

REALISATION PROFESSIONNELLE

Projet n° 1

GREPILLOUX Antonin
BTS SIO



Table des matières

I – Présentation :.....	3
b. Schéma de l'infrastructure réseau :.....	4
II – Mise en œuvre de la solution :.....	5
a. Installation Active Directory	5
b. Installation DHCP	6
c. Installation DFS	7
d. Installation GPO	8
e. Installation DNS	10
f. Installation supplémentaire (Wireshark)	11

I – Présentation :

a. Contexte :

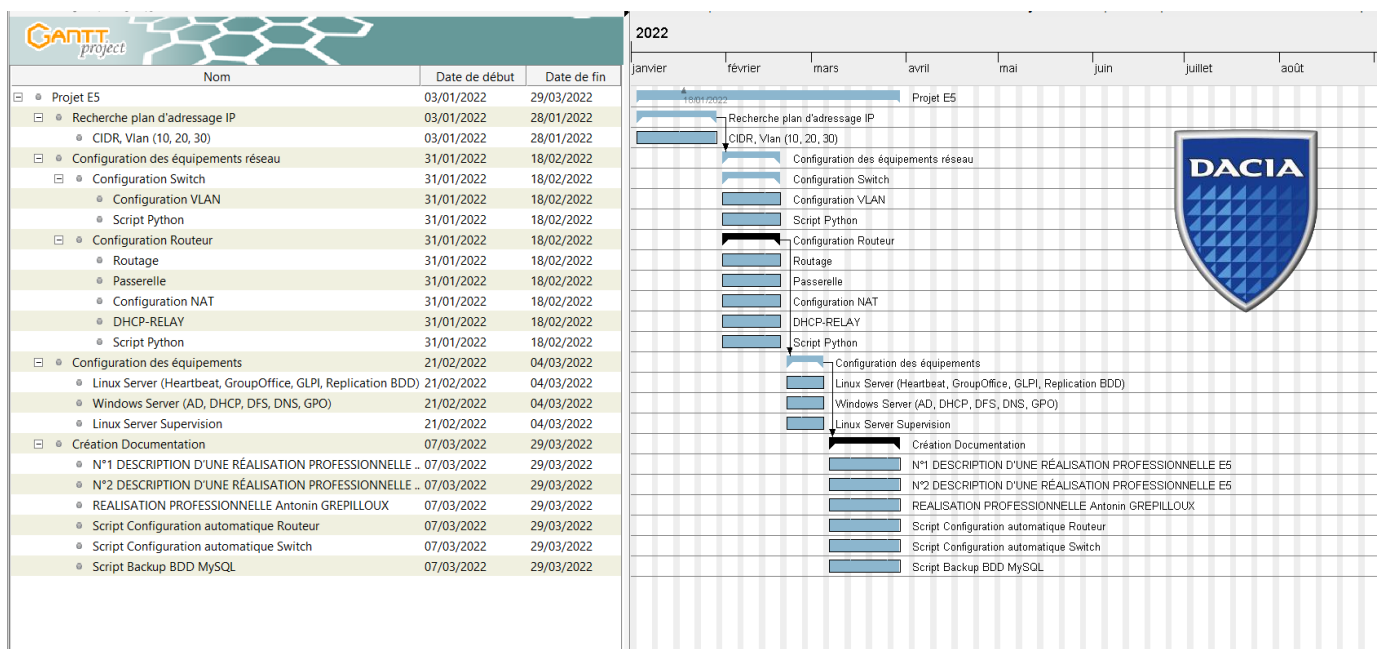
L'entreprise nommée « Logan » créée en 2012 est basée en France. C'est une entreprise de 5 salariés qui est spécialisée dans la communication et le marketing.

Seuls 2 salariés s'occupent du pôle marketing, qui sont ensuite vendus par un commercial. La société est également constituée de deux membres au service informatique. Tout le personnel dispose d'un poste sous Windows 10.

L'entreprise souhaiterait s'améliorer et ouvrir d'autres applications internes à l'entreprise. Le directeur a analysé leur système informatique pour évaluer le tarif de ses équipements informatiques et a remarqué qu'aucun poste ne disposait d'adresse DHCP, ni de session utilisateurs.

De plus, certains employés se plaignaient de problèmes récurrents concernant l'ajout d'ordinateurs personnels dans l'entreprise ou le transfert de documents entre employés, ces derniers commençaient à devenir problématiques.

En tant que membre du service informatique et jeune diplômé, j'ai eu pour mission de mettre en place une configuration réseau et deux serveurs Windows avec un Active Directory, DHCP, DFS, GPO, DNS, Wireshark apportant les compétences acquises lors de mon BTS SIO.

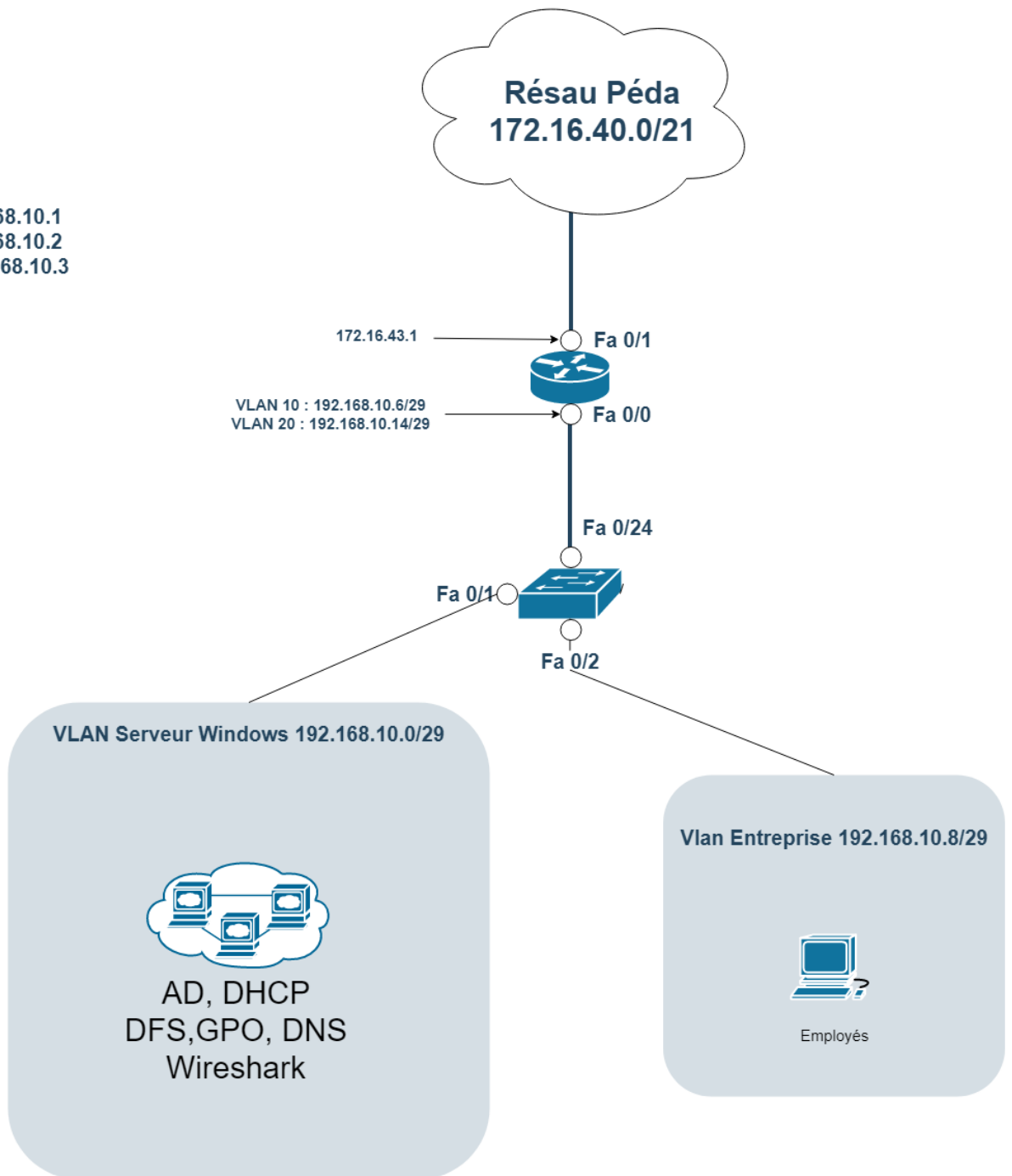


b. Schéma de l'infrastructure réseau :

IP FIXES

VLAN 10 :
Win-Srv1 192.168.10.1
Win-Srv2 192.168.10.2
IP Cluster 192.168.10.3

VLAN 20 :
DHCP



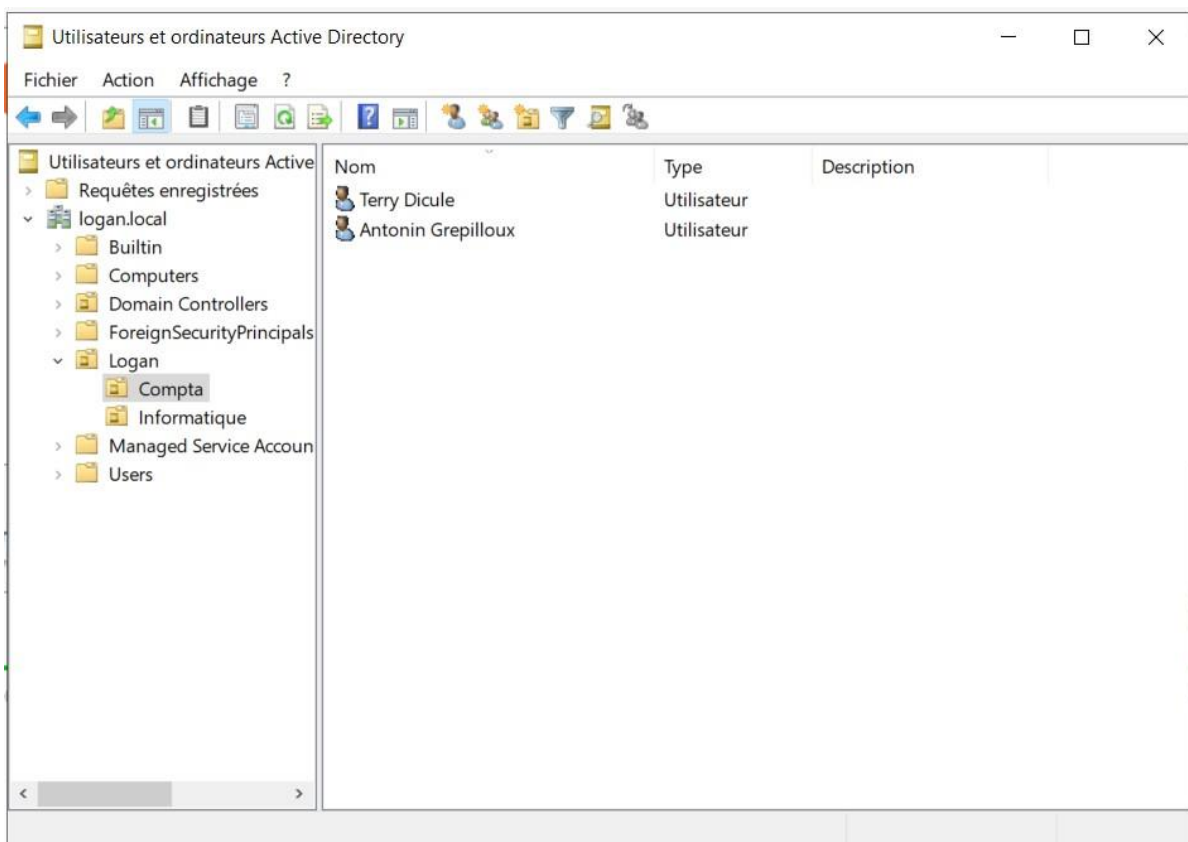
II – Mise en œuvre de la solution :

a. Installation Active Directory

Active Directory est un annuaire permettant de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité, ...). La base de données d'AD est distribuée ce qui lui améliore la tolérance de pannes.

La mise en place de l'Active Directory est importante dans l'ensemble de l'infrastructure. L'Active Directory permet d'ouvrir les sessions aux employés de l'entreprise, accéder à leurs dossiers partagés ou se connecter sur une application telle que GLPI via leurs identifiants LDAP.

La mise en place des utilisateurs dans l'Active Directory se fait en trois groupes. Un groupe Compta pour les employés de la comptabilité. Un groupe Informatique pour le SI de l'entreprise. Et le dernier groupe est un groupe à part pour les stagiaires ou sous-traitant.



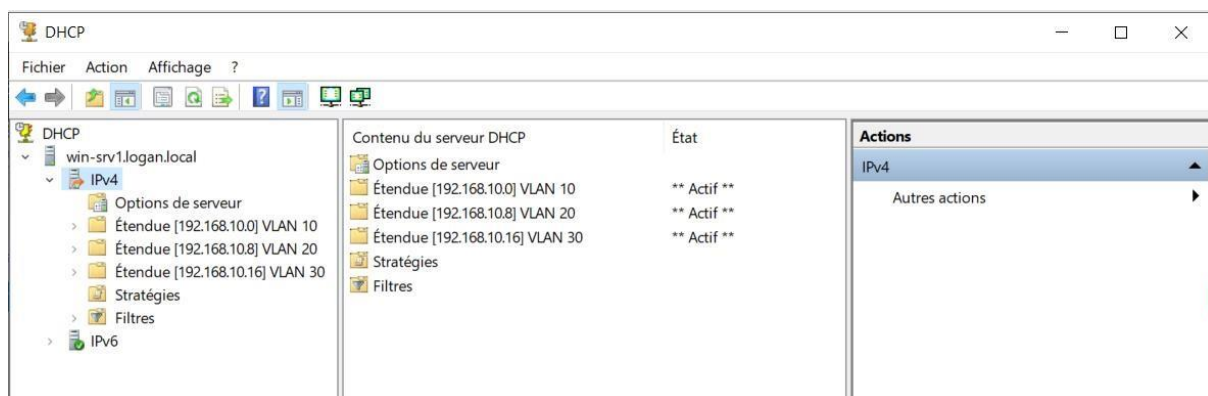
b. Installation DHCP

Fonctionnement du DHCP : Le DHCP (Dynamic Host Configuration protocol) est un protocole réseau permettant d'assurer la configuration automatique des paramètres IP d'un poste. Le serveur DHCP peut attribuer une adresse IP, un masque de sous-réseau, une passerelle, des DNS... Le serveur DHCP attribuera des adresses en fonction des plages d'adresses (étendues) qui ont été créés et configurées. Les postes clients n'auront aucune configuration à faire puisque leur adressage sera automatique.

Fonctionnement de l'Agent-Relais : L'Agent-Relais est une fonctionnalité qui permet de diffuser des plages d'adresses qui ne sont pas sur le même réseau que celui du serveur DHCP. Il permet d'assurer le routage entre les réseaux, pour cela la mise en place de l'agent-relais est nécessaires sur le Routeur Cisco en indiquant dans chaque vlan leurs Agent-Relais. (Voir Annexe Configuration Routeur Cisco).

La distribution automatique d'adresse IP se fait par deux serveurs Windows auquel nous avons mis en place une répartition de charge. L'un s'occupe de 50% et l'autre, les 50% restant.

Il existe trois plages d'adresses IP, nommé chacune VLAN 10 Windows, VLAN 20 Client, VLAN 30 Linux. Chacun distribue des adresses IP automatiquement. Comme le VLAN 20 Client où aucune exclusion n'est mise en place. Par contre le VLAN 10 ET 30 ont des exclusions. Il est logique que nos serveurs et équipement important ont besoin de rester en ip statique.



c. Installation DFS

Le DFS (Distributed File System ou Système de Fichiers Distribués) est un système de fichier hiérarchisé permettant de structurer les fichiers partagés sur différents serveurs de façon logique. A noter que le DFS à un impact sur l'utilisateur. Comme le DFS synchronise les données disponibles sur plusieurs serveurs, l'utilisateur ne verra pas le nom du serveur sur lequel il accède pour lire les données. Mais plutôt le nom de domaine. (\\logan.local\)

Avec le DFS nous avons activés les fonctionnalités suivantes :

- La réplication DFS
- Espaces de noms DFS

La réplication DFS permet de répliquer les données sur le deuxième Serveurs Windows. Cela permet une redondance et une transparence pour l'utilisateur si le serveur primaire tombe en panne.

Puis l'espaces de noms DFS permettent la redondance de l'accès au DFS grâce à la possibilité de définir plusieurs serveurs pour un même espace de noms DFS.

Grâce à cela, l'utilisateur n'aura pas besoin de taper le nom du serveur Windows mais plutôt le nom de domaine. Puis cela permet une redondance et une transparence pour l'utilisateur si le serveur primaire tombe en panne.

The image shows two screenshots of the Windows DFS Management console. The top screenshot displays the 'Backup' folder configuration. The bottom screenshot displays the 'Partage' folder configuration. Both screenshots show a table of replicated folders with columns for status, local path, replication status, member server, replicated folder name, and quota.

État	Chemin d'accès local	Statut de l'appartenance	Membre	Dossier répliqué	Quota intermédiaire
Dossier répliqué : Backup (2 éléments)					
	C:\Backup	Activé	WIN-SRV1	Backup	4,00 Go
	C:\Backup	Activé	WIN-SRV2	Backup	4,00 Go

État	Chemin d'accès local	Statut de l'appartenance	Membre	Dossier répliqué	Quota intermédiaire
Dossier répliqué : Partage (2 éléments)					
	C:\Partage	Activé	WIN-SRV1	Partage	4,00 Go
	C:\Partage	Activé	WIN-SRV2	Partage	4,00 Go

d. Installation GPO

GPO : « Group Policy »

Une GPO est un ensemble de paramètres qui s'appliquent automatiquement à des utilisateurs ou des groupes sur des postes clients ou des serveurs

Les paramètres concernent :

L'interface utilisateur, par exemple : Rediriger le répertoire « Mes Documents » vers un partage réseau.

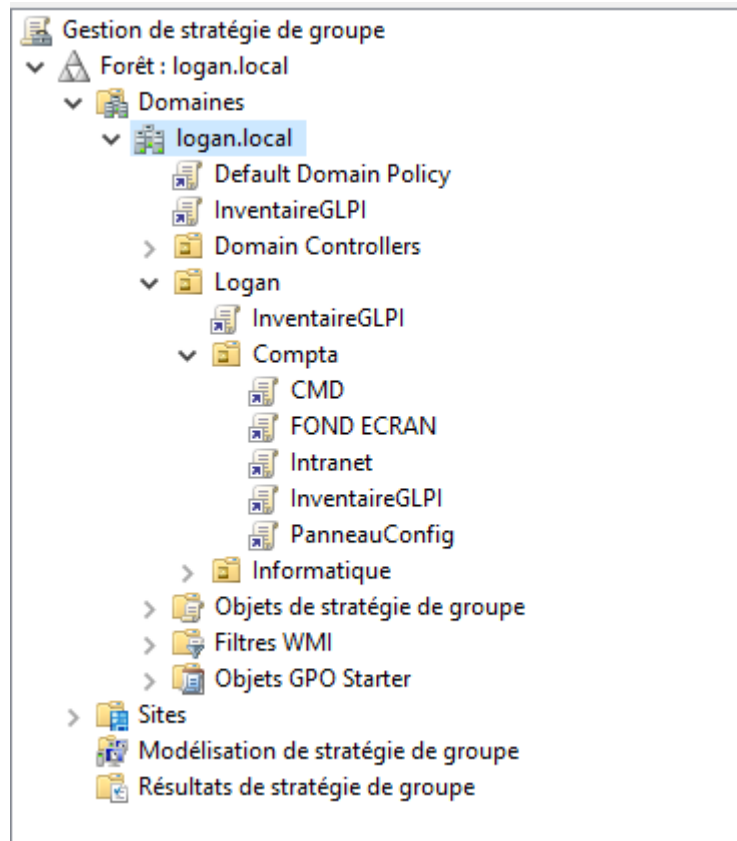
Le paramétrage d'une application, par exemple : Ajouter des sites de confiance à Internet Explorer, configurer les paramètres de proxy de Firefox.

Le déploiement d'une application, par exemple : Installer automatiquement un logiciel sur tous les postes.

Un élément de sécurité, par exemple : Sécuriser le poste client en désactivant l'utilisation de certains logiciels ou des outils de Windows tels que l'invité de commande ou le panneau de configuration.

Les GPO facilitent la gestion d'un domaine contenant de multiples ressources. Elle rend possible un paramétrage automatique des postes clients en évitant un travail répétitif.

Les GPO peuvent s'appliquer soit sur un utilisateur, soit sur un ordinateur. Dans le cadre de ce document, nous avons mis en place des GPO permettant la création d'un raccourci sur le bureau de l'utilisateur qui redirige vers la page web intranet de l'entreprise, le blocage de l'invité de commandes et le panneau de configuration, puis la mise en place d'un fond d'écran pour chaque groupe d'utilisateurs. Un fond d'écran spécifique pour le groupe Compta et un autre fond d'écran différent mais pour le groupe Informatique. Et la mise en place d'un GPO pour l'installation silencieuse de FusionInventory.



e. Installation DNS

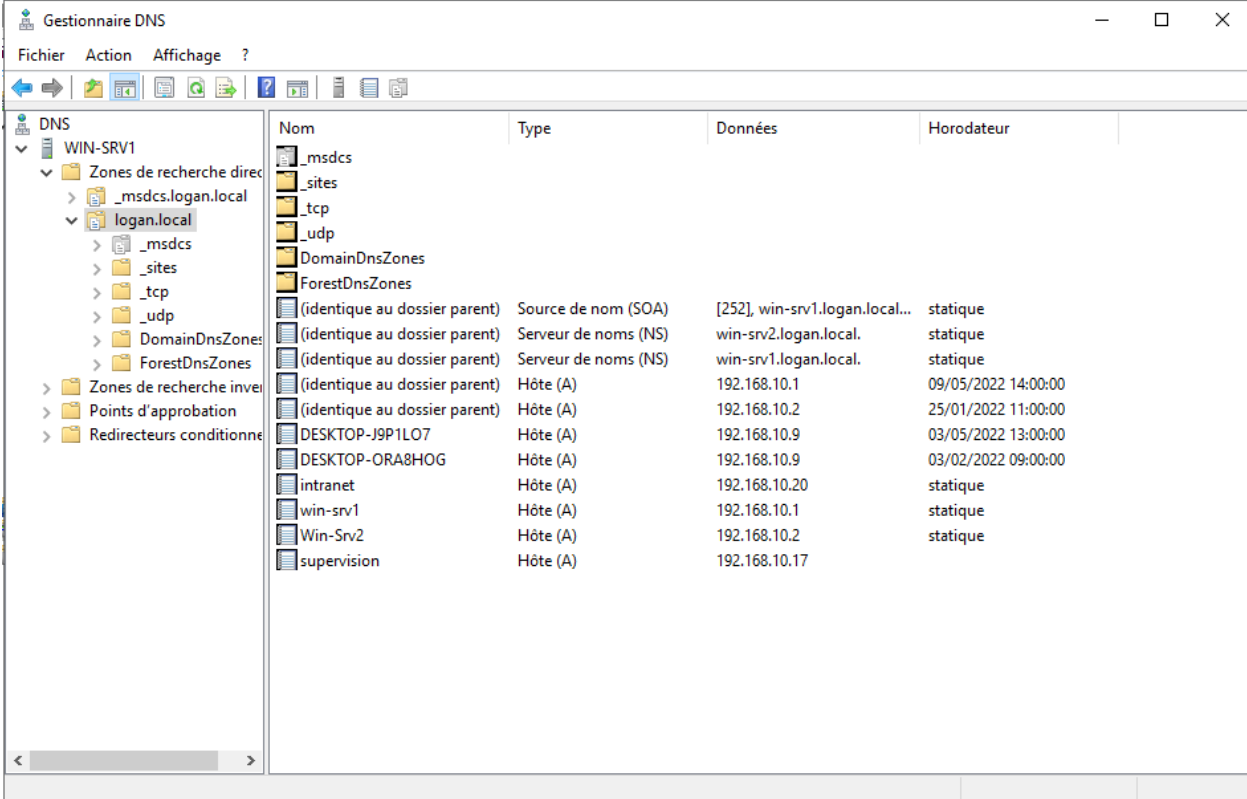
DNS : Domain Name Server

Le rôle du DNS est d'établir une correspondance entre adresses IP, par exemple 192.168.10.1 et noms de domaines, logan.local

Le DNS permet une Résolution comme cité précédemment IP vers nom de domaine, mais aussi permet une résolution inverse, de nom de domaine vers IP.

Le nom de domaine étant logan.local, alors il sera utilisé pour le DFS et la page web intranet.

Pour la page web intranet nous créons une entrée DNS « intranet ». Donc la page web intranet sera accessible via l'URL suivante : intranet.logan.local au lieu de l'IP qui héberge la page intranet.



The screenshot shows the Windows DNS Manager console for the logan.local domain. The left pane shows the tree structure, and the right pane shows a table of DNS records.

Nom	Type	Données	Horodateur
(identique au dossier parent)	Source de nom (SOA)	[252], win-srv1.logan.local...	statique
(identique au dossier parent)	Serveur de noms (NS)	win-srv2.logan.local.	statique
(identique au dossier parent)	Serveur de noms (NS)	win-srv1.logan.local.	statique
(identique au dossier parent)	Hôte (A)	192.168.10.1	09/05/2022 14:00:00
(identique au dossier parent)	Hôte (A)	192.168.10.2	25/01/2022 11:00:00
DESKTOP-J9P1LO7	Hôte (A)	192.168.10.9	03/05/2022 13:00:00
DESKTOP-ORA8HOG	Hôte (A)	192.168.10.9	03/02/2022 09:00:00
intranet	Hôte (A)	192.168.10.20	statique
win-srv1	Hôte (A)	192.168.10.1	statique
Win-Srv2	Hôte (A)	192.168.10.2	statique
supervision	Hôte (A)	192.168.10.17	

f. Installation supplémentaire (Wireshark)

Wireshark permet de filtrer les paquets à capturer en fonction des informations des différentes couches d'encapsulation.

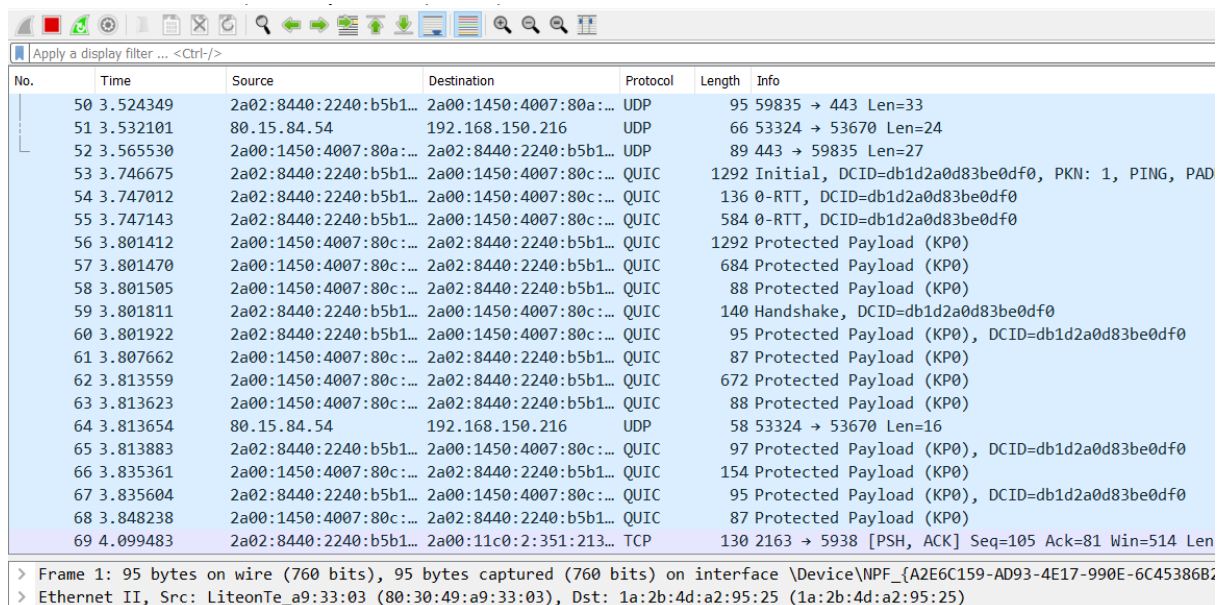
L'installation de Wireshark sur les serveurs Windows peut être utile dans certains cas, mais elle peut parfois être inutile.

Wireshark possède une interface graphique de filtrage permettant d'ajuster les informations affichées. Cette fonctionnalité est utile pour la sécurité.

Les règles de filtrage sont applicables à l'ensemble des couches de communication, mais leur utilisation est plus utile sur les couches Application et Transport.

La règle de filtrage utilisant le protocole TCP est particulièrement utile.

Dans une expérience d'analyse réseau, la connaissance de l'hôte client permet d'identifier une partie des services et applications utilisés par l'utilisateur. Cette information peut-être déjà connue, mais elle peut également permettre d'étendre la liste des services qui sont présents sur un réseau.



No.	Time	Source	Destination	Protocol	Length	Info
50	3.524349	2a02:8440:2240:b5b1...	2a00:1450:4007:80a:...	UDP	95	59835 → 443 Len=33
51	3.532101	80.15.84.54	192.168.150.216	UDP	66	53324 → 53670 Len=24
52	3.565530	2a00:1450:4007:80a:...	2a02:8440:2240:b5b1...	UDP	89	443 → 59835 Len=27
53	3.746675	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	1292	Initial, DCID=db1d2a0d83be0df0, PKN: 1, PING, PAD
54	3.747012	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	136	0-RTT, DCID=db1d2a0d83be0df0
55	3.747143	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	584	0-RTT, DCID=db1d2a0d83be0df0
56	3.801412	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	1292	Protected Payload (KP0)
57	3.801470	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	684	Protected Payload (KP0)
58	3.801505	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	88	Protected Payload (KP0)
59	3.801811	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	140	Handshake, DCID=db1d2a0d83be0df0
60	3.801922	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	95	Protected Payload (KP0), DCID=db1d2a0d83be0df0
61	3.807662	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	87	Protected Payload (KP0)
62	3.813559	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	672	Protected Payload (KP0)
63	3.813623	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	88	Protected Payload (KP0)
64	3.813654	80.15.84.54	192.168.150.216	UDP	58	53324 → 53670 Len=16
65	3.813883	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	97	Protected Payload (KP0), DCID=db1d2a0d83be0df0
66	3.835361	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	154	Protected Payload (KP0)
67	3.835604	2a02:8440:2240:b5b1...	2a00:1450:4007:80c:...	QUIC	95	Protected Payload (KP0), DCID=db1d2a0d83be0df0
68	3.848238	2a00:1450:4007:80c:...	2a02:8440:2240:b5b1...	QUIC	87	Protected Payload (KP0)
69	4.099483	2a02:8440:2240:b5b1...	2a00:11c0:2:351:213...	TCP	130	2163 → 5938 [PSH, ACK] Seq=105 Ack=81 Win=514 Len

> Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface \Device\NPF_{A2E6C159-AD93-4E17-990E-6C45386B2...}
> Ethernet II, Src: LiteonTe_a9:33:03 (80:30:49:a9:33:03), Dst: 1a:2b:4d:a2:95:25 (1a:2b:4d:a2:95:25)

REALISATION PROFESSIONNELLE

Projet n° 2

GREPILLOUX Antonin
BTS SIO



Table des matières

I – Présentation :.....	14
a. Contexte :.....	14
b. Schéma de l'infrastructure réseau :.....	15
II – Mise en œuvre de la solution :.....	16
a. Installation Hearbeat	16
b. Réplication MySQL.....	18
c. Installation GroupOffice.....	19
d. Installation GLPI	20
e. Installation Zabbix	22

I – Présentation :

a. Contexte :

L'entreprise nommée « Logan » créée en 2012 est basée en France. C'est

une entreprise de 5 salariés qui est spécialisée dans la communication et le marketing. Seuls 2 salariés s'occupent du pôle marketing, qui sont ensuite vendus par un commercial. La société est également constituée de deux membres au service informatique. Tout le personnel dispose d'un poste sous Windows 10.

L'entreprise souhaiterait s'améliorer et ouvrir d'autres applications internes à l'entreprise. Le directeur a analysé leur système informatique pour évaluer le tarif de ses équipements informatiques et a remarqué qu'aucun système d'inventaire n'était en place. De plus, certains employés se plaignaient de problèmes récurrents et aucune amélioration ni suivis de ces derniers commençaient à devenir problématiques.

En tant que membre du service informatique et jeune diplômé, j'ai eu pour mission de mettre en place un système d'inventaire des machines et de gestion d'incidents, un pad collaboratif entre employés, et un serveur de supervision en apportant les compétences acquises lors de mon BTS SIO.

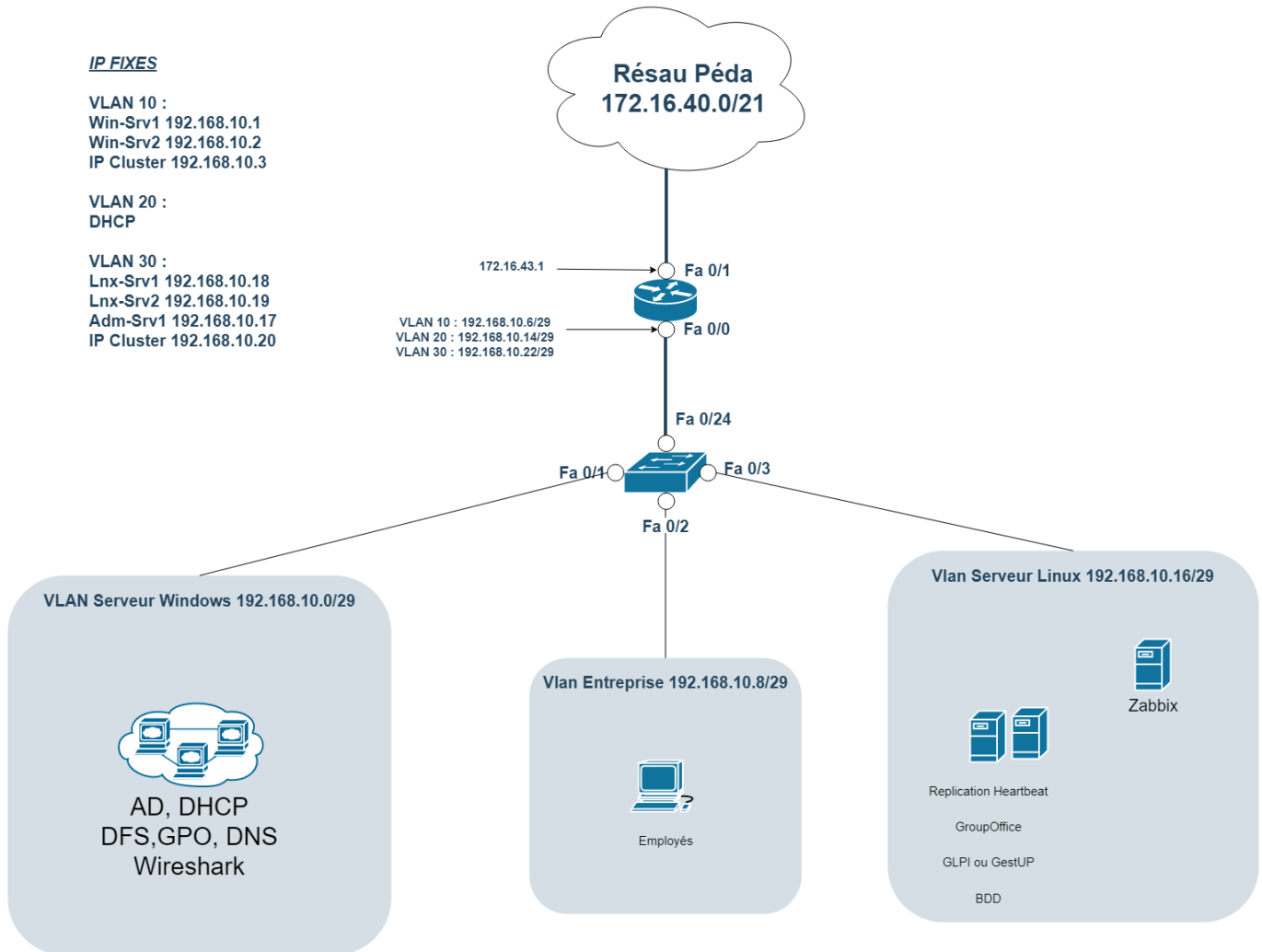
b. Schéma de l'infrastructure réseau :

IP FIXES

VLAN 10 :
Win-Srv1 192.168.10.1
Win-Srv2 192.168.10.2
IP Cluster 192.168.10.3

VLAN 20 :
DHCP

VLAN 30 :
Lnx-Srv1 192.168.10.18
Lnx-Srv2 192.168.10.19
Adm-Srv1 192.168.10.17
IP Cluster 192.168.10.20

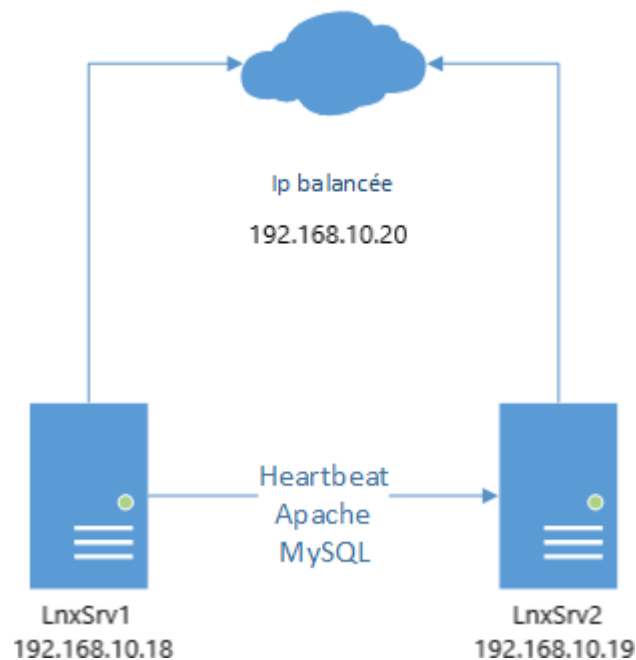


II – Mise en œuvre de la solution :

a. Installation Hearbeat

Heartbeat est un logiciel de surveillance de la disponibilité des programmes, pour les systèmes d'exploitation Linux, FreeBSD, OpenBSD, Solaris et MacOS X. Il est distribué sous licence GPL.

Heartbeat écoute les battements de cœur – des signaux émis par les services d'une grappe de serveurs lorsqu'ils sont opérationnels. Lorsque qu'un serveur devient défaillant, Heartbeat le détecte (puisqu'il n'entend plus ses battements de coeurs) et bascule les services surveillés sur un autre serveur. Pour que cela soit transparent pour les utilisateurs, Heartbeat met en place une IP virtuelle unique qui est balancée entre les deux serveurs.



Fichier de configuration pour indiqu  l'ip balanc e et les services a d marr  :

```
GNU nano 3.2 /etc/ha.d/haresources
LnxFrv1 IPaddr::192.168.10.20/29/ens33 mysql apache2
```

Nous pouvons voir que l'ip balanc e est bien actif.

```
root@LnxFrv1:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:88:88:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.10.18/29 brd 192.168.10.23 scope global ens33
        valid_lft forever preferred_lft forever
    inet 192.168.10.20/29 brd 192.168.10.23 scope global secondary ens33:0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe88:8813/64 scope link
        valid_lft forever preferred_lft forever
root@LnxFrv1:~#
```

Dans la configuration d'Heartbeat, il existe plusieurs options qu'on peut d finir. Comme auto-balancement, qui re-balance les services sur le node primaire quand il revient en ligne.

```
GNU nano 3.2 /etc/ha.d/ha.cf
mcast ens33 239.0.0.10 694 1 0

warntime 4
deadtime 5
initdead 15
keepalive 2

#Re-balance les services sur le node primaire quand il revient en ligne
auto_failback on

#Serveurs du cluster
node LnxFrv1
node LnxFrv2
```

b. Réplication MySQL

MySQL prend en charge en natif la réplication en tant que fonctionnalité standard de la base de données. Selon la configuration, on peut répliquer toutes les bases de données, une sélection de bases de données ou même des tables sélectionnées dans une base de données.

Dans notre cas, nous allons répliquer toutes les bases de données. Sur nos deux serveurs Linux nous indiquons qui est le serveur maître, et qui est le serveur esclave. Suite à cela nous pouvons configurer la réplication MySQL entre les deux serveurs.

Cela permet aux bases de données des applications web telles que GroupOffice et GLPI d'être répliqué. Sachant que nous avons heartbeat d'actif sur les deux serveurs, alors si un serveur tombe en panne alors le deuxième serveur reprend l'ip balancé plus les bases de données répliquer. Donc cela donne une totale transparence pour l'utilisateur car, il ne perd pas ses applications web, ni même les données.

De plus, pour approfondir la réplication MySQL, l'ajout d'un script permettant l'exportation des bases de données peut être utile dans un cas extrême si les deux serveurs tombent en panne.

Ce script est fait en bash. Il exporte les bases de données sous un nom de dossier spécifique tel que « Année-Mois-Jour » puis les envoie sur un dossier partagé sous le format .gz pour éviter les fichiers trop volumineux. (Voir Annexe Script Linux)

Ce script s'exécute tous les midis grâce au cron.

```
#!/bin/bash
TIMESTAMP=$(date +%F)
MYSQL="/usr/bin/mysql"
MYSQL_USER="root"
MYSQL_PASSWORD="root"
SMB_BACKUP_DIR="/mnt/backup"
SMB_BACKUP_SOURCE="//logan.local/Backup"
SMB_BACKUP_USER="backup"
SMB_BACKUP_PASSWORD="00sqR542**"
BACKUP_DIR="$SMB_BACKUP_DIR/$TIMESTAMP"

mkdir -p $SMB_BACKUP_DIR
mount -t cifs "$SMB_BACKUP_SOURCE" "$SMB_BACKUP_DIR" -o
username="$SMB_BACKUP_USER",password="$SMB_BACKUP_PASSWORD"
mkdir -p $BACKUP_DIR

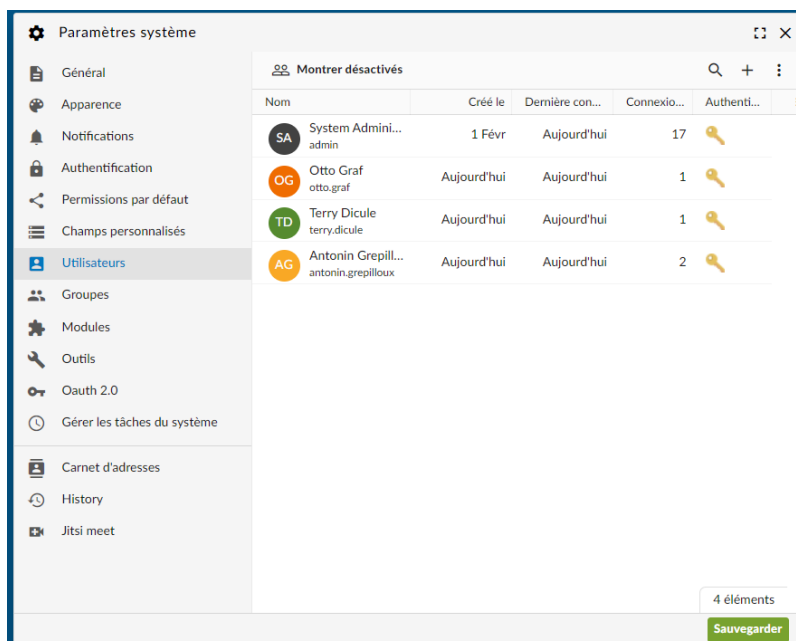
databases=`$MYSQL --user=$MYSQL_USER -p$MYSQL_PASSWORD -e "SHOW DATABASES;" |
grep -Ev "(Database|information_schema)" | grep -Ev
"(Database|performance_schema)" | grep -Ev "(Database|$
for db in $databases; do
mysqldump --force --opt --user=$MYSQL_USER -p$MYSQL_PASSWORD --databases $db
| gzip > "$BACKUP_DIR/$db.gz"
done

umount $SMB_BACKUP_DIR
```

c. Installation GroupOffice

Group-Office est un outil de gestion de la relation client (CRM) et de groupware. Partagez des projets, des calendriers, des fichiers et des e-mails en ligne avec des collègues et des clients. Facile à utiliser et entièrement personnalisable.

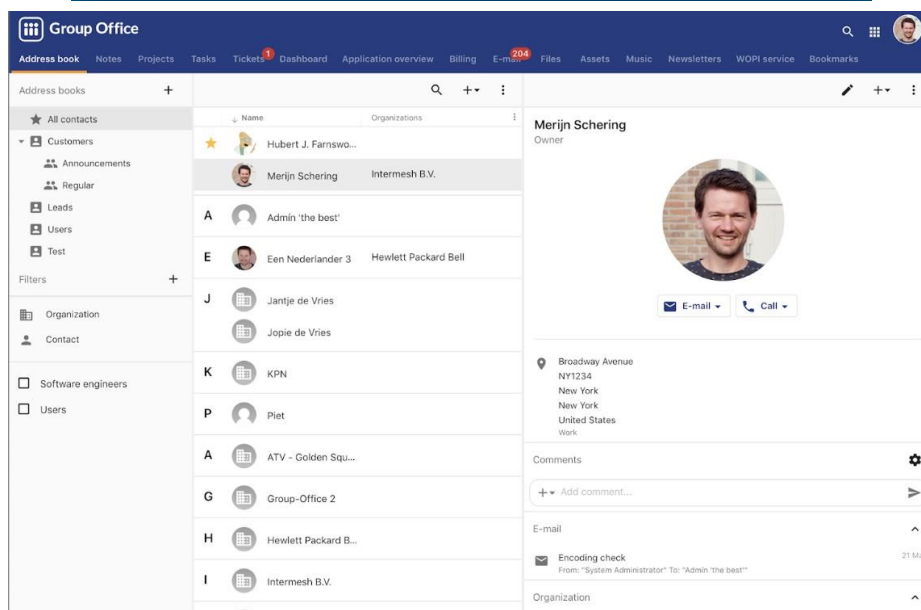
L'utilisation de GroupOffice est parfaite dans l'utilisation interne entre employés, elles disposent de plusieurs fonctionnalités qui permettent une bonne communication au sein de l'entreprise. Que ce soit le calendrier pour les tâches futures ou comme la création de notes. Cette application est importante pour une bonne communication.



Montrer désactivés					
Nom	Créé le	Dernière con...	Connexio...	Authenti...	
SA System Admini... admin	1 Févr	Aujourd'hui	17	🔑	
OG Otto Graf otto.graf	Aujourd'hui	Aujourd'hui	1	🔑	
TD Terry Dicule terry.dicule	Aujourd'hui	Aujourd'hui	1	🔑	
AG Antonin Grepill... antonin.grepilloux	Aujourd'hui	Aujourd'hui	2	🔑	

4 éléments

Sauvegarder



Group Office

Address book

All contacts

- Customers
- Announcements
- Regular
- Leads
- Users
- Test

Filters

- Organization
- Contact
- Software engineers
- Users

Organizations

- Hubert J. Farnsw...
- Merijn Schering Intermesh B.V.
- Admin 'the best'
- Een Nederlander 3 Hewlett Packard Bell
- Jantje de Vries
- Jopie de Vries
- KPN
- Piet
- ATV - Golden Squ...
- Group-Office 2
- Hewlett Packard B...
- Intermesh B.V.

Merijn Schering
Owner

Broadway Avenue
NY1234
New York
New York
United States
Work

Comments

Add comment...

E-mail

Encoding check
From: "System Administrator" To: "Admin 'the best'"
21 May

Organization

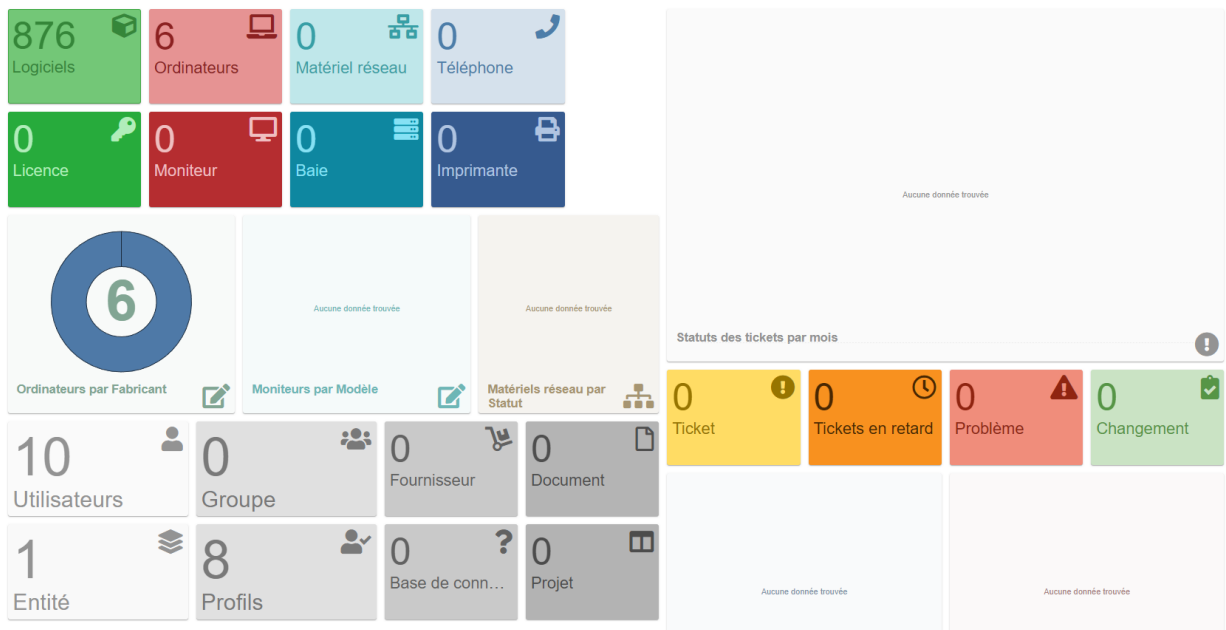
d. Installation GLPI

GLPI est une application de gestion de parc informatique et de gestion des demandes. Elle permet la gestion de l'inventaire des composantes matérielles ou logicielles d'un parc informatique, la gestion de l'assistance aux utilisateurs et La gestion de la demande (ticketing).

GLPI est une application importante pour l'entreprise, elle permet de connaître l'ensemble de son parc informatique avec son nombre de machines, ses composants, et d'autres informations utiles. Tout cela permet de prévoir de futurs achats pour remplacer des machines trop anciennes ou tomber en panne.

La gestion de son parc informatique est pratique pour bon nombre d'entreprises. De plus GLPI possède un outil de ticketing, permettant à ces utilisateurs de faire remonter leurs problèmes au service informatique via la création d'un ticket.

Puis, nous pouvons lier les comptes utilisateurs de l'Active Directory à GLPI, permettant aux utilisateurs de se connecter avec leurs comptes de session et n'aurons pas besoin de créer un nouveau compte auprès du SI.



Affichage (nombre d'éléments) : 20 Page courante en PDF paysage De 1 à 6 sur 6

Nom	Statut	Fabricant	Numéro de série	Type	Modèle	Système d'exploitation - Nom	Lieu	Dernière modification	Composants - Processeur
DESKTOP-J9P1LO7		VMware, Inc.	VMware-56 4d c3 ef 24 bd 46 d1-1f c1 5e 48 9b c5 b0 01	VMware	VMware Virtual Platform	Windows		2022-05-06 14:16	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
LnxFrv1		VMware, Inc.	VMware-56 4d df 8a ed 0c 2d 68-ac 34 e4 33 2a 88 88 13	VMware	VMware Virtual Platform	Debian GNU/Linux		2022-05-06 14:13	Intel(R) Core(TM) i5-9300HF CPU @ 2.40GHz
LnxFrv2		VMware, Inc.	VMware-56 4d 51 42 68 f0 8f 99-f6 9c 32 13 82 ad 14 4d	VMware	VMware Virtual Platform	Debian GNU/Linux		2022-05-03 14:36	Intel(R) Core(TM) i5-9300HF CPU @ 2.40GHz
Win-Srv1		VMware, Inc.	VMware-56 4d d5 e7 f7 59 ec de-22 8e 77 ef 14 f3 91 95	VMware	VMware Virtual Platform	Windows		2022-05-06 13:34	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
Win-Srv2		VMware, Inc.	VMware-56 4d ea f9 81 5f 86 dd-3d 06 63 9d b7 d6 90 3b	VMware	VMware Virtual Platform	Windows		2022-05-06 13:34	Intel(R) Core(TM) i7-7700 CPU @ 3.60GHz
zabbix-ag		VMware, Inc.	VMware-56 4d 9d a6 d5 16 3b 70-bb c9 57 89 9c 1f 94 8f	VMware	VMware Virtual Platform	Debian GNU/Linux		2022-05-03 14:39	Intel(R) Core(TM) i5-9300HF CPU @ 2.40GHz

⌵ Général
⌵ Tâches
⌵ Règles
⌵ Réseau
⌵ Déployer
⌵ Guide

Inventaire automatique vs ajout manuel

● Ordinateurs FusionInventory : 6 ● Autres ordinateurs : 0

Inventaires d'ordinateurs durant les dernières heures

Déploiement

● Préparé et en attente : 0 ● En cours : 0 ● Succès : 0
● En erreur : 0

Inventaire réseau par SNMP

● Équipements réseaux : 0 ● Imprimantes : 0

Ports sur les équipements réseaux (inventaire remonté par SNMP)

● Lié avec un matériel : 0
● Ports de switch SNMP non connectés : 0

Ports sur tout les équipements réseaux

● Lié avec un matériel : 0 ● Non lié : 0

e. Installation Zabbix

Zabbix est un logiciel de supervision et monitoring qui permet de surveiller en temps réel une infrastructure IT : l'état du réseau, des serveurs et autres équipements réseaux (routeur, imprimante...).

Le fonctionnement de Zabbix repose sur un serveur et un agent et il réagit par rapport à des événements. La supervision et métrologie Zabbix peut superviser soit des services système, des services applicatifs en relation à des applications métiers, de la disponibilité de service, etc....

L'ajout d'un serveur de supervision dans l'ensemble de l'infrastructure, permet de superviser les équipements et réagir en fonction des alertes.

Zabbix est une bonne solution car elle est simple d'utilisation et possède des modèles de supervision pour certains équipements, ce qui facilite la tâche pour superviser certains équipements spécifiques. De plus la supervision permet d'agir rapidement en cas de problèmes sur des équipements importants de l'infrastructure telle que les serveurs Windows et Linux.

Pour cela, superviser les serveurs semble important, nous pouvons surveiller leur performance, et certaines données qui peuvent être importantes à surveiller.

Pour le cas des serveurs linux, surveillé Apache est important car sans Apache, pas d'application web, donc pas de GLPI ni de GroupOffice.

Pareil pour tous ce qui est équipement Cisco, Zabbix possède des templates pouvant superviser des équipements Cisco. Les templates Cisco sont intéressantes car on peut superviser les interfaces, donc voir la bande passante et agir en conséquence.

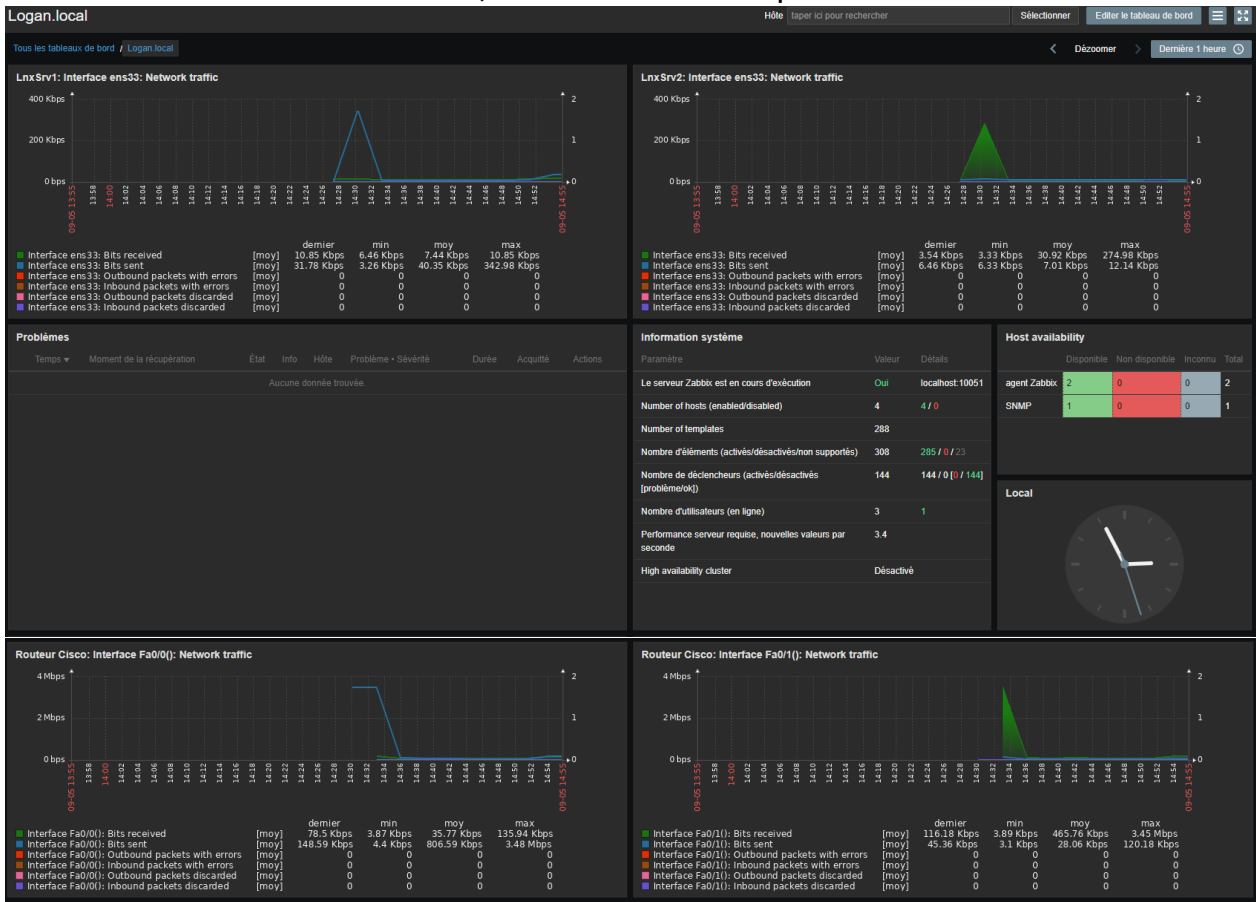
Mais tout cela doit donner des alertes au SI. Donc pour cela, la mise en place de l'envoi de mail est cruciale. Définir l'envoi de mail dès lors qu'une alerte apparaît est obligatoire. Cela permet de réagir rapidement.

il existe d'autres moyens pour alerter le SI de ce genre d'incident.

Dans notre cas, l'envoi de mail est actif mais par mesure de sécurité nous pouvons ajouter l'envoi de messages Discord via des Webhook.

Nous aurons alors deux moyens de prévention. Si l'un des deux n'est pas fonctionnel alors celui qui est encore fonctionnel alertera dans tous les cas.

Ci-dessous le tableau de bord, avec les alertes et plusieurs informations :



Liste des équipements supervisé :

Nom	Interface	Disponibilité	Tags	Problèmes	État	Dernières données	Problèmes	Graphiques	Tableaux de bord	Web
LnxSrv1	192.168.10.18:10050	ZBX			Activé	Dernières données	Problèmes	Graphiques 10	Tableaux de bord 2	Web
LnxSrv2	192.168.10.19:10050	ZBX			Activé	Dernières données	Problèmes	Graphiques 10	Tableaux de bord 2	Web
Routeur Cisco	172.16.43.1:161	SNMP			Activé	Dernières données	Problèmes	Graphiques 9	Tableaux de bord 1	Web
Zabbix server	127.0.0.1:10050	ZBX			Activé	Dernières données	Problèmes	Graphiques 24	Tableaux de bord 3	Web

Affichage de 4 sur 4 trouvés

Moyens de communication pour la remonté d'alerte :

Utilisateur	Type	Envoyer	Lorsque actif	Utiliser si sévérité	État	Action
Discord	https://discordapp.com/api/webhooks/94821717522581...	1-7,00:00-24:00	N I A M H D	Activé	Édition	Supprimer
Email	antonin.grepilloux.sio@gmail.com	1-7,00:00-24:00	N I A M H D	Activé	Édition	Supprimer

Buttons: Actualiser, Supprimer, Annuler

Données récupérer via l'agent zabbix :

Hôte	Nom	Dernière vérification	Dernière valeur	Changer	Tags
Zabbix server	/: Free inodes in %	15/03/2022 16:28:49	90.5265 %		Application: Filesystem /
Zabbix server	/: Space utilization	15/03/2022 16:28:48	32.5119 %	+0.000118 %	Application: Filesystem /
Zabbix server	/: Total space	15/03/2022 16:28:47	6.84 GB		Application: Filesystem /
Zabbix server	/: Used space	15/03/2022 16:28:46	2.1 GB	+8 KB	Application: Filesystem /
Zabbix server	Available memory	15/03/2022 16:28:19	3.28 GB	-11.55 MB	Application: Memory
Zabbix server	Available memory in %	15/03/2022 16:28:17	86.2632 %	-0.2966 %	Application: Memory
Zabbix server	Checksum of /etc/passwd	15/03/2022 16:21:34	c7b7ffe1ceec2291...		Application: Security
Zabbix server	Cluster node []: Address	15/03/2022 16:25:25	localhost:10051		Application: Cluster no...
Zabbix server	Cluster node []: Last access age	15/03/2022 16:28:25	00:00:01		Application: Cluster no...
Zabbix server	Cluster node []: Last access time	15/03/2022 16:28:25	15/03/2022 16:28:24	+00:01:00	Application: Cluster no...
Zabbix server	Cluster node []: Status	15/03/2022 16:25:25	Active (3)		Application: Cluster no...
Zabbix server	Context switches per second	15/03/2022 16:29:03	499.8849	+30.4751	Application: CPU
Zabbix server	CPU guest nice time	15/03/2022 16:29:04	0 %		Application: CPU
Zabbix server	CPU guest time	15/03/2022 16:29:05	0 %		Application: CPU
Zabbix server	CPU idle time	15/03/2022 16:28:13	99.5502 %	+0.2131 %	Application: CPU
Zabbix server	CPU interrupt time	15/03/2022 16:29:07	0 %		Application: CPU
Zabbix server	CPU iowait time	15/03/2022 16:29:02	0.121 %	+0.05853 %	Application: CPU
Zabbix server	CPU nice time	15/03/2022 16:29:09	0 %		Application: CPU
Zabbix server	CPU softirq time	15/03/2022 16:29:06	0.06258 %	+0.004282 %	Application: CPU
Zabbix server	CPU steal time	15/03/2022 16:29:08	0 %		Application: CPU
Zabbix server	CPU system time	15/03/2022 16:29:12	0.2962 %	+0.05471 %	Application: CPU

REALISATION PROFESSIONNELLE

Annexe

GREPILLOUX Antonin
BTS SIO



Script python pour le commutateur :

```
from time import sleep
import pyautogui

#attribution d'un nom aux vlan
sleep(5)
pyautogui.typewrite("en")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("conf t")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("vlan 10")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("name Windows")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("vlan 20")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("name Client")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("vlan 30")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("name Linux")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

```
#configuration vlan access et trunk

pyautogui.typewrite("Interface FastEthernet 0/1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("switchport access VLAN 10")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("Interface FastEthernet 0/2")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("switchport access VLAN 20")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("Interface FastEthernet 0/3")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("switchport access VLAN 30")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("Interface FastEthernet 0/24")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("switchport mode trunk")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("switchport trunk allowed vlan all")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("write")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

Script python du routeur :

```
from time import sleep
import pyautogui

##Démarrage + Enable

sleep(5)
pyautogui.typewrite("en")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("conf t")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)

##Configuration Interface fe0/0 - fe 0/1

pyautogui.typewrite("Interface FastEthernet 0/0")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("no sh")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("Interface FastEthernet 0/1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip address 172.16.43.1 255.255.248.0")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("no sh")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

```
##Configuration Interface Fe0/0.10

pyautogui.typewrite("Interface FastEthernet 0/0.10")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("encapsulation dot1Q 10")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip address 192.168.10.6 255.255.255.248")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.2")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat inside")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)

##Configuration Interface Fe0/0.20

pyautogui.typewrite("Interface FastEthernet 0/0.20")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("encapsulation dot1Q 20")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip address 192.168.10.14 255.255.255.248")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.2")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat inside")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

```
##Configuration Interface Fe0/0.30

pyautogui.typewrite("Interface FastEthernet 0/0.30")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("encapsulation dot1Q 30")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip address 192.168.10.22 255.255.255.248")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip helper-address 192.168.10.2")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat inside")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)

##Routage
pyautogui.typewrite("ip routing")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip route 172.16.40.0 255.255.248.0 172.16.43.1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip route 0.0.0.0 0.0.0.0 172.16.47.254")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

```
##Configuration NAT

pyautogui.typewrite("Interface FastEthernet 0/0")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat inside")
sleep(0.2)
pyautogui.press('enter')
sleep(10)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("Interface FastEthernet 0/1")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat outside")
sleep(0.2)
pyautogui.press('enter')
sleep(10)
pyautogui.typewrite("exit")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)

##Activation NAT

pyautogui.typewrite("access-list 1 permit 192.168.10.0 0.0.0.255")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
pyautogui.typewrite("ip nat inside source list 1 interface FastEthernet 0/1
overload")
sleep(0.2)
pyautogui.press('enter')
sleep(0.2)
```

Script Bash Backup MySQL:

```
#!/bin/bash

TIMESTAMP=$(date +%F)
MYSQL="/usr/bin/mysql"
MYSQL_USER="root"
MYSQL_PASSWORD="root"
SMB_BACKUP_DIR="/mnt/backup"
SMB_BACKUP_SOURCE="//logan.local/Backup"
SMB_BACKUP_USER="backup"
SMB_BACKUP_PASSWORD="00sqr542**"
BACKUP_DIR="$SMB_BACKUP_DIR/$TIMESTAMP"

mkdir -p $SMB_BACKUP_DIR
mount -t cifs "$SMB_BACKUP_SOURCE" "$SMB_BACKUP_DIR" -o
username="$SMB_BACKUP_USER",password="$SMB_BACKUP_PASSWORD"
mkdir -p $BACKUP_DIR

databases=`$MYSQL --user=$MYSQL_USER -p$MYSQL_PASSWORD -e "SHOW DATABASES;" |
grep -Ev "(Database|information_schema)" | grep -Ev
"(Database|performance_schema)" | grep -Ev "(Database|$
for db in $databases; do
mysqldump --force --opt --user=$MYSQL_USER -p$MYSQL_PASSWORD --databases $db
| gzip > "$BACKUP_DIR/$db.gz"
done

umount $SMB_BACKUP_DIR
```