

8 conseils techniques pour renforcer le niveau de sécurité et de conformité

Réduisez les risques, appliquez vos configurations et politiques de sécurité et aidez votre entreprise à respecter la réglementation grâce aux fonctionnalités de sécurité et de conformité de Red Hat® Enterprise Linux®.

1 Gestion des paramètres de conformité standardisée

La politique de chiffrement à l'échelle du système offre un moyen cohérent de mettre en œuvre des paramètres de conformité basés sur des standards et d'en assurer le respect dans votre infrastructure.

D'une simple commande, vous pouvez sélectionner une politique de chiffrement intégrée et l'appliquer de manière cohérente à toutes les applications de votre système. De plus, si vous avez des exigences particulières en matière de conformité réglementaire, vous pouvez créer une politique personnalisée pour atteindre vos objectifs.

[En savoir plus](#) sur la gestion de la conformité

2 Automatisation de la configuration de la sécurité à l'aide des rôles système

Les rôles système de Red Hat Enterprise Linux, optimisés par Red Hat Ansible® Automation Platform, permettent aux administrateurs d'utiliser l'automatisation pour installer et gérer les paramètres de sécurité à grande échelle en peu de temps.

Les rôles système sont conçus pour fonctionner avec de multiples versions de Red Hat Enterprise Linux dans divers environnements, ce qui permet aux administrateurs d'appliquer les meilleures pratiques liées aux solutions Red Hat. Il suffit d'une commande ou d'un workflow pour configurer de nouveaux paramètres de sécurité et assurer leur bon fonctionnement sur tous vos systèmes.

[En savoir plus](#) sur l'automatisation de la sécurité

3 Centralisation des authentifications et des autorisations

La solution Red Hat Enterprise Linux inclut des capacités de gestion centralisée des identités qui vous permettent d'authentifier des utilisateurs et de mettre en œuvre des contrôles d'accès basés sur les rôles à l'aide d'une interface unique et évolutive qui couvre l'ensemble de votre datacenter. Les fonctions de gestion des identités de Red Hat Enterprise Linux s'utilisent avec Microsoft Active Directory, le protocole LDAP et d'autres solutions de gestion des accès et des identités tierces par le biais d'API standard.

Il est également possible de centraliser la gestion de l'authentification et de l'autorisation pour les services qui utilisent des techniques basées sur les certificats.

[En savoir plus](#) sur la gestion des identités

4 Personnalisation des politiques

SELinux (Security-Enhanced Linux) est une mise en œuvre du contrôle d'accès obligatoire dans le noyau Linux. Les conteneurs Red Hat Enterprise Linux s'exécutent par défaut avec SELinux, ce qui renforce la sécurité du système d'exploitation et empêche l'interruption des conteneurs et l'écrasement du système d'exploitation hôte sous-jacent ou d'autres conteneurs dans le système. Udraca permet aux administrateurs système et aux développeurs de conteneurs d'analyser un conteneur en cours d'exécution et de générer automatiquement une politique avec des règles SELinux spécifiques aux conteneurs. Cette solution simplifie la rédaction des politiques et réduit les risques, car elle élimine la nécessité d'exécuter les conteneurs avec des privilèges de super-utilisateur.

[Tester et en apprendre plus](#) sur le verrouillage des politiques

5 Application de correctifs avec un minimum de temps d'arrêt

Pour les versions Extended Update Support (EUS), Red Hat fournit des correctifs de noyau en direct qui éliminent les CVE (Common Vulnerabilities and Exposures) graves ou importantes, sans coût supplémentaire. Ainsi, vous pouvez appliquer des correctifs sur le noyau en cours d'exécution pour corriger immédiatement une vulnérabilité sans redémarrer votre système, ce qui réduit les temps d'arrêt sans compromettre la sécurité.

[Tester et en apprendre plus](#) sur l'application des correctifs du noyau en direct

6 Gestion de la sécurité et de la conformité à grande échelle

Inclus dans la souscription Red Hat Enterprise Linux sans coût supplémentaire, Red Hat Insights est une offre SaaS (Software-as-a-Service) qui fournit aux utilisateurs des données de sécurité exploitables sur leurs déploiements. Identifiez et traitez les risques liés aux opérations et aux vulnérabilités, analysez vos systèmes plus rapidement pour déterminer quels sont les correctifs manquants et accordez la priorité aux correctifs critiques. Vous pouvez créer, modifier, mettre en œuvre et assurer le respect des politiques de configuration de sécurité sur tous vos systèmes Red Hat Enterprise Linux à partir d'une seule interface web. Avec une souscription Red Hat Smart Management, vous pouvez également exécuter, mettre à l'échelle et automatiser les plans de correction à partir de Red Hat Insights.

[En savoir plus](#) sur la conformité

7 Enregistrement des activités du système pour assurer les objectifs de conformité

Red Hat Enterprise Linux inclut l'enregistrement des sessions avec des fonctionnalités d'audit et de journalisation qui permettent aux administrateurs de la sécurité de capturer les saisies et les activités d'un groupe d'utilisateurs donné sur un système. Ces données, enregistrées dans le même fichier journal que toutes les autres activités, peuvent être analysées et mises en corrélation à l'aide des fonctions de relecture et de pause incluses dans l'outil de lecture.

[Tester](#) l'enregistrement de sessions

8 Blocage de l'exécution des applications non autorisées

La liste des applications autorisées peut réduire les vecteurs d'attaque potentiels et empêcher l'exécution des applications non autorisées sur votre système. Le démon de politique d'accès aux fichiers (fapolicyd) intègre une liste d'applications autorisées qui permet à un utilisateur de lancer uniquement les exécutable approuvés sur un système. Les administrateurs système peuvent configurer fapolicyd avec des politiques par défaut ou créer les leurs pour empêcher l'exécution d'applications modifiées ou non autorisées.

[En savoir plus](#) sur les listes d'applications autorisées

À propos de Red Hat

Red Hat aide ses clients à standardiser leurs environnements, à développer des applications cloud-native et à intégrer, automatiser, sécuriser et gérer

des environnements complexes en offrant des services d'assistance, de formation et de consulting [primés](#).



facebook.com/redhatinc

[@RedHatFrance](https://twitter.com/RedHatFrance)

linkedin.com/company/red-hat

fr.redhat.com
O-F31208

EUROPE, MOYEN-ORIENT
ET AFRIQUE (EMEA)

00800 7334 2835

europe@redhat.com

FRANCE

00 33 1 41 91 23 23

fr.redhat.com