

Section 1 : Introduction au métier d'Administrateur d'Infrastructures Sécurisées

1.1. Présentation générale du métier

L'Administrateur d'Infrastructures Sécurisées (AIS) est un acteur clé du système d'information (SI) d'une organisation. Il est le **garant de la disponibilité, de la performance, de la sécurité** et de **l'évolution technique** de l'infrastructure IT de l'entreprise, qu'elle soit **hébergée localement ou dans le cloud**.

Ce professionnel agit en **hybride**, à la croisée des mondes physiques (on-premise) et virtuels (cloud AWS, Azure, etc.). Il est aussi un **technicien de haut niveau**, souvent spécialisé, qui assume une **responsabilité transversale** dans les domaines suivants :

- Réseaux (commutateurs, routeurs, VPN, VLAN...)
- Systèmes (Windows Server, Linux, Unix, Active Directory...)
- Virtualisation (VMware, Hyper-V, Proxmox...)
- Cloud (AWS, Azure, Google Cloud)
- Cybersécurité (politiques, détection, audits, traitement des incidents)

L'Administrateur AIS s'inscrit dans un **écosystème collaboratif** où il travaille aux côtés des chefs de projets, des exploitants, des RSSI, des techniciens, des utilisateurs finaux, et des prestataires. Son rôle stratégique le positionne comme **maillon central** entre les impératifs de performance opérationnelle et ceux de sécurité.

1.2. Objectifs de la fonction AIS

Les missions d'un Administrateur d'Infrastructures Sécurisées sont structurées autour de 3 grands objectifs :

1. **Maintien en Condition Opérationnelle (MCO)** : assurer la disponibilité des systèmes et réseaux.
 2. **Maintien en Condition de Sécurité (MCS)** : appliquer les règles de sécurité et veiller à leur mise en œuvre opérationnelle.
 3. **Évolution & adaptation du SI** : répondre aux nouveaux besoins techniques, métiers et réglementaires (RGPD, ANSSI, etc.).
-

1.3. Environnements d'intervention

Un AIS peut intervenir dans différents **contextes organisationnels et techniques** :

Type de structure	Spécificités
Grandes entreprises	Environnement complexe, segmentation des responsabilités, travail en équipe pluridisciplinaire
Collectivités / administrations	Fortes exigences de conformité (RGPD, accessibilité), contraintes budgétaires, gouvernance IT centralisée

Type de structure	Spécificités
PME ou ETI	Polyvalence accrue, autonomie dans les décisions, infrastructures parfois hétérogènes
Entreprises de Services Numériques	Missions clients, mobilité, orientation projet, exigences de certification et de rentabilité
Établissements de santé	Spécificités liées à la confidentialité des données patients, conformité HDS, continuité de service critique

1.4. Posture professionnelle et responsabilité

L'administrateur AIS est soumis à des exigences **éthiques, réglementaires** et **techniques** :

- **Responsabilité technique** : chaque action peut avoir un impact majeur sur la continuité d'activité.
 - **Confidentialité** : respect des politiques internes, secret professionnel, journalisation des accès.
 - **Réactivité et rigueur** : capacité à intervenir en astreinte, en situation de crise (cyberattaque, panne).
 - **Communication** : il adapte son langage selon l'interlocuteur (direction, utilisateurs, techniciens).
 - **Autonomie encadrée** : il prend des décisions dans son périmètre mais alerte sa hiérarchie au besoin.
-

1.5. Compétences requises (synthèse des blocs)

Les **compétences cœur** attendues sont :

▪ Techniques :

- Administration des serveurs, réseaux et plateformes cloud
- Supervision et monitoring d'infrastructures
- Sécurisation des systèmes et réseaux (pare-feu, MFA, PSSI...)
- Gestion d'incidents et de vulnérabilités
- Intégration de solutions techniques

▪ Organisationnelles :

- Planification, documentation, mise en œuvre de procédures
- Utilisation d'outils ITSM et de ticketing (GLPI)
- Reporting, gestion des changements

▪ Transversales :

- Communication professionnelle orale/écrite en français et en anglais

- Veille technologique permanente
 - Connaissances des normes ISO, ANSSI, RGPD, ITIL
-

1.6. L'environnement technologique de l'AIS

Un administrateur d'infrastructures sécurisées doit maîtriser des **technologies variées**, parmi lesquelles :

- **Réseaux** : Cisco, Mikrotik, Fortinet, VLAN, QoS, HSRP, VPN IPsec
 - **Systèmes** : Windows Server, Linux Ubuntu/CentOS, Active Directory, PowerShell
 - **Cloud** : AWS (EC2, S3, IAM), Azure (VM, AD Connect, NSG)
 - **Supervision** : Zabbix, Centreon, Grafana, Prometheus
 - **Sécurité** : SIEM (Wazuh, Splunk), IDS/IPS, MFA, Firewall UTM
 - **Outils de gestion** : GLPI, Git, GitLab, Jenkins, Ansible, Terraform
-

1.7. Évolutions du métier

Le métier évolue sous l'effet de plusieurs tendances fortes :

- **Hybridation infrastructurelle** : on-premise + cloud = SI hybride
 - **Explosion de la cybersécurité** : rôle renforcé dans la prévention et la réponse aux attaques
 - **Automatisation croissante** : scripting, orchestration, Infrastructure as Code (IaC)
 - **Accès distant et BYOD** : nouveaux risques, nouveaux outils de contrôle
 - **Obligations légales accrues** : conformité RGPD, RGS, référentiels ANSSI
-

1.8. Relations et collaboration

L'AIS collabore avec un large éventail d'interlocuteurs :

Interlocuteurs	Rôle
DSI / RSI	Pilotage du SI, définition des politiques techniques
RSSI	Encadrement de la sécurité, application de la PSSI
Exploitants / techniciens	Mise en œuvre des opérations quotidiennes
Chefs de projet	Coordination lors de changements d'infrastructure
Fournisseurs / prestataires	Support, livraison, expertise
Utilisateurs finaux	Bénéficiaires des services, clients internes
Analystes cybersécurité, SOC, CERT	Détection et gestion des incidents de sécurité

1.9. Enjeux éthiques et réglementaires

Les AIS évoluent dans un cadre soumis à plusieurs règles de conformité :

- **RGPD** : traitement des données personnelles, droits des utilisateurs
 - **ANSSI** : recommandations de sécurité, référentiels PSSI
 - **Accessibilité** : conformité RGAA, éco-conception numérique
 - **Traçabilité** : journalisation des accès, preuves numériques
 - **Confidentialité et intégrité** : protection de l'information sensible
-

1.10. Intégration de l'alternance dans le parcours de formation

La formation au Greta est organisée en **alternance**, combinant :

- **Cours théoriques** (distanciels et présentiels)
- **Pratique en entreprise** (missions réelles)
- **Suivi pédagogique** (tutorat, carnet de liaison, e-portfolio)

Ce format renforce :

- L'acquisition de **réflexes professionnels**
- La capacité à travailler en **conditions réelles**
- L'appropriation de **méthodologies** et d'**outils utilisés en entreprise**