

Section 7 : Mise en production d'évolutions de l'infrastructure

7.1. Introduction à la mise en production

La mise en production désigne le **processus contrôlé qui permet d'introduire une évolution technique dans l'environnement opérationnel** de l'entreprise, sans compromettre la disponibilité, la performance ou la sécurité des systèmes.

Elle suit les étapes précédentes de conception et de test, et constitue un moment **crucial dans la vie d'un système d'information**.

Exemples d'évolutions :

- Migration d'un serveur
 - Déploiement d'une nouvelle application
 - Ajout d'un service cloud
 - Modification du schéma de réseau
 - Renouvellement d'un composant critique
-

7.2. Planification du changement (change management)

La mise en production s'inscrit dans un processus de **gestion des changements (ITIL)** :

1. **Demande de changement** : initiée par l'AIS, un chef de projet, ou une direction.
2. **Étude d'impact** : disponibilité, sécurité, performance, budget.
3. **Comité de validation** : acceptation du changement.
4. **Planification** : date, ressources, responsabilités, procédure.
5. **Communication** : aux équipes techniques, utilisateurs, support.

Outils :

- GLPI (module de gestion des changements)
 - ServiceNow, iTop, Jira
 - Documentation technique partagée (Wiki, GitLab)
-

7.3. Méthodes de déploiement

Méthode	Description	Usage
Déploiement direct	Tout ou rien	Petits changements
Déploiement progressif	Étapes successives	Réseaux, postes, utilisateurs
Déploiement parallèle	Ancienne et nouvelle version en parallèle	Migration de services critiques
Déploiement bleu/vert	Environnement en attente	Services web, cloud

7.4. Préparation technique à la mise en production

Avant toute mise en production, l'AIS prépare un **plan d'action détaillé** :

- Étapes de déploiement
- Procédures de retour arrière (rollback)
- Sauvegardes complètes
- Tests de validation
- Affectation des rôles
- Créneaux de bascule (nuit, week-end...)

Environnements requis :

- **Environnement de développement** (dev)
 - **Environnement de test/préproduction** (test)
 - **Environnement de production** (prod)
-

7.5. Tests de validation (VSR - Vérification de Service Rendu)

Une fois la mise en production effectuée, des **tests doivent valider la conformité de la solution** :

- Tests fonctionnels : le service fonctionne-t-il ?
- Tests de charge : performance sous contrainte ?
- Tests de sécurité : ports ouverts, accès interdits, logs ?
- Supervision : les métriques remontent-elles ?

Chaque test doit être documenté :

- Résultat
 - Date et heure
 - Nom du validateur
-

7.6. Documentation des évolutions

Une mise en production doit être **entièrement documentée**, pour assurer la traçabilité, la maintenance future et la sécurité :

- Fiche de changement (date, objet, responsable)
- Procédure de mise en œuvre (pas à pas)
- Capture d'écran, logs, configurations modifiées
- Procédure de rollback
- Journaux d'événements

- Mise à jour du référentiel de configuration (CMDB)
-

7.7. Communication et formation des utilisateurs

L'évolution d'infrastructure peut impacter les utilisateurs :

- Interruption temporaire
- Nouveaux usages, nouvelles interfaces
- Modifications d'authentification ou de politique

L'AIS participe à la **communication pédagogique** :

- Messages d'information en amont
 - Mise à disposition de guides utilisateurs
 - Assistance post-migration
 - Recueil de retours (satisfaction, bugs, besoins)
-

7.8. Retour d'expérience (RETEX) et amélioration continue

Le retour d'expérience post-mise en production permet de :

- Identifier les points forts et faiblesses
- Capitaliser les bonnes pratiques
- Alimenter la base de connaissance (Wiki, Git)
- Adapter les procédures futures

RETEX = étape indispensable dans la logique DevOps / ITIL

7.9. Intégration dans la politique de sécurité

Chaque évolution doit respecter :

- La **PSSI de l'organisation**
- Les **règles de contrôle d'accès**
- Le **chiffrement des données sensibles**
- La **journalisation** des événements
- Les **mesures anti-régression de sécurité**

Contrôles ANSSI :

- Test de sécurité après modification
- Vérification des droits
- Revue annuelle des configurations

7.10. Études de cas, projets et évaluations

Cas pratiques :

- Mise en production d'un nouveau serveur applicatif
- Migration d'un serveur de fichiers vers le cloud
- Déploiement d'une nouvelle politique GPO
- Ajout d'un VLAN sécurisé sur un réseau existant

Évaluation :

- QCM sur les procédures ITIL / MEP
- Étude de cas documentée
- Présentation orale du plan de changement