

红帽公司

RedHat（红帽）公司（NYSE: RHT）是全球开源解决方案领导者，也是标准普尔 500 指数成员。总部位于美国北卡罗来纳州的罗利市。红帽公司依托社区力量为客户提供稳定可靠及高性能的云技术、Linux、中间件、存储和虚拟化产品和服务。红帽的开放源码模式提供跨物理、虚拟和云端环境的企业运算解决方案，以帮助企业降低成本并提升效能、稳定性与安全性。

- ✓ 全球第一大开源软件公司
- ✓ 目前世界上最资深的开放源代码提供商
- ✓ 基于开源软件的商用 IT 产品和解决方案的全球排名第一的提供商
- ✓ 全球第一个超过 30 亿美元收入的开源公司
- ✓ 两次登上《福布斯》杂志“全球最具创新力企业”榜单
- ✓ 福布斯 2019 年全球最佳雇主第 3 名（#1 Google; #2 Microsoft; #3 Red Hat; #4 Apple; #5 SAP）
- ✓ 史无前例地连续 71 个季度实现营收增长，是全球为数不多的在云计算业务中经营收入和自由现金流双增长的公司

红帽开源解决方案遍及世界各地最高标准的数据中心和云端：

- ✓ 超过 90% 的世界财富 500 强企业使用红帽产品和解决方案
- ✓ 100% 世界《财富》500 强中的航空公司
- ✓ 100% 世界《财富》500 强中的电信服务提供商
- ✓ 100% 世界《财富》500 强中的商业银行
- ✓ 100% 世界《财富》500 强中的医疗保健公司

红帽培训与认证

红帽公司同时也为全球客户或通过领先合作伙伴为客户提供技术支持、培训和咨询服务。红帽培训提供了数十门涵盖 5 大技术领域（云计算、存储、虚拟化、中间件、操作系统）的专业课程。红帽认为将培训作为部署和维护战略的一部分，企业可以实现开源技术价值和性能的最大化。

红帽认证是由红帽公司推出并提供的安全可靠、值得信赖的全球认证服务。自 1999 年以来，红帽认证项目成功实现了培养和验证 IT 人士专业技能的重要目标。红帽认证与行业其他认证的区别就在于其安全严格、注重动手实践的测试过程。红帽认证考试采用上机实际操作形式，考生必须通过执行实际任务来展示个人技能，就像在日常工作一样使用应用程序或编写代码。简言之，考生必须充分展示个人技术熟练水平，才能通过某项技术或产品的相关认证。红帽负责考试的安全和监考事宜，因此认证在业内的诚信度和声誉显赫。

红帽公司针对红帽认证制定了完善的专业评估与认证标准，其认证主要包括基础架构技术方向的红帽认证系统管理员（RHCSA）、红帽认证工程师（RHCE）以及企业应用开发方向的红帽认证 JBoss 开发员（RHCJD）和红帽认证企业应用开发者（RHCEAD）；红帽认证企业微服务开发者（RHCEMD）以及两个方向上的红帽认证架构师（RHCA）。

红帽企业培训金字塔



- 获得**红帽认证系统管理员 (RHCSA)** 的 IT 专业人士, 具备红帽企业 Linux 环境所需的核心系统管理技能。报考人员必须成功通过红帽认证系统管理员 (RHCSA) 考试 (EX200) 方可获得此项专业技能认证。
- **红帽认证工程师 (RHCE)** 是指具备以下能力的红帽认证系统管理员 (RHCSA): 实现红帽®企业 Linux® 任务自动化、集成红帽新兴技术、应用自动化来提高效率和促进创新。
- **红帽认证架构师 (RHCA)** 是红帽的最高级别认证, IT 人员在通过红帽认证工程师 (RHCE®)、红帽认证企业微服务开发人员 (RHCEMD) 或红帽认证 JBoss® 开发人员 (RHCJD) 认证后, 还需再通过系统管理员和开发人员认证列表中的五项额外认证 (并保持有效认证状态) 方可获得。红帽提供两种不同的红帽认证架构师认证路径: 红帽基础架构认证架构师和红帽企业应用认证架构师。申请人可以同时选择这两条认证路径, 也可选择参加 RHCA 认证路径中未包含的考试。

红帽培训与认证的价值

- 在项目预算中增加 **1.5%** 的培训预算, 可以将项目成功率从 **50%** 提高到 **80%**。
- 企业为 IT 团队提供红帽®培训后的主要收益:
 - ✓ 基础架构管理效率提高 **20%**
 - ✓ 支持部门解决问题的速度加快 **50%**
 - ✓ 意外停机减少 **71%**
- 企业引入红帽®认证专业人员后的主要收益:
 - ✓ 服务器管理效率提高 **36%**
 - ✓ 支持部门工作效率提高 **61%**
 - ✓ 故障解决速度加快 **54%**
- 红帽认证可带来更多价值——投资分析: 3 年投资回报率为 **403%**。

数据来源: IDC InfoBrief: “充分发掘红帽解决方案的价值”。2018 年 6 月。 <https://www.redhat.com/en/resources/training-certification-idc-infobrief>

红帽核心课程概览

职能	认证方向	课程编码	课程名称	培训天数	培训点数	
企业Linux工程师方向	RHCSA (红帽认证系统管理员)	RH200	红帽系统管理一/二: 企业Linux核心系统管理 (带RHCSA考试)	5	16	
	RHCE (红帽认证工程师)	RH295	红帽系统管理三: 企业Linux自动化 (带RHCE考试)	5	13	
云化平台系统管理员方向	红帽 OpenStack 认证系统管理员	CL110	红帽OpenStack管理一: 云管理员的核心操作	5	13	
		CL210	红帽 OpenStack 管理二: 云管理员的基础架构配置	4	11	
		EX210	红帽 OpenStack 认证系统管理员考试	4 Hours	4	
	红帽 OpenStack 认证工程师	CL310	红帽OpenStack 管理三: 网络和构造NFV	4	11	
		EX310	红帽OpenStack认证工程师考试	3 Hours	4	
	红帽 Ceph 存储管理认证专家	云化定向技术深入培训课程	Ceph125	红帽Ceph存储架构和管理	4	11
			EX125	红帽Ceph存储管理专业技能考试	3 Hours	4
		云化定向技术深入培训课程	RH342	红帽企业 Linux 诊断和故障排除	4	12
			EX342	红帽企业 Linux 诊断和故障排除考试	4	4
			RH415	红帽安全: 物理机, 虚拟机和云端的Linux	4	12
			EX415	红帽Linux安全认证专家	3	4
	RH442	红帽企业性能调优	4	12		
EX442	红帽性能调优专业技能证书考试	4	4			
维护自动化工程师培训方向	红帽运维自动化最佳实践	RH447	红帽认证高级自动化专家: Ansible 最佳实践考试	4	12	
		EX447	高级自动化: Ansible 最佳实践	4	11	
容器化/PaaS化/DevOps化 开发运维一体化工程师培训方向	红帽 OpenShift 管理认证专家	DO285	容器、Kubernetes 和红帽 OpenShift 管理一	5	14	
		EX280	红帽认证OpenShift管理专业技能考试	3 Hours	4	
	红帽 OpenShift 应用开发认证专家	DO288	红帽OpenShift开发一: 容器化应用程序	3	9	
		EX288	红帽认证 OpenShift 应用开发专家考试	3 Hours	4	
	红帽 DevOps 能力提升课程	DO425	红帽安全: 容器和OpenShift	4	11	
		DO500	DevOps文化与与实践	5	14	
DO700	容器技术训练营	10	66			

红帽 OpenShift 核心课程推荐

课程编码	英文名称	中文名称	培训费用	培训时间
DO285	Containers, Kubernetes, and Red Hat OpenShift Administration I	容器、Kubernetes 和红帽 OpenShift 管理一	¥11,660.00	5 天
EX280	Red Hat Certified Specialist in OpenShift Administration Exam	红帽认证OpenShift管理专业技能考试	¥2,968.00	3 小时
DO288	Red Hat OpenShift Development I: Containerizing Applications	红帽OpenShift开发一: 容器化应用	¥9,328.00	4 天
EX288	Red Hat Certified Specialist in OpenShift Application Development Exam	红帽认证 OpenShift 应用开发专家考试	¥2,968.00	3 小时
DO425	Red Hat Security: Containers and OpenShift	红帽安全: 容器和OpenShift	¥9,328.00	4 天
EX425	Red Hat Certified Specialist in Security: Containers and OpenShift Exam	红帽认证安全专业考试: 容器和OpenShift	¥2,968.00	3 小时

红帽 OpenShift 核心推荐课程大纲

DO285 容器、Kubernetes 和红帽 OpenShift 管理一（5 天公开课）

课程介绍：

学习如何构建和管理 Linux 容器以及如何配置和管理 OpenShift 集群。

容器、Kubernetes 和红帽 OpenShift 管理一（DO285）将帮助您掌握有关构建和管理 Linux® 容器及红帽® OpenShift® 容器平台的核心知识。此课程以实操练习为主，将向您展示如何将示例应用部署到本地容器运行时或 OpenShift 集群，以及如何配置和管理 OpenShift 集群。如果您是开发人员、管理员或站点可靠性工程师，掌握这些技能会令您受益匪浅。

培训对象：

- 想要实现软件应用容器化的开发人员
- 刚开始接触容器技术和容器编排的管理员
- 考虑要在软件架构中采用容器技术的架构师
- 想详细了解 OpenShift 的系统管理员
- 想详细了解 OpenShift 的系统架构师
- 想要安装和配置 OpenShift 的架构师和开发人员

内容概要：

- 了解容器和 OpenShift 架构。
- 管理容器和容器镜像。
- 创建自定义容器镜像。
- 在 OpenShift 上部署应用及对应用进行故障排除。
- 以本地用户身份配置身份验证。
- 使用基于角色的访问权限控制来控制对项目的访问。
- 配置服务和容器网络。
- 使用标签和选择器来配置容器集的调度。
- 限制计算资源的使用。
- 扩展集群。
- 监控集群事件和警报。

课程大纲

- 容器技术简介
介绍应用如何在经过红帽 OpenShift 容器平台编排的容器中运行。
- 创建容器化服务
利用容器技术部署服务。
- 管理容器
修改预构建的容器镜像以创建和管理容器化服务。
- 管理容器镜像
管理容器镜像的整个生命周期（从创建到删除）。



- ❑ 创建自定义容器镜像
设计 Dockerfile 和编写代码，构建自定义容器镜像。
- ❑ 在 OpenShift 上部署容器化应用
使用 OpenShift 容器平台部署单容器应用。
- ❑ 部署多容器应用
部署使用多容器镜像容器化的应用。
- ❑ 探索红帽 OpenShift 容器平台
讲解 OpenShift 容器平台的架构。
- ❑ 验证集群
检查安装方法并验证新安装的集群的功能。
- ❑ 配置身份验证
利用身份提供商来配置身份验证。
- ❑ 控制对 OpenShift 资源的访问
定义并应用基于角色的访问权限控制，并利用 Secret 来保护敏感信息。
- ❑ 配置 OpenShift 网络组件
识别 OpenShift 容器平台软件定义网络的组件并配置其中一些组件。
- ❑ 控制容器集的调度
控制运行容器集的节点。
- ❑ 扩展 OpenShift 集群
控制 OpenShift 集群的规模。
- ❑ 执行集群更新
描述如何执行集群更新。
- ❑ 使用 Web 控制台管理集群
使用 Web 控制台管理红帽 OpenShift 集群。
- ❑ 进行综合复习
对面向企业使用的 OpenShift 集群进行验证、管理和故障排除。

培训成果：

本课程将帮助您了解基于容器的架构的潜力，带您快速踏上企业和数字化转型之路。容器和红帽 OpenShift 已迅速成为真正的敏捷开发和应用部署解决方案。本课程旨在培养安装、配置和管理红帽 OpenShift 容器平台所需的技能，以部署具有出色可用性、弹性和可扩展性的容器化应用。红帽 OpenShift 容器平台可实现快速应用开发和部署，并实现应用的跨环境可移植性，而且能够简化改编版或云原生应用的扩展、管理和维护。

完成本课程后，您应该能够掌握使用 Podman 创建和管理本地容器、新建 OpenShift 集群、执行集群的初始配置以及日常管理集群的技能。本课程的目标之一就是帮助您检测和解决后期遇到的常见问题。同时，您还应该具备以下技能：

- ❑ 安装 OpenShift 容器平台以创建简单集群。
- ❑ 配置和管理 OpenShift 主结点和节点。
- ❑ 利用简单的内部身份验证机制来保护 OpenShift。
- ❑ 控制对于 OpenShift 资源的访问。
- ❑ 利用“源至镜像”（S2I）功能在 OpenShift 上部署应用。
- ❑ 配置和管理 OpenShift 容器集、服务、路由、机密和其他资源。

DO288 OpenShift 企业开发一：容器化应用（3 天 公开课）

课程介绍：

本课程将学习通过 OpenShift 集群来设计、构建和部署容器化应用，动手实验包括编写容器原生应用和迁移现有应用等，课程包含将应用从容器镜像、Dockerfiles 和源代码部署至 OpenShift 集群，利用 OpenShift Web 控制台和 OpenShift CLI 来管理应用，将配置数据和机密信息注入应用，发布应用容器镜像至外部注册表，管理应用构建版本并生成创建钩子，从 OpenShift 模板创建应用，管理应用部署，将应用迁移至容器和微服务等知识点。

培训对象：

有兴趣采用容器作为应用部署首选方法的软件开发人员和软件架构师。红帽建议学员应事先已获得红帽认证系统管理员资历，或具有同等的红帽企业 Linux 系统管理经验。

内容概要：

- 将应用从容器镜像、Dockerfiles 和源代码部署至 OpenShift 集群。
- 利用 OpenShift Web 控制台和 OpenShift CLI 来管理应用。
- 将配置数据和机密信息注入应用。
- 将应用容器镜像发布至外部注册表。
- 管理应用构建版本并生成钩子。
- 从模板创建应用。
- 管理应用部署。
- 使用探针监视应用是否正常运行。
- 将应用迁移至容器和微服务。

培训成果：

本课程旨在培养将软件应用容器化并部署至红帽 OpenShift 容器平台集群所需的技能。这些技能有助于学员利用平台和架构在企业中推广 DevOps 文化。红帽 OpenShift 容器平台为开发人员提供使用 DevOps 模型（如持续集成和部署）部署应用的自调配环境。并且提供许多语言和数据库运行时、容器化红帽中间件等，以减少开发人员对自定义容器化的需要，从而缩短产品上市时间。学习完本课程后，学员将能够对应用进行容器化操作，并在红帽 OpenShift 容器平台上进行部署。同时还应该具备以下技能：

- 将应用部署至 OpenShift 集群，并通过命令行客户端和 Web 控制台进行管理。
- 设计和构建应用容器，以便成功部署至 OpenShift 集群。
- 将容器镜像发布至企业注册表。
- 使用源至镜像功能构建容器化应用。
- 使用 OpenShift 模板创建应用。
- 从单个完整应用中提取服务，并将其作为微服务部署于集群中。
- 迁移应用以便在 OpenShift 集群上运行。

DO425 红帽安全：容器和 OpenShift（4 天公开课）

课程介绍：

学习如何减轻和管理 OpenShift 容器基础架构面临的威胁。红帽安全：保护容器和 OpenShift (DO425) 旨在帮助基础架构管理员和安全专家学习如何识别和减轻 OpenShift 容器基础架构面临的威胁。本课程还介绍了如何针对现代容器化应用和

软件定义网络，实施和管理安全架构、策略和程序。您将学习以下内容：使用安全可靠的容器镜像、镜像仓库和源代码；管理网络和存储隔离；实施应用单点登录；配置适当的安全限制措施和基于服务角色的访问控制。您还将了解现有核心 Linux 技术（如命名空间、cgroup、seccomp、功能和 SELinux）能够如何为强大且成熟的主机环境提供高度安全的容器。

培训对象：

本课程专为利用红帽企业 Linux 系统和红帽 OpenShift 容器平台，负责设计、实施、维护和管理容器化应用安全性的专业人员而设计，包括：

- 系统管理员
- IT 安全管理员
- IT 安全工程师
- DevOps 工程师
- 云开发人员
- 云架构师

内容概要：

- 学习 Linux 多租户隔离和最小特权技术。
- 调查可信的存储库，以及签名和扫描镜像。
- 安全防护持续集成和持续开发（CI/CD）流程。
- 集成 Web 应用单点登录。
- 自动化基于策略的部署工作。
- 配置安全环境限制（SCC）。
- 管理 API 访问控制。
- 提供安全网络 I/O。
- 提供安全存储 I/O。

培训成果：

容器和容器编排平台（如 OpenShift 和 Kubernetes），已在企业计算中越来越普及。而容器环境中也已开始出现新的攻击途径、漏洞和漏洞利用。安全防护对企业而言至关重要，而向容器化微服务的迁移颠覆了基于网络的传统安全模型。开发人员必须证明自己的代码、镜像和部署工作安全可靠。

本课程旨在帮助学员培养所需的技能，确保为不断发展的容器化应用和 OpenShift 项目提供持续强效的安全防护。

OpenShift 是一个基于容器的企业级应用平台，不仅提供红帽企业 Linux 成熟的安全功能，还提供额外机制来保障服务角色访问控制、强化构建流程、源镜像分层信任和受控部署管理。这些安全功能可以帮助企业有效降低安全漏洞的风险，避免因业务中断、品牌受损、失去客户和股东信任及事后补救带来的高昂成本。此外，企业还可借助本课程中的工具来检验是否符合客户、审计员或其他利益相关方设定的合规要求。学习本课程后，您应能够使用红帽 OpenShift 容器平台和红帽企业 Linux 中包含的安全技术来管理安全风险，并帮助满足合规性要求。同时，您还应该掌握以下技能：

- 使用推荐实践，确保用于容器部署的镜像来源可靠，包括使用安全的镜像仓库、签名镜像、安全访问协议和授权访问控制。
- 掌握并实施高级 SELinux 技术，以限制用户、流程和虚拟机的访问。
- 配置安全环境限制措施，以便控制容器集有权执行的操作并明确容器集有权访问的内容。
- 实施 Linux 计算机安全防护（seccomp）和 Linux 功能，以控制容器化应用的漏洞占用空间。
- 为 Web 应用实施和配置单点登录，包括通过 JWT 共享令牌。
- 掌握并实施网络隔离和加密技术，以隔离应用流量，仅允许授权访问。



Red Hat Training and Certification

- ❑ 实施和掌握存储管理技术，以隔离卷存储 I/O，仅允许授权访问。
- ❑ 观察并掌握如何在构建过程中纳入自动安全测试和漏洞扫描，避免向待部署的最终容器镜像中引入任何漏洞利用。
- ❑ 管理容器部署策略和配置，以控制应用配置、资源容量、容器关联和应用需求扩展。
- ❑ 管理 OpenShift 项目访问和配额，以保障私人 and 授权的自助服务访问，并限制恶意令牌和拒绝服务攻击的风险。