Axes d'Évolution et Scalabilité de l'Infrastructure

Introduction

Avec une infrastructure réseau désormais stable, sécurisée et fonctionnelle, il est important d'anticiper l'évolution de l'environnement informatique afin de garantir sa pérennité, sa performance et sa capacité à absorber une montée en charge. Cette section présente les axes d'évolution envisageables, ainsi que des recommandations pour leur mise en œuvre progressive.

1. Mise en place d'un gestionnaire d'impression centralisé

Objectif :

Offrir aux utilisateurs une solution unifiée et sécurisée pour l'impression, quel que soit le poste client utilisé.

Solutions recommandées :

- **CUPS (Common Unix Printing System)** en mode serveur :
    - Installation sur un serveur dédié ou mutualisé avec d'autres services non critiques.
    - Connexion des imprimantes via USB, réseau ou IPP.
    - Mise en place de **quotas d'impression** via des outils comme **PyKota** ou **PaperCut**.
    - Authentification LDAP possible pour la gestion des utilisateurs et des droits d'accès aux imprimantes.

Sécurité

- Restreindre l’accès au serveur CUPS via le VPN.
- Gestion des droits d’impression par groupes LDAP.
- Journaux d’impression pour audit.

2. Sauvegarde des configurations critiques

Objectif :

Préserver les configurations système et réseau essentielles en cas de panne, erreur humaine ou attaque.

Composants à sauvegarder :

- **Fichiers de configuration** : `/etc`, `/var/lib/ldap`, `/etc/named`, `/etc/dhcp`, `/etc/nfs.conf`, `/etc/openvpn`, etc.

- Scripts d'automatisation, tâches cron, configurations RAID, règles iptables/nftables.

Outils et stratégies :

- **Rsync + cron** pour une sauvegarde automatique vers un NAS ou un serveur distant.
- **Rdiff-backup** ou **BorgBackup** pour une gestion efficace des versions et déduplication.
- **Sauvegarde chiffrée** en externe (sur site distant ou cloud chiffré via Rclone + crypt).
- Automatisation via Ansible pour re-déployer une configuration en quelques minutes.

Fréquence :

- Quotidienne ou hebdomadaire selon criticité.
- Sauvegarde incrémentielle avec rotation sur 7 à 30 jours.

3. Duplication des données du serveur NFS

Objectif :

Assurer une haute disponibilité et une résilience des données utilisateurs.

Solutions possibles

a) Réplication vers un NAS local

- Utilisation de **Rsync** avec une planification (toutes les nuits par exemple).
- Monté en **RAID 6 ou 10** pour garantir tolérance aux pannes.
- Option d'instantanés (snapshots) sur les NAS modernes (Synology, TrueNAS).

b) Réplication distante (off-site)

- **VPN site-à-site** pour synchronisation vers un autre site (ex : autre local de l'association).
- Chiffrement des données via **SSH**, **rsync+SSH** ou **Restic**.
- Sauvegarde dans un **cloud privé (Nextcloud)** ou public (Backblaze, S3, etc.) avec chiffrement.

c) Mise en place d'un système distribué :

- **GlusterFS** ou **CephFS** pour gérer la haute disponibilité et la répartition de la charge (plus complexe mais scalable).

Points d’attention :

- Gérer les conflits si multi-écriture.
- Assurer la cohérence (verrouillage, synchronisation).
- Surveillance de l’espace disque et alertes.

4. Autres pistes d’évolution

Supervision avancée :

- Déploiement de **Zabbix**, **Grafana + Prometheus**, ou **Nagios** pour la supervision réseau, charge CPU, RAM, services LDAP/DNS/DHCP/NFS.

Interface d’administration centralisée

- Utilisation d’**Ansible AWX** ou **Cockpit** pour l’interface Web de gestion.
- Centralisation des logs avec **Graylog** ou **ELK Stack** (ElasticSearch, Logstash, Kibana).

Intégration d’un annuaire centralisé de type SSO

- Mise en œuvre de **Keycloak** pour fédération d’identités, gestion MFA et SSO pour les services Web (Nextcloud, portail interne, interface de gestion, etc.).

Conclusion

Cette documentation fournit une base pour faire évoluer l’architecture actuelle vers un système plus robuste, sécurisé et capable de répondre à une montée en charge ou à une distribution géographique. Ces évolutions peuvent être planifiées progressivement, en priorisant les besoins immédiats (sauvegarde, gestion centralisée) avant d’aborder des solutions plus complexes (systèmes distribués, supervision avancée).