Red Hat Enterprise Linux

为 Linux 环境中的零信任建立基础

零信任架构可以帮助您更好地保护您的 IT 环境和企业。

红帽采取多项关键原则以指导零信任架构的实施：

- 绝不对参与者进行隐式信任，始终需要验证。
- 采用最低权限访问策略。
- 假设默认情况下网络和网络流量会遭到破坏。

现代 IT 环境需要新的安全防护方法

作用于边界的传统安全防护方法无法有效保护分布广泛、基于云的新环境。安全威胁和入侵造成的影响在持续增长。这些漏洞通常是由于过时的安全模式（如单一因素认证、隐式信任、基于边界的架构和不到位的用户和事件行为追踪）所导致的，并且会遭到不法分子的利用。

实施零信任架构可以帮助您保护您的 IT 环境和企业。本概述讨论了在 Linux® 环境中建立零信任架构的技术注意事项。

什么是零信任，它是如何工作的？

零信任是一种架构模式，它将安全防护应用于每个资产，而不是仅通过网络边界或通过集中安全管理解决方案来管理安全防护。零信任模型的基本原则是，在安全防护边界内或安全防护边界外运行的任何参与者、系统、网络或服务均不受隐式信任。为使一个资源连接到另一个资源，会话必须经过身份验证和授权来建立显式信任。

身份管理和访问权限管理是零信任架构的核心。默认情况下，零信任架构应拒绝访问资产。每一个想要与资产交互的主体都必须针对该特定交互申请明确的访问权限，并且在允许访问之前应该对该交互的风险进行评估。了解主体的身份和属性对该评估至关重要。您需要确定是谁请求访问、需要访问哪些资产、事务的目的，以及如何根据时间、方法和功能限制访问。

做出访问决策后，您必须以受保护且一致的方式存储、管理、整理并更新身份和身份属性。大多数企业使用一个或多个身份管理、目录服务器和凭据管理系统来管理此类信息。还应不断重新评估这些访问决策，以确保这些决策随着时间的推移仍然有效。

实施零信任架构的注意事项

尽管采用零信任安全防护方法通常涉及对安全性和 IT 理念和流程的更改，但是还需要具备大量技术功能。以下章节讨论了采用零信任架构时需要的关键操作系统和身份管理解决方案的功能和特性。

操作系统的功能和特性

操作系统是 IT 环境和零信任架构的基础。

红帽官方微博　红帽官方微信

Red Hat Enterprise Linux

信任边界是什么？

信任边界是组件之间的任何逻辑区隔，参与交互的主体会在这里更改其信任状态（通常在“*受信任*”和“*不受信任*”两种状态之间）。一般来说，从不受信任到受信任的转变需要完成两件事：

- **验证**：验证和确认主体的身份。
- **授权**：验证和确认访问资产的权利和要求。

值得信赖的操作系统供应链

零信任模型要求您的操作系统尽可能安全，并能够在默认情况下拒绝所有访问。选择安全至上的操作系统，通过值得信赖的软件供应链交付，以降低您的风险。考虑提供以下功能的操作系统供应商：

- 整个操作系统的静态代码分析，以识别编程风格、内存引用方法和输入流验证中的错误，并确保符合编码最佳实践。
- 用于以非预测方式运行应用程序和分配内存段的编译器标志，以防止堆栈损坏、减轻内存损坏并提供控制流完整性硬件支持。
- 广泛的质量工程（QE）测试，以在交付前将安全缺陷降至最低。
- 漏洞修补程序，定期针对已知漏洞提供补救。

强制访问控制

您的操作系统还必须能够单独隔离和控制对资源的访问。强制访问控制（MAC）技术，如安全增强型 Linux（SELinux）等，可以根据集中管理的安全策略来实现这一点。寻找以下操作系统功能：

- 内置 MAC，可为文件、流程、用户和应用配备精细定制的的访问控制，以最大程度地降低不当权限提升的风险。
- 能够默认拒绝所有访问，以符合零信任原则

现代、可扩展、基于策略的加密技术

通过对数据和网络流量进行加密，可增强对您的 IT 环境和企业的防护。一些行业标准（包括联邦信息处理标准（FIPS）140）要求在系统范围内应用加密设置。基于策略的加密使您可以跨系统应用一致的配置，以帮助满足法规遵从性要求。选择包含以下功能的操作系统：

- 基于策略的加密控制，使您能够在系统中一致地应用设置。
- 适用于通用安全标准（如 FIPS 140）的默认配置文件。
- 自动化策略应用和实施，以简化管理、减少错误，并仅在策略明确允许的情况下解密文件和软件卷。
- 可自定义的策略和设置，以满足您企业的需求。

应用白名单

应用白名单是指将一些被批准的应用或可执行文件列在清单中，只有这些应用或文件才能由指定的用户在系统上运行。这种做法是对强制访问控制的补充，强制访问控制可以控制应用行为，但无法知道哪些应用是可信任的。

选择可提供内置应用白名单功能（如文件访问策略守护进程（fapolicyd））的操作系统，以检测和防止未经授权的应用在系统或网络上运行，操作系统还应具有预定义和可自定义的白名单策略。

Red Hat Enterprise Linux

基于硬件的信任根

基于硬件的信任根功能可帮助您验证系统的完整性，确保您的系统未被修改或篡改。选择一个能让您将加密密钥从软件中移出并转移到防篡改硬件设备（如智能卡、硬件安全模块（HSM）和可信平台模块（TPM））上的操作系统。

合规性扫描

不遵守企业和行业标准及法规可能会给您的企业带来巨大的成本和风险。诸如开放安全内容自动化协议（OpenSCAP）之类的系统扫描工具可以简化审核并帮助您修复不合规的系统。寻找可提供以下功能的操作系统：

- 内置扫描工具，具有预定义和可自定义的合规性配置文件。
- 报告和基线生成功能，以简化审核和显示偏移。
- 自动修复不合规系统。
- 自动化以及与其他工具的集成，以实现规模化管理。

事务监控和日志记录

监控和记录可以审核用户的行为，以确定是否发生了恶意行为。会话记录和日志聚合工具可以帮助您深入了解整个环境中的操作。选择提供以下功能的操作系统：

- 对输入、输出、系统状态和环境变量进行日志记录，以提供上下文洞察。
- 系统外日志存储，以防止篡改。
- 可自定义的记录设置，以简化审核。

主要安全标准

- FIPS 140
- 通用准则（CC）
- 安全技术实施指南（STIG）

独立证明和安全认证

让第三方来验证您的操作系统是否符合安全标准，使您能够更放心地运行。选择符合通用标准的操作系统。

身份管理解决方案的功能和特性

您的身份管理解决方案包括身份、属性、凭据、证书以及授权和验证访问资产所需的其他项目。

身份存储

域控制器允许您管理用户、服务和主机的身份、访问权限和策略。使用集中式身份存储和域控制器有助于减少管理开销，简化安全管理，并确保整个环境的一致性。考虑具备集中式身份管理功能的解决方案，以简化操作并提高一致性。您的解决方案还应该支持您现在使用并打算在将来使用的基础架构和平台。

Red Hat Enterprise Linux

主要验证类型

- 普通密码、一次性密码和加强密码
- 远程身份验证拨入用户服务（RADIUS）
- 用于初始身份验证的公钥加密（PKINIT）

与其他身份管理系统集成

大多数企业已经为其 Linux 和 Windows 环境使用一个或多个身份管理系统。将这些系统集成到单个整体解决方案中有助您集中运维并确保整个企业的一致性。选择与 Microsoft Active Directory 等主流工具配合使用的身份管理解决方案，以跨混合环境管理身份。

策略管理

基于策略的身份管理方法可以帮助您提高一致性、效率和安全性。借助身份管理解决方案，您可以在集中式界面中设置和应用基于策略的控制，确保身份、访问和资源的正确配置。寻找以下特性和功能：

- 基于角色的访问权限控制（RBAC）和基于策略的访问权限控制功能
- 可自定义的身份和访问策略
- 身份验证和授权管理功能
- 会话记录、审核和日志记录功能

多因素身份验证

多因素身份验证（MFA）增加了额外一层安全防护，需要在授予访问权限之前进行多次检查以验证身份。选择的身份管理解决方案应支持可配置的身份验证类型，并支持通过硬件令牌和智能卡实现 MFA。

通用认证协议和标准

- X.509
- 自动化证书管理环境（ACME）
- 简单证书注册协议（SCEP）
- 安全套接字层（SSL）
- 传输层安全性（TLS）

认证管理

数字证书包含验证用户、应用、网站和其他主体的身份所需的信息。应根据最低权限原则创建、监控、更新和停用数字证书。选择可提供以下功能的身份管理解决方案：

- 完整的用户、主机和服务证书的生命周期管理。
- 支持通用协议和标准。
- 自动跟踪证书的到期日期，以确保及时续订。
- 支持公钥基础架构（PKI）身份验证。

单点登录

每个服务、设备和服务器都需要单独的访问权限身份验证。单点登录（SSO）系统通过使用中央身份服务，使服务器可以检查经验证的用户，从而简化了访问流程。用户进行一次身份验证，即可访问多个服务。选择的身份管理解决方案应支持 Web 身份验证以及您现在使用和计划将来使用的服务。

借助红帽企业 Linux 为零信任奠定基础

红帽提供了可用于设计、构建和管理零信任架构的基础技术。红帽 ® 企业 Linux 提供采用零信任模式所需的安全技术、控制、认证和支持。它满足本概述中讨论的所有操作系统要求，具备可信赖供应链、SELinux 访问控制、全系统加密策略、应用白名单、基于硬件的信任根、会话记录功能以及系统角色。它还包括内置 OpenSCAP 扫描程序和红帽智能分析预测性分析和修复服务。此外，红帽企业 Linux 符合多项政府安全标准，如 CC、FIPS 140、STIG 和 Section 508。

借助专家服务加快部署速度

红帽提供的服务可帮助您采用基于红帽平台和产品的零信任架构。

- 红帽开放创新实验室是一个沉浸式的驻留培训，它可将工程师与开源专家结对，以帮助您实现真正的业务成果。
- 红帽服务：零信任采用之旅是一项咨询服务，可帮助您评估当前情况并制定构建零信任架构的计划。

红帽企业 Linux 还包括红帽身份管理，可帮助您在整个环境中集中管理身份、实施安全控制并遵守安全标准。它具备实施零信任最佳实践所需的功能，同时可简化您的身份管理基础架构，还可通过标准接口与 Microsoft Active Directory、轻量级目录访问协议（LDAP）和其他第三方解决方案集成。红帽身份管理还支持基于证书的身份验证和授权技术。

红帽企业 Linux 和红帽身份管理可与红帽产品组合中的其他组件集成，为零信任架构提供了统一的基础。

- 红帽单点登录提供基于主流标准的网络单点登录功能。
- 红帽卫星是一款基础架构管理产品，旨在帮助您的红帽企业 Linux 环境保持高效运行、享受可靠保护并且符合各类标准。
- 红帽 Ansible® 自动化平台可提供一个企业框架，用于大规模构建、运维和管理 IT 自动化。
- 红帽认证系统是一个证书颁发机构，支持高级管理活动，如智能卡置备、自定义证书类型和受保护的机密存储。
- 红帽目录服务器是一个独立于操作系统且联网、可扩展的注册表，可让您针对分散目录拓扑，集中存储用户身份和应用信息。

后续步骤

- 了解有关红帽企业 Linux 安全防护的更多信息。
- 阅读有关红帽混合云安全防护方法的信息。

销售及技术支持

800 810 2100
400 890 2100

红帽北京办公地址

北京市朝阳区东大桥路 9 号侨福芳草地大厦 A 座 8 层　邮编：100020
8610 6533 9300

红帽官方微博　红帽官方微信

cn.redhat.com
F31712_0522_KVM