

23/05/2020

Projet UF

Gestion d'un Intranet

0

Louis LE SAUX, Ludovic SACHOT
YNOV CAMPUS

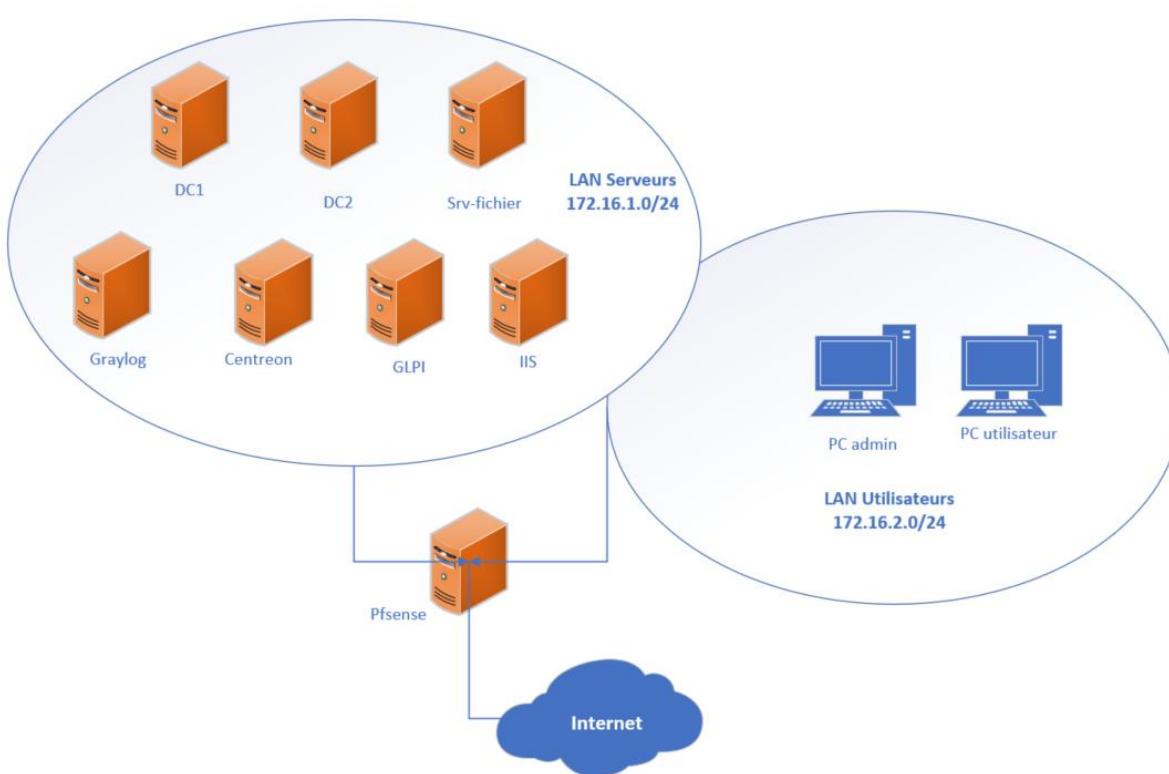
Table des matières

Contexte	2
Schéma de l'infrastructure par zone :	2
Service(s) par serveur :	3
Adressage IP :	3
Détail des bonnes pratiques :	4
Mise en place des contrôleurs de domaine :	5
1) Active directory	5
2) DNS.....	7
3) DHCP.....	9
Serveur de fichier :	10
Puit de log (Graylog) :	14
1) Linux	15
2) Windows.....	17
Logiciel de supervision (Centreon) :	19
Mise en place de l'intranet (IIS) :	20
Gestionnaire de tickets (GLPI)	24
Portail captif	32
Routeur/Firewall (Pfsense) :	37
Sauvegarde des VM :	43

Contexte

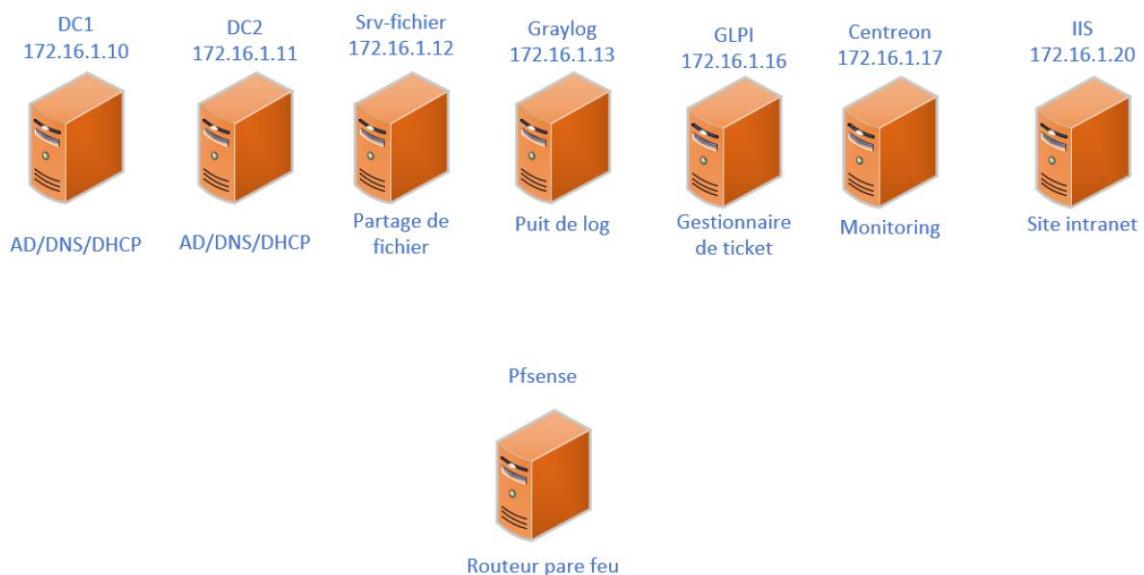
L'objectif de notre projet était de mettre en place une gestion simplifiée de l'ensemble de services IT d'une entreprise. Nous avons donc mis en place différents services telle qu'un contrôleur de domaine (AD/DNS/DHCP). Nous avons également ajouté une deuxième machine virtuelle portant les mêmes rôles pour pouvoir ajouter de la redondance. Nous avons également mis en place un serveur de fichier pour que les utilisateurs du domaine puissent stocker leurs données. Nous avons également ajouté des machines virtuelles pour pouvoir centraliser les logs et monitorer notre infrastructure. Un serveur web (IIS) a aussi été mis en place pour que les utilisateurs puissent accéder à l'Intranet. Cette intranet permet aux utilisateurs du domaine d'accéder à leur messagerie (Gmail), à au gestionnaire de ticket (GLPI) mais aussi à leur agenda.

Schéma de l'infrastructure par zone :



Nous avons mis en place un PfSense pour avoir 2 réseau distant. Un réseau pour les utilisateurs et un réseau pour les serveurs. Les noms de ces derniers y sont retranscrits et appartiennent au domaine « uf_infra_B.local ».

Service(s) par serveur :



Adressage IP :

LAN Serveur

Hotes	Adresse IP	Passerelle
DC1	172.16.1.10	172.16.1.1
DC2	172.16.1.11	172.16.1.1
srv-fichier	172.16.1.12	172.16.1.1
Graylog	172.16.1.13	172.16.1.1
glpi	172.16.1.16	172.16.1.1
centreon	172.16.1.17	172.16.1.1
IIS	172.16.1.20	172.16.1.1

Pfsense

Interface	LAN segment
192.168.1.19	WAN
172.16.1.1	LAN Serveurs
172.16.2.1	LAN User

LAN User

Note	Adresse IP	Passerelle
PC admin	172.16.2.10	172.16.2.1
PC user	172.16.2.100	172.16.2.1

Détail des bonnes pratiques :

- Les utilisateurs de l'entreprise doivent changer leur mot de passe tous les mois.
- Forme du mot de passe : caractère spéciaux, chiffre, lettre majuscule obligatoire).
- Sauvegarde régulière vers google drive.
- Seuls les administrateurs ont le rôle d'admin du domaine.
- Les utilisateurs n'ont pas le droit de circuler sur les sites pouvant nuire à leur travail (Réseaux sociaux, site pornographique, etc...).
- Configuration d'une redondance pour le contrôleur de domaine.
- Réseaux sécurisés.
- Les mises à jour sont effectuées régulièrement.

Mise en place des contrôleurs de domaine :

Nous avons commencé par ajouter les rôles AD/DNS/DHCP sur les deux serveurs. Nous avons ensuite créé notre nom de domaine (uf_infra_B.local). Après avoir créé notre domaine sur le premier contrôleur de domaine, nous avons ajouté le second à celui-ci. Nous l'avons ensuite promu en tant que contrôleur de domaine à un domaine existant.

Adressage IP des serveurs :

Nom = DC1.uf_infra_B.local

@IP = 172.16.1.10/24

Passerelle = 172.16.1.1

DNS primaire : lui-même

DNS secondaire : DC2 (172.16.1.11)

Nom = DC2.uf_infra_B.local

@IP = 172.16.1.11/24

Passerelle = 172.16.1.1

DNS Primaire = Lui-même

DNS secondaire = DC1 (172.16.1.10)

1) Active directory

Nous avons ensuite configuré l'Active Directory en ajoutant 13 utilisateurs séparé en plusieurs service (groupe).

Administrateurs	Développeurs	Equipe administrative	Chef de projet
Louis Le Saux	Gaetan Maltruno	Marc Henry	Carles Dariot
Ludovic Sachot	Eric Malenc	Marie Darienzo	Jessica Pontier
	Franck		
Maxime Lacharge	Hernandez	Segolène Namache	
	Jack Lelouche		
	Olivia Mourneau		

Chef d'équipe	Direction	RH
Maxime Lacharge	Marc Henry	Segolène Namache
Gaetan Maltruno	Marie Darienzo	

Les différents utilisateurs ont été créés dans l'AD et placé dans des OU spécifiques.

	Nom	Type	Description
Requêtes enregistrées			
uf_infra_B.local			
> Builtin			
> Computers			
> Domain Controllers			
> ForeignSecurityPrincipal			
> Groupes			
> Managed Service Account			
> Ordinateurs			
> Serveurs			
> Users			
> Utilisateurs			
> Administratif			
> Admins			
> Chef de projet			
> Développeur			
eric malenc	Utilisateur		
Franck Hernandez	Utilisateur		
Gaetan Maltruno	Utilisateur		
Jack Lelouche	Utilisateur		
Olivia Mourneau	Utilisateur		

Ils ont également été ajoutés à leur groupe respectif (nous verrons que les groupes sont importants pour le serveur de fichiers).

Nom	Type	Description
grp_Administrateur	Groupe de sécurité	
grp_Administratif	Groupe de sécurité	
grp_Chef de projet	Groupe de sécurité	
grp_Chef d'équipe	Groupe de sécurité	
grp_Développeur	Groupe de sécurité	
grp_Direction	Groupe de sécurité	
grp_RH	Groupe de sécurité	

Propriétés de : grp_Administrateur

Membres :

Nom	Dossier Services de domaine Active Directory
louis le saux	uf_infra_B.local/Utilisateurs/Admins
ludovic sachot	uf_infra_B.local/Utilisateurs/Admins
Maxime Lach...	uf_infra_B.local/Utilisateurs/Admins

Les administrateurs ont été ajoutés au groupe « admins du domaine ».

Les différents serveurs installés ont tous été ajoutés au domaine :

Nom	Type	Type de contrôleur	Site	Description
DC1	Ordinateur	GC	Default-First-Site	
DC2	Ordinateur	GC	Default-First-Site	

Nom	Type	Description
CENTREON	Ordinateur	
GLPI	Ordinateur	
GRAYLOG	Ordinateur	
IIS	Ordinateur	
SRV-FICHIER	Ordinateur	

Ainsi que les postes de travail :

Nom	Type	Description
DESKTOP-45C1E9U	Ordinateur	PC utilisateurs
DESKTOP-IDUGKSS	Ordinateur	PC admin

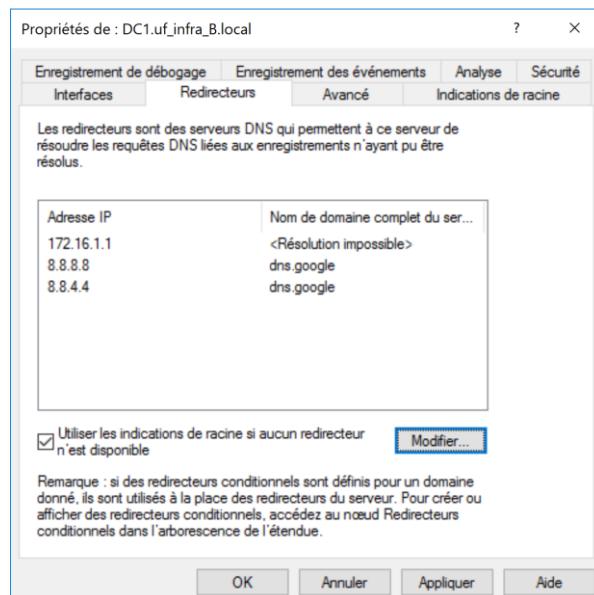
2) DNS

Dans le gestionnaire DNS, nous avons ajouté tous les hôtes avec leur adresse IP dans les zones de recherche directes.

ForestDNSZones			
(identique au dossier parent)	Source de nom (SOA)	[345], dc1.uf_infra_b.local....	statiqu
(identique au dossier parent)	Serveur de noms (NS)	dc1.uf_infra_b.local.	statiqu
(identique au dossier parent)	Serveur de noms (NS)	dc2.uf_infra_b.local.	statiqu
(identique au dossier parent)	Hôte (A)	172.16.1.10	18/05/
(identique au dossier parent)	Hôte (A)	172.16.1.11	21/05/
centreon	Hôte (A)	172.16.1.17	statiqu
dc1	Hôte (A)	172.16.1.10	statiqu
DC2	Hôte (A)	172.16.1.11	statiqu
DESKTOP-45C1E9U	Hôte (A)	192.168.1.160	30/03/
DESKTOP-IDUGKSS	Hôte (A)	172.16.1.100	22/05/
glpi	Hôte (A)	172.16.1.16	statiqu
graylog	Hôte (A)	172.16.1.13	statiqu
IIS	Hôte (A)	172.16.1.20	22/05/
Intranet	Alias (CNAME)	IIS.uf_infra_B.local.	statiqu
srv-fichier	Hôte (A)	172.16.1.12	statiqu

Nous avons également ajouté un alias pour le serveur IIS pour qu'il soit joignable via le nom « Intranet ». Cela sera utile lorsque l'on mettra en place l'intranet.

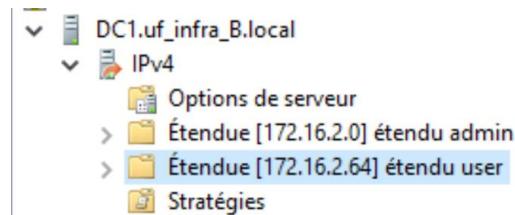
Nous avons également ajouté des redirecteurs au cas où les contrôleurs de domaine n'arrivent pas à résoudre des requêtes DNS.



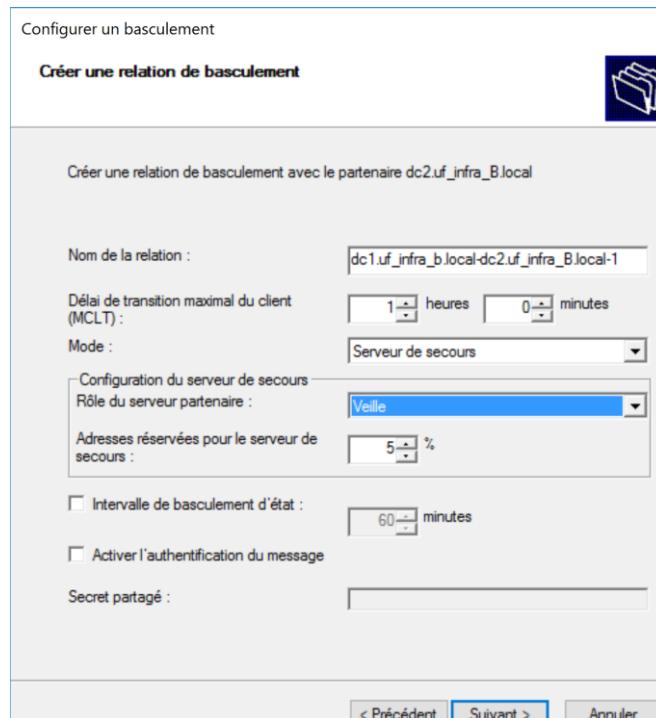
3) DHCP

Nous avons mis en place 2 étendus pour notre infrastructure.

La première est réservée aux PC des administrateurs. La seconde est réservée aux utilisateurs de l'entreprise.



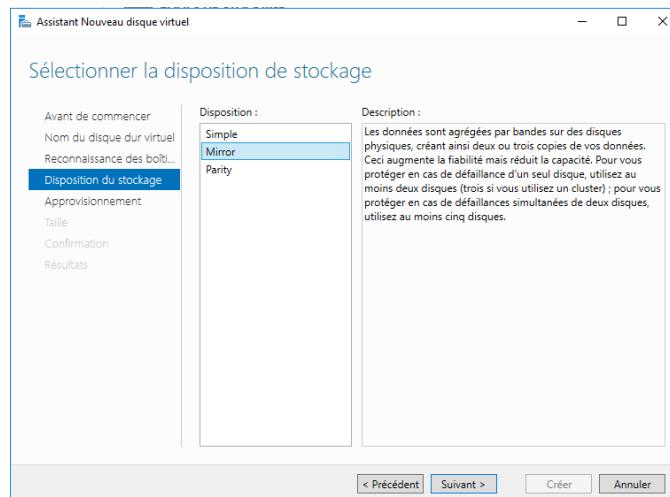
Nous avons également prévu un basculement entre les deux contrôleurs de domaine. Il a été décidé que le 1^{er} contrôleur de domaine (DC1) serait le serveur DHCP principale. Le DC2 sera donc le serveur de secours. Nous avons choisi de mettre cela en place pour pallier à une éventuelle panne du DC1. Le second contrôleur de domaine délivrera les adresses aux différents PC.



Serveur de fichier :

Nous avons donc mis un serveur de fichier pour que les utilisateurs de l'entreprise puissent stocker leur document dans des dossiers partagés.

Pour cela, nous avons choisi d'utiliser deux disques pour pouvoir faire du miroir sur ces deux disques. Dans ce cas, les données seront écrites sur les deux disques en simultanément.

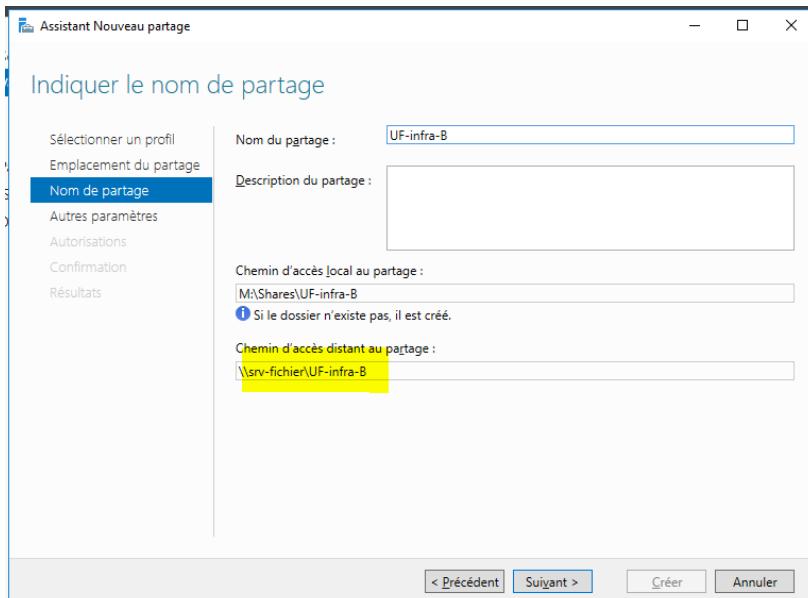


Nous avons également choisi d'utiliser un approvisionnement fixe permettant ainsi d'utiliser la totalité de l'espace disque.

Nous avons, dans un premier temps, créé le volume « M » avec le disque virtuel créé précédemment.

Dans un second temps, nous avons créé notre dossier partagé avec un partage SMB simple (pas besoin de gestionnaire de quotas ou autres car nous sommes une petite entreprise).

Pour pouvoir accéder au partage depuis un poste utilisateur, il faudra noter le chemin suivant dans l'explorateur de fichier <\\srv-fichier\uf-infra-B> (srv-fichier étant le nom du serveur et uf-infra-B le nom du dossier partagé).



Test avec le compte I.lesaux (admins du domaine) :

The screenshot shows the Windows File Explorer interface displaying the contents of the '\\SRV-FICHIER\UF-infra-B' share. The left sidebar shows 'Accès rapide' (Quick access) with links to Bureau, Téléchargements, Documents, Images, conf, and System32. The main pane lists files and folders with the following details:

Nom	Modifié le	Type	Taille
00-Global	24/03/2020 13:47	Dossier de fichiers	
01-Direction	24/03/2020 13:39	Dossier de fichiers	
02-Service ressources humaines	24/03/2020 13:38	Dossier de fichiers	
03-Chefs d'équipes global	24/03/2020 13:39	Dossier de fichiers	
04-Chef de projet	24/03/2020 13:38	Dossier de fichiers	
05-Service développement	24/03/2020 13:38	Dossier de fichiers	
06-Service serveurs, Réseau, bureautique	24/03/2020 13:39	Dossier de fichiers	

Les comptes Admins du domaine ont accès à tous les dossiers en contrôle total pour que ceux-ci puissent répondre aux demandes utilisateurs (demande d'accès, etc...).

Les accès au dossier sont gérés uniquement par des groupes (groupe AD créé précédemment).

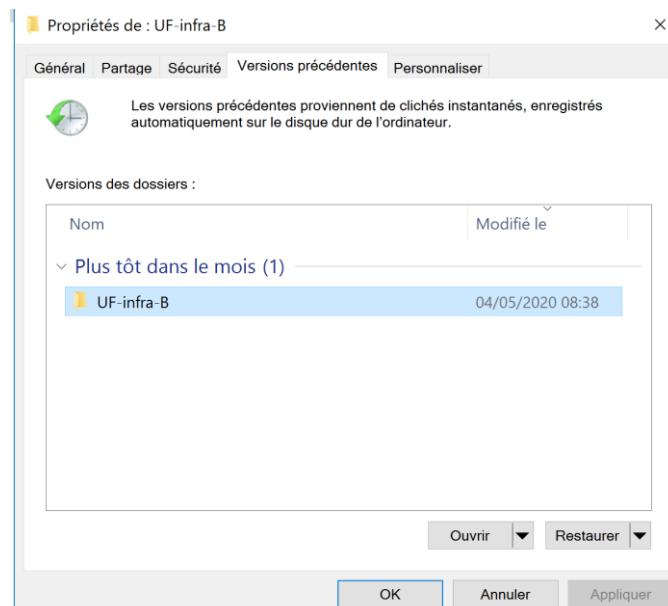


Cela permet donc de faciliter l'administration du serveur de fichiers.

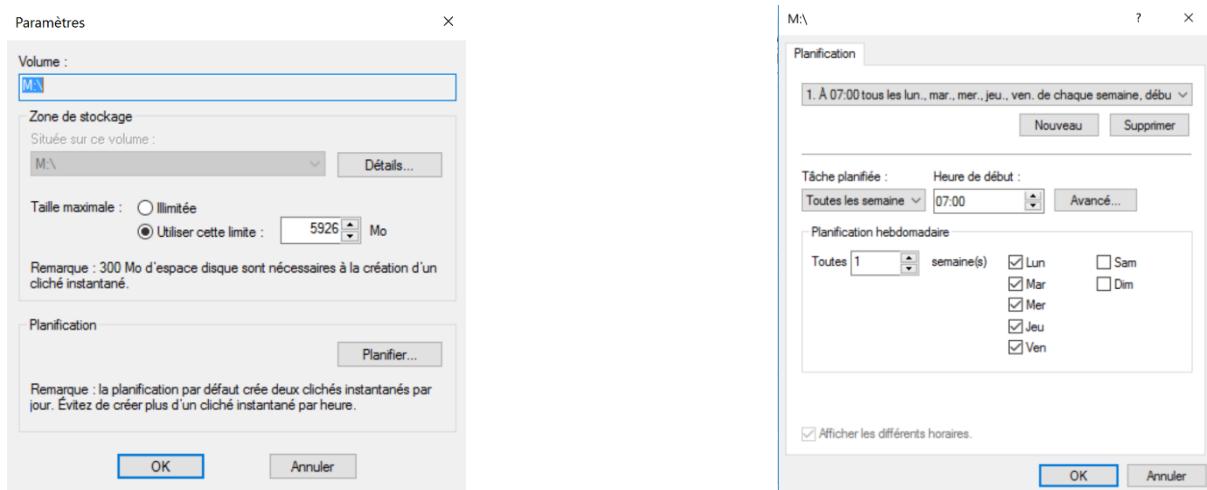
00-Global	01-Direction	02-Service Ressources humaines
Utilisateurs du domaine	grp_Direction	grp_RH
03-Chefs d'équipe global	04-Chef de projet	05-Service développement
grp_Chef d'équipe	grp_Chef de projet	grp_développeur
06-Service serveurs, Réseau, Bureautique		
Admins du domaine		

Cette gestion par groupe permet aux administrateurs de gérer plus efficacement les accès dossiers. L'intérêt de cette méthode paraît limité dans le cadre d'une petite entreprise mais devient intéressante sur des plus grandes entreprises

Nous avons également mis en place les versions précédentes sur ce dossier. Cela est utile dans le cas où un utilisateur supprime malencontreusement un dossier ou un fichier.



Pour cela, nous avons mis en place les clichés instantanées sur le disque M (disque partagé).



Ces clichés instantanés sont planifiés tous les jours ouvré de la semaine à partir de 7h avant que les utilisateurs commencent à travailler. Dans le cas d'une grande entreprise, il est préférable d'effectuer cela pendant la nuit pour éviter tous ralentissement car l'opération risque d'être longue si le nombre de dossiers et fichiers est très grand.

Puit de log (Graylog) :

Nous avons décidé de mettre en place un puit de logs pour pouvoir récolter tous les logs systèmes de tous les serveurs de notre infrastructure. Nous avons donc décidé de mettre en place un Graylog.

Source d'installation :

<https://www.itzgeek.com/how-tos/linux/centos-how-tos/how-to-install-graylog-on-centos-7-rhel-7.html>

Graylog a besoin de certains prérequis avant de commencer l'installation :

- Installation de java car Graylog et Elasticsearch sont tous les deux basés sur ce langage.
- Elasticsearch : Graylog utilise Elasticsearch pour stocker les **messages du journal** et propose également une fonction de recherche.
- MongoDB : Graylog utilise MongoDB comme base de données pour stocker des métadonnées (informations utilisateurs ou configuration de flux) et des configurations. (Stocker les données de CONFIGURATION et non pas les données de JOURNAL). MongoDB n'a pas un gros impact sur le système (pas nécessaire de le faire évoluer).

Après avoir installé le serveur Graylog, il nous est possible d'accéder à l'interface web (via l'adresse IP du serveur) nous permettant de configurer la centralisation des logs.

The screenshot shows the Graylog web interface. At the top, there is a navigation bar with links for Search, Streams, Alerts, Dashboards, Sources, and System. A red notification badge with the number '1' is visible on the System link. Below the navigation bar, the title 'Getting Started - Graylog v3.0.2+1686930' is displayed. A sub-header below it says 'No one is born a master. Use this page if you need assistance with your first steps. Make sure to ask the community if you have any questions.' Below this, there is a numbered list of four steps:

- 1 **Send in first log messages**
Graylog is pretty useless without some log data in it. Let's start by sending in some messages.
- 2 **Do something with your data**
Perform searches to solve some example use cases and get a feeling for the basic Graylog search functionality.
- 3 **Create a dashboard**
Dashboards are a great way to organize information that you look at often. Learn how to create them and how to use them effectively.
- 4 **Be alerted**
Immediately receive alerts and trigger actions when something interesting or unusual happens.

Pour pouvoir centraliser les logs des différents serveurs sur le graylog, nous avons dû ajouter des agents sur les différents serveurs. Bien sûr, la procédure est différente entre les serveurs Linux et Windows

Nous avons ajouté tous les serveurs pour pouvoir centraliser leur log dans une seule interface (DC1, DC2, srv-fichier, IIS, Graylog, GLPI, Centreon)

1) Linux

Pour commencer, sur l'interface web de Graylog, ajoutez une règle « inputs ».

The screenshot shows the Graylog search interface. The left sidebar lists various fields like action, app, appcat, date, devid, devname, and dstcountry. The right sidebar shows a navigation tree under 'System' with 'Inputs' highlighted. A message at the top says 'Found 2,267 messages in 8 ms, searched in 1 index.'

Ensuite, ajoutez un input Syslog (TCP et UDP) puis cliquez sur « Launch new input »

Inputs

Graylog nodes accept data via inputs. Launch or terminate as many inputs as you want here.

The screenshot shows the 'Inputs' page with a search bar containing 'Syslog TCP'. Below it are two buttons: 'Launch new input' and 'Find more inputs'.

Ajoutez les config suivantes puis cliquez sur valider :

The configuration dialog for a new Syslog TCP input. It includes fields for 'Global' (checkbox), 'Node' (dropdown set to '0792ebf4 / graylog.ghb.local'), 'Title' (text input 'Syslog Test'), 'Bind address' (text input '0.0.0.0'), and 'Port' (text input '514').

Node représente le serveur sur lequel nous voulons ajouter les logs (notre serveur).

Nous avons choisi le port 1514 car nous ne pouvons pas utiliser le port 514 comme préciser dans sur le site « itzgeek.com ».

Après avoir configurer les deux « inputs » vous pouvez passer à l'étape suivante.

Syslog TCP Syslog TCP RUNNING
On node ★ 0792ebf4 / graylog.ghb.local

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
max_message_size: 2097152
number_worker_threads: 4
override_source: <empty>
port: 1514
recv_buffer_size: 1048576
store_full_message: false
tcp_keepalive: false
tls_cert_file: <empty>
tls_client_auth: disabled
tls_client_auth_cert_file: <empty>
tls_enable: false
tls_key_file: <empty>
tls_key_password: *****
use_null_delimiter: false
```

Syslog UDP Syslog UDP RUNNING
On node ★ 0792ebf4 / graylog.ghb.local

```
allow_override_date: true
bind_address: 0.0.0.0
expand_structured_data: false
force_rdns: false
number_worker_threads: 4
override_source: <empty>
port: 1514
recv_buffer_size: 262144
store_full_message: false
```

Ensute, entrez dans le fichier de config `/etc/rsyslog.conf`

Ajouter la ligne suivante à la fin du fichier de config (*.*) @ « @ip du graylog » : « port utilisé ») puis enregistrer.

Cette ligne permet de répertorier « tous les logs » du serveur en question sur le serveur Graylog.

```
GNU nano 2.3.1                               Fichier : /etc/rsyslog.conf

# Save news errors of level crit and higher in a special file.
*.* @172.16.1.13:1514          /var/log/spooler

# Save boot messages also to boot.log
local7.*                                /var/log/boot.log

### begin forwarding rule ####
# The statement between the begin ... end define a SINGLE forwarding
# rule. They belong together, do NOT split them. If you create multiple
# forwarding rules, duplicate the whole block!
# Remote Logging (we use TCP for reliable delivery)

# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
$ActionQueueFileName fwdRule1 # unique name prefix for spool files
$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
$ActionQueueType LinkedList  # run asynchronously
$ActionResumeRetryCount -1   # infinite retries if host is down
*.* @172.16.1.13:1514
### end of the forwarding rule ###
```

Redémarrer le service rsyslog `service rsyslog restart`

Ouvrir le port 9000, 514 et 1514 + les service http et https sur le serveur ayant besoin de l'agent.

Ouvrir le port 514 et 1514 sur le serveur graylog.

2) Windows

Sur l'interface web Graylog, nous avons ajouté l'entrée suivante :

```

nxlog UDP GELF UDP RUNNING
On node ★ 7b0c4af5 / graylog

bind_address: 0.0.0.0
decompress_size_limit: 8388608
number_worker_threads: 1
override_source: <empty>
port: 1514
recv_buffer_size: 262144

```

Sur les serveurs Windows sur lesquels nous voulons récupérer les logs, nous avons installé nxlog.

Ensuite, nous avons modifier le fichier nxlog.conf « C:\Program Files (x86)\nxlog\conf\nxlog.conf »

```

<Extension _syslog>
    Module      xm_syslog
    #Module    xm_gelf
</Extension>

<Input in>
    Module      im_msvistalog
</Input>

<Output out1>
    Module      om_tcp
    host        172.16.1.13
    Port        1514
    Exec        to_syslog_snare();
    #OutputType GELF
</Output>

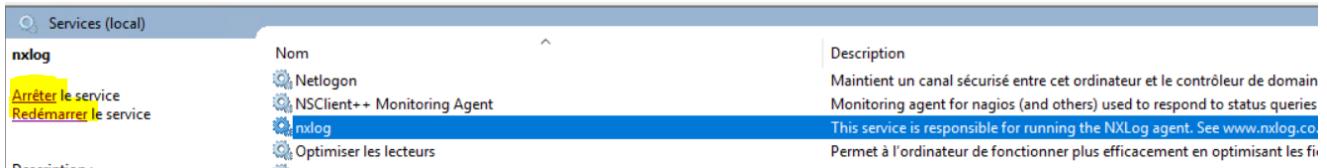
<Output out2>
    Module      om_udp
    Host        172.16.1.13
    Port        1514
    Exec        to_syslog_snare();
    #OutputType GELF
</Output>

<Route 1>
    Path in=> out1, out2

```

Enregister le fichier modifié.

Windows+R → services.msc et rechercher nxlog. Cliquer sur démarrer



Le serveur remonte après sur le graylog,

Après avoir effectuée cette opération sur tous les serveurs, nous pouvons constater dans l'onglet « Search » que de tous les logs des serveurs remontent sur le graylog.

2020-05-23 08:44:29.000	DC1.uf_infra_B.local	DC1.uf_infra_B.local MSWinEventLog 1 Microsoft-Windows-GroupPolicy 1 N/A La tâche de transfert est terminée. Utilisateur : \Système Nombre de fichiers : 1 10276
2020-05-23 08:44:29.000	DC1.uf_infra_B.local	DC1.uf_infra_B.local MSWinEventLog 1 Security 6 Sat May 23 10 n compte. Sujet : ID de sécurité : S-1-5-18 Nom du compte : D rite est supprimé. Il peut être associé à un événement d'ouverture sur un même ordinateur. 37368
2020-05-17 18:24:34.000	IIS.uf_infra_B.local	IIS.uf_infra_B.local MSWinEventLog 1 System 11 Sun May 17 20: entré dans l'état : arrêté. 4466
2020-05-17 18:24:06.000	graylog	graylog [sssd[ldap_child[1907]]]: Failed to initialize decrypted LDAP connection.
2020-05-17 18:24:06.000	graylog	graylog [sssd[ldap_child[1906]]]: Failed to initialize decrypted LDAP connection.
2020-05-17 18:23:56.000	graylog	graylog [sssd[ldap_child[1905]]]: Failed to initialize decrypted LDAP connection.
2020-05-17 18:23:53.000	graylog	graylog [sssd[ldap_child[1904]]]: Failed to initialize decrypted LDAP connection.
2020-05-17 18:23:50.000	IIS.uf_infra_B.local	2020-05-23 14:16:51.000 srv-fichier.uf_infra_B.local
		srv-fichier.uf_infra_B.local MSWinEventLog 1 Microsoft-Windows-System 13 S automatique Windows Update Windows Update a démarré le télé
		2020-05-17 14:32:00.000 glpi
		glpi systemd[1]: Reloading.
		2020-05-17 14:31:58.000 graylog
		graylog [sssd[ldap_child[1933]]]: Failed to initialize decrypted LDAP connection.
		2020-05-17 14:31:01.000 centreon
		centreon systemd: Created slice User Slice of centreon.

Logiciel de supervision (Centreon) :

Nous avons choisi d'installer Centreon pour pouvoir superviser l'ensemble de notre infrastructure. Nous n'avons pas eu le temps d'ajouter tous les connecteurs souhaités par manque de temps et car nous avons été confrontés à d'autres problèmes.

Nous pouvons donc accéder à Centreon via l'adresse IP du serveur (<http://172.16.1.17/centreon>).

Nous avons donc ajouté tous les serveurs de notre infrastructure.

<input type="checkbox"/> Nom	Alias	Adresse IP / DNS	Collecteur
<input type="checkbox"/> DC1	⚙️	172.16.1.10	Central
<input type="checkbox"/> DC2	⚙️	172.16.1.11	Central
<input type="checkbox"/> glpi	⚙️	172.16.1.16	Central
<input type="checkbox"/> graylog	⚙️	172.16.1.13	Central
<input type="checkbox"/> IIS	⚙️	172.16.1.20	Central
<input type="checkbox"/> srv-fichier	⚙️	172.16.1.12	Central

Nous avons également regroupé ces hôtes en groupe.

Plus d'actions... ▾
Ajouter

<input type="checkbox"/> Nom
<input type="checkbox"/> Serveur_Linux
<input type="checkbox"/> Serveur_Windows

Plus d'actions... ▾
Ajouter

Ensuite, nous avons ajouté le modèle PING pour savoir si les serveurs sont allumés ou non.

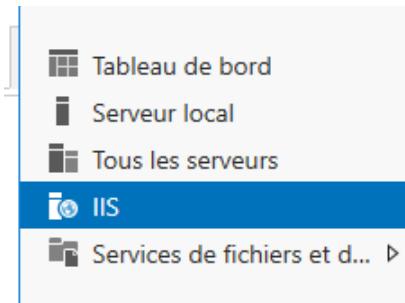
<input type="checkbox"/> Groupe d'hôtes	Service	Planification	Modèle
<input type="checkbox"/> Serveur_Linux	⚙️ Ping Serveurs	5 min / 1 min	> Base-Ping-LAN > generic-active-service-custom > generic-active-service
<input type="checkbox"/> Serveur_Windows	⚙️ Ping Serveurs	5 min / 1 min	> Base-Ping-LAN > generic-active-service-custom > generic-active-service

Nous avons donc ajouté uniquement un test de la requête ping permettant de faire remonter les serveurs qui seraient fonctionnel.

Mise en place de l'intranet (IIS) :

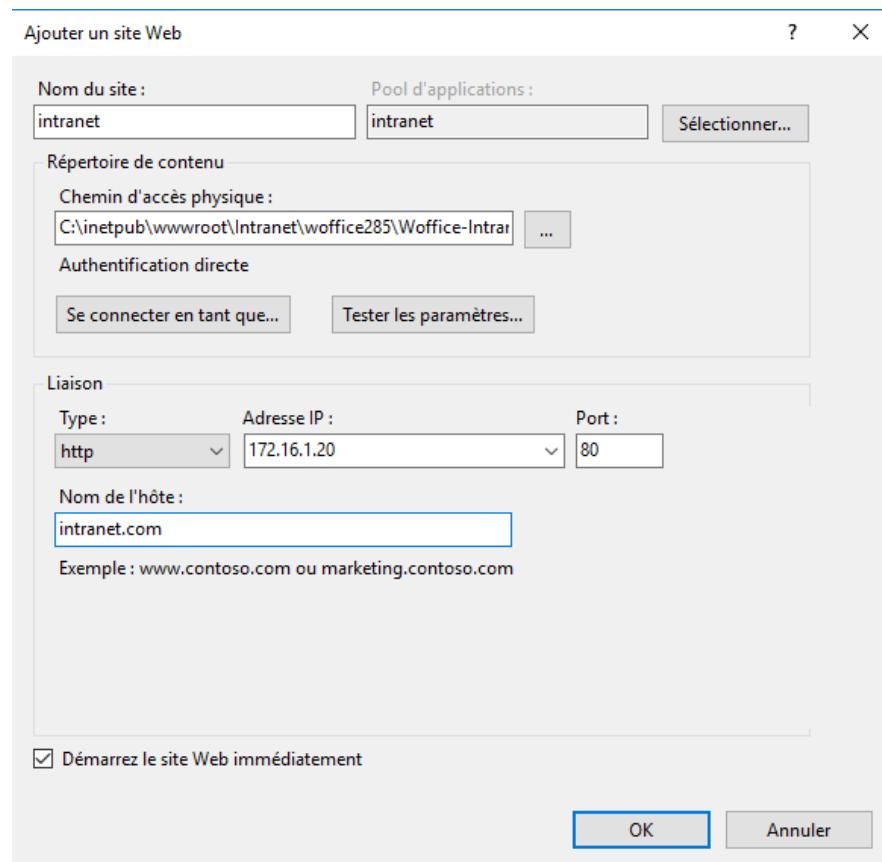
L'intranet de l'entreprise sera hébergé sur un serveur Web IIS. Nous avons décidé d'utiliser un Template Wordpress à cette adresse : <https://www.vestathemes.com/>; cette solution nous permet de gagner du temps tout en ayant un site opérationnel

Le rôle « IIS » devra être installé sur notre Windows Server 2016

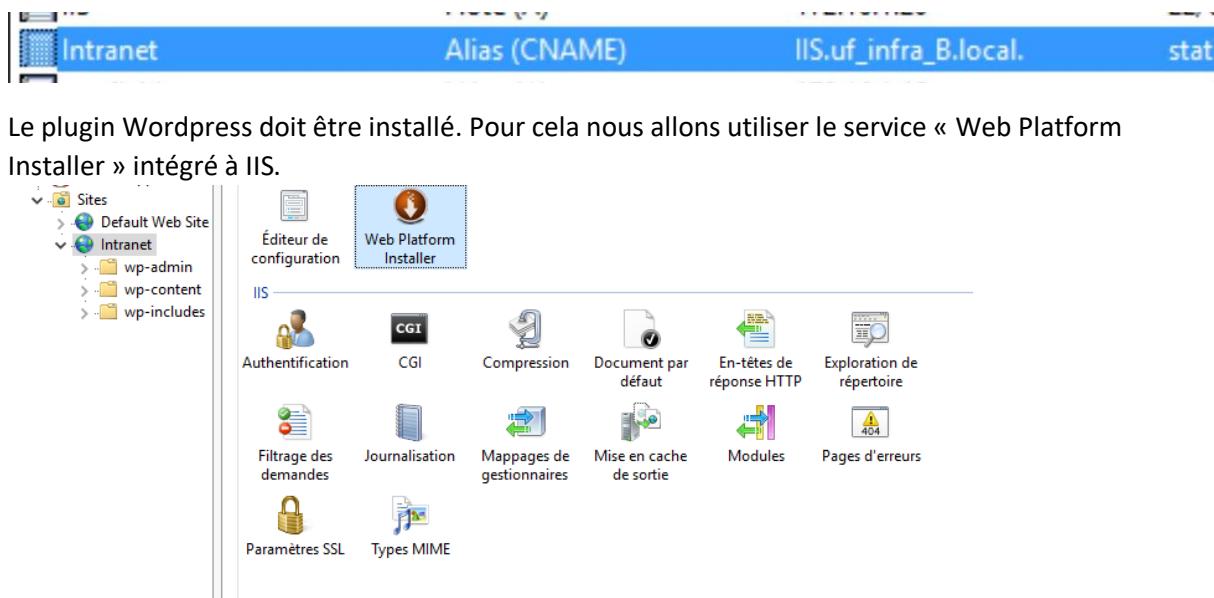


Nous pouvons désormais ajouter un site Web sur IIS :

- Nous le nommons « Intranet »
- Nous définissons son emplacement physique
- On renseigne son IP (ici nous prenons l'IP du serveur) ainsi que son port. Étant donné que notre intranet sera en http, nous choisissons le port 80



Ajout de l'alias « Intranet »

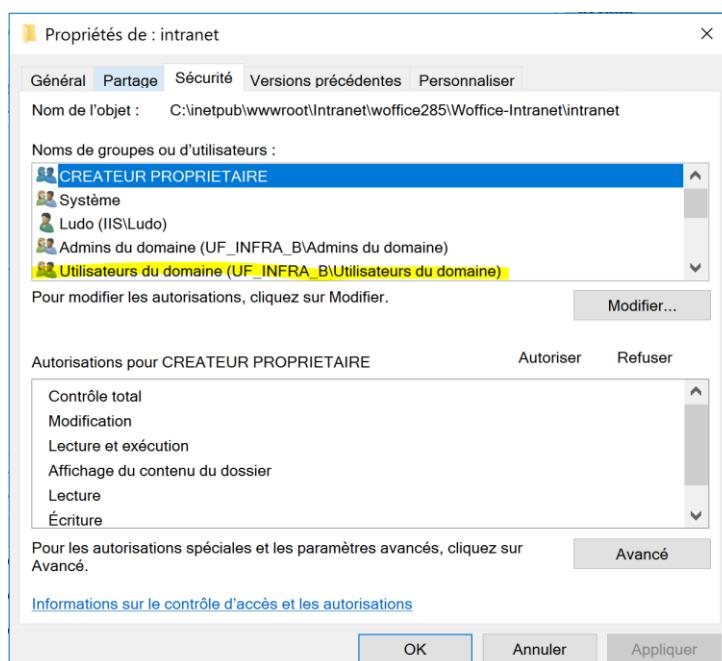


Le plugin Wordpress doit être installé. Pour cela nous allons utiliser le service « Web Platform Installer » intégré à IIS.

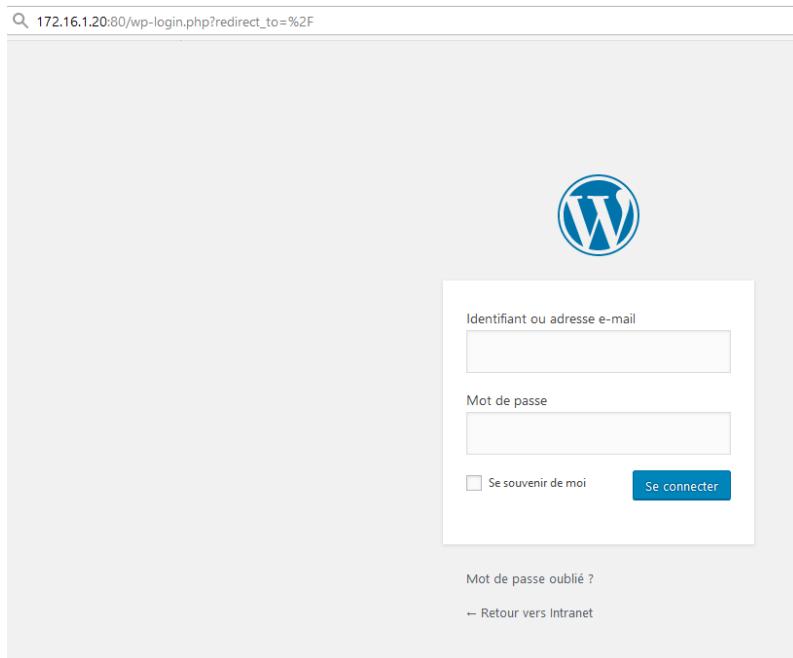
Gestion des authentifications : Nous avons ajouté l'authentification Windows afin que les clients puissent accéder au site grâce à leur compte du domaine

Regrouper par :	Aucun regroupement	
Nom	État	Type de réponse
Authentification anonyme	Activé	
Authentification Windows	Activé	Stimulation HTTP 401
Emprunt d'identité ASP.NET	Désactivé	

Gestion des droits : Permettre l'accès en lecture au dossier « Intranet » pour les utilisateurs du domaine afin de leur permettre de naviguer sur le site.



Il est désormais possible d'accéder à Wordpress depuis un navigateur



Nous atterrissions sur la page d'accueil de l'intranet



Nous avons implanté 2 boutons :

- Gmail : Permet aux collaborateurs d'accéder rapidement à leur boîte mail.
- GLPI : Permet d'accéder rapidement au service de ticketing de GLPI.

[Help Desk](#) | [My account](#) | [Checklist](#) | [Cart](#) | [Sign in](#) | [Blog](#) | [About](#) | [FAQ & Examples](#)

Home

L	M	M	J	V	S	D
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

[« Mar](#)

mai 2020

[Gmail](#)[GLPI](#)

Gestionnaire de tickets (GLPI)

Le GLPI ou Helpdesk permet de centraliser l'ensemble du matériel informatique de l'entreprise de manière numérique. Il intègre notamment un service de « ticketing » qui permet de faciliter l'assistance informatique aux utilisateurs.

- GLPI tourne sur une VM Linux Debian 9
- Nous avons installé la version 9.3.3

GLPI à besoin d'un serveur Web pour être exploité. Nous avons décidé d'installer la pile LAMP :

- Linux → OS
- Apache → serveur Web -> version 2.4.25
- MariaDB → base de données -> version 10.1.44
- PHP → langage utilisé par GLPI -> version 7.0.33

Installation Apache

```
apt install apache2
```

Installation PHP

```
apt install php7.0 php7.0-curl php7.0-json php7.0-gmp php7.0-mbstring
php7.0-gd php7.0-mcrypt libapache2-mod-php7.0 php7.0-mysql php7.0-intl
php7.0-sqlite3 php7.0-xml php7.0-zip
```

Installation MariaDB & Configuration

```
apt install mariadb-server-10.1
```

Création de la database « GLPI ».

```
CREATE DATABASE glpi ;
```

Database
glpi
information_schema
mysql
performance_schema

Création de l'utilisateur « GLPI » et attribution des droits d'écriture/lecture

```
GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' WITH GRANT OPTION;
```

```
+---+
| user |
+---+
| glpi |
| root |
+---
```

On applique les modifications avec la commande `FLUSH PRIVILEGES;`

Configuration & Installation de GLPI

- Récupération de l'archive depuis GitHub.

```
wget https://github.com/glpi-project/glpi/releases/download/9.3.3/glpi-9.3.3.tgz
```

- Extraction de celle-ci

```
tar zxvf glpi-9.3.3.tgz
```

Afin que notre serveur Web puisse prendre en charge GLPI, nous devons déplacer son dossier dans `/var/www`, le répertoire prévu par Apache pour accueillir les services Web.

```
cp -r glpi /var/www/
```

Attribution des droits à « `www-data` », l'utilisateur qu'Apache utilise pour la gestion de ses services sur le dossier « GLPI »

```
chown -R www-data
```

Modification du fichier de conf Apache : Nous voulons que ce dernier voie notre site qui est situé dans `/var/www`. Par défaut Apache ne voit que les sites situés dans `/var/www/html`.

```
nano /etc/apache2/sites-available/000-default.conf
```

La ligne `DocumentRoot /var/www/html` devient `DocumentRoot /var/www/`

Installation d'extensions complémentaires

Nous installons certaines extensions optionnelles au bon fonctionnement de GLPI, notamment l'extension « LDAP », qui permettra l'interrogation des services d'annuaire (ici le LDAP d'Active Directory)

```
apt-get install php7.0-ldap php7.0-xmlrpc php7.0-imap php-apcu php-cas
```

Autorisation de la réécriture

```
a2enmod rewrite
```

```
nano /etc/apache2/sites-available/000-default.conf
```

```
<Directory /var/www/glpi>
    Options Indexes FollowSymLinks
    AllowOverride All
    Require all granted
</Directory>
```

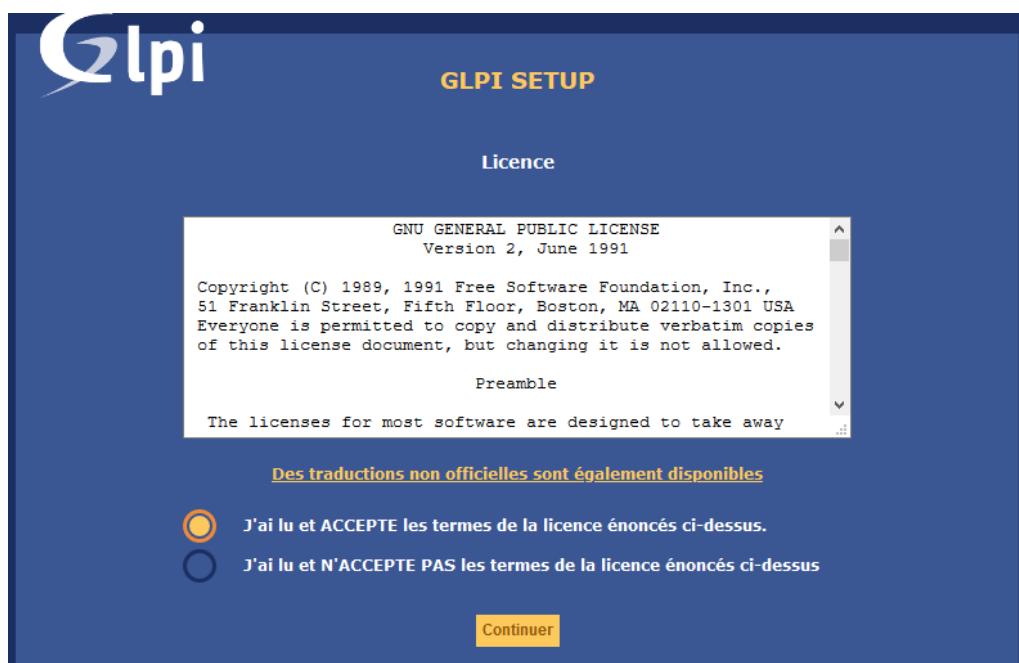
- Nous redémarrons Apache afin d'appliquer les changements

```
systemctl restart apache2
```

Nous pouvons désormais accéder à l'interface Web de la configuration de GLPI via un navigateur



Acceptation des termes de la licence



Nous voulons installer GLPI. Nous cliquons donc sur « Installer »



L'ensemble des tests de notre environnement est positif. Nous pouvons continuer.

The screenshot shows the "Étape 0" (Step 0) screen of the GLPI Setup process. The title "GLPI SETUP" is at the top, followed by "Étape 0". Below this, the heading "Vérification de la compatibilité de votre environnement avec l'exécution de GLPI" is shown. A table titled "Tests effectués" (Tests performed) lists various compatibility checks, all of which have passed, indicated by green checkmarks in the "Résultats" (Results) column. At the bottom of the table is the message "L'accès web au répertoire des fichiers est protégé" (Web access to the files directory is protected). A "Continuer" (Continue) button is located at the bottom right of the page.

Tests effectués	Résultats
Test du Parseur PHP	✓
Test des sessions	✓
Test de l'utilisation de Session_use_trans_sid	✓
Test de l'extension mysqli	✓
Test de l'extension ctype	✓
Test de l'extension fileinfo	✓
Test de l'extension json	✓
Test de l'extension mbstring	✓
Test de l'extension zlib	✓
Test de l'extension curl	✓
Test de l'extension gd	✓
Test de l'extension simplexml	✓
Test de l'extension xml	✓
Test de l'extension ldap	✓
Test de l'extension imap	✓
Test de l'extension Zend OPcache	✓
Test de l'extension APCu	✓
Test de l'extension xmlrpc	✓
Test de l'extension CAS	✓
Test de la mémoire allouée	✓
Test d'écriture des fichiers de journal	✓
Test d'écriture du fichier de configuration	✓
Test d'écriture de fichiers documents	✓
Vérification des droits d'écriture du fichier de sauvegarde	✓
Test d'écriture des fichiers de sessions	✓
Test d'écriture des fichiers des actions automatiques	✓
Vérification des droits d'écriture des fichiers graphiques	✓
Test d'écriture des fichiers de verrouillage	✓
Test d'écriture des documents des plugins	✓
Test d'écriture des fichiers temporaires	✓
Test d'écriture des fichiers de cache	✓
Test d'écriture de fichiers RSS	✓
Test d'écriture des fichiers téléchargés	✓
Test d'écriture de fichiers photos	✓
L'accès web au répertoire des fichiers est protégé	✓

Nous spécifions :

- Où se trouve la base de données GLPI
- L'utilisateur associé à cette même base



Sélection de la BDD « GLPI »



Initialisation de la BDD OK



Nous sommes renseignés des login précrées par GLPi ainsi que de leur utilité



Nous pouvons désormais nous connecter.



Après avoir ajouté le serveur GLPI au domaine (uf_infra_B.local), nous avons récupéré les utilisateurs de l'annuaire LDAP.

c.dariot	Dariot
e.malenc	Malenc
f.hernandez	Hernandez
g.maltruno	Maltruno
glpi	
j.lelouche	Lelouche
j.pontier	Pontier
l.lesaux	Le Saux
l.sachot	Sachot
m.darienzo	Darienzo
m.henry	Henry
m.lacharge	Lacharge
normal	
o.mourneau	Mourneau

Pour cela, grâce au compte administrateur du GLPI, nous sommes allés dans :

Configuration → authentification puis dans « annuaire LDAP ».

Ici, nous avons ajoutés l'adresse IP du DC1 puis nous avons référencé l'endroits où se situe tous les comptes utilisateurs de l'AD (OU=Utilisateurs,DC=uf_infra_B,DC=local).

Nous avons également créé un compte administrateur pour GLPI sur l'AD (adminGLPI).

Changements

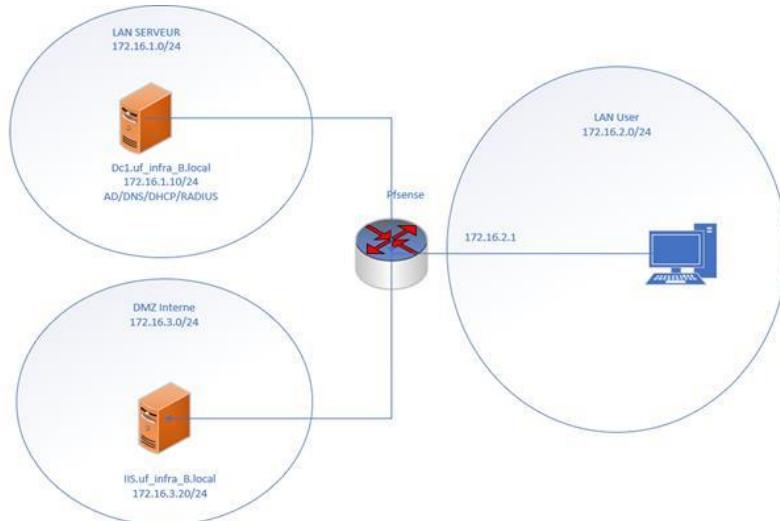
Annuaire LDAP

Nom	DC1	Dernière modification	2020-05-22 13:31
Serveur par défaut	Oui	Actif	Oui
Serveur	172.16.1.10	Port (par défaut 389)	389
Filtre de connexion	(&(objectClass=user)(objectCategory=person)!(userAccountControl:1.2.840.113556.1.4.803:=2))		
BaseDN	OU=Utilisateurs,DC=uf_infra_B,DC=local		
DN du compte (pour les connexions non anonymes)	CN=adminGLPI,CN=Users,DC=uf_infra_B,DC=local		
Mot de passe du compte (pour les connexions non anonymes)	<input type="password"/>	Effacer	
Champ de l'identifiant	samaccountname	Commentaires	
Champ de synchronisation	objectguid		
Créé le 2020-05-09 10:20	Dernière mise à jour le 2020-05-22 13:31		

Après avoir tester si les comptes était bien remonté, nous avons créé une simulation de ticket envoyé par le directeur à l'équipe serveur pour « un oubli de mot de passe ».

Dernière modification	2020-05-09 10:39 par le saux louis				
Temps de prise en charge	<input type="text"/>	<input type="button" value=""/>	Temps de résolution	<input type="text"/>	<input type="button" value=""/>
Temps interne de prise en compte	<input type="text"/>	<input type="button" value=""/>	Temps interne de résolution	<input type="text"/>	<input type="button" value=""/>
Type	Incident	<input type="button" value=""/>	Catégorie	-----	<input type="button" value=""/> i
Statut	En cours (Attribué)	<input type="button" value=""/>	Source de la demande	Helpdesk	<input type="button" value=""/> i
Urgence	Moyenne	<input type="button" value=""/>	Validation	Non soumis à validation	<input type="button" value=""/>
Impact	Moyen	<input type="button" value=""/>	Lieu	-----	<input type="button" value=""/> i
Priorité	Moyenne	<input type="button" value=""/>			
Acteur	Demandeur +	Observateur +	Attribué à +		
	Henry Marc i	Darienzo Marie i le saux louis i Lacharge Maxime i	grp_Administrateur - i		
Titre	Problème connexion compte microsoft				
Description * i	Bonjour, Je ne me souviens plus de mon mot de passe. Pouvez-vous me le réinitialiser s'il vous plaît? Cordialement. Marc Henry				
Tickets liés +	<input type="text"/>				

Portail captif



Afin de permettre un accès à certaines applications depuis l'extérieur du réseau de l'entreprise depuis n'importe quel appareil, connecté au domaine ou non, il est possible de mettre en place un portail captif hébergé sur le routeur Pfsense

Cette partie n'a pas été réalisée par manque de temps et de moyens. Sa mise en place sera tout de même expliquée. Les captures d'écrans qui vont suivre proviennent d'Internet

➤ Installation du service de stratégies et d'accès réseau

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Services de stratégie et d'...

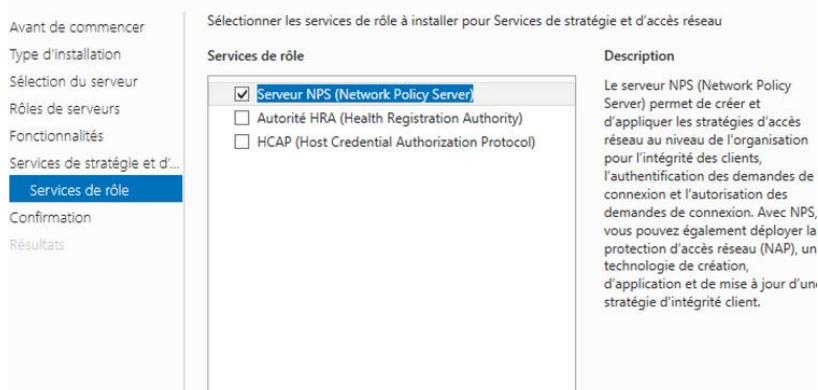
Confirmation

Résultats

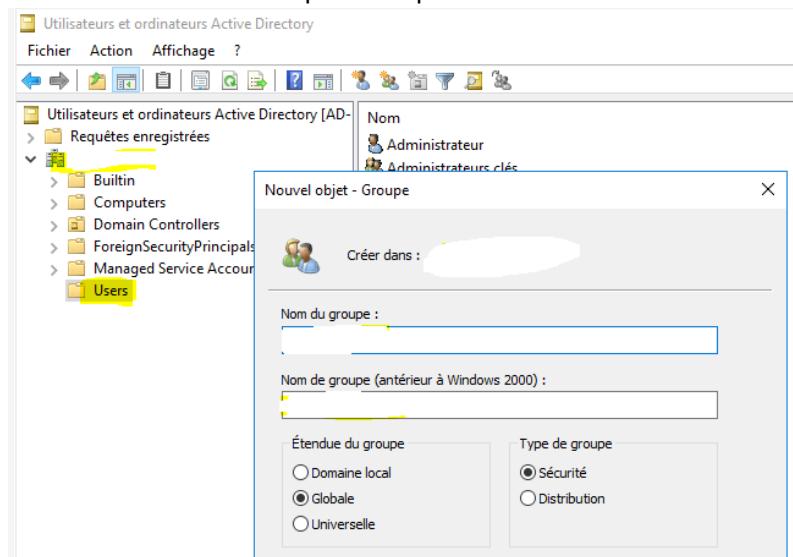
Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles	Description
<input type="checkbox"/> Hyper-V	Les services de stratégie et d'accès réseau fournissent un serveur NPS (Network Policy Server) qui contribue à garantir la sécurité de votre réseau.
<input type="checkbox"/> MultiPoint Services	
<input type="checkbox"/> Serveur de télécopie	
<input type="checkbox"/> Serveur DHCP	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
<input type="checkbox"/> Serveur Web (IIS)	
<input type="checkbox"/> Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
<input type="checkbox"/> Services AD LDS (Active Directory Lightweight Direct)	
<input type="checkbox"/> Services AD RMS (Active Directory Rights Manage)	
<input type="checkbox"/> Services Bureau à distance	
<input type="checkbox"/> Services d'activation en volume	
<input type="checkbox"/> Services d'impression et de numérisation de docu	
<input type="checkbox"/> Services de certificats Active Directory	
<input type="checkbox"/> Services de déploiement Windows	
<input type="checkbox"/> Services de fédération Active Directory (AD FS)	
<input checked="" type="checkbox"/> Services de fichiers et de stockage (2 sur 12 installé)	
<input checked="" type="checkbox"/> Services de stratégie et d'accès réseau	
<input type="checkbox"/> Services WSUS (Windows Server Update Services)	

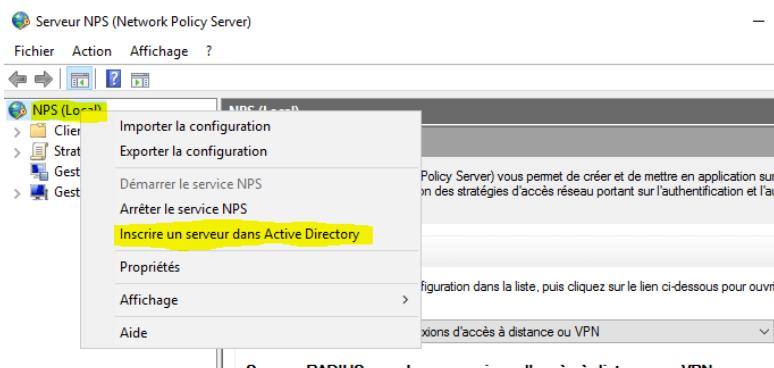
➤ Installation du rôle NPS

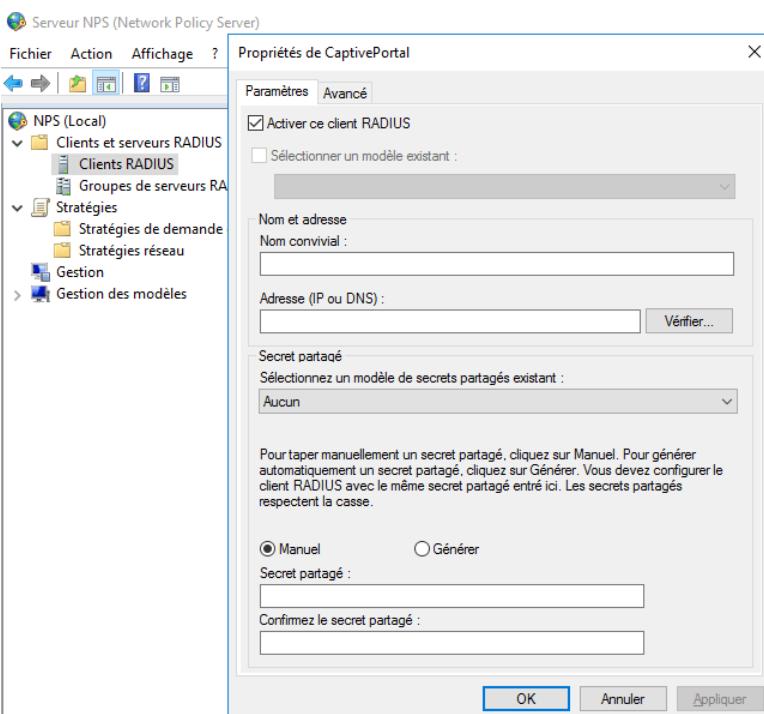


➤ Créeation d'un groupe de sécurité « portail captif » rassemblant tous les utilisateurs ayant le droit de se connecter au portail captif

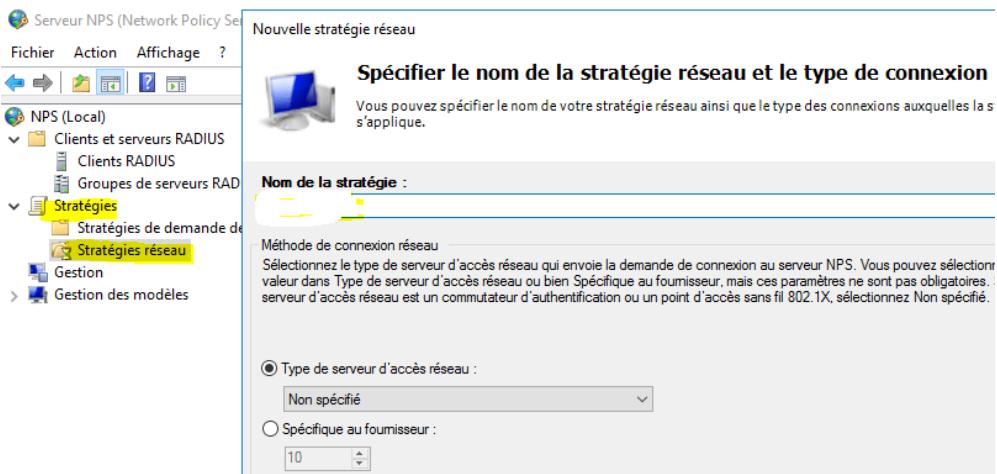


➤ Créeation d'un nouveau client RADIUS : le renseignement d'un secret partagé permet de chiffrer les transactions entre les clients et le serveur RADIUS. Il est donc à retenir

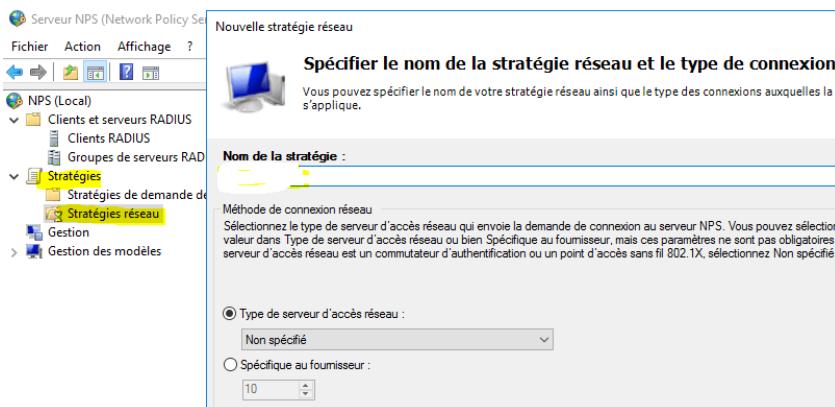




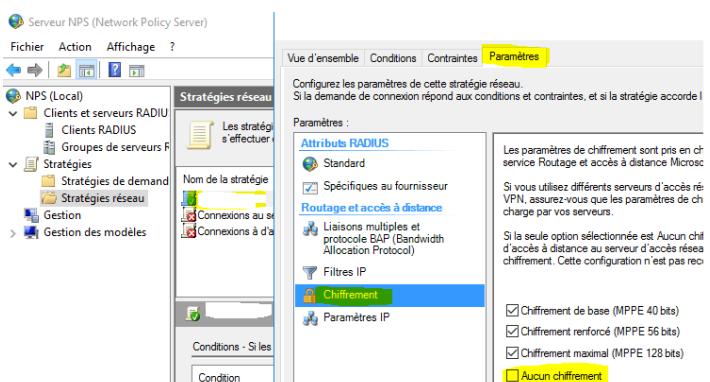
Configuration d'une stratégie réseau. Elle gérera les droits d'accès et permettra d'autoriser l'accès au portail le groupe de sécurité « portail captif » crée précédemment.



Nous ajoutons le groupe « portail captif » créé précédemment afin d'autoriser les membres à communiquer avec RADIUS

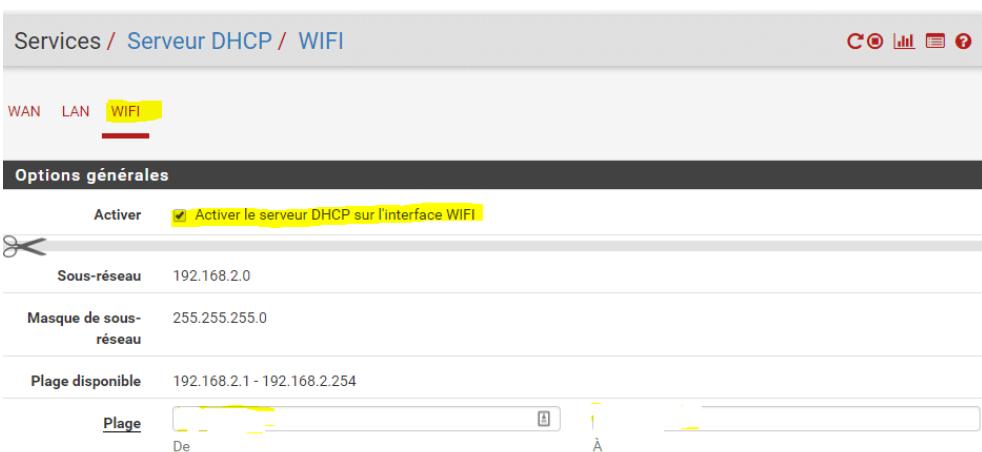


Afin de garantir un niveau de sécurité élevé, nous décochons la case « Aucun chiffrement »



Configuration Pfsense

- Activer le serveur DHCP sur l'interface WIFI



➤ Activation de la résolution DNS

Nous renseignons un nom descriptif, le type et le protocole d'authentification , le secret partagé, les ports d'écoute et l'IP sur serveur RADIUS.

Paramètres du serveur

Nom descriptif: [Yellowed]

Type: RADIUS

Paramètres du serveur Radius

Protocole: MS-CHAPv2

Nom d'hôte ou adresse IP: [Yellowed]

Secret partagé: [Yellowed]

Services offerts: Authentification et comptabilité

Port d'authentification: 1812

Port de comptabilité: 1813

Délai d'expiration de l'authentification: [Yellowed]
Cette valeur contrôle la durée, en secondes, que le serveur RADIUS peut prendre pour répondre à une demande d'authentification. Si elle est laissée vide, la valeur par défaut est de 5 secondes. REMARQUE: si vous utilisez un système d'authentification interactif à deux facteurs, augmentez ce délai pour tenir compte de la durée qu'il faudra à l'utilisateur pour recevoir et entrer un jeton.

Attribut IP RADIUS NAS: [Yellowed]
Enter the IP to use for the "NAS-IP-Address" attribute during RADIUS Access-Requests.
Please note that this choice won't change the interface used for contacting the RADIUS server.

Configuration du portail captif

- **Activer le Portail Captif**
 - Interfaces : **WIFI**
 - **Activer la fenêtre de dialogue de fermeture de session**
 - Après authentification Redirection URL : <https://google.fr>
- Allez dans la partie **Authentification**
 - Méthode d'authentification : **Use an Authentication backend**
 - Serveur d'authentification : **CaptivePortal**
 - **Réauthentifier les utilisateurs connectés chaque minute**
- Allez dans la partie Comptabilité
 - **Send RADIUS accounting packets.**

Routeur/Firewall (Pfsense) :

Pour notre infrastructure, nous avons mis en place 2 réseau LAN différents. Le « LAN serveurs » (172.16.1.0/24) dédié à tous les serveurs installés précédemment et le « LAN user » dédié au poste de travail des utilisateurs de notre infrastructure. Il y a également une interface « WAN » dédié à la sortie vers Internet.

```
WAN (wan)      -> em0          -> v4: 192.168.1.200/24
LANSERVEURS (lan) -> em1        -> v4: 172.16.1.1/24
LANUSERS (opt1) -> em2         -> v4: 172.16.2.1/24
```

Règles pare-feu :

Tout d'abord, pour le LAN Users, nous avons ajouté une règle qui bloque tout le trafic. Cette règle sera positionnée en dernière position permettant de bloquer tous ce que nous n'avons pas ouvert.



Nous avons ensuite ouvert les ports 53, 389, 445, 139, 1025, 1026, 3268, 88, 137 et 138. L'ouverture de ces ports est obligatoire pour que les postes de travail des utilisateurs puissent communiquer dans le domaine.

Nous avons également ouvert les ports 80 et 443 pour que les utilisateurs puissent accéder à Internet.

Les ports 67 (serveur DHCP) et 68 (client DHCP) ont également été ouvert pour que les clients puissent récupérer leur adresse IP auprès du serveur DHCP (DC1.uf_infra_B.local).

Nous avons également ouvert le protocole ICMP pour pouvoir effectuer des tests.

PROJET UF

	États	Protocole	Source	Port	Destination	Port	Passerelle	d'attente	Ordonnancement	Description	Actions
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	67 - 68	*	aucun	DHCP		
<input type="checkbox"/>	✓ 0 / 57.62 MiB	IPv4 TCP/UDP	LANUSERS net	*	*	443 (HTTPS)	*	aucun			
<input type="checkbox"/>	✓ 0 / 105.11 MiB	IPv4 TCP/UDP	LANUSERS net	*	*	80 (HTTP)	*	aucun			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	LANUSERS net	*	LANSERVEURS net	138 (NetBIOS-DGM)	*	aucun			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 UDP	LANUSERS net	*	LANSERVEURS net	137 (NetBIOS-NS)	*	aucun			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	88	*	aucun	kerberos		
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	3268	*	aucun	LDAP Global Catalogue		
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	1025 - 1026	*	aucun	RPC		
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	139 (NetBIOS-SSN)	*	aucun			
<input type="checkbox"/>	✓ 0 / 20 KiB	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	445 (MS DS)	*	aucun			
<input type="checkbox"/>	✓ 0 / 0 B	IPv4 TCP	LANUSERS net	*	LANSERVEURS net	389 (LDAP)	*	aucun			
<input type="checkbox"/>	✓ 0 / 1 KiB	IPv4 TCP/UDP	LANUSERS net	*	LANSERVEURS net	53 (DNS)	*	aucun			
<input type="checkbox"/>	✓ 0 / 0 B	IPv6 ICMP any	LANUSERS net	*	*	*	*	aucun			
<input type="checkbox"/>	✓ 0 / 5 KiB	IPv4 ICMP any	LANUSERS net	*	*	*	*	aucun	autoriser lan user vers tout le monde		
<input type="checkbox"/>	✗ 0 / 0 B	IPv4 *	*	*	*	*	*	aucun	bloquer tout		

Relai DHCP :

Nous avons également configuré le relai DHCP sur le PFsense pour que le LAN User puisse récupérer des adresses IP auprès du serveur DHCP.

Configuration de relais DHCP

Activer Activer le relais DHCP sur l'interface

Interface(s)

WAN
LANSERVEURS
LANUSERS

Les interfaces sans adresse IP ne seront pas affichées.

Ajouter l'ID du circuit et l'ID de l'agent aux requêtes
Si cette option est activé, le relais DHCP ajoutera le circuit ID (pfSense numéro de l'interface) et l'ID de l'agent à la requête DHCP.

Serveur de destination

<input type="text" value="172.16.1.10"/>	Supprimer
Il s'agit de l'adresse IPv4 du serveur auquel les requêtes DHCP sont relayées.	

<input type="text" value="172.16.1.11"/>	Supprimer
Il s'agit de l'adresse IPv4 du serveur auquel les requêtes DHCP sont relayées.	

Mise en place des Blacklists :

Nous avons décidé, comme tout bon administrateur, de bloquer certains site web pour que les utilisateurs se concentrent uniquement sur leur travail.

Nous avons donc récupéré une liste existante faite par l'université de Toulouse 1 Capitole :

http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz.

Nous avons donc commencé par télécharger les paquets « Squid ».

Paquets installés					Actions
Nom	Catégorie	Version	Description	Dépendances du paquet:	
✓ Lightsquid	www	3.0.6_6	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package.	↳ lighttpd-1.4.54 ↳ lightsquid-1.8_5	
✓ squid	www	0.4.44_25	High performance web proxy cache (3.5 branch). It combines Squid as a proxy server with its capabilities of acting as a HTTP / HTTPS reverse proxy. It includes an Exchange-Web-Access (OWA) Assistant, SSL filtering and antivirus integration via C-ICAP.	↳ squidclamav-7.1 ↳ squid_radius_auth-1.10 ↳ squid-4.10 ↳ c-icap-modules-0.5.4	
✓ squidGuard	www	1.16.18_5	High performance web proxy URL filter.	↳ squidguard-1.4_15	

Ensuite, nous allons activer les blacklists sur le Pfsense et ajouter l'URL de téléchargement.

Blacklist options

Blacklist Check this option to enable blacklist

Do NOT enable this on NanoBSD installs!

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.

Format: host:[port login:pass] . Default proxy port 1080.

Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or

Ensuite, nous avons téléchargé la blacklist de Toulouse dans « SquidGuard Proxy Filter ».

The screenshot shows a web-based configuration interface for SquidGuard. At the top, there is a progress bar indicating "0 % http://dsi.ut-capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz". Below the progress bar are three buttons: "Download" (green), "Cancel" (orange), and "Restore Default" (blue). A text input field below the buttons says "Enter FTP or HTTP path to the blacklist archive here." Underneath, a section titled "Blacklist update Log" contains the following log output:

```

Begin blacklist update
Start download.
Download archive http://dsi.ut-
capitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz
Download complete
Unpack archive
Scan blacklist categories.
Found 62 items.
Start rebuild DB.
Copy DB to workdir.
Reconfigure Squid proxy.
Blacklist update complete.

```

Après cela, dans le service « Squid Proxy Server », nous avons activer le serveur proxy en précisant qu'il sera actif sur l'interface du LAN user sur le port 3128.

The screenshot shows the configuration interface for the Squid Proxy Server. It includes several settings sections:

- Enable Squid Proxy**: A checked checkbox with the instruction "Check to enable the Squid proxy." and a note: "Important: If unchecked, ALL Squid services will be disabled and stopped."
- Keep Settings/Data**: A checked checkbox with the instruction "If enabled, the settings, logs, cache, AV defs and other data will be preserved across pack" and a note: "Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upg"
- Listen IP Version**: Set to "IPv4". A note below says "Select the IP version Squid will use to select addresses for accepting client connections."
- Proxy Interface(s)**: A dropdown menu showing "LANSERVEURS", "LANUSERS" (highlighted in yellow), "WAN", and "boucle locale". A note says "The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces."
- Port du mandataire (« proxy »)**: Set to "3128". A note below says "This is the port the proxy server will listen on. Default: 3128"

Pour finir, nous sommes retournés dans l'onglet « SquidGuard Proxy Filter » et nous avons activer squidGuard.

Options générales

Activer Check this option to enable squidGuard.
Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
 The Save button at the bottom of this page must be clicked to save configuration changes.
 To activate squidGuard configuration changes, **the Apply button must be clicked**.

✓ ApplySquidGuard service state: **STARTED**

Ensute, sur la machine cliente, nous avons ajoutés un proxy (en ajoutant l'adresse de l'interface et le port utilisé).

Proxy

Utiliser un serveur proxy

 Activé

Adresse

172.16.2.1

Port

3128

Utilisez le serveur proxy sauf pour les adresses qui commencent par les entrées suivantes. Utilisez des points-virgules (;) pour séparer les entrées.

Ne pas utiliser le serveur proxy pour les adresses (intra) locales

Nous avons choisi un site de la blacklist et nous voyons bien que celle-ci est fonctionnelle.



Reason:

Client address: 172.16.2.10

Client name: 172.16.2.10

Client group: default

Target group: none

URL: http://elle.fr/love-sexe

OpenVPN :

Il est possible avec PfSense de mettre en place directement le VPN sur le routeur, ce qui nous évite d'avoir un serveur dédié à cette tâche.

Pour cela, nous allons commencer par créer notre autorité de certification.

The screenshot shows a search interface with a term 'pfsense firewall'. Below it, a table lists a single certificate entry:

Nom	Interne	Émetteur	Certificats	Nom distinctif	En cours d'utilisation	Actions
pfsense firewall	✓	auto-signé	2	ST=PACA, OU=B3, O=Ynov Campus, L=Marseille, CN=internal-ca, C=FR Valable depuis: Sun, 24 May 2020 16:06:32 +0200 Valide jusqu'au: Wed, 22 May 2030 16:06:32 +0200		

Ensuite, nous avons créé un certificat pour le serveur.

This screenshot shows a detailed view of a certificate for 'Client VPN User'. The certificate is issued by 'pfsense firewall' and has the following details:

- Subject: ST=PACA, OU=B3, O=Ynov Campus, L=Marseille, CN=pfsense.uf_infra_B.local, C=FR
- Valid since: Sun, 24 May 2020 16:10:49 +0200
- Valid until: Wed, 22 May 2030 16:10:49 +0200

Nous avons également créé un utilisateur sur le Pfsense. A la fin, celui-ci pourra se connecter au réseau local via le VPN.

A user profile for 'l.sachot' is shown, with 'Client VPN' selected in the dropdown menu.

Ensute, nous allons ajouter un certificat client VPN à cet utilisateur.

This screenshot shows a certificate for 'l.sachot' issued by 'pfsense firewall'. The details are identical to the previous certificate entry:

- Subject: ST=PACA, OU=B3, O=Ynov Campus, L=Marseille, CN=pfsense.uf_infra_B.local, C=FR
- Valid since: Sun, 24 May 2020 16:12:38 +0200
- Valid until: Wed, 22 May 2030 16:12:38 +0200

Après avoir créé les certificats, nous avons ajoutés les paquets OpenVPN-Client-Export sur le Pfsense.

The screenshot shows a package management interface where 'openvpn-client-export' is selected. The package details are as follows:

- Name: openvpn-client-export
- Version: 1.4.23
- Description: Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.
- Dependencies: openvpn-client-export-2.4.9, openvpn-2.4.9, zip-3.0_1, p7zip-16.02_2

(Nous n'avons pas eu le temps de terminer cette installation.) Nous avons donc uniquement créé les certificats pour nous connecter au VPN, mais nous n'avons pas mis en place le serveur VPN.

Sauvegarde des VM :

Il est très important dans une entreprise de sauvegarder les serveurs dans un réseau distant. Dans ce cas, si l'entreprise subit une attaque de grande ampleur, il est facile de remettre en place l'infrastructure en faisant remonter les sauvegardes. Pour cela, il est donc primordial que ces sauvegardes soit dans un réseau distant.

Dans notre cas, nous avons décidé de les intégré dans un dossier du one drive Ynov campus. Ce dossier est partagé entre les membres de l'équipe.

Fichiers > Sauvegarde serveurs

Nom	Modifié	Modifié par	Taille du fichier	Partage
Centreon	Il y a 2 heures	LE SAUX Louis	4 éléments	Partagé
DC1	Il y a quelques secondes	LE SAUX Louis	1 élément	Partagé
DC2	Il y a environ une heure	LE SAUX Louis	0 éléments	Partagé
GLPI.uf_infra_B.local	Il y a environ une heure	LE SAUX Louis	0 éléments	Partagé
Graylog	Il y a environ une heure	LE SAUX Louis	4 éléments	Partagé
IIS.uf_infra_B.local	Il y a environ une heure	LE SAUX Louis	4 éléments	Partagé
PC admin	Il y a environ une heure	LE SAUX Louis	3 éléments	Partagé
PC user	Il y a environ une heure	LE SAUX Louis	0 éléments	Partagé
Pfsense	Il y a environ une heure	LE SAUX Louis	0 éléments	Partagé
Serveur de fichier	Il y a environ une heure	LE SAUX Louis	3 éléments	Partagé