Red Hat Advanced Cluster Management for Kubernetes 2.4

发行注记

参阅更多与发行注记相关的信息，了解新的、勘误更新、已知问题、弃用和删除以及 GDPR 和 FIPS 就绪的产品注意事项。

Last Updated: 2023-03-08

Red Hat Advanced Cluster Management for Kubernetes 2.4 发行注记

参阅更多与发行注记相关的信息，了解新的、勘误更新、已知问题、弃用和删除以及 GDPR 和 FIPS 就绪的产品注意事项。

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

Copyright © 2022 | You need to change the HOLDER entity in the en-US/Release_notes.ent file |.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at
http://creativecommons.org/licenses/by-sa/3.0/
. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

摘要

参阅更多与发行注记相关的信息，了解新的、勘误更新、已知问题、弃用和删除以及 GDPR 和 FIPS 就绪的产品注意事项。

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. 集群 6
1.1.3. Applications 6
1.1.4. 监管 7
1.2. 勘误更新 7
1.2.1. Errata 2.4.9 7
1.2.2. Errata 2.4.8 7
1.2.3. Errata 2.4.7 7
1.2.4. Errata 2.4.6 8
1.2.5. Errata 2.4.5 8
1.2.6. Errata 2.4.4 8
1.2.7. Errata 2.4.3 8
1.2.8. Errata 2.4.2 9
1.2.9. Errata 2.4.1 9
1.3. 已知问题 9
1.3.1. 已知的与文档相关的问题 10
1.3.1.1. 客户门户网站中的文档链接可能会链接到更高级别的部分 10
1.3.2. 已知的与安装相关的问题 11
1.3.2.1. 升级 Red Hat Advanced Cluster Management 后可能会没有备份 Pod 11
1.3.2.2. 从 2.2.x 升级到 2.3.4 可能会导致 klusterlet 删除 11
1.3.2.3. 从 2.2.x 升级到 2.3.1 版本无法进行 12
1.3.2.4. OpenShift Container Platform 集群升级失败的状态 12
1.3.3. 已知的与 Web 控制台相关的问题 13
1.3.3.1. Cluster 页面和搜索结果之间节点的不同 13
1.3.3.2. LDAP 用户名是区分大小写的 13
1.3.3.3. Firefox 的较老版本可能无法显示控制台的功能 13
1.3.3.4. searchcustomization 存储大小的限制 13
1.3.4. 已知的可观察性问题 13
1.3.4.1. Service-level Overview 仪表板上重复的 local-clusters 13
1.3.4.2. Observability endpoint operator 无法拉取镜像 13
1.3.4.3. 没有来自 ROKS 集群的数据 14
1.3.4.4. ROKS 集群没有 etcd 数据 14
1.3.4.5. search-collector pod 的高 CPU 使用率 14
1.3.4.6. 因为证书无效，搜索 pod 无法完成 TLS 握手过程 14
1.3.4.7. Grafana 控制台中没有指标数据 14
1.3.4.8. 受管集群上的 Prometheus 数据丢失 15
1.3.4.9. 消耗不按顺序示例时出错 15
1.3.5. 已知的与集群管理相关的问题 16
1.3.5.1. cluster 和 clusterimageset 频道不会自动同步 16
1.3.5.2. 使用自定义 CA 证书恢复到其恢复的 hub 集群连接可能会失败 16
1.3.5.3. local-cluster 可能无法自动重新创建 16
1.3.5.4. 在创建内部集群时需要选择子网 16
1.3.5.5. Google Cloud Platform 上的集群置备失败 17
1.3.5.6. 使用 Infrastructure Operator 进行集群置备失败 17
1.3.5.7. 无法休眠 Azure Government 集群 18
1.3.5.8. 使用不同名称重新导入后 local-cluster 状态为离线 18
1.3.5.9. 在代理环境中使用 Ansible 自动化进行集群置备失败 19
1.3.5.10. klusterlet Operator 的版本必须与 hub 集群相同 19

1.3.5.11. 无法手动删除受管集群命名空间 19
1.3.5.12. 升级到 2.3 后无法更改集群中的凭证 19
1.3.5.13. hub 集群和受管集群的时钟未同步 19
1.3.5.14. 不支持导入 IBM OpenShift Container Platform Kubernetes Service 集群的特定版本 19
1.3.5.15. 分离 OpenShift Container Platform 3.11 不会删除 open-cluster-management-agent 19
1.3.5.16. 不支持为置备的集群进行自动 secret 更新 20
1.3.5.17. 无法在搜索中查看受管集群的节点信息 21
1.3.5.18. 销毁集群的进程没有完成 21
1.3.5.19. 无法使用控制台在 OpenShift Container Platform Dedicated 上升级 OpenShift Container Platform 受管集群 22
1.3.5.20. 工作管理器附加搜索详情 22
1.3.5.21. 在跨架构创建集群时，需要手动创建的发行镜像 22
1.3.5.22. IBM Power 或 IBM Z 系统 hub 集群不支持 Argo CD 24
1.3.5.23. 无法使用 Ansible Tower 与 IBM Power 或 IBM Z 系统 hub 集群集成 24
1.3.5.24. 非 Red Hat OpenShift Container Platform 受管集群必须启用 LoadBalancer 24
1.3.6. 已知的与应用程序管理相关的问题 25
1.3.6.1. 除非根据订阅管理员部署策略资源 25
1.3.6.2. 带有多个订阅的应用程序拓扑集群没有正确分组 25
1.3.6.3. 应用程序 Ansible hook 独立模式 26
1.3.6.4. 为应用程序编辑角色错误 27
1.3.6.5. 编辑放置规则错误的角色 27
1.3.6.6. 在更新的放置规则后没有部署应用程序 27
1.3.6.7. Subscription operator 不会创建一个 SCC 28
1.3.6.8. 应用程序频道需要唯一的命名空间 29
1.3.6.9. Ansible Automation Platform 作业失败 29
1.3.6.10. Ansible Automation Platform operator 在代理外访问 Ansible Tower 29
1.3.6.11. 在版本 2.4 中编辑 Helm Argo 应用程序时不会显示模板信息 29
1.3.6.12. 应用程序名称要求 29
1.3.6.13. 应用程序控制台表 30
1.3.7. 已知的监管问题 30
1.3.7.1. 无法从 Red Hat Advanced Cluster Management 注销 30
1.3.7.2. 放置资源限制 30
1.3.7.3. Gatekeeper operator 安装失败 31
1.3.7.4. 当命名空间处于 Terminating 状态时，配置策略列出了 complaint 31
1.3.8. 备份和恢复已知问题 31
1.3.8.1. 备份和恢复功能不适用于 IBM Power 和 IBM Z 31
1.3.8.2. 在恢复操作后，应用程序和策略在受管集群中没有资源状态 31
1.4. 弃用和删除 31
1.4.1. API 弃用和删除 32
1.4.1.1. API 弃用 32
1.4.2. Red Hat Advanced Cluster Management 弃用 32
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 35
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 40
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 41
1.5.10. 数据删除 41
1.5.11. 限制使用个人数据的能力 42
1.5.12. 附录 42
1.6. FIPS 就绪性 43
1.6.1. 限制 43

第 1 章 发行注记

Red Hat Advanced Cluster Management 的 2.3 版本 *被删除* 且不再被支持。其文档可能仍然可用，但不再有任何新的勘误或其他更新。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
- FIPS 就绪性

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。
- 有关该产品的主要组件的更多信息，请参阅 多集群架构。
- 入门指南 引用了您开始使用的常见任务，以及 *故障排除指南*。
- Web 控制台
  - Observability（可观察性）
- 集群
- Applications
- 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。

1.1.1.1. Observability（可观察性）

- 在可观察性服务中添加了记录规则，以计算 Kubernetes API 服务器服务级别指示器 (SLI) 和服务级别目标 (SLO)。如需了解更多详细信息，请参阅 创建自定义规则。

- 现在，您可以从 Grafana 仪表板查看 Kubernetes API 服务器的服务级别概述中的集群聚合。请参阅 查看 Kubernetes API 服务器仪表板的集群群服务级别概述。
- 通过 Grafana 仪表板查看在 7 或 30 天期间内出现的错误预算和时间，服务可在 Kubernetes API 服务器的集群服务级别概述中使用停机时间。请参阅查看 Kubernetes API 服务器仪表板的集群服务级别概述。
- 使用 Red Hat Advanced Cluster Management 和 Grafana 8.1.3 查看指标数据。如需更多信息，请参阅 Observing 环境。
- 从 Grafana 仪表板查看 Kubernetes API 服务器的集群服务级别概述。请参阅查看 Kubernetes API 服务器仪表板的集群服务级别概述。

1.1.2. 集群

- 现在，您可以在以下平台上托管 OpenShift Container Platform hub 集群，并管理在这些平台上置备的集群：
  - IBM Z 和 LinuxONE
  - IBM Power 系统
- 使用 Red Hat Advanced Cluster Management 控制台创建和管理 Microsoft Azure Government 集群。如需更多信息，请参阅为 Microsoft Azure 创建凭证。
- 创建基础架构环境以管理您的内部集群。如需更多信息，请参阅 创建基础架构环境。
- 使用 Red Hat Advanced Cluster Management 控制台在基础架构环境中创建内部集群。如需更多信息，请参阅在内部环境中创建集群。
- 根据附加组件的状态选择受管集群。如需更多信息，请参阅 附加状态。
- 现在，在创建集群时，您可以使用 Red Hat Advanced Cluster Management 控制台为集群配置代理信息。如需更多信息，请参阅创建集群。

技术预览：

- 使用集群备份和恢复操作器来调度集群资源的备份和恢复。如需更多信息，请参阅 集群备份和恢复 Operator（技术预览）。
- 使用零接触调配部署多个 SNO 集群.如需更多信息，请参阅 OpenShift Container Platform 文档中的在断开连接的环境中大规模部署分布式单元。
- 使用 VolSync 复制持久性卷，这可让您在持久性卷中创建数据副本。如需更多信息，请参阅使用 VolSync 复制持久性卷。

1.1.3. Applications

从 Application 控制台 **Create application** 下拉菜单中选择要创建的应用程序类型。您可以选择创建 Git 仓库、Helm 仓库或对象存储仓库订阅。订阅是频道中的 Kubernetes 资源（源仓库）。

技术预览： 现在，您还可以选择从同一下拉菜单中选择 Argo CD ApplicationSet，以便您可以在更多集群中管理 Argo CD 应用程序。

通过 YAML Editor，您可以在修改字段时看到创建或编辑应用程序时的文件更新。

您可以在创建应用程序时或之后指定辅助频道。当您创建辅助频道时，应用程序会在主频道失败时使用辅助频道。

作为订阅管理员，您可以创建一个允许和拒绝列表。现在，您还可以将所有应用程序资源部署到订阅命名空间中。有关订阅管理员任务和其他高级配置主题的更多信息，请参阅应用程序高级配置。

有关其他应用程序主题，请参阅管理应用程序。

1.1.4. 监管

- 您可以使用 *Governance* 页面中显示的新列。使用控制台中的 *Source* 列来确定使用 GitOps 部署的策略。使用 *Status* 列来验证策略的启用。如需更多信息，请参阅管理安全策略。
- 现在，您可以使用已就绪的 Red Hat Advanced Cluster Management 集群。如需了解更多详细信息，请参阅 FIPS 就绪。
- 使用 Red Hat Insights 和监管的集成来发送监管违反情况的警报。您还可以识别发送违反情况的组件。如需更多信息，请参阅管理 Insights PolicyReports。
- 使用支持批量操作的新过滤选项自定义仪表板。如需更多信息，请参阅自定义监管页面。
- 使用 **policy_governance_info** 指标查看趋势并分析任何策略故障。如需了解更多详细信息，请参阅监管指标。

如需了解更多有关仪表板和策略框架的信息，请参阅监管。

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 2.4，这个列表包括两个 *未被* FIPS 批准的加密方式。如果您从 2.4.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加密方式：ECD **HE-ECDSA-CHACHA20-POLY1305** 和 **ECDHE-RSA-CHACHA20-POLY1305**。

1.2.1. Errata 2.4.9

- 修复了在将带有特定键和值的自定义标签添加到策略时导致服务拒绝所有策略的问题。
- 修复了在从 Red Hat OpenShift Container Platform 控制台启动升级作业时所报告的升级版本和进度的问题。(Bugzilla 程序9684)
- 为一个或多个产品容器镜像提供更新。

1.2.2. Errata 2.4.8

- 为一个或多个产品容器镜像和安全修复提供更新。

1.2.3. Errata 2.4.7

- 修复了阻止某些 Grafana 仪表板中的数据显示的问题。
- 为一个或多个产品容器镜像提供更新。

1.2.4. Errata 2.4.6

- 修复了有时会导致一个空白应用程序 *概述页* 的问题。(Bugzilla #2036197)
- 从集群创建过程中删除已弃用的 API。(Bugzilla #2041540)
- 现在，在创建 VMware vSphere 集群时，可以在网络名称中使用空白空格。(Bugzilla #2074766)
- 解决了在 Red Hat Advanced Cluster Management 中更新 **local-cluster** 的选项，在使用 OpenShift Container Platform 控制台手动应用更新时会导致同一集群挂起的问题。(Bugzilla #2079418)
- 修复了在从 Red Hat Advanced Cluster Management 版本 2.2 升级完成后防止使用 Red Hat Advanced Cluster Management 2.4 创建集群的问题。(Bugzilla #2089490)
- 置备网络设置现在是可选的，以支持不需要 provisioning 网络的裸机部署。(Bugzilla #2096406)
- 修复了在尝试创建与现有集群相同的名称和命名空间时导致现有集群销毁的问题。(Bugzilla #2102436)
- 为一个或多个产品容器镜像提供更新。

1.2.5. Errata 2.4.5

- 修复了可观察性升级问题。(Bugzilla #2087277)
- 解决 Redis 中导致大量错误日志的搜索和失败。健康监控已被解决，允许搜索组件恢复并减少日志详细程度。(Bugzilla #2065318)
- 修复了在没有反馈的情况下创建卡在 **创建** 阶段的受管 VMware 集群的问题。(Bugzilla #1937078)

1.2.6. Errata 2.4.4

- 修复了显示为集群创建状态的问题，但为集群提供的无效信息会导致创建失败。**(Bugzilla #1995380)**
- **解决了链接到额外登录页面的问题，有时会在一小时登录或自动注销时导致无限循环。(Bugzilla #2061958)**
- **为一个或多个产品容器镜像提供更新。**

1.2.7. Errata 2.4.3

- 修复了在使用 ecdsa-sha2-nistp521 ssh 密钥时阻止集群创建的问题。(Bugzilla #2048500)

- 为一个或多个产品容器镜像提供更新。

1.2.8. Errata 2.4.2

- 修复了一个问题，阻止一些支持 LimitRange 的策略在 pod 重启后对一些属性采用更改。(GitHub #19160)

- 为一个或多个产品容器镜像提供更新。

1.2.9. Errata 2.4.1

- 从受管集群详情视图中显示的 PolicyReport 数据，过滤掉由监管和风险提供的所有策略，因为这些策略的数量会在该页面的其他位置显示。(GitHub #17438)

- 删除 Operatorhub Installation 控制台中的可选 imagepullsecret 参数示例，以防止意外使用集群中不存在的 pull secret。(GitHub #17884)

- 修复了在销毁集群时使集群池中的休眠集群一直处于 Detaching 状态，受管集群状态不会变为 Unknown 的问题。升级到 ACM 2.4.1 后，处于 Detaching 状态的所有集群及其命名空间会自动终止并恢复预期的行为。无需手动干预来清理这些集群或 hub 集群中的命名空间。(GitHub #18249)

- 删除必要的步骤，以启用功能门来添加中央基础架构管理(CIM)环境。

- 修复了防止 ClusterDeployment 在 Cluster Pool 控制台中显示失败导致验证错误的问题。(Bugzilla #1995380)

- 为一个或多个产品容器镜像提供更新。

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。

- 已知的与文档相关的问题
- 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
- 备份和恢复已知问题

1.3.1. 已知的与文档相关的问题

1.3.1.1. 客户门户网站中的文档链接可能会链接到更高级别的部分

在某些情况下，客户门户网站中的 Red Hat Advanced Cluster Management 文档的其他部分的内部链接不会直接链接到指定部分。在某些情况下，链接会指向最高级别的部分。

如果发生这种情况，您可以手动找到指定的部分，或者完成以下步骤以解决：

1. 复制未解析到正确部分的链接，并将它粘贴到浏览器地址栏中。例如，它可能是：https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.4/html/clusters/index#volsync。

2. 在链接中，将 html 替换为 html-single。新 URL 应当如下所示：
https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.4/html-single/clusters/index#volsync

3. 链接到新 URL 以在文档中找到指定部分。

1.3.2. 已知的与安装相关的问题

1.3.2.1. 升级 Red Hat Advanced Cluster Management 后可能会没有备份 Pod

将 Red Hat Advanced Cluster Management 升级到新版本后，属于 StatefulSet 的少数 pod 可能会处于 失败状态。这种不常用的事件是由已知 Kubernetes 问题 造成的。

这个问题的一个临时解决方案是删除失败的 pod。Kubernetes 会自动使用正确的设置重新启动它。

1.3.2.2. 从 2.2.x 升级到 2.3.4 可能会导致 klusterlet 删除

从 2.2.x 升级到 2.3.4 后，可能会删除 Klusterlet。请参阅以下流程来解决这个问题：

1. 将 work-agent 升级到 2.3.3。

   a. 创建一个 JSON 文件 work-image-override.json，其中包含以下 JSON 内容：

```
[
  {
    "image-name": "work-rhel8",
    "image-remote": "registry.redhat.io/rhacm2",
    "image-digest":
"sha256:b6606f6bb6504acfb48f13cd5296473c17088caf380097ff7ce316f781c4f196",
    "image-key": "work"
  }
]
```

   b. 为 hub 集群上的镜像覆盖创建 ConfigMap：

```
kubectl -n open-cluster-management create configmap work-image-override --from-file=./work-image-override.json
```

c. **通过在 hub 集群中注解 mch 来启用镜像覆盖。**

```
kubectl -n open-cluster-management annotate mch multiclusterhub --overwrite mch-imageOverridesCM=work-image-override
```

d. **重启 multiclusterhub-operator 以强制执行更改。**

```
kubectl -n open-cluster-management delete pod multiclusterhub-operator-xxxxx-xxxxx
```

等待大约 30 分钟，确保所有受管集群上运行的 work-agent 都通过覆盖的镜像重启。

2. **从 2.2.x 升级到 2.3.4。**

3. 为 **work-agent 禁用镜像覆盖。**

4. **升级完成后，为 work-agent 删除镜像覆盖是安全的。**

```
kubectl -n open-cluster-management annotate mch multiclusterhub mch-imageOverridesCM--overwrite
kubectl -n open-cluster-management delete configmap work-image-override
```

1.3.2.3. 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。

1.3.2.4. 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。

1.3.3. 已知的与 Web 控制台相关的问题

1.3.3.1. 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。

1.3.3.2. 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。

1.3.3.3. 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。

1.3.3.4. 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
```

1.3.4. 已知的可观察性问题

1.3.4.1. Service-level Overview 仪表板上重复的 local-clusters

当各种 hub 集群使用相同的 S3 存储部署 Red Hat Advanced Cluster Management observability 时，可以在 *Kubernetes/Service-Level Overview/API Server* 仪表板中检测并显示*重复*的 local-clusters。重复的集群在以下面板中影响结果： *Top Clusters*、*超过 SLO 的集群数*，以及*满足 SLO 的集群数量*。local-clusters 是与共享 S3 存储关联的唯一集群。要防止多个 local-clusters 显示在仪表板中，建议每个唯一的 hub 集群使用针对 hub 集群的 S3 存储桶来部署可观察性。

1.3.4.2. 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。

1.3.4.3. 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)

1.3.4.4. 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。

1.3.4.5. search-collector pod 的高 CPU 使用率

当在管理 1000 个集群的 hub 集群中禁用搜索时，search-collector pod 会因为内存不足(OOM)而崩溃。完成以下步骤：

1. 如果在 hub 集群上禁用了搜索，这意味着没有部署 search-redisgraph-pod，通过将 search-collector 部署缩减为 0 个副本来减少内存用量。

2. 如果在 hub 集群上启用了搜索，这意味着部署了 search-redisgraph-pod，请编辑 search-collector 部署来增加分配的内存。

1.3.4.6. 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。

1.3.4.7. 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。../../html-single/access_control#role-based-access-control

1.3.4.8. 受管集群上的 Prometheus 数据丢失

默认情况下，OpenShift 上的 Prometheus 使用临时存储。Prometheus 会在重启时丢失所有指标数据。

如果在由 Red Hat Advanced Cluster Management 管理的 OpenShift Container Platform 受管集群上启用或禁用了可观察性，observability 端点 Operator 会添加额外的 alertmanager 配置来自动重启本地 Prometheus，以此更新 cluster-monitoring-config ConfigMap。

1.3.4.9. 消耗不按顺序示例时出错

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。当出现问题时，Thanos 接收器丢弃数据，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。

1.3.5. 已知的与集群管理相关的问题

1.3.5.1. cluster 和 clusterimageset 频道不会自动同步

clusterimageset 处于 "fast" 频道，但置备的集群处于 "stable" 频道。目前，该产品不会将 "channel" 同步到置备的 OpenShift Container Platform 集群。

在 OpenShift Container Platform 控制台中进入正确的频道： Administration > Cluster Settings > Details Channel。

1.3.5.2. 使用自定义 CA 证书恢复到其恢复的 hub 集群连接可能会失败

恢复受管集群使用自定义 CA 证书的 hub 集群的备份后，受管集群和 hub 集群之间的连接可能会失败。这是因为在恢复的 hub 集群上没有备份 CA 证书。要恢复连接，将受管集群的命名空间中自定义 CA 证书信息复制到恢复的 hub 集群上的 <managed_cluster>-admin-kubeconfig secret。

提示： 如果您在创建备份副本前将此 CA 证书复制到 hub 集群，备份副本会包括 secret 信息。当使用备份副本来恢复时，hub 和受管集群之间的连接会自动完成。

1.3.5.3. local-cluster 可能无法自动重新创建

如果在 disableHubSelfManagement 被设置为 false 时删除 local-cluster，则 MulticlusterHub operator 会重新创建 local-cluster。分离 local-cluster 后，可能不会自动重新创建 local-cluster。

- 要解决这个问题，修改由 MulticlusterHub operator 监控的资源。请参见以下示例：

```
oc delete deployment multiclusterhub-repo -n <namespace>
```

- 要正确分离 local-cluster，在 MultiClusterHub 中将 disableHubSelfManagement 设置为 true。

1.3.5.4. 在创建内部集群时需要选择子网

当使用 Red Hat Advanced Cluster Management 控制台创建内部集群时，您必须为集群选择一个可

用子网。它没有标记为必填字段。

1.3.5.5. 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。

1.3.5.6. 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

- **4.9.6 及更早版本**

为了避免这个错误，将 **OpenShift Container Platform** 升级到 **4.8.18** 或更高版本，或 **4.9.7** 或更高版本。

1.3.5.7. 无法休眠 Azure Government 集群

当您尝试休眠 **Azure Government** 集群时，休眠会失败，并显示添加到置备 **pod** 日志中的以下错误：

```
Confidential Client is not supported in Cross Cloud request
```

1.3.5.8. 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** 和重新导入的集群的状态将 离线。

要从这个问题单中恢复，请完成以下步骤：

1. 在 **hub** 集群中运行以下命令，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**。

1.3.5.9. 在代理环境中使用 Ansible 自动化进行集群置备失败

当满足以下任一条件时，配置为自动置备受管集群的 AnsibleJob 模板可能会失败：

- hub 集群启用了集群范围代理。
- Ansible Tower 只能通过代理来访问。

1.3.5.10. klusterlet Operator 的版本必须与 hub 集群相同

如果您通过安装 klusterlet operator 导入受管集群，klusterlet Operator 的版本必须与 hub 集群的版本相同，或者 klusterlet Operator 将无法正常工作。

1.3.5.11. 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。

1.3.5.12. 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。

1.3.5.13. 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。

1.3.5.14. 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。

1.3.5.15. 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
```

1.3.5.16. 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}"} }]'
```

1.3.5.17. 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。

1.3.5.18. 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***。

1.3.5.19. 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。

1.3.5.20. 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。

1.3.5.21. 在跨架构创建集群时，需要手动创建的发行镜像

要在与 hub 集群架构不同的架构中创建受管集群，您需要创建包含这两个架构文件的发行镜像 (ClusterImageSet)。例如，如果要从 ppc64le 或 s390x hub 集群创建 x86_64 集群，则需要创建发行镜像。如果使用两组文件创建发行镜像，集群创建成功，因为新发行镜像启用 OpenShift Container Platform 发行 registry 来提供多架构镜像清单。

要临时解决这个问题，请针对您的架构类型完成类似以下示例的步骤：

1. 在 OpenShift Container Platform release registry 中，创建一个包含 x86_64、s390x 和 ppc64le 发行镜像的清单列表。

   a. 从 Quay 存储库拉取环境中这两个架构的清单列表：

   ```
   $ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-x86_64
   $ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-ppc64le
   $ podman pull quay.io/openshift-release-dev/ocp-release:4.9.1-s390x
   ```

   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:4.9.1-x86_64 <private-
repo>/ocp-release:4.9.1-x86_64
$ podman push quay.io/openshift-release-dev/ocp-release:4.9.1-ppc64le <private-
repo>/ocp-release:4.9.1-ppc64le
$ podman push quay.io/openshift-release-dev/ocp-release:4.9.1-s390x <private-
repo>/ocp-release:4.9.1-s390x
```

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:4.9.1-x86_64
$ podman manifest add mymanifest <private-repo>/ocp-release:4.9.1-ppc64le
$ podman manifest add mymanifest <private-repo>/ocp-release:4.9.1-s390x
```

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:4.9.1
```

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: img4.9.1-appsub
spec:
  releaseImage: <private-repo>/ocp-release:4.9.1
```

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。

1.3.5.22. IBM Power 或 IBM Z 系统 hub 集群不支持 Argo CD

Argo CD 与 Red Hat Advanced Cluster Management 集成无法在在 IBM Power 或 IBM Z 系统上运行的 Red Hat Advanced Cluster Management hub 集群上工作，因为没有可用的 ppc64le 或 s390x 镜像。

1.3.5.23. 无法使用 Ansible Tower 与 IBM Power 或 IBM Z 系统 hub 集群集成

当 Red Hat Advanced Cluster Management for Kubernetes hub 集群在 IBM Power 或 IBM Z 系统上运行时，您无法使用 Ansible Tower 集成，因为 Ansible Automation Platform Resource Operator 不提供 ppc64le 或 s390x 镜像。

1.3.5.24. 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。

1.3.6. 已知的与应用程序管理相关的问题

1.3.6.1. 除非根据订阅管理员部署策略资源

对于 Red Hat Advanced Cluster Management 版本 2.4，默认情况下，policy.open-cluster-management.io/v1 资源不再被应用程序订阅部署。

订阅管理员需要部署应用程序订阅以更改此默认行为。

如需更多信息，请参阅创建 allow 和 deny 列表 作为订阅管理员。在之前的 Red Hat Advanced Cluster Management 版本中，由现有应用程序订阅部署的 policy.open-cluster-management.io/v1 资源仍然保留，除非应用程序订阅由订阅管理员部署。

1.3.6.2. 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。

1.3.6.3. 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。

1.3.6.4. 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。

1.3.6.5. 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。

1.3.6.6. 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。

1.3.6.7. 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
```

1.3.6.8. 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。

1.3.6.9. Ansible Automation Platform 作业失败

当您选择不兼容的选项时，Ansible 作业无法运行。只有选择了 -cluster 范围内的频道选项时，Ansible Automation Platform 才起作用。这会影响需要执行 Ansible 作业的所有组件。

1.3.6.10. Ansible Automation Platform operator 在代理外访问 Ansible Tower

Ansible Automation Platform(AAP)Operator 无法访问支持代理的 OpenShift Container Platform 集群外的 Ansible Tower。要解决这个问题，您可以在代理中安装 Ansible tower。请参阅 Ansible Tower 提供的安装步骤。

1.3.6.11. 在版本 2.4 中编辑 Helm Argo 应用程序时不会显示模板信息

当创建 Helm Argo 应用程序时，模板信息会在 YAML 文件正确时会出现空的。升级到 Errata 2.4.1 以修复错误。

1.3.6.12. 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'**

1.3.6.13. 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。

1.3.7. 已知的监管问题

1.3.7.1. 无法从 Red Hat Advanced Cluster Management 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。

1.3.7.2. 放置资源限制

提示，策略必须使用 PlacementRule 或 Placement 资源来控制策略部署到特定受管集群。如果创建使用放置资源的策略，您可能会遇到以下限制：

- 当您从控制台查看策略详情时，放置信息不会被显示。

- 从控制台删除策略时，不会删除放置信息。

- 从控制台编辑策略时，放置详情不会更新。

使用 Placement 资源时，使用命令行界面(CLI)来更新策略。

1.3.7.3. 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。

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

当您有为 complianceType 参数和 remediationAction 参数配置了 mustnothave 的配置策略时，策略会在向 Kubernetes API 发出删除请求后列为合规。因此，在策略列为合规时，Kubernetes 对象可能会处于 Terminating 状态。

1.3.8. 备份和恢复已知问题

1.3.8.1. 备份和恢复功能不适用于 IBM Power 和 IBM Z

hub 集群的备份和恢复功能需要 OpenShift API 数据保护(OADP)操作器。OADP operator 不适用于 IBM Power 或 IBM Z 架构。

1.3.8.2. 在恢复操作后，应用程序和策略在受管集群中没有资源状态

当使用从另一个 hub 集群备份的数据在新的 hub 集群上运行时，应用程序和策略不会显示受管集群中资源的状态。这是因为搜索和策略附加组件没有重置为新的 hub 集群。

在新 hub 集群中，您必须重启 addon-certpolicyctrl 和 addon-search 用于所有受管集群。运行以下命令以重启 pod：

```
oc get pods -n open-cluster-management-agent-addon | grep search | awk '{print $1}' | xargs kubectl delete pod
```

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 2.3 版本 *被删除* 且不再被支持。其文档可能仍然可用，但不再有任何新的勘误或其他更新。文档的早期版本也不被支持。**

- **升级到 Red Hat Advanced Cluster Management 的最新版本是最佳实践。**

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。**

1.4.1.1. API 弃用

产品或类别	受影响的项	Version	推荐的操作	详情和链接
Applications	**v1alpha1** API 已完全删除。GitOps 集群 API 升级至 **V1beta1**。	2.4	使用 **V1beta1**。	无

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
Applications	管理 secret	2.4	使用策略 hub 模板用于 secret。	请参阅 管理安全策略。
监管控制台	**pod-security-policy**	2.4	无	无
安装程序	在 **operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 中分隔 cert-manager 设置	2.3	无	无
klusterlet operator	**release-2.4,release-2.3** 频道不会接收更新	2.3 及更高版本	要导入和管理 Red Hat OpenShift 专用集群，您必须升级到 2.5 才能接收更新。	请参阅使用 operator 升级。
监管	自定义策略控制器	2.3	无	无
Applications	**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

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
Red Hat Advanced Cluster Management 控制台	Visual Web Terminal（技术预览）	2.4	使用终端代替	无
Applications	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
Applications	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
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。
Applications	频道类型：Namespace，完全删除	2.2	无	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。

1.6. FIPS 就绪性

为 Red Hat Advanced Cluster Management for Kubernetes 完成 FIPS 就绪。Red Hat Advanced Cluster Management 使用相同的工具来确保将加密调用传递给 Red Hat OpenShift Container Platform 使用的 Red Hat Enterprise Linux(RHEL)认证的加密模块。如需有关 OpenShift FIPS 支持的详情，请参阅 对 FIPS 加密的支持。

1.6.1. 限制

阅读 Red Hat Advanced Cluster Management 和 FIPS 中的以下限制。

- Red Hat OpenShift Container Platform 不支持 IBM Power(ppc64le)和 IBM Z(s390x)架构中的 FIPS。
- 以下技术预览组件没有 FIPS 就绪：
  - hub 集群备份和恢复
  - Red Hat OpenShift 的基础架构 Operator
  - Submariner
  - VolSync
- 在配置提供的存储时，必须对搜索和可观察组件使用的持久性卷声明(PVC)和 S3 存储进行加密。Red Hat Advanced Cluster Management 不提供存储加密，请参阅 OpenShift Container Platform 文档 支持 FIPS 加密。

- **当您从 Red Hat Advanced Cluster Management 置备受管集群时，您必须在 install-config.yaml 文件中设置 fips: true，然后才能部署新的受管集群。**