Déploiement SAMBA 3.6
Contrôleur de domaine
Serveur d’impression
Serveur de fichiers

SOMMAIRE

1 PRESENTATION DU DOCUMENT :

1.1 OBJECTIFS DE CE DOCUMENT :

Le but de ce document est d'expliquer comment :
- Configurer Red Hat Enterprise Linux.
- Déployer un contrôleur de domaine principal (PDC) SAMBA 3.6.
- Déployer un contrôleur de domaine secondaire (BDC) SAMBA 3.6.
- Déployer un serveur de fichiers et d'impression SAMBA 3.6.
- Intégrer une station de travail Windows 7 dans cet environnement

1.2 PRESENTATION DE L'ARCHITECTURE CIBLE :

1.2.1 LISTE DES MACHINES :

Cette architecture sera basée sur 4 machines :

MSREPORTPDC :
Cette machine sera contrôleur de domaine principal (PDC) du domaine MSREPORT. Elle disposera de SAMBA 3.6.12, OpenLDAP 2.4.23 et sera installée sous RedHat Enterprise Linux 6.2.
IP : 192.168.92.121 / 24
Passerelle : 192.168.92.2
Serveur DNS : 192.168.92.2
Serveur WINS : 192.168.92.121.

MSREPORTBDC :
Cette machine sera contrôleur de domaine secondaire (BDC) du domaine MSREPORT. Elle disposera de SAMBA 3.6.12, OpenLDAP 2.4.23 et sera installée sous RedHat Enterprise Linux 6.2.
IP : 192.168.92.125 / 24
Passerelle : 192.168.92.2
Serveur DNS : 192.168.92.2
Serveur WINS : 192.168.92.121

MSREPORTINF1 :
Cette machine sera un serveur de fichiers et d'impression membre du domaine MSREPORT. Elle disposera de SAMBA 3.6.12, CUPS et sera installée sous RedHat Enterprise Linux 6.2.
IP : 192.168.92.126 / 24
Passerelle : 192.168.92.2
Serveur DNS : 192.168.92.2
Serveur WINS : 192.168.92.121

MSREPORTW7 :
Cette machine sera installée sous Windows 7 et sera configurée en tant que membre du domaine MSREPORT (SAMBA).
IP : 192.168.92.43 / 24
Passerelle : 192.168.92.2
Serveur DNS : 192.168.92.2
Serveur WINS : 192.168.92.121

Remarque :
- La machine 192.168.92.2 est l'adresse de mon routeur (accès Internet) et fait aussi office de serveur DNS.

1.2.2 CONFIGURATION DES SERVEURS RED HAT ENTERPRISE LINUX :

Le pare feu de RedHat Entreprise Linux sera désactivé sur la maquette.
SE linux sera désactivé sur les serveurs OpenLDAP car il génère des problèmes au niveau d'OpenLDAP comme expliqué dans cet article : http://niranjanmr.wordpress.com/2012/03/29/n-waymmr/

Set the selinux to permissive mode temporarily till we configure N-Way MMR. Reason being when cn=config database is modified dynamically using ldapadd/modify/delete , It's better if those changes are saved back in /etc/openldap/slapd.d. Currently selinux would not allow the "slapd" process to write to slapd.d directory unless selinux is set to Permissive or create a selinux policy to allow the write operation

1.2.3 CONFIGURATION DE L'ANNUAIRE OPENLDAP :

L'annuaire SAMBA sera hébergé dans une base OpenLDAP.

Nous utiliserons le fichier *slapd.conf* pour gérer la configuration du serveur OpenLDAP.
OpenLDAP 2.4.12 peut en effet être configuré à l'aide de deux méthodes :
- Via le fichier de configuration *sladp.conf*.
- Via des entrées (objets) dans le conteneur CN=CONFIG de la base OpenLDAP.

La nouvelle méthode (CN=CONFIG) permet la prise en compte des changements dans la configuration d'OpenLDAP sans redémarrage du service. Un redémarrage est nécessaire si utilisation du fichier *sladp.conf.*
Cependant, l'administration du service OpenLDAP est plus complexe avec la nouvelle méthode :
- Il est nécessaire d'ouvrir de nombreux fichiers LDIF / effectuer des requêtes LDAP pour visualiser la configuration.
- Pour effectuer un changement, il est nécessaire de créer un fichier *slapd.conf* temporaire et d'utiliser la commande suivante pour injecter le changement dans le conteneur CN=CONFIG :
  slaptest -f slapd.conf -F /etc/openldap/slapd.d
  Ce conteneur est accessible sous forme de fichier LDIF dans le dossier */etc/openldap/slapd.d*

Pour plus d'informations, voir page 39 du document *OpenLDAP-Admin-Guide* 2.4 : http://www.openldap.org/doc/

Les modules suivants seront chargés au niveau d'OpenLDAP :
- *ppolicy.la* : ce module permettra la prise en charge des stratégies de mots de passe.
- *syncprov.la* : ce module permettra la prise en charge de la réplication Syncrepl et Deltasyncrepl

Pour optimiser les performances, il est recommandé d'indexer les attributs suivants :
- *sambaSID*
- *sambaPrimaryGroupSID*
- *sambaDomainName*
- *entryUUID* (si utilisation de la réplication OpenLDAP 2.4)
- *entryCSN* (si utilisation de la réplication OpenLDAP 2.4)

Pour plus d'informations, lire les deux articles ci-dessous et se reporter aux pages 162 et 166, 168 et 169 du guide OpenLDAP 2.4 :
http://pig.made-it.com/samba-accounts.html
http://www.zytrax.com/books/ldap/apa/indeces.htm

"On databases which support inequality indexing, setting an eq index on the entryCSN attribute and configuring contextCSN checkpoints will greatly speed up this scanning step".
"Note that using the session log requires searching on the entryUUID attribute. Setting an eq index on this attribute will greatly benefit the performance of the session log on the provider".

Le serveur OpenLDAP sera configuré pour répliquer en mode MIRRORMODE.
Il est en effet nécessaire de faire répliquer la base OpenLDAP pour disposer d'une solution tolérante au panne.
Le moteur de réplication *Slurpd* a été supprimé sous OpenLDAP 2.4 et est maintenant remplacé par le nouveau moteur *Syncrepl / Delta-syncrepl*.
SyncREPL nécessite de répliquer complètement un objet quand on modifie un attribut.
Delta-Syncrepl permet de répliquer uniquement un attribut et non tout l'objet. Delta-syncrepl nécessite cependant de maintenir une base de données de changement.

Pour plus d'informations, sur Syncrepl et Delta-syncrepl, voir page 163 du guide OpenLDAP.

Présentation du mode N-WAY MULTI-MASTER :
Avantages : Les deux serveurs OpenLDAP sont accessibles en lecture / écriture par les serveurs SAMBA (clients OpenLDAP). Chaque serveur SAMBA peut utiliser la base OpenLDAP du serveur et en second la base OpenLDAP de l'autre serveur. La bascule est automatique en cas de panne d'un des 2 serveurs.
Inconvénients : il y a un risque de corruption si l'application ne prend pas en charge ce mode de réplication (conflit au niveau des objets, http://www.openldap.org/faq/data/cache/1240.html). Cette méthode Nécessite que les deux serveurs OpenLDAP soient synchronisés au niveau horaire. Pour plus d'informations :
https://access.redhat.com/knowledge/solutions/273533
http://niranjanmr.wordpress.com/2012/03/29/n-waymmr/
http://sambaxp.org/fileadmin/user_upload/SambaXP2008-DATA/03-02-Hannes_Kasparick-OpenLDAP.pdf

Présentation du mode MIRRORMODE :
Avantages : en cas de défaillance du serveur avec l'ID à 1, le serveur OpenLDAP avec l'ID à 2 prend automatiquement le relais. Il y a donc moins de risque de conflit (un seul maître).
Inconvénients : seul un serveur OpenLDAP est accessible en lecture / écriture par les serveurs SAMBA à la fois. Il faut configurer les deux serveurs SAMBA pour utiliser le même 1er et 2ème serveur OpenLDAP. L'algorithme de réplication Delta-SyncREPL n'est pas supporté. Pour plus d'informations :
http://eric.quinton.free.fr/IMG/pdf/Configurer_samba_ldap_ubuntu10_avec_migration_CS3-CS4-2.pdf
http://sambaxp.org/fileadmin/user_upload/SambaXP2008-DATA/03-02-Hannes_Kasparick-OpenLDAP.pdf

Le mode MASTER / SLAVE :
Avantages : pas de problème de cohérence des données.
Inconvénients : les clients doivent être configurés pour écrire vers le même serveur OpenLDAP.
Pas de bascule automatique. Le serveur OpenLDAP esclave doit être promu manuellement en serveur maître. Pour plus d'informations :
http://sequanux.org/spip.php?article22
http://sambaxp.org/fileadmin/user_upload/SambaXP2008-DATA/03-02-Hannes_Kasparick-OpenLDAP.pdf

1.2.4 CONFIGURATION DE L'ANNUAIRE SAMBA :

L'authentification des machines Windows sera assurée par les serveurs MSREPORTPDC et MSREPORTBDC. Cela permettra de disposer d'un haut niveau de tolérance de panne.
Contrairement au fonctionnement d'un PDC / BDC Windows NT4, il sera possible de créer des objets utilisateurs et groupes sur MSREPORTBDC (le BDC) via les commandes SMBLDAP-TOOLS.

Cependant en cas de défaillance du PDC (MSREPORTPDC), les utilisateurs ne pourront plus :
- Changer de mots de passe.
- Changer le mot de passe de compte ordinateur (à valider).

Ce mode de fonctionnement est décrit dans les articles http://technet.microsoft.com/en-us/library/cc751445.aspx et http://support.microsoft.com/kb/185952/en-us. Les BDC NT4 répliquent uniquement les informations de verrouillage de compte et les changements de mots de passe de réplication au PDC comme expliqué dans l'article
En effet un BDC SAMBA reste identique à un BDC NT4 du point de vue des clients Windows.
Il est à noter que ce dernier ne sait pas retransmettre au PDC les demandes de changement de mot de passe ordinateur.

Les protocoles NTLM et NTLM V2 seront activés sur la maquette.
Pour des raisons de sécurité le protocole LanManager (LM) ne sera pas activé.
Les contrôleurs de domaine SAMBA 3.6 ne prennent pas en charge l'authentification Kerberos. Ce protocole d'authentification ne sera donc pas déployé sur la maquette.

1.2.5 CONFIGURATION DU SERVICE WINS :

Il sera nécessaire de déployer un serveur WINS afin de permettre aux stations de travail qui ne sont pas sur le même sous réseau IP que les contrôleurs de domaine de découvrir le domaine MSREPORT.

En effet dans un domaine NT4, les stations de travail font des requêtes WINS sur les entrées 1C ou de la diffusion pour découvrir qui sur le réseau est un contrôleur de domaine (http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html#id2566941)

Comme expliqué dans l'article http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetworkBrowsing.html#id2584196, SAMBA ne prend pas en charge la réplication WINS.
« *Samba-3 does not support native WINS replication. There was an approach to implement it, called wrepld, but it was never ready for action and the development is now discontinued* »

Deux solutions sont donc possibles :
- Déployer le serveur WINS sur MSREPORTPDC uniquement. Les stations de travail seront configurées avec MSREPORTPDC comme serveur WINS principal. Un fichier LMHOST sera déployé sur chaque station de travail Windows XP / Windows 7 et permettra de définir les entrées 1C et 1B requis pour l'authentification (pas de tolérance de panne WINS avec SAMBA). Ces entrées seront prioritaires sur le serveur WINS.
- Déployer le serveur WINS sur MSREPORTPDC et de configurer MSREPORTBDC comme serveur proxy WINS. Cela permettra d'utiliser le cache WINS de MSREPORTBDC lors d'un redémarrage de MSREPORTPDC.

Pour plus d'informations :
http://www.samba.org/samba/docs/man/Samba3-HOWTO/NetworkBrowsing.html#id2584196
http://support.microsoft.com/kb/150800/en-us
http://support.microsoft.com/kb/314108/fr

1.2.6 LES COMPOSANTS EN CHARGE DE L'AUTHENTIFICATION :

Les serveurs MSREPORTPDC et MSREPORTBDC vont s'appuyer sur les 5 composants suivants :
- **OpenLDAP :** *les ressources de l'annuaire seront stockées dans l'annuaire OpenLDAP. Toutes les attributs des comptes utilisateurs, groupes, ordinateurs) sont dans la base OpenLDAP (comme le SID, le login, le mot de pase). Le fichier « secrets.tdb » sur le serveur SAMBA contient uniquement le SID du domaine, du contrôleur de domaine et le mot de passe du compte Manager pour se connecter à la base OpenLDAP. Ce service se configure via le fichier /etc/openldap/slapd.conf.*
- **SAMBA (service SMB) :** *il permet aux machines Windows d'accéder aux ressources de l'annuaire OpenLDAP. Il émule le fonctionnement d'un PDC ou d'un BDC NT4. Les machines Windows ne peuvent pas se connecter directement à la base OpenLDAP. Ce service se configure via le fichier /etc/samba/smb.conf.*
- **PAM (Pluggable Authentication Module) :** *PAM est une interface unique qui permet d'interfacer les différents modules / méthodes d'authentification (authentification par login / mot de passe avec le fichier /etc/password, authentification login/mot de passe via une base OpenLDAP, authentification via certificat / carte à puce...) avec le système Linux (Red Hat Linux Enterprise 6). Ce service se configure via le fichier /etc/pam.d/system-auth.*
- **NSS (Name Service Switch) :** *ce composant permet d'indiquer où trouver les sources d'authentification / résolution de noms. C'est ce fichier que le système consulte pour localiser les sources d'authentifications (fichiers locaux ou base OpenLDAP, service SSSD, service WINBIND). Ce composant se configure via le fichier /etc/nsswitch.conf.*
- **SSSD (System Security Services Daemon) :** *il se présente sous la forme d'un service (SSSD) sur un serveur Red Hat Enterprise Linux 6. Il permet de fédérer plusieurs sources d'authentification (LDAP, NIS...). Ce service se configure via le fichier /etc/sssd/sssd.conf*

Complément d'informations sur PAM :
PAM (*Pluggable authentication modules*) permet de définir les modules d'authentification activées sur le système.
Toutes les applications de la machine LINUX vont s'appuyer sur le module d'authentification PAM.
Il existe une librairie PAM par méthode d'authentification.
La configuration de PAM se trouve dans */etc/pam.d.*
Chaque module d'authentification correspond à un fichier dans le répertoire /etc/pam.d

Il existe 4 types de module PAM :
- Les modules AUTH : fournissent l'authentification
- Les modules ACCOUNT : permettent de valider si l'accès est autoriser ou non

- Les modules PASSWORD : sont utilisés pour définir les mots de passe
- Les modules SESSION : exécutent les tâches nécessaires pour autoriser l'accès (montage du répertoire personnel, activation boîte aux lettres.

Les modules s'exécutent les uns après autres. Il est possible de configurer l'ordre d'application des modules PAM.
Il existe 4 types d'indicateur de contrôle PAM :

- Required : le module doit être vérifié avec succès pour que l'authentification soit accordée.
- Requisite : même principe que Required mais l'utilisateur est prévenu si la vérification échoue.
- Sufficient : en cas d'échec de la vérification du module, l'authentification n'est pas bloquée.
- Optional : en cas d'échec de la vérification du module, l'authentification n'est pas bloquée.

Sous Red Hat Enterprise Linux, les modules PAM se trouvent dans le répertoire */lib64/security*.

Pour plus d'informations sur PAM, NSS, SSD :
http://wiki.debian.org/fr/LDAP/NSS
http://fr.wikipedia.org/wiki/Name_Service_Switch
http://www.linux-kheops.com/doc/redhat72/rhl-rg-fr-7.2/s1-pam-config-files.html
http://www.linux-kheops.com/doc/redhat72/rhl-rg-fr-7.2/ch-pam.html
https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/SSSD-Troubleshooting.html
http://www.linuxtopia.org/online_books/rhel6/rhel_6_deployment/rhel_6_deployment_chap-SSSD_User_Guide-Setting_Up_SSSD.html

1.2.7 CONFIGURATION DES STATIONS DE TRAVAIL :

Clonage des stations de travail :
Afin de permettre un déploiement depuis une image, les stations de travail Windows XP / 7 doivent être préparées à l'aide d'un outil appelé SYSPREP.
Si cette action n'est pas effectuée, toutes les stations de travail Windows XP ont le même identifiant machine. Cela pose des problèmes avec des applications comme WSUS.
Il est possible d'utiliser l'outil PSGETSID pour déterminer si deux machines ont le même SID.
http://technet.microsoft.com/en-us/sysinternals/bb897417.aspx
http://technet.microsoft.com/fr-fr/sysinternals/bb897418.aspx

Gestion des stations de travail :
Les stratégies de groupe n'existe pas avec SAMBA 3.6 (c'est le cas avec SAMBA 4).
Il est possible de contourner en partie cette limitation en utilisant l'outil PSEXEC.EXE pour lancer des scripts avec des droits administrateurs sur les stations de travail. Cet outil nécessite de connaître un compte administrateur local sur la machine et nécessite que le partage C$ et ADMIN$ soient accessibles.
Pour plus d'informations, voir : http://technet.microsoft.com/fr-fr/sysinternals/bb897553.aspx
Cette solution est une alternative au script de login utilisé pour le déploiement d'application.
Il est toujours possible d'utiliser les scripts présents dans le partage NETLOGON avec le domaine SAMBA 3.6 pour mapper des imprimantes ou des lecteurs réseaux.

Configuration des machines Windows 7 pour joindre un domaine samba 3.6.x :
Les actions suivantes sur les stations de travail Windows 7 :

- Désactivation du pare feu (risque de problème avec les applications métiers).
- Désactivation de l'UAC (bloque les scripts de login qui effectue des actions d'administrations).
- Configuration d'IPV4 en tant que protocole réseau prioritaire sur IPV6.
- Démarrage du service Explorateur d'ordinateur si les utilisateurs utilisent le voisinage réseau.
- Activation des machines Windows avec des clés MAK.
- Appliquer la procédure suivante : https://wiki.samba.org/index.php/Windows7

Voir procédure dans le support de cours suivants :
http://msreport.free.fr/articles/Administration_Windows_7.pdf

1.2.8 CONFIGURATION DU SERVEUR DE TEMPS :

Configuration de la synchronisation horaire :
Le service NTPD sur MSREPORTPDC et MSREPORTBDC sera configuré pour se synchroniser avec une source de temps externe (client NTP).
Les machines Windows seront configurées pour se synchroniser sur les serveurs SAMBA MSREPORTPDC et MSREPORTBDC ou avec les mêmes serveurs de temps externes (ceux utilisés par les serveurs SAMBA).

Présentation du protocole NTP :
Les horloges atomiques, récepteurs GPS (sources de temps fiable) sont dit de strate 0 (niveau 0).
Les serveurs qui sont connectés sur ces horloges sont de de strate 1 (niveau 0).
Les serveurs NTP qui synchronisent leur heure sur ces serveurs sont dits de strate 2.
Il est recommandé de se synchroniser sur des serveurs de strate 2 comme :

- Time.Windows.com
- server 0.rhel.pool.ntp.org
- pool.ntp.org (il s'agit d'un cluster de serveur NTP publique)

Il n'est pas nécessaire de disposer d'une machine dédiée pour le service NTP. Un serveur NTP peut répondre à des milliers de machines.
La charge réseau généré par le protocole NTP est faible. Un paquet NTP fait environ 90 octets.
Le service NTP est basé sur le port UDP 123. Il sera donc nécessaire d'autoriser le trafic UDP 123 depuis MSREPORTPDC et MSREPORTBDC vers le serveur de temps.

Pour plus d'informations :
http://doc.ubuntu-fr.org/ntp
http://www.admin-sys.com/spip.php?article92

Le service NTP sous Windows XP / 7 :
Par défaut, les machines Windows XP membres d'un domaine Active Directory se synchronisent avec le contrôleur de domaine. Cela ne fonctionne pas avec un domaine SAMBA 3.6 car ce dernier est considéré comme un domaine NT4 par les stations de travail Windows XP / 7. Le message suivant apparaît dans les observateurs d'événements.

Log Name: System
Source: Microsoft-Windows-Time-Service
Date: 04/03/2013 23:08:54
Event ID: 13
Task Category: None
Level: Warning
Keywords:
User: LOCAL SERVICE
Computer: MSREPORTW7
Description:
Time Provider NtpClient: This machine is configured to use the domain hierarchy to determine its time source, but the computer is joined to a Windows NT 4.0 domain. Windows NT 4.0 domain controllers do not have a time service and do not support domain hierarchy as a time source…

Il est donc nécessaire de forcer les machines Windows de se synchroniser avec le PDC et le BDC en tapant la commande suivante :
w32tm /config /manualpeerlist:MSREPORTPDC,MSREPORTBDC /syncfromflags:manual /update

Cela modifie les clés suivantes :
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Parameters\Type : *passage de la valeur NT5DS à NTP*.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\W32Time\Parameters\NtpServer : *passage de la valeur time.windows.com,0x9 à MSREPORTPDC,MSREPORTBDC*

Le message suivant apparaît dans les observateurs d'événements Windows :
Log Name: System
Source: Microsoft-Windows-Time-Service
Date: 04/03/2013 23:33:40

Event ID: 37
Task Category: None
Level: Information
Keywords:
User: LOCAL SERVICE
Computer: MSREPORTW7
Description:
The time provider NtpClient is currently receiving valid time data from MSREPORTPDC (ntp.m|0x0|0.0.0.0:123->192.168.92.121:123).

Pour plus d'informations :
http://technet.microsoft.com/en-us/library/w32tm(v=ws.10).aspx

Le service NTP sous linux Red Hat Enterprise Linux :
Le service NTP de Red Hat Enterprise Linux 6 peut faire office de client NTP et de serveur NTP.
Il existe deux méthodes pour synchroniser l'heure depuis un autre serveur NTP (client NTP) :

- Avec l'outil NTPDATE
- Avec le service NTPD.

Ces deux méthodes ne peuvent pas être utilisées en même temps.

Il est possible de restreindre de restreindre les accès au serveur NTP :
http://support.ntp.org/bin/view/Support/AccessRestrictions
Pour permettre au serveur NTP se synchroniser avec une autre source de temps, il faut autoriser les sources de temps externe à accéder au serveur NTP :
server x.y.z.w
Où *x.y.z.w* est la source de temps externe.
Pour plus d'informations :
http://support.ntp.org/bin/view/Support/AccessRestrictions

1.2.9 CONFIGURATION DES STRATEGIES DE MOTS DE PASSE :

Les stratégies de mots de passe suivantes pour le domaine SAMBA seront mises en place pour les comptes utilisateurs standards :

- Mot de passe avec 8 caractères.
- Expiration des mots de passe au bout de 90 jours.
- Verrouillage du compte au bout de 10 erreurs pendant 1 minute (déverrouillage automatique).
- Complexité des mots de passe activé.

Le compte utilisateur utilisé pour démarrer des services (comptes de services) seront configurés pour que le mot de passe n'expire jamais.

2 INSTALLATION ET CONFIGURATION DE REDHAT ENTERPRISE LINUX :

2.1 INSTALLATION DE REDHAT ENTERPRISE LINUX 6.3 :

Lancer l'installation depuis le DVD de RedHat 6.2.
Par défaut, RedHat s'installe sans interface graphique.
Pour déployer un serveur avec interface graphique, sélectionner la case « Personnaliser maintenant ».
Aller dans Bureaux et cocher « *Système X Windows* » et « *Bureau* ». Cela permet d'installer l'interface GNOME.
Une fois l'installation terminée, un assistant apparaît et demande à créer un compte utilisateur avec des accès standard.

2.2 ACTIVATION DE REDHAT ENTERPRISE 6.X :

Le serveur RedHat doit maintenant être activé. Pour cela, taper la commande suivant : *rhn_register*
Entrer vos identifiants (fournis par RED Hat).

2.3 MISE A JOUR DU SYSTEME :

La commande suivant permet d'afficher la liste des mises à jour nécessaire :
Yum check-update
Pour mettre à jour le système, taper la commande :
yum update

2.4 INSTALLATION DES VMWARE TOOLS (EXEMPLE AVEC VMWARE WORKSTATION) :

Si vous déployer les 4 machines sur une plateforme de virtualisation comme VMware Workstation 9 ou VMware ESX, il est nécessaire d'installer les VMware Tools.

Installer les headers de RedHat Enterprise Linux 6.X :
*Yum install kernel-devel-**
Installer GCC pour compiler les VMware Tools.
Yum install gcc
Sous VMware Workstation 9, aller dans le menu *VM* | *Install VMware Tools*.
Créer un dossier */VMwaretools : mkdir /VMwareTools*
Copier le fichier les VMwareTools dans */VMwaretools.*
Se positionner dans /VMwareTools : cd */VMwaretools*
Décompresser le fichier VMTools *tar xzf /VMwaretools/VMwareTools-8.4.2-261058.tar.gz*
Se positionner dans le répertoire *cd /VMwaretools/vmware-tools-distrib/*
Lancer le script *./vmware-install.pl*
Répondre par défaut aux questions (touche entrée).
Les VMware Tools doivent s'installer et le CD-Rom virtuel se démonte automatiquement.

2.5 CONFIGURATION DE LA CARTE RESEAU ET DU NOM DE LA MACHINE :

La configuration réseau se fait via l'édition des fichiers suivant :
/etc/sysconfig/network-scripts/ifcfg-eth0
/etc/resolv.conf

Il est aussi possible de définir la configuration réseau via l'interface graphique (si installation des outils de gestion réseau d'interface graphique). L'utilisation de l'interface graphique modifie les fichiers */etc/sysconfig/network-scripts/ifcfg-eth0* et /etc/resolv.conf
Attention si l'interface graphique est utilisée, la configuration du fichier */etc/resolv.conf* est écrasée automatiquement par le « *Network Manager* ».

2.6 DESACTIVATION DU PARE FEU ET DE SELINUX :

SELINUX et un pare feu sont actifs par défaut sous RedHat Linux Enterprise 6.X.
Pour désactiver le pare feu, taper la commande *ntsysv* pour afficher la liste des services actifs au démarrage.
Désactiver les services *iptables* et *ip6tables*.

Désactiver SELINUX en éditant le fichier */etc/selinux/config* et en configurant la ligne suivante :
SELINUX=disabled

2.7 CONFIGURATION DES NOMS DE MACHINE :

Sur MSREPORTPDC, taper la commande suivante pour définir le nom de la machine :
hostname MSREPORTPDC
Sur MSREPORTBDC, taper la commande suivante pour définir le nom de la machine :
hostname MSREPORTBDC
Sur MSREPORTINF1, taper la commande suivante pour définir le nom de la machine :
hostname MSREPORTINF1

3 DEPLOIEMENT DE L'ARCHITECTURE CIBLE SAMBA :

3.1 INSTALLATION DES PAQUETS OPENLDAP, SAMBA ET SMBLDAPTOOLS :

3.1.1 MISE A JOUR DES PAQUAGES YUM :

Sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
Ajouter les dernières sources SAMBA :
cd /etc/yum.repos.d
wget http://ftp.sernet.de/pub/samba/3.6/rhel/6/sernet-samba.repo
Ajouter Perl-Crypt (prérequis pour installer smbldap-tools) :
wget http://pkgs.repoforge.org/perl-Crypt-SmbHash/perl-Crypt-SmbHash-0.12-1.2.el6.rf.noarch.rpm
Ajouter le RPM pour SMBLDAP-TOOLS :
wget http://download.gna.org/smbldap-tools/packages/el6/smbldap-tools-0.9.9-1.el6.noarch.rpm

3.1.2 INSTALLATION DES COMPOSANTS OPENLDAP :

Sur MSREPORTPDC et MSREPORTBDC uniquement :
Taper la commande suivante :
yum install openldap openldap-clients openldap-servers perl-LDAP
Vérifier que tous les composants nécessaires sont installés en tapant la commande :
rpm -qa | grep ldap

3.1.3 INSTALLATION DES COMPOSANTS SAMBA :

Sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
Taper la commande suivante :
yum install samba3 samba3-winbind samba3-utils samba3-doc samba3-client
Vérifier que tous les composants nécessaires sont installés en tapant la commande :
rpm -qa | grep samba

3.1.4 INSTALLATION DES COMPOSANTS SMBLDAP-TOOLS :

SMBLDAP-TOOLS est une suite de commande qui va nous permettre d'administrer le serveur SAMBA / OpenLDAP (création de comptes utilisateur / groupes / comptes ordinateur / définition des mots de passe….).

Sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
Taper les commandes suivantes :
*yum install perl-Crypt-SmbHash**
*yum install smbldap-tools**

3.2 CONFIGURATION D'OPEN LDAP :

On va maintenant configurer les serveurs MSREPORTPDC et MSREPORTBDC en tant que serveur OpenLDAP avec un accès en lecture / écriture. Les deux serveurs seront configurés pour répliquer la base OpenLDAP en mode MIRROIR.

3.2.1 ARRETER LE SERVICE OPENLDAP SUR MSREPORTPDC ET MSREPORTBDC :

Taper la commande ci-dessous pour arrêter le service OpenLDAP :
service slapd stop

3.2.2 CONFIGURER OPENLDAP POUR UTILISER UNIQUEMENT LE FICHIER SLAPD.CONF :

Il a été validé que le fichier SLAPD.CONF serait utilisé pour gérer la configuration du serveur OpenLDAP (au lieu du conteneur CN=CONFIG).

Taper la commande suivante pour éditer le fichier de configuration centrale d'OpenLDAP :
vi /etc/sysconfig/ldap
Remplacer la ligne
#SLAPD_OPTIONS=
Par la ligne
SLAPD_OPTIONS="-f /etc/openldap/slapd.conf"

Déplacer le dossier */etc/openldap/slapd.d*. Cela déplace en fait tous les fichiers LDIF (permettant de charger les entrées dans CN=CONFIG).
mv /etc/openldap/slapd.d /tmp/slapd.d.old

Complément d'informations :
Si le répertoire */etc/openldap/slapd.d* est absent, le fichier */etc/openldap/slapd.conf* est utilisé.
Si la ligne *SLAPD_OPTIONS="-f /etc/openldap/slapd.conf"* est présente dans le fichier */etc/sysconfig/ldap*, le fichier */etc/openldap/slapd.conf* est utilisé.
https://access.redhat.com/kb/docs/DOC-60150
https://access.redhat.com/kb/docs/DOC-48122

3.2.3 DEFINIR LE MOT DE PASSE DU MANAGER :

Taper la commande suivante pour définir le mot de passe du Manager.
slappasswd -v -s Msreport -h {SSHA}

Cette commande génère un HASH du mot de passe du compte Manager qu'il faudra copier au niveau de la ligne rootpw dans le fichier slapd.conf (section en rouge dans le paragraphe suivant).
rootdn "cn=Manager,DC=MSREPORT,DC=LAN"
rootpw {SSHA}vlD90UNVapN6H1ZolUUxnh4JrpFBvWpq

3.2.4 CREER LE FICHIER SLAPD.CONF :

Sur le serveur MSREPORTPDC :
Taper la commande suivante pour créer le fichier slapd.conf :
vi /etc/openldap/slapd.conf
Taper la lettre i pour passer en mode insertion et copier le contenu ci-dessous dans le fichier :

```
####### CHARGEMENT SCHEMA

# Chargement des classes OpenLdap standard
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
```

```
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema

# Ajout du schéma SAMBA
include         /etc/openldap/schema/samba3.schema

# AUTORISER LDAP V2
allow bind_v2

# FICHIER SYSTEME OPEN LDAP
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args

# CONFIGURATION DU NIVEAU DE LOG
loglevel 0

# CHARGEMENT DES MODULES
modulepath /usr/lib64/openldap/
# Pour la gestion des stratégies de mots de passe
moduleload ppolicy.la

# TAILLE DES REQUETES (1000 réponses, TimeOut au bout de 10 minutes)
sizelimit 10000
timelimit 600

# DEFINITION BASE DE DONNEEES
serverID 1
database        bdb
suffix          "DC=MSREPORT,DC=LAN"
# Création d'un checkpoint tous les 15 minutes ou tous les 1 Mo écriture
checkpoint      1024 15
# Définit la taille en mémoire réservée pour la base de données (taille recommandée = taille base de données)
cachesize 2000
cachefree 25
# Définit la taille en mémoire réservée pour une requête (taille recommandée = taille cachesize)
idlcachesize 2000
rootdn          "cn=Manager,DC=MSREPORT,DC=LAN"
rootpw          {SSHA}vlD90UNVapN6H1ZolUUxnh4JrpFBvWpq
# Le répertoire de la base OpenLDAP
directory       /var/lib/ldap

# INDEXES
# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname,displayName      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index uniqueMember                      eq,pres
index nisMapName,nisMapEntry            eq,pres,sub
index mailLocalAddress                  eq,pres

# index pour le controleur de domaine SAMBA
```

```
index sambaSID                          eq
index sambaSIDList              eq
index sambaGroupType                    eq
index sambaPrimaryGroupSID      eq
index sambaDomainName           eq

# REPLICATION
syncrepl rid=001
  provider=ldap://192.168.92.125
  type=refreshAndPersist
  retry="60 +"
  searchbase="DC=MSREPORT,DC=LAN"
  scope=sub
  schemachecking=on
  bindmethod=simple
  binddn="cn=Manager,DC=MSREPORT,DC=LAN"
  credentials="Msreport"
mirrormode true
moduleload syncprov
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
index entryCSN,entryUUID        eq

# MONITORING
database monitor

# GESTION DES DROITS SUR LA BASE OPENLDAP

access to attrs=userPassword,sambaNTPassword,sambaLMPassword
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="cn=syncrepl,DC=MSREPORT,DC=LAN" read
        by self write
        by anonymous auth
        by * none

# ACL d acces a la branche Netasq (vpn ssl)
access to dn="ou=conf,DC=MSREPORT,DC=LAN"
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="cn=NetasqAdmin,DC=MSREPORT,DC=LAN" write
        by * none

# ACL d acces a l annuaire complet (regle par defaut)
access to *
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="uid=root,ou=Utilisateurs,DC=MSREPORT,DC=LAN" write
        by self write
        by dn="cn=syncrepl,DC=MSREPORT,DC=LAN" read
        by dn="cn=ennovSync,DC=MSREPORT,DC=LAN" read
        by * read
```

Pour plus d'informations sur le paramètre checkpoint :
http://www.zytrax.com/books/ldap/ch6/bdb.html
Pour plus d'informations sur les limites :
http://www.openldap.org/doc/admin24/limits.html
Pour les paramètres « *cacheSize* » et « *idlcachesize* » :
http://www.openldap.org/doc/admin24/tuning.html

Sur le serveur MSREPORTBDC :
Taper la commande suivante pour créer le fichier slapd.conf :
vi /etc/openldap/slapd.conf
Taper la lettre i pour passer en mode insertion et copier le contenu ci-dessous dans le fichier.

```
####### CHARGEMENT SCHEMA

# Chargement des classes OpenLdap standard
include         /etc/openldap/schema/corba.schema
include         /etc/openldap/schema/core.schema
include         /etc/openldap/schema/cosine.schema
include         /etc/openldap/schema/duaconf.schema
include         /etc/openldap/schema/dyngroup.schema
include         /etc/openldap/schema/inetorgperson.schema
include         /etc/openldap/schema/java.schema
include         /etc/openldap/schema/misc.schema
include         /etc/openldap/schema/nis.schema
include         /etc/openldap/schema/openldap.schema
include         /etc/openldap/schema/ppolicy.schema
include         /etc/openldap/schema/collective.schema

# Ajout du schéma SAMBA
include         /etc/openldap/schema/samba3.schema

# AUTORISER LDAP V2
allow bind_v2

# FICHIER SYSTEME OPEN LDAP
pidfile         /var/run/openldap/slapd.pid
argsfile        /var/run/openldap/slapd.args

# CONFIGURATION DU NIVEAU DE LOG
loglevel 0

# CHARGEMENT DES MODULES
modulepath /usr/lib64/openldap/
# Pour la gestion des stratégies de mots de passe
moduleload ppolicy.la

# TAILLE DES REQUETES (1000 réponses, TimeOut au bout de 10 minutes)
sizelimit 10000
timelimit 600

# DEFINITION BASE DE DONNEEES
serverID 2
database        bdb
suffix          "DC=MSREPORT,DC=LAN"
# Création d'un checkpoint tous les 15 minutes ou tous les 1 Mo écriture
checkpoint      1024 15
# Définit la taille en mémoire réservée pour la base de données (taille recommandée = taille base de données)
cachesize 2000
cachefree 25
# Définit la taille en mémoire réservée pour une requête (taille recommandée = taille cachesize)
idlcachesize 2000
rootdn          "cn=Manager,DC=MSREPORT,DC=LAN"
rootpw          {SSHA}vlD90UNVapN6H1ZolUUxnh4JrpFBvWpq
# Le répertoire de la base OpenLDAP
directory       /var/lib/ldap

# INDEXES
```

```
# Indices to maintain for this database
index objectClass                       eq,pres
index ou,cn,mail,surname,givenname,displayName      eq,pres,sub
index uidNumber,gidNumber,loginShell    eq,pres
index uid,memberUid                     eq,pres,sub
index uniqueMember                      eq,pres
index nisMapName,nisMapEntry            eq,pres,sub
index mailLocalAddress                  eq,pres

# index pour le controleur de domaine SAMBA
index sambaSID                                  eq
index sambaSIDList                      eq
index sambaGroupType                            eq
index sambaPrimaryGroupSID              eq
index sambaDomainName                   eq

# REPLICATION
syncrepl rid=001
  provider=ldap://192.168.92.121
  type=refreshAndPersist
  retry="60 +"
  searchbase="DC=MSREPORT,DC=LAN"
  scope=sub
  schemachecking=on
  bindmethod=simple
  binddn="cn=Manager,DC=MSREPORT,DC=LAN"
  credentials="Msreport"
mirrormode true
moduleload syncprov
overlay syncprov
syncprov-checkpoint 100 10
syncprov-sessionlog 100
index entryCSN,entryUUID                eq

# MONITORING
database monitor

# GESTION DES DROITS SUR LA BASE OPENLDAP

access to attrs=userPassword,sambaNTPassword,sambaLMPassword
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="cn=syncrepl,DC=MSREPORT,DC=LAN" read
        by self write
        by anonymous auth
        by * none

# ACL d acces a la branche Netasq (vpn ssl)
access to dn="ou=conf,DC=MSREPORT,DC=LAN"
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="cn=NetasqAdmin,DC=MSREPORT,DC=LAN" write
        by * none

# ACL d acces a l annuaire complet (regle par defaut)
access to *
        by dn="cn=Manager,DC=MSREPORT,DC=LAN" write
        by dn="uid=root,ou=Utilisateurs,DC=MSREPORT,DC=LAN" write
        by self write
        by dn="cn=syncrepl,DC=MSREPORT,DC=LAN" read
        by dn="cn=ennovSync,DC=MSREPORT,DC=LAN" read
        by * read
```

3.2.5 SUPPRESSION DES BASES DE DONNEES EXISTANTES :

Taper les commandes suivantes pour supprimer les bases de données existantes :
*rm -fr /var/lib/ldap/**

Copier le fichier DB_CONFIG (optimisation des performances) :
cp -p /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/DB_CONFIG

3.2.6 CONFIGURER LE COMPTE OPENLDAP EN TANT QUE PROPRIETAIRE SUR TOUS LES DOSSIERS OPENLDAP :

Sous RedHat le service OpenLDAP s'exécute dans le contexte du compte local ldap (/etc/passwd).
Il faut donc définir le compte ldap et le groupe ldap comme propriétaire des dossiers utilisés par OpenLDAP. Pour cela, taper la commande suivante :
*chown ldap:ldap /var/lib/ldap/**
*chown ldap:ldap /etc/openldap/**
chown ldap:ldap /usr/sbin/slapd

3.2.7 VALIDATION DE LA CONFIGURATION D'OPENLDAP ET DEMARRAGE D'OPENLDAP :

Taper la commande suivante pour valider la configuration de la base OpenLDAP :
slaptest
Des erreurs peuvent apparaître à cette étape.
Elles sont liés au fait que l'on a supprimé initialement tous les fichiers du répertoire */var/lib/ldap* qui contenait toutes les bases systèmes.
Démarrer OpenLDAP :
service slapd start

Les bases de données OpenLDAP système sont régénérées à cette étape. Le compte est propriétaire de ces fichiers.
Il faut donc relancer la commande suivante pour définit le compte et le groupe ldap comme propriétaire.
*chown ldap:ldap /var/lib/ldap/**

Taper la commande suivante pour valider la configuration de la base OpenLDAP :
slaptest
Vous devez obtenir le résultat suivant.

Redémarrer OpenLDAP
service slapd restart

3.3 CONFIGURATION DU SERVEUR DE TEMPS SUR LES SERVEURS MSREPORTPDC ET MSREPORTBDC :

Rappel configuration :
Le service NTPD sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 sera configuré pour se synchroniser avec une source de temps externe (client NTP).
Les machines Windows seront configurées pour se synchroniser sur les contrôleurs de domaine. Les serveurs MSREPORTPDC et MSREPORTBDC seront donc serveurs de temps.

Pour configurer le service NTP sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
Configurer le service NTD pour démarrer automatiquement :
Taper la commande *ntsysv*
Sauvegarder le fichier */etc/ntp.conf*.
Taper la commande suivante pour éditer le fichier :
vi /etc/ntp.conf
On va pour cela s'appuyer sur le document suivant :

https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/sect-Date_and_Time_Configuration-Command_Line_Configuration-Network_Time_Protocol.html

Remplacer le contenu du fichier */etc/ntp.conf* par :

```
# Adresse IP en écoute (toutes) :
listen on *
# Permet de spécifier les serveurs de temps.
# Le paramètre iburst permet d'accélérer la synchronisation initiale
server time.windows.com iburst
server 0.rhel.pool.ntp.org iburst
server 1.rhel.pool.ntp.org iburst
server 2.rhel.pool.ntp.org ibust

# Fichier qui stocke le décalage horaire :
driftfile /var/db/ntp.drift
# PERMISSION
# No query : les clients ne peuvent pas obtenir d'informations sur le statut du service NTPD.
# No modify : les clients ne peuvent pas changer la configuration du serveur NTP
# No serve : les clients ne peuvent pas mettre à jour leur heure à partir du serveur NTP
# Voir http://www.gsp.com/cgi-bin/man.cgi?topic=ntp.conf
# Permettre un accès non restreint à la LOCAHOST (IPV4 only)
restrict 127.0.0.1
# Autoriser réseau 192.168.92.0 à se synchroniser avec ce serveur
restrict 192.168.92.0 mask 255.255.255.0 kod nomodify notrap nopeer noquery
# Interdire le trafic IPV6
restrict -6 default ignore
```

Taper la commande suivante pour forcer la synchronisation horaire :
service ntpd restart

Taper la commande suivante pour valider la configuration du serveur NTP :
ntpq -p 127.0.0.1

Analyse résultat de la commande NTPQ :
Offset : la différence en milliseconde entre le serveur NTP local et son serveur de temps.
Delay : le nombre de milliseconde pour faire un allé / retour entre le serveur NTP local et son serveur de temps.
Refid : indique le serveur de temps utilisé par ce serveur NTP.
St : c'est le niveau du serveur NTP utilisé (niveau 2 dans l'exemple).
When : nombre de secondes depuis la dernière synchronisation entre le serveur NTP et le serveur de temps.
On peut voir dans l'exemple ci-dessous qu'un seul serveur est de strate 3.
Vérifier si le serveur est synchronisé (c'est le cas sur la capture ci-dessous).
ntpstat
La commande date permet de connaître l'heure et la date en cours.

3.4 CONFIGURATION DES SERVEURS DE TEMPS SUR LES MACHINES WINDOWS XP ET WINDOWS 7 :

Les machines Windows XP et Windows 7 ne sont pas capables de se synchroniser avec un contrôleur de domaine NT4 (SAMBA 3.6.X).
Il est donc nécessaire d'exécuter au moins une fois cette commande sur les stations de travail :
w32tm /config /manualpeerlist:MSREPORTPDC,MSREPORTBDC /syncfromflags:manual /update

3.5 CONFIGURATION DE SAMBA SUR MSREPORTPDC ET MSREPORTBDC :

Cette étape va nous permettre de configurer le PDC et BDC du domaine MSREPORT.
La configuration du serveur MSREPORTINF1 se fera plus loin dans ce document.

3.5.1 ARRETER LES SERVICES SAMBA :

Taper la commande suivante sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
service smb stop
Le service SAMBA sera redémarré après configuration.

3.5.2 COPIER LE FICHIER SMB.CONF SUIVANT SUR MSREPORTPDC :

Copier le contenu suivant dans le fichier */etc/samba/smb.conf* :

```
[global]
        dos charset = 850
        unix charset = ISO8859-1
        workgroup = MSREPORT
        server string =
        map to guest = Bad User
        passdb backend = ldapsam:"ldap://127.0.0.1 ldap://192.168.92.125"
        passwd program = /usr/sbin/smbldap-passwd -u "%u"
        passwd chat = "Changing password for*\nNew password*" %n\n "*Retype new password*" %n\n"
        unix password sync = Yes
        syslog = 0
        log file = /var/log/samba/%m.log
        max log size = 500
        smb ports = 139
        time server = Yes
        deadtime = 15
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        add user script = /usr/sbin/smbldap-useradd -m "%u"
        delete user script = /usr/sbin/smbldap-userdel "%u"
        add group script = /usr/sbin/smbldap-groupadd -p "%g"
        delete group script = /usr/sbin/smbldap-groupdel "%g"
        add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
        delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
        set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
        add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
        logon script = script.vbs
        logon path =
        logon home = \\MSREPORTINF1\perso\%U
        logon drive = H:
        domain logons = Yes
        os level = 65
        preferred master = Yes
        domain master = Yes
        wins support = Yes
        ldap admin dn = cn=Manager,DC=MSREPORT,DC=LAN
        ldap group suffix = ou=Groupes
        ldap machine suffix = ou=Machines
        ldap suffix = DC=MSREPORT,DC=LAN
    ldap ssl = no
        ldap user suffix = ou=Utilisateurs
        create mask = 0770
        directory mask = 0770
        case sensitive = No
```

```
        veto files = /lost+found/.recycle/.Desktop/.bash_history/
        hide files = /~$*.doc/~WRL*.tmp/
        dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
    security = user
    template shell = /bin/false

[netlogon]
        comment = Network Logon Service
        path = /home/netlogon/
        write list = @informatique,root
        browseable = Yes

[homes]
    comment = Repertoire personnel
    browseable = no
    writeable = yes
```

Pour plus d'informations :
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html

3.5.3 COPIER LE FICHIER SMB.CONF SUIVANT SUR MSREPORTBDC :

Copier le contenu suivant dans le fichier */etc/samba/smb.conf* :

```
[global]
        dos charset = 850
        unix charset = ISO8859-1
        workgroup = MSREPORT
        server string =
        map to guest = Bad User
        passdb backend = ldapsam:"ldap://127.0.0.1 ldap://192.168.92.121"
        passwd program = /usr/sbin/smbldap-passwd -u "%u"
        passwd chat = "Changing password for*\nNew password*" %n\n "*Retype new password*" %n\n"
        unix password sync = Yes
        syslog = 0
        log file = /var/log/samba/%m.log
        max log size = 500
        smb ports = 139
        time server = Yes
        deadtime = 15
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        printcap name = cups
        add user script = /usr/sbin/smbldap-useradd -m "%u"
        delete user script = /usr/sbin/smbldap-userdel "%u"
        add group script = /usr/sbin/smbldap-groupadd -p "%g"
        delete group script = /usr/sbin/smbldap-groupdel "%g"
        add user to group script = /usr/sbin/smbldap-groupmod -m "%u" "%g"
        delete user from group script = /usr/sbin/smbldap-groupmod -x "%u" "%g"
        set primary group script = /usr/sbin/smbldap-usermod -g "%g" "%u"
        add machine script = /usr/sbin/smbldap-useradd -t 0 -w "%u"
        logon script = script.vbs
    logon home = \\MSREPORTINF1\perso\%U
    logon drive = H:
        logon path =
        domain logons = Yes
        os level = 65
        preferred master = No
        domain master = No
        wins server = 192.168.92.121
        ldap admin dn = cn=Manager,DC=MSREPORT,DC=LAN
```

```
        ldap group suffix = ou=Groupes
        ldap machine suffix = ou=Machines
        ldap suffix = DC=MSREPORT,DC=LAN
        ldap ssl = no
        ldap user suffix = ou=Utilisateurs
        create mask = 0770
        directory mask = 0770
        case sensitive = No
        veto files = /lost+found/.recycle/.Desktop/.bash_history/
        hide files = /~$*.doc/~WRL*.tmp/
        dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
    security = user
    template shell = /bin/false

[homes]
        comment = Repertoire personnel
        browseable = no
        writeable = yes
[netlogon]
        comment = Network Logon Service
        path = /home/netlogon/
        write list = @informatiquei,root
        browseable = Yes
```

3.5.4 CORRECTION DES ERREURS REMONTEES PAR LA COMMANDE SLAPTEST :

L'utilitaire *testparm* peut remonter les erreurs suivantes : *rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)*
Pour corriger cette erreur, éditer le fichier */etc/security/limits.conf*
Ajouter au début du fichier, la chaine de caractère suivante : ** - nofile 16384*
Redémarrer le serveur SAMBA.

3.5.5 CONFIGURATION DU FICHIER SECRET.TDB SUR MSREPORTBDC :

Démarrer le service OpenLDAP sur MSREPORTPDC et MSREPORTBDC.
service slapd start
Arrêter le service SAMBA sur MSREPORTPDC et MSREPORTBDC
service smb stop
A l'aide d'Apache Directory, relever la valeur du SID du domaine :
Dans notre cas le SID du domaine est *S-1-5-21-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXXX*
Sur MSREPORTPDC uniquement, taper les commandes suivantes :

```
cp /etc/samba/secrets.tdb /etc/samba/secrets.tdb.bak
rm /etc/samba/secrets.tdb
smbpasswd -w Msreport
net setlocalsid S-1-5-21-1389896759-1016571666-2475258077
service smb start
net rpc getsid
net getlocalsid
```

Taper la commande suivante pour valider le contenu du fichier TDB :
tdbdump /etc/samba/secrets.tdb

Sur <u>MSREPORTBDC uniquement</u>, taper les commandes suivantes :

```
cp /etc/samba/secrets.tdb /etc/samba/secrets.tdb.bak
rm /etc/samba/secrets.tdb
smbpasswd -w Msreport
net setlocalsid S-1-5-21-1389896759-1016571666-2475258077
```

service smb start
net rpc getsid
net getlocalsid

Taper la commande suivante pour valider le contenu du fichier TDB :
tdbdump /etc/samba/secrets.tdb

3.6 CONFIGURATION DE SMBLDAP-TOOLS :

Cette action doit être effectuée sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1.

3.6.1 MODIFIER LE FICHIER /ETC/SMBLDAP-TOOLS/SMBLDAP.CONF

Taper la commande *vi /etc/smbldap-tools/smbldap.conf* et copier le contenu suivant :

```
SID="S-1-5-21-XXXXXXXXXX- XXXXXXXXXX - XXXXXXXXXX"
sambaDomain="MSREPORT"
masterLDAP="ldap://192.168.92.121"
slaveLDAP="ldap://192.168.92.125"
ldapTLS="0"
verify="require"
cafile="/etc/smbldap-tools/ca.pem"
clientcert="/etc/smbldap-tools/smbldap-tools.example.com.pem"
clientkey="/etc/smbldap-tools/smbldap-tools.example.com.key"
# LDAP Suffix
suffix="DC=MSREPORT,DC=LAN"
usersdn="ou=Utilisateurs,${suffix}"
computersdn="ou=Machines,${suffix}"
groupsdn="ou=Groupes,${suffix}"
idmapdn="ou=Idmap,${suffix}"
sambaUnixIdPooldn="sambaDomainName=${sambaDomain},${suffix}"
# Default scope Used
scope="sub"
password_hash="SSHA"
password_crypt_salt_format="%s"
# Unix Accounts Configuration
userLoginShell="/bin/bash"
# Home directory
userHome="/home/%U"

# Default mode used for user homeDirectory
userHomeDirectoryMode="700"
# Gecos
userGecos="System User"
# Default User (POSIX and Samba) GID
defaultUserGid="513"
# Default Computer (Samba) GID
defaultComputerGid="515"
# Skel dir
skeletonDir="/etc/skel"
# Treat shadowAccount object or not
shadowAccount="1"
# Default password validation time (time in days) Comment the next line if
# you don't want password to be enable for defaultMaxPasswordAge days (be
# careful to the sambaPwdMustChange attribute's value)
defaultMaxPasswordAge="45"
# SAMBA Configuration
userSmbHome=""
userProfile=""
userHomeDrive=""
userScript=""
```

mailDomain=""
 # Allows not to use smbpasswd (if with_smbpasswd="0" in smbldap.conf) but
 # prefer Crypt::SmbHash library
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
 # Allows not to use slappasswd (if with_slappasswd="0" in smbldap.conf)
 # but prefer Crypt:: libraries
with_slappasswd="0"
slappasswd="/usr/sbin/slappasswd"

Pour obtenir le SID du domaine (élément en rouge à changer), il faut taper la commande
net getlocalsid

3.6.2 MODIFIER LE FICHIER /ETC/SMBLDAP-TOOLS/SMBLDAP_BIND.CONF

Créer le fichier /etc/smbldap-tools/smbldap_bind.conf avec le contenu ci-dessous :
masterDN="cn=admin,dc=msreport,dc=lan"
masterPw="Msreport"
slaveDN="cn=admin,dc=msreport,dc=lan"
slavePw="Msreport"

3.6.3 PEUPLER LA BASE OPENLDAP (CREATION DES OU DE BASES) :

On va maintenant écrire dans l'annuaire et préparer l'arborescence de domaine.
Pour cela on va lancer la commande suivante :
smbldap-populate

3.7 CONFIGURATION DU SERVICE SSSD :

Cette action est à effectuer que sur MSREPORTPDC et MSREPORTBDC. Elle sera effectuée plus loin pour MSREPORTINF1.

3.7.1 METHODE MANUELLE :

Comme expliqué dans la documentation RedHat (paragraphes 11.2.5 et 11.2.6) disponible à l'adresse
https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/Configuration_Options-NSS_Configuration_Options.html

Sur MSREPORTPDC et MSREPORTBDC, copier le contenu ci-dessous dans le fichier */etc/nsswitch.conf*

passwd: files sss
shadow: files sss
group: files sss
hosts: files wins dns
bootparams: nisplus [NOTFOUND=return] files
ethers: files
netmasks: files
networks: files
protocols: files
rpc: files
services: files
netgroup: files sss
publickey: nisplus
automount: files ldap
aliases: files nisplus

Sur MSREPORTPDC et MSREPORTBDC, copier le contenu ci-dessous dans le fichier */etc/sssd/sssd.conf.*

```
[sssd]
config_file_version = 2
services = nss, pam
domains = default
[nss]
[pam]
[domain/default]
auth_provider = ldap
ldap_id_use_start_tls = False
chpass_provider = ldap
cache_credentials = True
ldap_search_base = DC=MSREPORT,DC=LAN
id_provider = ldap
ldap_uri = ldap://192.168.92.121,ldap://192.168.92.125
```

Sur MSREPORTPDC et MSREPORTBDC, copier le contenu ci-dessous dans le fichier */etc/pam.d/system-auth* :

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        sufficient    pam_sss.so use_first_pass
auth        required      pam_deny.so
account     required      pam_unix.so broken_shadow
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     [default=bad success=ok user_unknown=ignore] pam_sss.so
account     required      pam_permit.so

password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so md5 shadow nullok try_first_pass use_authtok
password    sufficient    pam_sss.so use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
session     optional      pam_sss.so
```

3.7.2 METHODE AUTOMATIQUE :

Sur MSREPORTPDC et CHFGBDC, taper la commande suivante :
authconfig-tui
Cette commande va permettre d'éditer les fichiers */etc/nsswitch.conf*, */etc/sssd/sssd.conf* et */etc/pam.d/system-auth*

Sélectionner les cases suivantes dans la première fenêtre :
Utiliser LDAP
Utiliser des mots de passe MD5
Utiliser des mots de passe masqués
Utiliser l'authentification LDAP
Une autorisation locale est suffisante

Dans la fenêtre paramètres LDAP :
Serveur : ldap://192.168.92.121, ldap://192.168.92.125
DN de base : DC=msreport,dc=lan

Remarque :
La commande ci-dessous permet d'activer le support du service SSSD sans configurer l'adresse du serveur LDAP.
authconfig --enablesssd --update
Elle modifie automatiquement les fichiers */etc/nsswitch.conf*, */etc/sssd/sssd.conf* et */etc/pam.d/system-auth.*

3.8 RESYNCRHONISER LE MOT DE PASSE ROOT :

Effectuer cette action uniquement sur MSREPORTPDC :
smbldap-passwd root

3.9 CREATION DES REPERTOIRES SUR MSREPORTPDC ET MSREPORTBDC :

Remarque sur le répertoire NETLOGON :
Le contenu du répertoire */home/netlogon* devra être synchronisé manuellement car il contient les scripts d'ouverture de session. Comme ce répertoire est faiblement modifié, synchroniser le manuellement.
Il faut maintenant créer les dossiers NETLOGON et PROFILES indiqués dans le fichier *smb.conf*
mkdir /home/netlogon
mkdir /home/profiles
mkdir /home/public
chown root:"Domain Users" /home/netlogon /home/profiles /home/public
chmod 770 /home/netlogon
chmod 770 /home/profiles

Si on regarder les logs (*tail -f /var/log/samba/MSREPORTW7.log*) pendant la connexion avec le compte utilisateur *monique.mathieu*, on peut voir l'erreur suivante dans les logs :

Elle se produit quand le dossier personnel de l'utilisateur n'est pas créé. Elle génère aussi une lecteur à l'ouverture de session. Elle ralentit l'ouverture de session.
Pour que cela fonctionne il faut créer d'avance le répertoire personnel lors de la création du compte ou en le créer manuellement.

3.10 CONFIGURATION DE LA RESOLUTION WINS :

3.10.1 PRESENTATION DU SERVICE WINS ET DE LA RESOLUTION VIA LE FICHIER LMHOST :

Lire les documents suivant :
http://www.samba.org/samba/docs/using_samba/ch07.html
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html#id2566941
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetworkBrowsing.html#id2584196
http://support.microsoft.com/kb/150800/en-us
http://support.microsoft.com/kb/314108/fr

3.10.2 CONFIGURATION DU SERVEUR WINS MSREPORTPDC :

Se connecter sur MSREPORTPDC :
Vérifier que le serveur est en IP fixe (c'est déjà le cas à cette étape normalement).
Editer le fichier */etc/samba/smb.conf* :

Valider la présence des lignes suivantes dans le fichier SMB.CONF.
wins support = yes
dns proxy = no
name resolve order = wins lmhosts host bcast

Attention, le serveur WINS est obligatoirement client WINS de lui-même.
Ne pas définir le paramètre *wins server = 192.168.92.121* sur MSREPORTPDC : 192.168.92.121 dans l'exemple).

Dans le cas contraire on a l'erreur ci-dessous :
ERROR : both 'wins support = true' and 'wins server'= server list cannot be set in the smb.conf file….

3.10.3 CONFIGURATION DE MSREPORTBDC ET MSREPORTINF1 :

Comme il n'est pas possible / supporté de répliquer les bases WINS avec SAMBA 3.6.X, MSREPORTBDC sera configuré en tant que client WINS.

Se connecter sur MSREPORTBDC et MSREPORTINF1 :
Editer le fichier */etc/samba/smb.conf* :
Valider la présence des lignes suivantes dans le fichier SMB.CONF.
wins server = 192.168.92.121
Dans l'exemple ci-dessous l'adresse IP de MSREPORTPDC est 192.168.92.121.

Validation de la configuration du WINS sur MSREPORTPDC, MSREPORTBDC et MSREPORTINF1 :
Faire un ping du serveur MSREPORTPDC depuis MSREPORTBDC échoue à cette étape.

Sur MSREPORTPDC, MSREPORTBDC, MSREPORTINF1 :
Il faut configurer le fichier */etc/nsswitch.conf* afin de déclarer au système Red Hat Enterprise Linux qu'il doit utiliser le WINS pour la résolution de noms.
Pour cela, au niveau de la ligne HOSTS, ajouter *wins*.

Il est important de conserver l'entrée « *files* » au niveau de la ligne HOSTS car c'est cette dernière qui permet l'utilisation du fichier */etc/host*.

Taper la commande suivante pour afficher / purger le cache WINS et tester la résolution de noms sur la machine LINUX :
net cache list
net cache purge
net cache list
ping MSREPORTPDC

3.10.4 CONFIGURATION DE LA MACHINE WINDOWS (MSREPORTW7) :

La station de travail Windows 7 MSREPORTW7 va être configurée pour utiliser MSREPORTPDC comme serveur WINS.
Cette station de travail sera aussi configuré avec un fichier LMHOST afin que la station de travail soit capable de résoudre les entrées 1B et 1C du domaine en cas de panne du serveur WINS.

Pour rappel, la résolution de noms LMHOST est prioritaire sur Windows par rapport à la résolution WINS.
Si la station de travail et le PDC / BDC ne sont pas dans le même sous réseau et que la diffusion (BROADCAST) est bloquée au niveau des routeurs, la station de travail cliente doit obligatoirement être capable de résoudre les entrées 1C et 1B pour se connecter avec les comptes du domaine.

Pour définir MSREPORTPDC en tant que serveur WINS sur MSREPORTW7 :
Cliquer sur "*Start* | *Control Pannel* | *Network and Internet* | *Network and Sharing Center* | *Change adapter settings*"
Faire un clic droit et sélectionner « *Properties* » sur la carte réseau.
Sélectionner « *Internet Protocol Version 4* » et cliquer sur « *Properties* ».
Cliquer ensuite sur « ADVANCED ». Aller dans l'onglet WINS et taper l'IP de MSREPORTPDC.

Pour éditer le fichier LMHOST :
Editer avec NOTEPAD le fichier C:\Windows\System32\drivers\etc\lmhost.sam

Supprimer le contenu de ce fichier et ajouter les lignes suivantes :
192.168.92.121 "MSREPORT \0x1b" #PRE
192.168.92.121 MSREPORTPDC #PRE #DOM:MSREPORT
192.168.92.125 MSREPORTBDC #PRE #DOM:MSREPORT

Renommer le fichier en C:\Windows\System32\drivers\etc\lmhost.

D'après la base de connaissance Microsoft : http://support.microsoft.com/kb/314108/fr
« Notez également que DOMAIN_NAME, dans cette entrée, respecte la casse. Veillez à n'utiliser que des majuscules. Remplacez 10.0.0.1 par l'adresse IP de votre contrôleur principal de domaine, PDCName par le nom NetBIOS de votre contrôleur principal de domaine et DOMAIN_NAME par le nom de votre domaine Windows NT. ***Un espacement correct de ces entrées est obligatoire. Sur la ligne où apparaissent les guillemets ("), ces derniers doivent être séparés par 20 caractères exactement****. Pour obtenir ces 20 caractères, tapez le nom du domaine, ajoutez des espaces jusqu'à concurrence de 15 caractères, puis ajoutez la barre oblique inverse et le nombre hexadécimal NetBIOS qui représente le type de service. »*

Taper la commande *nbtstat -c* pour visualiser que les entrées du fichier LMHOST ont été prises en compte par la machine Windows. On doit voir les IP des contrôleurs de domaine SAMBA.

3.10.5 QUELQUES COMMANDES A CONNAITRE LIES A LA RESOLUTION DE NOMS NETBIOS (WINS / LMHOST) :

Pour éditer le contenu de la base WINS sur MSREPORTPDC :
vi /var/lib/samba/wins.dat

Pour gérer la résolution WINS / LMHOST sur une machine linux :
Pour voir le cache WINS : *net cache list*
Pour purger le cache WINS : *net cache flush*
Pour tester le bon fonctionnement de la résolution WINS / LMHOST sur une machine LINUX : *nmblookup*
Pour plus d'informations, voir http://www.linuxcertif.com/doc/keyword/nmblookup/

Pour gérer la résolution WINS / LMHOST sur une station de travail Windows :
Pour forcer la machine Windows à s'enregistrer dans la base WINS : *nbtstat –RR :*
Pour forcer la purge du cache WINS / LMHOST sur une machine Windows : *nbtstat –R*
Pour afficher le cache WINS / LMHOST sur une machine Windows : *nbtstat –c*

3.11 CONFIGURATION DES SCRIPTS DE LOGIN :

L'objectif est de mapper le lecteur réseau T:\ sur le répertoire partage1 de MSREPORTINF1.
Ouvrir une session avec le compte root du domaine MSREPORT.
Se connecter sur \\MSREPORTPDC\netlogon\
Configurer le profil de l'utilisateur root pour afficher les extensions de fichiers et les fichiers cachés et les fichiers systèmes.
Créer le fichier *script.vbs*
Copier le contenu ci-dessous dans le fichier *script.vbs*.

```
'On error Resume Next
Dim L1, M1
Set wshNetwork = CreateObject("WScript.Network")
Set ADSysInfo = CreateObject("ADSystemInfo")
DelPart("T")
MapDrv "T","\\MSREPORTINF1\public"

'Fonction de suppression des mappages réseau
Function DelPart(L1)
Dim L1b
Set WshNetwork = CreateObject("WScript.Network")
Set fso = CreateObject("Scripting.filesystemobject")
If fso.DriveExists(L1) Then
 L1b = L1&":"
 WshNetwork.RemoveNetworkDrive L1b, True, True
End If
End Function

'Fonction de mappage des lecteurs reseau
Function MapDrv(M1,M2)
```

Dim M1b
Set WshNetwork = CreateObject("WScript.Network")
M1b = M1&":"
WshNetwork.MapNetworkDrive M1b, M2
End Function

Recopier ce fichier sur \\MSREPORTBDC\netlogon.
Tester l'exécution manuelle de ce script en tapant la commande : *cscript \\MSREPORTPDC\netlogon\script.vbs*
Le fichier *smb.conf* de MSREPORTPDC et MSREPORTBDC doit contenir le paramètre suivant pour que tous les utilisateurs mappent le lecteur T à l'ouverture de session : *logon script = script.vbs*
Vérifier que tous les utilisateurs ont accès au script.
chmod 774 /home/netlogon/script.vbs

3.12 CONFIGURATION DU HOME FOLDER :

Comme nous disposons de deux contrôleurs de domaine, déplacer les données utilisateurs (répertoire Home) vers un nouveau partage appelé *PERSO* sur le serveur de fichiers MSREPORTINF1.

Sur MSREPORTINF1, créer le partage [homes] masqué.

[perso]
comment = Repertoire personnel
path = /profiles
browseable = No
writeable = Yes

Pour chaque utilisateur il sera nécessaire de créer un dossier correspondant à cet utilisateur dans ce répertoire.
L'utilisateur sera le seul à accéder à ce répertoire et sera propriétaire de ce dossier.
chmod 770 /profiles/cleo.mathieu/
Seul root dispose des accès à ce répertoire. Par défaut le niveau d'accès est 744. Tous les autres utilisateurs ont un accès en lecture.
Pour des raisons inconnus, SAMBA sur la maquette semble ignorer les permissions EXT4 données à un utilisateur individuellement sur un dossier.
Il faut ajouter notre utilisateur à un groupe (où il sera seul) et donner des permissions à ce groupe.
Cela fonctionne alors.
setfacl -m g:test75:rwx /profiles/cleo.mathieu

Configurer le fichier smb.conf de MSREPORTPDC et MSREPORTBDC pour rediriger vers ce répertoire Home.
logon home = \\MSREPORTINF1\perso\%U
logon drive = H:

3.13 CONFIGURATION DES STRATEGIES DE MOTS DE PASSE :

Définir la taille minimum du mot de passe :
pdbedit -P "min password length" -C 8

Définir la durée de vie minimum du mot de passe :
pdbedit -P " minimum password age" -C 0

Voir : http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/passdb.html

3.14 CONFIGURATION DE MSREPORTW7 EN TANT QUE MEMBRE DU DOMAINE :

3.14.1 CONFIGURATION DES CLIENTS WINDOWS XP PRO:

Pour joindre une machine Windows XP au domaine, il faut créer l'entrée de registre suivante :
[HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\Netlogon\Parameters]
"requiresignorseal"= dword:00000000
Joindre la machine dans le domaine :
Si on ne configure pas la machine Windows XP on a ce message « *The following error occured attempting to join the domain « msreport ». Login failure : unknown user name or bad password* »

Pour plus d'informations :
http://www.gcolpart.com/howto/samba.php4

3.14.2 CONFIGURATION D'UNE MACHINE WINDOWS 7 :

Pour permettre à une machine Windows 7 de joindre le domaine, déployer un fichier .REG contenant ces deux valeurs de registre :
HKLM\System\CCS\Services\LanmanWorkstation\Parameters
DWORD DomainCompatibilityMode = 1
DWORD DNSNameResolutionRequired = 0

Afin d'optimiser les performances ou de simplifier l'administration du parc informatique, effectuer les actions suivantes :
- La désactivation du pare feu
- La désactivation de l'UAC
- La configuration d'IPV4 en tant que protocole préférée à IPV6 (*DisabledComponents* à 0x20)
- Le démarrage du service « Explorateur d'ordinateur »
- L'activation de l'os Windows
- L'installation du correctif suivant : http://support.microsoft.com/kb/323928/en-us
- Ajouter l'entrée de registre "*WaitForNetwork*" à 0 dans la clé *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System*

L'entrée de registre "*WaitForNetwork*" correspond à la stratégie de groupe « *Définir le délai maximum d'attente pour le réseau si l'utilisateur a un profil distant ou un home directory distant ».*

Pour éditer les stratégies de groupe, cliquer sur « *Démarrer* | *Exécuter* | *mmc* »
Aller dans le menu *Fichier* puis cliquer sur « *Ajouter un composant logiciel enfichable* ».
Sélectionner le composant « Editeur d'objets de stratégie de groupe ». Cliquer sur Ordinateur local puis OK.
Aller dans Configuration ordinateur | Modèles d'administration | System | Profil Utilisateurs et activer la GPO « *Définir le délai maximum d'attente pour le réseau si l'utilisateur a un profil distant ou un home directory distant* ».
Mettre une valeur comme 2 (pour 2 secondes).

Pour plus d'informations :
http://www.group-policy.com/ref/policy/2844/Set_maximum_wait_time_for_the_network_if_a_user_has_a_roaming_user_profile_or_remote_home_directory
https://wiki.samba.org/index.php/Windows7.

3.15 CONFIGURATION DE MSREPORTINF1 EN TANT QUE SERVEUR DE FICHIERS :

L'objectif est maintenant d'installer MSREPORTINF1 en tant que serveur de fichiers et d'impression membre du domaine MSREPORT.

Il existe plusieurs configuration possible pour qu'un serveur de fichiers / impression membre interroge la base du domaine SAMBA 3.6 CHGOUGERES :

- Configuration 1 : via la configuration de WINDBIND et NSS : ce mode permet de joindre des domaines SAMBA 3.X et NT4. Il n'est d'utiliser des utilisateurs / groupes des domaines approuvées par le domaine SAMBA CHFOUGERS.
- Configuration 2 : via la configuration de NSS et du client LDAP: ce mode permet de joindre des domaines SAMBA uniquement.
- Configuration 3 : via la configuration du service SSSD. Un accès LDAPS est obligatoire.

Dans cette architecture, nous allons configurer le serveur de fichier via la configuration du service NSS et comme un client LDAP standard (configuration 2).

Pour plus d'informations
https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/4/html/Reference_Guide/s2-samba-domain-member.html
http://www.samba.org/samba/docs/man/Samba-Guide/unixclients.html
http://www.linuxquestions.org/questions/linux-enterprise-47/rhel-6-ldap-now-requires-tls-843917/

3.15.1 CONFIGURATION DU FICHIER /ETC/SAMBA/SMB.CONF :

```
[global]
        dos charset = 850
        unix charset = ISO8859-1
        workgroup = MSREPORT
        server string =
        passdb backend = ldapsam: "ldap://192.168.92.121 ldap://192.168.92.125"
        syslog = 0
        log file = /var/log/samba/%m.log
        max log size = 500
        smb ports = 139
        time server = Yes
        deadtime = 15
        socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
        # Configure samba to create a share automatically for each printer.
        # Printers settings use default configuration based on [PRINTERS] SECTION.
        load printers = yes
        # Define cups as the printer system
        printing = cups
        printcap name = cups
        wins server = 192.168.92.121
        ldap admin dn = cn=Manager,DC=MSREPORT,DC=LAN
        ldap group suffix = ou=Groupes
        ldap machine suffix = ou=Machines
        ldap suffix = DC=MSREPORT,DC=LAN
        ldap ssl = no
        ldap user suffix = ou=Utilisateurs
        case sensitive = No
        veto files = /lost+found/.recycle/.Desktop/.bash_history/
        hide files = /~$*.doc/~WRL*.tmp/
        dont descend = /proc,/dev,/etc,/lib,/lost+found,/initrd
        security = domain
        template shell = /bin/false
[Informatique]
```

```
        comment = Service Informatique
        path = /home/domaines/informatique
        valid users = @informatique, nboisgerault, msoyris
        read only = No
        browseable = Yes
[IT]
        comment = IT
        path = /IT
        valid users = @IT
        read only = No
        browseable = Yes
[EDN]
        comment = EDN
        path = /EDN
        valid users = @GG_EDN
        read only = No
        browseable = Yes
[public]
        comment = public
        path = /public
        read only = Yes
        browseable = Yes
[PRINTERS]
        comment = Partage-imprimante
        path = /var/spool/samba
        browseable = yes
        public = yes
        guest ok = yes
        writable = no
        # Define that the share is a printer not a folder.
        printable = yes
[print$]
        comment = drivers
        path = /var/lib/samba/drivers
        browseable = yes
        guest ok = no
        read only = yes
[perso]
    comment = Repertoire personnel
    path = /profiles
    browseable = No
    writeable = Yes
```

3.15.2 CONFIGURATION DE REDHAT POUR NE PAS UTILISER LE SERVICE SSSD POUR L'AUTHENTIFICATION LDAP :

Il faut pour cela :

- Installer le paquet NSS-PAM-LDAP et PAM-LDAP
- Configurer le fichier */etc/sysconfig/authconfig*) avec le paramètre FORCELEGACY=YES au lieu de FORCELEGACY=NO.
- Relancer la commande *authconfig-tui* or *authconfig-gtk* pour configurer les fichiers
- Configurer le service SSSD pour ne pas démarrer automatiquement.
- Configurer le service NSLCD pour démarrer automatiquement.

Taper la commande suivante :
*yum install *nss-pam-ldapd**

Editer le fichier */etc/sysconfig/authconfig* et valider le paramètre suivant :
FORCELEGACY = Yes
Taper la commande suivante pour configurer l'authentification via la base OpenLDAP :

authconfig-tui
Cocher les cases suivantes dans la fenêtre « Configuration de l'authentification ».
Utiliser LDAP
Utiliser l'authentification LDAP
Une autorisation locale est suffisante

Dans la fenêtre Paramètres LDAP, entrer les paramètres suivantes :
Serveur : ldap://192.168.92.121,ldap://192.168.92.125
DN de base : DC=msreport,dc=lan

Taper la commande suivant pour configurer le démarrage automatique des services :
ntsysv
Cocher les cases NSLCD et SSSD.

Pour plus d'informations :
http://blog.yibi.org/2011/01/10/ldap-authentication-on-red-hat-enterprise-6

Vérifier que la commande *getent* renvoie bien la liste des utilisateurs du domaine SAMBA.

La commande *authconfig-tui* a modifié les fichiers suivants :
- */etc/openldap/ldap.conf*
- */etc/nssswitch.conf*
- */etc/pam_ldap.conf*

Taper la commande suivante :
vi /etc/nsswitch.conf
Vérifier que le paramètre hosts (résolution de noms) est toujours sur *files wins dns*

```
passwd:     files ldap
shadow:     files ldap
group:      files ldap
hosts:      files wins dns
bootparams: nisplus [NOTFOUND=return] files
ethers:     files
netmasks:   files
networks:   files
protocols:  files
rpc:        files
services:   files
netgroup:   files
publickey:  nisplus
automount:  files ldap
aliases:    files nisplus
```

3.15.3 CONFIGURATION DU SERVEUR SAMBA POUR POUVOIR ACCEDER A LA BASE OPENLDAP :

Taper la commande suivante :
smbpasswd –w Msreport

3.15.3.1 CREATION DE L'OU IDMAP (SI CONFIGURATION PLUS TARD AVEC WINBIND) :

La commande ci-dessous indique que l'annuaire OpenLDAP ne dispose pas d'un conteneur IDMAP :
slapcat | grep -i idmap

Créer l'OU idmap manuellement via l'outil Apache Directory Studio (administration de la base OpenLDAP via une interface graphique sous Windows).

3.15.4 JOINDRE MSREPORTINF1 DANS LE DOMAINE

Taper la commande suivante :
net rpc join

3.15.5 DEFINITION DES PERMISSIONS :

Pour accéder à un fichier partagé par un serveur SAMBA, il faut disposer des accès sur le système de fichiers ESXT4 et au niveau de SAMBA.

Pour donner des permissions sur le partage appelé *EDN* à l'utilisateur monique.mathieu.
Ajoutere monique.mathieu dans le groupe GG_EDN.

Création d'un groupe avec SID :
smbldap-groupadd -a GG_EDN

Ajout de l'utilisateur monique.mathieu dans le groupe GG_EDN.
smbldap-groupmod -m monique.mathieu GG_EDN

Pour vérifier que l'utilisateur appartient bien au groupe IT, taper la commande
smbldap-groupshow GG_EDN

Fermer la session de l'utilisateur et la rouvrir pour que les appartenances aux groupes soient actualisées sur MSREPORTW7.

Créer le répertoire /EDN :
mkdir /EDN

Lister les droits par défaut sur le répertoire /EDN :
getfacl /EDN

Par défaut les autres utilisateurs ont un accès en lecture. Taper la commande suivante pour restreindre cet accès par défaut :
chmod 770 /EDN

Lister les droits sur le répertoire /EDN :
getfacl /EDN

Seul l'utilisateur root et le groupe root ont maintenant les droits sur ce dossier.

Partager le répertoire /EDN sur MSREPORTINF1 :
Editer le fichier */etc/samba/smb.conf*

```
[EDM]
    comment = EDN
    path = /EDN
    valid users = @EDN
    read only = No
    browseable = Yes
```

Redémarrer le service SAMBA en tapant la commande suivante :
service smb restart

Ouvrir une session avec l'utilisatrice monique.mathieu et tester l'accès au partage EDN.
L'accès est refusé pour le répertoire EDN. Le système demande une authentification.

Quand on n'a pas les droits au niveau du système de fichiers EXT4, on a le message suivant qui apparaît :
You do not have permission to access \\MSREPORTINF1\nom_dossier
Quand on a une erreur de droits au niveau de SAMBA, on a une fenêtre POPUP qui demande que l'on s'authentifie avec un autre compte.

Dans l'exemple ci-dessous on a les droits d'accéder aux répertoires IT.
On peut par contre accéder au répertoire IT.

Pour corriger le problème, il faut donner les droits sur le répertoire /EDN au niveau du système de fichiers EXT4. Pour cela taper la commande suivante :
setfacl -m u:monique.mathieu:rwx /EDN
getfacl /EDN
L'utilisatrice monique.mathieu a maintenant un accès en lecture sur le répertoire.

Pour rappel :
- r : accès en lecture
- w : accès en écriture
- x : accès en exécution

Si l'on teste l'accès ce dernier n'est toujours pas fonctionnel car SAMBA semble ignorer les permissions donnés à un utilisateur. En donnant des droits à un groupe on contourne le problème.

setfacl -m g:GG_EDN:rwx /EDN
On peut maintenant accéder au partage EDN.
Avec SAMBA, il faut que le groupe défini en tant que « Valid users » est des accès ou que l'on définisse des droits aux par défaut (chmod 775 sur /EDN).

Pour plus d'infrmation sur la commande SETFACL :
https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/6/html/Storage_Administration_Guide/s1-acls-setting.html

3.16 CONFIGURATION DE MSREPORTINF1 EN TANT QUE SERVEUR D'IMPRESSION :

3.16.1 PRESENTATION DE CUPS :

La version installée de CUPS par défaut dans Red Hat Enterprise Linux 6.2 est CUPS 1.4.2.
Il existe deux interfaces d'administration pour CUPS :
- Une interface graphique :
- Une interface web : http://127.0.0.1:631/

Remarque :
- Pour accéder à la page de configuration de CUPS, il faut se connecter en HTTPS.
- L'utilisation de l'interface graphique écrase tous les paramètres du fichier */etc/cupsd.conf*.

3.16.2 INSTALLATION DES COMPOSANTS :

CUPS et son interface web sont installés de base.
Pour installer l'interface graphique d'administration de CUPS, taper la commande :
yum install system-config-printer
Pour installer la dernière version de CUPS ou d'autres composants de CUPS, taper la commande suivante :
*yum install CUPS**

Installer ou mettre à jour les paquets suivants
cups-devel
cups-lpd
cups-pk-helper

3.16.3 CONFIGURATION DU FICHIER /ETC/CUPS/CUPSD.CONF :

Configurer CUPS pour écouter sur l'IP du serveur (192.168.92.126 dans notre cas).
 # Only listen for connections from the local machine.

Listen localhost:631
Listen /var/run/cups/cups.sock
Listen 192.168.92.126:631

Configurer CUPS pour autoriser l'accès au service CUPS depuis le réseau 192.168.92.0/24

```
# Restrict access to the server...
<Location />
  Order allow,deny
  Allow from 192.168.92.0/24
</Location>

# Restrict access to the admin pages...
<Location /admin>
  Order allow,deny
  Allow from 192.168.92.0/24
</Location>
```

Redémarrer le service CUPS :
service cups restart
Attention, si vous utilisez l'interface graphique, les paramètres du fichier */etc/cupsd.conf* sont écrasés.

3.16.4 CONFIGURATION DE SAMBA :

Ajouter dans la section [GLOBAL] du fichier */etc/samba/smb.conf* les instructions suivantes :

```
# Configure samba to create a share automatically for each printer.
# Printers settings use default configuration based on [PRINTERS] SECTION.
load printer = yes
# Define cups as the printer system
printing = cups
printcap name = cups.
```

Il faut maintenant configurer les paramètres par défaut des partages d'imprimantes créés automatiquement par SAMBA. Pour cela on définit le partage [PRINTERS]

```
[PRINTERS]
comment = Partage-imprimante
path = /var/spool/samba/
browseable = yes
public = yes
guest ok = yes
writable = no
# Define that the share is a printer not a folder.
printable = yes
```

Pour terminer il faut créer le partage [print$] qui contiendra tous les pilotes d'impression.

```
[print$]
comment = drivers
path = /var/lib/samba/drivers
browseable = yes
guest ok = no
read only = yes
```

3.16.5 AJOUT DES IMPRIMANTES SUR LE SERVEUR LINUX :

Cette opération peut être effectuée via l'interface graphique Red Hat (dans les outils d'administration)
L'interface est très proche de l'assistant sous Windows.
Il est aussi possible d'utiliser l'interface web de CUPS. Se connecter sur https://192.168.92.126:631/admin/

3.16.6 DELEGUER AUX UTILISATEURS DU DOMAINE LE FAIT DE POUVOIR AJOUTER UNE IMPRIMANTE :

Taper la commande suivante :
net rpc rights grant "MSREPORT\Domain users" SePrintOperatorPrivilege -U root

3.16.7 AJOUT DES PILOTES D'IMPRESSION :

Il faut maintenant installer les pilotes d'impressions.
Pour cela, se loguer en tant que root et mapper une imprimante. Windows va demander d'insérer les pilotes. Ces derniers vont être copiés sur le serveur.

3.16.8 POUR PLUS D'INFORMATIONS SUR CUPS :

https://wiki.samba.org/index.php/Samba_as_a_print_server
http://asoyeur.free.fr/linux/samba/cups.html
http://coagul.org/drupal/node/591/
http://sequanux.org/spip.php?article23
http://www.samba.org/samba/docs/man/Samba-Guide/happy.html#id2582657
http://sequanux.org/spip.php?article23
http://wiki.archlinux.fr/CUPS
http://fr.wikipedia.org/wiki/Common_Unix_Printing_System
http://asoyeur.free.fr/linux/samba/cups.html
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/CUPS-printing.html
http://www.tldp.org/HOWTO/Debian-and-Windows-Shared-Printing/sharing_with_windows.html#share_cups_config
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/CUPS-printing.html
http://doc.ubuntu-fr.org/cups-pdf

4 PROCEDURE D'ADMINISTRATION :

4.1 LES OUTILS D'ADMINISTRATION :

Les commandes smbldap-* permettent de gérer les comptes utilisateurs groupes et les comptes ordinateurs (avec un backend OpenLDAP).
Exemple de commandes : *smbldap-groupadd, smbldap-passwd*

La commande *net rpc* permet de gérer les fonctionnalités avancées de SAMBA comme la création d'une relation d'approbation : *net rpc trustdom*

Quand on utilise un BACKEND LDAP, certaines commandes ne sont pas fonctionnelles comme la création de groupes. Il faut en effet utiliser les commandes SMBLDAP-XXX pour effectuer ces actions.
http://lists.samba.org/archive/samba/2005-September/110425.html
http://thr3ads.net/samba/2005/05/1764321-Samba-net-rpc-group-add-NT_STATUS-_ACCESS_DENIED

Pour plus d'informations sur la commande NET :
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetCommand.html

La commande *pdbedit* permet de gérer les stratégies de mots de passes et les ressources SAMBA.

4.2 LOGS SAMBA :

Pour valider le bon fonctionnement de l'ouverture de session :
Tail –f /var/log/samba.log
Tail –f /var/log/nommachine.log

Pour plus d'informations :
http://www.samba.org/samba/docs/using_samba/ch12.html

4.3 LISTE DES CORRECTIFS SAMBA :

https://wiki.samba.org/index.php/Samba_3.4_Features_added/changed

4.4 DOCUMENTATION :

4.4.1 DOCUMENTATION GENERALE SUR SAMBA :

http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/
http://wiki.samba.org/index.php/Main_Page
http://sequanux.org/spip.php?article22
http://eric.quinton.free.fr/IMG/pdf/Configurer_samba_ldap_ubuntu10_avec_migration_CS3-CS4-2.pdf
http://download.gna.org/smbldap-tools/docs/samba-ldap-howto/
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/
http://romain.therrat.fr/samba-modifier-son-nom-netbios-backend-ldap/

4.4.2 INSTALLATION D'UN BDC :

http://sambaxp.org/fileadmin/user_upload/SambaXP2008-DATA/03-02-Hannes_Kasparick-OpenLDAP.pdf
http://www.openldap.org/doc/admin23/syncrepl.html
https://wiki.samba.org/index.php/2.0:_Configuring_LDAP
http://contribs.martymac.org/samba2.2-Ldap/html/9/
http://www.openldap.org/doc/admin24/replication.html
http://pegasus45.free.fr/index.php?title=Debian_5:_Installation_d'un_serveur_Samba_en_BDC_coupl%C3%A9_%C3%A0_un_serveur_OpenLDAP
http://pegasus45.free.fr/index.php?title=Debian_5:_Installation_d'un_serveur_Samba_en_BDC_coupl%C3%A9_%C3%A0_un_serveur_OpenLDAP
http://romain.therrat.fr/samba-modifier-son-nom-netbios-backend-ldap/

4.4.3 REPLICATION WINS :

http://www.samba.org/samba/docs/using_samba/ch07.html
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/samba-bdc.html#id2566941
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/NetworkBrowsing.html#id2584196
http://support.microsoft.com/kb/150800/en-us
http://support.microsoft.com/kb/314108/fr

4.4.4 MISE EN ŒUVRE DE CUPS :

https://wiki.samba.org/index.php/Samba_as_a_print_server
http://asoyeur.free.fr/linux/samba/cups.html
http://coagul.org/drupal/node/591/
http://sequanux.org/spip.php?article23
http://www.samba.org/samba/docs/man/Samba-Guide/happy.html#id2582657
http://sequanux.org/spip.php?article23
http://wiki.archlinux.fr/CUPS
http://fr.wikipedia.org/wiki/Common_Unix_Printing_System
http://asoyeur.free.fr/linux/samba/cups.html
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/CUPS-printing.html
http://www.tldp.org/HOWTO/Debian-and-Windows-Shared-Printing/sharing_with_windows.html#share_cups_config
http://www.samba.org/samba/docs/man/Samba-HOWTO-Collection/CUPS-printing.html
http://doc.ubuntu-fr.org/cups-pdf

4.4.5 LISTE DES CORRECTIFS SAMBA :

https://wiki.samba.org/index.php/Samba_3.4_Features_added/changed

4.4.6 DEPANNAGE SAMBA :

http://www.samba.org/samba/docs/using_samba/ch12.html