

GESTION DES INCIDENTS ITSM

EXERCICE 1

Introduction à la gestion des incidents et support ITSM

Objectifs :

- Comprendre les concepts clés d'ITSM et ITIL.
- Identifier les objectifs du support IT.
- Cerner les enjeux de la gestion des incidents.
- Repérer les acteurs du support et leurs rôles.
- Comprendre le processus ITSM.

Exercice : Simulation de Gestion d'Incident

Objectif : Appliquer les connaissances acquises sur le processus de gestion des incidents en simulant un scénario réel.

Énoncé : Vous travaillez dans le département IT d'une entreprise et vous recevez un rapport indiquant qu'un service critique est hors ligne. Suivez le processus de gestion des incidents pour enregistrer, catégoriser, prioriser et attribuer cet incident. Rédigez un rapport détaillé des étapes que vous suivez, y compris le diagnostic initial, les actions de résolution tentées et la communication avec les parties prenantes concernées.

Décrivez également comment vous surveillerez et communiquerez sur l'avancement jusqu'à la résolution de l'incident.

Proposition de solution:**Contexte:**

- **Nom du service concerné** : Application interne de facturation.
- **Nature de l'incident** : Le service est hors ligne (erreur 503 – Service indisponible)
- **Signalement** : Appel utilisateur + alerte du système de monitoring Zabbix
- **Impact** : Blocage de la génération des devis et factures – impact direct sur le service client.

1. Enregistrement de l'incident:

Élément	Détail
Numéro de ticket	INC-2025-0012
Date / Heure de détection	01/09/2025 – 08h42
Origine du signalement	Utilisateur + supervision
Description initiale	Impossible d'accéder à l'application FactuPro – message "Erreur 503"
Utilisateur affecté	Équipe commerciale – 25 utilisateurs
Outil de gestion utilisé	GLPI (ou Jira Service Management)

2. Catégorisation et priorisation:

- **Catégorie** : Service applicatif → Application métier → Facturation
- **Type** : Incident technique – Application inaccessible
- **Impact** : Élevé – Service critique affectant directement le chiffre d'affaires
- **Urgence** : Élevée – Blocage total de l'activité commerciale

- **Priorité calculée** (Impact x Urgence) : Critique (P1)

3. Affectation:

- Support N1 a enregistré et qualifié l'incident.
- Transfert immédiat à l'équipe N2 (administrateurs applicatifs) pour investigation.
- Notification automatique envoyée à l'Incident Manager (car incident critique).

4. Diagnostic initial:

Vérifications réalisées (support N2) :

- L'application FactuPro ne répond pas sur le port 443 (HTTPS)
- Le serveur web répond au ping, mais pas à la requête HTTP
- Le service Apache est à l'arrêt
- Journal /var/log/httpd/error.log : erreurs liées à un fichier de configuration manquant

5. Actions de résolution:

1. Redémarrage du service Apache → Échec (erreur de configuration)
2. Restauration de la dernière version fonctionnelle du fichier httpd.conf
3. Vérification des dépendances applicatives (base de données, certificat SSL)
4. Relance complète de l'application + tests utilisateurs
5. Rétablissement du service confirmé à 10h12

Durée totale de l'incident : 1h30

6. Communication pendant l'incident

Heure	Message
08h45	Alerte envoyée aux utilisateurs via Teams : "Incident en cours sur l'application de facturation, investigations en cours."
09h15	Point d'avancement : "Cause probable identifiée, intervention technique en cours."
10h15	Message de rétablissement : "Service FactuPro rétabli. Veuillez nous signaler tout dysfonctionnement."

- Mise à jour en temps réel dans l'outil de ticketing
- Communication proactive avec le chef de service commercial.

7. Clôture et post-mortem:

Élément	Détail
Date / heure de clôture	01/09/2025 – 10h20
Solution appliquée	Restauration de fichier de conf + redémarrage service web
Résolution validée par	Utilisateur référent de l'équipe commerciale
Analyse post-incident	Le fichier httpd.conf a été modifié par erreur suite à un déploiement sans validation par le Change Manager

8. Suivi et amélioration continue:

- **Ajout de ce scénario dans la base de connaissance (KEDB)** : “Erreur 503 - Apache”
- **Action préventive** : Renforcement de la procédure de déploiement (soumise à CAB)
- **Mise à jour CMDB** : Modification du composant WebServer-FactuPro
- **Suivi KPI mensuel** : Incident critique résolu sous 2h → Respect du SLA

Conclusion:

L'incident a été détecté rapidement grâce à la supervision et la remontée utilisateur.
L'application du processus ITIL a permis :

- Une qualification rapide;
- Une communication transparente;
- Une résolution sous délai critique;
- Une capitalisation pour éviter sa réapparition.