PPE 3

Samy Lefebvre Eva gonzalez

Francois beck Aziz ouattara

BTS SIO 2.2

**Sommaire**

1. **Présentation**
2. **Administration système**
   1. Mission 1 : Mise en place d’un serveur de déploiement multi-images
   2. Mission 2 : Mise en place d’un serveur d’application
   3. Mission 3 : Mise en place d’outils de gestions de par cet d’incidents
3. **Administration réseau**
   1. Mission 1 : Service d’accès sécurisé Internet – DMZ
   2. Mission 2 : Service d’administration à distance sécurisée
   3. Mission 3 : Service de haute disponibilité
4. **Economie Management**
5. **Droit**
6. **Présentation**

La *Maison des Ligues* (La M2L), établissement du Conseil Régionalde Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d’autres structures hébergées. La M2L, comme vous le constaterez dans l’interview avec son responsable, doit fournir les infrastructures matérielles, logistiques et des services à l’ensemble des ligues sportives installées.

Pour assurer le développement du système éducatif sportif de la région Lorraine et des offres aux usagers, le conseil régional et la direction de la M2L ont décidé de développer des services et des capacités d’hébergement pour les ligues sportives.

La M2L comprend plusieurs départements et son organisation lui permet de répondre aux exigences de la région pour assurer l’offre de services et de support technique aux différentes ligues déjà  implantées (ou à venir) dans la région.

1. **Administration système**
   1. Mission 1 : Mise en place d’un serveur de déploiement multi-images

*Windows Deployement Service*

Introduction

Windows Deployment Services a été introduit avec Windows Server 2008 afin de remplacer le « vieillissant » RIS. WDS fournit un système de déploiement automatisé afin de distribuer des images systèmes via le réseau. Grâce à lui il est possible de déployer rapidement un parc informatique.

WDS se base sur de nombreux services Windows. Aussi il convient de maîtriser les services Windows tels qu’Active Directory et DHCP.

Qu’est-ce que WDS ?

* WDS (Windows Deployment Service) est une solution de masteurisation proposée par Microsoft.
* Lors d’un déploiement conséquent comme (installation de système d’exploitation sur plusieurs postes d’une société par exemple), il serait très long d’envisager installer un à un le système d’exploitation voulu sur chaque poste. D’où le besoin d’utilisation de solution tel que WDS, qui consiste au déploiement de système d’exploitation sur plusieurs postes en même temps.
* Le service WDS fonctionne depuis un serveur. Sur les différents systèmes Windows Server (2003, 2008,…) par exemple, le service est proposé à l’installation directement dans le gestionnaire de serveur comme l’installation d’un service classique (DNS, DHCP,…).
* Les composants incluent un serveur PXE (Preboot Execution Environment) et un serveur TFTP (Trivial File Transfer Protocol) pour le démarrage réseau d’un client dans le but de charger et d’installer un système d’exploitation. Un dossier partagé et un référentiel d’images sont également inclus ; ils contiennent les images de démarrage, les images d’installation et les fichiers dont vous avez besoin spécifiquement pour le démarrage réseau.

Services obligatoires pour l’installation de l’agent WDS

* AD DS

Un serveur des services de déploiement Windows doit être membre d’un domaine AD DS. Permettant de s’identifier pour poursuivre l’installation via le réseau.

* DHCP

Vous devez posséder un serveur DHCP puisque les services de déploiement Windows utilisent l’environnement d’exécution de pré-démarrage (PXE) qui s’appuie sur le protocole DHCP pour l’adressage IP.

* DNS

Vous devez posséder un serveur DNS pour exécuter les services de déploiement Windows.

* Volume NTFS

Le serveur qui exécute les services de déploiement Windows nécessite un volume du système de fichiers NTFS pour le magasin d’images.

* Avantage/Inconvenant

Avantages :

◊ Déploiement et sauvegarde via le réseau

◊ Déploiement Windows 7 personnalisable

◊ Solution relativement rapide

◊ Service sécurisé

◊ Automatisation (XML), MDT 2012

◊ Gestion centralisé des images

◊ Gestion des pilotes

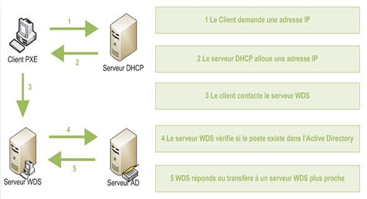
◊ Service entièrement gratuit

Inconvénients :

◊ Coût du serveur

◊ Parc homogène

◊ Configuration réseau pouvant poser problème sur certaine topologie



Installation et configuration du serveur

* Pré requis

Avant de commencer, il est nécessaire de disposer d’une version de Windows Server 2008 R2 Entreprise. Notre solution sera réalisé via le logiciel de virtualisation qui est "VirtualBox".

Pour cette installation, il faut 2 serveurs membres du même domaine et une machine cliente sans système d’installé :

* SRV-AD : Serveur Contrôleur de domaine (net.lan) Active Directory/DNS/DHCP
* SRV-WDS : Serveur Contrôleur de domaine secondaire (net.lan) Active Directory/Service

    WDS/Framework 3.5

* PC-CLIENT : poste accueillant les images systèmes personnalisées
* Configuration réseau TCP/IP :
* SRV-AD : 172.16.2.61
* SRV-WDS : 172.16.2.58
* PC-CLIENT : IP Dynamique (DHCP)

Logiciels à se munir :

*Microsoft Deployment Toolkit :*

Microsoft Deployment Toolkit (MDT) est un ensemble complet d'outils et de recommandations qu'en qualité de partenaire Microsoft, pouvez utiliser gratuitement. MDT propose une partie des ressources à tous, comprenant un ensemble complet d'outils et de recommandations qui facilitent les déploiements à grande échelle sur les postes de travail et les serveurs.

Avantages et fonctionnalités :

◊ Accélérer et automatiser les déploiement du système d'exploitation Windows 7 ou Windows Server, de Microsoft Office 2010 et des autres produits Microsoft ;

◊ Réduire la durée de déploiement grâce à des images de poste de travail et de serveur standardisées ;

◊ Utiliser la détection de plateforme (32 ou 64 bits) automatique pour assurer le déploiement des pilotes pris en charge;

◊ Permettre aux utilisateurs finaux d'initier et de personnaliser le déploiement à l'aide d'un Assistant simple d'utilisation dans Microsoft System Center Configuration Manager ;

◊ Automatiser entièrement les déploiements d'installation sans aucune intervention en utilisant System Center Configuration Manager 2007 Service Pack 2 et les outils de déploiement Windows.

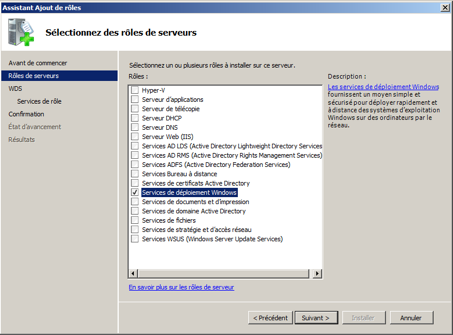
*Windows AIK :*

Ce Kit d’installation automatisée (Windows AIK) pour Windows 7 aide à installer et à déployer une version pré-configurée de Windows 7 sur les postes de travail de notre parc informatique. En utilisant Windows AIK, nous pouvons automatiser les installations Windows, capturer des images disques Windows avec ImageX, configurer et modifier ces images en utilisant l'imagerie de déploiement de service et de gestion, créer des images Windows PE, et migrer les profils utilisateur et des données avec l'outil de migration.

Procédure d’installation du service WDS

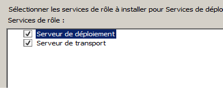
Le service WDS de Microsoft est déjà inclut, comme expliqué plus haut, dans Windows Server 2008 (que nous utiliserons dans cette procédure). Pour l’ajouter, il suffit de le cocher dans l’ajout de rôles du gestionnaire de serveur.

Procédure d’installation de WDS :



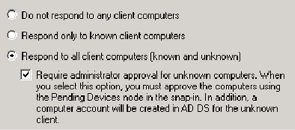
ATTENTION : Pour la suite, et afin que l’installation fonctionne correctement, il faut que votre serveur soit lié à un domaine. Dans notre cas, ce sera un serveur à part, également sous Windows Server 2008,  qui fera office de serveur DNS et toutes les machines seront dans un domaine nommé « m2l.fr ». Nous installerons également un service DHCP sur le serveur WDS.

Cochez « Serveur de déploiement » et « Serveur de transport »

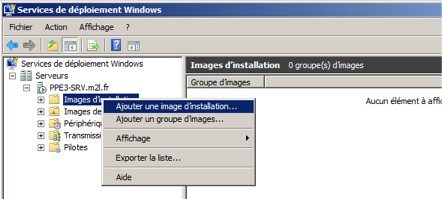


Ouvrez les « Services de déploiement Windows » et faites un clic droit sur le serveur, « Propriétés ». Cochez les 2 cases concernant PXE, et « répondre à toutes les demandes client connus et inconnus » en cochant la case du dessous afin que l’administrateur puisse approuver les demandes.

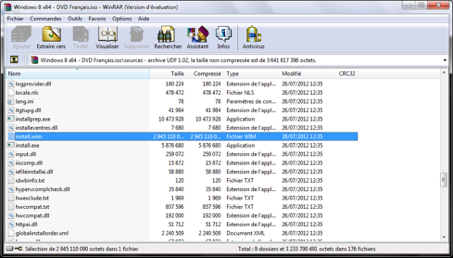
https://lh6.googleusercontent.com/KP2mjYWyyj0UwoIRlaMNV-RqcennRM6R0hupypove1Fg3iLP0ajU22iNxCluYLLF8vM7drjWc_mCkbGrZ2iypEMPMCC1hCBH5jZGtLOPdXmy1tkD_I7be4ZmnVz-UwCasA



Nous allons maintenant ajouter une images du système que l’on souhaite installer sur la ou les machines distantes. Faites un clic droit sur « Images d’installation », « Ajouter une images d’installation… »



Il vous faudra par la suite 2 fichiers : install.wim et boot.wim qui sont des images du système d’exploitation que vous souhaitez installer. Ces 2 images sont trouvables sur le CD de votre système, dans le dossier « sources ».



Ajoutez une de ces 2 images et son nom. Les images systèmes

Conclusion sur l’utilisation du service WDS (avantages / inconvénients) (ajouter comparaison avec d’autres solutions de masteurisation ?)

-----

WDS (Windows deployment service) = solution de masteurisation proposée par Microsoft. Consiste, à partir d’une image système, à cloner et déployer des systèmes d’exploitation sur un réseau (win7, win8,…).

* 1. Mission 2 : Mise en place d’un serveur d’application

**Introduction :**

Terminal Server (TSE) est un composant de Microsoft Windows qui permet à un utilisateur d’accéder à des applications et des données sur un ordinateur distant.

Afin de faciliter les ligues et les services de la M2L dans leur installation, l’administrateur envisage de mettre en place un serveur d’application basé sur TSE permettant aux utilisateurs d’accéder et d’utiliser les applications qui y sont installées. Le serveur est hébergé dans le VLAN informatique dans un serveur suffisamment redimensionné, car tous les traitements se font au niveau du serveur. La solution offre plusieurs avantages : côté administration système, cela réduit les coûts d’exploitation, sécurise le serveur et les applications, utiliser les PC clients en tant que clients légers ne nécessitant pas de performance. Côté utilisateurs, ils peuvent accéder à partir du bureau à distance ou depuis une interface WEB, aux applications qui leurs affectées.

La solution peut être enrichie pour la mise en place d’une ferme de serveurs TSE pour assurer une haute disponibilité et la répartition de charge.

Il est donc vital, compte tenu du contexte, d’intégrer ce nouveau service dans l’infrastructure de la M2L.

|  |  |
| --- | --- |
| **DESCRIPTION DE LA SOLUTION RETENUE** |  |
| **Conditions initiales** | * Un serveur Windows 2008 R2 avec les rôles d’Active directory et de DNS. * L’administration du serveur à distance est impossible. |
| **Conditions finales** | * L’administration du serveur est impossible à partir d’un poste client. * La prise de contrôle à distance est possible. |
| **Outils utilisés** | * Administration des services de Windows Server 2008 R2. * Terminal Server. |
| **DEROULEMENTS DES ACTIVITEES** | |
| Définition du besoin L’école Suger qui est situé à Vaucresson a mis en place dans l’établissement le logiciel 4D pour le service comptabilité qui est situé à Paris ainsi que pour certains employés, pour pouvoir utiliser ce logiciel, nous avons décidé de mettre en place un TSE (Terminal serveur) qui est un composant de Microsoft et qui permet à un utilisateur d’accéder à l’application 4D et à des données sur un ordinateur distant. Installation de l’autorité de Certification Dans le gestionnaire de serveur, il faut installer le rôle **« Service de certificats Active Directory »**  C:\Users\admin\Desktop\PPE 2013\TSE-ROLE.png  On sélectionne ensuite **« Autorité de certification »**, puis **« Entreprise »** car nous avons un domaine, ensuite on choisit **« Autorité de certification racine »**, et**« Créer une nouvelle clé privé »**. On clique enfin sur **« installer »**. Installation des services du Terminal Serveur Dans le gestionnaire de serveur, on sélectionne le rôle **« Service Bureau à Distance »**  Puis on coche les fonctionnalités suivantes :  - Hôte de session bureau à distance  - Gestionnaire de licences des services Bureau à distance  - Service Broker pour les connexions bureau à distance  - Passerelle des services Bureau à distance  - Accès Bureau à distance par le Web  C:\Users\admin\Desktop\PPE 2013\TSE-SERVICE.png  L’installation du service **« Hôte de session Bureau à distance »** n’est pas recommandé sur le serveur contrôleur de domaine pour des raisons de sécurité, il est préférable de séparer le serveur TSE du serveur d’Active directory.  Il est nécessaire d’installer le service IIS,  qui se configurera automatiquement, en fonction de la sélection des services web précédemment en cliquant sur **« Ajouter les services de rôle requis »**. Une fois ce service installé on choisit une méthode d’authentification pour les services de **« Bureau à distance »**, pour avoir une compatibilité avec les anciennes versions du bureau à distance on choisit sur **« Ne nécessite pas l’authentification au niveau du réseau »**. On configure maintenant l’étendue de découverte pour le serveur de licence, en allant sur **« Ce domaine »**, puis on sélectionne le certificat pour le chiffrement SSL qui a été généré précédemment.  Pour la création d’une stratégie d’autorisation on coche **« Ultérieurement »**. Une fois l’installation terminée, on redémarre la machine.  Dans les Outils d’administrations, on clique sur **« Gestionnaire de licences des services Bureau  distance »**, puis clic-droit **« Activer le server »**. On fait le choix de la méthode pour l’activation des licences qu’on laissera en auto. Puis on sélectionne le programme de licence selon les licences acquises et on valide le numéro de série. Configuration des Sessions On clique sur **« Configuration d’hôte de session Bureau à distance »** dans les outils d’administration, puis on va dans propriétés de RDP-tcp.  C:\Users\admin\Desktop\PPE 2013\TSE-TS.png  Nous modifions les paramètres pour les sessions déconnectées afin d’éviter l’utilisation inutile de licences. Configuration des RemoteApp On ira ensuite sur **« Gestionnaire RemoteApp »** dans les outils d’administration pour ajouter les programmes auxquels on veut donner un accès à distance.  C:\Users\admin\Desktop\PPE 2013\TSE-remoteapp.png  A partir de **« Paramètre des signatures numériques »**, on va sur **« Modifier »**. Ensuite on coche **« Signer avec un certificat numérique »** et on sélectionne le certificat que l’on a créé. Enfin on définit si le programme est accessible via internet.  C:\Users\admin\Desktop\PPE 2013\tse-remoteapp2.png Configuration d’active directory On ouvre **« Utilisateurs et ordinateurs Active directory »** afin de créer une nouvelle **« Unité d’organisation »** que l’on nommera **« TSE »**. On crée alors un nouveau groupe aussi nommé **« TSE »** que l’on définit comme membre du groupe **« Utilisateurs du bureau à distance »**.  Ensuite, il faut aller dans **« Attribution des droits d’utilisateur »** qui se situe dans la **« Stratégie de sécurité local »**, puis dans **« Stratégie locales »**, et enfin dans **« Attribution des droits utilisateur »**.Ici on ajoutera le groupe **« TSE »** que l’on vient de créer à la stratégie **« Autoriser l’ouverture de session par les services Bureau à Distance »**.  C:\Users\admin\Desktop\PPE 2013\TSE-stratégie de sécurité.png  Dans **Configuration Ordinateur / Stratégie / Paramètres Windows / Paramètres de sécurité / Stratégies Locales / Attribution des droits utilisateurs**, on édite les clés : **« Autoriser l’ouverture de session Terminal serveur »** ainsi que **« Permettre l’ouverture d’une session locale »** pour ajouter le groupe TSE que l’on a créé. Configuration des Stratégies de groupe Il s’agit à présent de définir les droits pour chaque utilisateur ou chaque groupe d’utilisateurs,  dans **« Gestion de Stratégie de groupe »** du groupe **« TSE »** précédemment établi. On crée un **« Nouvel Objet GPO »** et on le lis.  C:\Users\admin\Desktop\PPE 2013\tse-stratégie de groupe.png UtilisationConnexion au Bureau à distance La configuration du TSE s’effectue sur le serveur où il a été mis en place avec le compte administrateur. Les utilisateurs peuvent l’utiliser soit par **« connexion au bureau à distance »** de Windows soit par un simple navigateur web. Il faut alors utiliser l’adresse IP ou le nom de domaine du réseau où l’on veut se connecter. Et ce en utilisant un compte membre du groupe **« TSE »**. RemoteApp On va dans le **« Gestionnaire RemoteApp »** qui se trouve dans les **« Outils d’administration »**. On sélectionne l’application à laquelle on veut donner l’accès à distance puis on crée un fichier **« .rdp »**. On le partage dans le dossier **« C:\Program Files\Packaged Programs »**    C:\Users\admin\Desktop\PPE 2013\tse-remoteapp3.png | |

|  |
| --- |
| **CONCLUSION** |
| L’objectif a été atteint, les professeurs peuvent remplir les « manquements » des élèves depuis la salle des professeurs, ou encore depuis chez eux en utilisant le fichier « .rdp » que nous leur avons transmis ou en utilisant la connexion au bureau à distance si ils ont les informations nécessaires pour accéder au logiciel. |

* 1. Mission 3 : Mise en place d’outils de gestions de par cet d’incidents

Notre solution pour gérer le parc informatique s’appuie sur le logiciel open-source GLPI, enrichie de la solution de gestion technique de parc informatique OCS Inventory NG.

Cette solution a pour fonctionnalités principales :

* Gestion et suivi des ressources informatiques Gestion et suivi des licences
* Gestion et suivi des consommables
* Base de connaissances
* Gestion des réservations
* ServiceDesk (helpdesk, SLA ...)
* Inventaire automatisé
* Télé-déploiement

La solution est rapide à déployer et simple à utiliser :

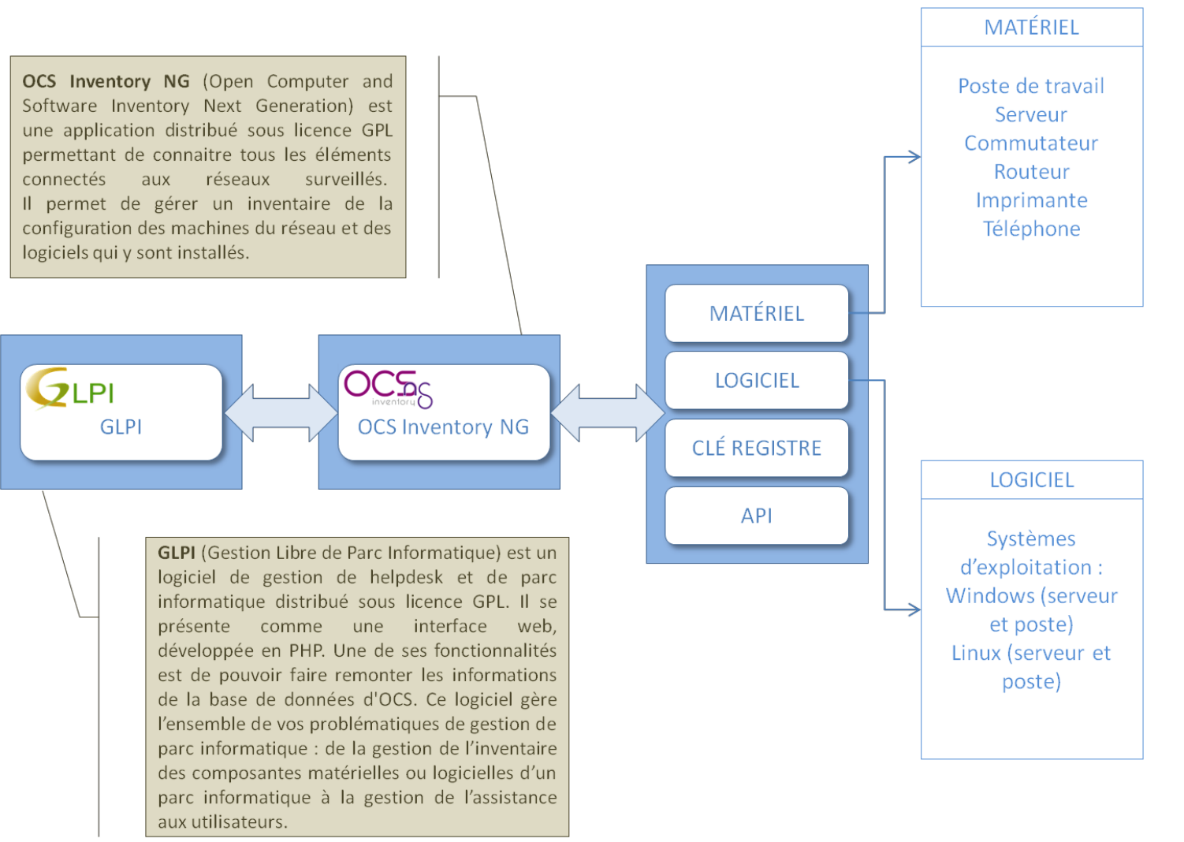
* Pré-requis techniques minimums
* Mise en production immédiate
* Accessible depuis un simple navigateur Web
* Interface paramétrable
* Utilisation intuitive
* Ajout aisé de fonctionnalité grâce à un système de plugins Communication avec des annuaires existants
* Communication avec des annuaires existants                

    Figure 6 - Gestion parc informatique par GLPI et OCS Inventory NG

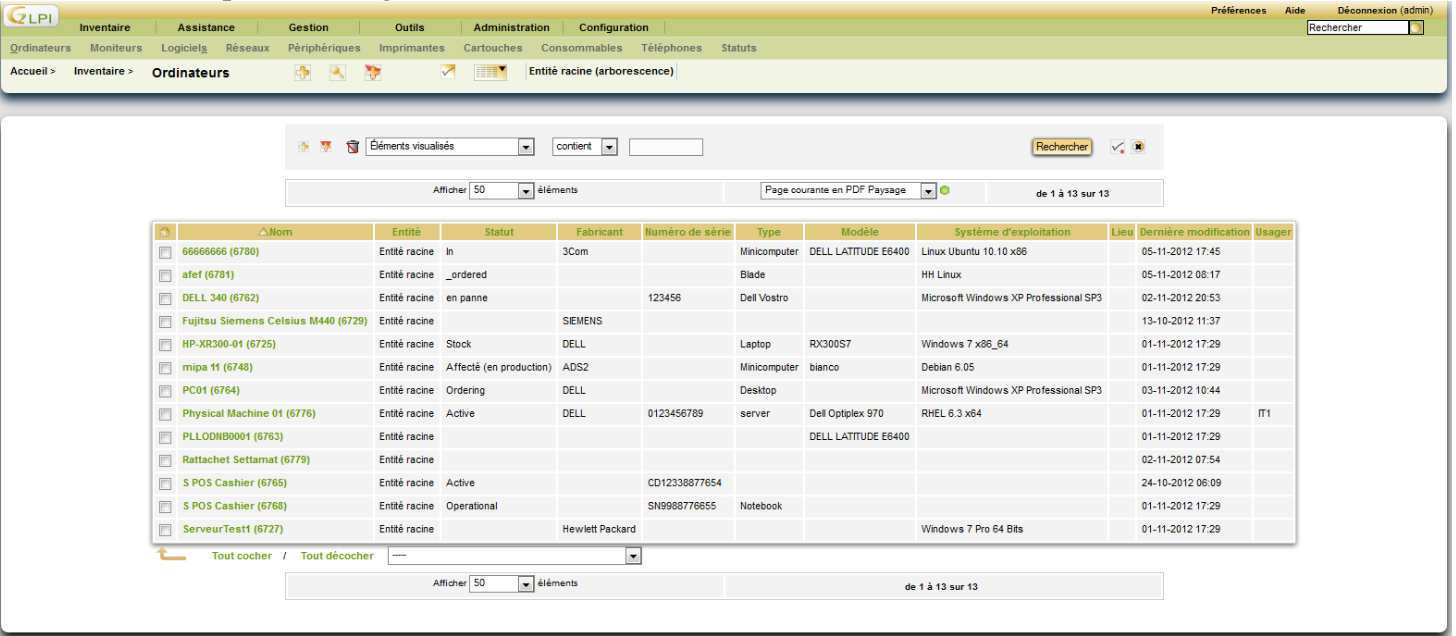
        Ci-dessous, un aperçu du logiciel GLPI :

Figure 7 - Gestion de l'inventaire des ordinateurs

Il est possible de modifier, ajouter, supprimer des articles de la base de données.



Figure 8 - Gestion des articles dans la base de données

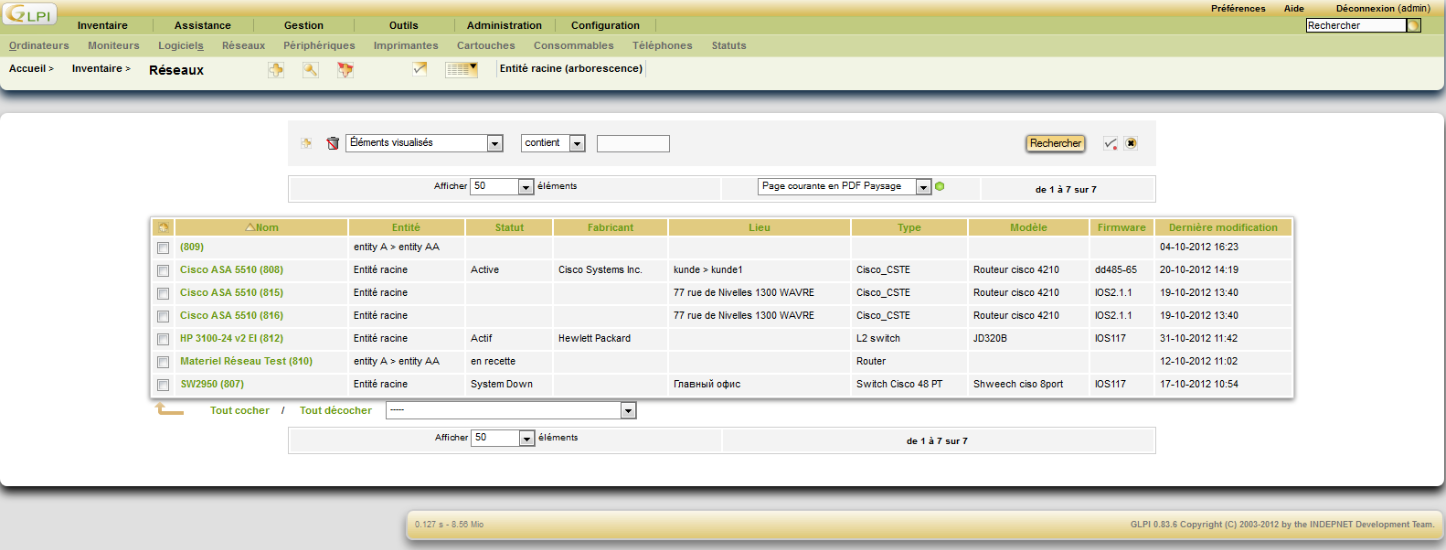


Figure 9 - Gestion du réseau de la base de données

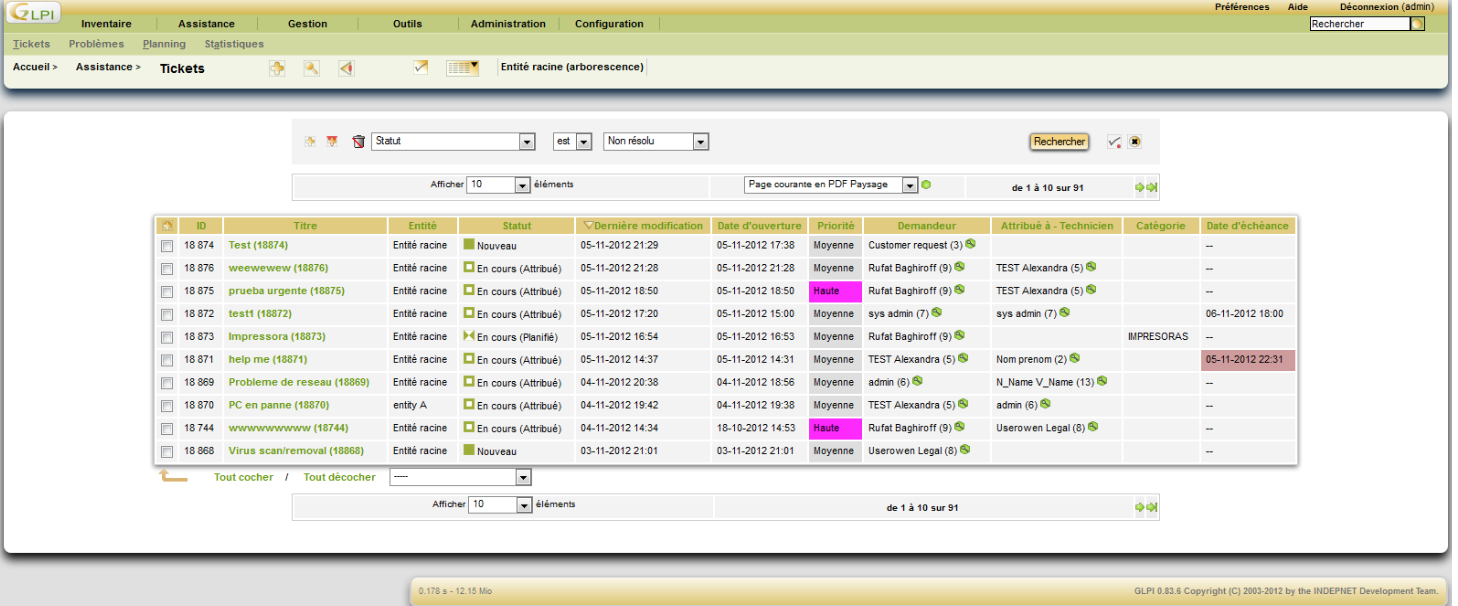


Figure 10 - Gestion des tickets

OCS Inventory est une solution modulable constituée de nombreux plugins et un interfaçage avec la solution de gestion de parc informatique GLPI.

Ci-dessous, un aperçu du logiciel OCS Inventory :

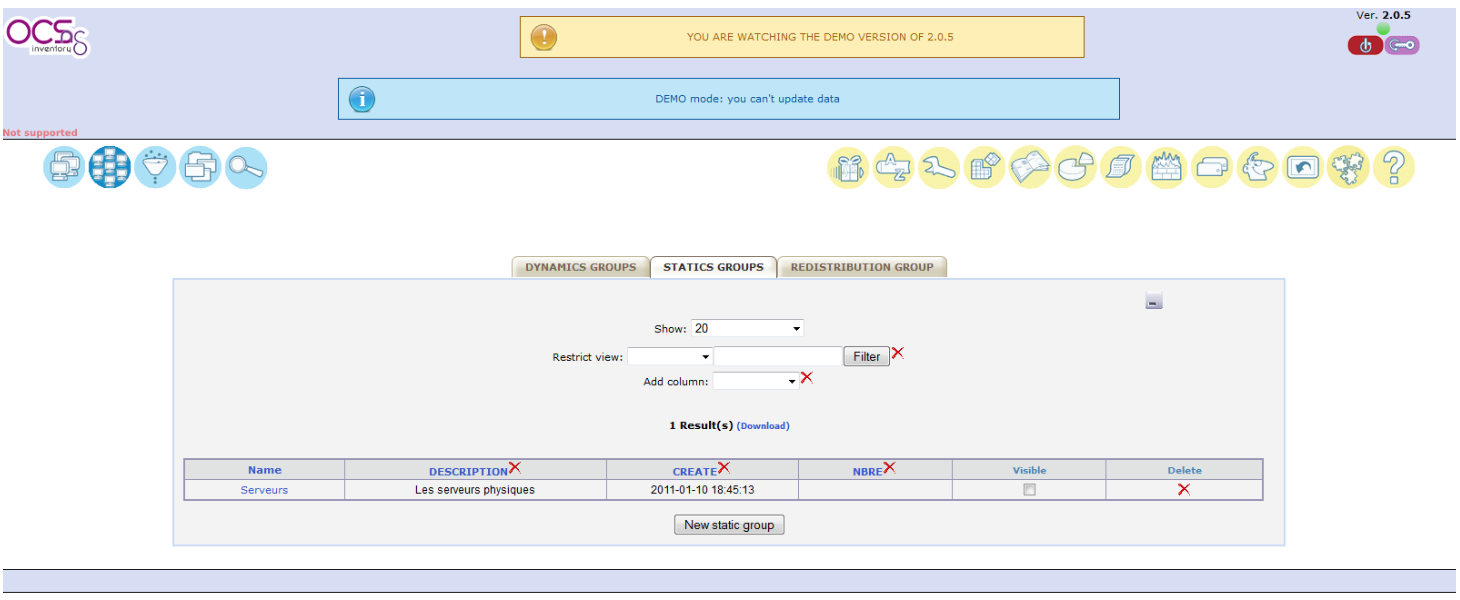


Figure 11 - Gestion serveur sur OCS Inventory

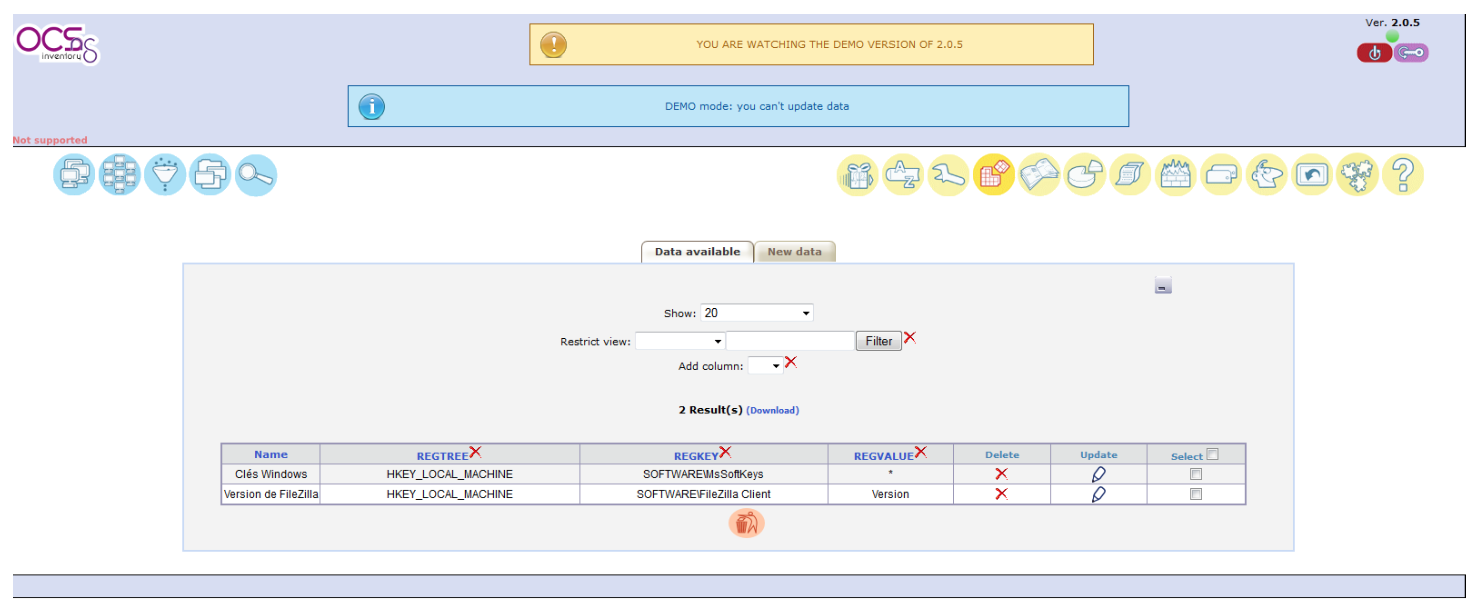


Figure 12 - Gestion des clés de registre sur OCS Inventory

1. **Administration réseau**
   1. Mission 1 : Service d’accès sécurisé Internet – DMZ
   2. Mission 2 : Service d’administration à distance sécurisée

**Mission 2 : Service d’administration à distance sécurisée**

En général, il y a le choix entre l'administration web sécurisée ou pas (protocole http ou https) et/ou l'administration en ligne de commande sécurisée ou pas (telnet ou ssh).  
L'administration du switch en utilisant une interface web peut être pratique. Mais nous choisirons en priorité l'administration du switch en utilisant la ligne de commande pour les raisons suivantes:

* En cas de coupure réseau, il nous faudra intervenir directement sur le switch, donc autant être habitué à travailler en ligne de commande,
* L'interface web peut être moins stable que l'interface en ligne de commande (CLI),
* Les configurations avancées sont souvent disponibles uniquement au travers de la ligne de commande,

Ainsi les interfaces web seront désactivées.  
Il nous reste à choisir entre telnet et ssh. Le second étant nettement plus sécurisé que le premier, il est préférable (quand cela est possible) d'activer uniquement ssh sur le switch.

Pour sécuriser les accès d’administration à distance sur les routeurs ou les switch, il est nécessaire d’utiliser un protocole en mode crypté comme SSH.

Il faut tout d’abord configurer un nom et déclarer le switch ou routeur dans un domaine.

Router(config)#**hostname *Nom***

Nom(config)#**ip domain-name *domaine.xxx***

Puis on configure les mots de passe d’entrée enable et username. Il faut des MDP forts.

Nom (config)#**enable secret *mot de passe***

Nom (config)#**username *User* password *mot de passe***

Ensuite on génère les clés utilisées par SSH en spécifiant leur taille et leur type (ici on choisit le cryptage RSA).

Nom (config)# **crypto key generate rsa**

***How many bits in the modulus [256]* : *Taille***

A ce stade, le routeur (ou switch) crée un couple de clé (clé publique et clé privée) sur la base des informations nom de domaine, username et loging.

On termine de configurer les paramètres de base de SSH.

Nom (config)# **ip ssh version *X***

Nom (config)# **ip ssh time-out *Y***

Nom (config)# **ip ssh authentication-retries *N***

On configure ensuite dans un premier temps le contrôle d’accès à distance via la console 0 Telnet :

Nom(config)# **line vty 0 15**

Nom(config-line)#**password *mot de passe***

Nom(config-line)#**login**

Nom(config-line)#**exit**

On crypte ensuite tous les mots de passe :

Nom(config)#**service password-encryption**

On valide enfin le protocole SSH pour la console d'accès à distance (VTY)

Nom(config)# **line vty 0 15**

Nom(config-line)# **transport input ssh**

Nom(config-line)#**login local**

Nom(config-line)# **exit**

* 1. Mission 3 : Service de haute disponibilité

**Mission 3 : Service de haute disponibilité**

Spanning tree

Pour rappel l’algorithme Spanning-Tree et ses variantes permettent dans un environnement d’éviter les boucles de transmission lorsque des paquets de diffusion transitent sur les switch.

Le principe du spanning-tree consiste à bloquer un port d’un switch participant à la boucle de diffusion. Le critère de décision s’effectue sur la base de l’élection d’un switch racine décidant quel port bloquer.

SW1(config)#**spanning-tree mode rapid-pvst** (sélection du mode Spanning Tree Protocol)

SW1(config)#**spanning-tree vlan 10 root primary** (le switch 1 est choisi comme pont racine principal pour le VLAN 10)

SW2(config)#**spanning-tree mode rapid-pvst** (sélection du mode STP)

SW2(config)#**spanning-tree vlan 10 root secondary** (le switch 2 est choisi comme pont racine de secours (root secondary))

* HSRP

Le protocole HSRP permet d’assurer une haute disponibilité de service sur les routeurs dans un réseau. Un routeur qui assure des fonctions importantes se doit d’être secondé par un ou plusieurs autres routeurs évitant ainsi une rupture de service en cas de panne d’un élément de la chaîne.

Pour cela on place en parallèle plusieurs routeurs physiques qui seront par configuration liés à un routeur virtuel unique. Ce routeur présente une adresse IP et une adresse MAC commune aux 2 routeurs sur lesquels s’appuient les postes du réseau local.

**Configuration de l’interface physique routeur maître (actif) :**

Routeur(config)#**int Fa 0/0** (On entre dans l’interface qui sera affectée au HSRP)

Routeur(config)# **ip address a definir**

Routeur(config)# **no shutdown**

Configuration du HSRP (on utilise l’identifiant 10 pour désigner le groupe de routeurs HSRP)

Routeur(config)# **standby 100 ip 192.168.0.1** (on configure l’adresse IP virtuelle)

Routeur(config)# **standby 100 priority 110** (La priorité qui désigne le routeur maître)

Routeur(config)#**standby 10 preempt** (Le routeur maître reprend la main dès que la panne disparaît.)

Routeur(config)#**standby 10 track Interface** 🡪 Le routeur maître surveille l’interface opposée à l’interface HSRP.

Routeur(config)#**exit**

**Configuration de l’interface physique routeur esclave (standby) :**

Routeur(config)#**int Fa 0/0**

Routeur(config)# **ip address a definir**

Routeur(config)#**no shutdown**

Configuration du HSRP :

Routeur(config)# **standby 100 ip a definir**

Routeur(config)#**standby 10 preempt** 🡪 Le routeur prend la main dès que le routeur principal disparaît.

Routeur(config)#**exit**

Le routeur maître doit avoir un numéro de priorité supérieur au routeur secondaire. En cas de panne (routeur, liaison HSRP ou liaison opposée) cette priorité est diminuée de -10 et doit passer en dessous de la priorité du routeur secondaire. Le routeur esclave (standby) passe alors en état actif. Une fois la panne disparue, le routeur principal repasse en maître par la fonction preempt.

Le routeur principal doit surveiller l’interface qui n’est pas gérée par le HSRP car il doit passer en standby si celle-ci n’est plus disponible.

1. **Economie Management**

**Statut juridique :**

La Maison des Ligues est un établissement du Conseil Régional. Ce n’est pas une entité juridique en propre.

**Financement de la M2L :**

Elle est financée à 100 % (pour son fonctionnement et pour la construction récente de l’extension des bâtiments C et D) par le Conseil Régional et sans aucune participation du Conseil Général de Meurthe et Moselle, bien qu’elle abrite un certain nombre de comités départementaux. Une convention de cogestion a été passée entre le Conseil Régional et le Comité Régional Olympique et Sportif de Lorraine pour la gestion de l’outil « Maison des Ligues ». Le CROSL est une association financée par le ministère via le CNDS (Centre National de Développement du Sport).

En échange des services offerts par la M2L, les ligues sportives donnent une contrepartie financière.

**Revenus :**

* 6€ /m²/ligues/mois payé tous les trimestres.
* Réservation de salle : 4 niveaux de tarifications.
* Plan impact emploi associations.
* Service d’établissement de bulletin de salaire.
* Service d’impression / affranchissement.
* Location de téléphonie IP

**Dépenses :**

* Achat de matériels (Ordinateurs, switches, serveurs, etc…)
* Salaires
* Impôts

**Coûts du PPE 1.1 :**

* Imprimantes : 12 898 euros TTC
* Fournisseur Internet : 1079 euros/an TTC
* Switches : 16 908 euros TTC
* Câblage / Connectique : 10825  € TTC
* Serveurs : 2 000 € TTC
* Postes fixes : 27 000 € TTC
* Poste portables : 12 000 € TTC
* Ecrans : 5 000 € TTC
* Licences OS : 2 000 € TTC (Windows 7, Windows Server 2008 R2)
* Coût total PPE 1.1 : **89 710 €** TTC

**Coûts du PPE 1.2 :**

* SAN / NAS : 17 000 € TTC
* Appliance : 16 000 € TTC
* Coût total PPE 1.2 : **33 000 €** TTC

**Coûts du PPE 2.1 :**

* Salaires : **10 000 €** /mois
* Chef de projet (4 000 € /mois)
* Techniciens : 1 expert réseaux ,1 expert système et 1 technicien polyvalent (2 000 € /mois chacun)

Le personnel se répartira les tâches de façon à assurer l’installation, l’exploitation ainsi que la maintenance du projet.

* Matériel : **7 376 €** TTC
* Switches (x4) : 1 420 € chacun donc 5 680 €
* Routeurs + cartes réseaux (x2 : M2L et Ligue) : 800 € chacun donc 1 600 €
* Câblage : 8 sachets de 50 connecteurs RJ45 : 96 €
* Coût total PPE 2.1 : **24 752 €** TTC

**Coûts du PPE 3.1 :**

* Salaires : **8 000 €** /mois
* Chef de projet (4 000 € /mois)
* Techniciens : 1 expert réseaux ,1 expert système (2 000 € /mois chacun)

Le personnel se répartira les tâches de façon à assurer l’installation, l’exploitation ainsi que la maintenance du projet.

* Matériel : Serveur 2000 € TTC
* Licence OS : Windows Server 2008 R2 environ 250 € TTC
* Coût total PPE 3.1 : **10 250€** TTC

* **COUT TOTAL DU PROJET** : environ **157 712 €** TTC

**Durée** : Projet effectué sur 2 ans

1. **Droit**

**Cahier des charges**

Ce cahier des charges fait référence aux données duplan d’adressage IPlivréesdans le PPE2. Pour vos réponses vous utiliserez tous documents, ou autres sources Internet vous permettant d’accéder aux informations utiles et en particulier les documents ***FTA 08 Commandes CLI Cisco*** et ***FT sécurité des données***.

**Les services de haute disponibilité** sur les nœuds du réseau concernent le réseau de commutation des ligues, le service DHCP et la redondance du réseau d’accès à Internet. Les techniques qui seront employées pour la réalisation de ces projets font appel aux documents de spécification technique ***FTA 08 Commandes CLI Cisco*** et ***FT05 Commutation Ethernet*** ainsi que les documents officiels sur le site des constructeurs.

Les liaisons en double attachement reliant les commutateurs d’accès au commutateur de distribution doivent être utilisées pour transporter la totalité du trafic des ligues. Le spanning-tree doit être configuré pour privilégier le trafic sur ces liaisons en phase opérationnelle (la liaison entre SW2LIG et SW3LIG est un secours en cas de défaillance des liaisons principales.

La continuité de service pour l’accès à Internet est réalisée à l’aide de 2 routeurs physiques vus comme un seul routeur virtuel par le routeur M2L, ces 2 routeurs se relaient en cas de panne. Cette fonction sera assurée par le protocole VRRP ou HSRP chez Cisco.

HSRP permet à un routeur de secours de prendre immédiatement le relais de façon transparente dès qu’un problème physique apparaît sur le routeur principal.

Si le routeur, que nous appellerons primaire, devient indisponible le routeur secondaire prendra sa place automatiquement. Les paquets continueront de transiter de façon transparente car les 2 routeurs partagent une même adresse de passerelle IP et MAC virtuelle.

1. **Déroulement de la mission**

Dans cette prestation vous devrez produire pour chacune des 3 missions les documents de  déploiement des services et le dossier de tests pour la validation du service. Vous réaliserez une maquette mettant en œuvre les différentes fonctionnalités conformément au cahier des charges ci-dessus.

* 1. **Modalités de réponse**

Vous constituerez le dossier du projet en y incluant le document d’étude et d’analyse des solutions, les documents d’architecture de configuration et de test des éléments de réseau. Vous intègrerez aussi le document de recette contenant les fiches de test en indiquant la couverture de test du réseau. Les Annexes 3 et 4 présentent le format des fiches de test à intégrer au dossier.

Votre projet sera accompagné d’une maquette qui permettra de présenter et valider la faisabilité technique de ce projet.