Red Hat Advanced Cluster Management for Kubernetes 2.3

发行注记

了解有关发行说明中关于 GDPR 和 FIPS 准备功能的信息，新功能、勘误更新、已知问题、弃用和删除以及产品注意事项。

Last Updated: 2023-02-24

Red Hat Advanced Cluster Management for Kubernetes 2.3 发行注记

了解有关发行说明中关于 GDPR 和 FIPS 准备功能的信息，新功能、勘误更新、已知问题、弃用和删除以及产品注意事项。

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律通告

摘要

了解有关发行说明中关于 GDPR 和 FIPS 准备功能的信息，新功能、勘误更新、已知问题、弃用和删除以及产品注意事项。

目录

第 1 章 发行注记 **5**

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 的新内容 5

1.1.1. Web 控制台 5

1.1.1.1. Observability（可观察性） 5

1.1.2. Clusters 6

1.1.2.1. 集群（技术预览） 7

1.1.3. 应用程序 7

1.1.4. 监管 8

1.2. 勘误更新 8

1.2.1. Errata 2.3.12 8

1.2.2. Errata 2.3.11 8

1.2.3. Errata 2.3.10 8

1.2.4. 勘误 2.3.9 8

1.2.5. Errata 2.3.8 8

1.2.6. Errata 2.3.7 9

1.2.7. Errata 2.3.6 9

1.2.8. 勘误 2.3.5 9

1.2.9. Errata 2.3.4 9

1.2.10. Errata 2.3.3 9

1.2.11. Errata 2.3.2 10

1.2.12. Errata 2.3.1 10

1.3. 已知问题 10

1.3.1. 已知的与安装相关的问题 10

1.3.1.1. 与 OpenShift Container Platform 版本 4.9 的兼容性问题 10

1.3.1.2. 从 2.2.x 升级到 2.3.1 版本无法进行 10

1.3.1.3. 从 2.3.0 升级到 2.3.1 会失败并显示 ImagePullBackOff 错误 11

1.3.1.4. OpenShift Container Platform 集群升级失败的状态 11

1.3.2. 已知的与 Web 控制台相关的问题 11

1.3.2.1. Cluster 页面和搜索结果之间节点的不同 11

1.3.2.2. LDAP 用户名是区分大小写的 11

1.3.2.3. Firefox 的较老版本可能无法显示控制台的功能 11

1.3.2.4. 无法使用带有空空格的值搜索 12

1.3.2.5. 在注销用户 kubeadmin 时会出现一个额外浏览器标签页并显示空白页面 12

1.3.2.6. 不再显示 Secret 的内容 12

1.3.2.7. searchcustomization 存储大小的限制 12

1.3.3. 已知的可观察性问题 12

1.3.3.1. Observability endpoint operator 无法拉取镜像 12

1.3.3.2. 没有来自 ROKS 集群的数据 12

1.3.3.3. ROKS 集群没有 etcd 数据 12

1.3.3.4. search-collector pod 的高 CPU 使用率 12

1.3.3.5. 因为证书无效，搜索 pod 无法完成 TLS 握手过程 13

1.3.3.6. Grafana 控制台中没有指标数据 13

1.3.3.7. 在升级到 2.3.2 后集群会降级 13

1.3.3.8. Observability 有状态集在断开连接的环境中使用错误的镜像 13

1.3.3.9. Error ingesting out-of-order samples 13

1.3.4. 已知的与集群管理相关的问题 13

1.3.4.1. 删除受管集群时受管集群的命名空间处于终止状态 13

1.3.4.2. 无效的集群部署会出现创建 14

1.3.4.3. 使用 Infrastructure Operator 进行集群置备失败 14

1.3.4.4. Google Cloud Platform 上的集群置备失败 15

1.3.4.5. 使用不同名称重新导入后 local-cluster 状态为离线 15

1.3.4.6. 在 Ansible 集群创建失败后，集群状态在控制台的不同视图中有所不同 16
1.3.4.7. 可能不会自动重新导入 local-cluster 16
1.3.4.8. 受管集群的集群部署处于终止状态 16
1.3.4.9. 无法手动删除受管集群命名空间 16
1.3.4.10. 无法跨架构创建集群 17
1.3.4.11. 无法通过更改标签将集群重新分配给集群集 19
1.3.4.12. 无法使用 Ansible Tower 与 IBM Power hub 集群集成 19
1.3.4.13. 升级到 2.3 后无法更改集群中的凭证 19
1.3.4.14. 无法在 OpenShift Container Platform 版本 4.8 上创建裸机受管集群 19
1.3.4.15. 创建资源下拉列表错误 19
1.3.4.16. hub 集群和受管集群的时钟未同步 19
1.3.4.17. 不支持导入 IBM OpenShift Container Platform Kubernetes Service 集群的特定版本 20
1.3.4.18. 分离 OpenShift Container Platform 3.11 不会删除 open-cluster-management-agent 20
1.3.4.19. 不支持为置备的集群进行自动 secret 更新 20
1.3.4.20. 无法以非 root 用户身份运行 management ingress 21
1.3.4.21. 无法在搜索中查看受管集群的节点信息 21
1.3.4.22. 销毁集群的进程没有完成 21
1.3.4.23. 无法使用控制台在 OpenShift Container Platform Dedicated 上升级 OpenShift Container Platform 受管集群 22
1.3.4.24. 工作管理器附加搜索详情 22
1.3.4.25. IBM Power hub 集群不支持 Argo CD 22
1.3.4.26. 非 Red Hat OpenShift Container Platform 受管集群必须启用 LoadBalancer 22
1.3.5. 已知的与应用程序管理相关的问题 23
1.3.5.1. 应用程序搜索未定义错误 Application 表 23
1.3.5.2. 应用程序搜索未定义错误 Argo CD 23
1.3.5.3. 代理的应用程序创建过程中没有分支信息 23
1.3.5.4. 应用程序 Argo 搜索未定义错误 24
1.3.5.5. 带有多个订阅的应用程序拓扑集群没有正确分组 24
1.3.5.6. 应用程序拓扑订阅的切换 24
1.3.5.7. 应用程序 Ansible hook 独立模式 24
1.3.5.8. 在本地集群限制时部署应用程序 26
1.3.5.9. 命名空间频道订阅处于失败状态 26
1.3.5.10. 为应用程序编辑角色错误 26
1.3.5.11. 编辑放置规则错误的角色 27
1.3.5.12. 在更新的放置规则后没有部署应用程序 27
1.3.5.13. Subscription operator 不会创建一个 SCC 28
1.3.5.14. 应用程序频道需要唯一的命名空间 28
1.3.5.15. Ansible Automation Platform（早期访问）2.0.0 作业失败 29
1.3.5.16. 应用程序名称要求 29
1.3.5.17. 应用程序控制台表 29
1.3.6. 已知的监管问题 29
1.3.6.1. 即使没有新的策略违反情况启动自动化过程，Ansible 自动化作业还会继续每小时运行一次， 29
1.3.6.2. PlacementRule matchExpression 没有使用新的 matchLabel 删除 30
1.3.6.3. IAM 策略控制器不考虑组用户 31
1.3.6.4. 无法注销 31
1.3.6.5. Administrator 集群管理器无法创建自动化策略 31
1.3.6.6. Gatekeeper operator 安装失败 32
1.3.6.7. 当命名空间处于 Terminating 状态时，配置策略列出了 complaint 32
1.4. 弃用和删除 32
1.4.1. API 弃用和删除 32
1.4.2. Red Hat Advanced Cluster Management 弃用 33
1.4.3. 删除 33
1.5. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 平台针对 GDPR 的注意事项 34

1.5.1. 备注 34
1.5.2. 内容表 34
1.5.3. GDPR 35
1.5.3.1. 为什么 GDPR 很重要？ 35
1.5.3.2. 更多关于 GDPR 的信息 36
1.5.4. 针对 GDPR 的产品配置 36
1.5.5. 数据生命周期 36
1.5.5.1. Red Hat Advanced Cluster Management for Kubernetes 平台的数据流类型 37
1.5.5.2. 用于在线联系的个人数据 37
1.5.6. 数据收集 37
1.5.7. 数据存储 38
1.5.8. 数据访问 39
1.5.8.1. 身份验证 39
1.5.8.2. 角色映射 40
1.5.8.3. 授权 40
1.5.8.4. Pod 安全性 40
1.5.9. 数据处理 40
1.5.10. 数据删除 41
1.5.11. 限制使用个人数据的能力 41
1.5.12. 附录 42

第 1 章 发行注记

Red Hat Advanced Cluster Management 的 2.1 版本*已被删除*且不再被支持。其文档可能仍然可用，但是它已被弃用，将没有任何可用的勘误或其他更新。文档的早期版本也不被支持。

- Red Hat Advanced Cluster Management for Kubernetes 的新内容
- 勘误更新
- 限制和已知问题
- 弃用和删除
- Red Hat Advanced Cluster Management for Kubernetes 针对 GDPR 的注意事项

1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 的新内容

Red Hat Advanced Cluster Management for Kubernetes 为您提供了整个 Kubernetes 域的可见性，以及内置监管、集群生命周期管理和应用程序生命周期管理功能。在这个版本中，您可以在更多环境中移至管理集群，应用程序的 GitOps 集成等等。

重要：一些功能和组件作为技术预览发布。

了解更多本发行版本的新内容：

- 欢迎使用 Red Hat Advanced Cluster Management for Kubernetes 包括了 Red Hat Advanced Cluster Management for Kubernetes 的概述。
- 开源的 *Open Cluster Management* 存储库可用于开源社区的交互、增长和贡献。要参与，请参阅 open-cluster-management.io。您还可以访问 GitHub 存储库来获取更多信息。
- 多集群架构包括了与该产品主要组件相关的详细信息。
- 开始使用指南中包括了与开始使用的常见任务相关的信息，以及*故障排除指南*。
- Web 控制台
  - Observability（可观察性）
- Clusters
- 应用程序
- 监管

1.1.1. Web 控制台

- 侧边导航栏的变化与其他产品一致，提供更好的用户体验。通过导航，您可以访问各种产品功能。使用标头，您可以更轻松地访问 Red Hat OpenShift Container Platform、Search、*Configure client* 页面，查看 *About modal* 等。
- **技术预览：** 您可以从导航栏访问 Visual Web Terminal。

1.1.1.1. Observability（可观察性）

- Red Hat Advanced Cluster Management observability 服务支持 Grafana 的 7.4.2。如需更多信息，请参阅 Observability 服务部分。
- 现在，您可以为每个组件配置可观察存储大小。如需更多信息，请参阅创建 MultiClusterObservability CR。
- observability 的 API 存储版本现在是 **v1beta2**。使用 **v1beta2** 用于版本，检索 **v1beta1** 和 **v1beta2** 自定义资源定义。
- 您可以在可观察服务中添加记录规则，以指定来自聚合查询表达式的新指标。如需更多信息，请参阅添加自定义指标。
- 现在，您可以在 **MultiClusterObservability** 自定义资源中自定义**高级**配置。如需更多信息，请参阅添加*高级*配置。
- 现在，您可以删除默认指标。如需更多信息，请参阅删除默认指标。
- 现在，您可以在 Red Hat Insights 中收到连接的集群中的潜在问题的信息。如需更多信息，请参阅Red Hat Insights 的 Observability 。
- 现在，您可以从 Grafana 控制台查看 *etcd* 仪表板。请参阅查看 etcd 表。
- 您可以识别来自带有 SNO 标签的单个节点 OpenShift (SNO) 集群的指标。如需更多信息，请参阅查看和探索数据。
- 现在，您可以使用自带的 (BYO) 可观察证书认证机构 (CA) 证书。如需更多信息，请参阅BYO Observability 证书颁发机构 (CA) 证书。
- 现在，您可以为可观察 pod 更新副本数量。如需更多信息，请参阅从控制台更新 *multiclusterobservability* CR 副本。
- 您可以在 Red Hat Advanced Cluster Management hub 集群中将警报从受管集群转发到 **Alertmanager**。如需更多信息，请参阅转发警报。
- 您可以通过 OpenShift Container Platform 路由（**rbac-query-proxy**）使用外部 API 来查询指标。如需更多信息，请参阅使用外部指标查询。

1.1.2. Clusters

- 现在，您可以在 Red Hat Advanced Cluster Management 控制台中为集群升级选择 OpenShift Container Platform 版本 4.6 或更高版本频道。频道选择会通知您集群的可用升级。如需更多信息，请参阅选择频道。
- 通过控制台更新集群创建流程，并提供更直观的进度。如需更多信息，请参阅创建集群。
- 现在，您可以直接编辑 HiveConfig 资源，**MultiClusterHub** operator 不会恢复更改。如果删除了 HiveConfig 资源，**MultiClusterHub** operator 会按照在 **MultiClusterHub** 资源首次创建时进行配置。
- 现在，当您在 hub 集群中更新凭证时，您的凭证会自动更新在受管集群中。
- 使用 Red Hat Advanced Cluster Management 控制台在 Red Hat OpenStack Platform 上创建一个 OpenShift Container Platform 受管集群。如需更多信息，请参阅在 Red Hat OpenStack Platform 上创建集群。
- 现在，您可以导入 OpenShift Container Platform 集群以进行在 IBM Power 系统上托管的管理。

- 添加了有关使用 **BareMetalAsset** CR 和 Red Hat Advanced Cluster Management Web 控制台管理裸机资产的信息。如需更多信息，请参阅创建和修改裸机资产。

1.1.2.1. 集群（技术预览）

以下功能是本发行版本的*技术预览*：

- 您可以测试在 IBM Power 系统上托管 hub 集群的能力。
- 现在，您可以在 **ManagedClusterSet** 中对资源进行分组，以控制受管集群、集群池、集群部署和集群声明的 RBAC 访问权限。如需更多信息，请参阅创建和管理 ManagedClusterSets（技术预览）。
- 配置 **AnsibleJob** 模板，以启动受管集群的安装或升级。如需更多信息，请参阅配置 Ansible Tower 任务以在受管集群上运行。
- 您可以创建集群池来更好地管理资源，并配置了 OpenShift Container Platform 集群，以便在需要时进行声明。如需更多信息，请参阅管理集群池。
- 您可以休眠由 Red Hat Advanced Cluster Management 创建的特定 OpenShift Container Platform 受管集群，以更灵活地管理资源。如需更多信息，请参阅 Hibernating a created cluster。
- 现在，您可以在 VMware vSphere 和 Google Cloud Platform 受管集群上配置 Submariner 网络服务。如需更多信息，请参阅 Submariner 网络服务。
- 现在，您可以使用 Red Hat Advanced Cluster Management 控制台在集群中部署 Submariner。如需更多信息，请参阅使用控制台部署 Submariner。
- 您可以使用 Red Hat Advanced Cluster Management 或命令行使用 **MachinePools** 资源来扩展集群。如需更多信息，请参阅重新定义集群大小。
- 您可以通过 OpenShift Cluster Manager 来发现 OpenShift Container Platform 4 集群。发现集群后，您可以导入集群来管理。如需更多信息，请参阅发现服务简介（技术预览）。

1.1.3. 应用程序

- 现在，在从 *Search* 页中选择要查看的应用程序后，您会被定向到 *Applications* 页。如需更多信息，请参阅查询 ArgoCD 应用程序。
- 现在，如果您在使用 Red Hat Advanced Cluster Management 的 OpenShift Container Platform 集群上部署 Argo 应用程序，您可以在 *Applications* 表中和 *Topology* 视图中视觉化 Argo 应用程序。
- 在 *Overview* 或 *Topology* 概述中，您可以启动 Argo 编辑器并管理您的 Argo 应用。
- 应用程序控制台的其他改进包括 *Commit hash* 和 *Tag*，它们特定于 Git 存储库频道类型。另外，还会为 Git 和 Helm 仓库类型添加新协调输入。
- 现在，您可以选择在频道配置中选择协调频率选项：high、mport、low 和 off，以避免不必要的资源协调，从而防止订阅 operator 的超载。如需更多信息，请参阅订阅 Git 资源中的 *Reconcile 选项*。
- *Repository 协调率*添加到控制台中，默认值为设为 **medium**。如果禁用了 auto-reconcile，协调选项会被隐藏，因为资源不会合并或替换当前协调的内容。

- 您可以设置订阅来订阅在 Amazon Simple Storage Service (Amazon S3) 对象存储服务中定义的资源。如需更多信息，请参阅使用对象存储存储库管理应用程序。
- 在控制台中，您可以查看 **ApplicationSet**，它代表由 **ApplicationSet** 控制器生成的 Argo 应用程序。有关应用程序控制台的详情，请查看应用程序控制台概述。

有关应用程序的其他内容，请参阅管理应用程序。

1.1.4. 监管

- 现在，您可以在配置策略中添加或包含模板。如需更多信息，请参阅配置策略中的模板支持。
- Red Hat Advanced Cluster Management 现在使用 Red Hat OpenShift Container Platform Service Serving 证书。如需更多信息，请参阅证书。
- 现在，您可以使用 Ansible Tower 创建策略违反自动化。如需更多信息，请参阅配置 Ansible Tower 以进行监管。

请参阅监管，以了解更多有关仪表板和策略框架的信息。

要查看更多发行说明主题，请参阅发行说明。

1.2. 勘误更新

默认情况下，勘误更新会在发布时自动应用。如需更多信息，请参阅使用 operator 升级。

重要：为了参考，勘误 链接和 GitHub 号可能会添加到内容中并在内部使用。用户可能不能使用访问的链接。

FIPS 注意：如果您没有在 **spec.ingress.sslCiphers** 中指定自己的密码，则 **multiclusterhub-operator** 会提供默认密码列表。对于 2.3，这个列表包含两个 *未被* FIPS 批准的密码。如果您从 2.3.x 或更早版本升级并希望符合 FIPS 合规性，请从 **multiclusterhub** 资源中删除以下两个密码： **ECDHE-ECDSA-CHACHA20-POLY1305** 和 **ECDHE-RSA-CHACHA20-POLY1305**。

1.2.1. Errata 2.3.12

- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.2. Errata 2.3.11

- 修复了在从 2.2 版本升级后因为 pod 名称不正确而导致可观察性失败的问题。(Bugzilla #2087277)
- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.3. Errata 2.3.10

- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.4. 勘误 2.3.9

- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.5. Errata 2.3.8

- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.6. Errata 2.3.7

- 提供一个或多个产品容器镜像及安全修复的更新。

1.2.7. Errata 2.3.6

- 修复了升级时建议之前版本中 CRD 信息不会被更新的错误。(Bugzilla #2015663)
- 解决最近升级的受管集群中有限带宽的问题。(Bugzilla #2021128)
- 修复了在将 Red Hat Advanced Cluster Management 从 2.3.5 升级到 2.3.6 后，阻止受管集群的附加组件显示在 Red Hat Advanced Cluster Management 控制台中。(Bugzilla #2050847)
- 为一个或多个产品容器镜像提供更新。

1.2.8. 勘误 2.3.5

- 为一个或多个产品容器镜像提供更新。

1.2.9. Errata 2.3.4

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.3.4 更新的总结列表：

- 修复了阻止 Red Hat Advanced Cluster Management 版本 2.3 与 Red Hat OpenShift Container Platform 版本 4.9 正常工作的问题。从版本 2.3.4 开始，在 OpenShift Container Platform 版本 4.9 上运行时支持 Red Hat Advanced Cluster Management。(Bugzilla #1984470)
- 修复了阻止 Resource Optimization 仪表板在 OpenShift Container Platform 版本 4.9 集群的 CPU usage 面板中显示数据的问题。(Bugzilla #2021766)
- 为一个或多个产品容器镜像提供更新。

1.2.10. Errata 2.3.3

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.3.3 更新的总结列表：

- 修复了在启用了代理时导致应用程序订阅失败的问题，因为不会应用包含源 Git 存储库的 **NO_PROXY** 设置。(Bugzilla #2000951)
- 修复了导致 VMware 受管集群出现在控制台 *Overview* 页面中标记为 **Other** 的部分中的问题，而不是在 **VMware** 部分。(Bugzilla #2004188)
- 修复了一个导致 Grafana pod 的内存要求不断会随活跃的客户端的增长而不断增长的问题。(GitHub #13382)
- 在 Red Hat OpenShift Kubernetes Service(ROKS)上部署时，修复 OpenShift Container Platform 标头栏中的 Red Hat Advanced Cluster Management 控制台链接。(GitHub #14353)
- 修复有时会导致 **management-ingress** pod 在 **ppc64le** 环境中多次重启的问题。(GitHub #15729)
- 修复了阻止具有 **cluster-manager-admin** 角色的用户创建、编辑或删除策略自动化的问题。(GitHub #15750)

- 修复了在升级到 Red Hat Advanced Cluster Management 版本 2.3 后在 Red Hat Advanced Cluster Management 版本 2.1 中部署的应用程序无法正确显示拓扑的问题。(GitHub #15765)
- 修复了多集群可观察性 Operator 的问题，它们导致一些受管集群在升级后降级。(GitHub #15996, #16123)
- 为一个或多个产品容器镜像提供更新。

1.2.11. Errata 2.3.2

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.3.2 更新的总结列表：

- 修复控制台到凭据文档中的链接。(GitHub #14993)
- 修复阻止多集群可观察性操作对象成功升级的问题。(Bugzilla #1993188)
- 为一个或多个产品容器镜像提供更新。

1.2.12. Errata 2.3.1

修复了 2.3 版本中的几个镜像的问题。

1.3. 已知问题

查看 Red Hat Advanced Cluster Management for Kubernetes 中的已知问题。以下列表包含本发行版本的已知问题，或从上一版本中继承的问题。对于 Red Hat OpenShift Container Platform 集群，请参阅 OpenShift Container Platform 已知问题。

- 已知的与安装相关的问题
- 已知的与 Web 控制台相关的问题
  - 已知的可观察性问题
- 已知的与集群管理相关的问题
- 已知的与应用程序管理相关的问题
- 已知的监管问题

1.3.1. 已知的与安装相关的问题

1.3.1.1. 与 OpenShift Container Platform 版本 4.9 的兼容性问题

用于确定 OpenShift Container Platform 版本 4.9 和 Red Hat Advanced Cluster Management 版本 2.3 之间的兼容性的功能测试仍在进行中。在验证两者的兼容性前，在 OpenShift Container Platform 版本 4.9 中使用 Red Hat Advanced Cluster Management 版本 2.3 可能会出现兼容性问题。

1.3.1.2. 从 2.2.x 升级到 2.3.1 版本无法进行

当您将 Red Hat Advanced Cluster Management 从 2.2.x 升级到 2.3.1 时，升级会失败。**Multiclusterhub** 状态显示：**failed to download chart from helm repo**（在组件错误信息中）。您可能还会看与 **no endpoints available for service "ocm-webhook"** 问题相关的错误。

在 hub 集群中，在安装 Red Hat Advanced Cluster Management 的命名空间中运行以下命令以重启部署并升级到 2.3.1 版本：

```
oc delete deploy ocm-proxyserver ocm-controller ocm-webhook multiclusterhub-repo
```

注：错误解决，但协调过程可能不会立即启动。这可以通过在安装产品的同一命名空间中重启 **multicluster-operators-standalone-subscription** 来加快执行。

1.3.1.3. 从 2.3.0 升级到 2.3.1 会失败并显示 ImagePullBackOff 错误

当您将 Red Hat Advanced Cluster Management 从 2.3.0 版本升级到 2.3.1 时，受管集群中的 **open-cluster-management-agent-addon-addon** 命名空间中的 **klusterlet-addon-operator** pod 会返回 **ImagePullBackOff** 错误。

在 hub 集群中完成以下步骤以修复这个问题并升级到 2.3.1 版本：

1. 运行以下命令以删除 **MultiClusterHub** 清单的 **ConfigMap** ：

   ```
   oc delete cm -n open-cluster-management mch-image-manifest-2.3.0
   ```

2. 运行以下命令为控制器重启 pod：

   ```
   oc delete po -n open-cluster-management -lapp=klusterlet-addon-controller-v2
   ```

3. 在从 2.3.0 升级到 2.3.1 后，如果 hub 的 **open-cluster-management-observability** 命名空间中的 Grafana pod 也返回了 **ImagePullBackOff** 错误，请运行以下命令重启 pod，使其使用正确的镜像：

   ```
   oc delete po -n open-cluster-management -lname=multicluster-observability-operator
   ```

您正在运行 Red Hat Advanced Cluster Management 版本 2.3.1。

1.3.1.4. OpenShift Container Platform 集群升级失败的状态

当 OpenShift Container Platform 集群处于升级阶段时，集群 Pod 会被重启，并且集群可能在大约 1 到 5 分钟之内会处于**升级失败**状态。这个行为是正常的，在几分钟后自动解决。

1.3.2. 已知的与 Web 控制台相关的问题

1.3.2.1. Cluster 页面和搜索结果之间节点的不同

您可能会看到 *Cluster* 页面中显示的节点与 *搜索*结果之间的不同。

1.3.2.2. LDAP 用户名是区分大小写的

LDAP 用户名是区分大小写的。使用的名称必须与在 LDAP 目录中配置的方法完全相同。

1.3.2.3. Firefox 的较老版本可能无法显示控制台的功能

该产品支持 Mozilla Firefox 74.0 或 Linux、macOS 和 Windows 提供的最新版本。为了获得最好的兼容性，请升级至最新版本。

1.3.2.4. 无法使用带有空空格的值搜索

在控制台和 Visual Web 终端中，用户无法搜索包括一个空空格的值。

1.3.2.5. 在注销用户 kubeadmin 时会出现一个额外浏览器标签页并显示空白页面

在以 **kubeadmin** 登陆后，点下拉菜单中的 **Log out** 选项，控制台会返回到登录屏幕，但一个浏览器标签页会打开 **/logout** URL。该页面为空白，您可以关闭此页而不影响您的控制台。

1.3.2.6. 不再显示 Secret 的内容

出于安全考虑，搜索不再会显示在受管集群上发现的 secret 的内容。当您通过控制台搜索 secret 时，可能会收到以下出错信息：

```
Unable to load resource data - Check to make sure the cluster hosting this resource is online
```

1.3.2.7. searchcustomization 存储大小的限制

当您更新 **searchcustomization** CR 中的存储大小时，PVC 配置不会改变。如果您需要更新存储大小，使用以下命令更新 PVC（***<storageclassname>-search-redisgraph-0***）：

```
oc edit pvc <storageclassname>-search-redisgraph-0
```

1.3.3. 已知的可观察性问题

1.3.3.1. Observability endpoint operator 无法拉取镜像

如果您创建一个 pull-secret 用于部署到 MultiClusterObservability CustomResource（CR），且 **open-cluster-management-observability** 命名空间中没有 pull-secret，则 observability endpoint operator 会失败。当您导入新集群或导入使用 Red Hat Advanced Cluster Management 创建的 Hive 集群时，需要在受管集群上手动创建 pull-image secret。

如需更多信息，请参阅启用可观察性。

1.3.3.2. 没有来自 ROKS 集群的数据

Red Hat Advanced Cluster Management observability 不会在内置仪表板中显示 ROKS 集群中的数据。这是因为 ROKS 不会从它们管理的服务器公开任何 API 服务器指标。以下 Grafana 仪表板包含不支持 ROKS 集群的面板：**Kubernetes/API server**、**Kubernetes/Compute Resources/Workload**、**Kubernetes/Compute Resources/Namespace(Workload)**

1.3.3.3. ROKS 集群没有 etcd 数据

对于 ROKS 集群，Red Hat Advanced Cluster Management observability 不会在仪表板的 *etcd* 面板中显示数据。

1.3.3.4. search-collector pod 的高 CPU 使用率

当在管理 1000 个集群的 hub 集群上禁用搜索时，**search-collector** pod CPU 的使用率会高于正常状态。在四天时间内，CPU 的用量大约 2.148Mi。您可以通过将 **search-collector** 减少到 **0** 个副本来减少内存用量。

1.3.3.5. 因为证书无效，搜索 pod 无法完成 TLS 握手过程

在某些情况下，搜索 Pod 不会在证书更改后自动重新部署。这会导致服务 pod 间的证书不匹配，进而导致 Transfer Layer Security (TLS) 握手失败。要解决这个问题，重启搜索 Pod 以重置证书。

1.3.3.6. Grafana 控制台中没有指标数据

- 注解查询在 Grafana 控制台中会失败：
  当在 Grafana 控制台中搜索特定注解时，您可能会因为已过期的令牌收到以下错误消息：

  "Annotation Query Failed"

  重新刷新浏览器，验证您是否已登录到 hub 集群。

- *rbac-query-proxy* pod 中的错误：
  由于未授权访问 **managedcluster** 资源，您可能会在查询集群或项目时收到以下错误：

  no project or cluster found

  检查角色权限并进行相应的更新。如需更多信息，请参阅基于角色的访问控制。

1.3.3.7. 在升级到 2.3.2 后集群会降级

当您升级到启用了 observability 的 2.3.2 时，一些集群会降级，因为可观察性附加组件未就绪。运行以下命令重启 **multicluster-observability-operator** pod：

```
oc delete po multicluster-observability-operator -n open-cluster-management
```

observability pod 被重新创建。

1.3.3.8. Observability 有状态集在断开连接的环境中使用错误的镜像

在断开连接环境的个别情况下，observability **StatefulSet** 的一些 pod 会一直处于 **ErrPullImage** 状态，因为 pod 无法拉取镜像。这些 pod 中定义的镜像与相关的 **StatefulSet** 中定义的镜像不同。要解决这个问题，您需要删除使用错误镜像的 pod。pod 会自动重启，并且应使用正确的镜像。

1.3.3.9. Error ingesting out-of-order samples

Observability **receive** pod 报告以下出错信息：

```
Error on ingesting out-of-order samples
```

错误消息表示，在指标收集间隔期间，由受管集群发送的时间序列数据比在之前的集合间隔发送的时间序列数据旧。当出现这个问题时，Thanos 接收器会丢弃数据，这可能会在 Grafana 仪表板中显示的数据中造成差距。如果经常看到这个错误，建议将指标收集间隔增加到一个更高的值。例如，您可以将间隔增加到 60 秒。

只有在时间序列间隔被设置为较低值（如 30 秒）时，才会注意到这个问题。请注意，当指标收集间隔被设置为默认值 300 秒时，不会看到这个问题。

1.3.4. 已知的与集群管理相关的问题

1.3.4.1. 删除受管集群时受管集群的命名空间处于终止状态

在某些情况下，当您删除受管集群时，受管集群的命名空间可能会处于终止状态，因为它的 **manifestworks** 资源不会被删除。运行以下命令以删除剩余的 **manifestworks** 资源并删除命名空间：

```
kubectl -n <managed-cluster-namespace> get manifestworks | grep -v NAME | awk '{print $1}' | xargs
kubectl -n <managed-cluster-namespace> patch manifestworks -p '{"metadata":{"finalizers": []}}' --
type=merge
```

1.3.4.2. 无效的集群部署会出现创建

在部署集群时提供无效的信息时，不可避免的集群状态会显示 **创建** 状态，即使它无法启动。无效的信息（如部署中与 **install-config** 文件中指定的区域不匹配的区域）会导致在 Hive 置备 pod 中添加以下错误：

```
provision failed, requirements not met
```

Red Hat Advanced Cluster Management 版本 2.3 继续报告为集群创建的状态，但无效的信息会阻止创建集群。

1.3.4.3. 使用 Infrastructure Operator 进行集群置备失败

当使用 Infrastructure Operator 创建 OpenShift Container Platform 集群时，ISO 镜像的文件名可能会太长。镜像名称长会导致镜像置备和集群置备失败。要确定这是否是问题，请完成以下步骤：

1. **运行以下命令，查看您要置备的集群的裸机主机信息：**

```
oc get bmh -n <cluster_provisioning_namespace>
```

2. **运行 describe 命令以查看错误信息：**

```
oc describe bmh -n <cluster_provisioning_namespace> <bmh_name>
```

3. **类似以下示例的错误表示文件名的长度问题：**

```
Status:
  Error Count:    1
  Error Message:  Image provisioning failed: ... [Errno 36] File name too long ...
```

如果出现问题，通常位于以下 OpenShift Container Platform 版本上，因为基础架构操作员不使用镜像服务：

- 4.8.17 及更早版本

要避免这个错误，将 OpenShift Container Platform 升级到 4.8.18 或更高版本。

1.3.4.4. Google Cloud Platform 上的集群置备失败

当您尝试在 Google Cloud Platform(GCP)上置备集群时，可能会失败并显示以下错误：

```
Cluster initialization failed because one or more operators are not functioning properly.
The cluster should be accessible for troubleshooting as detailed in the documentation linked below,
https://docs.openshift.com/container-platform/latest/support/troubleshooting/troubleshooting-installations.html
The 'wait-for install-complete' subcommand can then be used to continue the installation
```

您可以通过在 GCP 项目中启用 网络安全 API 来解决这个问题，它允许集群安装继续进行。

1.3.4.5. 使用不同名称重新导入后 local-cluster 状态为离线

当您意外尝试以不同名称的集群形式重新导入名为 local-cluster 的集群时，local-cluster 和重新导入集群的状态会显示"offline"。

要从这个问题单中恢复，请完成以下步骤：

1. 在 hub 集群上运行以下命令，以临时编辑 hub 集群的自助管理设置：

```
oc edit mch -n open-cluster-management multiclusterhub
```

2. 添加 spec.disableSelfManagement=true 设置。

3. 在 hub 集群中运行以下命令以删除并重新部署 local-cluster：

```
oc delete managedcluster local-cluster
```

4. 输入以下命令删除 local-cluster 管理设置：

```
oc edit mch -n open-cluster-management multiclusterhub
```

5. 删除之前添加的 **spec.disableSelfManagement=true**。

1.3.4.6. 在 Ansible 集群创建失败后，集群状态在控制台的不同视图中有所不同

当您尝试创建集群时指定无效的 **Ansible** 作业模板名称并且失败时，集群会在控制台的不同屏幕上显示不同的状态。当通过 **Infrastructure > Clusters > Managed cluster** 查看状态时，它会显示一个 **Failed** 状态。当选择：**Infrastructure > Clusters > Cluster sets > <your_cluster_set_name> > Managed clusters**，状态会一直处于 **Creating**。正确的状态应该为 **Failed**。您可以尝试再次创建集群，并输入正确的 **Ansible** 模板名称。

1.3.4.7. 可能不会自动重新导入 local-cluster

有时，在分离本地集群后，**local-cluster** 可能无法自动重新导入。当发生这种情况时，**local-cluster** 在 **Red Hat Advanced Cluster Management** 控制台中会显示 **Pending Import** 状态。

要重新导入 **local-cluster**，请完成以下步骤：

1. 运行以下命令来删除 **klusterlet** 部署：

```
oc -n open-cluster-management-agent delete deployment klusterlet
```

2. 运行以下命令重启 **managedcluster-import-controller** ：

```
oc -n open-cluster-management get pods -l app=managedcluster-import-controller-v2 | awk 'NR>1{print $1}' | xargs oc -n open-cluster-management delete pods
```

1.3.4.8. 受管集群的集群部署处于终止状态

当您删除使用 **Red Hat Advanced Cluster Management** 控制台创建的受管集群时，受管集群的 **clusterdeployment** 可能会处于终止状态。要绕过这个问题并删除这个 **clusterdeployment**，通过编辑集群的 **agentclusterinstall** 资源来手动删除 **agentclusterinstall.agent-install.openshift.io/ai-deprovision finalizer**。

1.3.4.9. 无法手动删除受管集群命名空间

您无法手动删除受管集群的命名空间。受管集群命名空间会在受管集群分离后自动删除。如果在分离

受管集群前手动删除受管集群命名空间，受管集群会在删除受管集群后显示持续终止状态。要删除此正在终止的受管集群，请从分离的受管集群中手动删除终结器。

1.3.4.10. 无法跨架构创建集群

您无法在不创建包含这两个架构文件的发行镜像 (ClusterImageSet) 的情况下在与 hub 集群架构不同的架构中创建受管集群。例如，您无法从 ppc64le hub 集群创建 x86_64 集群。集群创建失败，因为 OpenShift Container Platform 发行 registry 不提供多架构镜像清单。

要临时解决这个问题，请完成以下步骤：

1. 通过 OpenShift Container Platform release registry，创建一个包括 x86_64 和 ppc64le 发行镜像的清单列表。

   a. 从 Quay 存储库拉取这两个架构的清单列表：

   ```
   $ podman pull quay.io/openshift-release-dev/ocp-release:4.8.1-x86_64
   $ podman pull quay.io/openshift-release-dev/ocp-release:4.8.1-ppc64le
   ```

   b. 登录到维护镜像的私有存储库：

   ```
   $ podman login <private-repo>
   ```

   使用存储库的路径替换 private-repo。

   c. 运行以下命令，将发行镜像清单添加到私有存储库中：

   ```
   $ podman push quay.io/openshift-release-dev/ocp-release:4.8.1-x86_64 <private-repo>/ocp-release:4.8.1-x86_64
   $ podman push quay.io/openshift-release-dev/ocp-release:4.8.1-ppc64le <private-repo>/ocp-release:4.8.1-ppc64le
   ```

   使用存储库的路径替换 private-repo。

   d. 为新信息创建清单：

```
$ podman manifest create mymanifest
```

e. **将两个发行镜像的引用添加到清单列表中：**

```
$ podman manifest add mymanifest <private-repo>/ocp-release:4.8.1-x86_64
$ podman manifest add mymanifest <private-repo>/ocp-release:4.8.1-ppc64le
```

使用存储库的路径替换 private-repo。

f. **将清单列表中的列表与现有清单合并：**

```
$ podman manifest push mymanifest docker://<private-repo>/ocp-release:4.8.1
```

使用存储库的路径替换 private-repo。

2. **在 hub 集群中，创建一个发行版本镜像来引用存储库中的清单。**

a. **创建一个 YAML 文件，其中包含类似以下示例的信息：**

```
apiVersion: hive.openshift.io/v1
kind: ClusterImageSet
metadata:
  labels:
    channel: fast
    visible: "true"
  name: img4.8.1-appsub
spec:
  releaseImage: <private-repo>/ocp-release:4.8.1
```

使用存储库的路径替换 private-repo。

b. **在 hub 集群中运行以下命令以应用更改：**

```
oc apply -f <file-name>.yaml
```

将 file-name 替换为您刚才创建的 YAML 文件的名称。

3. 在创建 OpenShift Container Platform 集群时选择新的发行镜像。

创建流程使用合并的发行镜像来创建集群。

1.3.4.11. 无法通过更改标签将集群重新分配给集群集

您无法通过将集群的标签更新至新集群集，将集群或集群集从一个集群设置为另一个集群。要将集群或集群设置为另一个集群，请使用 Red Hat Advanced Cluster Management 控制台将其从集群集中删除。从集群集合中删除后，使用控制台将其添加到新集群中。

1.3.4.12. 无法使用 Ansible Tower 与 IBM Power hub 集群集成

当 Red Hat Advanced Cluster Management for Kubernetes hub 集群在 IBM Power 上运行时，您无法使用 Ansible Tower 集成，因为 Ansible Automation Platform Resource Operator 不提供 ppc64le 镜像。

1.3.4.13. 升级到 2.3 后无法更改集群中的凭证

将 Red Hat Advanced Cluster Management 升级到 2.3 后，您无法在升级前更改由 Red Hat Advanced Cluster Management 创建和管理的任何受管集群的凭证 secret。

1.3.4.14. 无法在 OpenShift Container Platform 版本 4.8 上创建裸机受管集群

当 hub 集群在 OpenShift Container Platform 版本 4.8 上托管时，您无法使用 Red Hat Advanced Cluster Management hub 集群创建裸机受管集群。

1.3.4.15. 创建资源下拉列表错误

当您分离一个受管集群时，*Create resource* 页面可能会临时中断并显示以下错误：

```
Error occurred while retrieving clusters info. Not found.
```

等待命名空间自动被删除，这在分离集群后需要 5-10 分钟完成。或者，如果命名空间处于终止状态，则需要手动删除命名空间。返回该页面查看错误是否已解决。

1.3.4.16. hub 集群和受管集群的时钟未同步

hub 集群和管理集群的时间可能会不同步，在控制台中显示 unknown，当在几分钟内会变为 available。确保正确配置了 Red Hat OpenShift Container Platform hub 集群时间。请参阅 自定义节点。

1.3.4.17. 不支持导入 IBM OpenShift Container Platform Kubernetes Service 集群的特定版本

您无法导入 IBM OpenShift Container Platform Kubernetes Service 版本 3.11 集群。支持 IBM OpenShift Kubernetes Service 的更新的版本。

1.3.4.18. 分离 OpenShift Container Platform 3.11 不会删除 *open-cluster-management-agent*

当您分离 OpenShift Container Platform 3.11 上的受管集群时，open-cluster-management-agent 命名空间不会被自动删除。运行以下命令来手动删除命名空间：

```
oc delete ns open-cluster-management-agent
```

1.3.4.19. 不支持为置备的集群进行自动 secret 更新

当更改您的云供应商访问密钥时，置备的集群访问密钥不会在命名空间中更新。当凭证在托管受管集群的云供应商过期并尝试删除受管集群时，需要此项。如果发生了这种情况，请为您的云供应商运行以下命令来更新访问密钥：

- **Amazon Web Services (AWS)**

  ```
  oc patch secret {CLUSTER-NAME}-aws-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"aws_access_key_id": "{YOUR-NEW-ACCESS-KEY-ID}","aws_secret_access_key":"{YOUR-NEW-aws_secret_access_key}"} }]'
  ```

- **Google Cloud Platform (GCP)**

  在试图销毁集群时如果出现多个重复的 Invalid JWT Signature 日志错误信息，则代表发生了这个问题。如果您的日志包含此消息，请获取新的 Google Cloud Provider 服务帐户 JSON 密钥并输入以下命令：

  ```
  oc set data secret/<CLUSTER-NAME>-gcp-creds -n <CLUSTER-NAME> --from-file=osServiceAccount.json=$HOME/.gcp/osServiceAccount.json
  ```

  将 *CLUSTER-NAME* 替换为集群的名称。

将文件 **$HOME/.gcp/osServiceAccount.json** 替换为包含新 **Google Cloud Provider** 服务帐户 **JSON** 密钥的文件的路径。

- **Microsoft Azure**

```
oc set data secret/{CLUSTER-NAME}-azure-creds -n {CLUSTER-NAME} --from-file=osServiceAccount.json=$HOME/.azure/osServiceAccount.json
```

- **VMware vSphere**

```
oc patch secret {CLUSTER-NAME}-vsphere-creds -n {CLUSTER-NAME} --type json -p='[{"op": "add", "path": "/stringData", "value":{"username": "{YOUR-NEW-VMware-username}","password":"{YOUR-NEW-VMware-password}"} }]'
```

1.3.4.20. 无法以非 root 用户身份运行 management ingress

您必须以 **root** 身份登录才能运行 **management-ingress** 服务。

1.3.4.21. 无法在搜索中查看受管集群的节点信息

搜索 **hub** 集群中资源的 **RBAC** 映射。根据 **Red Hat Advanced Cluster Management** 的用户 **RBAC** 设置，用户可能不会看到来自受管集群的节点数据。搜索的结果可能与集群的 ***Nodes*** 页面中显示的结果不同。

1.3.4.22. 销毁集群的进程没有完成

当销毁受管集群时，在一小时后仍然继续显示 **Destroying** 状态，且集群不会被销毁。要解决这个问题请完成以下步骤：

1. 手动确保云中没有孤立的资源，，且清理与受管集群关联的所有供应商资源。
2. 输入以下命令为正在删除的受管集群打开 **ClusterDeployment**：

```
oc edit clusterdeployment/<mycluster> -n <namespace>
```

将 ***mycluster*** 替换为您要销毁的受管集群的名称。

使用受管集群的命名空间替换 ***namespace***。

3. 删除 **hive.openshift.io/deprovision finalizer**，以强制停止尝试清理云中的集群资源的进程。

4. 保存您的更改，验证 **ClusterDeployment** 是否已不存在。

5. 运行以下命令手动删除受管集群的命名空间：

```
oc delete ns <namespace>
```

使用受管集群的命名空间替换 ***namespace***。

1.3.4.23. 无法使用控制台在 OpenShift Container Platform Dedicated 上升级 OpenShift Container Platform 受管集群

您不能使用 Red Hat Advanced Cluster Management 控制台升级 OpenShift Container Platform Dedicated 环境中的 OpenShift Container Platform 受管集群。

1.3.4.24. 工作管理器附加搜索详情

特定受管集群中特定资源的搜索详情页面可能会失败。在进行搜索前，您必须确保受管集群中的 **work-manager** 附加组件处于 **Available** 状态。

1.3.4.25. IBM Power hub 集群不支持 Argo CD

Argo CD 与 Red Hat Advanced Cluster Management 集成无法在在 IBM Power 上运行的 Red Hat Advanced Cluster Management hub 集群上工作，因为没有可用的 ppc64le 镜像。

1.3.4.26. 非 Red Hat OpenShift Container Platform 受管集群必须启用 LoadBalancer

Red Hat OpenShift Container Platform 集群和非 OpenShift Container Platform 集群都支持 pod 日志功能，但非 OpenShift Container Platform 集群需要启用 LoadBalancer 来使用该功能。完成以下步骤以启用 LoadBalancer：

1. 云供应商有不同的 LoadBalancer 配置。有关更多信息，请访问您的云供应商文档。

2. 检查 loggingEndpoint 是否显示 managedClusterInfo 状态来验证 Red Hat Advanced Cluster Management 上是否启用了 LoadBalancer。

3. 运行以下命令，以检查 loggingEndpoint.IP 或 loggingEndpoint.Host 是否具有有效的 IP 地址或主机名：

```
oc get managedclusterinfo <clusterName> -n <clusterNamespace> -o json | jq -r
'.status.loggingEndpoint'
```

如需有关 LoadBalancer 类型的更多信息，请参阅 Kubernetes 文档中的 *Service* 页面。

1.3.5. 已知的与应用程序管理相关的问题

1.3.5.1. 应用程序搜索未定义错误 Application 表

当您 按 *Applications 表* 上的行操作按钮点击 *Search* application 时，您会被定向到 *Search* 页面，其结果可能与 *应用程序详情页面中的* 相同预设置过滤器不同。

1.3.5.2. 应用程序搜索未定义错误 Argo CD

当从 Argo CD 应用程序的应用程序详情页面中点链接 Search all related applications，搜索页面会返回无效的 preset 过滤器。

您可以在搜索控制台中删除目录过滤器来解决这个问题。

1.3.5.3. 代理的应用程序创建过程中没有分支信息

当使用 Create application 编辑器创建 Red Hat Advanced Cluster Management 应用程序时，当 hub 集群位于代理后面时，可能会收到 Git 存储库的以下错误：

与 Git 存储库的连接失败。无法获取分支。

您可以使用 Git 存储库 URL 而不是使用分支信息。在指定了分支时应用会正确部署。

1.3.5.4. 应用程序 Argo 搜索未定义错误

Argo 应用的集群节点搜索链接可能会返回 name:undefined。

当您从 Argo 应用的集群节点详情中点 Launch resource in search 链接时，搜索过滤器可能会包含 name:undefined。

您可以通过将未定义的值替换为集群节点详情中的集群名称来解决这个问题。

1.3.5.5. 带有多个订阅的应用程序拓扑集群没有正确分组

如果集群使用多个订阅，集群可能无法在*应用程序拓扑*中正确分组。

当您使用多个订阅部署应用程序时，在 ***All Subscription*** 视图中的集群节点可能没有被正确分组。

例如，当使用多个订阅部署一个包含 ***Helm*** 和 ***Git*** 仓库组合在一起的应用程序时，***All subscriptions*** 视图无法正确显示 Helm 订阅中资源的状态。

查看各个订阅视图中的拓扑，以显示正确的集群节点分组信息。

1.3.5.6. 应用程序拓扑订阅的切换

当您使用订阅下拉菜单在应用程序订阅间切换时，应用程序拓扑可能会失败。

要解决这个问题，尝试切换到其他订阅，或者刷新浏览器来查看拓扑显示的刷新。

1.3.5.7. 应用程序 Ansible hook 独立模式

不支持 Ansible hook 独立模式。要使用订阅在 hub 集群上部署 Ansible hook，您可以使用以下订阅 YAML：

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
     name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    local: true
```

但是，此配置可能永远不会创建 Ansible 实例，因为 spec.placement.local:true 有以 standalone 模式运行的订阅。您需要在 hub 模式中创建订阅。

1. 创建部署到 local-cluster 的放置规则。请参见以下示例：

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: <towhichcluster>
  namespace: hello-openshift
spec:
  clusterSelector:
    matchLabels:
      local-cluster: "true" #this points to your hub cluster
```

2. 在您的订阅中引用该放置规则。请参见以下信息：

```
apiVersion: apps.open-cluster-management.io/v1
kind: Subscription
metadata:
  name: sub-rhacm-gitops-demo
  namespace: hello-openshift
annotations:
  apps.open-cluster-management.io/github-path: myapp
  apps.open-cluster-management.io/github-branch: master
spec:
  hooksecretref:
     name: toweraccess
  channel: rhacm-gitops-demo/ch-rhacm-gitops-demo
  placement:
    placementRef:
      name: <towhichcluster>
      kind: PlacementRule
```

应用两者后，您应该看到 hub 集群中创建的 Ansible 实例。

1.3.5.8. 在本地集群限制时部署应用程序

如果在创建或编辑应用程序时选择了 Deploy on local cluster，则应用程序拓扑无法正确显示。在本地集群上部署 是选项,可在 hub 集群上部署资源,以便可以将其作为 本地集群 管理,但这不是本发行版本的最佳实践。

要解决这个问题，请执行以下步骤：

1. 在控制台中取消选择 Deploy on local cluster 选项。
2. 选择 Deploy application resources only on clusters matching specified labels 选项。
3. 创建以下标签： local-cluster : 'true'。

1.3.5.9. 命名空间频道订阅处于失败状态

当订阅了命名空间频道且修复其他相关资源（如频道、 secret、 ConfigMap 或放置规则等）后，订阅会处于 FAILED 状态，命名空间订阅不会持续被协调。

要强制订阅再次进行协调以退出 FAILED 状态，完成以下步骤：

1. 登录到您的 hub 集群。
2. 使用以下命令手动在订阅中添加一个标签：

```
oc label subscriptions.apps.open-cluster-management.io the_subscription_name reconcile=true
```

1.3.5.10. 为应用程序编辑角色错误

具有 Editor 角色的用户应只拥有应用程序的 read 或 update 授权。但这样的用户会错误地具有应用程序的 create 和 delete 的权限。OpenShift Container Platform Operator Lifecycle Manager 默认设

置会更改产品的设置。要解决这个问题，请遵循以下步骤：

1. 运行 oc edit clusterrole applications.app.k8s.io-v1beta2-edit -o yaml 以打开应用程序编辑集群角色。
2. 从 verbs 列表中删除 create 和 delete。
3. 保存更改。

1.3.5.11. 编辑放置规则错误的角色

在 Editor 角色中执行的用户应该对放置规则只有 read 或 update权限，但因为存在错误，编辑器也可能会有 create 和 delete 权限。OpenShift Container Platform Operator Lifecycle Manager 默认设置会更改产品的设置。要解决这个问题，请遵循以下步骤：

1. 运行 oc edit clusterrole placementrules.apps.open-cluster-management.io-v1-edit 以打开应用程序编辑集群角色。
2. 从 verbs 列表中删除 create 和 delete。
3. 保存更改。

1.3.5.12. 在更新的放置规则后没有部署应用程序

如果应用程序在更新放置规则后没有部署，验证 klusterlet-addon-appmgr pod 是否正在运行。klusterlet-addon-appmgr 是需要在端点集群中运行的订阅容器。

您可以运行 oc get pods -n open-cluster-management-agent-addon 来验证。

您还可以在控制台中搜索 kind:pod cluster:yourcluster 来查看 klusterlet-addon-appmgr 是否在运行。

如果无法验证，请尝试再次导入集群并重新验证。

1.3.5.13. Subscription operator 不会创建一个 SCC

如需了解更多与 Red Hat OpenShift Container Platform SCC 相关的信息，请参阅 管理 Security Context Constraints (SCC)。它是受管集群所需的一个额外的配置。

不同的部署有不同的安全性上下文和不同的服务帐户。订阅 operator 无法自动创建一个 SCC。pod 的管理员控制权限。需要一个安全性上下文约束（SCC）CR，以便为相关服务帐户启用适当的权限，以便在非默认命名空间中创建 pod:

要手动在命名空间中创建 SCC CR，完成以下操作：

1. 找到在部署中定义的服务帐户。例如，查看以下 nginx 部署：

```
nginx-ingress-52edb
nginx-ingress-52edb-backend
```

2. 在命名空间中创建 SCC CR 为服务帐户或帐户分配所需的权限。请参见以下示例， 其中添加了 SecurityContextConstraints：

```
apiVersion: security.openshift.io/v1
defaultAddCapabilities:
kind: SecurityContextConstraints
metadata:
  name: ingress-nginx
  namespace: ns-sub-1
priority: null
readOnlyRootFilesystem: false
requiredDropCapabilities:
fsGroup:
  type: RunAsAny
runAsUser:
  type: RunAsAny
seLinuxContext:
  type: RunAsAny
users:
- system:serviceaccount:my-operator:nginx-ingress-52edb
- system:serviceaccount:my-operator:nginx-ingress-52edb-backend
```

1.3.5.14. 应用程序频道需要唯一的命名空间

在同一命名空间中创建多个频道可能会导致 hub 集群出现错误。

例如，安装程序将命名空间 charts-v1 作为 Helm 类型频道使用，因此不要在 charts-v1 中创建任何其他频道。确保您在唯一命名空间中创建频道。所有频道需要单独的命名空间，但 GitHub 频道除外，它们可与另一个 GitHub 频道共享命名空间。

1.3.5.15. Ansible Automation Platform（早期访问）2.0.0 作业失败

当安装了 Ansible Automation Platform（早期访问）2.0.0 时，AnsibleJobs 无法运行。如果要通过 Red Hat Advanced Cluster Management 提交 prehook 和 posthook AnsibleJobs，请使用 Ansible Automation Platform Resource Operator 0.1.1。

1.3.5.16. 应用程序名称要求

应用程序名称不能超过 37 个字符。如果字符超过这个数量，应用部署将显示以下错误：

```
status:
  phase: PropagationFailed
  reason: 'Deployable.apps.open-cluster-management.io "_long_lengthy_name_" is invalid:
metadata.labels: Invalid value: "_long_lengthy_name_": must be no more than 63
characters/n'
```

1.3.5.17. 应用程序控制台表

参阅控制台中不同 *Application* 表的限制：

- 在 *Overview* 页面的 *Applications* 表和 *Advanced 配置*页面上的 *Subscriptions* 表中，*Clusters* 列会显示部署应用程序资源的集群计数。因为应用程序是由本地集群上的资源定义的，所以本地集群会包含在搜索结果中，无论实际的应用程序资源是否在本地集群中部署。
- 在 *Subscriptions* 的 *Advanced configuration* 列表中，*Applications* 栏显示使用该订阅的应用程序总数，如果订阅部署了子应用程序，它们也会包含在搜索结果中。
- *Channels* 的 *Advanced configuration* 列表中，*Subscriptions* 栏显示使用该频道的本地集群中的订阅总数，但这不包括由其他订阅部署的订阅，这些订阅包含在搜索结果中。

1.3.6. 已知的监管问题

1.3.6.1. 即使没有新的策略违反情况启动自动化过程，Ansible 自动化作业还会继续每小时运行一次，

在 OpenShift Container Platform 4.8 中，默认启用 Finished 资源的 TTL Controller，这意味着作业会每小时被删除。此作业清理会导致 Ansible Automation Platform Resource Operator 重新运行关

联的自动化。再次使用由策略框架创建的 AnsibleJob 资源中的现有详情运行自动化。提供的详细信息可能包括之前确定的违规行为，这些违规行为可能会错误地显示为重复违规行为。您可以禁用清理作业的控制器，以防止这些重复的违反情况。要禁用清理作业的控制器，请完成以下步骤：

1. 运行以下命令来编辑 kubeapiservers.operator.openshift.io 资源：

```
oc edit kubeapiservers.operator.openshift.io cluster
```

2. 找到 unsupportedConfigOverrides 部分。

3. 更新 unsupportedConfigOverrides 部分，使其包含类似以下示例的内容，该示例禁用了作业清理功能：

```
unsupportedConfigOverrides:
  apiServerArguments:
    feature-gates:
    - TTLAfterFinished=false
```

4. 运行以下命令来编辑 kubecontrollermanager 资源：

```
oc edit kubecontrollermanager cluster
```

5. 完成第 2 和 3 步，以更新 kubecontrollermanager 资源中的相同部分。

1.3.6.2. PlacementRule matchExpression 没有使用新的 matchLabel 删除

当您将策略 PlacementRule 从 matchExpressions 更新至 matchLabels 时，旧的 matchExpression 不会被删除。

请参阅以下示例中第一个示例中的 matchExpressions 更改为 matchLabels，但 matchExpressions 不会被删除。

```
apiVersion: apps.open-cluster-management.io/v1
kind: PlacementRule
metadata:
  name: placement-policy-etcdencryption
spec:
  clusterConditions:
  - status: "True"
```

```
    type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions:
      - {key: environment, operator: In, values: ["test"]}
```

```
spec:
  clusterConditions:
  - status: "True"
    type: ManagedClusterConditionAvailable
  clusterSelector:
    matchExpressions: []
    matchLabel: {}
```

1.3.6.3. IAM 策略控制器不考虑组用户

当决定具有给定 ClusterRole 权限的用户数量时，IAM 策略控制器只会检查 Kubernetes User 资源，且不考虑 Kubernetes Group 资源中的用户。

1.3.6.4. 无法注销

当您使用外部身份提供程序登录到 Red Hat Advanced Cluster Management 时，您可能无法从 Red Hat Advanced Cluster Management 注销。当您使用与 IBM Cloud 和 Keycloak 作为身份提供程序一起安装的 Red Hat Advanced Cluster Management 时会出现这种情况。

在尝试从 Red Hat Advanced Cluster Management 注销前，您必须从外部身份提供程序注销。

1.3.6.5. Administrator 集群管理器无法创建自动化策略

具有集群范围角色绑定到 open-cluster-management:cluster-manager-admin 的用户无法创建自动化策略。若要修复此问题，您必须手动将角色添加到自动化策略中。

创建或更新集群角色(ClusterRole)，为 Ansible 资源向 cluster-manager-admin 角色添加规则。您的 YAML 可能会重新排序以下文件：

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: add-ansible-rules
  labels:
    rbac.authorization.k8s.io/aggregate-to-ocm-cluster-manager-admin: "true"
rules:
- apiGroups: ["tower.ansible.com"]
  resources: ["ansiblejobs"]
  verbs: ["create","get", "list", "watch", "update", "delete", "deletecollection", "patch"]
```

1.3.6.6. Gatekeeper operator 安装失败

当您在 Red Hat OpenShift Container Platform 版本 4.9 上安装 gatekeeper operator 时，安装会失败。在将 OpenShift Container Platform 升级到 4.9.0 之前，您必须将 gatekeeper operator 升级到 0.2.0 版本。如需更多信息，请参阅升级 gatekeeper 和 gatekeeper operator。

1.3.6.7. 当命名空间处于 *Terminating* 状态时，配置策略列出了 complaint

当您有一个配置策略，它的 complianceType 参数被设置为 mustnothave，remediationAction 参数被配置为 enforce，策略会在向 Kubernetes API 发出删除请求后被列为合规。因此，在策略列为合规时，Kubernetes 对象可能会一直处于 Terminating 状态。

1.4. 弃用和删除

了解产品将在什么时候被弃用，或从 Red Hat Advanced Cluster Management for Kubernetes 中删除。考虑*推荐操作*中的备选操作和详细信息，它们显示在当前版本的表中和之前两个版本。

重要：

- Red Hat Advanced Cluster Management 的 2.1 版本*已被删除*且不再被支持。其文档可能仍然可用，但是它已被弃用，将没有任何可用的勘误或其他更新。文档的早期版本也不被支持。
- 升级到 Red Hat Advanced Cluster Management 的最新版本是最佳选择。

1.4.1. API 弃用和删除

Red Hat Advanced Cluster Management 的 API 会遵循 Kubernetes 弃用指南。有关相关策略的详情，请参阅 Kubernetes 弃用策略。

Red Hat Advanced Cluster Management API 只在以下时间线外才会被弃用或删除：

- 所有 V1 API 会提供 12 个月或跨 3 个发行版本（以更长的时间为准）的支持。V1 API 没有被删除，但可能会在这个时间限制外被弃用。
- 所有 beta API 通常在 9 个月或跨 3 个发行版本（以更长的时间为准）内可用。Beta API 不会在这个时间限制外被删除。

- 所有 alpha API 都不是必需的，但如果对用户有好处，则可能会被列为已弃用或删除。

1.4.2. Red Hat Advanced Cluster Management 弃用

*弃用（deprecated）*组件、功能或服务会被支持，但不推荐使用，并可能在以后的版本中被删除。考虑使用*推荐操作*中的相应的替代操作，详情在下表中提供：

产品或类别	受影响的项	Version	推荐的操作	详情和链接
应用程序	**HelmRepo** 频道规格：**insecureSkipVerify: "true"** 已不再在 **configMapRef** 中使用	2.2	在没有 **configMapRef** 的频道中使用 **insecureSkipVerify: "true"**	请参阅 YAML 示例。
安装程序	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 中的 Hive 设置	2.2	安装，然后直接使用 **oc edit hiveconfig hive** 命令编辑 **hiveconfig**	无
klusterlet operator	**release-2.3** 频道没有接收更新	2.3 及更高版本	要导入和管理 Red Hat OpenShift 专用集群，您必须升级。	请参阅使用 operator 升级。
安装程序	在 **operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 中分隔 cert-manager 设置	2.3	无	无
监管	自定义策略控制器	2.3	无	无

1.4.3. 删除

一个*删除（removed）*的项通常是在之前的版本中被弃用的功能，在该产品中不再可用。您必须将 alternatives 用于删除的功能。考虑使用*推荐操作*中的相应的替代操作，详情在下表中提供：

产品或类别	受影响的项	Version	推荐的操作	详情和链接
Observability 拓扑	从 *Observe 环境*进行拓扑访问会被完全删除	2.2	无	应用程序拓扑位于*应用程序管理*中，不再包括在 *Observability 控制台*中。
应用程序	频道类型：Namespace，完全删除	2.2	无	无
应用程序	单个 ArgoCD 导入模式，导入至 hub 集群中的一个 ArgoCD 服务器的 secret	2.3	您可以将集群 secret 导入到多个 ArgoCD 服务器中	无
应用程序	ArgoCD 集群集成：**spec.applicationManager.argocdCluster**	2.3	创建 GitOps 集群和放置自定义资源以注册受管集群。	在受管集群中配置 GitOps
监管	cert-manager 内部证书管理	2.3	不需要操作	无

1.5. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 平台针对 GDPR 的注意事项

1.5.1. 备注

本文档旨在帮助您准备 General Data Protection Regulation（GDPR）就绪。它提供有关您可以配置的 Red Hat Advanced Cluster Management for Kubernetes 平台的功能信息，以及产品的使用情况，以满足 GDPR 就绪的要求。因为用户可以选择不同的方式来配置功能，并且产品的使用方式及第三方集群和系统都会有所不同，所以这里介绍的信息可能并没有覆盖所有情况。

客户需要负责确保自己遵守各种法律及条例，包括欧盟的 GDPR 条例。获取法律法规建议，确定并解释可能影响客户业务的相关法律及规范，以及客户可能需要为遵守此类法律及规范而可能需要执行的任何行动完全由客户自己负责。

这里描述的产品、服务和其他功能不适用于所有客户情况，且适用性可能有限制。红帽不提供法律、会计、审计方面的建议，也不代表或者认为其服务或产品会确保客户遵守任何法律和规范。

1.5.2. 内容表

- GDPR
- 针对 GDPR 的产品配置
- 数据生命周期
- 数据收集
- 数据存储
- 数据访问
- 数据处理
- 数据删除
- 限制使用个人数据的能力
- 附录

1.5.3. GDPR

欧盟（"EU"）已采用了 General Data Protection Regulation（GDPR）并从 2018 年 5 月 25 日起生效。

1.5.3.1. 为什么 GDPR 很重要？

GDPR 为处理个人数据建立了更强大的数据保护框架。GDPR 可以带来：

- 新的和增强的个人权利

- 扩展了个人数据的定义
- 数据处理方新的责任
- 非遵守方可能在经济上会受到大量处罚
- 强制数据违反通知

1.5.3.2. 更多关于 GDPR 的信息

- EU GDPR Information Portal
- Red Hat GDPR website

1.5.4. 针对 GDPR 的产品配置

以下小节描述了 Red Hat Advanced Cluster Management for Kubernetes 平台的数据管理的各个方面，并提供了有关帮助客户端满足 GDPR 要求的能力信息。

1.5.5. 数据生命周期

Red Hat Advanced Cluster Management for Kubernetes 是一个应用程序平台，用于开发并管理内部、容器化的应用程序。它是一个用于管理容器的集成环境，包括容器编配器 Kubernetes、集群生命周期、应用程序生命周期以及安全框架（监管、风险和合规）。

因此，Red Hat Advanced Cluster Management for Kubernetes 平台主要处理与平台的配置和管理相关的技术数据，其中的一些数据可能会涉及到受 GDPR 影响的数据。Red Hat Advanced Cluster Management for Kubernetes 平台还处理管理平台的用户的信息。在这个文档中会介绍这些数据，以使负责满足 GDPR 要求的用户了解这些内容。

这些数据会在本地或者远程文件系统中，以配置文件或数据库的形式存在。在 Red Hat Advanced Cluster Management for Kubernetes 平台上运行的应用程序可能会涉及到其它形式的、受 GDPR 影响的个人数据。用于保护和管理平台数据的机制也可用于平台上运行的应用程序。对于在 Red Hat Advanced Cluster Management for Kubernetes 平台上运行的应用程序所收集个人数据，可能还需要额外的机制来进行管理和保护。

为了更好了解 Red Hat Advanced Cluster Management for Kubernetes 平台及其数据流，您需要对 Kubernetes、Docker 和 Operator 的工作原理有所了解。这些开源组件是 Red Hat Advanced Cluster Management for Kubernetes 平台的基础。您使用 Kubernetes 部署来放置应用程序实例，这些实例会被内置到引用 Docker 镜像的 Operator 中。Operator 包含应用程序的详细信息，Docker 镜像包含应用程序需要运行的所有软件包。

1.5.5.1. Red Hat Advanced Cluster Management for Kubernetes 平台的数据流类型

作为一个平台，Red Hat Advanced Cluster Management for Kubernetes 需要不同类别的技术数据，这些数据可能会被视为个人数据，如管理员用户 ID 和密码、服务用户 ID 和密码、IP 地址以及 Kubernetes 节点名称。Red Hat Advanced Cluster Management for Kubernetes 平台还处理管理平台的用户的信息。在平台中运行的应用程序可能会使用与平台无关的其他类别的个人数据。

本文档后续部分将介绍如何收集/创建这些技术数据、存储、访问、安全、日志和删除。

1.5.5.2. 用于在线联系的个人数据

用户可以以各种方式提交在线评论/反馈/请求，主要有：

- 如果使用 Slack 频道，公共的 Slack 社区
- 产品文档中的公共注释或问题单
- 技术社区中的公共对话

通常，只使用客户名称和电子邮件地址，以便可以进行回复，对个人数据的使用符合 红帽在线隐私声明。

1.5.6. 数据收集

Red Hat Advanced Cluster Management for Kubernetes 平台不会收集敏感的个人数据。它会创建和管理技术数据，如管理员用户 ID 和密码、服务用户 ID 和密码、IP 地址以及 Kubernetes 节点名称。这些数据可能会被视为个人数据。Red Hat Advanced Cluster Management for Kubernetes 平台还处理管理平台的用户的信息。只有系统管理员才可以通过使用基于角色的访问控制的管理控制台访问此类信息，或者系统管理员登陆到一个 Red Hat Advanced Cluster Management for Kubernetes 平台节点才可以访问。

在 Red Hat Advanced Cluster Management for Kubernetes 平台上运行应用程序可能会收集个人数据。

当您在评估 Red Hat Advanced Cluster Management for Kubernetes 运行容器化应用程序，并需要符合 GDPR 要求时，您必须考虑应用程序收集的个人数据类型以及是如何管理这些数据的，例如：

- 当数据流向应用程序或从应用程序流出时，数据是如何被保护的？数据是否在传输中加密？
- 数据是如何被应用程序存储的？数据在不用时是否被加密？
- 用于访问应用程序的凭证是如何被收集和存储的？
- 应用程序用于访问数据源所使用的凭证是如何被收集和存储的？
- 如何根据需要删除应用程序收集的数据？

这不是 Red Hat Advanced Cluster Management for Kubernetes 平台所收集的数据类型的完整列表。它只作为一个示例以供考虑。如果您对数据类型有任何疑问，请联络红帽。

1.5.7. 数据存储

对于与配置和管理平台相关的技术数据，Red Hat Advanced Cluster Management for Kubernetes 平台会把它们以配置文件或数据库的形式保存在本地或远程文件系统中。对于存储的数据，必须考虑它们的安全性。Red Hat Advanced Cluster Management for Kubernetes 平台支持使用 dm-crypt 对存储的数据进行加密。

下面是主要的数据存储形式，您可能需要进行与 GDPR 相关的考虑。

- 平台配置数据： 通过更新带有常规设置、Kubernetes、日志、网络、Docker 和其他设置属性的配置 YAML 文件，可以自定义 Red Hat Advanced Cluster Management for Kubernetes 平台的配置。这些数据会作为 Red Hat Advanced Cluster Management for Kubernetes 平台的安装程序的输入被使用来部署节点。这些属性还包括用于 bootstrap 的管理员用户 ID 和密码。

- Kubernetes 配置数据： Kubernetes 集群状态数据保存在分布式“键-值”存储 etcd 中。

- 用户身份验证数据，包括用户 ID 和密码： 通过客户端企业级 LDAP 目录处理用户 ID 和密码管理。在 LDAP 中定义的用户和组可添加到 Red Hat Advanced Cluster Management for Kubernetes 平台的团队中，并分配访问角色。Red Hat Advanced Cluster Management for Kubernetes 平台会储存来自 LDAP 的电子邮件地址和用户 ID，但不保存密码。Red Hat Advanced Cluster Management for Kubernetes 平台会存储组名称，并在登录时缓存用户所属的可用组。组成员不会以长期形式有效。必须考虑在企业级 LDAP 中保护用户和组数据。Red Hat Advanced Cluster Management for Kubernetes 平台也包括了一个身份认证服务 Open ID Connect（OIDC），它与企业目录服务进行交互并维护访问令牌。此服务使用 ETCD 作为后端存储。

- 服务身份验证数据，包括用户 ID 和密码： Red Hat Advanced Cluster Management for Kubernetes 平台组件使用的、用于在组件间进行访问的凭证被定义为 Kubernetes Secret。所有 Kubernetes 资源定义都保留在 etcd 键-值形式的数据存储中。初始凭证值在平台配置数据中定义，作为 Kubernetes Secret 配置 YAML 文件。如需更多信息，请参阅管理 secret。

1.5.8. 数据访问

您可以通过以下定义的产品接口集合访问 Red Hat Advanced Cluster Management for Kubernetes 平台数据。

- Web 用户界面（控制台）

- Kubernetes kubectl CLI

- Red Hat Advanced Cluster Management for Kubernetes CLI

- oc CLI

这些接口可用于对 Red Hat Advanced Cluster Management for Kubernetes 集群进行管理级别的更改。当发出一个请求时，安全使用 Red Hat Advanced Cluster Management for Kubernetes 的管理访问权限涉及三个逻辑的、有特定顺序的阶段： 身份验证、角色映射和授权。

1.5.8.1. 身份验证

Red Hat Advanced Cluster Management for Kubernetes 平台的身份验证管理程序接受来自控制

台的用户凭证，并将凭证转发到后端的 OIDC 供应商，后者根据企业目录验证用户凭证。然后，OIDC 供应商会向身份验证程序返回一个带有 JSON Web Token（JWT）内容的身份验证 cookie（auth-cookie）。JWT 令牌包括了身份验证请求时的组成员信息，以及用户 ID 和电子邮件地址等信息。然后，这个身份验证 cookie 会发送到控制台。在会话存在期间，cookie 会被刷新。在退出控制台或关闭浏览器后，这个 cookie 会在 12 小时内有效。

对于所有来自控制台的验证请求，前端 NGINX 服务器对请求中的可用身份验证 cookie 进行解码，并通过调用验证管理程序来验证请求。

Red Hat Advanced Cluster Management for Kubernetes 平台的 CLI 需要用户在登陆时提供凭证。

kubectl 和 oc CLI 也需要凭证来访问集群。这些凭证可以从管理控制台获得，并在 12 小时后过期。支持通过服务帐户访问。

1.5.8.2. 角色映射

Red Hat Advanced Cluster Management for Kubernetes 平台支持的基于角色的控制访问（RBAC）。在角色映射阶段，身份验证阶段提供的用户名映射到用户或组角色。在授权哪些管理操作可由经过身份验证的用户执行时使用角色。

1.5.8.3. 授权

Red Hat Advanced Cluster Management for Kubernetes 平台对集群配置操作的角色控制访问，适用于 catalog 和 Helm 资源，以及 Kubernetes 资源。提供了几个 IAM（Identity and Access Management）角色，包括 Cluster Administrator、Administrator、Operator、Editor、Viewer。在将用户或用户组添加到一个团队时，会为用户或用户组分配一个角色。对资源的团队访问可以由命名空间控制。

1.5.8.4. Pod 安全性

Pod 安全策略用于设置集群级别的控制，控制 pod 可以做什么或可以访问什么。

1.5.9. 数据处理

Red Hat Advanced Cluster Management for Kubernetes 的用户可以通过系统配置，来处理和保护与配置和管理相关的技术数据。

基于角色的访问控制 （RBAC）可控制用户可访问哪些数据和功能。

Data-in-transit 通过使用 TLS 加以保护。HTTP （TLS 底层）是用来在用户客户端和后端服务间进行安全的数据传输。用户可以指定在安装过程中要使用的 root 证书。

Data-at-rest 的保护是通过使用 dm-crypt 加密数据来实现的。

那些用来管理和保护 Red Hat Advanced Cluster Management for Kubernetes 平台的技术数据的机制，同样可用于对用户开发的或用户提供的应用程序的个人数据进行管理和保护。客户可以开发自己的功能进行进一步的控制。

1.5.10. 数据删除

Red Hat Advanced Cluster Management for Kubernetes 平台提供了命令、API 和用户界面操作以删除由产品创建或收集的数据。用户可以使用这些功能删除技术数据，如服务用户 ID 和密码、IP 地址、Kubernetes 节点名称或其他平台配置数据，并可以管理平台的用户的信息。

Red Hat Advanced Cluster Management for Kubernetes 平台中可用来进行数据删除的方法：

- 与平台配置相关的所有技术数据，都可通过管理控制台或 Kubernetes kubectl API 删除。

Red Hat Advanced Cluster Management for Kubernetes 平台中用于删除帐户数据的方法：

- 与平台配置相关的所有技术数据，都可通过 Red Hat Advanced Cluster Management for Kubernetes 或 Kubernetes kubectl API 删除。

删除通过企业级 LDAP 目录管理的用户 ID 和密码数据的功能，需要由与 Red Hat Advanced Cluster Management for Kubernetes 平台集成的 LDAP 产品提供。

1.5.11. 限制使用个人数据的能力

通过本文档中介绍的工具，Red Hat Advanced Cluster Management for Kubernetes 平台可以对最终用户对个人数据的使用加以限制。

根据 GDPR，用户的访问、修改和处理权限都需要被加以限制。请参考本文档的其它部分来控制以下内容：

- 访问权限
  - Red Hat Advanced Cluster Management for Kubernetes 平台管理员可以使用 Red Hat Advanced Cluster Management for Kubernetes 平台的功能提供个人对他们的数据的独立访问。
  - Red Hat Advanced Cluster Management for Kubernetes 平台管理员可以使用 Red Hat Advanced Cluster Management for Kubernetes 平台的功能，可以提供 Red Hat Advanced Cluster Management for Kubernetes 平台为某个个人保存的什么个人数据的信息。
- 修改权限
  - Red Hat Advanced Cluster Management for Kubernetes 平台管理员可以使用 Red Hat Advanced Cluster Management for Kubernetes 平台的功能来允许一个个人修改自己的数据。
  - Red Hat Advanced Cluster Management for Kubernetes 平台管理员可以使用 Red Hat Advanced Cluster Management for Kubernetes 平台的功能为一个个人修改其个人数据。
- 限制处理的权利
  - Red Hat Advanced Cluster Management for Kubernetes 平台管理员可以使用 Red Hat Advanced Cluster Management for Kubernetes 平台的功能停止处理一个个人的数据。

1.5.12. 附录

作为一个平台，Red Hat Advanced Cluster Management for Kubernetes 需要不同类别的技术数据，这些数据可能会被视为个人数据，如管理员用户 ID 和密码、服务用户 ID 和密码、IP 地址以及 Kubernetes 节点名称。Red Hat Advanced Cluster Management for Kubernetes 平台也会处理管理平台的人员的信息。在平台中运行的应用程序可能会引入其它在平台中未知的个人数据类别。

本附录包含平台服务日志记录的数据详情。