ITIL V3

Exploitation des services :
La gestion des événements

Création : janvier 2008
Mise à jour : août 2009

Pascal Delbrayelle Consultant
+33 (0)6 61 95 41 40
http://www.itilfrance.com

A propos

A propos du document

Ce document de référence sur le référentiel ITIL V3 a été réalisé en se basant directement sur les 5 livres ITIL de la version 3 : *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* et *Continual Service Improvement* parus en 2007.

Il est mis à la disposition de la communauté francophone ITIL pour diffuser les connaissances de base sur ce référentiel.

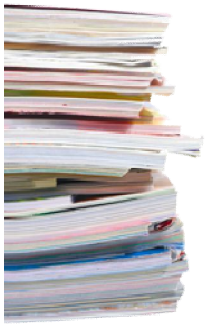
Ce document peut être utilisé de manière libre à condition de citer le nom du site (www.itilfrance.com) ou le nom de l'auteur (Pascal Delbrayelle).

A propos de l'auteur

Pascal Delbrayelle intervient avec plus de 25 ans d'expérience comme consultant sur les projets d'une direction informatique ayant comme facteur de succès la mise en oeuvre des bonnes pratiques ITIL comme, par exemple, la mise en place d'un site de secours, la mise en place d'un outil de gestion des configurations ou la définition des normes et standards techniques des environnements de production.

Ces projets requièrent :

- la connaissance des différents métiers du développement et de la production informatique
- la pratique de la conduite de projets techniques de la direction informatique
- la maîtrise de la définition et de la mise en place de processus pour rationaliser et adapter les méthodes de travail au sein de la direction informatique



A propos de mission et de formation

Si vous pensez que l expérience de l auteur sur le référentiel ITIL ou la formalisation de documents sur le sujet peut vous aider dans vos projets de production ou de mise en oeuvre des processus ITIL, n hésitez pas à le contacter pour toute question ou demande :

- par mail : pascal.delbrayelle@itilfrance.com
- par téléphone : +33 (0)6 61 95 41 40

Quelques exemples de mission :

- Modélisation simple des processus de gestion des changements, des projets et des mises en production en vue de la sélection, l'achat et l'implantation d'un outil de gestion de projets avec planification, gestion des ressources, des budgets, des livrables et des connaissances
- Accompagnement avec la réorganisation d'un DSI passant d'une organisation en silos techniques vers une organisation inspirée du référentiel ITIL et la mise en oeuvre d'outils pour institutionnaliser les processus ITIL
- Accompagnement d'une DSI dans la formulation de l'appel d'offres au futur centre de services en se basant sur les processus et la fonction centre de services du référentiel ITIL

Sommaire

1 Définition d'un événement

Un événement est une occurrence détectable ou discernable ayant :

- **une signification sur la gestion d une infrastructure ou la fourniture d un service et**
- **une évaluation de l impact indiquant qu une déviation pourrait apparaître sur les services**

Ils sont typiquement des notifications émises par un service des TI, un item de configuration ou un outil de supervision.

Il existe deux familles d outils de supervision :

- outils actifs qui interrogent régulièrement les items de configuration sur leur état et leur disponibilité ; toute exception déclenche une alerte transmise à l outil ou l équipe appropriée
- outils passifs qui détectent les alertes et communications en provenance des items de configuration et qui font des corrélations pour identifier des exceptions

2 Objectifs du processus

2.1 Objectif du processus

Détecter les événements, leur donner une signification et déterminer la réaction appropriée

Les événements transmis peuvent aussi servir de base à des routines automatisées (exécution de scripts, soumission de traitements batch, équilibrage dynamique de la charge d un service sur plusieurs ressources physiques, etc.)

Ils fournissent aussi des données de base pour comparer performance et comportement face à des standards et les SLA (accords de niveau de service)

2.1.1 Périmètre du processus

Le processus s applique à tout aspect de la gestion des services nécessitant d être contrôlé de manière automatisée :

- items de configuration
  - certains doivent rester dans un état précis
  - d autres ont un statut qui change fréquemment (mise à jour automatique de la CMS Configuration Management System)
- environnement informatique (détecteurs d incendie,)
- licences logicielles : contrôle de l usage
- sécurité (détection d intrusion,...)
- activité normale (traçage de l utilisation d une application,)

2.1.2 Valeur apportée à l entreprise

Généralement indirect :

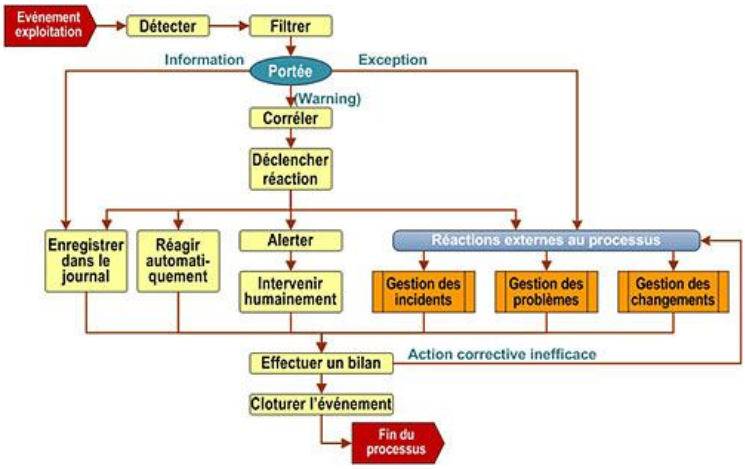
- **fournit des mécanismes pour une détection rapide des incidents** : Ils sont assignés à l équipe de support appropriée avant même qu un utilisateur ne signale un dysfonctionnement
- **rend possible la surveillance de certaines activités par exception** : Cela permet d éviter le coût d une surveillance en temps réel
- **en liaison avec les autres processus (disponibilité, capacité,)** : signale les changements et les exceptions aux équipes appropriées pour une réponse rapide ; processus plus efficaces et efficients pour les organisations métiers
- **permet aux personnes de se concentrer sur des activités innovantes pour accroître la compétitivité**

2.1.3 Concepts de base

Différents types d événement :

- **signale une opération normalement effectuée** :
  - notification de la bonne fin d un traitement batch
  - connexion d un utilisateur à une application
  - email reçu par son destinataire
- **signale une exception :**
  - tentative de connexion d un utilisateur avec un mot de passe erroné
  - situation inhabituelle dans un processus métier nécessitant une investigation (par ex. alerte d une page web signalant qu un site d autorisation de paiement est indisponible)
  - scan d un poste de travail repérant un logiciel installé non autorisé
- **signale une opération inhabituelle :**
  - indication d une situation nécessitant une surveillance plus serrée (par ex. le temps d éxécution d une requête est supérieure de 10% à la normale)

3 Activités du processus



3.1 Déclenchement du processus

Les événements surviennent continuellement mais ils ne sont pas tous détectés ou enregistrés.

Il est important que chaque personne impliquée dans :

- la conception,
- le développement,
- la gestion et
- le support des services des TI et des infrastructures

identifient les types d événements nécessitant leur détection.

3.2 Activité « Détecter »

Dans un monde idéal : identifier en phase de conception du service les événements à détecter.

Dans le monde réel : les événements sont identifiés par tatonnements et erreurs.

Point de départ : le paramétrage standard des items de configuration.

A compléter en intégrant l amélioration du paramétrage dans les activités d amélioration permanente.

Principe général : la notification doit contenir des informations pertinentes, facilitant et accélérant l interprétation de l événement et la réaction :

« Erreur survenue pendant le traitement »

3.3 Activité « Filtrer »

Décider ensuite si l événement détecté doit être transmis à un outil de supervision ou ignoré.

Ignoré signifie enregistrer l événement dans un fichier trace sans autre action.

Cas d utilisation :

- la génération d événements ne peut pas être coupée
- seul le premier événement d une série sera transmise

Il faut aussi déterminer la portée de l événement : information, avertissement (warning) ou exception.

3.4 Activité « Corréler les événements »

Corréler plusieurs événements permet d affiner ou de modifier la catégorisation des événements :

- nombre significatif d événements similaires (par ex. 3ème tentative de connexion d un utilisateur avec un mot de passe erroné)
- nombre significatif d items de configuration générant des événements similaires
- comparaison avec une valeur limite (dépassement d un seuil)