

PARIS PANTHÉON-ASSAS UNIVERSITÉ



Authentification LDPA et LDAPS

BTS SIO SISR 2022 – 2024

i

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

Paramètres	🖅 Exécuter	×
Explorateur de fichiers Rechercher	Entrez le nom d'un programme, dossier, document ou ressource Internet, et Windows l'ouvrira pour vous.	
Exécuter 2	Ouvrir : Idp.exe Cette tâche sera créée avec les autorisations d'administrateur.	
Arrêter ou se déconnecter > Bureau Clique droit	OK Annuler Parcourir	
 Talez ici pour effectuer une recherche		

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**

🔓 Ldp → - □ ×	
Connexion Parcourir Affichage Options Outils ?	Se connecter X
Se connecter	
Sé déconnecter	Serveur : hermes
Nouveau Ctrl+N	
Enregistrer	Port : 389 Non connecté
Enregistrer sous	SSL
Quitter	
	OK Annuler

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

Paramètres	🖾 Exécuter 🛛 🗙
Explorateur de fichiers	Entrez le nom d'un programme, dossier, document ou
Rechercher	ressource Internet, et Windows l'ouvrira pour vous.
Exécuter 2	Ouvrir: Idp.exe 🗸
Arrêter ou se déconnecter >	Cette tâche sera créée avec les autorisations d'administrateur.
Bureau Clique droit	OK Annuler Parcourir
Talez ici pour effectuer une recherche	

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

😭 Ldp 🕞	- 🗆 ×	Se connecter	×
Connexion Parcourr Affichage Options Outils ? Se connecter Lier Se déconnecter		Serveur : hermes.sitka.local	
Nouveau Ctrl+N Enregistrer Enregistrer sous		Port : 636 Non connecté	
Quitter		OK Annuler	
Connexion Parcourin	Affichage Options Outils ?		
	Id = Idap_sslint(Thermes.sitka.locaf, 636, 1); Error 6 = Idap_sot_option(hLdap, LDAP_OPT_PROTO Error 6 = Idap_connect(hLdap, NULL); Server error; «empty» Error -0x51>: Fail to connect to hermes.sitka.local.	COL_VERSION, 3)	
	Ldp >	× 	

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

Assistant Ajout de rôles et de fonctionnalités Sélectionner des services de rôle Avant de commencer Type d'initializion Sélection du serveurs Rôles de ser	- C × SERVEUR DE DESTINATION Memorialitation de certificats Active Directory Description Euróption de l'autorité de certificats de Veb fournit une interface Web simple permettant aux utilisations d'infecture des tables teneouvellement de certificats, la	Assistant Ajout de rôles et de fonctionnalités Confirmer les sélections d'installation Avant de commencer Type d'installation Sélection du serveur Rôles de serveurs Fonctionnalités D CS Services de rôle Outlis d'administration de srèuer ui distan	– – – – – – – – – – – – – – – – – – –
Services de rôle Confirmation Résultats	récupération des listes de révoc ation de certificate et l'incorpion à des certificats de carte à puce.	Confirmation Dublis des services de certificat Resultars	s Active Directory onté de certification Précédent Sulvant > Installer Annuler

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

Progression de l'i	nstallation SERVEUR DE DESTINATI
	Afficher la progression de l'installation
	Installation de fonctionnalité
	Configuration requise. Installation réussie sur hermes.sitka.local.
	Services de certificats Active Directory
	Des étapes supplémentaires sont nécessaires pour la configuration des services de certificats
	Active Directory sur le serveur de destination.
	Autorité de certification
	On the disclosed sector of a second distant
Resultats	Outlis d'administration de serveur distant
Resultats	Outils d'administration de serveur distant Outils d'administration de rôles
Resultats	Outils d'administration de s'erveur distant Outils d'administration de rôles Outils des services de certificas Active Directory Outils des services de certification
Kesultats	Outils d'administration de selveur ossant Outils datministration de rôles Outils des services de certificats Active Directory Outils de gestion de l'autorité de certification
Resultats	Outils d'administration de rôles Outils d'administration de rôles Outils d'administration de rôles Outils de gestion de rôles Outils de gestion de l'autorité de certification Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examine leur progression ou rouvez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

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 ce	rtificats Active Directory -
Clé privée	SERVEUR DE DESTINATION hermes.sitka.loca
Informations d'identificati Services de rôle	Spécifier le type de la clé privée
Type d'installation Type d'AC	Pour générer et émettre des certificats aux clients, une autorité de certification doit posséder une clé privée.
Clé privée Chiffrement	Créer une clé privée Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
Nom de l'AC Période de validité	 Utiliser la clé privée existante Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.
Base de données de certi Confirmation	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.
Résultats	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.
باری	En savoir plus sur la clé privée
	< Précédent Suivant > Configurer Annuler

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

Configuration des services de ce	rtificats Active Directory		194 <u>1</u> 24		\times
Chiffrement pour	l'autorité de certification		SERVEUR DE	DESTINA mes.sitka	TION local
Informations d'identificati Services de rôle	Spécifier les options de chiffrement				
Type d'installation	Sélectionnez un fournisseur de chiffrement :		Longueur de l	a clé :	
Type d'AC	RSA#Microsoft Software Key Storage Provider	~	4096		~
Clé privée	Sélectionnez l'algorithme de bachage nour signer les certifi	cate ómic	par cette AC :		
Chiffrement	SHA256	~			
Résiede de validité	SHA384				
Base de données de certi	SHA1	~			
Confirmation Progression Résultats	Autorisez l'interaction de l'administrateur lorsque l'auto privée.	rité de ce	rtification accèc	le à la clé	
	En savoir plus sur le chiffrement	~	Configurer	Annu	ler

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

Ta Configuration des services de ce	tificats Active Directory			\times
Nom de l'autorité	de certification	RVEUR DE D	ESTINAT es.sitka.l	ION ocal
Informations d'identificati Services de rôle Type d'installation Type d'AC Clé privée Chiffrement	Spécifier le nom de l'AC Tapez un nom commun pour identifier cette autorité de certification. Ce r certificats émis par l'autorité de certification. Les valeurs des suffixes du n automatiquement, mais elles sont modifiables. Nom commun de cette AC :	nom est ajout Iom unique se	é à tous ont géné	les rées
Nom de l'AC Période de validité Base de données de certi Confirmation Progression Résultats	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 > C	onfigurer	Annul	er

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

BTS SIO 2024

Résultats	SERVEUR DE DESTINATIO hermes.sitka.loc
Informations d'identificati Services de rôle	Les rôles, services de rôle ou fonctionnalités ci-après ont été configurés :
Type d'installation Type d'AC Clé privée Chiffrement Nom de l'AC Période de validité Base de données de certi Confirmation	Autorité de certification
Résultats	

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

Se connecter X	gaps://nermes.sitka.iocai/DC=sitka,DC=local — Ц
Serveur : hermes.sitka.local Port : 636 Non connecté SSL OK Annuler	Connexion Parcourir Affichage Options Outline Id Idap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, 3); Error 0 = Idap_connect(hLdap, NULL); Error 0 = Idap_connect(hLdap, LDAP_OPT_SSL,(void*)&Iv); Host supports SSL, SSL cipher strength = 256 bits Established connection to hermes.sitka.local. Retrieving base DSA information Getting 1 entries: Dn: (RootDSE) configurationNamingContext: CH=Configuration.DC=sitka.DC=local; domainControllerFunctionality: 7 = (WIN2016); domainControllerFunctionality: 7 = (WIN2016); highestCommittedUSN: 192580; in Calbade(TatanDEaadv: TBUE);

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 derectement 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 Promp



On tape la commande suivante :

Advanced Users Only The canabilities offered here can be dangerous. No support is available. Use				
· · · · · · · · · · · · · · · · · · ·	them at your own risk!			
Execute Shell Command				
openssl s_client -showcerts -connect 172.20.0.14:636		×		

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



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 permettrons 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 🛨 Add pour rajouter une authentification Servers

of sense, System - Inte	erfaces 👻 Firewall 👻	Services → VPN → Status →	Diagnostics - H	lelp 🗸	1 0
System / User Manager	/ Authentication Se	ervers			0
Users Groups Settings	Authentication Servers				
Authentication Servers		•			
Server Name	Туре	Host Name		Actions	
Local Database		pfsense			
					🕂 Ad

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 faires : on tape cn dans le champ **Authentification containers** puis on clique sur **select a container**

Authentication containers	cn 1	Q Select a container 2
---------------------------	-------------	------------------------

Users Groups	Settings Authentication Servers
Server Settings	
Descriptive nam	ne authentification Idap
Tv	
LDAP Server Sett	ings
Hostname or IP addre	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 val	ue 389
Transpo	Standard TCP
Peer Certificate Author	ity 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 versio	Select LDAP containers for authentication
Server Timeo	Timeout for LDAP operations (sec
Search sco	pe Level CN=Users,DC=sitka,DC=local
	Entire Subtree
	12 12
	DC=sitka,DC=local
Authentication containers	OU=Asgard,DC=sitka,DC=local
	Note: Semi-Colon separated. This will be prepended to the search base
	component. on clique sur Select a container
	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	e cn
Group member attribute	memberOf
RFC 2307 Groups	EDAP 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 Div	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
UTE8 Encode	□ IITE8 encode I DAP parameters before sending them to the server
on o Elcoue	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	Allow unauthenticated bind
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.
	B Save

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

Users Groups S	Authentication Servers		
Server Settings			
Descriptive name	authentification Idaps		
Туре	LDAP	~	
LDAP Server Settings			
Hostname or IP address	hermes.sitka.local NOTE: When using SSL/TLS or STARTTI server SSL/TLS Certificate.	S, this hostname MUST match a Subject Alternative Name (SAN) or the Common Name (CN) of the LDAP	
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 Q Select a container

Authentication containers	cn	63	Q Select a container

La boite 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 apparait 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 reconnait pas le certificat

	hernet0					- 🗆 ×
Fichier	Editer Vue A	ller Capture Analyser	Statistiques Telephor	nie Wireless Outils Aide		
	1 0 L D					
ssl				<u> </u>		
No.	Time	Source	Destination	Protocol Length Tofo		
	10 0.869552	172,20,0,250	172.20.0.14	TLSv1.2 106 Applica	ition Data	
	19 0.918263	172.20.0.250	172.20.0.14	TLSv1.2 361 Client	Hello	
	20 0.930438	172.20.0.14	172,20,0,250	TLSv1.2 2322 Server	Hello, Certificate, Server Key Exchange	. Certificate Request
	23 0.932646	172,20,0,250	172,20,0,14	TLSv1.2 73 Alert	Level: Fatal, Description: Unknown CA)	1
-	27 0.935831	172.20.0.250	172.20.0.14	TLSv1.2 531 Applica	ition Data	
	28 0.937566	104.26.10.240	172.20.0.14	TLSv1.2 576 Applica	tion Data, Application Data	
> Fra	me 23: 73 bytes	s on wire (584 bits)	, 73 bytes captured	(584 bits) on interface \D	evice\NPF_{CD7E2F95-314F-4B15-B68B-1106	3A9E5CCE}, id 0
> Eth	ernet II. Src:	VMware cb:74:c4 (00	:0c:29:cb:74:c4), D:	t: VMware 23:11:5f (00:0c:	29:23:11:5f)	
> Int	ernet Protocol	Version 4, Src: 172	.20.0.250, Dst: 172.	20.0.14		
> Tra	nsmission Contr	ol Protocol, Src Po	rt: 38899, Dst Port:	636, Seq: 296, Ack: 2257,	Len: 7	
> Tra	nsport Layer Se	curity				
8888	00 0c 29 23 11	5f 00 0c 29 cb 74	c4 98 99 45 99 ···)#)-+E-		
0010	00 3b 00 00 40	00 40 06 el 8c ac	14 00 fa ac 14 .:	· @ @ · · · · · · · · · · ·		
0020	00 0e 97 f3 02	7c 02 26 50 06 98	4a e3 f0 80 18 ···	···· · & P · · J · · · ·		
0030	02 02 0f 4f 00	00 01 01 08 0a 8b	5e fb d9 02 13 ···	·0····		
0040	d0 04 15 03 03	00 02 02 30	2.2			

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 Ajouter/Supprimer un composant logiciel enfichable... 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

el\Certificats] Dé cal HE ir es les tâches > >er	élivré par ERMES-CA ERMES-CA Ouvrir Demander	Actions Certificats Autres actions HERMEC.CA	_ ×
De cal He ir es les tâches > per	élivré par ERMES-CA ERMES-CA Ouvrir Demander	Actions Certificats Autres actions HERMEC.CA	
cal Hi Hi rs les táches > >er	ERMES-CA ERMES-CA Ouvrir Demander	Certificats Autres actions HERMEC_CA	
Hi ir es les táches > >er	Ouvrir Demander u		
es les tâches >	Ouvrir Demander u	HERMES_CA	
es les tâches >	Ouvrir Demander u	un certificat avec une nouvelle clé	
oer	Demander u	un certificat avec une nouvelle clé	
rimer	Renouveler Gérer les clé	er certificat avec une nouvelle clé	
riétés	Opérations	avancées	>
	Exporter		
	riétés	riétés Opérations Exporter	riétés Opérations avancées Exporter

On choisit de ne pas exporter la clé privée

🚰 Assistant Exportation du certificat	← 🖉 Assistant Exportation du certificat
Bienvenue dans l'Assistant Exportation du certificat	Exporter la clé privée Vous pouvez choisir d'exporter la clé privée avec le certificat.
Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un magasin de certificats vers votre diaque. Un certificat, émis par une autorité de certification, confirme votre identité et content des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.	Les dés privées sont protégées par mot de passe. Si vous voulez exporter la dé privée avec le certificat, vous devez taper un mot de passe dans une prochaine page. Voulez-vous exporter la dé privée avec le certificat ? Out, exporter la dé privée
Pour continuer, cliquez sur Sulvant.	Whon, ne pas exporter la de privee

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

ormat du fichier d'exportation Les certificats peuvent être exportés dans divers formats de fichiers.	Fichier à exporter Spécifiez le nom du fichier à exporter
Sélectionnez le format à utiliser :	Nom du fichier : C:\Users\Administrateur\Documents\hermes-ca.cer
○X.509 binaire encodé DER (*.cer)	
• X.509 encodé en base 64 (*.cer)	
Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)	
Indure tous les certificats dans le chemin d'accès de certification, si possible	
Échange d'informations personnelles - PKCS #12 (.PFX)	
Indure tous les certificats dans le chemin d'accès de certification, si possible	
Supprimer la dé privée si l'exportation réussit	
Exporter toutes les propriétés étendues	
Activer la confidentialité de certificat	
O Magasin de certificats sérialisés Microsoft (.SST)	
2017 Mar 18	

- 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 **cerificate manager + Cas** on clique sur ad pour rajouter une autorité de certification

	SC System	n - Interface	s - Firewall -	Services -	VPN 👻	Status 👻	Diagnostics 👻	Help 🗸	G
Systen	n / Certifi	cate Manag	er/ CAs						0
CAs	Certificates	Certificate Rev	ocation						
Search									•
Search te	erm	Enter a sear	ch string or *nix rec	ular expression to	search certific	E cate names and	oth	S.	
Certifica	ate Authorit	ies					_		
Name	Internal	Issuer	Certificates	Distinguished	Name			In Use	Actions
CA-Sitka	~	self-signed	1	ST=IDF, OU=S	SK, O=sitka, L=	Paris, CN=Ca-s	iitka, C=GB 🕕	OpenVPN Server	Ø₽C
				Valid From: Wee Valid Until: Sat,	d, 22 Dec 2021 1 21 Dec 2024 10	10:15:57 +0100 :15:57 +0100			
									+ Add

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

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

System / Certific	ate Manager / CAs / Edit
CAs Certificates	Certificate Revocation
Create / Edit CA	
Descriptive name	hermes-ca
Method	Import an existing Certificate Authority
Trust Store	Construct the contents of the CA will be added to the 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 certifices 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.
Certificate data	Concolle ici le certificat de hermes On colle ici le certificat de hermes On colle ici le certificat de hermes DEAQ0FADEC RUMEWYKCZIMIZPYLGQBGRYFbG9jYWwxFTATBg0JKiBJK/ISIAEZFg Paste a certificate in X.509 PEM format here.
Certificate Private Key (optional)	Paste the private key for the above certificate here. This is optional in most cases, but is required when generating a Certificate Revocation List (CRL).
Next Certificate Serial	Enter a decimal number to be used as a sequential serial number for the next certificate to be signed by this CA.
	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	*themet0 × hier Editer Vue Aller Capture Analyzer Statistiques Telephonie Wireless Outils Aide × ************************************										
Fichier Editer Vue	Aller Capture Analyse	r Statistiques Telep	honie Wireless O	utils Aide							
	× • • • •										
			~~~ …								
ssi											+
lo. Time	Source	Destination	Protocol	Length Info							
24 3.180984	172.20.0.14	172.20.0.250	TLSv1.2	381 Appl	cation Data						
27 3.181661	172.20.0.250	172.20.0.14	TLSv1.2	89 Appl	cation Data						
35 3.188387	172.20.0.250	172.20.0.14	TLSv1.2	361 Clie	t Hello						
36 3.190890	172.20.0.14	172.20.0.250	TLSv1.2	2322 Serv	r Hello, Cert	tificate, Serve	Key Exchange	, Certificate	Request	,	-
40 3.194817	172.20.0.250	172.20.0.14	TLSv1.2	236 Cert	ficate, Clier	nt Key Exchange	, Change Ciphe	r Spec, Encryp	ted Han	ds.	
41 3.196216	172.20.0.14	172.20.0.250	TLSv1.2	117 Chan	e Cipher Spe	;, Encrypted Ha	ndshake Messag	e			
43 3.196628	172.20.0.250	172.20.0.14	TLSv1.2	158 Appl	cation Data						-
Transport Layer S	ecurity	rt: 636, Dst Port	: 42252, Seq: 22	57, ACK: 4	6, Len: 51						
000 00 0c 29 cb 7	4 c4 00 0c 29 23 11	5f 08 00 45 00	···)·t··· )#· ···								
010 00 67 e0 d8 44	0 00 80 06 00 00 ac	14 00 0e ac 14	·g··@···								
020 00 fa 02 7c a	5 0c 95 6c 8f 69 93	14 7d 6e 80 18	···· ···1 ·i··}n·								
1030 20 02 59 8a 01	0 00 01 01 08 0a 02	7d 1f f7 ae 96	·Y·····}···								
040 c7 46 14 03 0	3 00 01 01 16 03 03	00 28 00 00 00	- F (								
9926 66 66 66 66 66 66	0 55 42 /5 a/ 1e b6	de at 60 26 ta	OBu a	1.							
-E 12 J1 75 J				IS .							
0060 c5 13 d1 75 d	d	00 00 04 04 00	8								
0060 c5 13 d1 75 d 0070 5f 38 7f d5 10	d	00 00 04 04 00	_8								
0060 c5 13 d1 75 d 0070 5f 38 7f d5 10	d	00 00 04 04 00	_8								
0060 c5 13 d1 75 d 0070 5f 38 7f d5 1	d	00 00 00 00 00	_8								
0060 c5 13 d1 75 d: 0070 5f 38 7f d5 14	d		_8								<b>1</b>

#### 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 réussit

Diagnostics / Aut	thentication	<b>≡ 0</b>
User kaiser authenticated s	successfully. This user is a member of groups:	
Authentication Test		
Authentication Server	authentification Idap	
Username	kaiser	
Password		

#### L'authentification Active directory en utilisant LDAPS a réussit

iagnostics / Aut	nentication		≡ (
ser kaiser authenticated s	ccessfully. This user is a member of groups:		
uthentication Test			
uthentication Test	authentification Idaps	~	
uthentication Test Authentication Server	authentification Idaps Select the authentication server to test against.	~	
uthentication Test <u>Authentication Server</u> <u>Username</u>	authentification Idaps Select the authentication server to test against. kaiser	~	

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

System / User Manager / Groups		6	
Users Groups	Settings Authentication Servers		
Groups	Description	Member Count	Actions
roup name			
noup name	All Users	1	1

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

Group Properties	3		
Group name	pfsense		
Scope	Remote	~	
	Warning: Changing this setting may affect take effect.	the local groups file, in which case a reboot may	y be required for the changes to
Description	compte active directory		
	Group description, for administrative info	mation only	
Group membership	admin	-	
		-	
	Not members	Members	
	>> Move to "Members"	K Move to "Not members	
	the second s		

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

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

Dans assigned Privilèges je clique sur add

-

Name	Description	Action

Je sélectionne WebCfg – All pages comme droit

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: SISH tunneling	
	User - VPN: L2TP Dialin	
	User - VPN: PPPOE Dialin WebCfg - AJAX: Get Queue Stats	
	WebCfg - AJAX: Get Service Providers WebCfg - AJAX: Get Stats	
	WebCfg - All pages WebCfg - Crash reporter	-
	WebCfg - Dashboard (all)	
	WebCfg - Dashboard widgets (direct access).	~

On remarque le groupe pfsense aura tous les droits

🖺 Save 🝸 Filter 🗶 Clear			
Allow access to all pages (This privile	ge effectively gives administrator-le	vel access to users in the group)	

#### On enregistre notre configuration

leges		
Name	Description	Action
WebCfg - All pages	Allow access to all pages (admin privilege)	<b>a</b>
Security notice: Users in this	group effectively have administrator-level access	
		- <b>-</b> - ^
B Save		

On fait un test de connexion avec la base LDAP

System / User M	anager / Settings	
Isers Groups	iettings Authentication Servers	
ettings		
Session timeout	30 Time in minutes to expire idle management sessions. The default is 4 hours (240 minutes). Enter 0 to risk!	o never expire sessions. NOTE: This is a securi
Authentication Server	authentification Idap 🗸	
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 LC To allow logins with RADIUS credentials, equivalent local users with the expected privileges must be To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP	ocal Database is used. created first. ? server configuration page.
Auth Refresh Time	Time in seconds to cache authentication results. The default is 30 seconds, maximum 3600 (one hoi	ur). Shorter times result in more frequent quer

#### La connexion a réussi

#### LDAP settings



On fait un test de connexion avec la base LDAPS

sers Groups S	Settings Authentication Servers	
Session timeout	20	-
Second timeout	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 s	ec
A state state of the state	riski	
Authentication Server	authentification ldaps	
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	To allow logins with LDAP credentials, Shell Authentication Group DN must be specified on the LDAP server configuration page.	

#### La connexion a réussi

P settings	5		
Test results	Attempting connection to	hermes.sitka.local	
	Attempting bind to	hermes.sitka.local	
	Attempting to fetch Organizational Units from	hermes.sitka.local	
	Organization units found		
	OU=Asgard,DC=sitka,DC=local		
	OU=Domain Controllers,DC=sitka,DC=local		
	OU=Microsoft Exchange Security Groups,DC=sitka,DC=local		

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

🗂 🗖 pfSense - Login 🤉	< +				0	$\times$
$\leftarrow$ $\rightarrow$ $C$ $rac{https://heimodeline$	all.sitka.local	i aite 🛧	£^≡	Ē		
<i>pf</i> sense			Logi	n to pf	Sense	9
	SIGN IN					
	kaiser					
	SIGN IN					
pfSense is developed	and maintained by Netgate. @ ES	SF 2004 - 2022 Vie	w license	h.c		

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

heimdall.sit	tka.local - Status: Dasi 🗙	+					_	-	$\times$
$- \rightarrow c$	🕆 https://heimdall.	sitka.local	Ð	രക	20	E=	€Ð		
Status / D	ashboard							+ 0	
System Infor	mation			_			F	• •	
System Infor Name	mation heimdall.sitka	local					J	00	
System Infor Name User	heimdall.sitka kaiser@172.2	.local 0.0.14 (LDAP/authenti	ification Idaps)				¥	00	
System Infor Name User System	mation heimdall.sitka kaiser@172.2 VMware Virtu	.local 0.0.14 (LDAP/authent al Machine	ification Idaps)				×	08	
System Infor Name User System	mation heimdall.sitka kaiser@172.2 VMware Virtu Netgate Devic	.local 0.0.14 (LDAP/authent al Machine e ID: <b>7c777c1ee8ed</b>	ification Idaps) 9111e66				¥	00	
System Infor Name User System BIOS	Mation heimdall.sitka kaiser@172.2 VMware Virtu Netgate Devic Vendor: Phoe	.local 0.0.14 (LDAP/authent al Machine :e ID: 7c7777elee8ed nix Technologies LTD	ification Idaps) 9111e66				¥	00	
System Infor Name User System BIOS	Mation heimdall.aitka kaiser@172.2 VMware Virtu Netgate Devic Vendor: Phoe Version: 6.00	.local 0.0,14 (LDAP/authent al Machine e ID: 7c7777e1ee8ed nix Technologies LTD	ification Idaps) 9111e66				Æ	00	