Qu'est-ce que le FinOps ?

FinOps (contraction de *Finance* et *DevOps*) est une pratique de gestion qui vise à **optimiser les coûts liés au Cloud** tout en favorisant la collaboration entre les équipes *financières*, *techniques* et *opérationnelles*.
L'objectif principal est d'assurer un **équilibre entre performance, innovation et maîtrise budgétaire** dans l'utilisation des ressources Cloud.

Principes clés du FinOps :

- **Visibilité des coûts :** suivre et analyser la consommation des ressources Cloud.
- **Responsabilisation :** impliquer les équipes techniques dans la maîtrise des dépenses.
- **Optimisation continue :** adapter les services (dimensionnement, arrêt automatique, réservation).
- **Collaboration :** créer un langage commun entre IT, finance et management.

Exemples de pratiques FinOps :

- Mettre en place des tableaux de bord de suivi des dépenses Cloud.
- Identifier les ressources sur-provisionnées ou inutilisées et les supprimer.
- Comparer les modèles de facturation (*on-demand*, *reserved instances*, *spot*).

Qu'est-ce que le Shadow IT ?

Le **Shadow IT** désigne l'ensemble des outils, logiciels, applications ou services numériques utilisés dans une organisation **sans validation ni contrôle préalable de la DSI (Direction des Systèmes d'Information)**.
Ces solutions peuvent être mises en place par les employés pour répondre à un besoin métier immédiat (ex. : stockage Cloud personnel, messagerie non officielle, applications collaboratives).

Exemples de Shadow IT :

- Utiliser un compte *Dropbox* ou *Google Drive* personnel pour partager des fichiers professionnels.
- Installer un logiciel non autorisé sur son poste de travail.
- Employer une messagerie instantanée non validée (WhatsApp, Slack non officiel).
- Souscrire à un service SaaS sans l'accord de la DSI.

Risques liés au Shadow IT :

- **Sécurité :** fuite de données, absence de chiffrement, absence de mises à jour.
- **Conformité :** non-respect des réglementations (RGPD, ISO 27001).
- **Gestion des coûts :** abonnements redondants, dépenses non maîtrisées.
- **Support :** absence de garantie et d'intégration avec le SI officiel.

Mesures de prévention :

- Sensibiliser les utilisateurs aux risques du Shadow IT.
- Mettre en place des solutions officielles répondant aux besoins métiers.
- Surveiller le réseau et les postes pour détecter les usages non conformes.
- Encourager la communication entre utilisateurs et DSI.

Qu'est-ce qu'un Helpdesk ?

Un **helpdesk** (ou centre de support) est un *point de contact centralisé* entre les utilisateurs d'un système informatique et l'équipe de support technique. Il a pour mission de **répondre aux incidents**, de **traiter les demandes d'assistance** et de **faciliter la communication** entre les utilisateurs et la DSI.

Rôles principaux :

- Enregistrer et classifier les incidents ou demandes utilisateurs.
- Fournir une assistance de premier niveau (ex. : mot de passe oublié, problème d'impression).
- Escalader les problèmes complexes aux niveaux supérieurs de support.
- Suivre et documenter les tickets jusqu'à leur résolution.
- Produire des rapports pour améliorer la qualité des services IT.

Niveaux typiques de support :

- **Niveau 1 :** support de base, résolution des problèmes courants.
- **Niveau 2 :** experts techniques, résolution plus approfondie.
- **Niveau 3 :** spécialistes ou éditeurs, résolution des problèmes complexes.

Exemple en entreprise :

- Un utilisateur ne peut pas se connecter à son compte → création d'un ticket au helpdesk.
- Le helpdesk réinitialise son mot de passe (Niveau 1).
- Si le problème persiste, le ticket est transféré à l'équipe systèmes/réseaux (Niveau 2).

Outils de helpdesk courants : GLPI, OTRS, Freshdesk, Zendesk, Jira Service Management.

Qu'est-ce qu'un SLA (Service Level Agreement) ?

Un **SLA (Service Level Agreement)** ou *accord de niveau de service* est un **contrat formel entre un fournisseur de services et un client** qui définit précisément le *niveau de service attendu*. Il sert de référence pour mesurer la qualité des prestations fournies et établir des obligations réciproques.

Éléments clés d'un SLA :

- **Description du service :** portée, fonctionnalités, responsabilités.
- **Indicateurs de performance (KPI) :** disponibilité, temps de réponse, taux d'erreurs.
- **Objectifs de service :** taux de disponibilité garanti (ex. 99,9%), délai moyen de résolution d'incidents.
- **Obligations du client :** respect des procédures de signalement, fourniture des informations nécessaires.
- **Pénalités et compensations :** remises ou crédits en cas de non-respect des engagements.

Exemples concrets :

- Un fournisseur Cloud garantit une disponibilité de son service à **99,95%**.
- Un helpdesk s'engage à répondre aux tickets critiques sous **15 minutes**.
- Un opérateur télécom garantit un temps de rétablissement maximal de **4 heures**.

Rôle dans la gestion informatique : Le SLA est essentiel pour assurer la transparence, éviter les malentendus, et établir une base de confiance entre l'entreprise et ses prestataires ou services internes.

La CMDB et son intégration avec GLPI

Définition

La **CMDB** (Configuration Management DataBase) est une base de données qui centralise et organise les informations relatives aux **éléments de configuration (CI – Configuration Items)** d'un système d'information.
Un **élément de configuration (CI)** peut être :

- un serveur physique ou virtuel,
- une application,
- un service métier (ex : messagerie, ERP),
- un équipement réseau (switch, routeur, firewall),
- un poste utilisateur ou une imprimante,
- un utilisateur ou un groupe.

But de la CMDB

- **Analyser l'impact d'une panne** : si un serveur tombe, savoir quels services et utilisateurs sont affectés.
- **Mieux gérer les changements** : comprendre les dépendances avant de mettre à jour ou remplacer un composant.
- **Assurer la traçabilité** : conserver l'historique des modifications sur les CI.
- **Optimiser la gestion des actifs IT (ITAM)**.

Liens entre les CI

La force de la CMDB réside dans la capacité à **modéliser les relations** :

- Service → Application → Serveur → Équipement réseau.
- Utilisateur → Poste de travail → Applications utilisées.
- Serveur → Dépendances avec d'autres serveurs (ex : base de données).

Ainsi, une panne d'un serveur de base de données permet immédiatement d'identifier les applications et utilisateurs impactés.

CMDB dans GLPI

GLPI intègre une **CMDB complète**, accessible via le module « Gestion des éléments de configuration ».

- Chaque matériel, logiciel, utilisateur est un CI.
- Les relations entre CI peuvent être définies (*ex. ce serveur héberge telle application, utilisée par tel service*).
- La CMDB est intégrée avec l'**inventaire automatique** (FusionInventory ou OCS Inventory).
- Elle alimente les processus ITIL : gestion des incidents, des problèmes, des changements.

Exemple concret

- Un serveur « `SRV-DB01` » héberge la base de données de l'application de facturation.
- Cette application est utilisée par le service Comptabilité.
- Si `SRV-DB01` tombe en panne :
  - la CMDB montre immédiatement que « Application Facturation » est impactée,
  - et donc que le service Comptabilité est bloqué.

Avantages pour l'entreprise

- Vision globale et centralisée du SI.
- Aide à la décision avant un changement.
- Réduction des risques et meilleure continuité de service.
- Support aux bonnes pratiques ITIL.