

Mis à jour le 29/01/2026

S'inscrire

Formation EPM Ivanti patching et conformité

2 jours (14 heures)

Présentation

Cette formation EPM Ivanti vous apprend à industrialiser le patching et à piloter la conformité sur un parc Windows, avec des résultats mesurables (réduction du risque, visibilité, audits). Vous travaillez sur des cas d'usage concrets : déploiement de correctifs, gestion des exceptions, et preuves de conformité.

Lors de cette formation, nous abordons la chaîne complète : inventaire, analyse de vulnérabilités, création de groupes cibles, planification, déploiement, contrôle post-installation et remédiation. L'objectif est de sécuriser les postes et serveurs tout en limitant l'impact utilisateur (fenêtres de maintenance, redémarrages, rollback).

L'approche est pratique : ateliers guidés, démos d'administration, exercices de troubleshooting et construction de tableaux de bord. Vous repartez avec des livrables réutilisables : modèles de politiques de patching, checklists de conformité, procédures d'exploitation et rapports type pour audit.

Objectifs

- Configurer l'inventaire et la collecte d'état de patches dans Ivanti EPM.
- Construire des campagnes de patching (ciblage, planification, redémarrages, maintenance).
- Automatiser la remédiation via tâches, scripts et règles de conformité.
- Analyser les échecs et dépanner les déploiements (agent, distribution, prérequis).
- Produire des rapports de conformité et des preuves d'audit exploitables.

Public visé

- Administrateurs systèmes / postes de travail
- Ingénieurs exploitation / support N2-N3
- Responsables sécurité / GRC en charge de la conformité
- Chefs de projet outillage ITSM / endpoint management

Pré-requis

- Administration Windows (services, registre, droits, logs)
- Notions de réseau (DNS, ports, proxy, segmentation)
- Compréhension des cycles de patching et des risques vulnérabilités
- Lecture de journaux et diagnostic de base

Pré-requis techniques

- PC avec 16 Go de RAM recommandés (8 Go minimum) et CPU 4 cœurs
- Windows 10/11 ou Windows Server (accès admin local)
- Accès à une console Ivanti EPM (environnement de test) et à un compte admin EPM
- Outils : PowerShell, navigateur moderne, accès réseau aux endpoints de lab

Programme de formation EPM Ivanti patching et conformité

[Jour 1 - Matin]

Fondamentaux Ivanti EPM et préparation du patch management

- Architecture EPM : Core Server, Agents, Console, rôles et flux réseau
- Inventaire matériel/logiciel : sources, fréquence, qualité des données et normalisation
- Pré-requis patching : fenêtres de maintenance, redémarrages, dépendances et contraintes métiers
- Bonnes pratiques de segmentation : groupes, requêtes, cibles pilotes et anneaux de déploiement
- Atelier pratique : Construire une segmentation (Pilote/Pré-prod/Prod) à partir de l'inventaire.

[Jour 1 - Après-midi]

Mise en œuvre du patching : contenu, déploiements et contrôle d'exécution

- Gestion du contenu patch : catalogues, synchronisation, approbation et exclusions
- Création de tâches de patch : ciblage, planification, pré/post-actions et redémarrage
- Stratégies de déploiement : progressive, deadlines, maintenance windows et gestion de la bande passante
- Suivi d'exécution : états, logs agent, erreurs fréquentes et remédiations
- Atelier pratique : Déployer un lot de correctifs sur un groupe pilote et analyser les retours d'exécution.

[Jour 2 - Matin]

Conformité et reporting : indicateurs, tableaux de bord et preuves d'audit

- Définir la conformité : niveaux de patch, SLA, exceptions et périmètres (serveurs/postes)
- Rapports EPM : modèles, filtres, planification et diffusion contrôlée
- KPIs opérationnels : taux de conformité, couverture, délai de remédiation et top vulnérabilités
- Traçabilité : historisation, preuves de déploiement, gestion des dérogations et justificatifs
- Atelier pratique : Produire un rapport de conformité mensuel avec exceptions documentées.

[Jour 2 - Après-midi]

Durcissement du processus : gouvernance, automatisation et gestion des incidents patch

- Gouvernance patch : RACI, cycles (hebdo/mensuel), communication et validation du changement
- Automatisation : anneaux, règles d'approbation, déploiements récurrents et contrôles prérequis
- Gestion des échecs : diagnostics (agent, contenu, WUA, prérequis), contournements et relance
- Amélioration continue : post-mortem, réduction du backlog, optimisation réseau et standardisation
- Atelier pratique : Mettre en place un runbook de remédiation et une routine d'automatisation de patching.

Sociétés concernées

Cette formation s'adresse à la fois aux particuliers ainsi qu'aux entreprises, petites ou grandes, souhaitant former ses équipes à une nouvelle technologie informatique avancée ou bien à acquérir des connaissances métiers spécifiques ou des méthodes modernes.

Positionnement à l'entrée en formation

Le positionnement à l'entrée en formation respecte les critères qualité Qualiopi. Dès son inscription définitive, l'apprenant reçoit un questionnaire d'auto-évaluation nous permettant d'apprécier son niveau estimé sur différents types de technologies, ses attentes et objectifs personnels quant à la formation à venir, dans les limites imposées par le format sélectionné. Ce questionnaire nous permet également d'anticiper certaines difficultés de connexion ou de sécurité interne en entreprise (intraentreprise ou classe virtuelle) qui pourraient être problématiques pour le suivi et le bon déroulement de la session de formation.

Méthodes pédagogiques

Stage Pratique : 60% Pratique, 40% Théorie. Support de la formation distribué au format numérique à tous les participants.

Organisation

Le cours alterne les apports théoriques du formateur soutenus par des exemples et des séances de réflexions, et de travail en groupe.

Validation

À la fin de la session, un questionnaire à choix multiples permet de vérifier l'acquisition correcte

des compétences.

Sanction

Une attestation sera remise à chaque stagiaire qui aura suivi la totalité de la formation.