AYI NEDJIMI Consultants

Just-In-Time Access : élévation de privilèges contrôlée

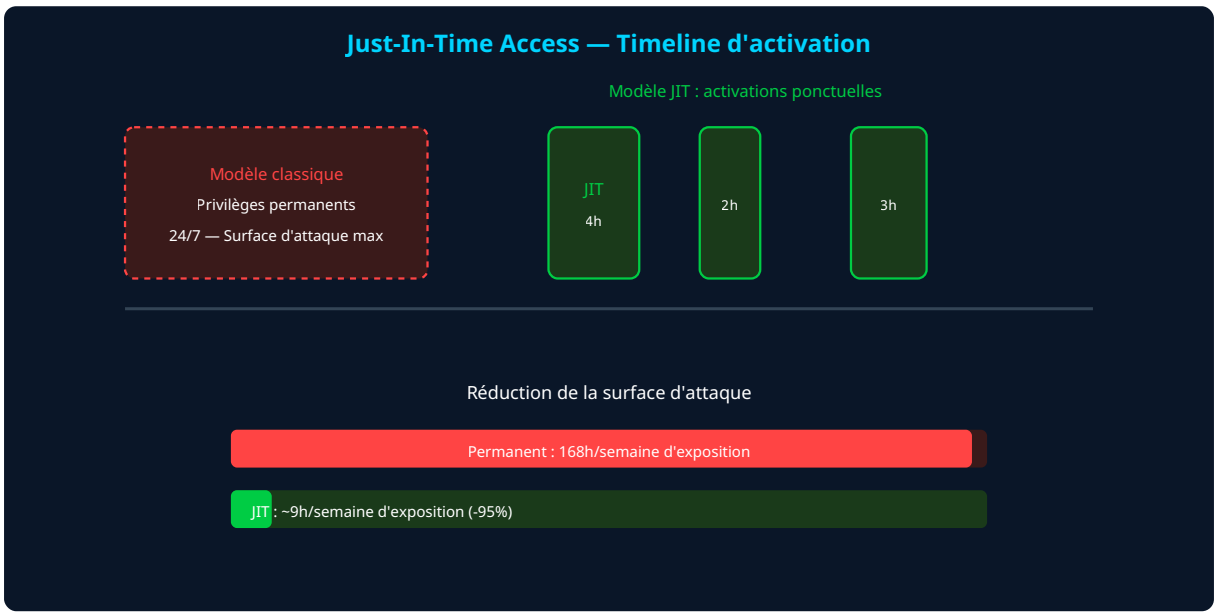
Catégorie : IAM et Gestion des Identités Lecture : 6 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Just-In-Time Access : déployez l'élévation de privilèges temporaire et contrôlée pour réduire votre surface d'attaque avec PIM, PAM et workflows.

Vos administrateurs ont-ils vraiment besoin de leurs privilèges 24 heures sur 24, 7 jours sur 7 ? La réponse est non. Un administrateur Exchange utilise ses droits d'administration quelques heures par semaine. Un DBA accède à la base de production pour des maintenances ponctuelles. Pourtant, dans la majorité des organisations, ces comptes disposent de privilèges permanents qui restent actifs en continu — y compris la nuit, le week-end et pendant les vacances. Le Just-In-Time Access (JIT) renverse cette logique en transformant les accès permanents en activations temporaires, contextuelles et traçables. Quand un administrateur a besoin de ses droits, il les active pour une durée définie avec justification et, selon le niveau de criticité, approbation d'un pair. Une fois la fenêtre expirée, les privilèges sont automatiquement révoqués. Ce guide détaille les architectures JIT, les outils disponibles, les workflows d'approbation et les métriques de succès. Vous découvrirez comment réduire votre surface d'attaque de manière drastique sans impacter la productivité des équipes techniques.

Points clés à retenir

- Le **JIT Access** réduit la fenêtre d'exposition des privilèges de 99% (de 24/7 à quelques heures par semaine)
- **PIM** (Entra ID) et les solutions **PAM** sont les deux vecteurs de déploiement JIT
- Chaque activation génère un audit trail complet : qui, quoi, quand, pourquoi, approuvé par qui
- Le workflow d'approbation doit être rapide (< 15 minutes) pour ne pas frustrer les équipes
- La combinaison JIT + session recording offre le meilleur compromis sécurité/opérationnel



Pourquoi les privilèges permanents sont un risque majeur

Un compte Domain Admin actif en permanence est une cible de choix. Si ce compte est compromis — par phishing, credential stuffing ou mouvement latéral — l'attaquant hérite immédiatement de tous les privilèges associés. Avec le JIT, ce même compte ne possède aucun privilège la plupart du temps. L'attaquant qui compromet un compte JIT obtient un accès standard, sans possibilité d'escalade immédiate. La fenêtre d'exploitation se réduit de 168 heures par semaine (accès permanent) à quelques heures réparties sur la semaine.

Les attaques ciblant Active Directory exploitent massivement les comptes à privilèges permanents. Kerberoasting, Golden Ticket, DCSync — toutes ces techniques nécessitent des privilèges élevés au moment de l'exécution. Si les comptes concernés sont en mode JIT et inactifs au moment de l'attaque, ces techniques échouent. Le graphe d'attaque BloodHound montre clairement la différence de surface d'attaque entre un environnement avec et sans JIT.

PIM dans Entra ID : le JIT natif Microsoft

Privileged Identity Management (PIM) est la solution JIT native d'Entra ID. PIM transforme les attributions de rôles permanentes (Global Admin, Exchange Admin, Security Admin) en attributions éligibles. Un administrateur éligible doit activer explicitement son rôle quand il en a besoin. L'activation requiert une justification textuelle, un MFA et, pour les rôles critiques, l'approbation d'un pair ou d'un manager.

La configuration recommandée : durée d'activation maximale de 8 heures pour les rôles standards, 4 heures pour Global Admin et Security Admin. Notification par email à chaque activation (au titulaire et au security team). Revue d'accès trimestrielle automatique via Access Reviews. PIM couvre les rôles Entra ID mais aussi les rôles Azure RBAC (Owner, Contributor sur les subscriptions). Pour le périmètre on-premise, le PAM prend le relais avec des mécanismes JIT équivalents.

JIT via les solutions PAM

Les solutions PAM comme **CyberArk**, **BeyondTrust** et **Delinea** implémentent le JIT différemment de PIM. Au lieu d'activer un rôle, l'administrateur demande l'accès à une ressource spécifique (serveur, base de données, console cloud). Le PAM vérifie la politique d'accès, déclenche le workflow d'approbation si nécessaire, puis injecte les credentials temporaires via le bastion. À l'expiration de la session, les credentials sont automatiquement changés.

L'avantage du PAM sur PIM pour le JIT : la granularité. PIM accorde un rôle entier (Exchange Admin = tous les droits Exchange). Le PAM peut accorder l'accès à un serveur spécifique pour une tâche spécifique avec des *commandes autorisées* restreintes. CyberArk Endpoint Privilege Manager va encore plus loin en permettant l'élévation de privilèges au niveau processus : l'utilisateur exécute une application spécifique avec des droits admin sans disposer d'un compte admin complet. Pour les secrets applicatifs et clés API, le JIT se traduit par des tokens à durée de vie courte (1 heure) plutôt que des credentials statiques.

Critère	PIM (Entra ID)	PAM (CyberArk/BeyondTrust)
Périmètre	Rôles Entra ID + Azure RBAC	Serveurs, BDD, applications, cloud
Granularité	Rôle complet	Ressource + commandes spécifiques
Approbation	Workflow natif Entra ID	Workflow PAM + ITSM intégré
Session recording	Non	Oui (vidéo + keystroke)
Coût additionnel	Inclus dans Entra ID P2	Licence PAM dédiée
Complexité	Faible	Moyenne à élevée

Concevoir le workflow d'approbation optimal

Le workflow d'approbation est le talon d'Achille du JIT. Trop lent, il frustre les équipes techniques et provoque des contournements. Trop permissif, il perd son intérêt sécuritaire. L'équilibre repose sur une classification des accès en trois niveaux. Les accès de **niveau 1** (faible risque, tâches récurrentes) s'activent avec justification seule, sans approbation — le contrôle se fait a posteriori via l'audit. Les accès de **niveau 2** (risque moyen) requièrent l'approbation d'un pair technique. Les accès de **niveau 3** (risque élevé, production, données sensibles) nécessitent l'approbation d'un manager et d'un membre de l'équipe sécurité.

Le SLA d'approbation cible : 5 minutes pour le niveau 2, 15 minutes pour le niveau 3. Pour atteindre ces SLA, configurez les notifications en temps réel (Teams, Slack, SMS) vers les approbateurs et mettez en place des approbateurs de backup en cas d'indisponibilité. Un SOC externalisé peut servir d'approbateur de dernier recours pour les accès en dehors des heures ouvrées, garantissant une couverture 24/7.

Métriques et reporting JIT

Le suivi de l'efficacité JIT repose sur cinq *KPIs* principaux. Le **taux de couverture JIT** mesure le pourcentage de comptes à privilèges gérés en mode JIT versus permanent — la cible est 95% minimum. La **durée moyenne d'activation** indique si les fenêtres sont calibrées correctement (trop long = sur-provisioning, trop court = réactivations fréquentes). Le **taux d'approbation** détecte les anomalies (un taux de refus > 10% signale un problème de process). Le nombre d'activations par utilisateur par semaine révèle les patterns d'usage. Le temps moyen d'approbation mesure l'impact sur la productivité.

Intégrez ces métriques dans un tableau de bord aligné sur le NIST Cybersecurity Framework. Présentez-les trimestriellement au COMEX pour démontrer la réduction de la surface d'attaque. Un reporting clair et visuel transforme le JIT d'une contrainte technique perçue en un avantage de sécurité valorisé par la direction.

Déploiement progressif du JIT

Le déploiement JIT suit une approche progressive en quatre étapes. Première étape : activez PIM pour les rôles Entra ID les plus sensibles (Global Admin, Security Admin, Exchange Admin) — c'est un quick win réalisable en une semaine. Deuxième étape : étendez PIM à tous les rôles d'administration Azure (2-3 semaines). Troisième étape : déployez le JIT PAM pour les accès serveurs et bases de données de production (4-8 semaines). Quatrième étape : intégrez le JIT dans les pipelines CI/CD et les accès cloud multi-tenant (4-6 semaines).

Chaque étape s'accompagne d'une communication aux équipes concernées, d'une phase de dry-run en mode audit-only et d'un ajustement des durées d'activation en fonction des retours terrain. La patience paie : un déploiement JIT progressif sur 4 mois a un taux de succès de 90%, contre 40% pour un déploiement big bang selon les données de CyberArk.

Questions fréquentes sur le Just-In-Time Access

Que se passe-t-il en cas d'urgence si l'approbateur n'est pas disponible ?

Trois mécanismes de secours existent. Les comptes break-glass (exclus du JIT) permettent un accès d'urgence immédiat avec alerting automatique. Les chaînes d'approbation multi-niveaux avec timeout automatique escaladent la demande au niveau supérieur après 15 minutes. L'auto-approbation conditionnelle peut être activée pour des scénarios d'urgence prédéfinis (incident P1 déclaré dans l'ITSM). Chaque utilisation de ces mécanismes de secours déclenche une revue post-incident obligatoire.

Comment les comptes de service fonctionnent-ils avec le JIT ?

Les comptes de service ne peuvent pas utiliser de workflow d'approbation interactif. Le JIT s'applique différemment : rotation automatique des credentials toutes les heures via le coffre-fort PAM, tokens à durée de vie courte (OAuth2 avec expiration de 1 heure) et accès réseau limité par IP source. Pour les batch jobs planifiés, le PAM accorde l'accès au compte de service uniquement pendant la fenêtre d'exécution programmée et le révoque après.

Le JIT ralentit-il les équipes techniques au quotidien ?

L'impact perçu est souvent surestimé. Les mesures terrain montrent que l'activation PIM prend en moyenne 45 secondes (justification + MFA). L'approbation de niveau 2 arrive en 3 minutes en moyenne. Sur une semaine type, un administrateur active ses privilèges 5 à 10 fois. Le temps total ajouté est de 10 à 20 minutes par semaine — un investissement dérisoire au regard du gain de sécurité. La clé : des workflows fluides et des approbateurs réactifs.

Sources et références : ANSSI · MITRE ATT&CK

Synthèse et prochaines actions

Le Just-In-Time Access est probablement le quick win à plus fort impact sécuritaire que vous pouvez déployer sur votre environnement. La réduction de 95% de la surface d'attaque des comptes à privilèges justifie à elle seule l'investissement. Commencez par PIM sur les rôles Entra ID critiques cette semaine, puis élargissez progressivement. Mesurez, ajustez, communiquez. Vos équipes techniques s'adapteront plus vite que vous ne le pensez — surtout quand elles réaliseront qu'elles n'ont plus besoin de mémoriser les mots de passe des comptes admin.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr