Gestion du parc informatique et procédures de MAJ

Association Linuxisgood
Gestion des postes utilisateurs itinérants avec authentification LDAP et profils NFS

Sommaire

1. Introduction
2. Glossaire
3. Présentation de l'architecture réseau
4. Gestion des utilisateurs et profils itinérants
5. Procédures de mise à jour des machines
6. Sécurisation de l'infrastructure
7. Interface de gestion centralisée
8. Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA)
9. Annexes et ressources

---

1. Introduction

Cette documentation explique comment gérer et maintenir l'infrastructure informatique de l'association Linuxisgood. Elle est destinée aux responsables techniques et aux administrateurs du parc informatique, avec un langage accessible pour les personnes moins expérimentées.

L'objectif principal est de garantir que chaque utilisateur dispose d'un profil personnalisé et accessible sur n'importe quel poste, via une authentification centralisée LDAP et un montage des répertoires personnels (/home) stockés sur un serveur NFS.

2. Glossaire

- **LDAP (Lightweight Directory Access Protocol)** : protocole permettant de centraliser et gérer les informations des utilisateurs et leurs droits d'accès.

- **NFS (Network File System)** : système de fichiers réseau qui permet à plusieurs clients d'accéder aux mêmes fichiers sur un serveur distant.
- **PAM (Pluggable Authentication Modules)** : modules utilisés par Linux pour gérer l'authentification des utilisateurs.
- **Raid 5** : technique de stockage qui utilise plusieurs disques pour assurer la redondance et la performance.
- **DHCP (Dynamic Host Configuration Protocol)** : service qui attribue automatiquement des adresses IP aux machines du réseau.
- **DNS (Domain Name System)** : service qui traduit les noms de domaine en adresses IP.
- **VPN (Virtual Private Network)** : réseau privé virtuel qui sécurise les connexions depuis l'extérieur.
- **MFA (Multi-Factor Authentication)** : authentification multi-facteurs qui ajoute une couche de sécurité supplémentaire.
- **Failover** : mécanisme permettant de basculer automatiquement vers un système de secours en cas de panne.
- **CLI (Command Line Interface)** : interface en ligne de commande.
- **GUI (Graphical User Interface)** : interface graphique utilisateur.

3. Présentation de l'architecture réseau

3.1 Infrastructure physique et logique

- Serveur principal (Passerelle Internet) avec deux interfaces réseau:
  - WAN (accès internet)
  - LAN (réseau local 192.168.15.0/24)

Configuration IP statique (exemple serveur NFS)

```
sudo nano /etc/network/interfaces
auto eth0
iface eth0 inet static
    address 192.168.15.254
    netmask 255.255.255.0
    gateway 192.168.15.1
```

Puis redémarrer le service réseau :

```
sudo systemctl restart networking
```

- Services hébergés sur plusieurs VMs :
    - Serveurs DHCP, DNS, LDAP en master/slave avec IP failover (192.168.15.250)
    - Serveur NFS sur un RAID 5 (192.168.15.254) pour héberger les /home

- VPN configuré pour accès sécurisé externe

3.2 Configuration IP et domaines

Service	Adresse IP	Rôle
NFS Server	192.168.15.254	Partage des profils /home
DHCP1	192.168.15.253	Attribution IP
DHCP2	192.168.15.252	Redondance DHCP
Failover IP	192.168.15.250	IP flottante pour master/slave
DHCP Range	192.168.15.100-150	Plage IP attribuée aux clients
Domaine	linuxisgood.local	Nom de domaine interne

4. Gestion des utilisateurs et profils itinérants

4.1 Authentification centralisée

Les postes clients utilisent **PAM-LDAP pour s'authentifier auprès du serveur LDAP**.

Cela signifie qu'un utilisateur peut se connecter à n'importe quel poste avec son identifiant unique.

Guide pas à pas : Configuration PAM-LDAP

Sur le serveur LDAP (master)

1. Installer les paquets nécessaires :
   sudo apt update
   sudo apt install slapd ldap-utils

2. Reconfigurer slapd pour définir ton domaine **linuxisgood.local:**

   sudo dpkg-reconfigure slapd

Nom de domaine : linuxisgood.local

Organisation : linuxisgood

Mot de passe admin LDAP : à définir (note bien ce mot de passe)

Choisir "Oui" pour la base de données HDB ou MDB

Ne pas supprimer la base de données lors de la reconfiguration

3. Vérifier que le service est actif
sudo systemctl status slapd

4. Créer l'arborescence LDAP (exemple pour utilisateurs et groupes)

Créer un fichier base.ldif

```
dn: dc=linuxisgood,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: linuxisgood
dc: linuxisgood

dn: ou=users,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: users

dn: ou=groups,dc=linuxisgood,dc=local
objectClass: organizationalUnit
ou: groups
```

Importer cette base
`ldapadd -x -D cn=admin,dc=linuxisgood,dc=local -W -f base.ldif`

5.Ajouter un utilisateur type dans users.ldif

```
dn: uid=sari,ou=users,dc=linuxisgood,dc=local
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: Samet Ari
sn: Ari
uid: sari
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/sari
loginShell: /bin/bash
userPassword: {SSHA}xxxxxxxxxx # mot de passe chiffré à générer
```

Réitérer autant de fois que nécessaire, pour chaque utilisateur.

Pour **générer** le mot de passe chiffré
`slappasswd`

Puis remplacer `{SSHA}xxxxxxxxxx` par la sortie.

Importer l'utilisateur
`ldapadd -x -D cn=admin,dc=linuxisgood,dc=local -W -f users.ldif`

6. Ajouter un groupe dans groups.ldif :

```
dn: cn=users,ou=groups,dc=linuxisgood,dc=local
objectClass: posixGroup
cn: users
gidNumber: 10000
memberUid: sari
```

Importer le groupe
ldapadd -x -D cn=admin,dc=linuxisgood,dc=local -W -f groups.ldif

Sur les clients (Debian 12)

1. Installer les paquets LDAP et PAM
   sudo apt update
   sudo apt install libnss-ldap libpam-ldap nslcd ldap-utils

Pendant l'installation, renseigner :

- URI LDAP : ldap://192.168.15.250 (IP failover)
- Base DN : dc=linuxisgood,dc=local
- LDAP version : 3

2. Configurer NSS pour utiliser LDAP
   sudo nano /etc/nsswitch.conf

Modifier les lignes passwd, group et shadow pour inclure ldap

```
passwd:         files ldap
group:          files ldap
shadow:         files ldap
```

3. Configurer PAM pour l'authentification LDAP
sudo pam-auth-update

Cochez LDAP Authentication et Create home directory on login.

4. Tester l'authentification
   getent passwd jdupont

Cela doit retourner les informations LDAP de l'utilisateur.

4.2 Profils itinérants via NFS

Le répertoire personnel /home est monté automatiquement depuis le serveur NFS au moment de la connexion de l'utilisateur. Ses documents, images et paramètres sont donc conservés centralement, accessibles sur tous les postes.

Guide pas à pas : Montage automatique du /home via NFS

Sur le serveur NFS

1. Installer le serveur NFS
   sudo apt update
   sudo apt install nfs-kernel-server

2. Exporter le dossier /home
   sudo nano /etc/exports

Ajouter
/home 192.168.15.0/24(rw,sync,no_subtree_check)

3. Appliquer la configuration
   sudo exportfs -a
   sudo systemctl restart nfs-kernel-server

Sur les clients

1. Installer le client NFS
   sudo apt update
   sudo apt install nfs-common

2. Créer un point de montage temporaire (si nécessaire)
   sudo mkdir /mnt/nfs_home

3. Monter manuellement pour test
   sudo mount 192.168.15.254:/home /mnt/nfs_home

4. Pour montage automatique du répertoire /home, modifier /etc/fstab
   sudo nano /etc/fstab

Ajouter la ligne
192.168.15.254:/home /home nfs defaults,_netdev 0 0

L'option _netdev garantit que le montage attend que le réseau soit actif.

Pour éviter les conflits avec le dossier /home local (sur client), il est conseillé que le client n'ait pas de dossiers utilisateurs locaux.

Ou, on peut configurer **PAM** pour créer /home sur NFS uniquement après authentification (via **pam_mkhomedir**).

5. Procédures de mise à jour des machines

5.1 Script de mise à jour centralisée

Un script bash est déployé sur chaque machine pour :

- Mettre à jour les paquets système (**apt update && apt upgrade**)
- Synchroniser les configurations critiques
- Redémarrer les services nécessaires

Ce script est exécuté régulièrement via **cron** ou manuellement à partir d'un serveur de gestion.

Nom du script : **maj.sh**

```
#!/bin/bash

# Met à jour la liste des paquets
apt update

# Met à jour tous les paquets installés sans interaction
apt upgrade -y

# Nettoie les paquets inutiles
apt autoremove -y

# Redémarre les services critiques si besoin (exemple)
systemctl restart nslcd
systemctl restart nfs-common

echo "Mise à jour terminée sur $(hostname)"
```

Déploiement du script sur l'**ensemble des machines**, avec un **accès SSH** aux machines, on peut également lancer ce script à distance

```
for ip in $(seq 100 150); do
   ssh admin@192.168.15.$ip 'bash -s' < maj.sh &
done
wait
echo "Mise à jour déployée sur tous les clients."
```

5.2 Étapes pour lancer la mise à jour

1. **Se connecter** au serveur de gestion

2. **Lancer** le script de mise à jour à distance (via SSH) sur l'ensemble des machines

   Se positionner dans le répertoire courant et lancer le script
   `cd /home/scripts/`

   Puis lancer
   `./maj.sh`

   Si l'on se trouve ailleurs, lancer le script en donnant le chemin complet
   `/home/scripts/maj.sh`

Rendre le script exécutable
chmod +x nomduscript.sh

3. **Vérifier les logs** pour s'assurer du bon déroulement

/var/log/apt/history.log
→ Historique des opérations apt (install, upgrade, remove)

Aperçu des dernières MaJ
tail -n 50 /var/log/apt/history.log

/var/log/apt/term.log
→ Détail complet de l'exécution des commandes apt, utile pour trouver des erreurs

/var/log/syslog
→ Logs système généraux, parfois utile si un service plante après mise à jour

+ Rediriger la sortie du script vers un fichier log personnalisé
./maj.sh > /var/log/maj_$(date +%F).log 2>&1

Puis consulter ce fichier en cas de problème.

4. **Signaler** toute erreur pour intervention manuelle

En cas d'erreur détectée dans les logs ou de dysfonctionnement après mise à jour, merci de **créer un ticket via le système interne** de gestion des incidents et de le remonter à l'administrateur de l'infrastructure pour intervention rapide.

6. Sécurisation de l'infrastructure

6.1 Accès VPN obligatoire depuis l'extérieur

Seul le VPN est accessible depuis l'extérieur pour protéger les services internes.

6.2 Sécurisation LDAP

- Utilisation de LDAPS (**LDAP over SSL/TLS**) pour chiffrer les échanges
- Mise en place d'un **mot de passe fort** et renouvellement périodique
- Activation de **MFA** pour les comptes utilisateurs (via l'application **Google Authenticato**r ou **token**)

6.3 Pare-feu

Le pare-feu est configuré pour limiter les accès aux seuls ports nécessaires (VPN, LDAP, NFS, DHCP, DNS).

Service	Port(s) TCP/UDP	Remarques
SSH	22 TCP	Administration distante
VPN (exemple OpenVPN)	1194 UDP	Accès sécurisé externe
LDAP	389 TCP	Authentification LDAP (non sécurisé)
LDAPS	636 TCP	LDAP sécurisé
NFS	2049 TCP/UDP	Partage fichiers /home
RPC (portmapper)	111 TCP/UDP	Nécessaire pour NFS et autres
DHCP	67/68 UDP	Attribution IP (serveur & client)
DNS	53 TCP/UDP	Résolution noms
HTTP/HTTPS (optionnel UI)	80/443 TCP	Interface graphique (si présente)

Pour des raisons de sécurité, il est **préférable de modifier les numéros de ports pour réduire la surface d'attaque**.

À coupler avec les autres paramètres de sécurité tels que VPN, MFA, pare-feu strict et monitoring.

Ex pour **SSH** :

- Modifier `/etc/ssh/sshd_config`

sudo nano /etc/ssh/sshd_config

Port 2222

(pour passer le SSH au port 2222 par exemple)

- Redémarrer le service SSH :

sudo systemctl restart sshd

- Modifier le pare-feu pour autoriser le nouveau port 2222

iptables -A INPUT -p tcp --dport 2222 -j ACCEPT

Pour LDAP, NFS, etc.

- **LDAP :** modifier le port dans la config slapd (pas trivial, mais possible). Souvent mieux de sécuriser via LDAPS et firewall.

- **NFS :** les ports peuvent être configurés (notamment portmapper et nfsd) pour utiliser des ports fixes. Sinon c'est plus compliqué car NFS utilise plusieurs ports RPC.

Recommandation

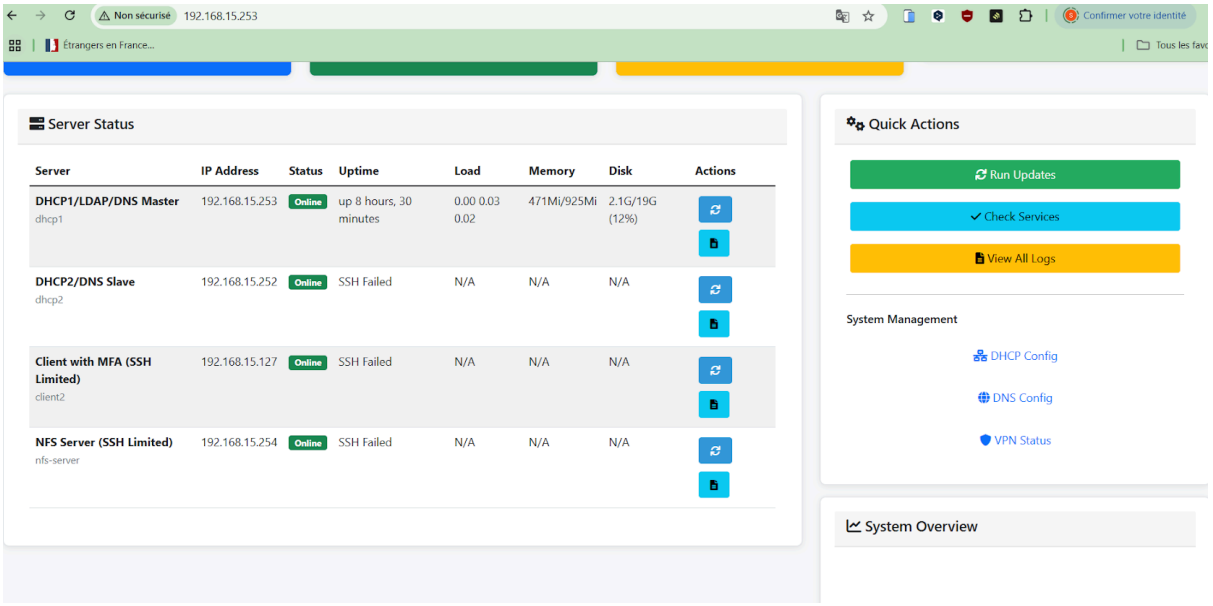
- Changer le port SSH au minimum
- Pour LDAP, privilégier LDAPS (636) avec firewall strict et VPN
- Pour NFS, fixer les ports RPC mais gestion avec prudence et attention (via **/etc/default/nfs-kernel-server**)

7. Interface de gestion centralisée

Une interface graphique (UI) est mise en place pour permettre la gestion simplifiée :

- Création et suppression d’utilisateurs LDAP
- Configuration des partages NFS
- Gestion des services DHCP et DNS
- Visualisation des journaux et alertes

Cette interface est accessible uniquement en interne via authentification sécurisée.



8. Plan de Reprise d’Activité (PRA) et Plan de Continuité d’Activité (PCA)

8.1 Objectifs

Garantir la disponibilité rapide des services critiques en cas d’incident majeur (panne serveur, attaque, coupure réseau).

8.2 Sauvegardes

- Sauvegardes quotidiennes des données LDAP, NFS et configurations sur un serveur dédié externe
- Vérification régulière de l'intégrité des sauvegardes

8.3 Basculement automatique

- Le système master/slave avec IP failover permet de basculer automatiquement vers le serveur secondaire en cas de panne.
- Test de basculement réalisé périodiquement.

8.4 Procédure de restauration

1. Détecter l'incident
2. Basculement sur le serveur secondaire si possible
3. Restaurer les données à partir des sauvegardes si nécessaire
4. Réparer ou remplacer le serveur défaillant
5. Retour en mode normal après validation des services

9. Annexes et ressources

- Liste des commandes utiles
- Références documentaires officielles (Debian, LDAP, NFS)
- Contacts techniques de l'association