

Gestion des incidents et des demandes d'assistance

10.1. Introduction à la gestion des incidents

La gestion des incidents constitue l'une des missions les plus visibles et récurrentes d'un administrateur AIS. Elle consiste à **identifier, qualifier, traiter et résoudre les dysfonctionnements affectant les systèmes ou les utilisateurs**, tout en respectant les engagements de service (SLA) et la **politique de sécurité de l'entreprise**.

Objectifs :

- Rétablir la situation normale le plus rapidement possible,
 - Minimiser l'impact sur les utilisateurs,
 - Maintenir un historique complet des problèmes et solutions,
 - Détecter les causes récurrentes,
 - Garantir la traçabilité et la conformité.
-

10.2. Typologie des incidents

Type d'incident	Exemples
Matériel	Panne serveur, disques défectueux
Logiciel	Application figée, bug système
Réseau	Perte de connectivité, latence
Sécurité	Compte bloqué, tentative d'intrusion
Utilisateurs	Mot de passe oublié, erreur de manipulation
Cloud / SaaS	Service inaccessible, synchronisation échouée

10.3. Cycle de vie d'un incident (modèle ITIL)

1. **Enregistrement** : via ticket, mail, appel
 2. **Qualification** : niveau de gravité, service impacté
 3. **Priorisation** : selon l'urgence et l'impact
 4. **Affectation** : technicien, équipe ou prestataire
 5. **Diagnostic** : analyse des causes probables
 6. **Résolution** : application de la solution
 7. **Clôture** : validation par l'utilisateur
 8. **Post-mortem** (si incident majeur)
-

10.4. Outils de gestion des incidents

Systèmes de gestion de tickets :

Outil	Fonction
GLPI	Open source, base de parc, tickets, CMDB
iTop	ITSM structuré
OTRS	Gestion multicanal des demandes
Jira Service Management	Intégration DevOps
Freshservice	SaaS cloud simple d'usage

Fonctionnalités clés :

- Numéro de ticket, SLA, historique
 - Catégorisation et affectation automatique
 - Liens avec base de connaissance
 - Notifications automatiques
 - Statistiques de suivi
-

10.5. Communication et gestion des utilisateurs

L'administrateur AIS doit faire preuve :

- De **clarté** (explications compréhensibles),
- De **pédagogie** (éviter le jargon technique),
- De **réactivité** (respect des délais),
- De **courtoisie** (même en cas de stress).

Bonnes pratiques :

- Confirmer la réception du ticket
 - Rappeler les étapes prévues
 - Informer lors de la prise en charge
 - Proposer des alternatives en attendant la résolution
 - Faire valider la clôture par l'utilisateur
-

10.6. Dépannage technique et diagnostic structuré

Étapes du diagnostic :

1. **Identification précise du symptôme**
2. **Délimitation du périmètre** (utilisateur, machine, réseau ?)
3. **Consultation des journaux (logs, Event Viewer, syslog)**

4. **Tests ciblés (ping, nslookup, netstat, etc.)**
5. **Consultation base de connaissance / historique**
6. **Hypothèse + test + vérification**

Exemples d'outils :

- ping, tracer, nslookup, ipconfig, netstat
 - Event Viewer, journaux système
 - GLPI + historique de la machine
 - Outils de monitoring (Zabbix, Grafana)
-

10.7. Incidents majeurs et gestion de crise

Un incident est **majeur** si :

- Il affecte un **grand nombre d'utilisateurs**
- Il concerne un **système critique**
- Il touche à la **sécurité**

Procédures associées :

- Activation de la **cellule de crise** (DSI, RSSI, direction)
 - **Communication centralisée** et coordonnée
 - **Traçabilité absolue** des décisions
 - **Déclaration CNIL** si données personnelles compromises
 - **Post-mortem** obligatoire
-

10.8. Gestion des demandes (support de niveau 1 à 3)

Les demandes sont différentes des incidents : il s'agit d'**actions souhaitées par les utilisateurs sans dysfonctionnement**.

Niveau	Exemple
Niveau 1	Réinitialisation de mot de passe
Niveau 2	Installation de logiciel spécifique
Niveau 3	Intervention sur le serveur, migration, stratégie AD

Traitement :

- Même outil que les incidents
- Priorisation selon l'impact
- Historique et traçabilité identiques
- Possibilité d'**automatiser certaines tâches** (self-service, script)

10.9. Exploitation des tickets et amélioration continue

La base de tickets est une **mine d'informations** :

- Identifier les **incidents récurrents** = candidats à une **automatisation** ou une **formation utilisateur**
 - Réduire le **temps moyen de traitement** (MTTR)
 - Fournir des **rapports mensuels à la DSI**
 - Alimenter la **base de connaissance**
-

10.10. Activités pratiques et évaluation

Projets pédagogiques :

- Configuration de GLPI avec création de tickets
- Simulation d'incident (postes + réseau + serveur)
- Création de modèles de réponses types
- Construction d'un tableau de bord de suivi d'incidents

Évaluations :

- QCM ITIL + diagnostic réseau
- Étude de cas (analyse + solution + rédaction ticket)
- Présentation d'un incident résolu (dossier + oral)