

BTS SIO

Situation professionnelle numéro 3

Câblage, installation et paramétrage d'un réseau informatique

Description :

Le câblage et l'installation d'un réseau informatique est indispensable pour une société. L'ensemble du parc fonctionne sous Windows.

Mots-clés :

serveur
vyatta VPN
NOD32 AD
switch routeur
cablages
RJ45 IA-568-B
NAT
DHCP

Validation de la situation professionnelle

Nom	Date	Tampon
	26/05/2014	

Plan de la situation

Le cahier des charges.....	3
L'expression des besoins	3
La description de l'existant.....	3
L'analyse des choix.....	3
Mise en œuvre	4
Schéma passage des câbles.....	4
Schéma topologique du réseau :	5
Configuration de la DMZ sur une BBOX professionnelle :	6
Le serveur HP avec VMWare ESXi5.....	7
Le routeur logiciel : Vyatta.....	8
Le serveur : Windows 2008R2	9
Le rôle Active Directory	9
Ajout d'utilisateur et d'un groupe dans l'AD :.....	9
Service de fichiers.....	11
Serveur DHCP.....	12
L'adressage dans le réseau.....	13
Les progiciels et logiciels présents sur le serveur	13
Le commutateur Cisco SG300	14
La sauvegarde sur le NAS LACIE.....	15
Conclusion	16

Le cahier des charges

L'expression des besoins

La société ACDEF est située en Ardèche et elle souhaite disposer d'un réseau informatique. Le câblage du réseau, l'installation et le paramétrage des interconnexions devra être effectué. Elle souhaite disposer d'un serveur interne et d'une solution d'accès à distance, afin de permettre aux différents techniciens de l'entreprise d'effectuer un travail distant. Accord de l'entreprise pour publication.

La description de l'existant

Suite à un déménagement, le réseau informatique dont elle dispose est un réseau « scotché » sur le sol. Actuellement, la société utilise les périphériques suivants sur le réseau :

Une BBOX professionnel
Un switch DLINK (8port) non manageable
Un NAS domestique LACIE
Deux imprimantes multifonction

Le serveur de comptabilité est exécuté sur le poste « client » du PDG de la société. Aucun connexion distante n'est effectuée avec la BBOX.

L'analyse des choix

Dans notre analyse, nous avons pris en compte les besoins du client et son budget prévisionnel. Voici la phase de déploiement que nous avons réalisée :

- Création du câblage physique du réseau informatique (3 jours).
- Mise en place d'un hyperviseur sur le serveur avec deux VM (2 jours).
- Création des services et configuration des postes clients (1 jour).
- Sécurisation du switch. (1/2 journée).

Mise en œuvre

Le passage des cables

La réalisation du câblage du réseau a été la partie la plus longue car nous avons déployé des cables dans l'ensemble des pièces du local de l'entreprise, ajouté des goulottes, serti des prises RJ45, fixé une petite baie réseau, câblé une prise électrique et nous l'avons reliée au tableau électrique.

L'ensemble du matériel cité ci-dessus, a été commandé chez Rexel à Portes-Les-Valence.

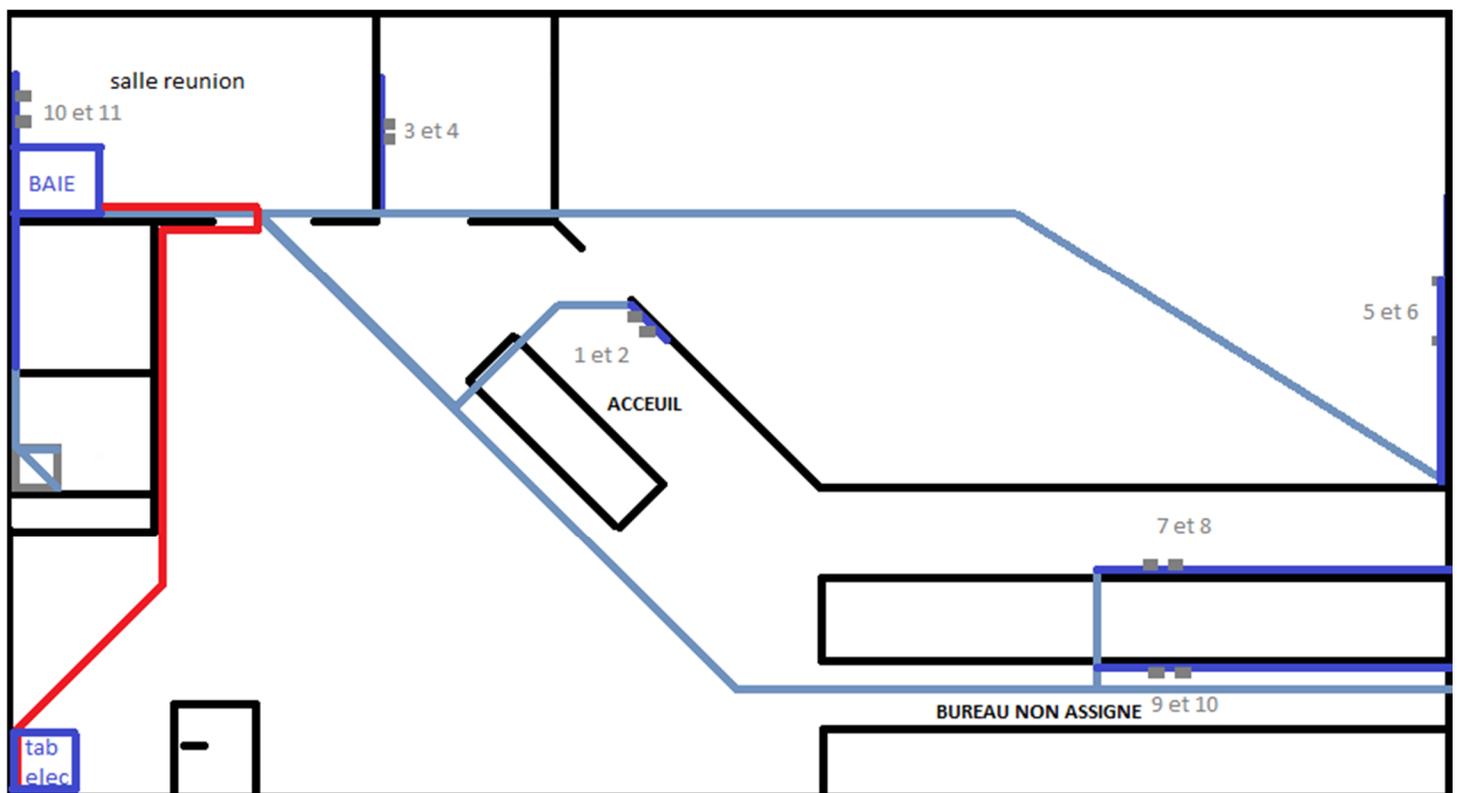
Parfois, il nous a été nécessaire de percer le mur afin de permettre le passage des câbles de la baie jusqu'au différents bureaux.

Des câbles réseaux de catégorie 6 ont été mis en place, ils garantissent des débits théoriques de 1 Gigabyte . C'était ma seconde expérience d'un câblage réseau, cependant le câble a été plus long que ma première expérience.

Schéma passage des câbles

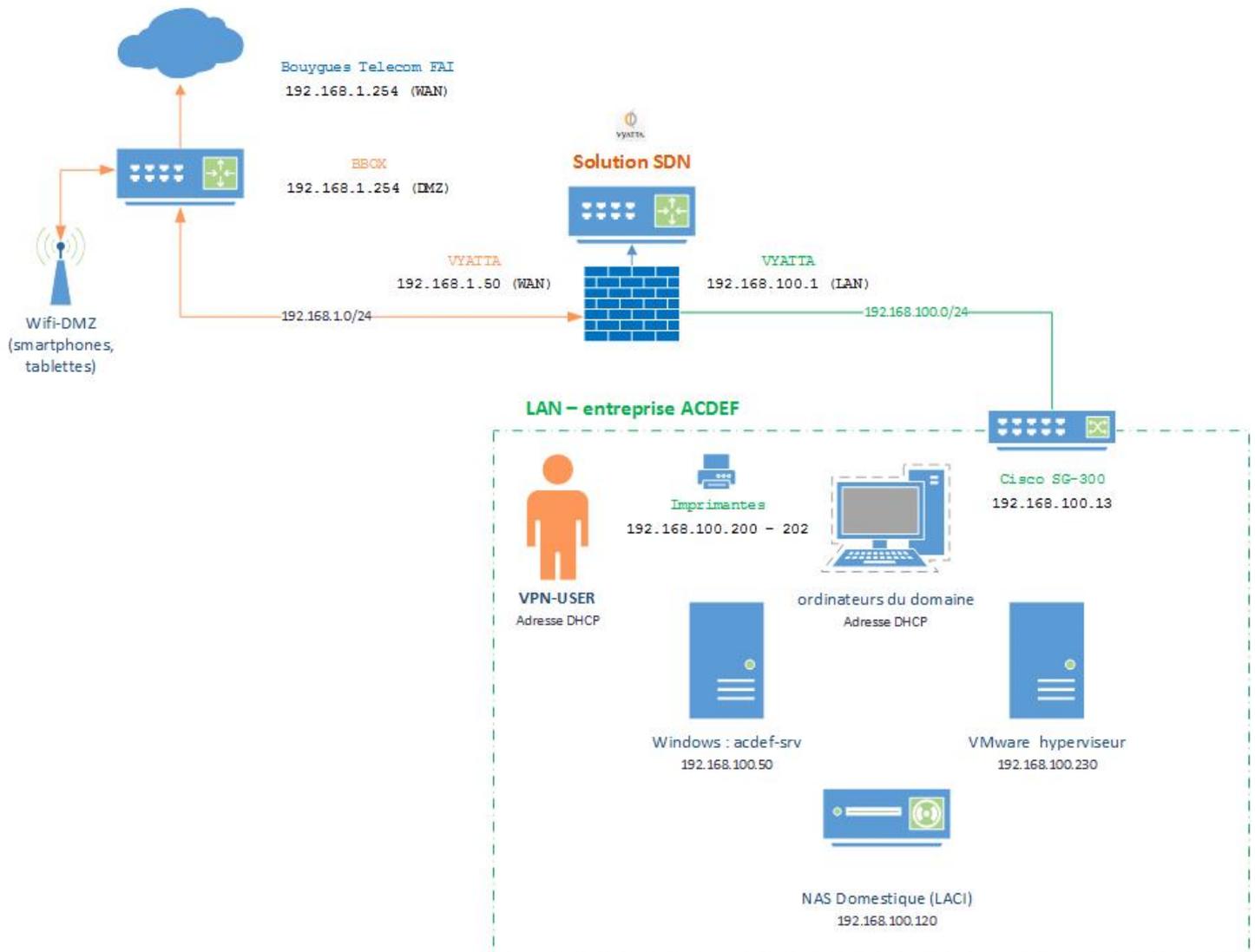
Nous ne disposons pas du plan des locaux, nous avons donc rapidement établi le passage des câbles. La visualisation ci-dessous schématise le local :

- BAIE, TABLEAU ELECTRIQUE, CABLES GOULOTTES
- CABLES RESEAU DANS PLAFOND
- CABLES ELECTRIQUE
- CONNECTIQUES RESEAU



Le « Schéma » ci-dessus a été réalisé très rapidement avec le logiciel PAINT.

Schéma topologique du réseau :



La réalisation de ce réseau informatique est extrêmement simple car il y a peu d'hotes sur le réseau.

Configuration de la DMZ sur une BBOX professionnelle :

Une DMZ se réalise grâce à un pare-feu, Les DMZ sont généralement utilisées en entreprise car elle ont un souhait de sécuriser un minimum leur réseau.

Pour accéder à la BBOX, nous nous connectons directement à l'interface web : <http://192.168.1.254>

The screenshot shows the Bouygues Telecom Bbox web interface. The top navigation bar includes the Bouygues Telecom logo and the text 'Bbox'. On the left, there are two main menu sections: 'PRÉFÉRENCES GÉNÉRALES' (General Preferences) with sub-items 'État des connexions', 'Jeux et Applications', and 'Schéma de mon réseau'; and 'CONFIGURATION AVANCÉE' (Advanced Configuration) with sub-items 'Configuration WiFi', 'Contrôle du WiFi', 'Périphériques connectés', 'Configuration du routeur', 'Modification du mot de passe', 'Sauvegarde et Restauration', 'Prise en main à distance', and 'Réinitialisation Bbox'. The main content area is titled 'État des connexions' and has two tabs: 'Services' and 'Bbox'. Below the tabs, a summary box states: 'Cette page résume les informations principales concernant votre connexion internet et votre réseau WiFi ainsi que vos services de téléphonie et de TV.' There are two columns of information: 'INTERNET' and 'WIFI'. Under 'INTERNET', it shows 'Connecté' with a green checkmark, 'Adresse IP Publique: [redacted]', 'Débit Upload: 854 Kbps', and 'Débit Download: 7430 Kbps'. Under 'WIFI', it shows 'Activé' with a green checkmark, 'Nom du réseau 2,4 GHz: [redacted]', 'Nom du réseau 5 GHz: [redacted]', and 'Type de cryptage: WPA/WPA2'. A 'Désactiver le WiFi' button is located at the bottom right of the WiFi section.

Pour activer une DMZ rendons nous dans l'onglet « Configuration Avancée » puis « DMZ » :

The screenshot shows the 'Configuration du routeur' (Router Configuration) page in the Bouygues Telecom Bbox interface. The left sidebar is identical to the previous screenshot. The main content area has a title 'Configuration du routeur' and a series of tabs: 'Pare-Feu', 'DynDNS', 'DHCP', 'NAT/PAT', 'WoL/WoW', 'DMZ', and 'UPnP'. The 'DMZ' tab is selected. A summary box at the top states: 'Le service DMZ permet de rediriger tous les flux venant d'Internet vers l'un de vos équipements du foyer.' Below this, it says 'Le service DMZ est activé' followed by a 'DESACTIVER LE SERVICE' button. The 'Adresse IP ou nom de l'ordinateur' field contains '192.168.1.50' and has a red 'x' icon and a pencil icon next to it. At the bottom, there are two buttons: 'ANNULER LES MODIFICATIONS' (left) and 'VALIDER' (right).

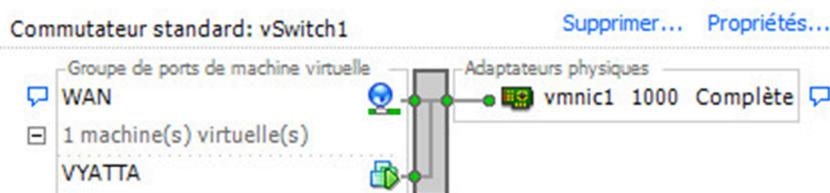
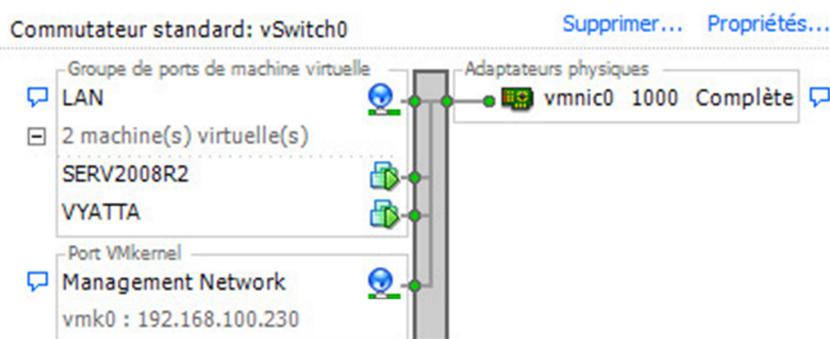
Le serveur HP avec VMXare ESXi5

Le serveur que nous allons installer est un HP ProLiant ML310e Gen8

La configuration du materiel :

	ML310e Gen8
Processeurs-CPU	XEON E3-1230v2 @3,30Ghz (4CPU)
Mémoire-RAM	8Go
Stockage-DISQUES	1000Go
Puissance-ALIMENTATION	460W
PCI-EXPRESS-16X	CARTE RAID1
PCI-EXPRESS-X	CARTE RESEAU x2 (1G/Bytes)

La mise en réseau de notre hyperviseur :



Informations complémentaires :

Une carte physique est reliée au réseau internet (WAN)

- Une carte virtuelle de Vyatta

Une carte physique est reliée au réseau local (LAN)

- Une carte virtuelle de Vyatta

- Une carte virtuelle de Windows

Nous disposerons uniquement de 2 machines virtuelles dans notre hyperviseur.

Le routeur logiciel : Vyatta

Le routeur/pare feu de Vyatta va être déployé chez notre client afin de faire du routage et du VPN.
Les étapes de configuration seront les suivantes :

1. Configuration de 2 interfaces (WAN-LAN)
2. Ajout de la route par défaut vers notre passerelle et la résolution de nom DNS.
3. Configuration des règles de NAT (WAN-LAN et LAN-WAN)
4. Configuration de l'accès distant VPN en mode PPTP.

Etape 1 : Configuration des interfaces réseaux

```
set interfaces ethernet eth0 address 192.168.100.1/24
set interfaces ethernet eth0 description LAN
set interfaces ethernet eth1 address 192.168.100.50/24
set interfaces ethernet eth1 description WAN
```

Etape 2 : Configuration du systeme

```
set system host-name vyatta
set system login user vyatta authentication encrypted-password
set system name-server 192.168.100.50
set system gateway-address 192.168.1.254
```

Etape 3 : Configuration du NAT

```
set nat source rule 1 outbound-interface eth1
set nat source rule 1 source address 192.168.100.0/24
set nat source rule 1 translation address 192.168.1.50
set nat source rule 2 outbound-interface eth0
set nat source rule 2 source address 192.168.100.1/24
set nat source rule 2 translation address masquerade
```

Etape 4 : Configuration de l'accès distant VPN (PPTP)

```
set vpn pptp remote-access authentication mode local
set vpn pptp remote-access dns-servers server-1 8.8.8.8
set vpn pptp remote-access client-ip-pool start 192.168.100.120
set vpn pptp remote-access client-ip-pool stop 192.168.100.140
set vpn pptp remote-access authentication local-users username es2com password p4ssw0rd
```

Nous avons trois employés qui utilisent l'accès à distance.

Le serveur : Windows 2008R2

Windows serveur nous permettra de proposer des services Microsoft dans le réseau mis en œuvre. Nos clients sont intégralement dans un parc Windows, le serveur utilisera les services suivants :

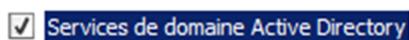
- Active Directory
- Services de fichiers
- Serveurs d'impression
- Serveur DHCP

La mise en place des différents services : AD, fichiers et DHCP seront détaillés.

Le rôle Active Directory

L'Active Directory est un service d'annuaire, centralisé d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows.

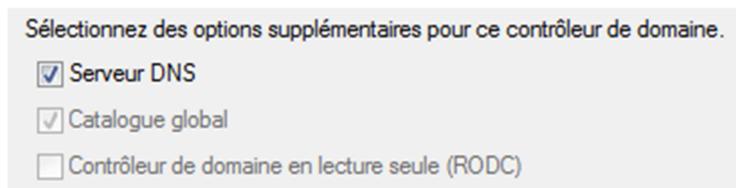
L'installation du rôle se déroule dans « gestionnaire de serveur » puis « ajout d'un rôle » :



(Pour information, la fonctionnalité du .NET Framework 3.5.1 s'installera sur le serveur)

Nous allons sélectionner le « mode avancé » et procéder comme suit :

1. Via, menu démarrer lancer l'installation des services de domaine AD avec « dcpromo.exe ».
2. Puis, créer un domaine dans une nouvelle forêt avec le nom de domaine et Netbios complet : ACDEF.FR
3. Le niveau fonctionnel de la forêt sous : Windows Server 2008R2
4. Voici les options supplémentaires sélectionnées, pour le contrôleur de domaine :



5. L'emplacement de la base de données, des journaux et de SYSVOL sont par défaut
6. Le mot de passe administrateur de restauration AD est configuré
7. L'assistant d'installation nous informe de la mise en place des services AD, c'est terminé.

Nous pouvons maintenant utiliser l'annuaire de l'active directory dans notre réseau.

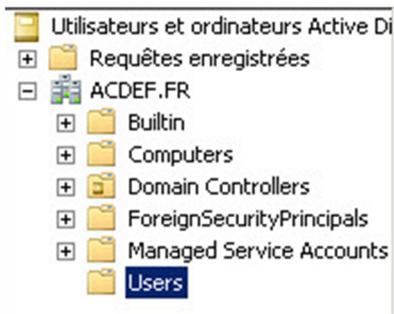
Ajout d'utilisateur et d'un groupe dans l'AD :

Pour ajouter des utilisateurs et des groupes dans l'AD, nous nous rendons dans :

Démarrer/Outils d'administration/Utilisateurs et ordinateur Active Directory

Pour créer un utilisateur nous cliquons droit sur « users » puis « nouveaux » et « utilisateurs » :

Par exemple l'utilisateur « es2com » :

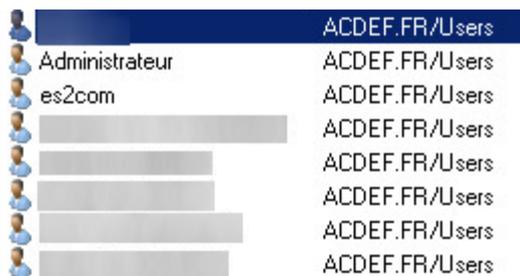


Prénom :	es2com	Initiales :	
Nom :			
Nom complet :	es2com		
Nom d'ouverture de session de l'utilisateur :			
es2com			@ACDEF.FR
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
ACDEF\	es2com		

Les caractéristiques des mots de passe :

- L'utilisateur ne peut pas changer de mot de passe
- Le mot de passe n'expire jamais

La création de groupe est similaire cependant nous choisissons « nouveaux » et « groupe ». Une fois le groupe créé nous pouvons désormais ajouter nos utilisateurs à l'intérieur de celui-ci. Par exemple voici le groupe « commun » avec nos différents utilisateurs :



Nous avons désormais créé nos différents utilisateurs et nos groupes dans le domaine. Les fonctions de base de l'AD ont été mises en œuvre avec l'annuaire d'entreprise Windows.

Voici les administrateurs du domaine :

Login utilisateur	Password utilisateur	Lecteur réseau autorisé
Administrateur	/	Accès total au serveur
client	/	Accès total au serveur

Désormais nous allons utiliser les groupes définis pour l'ajout des accès réseaux

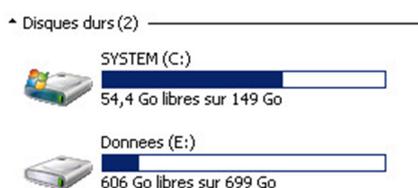
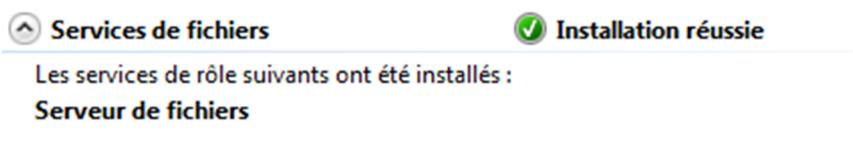
Service de fichiers

Le rôle serveur Services de fichiers dans Windows Server 2008 nous permettra de gérer les dossiers partagés et d'activer la réplication de fichiers.

L'installation du rôle se déroule dans « gestionnaire de serveur » puis « ajout d'un rôle » :



Nous cocherons dans ce rôle, uniquement la fonction « serveur de fichier ». L'installation se termine rapidement



Nous possédons deux disques sur la VM

Les partages sont présents ci-dessous :

Protocole : SMB (11 éléments)					
	_Informati...	SMB	E:_Informatique		606 Go
	ADMIN\$	SMB	C:\Windows		54,5 Go
	C\$	SMB	C:\		54,5 Go
	COMMUN	SMB	E:\COMMUN		606 Go
	COMPTA	SMB	E:\COMPTA		606 Go
	DIRECTION	SMB	E:\DIRECTION		606 Go
	E\$	SMB	E:\		606 Go
	IPC\$	SMB			-
	NETLOG...	SMB	C:\Windows\SY...		54,5 Go
	STAGIAIRE	SMB	E:\STAGIAIRE		606 Go
	SYSVOL	SMB	C:\Windows\SY...		54,5 Go

Les partages réseaux du domaine sont : Z:\ COMMUN; Y:\ COMPTA ; X:\ DIRECTION et W:\ STAGIAIRE

Login utilisateur	Password utilisateur	Lecteur réseau autorisé
User1	/	Z:\ Y:\ X:\ W:\
User2	/	Z:\ Y:\ X:\ W:\
User3	/	Z:\
User4	/	Z:\
User5	/	Z:\ Y:\ X:\
stagiaire	/	W:\

Serveur DHCP

Le serveur DHCP va fournir automatiquement des adresses IP valides aux ordinateurs clients IP. Des paramètres de configuration supplémentaires, « options DHCP » seront mis en place.

L'installation du rôle se déroule également dans « gestionnaire de serveur » puis « ajout d'un rôle » :

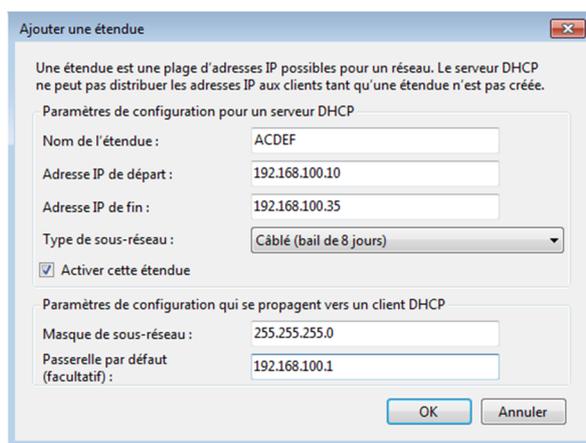


La demande de configuration est immédiate, le rôle DHCP détecte notre carte réseau :



Ensuite, le domaine Parent est toujours : ACDEF.FR avec le DNS préféré : 127.0.0.1
(le serveur WINS ne sera pas activé)

Voici la configuration de notre étendue DHCP :

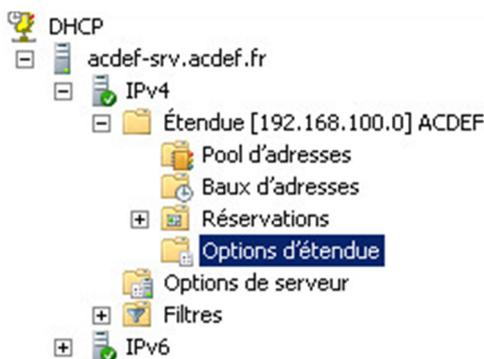


Le mode sans état DHCPV6 sera activé, et nous utiliserons les informations d'identification actuelles. L'installation du rôle DHCP est terminée :



Pour ajouter des options : Démarrer/Outils d'administration/DHCP :

Les options d'étendue sont les suivantes :



003 Routeur	Standard	192.168.100.1	Aucun
006 Serveurs DNS	Standard	192.168.100.50	Aucun

Nous avons terminé la configuration du rôle DHCP dans notre domaine.

L'adressage dans le réseau

Nous avons terminé la configuration du rôle DHCP dans notre domaine.

<i>NOM DE L'APPAREIL</i>	<i>ADRESSE STATIQUE</i>	<i>ROLE AU SEIN DE LA SOCIÉTÉ</i>
<i>BBOX Routeur</i>	192.168.1.254	Permet de sortir sur internet
<i>Vyatta Routeur/Firewall</i>	192.168.100.1	Routeur/pare-feu/VPN
<i>Switch CISCO</i>	192.168.100.13	Commutateur du réseau
<i>WINDOWS SERVEUR 2008R2</i>	192.168.100.50	Serveur AD, DHCP, DNS Partage de fichiers et progiciel.
<i>NAS – LACIE</i>	192.168.100.120	Sauvegarde Backup
<i>IMPRIMANTE HP – client</i>	192.168.100.200	Imprimante du PDG
<i>IMPRIMANTE KONICA - commun</i>	192.168.100.201	Imprimante commune
<i>IMPRIMANTE BROTHER – commun2</i>	192.168.100.202	Imprimante commune 2
<i>VMWare ESX5</i>	192.168.100.230	Serveur de virtualisation

Les progiciels et logiciels présents sur le serveur

Le serveur Windows héberge deux logiciels de comptabilité, et ils ont été installés par l'éditeur.

Nom du progiciel	Version	Qui y accède ?
Nexus Base de donnée	V 1.07	Utilisateur du domaine
Gestion_CS	V 1.65	Utilisateur du domaine
Compta_CS	V 2.57	Utilisateur du domaine

Le serveur Windows utilise des logiciels de sécurité et de sauvegarde :

Nom du programme	Version	Accès local
Panda Endpoint protection	V 6.20.11	oui
Panda cloud security	Agent	oui
Cobian Backup	V 11	oui

Nous avons également installé sur l'ensemble des postes l'antivirus Eset Smart Security 6.

Le commutateur Cisco SG300

La configuration du mode “port security” sur Switch Cisco permettra aux seules adresse MAC autorisées de se connecter au port du switch .

Si, un hôte non-autorisé se connecte, le switch réagira à cette violation de sécurité.

Par exemple, le port est attaqué ? Il passe en mode err-disabled.

Que faire ? Une intervention manuelle est nécessaire pour remonter le port.

Pourquoi ? Nous pourrions alors mieux constater l’attaque et l’identifier.

Méthode de configuration avec une seule interface :

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address sticky
```

```
Switch>enable
Switch#Configure terminal
Switch(config)#interface FastEthernet 0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security violation shutdown
```

Voici la configuration de chaque port :

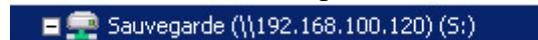
Nom du poste	Numero du port	Portsecurity
User1-nom_de_société	3	actif
User2-nom_de_société	7	actif
User3-nom_de_société	5	actif
User4-nom_de_société	6	actif
Stagiaire-nom_de_société	2	actif

la sauvegarde sur le NAS LACIE



La sauvegarde se fait avec un logiciel de backup disponible sur le serveur Windows nommée : Cobian Backup 11

Le lecteur réseau est disponible dans notre serveur Windows :

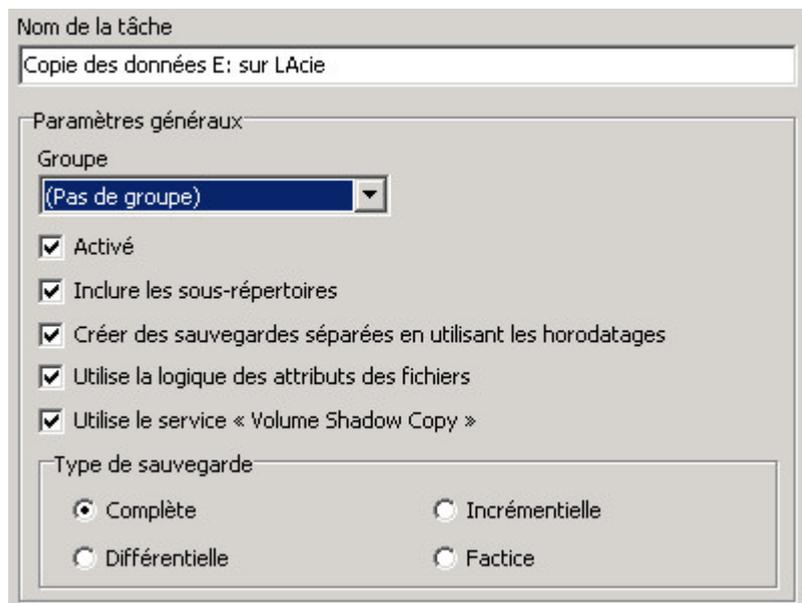


Nous n'aborderons pas l'installation et la solution de stockage, cependant intéressons nous à la configuration de sauvegarde du logiciel.

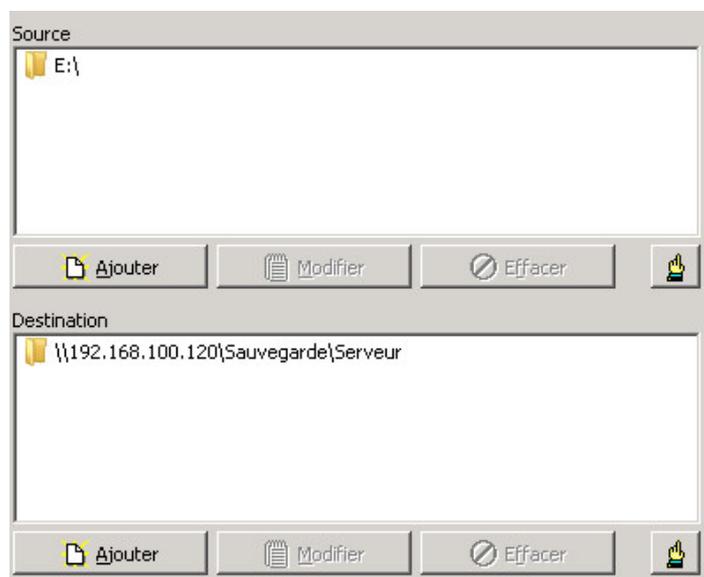
Une tâche est programmée dans le logiciel Cobian Backup 11 :



Le type de sauvegarde est « complète » :



Le répertoire source E :à destination du Lacie :



La planification de la sauvegarde est hebdomadaire les jours cochés ci-dessous, à 21h :

Type de planification
Hebdomadaire Sélectionnez le jour de la semaine

Le...
 Premier
 Second
 Troisième
 Quatrième
 Dernier

Jours de la semaine
 Lundi
 Mardi
 Mercredi
 Jeudi
 Vendredi
 Samedi
 Dimanche

Date/Heure
Date: 17/07/2013
Heure: 21:00:00
Jours du mois: 1
Mois: Janvier
Minuteur (minutes): 180
De : 00:00:00
Jusqu'à : 23:59:59

Aucun cryptage de la sauvegarde n'est mis en place dans notre tâche planifiée.

Conclusion

La mise en place du réseau informatique de la société ACDEF a été une expérience enrichissante dans le cadre de mon apprentissage. Elle m'a permis de comprendre les attentes d'un client et de suivre un projet du début jusqu'à la fin. La manipulation des câbles et l'ajout d'une baie informatique m'ont montrées qu'un administrateur réseau est avant tout capable de câbler correctement son réseau physique.

Pour le reste, des imprévus arrivent et il faut savoir être réactif à chaque nouveau problème rencontré, le client doit être rassuré de l'avancement de nos travaux.

Finalement je garderai de cette expérience de bons souvenirs car l'ensemble de la société ACDEF nous ont fait confiance dès le début et ils ont choisis es2com dans leurs projets de câblage, d'installation et de paramétrage du parc informatique.

Aujourd'hui encore nous dépannons la société avec un logiciel de télémaintenance, merci pour leur confiance !