

Rapport de stage
BTS SIO 2^{ère} année



Stage effectué à Brainix-IT

Du 17 Janvier au 25 Février 2022

Stagiaire : Keanu Raffaelli

Tuteur : Noel Lechene

SOMMAIRE

REMERCIEMENTS	4
PRESENTATION DE L'ENTREPRISE	5
Objectif du stage	7
Présentation de EOLE	7
Présentation des modules pour la réalisation du projet	8
Prés-requis	8
Configuration du module Amon	10
Onglet Général	11
Onglet Services	13
Onglet interfaces	14
Interface-0	14
Interface-3	16
Onglet réseau avancé	17
Onglet relai DHCP	20
Onglet Eole SSO	21
Onglet Zones-dns	22
Onglet Authentification	23
Onglet Proxy authentifié	23
Onglet Wpad	24
Configuration du module Seth	25
Onglet Général	25
Onglet Services	26
Onglet Interface-0	27
Onglet DHCP	29
Configuration du module Scribe	30
Onglet Général	30
Onglet Interface-0	31
Onglet Certificats SSL	33
Onglet OpenLdap	33

Onglet Eolead	34
Onglet Saslauthd	35
Intégration du certificat du Seth au Java Keystore de Scribe	35
EAD 2	36
Création de UO et de GPO sur l'AD via l'outil Rsat.	38
L'outil Rsat	38
Synchronisation des utilisateurs à l'Active Directory	41
Création de GPO	42

REMERCIEMENTS

Avant le début du rapport de stage, j'aimerais commencer par de profonds remerciements à l'entreprise Brainix-IT qui a bien voulu accepter ma demande de stage. Remercier mon maître de stage Noel LECHENE pour l'aide, la connaissance qu'il m'a apportée durant ce 1 mois et demi de stage. Remercier également Clément CHÈNE, le technicien informatique de Brainix-IT qui a été un soutien, une aide à la réalisation et au bon fonctionnement du projet sur lequel nous avons travaillé.

Je souhaite remercier aussi l'établissement du lycée Paul Gauguin de m'avoir accueilli pour réaliser le projet qui m'a été confié. Pour finir, remercier notre professeur principale Mr MALINOWSKI pour l'aide qu'il m'a fournie pour trouver un stage et tous les professeurs pour les connaissent qu'ils m'ont apporté.



PRESENTATION DE L'ENTREPRISE



REFERENT & COORDONNEES :

M. Noel LECHENE

BP 4014

98713 PAPEETE – TAHITI

Tél : 87 20 27 05

contact@BRAINIX IT.com

RCS : TPI 18123A

Brainix-IT a été créée en janvier 2018, elle a le statut d'entreprise individuelle immatriculée en Polynésie-Française.

Elle est gérée par M. Noël LECHENE ayant acquis une expérience de plus 25 ans dans les domaines des réseaux, des systèmes d'information et de la sécurité informatique.

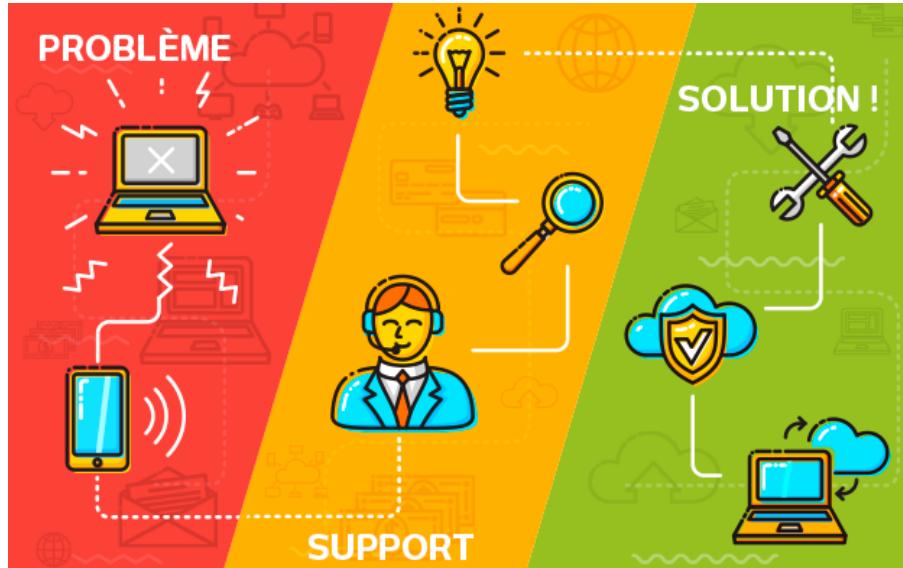
Depuis 3 ans et demi l'entreprise Brainix-IT propose des solutions et des services permettant d'accompagner les établissements publics, les établissements scolaires et les sociétés privées.

Son activité principale est exercée auprès d'institutions publiques du secteur de l'éducation. Les missions réalisées sont le maintien en condition opérationnelle du parc informatique avec une implication de MOAT/MOE1 sur les couches métiers et en complément une cellule de veille qui permet de faire évoluer continuellement les infrastructures systèmes et réseaux.

Brainix-IT porte une attention toute particulière aux projets qui touchent le secteur de l'éducation.

Ces derniers services d'accompagnement ont principalement tourné autour de l'analyse des besoins de ces institutions et des parties prenantes, l'étude de solutions numériques pédagogiques envisageables, la pré-mise en place d'une démarche de communication pour les parties prenantes au sujet de la transition digitale, la discussion sur de potentiels approches en termes d'équipements numériques et d'offres tarifaires.

Les principaux piliers de notre charte qualité : s'entourer des collaborateurs les plus compétents, être à l'écoute et au service du client afin de créer la synergie pour réussir.



Objectif du stage

La société Brainix-IT a mis en place une maquette de l'environnement Eole 2.7, mon objectif était de migrer cette environnement Eole 2.7 à un environnement Eole 2.8 pour permettre que l'environnement soit à la version majeure de nos jours.

Présentation de EOLE

Le projet EOLE naît à l'Académie de Dijon en 2000 pour répondre au besoin des établissements scolaires de partager un accès Internet unique. Le projet devient Projet National en 2001 à la demande du Ministère National de l'Enseignement Supérieur et de la Recherche (MENESR) dans le but de protéger les élèves et les données administratives.

EOLE est l'acronyme d'Ensemble Ouvert Libre et Évolutif. C'est un projet collaboratif basé sur la philosophie du logiciel libre, la mutualisation des compétences et des moyens permet de réaliser des solutions économiques, fiables et performantes.



Le projet EOLE offre des solutions clé en main pour la mise en place de serveurs dans les établissements scolaires et académiques.

Les objectifs du projet EOLE sont les suivants :

- Offrir des solutions libres ;
- Réaliser des produits modulaires, évolutifs et ouverts ;
- Faciliter les mises en œuvre et les déploiements ;
- Offrir un service d'administration à distance ;
- Offrir des services mutualisés (Réseau Global Établissement) ;
- Aider au respect des contraintes légales (droit d'auteur, brevet d'invention, droit des personnes et des enfants).

Les versions de EOLE

Version	Date de publication	Date d'obsolescence	Distribution et version de base	Version du noyau
EOLE 1.0	2001	-	Mandrake Linux 8	-
EOLE 2.0	octobre 2007	octobre 2008	Ubuntu 7.04	2.6.20
EOLE 2.1	mai 2008	avril 2009	Ubuntu 7.10	2.6.22
EOLE 2.2	janvier 2009	mai 2013	Ubuntu 8.04 LTS	2.6.24
EOLE 2.3	juin 2011	avril 2015	Ubuntu 10.04 LTS	2.6.32
EOLE 2.4	juin 2014	Juin 2017	Ubuntu 12.04 LTS	3.2.0
EOLE 2.5	juillet 2015	Juin 2019	Ubuntu 14.04 LTS	3.13.0
EOLE 2.6	décembre 2016	Juin 2021	Ubuntu 16.04 LTS	4.4
EOLE 2.7	décembre 2018	Juin 2023	Ubuntu 18.04 LTS	4.15
EOLE 2.8	décembre 2020	Juin 2025	Ubuntu 20.04 LTS	5.4

Présentation des modules pour la réalisation du projet

Pour que mon environnement Eole fonctionne, j'ai installé et configuré 3 modules :

Le module Amon, il aura pour rôle de pare-feu pour l'infrastructure réseaux de l'établissement. Ensuite, il va être le routeur pour que les zones puissent accéder à internet. Enfin, il sera le relais DHCP car le serveur DHCP ne sera pas dans la même zone où le DHCP sera appliqué.

Le module Scribe, il sera l'annuaire OpenLDAP, le serveur de fichier et le serveur de messagerie.

Le module Seth, il aura pour rôle d'être le serveur DHCP pour une des zones qu'on aura. Il sera aussi d'office d'Active Directory afin d'appliquer des GPO dans le but de restreindre et sécuriser l'utilisation du matériel informatique des utilisateurs.

Prés-requis

Avant de commencer nos configurations, nous allons télécharger notre image ISO eole 2.8.1 sur le site de Eole : <http://eole.ac-dijon.fr/pub/iso/EOLE-2.8/latest/>

Puis, sur notre hyperviseur de niveau 1 Proxmox nous ajoutons l'image ISO.

Pour ce faire nous irons sur local (maq-proxmox) ISO images Upload.

The screenshot shows the Proxmox VE interface. In the left sidebar, under 'Datacenter', there's a 'Storage' section for 'local' on node 'mq-proxmox'. Under 'ISO Images', several ISO files are listed:

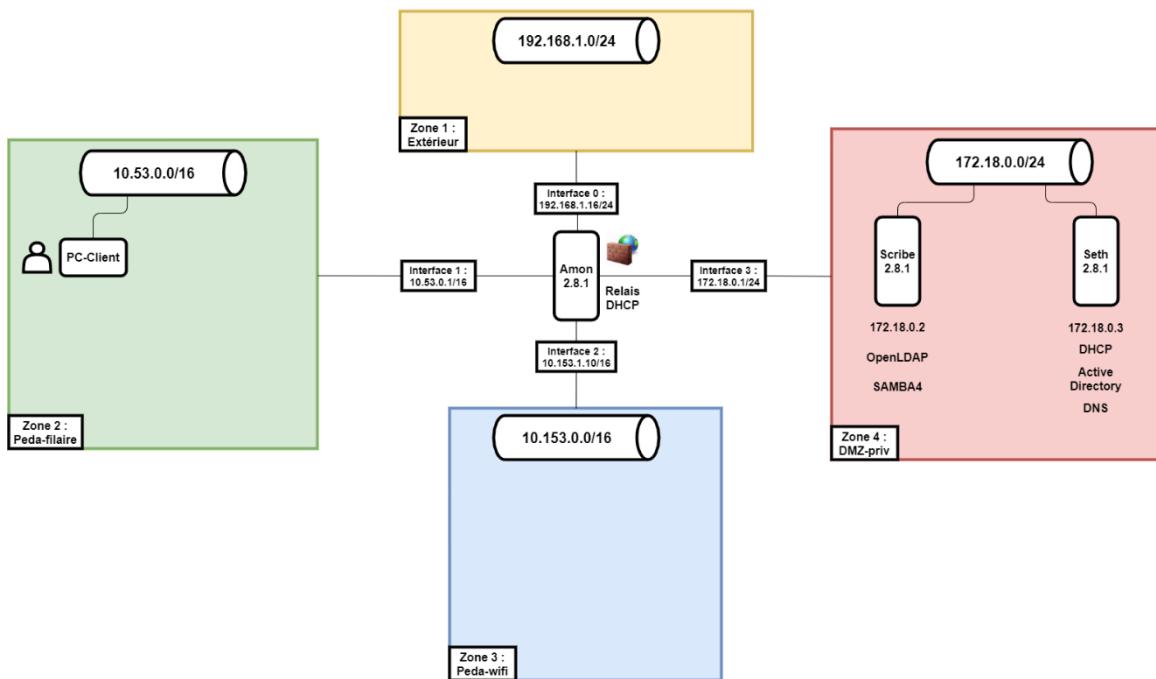
Name	Date	Format	Size
debian-10.5.0-amd64-netinst.iso	2021-12-09 11:13:01	iso	365.95 MB
debian-10.9.0-amd64-netinst.iso	2022-02-22 13:27:35	iso	353.37 MB
debian-11.0.0-amd64-netinst.iso	2022-01-20 14:01:21	iso	396.36 MB
eole-2.6.2-alternate-amd64.iso	2022-02-17 16:36:16	iso	1.51 GB
eole-2.7.2-alternate-amd64.iso	2022-02-20 00:46:59	iso	1.62 GB
eole-2.8.1-alternate-amd64.iso	2022-01-20 08:44:47	iso	1.97 GB
fr_windows_server_2008_r2_standard_enterprise_datacenter_web_x64_dvd_x15-50366.iso	2022-02-03 13:23:43	iso	3.10 GB
fr_windows_server_2012_r2_x64_dvd_2707985.iso	2022-02-03 13:28:23	iso	4.31 GB

Puis nous avons préétablis nos différentes cartes réseaux pour nos différentes zones.

vmbr0	Linux Bridge	Yes	Yes	Yes	eno1	INTERCO - DMZ PUB - 192....
vmbr1	Linux Bridge	Yes	Yes	Yes	eno2	PEDA-FILAIRE - 10.53.0.0/1...
vmbr3	Linux Bridge	Yes	Yes	Yes	enp6s0f1	PEDA-WIFI - 10.153.0.0/16 - ...
vmbr5	Linux Bridge	Yes	Yes	Yes		DMZ-PRIVEE - 172.18.0.0/16

Enfin, pour réaliser mon projet, j'ai effectué un plan réseau avec les différentes zones pour configurer les différents modules.

OBJECTIF



Nom de l'interface	Adresse réseau	Masque de sous-réseau	Nom de la zone	Nom de la zone pour le DNS
Interface-0	192.168.1.16	255.255.255.0	Extérieur	/
Interface-1	10.53.0.1	255.255.0.0	Peda-filaire	Peda-filaire
Interface-2	10.153.1.10	255.255.0.0	Peda-wifi	Peda-wifi
Interface-3	172.18.0.1	255.255.255.0	Dmz-privé	Dmz-privé

Configuration du module Amon

Nous allons créer une VM avec l'image ISO de Eole 2.8.1. Eole utilise la distribution Ubuntu 20.04. Nous arriverons à une interface où nous devrons choisir le module à installer.



Nous prenons le module Amon puis on appui « entrer » pour lancer l'installation.

Lorsque l'installation sera finie, nous arriverons sur l'interface d'identification.

```
EOLE tty1
Mot de passe par défaut de l'utilisateur root est : nag{ie4eiMey
amon login:
```

Eole génère automatiquement un mot de passe pour l'utilisateur root.

Il est possible de changer le mot de passe via la commande :

```
root@1yclpg-amon2:~# passwd _
```

Pour configurer le module Amon nous allons passer par l'interface de configuration du module « GenConfig »

```
root@lyclpg-amon2:~# gen_config_
```

Nous arrivons sur l'interface du « GenConfig »



On s'authentifie avec le login « root »

Onglet Général

Tout d'abord, on choisit le mode expert pour avoir toutes les configurations possibles sur le module Amon.

- **Identifiant de l'établissement (exemple UAI)** : C'est un identifiant qui est propre à un établissement scolaire, dans notre cas c'est celui du lycée Paul Gauguin.
- **Nom de l'établissement** : Nous indiquerons le nom de l'établissement qui est « Lycee Paul Gauguin ».
- **Nom de la machine** : Nous indiquerons le nom de la machine qui sera « lyclpg-amon2 » *attention : Si l'authentification NTLM/KERBEROS est activée sur le proxy, le Nom de machine ne peut être supérieur à 15 caractères. En effet un nom de machine supérieur à 15 caractères rend impossible l'intégration du module au domaine AD.
- **Nom DNS du réseau local** : Le lycée Paul Gauguin est un établissement public par conséquent il dépend de la DGEE, nous devrons donc mettre l'abréger de l'établissement suivi de « itereva.pf » qui représente la DGEE. Ce qui donne « lyclpg.itereva.pf ».
- **Nom de domaine académique (ex : ac-dijon)** : Nous indiquerons le domaine académique de l'établissement qui est « ac-polynesie ».
- **Suffixe du nom de domaine académique** : Nous indiquerons le suffixe académique qui est « pf ».
- **Nombre d'interface à activer** : Nous indiquerons 4 interfaces car il aura une interface la zone « Dmz-priv », une pour la zone « Peda-wifi », une pour la zone « Peda-filaire » et une pour la zone « Extérieur »

Nom de l'interface	Adresse réseau	Masque de sous-réseau	Nom de la zone	Nom de la zone pour le DNS
Interface-0	192.168.1.16	255.255.255.0	Extérieur	/
Interface-1	10.53.0.1	255.255.0.0	Peda-filaire	Peda-filaire
Interface-2	10.153.1.10	255.255.0.0	Peda-wifi	Peda-wifi
Interface-3	172.18.0.1	255.255.255.0	Dmz-privé	Dmz-priv

- **Utiliser un serveur mandataire (proxy) pour accéder à internet** : Nous indiquerons non car le module n'utilise pas de proxy pour accéder à internet.
- **Adresse IP du serveur DNS** : Nous indiquerons l'adresse IP du module Seth (172.18.0.3) car nous voulons que Amon utilise son DNS. Ensuite, nous utiliserons le serveur DNS de la zone Extérieur (192.168.1.254).

Onglet Services

The screenshot shows the Amon 2.8.1 web interface with the 'Services' configuration page selected. The left sidebar lists various configuration modules. The main panel displays a list of services with their status set to 'non' except for 'Activer l'interface de configuration du module (GenConfig)' which is set to 'oui'. Each service has a red circular icon with a white letter indicating its status.

Service	Statut
Activer la gestion des logs centralisés	non
Activer l'anti-virus ClamAV	non
Activer le relai DHCP	oui
Activer la gestion de l'onduleur NUT	non
Activer le réseau virtuel privé RVP	non
Utiliser un serveur EoleSSO	distant
Activer l'interface web de l'EAD	oui
Activer le filtrage sur le proxy	oui
Activer le support de WPAD	oui
Activer la publication d'applications web par Nginx	oui
Activer le reverse proxy Nginx	oui
Activer l'interface d'administration du module (EAD3)	non
Activer l'interface de configuration du module (GenConfig)	oui

- **Activer le relai DHCP :** Nous indiquerons oui car notre serveur DHCP n'est pas dans la même zone où le DHCP sera appliqué.
- **Utiliser un serveur EoleSSO :** Nous indiquerons distant car EoleSSO est un service d'authentification unique et Le serveur EoleSSO sera sur Scribe car il se base sur des serveurs LDAP qui est le module Scribe pour authentifier les utilisateurs et récupérer leurs attributs.
- **Activer l'interface web de l'EAD :** Nous indiquerons oui pour permettre d'administrer les serveurs Eole via une interface Web.
- **Activer le filtrage sur le proxy :** Nous indiquerons oui pour filtrer les recherches Web des utilisateurs.
- **Activer le support de WPAD :** Nous indiquerons oui pour permettre la découverte automatique du proxy par les navigateurs.

Onglet interfaces

Nous avons précédemment indiqué que le module Amon aura 4 interfaces :

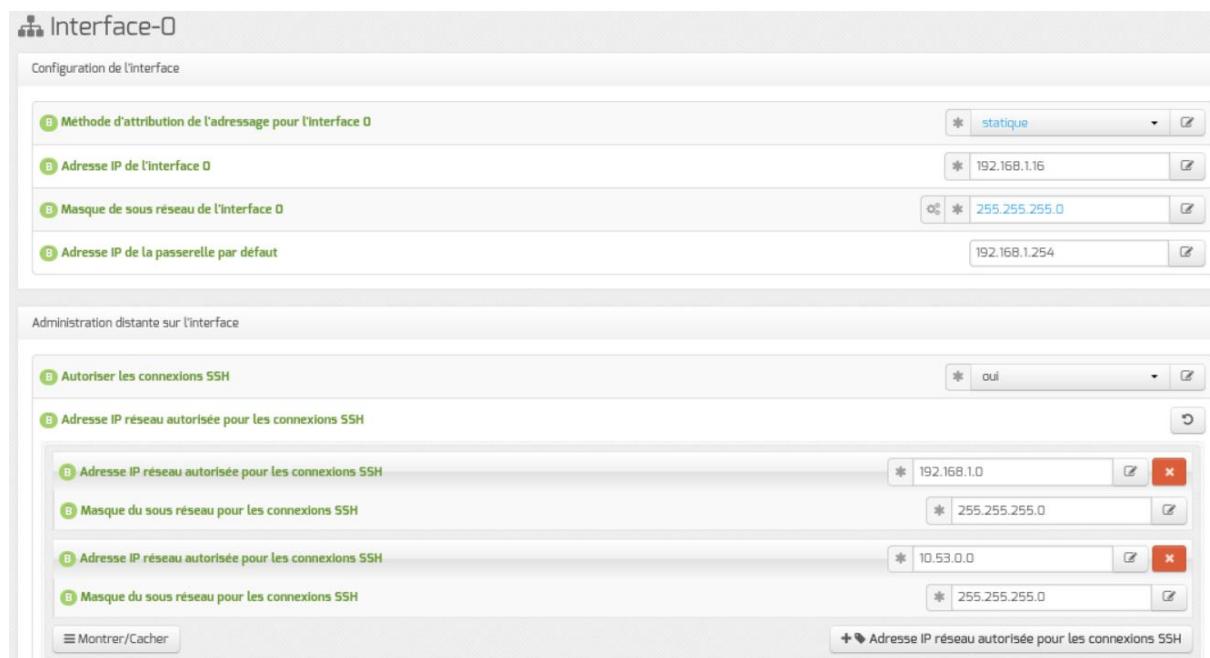


Chaque interface représente une zone pour notre projet.
Nous allons nous concentrer uniquement sur les interfaces 0 et 3 car ce sont les plus importantes.

Nom de l'interface	Adresse réseau	Masque de sous-réseau	Nom de la zone	Nom de la zone pour le DNS
Interface-0	192.168.1.16	255.255.255.0	Extérieur	/
Interface-1	10.53.0.1	255.255.0.0	Peda-filaire	Peda-filaire
Interface-2	10.153.1.10	255.255.0.0	Peda-wifi	Peda-wifi
Interface-3	172.18.0.1	255.255.255.0	Dmz-privé	Dmz-priv

Interface-0

La configuration de la première carte réseau sera dédiée au réseau extérieur, grâce à cette carte les autres zones pourront accéder à internet.

A screenshot of a software interface titled 'Interface-0' showing network configuration settings. The interface is divided into sections: 'Configuration de l'interface' and 'Administration distante sur l'interface'. In the first section, fields include 'Méthode d'attribution de l'adresses pour l'interface 0' (static), 'Adresse IP de l'interface 0' (192.168.1.16), 'Masque de sous réseau de l'interface 0' (255.255.255.0), and 'Adresse IP de la passerelle par défaut' (192.168.1.254). In the second section, under 'Administration distante sur l'interface', there are fields for 'Autoriser les connexions SSH' (oui) and 'Adresse IP réseau autorisée pour les connexions SSH'. This section contains two tables of IP ranges: one for 'Adresse IP réseau autorisée pour les connexions SSH' (192.168.1.0, 255.255.255.0) and another for 'Masque du sous réseau pour les connexions SSH' (10.53.0.0, 255.255.255.0). A 'Montrer/Cacher' button is also present.

1. Configuration de l'interface

Nous indiquons que la configuration sera en **statique** avec l'adresse IP pour la zone extérieure qui est **192.168.1.16/24**, on utilisera la passerelle **192.168.1.254**

2. Administration distante sur l'interface

Nous autoriserons les connexions SSH, nous autoriserons l'adresse réseau de la zone extérieur et la zone peda-filaire qui sont **192.168.1.0/24** et **10.53.0.0/24**.

Configuration de l'accès au backend EAD

E Autoriser l'accès au backend EAD depuis des frontend EAD distants

oui

B Adresse IP réseau autorisée à accéder au backend EAD

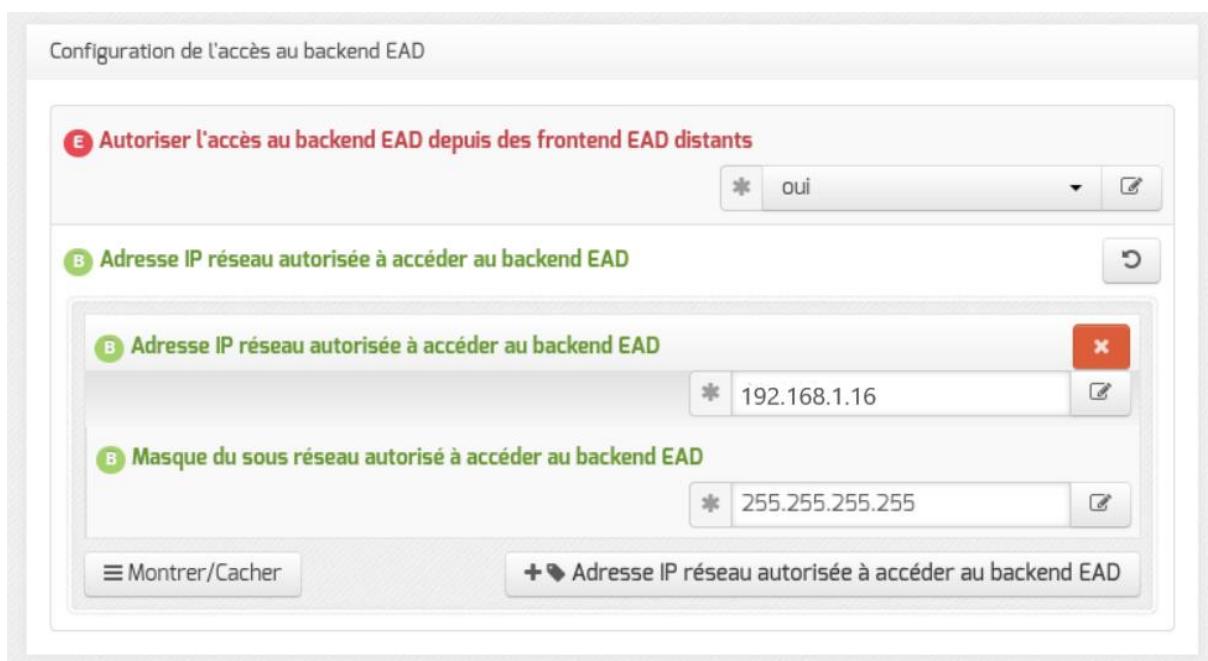
B Adresse IP réseau autorisée à accéder au backend EAD

* 192.168.1.16

B Masque du sous réseau autorisé à accéder au backend EAD

* 255.255.255.255

≡ Montrer/Cacher + Adr. IP réseau autorisée à accéder au backend EAD

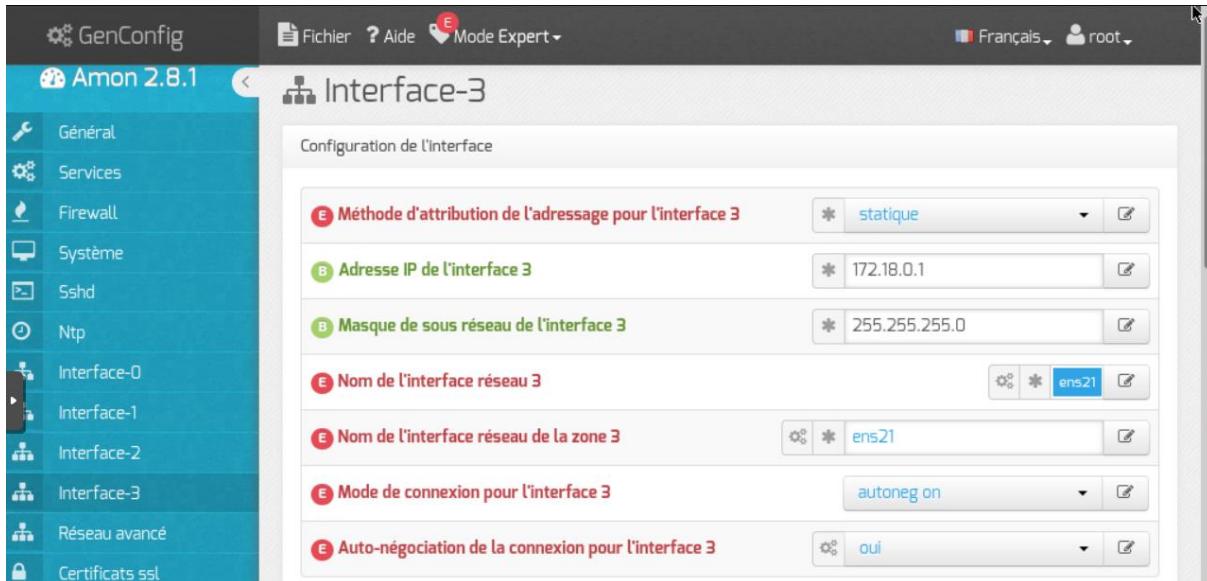


3. Configuration de l'accès au backend EAD

On autorise l'accès au backend EAD pour cette interface en indiquant que la seule adresse IP qui est **192.168.1.16/32** pour accès via un navigateur l'interface web EAD grâce à cette IP.

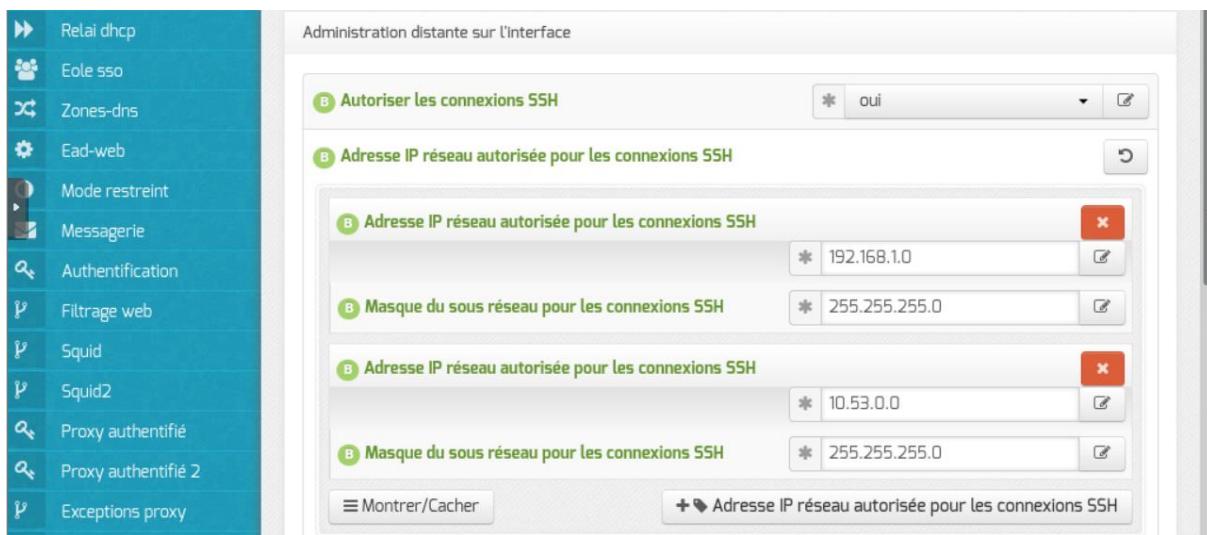
Interface-3

Cette interface sera dédiée pour la zone dmz-priv. C'est la zone où se trouve tous les autres modules comme Scribe et Seth.



1. Configuration de l'interface

L'adresse IP de notre Amon pour la dmz-priv sera **172.18.0.1/24**



2. Administration distante sur l'interface

Nous autoriserons les connexions SSH, nous autoriserons l'adresse réseau de la zone extérieur et la zone peda-filaire qui sont **192.168.1.0/24** et **10.53.0.0/24**.

Configuration DNS sur l'interface

N Serveur master DNS de cette zone	* oui
N Autoriser cette zone à utiliser les DNS des zones forward additionnelles	* oui
N Nom de la zone (pour résolution DNS)	* dmz-priv

3. Configuration DNS sur l'interface

Nous activons le service DNS pour cette interface, le nom de la zone sera « dmz-priv ». L'interface utilisera les DNS des zones forward ce qui veut dire que chaque machine de cette zone pourra résoudre les noms d'hôtes des domaines qui seront dans le « Forward de zone DNS »

Onglet réseau avancé

Cette partie va permettre de configurer les routes réseaux pour que chaque zone passe par le module Amon pour sortir vers internet.

1. Configuration

On active le routage pour que chaque machine de chaque zone passe par Amon pour accéder à internet.

2. Ajout d'hôtes

Amon utilisera le DNS du serveur Seth par conséquent, nous devons l'ajouter avec son adresse IP, le nom long et son nom.

Ajout de routes statiques

E Ajouter des routes statiques * oui

E Adresse IP ou réseau à ajouter dans la table de routage

E Adresse IP ou réseau à ajouter dans la table de routage *	192.168.1.0
E Masque de sous réseau (mettre à 255.255.255.255 si adresse host)	255.255.255.0
E Adresse IP de la passerelle pour accéder à ce réseau *	192.168.1.16
E Interface réseau reliée à la passerelle *	0

E Adresse IP ou réseau à ajouter dans la table de routage * 10.53.0.0 |

E Masque de sous réseau (mettre à 255.255.255.255 si adresse host)	255.255.0.0
E Adresse IP de la passerelle pour accéder à ce réseau *	10.53.0.1
E Interface réseau reliée à la passerelle *	1

3. Ajout de routes statiques

Dans cette partie, nous identifierons les différentes routes pour que chaque zone puisse accéder au serveur Amon puisque chaque zone doit passer par Amon pour avoir internet.

Nous avons la zone **extérieur** qui passera par le **192.168.1.16/24** et la zone **peda-filaire** qui passera par le **10.53.0.1/16**.

The screenshot shows a configuration interface for a router or firewall. It displays two route entries in a table format:

Route	Address	Gateway	Interface
1	10.153.0.0/16	10.153.1.10	2
2	172.18.0.0/24	172.18.0.1	3

Below the table are buttons for "Montrer/Cacher" (Show/Hide) and a "Ajouter" (Add) button.

Ensuite, nous avons identifié la route de la zone **peda-wifi** et de la zone **dmz-priv** qui sont le **10.153.1.10/16** et le **171.18.0.1/24**.

Onglet relai DHCP

Nous passons au service **relai DHCP** qui permet à la zone **peda-filaire** de recevoir une configuration IP dynamique depuis le serveur DHCP Seth qui est dans la zone **dmz-priv**.



1. Configuration

Le relai DHCP s'appliquera pour l'**interface-1** car c'est celle-ci où se trouve la zone peda-filaire. Le serveur DHCP se trouve dans l'**interface-3** (la zone dmz-priv) avec une adresse IP qui est **172.18.0.3**.

Onglet Eole SSO

Eole SSO est un service d'authentification unique et Le **serveur Eolessso sera sur Scribe** car il se base sur des serveurs LDAP qui est le module Scribe pour authentifier les utilisateurs et récupérer leurs attributs.



1. Configuration

Nous identifions un nom de domaine de Scribe avec le port à utiliser pour qu'il accède à celui-ci.

Onglet Zones-dns

Nous allons définir la zone forward ce qui veut dire que chaque machine de cette zone pourra résoudre les noms d'hôtes des domaines qui seront dans le « Forward de zone DNS »

The screenshot shows a web-based configuration interface for DNS zones. At the top, there's a header 'Zones-dns' with a sub-section title 'Ajout de domaines locaux supplémentaires (DNS master sur ces domaines)'. Below this, there's a field labeled 'E Nom domaine local supplémentaire ou rien' with a 'Pas de valeur' button and a pencil icon. The main section is titled 'Forward de zones DNS'. It contains a field 'E Déclarer des zones DNS à forwarder' with a dropdown menu set to 'oui'. Underneath, there's a 'Nom DNS de la zone' field containing 'lyclpg-peda.lyclpg.itereva.pf', a 'Montrer/Cacher' button, and a 'Nom DNS de la zone' button. Another field shows 'Adresse IP du serveur DNS de la zone' as '172.18.0.3'.

1. Forward de zones DNS

Nous indiquons le domaine de la zone à forward qui est **lyclpg-peda.lyclpg.itereva.pf** avec son serveur DNS de la zone qui est Seth en **172.18.0.3**.

Onglet Authentification

Dans cet onglet nous activerons l'authentification web (proxy) pour tous les accès web (http et HTTPS) demanderons une phase d'authentification.

Authentification

Configuration

B Activer l'authentification web (proxy)	*	oui	<input type="button" value=""/>
N Activer une deuxième instance de Squid	*	oui	<input type="button" value=""/>
N Activer le service FreeRADIUS	*	non	<input type="button" value=""/>

Onglet Proxy authentifié

Maintenant nous allons choisir quel type d'authentification.

Proxy authentifié

Configuration

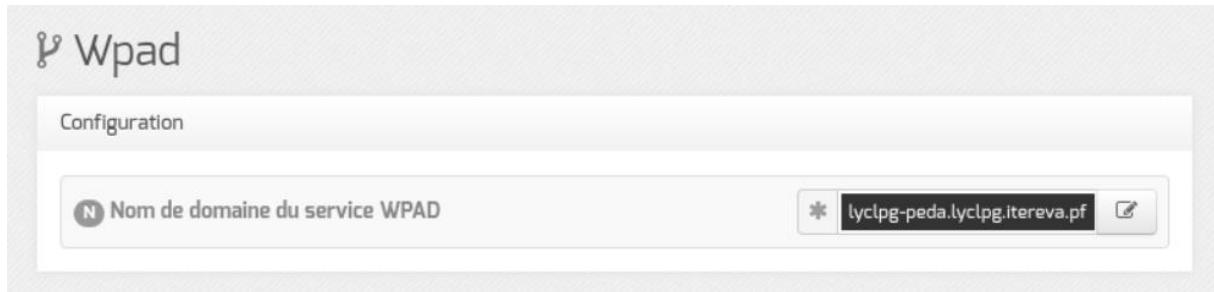
B Type d'authentification	*	NTLM/KERBEROS	<input type="button" value=""/>
B Nom du domaine KERBEROS (realm)	*	lyclpg-peda.lyclpg.itereva.pf	<input type="button" value=""/>
B Nom du contrôleur de domaine KERBEROS	*	lyclpg-seth	<input type="button" value=""/>
N Limiter l'authentification au DC renseigné	*	oui	<input type="button" value=""/>
N Adresse IP du contrôleur de domaine KERBEROS	172.18.0.3		
N Activer le proxy NTLM	*	oui	<input type="button" value=""/>
E Port d'écoute du proxy NTLM	*	3127	<input type="button" value=""/>

1. Configuration

Nous allons choisir **NTML/KERBEROS** comme authentification, c'est une authentification transparente pour les postes utilisateurs Windows intégrés dans un domaine Active Directory. Cette configuration est à choisir si on dispose d'un serveur Scribe ou Horus en mode AD ou d'un serveur Microsoft AD ce qui est le cas. Notre contrôleur de domaine est Seth donc on le met comme nom, on met son domaine et son IP.

Onglet Wpad

Ici nous allons indiquer le domaine où le Wpad sera appliqué.



1. Configuration

Le Wpad sera appliqué sur le domaine **lyclpg-peda.lyclpg.iteрева.рф**

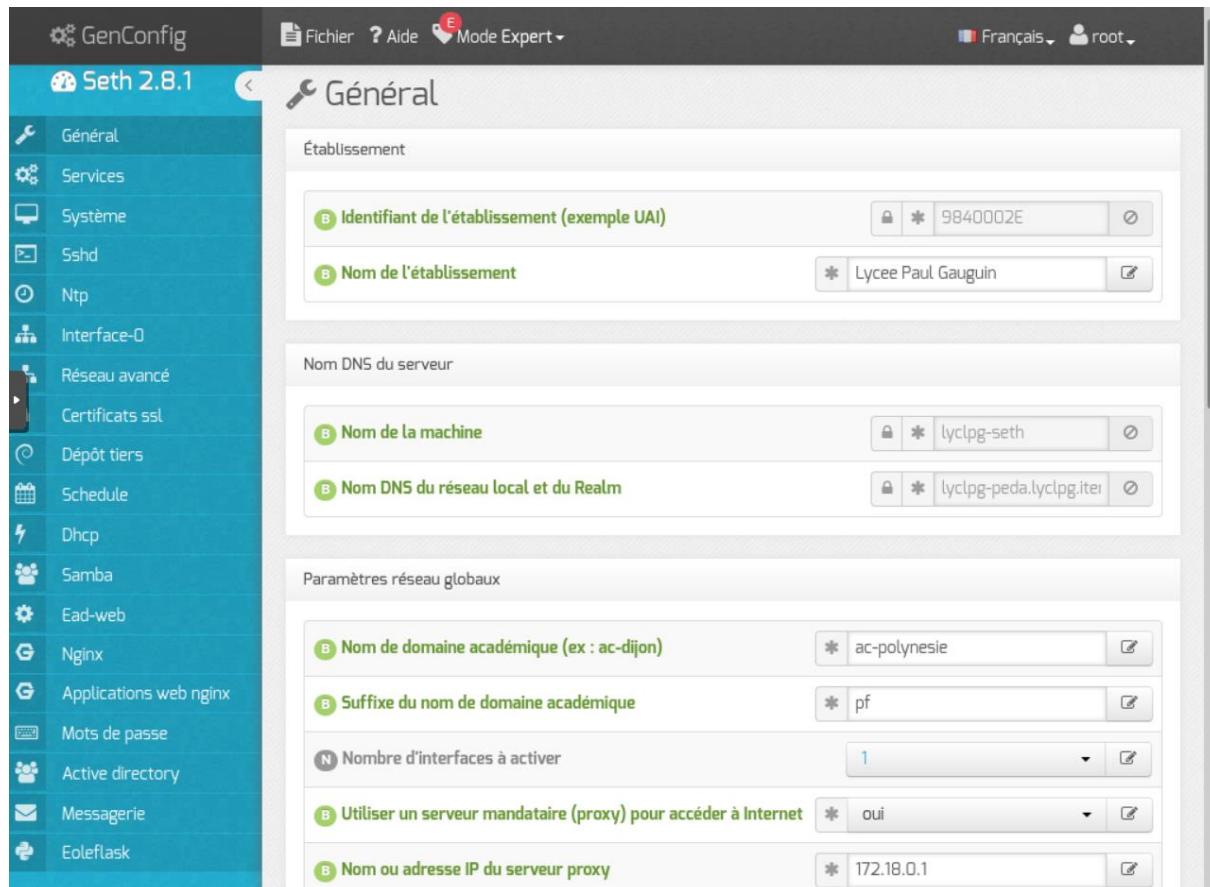
Pour finir, lorsque toutes les configurations du module seront faites, il ne nous restera qu'à faire l'**instance** du module puis la **reconfigure**.

Pas de soucis si des services de Amon ne sont pas activés, c'est au fait que le module Scribe et Seth ne sont pas configurés.

Configuration du module Seth

Le module Seth nous servira comme serveur DHCP et Active Directory.

Onglet Général



- **Identifiant de l'établissement (exemple UAI)** : C'est un identifiant qui est propre à un établissement scolaire, dans notre cas c'est celui du lycée Paul Gauguin.
- **Nom de l'établissement** : Nous indiquerons le nom de l'établissement qui est **Lycee Paul Gauguin**.
- **Nom de la machine** : Nous indiquerons le nom de la machine qui sera **lyclpg-seth**.
- **Nom DNS du réseau local et du Realm** : Nous indiquerons le nom de domaine de la zone où il sera appliqué qui sera **lyclpg-peda.lyclpg.iteva.pf**
- **Nom de domaine académique (ex : ac-dijon)** : Nous indiquerons le domaine académique de l'établissement qui est « ac-polynesie ».

- **Suffixe du nom de domaine académique** : Nous indiquerons le suffixe académique qui est « pf ».
- **Nombre d'interface à activer** : Nous indiquerons 1 interface
- **Utiliser un serveur mandataire (proxy) pour accéder à internet** : Nous indiquerons oui car il utilisera le serveur proxy du module Amon.
- **Nom ou adresse IP du serveur proxy** : Nous indiquerons l'adresse IP du module Amon **172.18.0.1**.

Onglet Services

The screenshot shows the 'Services' configuration page with the following settings:

Service	Statut
Activer la gestion des logs centralisés	non
Activer l'anti-virus ClamAV	non
Activer le serveur DHCP	oui
Activer l'utilisation d'un serveur PXE/TFTP	non
Activer la gestion de l'onduleur NUT	non
Activer l'interface web de l'EAD	oui
Activer la publication d'applications web par Nginx	oui
Activer le reverse proxy Nginx	non
Activer l'interface d'administration du module (EAD3)	non
Activer l'interface de configuration du module (GenConfig)	oui

On active le **serveur DHCP** et **l'interface web de l'EAD** pour pouvoir administrer le module via l'interface web.

Onglet Interface-0

Interface-0

Configuration de l'interface

B	Adresse IP de l'interface 0	*	172.18.0.3	<input type="button" value=""/>
B	Masque de sous réseau de l'interface 0	*	255.255.255.0	<input type="button" value=""/>
B	Adresse IP de la passerelle par défaut		172.18.0.1	<input type="button" value=""/>
E	Nom de l'interface réseau 0	*	ens18	<input type="button" value=""/>
E	Nom de l'interface réseau de la zone 0	*	ens18	<input type="button" value=""/>
E	Mode de connexion pour l'interface 0 (obsolète)		autoneg on	<input type="button" value=""/>
E	Auto-négociation de la connexion pour l'interface 0	*	oui	<input type="button" value=""/>

1. Configuration de l'interface

Le module aura comme adresse IP **172.18.0.3/24** et il passera par la passerelle **172.18.0.1** qui est Amon.

Administration distante sur l'interface

B	Autoriser les connexions SSH	*	oui	<input type="button" value=""/>
B	Adresse IP réseau autorisée pour les connexions SSH		<input type="button" value=""/>	
B	Adresse IP réseau autorisée pour les connexions SSH	*	192.168.1.0	<input type="button" value=""/>
B	Masque du sous réseau pour les connexions SSH	*	255.255.255.0	<input type="button" value=""/>
B	Adresse IP réseau autorisée pour les connexions SSH	*	10.53.0.0	<input type="button" value=""/>
B	Masque du sous réseau pour les connexions SSH	*	255.255.255.0	<input type="button" value=""/>
<input type="button" value="Montrer/Cacher"/>		<input type="button" value="+ Adr. IP réseau autorisée pour les connexions SSH"/>		

2. Administration distante sur l'interface

On ajoute les adresse IP réseau pour la connexion SSH qui sont **192.168.1.0/24** et **10.53.0.0/24**.

Configuration de l'accès au backend EAD

E Autoriser l'accès au backend EAD depuis des frontend EAD distants

oui

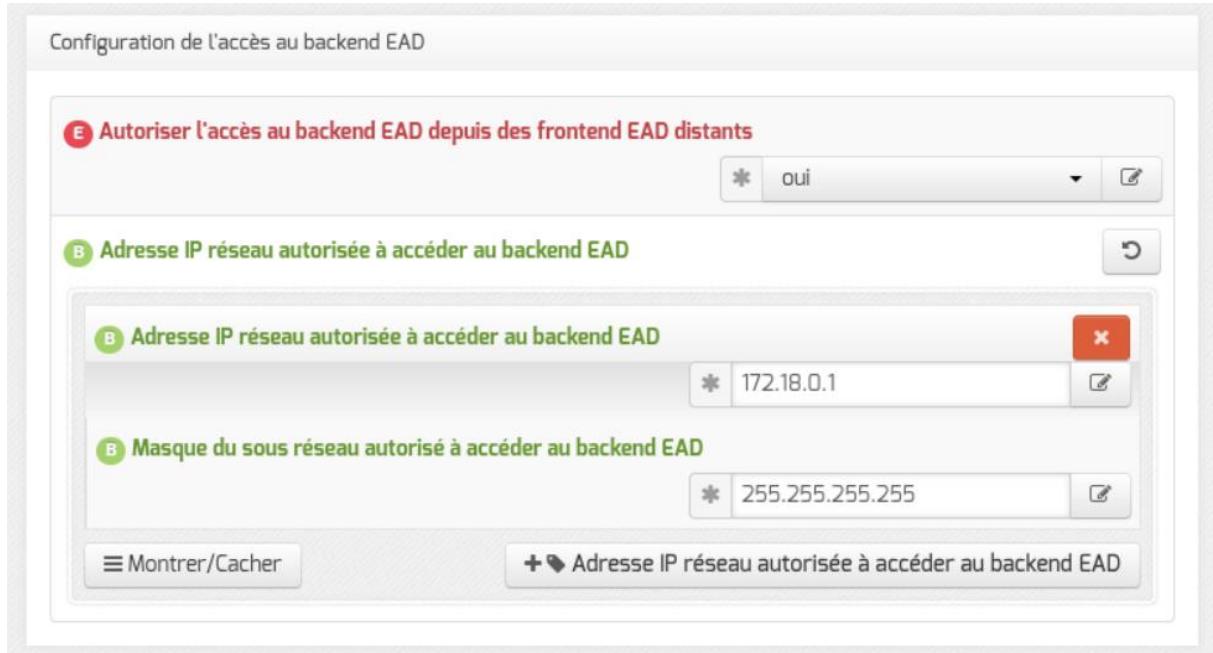
B Adresse IP réseau autorisée à accéder au backend EAD

B Adresse IP réseau autorisée à accéder au backend EAD

172.18.0.1

B Masque du sous réseau autorisé à accéder au backend EAD

255.255.255.255



3. Configuration de l'accès au backend EAD

On autorise l'accès EAD et qui utilisera comme adresse IP **172.18.0.1/32** qui est Amon.

Onglet DHCP

Définition des sous-réseaux

B Adresse réseau de la plage DHCP

B Masque de sous-réseau de la plage DHCP

B Nom de la plage DHCP

B IP basse de la plage DHCP

B IP haute de la plage DHCP

N Distribuer des IP statiques pour cette plage (compatible EAD3 seulement)

B Nom de domaine à renvoyer aux clients DHCP

B Adresse IP du routeur à renvoyer aux clients DHCP

B Adresse IP du DNS à renvoyer aux clients DHCP

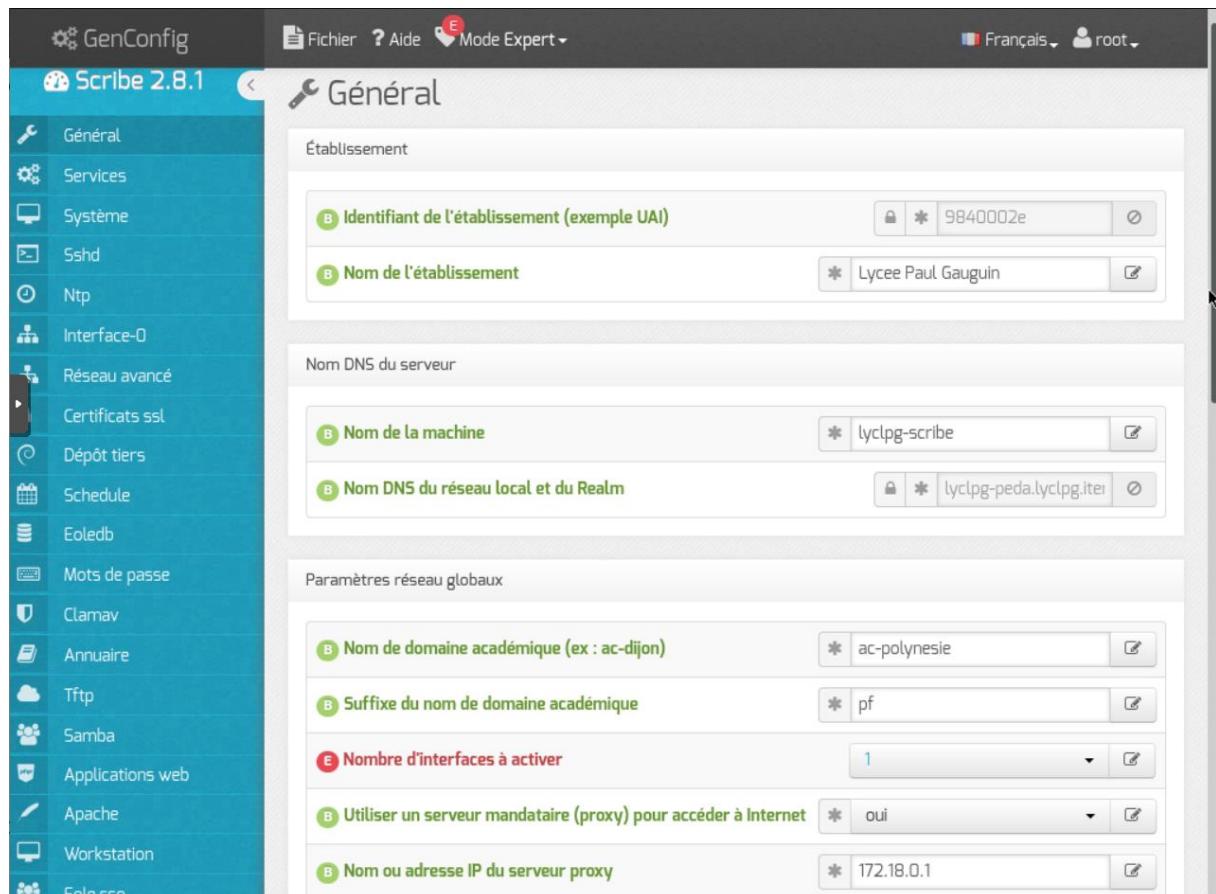
1. Définition des sous-réseaux

L'adresse réseau de la plage DHCP sera **10.53.0.0/16**, il aura comme nom **lyclpg-peda-dhcp**. L'IP la plus basse sera **10.53.5.0** et l'IP la plus haute sera **10.53.6.254**. Le domaine de la plage sera **lyclpg-peda.lyclpg.itereva.pf**, sa passerelle sera Amon en **10.53.0.1** et le DNS de la plage sera Seth en **172.18.0.3**.

Configuration du module Scribe

Dans cette partie nous verrons les configurations du module Scribe qui sera utilisé pour son annuaire OpenLDAP et son EoleAD.

Onglet Général



- **Identifiant de l'établissement (exemple UAI)** : C'est un identifiant qui est propre à un établissement scolaire, dans notre cas c'est celui du lycée Paul Gauguin.
- **Nom de l'établissement** : Nous indiquerons le nom de l'établissement qui est **Lycee Paul Gauguin**.
- **Nom de la machine** : Nous indiquerons le nom de la machine qui sera **lyclpg-scribe**.
- **Nom DNS du réseau local et du Realm** : Nous indiquerons le nom de domaine de la zone où il sera appliqué qui sera **lyclpg-peda.lyclpg.itereva.pf**

- **Nom de domaine académique (ex : ac-dijon)** : Nous indiquerons le domaine académique de l'établissement qui est « ac-polynesie ».
- **Suffixe du nom de domaine académique** : Nous indiquerons le suffixe académique qui est « pf ».
- **Nombre d'interface à activer** : Nous indiquerons 1 interface
- **Utiliser un serveur mandataire (proxy) pour accéder à internet** : Nous indiquerons oui car il utilisera le serveur proxy du module Amon.
- **Nom ou adresse IP du serveur proxy** : Nous indiquerons l'adresse IP du module Amon **172.18.0.1**.

Onglet Interface-0

The screenshot shows the 'Interface-0' configuration page with the following settings:

- Adresse IP de l'interface 0**: 172.18.0.2
- Masque de sous réseau de l'interface 0**: 255.255.255.0
- Adresse IP de la passerelle par défaut**: 172.18.0.1
- Nom de l'interface réseau 0**: ens18
- Nom de l'interface réseau de la zone 0**: ens18
- Mode de connexion pour l'interface 0 (obsolète)**: autoneg on
- Auto-négociation de la connexion pour l'interface 0**: oui

1. Configuration de l'interface

Le module aura comme adresse IP **172.18.0.2/24** et il passera par la passerelle **172.18.0.1** qui est Amon.

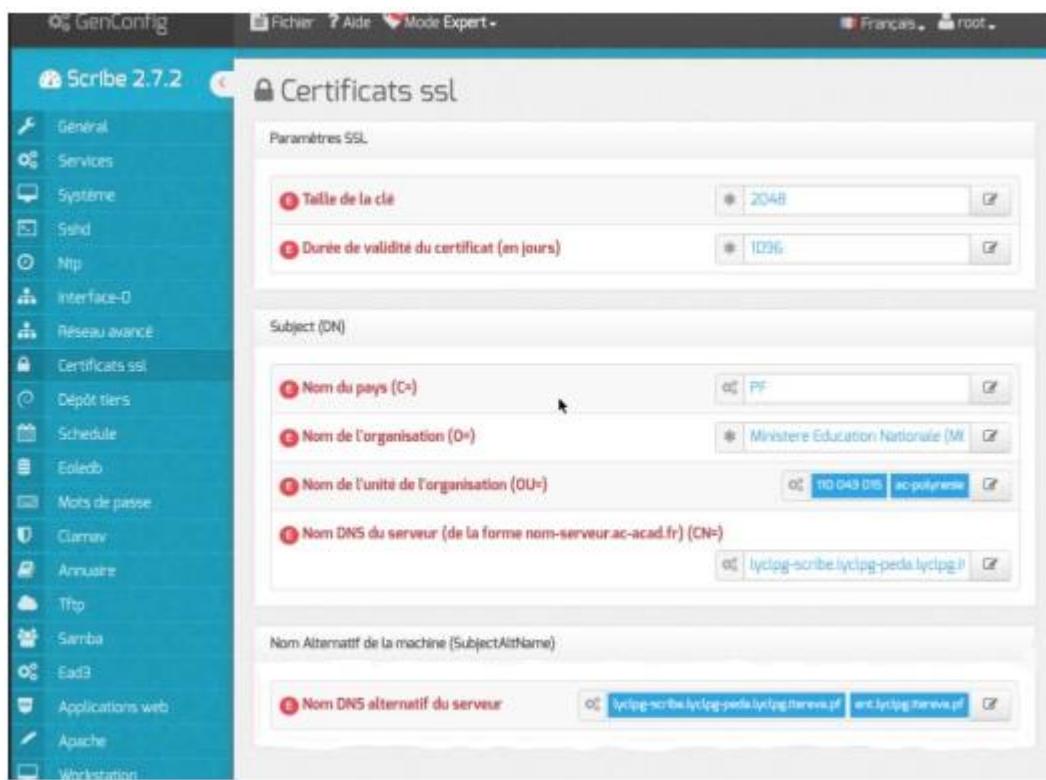
2. Administration distante sur l'interface

On ajoute les adresse IP réseau pour la connexion SSH qui sont **192.168.1.0/24** et **10.53.0.0/24**.

3. Configuration de l'accès au backend EAD

On autorise l'accès EAD et qui utilisera comme adresse IP **172.18.0.1/32** qui est Amon.

Onglet Certificats SSL



1. Nom alternative de machine (SubjectAltName)

Nous ajouterons les noms de domaine de Scribe qui sont **lycpg-scribe.lycpg-peda.lycpg.itereva.pf** et **ent.lycpg-itereva.pf** (ent.itereva.pf est important pour la gestion du service Eole SSO)

Onglet OpenLdap

Openldap

Configuration

E Niveau de log	* 512
E Nombre maximum d'entrées à retourner lors d'une requête	* 5000
E Temps de réponse maximum à une requête (en secondes)	* 3600
E Taille du cache (en nombre d'entrées)	* 1000
E Activer LDAP sur le port SSL	* oui
E Utilisateur autorisé à accéder à distance au serveur LDAP	* tous
E Utiliser la délégation d'authentification SASL	* oui

Nous activons le port SSL sur LDAP pour que nous effectuons la synchronisation LDAPS, ce qui est nécessaire pour la synchronisation OpenLDAPS sur l'AD.

Onglet Eolead

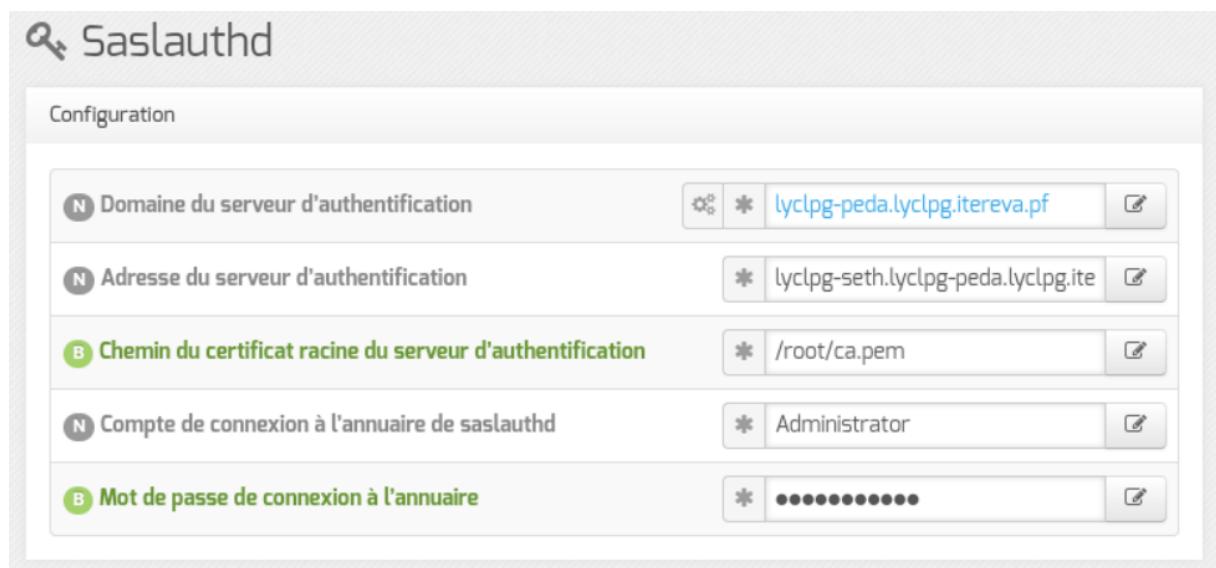
Eolead

Configuration

B Utiliser le serveur Active Directory local	[lock] * non
B Nom du serveur Active Directory	* lyclpg-seth
B Adresse IP du serveur Active Directory	* 172.18.0.3
N Adresse IP du serveur DNS de secours	
N Compte administrateur du domaine AD	* Administrator
N Conteneur Active Directory hébergeant les comptes du module EOLE	* CN=Users
N Synchroniser l'annuaire en LDAPS	* oui

Pour que l'OpenLDAP de Scribe se synchronise à l'AD de Seth, on n'utilise pas le serveur AD en local. Ensuite, on renseigne les informations de Seth et on active la synchronisation de l'annuaire en LDAPS.

Onglet Saslauthd



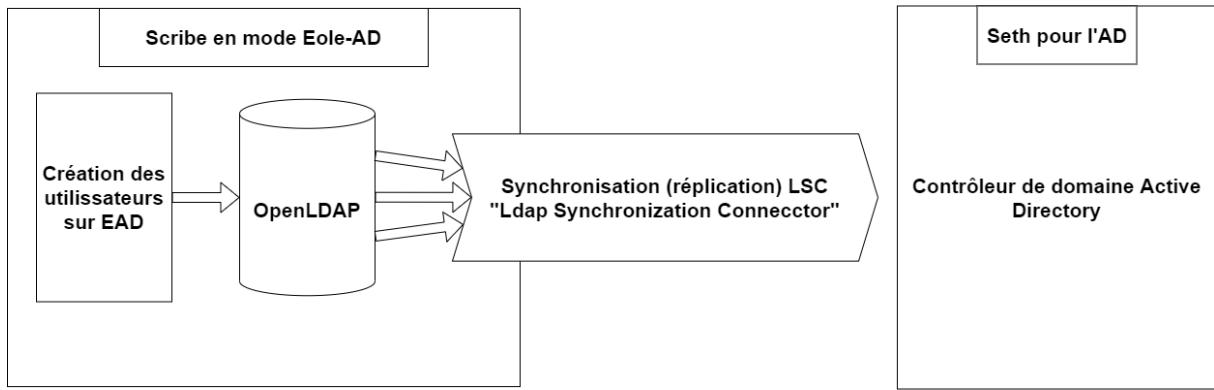
C'est un onglet obligatoire pour la synchronisation OpenLDAP à l'AD, il va nous permettre de nous identifier pour la synchronisation.

Nous ajoutons un nom de domaine de Seth qui est **lyclpg-peda.lyclpg.itereva.pf**. Ensuite, on indique l'adresse du serveur qui est Seth donc **lyclpg-seth.lyclpg-peda.lyclpg.itereva.pf**, le chemin du certificat racine (le certificat utilisé pour valider la connexion LDAPS avec le serveur d'authentification) et les identifiants du compte « Administrator ».

Intégration du certificat du Seth au Java Keystore de Scribe

La synchronisation de l'annuaire est configurée pour utiliser le protocole LDAPS, il est impératif d'enregistrer les certificats d'autorité du serveur AD dans le fichier Java keystore par défaut du module Scribe. Nous effectuerons alors ces commandes :

```
root@scribe:~# scp root@seth:/etc/ssl/certs/ca.crt /root/ca.pem
root@scribe:~# keytool -import -trustcacerts -keystore /etc/ssl
/certs/java/cacerts -storepass changeit -noprompt -alias eole-ad
-file /root/ca.pem
```



Après cela nous devons faire une « instance », durant l’instance Scribe demandera l’utilisateur pour entrer dans le domaine de Seth. L’utilisateur est « Administrator ».

EAD 2

Tous les modules de Eole possèdent d’une interface d’administration web nommée EAD (Eole Admin). L’EAD va nous permettre de gérer nos 3 modules sur une seule interface. Elle est atteignable via l’adresse IP de Amon tapé sur un navigateur, au l’occurrence <https://192.168.1.16:4200>. Ce qui nous donne le résultat suivant après ajouté tous les modules :



Préalablement, nous devons intégrer chaque certificat de chaque module dans Amon :

```
1 root@amon:~# scp root@scribe:/etc/ssl/certs/ca_local.crt /usr/local/share/ca-certificates/
2 root@amon:~# update-ca-certificates
```

Ensute, nous retournons sur l'interface web, nous allons dans **Ajouter un serveur** pour continuer notre manipulation :

The screenshot shows the 'AJOUTER UN SERVEUR' (Add Server) page. On the left, there's a sidebar with 'Administration' and various menu items. A dropdown for 'Choix de la position du menu:' is set to 'main1.css'. The main content area has tabs for three servers: 'lyclpg-amon2', 'lyclpg-seth', and 'lyclpg-scribe'. The 'lyclpg-scribe' tab is selected. The form fields are:

- Nom DNS du serveur (pas de https ni d'adresse IP): eda.lyclpg.itereva.pf
- Port du serveur de commande: 4201
- Nom du serveur (affiché dans l'onglet): lyclpg-scribe
- Login (local sur le serveur cible): root
- Mot de passe: (masked)

At the bottom are 'Ajouter' (Add) and 'Aide' (Help) buttons.

- **Nom DNS du serveur (pas de https ni d'adresse IP)** : Cela correspond au nom de domaine de la machine qui se trouve dans le certificat SSL du module.
- **Port du serveur de commande** : On laisse le port par défaut qui est **4201**.
- **Login (local sur le serveur cible)** : L'identifiant du module.
- **Mot de passe** : le mot de passe du module.

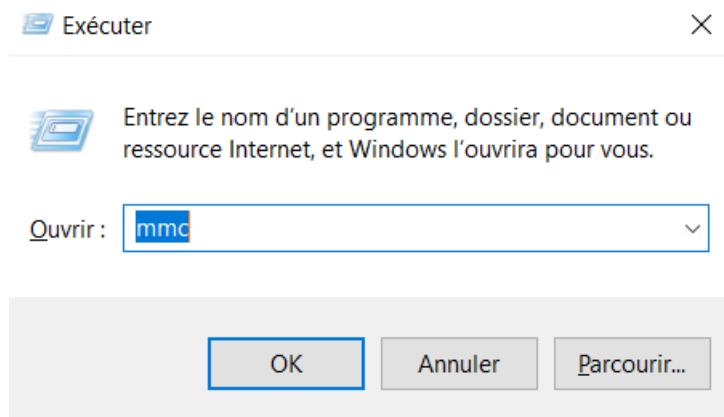
Et on refait la même manipulation pour tous les autres modules.

Création de UO et de GPO sur l'AD via l'outil Rsat.

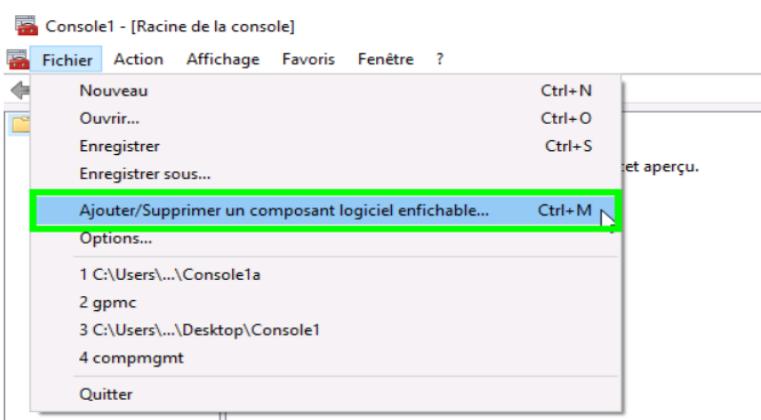
L'outil Rsat

Préalablement, dans le labo il y avait déjà une machine sous Windows 10 dans la zone peda-filaire où la fonctionnalité Rsat (Remote Server Administration Tools) est installée. La fonctionnalité Rsat est un outil fourni par Microsoft qui permet aux administrateurs système de gérer un serveur Windows Server (de 2008 à 2012 R2) depuis une version cliente de Windows telle que Windows 10. Nous avons donc ajouté cette machine au domaine de Seth pour que nous puissions gérer l'Active Directory et appliquer/créer des stratégies de groupe.

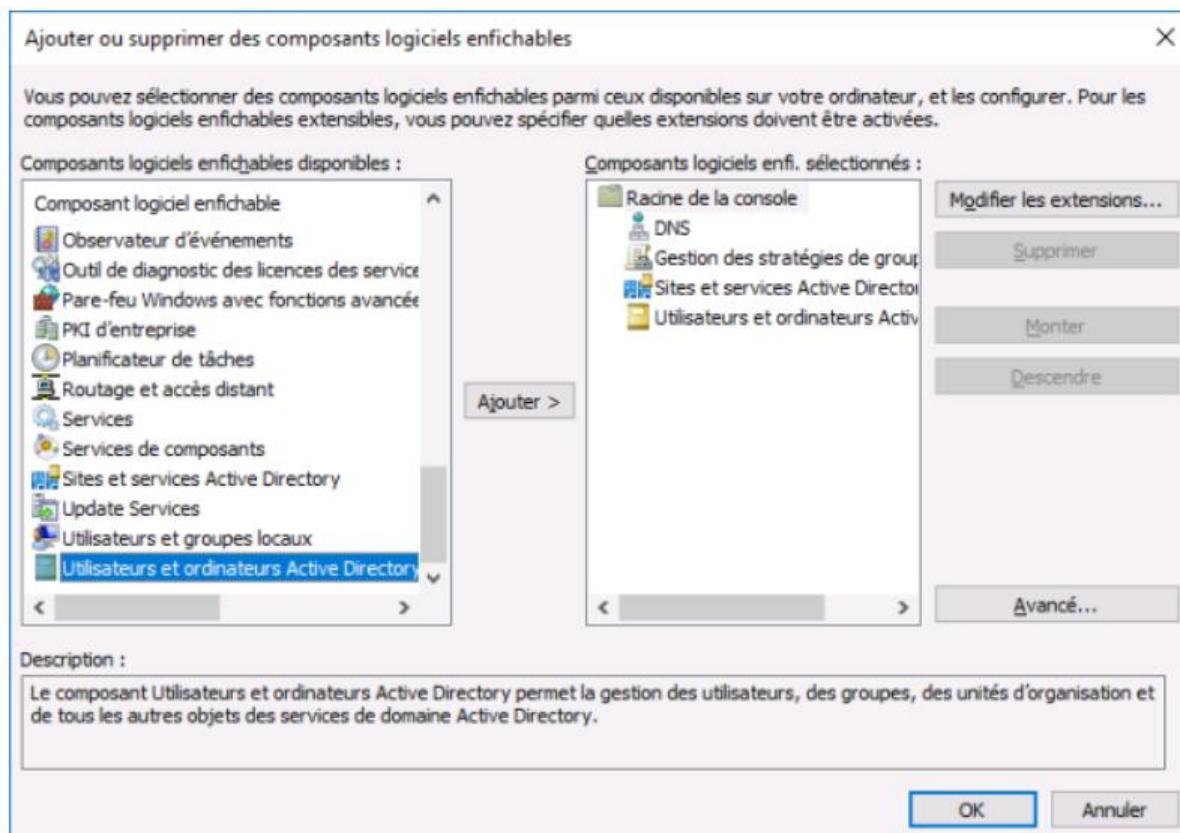
Nous lançons le « mmc » pour utiliser les outils d'administration.



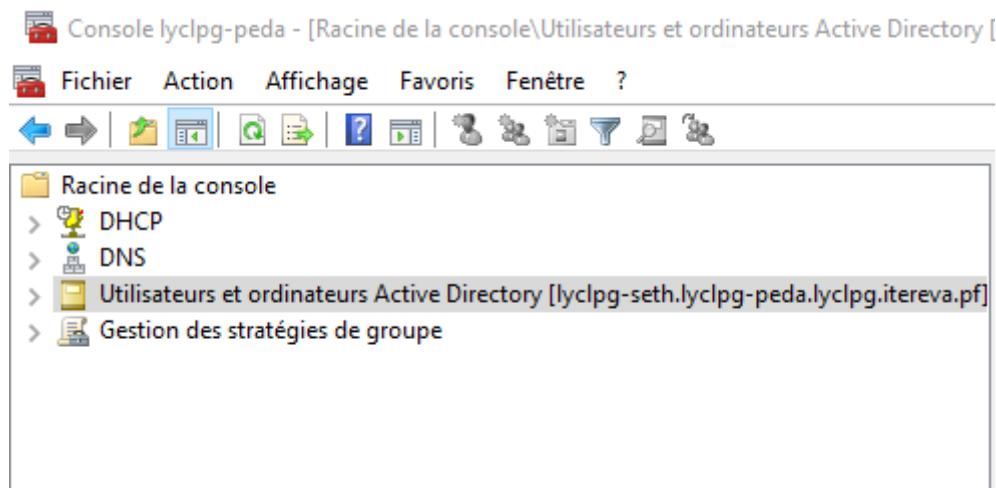
Nous allons sur « Ajouter/Supprimer un composant logiciel enfichable » afin d'ajouter des composants de gestion telle que DNS, Gestion des stratégies de groupe...



Maintenant choisissons les outils pour la gestion de l'Active Directory :



Nous voyons que nos outils n'ont pas de problème car on voit notre domaine :



Synchronisation des utilisateurs à l'Active Directory

Préalablement, j'ai créé des utilisateurs sur l'EAD de Scribe :

LISTER DES UTILISATEURS

OUTIL DE RECHERCHE D'UTILISATEUR

Lister les utilisateurs

Première lettre du login

Membre de la classe

Membre du groupe

Type d'adresse mail

Type de l'utilisateur

Partie du nom de famille

Nombre de résultats par page

40

Tri par

login

[Lister]

Nombre d'utilisateurs : 9

Nom	Mot de passe	Editer	Supprimer
admin (enseignant)	Changer le mot de passe	Editer	Supprimer
chansay (enseignant)	Changer le mot de passe	Editer	Supprimer
clement (administratif)	Changer le mot de passe	Editer	Supprimer
keanu (autre)	Changer le mot de passe	Editer	Supprimer
mali (enseignant)	Changer le mot de passe	Editer	Supprimer
mika (eleve)	Changer le mot de passe	Editer	Supprimer
noel (administratif)	Changer le mot de passe	Editer	Supprimer
supersapau (eleve)	Changer le mot de passe	Editer	Supprimer
test (autre)	Changer le mot de passe	Editer	Supprimer

Voici le résultat sur l'AD :

Console lyclpg-peda - [Racine de la console\Utilisateurs et ordinateurs Active Directory [lyclpg-seth.lyclpg-peda.lyclpg.itereva.pf]\lyclpg-peda.lyclpg.iterev]

Fichier Action Affichage Favoris Fenêtre ?

Racine de la console

DHCP

DNS

Utilisateurs et ordinateurs Active Directory [lyclpg-seth.lyclpg-peda.lyclpg.itereva.pf]

Requêtes enregistrées

lyclpg-peda.lyclpg.itereva.pf

Domain Controllers

Tout_le_monde

Classes

BTS

SIO

Machine

Profs

BTS

SIO

ForeignSecurityPrincipals

Users

Builtin

Managed Service Accounts

Computers

test

Gestion des stratégies de groupe

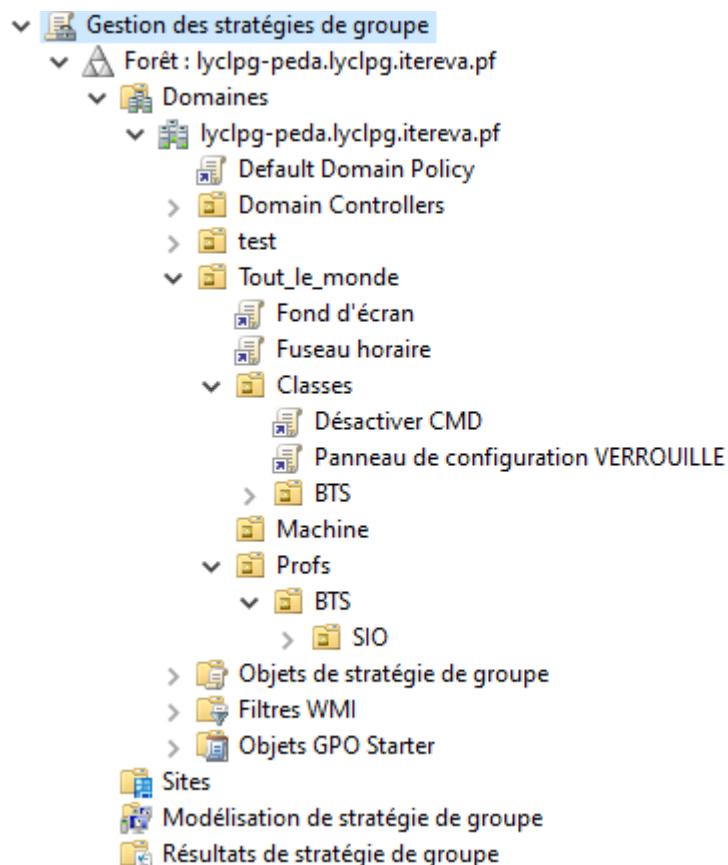
Nom	Type	Description
mika	Utilisateur	
supersapau	Utilisateur	
BTSSIO	Groupe de sécurité - Gl... Classe de BTS SIO	

Lors de nos tests, nous remarquons que la synchronisation peut mettre du temps et que la suppression d'un utilisateur est asynchrone et de ce fait nous avons une commande qui permet de forcer la synchronisation :

```
/usr/bin/lsc -f /etc/lsc -s all -c all -t 1
```

Création de GPO

Les stratégies de groupe vont permettre la gestion, la sûreté et la sécurité des ordinateurs et des utilisateurs dans l'environnement de l'AD. Pour notre part, voici les gestion mis en place :



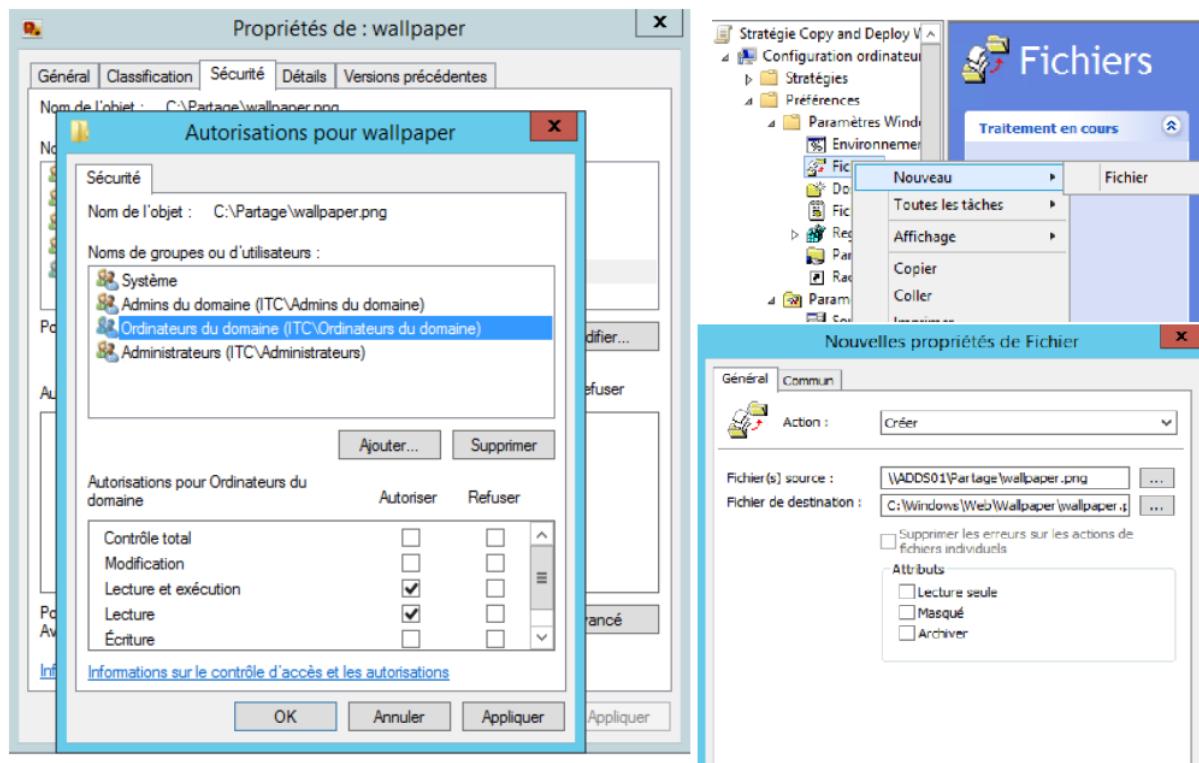
- **Fuseau horaire** : cela va permettre de toutes les machines du domaine d'avoir le même horaire.
- **Fond d'écran** : cela va harmoniser les fonds d'écrans de chaque ordinateur.

- **Désactiver CMD** : Limiter l'accès à l'invite de commande pour certain groupe d'utilisateur permet de sécuriser l'environnement contre possible geste malveillante.
- **Panneau de configuration VERROUILLE** : Limiter l'accès au panneau de configuration pour certain groupe d'utilisateur permet de sécuriser l'environnement contre possible geste malveillante.

Voici comment mettre en place les GPO :

Fond d'écran :

Il faut partager le fichier du fond d'écran, il doit être accessible par le réseau par les postes clients.



The screenshot shows the Group Policy Management Editor interface. On the left, a tree view displays various policy categories. In the center, a detailed configuration window for the 'Papier peint du Bureau' policy is open. The window has tabs for 'Paramètre précédent' and 'Paramètre suivant'. It includes sections for 'Commentaire', 'Pris en charge sur:', and 'Options'. A large text input field contains the path 'C:\Windows\Web\Wallpaper\wallpaper.jpg'. Below this, there's an 'Exemple' section with both local and UNC paths. A dropdown menu for 'Style du papier peint' is set to 'Center'. To the right of the main window is a detailed description of the policy, explaining its purpose and how it affects user desktops.

Désactiver CMD :

This screenshot shows the 'Système' section of the Group Policy Management Editor. A specific policy named 'Désactiver l'accès à l'invite de commandes' is selected. The left pane shows the full navigation tree. The right pane displays the policy details, including its description, configuration options, and a large list of associated parameters. The 'Paramètre' section lists items like 'Accès au stockage amovible' and 'Gestion de l'alimentation'. The 'Description' section explains the purpose of the policy, which is to prevent users from running command-line programs. A detailed description of the policy's behavior is provided below the main configuration area.

Panneau de configuration VERROUILLE :

