红帽 Kubernetes 高级集群管理

关键优势

- 借助自助服务置备，加速应用开发。
- 通过可自动交付应用的自助服务集群部署，使 IT 团队从手动置备中解放出来。
- 在更短时间内跨分布式集群部署传统应用和云原生应用，从而提高应用的可用性。
- 通过跨集群的集中实施策略，增强安全合规性。
- 通过统一的管理界面，降低运维成本。

前言

在将最新应用从开发环境转移到生产环境时，为了支持 DevOps 管道的持续集成/持续交付（CI/CD），拥有多个专用 Kubernetes 集群通常是合理的做法。随着企业为满足特定需求（如边缘部署、加快响应速度、降低延迟、减少资本支出（CapEx）、遵守数据驻留要求等）而添加新的集群，这种集群的蔓延趋势会不断继续下去。

无论企业是刚从单个集群起步，还是已在多集群环境中运行，都可能会面临一些棘手的难题，例如：

- 如何使用单个控制平面来管理驻留在本地或位于公共云环境上的多个集群的生命周期？
- 如何更便捷地了解集群运行状况及其对应用可用性的影响？
- 如何自动执行集群的置备和取消置备？
- 如何确保所有集群都符合相关标准和自定义策略？
- 如何获得有关配置偏差的警报并加以修复？
- 如何根据策略来自动放置工作负载？

红帽 Kubernetes 高级集群管理

红帽® Kubernetes 高级集群管理可跨多个数据中心和公共云环境，为集群和应用生命周期提供端到端管理、可见性和控制，同时改进整个 Kubernetes 域的安全性和合规性。

红帽 OpenShift® 是容器编排的理想选择，可让用户在标准且一致的控制平面中部署和管理容器。红帽 OpenShift 和红帽高级集群管理提供混合云管理平台和功能，可解决管理员和站点可靠性工程师（SRE）在跨各种环境工作时所面临的常见挑战，例如多个数据中心及运行 Kubernetes 集群的私有云和公共云环境，包括远程边缘站点。有些行业（如美国的公共部门）需要保持严格的合规性并支持美国联邦信息处理标准（FIPS）模式，而红帽高级集群管理能够满足这方面的需求。

有了红帽高级集群管理，企业可以从一个位置管理多个 Kubernetes 集群。企业可以在多种环境中置备新的红帽 OpenShift 集群，包括 Amazon Web Services（AWS）、微软 Azure、Google Cloud Platform（GCP）、微软 Azure Government（MAG）、AWS GovCloud、裸机、红帽 OpenStack® 平台、红帽虚拟化和 VMware vSphere 等环境。此外，也可以导入和管理现有的红帽 OpenShift 集群，例如 IBM Cloud 上的红帽 OpenShift、微软 Azure 红帽 OpenShift、红帽 OpenShift 专业版、红帽 OpenStack 平台上的红帽 OpenShift、IBM Z 上的红帽 OpenShift、IBM Power 上的红帽 OpenShift、Amazon 上的红帽 OpenShift、ARM 架构上的红帽 OpenShift。

红帽官方微博　红帽官方微信

红帽高级集群管理还可以导入和管理现有的公共云 Kubernetes 集群，如 Amazon Elastic Kubernetes Service（Amazon EKS）、IBM Cloud Kubernetes Service（IKS）、Azure Kubernetes Service（AKS）和 Google Kubernetes Engine（GKE）。

特性和优势

如需了解更多信息，请访问：redhat.com/clustermanagement。

借助多集群观测能力，监控多集群运行状况并进行优化

开箱即用的多集群仪表板，能够存储长期历史数据并提供对多集群运行状况和优化的概览，为 SRE 带来更好的运维体验。

表 1. 多集群观测能力的特性和优势

特性	优势
监控多集群运行状况	通过 Grafana，对单个集群和用户工作负载或聚合的多集群进行排序、筛选和扫描。使用开源的 Thanos 项目，进行可扩展的指标收集并长期保留数据。利用多个开箱即用的 Grafana 仪表板，获取 OpenShift 集群和非 OpenShift 集群（如 EKS、GKE、AKS 和 IKS）的运行状况指标。
自定义指标和仪表板	根据自定义指标和预定义指标来定制 Grafana 仪表板。定义集群或平台服务的服务级别目标（SLO），根据 SLO 目标衡量性能，并按照根本原因分析的需求进行动态调整，以在关键事件期间进行更深入的数据收集。
动态搜索	使用图形控制台或应用编程接口（API）来识别、排查和解决影响分布式工作负载的问题。应用 SRE 可以查看应用资源 YAML 并从部署中实时获取日志，从而缩短断定和解决问题的时间。通过可配置的数据收集来改进控制，为大规模环境和安全锁定提供机会，以限制从托管集群收集的信息。
通过用于红帽 OpenShift 的红帽智能分析进行分析	根据基于红帽 OpenShift 的遥测和红帽专业知识提供的分析，获取整个托管多集群的集群运行状况情报，并根据需要采取主动措施和修复操作。
自动将托管集群的警报转发到红帽高级集群管理中心	将集群运行状况指标和所有策略违规行为的集中警报发送到第三方工具（如 Slack 和 PagerDuty），从而更轻松地响应和排除故障。
全局中心	全局中心架构提供了跨多个中心的集中式策略合规性视图，即便是在多个区域数据中心有着大规模部署和/或严格划分的企业，也仍然能够从一个中央界面获得整个安全合规性态势的整体视图。

统一多集群生命周期管理

借助支持基础架构即代码（IaC）最佳实践和设计原理的开源编程模式，大规模且可靠一致地创建、升级和销毁 Kubernetes 集群。

表 2. 统一多集群生命周期管理的特性和优势

特性	优势
集群生命周期管理	利用开源Hive API，提升集群生命周期管理 Day 1 运维体验。使用红帽高级集群管理控制台，创建和升级新的红帽 OpenShift 集群，或者导入现有的 OpenShift 和托管式 Kubernetes 集群。
受支持的云提供商	红帽高级集群管理支持在 AWS、微软 Azure、Google Cloud Platform（GCP）、微软 Azure Government、AWS GovCloud、裸机、红帽 OpenStack 平台、红帽虚拟化和 VMware vSphere 上创建 OpenShift 集群。
增强的集群生命周期管理	充分利用各种功能，如工作池扩展（借助自动扩展配置）、集群 Hibernate®（技术预览）和集群池恢复（技术预览）等，加快集群部署速度。将集群分组为多个集群集合，以更清晰地定义访问控制权限。
红帽 Ansible® 自动化平台集成	在集成过程中，借助 Kubernetes 多集群引擎 Operator 提供的强大多集群管理层，加上红帽高级集群管理和 stolotron.core Ansible 内容集，大幅增强 Playbook，在 Kubernetes 多集群上实现直观明了、安全至上的 Ansible 原生访问。使用 pre-hook 和 post-hook，在红帽高级集群管理中调用 Ansible 来进行集群生命周期管理。
借助 Submariner，实现多集群联网	借助 Submariner，为跨多个集群部署的应用组件提供丰富的多集群联网功能。降低跨集群部署应用组件的复杂性和联网要求。
托管控制平面	通过大规模托管和置备容器化红帽 OpenShift 控制平面，有效解决成本、占用空间、置备时间、跨云环境可移植性等问题，并在管理与工作负载之间实现明确的关注点分离。此功能通常适用于裸机和红帽 OpenShift 虚拟化，也作为技术预览面向 AWS 提供。
用于裸机部署的中央基础架构管理（CIM）	使用自助服务模式，允许基础架构所有者为开发人员提供对裸机基础架构资源的访问权限，以便置备 OpenShift 集群。使用适当的基础架构环境，以便运维人员轻松地维护裸机主机清单。

基于策略的监管、风险和合规保障

应用基于策略的监管方法来自动监控，确保与安全性、弹性和软件工程相关的控制措施处于所需的最佳实践配置状态，并按照行业合规标准或自行规定的企业标准来运行。

表 3. 基于策略的监管、风险和合规保障的特性和优势

特性	优势
开箱即用的策略模板，改进安全性、弹性和配置管理	使用预构建的策略模板，实施有关 Kubernetes 配置（如 etcd 加密）、身份和访问管理（IAM）及证书管理的策略，并在集群中部署和配置各种 operator，如 Compliance Operator、Gatekeeper/Open Policy Agent（OPA）和 Container Security Operator。利用开源策略集合存储库，通过 GitOps 实施基于策略的监管来满足内部和外部标准。
监管和风险仪表板	使用监管和风险仪表板，查看和管理所有集群和应用中的安全风险和策略违规情况。获取有关违规历史记录的详细信息。从红帽高级集群管理中心集中访问托管集群的详细信息，深入了解违规详情。
自定义策略违规监管视图	自定义各种合规标准的策略、监管仪表板视图，还可自定义受特定标准影响最大的控制措施的视图。
开源的可扩展策略框架和策略集合存储库	借助策略集合存储库，充分利用上游协作贡献的策略。
与 Gatekeeper 和开源策略代理（OPA）集成	获取享有全面支持的 Gatekeeper 和 OPA Operator，支持使用合规性策略将 Gatekeeper Operator 部署到多集群中。在多集群中启动 Gatekeeper 控制，以实施各种各样的 OPA 策略。集中查看和深入研究所有 Gatekeeper 和 OPA 策略的违规情况。
通过策略集实现更高效的策略管理	针对特定用途（例如，红帽 OpenShift 平台 Plus 部署、红帽高级集群管理强化、托管集群强化、分组 Gatekeeper 策略、PCIStoreFront、HIPAA 后端等），对策略进行分组，从而大规模组织、管理和实施针对集群的策略或策略集，确保用户获得更加友好的体验。预配置的策略集可通过 GitOps 获得，作为使用此功能的起点。
与 Kyverno 策略集相集成	通过 Kyverno 策略集，获得增强的准入控制功能和动态适应功能。利用策略生成器提供的集成，通过 Kyverno 集成来生成和验证 Kubernetes 资源（Kyverno 由社区提供支持）。
与 Compliance Operator 相集成	在多集群中大规模部署 Compliance Operator，使用红帽高级集群管理来实施各种安全配置集以满足合规性标准，例如 E8 Essential 扫描。集中查看和深入研究所有安全配置集的违规情况。

特性	优势
Ansible 自动化平台集成	将 Ansible 自动化平台与红帽高级集群管理相集成，以自动修复不合规情况，并收集有关集群的审计信息进行分析，从而针对红帽高级集群管理检测到的策略违规情况主动采取措施。
红帽 OpenShift 平台 Plus 策略集	通过创建由策略生成器开发的策略集，使用红帽高级集群管理控制台在中心集群和托管集群之间一致地部署 OpenShift 平台 Plus 组件，从而获得一致的体验。
策略生成器	可通过 OpenShift GitOps 从现有的 Kubernetes 配置、Gatekeeper 和 Kyverno 策略中自动生成和部署策略。
使用模板化策略来加强安全性和边缘可扩展性	使用模板化策略及其底层加密（来自机密和保护功能），从中心集群到托管集群，安全地交付和实施内容。

高级应用生命周期管理

利用集成到现有 CI/CD 管道和监管控制措施中的放置规则，应用开放标准并部署应用。

表 4. 高级应用生命周期管理的特性和优势

特性	优势
应用拓扑视图	更全面地了解应用拓扑，并轻松查看服务端点和容器集的运行状况，以及所有连接的依赖项，如镜像版本、相关的放置规则、Kubernetes 资源和 ConfigMap，无论应用是在红帽高级集群管理、红帽 OpenShift 还是 ArgoCD 和 Flux 等 GitOps 工具中创建的。
频道和订阅	通过订阅不同的工作负载（资源）频道（如 GitHub、Helm 存储库和 ObjectStore 类型），自动将应用部署到特定的集群。
放置规则	根据放置规则定义和时间窗口，在多集群中快速部署工作负载，或仅部署到特定的集群，以控制应用的部署时间和位置。
Ansible 自动化平台集成	通过 pre-hook 和 post-hook Ansible 作业模板和工作流，在 Kubernetes 之外自动执行与应用部署相关的一切。例如，使用 Ansible 自动化平台集成，自动执行并配置网络、数据库、负载平衡器和防火墙。
应用构建器	创建直观的应用，使用基于表单的输入和上下文帮助来引导用户定义应用组件，而无需直接处理 YAML。
OpenShift GitOps/Argo CD 集成	利用红帽高级集群管理，使 OpenShift GitOps/Argo CD 在集群上线或导入时自动交付内容。红帽高级集群管理策略与 Argo CD 协同配合，确保对合规性和配置事宜进行大规模管理和维护，从而实现更紧密的 CI/CD 一致性。在高级集群管理应用拓扑视图中，查看由 Argo CD 部署的应用并进行故障排查。直接从红帽高级集群管理控制台操作，为在 Argo 中注册的集群创建应用集对象。

大规模边缘管理

借助单节点 OpenShift 集群和红帽高级集群管理，实现持续扩展，并确保在高延迟、低带宽的边缘用例中也能具有一定的可用性。

表 5. 大规模边缘管理的特性和优势

特性	优势
增强的可扩展性	单个红帽高级集群管理中心可以管理多达 3500 个 OpenShift 集群。此外，IPV6 双栈支持可简化对于横向扩展边缘架构的管理。这些特性可确保在低带宽、高延迟的连接和断网站点中实现一定的可扩展性。
零接触置备	使用红帽高级集群管理及本地辅助安装程序和拓扑感知生命周期管理器（TALM）来进行大规模集群部署，满足电信和边缘场景的需求。
单节点 OpenShift 管理	为单节点 OpenShift 集群赋予完整的管理能力，满足边缘用例的基本功能需求。
中心端策略模板	允许策略引用来自中心资源的数据，减少大规模管理场景中的策略数量。TALM Operator 使用红帽高级集群管理策略对目标集群执行更改。

业务连续性

使用红帽高级集群管理和更广泛的红帽产品组合，确保业务所依赖的应用和有状态应用始终正常运行。

表 6. 业务连续性的特性和优势

特性	优势
红帽高级集群管理中心的备份和恢复	使用基于 OpenShift API for Data Protection（OADP）的备份解决方案，备份中心配置并恢复到其他中心集群。确保管理配置不会丢失，并保障业务的连续性，同时应用也能继续在多集群中运行。
红帽 OpenShift 数据基础用于灾难恢复（DR）、Metro-DR 和区域性 DR	利用 OpenShift 数据基础和红帽高级集群管理，为有状态应用提供可靠的多站点、多集群灾难恢复策略。OpenShift 数据基础可以确保一致、频繁地复制应用数据卷和持久卷（PV）。使用红帽高级集群管理设置的 DR Operator，可以自动执行 DR 故障转移和故障恢复流程，与区域性 DR 异步实现最低恢复点目标（RPO），或与 Metro-DR 同步实现零 RPO。
使用 VolSync 进行持久卷复制	提供事先规划好的跨集群应用迁移策略，确保业务所依赖的有状态应用的弹性。在使用其他供应商的存储或异构存储产品时，用户也可以使用 VolSync 来创建自己的 DR 解决方案。

技术规格

中心集群

- 基于 Operator 的安装
- 可在 OperatorHub.io 上获得
- 需要红帽 OpenShift 容器平台 4.12 或更高版本

托管集群

- 完整的生命周期管理：任何 OpenShift 容器平台 4.12 及以上版本：
  - 在 AWS、微软 Azure、Google Cloud Platform、微软 Azure Government、AWS GovCloud、VMware vSphere、红帽 OpenStack 平台、OpenShift 虚拟化和裸机上，管理红帽 OpenShift 服务
  - 托管控制平面提供商：AWS（技术预览）、裸机和 OpenShift 虚拟化（ KubeVirt）
- 导入和管理：
  - 红帽 OpenShift 容器平台 3.11
  - IBM Power 上的红帽 OpenShift
  - IBM Z 上的红帽 OpenShift
  - IBM Cloud 上的红帽 OpenShift
  - AWS 上的红帽 OpenShift 服务
  - 微软 Azure 红帽 OpenShift
  - 红帽 OpenShift 专业版
  - ARM Developer 上的 OpenShift
- 对托管式 Kubernetes 集群的有限生命周期支持：
  - Amazon Elastic Kubernetes 服务（Amazon EKS）
  - Azure Kubernetes 服务（AKS）
  - IBM Cloud Kubernetes 服务（IKS）
  - Google Kubernetes 引擎（GKE）
- 红帽高级集群管理为导入的集群提供可观测性、应用生命周期管理、基于策略的管理和安全至上的网络通信。
- 红帽高级集群管理提供完整的集群生命周期管理（创建、升级、销毁），并为 OpenShift 容器平台集群提供额外的安全合规功能。

高可用性

- 支持 OpenShift 容器平台可用性区域

资源要求

- 3 个主控机、3 个基础架构节点、6 个 vCPU、16GB RAM

关于红帽

红帽是世界领先的企业开源软件解决方案供应商，依托强大的社区支持，为客户提供稳定可靠且高性能的 Linux、混合云、容器和 Kubernetes 技术。红帽致力于帮助客户开发云原生应用，集成现有和新的 IT 应用，并实现复杂环境的自动化和管理。作为深受《财富》500 强公司信赖的技术顾问，红帽旨在提供一流的支持、培训和咨询服务，努力将开放创新的优势赋能于各行各业。红帽作为全球企业、合作伙伴和社区网络的互连枢纽，致力于帮助企业发展、转型，并拥抱数字化未来。

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
#583501_1023