




2020-2021

Epreuve-E6 BTS SIO



Xavier Tofili
IRIS-STRASBOURG
2020-2021

	BTS SIO		Orange WF
	Services Informatiques aux Organisations		
	Option	SISR	
	Session	2021	

TOFILI Xavier	Activité professionnelle N°	5
----------------------	------------------------------------	---

NATURE DE L'ACTIVITE	Mise en place d'un Domaine LDAP avec Samba
Contexte	Dans le cadre de mon stage en entreprise, il m'a été demandé de mettre en place une solution d'authentification. J'ai donc mis en place dans un Proxmox deux serveurs LDAP via SAMBA. Un qui sera le contrôleur de domaine principal et le second qui sera une roue de secours en cas de panne du premier.
Objectifs	Avoir un contrôleur de domaine principal pour permettre l'authentification dans le réseau et un second serveur qui sera un réplica du premier.
Lieu de réalisation	Orange WF – Wallis-et-Futuna

DESCRIPTION DE LA SOLUTION RETENUE	
Conditions initiales	Réseau sans solution d'authentification
Conditions finales	Réseau avec contrôleur de domaine comme solution d'authentification
Outils utilisés	Serveur Proxmox, samba, MobaXterm

CONDITIONS DE REALISATION	
Matériels	Serveur Proxmox
Logiciels	Samba, MobaXterm
Contraintes	Avoir des bases Linux, permettre la connexion SSH depuis l'extérieur vers la VM à l'intérieur de proxmox.

COMPETENCES MISES EN OEUVRE POUR CETTE ACTIVITE PROFESSIONNELLE	
A1.1.1	Analyse du cahier des charges d'un service à produire
A1.2.4	Détermination des tests nécessaires à la validation d'un service
A1.4.1	Participation à un projet
A3.1.1	Proposition d'une solution d'infrastructure
A3.1.2	Maquettage et prototypage d'une solution d'infrastructure
A3.2.1	Installation et configuration d'éléments d'infrastructure
A3.3.1	Administration sur site ou à distance des éléments d'un réseau, de serveurs...
A4.1.8	Réalisation des tests nécessaires à la validation d'éléments adaptés ou développés
A4.1.9	Rédaction d'une documentation technique.

Sommaire

Cahier des charges.....	3
Expression du besoin	3
Analyse et proposition de réponse... ..	3
Plan de travail.....	4
Mise en œuvre	4
Installation du domaine principal.....	5
Installation du domaine secondaire.....	8

Cahier des charges

Expression du besoin

Le besoin de l'entreprise est de disposer d'un système d'authentification

Analyse et proposition de réponse

Objectif :

Mise en place d'une solution d'authentification

Introduction

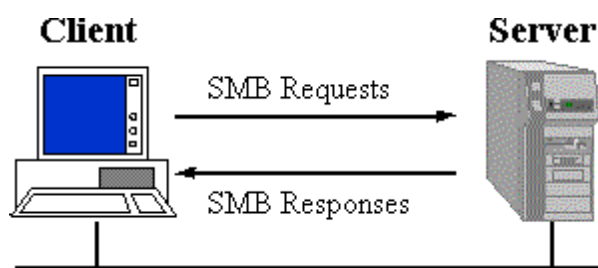
En général, un contrôleur de domaine est le principal chef sur un réseau. C'est à ce serveur que tous les clients se réfèrent pour les authentifications d'utilisateurs, de machines... Etant donné que la centralisation est risquée, le serveur principal CPD en français pour (Controller Principal de Domaine), est souvent secondé par un BDC (Backup Domain Controller). C'est un serveur de secours qui garantira une continuité de service grâce à une sauvegarde des groupes, comptes et permissions des utilisateurs en cas de panne du CPD.

Solution

Pour permettre l'authentification des postes de travail dans le réseau, il a été décidé de mettre en place un serveur samba qui fera office de contrôleur de domaine. Samba est un logiciel d'interopérabilité implémentant le protocole propriétaire SMB/CIFS de Microsoft. Les principales fonctionnalités de Samba sont les suivantes :

- Partager un disque Linux pour des machines Windows
- Partager une imprimante Linux avec des machines Windows
- Partager une imprimante Windows à partir d'un hôte Linux
- Devenir un contrôleur de domaine (simuler le système Windows NT Server) et permettre ainsi les authentifications réseaux sur un domaine, le stockage centralisé des profils Windows et l'exécution de scripts de démarrage
- Gérer des listes de machines présentes sur le réseau et leur mise à disposition pour tous types de clients
- Devenir membre d'un domaine NT existant et ainsi être capable d'utiliser un CPD NT pour authentifier toutes les connexions faites par des utilisateurs Windows

Fonctionnement de SAMBA-AD



Le protocole permettant la communication entre Linux et Windows, est SMB (Server Message Block).

Son fonctionnement est conforme au schéma client-serveur suivant :

Après authentification, le serveur donnera accès au client à ses ressources. Cela est permis par les Daemon, SMBD pour le service serveur et NMBD pour le service de résolutions de nom NetBios.

Liste d'authentification autorisé :

Pour optimiser notre annuaire AD, seront créés différentes OU (unité d'organisation). Dans chaque OU, il y aura différents types de groupes dans lesquels les utilisateurs seront placés en fonction de leurs qualifications.

Exemple :

Nous allons créer une OU qui se nommera Stagiaire, et dans cette OU nous créerons un groupe nommé G_Stagiaire dans lequel sera ajouté un utilisateur Stagiaire1.

Plan de travail

Pour la mise en place de l'AD, nous allons suivre quatre grandes étapes :

- Etape 1 – Préparer le serveur debian
- Etape 2 – Installer et configurer Samba AD
- Etape 3 – Création du domaine
- Etape 4 – Mise en service du domaine Samba

Mise en œuvre

Installation du domaine principal

Etape 1 – Préparer le serveur debian

--changer le nom de la machine par le nom de domaine--

```
root@srvads:~# nano /etc/hostname
srvads.uvea.xyz
```

--faire la même chose sur le fichier /etc/hosts--

```
root@srvads:~# nano /etc/hosts
127.0.0.1 localhost
::1 localhost ip6-localhost ip6-loopback
10.70.10.111 srvads.uvea.xyz      srvads
```

--attribuer une IP fixe à la machine--

```
root@srvads:~# nano /etc/network/interfaces
auto eth0
iface eth0 inet static
    address 10.70.10.111/24
    gateway 10.70.10.100
```

--redémarrer le système--

```
root@srvads:~# reboot
```

Etape 2 – Installer et configurer Samba AD

--entrer la commande suivante pour installer samba et les paquets dont il a besoin--

```
root@srvads:~# apt -y install samba krb5-config winbind smbclient
```

--le message suivant s'affichera, sélectionner no car la machine est configurée en IP statique--

If your computer gets IP address information from a DHCP server on the network, the DHCP server may also provide information about WINS servers ("NetBIOS name servers") present on the network. This requires a change to your smb.conf file so that DHCP-provided WINS settings will automatically be read from /var/lib/samba/dhcp.conf. The dhcp-client package must be installed to take advantage of this feature.

Modify smb.conf to use WINS settings from DHCP?

<Yes>

<No>

--ensuite indiquer le nom de domaine--

When users attempt to use Kerberos and specify a principal or user name without specifying what administrative Kerberos realm that principal belongs to, the system appends the default realm. The default realm may also be used as the realm of a Kerberos service running on the local machine. Often, the default realm is the uppercase version of the local DNS domain.

Default Kerberos version 5 realm:

UVEA.XYZ_____

<Ok>

--indiquer le nom du serveur et du nom de domaine--

Enter the hostnames of Kerberos servers **in** the SRV.WORLD Kerberos realm separated by spaces.

Kerberos servers **for** your realm:

SRVADS.UVEA.XYZ_____

<Ok>

--encore une fois--

Enter the hostnames of Kerberos servers **in** the SRV.WORLD Kerberos realm separated by spaces.

Kerberos servers **for** your realm:

SRVADS.UVEA.XYZ_____

<Ok>

Etape 3 – Création du domaine

--renommer le fichier de configuration de samba--

```
root@srvads:~# mv /etc/samba/smb.conf /etc/samba/smb.conf.old
```

--lancer la provision du domaine--

```
root@srvads:~# samba-tool domain provision
```

--laisser les choix par défaut pour les quatre premières propositions--

Realm [UVEA .XYZ]:

Domain [UVEA]:

Server Role (dc, member, standalone) [dc]:

DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:

--entrer l'IP du serveur DNS au choix s'il n'y a pas de redirecteur déjà configuré—

Dans mon cas, j'ai laissé le DNS 1.1.1.1 par défaut car je disposais déjà d'un nom de domaine soit « uvea.xyz ». Le DNS 1.1.1.1 est un résolveur DNS de CloudFare.

```
DNS forwarder IP address (write 'none' to disable forwarding) [1.1.1.1]:
```

Dans le cas où vous ne disposeriez pas d'un nom de domaine public, il faudra alors configurer le DNS en local comme l'exemple suivant :

Éditer le fichier /etc/samba/smb.conf

```
GNU nano 3.2
#Global parameters
[global]
    dns forwarder = "IP de votre serveurur DNS"
    netbios name = "Nom netbios de votre Domaine"
    realm = "Votre Domaine, exemple : UVEA.LAN"
    server role = active directory domaine controller
    workgroup = UVEA
    idmap_ldb:use rfc2307 = yes

[sysvol]
    path = /var/lib/samba/sysvol
    read oonly = No

[netlogon]
    path = /var/lib/samba/sysvol
    read only = No
```

Explication :

Le « dns forwarder » : sera l'IP de votre serveur DNS capable de résoudre des noms de domaine externes, par exemple votre box opérateur.

Il vous sera donc nécessaire d'avoir un serveur DNS local, pour cela il faut au préalable avoir installer BIND et le configurer.

Installation de BIND sous Debian :

Installer les package suivant :

```
apt-get install -y bind9 bind9utils
```

Avec les distributions sous Debian, il y'a 5 fichier de configuration bind9 :

```
/ etc / default / bind9
/etc/bind/named.conf
/etc/bind/named.conf.options
/etc/bind/named.conf.local
/etc/bind/named.conf.default-zones
```

Parmi ces fichiers de configuration seulement 2 fichiers doivent être configurés :

Si vous utilisez uniquement de l'IPv4 ce qui est notre cas il faut éditer le fichier **/etc/default/bind9** et le modifier ainsi :

Repérer la ligne **OPTIONS = '' - u bind ''** et la modifier en **OPTION = '' - u bind 4 ''**.

Ensuite modifier également le fichier **/etc/bind/named.conf.options**, c'est le fichier à configurer pour l'Active Directory et pour configurer les ACL par défaut pour Bind9 :

On doit alors ajouter l'adresse de notre serveur DNS primaire :

```
options {  
    listen-on port 53 { IP_SERVER; localhost; };
```

On peut ensuite préciser si l'on souhaite utiliser le mode récursif lorsque des requêtes sont émises et autoriser les réseaux ou zones sur lesquelles on peut envoyer ces requêtes en cas de réponse vide :

```
recursion yes;  
  
allow-query    { IP_SERVER; 127.0.0.1/8; localhost; };
```

Si l'on dispose d'un serveur secondaire et qu'on souhaite transférer les requêtes circulant vers un serveur secondaire, on peut le déclarer de la manière suivante :

```
allow-transfer { IP_SERVER2; localhost; };
```

Si on dispose d'autres autorités DNS, on peut également leur transférer les requêtes provenant des clients en déclarant la ligne suivante :

```
forwarders { 1.1.1.1; 8.8.8.8; };
```

Donc une fois votre serveur DNS configuré il faudra renseigner l'ip du serveur en DNS forwarder. Puis continuer.

--entrer le mot de passe administrator--

Administrator password:

Retype password:

--si tout s'est bien passé jusqu'à maintenant voici ce qu'il faut avoir--

Looking up IPv4 addresses

Looking up IPv6 addresses

No IPv6 address will be assigned

Setting up share.ldb

Setting up secrets.ldb

Setting up the registry

Setting up the privileges database

Setting up idmap db

Setting up SAM db

Setting up sam.ldb partitions and settings

Setting up sam.ldb rootDSE

Pre-loading the Samba 4 and AD schema

Unable to determine the DomainSID, can not enforce uniqueness constraint on local domainSIDs

Adding DomainDN: DC=office,DC=local

Adding configuration container

Setting up sam.ldb schema

Setting up sam.ldb configuration data

Setting up display specifiers

Modifying display specifiers and extended rights

Adding users container

Modifying users container

Adding computers container

Modifying computers container

Setting up sam.ldb data

Setting up well known security principals

Setting up sam.ldb users and groups

Setting up self join

Adding DNS accounts

Creating CN=MicrosoftDNS,CN=System,DC=office,DC=local

Creating DomainDnsZones and ForestDnsZones partitions

Populating DomainDnsZones and ForestDnsZones partitions

Setting up sam.ldb rootDSE marking as synchronized

Fixing provision GUIDs

A Kerberos configuration suitable **for** Samba AD has been generated at /var/lib/samba/private/krb5.conf

Merge the contents of this file with your system krb5.conf or replace it with this one. **Do** not create a symlink!

Once the above files are installed, your Samba AD server will be ready to use

Server Role: active directory domain controller

Hostname: srvdc

NetBIOS Domain: OFFICE

DNS Domain: office.local

DOMAIN SID: *_*_*_*_*****_*****_*****

Etape 4 – Mise en service du domaine Samba

--faire une copie du fichier de configuration kerberos dans le répertoire /etc--

```
root@srvads:~# cp /var/lib/samba/private/krb5.conf /etc/
```

--arrêter les services SMB, NMBD et BIND--

```
root@srvads:~# systemctl stop smbd nmbd winbind
```

--désactiver les services--

```
root@srvads:~# systemctl disable smbd nmbd winbind
```

--rendre visible le service Samba AD DC--

```
root@srvads:~# systemctl unmask samba-ad-dc
```

--démarrer le service--

```
root@srvads:~# systemctl start samba-ad-dc
```

--activer le service--

```
root@srvads:~# systemctl enable samba-ad-dc
```

--vérification du statut de samba AD--

```
root@srvads:/etc# smbclient -L localhost -U%

      Sharename      Type      Comment
      -----
      netlogon       Disk
      sysvol         Disk
      IPC$           IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup       Master
      WORKGROUP      SRVADS

root@srvads:/etc#
```

--vérification du niveau du domaine--

```
root@srvads:~# samba-tool domain level show
Domain and forest function level for domain 'DC=uvea,DC=xyz'

Forest function level: (Windows) 2008 R2
Domain function level: (Windows) 2008 R2
Lowest function level of a DC: (Windows) 2008 R2
root@srvads:~#
```

Le domaine étant créé, il est désormais possible de joindre des PC-Windows à notre domaine pour les authentifier.

Installation du domaine secondaire

Il est recommandé de disposer d'un contrôleur de domaine secondaire pour assurer une haute disponibilité du service.

Pour ajouter un autre Contrôleur de Domaine, il faudra reprendre toutes les étapes depuis le début et remplacer la commande de l'étape « **3 Création du domaine : lancer la provision du Domain** » par :

```
1 samba-tool domain join DomainPrincipal.lan DC --server=DC1 \
2 --option='idmap_ldb:use rfc2307 = yes' \
3 --option="dns forwarder=172.27.1.1" \
4 -U"UVEA\administrator"
```

DomainPrincipal.lan : Nom du domaine à rejoindre.

--option="dns forwarder= 1.1.1.1" : IP du serveur DNS de résolution externe.

--server=DC1 : Contrôleur de domaine existant sur lequel s'authentifier.

-U"UVEA\administrator" : Nom de l'utilisateur ayant le droit d'intégrer un nouveau contrôleur de domaine.