Présentation de la gestion des incidents

Qu’est-ce qu’un incident ?

Dès que qu’un service est **arrêté** ou que la **qualité du service diminue**, il y a un incident.

Quelques exemples d’incidents :

- ma souris ne fonctionne plus ;
- une application métier se bloque ;
- je n’arrive plus à accéder à mes documents sur le serveur distant ;
- une transaction sur un serveur distant qui dure en moyenne 2 à 3 secondes ne donne pas de réponse au bout de 10 secondes ;
- mon imprimante n’a plus de toner.

Un incident est détecté soit par un utilisateur qui va contacter le **Centre de services** en appelant un numéro spécifique, soit par des outils de supervision.

Le contrat de service et gestion des incidents

Les bonnes pratiques **ITIL** permettent de contractualiser la gestion des incidents en définissant et en gérant des niveaux de service.

Cycle de vie du service : expression du besoin, solution mise en œuvre, exploitation et support.

Le **client** (donneur d’ordre) doit trouver un **accord** auprès du **prestataire informatique** sur la solution mise en œuvre et son coût. Cet engagement réciproque est formalisé dans un **contrat de service**.

Le contrat de service

Le contrat de services ou **SLA** (Service Level Agreement), lie le client et le fournisseur des services informatiques (interne ou externe à l’organisation).

Le SLA est :

- un accord sur le **service proposé**,
- un accord sur les **niveaux** de services associés
- un accord sur le **coût** de la solution.
- un **engagement de résultat** sur des objectifs à atteindre pour un ou plusieurs services.

Le SLA précise les **droits** et les **devoirs** de chaque partie, les responsabilités de chacun pour une **période donnée**. A **l’échéance** du contrat, celui-ci est **renégocié**.

Que contient le contrat de service ?

Voici des exemples d’informations que doit contenir le SLA :

- Une **description** du service en termes de fonctionnalités.
- Le **taux de disponibilité** sur une période donnée avec la durée maximale d’indisponibilité.
- Les modalités de **support** et en particulier les heures d’ouverture du centre de services.
- Les **coûts** associés à la production du service.
- Les **indicateurs** permettant de vérifier que les engagements sont tenus.
- Les modalités de **production** des **tableaux de bord** (fréquence, communication)
- Les **pénalités** pour non-respect des engagements de la part du fournisseur du service. Si le prestataire est un service informatique interne, il n’y a pas nécessairement de pénalités.
- La **durée** du contrat.

Les états d’un service

Ces précisions sur la notion d’incident permettent de définir la notion d’état d’un service :

- un service est **nominal** s'il fonctionne comme il a été conçu et architecturé.

Exemple : une plateforme de virtualisation est architecturée avec quatre serveurs en cluster et ces quatre serveurs sont opérationnels.

- Un service est **normal** (ou standard) quand il fonctionne en **conformité** avec l'accord de niveaux de services (SLA).

En reprenant l'exemple précédent, si un des serveurs de la plate-forme de virtualisation est arrêté à cause d'une panne ou pour des opérations de maintenance mais que les performances ne sont pas dégradées et que les utilisateurs ne s'en rendent pas compte, alors le service est normal.

- Un service est **dégradé** s'il fonctionne avec un **niveau de qualité en dessous** de ce qui est mentionné dans l'accord de niveaux de services (SLA).

Par exemple si cette fois-ci deux des quatre serveurs sont arrêtés, les applications sont moins réactives et les utilisateurs s'aperçoivent de cette dégradation.

- Un service est **arrêté** et ne fonctionne donc plus.

Incident : un incident survient lorsqu'un service passe de l'état nominal ou normal à l'état dégradé ou arrêté.

Impact, urgence, priorité

Chaque incident doit être codifié pour déterminer la priorité que l'on va lui attribuer. Une notation est utilisée en général sur une échelle de 1 à 3 ou de 1 à 5 (1 : Élevé, 3 ou 5 : Faible).

Il faut distinguer **l'impact** de **l'urgence** d'un incident :

- **L'impact** est l'effet de l'incident sur **l'utilisation** du service comme par exemple la perte d'exploitation (serveurs indisponible), ou le nombre d'utilisateurs qui ne peuvent pas travailler, etc.
- **L'urgence** est le temps nécessaire pour **rétablir** le service avant que les effets de l'incident ne se fassent sentir. Par exemple, la non disponibilité de l'application de gestion de la paie n'a pas la même importance si cela arrive en début de mois ou en fin de mois quand il faut établir les bulletins de paie.

La **priorité de l'incident** résulte de son impact et son urgence sur l'activité métier. Cette priorité permet d'identifier l'importance relative des incidents les uns par rapport aux autres.

Voici un tableau montrant un exemple de calcul de la priorité en fonction de l'impact et de l'urgence.

Impact / Urgence	**1**	**2**	**3**
1	P1	P2	P2
2	P2	P2	P3
3	P3	P3	P3

À chaque **niveau** de priorité (P1, P2, P3), on affecte un **délai de rétablissement**.

Par exemple : P1 = 2h, P2 = 8h, P3 = 24h.

Ces **codifications** d'un incident (impact, urgence, matrice d'attribution des niveaux de priorité et délais de rétablissement) doivent être explicitées dans le SLA avant la mise en exploitation du service.

Incident majeur

Les incidents qui ont un **impact très important** sur l'activité métier sont des incidents majeurs et sont de ce fait **hors grille de codification. Ils sont traités différemment des autres incidents et nécessite une procédure de "crise**".

Les objectifs de la gestion des incidents

En cas d'incident, il faut **rétablir** au plus vite le service dans un état **normal**, conformément à l'accord de niveaux de services associé (SLA) et **minimiser l'impact** de l'incident sur les utilisateurs.

Rétablir le service

Rétablir le service ne signifie pas nécessairement trouver une solution, mais **remettre en marche** le service afin et qu'il fonctionne à nouveau dans un état normal ou standard. C'est le processus de **gestion des problèmes** qui permettra d'apporter une réponse durable.

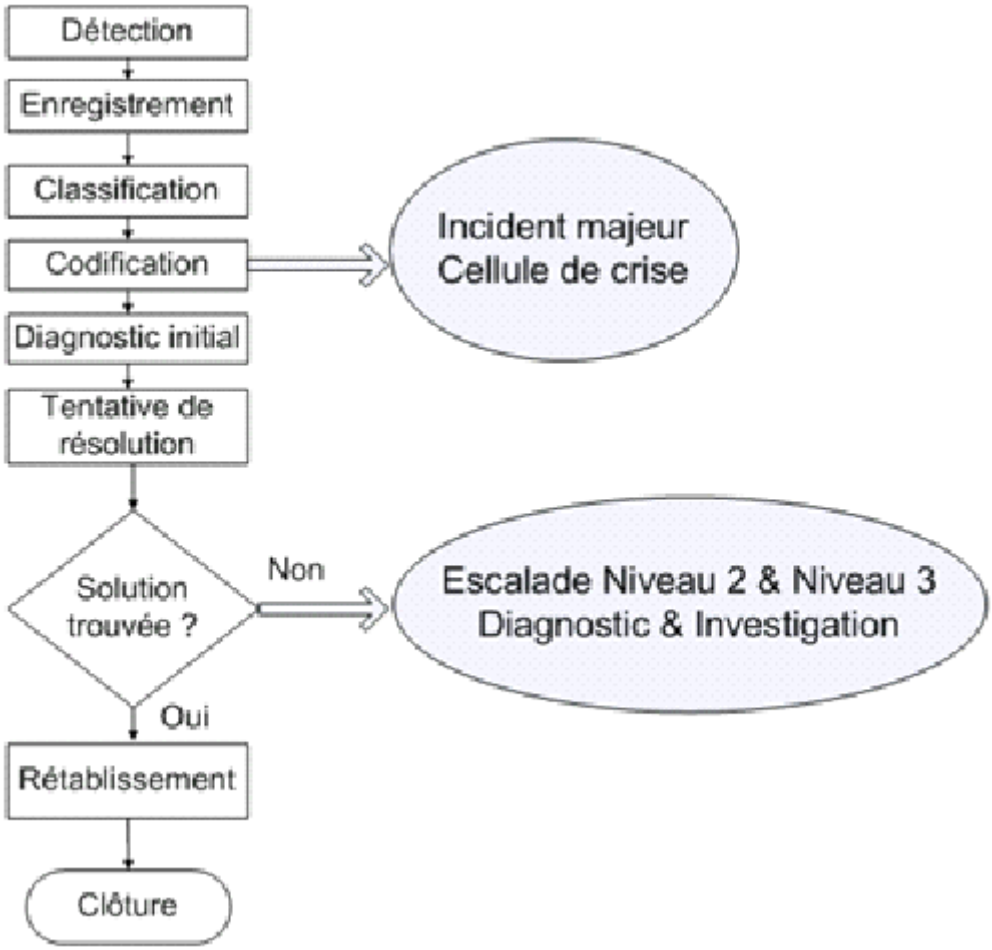
Exemple : Une application ne fonctionne plus correctement sur un serveur d'exploitation. Il peut être possible de rétablir le service en relançant le serveur et si nécessaire en restaurant une sauvegarde. En procédant ainsi, on rétablit le service sans pour autant avoir compris la cause de cet arrêt de service. Comme le service fonctionne à nouveau dans l'état normal, vous avez résolu l'incident ce qui est attendu par le client et les utilisateurs du service. Ce n'est probablement pas satisfaisant pour le service informatique car la panne pourra à nouveau se reproduire. C'est le processus de gestion des problèmes qui permet de résoudre cette situation.

Minimiser l'impact

Gérer un incident c'est également **minimiser** son impact sur l'activité métier des utilisateurs. En faisant le nécessaire pour remettre le service ou une partie du service en état de fonctionnement, le résultat pourra être un fonctionnement avec une dégradation de la qualité du service (moindre performances, fonctionnalités limitées, etc.).

Les activités du processus de gestion des incidents

Voici un schéma de l'enchaînement des principales activités du processus de gestion des incidents.



- **Détection** : une situation est identifiée comme un incident quand l'utilisateur contacte le centre de services ou par le personnel chargé de l'exploitation.
- **Enregistrement** : à chaque incident, il y a ouverture d'un **ticket d'incident** avec les informations administratives (date et heure, nom de la personne qui a détecté l'incident, lieu et site, numéro de contrat si nécessaire...).
- **Classification** : à partir de **modèles d'incidents**, le centre de service catégorise l'incident selon leur type prédéfini. Pour cela une série d'étapes, de **questions hiérarchisées** permettront de déterminer le type de l'incident ce qui déterminera les ressources à mobiliser pour le résoudre.
- **Codification** : une **priorité** est attribuée avec les délais de rétablissement prévue par contrat. Ce n'est pas l'utilisateur mais le centre de services qui assume cette responsabilité. La codification peut déclencher la procédure de crise dans le cas d'un incident majeur.
- **Diagnostic initial** : une recherche est effectuée pour déterminer si la situation décrite est déjà connue dans les bases de connaissance.
- **Tentative de résolution** : une procédure de rétablissement permet de **restaurer** le service. Cette résolution est facilitée si la situation décrire est déjà mémorisée dans la base de connaissance. Le centre de service est le **niveau 1 de support**. S'il ne peut

résoudre l'incident, il y a **escalade** (transfert) vers les niveaux supérieurs, niveau 2, puis niveau 3.
- **Clôture** : il s'agit de **fermer le ticket** d'incident en y ajoutant toutes les informations utiles (temps d'indisponibilité, actions effectuées pour rétablir le service, nom du ou des intervenants, etc.). La clôture doit se faire avec **l'accord** de l'utilisateur concerné, en essayant de **mesurer sa satisfaction**.

Ce qui est **important** dans la gestion des incidents :

- **Tous** les incidents doivent être **tracés**.
- La **détection** d'un incident doit être effectuée le plus **tôt possible**. L'utilisateur doit être sensibilisé pour qu'il informe le plus rapidement possible le centre de service dès qu'il constate une situation anormale. Des outils de surveillance permettent également de faire remonter des alertes (outils de supervision réseaux).

La procédure d'escalade

Quand un utilisateur **constate** un problème et contacte le centre de service, le processus de gestion des incidents peut activer une **démarche d'escalade en fonction de la complexité** de l'événement.

Le **premier niveau** est placé sur le **centre de services** qui s'efforce de diagnostiquer l'événement et d'apporter une solution.

Si le centre de service **ne peut résoudre** l'incident, alors, par escalade, l'événement est transmis à un niveau 2 pour être pris en charge par des expertises plus pointues. Ce 2ème niveau peut ne pas être situé dans le centre de services mais dans un autre service informatique ou chez un prestataire informatique spécialiste du domaine informatique concerné (système, réseau, application, développement).

Si nécessaire, d'autres niveaux d'escale seront sollicités jusqu'à la résolution de l'incident. Le plus haut niveau d'escalade correspond aux laboratoires du constructeur ou de l'éditeur.