Red Hat
Enterprise Linux

Posez les bases d'une sécurité Zero Trust dans les environnements Linux

Une architecture Zero Trust vous aide à mieux protéger votre environnement informatique et votre entreprise.

Red Hat propose plusieurs principes fondamentaux pour vous guider dans la mise en œuvre d'une architecture Zero Trust :

- Ne faites confiance à rien ni personne de prime abord, vérifiez toujours les identités.
- Appliquez les principes du moindre privilège.
- Considérez que les réseaux et le trafic réseau sont compromis par défaut.

Les environnements informatiques modernes nécessitent de nouvelles approches en matière de sécurité

Les approches de sécurité classiques basées sur le périmètre ne protègent pas efficacement les nouveaux environnements cloud hautement distribués. En parallèle, les menaces et les effets des failles ne cessent d'augmenter. Les pirates exploitent les vulnérabilités qui apparaissent souvent 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.

La mise en œuvre d'une architecture Zero Trust vous aide à protéger votre environnement informatique et votre entreprise. Dans cet aperçu, nous allons aborder les éléments à prendre en compte pour l'établissement d'architectures Zero Trust dans les environnements Linux®.

Présentation et fonctionnement 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.

La gestion des identités et des accès est au cœur des architectures Zero Trust. Ce type d'architecture devrait refuser l'accès des ressources 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. Cette évaluation repose notamment sur une analyse de l'identité et des attributs du sujet. 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 ainsi que 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.

Éléments à prendre en compte pour la mise en œuvre d'une architecture Zero Trust

Outre l'évolution de la culture informatique et des processus en matière de sécurité, l'adoption d'une approche de sécurité Zero Trust requiert un certain nombre de capacités technologiques. Dans la suite de ce document, nous parlerons des fonctions et capacités principales à rechercher dans une solution de gestion du système d'exploitation et des identités si vous souhaitez adopter une architecture Zero Trust.

Fonctions et capacités du système d'exploitation

Votre système d'exploitation représente la base de votre environnement informatique et de votre architecture Zero Trust.

Red Hat Enterprise Linux

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 entre le statut non fiable et fiable nécessite deux étapes :

- **l'authentification** : vérification et validation de l'identité du sujet ;
- **l'autorisation** : vérification et validation du droit et de la nécessité d'accéder à une ressource.

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 et capable de refuser tous les accès par défaut. Afin de diminuer les risques, choisissez un système d'exploitation axé sur la sécurité, fourni via une chaîne d'approvisionnement des logiciels fiable. Choisissez des fournisseurs de système d'exploitation qui proposent les éléments suivants :

- Des analyses statiques du code du système d'exploitation tout entier pour identifier 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 meilleures pratiques de programmation
- Des indicateurs de compilation pour exécuter des applications et assigner des segments de mémoire de manière non prédictive afin d'éviter l'écrasement de la pile, de réduire les corruptions de mémoire et de prendre en charge l'intégrité du flux de contrôle du matériel
- Des tests d'ingénierie qualité pour minimiser les failles de sécurité avant le déploiement.
- Des processus de correction des failles qui appliquent régulièrement des correctifs pour les vulnérabilités connues

Contrôle d'accès obligatoire

Votre système d'exploitation doit également être capable d'isoler et de contrôler l'accès aux ressources de manière individuelle. Les technologies de contrôle d'accès obligatoire comme SELinux (Security-Enhanced Linux) répondent à ce besoin en se basant sur des politiques de sécurité gérées de manière centralisée. Optez pour un système d'exploitation qui présente les capacités suivantes :

- Des contrôles d'accès obligatoires intégrés, avec un contrôle granulaire et personnalisé des fichiers, processus, utilisateurs et applications pour minimiser les risques de réattribution inadaptée des privilèges
- La capacité de refuser l'accès par défaut pour s'aligner avec les principes Zero Trust

Chiffrement moderne, évolutif et basé sur les politiques

Le chiffrement des données et du trafic réseau améliore la protection de votre environnement informatique et de votre entreprise. Plusieurs standards du secteur, notamment la norme FIPS 140, exigent des paramètres de chiffrement à l'échelle du système. Le chiffrement basé sur les politiques vous permet de configurer vos systèmes de manière cohérente afin de respecter les exigences de conformité. Optez pour un système d'exploitation qui comprend les éléments suivants :

- Des contrôles de chiffrement basés sur les politiques qui vous permettent d'appliquer des paramètres de manière cohérente sur tous vos systèmes
- Des profils par défaut pour les normes de sécurité courantes, comme la norme FIPS 140
- L'automatisation de l'application des politiques pour rationaliser la gestion, réduire les erreurs et ne déchiffrer les fichiers et les volumes logiciels que lorsque cela est spécifiquement autorisé par une politique
- Des politiques et paramètres personnalisables pour répondre aux besoins de votre entreprise

Liste blanche d'applications

La mise sur liste blanche des applications consiste à spécifier un index d'applications approuvées ou de fichiers autorisés à être exécutés sur un système par un utilisateur particulier. Cette pratique complète les contrôles d'accès obligatoires, qui permettent de contrôler le comportement des applications, mais sans pouvoir identifier celles qui sont fiables.

Choisissez un système d'exploitation qui intègre des capacités de création de listes blanches, comme le démon File Access Policy Daemon (fapolicyd), pour détecter les applications non autorisées et empêcher leur exécution sur vos systèmes ou réseaux, ainsi que des politiques de liste blanche prédéfinies et personnalisables.

Red Hat Enterprise Linux

Racine de confiance basée sur le matériel

Les technologies de racine de confiance matérielle vous permettent de vérifier l'intégrité des systèmes et de garantir que ces derniers n'ont pas été modifiés ou falsifiés. Choisissez un système d'exploitation qui vous permet de retirer 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).

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 les coûts. Les outils d'analyse des systèmes comme OpenSCAP (Open Security Content Automation Protocol) facilitent les audits et vous aident à corriger vos systèmes non conformes. Optez pour un système d'exploitation qui inclut les éléments suivants :

- Des outils d'analyses intégrés avec des profils de conformité prédéfinis et personnalisables
- Des capacités de création de rapports et de génération de références pour faciliter l'audit et afficher les écarts
- La correction automatisée des systèmes non conformes
- L'automatisation et l'intégration à d'autres outils pour permettre la gestion à grande échelle

Surveillance et journalisation des transactions

La surveillance et la journalisation vous permettent de vérifier les actions des utilisateurs pour détecter les comportements suspects. L'enregistrement de session et les outils de compilation des journaux vous aident à tirer des informations sur les actions dans l'ensemble de votre environnement. Optez pour un système d'exploitation qui comprend les capacités suivantes :

- La journalisation des variables d'entrée, de sortie, d'état du système et de l'environnement pour fournir des informations contextuelles
- Le stockage des journaux hors du système pour éviter la falsification
- Des paramètres d'enregistrement personnalisables pour faciliter les audits

Principales normes de sécurité

- FIPS 140
- Critères communs (CC)
- Directives STIG (Secure Technical Implementation Guidelines)

Attestations indépendantes et certifications de sécurité

La vérification par un tiers de la conformité de votre système d'exploitation avec les normes de sécurité vous permet de mener vos activités en toute confiance. Sélectionnez un système d'exploitation qui garantit la conformité avec les normes courantes.

Fonctions et capacités de la solution de gestion des identités

Votre solution de gestion des identités couvre les identités, leurs attributs, les informations d'identification, les certificats et d'autres éléments nécessaires pour autoriser et authentifier l'accès aux ressources.

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. Un système de stockage d'identités et un contrôleur de domaine peuvent vous aider à réduire la charge de travail d'administration, simplifier la gestion de la sécurité et garantir la cohérence dans l'ensemble de votre environnement. Envisagez une solution qui propose des capacités de gestion centralisée des identités pour rationaliser l'exécution et favoriser la cohérence. Votre solution doit également prendre en charge vos infrastructures et plateformes actuelles ainsi que celles que vous prévoyez d'utiliser à l'avenir.

Red Hat
Enterprise Linux

Principaux types d'authentification

- Mots de passe normaux, à usage unique et renforcés
- Protocole RADIUS (Remote Authentication Dial-In User Service)
- Protocole PKINIT (Public Key Cryptography for Initial Authentication)

Intégrations avec d'autres systèmes de gestion des identités

La plupart des entreprises utilisent 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 et à garantir la cohérence dans votre entreprise. Optez pour une solution de gestion des identités qui fonctionne avec les outils les plus fréquemment utilisés, comme Microsoft Active Directory, pour gérer les identités dans vos environnements mixtes.

Gestion des politiques

Une approche de gestion des identités basée sur les politiques contribue à améliorer la cohérence, l'efficacité et la sécurité. Les solutions de gestion des identités qui vous permettent de paramétrer et d'appliquer des contrôles basés sur les politiques à partir d'une interface centralisée garantissent la configuration adéquate des identités, des accès et des ressources. Recherchez les éléments suivants :

- Des capacités de contrôle d'accès basés sur les rôles et les politiques
- Des politiques personnalisables sur les identités et les accès
- Des capacités de gestion des authentifications et des autorisations
- Des capacités d'enregistrement, d'audit et de connexion pour les sessions

Authentification à plusieurs facteurs

L'authentification à plusieurs facteurs (MFA) ajoute une couche supplémentaire de sécurité qui met en place plusieurs étapes de vérification de l'identité avant d'accorder l'accès au système ou service. Choisissez des solutions de gestion des identités qui proposent des types d'authentification configurables et prennent en charge la MFA via des jetons matériels et des cartes à puce.

Normes et protocoles fréquents sur les certifications

- X.509
- Protocole ACME (Automated Certificate Management Environment)
- Protocole SCEP (Simple Certificate Enrollment Protocol)
- Protocole SSL (Secure Sockets Layer)
- Chiffrement TLS (Transport Layer Security)

Gestion des certificats

Les certificats numériques contiennent les informations requises pour authentifier 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. Choisissez une solution de gestion des identités qui fournit les avantages suivants :

- La gestion de l'ensemble du cycle de vie pour les certificats des utilisateurs, des hôtes et des services
- Une assistance pour les normes et les protocoles courants
- Le suivi automatique des dates d'expiration des certificats pour ne pas manquer les renouvellements
- La prise en charge de l'authentification des infrastructures à clé publique (PKI)

Authentification unique

Chaque service, appareil ou serveur requiert une authentification d'accès séparée. Les systèmes d'authentification unique (SSO) simplifient les accès à l'aide d'un service d'identité centralisé pour permettre aux serveurs de connaître les utilisateurs vérifiés. Ceux-ci n'ont alors à s'authentifier qu'une seule fois pour accéder à plusieurs services. Choisissez une solution de gestion des identités qui prend en charge l'authentification sur internet ainsi que les services que vous utilisez maintenant et prévoyez d'utiliser.

Posez les bases d'une sécurité Zero Trust avec Red Hat Enterprise Linux

Red Hat apporte une base technologique sur laquelle vous pouvez vous appuyer pour concevoir, créer et gérer des architectures Zero Trust. La solution Red Hat® Enterprise Linux apporte les technologies, contrôles et certifications de sécurité, ainsi que l'assistance dont vous avez besoin pour adopter des

Accélérez les déploiements grâce aux services d'experts

Red Hat propose des services pour vous aider à adopter une architecture Zero Trust basée sur les plateformes et produits Red Hat.

- Red Hat Open Innovation Labs est un stage en immersion qui réunit des ingénieurs et des spécialistes de l'Open Source pour vous aider à obtenir des résultats métier concrets.
- Services Red Hat : parcours d'adoption du modèle Zero Trust est un contrat de consulting qui vous aide à évaluer votre situation actuelle et à élaborer un plan pour mettre en place une architecture Zero Trust.

modèles Zero Trust. Elle respecte toutes les exigences liées au système d'exploitation abordées dans ce document, à savoir : distribution par une chaîne d'approvisionnement fiable, contrôles d'accès SELinux, politiques de chiffrement à l'échelle du système, listes blanches d'application, mécanismes de racine de confiance matérielle, capacités d'enregistrement de session et rôles système. Elle intègre également un outil d'analyse OpenSCAP ainsi que le service d'analyses prédictives et de correction Red Hat Insights. Enfin, la solution Red Hat Enterprise Linux est certifiée conforme à de nombreuses normes de sécurité gouvernementales, telles que les critères communs, la norme FIPS 140, les directives STIG et la section 508.

Incluse avec Red Hat Enterprise Linux, la solution Red Hat Identity Management peut vous aider à centraliser la gestion des identités, appliquer les contrôles de sécurité et faire respecter les normes de sécurité dans l'ensemble de votre environnement. Elle offre les capacités nécessaires pour adopter les meilleures pratiques Zero Trust tout en simplifiant l'infrastructure de gestion des identités. Elle s'intègre avec Microsoft Active Directory, le protocole LDAP ainsi que d'autres solutions tierces par le biais d'interfaces standard. Red Hat Identity Management prend également en charge les techniques d'authentification et d'autorisation basées sur des certificats.

Les solutions Red Hat Enterprise Linux et Red Hat Identity Management s'intègrent aux autres produits Red Hat pour fournir une base unifiée aux architectures Zero Trust.

- Red Hat Single Sign-On fournit des capacités d'authentification unique et unifiée sur le Web, basées sur les normes les plus courantes.
- Red Hat® Satellite est un produit de gestion d'infrastructure conçu pour assurer l'efficacité, la sécurité et la conformité des environnements Red Hat Enterprise Linux.
- Red Hat Ansible® Automation Platform fournit un cadre pour le déploiement et la gestion de l'automatisation à l'échelle de l'entreprise.
- Red Hat Certificate System est 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 la protection des stockages secrets.
- Red Hat Directory Server est un registre réseau indépendant du système d'exploitation et évolutif, qui vous permet de stocker de façon centralisée les informations relatives à l'identité des utilisateurs et aux applications pour les topologies d'annuaires distribués.

Et après ?

- En savoir plus sur la sécurité de Red Hat Enterprise Linux
- Découvrir l'approche de Red Hat en matière de sécurité du cloud hybride

À propos de Red Hat

Premier éditeur mondial de solutions Open Source, Red Hat s'appuie sur une approche communautaire pour fournir des technologies Linux, de cloud hybride, de conteneurs et Kubernetes fiables et performantes. Red Hat aide ses clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et à automatiser des environnements complexes. Conseiller de confiance auprès des entreprises du Fortune 500, Red Hat propose des services d'assistance, de formation et de consulting reconnus qui apportent à tout secteur les avantages de l'innovation ouverte. Situé au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, Red Hat participe à la croissance et à la transformation des entreprises et les aide à se préparer à un avenir toujours plus numérique.

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat

fr.redhat.com
F31712_0522_KVM