

BTS SIO

Situation professionnelle numéro 2

Conception d'une infrastructure externalisée chez online.net

Description :

L'externalisation d'un client permet le transfert d'activité vers un prestataire externe. Elle permet au client de se focaliser sur son cœur de métier.

Mots-clés :

VMware ESXi Online.net
LUN Windows TSE VMkernel
Vyatta Tempo ISCSI Datacenter
RPN-SAN

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
Les offres du marché :.....	4
L'analyse du tableau :.....	4
Notre choix : Online.net.....	5
Mise en œuvre	6
Installation de l'hyperviseur VMware chez online.net	6
Demande de licence gratuite chez VMware	6
Ajouter la licence dans VMware ESXi 5.1	7
Comprendre la mise en réseau.....	7
La mise en réseau dans VMware ESXi 5.1	8
La mise en réseau de notre hyperviseur	9
La solution du ISCSI RPN-SAN de online.net.....	10
La configuration du ISCSI RPN-SAN de online.net.....	10
Profil de sécurité : activation du SSH.....	12
La configuration du ISCSI RPN-SAN de online.net (suite)	13
Ajouter le RPN-SAN dans un stockage LUN.....	14
Présentation des différentes VMs	15
Installation et configuration de la VM : VYATTA.....	16
Configuration de la VM : Windows 2008R2	17
Le progiciel Tempo :	19
L'administrateur du progiciel tempo.....	19
Mise en production de l'infrastructure	20

Le cahier des charges

L'expression des besoins

Une société d'interim située aux quatre coins de la France souhaite revoir son infrastructure externe. Leur souhait est de migrer leurs serveurs actuels (VPS) dans une infrastructure virtualisée. Elle souhaite centraliser ses utilisateurs sur un seul serveur distant (progiciel). Des règles de sécurité informatiques seront définis afin d'accéder au serveur.

La description de l'existant

Actuellement cette société d'interim dispose d'un serveur VPS sous Windows, hébergé chez ovh. Elle dispose aussi d'un site web sur une machine CentOS géré avec Plesk chez amen.fr

Les rôles et fonctionnalités installés sur le serveur windows sont les suivants : Active directory, Terminal serveur et des progiciels Propriétaires.

Aucun Antivirus n'est présent, le pare-feu Windows « semble » en fonctionnement.

Les mises à jour windows ne semblent pas avoir été faites depuis longtemps, et le serveur est accessible directement sur le réseau internet par différents ports et notamment via RDP (3389).

Les sauvegardes sont faites quotidiennement avec un serveur FTP externe fourni par OVH.

Après inspection, le serveur abrite plusieurs rootkits ainsi qu'un proxy qui redirige l'ensemble du système vers une IP extérieur afin de capter le flux de données.

Des pirates informatiques ont pris le dessus sur le système depuis quelques temps déjà.

L'analyse des choix

Nos choix ont été dictés par notre client, car leur souhait est d'avoir une infrastructure plus souple.

L'expression de leur besoin est claire : une infrastructure virtuelle de préférence chez OVH.

Aussi, nous leurs avons indiqués que leur serveurs étaient fortement compromis, nous avons constaté que l'ensemble des différentes agences de France l'était aussi. Le nombre de malwares sur les postes était très élevé avec plus de 1000 malwares par poste.... une notion de sécurité semble urgente !

Le choix est de réinstaller le tout sur un serveur propre et le sécuriser dans une infrastructure virtuelle.

Nous avons

- Recherché un hébergement disponible en France (rapidement).
- Utilisé l'hyperviseur VMware ESXi 5.1.
- Virtualisé et centralisé le réseau avec une solution SDN.
- Ajouté une machine virtuelle sous Windows 2008R2.
- Migré les données de l'ancien serveur vers le nouveau.
- Sauvegardé des VM sur ISCSI avec la solution GhettoVCB.

Les offres du marché :

Pour faire un choix parmi les différents hébergeurs nous avons comparé les leaders Français :

L'analyse du tableau :

Online.net : Avant gardiste sur les offres les moins chères du monde dans les années 2011, la filiale d'iliade semble continuer sur leur lancé avec des offres « Pro » intéressantes autant au niveau prix que matériel. Avec des services Anti-ddos et une bande passante de 1Gbp/s ainsi que des possibilités d'amélioration du serveur, Online.net est donc logiquement une valeur sûre dans le domaine des serveurs dédiés. Un chef de projet nous est attribué, les possibilités offertes par les serveurs HP sont vraiment bonnes telle que le ILO !

Amen.fr : Présent notamment sur les noms de domaine et les offres web mutualisées, il se sont ouvert au marché des serveurs dédiés, petit problème Amen ne semble pas communiquer sur les délais d'interventions sur leurs serveurs et le rapport qualité/prix du serveur n'est pas bon, malgré des serveurs Dell qui semblent de bonnes factures. On retiendra qu'ils n'ont pas de solution Anti-ddos transparente et gratuite pour l'utilisateur final et que des IP failover supplémentaires ne sont pas proposés, la sauvegarde est elle aussi oubliée...avec un petit 100Mbps/ maximum sur le serveur, le prix semble donc trop élevé pour un service dérisoire.

Ovh.com : Créée en 1999, la famille Klaba a rapidement envahi l'hexagone avec des datacenters aux quatre coins de la France et aussi à l'international. Des offres de serveurs dédiés complètes avec des gammes diverses et le rapport qualité prix est toujours intéressant malgré le Sold-out de septembre 2013. Une bande passante de 500Mbps/s permet d'avoir un juste milieu entre l'offre de Online et Amen.fr. Les options ne sont pas en reste car elle sont conséquentes telles que les Failovers, le stockage supplémentaire, vrack etc. un très bon choix !

1and1 : Très présent sur le marché des noms de domaine et des serveurs web mutualisés, 1&1 propose désormais des serveurs dédiés plutôt orientés gestion web avec une bande passante de 100 Mbps et avec une administration Plesk Panel 11. Très proche de Amen.fr sur les services disponibles, l'offre est trop pauvre pour espérer se lancer dans une infrastructure VMware, d'ailleurs elle ne propose pas cette solution.

Notre choix : Online.net

Notre comparatif nous a montré la force d'OVH avec un nombre élevé de Datacenter et d'offre, cependant en septembre 2013 l'hébergeur ne nous proposait plus de serveur car ils étaient en Sold Out général.

Des gammes de serveurs dédiés lancés fin juillet (2013) étaient proposés à partir de 2,99 euros. L'hébergeur n'a pas pu tenir ses engagements de livraison, avec les commandes massives (1000serveurs/semaine).

J'en ai personnellement fait les frais ayant moi-même acheté durant cette période trois serveurs, au prix respectif : 2.99€ (k2G), 13€ (k4G) et 42€ (mSP) ,mis à part le second serveur, ils ont tous été livrés plus de 2mois après la commande ce qui a conduit ovh à un SOLD-OUT de septembre(2013) à janvier(2014).

Nous avons décidé d'expliquer la situation à notre client qui souhaitaient se tourner vers ovh et finalement nous avons sélectionné un « Serveur Dedibox MD 2013 » chez Online.net :

Le tarif du serveur est de 64,99€ / mois (HT).



	HP DL120 G7
Processeurs-CPU	XEON E3 1240 @3.3Ghz (4CPU/8Threads)
Mémoire-RAM	24Go
Stockages-DISQUES	2x2To
Puissance-ALIMENTATION	/
PCI-EXPRESS-16X	CARTE RAID1 HP smart Array P410
PCI-EXPRESS-X	CARTE RESEAU x2 en 1Gbit/s

Voici les informations supplémentaires avec la configuration totale de notre serveur :

Supervision du matériel: iLO HP + KVM sur IP

Localisation: Datacenter DC3

Système d'exploitation : VMware ESXi 5.1

Informations complémentaires :

https://www.globalsecuritymag.fr/IMG/pdf/Carte_-_1.pdf

https://www.globalsecuritymag.fr/IMG/pdf/Carte_-_2.pdf

<http://www.1and1.fr/flash/centredcalcul/main.html>

Mise en œuvre

Installation de l'hyperviseur VMware chez online.net

Pour l'installation de notre distribution VMware ESXi 5.1, il nous faut nous rendre sur l'interface du manager disponible à cette adresse : <https://console.online.net>

Nous nous rendons dans l'onglet "Serveur" puis "Etat" et sur le champs "Installer".

Une fois terminé, voici notre serveur prêt à l'usage: (durée de l'installation :10 minutes)

Serveur Dedibox MD 2013 sd-49326

[m] Magic bar (serveur, domaine, IP...)

Etat	Statut
Statistiques	ESXi 5.1.0_HP (64BITS)
Sauvegarde	Niveau de service Niveau de service business
Journaux	Alimentation Up
Ipv6	Nom de la machine nterim Éditer
Failover	Contact abuse kl@es2com.fr Éditer
Plesk	Dernier reboot 2013-10-23 14:28:14
Monitoring	Localisation du serveur Datacenter : DC3 , Salle : 4 , Zone : 4-4 , Rangée : C , Baie : 12 , Bloc : A , Position : 28
Hardware watch	Votre avis Envoyez votre avis maintenant
DNS secondaires	
Infogérance	
Niveau de service & Options	

L'hyperviseur est configuré par défaut avec des prés-réglages réalisés automatiquement par online. Voici les différentes étapes de configuration que nous avons nous aussi réalisées :

- Faire une demande de clé valide et gratuite auprès de VMware.
- Configurer la mise en réseau de VMware et ajout d'une licence.
- Ajouter la solution ISCSI (RPN-SAN) d'Online.net dans l'hyperviseur.

Création de la machine : Vyatta SDN et Windows Serveur 2008R2 avec TSE/Progiciel

Demande de licence gratuite chez VMware

Les demandes se font sur le site officiel de l'éditeur VMware sur le site: <https://my.vmware.com>

Après la création du compte VMware, nous nous rendons dans le menu « downloads » et « all products ». Dans la liste proposée, VMware vSphere Hypervisor (ESXi) devrait être présent :

Product	Release Date	
VMware vSphere Hypervisor 5.1 Update 1	2013-04-25	Download

Une fois redirigé vers le produit, il vous suffit de « scroller » plus bas afin d'obtenir la licence officielle.

Après l'installation du client Vsphere, il suffit ensuite de le lancer et de se connecter à notre serveur ESXi.

Ajouter la licence dans VMware ESXi 5.1

Ajoutons, ensuite la licence VMware gratuite :

dans : /inventaire/configuration/fonction autorisées/Modifier/Affecter une nouvelle licence

Fonctions autorisées

Type de licence ESX Server

Produit: VMware vSphere 5 Hypervisor Autorisé pour 1 CPU physiques (noyaux illimités par CPU)

Clé de licence:

Expire: Jamais

Caractéristiques produits:

Jusqu'à 32 Go de mémoire

Multitraitement symétrique virtuel jusqu'à 8 voies

Comprendre la mise en réseau

La mise en réseau virtuelle est très importante dans tous types d'hyperviseurs.

Il est important de connaître les termes techniques avant de se lancer dans la mise en réseau :

- Un réseau virtuel (Vnetwork)

Un réseau virtuel est un réseau de machines virtuelles fonctionnant sur une machine physique.

Elles sont connectées entre elles comme sur un réseau physique standard.

Les machines virtuelles (VM) peuvent être ajoutées dans plusieurs réseaux virtuels.

- Le commutateur standard virtuel (Vswitch)

Un vSwitch peut être connecté à un ou plusieurs commutateurs physiques.

Un commutateur virtuel se comporte de la même façon qu'un Switch traditionnel.

Vous avez la possibilité de lui affecter une ou plusieurs cartes réseaux.

Par contre, un Vswitch ne dispose pas de fonctionnalités avancées comme sur un switch physique!

- Les groupes de ports dans un commutateur standard virtuel

Les groupes de port dans un commutateur virtuel permettent au VM de s'interconnecter.

Les ports sur les Vswitch sont identiques aux ports des switches physiques et peuvent être managés.

Par défaut il y a 120 ports disponibles par Vswitch, soit autant de VM possibles à connecter.

- Un réseau VMkernel

Une interface réseau VMkernel est utilisée pour vMotion, le stockage IP et Fault Tolerance.

C'est un groupe de ports dédié à la gestion de notre hôte.

La mise en réseau dans VMware ESXi 5.1

Nous allons utiliser deux autres Vswitch en plus du Vswitch0 et créer des groupes de ports. Le Vswitch1 utilisera donc quatre VLANS : 10,20,30 et 4095 et sera reparti comme ceci :

- VLAN10 : VM – Windows serveur 2012 (Adressage 192.168.10.0/24)
- VLAN20 : VM – Debian (Adressage 192.168.20.0/24)
- VLAN30 : Future machine pour le site web (Adressage 192.168.30.0/24)
- VLAN-tous : VM – Vyatta (Tous)

Le Vswitch2 utilisera la carte réseau en 100mbp/s pour la connexion RPN-SAN (ISCSI)

La mise en réseau de VMware se trouve dans "configuration" et "mise en réseau".

Pour ajouter : un Vswitch ou un Vmkernel, il faut cliquer sur "Ajouter une mise en réseau"

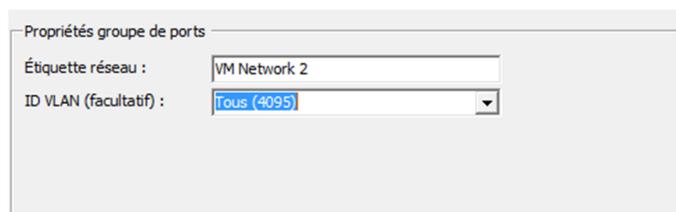
[Actualiser](#) [Ajouter une mise en](#) [Propriétés...](#)

Nous sélectionnons ensuite le type de réseau soit :

- Virtual Machine pour créer un nouveau vNetwork contenant des VM.
- VMKernel pour les services ESX(i): vMotion, iSCSI, NFS, ...

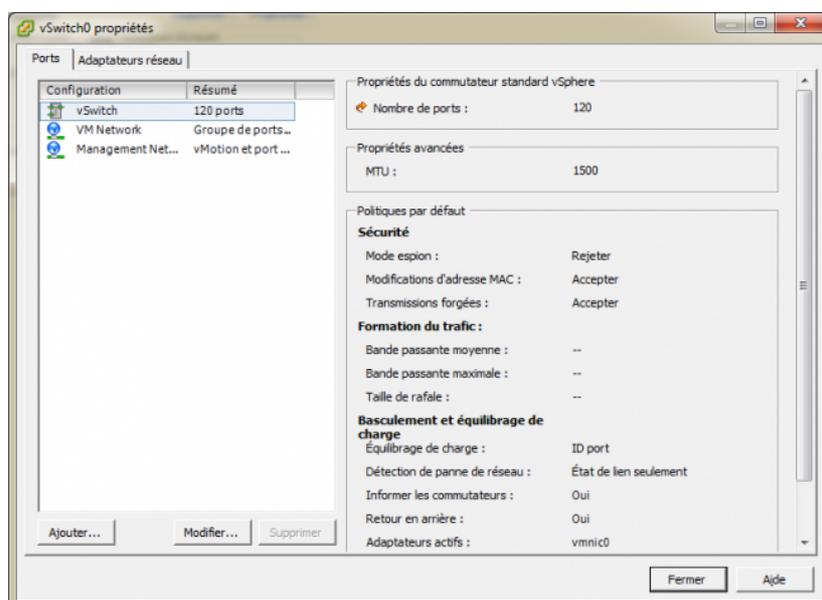
Choisissez maintenant sur quel vSwitch ce vNetwork doit être connecté.

Pour le 1er nous allons sélectionner un VLAN ID de 4095 :



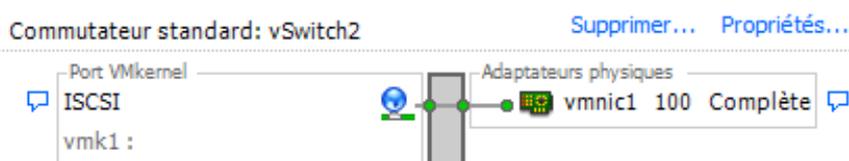
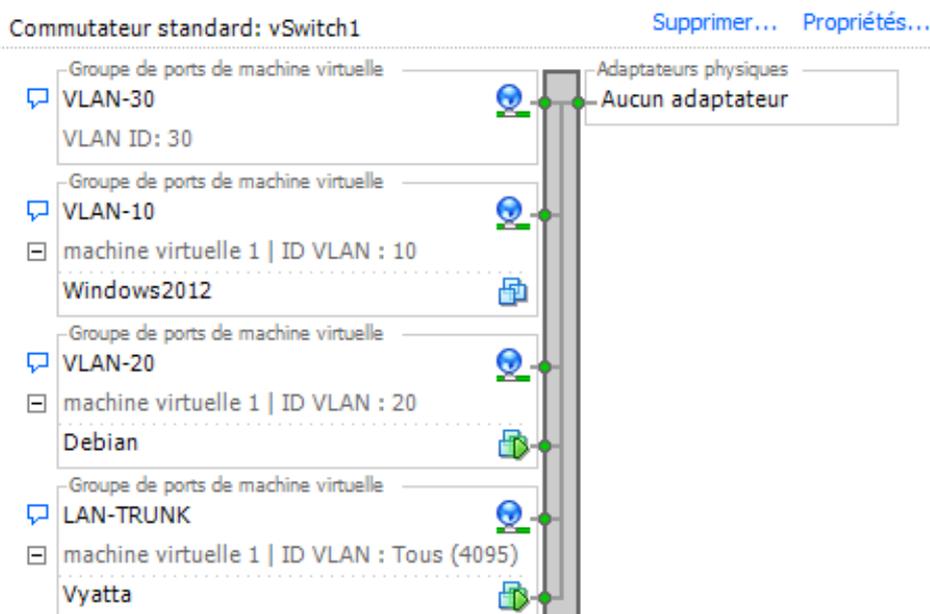
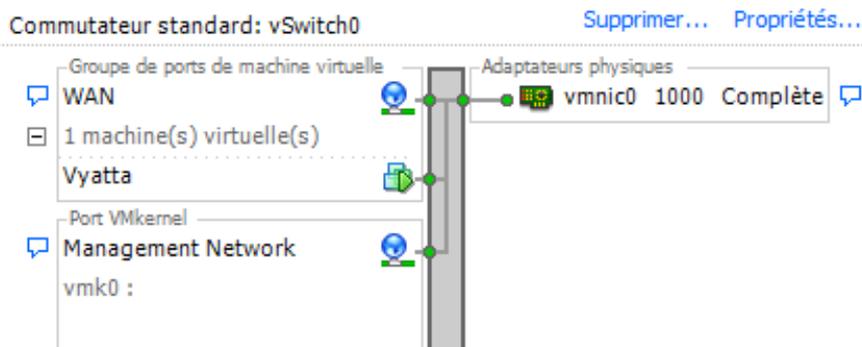
Pour modifier un Vswitch existant, cliquez sur "Propriétés" en haut à droite de celui ci.

Vous pouvez changer le nombre de ports sur un switch, configurez un VLAN sur un réseau, etc...



Nous reproduisons autant de fois la manipulation pour obtenir notre réseau virtuel final.

La mise en réseau de notre hyperviseur



Remarque : Vyatta utilise une seule carte réseau virtuelle fournie par l'hyperviseur dans son LAN !
Nous pouvons envoyer des trames dans les 4095 Vlans, il suffit maintenant de taguer nos trames.
On économise nos cartes réseaux virtuelles fournies pas l'hyperviseur VMware !

Pour des raisons de confidentialité nous avons enlevé les adresses IP de VMk0 et VMK1.

La solution du ISCSI RPN-SAN de online.net

Le RPN-SAN est une solution de stockage en mode block, axée performances et disponible en iSCSI au travers du réseau RPN. Vous pouvez utiliser les LUN iSCSI RPN-SAN directement sur vos machines virtuelles (compatible VMWare) : Nous allons utiliser cette solution pour faire des sauvegardes de la VM.

Les étapes de la configuration :

1. Création et configuration d'un VMKERNEL pour ISCSI.
2. Profil de sécurité ESXi pour activation de SSH.
3. Édition du fichier /etc/vmware/esx.conf
4. Connaître la gateway de votre RPN-SAN.
5. Finalisation de la configuration VMKERNEL pour ISCSI.
6. Configuration l'adaptateur de stockage.
7. Ajout du stockage LUN.

Présentation de L'ISCSI :

ISCSI est un protocole de stockage en réseau basé sur le protocole IP.

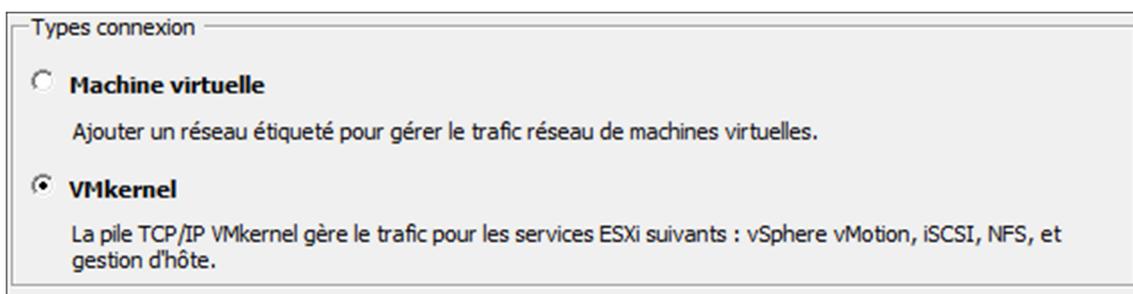
Il est économique comparé aux autres technologies : Fibre Channel et SAS.

ISCSI permet de relier et de gérer du stockage qu'il présente via le réseau à des hôtes sur le LAN.

Notre ESXi aura l'illusion que le stockage est local ! Mais il est bien distant et sur un SAN.

La configuration du ISCSI RPN-SAN de online.net

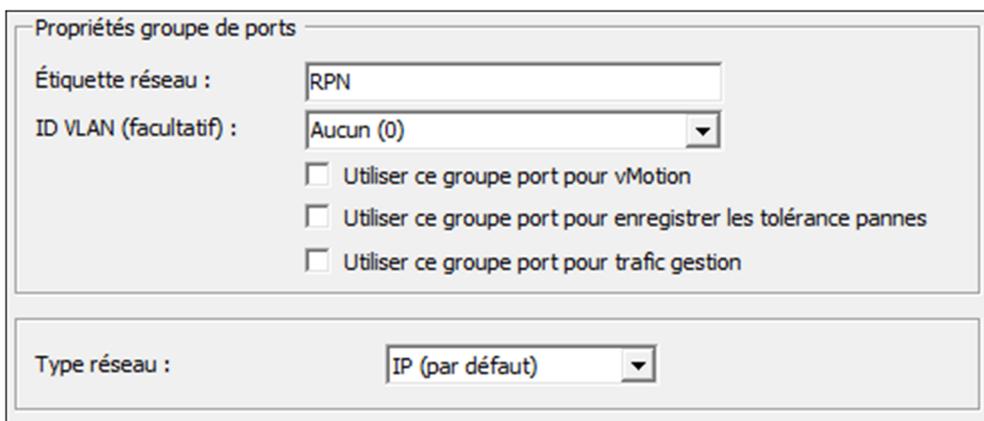
Il faut se rendre dans notre interface de gestion ESXi via Vsphere client puis, dans l'onglet de configuration sélectionner "mise en réseau" et ajouter "mise en réseau Vmkernel" :



Choisir la carte réseau vmnic 1 (100mb/s) :

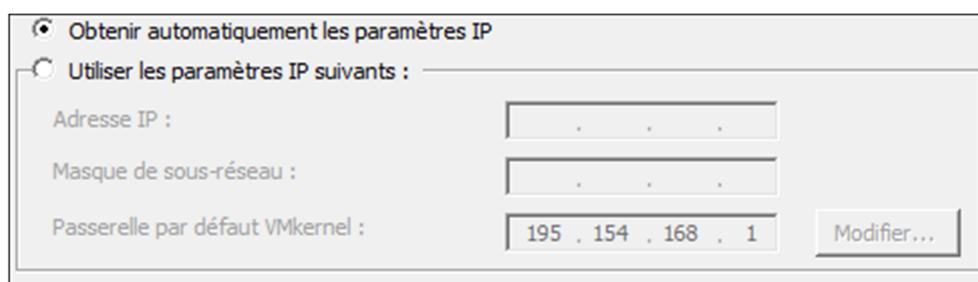
<input type="radio"/> Créer un commutateur standard vSphere	Vitesse	Réseaux
<input type="radio"/> Utiliser vSwitch0	Vitesse	Réseaux
Intel Corporation 82574L Gigabit Network Connection		
<input type="checkbox"/> vmnic0	1000 Complète	
<input type="radio"/> Utiliser vSwitch1	Vitesse	Réseaux
<input checked="" type="radio"/> Utiliser vSwitch2	Vitesse	Réseaux
Intel Corporation 82574L Gigabit Network Connection		
<input checked="" type="checkbox"/> vmnic1	100 Complète	0.0.0.1-255.255.255.254

Renommer le groupe de port en : "RPN" (recommandé par online.net)



Paramètres de connexion en "IP automatique" :

Ceci est du à une "configuration Dynamique" que nous lui affecterons plus tard.

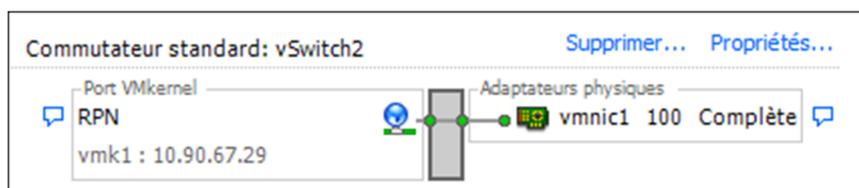


L'étape suivante nous permet de terminer notre mise en réseau de notre VMKERNEL (RPN).

Notre carte réseau n'est pas activée ! (une petite croix apparaît) dans la mise en réseau, c'est normal! Ceci est lié à la sécurité interne chez online.net (mac non reconnu)

La négociation MTU entre vswitch et RPN-SAN dans "la mise en réseau" :

Sur la configuration de votre vswitch2, cliquez sur "propriétés" :



Sur le Vswitch2 double clic puis "onglet général" ,modifiez le MTU à la valeur : "9000" .

Sur le RPN double clic puis "onglet général" ,modifiez le MTU à la même valeur : "9000".

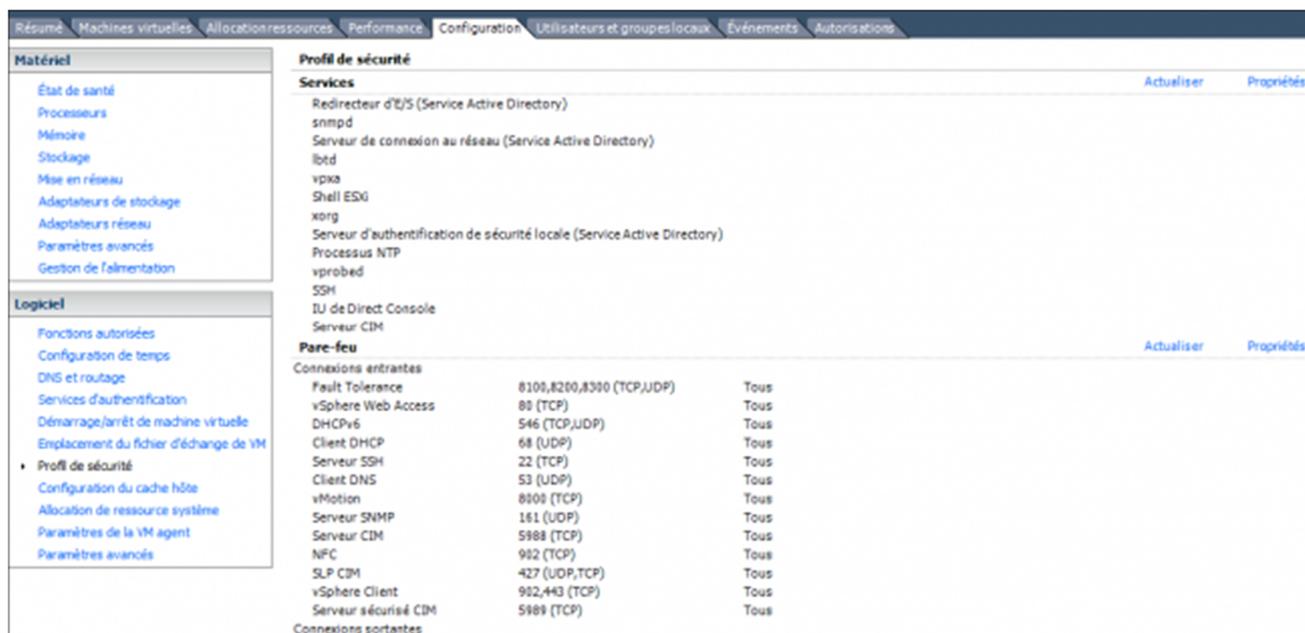
Nous validons les changements par "valider".

Cela permet au vswitch de négocier des paquets IP de la même longueur que le RPN-SAN.

Plus d'informations sur MTU : [wikipedia](https://fr.wikipedia.org/wiki/MTU)

Profil de sécurité : activation du SSH

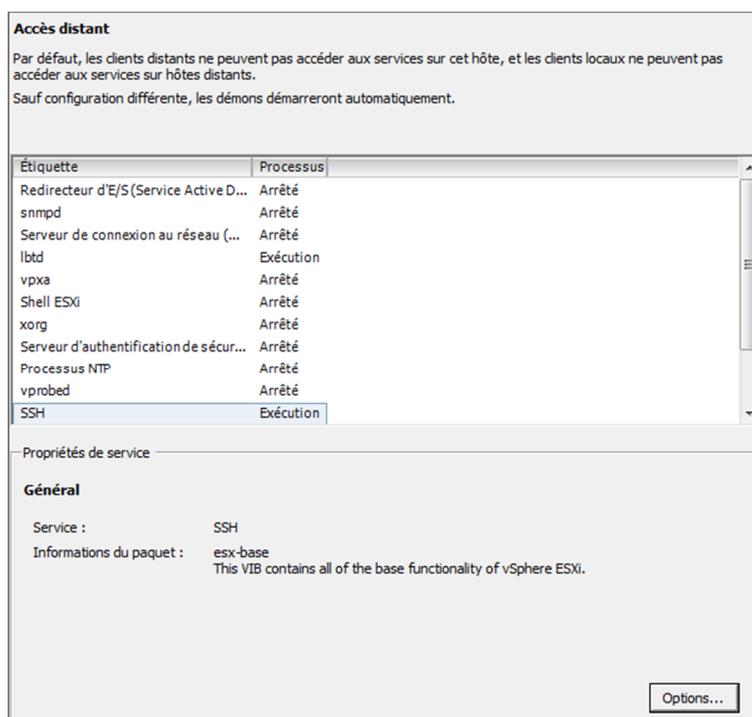
Toujours dans l'onglet configuration puis le dans panel de gauche 'logiciel' et "profil de sécurité".
Activation du protocole SSH dans le pare-feu ESXi :



The screenshot shows the ESXi configuration interface with the 'Configuration' tab selected. The left sidebar shows the 'Logiciel' (Software) section, with 'Profil de sécurité' (Security Profile) selected. The main area displays the 'Profil de sécurité' settings, including 'Services' and 'Pare-feu' (Firewall). The 'Pare-feu' section is expanded, showing a list of services and their firewall rules. The 'SSH' service is highlighted, and its status is 'Exécution' (Running).

Connexions entrantes	Port	Protocole	État
Fault Tolerance	8100,8260,8300	(TCP,UDP)	Tous
vSphere Web Access	80	(TCP)	Tous
DHCPv6	546	(TCP,UDP)	Tous
Client DHCP	68	(UDP)	Tous
Serveur SSH	22	(TCP)	Tous
Client DNS	53	(UDP)	Tous
vMotion	8000	(TCP)	Tous
Serveur SNMP	161	(UDP)	Tous
Serveur CIM	5988	(TCP)	Tous
NFC	992	(TCP)	Tous
SLP CIM	427	(UDP,TCP)	Tous
vSphere Client	902,443	(TCP)	Tous
Serveur sécurisé CIM	5989	(TCP)	Tous
Connexions sortantes			

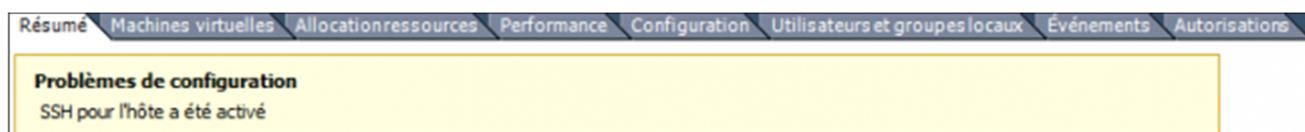
Nous cliquons sur : "propriétés" du pare-feu, une fenêtre apparaît :



The screenshot shows the 'Accès distant' (Remote Access) dialog box. The 'SSH' service is selected in the list, and the 'Options...' button is visible at the bottom right.

Étiquette	Processus
Redirecteur d'E/S (Service Active D...	Arrêté
snmpd	Arrêté
Serveur de connexion au réseau (...)	Arrêté
lbt	Exécution
vpva	Arrêté
Shell ESXi	Arrêté
xorg	Arrêté
Serveur d'authentification de sécur...	Arrêté
Processus NTP	Arrêté
vprobed	Arrêté
SSH	Exécution

Nous sélectionnons "SSH" puis "options" et la règle : "Démarrer et arrêter avec hôte" :
Pour vérifier le lancement de notre serveur SSH, allons dans l'onglet "Résumé" :



The screenshot shows the ESXi configuration interface with the 'Résumé' (Summary) tab selected. A yellow banner at the top indicates 'Problèmes de configuration' (Configuration Issues) and 'SSH pour l'hôte a été activé' (SSH for the host has been activated).

Nous pouvons désormais accéder à la console de notre hyperviseur par SSH pour continuer la configuration de notre ISCSI RPN-SAN fourni pas online.net.

La configuration du ISCSI RPN-SAN de online.net (suite)

Édition du fichier /etc/vmware/esx.conf

Maintenant il faut éditer le fichier de configuration ESXi afin de copier la mac adresse du portgroup RPN dans la mac du VMKERNEL RPN afin qu'elles soient identiques.

Éditons notre fichier esx.conf : `vi /etc/vmware/esx.conf`

Trouvons le numéro de child du portgroup RPN : `/net/vmkernelnic/child[0001]/portgroup = "RPN"`

Trouvons l'adresse mac de la carte réseau reliée au RPN correspondant :

`/net/pnic/child[0001]/mac = "X0:X0:X0:X0:X0:X0"`

Remplaçons la MAC du VMKernel RPN avec la MAC de la carte réseau reliée au RPN :

`/net/vmkernelnic/child[0001]/mac = "X0:X0:X0:X0:X0:X0"`

Pour que les changements soit effectifs, il faut redémarrer notre serveur ESXi.

Connaître la gateway de notre RPN-SAN

Online.net ne communique pas la gateway de notre RPN-SAN, nous devons la calculer!

Pour cela il nous faudra, par exemple une machine sous linux et installer "ipcalc".

Installation du paquet "ipcalc" : `apt-get install ipcalc`

Il nous suffit ensuite de calculer votre gateway comme ceci : `ipcalc -b [IP_RPN-SAN]/26 | grep HostMin`

La résultat de la commande nous renvoie la gateway : `HostMin: X.X.X.X`

La gateway ne ping pas ? Ceci est un comportement normal chez online.net.

Finaliser la configuration VMKERNEL-ISCSI

La dernière étape consiste à utiliser cette gateway afin de communiquer avec le RPN-SAN.

Vérifions nos routes sous ESXi : `esxcfg-route -n`

```
Neighbor MAC Address Interface Expiry
XXX.XXX.XXX.1 X2:X2:X2:X2:X2:X2 vmk0 19m55s
```

Si nous avons déjà la seconde route (qui se présente sous cette forme) :

```
Neighbor MAC Address Interface Expiry
X.X.X.X X0:X0:X0:X0:X0:X0 vmk1 18m14s
```

Alors notre route est déjà configurée et l'étape suivante ne nous concerne pas !

Sinon , cette étape ci dessous peut nous concerner !

Ajoutons la route pour le sous-réseau RPN via la gateway RPN :

`esxcfg-route -a 10.90.0.0/16 [IP_RPN-SAN]`

Pour vérifier que la route est correcte, un test ping suffit sur le RPN-SAN :

```
# ping san-1.rpn.online.net
PING 10.90.254.2 (10.90.254.2): 56 data bytes
64 bytes from 10.90.254.2: icmp_seq=0 ttl=61 time=0.241 ms
64 bytes from 10.90.254.2: icmp_seq=1 ttl=61 time=0.241 ms
```

Configuration de l'adaptateur de stockage

Dans l'onglet de configuration de notre ESXi : "adaptateurs de stockage" et "ajouter" puis choisir : "Software iSCSI Adapter" et terminé avec "ok".

Cliquons ensuite sur "Software Adapter" nommé "vmhba32" :

Périphérique	Type	W...
iSCSI Software Adapter		
vmhba32	iSCSI	iq...
Smart Array P410		
vmhba0	Bloquer le SCSI	

Cliquer sur "vmhba32" puis en bas a droite sélectionner : "propriété".

Se rendre dans l'onglet "découverte dynamique" pour lui attribuer une adresse IP!

Cliquer sur "ajouter" et inscrire dans "Serveur iSCSI" : san-1.rpn.online.net (voir ci-dessous) :

Emplacement serveur iSCSI
san-1.rpn.online.net:3260

Confirmer un rebalayage afin de voir votre périphérique et votre chemin iSCSI !

Finalement le disque IET apparaît :

vmhba32

Modèle : iSCSI Software Adapter
Nom iSCSI : ign
Alias iSCSI :
Câbles connectés : 1 Périphériques : 1 Chemins : 1

Afficher : Périphériques Chemins

Nom	Nom exécution	État opérationnel	LUN	Type	Type de lecteur	Transport	Capacité	Propriétaire	Accélération matérielle
IET iSCSI Disk (t10.945445000000...	vmhba32:C0:T0:L0	Monté	0	disk	Non SSD	iSCSI	1,00 To	NMP	Inconnue

Ajouter le RPN-SAN dans un stockage LUN

Dans l'interface vsphere et onglet de configuration aller dans : "stockage" puis "ajouter stockage" et cochez "Disque/LUN" :

Type de stockage

Disque/LUN
Créer banque de données sur Fibre Channel, iSCSI, ou un disque SCSI local, ou monter volume VMFS existant.

Système de fichiers réseau
Choisir cette option si vous voulez créer un système de fichiers réseau.

Ajouter une banque de données sur Fibre Channel ou iSCSI l'ajoutera à tous les hôtes ayant accès aux supports stockage.

Ensuite sélectionnons notre nouveau stockage RPN-SAN via iSCSI :

Nom, Identifiant, ID chemin, LUN, Capacité, Extensible ou Étiquette V...		Effacer			
Nom	ID ...	LUN	Type de lecteur	Capacité	Étiquette VM...
IET iSCSI Disk (t10.945445000000...	iqn...	0	Non SSD	1,00 To	

Cochez le système de fichier VMFS-5 puis on retrouve le périphérique iSCSI :

Partitions principales	Capacité
✓ VMFS (IET iSCSI Disk (t10.9454450...	1024,00 Go

Ensuite, ajoutons un nom de banque de données par exemple : datastore-ISCSI

Formatons, le disque disponible au maximum de sa capacité !

Terminons l'ajout de notre stockage LUN par liaison ISCSI puis validons par "Terminer" !

Au final notre LUN est disponible dans notre ESXi !

Banques de données

Identification	Périphérique	Type de lecteur	Capacité	Libre	Type	Dernière mise à jour	Accélération matérielle
datastore1	HP Serial Attached SCSI Disk...	Non SSD	1,81 To	1,65 To	VMFS5	23/10/2013 21:45:53	Inconnue
datastore-ISCSI	IET iSCSI Disk (t10.945445...	Non SSD	1 023,75 G	1 022,80 G	VMFS5	23/10/2013 21:45:55	Inconnue

Nous avons terminé la configuration de notre ISCSI RPN-SAN fournie par Online.net !

Pour plus d'informations la documentation officielle est disponible à l'[adresse](#) suivante.

Présentation des différentes VMs

VM – 1 : Vyatta

La VM logiciel de Vyatta nous servira de routeur/pare-feu et s'intègre parfaitement dans l'environnement virtualisé car elle centralise tous les flux réseaux.

Voici les différentes étapes de configuration :

1. Configuration de 2 interfaces (WAN-LAN)
2. Ajout des routes vers notre ESXi (Gateway)
3. Configuration des règles de NAT (WAN-LAN et LAN-WAN)

Le but de la machine est de filtrer et de protéger notre réseau privé du réseau internet.

VM – 2 : Microsoft Windows 2008R2

La machine Windows sera utilisée uniquement pour une connexion bureau à distance.

Le serveur contiendra trois progiciels de gestion d'interiminaire et d'un antivirus.

Une dizaine d'utilisateurs seront connectés chaque jour.

Mon employeur m'a donné les consignes suivantes :

Espace de stockage de : 1To

Mémoire RAM : 8Go

Processeur : 1Vcpu

Antivirus : Panda security

Workgroup : SERVEUR.SETT.FR

L'installation de Windows 2008R2 ne sera pas détaillée ni la configuration réseau statique.

Voici les différentes étapes que nous allons détaillées :

L'ensemble des mises à jour de Windows seront effectuées avant les étapes 1 à 3

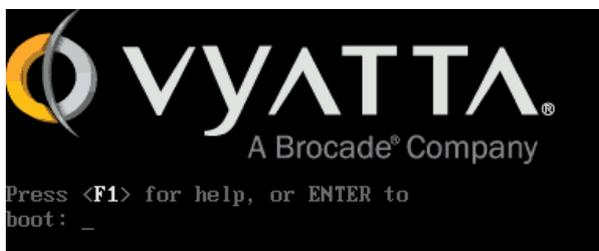
1. Ajout du rôle : Service bureau à distance.
2. Ajout des utilisateurs.
3. Installation des progiciels et administration de base.

Installation et configuration de la VM : VYATTA

L'installation de Vyatta

Lancement du boot sur Vyatta avec la touche : Entrée

Par défaut le login et le mot de passe sont vyatta et la configuration du clavier est en qwerty.



Pour lancer l'installation de Vyatta : `install-system`

Ensuite il y a 3 questions très simple et auxquelles il vous faut répondre par choix multiples.

La configuration de Vyatta

Configuration des interfaces :

```
set interfaces ethernet eth0 address X.X.X.X/X
set interfaces ethernet eth0 description WAN
set interfaces ethernet eth1 address 192.168.1.1/24
set interfaces ethernet eth1 description LAN
```

Ajout de résolution DNS

```
set system name-server 88.191.253.51
```

Mise en place de route statique et de la passerelle :

```
set protocols static interface-route X.X.X.X/X next-hop-interface eth0
set system gateway-address X.X.X.X/X
```

Pool DHCP pour réseau local

```
set service dhcp-server shared-network-name pool_lan1
set service dhcp-server shared-network-name pool_lan1 subnet 192.168.1.0/24 start
192.168.1.10 stop 192.168.1.15
set service dhcp-server shared-network-name pool_lan1 subnet 192.168.1.0/24 default-
router 192.168.1.1
set service dhcp-server shared-network-name pool_lan1 subnet 192.168.1.0/24 dns-server
88.191.253.51
```

Connexion du réseau local à internet (NAT)

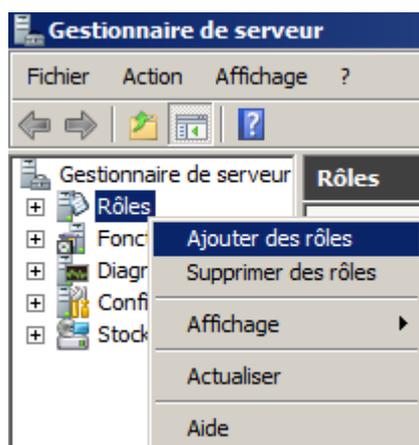
```
set nat source rule 10 source address 192.168.1.0/24
set nat source rule 10 outbound-interface eth0
set nat source rule 10 translation address masquerade
```

Configuration 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 172.168.0.10
set vpn pptp remote-access client-ip-pool stop 172.168.0.15
set vpn pptp remote-access authentication local-users username jeremie password p4ssw0rd
```

Configuration de la VM : Windows 2008R2

Installation du rôle : Services Bureau à distance sous Windows 2008R2 :



Ensuite nous allons sélectionner : Services Bureau à distance avec les choix suivants :

- Hôte de session Bureau à distance
- Hôte de virtualisation des services Bureau à distance
- Services de base
- RemoteFX
- Gestionnaire de licences des services Bureau à distance

Continuons, la suite de l'installation du rôle se passe comme ceci :

- Exiger l'authentification au niveau du réseau.
- Configurer les licences ultérieurement.
- Groupe d'administrateur : Administrateur et Utilisateur local.
- Expérience client : [X] Audio et Vidéo [X] Redirection Audio [X] Windows AERO.
- Aucune étendue de gestionnaire de licence.
- Redémarrage du serveur.

Nous allons activer les licences bureau à distance, pour cela il nous faut nous rendre dans :

“outils d'administration/services de bureau à distance/gestionnaire de licences des services bureau à distance”

Pour activer le serveur de licences

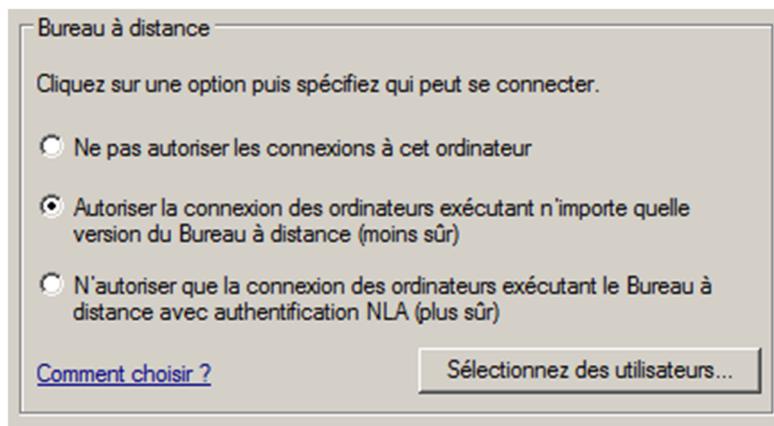
1. Cliquer sur Démarrer, cliquer sur Outils administratifs, cliquer sur Services Terminal Server puis, dans Outils avancés, et Gestionnaire des services bureau à distance.
2. Cliquer avec le bouton droit sur le serveur de licences que nous souhaitons installer, puis sur Activer le serveur. L'Assistant Activation du serveur s'ouvre.
3. Nous cliquons sur Suivant.
4. Dans la page Méthode de connexion, sous Méthode d'activation, nous choisissons Connexion automatique (recommandé), puis cliquer sur Suivant.
5. Cliquer sur Suivant. Le serveur de licences est activé.

6. Dans la page Fin de l'Assistant Activation du serveur, effectuer l'une des opérations suivantes :
- Pour installer des licences d'accès client aux services Terminal Server sur le serveur de licences, vérifier si la case à cocher Démarrer l'Assistant Installation de licences est activée, cliquer sur Suivant, puis suivre les instructions.
 - Pour installer les licences d'accès client ultérieurement, désactiver la case à cocher Démarrer l'Assistant Installation de licences, puis cliquer sur Terminer.

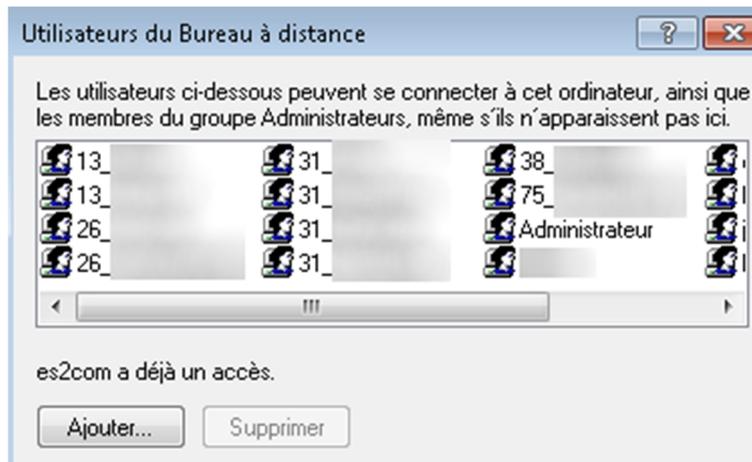
Ensuite, nous avons créer des utilisateurs locaux et nous les avons ajoutés dans des groupes d'utilisateurs.

Voici la méthode pour autoriser une connexion Bureau à distance aux utilisateurs :

Démarrer/Ordinateur/(clique droit) Propriétés/Paramètre système avancée/Utilisation à distance/



Nous allons maintenant cliquer sur "sélectionner des utilisateurs" et les ajouter.... voici le résultat :



Les logins ont été "flouter" pour la confidentialité des accès de nos clients.

Le progiciel Tempo :

Les progiciels utilisés par notre client : Sett-interim sont développés par la société : pldiffusion. C'est les équipes techniques de PLD qui ont pris la main à distance pour l'installation sur serveur.

Les logiciels : Tempo, Mikado, Banco sont édités par la société PL.Diffusion. Les entreprises de travail temporaire (ETT) doivent faire face à des contraintes et des évolutions permanentes. Tempo est un outil de pilotage d'activité interim: personnel, client, devis, planning, facturation, paie et analyse en temps réel.

Un exemple avec le logiciel : TEMPO

Tempo est un logiciel conçu pour Windows Serveur (2003, 2008, 2012) et est écrit en WinDEV.

Par défaut il s'installe dans C : et l'ensemble de sa structure est présente dans C:/tempo.

Dans la gestion de la base de données faite avec Hyperfile ,on retrouve les fichiers suivants :

- « .fic » la Database ; (C:/Interim/Pld)
- « .mmo » le Bloc d'image
- « .ndx » l'index (organisation de la structure)

Nous pouvons restaurer une base qui dysfonctionne seulement si le .fic est encore disponible.

Pour information, il n'y a aucun parent dans les tables, donc le nom du client revient sans cesse.

Tempo fonctionne uniquement avec des services Microsoft (Windows) et n'a pas d'API développées.

L'administrateur du progiciel tempo

Les outils d'administrations sont disponibles suivant le compte qui lance la session Windows.

L'interface est vraiment sur utilisée, et il y a bien trop d'icônes ,le plus simple est d'encore d'utiliser les menus et sous menus : fichier, intérimaires, attestations, clients, contract etc....

La plupart du temps nous seront amenés à utiliser le menu « outils » et sous menu suivant :

- Sauvegarde de la base
- Impression defectueuse

Version actuelle de tempo avec l'accès à l'administrateur « es2com » au dossier SETT81

Utilisateur : ES2CDM Droits : _ADMIN Dossier : SETT81 / Licence : Sett / Version du 23/01/2014 à 17h54 en 32Bits

La sauvegarde sera effectuée manuellement (dans l'attente d'une solution automatique) dans le menu « fichier » et sous menu « sauvegarde » :

Tempo c:\interim\plde7\
 SETT81=222 Mo TempoDoc

Avec index Serveur Samba Pour Portable

- Destination... c:\SvgTempo\
Sauvegarder les SvgPaie (Dern:30/01/2014)
Sauvegarder les Pdf

Sauvegarde datée
 Crypté Non crypté
Sett

L'ensemble des fichiers de sauvegarde se trouve à l'emplacement suivant : <C:/Interim/>

L'impression des contrats se trouve dans : (contrats et paramètres impression)

Les processus importants sont :

- Le processus de PLD Tempo est : pldint71.exe
- Le processus de PLD Benco est : pldpay71.exe
- Le processus de PLD Mikado est : pldcpt71.exe

Nous avons quelques éléments de dépannage fournis par notre client afin de gérer ce progiciel.

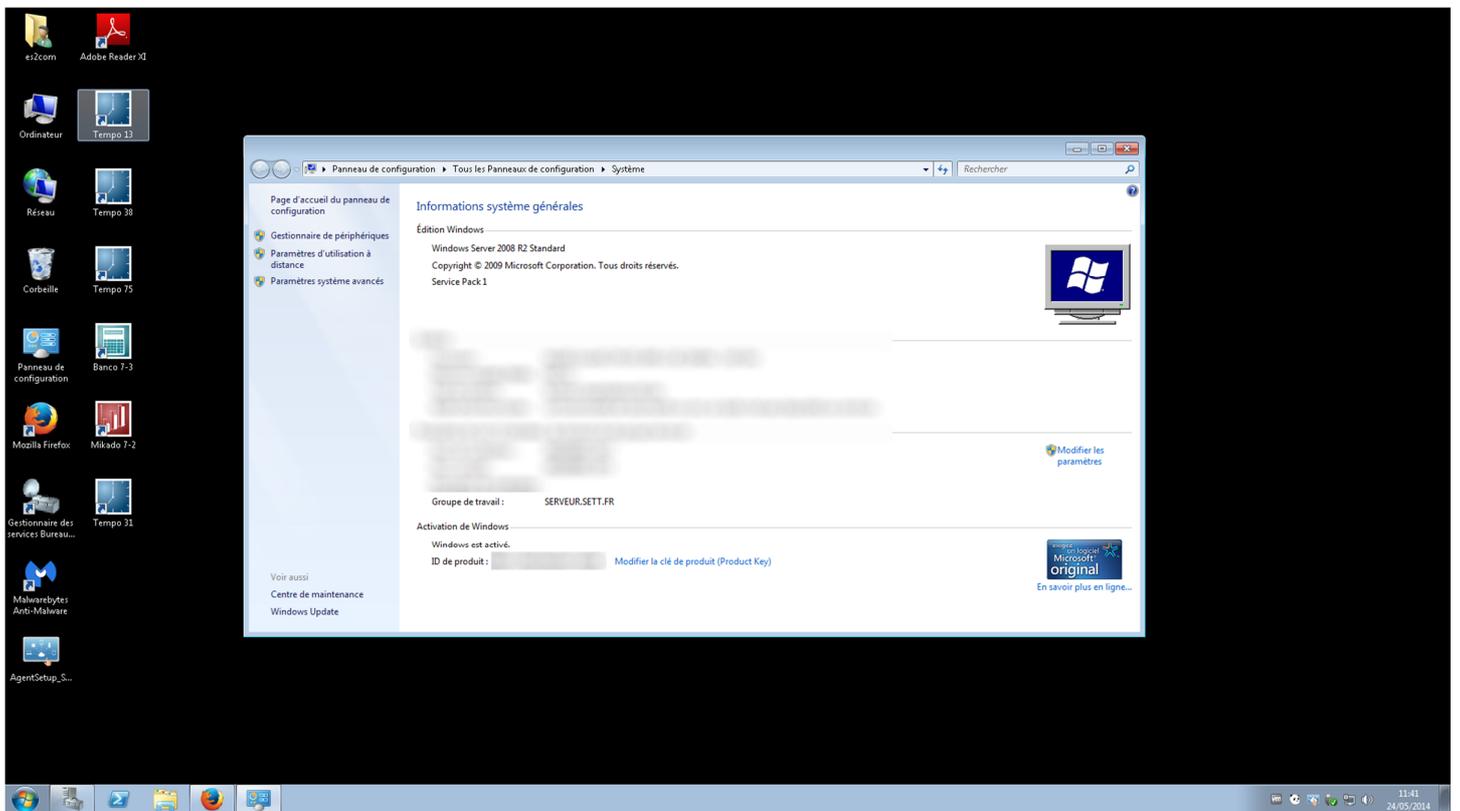
Si nous rencontrons des problèmes ,nous contactons directement l'éditrice du logiciel sur :

<http://www.pldiffusion.fr/>

Mise en production de l'infrastructure

Avant de terminer notre projet nous effectuons un test de connexion bureau à distance, une fois loggué en VPN.

Nous allons simplement utiliser l'outil : connexion bureau à distance d'un windows desktop 8.1 :



Le serveur est fonctionnel en RDP après la connexion VPN, les progiciels et l'ensemble du système fonctionne.