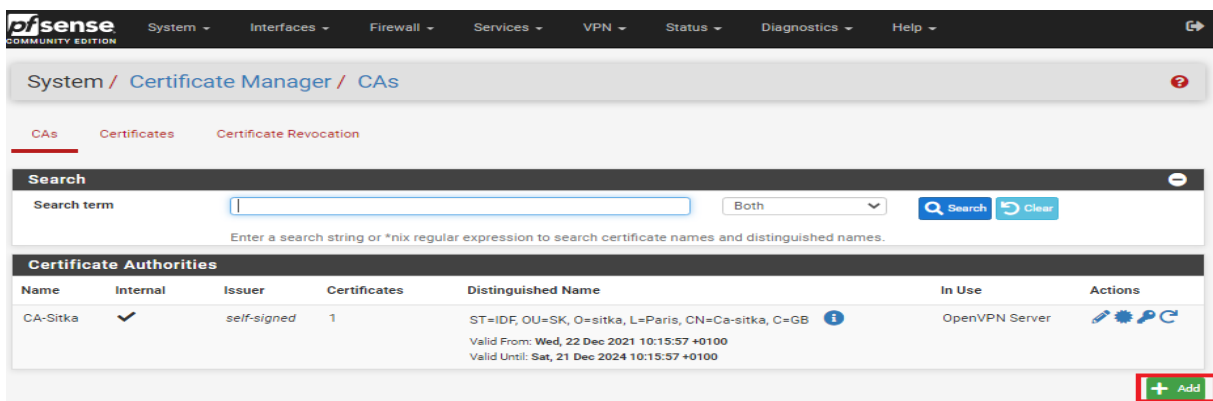
```

hermes-ca - Bloc-notes
Fichier Edition Format Affichage Aide
-----BEGIN CERTIFICATE-----
MIIFXzCCA0egAwIBAgIQ1JXTd1FepNC4G9VJL19MzANBgkqhkiG9w0BAQ0FADBC
MRUwEwYKKzIm1ZPyLQGBGRYFbG9jYmVwFTATBgo3k1a3k/1sZAEZFgVzaXRnYTES
MBAGAlUEaxMjSEVSVUVTUNBMB4XD01YHDEw0TAANDAYHfcoXDTI1HDEw0TAANDAX
DFowQ2JlVnBMcGcgc5JomTB1skARkMBwVvY2F5aMLuEwYKKzIm1ZPyLQGBGRYFz.210
a2ExEjA0BgNVBAMTCUhhFuk1Fuy1DQTCa31wDQYJKoZIhvcNAQEBBQADggIPADCC
AgoCggIBAM5gtahyPHGBcQRv4Q1IDARZML0DVvJX245+U0sU3rHPFYDgdURgndzu
mVxaQhpyr12x5LmaQ00S1ZF98m5tmQ2BF96kREvouKh7FHPxP2W1oGT1HPcQVpA
7AEwAUGN7YoIe2BBEBEkcNDV21kwaZfZBf65jB+vod3jG8eulVhWf7z7b00W/rMeJ
pobbx11Wx1bmLx0JVFkGpTxPqtN4KqShvqnOvVdxNMR=EsR81wXjX/wchAA3tLTx
/31yg8PhXL1A=sW75aHk12r5V/qppWE+GeRgzV5FED02L2UR0aZ4crJ9+8cQyD
ec2DN2k0hk4+1R7dz18Cn142AyYo1dU12sk1VH3brZbN3cuaxEAUnFRcs1Vf0rG1
h+vXjdrVgPb0JUBK50gsw+35Qc3q1t22Ku07eJjeP8gYvY1TSTaYAJ05g2kht2
Q1e3bbgHJHLcp2YOP5Xyaa7tcID7Jn11heukrnu+81+h0thcOMbpQjz1wVkbMRLz
rdfK7Kuf7YUxAKDZ1CUBG8x4e/kgaZWKvYL01hyJzx8J9frLmOV35nEakxdse93J
P1tw1tB1P5B/Nacd1W+Mlmd93L7k9XbJ80L VnXtc+Dqk jW6F1617+bV4acYhjeJ8q
hJP0VAl7azs3KcuF8Z5BV4Lwv3mJ/Ab01K2XhvK9KZc+kRmSd1AgMBAAQJUTBP
MAsGA1UdQwQEAwIBhJAP8gNVHRMBAF8BETADAQH/MB0GA1UdDgQNBQFXXzd9mJE
KEgEYosMkEMuQc1/9DAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQ0FAAOC
AgEAAIEYU7Yq0Huh7g7ua3X4F12bRaPfw7dmbYDJV7CbectrXsd5E+8GggnsWIT
hg14FokVXasyZvHr5g2kHhEpe9P91ueJZq50K1jQXF4jCn4G6srH6G5hFf8
tvXCUvV51fV5MuIoN6uOmX7G631rG+3H5uwr1723Mkrx81oF56d30QA7r9KuSX
F8QherPchjwY+FPeYQ9G81Z55n87FXFVvaxmsvM4VRD1E428fZ7x8T3yvDd92cxr
ly2DdV8j6Y1w1v0j4gXua0PbmZ+1CvbCo5gHCBVe4y2yNZ/51Lbt1fxwoY1yL1w
kqPQ6D1ZCnuhJD/c067Lnjk8FpurWqcp/1T08YTSMTNOEUPQRuqJ11Fs1KpTW
Q8/2kNs3TvEmSxwUrfWJJE/LMONEa7EOpg0Dcbl9Jvu64Q1ab5sqn150eIngu43e
TsFRDx/TxIfcd02Jm1Ey7aca5jUPGQ19A17V8Vc3LY0Kk/mLoBdJw7yD1bz3J1
9N1Ax/5ExuXfakzcyFc63JHYnot67UvJWNP1VeXRM6Kj+H9u0q9/798cRBRr2FZ
AQ2BTs1KHORECo4a/FSU2eLUhy0952qK3YAgZrYAlC87Hk021E7H1j7c1q/ARzw
bmG0BUKHyYsdn55E+j1aqpEw/BT1PaZK795H8m38X0WkL=
-----END CERTIFICATE-----

```

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**

System / Certificate Manager / CAs / Edit

CA's Certificates Certificate Revocation

Create / Edit CA

Descriptive name: hermes-ca

Method: Import an existing Certificate Authority

Trust Store: ☒ Add this Certificate Authority to the Operating System Trust Store
When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.

Randomize Serial: ☐ Use random serial numbers when signing certificates
When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Existing Certificate Authority

Certificate data: -----BEGIN CERTIFICATE-----
MIIFXzCCARegAwIBAgIQN1JXTd1fepNC4G9VJL19MzANBgkqhkiG9w
BAQ0FADBC
RUnEWYKCZIm1ZPyLQGBGRYFbG9JYwxFATBgoJkiaJk/IsZAEZFg
ZjZXRvYTES

On colle ici le certificat de hermes

Certificate Private Key (optional):

Next Certificate Serial:

Save

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

*Ethernet0

Fichier Editor Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide

ssl

No.	Time	Source	Destination	Protocol	Length	Info
24	3.189984	172.20.0.14	172.20.0.250	TLSv1.2	381	Application Data
27	3.181661	172.20.0.250	172.20.0.14	TLSv1.2	89	Application Data
35	3.188387	172.20.0.250	172.20.0.14	TLSv1.2	361	Client Hello
36	3.190890	172.20.0.14	172.20.0.250	TLSv1.2	2322	Server Hello, Certificate, Server Key Exchange, Certificate Request
40	3.194817	172.20.0.250	172.20.0.14	TLSv1.2	236	Certificate, Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
41	3.196216	172.20.0.14	172.20.0.250	TLSv1.2	117	Change Cipher Spec, Encrypted Handshake Message
43	3.196628	172.20.0.250	172.20.0.14	TLSv1.2	158	Application Data

> Frame 41: 117 bytes on wire (936 bits), 117 bytes captured (936 bits) on interface \Device\NPF_{CD7E2F95-314F-4B15-B68B-11063A9E5CCE}, id 0
> Ethernet II, Src: VMware_23:11:5f (00:0c:29:23:11:5f), Dst: VMware_cb:74:c4 (00:0c:29:cb:74:c4)
> Internet Protocol Version 4, Src: 172.20.0.14, Dst: 172.20.0.250
> Transmission Control Protocol, Src Port: 636, Dst Port: 42252, Seq: 2257, Ack: 466, Len: 51
> Transport Layer Security

0000 00 0c 29 cb 74 c4 00 0c 29 23 11 5f 08 00 45 00 ...)#...E
0010 00 67 a0 d8 40 00 00 00 ac 14 00 0e ac 14 ... @...n...
0020 00 fa 02 7c a5 0c 95 6c 8f 69 93 14 7d 6e 80 18 ... }...i...n...
0030 20 02 59 8a 00 00 01 01 08 0a 02 7d 1f f7 ae 96 ... Y... ..
0040 c7 46 14 03 03 00 01 16 03 03 00 28 00 00 00 ... P... ..
0050 00 00 00 00 55 42 75 a7 1e b6 de af 60 26 faUBU...&...
0060 c5 13 d1 75 d2 73 83 0d a7 a7 d4 8b ba 64 d4 6bu...s...d...k...
0070 5f 38 7f d5 1d ... _B...

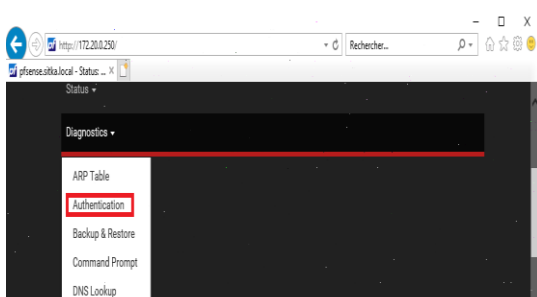
wireshark_Ethernet0W30DF1.pcapng

Paquets: 63 · Affichés: 20 (31.7%) · Perdus: 0 (0.0%)

Profile: Default

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

Diagnostics / Authentication

User kaiser authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server: authentication ldap

Username: kaiser

Password: *****

Test

- L'authentification Active directory en utilisant LDAPS a réussi

Diagnostics / Authentication

User kaiser authenticated successfully. This user is a member of groups:

Authentication Test

Authentication Server: authentication ldaps

Username: kaiser

Password: *****

Test

b- Configuration des groupes et des utilisateurs sur pfsense

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

System / User Manager / Groups

Users Groups Settings Authentication Servers

Group name	Description	Member Count	Actions
all	All Users	1	
admins	System Administrators	1	

+ Add

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

Users Groups Settings Authentication Servers

Group Properties

Group name: pfsense

Scope: Remote

Description: compte active directory

Group membership: admin

Not members: Members

Save

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

pfsense	compte active directory	0	
---------	-------------------------	---	--

Dans assigned Privileges je clique sur add

Assigned Privileges

Name	Description	Action
		+ Add

[Save](#)

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

Group Privileges

Group: pfsense

Assigned privileges

- System - HA node sync
- User - Config: Deny Config Write
- User - Notices: View
- User - Notices: View and Clear
- User - Services: Captive Portal login
- User - System: Copy files (scp)
- User - System: Copy files to home directory (chrooted scp)
- User - System: Shell account access
- User - System: SSH tunneling
- User - VPN: IPsec xauth Dialin
- User - VPN: L2TP Dialin
- User - VPN: PPPOE Dialin
- WebCfgr - AJAX: Get Queue Stats
- WebCfgr - AJAX: Get Service Providers
- WebCfgr - AJAX: Get Stats
- WebCfgr - All pages**
- WebCfgr - Crash reporter
- WebCfgr - Dashboard (all)
- WebCfgr - Dashboard widgets (direct access).
- WebCfgr - Diagnostics: ARP Table

On remarque le groupe pfsense aura tous les droits

[Save](#) [Filter](#) [Clear](#)

Allow access to all pages (This privilege effectively gives administrator-level access to users in the group)

On enregistre notre configuration

Assigned Privileges

Name	Description	Action
WebCfgr - All pages	Allow access to all pages (admin privilege)	Add

Security notice: Users in this group effectively have administrator-level access

[Save](#) [+ Add](#)

On fait un test de connexion avec la base LDAP

pfsense COMMUNITY EDITION

System - Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help

System / User Manager / Settings

Users Groups **Settings** Authentication Servers

Settings

Session timeout: 30
Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to never expire sessions. NOTE: This is a security risk!

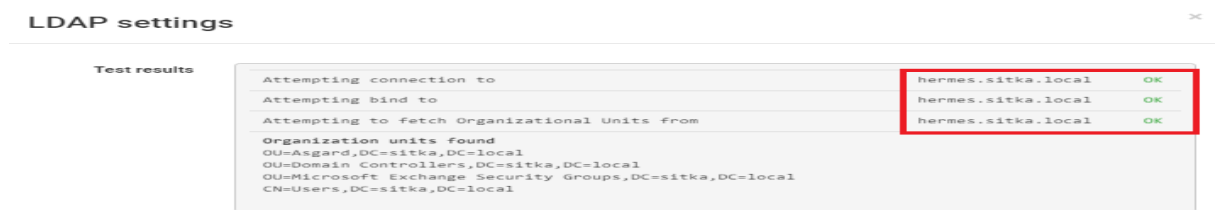
Authentication Server: authentication ldap

Shell Authentication: ☐ Use Authentication Server for Shell Authentication
If RADIUS or LDAP server is selected it is used for console and SSH authentication. Otherwise, the Local Database is used. To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be created first. To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.

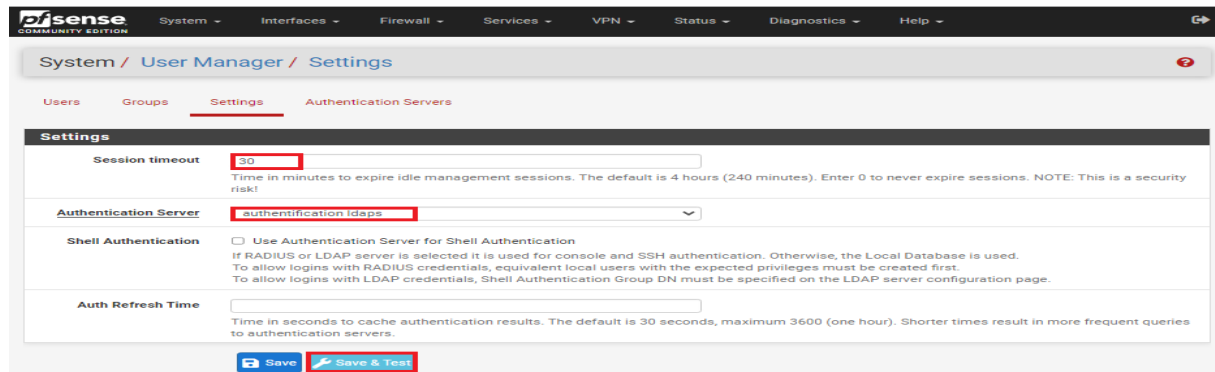
Auth Refresh Time:
Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hour). Shorter times result in more frequent queries to authentication servers.

[Save](#) [Save & Test](#)

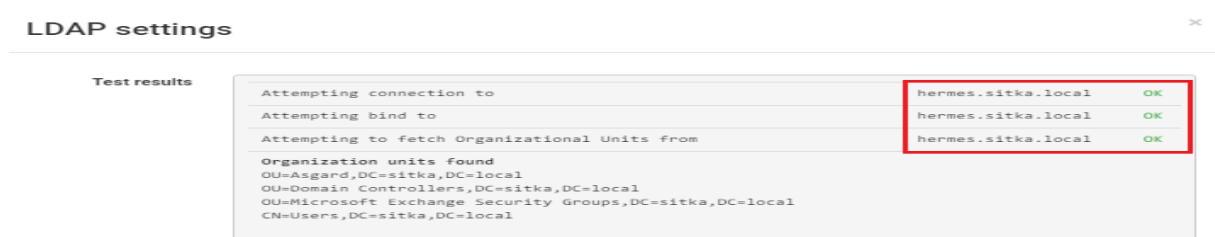
La connexion a réussi



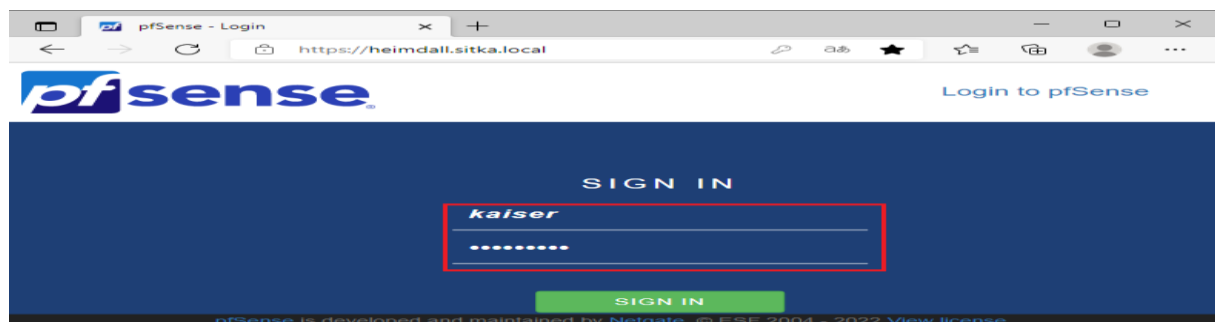
On fait un test de connexion avec la base LDAPS



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

