8 大技术诀窍帮您提高安全防护和合规性

降低风险、加强安全防护配置和政策，同时帮助您的企业遵从红帽® 企业 Linux® 的安全防护和合规性功能。

1 管理基于标准的合规性设置

系统范围的加密策略，为您基础架构中基于标准的合规性设置提供一致的实施和维护方法。

仅需要一个简化命令，您就可以选择内置加密策略，并在您系统上的所有应用中一致应用。此外，如果您有专门的法律合规性要求，则可以创建自定义策略以满足您的目标。

进一步了解合规性管理。

2 使用系统角色自动化安全防护配置

红帽企业 Linux 系统角色由红帽 Ansible® 自动化平台支持，允许管理员利用自动化在更短的时间内大规模安装和管理安全防护设置。

编写系统角色是为了跨各种环境与多个红帽企业 Linux 版本配合使用，从而使管理员能够使用红帽解决方案的最佳实践。使用单个命令或工作流，您可以配置新的安全防护设置并在所有系统上进行维护。

进一步了解安全自动化

3 集中式身份验证和授权

红帽企业 Linux 含有集中式身份管理（IdM）功能，您可以使用单一可扩展界面，跨整个数据中心对用户进行身份验证并实施基于角色的访问控制（RBAC）。红帽企业 Linux 中的身份管理还通过标准应用编程接口（API）与 Microsoft Active Directory、轻量级目录访问协议（LDAP）和其他第三方身份和访问管理解决方案集成。

您还可以使用基于证书的身份验证和授权技术集中管理服务的身份验证和授权。

进一步了解身份管理

4 自定义策略

安全增强型 Linux（SELinux）是在 Linux 内核实施的强制访问控制（MAC）。红帽企业 Linux 容器默认使用 SELinux 运行。这包括操作系统（OS）中额外的安全层，防止容器突发并覆盖系统上的底层主机操作系统或其他容器。Udica 允许系统管理员和容器开发人员分析正在运行的容器，并使用特定于容器的 SELinux 规则自动生成策略。这简化了策略编写，通过消除使用超级用户权限运行容器的需求来降低风险。

尝试并进一步了解策略锁定

5 使用最短停机时间修补系统

红帽免费为扩展更新支持（EUS）版本中被评为关键或重要的通用漏洞披露（CVE）提供内核实时补丁。内核实时修补（KLP）允许您修补正在运行的内核，在不重启系统的情况下立即解决漏洞，从而在不危害安全性的情况下最大限度地减少停机时间。

尝试并进一步了解 KLP

6 大规模管理安全防护和合规性

红帽企业 Linux 订阅包含红帽智能分析功能，无需额外付费，这款软件即服务（SaaS）产品可为用户提供有关其部署的可操作安全防护数据。发现并解决操作和漏洞风险，更快地扫描系统以确定缺少哪些补丁，然后确定优先级，明确首先应用哪些关键补丁。您可以从单个 Web 界面创建、修改、实施和维护所有红帽企业 Linux 系统的安全防护配置策略。此外，您还可以通过红帽智能管理订阅，从红帽智能分析执行、扩展和自动化修复计划。

进一步了解合规性

7 记录系统活动，支持合规性目标

红帽企业 Linux 包括会话记录，其所具有的审计和日志记录功能可以帮助安全管理员捕获系统上选定用户组的按键和活动。该数据与所有其他活动记录在同一系统日志或日志文件中，并且可以使用回放工具中的重播和暂停功能进行分析和关联。

尝试使用会话记录

8 阻止执行未经授权的应用

应用许可列表可以减少潜在的攻击途径，并防止恶意应用在您的系统上执行。文件访问权限策略守护进程（fapolicyd）提供内置的应用许可名单，它只允许用户在系统上运行经过批准的可执行文件。系统管理员可以使用默认策略配置 fapolicyd，或构建自己的 fapolicyd，从而防止未经授权的应用运行。

进一步了解应用许可名单

关于红帽

红帽帮助客户跨环境实现标准化、开发云原生应用，并通过一流的支持、培训和咨询服务，实现复杂环境的集成、自动化、安全防护和管理。

红帽官方微博　红帽官方微信

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

cn.redhat.com
O-F31208