FLASHMODZ ENTERPRISE

Cabinet d’expertise IT — Charleroi · Belgique & international

FlashModz

Red Hat Enterprise Linux en entreprise

Guide RHEL / Entreprise

RHEL : modèle de souscription, Satellite, Insights, IdM, montée de version 8 > 9, alternatives (Rocky, Alma) et critères de choix. Le guide pragmatique pour PME et ETI tournant sur Linux.

Scannez pour acceder
a la version en ligne

contact@flashmodz.be | +32 471 87 87 07

https://flashmodz.be

FlashModz

L'essentiel en 5 minutes

RHEL est l'écosystème Linux entreprise de référence en Europe. Bien industrialisé (Satellite + Insights + Ansible), il devient un actif fiab

1

Le modèle de souscription RHEL est rentable

Une souscription n'est pas une licence : c'est un abonnement annuel qui couvre les binaires, les errata de sécurité, le support éditeur (heures ouvrées en Standard, 24/7 sur incidents critiques en Premium), Insights et un cycle de vie de 10 ans par version majeure. Prix catalogue public : de l'ordre de 800 $ par an et par serveur en Standard, remises au volume via revendeur. À mettre en face du coût d'un seul incident sérieux sur un serveur critique.

2

Rocky Linux et AlmaLinux sont de vraies alternatives

Depuis la fin de CentOS Linux 8 en 2021, Rocky Linux et AlmaLinux sont des clones binaires de RHEL, gratuits, communautaires, mais avec une qualité production. Pour les serveurs non critiques ou les contextes budget contraint, ce sont des choix totalement légitimes. Bascule possible vers RHEL plus tard.

3

Satellite + Insights pour les parcs > 25 serveurs

Satellite se licencie par nœud géré (add-on Smart Management), en sus de la souscription RHEL. Il centralise patches, content views et cycles Dev/Test/Prod. Insights, inclus dans la souscription, audite la conformité en continu. Le gain se mesure en heures d'admin récupérées chaque mois et en fenêtres de patching réellement tenues.

4

Ansible est le standard d'automatisation Linux

Ansible (Community gratuit, AAP commercial) automatise la configuration, le déploiement, le patching. Permet de passer d'une infrastructure artisanale à du Infrastructure as Code (IaC) reproductible. Le bus factor passe structurellement de 1 à N.

5

IdM ou intégration AD pour l'auth centralisée

Pour 10+ serveurs Linux, gérer les comptes locaux et les clés SSH manuellement est ingérable. IdM (FreeIPA, gratuit avec RHEL) ou intégration Active Directory via SSSD résout cette dette. Comptes utilisateurs centralisés, sudo policies, certificats.

Et maintenant ?

Les pages qui suivent détaillent chacun de ces points avec exemples, chiffres et actions concrètes.

Document conçu pour PME & ETI — Red Hat Enterprise Linux · Lecture : ~15-20 min · Édition 2026

Table des matières

Naviguez rapidement vers les sections qui vous concernent.

Le marché belge en chiffres

Chapitre 1

10 ans

de support par version majeure RHEL (5 ans Full Support + 5 ans Maintenance), extensible via ELS

Sources : textes officiels (NIS2, RGPD, DORA) et publications des éditeurs cités

~3 ans

entre deux versions majeures : RHEL 8 (2019), RHEL 9 (2022), RHEL 10 (2025)

30 juin 2024

fin de maintenance de RHEL 7 : sans add-on ELS, plus aucun correctif de sécurité

16 systèmes

couverts gratuitement par la Developer Subscription Red Hat (usage individuel, labs)

Contexte & enjeux

Linux fait tourner l'essentiel des charges serveur en entreprise : web, bases de données, applications métier, conteneurs, virtualisation. Mais "Linux" recouvre des réalités très différentes : Ubuntu Server, Debian, RHEL, SUSE, Rocky, Alma, Oracle Linux. Choisir une distribution, c'est surtout choisir un cycle de vie, un modèle de support et un outillage d'exploitation. C'est là que les écarts se creusent.

Red Hat Enterprise Linux repose sur un modèle de souscription, pas de licence : un abonnement annuel qui donne accès aux binaires, aux errata de sécurité, au support éditeur et aux outils. Chaque version majeure est maintenue 10 ans (5 ans de Full Support, 5 ans de Maintenance), extensible via l'add-on ELS. SELinux est activé par défaut et confine les processus même en cas de compromission. L'écosystème couvre la gestion de parc (Satellite), l'analyse de conformité (Insights), l'identité (IdM) et l'automatisation (Ansible). RHEL est certifié pour SAP et Oracle, et supporté chez AWS, Azure et Google Cloud.

Le débat "RHEL vs Rocky/Alma vs Ubuntu" est légitime. **Rocky Linux** et **AlmaLinux**, nés après l'arrêt de CentOS Linux 8 fin 2021, sont compatibles binaires avec RHEL et gratuits. Pour des serveurs non critiques ou un budget serré, ce sont des choix sérieux, avec une bascule possible vers RHEL plus tard (l'outil Convert2RHEL existe pour ça). Ubuntu Server reste pertinent en environnement cloud-native et DevOps. **SUSE** garde ses places fortes, SAP en tête.

Pour une PME industrielle wallonne typique (10-50 serveurs Linux), la vraie question n'est pas "RHEL ou pas". C'est : comment industrialiser votre parc Linux pour qu'il devienne un actif fiable plutôt qu'un patchwork artisanal. Ce guide donne les leviers concrets : choix de distribution, souscriptions, Satellite, Insights, IdM, Ansible, et l'articulation avec NIS2.

> *"Linux entreprise sans Satellite et sans Ansible, c'est du sysadmin artisanal. RHEL bien industrialisé devient un actif silencieux qui ne réveille personne la nuit."*
>
> — Jérémy Manet, FlashModz Enterprise

Pourquoi Linux entreprise mérite RHEL (ou un clone)

Chapitre 2

Les pièges du Linux "gratuit" en production critique.

Vos serveurs Linux sont en versions disparates

Sans gestion centralisée, votre parc Linux dérive : certains servers en RHEL 7 (fin de support juin 2024), d'autres en RHEL 8, d'autres en Rocky 9, quelques CentOS 7 oubliés. Conséquences : versions de packages incohérentes, scripts incompatibles, sécurité hétérogène. Satellite résout ça en pilotant le parc complet.

Les patches sécurité sont irréguliers

Sans Satellite ou équivalent, les patches sont appliqués à la main par admin ou via des scripts maison. Résultat : certains servers sont à jour, d'autres ont 6 mois de retard. Une CVE critique exploitée comme Log4Shell ou Spring4Shell devient impossible à patcher en urgence sur 50 serveurs disparates.

Le bus factor sur votre Linux est de 1

Combien de personnes savent comment vos serveurs Linux ont été configurés ? Souvent une seule. Quand cette personne part, est malade ou en vacances : panique. La documentation est absente ou obsolète, les modifications sont dans la tête de l'admin, les scripts de configuration sont dispersés. Ansible + IaC résout ça structurellement.

L'authentification Linux est un patchwork

Comment vos utilisateurs se connectent aux serveurs Linux ? Mot de passe local sur chaque server ? Clés SSH copiées partout ? Active Directory via SSSD mal configuré ? Sans IdM ou intégration AD propre, c'est un cauchemar de gouvernance. IdM (FreeIPA) ou une intégration AD via SSSD bien faite règle l'essentiel du problème.

Vous payez RHEL mais n'utilisez pas Insights/Ansible

Beaucoup de PME ont des souscriptions RHEL mais n'activent jamais Insights (gratuit, inclus) ni n'utilisent Ansible (Community gratuit, AAP en souscription). Vous payez la Ferrari et vous restez sur l'autoroute en 50. Insights donne en 1 clic la conformité CIS, les CVE actives, les recommandations de tuning.

Migration RHEL 7 > 8 > 9 procrastinée

RHEL 7 a atteint sa fin de maintenance le 30 juin 2024. Sans add-on ELS payant, plus aucun correctif, même pour les CVE critiques. Beaucoup de PME ont encore des serveurs RHEL 7 en production en 2026. La migration 7 > 8 > 9 est un projet non trivial mais inévitable. Plus on attend, plus c'est cher.

Mythes vs Réalité

Chapitre 3

Six idées reçues qui empêchent d'agir — et ce qu'en disent les chiffres.

01

ON ENTEND SOUVENT

Linux est gratuit, RHEL c'est du Linux payant pour rien.

EN RÉALITÉ — *RHEL = support et écosystème pro*

Le kernel Linux est gratuit. Le support, les errata sécurité, les outils (Satellite, Insights, IdM, AAP), les certifications, c'est ce que vous payez avec RHEL. Pour un serveur critique, ce n'est pas un coût mais une assurance. Ubuntu et Rocky/Alma fonctionnent aussi mais avec un autre modèle de support.

02

ON ENTEND SOUVENT

CentOS Linux n'existe plus, donc l'écosystème RHEL est foutu.

EN RÉALITÉ — *Rocky + AlmaLinux remplacent CentOS*

CentOS Linux 8 a effectivement pris fin en 2021, mais Rocky Linux et AlmaLinux ont pris le relais comme clones gratuits de RHEL. CentOS Stream existe toujours (en amont de RHEL, version "rolling"). L'écosystème RHEL est plus dynamique que jamais avec ces 3-4 distributions binairement compatibles.

03

ON ENTEND SOUVENT

On utilise Ubuntu Server, pourquoi RHEL ?

EN RÉALITÉ — *Ubuntu vs RHEL = choix par contexte*

Ubuntu est excellent, particulièrement en cloud-native et DevOps moderne. RHEL est plus mature sur le support long terme (10 ans vs 5 ans Ubuntu LTS), les certifications applicatives (SAP, Oracle), et l'écosystème entreprise (Satellite, AAP). Le bon choix dépend de vos workloads et de votre culture tech.

04

ON ENTEND SOUVENT

Red Hat Satellite coûte une fortune, ce n'est pas pour une PME.

EN RÉALITÉ

Satellite pertinent dès ~25 serveurs

Satellite se paie par nœud géré, en sus de la souscription RHEL. Mettez ce coût en face du temps réellement passé en patching manuel sur 25 serveurs et plus : la comparaison tourne vite à l'avantage de Satellite. En dessous de ce seuil, Ansible seul suffit souvent.

05

ON ENTEND SOUVENT

On préfère rester sur RHEL 7 plutôt que de risquer une migration.

EN RÉALITÉ

EOL = risque qui ne se résorbe pas seul

RHEL 7 a atteint sa fin de maintenance en juin 2024 : sans add-on ELS, les CVE ne sont plus corrigées. Rester, c'est accepter un risque sécurité qui grandit chaque mois. La migration (7 > 8 puis 8 > 9) est non triviale mais maîtrisable avec Leapp, Ansible et un plan structuré. Mieux vaut un projet planifié qu'un incident d'urgence.

06

ON ENTEND SOUVENT

Insights envoie les données vers Red Hat, ce n'est pas RGPD.

EN RÉALITÉ

Insights = télémétrie système, pas data

Insights envoie des métadonnées système (versions de packages, configurations) vers le cloud Red Hat, pas vos données métier. Red Hat documente publiquement ce qui est collecté et propose l'obfuscation des hostnames et adresses IP. À valider avec votre DPO, mais le contenu applicatif ne quitte pas vos serveurs.

Cas concrets en Belgique

Chapitre 4

Trois scénarios types, inspirés de situations réelles et anonymisés.

PME industrielle wallonne (45 serveurs Linux)

Contexte: Mix RHEL 7 (en EOL), RHEL 8, et CentOS 7 oublié sur 3 serveurs. Pas de Satellite. Patches manuels. Bus factor de 1 (le sysadmin senior).

Impact: Plan de modernisation 12 mois : (1) inventaire et cartographie, (2) déploiement Satellite + Ansible AAP, (3) migration progressive RHEL 7 > 9 (15 serveurs), (4) bascule des CentOS 7 vers Rocky 9 (3 serveurs non critiques), (5) mise en place IdM pour l'auth centralisée. Résultat : 100% conforme, patches automatisés, bus factor remonté à 3.

Leçon: Une migration RHEL 7 > 9 est un projet de 12 mois pour 50 serveurs, mais elle se rentabilise vite : moins d'incidents, beaucoup moins d'heures perdues en patching manuel, et une conformité NIS2 nettement plus simple à démontrer.

Banque privée bruxelloise (28 serveurs Linux)

Contexte: Tous en RHEL 8/9. Souscriptions Standard et Premium selon criticité. Pas de Satellite. Pas d'usage d'Insights ou Ansible AAP. Déploiements manuels, parfois ad-hoc.

Impact: Audit DORA révèle des écarts : pas de gestion automatisée des patches, pas d'inventaire formel, pas d'IaC. Mise en place Satellite + Insights + AAP en 4 mois. Conformité DORA art. 6 (gestion risques TIC) et art. 9 (protection) considérablement renforcée.

Leçon: Pour un secteur régulé (DORA, NIS2 essentiel), l'industrialisation Linux n'est pas optionnelle. Satellite + Insights + Ansible est le triptyque attendu par les régulateurs.

PME tech namuroise (12 serveurs Linux)

Contexte: Stack tech moderne : conteneurs Docker, Kubernetes en cours d'évaluation. RHEL 9 sur 4 serveurs critiques (BDD, app), Ubuntu Server sur 8 serveurs (web, conteneurs). Pas de souscription Red Hat.

Impact: Cadrage : maintien de la stack mixte. Pas besoin de Satellite à 12 serveurs, mais Ansible (Community) en place pour automatiser. Souscriptions RHEL ajoutées sur les 4 serveurs critiques pour le support éditeur et l'accès Insights. Coût annuel maîtrisé, couverture réelle le jour où un incident sérieux tombe.

Leçon: À 12 serveurs, on peut être plus pragmatique : Ansible Community + souscriptions RHEL ciblées + Insights. Satellite a son sens à 25-30+ serveurs RHEL homogènes.

Avant / Après — la différence concrète

Chapitre 5

Ce qui change quand on passe d'une posture artisanale à une posture maîtrisée.

	Parc Linux artisanal	Parc RHEL industrialisé
01	**INVENTAIRE SERVEURS**	
	Excel partiel ou inexistant. Bus factor de 1.	Satellite : inventaire temps réel, conformité, life-cycle.
02	**PATCHES SÉCURITÉ**	
	Manuels, irréguliers, certains servers en retard de 6 mois.	Automatisés via Satellite, fenêtres planifiées, conformité tracée.
03	**CONFORMITÉ (CIS, NIS2)**	
	Inconnue, gérée en panique lors d'un audit.	Insights + CIS Benchmark : tableau de bord temps réel, écarts identifiés.
04	**AUTHENTIFICATION**	
	Comptes locaux, clés SSH copiées partout.	IdM ou AD : comptes centralisés, sudo policies, certificats.
05	**CONFIGURATIONS**	
	Scripts shell dispersés, modifications manuelles non tracées.	Ansible IaC : reproductible, versionné, peer-reviewable.
06	**MIGRATION DE VERSION**	
	Évitée. Serveurs en EOL en production.	Pilotée via Leapp + Ansible. Cycle structuré.
07	**BUS FACTOR**	
	1. Si l'admin senior part, panique.	3-5+. Documentation, IaC, knowledge partagée.

08 SUPPORT EN CAS D'INCIDENT

- Mailing-list, Stack Overflow, communauté.
- Support Red Hat : heures ouvrées (Standard) ou 24/7 sur incidents critiques (Premium).

Auto-évaluation de maturité

Chapitre 6

Faites le point en 5 minutes : où en êtes-vous vraiment ?

Pour chaque question, cochez la case qui correspond le mieux à votre situation actuelle.

SITUATION	NON	PARTIEL	OUI
1. Tous les serveurs Linux sont inventoriés (Satellite ou outil équivalent).	☐	☐	☐
2. Aucun serveur n'est en version EOL (RHEL 7 par exemple).	☐	☐	☐
3. Les patches sécurité sont déployés sous 7-14 jours après publication CVE critique.	☐	☐	☐
4. Insights est activé et la conformité CIS RHEL Benchmark est > 70%.	☐	☐	☐
5. L'authentification est centralisée via IdM ou Active Directory (pas de comptes locaux).	☐	☐	☐
6. Les configurations sont versionnées dans un repo Git et déployées via Ansible.	☐	☐	☐
7. Aucun serveur en production n'est inconnu, non documenté ou non monitoré.	☐	☐	☐
8. Une procédure formelle de gestion des changements existe (Satellite + Ansible + ticketing).	☐	☐	☐
9. Le bus factor sur Linux est de 3 ou plus (knowledge partagée, IaC, documentation).	☐	☐	☐
10. Les souscriptions Red Hat sont alignées avec le niveau de criticité de chaque serveur.	☐	☐	☐
11. Un plan de continuité prévoit la restauration de chaque serveur critique en <4h.	☐	☐	☐
12. Une revue annuelle évalue la maturité Linux et identifie les axes d'amélioration.	☐	☐	☐

SCORING : Non = 0 pt • Partiel = 1 pt • Oui = 2 pts

< 40% : Critique • 40-70% : À renforcer • > 70% : Bonne posture

Ce qu'on met en place avec vous

Chapitre 7

Du choix de souscription à l'industrialisation Satellite + Ansible.

Audit parc Linux & cartographie

Inventaire complet de vos serveurs Linux : distribution, version, criticité, dépendances applicatives, statut souscription. Identification des risques (EOL, CVE, configurations dérivées). Livrable : rapport et plan de modernisation. 5 jours.

Cadrage souscriptions Red Hat

Choix entre RHEL Standard, Premium, et alternatives (Rocky/Alma) selon vos besoins. Optimisation du nombre de souscriptions, négociation avec votre revendeur Red Hat. Inclut une matrice de décision par serveur.

Déploiement Satellite (gestion centralisée)

Installation et configuration Red Hat Satellite : intégration souscriptions, content views, lifecycle environments (Dev/Test/Prod), automation patches, déploiement de configurations. Pour 25+ serveurs RHEL.

Activation Insights & conformité CIS

Activation Insights sur le parc, configuration des règles CIS RHEL Benchmark, mise en place du tableau de bord conformité. Plan de remédiation des écarts. Inclut le hardening des serveurs critiques.

Migration RHEL 7/8 > RHEL 9

Migration des serveurs depuis RHEL 7 (EOL) ou RHEL 8 vers RHEL 9. Méthodologie : audit applicatif, environnement de test, validation, bascule par lots. Outillage : Leapp (upgrade in-place), Satellite (provisioning), Ansible (configuration).

Mise en place IdM (authentification centralisée)

Déploiement Red Hat IdM (FreeIPA) pour centraliser l'authentification Linux : comptes utilisateurs, certificats, politiques sudo, intégration AD optionnelle. Élimine les comptes locaux et les clés SSH dispersées.

Industrialisation Ansible (AAP ou Community)

Mise en place d'Ansible Automation Platform (AAP, version commerciale) ou Ansible Community : repos Git, playbooks de référence, rôles communs, exécution centralisée. Transition de scripts shell vers IaC structuré.

Run & maintien (option mensuelle)

Revue mensuelle Satellite + Insights, gestion des patches critiques, ajustement des configurations, accompagnement migrations. Forfait 2-5 jours/mois selon parc.

Notre façon de travailler

Une méthode en 4 étapes, progressive, pensée pour votre réalité. Pas de slides : des livrables concrets à chaque étape.

1

VOIR CLAIR

AUDIT

On commence par comprendre votre contexte : cartographie de l'existant, entretiens avec les équipes, identification des vrais risques. Pas de diagnostic à distance, pas d'hypothèses. On part de ce qui existe chez vous.

2

PRIORISER ENSEMBLE

PLAN

Qu'est-ce qui est urgent, qu'est-ce qui peut attendre ? On construit le plan avec vous, pas à votre place. Chaque action est pondérée par son impact, son effort et votre budget. Vous gardez la main sur les décisions.

3

STABILISER

ACTION

On corrige, on durcit, on protège. Des actions concrètes et mesurables, livrées par jalons. À chaque étape, vous validez avant qu'on avance. Pas de surprise, pas de dérive budgétaire.

4

TRANSMETTRE

AUTONOMIE

On documente tout ce qu'on fait, on forme vos équipes, on vous laisse les clés. Notre succès se mesure à votre capacité à continuer sans nous. Pas de dépendance, du transfert de compétences.

Feuille de route en phases

Chapitre 8

Un chemin balisé, du diagnostic à la maturité — étape par étape.

1	2	3	4	5
SEMAINE 1-2	SEMAINE 2-3	SEMAINE 3-10	MOIS 3-12	CONTINU
Audit	**Souscriptions**	**Industrialisation**	**Migration**	**Maintien**
• Inventaire parc • Versions + EOL • Cartographie criticité • Plan modernisation	• Optimisation contrats • Identification serveurs critiques • Activation Insights • Audit hardening	• Déploiement Satellite • Setup IdM • Repo Ansible • Playbooks de référence	• RHEL 7 > 9 par lots • Validation applicative • Bascule progressive • Décommissionnement	• Patches automatisés • Audit conformité • Mise à niveau continue • Documentation

Conseil méthodo

Chaque phase est un livrable autonome. Vous pouvez vous arrêter à n'importe quelle étape ou ralentir le rythme selon votre budget et votre charge interne. L'important n'est pas la vitesse — c'est de ne pas reculer.

Articulation RHEL / NIS2 / ISO 27001

Chapitre 9

Comment un parc RHEL bien géré sert directement votre conformité.

Patchs et conformité

NIS2 art. 21

NIS2 exige des mesures techniques : gestion des vulnérabilités, hardening des systèmes, contrôle des accès. Satellite + Insights répondent à ces 3 points pour le périmètre Linux.

BÉNÉFICE CACHÉ :

Lors d'un audit NIS2, démontrer un parc piloté par Satellite avec un tableau de bord Insights propre rassure immédiatement les inspecteurs.

Hardening et configuration sécurité

ISO 27001 A.8

Annex A d'ISO 27001:2022 (A.8.8 vulnérabilités, A.8.9 configurations sécurisées, A.8.32 changements) est directement servie par CIS RHEL Benchmark + Satellite + Ansible IaC.

BÉNÉFICE CACHÉ :

Auditeurs ISO connaissent le triptyque RHEL : Satellite (gestion), Insights (conformité), Ansible (configuration). Argumentaire facile à valider.

Gestion risques TIC secteur financier

DORA art. 6-7

Pour les acteurs financiers, DORA exige une cartographie des assets, une gestion des vulnérabilités prouvée, et une auditabilité des changements. Le triptyque RHEL + IaC + IdM répond aux 3 points.

BÉNÉFICE CACHÉ :

Les acteurs financiers belges qui ont industrialisé leur Linux passent les inspections BNB/FSMA sans difficulté sur le périmètre infra.

Référentiel gratuit reconnu

CIS RHEL Benchmark

Le CIS Red Hat Enterprise Linux Benchmark détaille plusieurs centaines de contrôles de durcissement (Niveau 1 essentiel, Niveau 2 avancé), mis à jour régulièrement. Disponible en rôles Ansible prêts à appliquer.

BÉNÉFICE CACHÉ :

Aligner votre parc RHEL sur CIS Niveau 1 constitue un socle de durcissement solide, reconnu par tous les auditeurs et inspecteurs cyber.

Checklist détachable — vos actions prioritaires

Imprimez cette page, cochez au fur et à mesure. Les colonnes EFFORT et IMPACT vous aident à séquencer.

	EFFORT	IMPACT	DÉLAI
☐ Inventaire complet du parc Linux : distributions, versions, criticité.	●●○○○	●●●●●	2 semaines
☐ Identifier et planifier la migration des serveurs en EOL (RHEL 7).	●●●○○	●●●●●	4 semaines
☐ Activer Insights sur tous les serveurs RHEL.	●○○○○	●●●●●	2 semaines
☐ Optimiser les souscriptions Red Hat (Standard vs Premium par criticité).	●●○○○	●●●○○	4 semaines
☐ Déployer Satellite si parc > 25 serveurs.	●●●●●	●●●●●	8 semaines
☐ Démarrer un repo Ansible avec playbooks de référence.	●●●○○	●●●●●	6 semaines
☐ Mettre en place IdM ou intégration AD propre via SSSD.	●●●●○	●●●●○	8 semaines
☐ Appliquer le CIS RHEL Benchmark Niveau 1 via Ansible.	●●●○○	●●●●●	8 semaines
☐ Migrer les serveurs RHEL 7 vers RHEL 9 (par lots).	●●●●●	●●●●●	6 mois
☐ Documenter chaque serveur (finalité, sauvegarde, monitoring, recovery).	●●○○○	●●●●○	8 semaines
☐ Procédure formelle de gestion des patches (pilote, prod, fenêtres).	●●○○○	●●●●○	6 semaines

		EFFORT	IMPACT	DÉLAI
☐	Tests de restauration semestriels, documentation à jour.	●●●○○	●●●●○	12 semaines

CONSEIL : Commencez par les actions à fort impact ET faible effort (les "quick wins").

Si vous bloquez sur une action, contactez-nous : on vous oriente gratuitement.

Questions fréquentes

Chapitre 10

Les questions que nos clients posent le plus souvent — et nos réponses sans détour.

Q1. Faut-il choisir RHEL ou Rocky/Alma ?

RHEL si : (1) support 24/7 critique, (2) certifications applicatives obligatoires (SAP, Oracle), (3) secteur régulé (banque, santé). Rocky/Alma si : (1) budget contraint, (2) workloads non critiques, (3) culture autonome. Mix possible : RHEL sur les 30% serveurs critiques, Rocky/Alma sur les 70% restants. Compatibilité binaire totale entre les deux.

Q2. Combien coûte une souscription RHEL ?

Prix catalogue public : de l'ordre de 800 $/an pour RHEL Server Standard (support en heures ouvrées) et 1 300 $/an en Premium (24/7 sur incidents critiques), par paire de sockets. L'add-on Smart Management, requis pour Satellite, s'ajoute par nœud géré. Au volume, remises via votre revendeur Red Hat. À noter : la Developer Subscription gratuite couvre jusqu'à 16 systèmes pour un usage individuel, pratique pour les labs.

Q3. Satellite ou Ansible : par quoi commencer ?

Si parc < 25 serveurs : Ansible suffit largement. Si parc 25-100 serveurs : Satellite + Ansible (Satellite gère le content/patches, Ansible gère les configurations). Si parc > 100 serveurs : Satellite + AAP (Ansible Automation Platform) pour orchestration centralisée. Insights est gratuit dans tous les cas, à activer en premier.

Q4. Comment migrer RHEL 7 > 9 ?

Outil : Leapp (in-place upgrade) supporte 7 > 8 et 8 > 9. Migration directe 7 > 9 nécessite 7 > 8 > 9. Approche : (1) clone du serveur en environnement test, (2) Leapp avec validation applicative, (3) si OK, bascule production. Alternatif : nouveau serveur RHEL 9 + migration applicative. Effort : 2-5 jours par serveur selon complexité applicative.

Q5. Linux + Active Directory : comment faire ?

Trois options : (1) Realmd + SSSD (intégration directe AD, simple), (2) IdM trust avec AD (plus robuste, IdM gère le Linux, trust avec AD), (3) Winbind (legacy, à éviter). Recommandation 2026 : Realmd + SSSD pour < 30 serveurs, IdM avec trust AD pour > 30 serveurs ou exigences fortes (sudo policies, certificats).

Q6. Quel rôle pour Ansible Tower / AAP ?

Ansible AAP (Ansible Automation Platform) est la version commerciale d'Ansible : interface web, RBAC, scheduling, audit logs, exécution centralisée. Pertinent à partir de 30+ serveurs ou quand plusieurs admins partagent les playbooks. Pour 5-15 serveurs et 1 admin : Ansible Community en CLI suffit largement.

Q7. OpenShift vs Kubernetes "vanilla", quelle différence ?

OpenShift est la distribution Kubernetes de Red Hat : support, sécurité durcie, GUI, CI/CD intégré, opérateurs nombreux. Kubernetes vanilla : open source pur, plus flexible mais demande plus d'expertise. Pour une PME : OpenShift si secteur régulé ou pas de Kubernetes expert en interne. Kubernetes vanilla (ou managé : EKS, AKS, GKE) si culture DevOps mature.

Q8. Faut-il désactiver SELinux ?

Non. C'est pourtant le premier réflexe de beaucoup d'équipes dès qu'une application refuse de démarrer. SELinux est un contrôle d'accès obligatoire intégré au noyau : il confine chaque processus et limite les dégâts d'une compromission. Le bon réflexe : passer temporairement en mode permissif pour diagnostiquer (les refus sont journalisés sans bloquer), corriger les contextes ou les booléens concernés, puis repasser en enforcing. Un parc RHEL avec SELinux désactivé partout est un signal d'alarme en audit.

Q9. Faut-il auditer son parc Linux annuellement ?

Oui, minimum. Audit recommandé annuellement : inventaire, versions, EOL, conformité CIS, hardening, gestion des accès. Audit blanc CIS RHEL Benchmark : 1-2 jours de consultant. Audit complet (incluant Ansible code review, IdM, sauvegardes) : 4-7 jours. Investissement raisonnable comparé au coût d'un incident production.

Glossaire

Chapitre 11

Tous les termes techniques de ce guide, expliqués en français clair.

802.1X

Standard IEEE d'authentification à l'accès réseau, filaire ou Wi-Fi. Chaque utilisateur ou machine s'authentifie auprès d'un serveur RADIUS avant d'obtenir un port ou un SSID. Base du Wi-Fi WPA-Enterprise.

Ansible

Outil d'automatisation IT par Red Hat. Configuration, déploiement et orchestration en playbooks YAML, sans agent. Standard de fait pour automatiser RHEL.

Auto VPN

Technologie Meraki MX qui établit automatiquement des tunnels VPN entre sites avec un clic. Simplifie radicalement le SD-WAN multi-sites.

DMZ

DeMilitarized Zone. Zone réseau intermédiaire entre Internet et le LAN, hébergeant les services exposés (web, mail). Réduit la surface d'attaque sur le LAN.

DPI

Deep Packet Inspection. Analyse du contenu des paquets réseau (pas juste les headers) pour identifier applications, malware, contenus inappropriés.

IdM (Identity Management)

Annuaire d'identités open source intégré à RHEL (basé sur FreeIPA). Gestion centralisée des comptes, certificats, politiques sudo. Alternative AD pour les flottes Linux.

Insights

Service Red Hat (cloud) d'analyse continue de la conformité, sécurité et performance de votre parc RHEL. Recommandations automatisées.

IPS/IDS

Intrusion Prevention/Detection System. Détection (IDS) ou blocage (IPS) en ligne d'attaques connues sur le trafic réseau. Souvent intégré dans firewalls modernes.

Meraki Dashboard

Console cloud Cisco Meraki pour piloter switches (MS), security appliances (MX), AP (MR), caméras (MV). Interface unifiée, configuration centralisée, multi-sites.

NSG / ACL

Network Security Group / Access Control List. Règles de filtrage trafic (source/destination/port/protocole). Pierre de base de toute segmentation réseau.

OpenShift

Plateforme Kubernetes entreprise de Red Hat. Conteneurisation, orchestration, CI/CD, supervision intégrés. Disponible on-prem, cloud, hybride.

PoE / PoE+

Power over Ethernet. Alimentation des AP, caméras, téléphones via le câble réseau. PoE (15W), PoE+ (30W), PoE++ (60-90W). Indispensable en infrastructure pro.

QoS

Quality of Service. Priorisation du trafic réseau (voix > vidéo > data > web) pour garantir l'expérience des apps temps réel sur des liens partagés.

RHEL

Red Hat Enterprise Linux. Distribution Linux entreprise de référence, modèle de souscription avec support 10 ans par version majeure, écosystème complet (Satellite, Insights, IdM, OpenShift).

Rocky Linux / AlmaLinux

Distributions communautaires basées sur RHEL, gratuites, créées après la fin de CentOS Linux 8 en 2021. Compatibilité binaire avec RHEL.

Satellite

Plateforme Red Hat de gestion centralisée de parcs RHEL : patches, déploiements, configurations, conformité, life-cycle. Équivalent Microsoft SCCM pour Linux.

SD-WAN

Software-Defined WAN. Pilotage centralisé du WAN multi-sites avec choix dynamique de chemin (MPLS, fibre, 4G/5G) selon la qualité et l'application.

SELinux

Security-Enhanced Linux. Contrôle d'accès obligatoire intégré au noyau, activé par défaut sur RHEL. Confine chaque processus à ce qu'il a le droit de faire, même si le service est compromis.

SNMP

Simple Network Management Protocol. Standard de supervision des équipements réseau (routeurs, switches, AP). v3 chiffrée recommandée.

UDM Pro

UniFi Dream Machine Pro. Appareil tout-en-un Ubiquiti : router/firewall + contrôleur UniFi + IDS/IPS + VPN. Recommandé pour PME 10-100 utilisateurs.

UniFi OS

OS Ubiquiti pour les contrôleurs UniFi (UDM, Cloud Key) qui héberge les apps UniFi Network, Protect (caméras), Talk (téléphonie), Access (contrôle d'accès).

VLAN

Virtual LAN. Découpage logique d'un réseau physique en plusieurs réseaux isolés (par tag 802.1Q). Permet d'isoler trafic voix/data/IoT/invités sans multiplier les câbles.

Wi-Fi 6 / 6E / 7

Normes Wi-Fi 802.11ax (Wi-Fi 6, 2019), 802.11ax 6GHz (Wi-Fi 6E, 2021), 802.11be (Wi-Fi 7, 2024). Wi-Fi 6E ouvre la bande 6 GHz, Wi-Fi 7 introduit MLO et 320 MHz.

Zero Trust Network

Modèle où aucune connexion n'est implicitement de confiance, même au sein du réseau interne. Vérification continue, micro-segmentation, accès minimal.

Ressources externes

Chapitre 12

Sites officiels, outils gratuits et lectures recommandées pour aller plus loin.

CIS Benchmarks

cisecurity.org/benchmarks

Référentiels gratuits de durcissement pour Cisco IOS, Juniper, RHEL, Ubuntu, Windows, etc. Versions niveau 1 (essentiel) et niveau 2 (avancé).

Red Hat Customer Portal

access.redhat.com

Portail Red Hat : documentation, knowledge base, errata sécurité, support. Accès complet avec souscription RHEL.

Ubiquiti Help Center

help.ui.com

Documentation officielle UniFi : guides d'installation, configurations type, scripts. Communauté très active sur le forum.

Cisco Meraki Documentation

documentation.meraki.com

Documentation officielle Meraki : architecture, déploiements, intégrations. Tutoriels vidéo, best practices, designs de référence.

NIST SP 800-115

csrc.nist.gov/publications/detail/sp/800-115/final

Guide NIST de tests sécurité réseau. Référentiel public pour les pentests et audits réseau.

CCB / CERT.be

ccb.belgium.be

Recommandations CCB sur la sécurité réseau, segmentation, gestion des accès. Alertes CERT.be sur les CVE actives.

Wireshark

wireshark.org

Analyseur réseau de référence, gratuit, open source. Pour diagnostiquer, dépanner, analyser le trafic en profondeur.

Ansible Galaxy

galaxy.ansible.com

Hub communautaire Ansible : milliers de rôles prêts à l'emploi pour déployer RHEL, configurer du réseau, automatiser.

CIS Red Hat Enterprise Linux Benchmark

cisecurity.org/benchmark/red_hat_linux

Référentiel de durcissement RHEL gratuit. Niveau 1 (essentiel) et niveau 2 (avancé). Aligné NIS2/ISO 27001.

BNB / FSMA / CCB ccb.belgium.be

Pour les secteurs régulés en Belgique : alertes spécifiques sur menaces réseau, recommandations sectorielles, partage d'incidents anonymisés.

À propos de FlashModz Enterprise

FlashModz Enterprise est un cabinet d'expertise IT opérationnelle, fondé par Jérémy Manet et basé à Farciennes, dans la région de Charleroi. Conseil et mise en œuvre concrète : sécurité, audit et pentest, automatisation Linux/DevOps et formations — pour les particuliers comme pour les entreprises, en Belgique et à l'international. Notre conviction : les ressources, les connaissances pointues et les outils des grandes entreprises doivent être accessibles aux PME et aux indépendants. À leur échelle. À leur budget. Avec la même rigueur.

CE QUE NOUS FAISONS

- Audit sécurité
- Pentest & rapport
- Sprint de stabilisation
- Team Lead fractionnel
- Formations Linux / DevOps

CERTIFICATIONS & RÉFÉRENTIELS

- CWNA · Ruckus
- Cisco Meraki
- Fortinet NSE
- Veeam
- Jamf · Apple
- OWASP / PTES
- NIS2
- ISO 27001
- RGPD

Jérémy Manet

Fondateur · Ingénieur & architecte système/réseau

Plus de 15 ans en architecture et ingénierie système/réseau : infrastructure, Wi-Fi d'entreprise, sécurité et virtualisation. Également management (people & technique) et gouvernance IT en tant que Process Owner COBIT, DORA et NIS2. Certifié CWNA, Cisco Meraki, Fortinet, Veeam, Jamf, Apple. Technologies : Aruba, HPE, Cisco, FortiGate, Nutanix.

Spécialités : Architecture · Réseau · Wi-Fi · Sécurité · Virtualisation · Gouvernance · NIS2 · DORA

De l’expertise IT pour ce qui compte vraiment.

contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

LinkedIn Facebook TikTok Avis Google

IDENTITÉ LÉGALE

FlashModz Enterprise

DÉNOMINATION	FlashModz Enterprise
FONDATEUR	Jérémy Manet
SIÈGE SOCIAL	Rue du Wainage 18, 6240 Farciennes (Belgique)
BCE / TVA	1035.510.038 · BE 1035.510.038
EU VAT	2.386.268.987
ZONES DESSERVIES	Charleroi et alentours (B2C) · Belgique & international (B2B)
CONTACT	contact@flashmodz.be · +32 471 87 87 07 · flashmodz.be

FlashModz

Cadrons votre stratégie RHEL

Chaque entreprise est unique. Chaque idée a ses contraintes, son contexte et ses priorités.

C'est pourquoi nous ne proposons pas de grille tarifaire figée. Nous préférons échanger avec vous, comprendre votre situation et construire une réponse adaptée à vos vrais besoins.

Parlons de votre situation

EMAIL

contact@flashmodz.be

TELEPHONE

+32 471 87 87 07

WEB

flashmodz.be

RETROUVEZ-NOUS

LinkedIn · Facebook · TikTok · Avis Google

Scannez pour accéder à ce document

BCE 1035.510.038 | Charleroi · Belgique & international