Red Hat Advanced Cluster Management for Kubernetes 2.5

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: 2023-07-14

Red Hat Advanced Cluster Management for Kubernetes 2.5 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。

法律通告

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

重要： Red Hat Advanced Cluster Management 2.5 和更早的版本已被删除，并不再被支持。2.5 及更早版本的文档不会更新。其文档可能仍然可用，但不再有任何新的勘误或其他更新。

最佳实践：升级到 Red Hat Advanced Cluster Management 的最新版本。

- 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。
- 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）
- 集群
- Applications
- 监管

1.1.1. Web 控制台

- 控制台侧导航栏与其他产品一致，提供更好的用户体验。通过导航，您可以访问各种产品功能。另外，*Search* 在 *Home* 标签页中的导航中，而不在标题栏中。

- 通过 Red Hat OpenShift Container Platform 4.10 发行版本 和一个更混合的控制台，您可以使用动态插件。请参阅 OpenShift Container Platform 文档中有关 在 OpenShift Container Platform Web 控制台中添加动态插件的内容，以便在运行时加载的集群中创建和部署动态插件。

- **注：** 在 OpenShift Container Platform 版本 4.8 到 4.10 时没有启用插件，Red Hat Advanced Cluster Management 可以在*视角交换器*中找到。要了解有关 Red Hat Advanced Cluster Management 控制台的信息，请参阅控制台概述。

- Red Hat Advanced Cluster Management 插件通常可用于从 OpenShift Container Platform 控制台启用。参阅控制台概述来了解如何启用它。

1.1.1.1. Observability（可观察性）

- Red Hat Advanced Cluster Management 支持 OpenShift Container Platform 版本 3.11 Grafana 仪表板。如需了解更多详细信息，请参阅*启用可观察性*中的创建 MultiClusterObservability CR 部分。

- 自定义用于访问用于可观察性服务的对象存储的证书。如需了解更多详细信息，请参阅自定义用于访问对象存储的证书。

- 使用安全 Service Token 凭证配置可观察性服务。有关配置内容的更多信息，请参阅 Observability API。

- 通过使用可观察性服务，您可以将指标导出到外部端点。如需了解更多详细信息，请参阅将指标导出到外部端点。

- 支持单节点 OpenShift(SNO)集群的动态指标集合。如需更多信息，请参阅单节点 OpenShift 集群的动态指标。

1.1.2. 集群

- 通过 Red Hat Advanced Cluster Management 集成 Submariner multicluster 网络服务的一些功能通常可用。如需更多信息，请参阅 Submariner multicluster networking 和 service discovery 。

- 启用 Globalnet 控制器在启用 Submariner 插件时解析重叠的 CIDR。如需更多信息，请参阅 Globalnet。

- 在 Advanced RISC Machines(ARM)架构上托管 hub 集群，以及导入和管理集群。

- Central Infrastucture Management 现在支持以下平台上的 Metal3：裸机、Red Hat OpenStack Platform、VMware vSphere 环境，或者在使用用户置备的基础架构(UPI)方法安装它时，平台为 **None**。

- 您可以在集群创建过程中发现主机并在基础架构环境中添加主机。如需更多信息，请参阅在内部环境中创建集群。

- 使用 **ManagedClusterSet** （现已正式发布）来管理组中所有受管集群的访问。**ManagedClusterSet** 为任何未特别分配给集合的受管集群创建一个 **default** 受管集群。如需更多信息，请参阅创建和管理 ManagedClusterSet。

- 指定集群池中可以立即可用于声明的集群数量。如需更多信息，请参阅扩展集群池。

- 使用 Red Hat Advanced Cluster Management 在 Red Hat Virtualization 上创建 OpenShift Container Platform 集群。如需更多信息，请参阅在 Red Hat Virtualization 上创建集群 。

- 使用污点和容限控制受管集群和受管集群集的放置。如需更多信息，请参阅使用污点和容限放置受管集群。

- 使用可扩展调度来控制集群的放置。如需更多信息，请参阅可扩展调度。
- 学习使用 **backup-restore-enabled** 策略恢复备份和恢复组件。如需更多信息，请参阅使用策略进行备份验证。
- 使用 Red Hat Advanced Cluster Management 发现来查找 OpenShift Cluster Manager 提供的 OpenShift 4 集群。发现通常可用，API 从 **v1alpha1** 更新至 **v1**。
  - 发现后，您可以导入集群进行管理。发现服务使用 Discover Operator 进行后端和控制台使用。请参阅发现服务简介。
- 现在，在使用 Red Hat Advanced Cluster Management 控制台为 VMware vSphere 或 Red Hat OpenStack Platform 创建集群时，您可以在凭证中指定断开连接的集群的属性。如需更多信息，请参阅为 VMware vSphere 创建凭证，和为 Red Hat OpenStack 创建凭证。

指定凭证中的代理同步属性。如需更多信息，请参阅管理凭证概述中的基础架构供应商的凭证主题。

- *multicluster engine* Operator 通常作为一个软件 operator 提供，用于增强集群机管理。multicluster engine operator 支持跨云和数据中心的 Red Hat OpenShift Container Platform 和 Kubernetes 集群生命周期管理。Red Hat OpenShift Container Platform 是 multicluster engine operator 的先决条件。

技术预览：

请参阅以下集群功能作为技术预览：

- **Managed-ServiceAccount** 组件允许您在受管集群中创建和删除服务帐户。组件被默认禁用。
  - 请参阅 Enabling ManagedServiceAccount add-ons（技术预览） 的 *multicluster engine operator* 文档，以了解更多信息。
  - 如需更多信息，请参阅 MultiClusterHub advanced configuration 中的 Red Hat Advanced Cluster Management 文档。
- **hypershift** 附加组件可帮助您大规模托管 OpenShift Container Platform control plane，将管理与工作负载分开。组件被默认禁用。
  - 如需更多信息，请参阅 Hypershift add-on（技术预览） 的 *multicluster engine operator* 文档。
  - 请参阅 Hypershift 附加组件的 Red Hat Advanced Cluster Management 文档（技术预览），以及使用托管 control plane 集群（技术预览） 来了解更多。
  - 使用 HyperShift 管理和配置托管 control plane 集群。如需更多信息，请参阅使用托管的 control plane 集群（技术预览）。

有关其他集群主题，请参阅管理集群。

1.1.3. Applications

- 放置和放置决策 API 从 **v1alpha1** 升级到 **v1beta1**。Placements 定义了目标集群，目标集群需要订阅一个 **ClusterSet**，它是订阅和应用程序集被提供到的位置。在控制台的**高级配置**中查看它们。
- 从单个应用程序概述中的各个标签页访问拓扑，以便您可以同时查看所有内容。从 **How to read topology** 中了解拓扑的信息，以了解每个拓扑元素的信息。

- **ApplicationSet** 通常作为 Argo CD 的子项目提供，它增加了对 Argo CD 应用程序的多集群支持。您可以从产品控制台编辑器创建 **ApplicationSet**。请参阅应用程序模型和定义。
- 受管集群和 hub 集群上的 **subscriptionReports** 的状态为轻便且更具扩展性。请参阅以下三种类型的子状态报告：
  - 软件包级的 **SubscriptionStatus** ：这是受管集群上的应用程序软件包状态，且应用程序在 **appsub** 命名空间中部署的所有资源的详细状态。
  - 集群级 **SubscriptionReport** ：这是与特定集群部署的所有应用程序的整体状态报告。
  - 应用程序级 **SubscriptionReport** ：这是部署特定应用程序的所有受管集群的总体状态报告。
    如需更多信息，请参阅订阅报告。

有关其他应用程序主题，请参阅管理应用程序。

1.1.4. 监管

- 使用可选的 YAML 字段 **metadataComplianceType** 来处理与其他字段不同的对象的标签和注解。如需更多信息，请参阅 Policy API。
- 创建策略集到将策略分组到一起。请参阅策略设置控制器。
- 现在，策略生成器支持策略设置生成。请参阅策略生成器。
- 您可以使用 **protect** 功能来保护 hub 集群策略模板上的敏感数据。另外， **toSecret** 功能现在包括在 hub 集群策略模板中。如需更多信息，请参阅 protect 功能部分

如需了解更多有关仪表板和策略框架的信息，请参阅监管。

1.1.5. 附加组件

- 在 Red Hat OpenStack Platform 集群上部署 Submariner。如需更多信息，请参阅为 Submariner 准备 Red Hat OpenStack Platform。

要查看更多发行说明主题，请参阅发行注记。

1.2. 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
- Submariner 已知问题

1.2.1. 已知的与文档相关的问题

1.2.1.1. 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/zh-cn/red_hat_advanced_cluster_management_for_kubernetes/2.5/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/zh-cn/red_hat_advanced_cluster_management_for_kubernetes/2.5/html-single/clusters/index#volsync**
3. 链接到新 URL 以在文档中找到指定部分。

1.2.2. 已知的与安装相关的问题

1.2.2.1. 升级 Red Hat Advanced Cluster Management 后一些 Pod 可能会处于不正常的状态

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 **failed** 状态。这个问题不经常出现，是由一个已知的 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。

1.2.2.2. 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。

1.2.2.3. 升级后，两个集群 curator 控制器在同时运行

从 2.4.x 升级到 2.5.0 后，两个集群 curator 控制器可能会同时运行。为 Cluster Lifecycle Ansible 集成的一些 prehook 和 posthook 创建了两个或多个 **AnsibleJob**。请参阅以下流程来解决这个问题：

1. 检查是否有两个集群 curator 控制器正在运行。运行以下命令，其中包含来自多集群引擎 operator 的 **multicluster-engine** 命名空间，以及 **open-cluster-management** 命名空间：

```
kubectl -n multicluster-engine get deploy cluster-curator-controller
```

```
kubectl -n open-cluster-management get deploy cluster-curator-controller
```

2. 如果两个集群 curator 控制器都在运行，删除 **open-cluster-management** 命名空间中的 **cluster-curator-controller**。运行以下命令：

```
kubectl -n open-cluster-management delete deploy cluster-curator-controller
```

1.2.2.4. Create MultiClusterEngine 按钮无法正常工作

在 Red Hat OpenShift Container Platform 控制台中安装 Red Hat Advanced Cluster Management for Kubernetes 后，会出现一个带有以下信息的弹出窗口：

MultiClusterEngine required

创建一个 MultiClusterEngine 实例来使用这个 Operator。

弹出窗口中的 **Create MultiClusterEngine** 按钮可能无法正常工作。要临时解决这个问题，在 Provided APIs 部分的 MultiClusterEngine 标题中选择 **Create instance**。

1.2.3. 已知的与 Web 控制台相关的问题

1.2.3.1. Red Hat Advanced Cluster Management 版本 2.5.x 不支持 dark 模式

虽然 Red Hat Advanced Cluster Management 版本 2.5.2 及更高版本支持在 Red Hat OpenShift Container Platform 版本 4.11 上支持 2.5.x 版本，但 Red Hat Advanced Cluster Management 2.5.x 不支持 dark 模式。在设置中禁用 dark 模式，或升级到 Red Hat Advanced Cluster Management 版本 2.6 来启用 dark 模式。

1.2.3.2. multicluster engine for Kubernetes operator 版本 2.0.x 不支持 dark 模式

虽然 multicluster engine for Kubernetes operator 2.0.2 及更新版本，但在 Red Hat OpenShift Container Platform 版本 4.11 上支持更新的 2.0.x 版本，但 multicluster engine for Kubernetes operator 2.0.x 不支持 dark 模式。在设置中禁用 dark 模式，或升级到 multicluster engine for Kubernetes operator 版本 2.1 来启用 dark 模式。

1.2.3.3. 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。

1.2.3.4. 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。

1.2.3.5. 搜索自定义中的存储大小限制

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
```

1.2.3.6. 搜索查询解析错误

如果环境变大，需要更多测试进行扩展，搜索查询可能会超时，导致解析错误消息。这个错误会在等待了搜索查询 30 秒后显示。

使用以下命令扩展超时时间：

```
kubectl annotate route multicloud-console haproxy.router.openshift.io/timeout=Xs
```

1.2.3.7. 无法编辑集群集的命名空间绑定

当您为带有 **admin** 角色的集群集编辑命名空间绑定时，您可能会遇到类似以下消息的错误：

ResourceError: managedclustersetbindings.cluster.open-cluster-management.io "<cluster-set>" is forbidden: User "<user>" cannot create/delete resource "managedclustersetbindings" in API group "cluster.open-cluster-management.io" in the namespace "<namespace>".

要解决这个问题，请确保还有权在您要绑定的命名空间中创建或删除 **ManagedClusterSetBinding** 资源。角色绑定只允许将集群集绑定到命名空间。

1.2.3.8. 集群详情中的假扩展警报

当您在控制台中查看集群详情时，可能会在 *Nodes* 或 *Machine pool* 选项卡中看到以下信息：

worker 节点当前正在从这个集群中移除。点 View machine 按钮查看扩展操作的状态（在此控制台中反映更改可能需要几分钟时间）。

如果没有机器池，则会出现使用 User Provisioned Infrastructure (UPI) 安装的供应商，忽略假的警报。当存在不是 control plane 一部分的 worker 节点时，会出现警报。如果 worker 节点直接添加到集群中，而不是扩展机器池，则可以使用 Installer Provisioned Infrastructure (IPI) 安装来置备的集群错误警报。

1.2.4. 已知的可观察性问题

1.2.4.1. 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。

1.2.4.2. 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。

1.2.4.3. 没有来自 ROKS 和 HyperShift 集群的数据

Red Hat Advanced Cluster Management observability 不会在内置仪表板中显示 ROKS 集群和 HyperShift 集群中的数据。这是因为 ROKS 和 HyperShift 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 和 HyperShift 集群的面板： **Kubernetes/API 服务器**,**Kubernetes/Compute Resources/Workload**,**Kubernetes/Compute Resources/Namespace(Workload)**

1.2.4.4. 没有来自 ROKS 和 HyperShift 集群的 etcd 数据

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

1.2.4.5. 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。

1.2.4.6. 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。

1.2.4.7. 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。

1.2.4.8. 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**。

1.2.4.9. 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。

1.2.4.10. Grafana 部署在受管集群中失败

如果清单的大小超过 50 千字节，Grafana 实例不会部署到受管集群。在部署了可观察性后，只有 **local-cluster** 出现在 Grafana 中。

1.2.5. 已知的与集群管理相关的问题

请查看以下与集群管理相关的已知问题和限制：

1.2.5.1. 无法为集群创建输入断开连接的安装设置，或在输入后被忽略

当使用裸机供应商并以断开连接安装的方式创建集群时，您必须将所有设置保存在 *Configuration for disconnected installation* 部分的凭证中。您不能在集群创建控制台编辑器中输入它们。

当使用 VMware vSphere 或 Red Hat OpenStack Platform 供应商和断开连接的安装创建集群时，如果需要一个证书才能访问镜像 registry，您必须在*断开连接的安装配置部分*的*附加信任捆绑包*字段中输入它。如果在集群创建控制台编辑器中输入该证书，它将被忽略。

1.2.5.2. 断开连接的安装程序的凭证无法区分不同的证书

当为裸机、VMware vSphere 或 Red Hat OpenStack Platform 供应商创建凭证时，请注意，*断开连接的安装的代理和配置*中的*附加信任捆绑包*字段包含了相同的值，因为安装程序无法区分证书。您仍然可以独立使用这些功能。如果代理和断开连接的安装需要不同的证书，您可以在字段中输入多个证书。

1.2.5.3. 删除附加组件时，手动删除受管集群上所需的 VolSync CSV

当您从 hub 集群中删除 VolSync **ManagedClusterAddOn** 时，它会删除受管集群上的 VolSync operator 订阅，但不会删除集群服务版本(CSV)。要从受管集群中删除 CSV，请在您要删除 VolSync 的每个受管集群中运行以下命令：

```
oc delete csv -n openshift-operators volsync-product.v0.4.0
```

如果您安装了不同版本的 VolSync，请将 **v0.4.0** 替换为您的安装版本。

1.2.5.4. 使用 sushy-tools 时置备裸机受管集群会失败

当您使用 sushy-tools 在裸机上置备受管集群时，置备可能会失败，并显示 **虚拟介质 cd 查询返回** 500 错误。对于长时间运行的集群，使用 sushy-tools 无法保证它是可靠的。

请确保您使用 sushy-tools 的最新版本，并重新启动 sushy 模拟器来解决这个问题。

1.2.5.5. 在 OpenShift Container Platform 4.10 中置备裸机集群在双堆栈 hub 中会失败

当您在运行 OpenShift Container Platform 版本 4.10 的双堆栈 hub 上置备裸机集群时，provision 会失败并显示以下错误消息：'timeout reached while the node'。要避免这个问题，请在 **install-config.yaml** 文件中禁用 provisioning 网络，如下例所示：

```
platform:
  baremetal:
    provisioningNetwork: "Disabled"
```

如需有关 provisioning 网络的更多信息，请参阅 OpenShift Container Platform 文档中的使用 provisioning 网络进行部署。

1.2.5.6. 删除受管集群集不会自动删除其标签

删除 **ManagedClusterSet** 后，添加到每个受管集群的标签不会被自动删除。从已删除受管集群集中包含的每个受管集群手动删除该标签。该标签类似以下示例：**cluster.open-cluster-management.io/clusterset:<ManagedClusterSet Name>**。

1.2.5.7. ClusterClaim 错误

如果您针对 **ClusterPool** 创建 Hive **ClusterClaim** 并手动将 **ClusterClaimspec** 生命周期字段设置为无效的 golang 时间值，Red Hat Advanced Cluster Management 会停止履行并协调所有 **ClusterClaims**，而不只是格式不正确的声明。

如果发生这个错误，您可以在 **clusterclaim-controller** pod 日志中看到以下内容，它是一个带有池名称和无效生命周期的特定示例：

```
E0203 07:10:38.266841       1 reflector.go:138] sigs.k8s.io/controller-runtime/pkg/cache/internal/informers_map.go:224: Failed to watch *v1.ClusterClaim: failed to list *v1.ClusterClaim: v1.ClusterClaimList.Items: []v1.ClusterClaim: v1.ClusterClaim.v1.ClusterClaim.Spec: v1.ClusterClaimSpec.Lifetime: unmarshalerDecoder: time: unknown unit "w" in duration "1w", error found in #10 byte of ...|time":"1w"}},{"apiVe|..., bigger context ...|clusterPoolName":"policy-aas-hubs","lifetime":"1w"}},
{"apiVersion":"hive.openshift.io/v1","kind":"Cl|...
```

您可以删除无效的声明。

如果删除了不正确的声明，则声明可以在不需要进一步交互的情况下再次成功进行协调。

1.2.5.8. 产品频道与置备的集群不同步

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

进入 OpenShift Container Platform 控制台中的正确频道。点 **Administration** > **Cluster Settings** > **Details Channel**。

1.2.5.9. 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。

1.2.5.10. 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。

1.2.5.11. 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。

1.2.5.12. 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。

1.2.5.13. 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。

1.2.5.14. 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
```

1.2.5.15. 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**。

1.2.5.16. 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。

1.2.5.17. 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。

1.2.5.18. 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。

1.2.5.19. 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。

1.2.5.20. 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。

1.2.5.21. 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。

1.2.5.22. 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
```

1.2.5.23. 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}"} }]'
  ```

1.2.5.24. 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。

1.2.5.25. 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***。

1.2.5.26. 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。

1.2.5.27. 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。

1.2.5.28. 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。

1.2.5.29. 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。

1.2.5.30. 升级后，cluster-proxy-addon 不会启动

从 2.4.x 升级到 2.5.0 后，**cluster-proxy-addon** 不会启动，**cluster-proxy-addon-manager** 会引发一个 nil 指针异常。

要临时解决这个问题，请完成以下步骤：

1. 禁用 **cluster-proxy-addon**。请参阅高级配置以了解更多信息。
2. 从 **open-cluster-management** 命名空间中删除 **cluster-proxy-signer** secret。
3. 启用 **cluster-proxy-addon**。

1.2.6. 已知的与应用程序管理相关的问题

请参阅以下对应用程序生命周期组件的已知问题。

1.2.6.1. 应用程序 ObjectBucket 频道类型无法使用 allow 和 deny 列表

您不能在 **subscription-admin** 角色中使用 ObjectBucket 频道类型指定 allow 和 deny 列表。在其他频道类型中，订阅中的 allow 和 deny 列表表示可以部署哪些 Kubernetes 资源，以及不应部署哪些 Kubernetes 资源。

1.2.6.2. Argo Application 无法部署到 3.x OpenShift Container Platform 受管集群

控制台中的 Argo **ApplicationSet** 无法部署到 3.x OpenShift Container Platform 受管集群，因为 **Infrastructure.config.openshift.io** API 在 3.x 上不可用。

1.2.6.3. 对 multicluster_operators_subscription 镜像的更改不会自动生效

在受管集群中运行的 **application-manager** 附加组件现在由 subscription operator 处理，后者之前由 klusterlet operator 处理。订阅 operator 没有管理 **multicluster-hub**，因此对 **multicluster-hub** 镜像清单 ConfigMap 中的 **multicluster_operators_subscription** 镜像的更改不会自动生效。

如果订阅 operator 使用的镜像通过更改 **multicluster-hub** 镜像清单 ConfigMap 中的 **multicluster_operators_subscription** 镜像覆盖，则受管集群中的 **application-manager** add-on 不会使用新镜像，直到订阅 operator pod 重启为止。您需要重启 pod。

1.2.6.4. 应用程序拓扑显示错误的应用程序

如果在不同的 Gitops 实例中创建具有相同名称的 **ApplicationSets**，则 Application topology 会显示错误的应用程序。如果安装了多个 Gitops 实例，则每个 Gitops 实例中具有相同名称的 **ApplicationSets**，并且 **ApplicationSets** 的拓扑将无法正确显示。这是因为拓扑没有区分所创建的 **ApplicationSets** 的命名空间。

确保在每个 Gitops 实例中使用不同的名称创建 **ApplicationSet**，以正确显示拓扑。

1.2.6.5. 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，请参阅以订阅管理员身份创建允许和拒绝列表。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。

1.2.6.6. 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。

1.2.6.7. 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。

1.2.6.8. 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。

1.2.6.9. 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。

1.2.6.10. 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
```

1.2.6.11. 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。

1.2.6.12. 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。

1.2.6.13. 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。

1.2.6.14. 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。

1.2.6.15. 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'
```

1.2.6.16. 应用程序控制台表限制

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。

1.2.6.17. 没有应用程序控制台拓扑过滤

2.5 的*应用程序*的 *Console* 和 *Topology* 已更改。控制台 Topology 页面中没有过滤功能。

1.2.6.18. ApplicationSet 资源不会在拓扑中显示状态

当您创建将资源部署到与 **ApplicationSet** YAML 中定义的命名空间的 **ApplicationSet** 应用程序时，资源状态不会出现在拓扑中。

1.2.6.19. 允许和拒绝列表在对象存储应用程序中无法正常工作

允许和决绝列表功能无法在对象存储应用程序订阅中工作。

1.2.6.20. ApplicationSet 向导不会自动获取路径

当使用与之前创建的 **ApplicationSet** 相同的 URL 和分支创建新 **ApplicationSet** 后，ApplicationSet 向导不会自动获取路径。

要临时解决这个问题，请在 **Path** 字段中输入路径。

1.2.7. 已知的监管问题

1.2.7.1. 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。

1.2.7.2. 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。

1.2.7.3. 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。

1.2.7.4. 使用策略部署的 Operator 不支持 ARM

虽然支持安装到 ARM 环境中，但使用策略部署的 operator 可能不支持 ARM 环境。安装 Operator 的以下策略不支持 ARM 环境：

- Red Hat Advanced Cluster Management for Quay Container Security Operator
- Red Hat Advanced Cluster Management for Compliance Operator

1.2.7.5. 策略模板问题

当您为配置策略编辑策略模板时，您可能会遇到以下问题：

- 当您将配置策略重命名为新名称时，带有旧名称的配置策略的副本会保留。
- 如果您从 hub 集群上的策略中删除配置策略，则配置策略会保留在受管集群中，但不会提供其状态。要解决这个问题，请禁用您的策略并重新启用它。您还可以删除整个策略。

1.2.8. 备份和恢复已知问题

1.2.8.1. 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。

1.2.8.2. 避免备份冲突

随着 hub 集群从被动更改为主集群和后端，不同的集群就可以在同一存储位置备份数据。这可能导致备份冲突，这意味着最新的备份是由被动 hub 集群生成的。

passive hub 集群会生成备份，因为在 hub 集群中启用了 **BackupSchedule.cluster.open-cluster-management.io** 资源，但它应该不再写入备份数据，因为 hub 集群不再是一个主 hub 集群。运行以下命令检查是否有备份冲突：

```
oc get backupschedule -A
```

您可能会收到以下状态：

```
NAMESPACE   NAME          PHASE       MESSAGE
```

> openshift-adp schedule-hub-1 BackupCollision Backup acm-resources-schedule-20220301234625, from cluster with id [be97a9eb-60b8-4511-805c-298e7c0898b3] is using the same storage location. This is a backup collision with current cluster [1f30bfe5-0588-441c-889e-eaf0ae55f941] backup. Review and resolve the collision then create a new BackupSchedule resource to resume backups from this cluster.

通过将 **BackupSchedule.cluster.open-cluster-management.io** 资源**状态**设置为 **BackupCollision** 来避免备份冲突。由 **BackupSchedule** 资源所创建的 **Schedule.velero.io** 资源会自动删除。

hub-backup-pod 策略会报告备份冲突。管理员必须验证哪个 hub 集群将数据写入存储位置。然后，从 passive hub 集群中删除 **BackupSchedule.cluster.open-cluster-management.io** 资源，并在主 hub 集群上重新创建新的 **BackupSchedule.cluster.open-cluster-management.io** 资源，以恢复备份。

如需更多信息，请参阅集群备份和恢复 Operator。

1.2.8.3. Velero 恢复限制

查看以下恢复限制：

- 新 hub 集群与初始 hub 集群不同，当在初始 hub 集群上恢复备份数据前，新的 hub 集群上有现有策略时。该策略不应在新 hub 集群上运行，因为这是一个无法使用备份资源的策略。
- 因为 Velero 跳过现有资源，所以新 hub 集群中的策略不会改变。因此，策略与初始 hub 集群上备份的策略不同。
- 当用户在新 hub 集群上恢复备份时，新的 hub 集群具有与活跃 hub 集群不同的配置。由于之前恢复的 hub 集群上有现有的策略，因此不会再次恢复。即使备份包含预期的更新，策略内容也不会由新的 hub 集群上的 Velero 更新。

要解决前面提到的限制，当创建 **restore.cluster.open-cluster-management.io** 资源时，集群备份和恢复 Operator 会运行一组步骤来通过清理 hub 集群前通过清理 hub 集群来准备恢复。如需更多信息，请参阅恢复前清理 hub 集群。

1.2.8.4. 不显示导入的受管集群

在主 hub 集群上手动导入的受管集群只显示在被动 hub 集群上恢复激活数据时。

1.2.8.5. 集群备份和恢复升级限制

如果您将集群从 2.4 升级到 2.5，并将 **enableClusterBackup** 参数设置为 **true**，则会出现以下信息：

> When upgrading from version 2.4 to 2.5, cluster backup must be disabled

在升级集群前，请通过将 **enableClusterBackup** 参数设置为 **false** 来禁用集群备份和恢复。**MultiClusterHub** 资源中的 **components** 部分可能类似以下 YAML 文件：

升级完成后可以重新启用备份和恢复组件。查看以下示例：

```
overrides:
    components:
      - enabled: true
        name: multiclusterhub-repo
      - enabled: true
        name: search
      - enabled: true
```

```
      name: management-ingress
    - enabled: true
      name: console
    - enabled: true
      name: insights
    - enabled: true
      name: grc
    - enabled: true
      name: cluster-lifecycle
    - enabled: true
      name: volsync
    - enabled: true
      name: multicluster-engine
    - enabled: false
      name: cluster-proxy-addon
    - enabled: true <<<<<<<<<
      name: cluster-backup
  separateCertificateManagement: false
```

如果您已手动安装 OADP，则必须在升级前手动卸载 OADP。升级成功并重新配置后，会自动安装 OADP。

1.2.8.6. 未恢复受管集群资源

当您恢复 **local-cluster** 受管集群资源的设置并覆盖新 hub 集群中的 **local-cluster** 数据时，设置会被错误配置。上一个 hub 集群 **local-cluster** 的内容没有备份，因为资源包含 **local-cluster** 特定信息，如集群 URL 详情。

您必须在恢复集群中手动应用与 **local-cluster** 资源相关的配置更改。如需了解更多详细信息，请参阅准备新 hub 集群。

1.2.8.7. 只有在首次创建 Velero 计划时，才调用 prepareForBackup

prepareForBackup 函数中定义的任何标签都不会添加到调度创建后创建的资源中。这会影响在备份启动前标记的 Red Hat OpenShift secret Hive 和 Infrastructure Operator。

查看受影响的资源列表：

- **clusterDeployments** 使用的由集群声明创建的 secret
- 集群池 secret
- 带有标签 **agent-install.openshift.io/watch** 和 **environment.metal3.io** 的Secret

更新 **BackupSchedule**、**veleroSchedule** 或 **veleroTTL** 值以启动一组新的调度。然后，为恢复使用结果备份，它被定义为为备份标记最新的资源。

1.2.8.8. 恢复的 Hive 受管集群可能无法与新的 hub 集群连接

当您为 Hive 受管集群恢复更改或轮转颁发机构 (CA) 的备份时，受管集群将无法连接到新的 hub 集群。连接会失败，因为此受管集群的 **admin kubeconfig** secret 通过备份提供，所以不再有效。

您必须在新 hub 集群中手动更新受管集群的恢复的 **admin kubeconfig** secret。

1.2.9. Submariner 已知问题

1.2.9.1. Submariner 目前仅支持 OpenShift SDN 作为 CNI 网络供应商

仅支持 OpenShiftSDN 作为 CNI 网络供应商。目前不支持 OVN。

1.2.9.2. Submariner 不支持一些 Red Hat Enterprise Linux 节点作为 worker 节点

当在包含 Red Hat Enterprise Linux worker 节点的集群中部署 Submariner 时，在 4.18.0-359.el8.x86_64 和 4.18.0-372.11.1.el8_6.x86_64 之间带有内核版本的 Red Hat Enterprise Linux worker 节点时，应用程序工作负载无法与远程集群通信。

1.2.9.3. Submariner 不支持 Red Hat Advanced Cluster Management 可以管理的所有基础架构供应商

在 Red Hat Advanced Cluster Management 的所有基础架构供应商不支持 Submariner。如需支持的供应商列表，请参阅 Red Hat Advanced Cluster Management 支持列表 。

1.2.9.4. Submariner 不支持从 Red Hat Advanced Cluster Management 控制台准备 Red Hat OpenStack Platform 基础架构

在 product-title-short} 控制台中，Submariner 不支持对 Red Hat OpenStack 集群的自动准备。您可以使用 Red Hat Advanced Cluster Management API 来手动准备云。

1.2.9.5. Submariner 不支持使用 Globalnet 的无标头服务

Submariner 支持使用 Globalnet 的无头服务。但是，当您从位于相同集群中使用 **clusterset.local** 域名的客户端访问导出的无头服务时，与无头服务关联的 **globalIP** 将返回到客户端，它不在集群中路由。

您可以使用 **cluster.local** 域名访问本地无头服务。

1.2.9.6. Submariner 不支持 air-gapped 集群

对于在 air-gapped 环境中置备的集群，Submariner 不会验证。

1.2.9.7. 无法部署大量网关

您无法部署多个网关。

1.2.9.8. 在启用 NAT 时 Submariner 不支持 VXLAN

带有 VXLAN 电缆驱动程序的 Submariner 目前仅在非NAT 部署中被支持。

1.2.9.9. Globalnet 限制

Red Hat OpenShift Data Foundation 灾难恢复解决方案不支持 Globalnet。对于地区性的灾难恢复情况，确保对集群和每个集群中的服务网络使用没有重叠的专用 IP 地址。

1.3. 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**。

1.3.1. Errata 2.5.9

- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.2. Errata 2.5.8

- **must-gather** 命令现在收集 Red Hat OpenShift Container Platform 版本号。(ACM-2857)
- 修复了导致 **MEMCACHED** 索引中的 **max_item_size** 设置无法对所有 **MEMCACHED** 客户端传播更改的问题。(ACM-4683)
- 现在，名称中带有点的策略状态会更快地更新。(ACM-4736)

1.3.3. Errata 2.5.7

- 修复控制台中的 **Edit time 窗口** 链接。这个链接现在打开正确的编辑页面。(ACM-2647)
- 修复了在创建应用程序时导致拓扑节点出现在应用程序控制台中的问题。(ACM-3340)

1.3.4. Errata 2.5.6

- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.5. Errata 2.5.5

- 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。

1.3.6. Errata 2.5.4

- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.7. Errata 2.5.3

- 修复了在使用不被支持的 **--validate-cluster-security** 标志作为 **HypershiftDeployment** 控制器参数时的权限问题。(Bugzilla 2109544)
- 更新搜索聚合器逻辑，以避免来自于受管集群的并发同步请求。(Bugzilla 2092863)
- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.8. Errata 2.5.2

- 从 Red Hat Advanced Cluster Management 版本 2.5.2 开始，Red Hat OpenShift Container Platform 版本 4.11 支持 Red Hat Advanced Cluster Management 版本 2.5.x。
- 从 multicluster engine for Kubernetes operator 版本 2.0.2 开始，在 Red Hat OpenShift Container Platform 版本 4.11 上支持 Kubernetes Operator 2.0.x 的多集群引擎。

- 修复了导致 Submariner Globalnet 无法在内部和公共集群间连接的 MTU 问题。(Bugzilla 2074547)
- 解决妨碍 management-ingress pod 安装后启动的问题。(Bugzilla 2082254)
- 修复了在创建包含大写字母标签的 **ClusterClaim** 时导致受管集群日志中出现错误的错误。(Bugzilla 2095481)
- 解决在 Red Hat OpenShift Container Platform 上安装时可能会导致 **MultiClusterHub** 处于**安装**阶段的问题。(Bugzilla 2099503)
- 在自定义 metrics **allowlist** 中增加自定义指标的限值，它允许它从受管集群收集更多指标。(Bugzilla 2099808)
- 修复了在更新控制台策略的内存值后，导致一个 LimitRange 策略被设置为显示 **enforce** 和**不合规**的状态。(Bugzilla 2100036)
- 修复了在将 **app-of-apps** 模式与订阅应用程序搭配使用时导致以下错误问题：**This application has no subscription match selector (spec.selector.matchExpressions)** (Bugzilla 2101577)
- 在使用 Red Hat Advanced Cluster Management 集群备份和恢复 operator (Bugzilla 2103653)恢复 Hub 集群后，解决了导致集群处于"未知"状态的问题。
- 在没有指定时，将 **NodePool.Release.Image** 的默认值设为为 **HostedClusterSpec.Release.Image** 指定的发行镜像。(Bugzilla 2105436)
- 解决导致使用 SSH 连接到私有托管 Git 服务器的应用程序订阅失败的问题。在这个版本中，SSH 连接到私有托管的 Git 服务器。(Bugzilla 2105885)
- 修复了在使用控制台删除策略时阻止关联的 **PolicyAutomation** 和 **AnsibleJob** 对象被删除的错误。(Bugzilla 2116060)

1.3.9. Errata 2.5.1

- 修复了一个程序错误，它会删除在受管集群中部署的一些应用程序。(Bugzilla 2101453)
- 解决 *Overview* 页面中的控制台错误，它显示 **The backend service is unavailable**。(Bugzilla 2096389)
- 解决策略附加组件的不健康状态或故障的集群附加组件控制台问题。(Bugzilla 2088270)

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 2.4 及更早的版本*已被删除*，并不再被支持。其文档可能仍然可用，但不再有任何新的勘误或其他更新。
- 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。

1.4.1.1. API 弃用

产品或类别	受影响的项	Version	推荐的操作	详情和链接
Discovery（发现）	DiscoveredCluster 和 DiscoveryConfig **v1alpha1** API 已被弃用。发现 API 已升级到 **V1**。	2.5	使用 **V1**。	无
放置	**v1alpha1** API 被升级到 **v1beta1**，因为 **v1alpha1** 已被弃用。	2.5	使用 **v1beta1**。	**Placement** API **v1alpha1** 中的 **spec.prioritizerPolicy.configurations.name** 字段会被删除。在 **v1beta1** 中使用 **spec.prioritizerPolicy.configurations.scoreCoordinate.builtIn**。
PlacementDecisions	**v1alpha1** API 被升级到 **v1beta1**，因为 **v1alpha1** 已被弃用。	2.5	使用 **v1beta1**。	无
Applications	**v1alpha1** API 已完全删除。GitOps 集群 API 升级至 **V1beta1**。	2.5	使用 **V1beta1**。	无
Applications	**deployables.apps.open-cluster-management.io**	2.5	无	可部署 API 只在升级路径中保留。任何可部署的 CR 创建、更新或删除都不会被协调。

产品或类别	受影响的项	Version	推荐的操作	详情和链接
CertPolicyController	**v1** API 已被弃用。	2.5	不要使用这个 API。	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	**v1** API 已被弃用。	2.5	不要使用这个 API。	ApplicationManager.agent.open-cluster-management.io
IAMPolicyController	**v1** API 已被弃用。	2.5	不要使用这个 API。	IAMPolicyController.agent.open-cluster-management.io
PolicyController	**v1** API 已被弃用。	2.5	不要使用这个 API。	PolicyController.agent.open-cluster-management.io
SearchCollector	**v1** API 已被弃用。	2.5	不要使用这个 API。	SearchCollector.agent.open-cluster-management.io
WorkManager	**v1** API 已被弃用。	2.5	不要使用这个 API。	WorkManager.agent.open-cluster-management.io
ManagedClusterSets	**v1alpha1** API 被升级到 **v1beta1**，因为 **v1alpha1** 已被弃用。	2.4	使用 **v1beta1**。	无
ManagedClusterSetBindings	**v1alpha1** API 被升级到 **v1beta1**，因为 **v1alpha1** 已被弃用。	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
集群	使用裸机资产创建集群	2.5	使用控制台创建基础架构环境	对于为受影响的已启用的区域，请参阅创建和修改裸机资产，以及在裸机上创建集群。对于以前的过程，请参阅在内部环境中创建集群。
Add-on operator	安装内置受管集群附加组件	2.5	无	无
Observability（可观察性）	**data.custom_rules.yaml.groups.rules** 已弃用	2.5	使用 **data.custom_rules.yaml.groups.recording_rules**。	请参阅自定义可观察性。
安装程序	**enableClusterProxyAddon** 和 **enableClusterBackup** 字段在 **operator.open-cluster-management.io_multiclusterhubs_crd.yaml**中	2.5	无	请参阅高级配置来配置安装。
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。
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
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
Applications	可部署控制器	2.5	无	已移除 Deployable 控制器。
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

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 Kubernetes 文档中的 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 仅在 **x86_64** 架构上支持 FIPS。
- 完整性 Shield 是没有可用的 FIPS 的技术预览组件。
- 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 。
- 当使用 Red Hat Advanced Cluster Management 控制台置备受管集群时，在受管集群创建的 *Cluster details* 部分中选中以下复选框来启用 FIPS 标准：

> FIPS with information text: Use the Federal Information Processing Standards (FIPS) modules provided with Red Hat Enterprise Linux CoreOS instead of the default Kubernetes cryptography suite file before you deploy the new managed cluster.