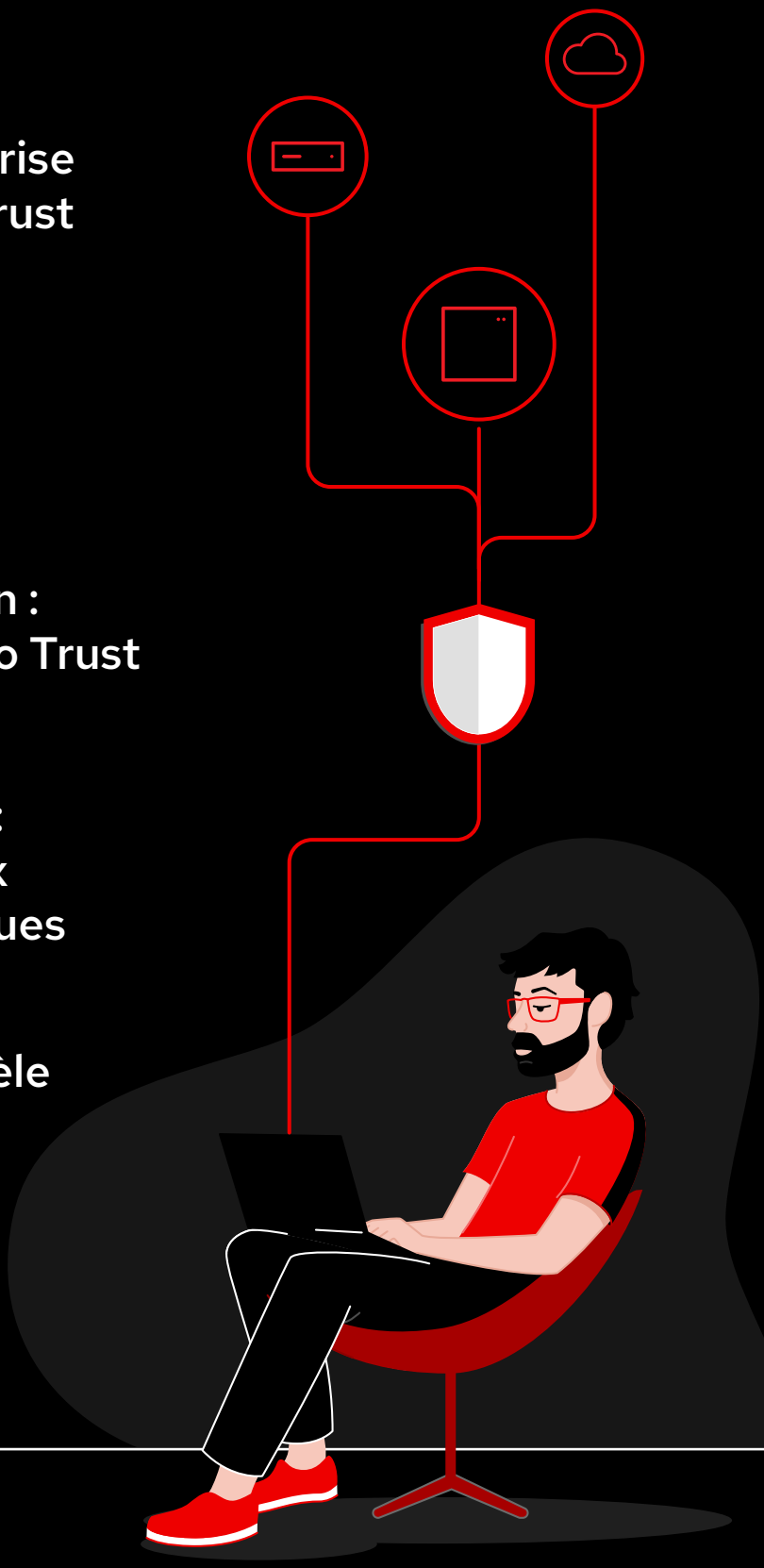
Red Hat
Enterprise Linux

Les principales fonctions de Red Hat Enterprise Linux pour réussir la mise en œuvre d'une architecture Zero Trust

Sommaire



Protégez votre entreprise avec le modèle Zero Trust

On observe aujourd'hui une généralisation du recours aux clouds publics, aux appareils mobiles et aux méthodes de travail à distance dans les entreprises. En conséquence, le périmètre des réseaux traditionnels se fragmente, posant de nouveaux défis liés à la sécurisation des environnements informatiques.

Les entreprises subissent de plus en plus d'attaques visant les vulnérabilités qui apparaissent dans les mécanismes de protection obsolètes, tels que l'authentification à facteur unique, la confiance implicite, les architectures basées sur le périmètre et un suivi inadéquat des comportements des utilisateurs et des événements. Dans ce contexte où les menaces se multiplient et où les effets des vulnérabilités ne cessent de croître, les entreprises doivent prendre conscience de la nécessité d'une stratégie de sécurité plus solide et proactive. Dans les faits, plus de la moitié des professionnels de la cybersécurité estiment que l'amélioration de la gestion des identités et des accès ainsi que la sécurisation des accès aux applications figurent parmi les priorités de sécurité actuelles[1].

La méthode Zero Trust propose une autre façon d'établir la confiance au sein d'un réseau. Elle rejette l'hypothèse selon laquelle tout ce qui se trouve à l'intérieur est sûr, contrairement à tout ce qui est à l'extérieur. Elle s'oppose également au modèle traditionnel, car elle part du principe qu'aucun utilisateur ni aucune ressource ne doivent être considérés comme fiables, que ce soit dans le périmètre ou à l'extérieur. Il faut continuellement les soumettre tous à des processus d'authentification et d'autorisation, quel que soit leur emplacement ou leur accès réseau.

Dans ce livre numérique, vous découvrirez les éléments à prendre en compte pour mettre en place une architecture Zero Trust au sein d'un environnement Linux®, et comment Red Hat® Enterprise Linux contribue à protéger votre environnement informatique et votre entreprise.

Le coût élevé des nouvelles menaces de sécurité

4,45 millions de dollars

Coût moyen d'une fuite de données, tous secteurs et régions confondus en 2023[2]

180 358 dollars

Diminution moyenne des coûts liés aux failles de sécurité lorsqu'un système de gestion des identités et des accès est déployé[2]

82 %

Pourcentage des failles qui ont concerné des données stockées dans des environnements cloud ou dans plusieurs environnements[2]

51 %

Pourcentage d'entreprises qui prévoient d'augmenter leurs investissements liés à la sécurité suite à une faille de sécurité[2]

1 *Rapport de Cybersecurity Insiders commissionné par Fortra, « 2023 Zero Trust Security Report », 2023*

2 *IBM Security, « Rapport 2023 sur le coût d'une violation de la confidentialité des données », juillet 2023*

Définition du modèle Zero Trust

Le Zero Trust est un modèle architectural qui applique des mesures de sécurité à chaque ressource, plutôt que d'assurer uniquement la sécurité au niveau du périmètre d'un réseau ou via une solution de gestion de la sécurité centralisée. Le principe de base veut qu'aucun acteur, système, réseau ou service intervenant à l'intérieur ou à l'extérieur du périmètre de sécurité ne soit implicitement considéré comme fiable. Pour établir une confiance explicite lorsqu'une ressource souhaite se connecter à une autre ressource, la session doit être authentifiée et autorisée.

Fonctionnement du modèle Zero Trust

La gestion des identités et des accès est au cœur des architectures Zero Trust, où l'accès aux ressources est refusé par défaut. Chaque sujet qui veut interagir avec une ressource doit demander un accès explicite pour cette interaction spécifique, et le risque inhérent à l'interaction doit être évalué avant d'autoriser l'accès. Une analyse de l'identité et des attributs du sujet est de ce fait essentielle. Vous devez déterminer qui demande l'accès, à quelles ressources, le but de cette transaction et les mesures à appliquer pour limiter cet accès en fonction du temps, de la méthode et de la fonction.

Une fois l'accès accordé, vous devez stocker, gérer, organiser et mettre à jour les identités et les attributs liés de manière cohérente et sécurisée. La plupart des entreprises utilisent un ou plusieurs systèmes de gestion des identités et d'informations d'identification, ou divers serveurs d'annuaire pour administrer ces informations. Enfin, il est aussi important de réévaluer en permanence les accès accordés pour garantir leur validité au fil du temps.

Une architecture Zero Trust qui repose sur ces principes clés vous aide à mieux protéger votre environnement informatique et votre entreprise :

1. Ne jamais faire confiance à qui ou quoi que ce soit de prime abord
2. Appliquer les principes du moindre privilège
3. Considérer que les réseaux et le trafic réseau sont compromis par défaut

Dans le cadre de notre approche Zero Trust, nous appliquons ces principes à la totalité de notre gamme de solutions, y compris à Red Hat Enterprise Linux, Red Hat Insights et Red Hat Identity Management.

Qu'est-ce qu'une limite de confiance ?

La limite de confiance désigne la séparation logique entre des composants au moment où le niveau de confiance accordé aux sujets participant à une interaction change, passant du statut *fiable* au statut *non fiable* et inversement. En général, la transition du statut *non fiable* à *fiable* nécessite à la fois le contrôle de l'identité du sujet et la vérification de ses droits et besoins d'accès à la ressource demandée.

Système d'exploitation : la base du modèle Zero Trust

Votre système d'exploitation représente la base de votre environnement informatique et de votre architecture Zero Trust. Il fournit des fonctions de sécurité essentielles, contrôle les accès des utilisateurs et des applications, chiffre les données sensibles et protège les secrets pour mettre en place et préserver la sécurité au sein de cet environnement.

Dans ce chapitre, vous découvrirez les principales fonctionnalités de systèmes d'exploitation utiles pour adopter une approche Zero Trust.

Chaîne d'approvisionnement du système d'exploitation fiable

Pour mettre en place un modèle Zero Trust, votre système d'exploitation doit être le plus sécurisé possible. La solution Red Hat Enterprise Linux est distribuée via une chaîne d'approvisionnement des logiciels fiable, ce qui réduit les risques d'apparition de vulnérabilités. Des analyses statiques du code du système d'exploitation tout entier identifient les erreurs présentes dans le style de programmation, les méthodes de référence mémoire et la validation du flux d'entrée, tout en garantissant la conformité avec les pratiques standard de codage. Des tests d'ingénierie qualité minimisent les failles de sécurité avant le déploiement et des processus de correction des failles appliquent régulièrement des correctifs pour les problèmes connus. Grâce aux nomenclatures logicielles publiées, vérifiez et évaluez les composants sélectionnés et testés de Red Hat Enterprise Linux, notamment le code source, les logiciels et bibliothèques Open Source, les middlewares et les frameworks de développement.

Contrôle d'accès obligatoire

Pour adopter une architecture Zero Trust, vous avez également besoin d'un système d'exploitation capable d'isoler et de contrôler l'accès aux ressources de manière individuelle. Red Hat Enterprise Linux inclut des contrôles d'accès obligatoires intégrés assurés par le système SELinux (Security-Enhanced Linux), une technologie de gestion des accès basée sur des politiques de sécurité centralisées. La mise en place d'un contrôle granulaire personnalisable sur les fichiers, processus, utilisateurs et applications contribue à minimiser le risque d'élévation non pertinente des privilèges, tandis que l'isolation des processus et la séparation des conteneurs permettent de réduire les attaques par élévation des privilèges. Enfin, la capacité de refuser l'accès par défaut s'aligne avec les principes Zero Trust et du moindre privilège.

Essayez de créer des profils de sécurité SELinux personnalisés pour les applications conteneurisées.

Accédez à l'**atelier interactif**.

Liste blanche d'applications

Une liste blanche d'applications établit un index des applications et des fichiers exécutables approuvés qu'un utilisateur donné est autorisé à exécuter. Cette pratique complète les contrôles d'accès obligatoires, qui permettent de contrôler le comportement des applications, mais sans pouvoir identifier celles qui sont fiables. Red Hat Enterprise Linux intègre des capacités de création de listes blanches qui utilisent le démon File Access Policy Daemon (fapolicyd) afin de détecter les applications non autorisées et d'empêcher leur exécution sur vos systèmes ou réseaux. De plus, les politiques d'autorisation prédéfinies et personnalisables donnent aux administrateurs système plus de contrôle sur les applications exécutées sur leurs serveurs et réseaux.

Apprenez à approuver des applications avec fapolicyd.

Accédez à l'**atelier interactif**.

Chiffrement moderne, évolutif et basé sur les politiques

Le chiffrement des données et du trafic réseau améliore la protection de l'environnement informatique et de l'entreprise. Plusieurs standards du secteur, notamment la norme FIPS 140 du NIST (National Institute of Standards and Technology), exigent des paramètres de chiffrement à l'échelle du système. La solution Red Hat Enterprise Linux propose des contrôles de chiffrement personnalisables basés sur des politiques pour assurer la cohérence des configurations sur tous vos systèmes ainsi que le respect des exigences. Des profils par défaut pour les normes de sécurité courantes facilitent la conformité. De même, l'automatisation de l'application des politiques rationalise la gestion, réduit les erreurs et contrôle le déchiffrement des fichiers et des volumes logiciels.

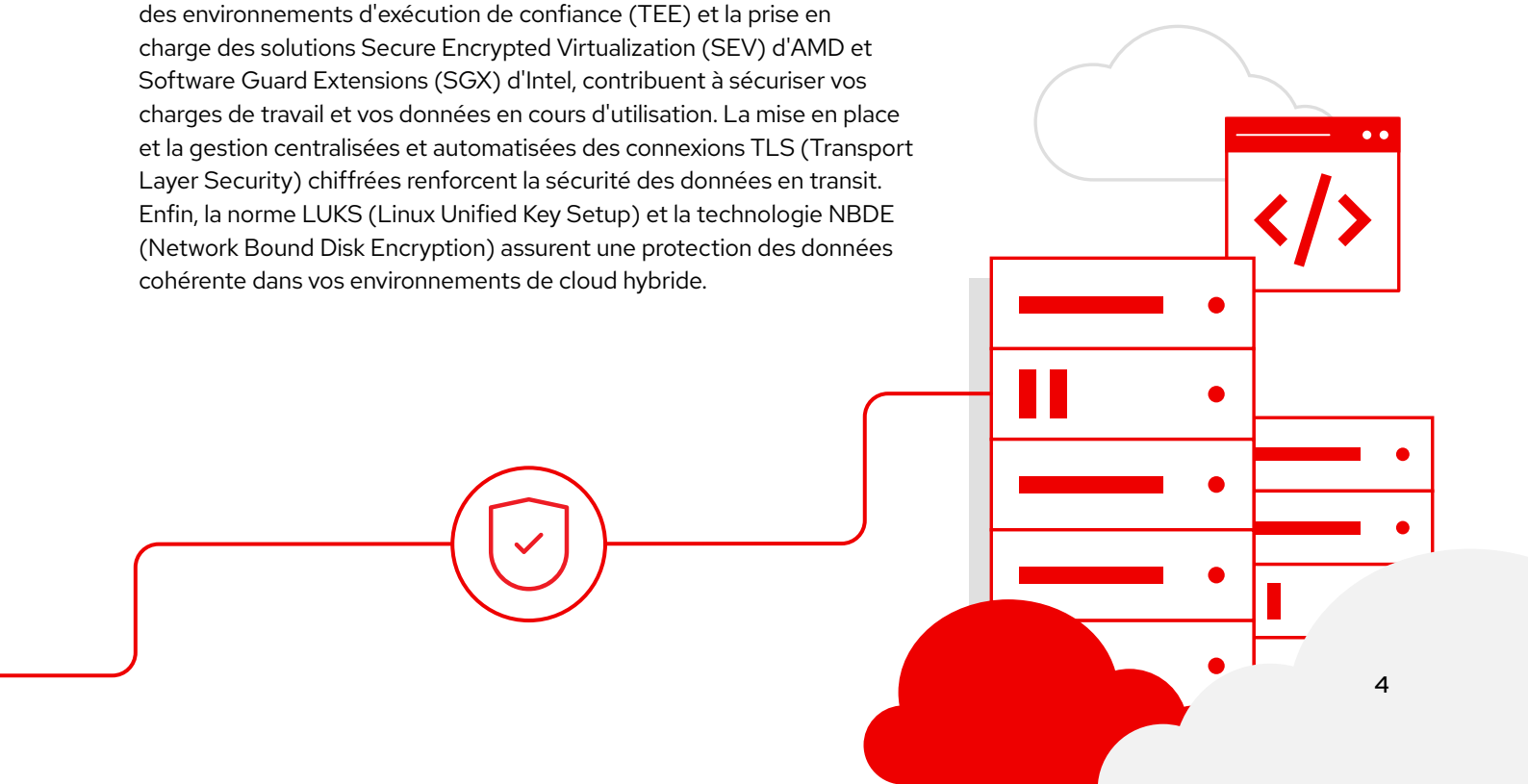
Apprenez à utiliser des politiques de chiffrement à l'échelle du système.

Accédez à l'**atelier interactif sur la configuration**.

Accédez à l'**atelier interactif sur la personnalisation**.

Protection des données à toutes les étapes

Les modèles Zero Trust exigent la sécurisation des données à tout moment : en cours d'utilisation, en transit ou au repos. La solution Red Hat Enterprise Linux prend en charge des technologies et des fonctionnalités qui protègent vos données en continu. Les fonctionnalités des environnements d'exécution de confiance (TEE) et la prise en charge des solutions Secure Encrypted Virtualization (SEV) d'AMD et Software Guard Extensions (SGX) d'Intel, contribuent à sécuriser vos charges de travail et vos données en cours d'utilisation. La mise en place et la gestion centralisées et automatisées des connexions TLS (Transport Layer Security) chiffrées renforcent la sécurité des données en transit. Enfin, la norme LUKS (Linux Unified Key Setup) et la technologie NBDE (Network Bound Disk Encryption) assurent une protection des données cohérente dans vos environnements de cloud hybride.



Racine de confiance basée sur le matériel

Les technologies de racine de confiance matérielle, d'attestation à distance et de démarrage mesuré vous permettent de vérifier l'intégrité de vos systèmes et de garantir que ces derniers n'ont pas été modifiés ou falsifiés. La solution Red Hat Enterprise Linux inclut des fonctionnalités clés qui prennent en charge ces technologies.

- Retirez vos secrets cryptographiques des logiciels pour les placer sur des dispositifs tels que des cartes à puce, des boîtes noires transactionnelles (BNT) et des modules TPM (Trusted Platform Module).
- Utilisez des modules TPM et des fonctionnalités de démarrage mesuré afin de calculer et de stocker de façon chiffrée les mesures hachées des processus de démarrage et des fichiers binaires d'exécution sécurisés.
- Contrôlez les mesures de démarrage à l'aide d'agents de certificat à distance pour déterminer si un système présente un risque avant de prendre des mesures correctives.

Analyse de la conformité

Le non-respect des normes et réglementations du secteur et de l'entreprise peut vous faire courir des risques et engendrer des coûts. Red Hat Enterprise Linux intègre des outils d'analyse de la conformité et de la vulnérabilité, dont Open Security Content Automation Protocol (OpenSCAP), pour vous aider à automatiser et simplifier les audits, détecter et corriger les systèmes mal configurés, ainsi que préserver plus facilement la conformité. Voici ses principales fonctions :

- Profils de conformité prédéfinis et personnalisables
- Capacités de création de rapports et de génération de références
- Intégration aux solutions Red Hat Satellite et Red Hat Insights pour gérer la conformité à grande échelle
- Mesures de sécurité intégrées pour la norme PCI-DSS (Payment Card Industry Data Security Standard), le profil de protection OSPP (Operating System Protection Profile), les normes Essential Eight de l'ACSC (Australian Cyber Security Centre), les critères CIS (Center for Internet Security), la loi HIPAA (Health Insurance Portability and Accountability Act) et les directives STIG (Security Technical Implementation Guidelines) de la DISA (Defense Information Systems Agency)

Essayez OpenSCAP pour assurer la conformité des systèmes de sécurité et analyser les vulnérabilités.

Accédez à l'**atelier interactif**.

Apprenez à corriger les vulnérabilités avec Red Hat Insights.

Accédez à l'**atelier interactif**.

Gestion automatisée des configurations

L'automatisation est essentielle pour assurer la cohérence des configurations de sécurité et respecter les exigences de gouvernance et de conformité à grande échelle. Avec les rôles système de la solution Red Hat Enterprise Linux, vous pouvez automatiser la configuration et la gestion de la sécurité dans vos environnements de cloud hybride et mettre en œuvre votre architecture Zero Trust sans être expert en la matière. Basé sur Red Hat Ansible® Automation Platform, ce contenu d'automatisation prédéfini facilite la configuration des outils de sécurité tels que SELinux, la technologie NBDE (Network Bound Disk Encryption), le protocole SSH (Secure Shell), les politiques de chiffrement, ainsi que la gestion des identités et des certificats.

Testez les rôles système Red Hat Enterprise Linux.

Accédez à l'**atelier interactif**.

Gestion des identités : contrôle des accès aux ressources informatiques

Les solutions de gestion des identités permettent de s'assurer que seuls les utilisateurs autorisés peuvent accéder aux ressources dont ils ont besoin. Elles englobent l'ensemble des politiques et technologies de l'entreprise, ce qui leur permet d'identifier, authentifier et autoriser les accès pertinents aux ressources par le biais de données d'identité, d'attributs, d'informations d'identification et de certificats.

Dans ce chapitre, vous découvrirez les principales fonctionnalités de gestion des identités utiles pour adopter une approche Zero Trust.

Système de stockage d'identités

Un contrôleur de domaine vous permet de gérer les identités, les accès et les politiques pour les utilisateurs, les services et les hôtes. Inclus dans la solution Red Hat Enterprise Linux, Red Hat Identity Management est un système centralisé de stockage d'identités et un contrôleur de domaine qui vous aide à réduire la charge de travail d'administration, simplifier la gestion de la sécurité et garantir la cohérence dans l'ensemble de votre environnement. Il vous permet de stocker toutes les informations liées à l'identité au même endroit, de regrouper des opérations et d'appliquer des politiques cohérentes au sein des ressources et environnements. Avec l'enregistrement simplifié du domaine, il est possible de créer un périmètre de sécurité fiable et de faciliter l'authentification pour offrir une meilleure expérience utilisateur.

Authentification unique et unifiée

Dans les architectures Zero Trust, chaque service, appareil ou serveur requiert une authentification d'accès séparée. Les systèmes d'authentification unique et unifiée (SSO) simplifient les accès à l'aide d'un service d'identité centralisé pour permettre aux serveurs de reconnaître les utilisateurs vérifiés. La solution Red Hat Enterprise Linux prend en charge la norme OAuth 2.0 ainsi que Red Hat Identity Management pour que les utilisateurs aient accès à plusieurs services avec une authentification unique et bénéficient d'une expérience simplifiée. Avec l'intégration de plusieurs services, dont l'authentification unique et unifiée de Red Hat, Microsoft AzureAD et GitHub, vous pouvez continuer à utiliser vos services de gestion des identités existants, tout en assurant une flexibilité suffisante pour l'avenir.

Intégrations avec d'autres systèmes de gestion des identités

La plupart des entreprises utilisent déjà un ou plusieurs systèmes de gestion des identités pour leurs environnements Linux et Windows. L'intégration de ces systèmes au sein d'une solution unique et complète vous aide à centraliser l'exploitation, à garantir la cohérence dans votre entreprise et à améliorer l'efficacité au niveau de l'administration. Le service Red Hat Identity Management s'intègre de façon native à Microsoft Active Directory pour assurer la gestion des identités dans des environnements mixtes et l'application de politiques de contrôle des accès directement dans votre domaine Red Hat Enterprise Linux.

Gestion des politiques

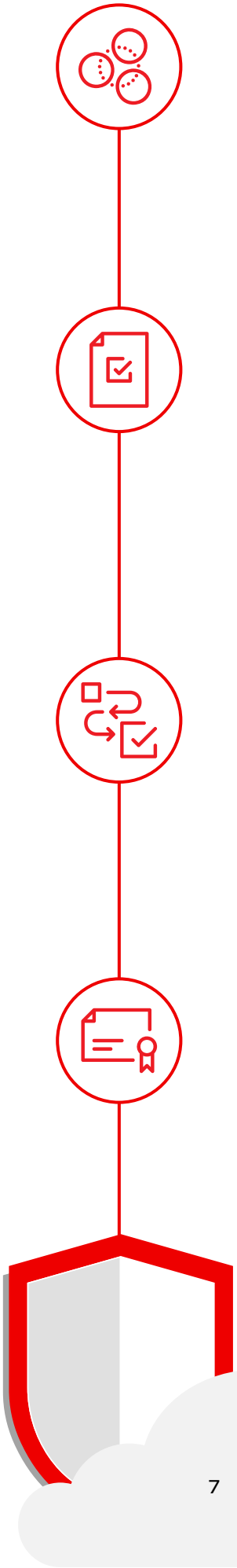
Une approche de gestion des identités basée sur les politiques contribue à améliorer la cohérence, l'efficacité et la sécurité. Le service Red Hat Identity Management vous permet de paramétrer et d'appliquer des contrôles basés sur les politiques à partir d'une interface centralisée, garantissant ainsi une configuration correcte des identités, accès et ressources. Les politiques personnalisables de gestion des identités et des accès contribuent à bloquer les tentatives d'élévation de privilèges au sein de votre environnement. De plus, le contrôle d'accès basé sur les rôles vous permet de répartir les tâches d'administration liées au serveur de gestion des identités, y compris la gestion de l'authentification et des autorisations, ainsi que l'enregistrement, la vérification et la journalisation des sessions, entre les membres de votre équipe.

Authentification à plusieurs facteurs

L'authentification à plusieurs facteurs (MFA) ajoute une couche supplémentaire de sécurité en appliquant plusieurs étapes de vérification de l'identité avant d'accorder l'accès à un système ou service donné. Le service Red Hat Identity Management prend en charge l'authentification à plusieurs facteurs (MFA) par le biais d'appareils de chiffrement tels que des jetons textuels et des cartes à puce. Vous pouvez également choisir et configurer différents types d'authentification, dont les mots de passe, les certificats, le service RADIUS (Remote Authentication Dial-In User Service), les mots de passe à usage unique et l'extension PKINIT (Public Key Cryptography for Initial Authentication), et définir des méthodes d'authentification par défaut pour tous les utilisateurs.

Gestion des certificats

Les certificats numériques contiennent les informations requises pour confirmer l'identité des utilisateurs, des applications, des sites internet et d'autres sujets. Vous devez les créer, surveiller, renouveler et retirer en fonction des principes du moindre privilège. Le service Red Hat Identity Management prend en charge la gestion de l'ensemble du cycle de vie pour les certificats des utilisateurs, des hôtes et des services. Vous pouvez également déployer Red Hat Certificate System, une autorité de certification qui prend en charge des tâches de gestion avancée comme le provisionnement des cartes à puce, les types de certificats personnalisés et les stockages secrets protégés. La prise en charge des normes et des protocoles courants, notamment la norme X.509, les protocoles ACME (Automatic Certificate Management Environment), SCEP (Simple Certificate Enrollment Protocol), SSL (Secure Sockets Layer) et TLS (Transport Layer Security), vous permet de créer des certificats adaptés à votre écosystème informatique. Le suivi automatique des dates d'expiration vous évite de manquer le renouvellement d'un certificat, tandis que l'authentification par infrastructure à clé publique (PKI) vérifie la fiabilité des identités.



Se lancer avec le modèle Zero Trust

Une architecture Zero Trust contribue à protéger vos ressources informatiques et métier dans un monde en constante évolution.

Les solutions Red Hat constituent une base fiable, intégrée et axée sur la sécurité pour vos architectures Zero Trust. D'ailleurs, votre entreprise utilise peut-être déjà certains éléments nécessaires à la mise en place de ce modèle. Avec Red Hat Enterprise Linux, vous bénéficiez des technologies de sécurité, des fonctions de contrôle, des certifications ainsi que d'un service d'assistance pour créer et gérer vos architectures Zero Trust. Le service Red Hat Identity Management, quant à lui, centralise la gestion des identités, applique les contrôles de sécurité et assure le respect des normes de sécurité dans l'ensemble de votre environnement.

Profitez d'un essai gratuit dès aujourd'hui en accédant à nos **ateliers interactifs en ligne**.

568051_0124_KVM

Red Hat