

Section 4 : Administration et sécurisation des infrastructures systèmes

4.1. Introduction à l'administration système

L'infrastructure système est l'ensemble des éléments logiciels (systèmes d'exploitation, services d'infrastructure, solutions collaboratives) qui permettent aux équipements, utilisateurs et applications de fonctionner.

L'administrateur AIS gère ces systèmes afin de garantir :

- La **stabilité et disponibilité** des services,
- La **sécurité** des données et des accès,
- La **performance** des environnements,
- La **conformité** avec les politiques de sécurité (PSSI), RGPD, et recommandations de l'ANSSI.

Les environnements visés sont :

- Serveurs physiques (on-premise),
 - Serveurs virtuels (VMware, Hyper-V),
 - Plateformes Cloud (Azure, AWS),
 - Solutions SaaS (Microsoft 365, Google Workspace).
-

4.2. Systèmes d'exploitation et environnements hétérogènes

Principaux OS gérés :

- **Windows Server** (2016, 2019, 2022)
- **Linux** (Ubuntu Server, Debian, CentOS, RedHat)
- **Unix** (Solaris, AIX – plus rares)

Missions principales :

- Installation, configuration, mise à jour
- Gestion des disques, partitions, RAID
- Gestion des services (NTP, DNS, DHCP...)
- Surveillance des performances système
- Analyse des journaux d'événements

Environnements hybrides :

- **Infrastructure cloud hybride** : Azure AD Connect, synchronisation AD local/Cloud

- **Interopérabilité** : partages de fichiers SMB/NFS, protocole LDAP, authentification SSO
-

4.3. Gestion des identités et des accès

La **gestion centralisée des utilisateurs, groupes, droits d'accès et authentifications** est au cœur de l'administration système.

Outils principaux :

- **Active Directory (AD)** : domaine, UO, GPO, scripts de connexion
- **Azure AD / Azure AD Connect**
- **LDAP, Samba**
- **Systèmes d'authentification forte** : MFA, OTP, certificat
- **Gestion des rôles et des permissions** : RBAC

Tâches typiques :

- Création de comptes utilisateurs
 - Affectation de permissions
 - Déploiement de stratégies de groupe (GPO)
 - Suivi des connexions, audit de sécurité
-

4.4. Services d'infrastructure essentiels

Les services doivent être **redondants, surveillés, sécurisés** :

Service	Fonction
DNS	Résolution de noms internes/externes
DHCP	Attribution dynamique d'adresses IP
RADIUS/NPS	Authentification réseau
Serveur de fichiers	Partage CIFS/SMB, quotas, DFS
Serveur d'impression	Gestion des files et des droits
Services de certificats (CA)	Gestion des certificats SSL, PKI

4.5. Outils de gestion système et d'automatisation

Outil	Usage
PowerShell	Scripts d'administration Windows
Bash	Scripts Linux
Ansible	Déploiement et configuration automatisés
GLPI / OCS Inventory	Inventaire, gestion des incidents
WSUS / SCCM	Déploiement de mises à jour Windows
Cron / Task Scheduler	Tâches planifiées

4.6. Sauvegardes et restauration

Les sauvegardes sont **une obligation réglementaire** (RGPD, ANSSI) et une condition essentielle de continuité d'activité (PRA/PCI).

Solutions :

- **VEEAM, Veritas Backup Exec, Acronis**
 - Sauvegarde complète, incrémentale, différentielle
 - Tests de restauration réguliers
 - Sauvegardes externalisées (cloud, off-site)
 - Chiffrement des sauvegardes
 - Journalisation des opérations
-

4.7. Supervision système et analyse des événements

L'administrateur surveille :

- L'utilisation des ressources système (CPU, RAM, disque)
- Les services critiques
- Les fichiers journaux et événements

Outils :

- **Event Viewer** (Windows)
 - **Syslog, Logwatch, Journalctl** (Linux)
 - **Zabbix, Nagios, Centreon**
-

4.8. Sécurisation des systèmes

Actions essentielles :

- **Durcissement (hardening)** des OS
- Fermeture des ports inutilisés
- Désactivation des services non essentiels
- Application des mises à jour de sécurité
- Gestion des droits par le principe du moindre privilège
- Utilisation d'**antivirus/EDR**
- Implémentation de la supervision de la sécurité (Wazuh, OSSEC)

Recommandations ANSSI :

- Utilisation de bastions pour les connexions distantes
 - Journalisation complète et horodatée
 - Tests réguliers de sécurité
-

4.9. Cloud et SaaS : gestion des services Microsoft 365

Un AIS administre aussi des environnements **100% cloud ou hybrides**.

Services Microsoft 365 :

- Exchange Online (boîtes mail)
- SharePoint / OneDrive
- Teams
- Intune (gestion de terminaux)
- Azure AD

Compétences nécessaires :

- Gestion des licences
 - Sécurisation des accès (MFA, Conditional Access)
 - Surveillance des logs
 - DLP, chiffrement, conformité RGPD
-

4.10. Mise en situation, projets et évaluation

Projets pédagogiques :

- Déploiement d'un contrôleur de domaine + GPO
- Configuration d'un serveur DNS/DHCP sécurisé
- Mise en place d'un cluster de fichiers sous Windows
- Script d'automatisation pour la création d'utilisateurs
- Déploiement d'Azure AD + MFA + SharePoint

Évaluation :

- **QCM** : commandes, principes, pratiques sécurisées
- **Étude de cas** : diagnostic d'un serveur défaillant
- **Projet** : documentation + mise en œuvre d'une solution