Red Hat Advanced Cluster Management for Kubernetes 2.1

发行注记

Red Hat Advanced Cluster Management for Kubernetes 发行注记

Last Updated: 2022-02-06

Red Hat Advanced Cluster Management for Kubernetes 2.1 发行注记

Red Hat Advanced Cluster Management for Kubernetes 发行注记

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

法律通告

摘要

Red Hat Advanced Cluster Management for Kubernetes 发行注记，新内容和已知问题

目录

第 1 章 RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 发行注记 4
1.1. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 的新内容 4
1.1.1. 安装 4
1.1.2. Web 控制台 4
1.1.3. 集群管理 4
1.1.4. 应用程序管理 5
1.1.5. 安全和合规性 5
1.2. 勘误更新 5
1.2.1. Errata 2.1.13 6
1.2.2. Errata 2.1.12 6
1.2.3. Errata 2.1.11 6
1.2.4. Errata 2.1.10 6
1.2.5. Errata 2.1.9 6
1.2.6. Errata 2.1.8 6
1.2.7. Errata 2.1.7 6
1.2.8. Errata 2.1.6 6
1.2.9. Errata 2.1.5 7
1.2.10. Errata 2.1.4 7
1.2.11. Errata 2.1.3 7
1.2.12. Errata 2.1.2 8
1.2.13. Errata 2.1.1 8
1.3. 已知问题 10
1.3.1. 已知的升级问题 10
1.3.1.1. 由于 Observability 附加组件的问题，从 2.1.x 升级到 2.3.2 会造成降级的问题 10
1.3.1.2. 升级到 2.1.x 会导致证书丢失 10
1.3.1.3. 升级到 2.1.1 会导致证书丢失 10
1.3.1.4. 升级到 2.1.1 版本无法成功完成，有 ClusterImageSet 错误 11
1.3.1.5. 升级到 2.1.1 禁用 klusterletaddonconfig CRD 11
1.3.1.6. OpenShift Container Platform 集群升级失败的状态 12
1.3.1.7. 从 2.0.4 升级到 2.1 版会使 ClusterServiceVersion 处于待处理状态 13
1.3.2. 已知的与安装相关的问题 14
1.3.2.1. 安装过程中必须不存在证书管理器 14
1.3.3. 已知的与 Web 控制台相关的问题 14
1.3.3.1. Cluster 页面和搜索结果之间节点的不同 14
1.3.3.2. LDAP 用户名是区分大小写的 14
1.3.3.3. Firefox 的较老版本可能无法显示控制台的功能 14
1.3.3.4. 无法使用带有空空格的值搜索 14
1.3.3.5. 在注销用户 kubeadmin 时会出现一个额外浏览器标签页并显示空白页面 14
1.3.3.6. 不再显示 Secret 的内容 14
1.3.3.7. 由于 MultiClusterObservability CR 名称，Observability 无法正常工作 14
1.3.4. 已知的与集群管理相关的问题 14
1.3.4.1. 可能不会显示新的裸机资产选项 15
1.3.4.2. 无法在 OpenShift Container Platform 版本 4.7 上创建裸机受管集群 15
1.3.4.3. 创建资源下拉菜单错误 15
1.3.4.4. hub 集群和受管集群的时钟未同步 15
1.3.4.5. 控制台可能会报告受管集群策略不一致 15
1.3.4.6. 导入集群可能需要两次尝试 15
1.3.4.7. 不支持导入 IBM OpenShift Kubernetes Service 集群的特定版本 15
1.3.4.8. 分离 OpenShift Container Platform 3.11 不会删除 open-cluster-management-agent 15
1.3.4.9. 不支持为置备的集群进行自动 secret 更新 16
1.3.4.10. 无法以非 root 用户身份运行 management ingress 16

1.3.4.11. 无法在搜索中查看受管集群的节点信息 16
1.3.4.12. 销毁集群的进程没有完成 16
1.3.4.13. Grafana 控制台中没有指标数据 17
1.3.5. 已知的与应用程序管理相关的问题 17
1.3.5.1. 应用程序部署窗口错误 17
1.3.5.2. 未部署资源拓扑状态 17
1.3.5.3. 在本地集群限制时部署应用程序 17
1.3.5.4. 编辑应用程序时，控制台中的合并更新选项会取消选择 18
1.3.5.5. 如果存在私有 Git URL，则 Git 分支和 URL 路径字段不会被填充 18
1.3.5.6. 控制台管道卡可能会显示不同的数据 18
1.3.5.7. 命名空间频道 18
1.3.5.8. 命名空间频道订阅处于失败状态 18
1.3.5.9. 在一个命名空间频道中可部署的资源 19
1.3.5.10. 为应用程序编辑角色错误 19
1.3.5.11. 编辑放置规则错误的角色 19
1.3.5.12. 在更新的放置规则后没有部署应用程序 19
1.3.5.13. Subscription operator 不会创建一个 SCC 20
1.3.5.14. 应用程序频道需要唯一的命名空间 20
1.3.6. 已知的与安全相关的问题 20
1.3.6.1. 在登录到控制台时出现内部错误 500 20
1.3.6.2. 在删除 helm 发行版本后恢复 cert-manager 21
1.4. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 平台针对 GDPR 的注意事项 21
1.4.1. 备注 21
1.4.2. 内容表 22
1.4.3. GDPR 22
1.4.3.1. 为什么 GDPR 很重要？ 22
1.4.3.2. 更多关于 GDPR 的信息 22
1.4.4. 针对 GDPR 的产品配置 23
1.4.5. 数据生命周期 23
1.4.5.1. Red Hat Advanced Cluster Management for Kubernetes 平台的数据流类型 23
1.4.5.2. 用于在线联系的个人数据 23
1.4.6. 数据收集 23
1.4.7. 数据存储 24
1.4.8. 数据访问 24
1.4.8.1. 身份验证 25
1.4.8.2. 角色映射 25
1.4.8.3. 授权 25
1.4.8.4. Pod 安全性 25
1.4.9. 数据处理 25
1.4.10. 数据删除 26
1.4.11. 限制使用个人数据的能力 26
1.4.12. 附录 27

第 1 章 RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES 发行注记

重要：

- Red Hat Advanced Cluster Management 的 2.1 版本*已被删除*且不再被支持。其文档可能仍然可用，但是它已被弃用，将没有任何可用的勘误或其他更新。
- 升级到 Red Hat Advanced Cluster Management 的最新版本是最佳选择。
  - Red Hat Advanced Cluster Management for Kubernetes 的新内容
  - 勘误更新
  - 限制和已知问题
  - Red Hat Advanced Cluster Management for Kubernetes 针对 GDPR 的注意事项

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

Red Hat Advanced Cluster Management for Kubernetes 为您提供了整个 Kubernetes 域的可见性，并带有内置监管、集群生命周期管理和应用程序生命周期管理的功能。

- 欢迎使用 Red Hat Advanced Cluster Management for Kubernetes 包括了 Red Hat Advanced Cluster Management for Kubernetes 的概述。
- 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*。

1.1.1. 安装

- 现在，您可以管理 hub 集群。安装 Red Hat Advanced Cluster Management 时，hub 集群会自动导入和管理。如需更多信息，请参阅在线安装。

1.1.2. Web 控制台

- 通过 Web 控制台，可以从一个中央视图访问、查看和管理集群。您可以从 Red Hat OpenShift Container Platform 访问 Red Hat Advanced Cluster Management 控制台，监控集群数据和详情，在集群中使用搜索组件，使用 Visual Web Terminal，并管理集群标签。如需了解更多有关控制台组件的详细信息，请参阅 Web 控制台。
- 现在，您可以启用多集群观察服务（**multicluster-observability-operator**）来查看受管集群的健康状态和优化情况。您可以检查从受管集群收集的指标数据和日志。如需更多信息，请参阅 Observing 环境。

1.1.3. 集群管理

- 现在，您可以在裸机环境中创建和管理集群。如需更多信息，请参阅在裸机上创建集群。
- 另外，您可以使用 Red Hat Advanced Cluster Management 在 VMware vSphere 供应商上创建和管理 Red Hat OpenShift Container Platform 集群。如需更多信息，请参阅在 VMware vSphere 上创建集群。

- 现在，您可以对集群进行分组，并通过创建 ManagedClusterSet 资源来授予用户对组的访问权限。如需更多信息，请参阅 ManagedClusterSets。

- 您可以将 Red Hat Advanced Cluster Management 与 Red Hat OpenShift Update Service operator 集成，以便在断开连接的环境中升级受管集群。如需更多信息，请参阅升级断开连接的集群。

1.1.4. 应用程序管理

- Red Hat Advanced Cluster Management for Kubernetes 应用程序管理提高了管理资源的控制台配置的可用性。现在，您可以在控制台中使用支持的频道创建应用程序，创建和编辑应用程序，配置 secret 设置等。请参阅管理应用程序资源。

- 在 **Advanced configuration** 中，您可以查看选择 *Subscriptions*、*Placement rules* 或 *Channels* 以在表格中查看您的资源。在表中，您还可以使用 YAML 格式编辑这些资源。

- Red Hat Advanced Cluster Management for Kubernetes Ansible Tower 集成现在为为技术预览，您可以从控制台部署和管理 Ansible 作业。您还可以在 *Resource topology* 中查看作业状态。请参阅 应用程序控制台。

- 作为应用程序管理的一部分，您可以将 Ansible Tower 作业集成到 Git 订阅中。对任务进行自动化并与外部服务（如 Slack 和 PagerDuty 服务）集成。如需了解更多有关使用 Ansible 的信息，请参阅 设置 Ansible Tower 任务（技术预览） 。

有关所有应用程序管理更改并改进的文档，请参阅管理应用程序。

1.1.5. 安全和合规性

- Red Hat Advanced Cluster Management for Kubernetes 支持多个角色并使用 Kubernetes 授权机制。更多信息，请参阅基于角色的访问控制。

- 对于证书策略控制器，现在可以使用 **disallowedSANPattern** 参数根据特定的特征检查 DNS 名称。如需更多信息，请参阅证书策略控制器 YAML 表。

- 现在，您可以通过使用产品监管框架添加策略，为开源社区、**open-cluster-management/policy-collection** 贡献。您可以集成第三方策略，如 Gatekeeper。如需更多信息，请参阅集成第三方策略控制器。

- 现在，您可以使用配置策略控制器来创建 ETCD 加密策略。使用 ETCD 加密策略启用敏感数据的加密。如需更多信息，请参阅 ETCD 加密策略。

- 现在，您可以选择 **local-cluster** 作为集群绑定来为自管 hub 集群（本地 hub 集群 ）创建策略。如需更多信息，请参阅创建安全策略。

- 现在，您可以在 *Status* 选项卡中查看策略违反历史记录。如需更多信息，请参阅管理安全策略。

如需了解更多有关仪表板和策略框架的信息，请参阅监管和风险。

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：为便于参考，勘误（Errata）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。

1.2.1. Errata 2.1.13

此勘误发行版本为一个或多个产品容器镜像提供更新。

1.2.2. Errata 2.1.12

此勘误发行版本为一个或多个产品容器镜像提供更新。

1.2.3. Errata 2.1.11

此勘误发行版本为一个或多个产品容器镜像提供更新。

1.2.4. Errata 2.1.10

此勘误发行版本为一个或多个产品容器镜像提供更新。

1.2.5. Errata 2.1.9

更新了镜像中所选容器。

1.2.6. Errata 2.1.8

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.1.8 更新的总结列表：

重要：您必须运行 Red Hat OpenShift Container Platform 版本 4.6 或更高版本，升级到 Errata 2.1.7 及更新的版本。如果无法将 Red Hat OpenShift Container Platform 版本 4.5 升级到更新的版本，您可以继续使用 Red Hat Advanced Cluster Management 版本 2.1.6。

- 在升级到 Red Hat OpenShift Container Platform 4.6.30 后，解决了 Observability **thanos-store-shard** pod 处于 **crashloopback** 状态的问题。(GitHub 13081)
- 修复了当用户删除禁用策略时，**放置规则**和**放置绑定**不会被删除的问题。(GitHub 12689)
- 更新了搜索代码，以使用来自其他字段的数据，因为删除 Kubernetes selfLink，这会影响依赖于这些字段的搜索逻辑。(GitHub 12701)

1.2.7. Errata 2.1.7

重要：您必须运行 Red Hat OpenShift Container Platform 版本 4.6 或更高版本，以升级到 Red Hat Advanced Cluster Management 版本 2.1.7。如果无法将 Red Hat OpenShift Container Platform 版本 4.5 升级到更新的版本，您可以继续使用 Red Hat Advanced Cluster Management 版本 2.1.6。

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.1.7 更新的总结列表：

- 修复了导致 Hive 控制器日志显示不正确的版本信息的问题。(GitHub 12014)
- 添加了具有查看权限的用户的授权以创建和删除 **ManagedClusterView** 资源，它还使具有查看权限的用户能够查看受管集群资源的 YAML 文件。(GitHub 11243)
- 启用具有 **cluster-manager-admin** 角色绑定的用户，以便在 **clusterimagesets** 资源上运行 create、update 和 delete 操作。这个更改允许具有 **cluster-manager-admin** 权限的用户使用 Red Hat Advanced Cluster Management 置备集群。(GitHub 11596)

1.2.8. Errata 2.1.6

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.1.6 更新的总结列表：

- 更新了在创建新集群时可用 Red Hat OpenShift Container Platform release ClusterImageSets 列表。(GitHub 10760)
- 在生成的导入命令中添加了引号，以避免在命令运行时出现可能的错误。(Bugzilla 1934184) (GitHub 9983)

1.2.9. Errata 2.1.5

备注：OpenShift Container Platform 版本 4.7 在裸机上不被支持。当 hub 集群在 OpenShift Container Platform 版本 4.7 上托管时，您无法使用 Red Hat Advanced Cluster Management hub 集群创建裸机受管集群。

- 修复了在订阅 CR 中错误地指定了 **packageOverrides** 时出现的日志错误。现在，错误会被正确记录，同时会忽略不正确的 **packageOverrides** 规格。(GitHub 10008)
- 更新了可用于添加集群的 Azure 区域列表。Bugzilla 1932430
- 修复了导致*应用程序拓扑*页显示意外错误的问题。(GitHub 9377)
- 修复了在使用 Helm 订阅从定义了 **spec.SecretRef** 的私有 Helm 频道订阅资源时，hub 集群订阅崩溃的问题。现在，对于这种类型的 Helm 订阅，hub 集群订阅不会崩溃。私有 Helm 仓库频道 secret 必须在同一个频道命名空间中定义。Bugzilla 1932430
- 修复了创建重复的 Ansible prehook 和 posthook 作业的问题。现在，应用程序订阅只创建一个 Ansible prehook 和 posthook 任务。(Bugzilla 1920654)
- *Overview* 页的更新，使其包含来自 hub 集群(local-cluster)的资源。(Bugzilla 1903446)

1.2.10. Errata 2.1.4

更新了镜像中所选容器。

1.2.11. Errata 2.1.3

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.1.3 更新的总结列表：

- 修复了 **multicluster-operators-hub** pod 中的 panic 错误，以便 **appsub** 成功部署（Bugzilla 1921531）。
- 修复了在 VMware 上创建的受管集群的问题，不使用为 worker 池 CPU、内存或磁盘大小提供的值。(GitHub 8930)
- 修复了证书策略控制器不会检测与策略中选择器匹配的已创建或删除命名空间。(GitHub 7639)
- 修复了 Grafana ClusterRoleBinding 对象失败的问题。(GitHub 7621)
- 修复了处理策略时配置策略控制器崩溃的问题。(GitHub 7569)
- 修复了编辑现有供应商连接时缺少命名空间的问题。(GitHub 7501)
- 修复了策略页面中的路由问题，以便在用户导航到不存在的策略的 URL 时显示 **No resource** 而不是加载动画。(GitHub 7445)

- 修复了在内容被复制粘贴时导致策略编辑器崩溃的问题；修复了当表单没有更新以显示有自定义规格时 **.spec.policyTemplate** 中的一个错误。(GitHub 7380)
- 添加了频道连接失败的信息，它可在订阅状态中找到。(GitHub 7177)
- 在控制台的 *Delete application* modal 中列出了可移动应用程序资源中的频道。现在无法在这个模式中删除频道。在这个版本中，只有订阅和放置规则才能在这个 modal 中被删除。(GitHub 7153)
- 修复了对 NIST 类别、标准和控制的显示问题，它们可以在所有策略元素间保持一致性，并会针对 NIST 内容进行调整。(GitHub 6954)
- 在默认安装中增加了搜索 pod 内存请求和限值，以便在不干预的情况下处理大多数工作负载：搜索 **redisgraph** pod 的内存限值为 4GB，搜索 API 的内存请求和 Redisgraph Pod 设置为 128MB。(GitHub 6890)
- 修复了 Git 频道与私有 Git 存储库连接失败的问题，在缺少 **secretRef** 时会导致 **multicluster-operators-hub-subscription** pod 崩溃。(GitHub 8764)
- 修复了因为 OpenShift Container Platform 4.6.10 安装的权限问题而造成启动 **cert-manager-webhook** 失败的问题。(GitHub 8517)
- 修复了高可用性配置会运行太多相互竞争的 compactor 的问题。在这个版本中，只会运行一个 compactor。(GitHub 7676)
- 修复了一个潜在的性能问题，有些 Grafana 仪表板自动刷新的时间间隔小于指标提取间隔。(GitHub 7665)
- 添加了对在 IBM Cloud 集群上导入 Red Hat OpenShift 的支持。（Bugzilla 1894778）
- 修复了 Git webhook 通知功能，通过订阅将所选 Git 存储库资源部署到目标集群。(GitHub 6785)
- 修复了成功部署但因为离线无法访问的应用程序拓扑资源的问题。现在，如果任何远程集群离线，集群节点会显示一个失败的状态。(GitHub 6298)

1.2.12. Errata 2.1.2

查看 Red Hat Advanced Cluster Management for Kubernetes Errata 2.1.2 更新的总结列表：

- 修复了一个会导致 hub 集群拒绝注册代理证书续订请求的问题，这个问题会导致一些注册代理在上一个月后出现离线问题。(GitHub 5628)
- 修复了在 Red Hat Advanced Cluster Management 升级时导致一些集群镜像集冲突的问题。(GitHub 7527)
- 修复了在升级过程中导致一些证书被删除的问题。(GitHub 7533)

1.2.13. Errata 2.1.1

查看 Red Hat Advanced Cluster Management Errata 2.1.1 更新总结列表：

- 更新了 **certificate** 和 **iam** 策略控制器，修复了一个阻止它们正确维护策略违反历史的问题。(GitHub 6014)
- 增加了 VMware 受管集群默认 worker 节点值（4 个 CPU、2 个内核、16384 MB 内存）与其他供应商保持一致。(GitHub 6206)

- 修复了在分离受管集群后在创建资源页面中导致临时错误的问题。(GitHub 6299)
- 修复了在关闭、修改和重新创建应用程序后， **Merge Update** 选项变为 **unset** 的问题。(GitHub 6349)
- 修复了在添加集群失败后阻止完全清理 Microsoft Azure 受管集群的问题。(GitHub 6353)
- 修复了应用程序拓扑在将 **helm** 类型应用程序部署到 **local-cluster** 后无法显示正确资源节点的问题。应用程序拓扑现在会显示所有类型的应用程序。(GitHub 6400)
- 应用程序订阅：为 Git **kustomization.yaml** 文件启用 **packageOverrides** YAML 内容，使其默认使用订阅注解中标识的路径。(GitHub 6476)
- 修复了当多个订阅使用同一分支共享同一 Git 频道时订阅被覆盖的问题。(GitHub 6476)
- 修复了在对象列表中使用 **musthave** 合规类型时其行为与 **mustonlyhave** 合规类型类似的问题。现在，您可以在对象列表中只指定一个字段，只要列表中的一个对象具有与策略中指定的对象匹配的字段时， **musthave** 策略就将其标记为合规。(GitHub 6492)
- 解决了配置所有 Thanos 接收器的问题，以便每个时间序列都存储 3 个副本。它还确保每个时间序列都成功写入目标散列中至少 2 个 Thanos 接收器。(GitHub 6547)
- 修复了在使用 **Create** 向导创建应用程序，然后在一个编辑器中打开它时导致 **merge update** 设置被清除的问题。(GitHub 6554)
- 修复了导致策略显示 **noncompliant** 状态的问题。(GitHub 6630)
- 修复了在频道和订阅上启用了 Git Webhook，但订阅的资源不会应用到目标集群的问题。(GitHub 6785)
- 解决可能导致 **create resource** 命令在第一次装载时出现 **Forbidden** 错误的问题。(GitHub 6798)
- 使用 Red Hat Advanced Cluster Management observability 组件为持久性卷公开以下额外指标：
  - **kubelet_volume_stats_available_bytes**
  - **kubelet_volume_stats_capacity_bytes**
  - **kube_persistentvolume_status_phase**
    这些指标不会在任何仪表板或警报规则中显式公开，但您可以查询它们并为它们设置自定义警报规则。(GitHub 6891)
- 修复了在创建新策略时的选择和取消选择不一致的问题。(GitHub 6897)
- 修复了导致裸机集群因为内存错误而无法升级到 2.1.0 的问题。(GitHub 6898) (Bugzilla 1895799)
- 修复了在 **open-cluster-management-observability** 命名空间中需要 pull secret 的问题，才能成功安装可观察性组件。现在，您不需要创建一个 pull secret 来安装可观察性组件。(GitHub 6911)
- 修复了导致监管和风险仪表板需要很长时间才能加载的问题。(GitHub 6925)
- 更正了启动新 Visual Web Terminal 会话时的 PATH 错误。(GitHub 6928)
- 修复了在运行时重启 Observability Operator 时，受管集群中可观察组件的时间问题，以使用不正确的镜像。(GitHub 6942)

- 添加了应用修复以针对私有 Git 存储库创建失败的应用程序进行操作的说明。(GitHub 6952) (Bugzilla 1896341)
- 修复了阻止 **klusterlet-addon-controller** 在 **open-cluster-management** 命名空间以外的命名空间中被识别的问题。(GitHub 6986)
- 修复了一个问题：当对象模板检查一个列表的字段时找到那个字段被设置但不是预期列表时会出现崩溃。(GitHub 7135)
- 修复了模板编辑器 YAML 过滤掉 placementRule **status:'True'** 设置的问题（当对所有在线集群上部署的一个应用程序做出更改时）。
  如果在保存更新的应用程序前，在 YAML 编辑器中为 placementRule 手动输入 **status：'True'** 时，设置会被保留。(GitHub 7152)
- 完成其他常规更改，以及未列出代码和文档的错误修复。

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。

- 已知的升级问题
- 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
- 已知的与安全相关的问题

1.3.1. 已知的升级问题

1.3.1.1. 由于 Observability 附加组件的问题，从 2.1.x 升级到 2.3.2 会造成降级的问题

从 2.1.x 升级到 2.3.2 后，一些集群可能会出现降级问题，因为 Observability 附加组件未就绪，镜像清单 ConfigMap 不会被正确读取，从而导致镜像不正确。

要解决这个问题，请运行以下命令重启 **multicluster-observability-operator** pod：

oc delete pod multicluster-observability-operator -n open-cluster-management

1.3.1.2. 升级到 2.1.x 会导致证书丢失

在将 Red Hat Advanced Cluster Management 从 2.0 升级到 2.1 后，指定在打开应用程序模板编辑器时不会预选应用程序的设置。如果您在应用程序模板编辑器中更改了应用程序设置，您必须在保存和关闭编辑器前选择应用部署设置。

1.3.1.3. 升级到 2.1.1 会导致证书丢失

当您的集群升级到 Red Hat Advanced Cluster Management 版本 2.1.1 时，您会丢失集群中的一些或全部证书。您可以输入以下命令之一来确认这种情况：

```
oc get certificates -n open-cluster-management
```

或

```
oc get pods -n open-cluster-management | grep -vE "Completed|Running"
```

如果您运行第一个命令时返回的证书数量少于预期，或者在运行第二个命令后返回一个以上 pod，请运行 **generate-update-issue-cert-manifest.sh** 脚本来更新证书。

1.3.1.4. 升级到 2.1.1 版本无法成功完成，有 ClusterImageSet 错误

在某些情况下，将 Red Hat Advanced Cluster Management for Kubernetes 2.1.0 升级到 Red Hat Advanced Cluster Management 2.1.1 无法完成，显示类似以下的错误：

```
failed to get candidate release: rendered manifests contain a resource
that already exists. Unable to continue with update: ClusterImageSet "img4.6.1-x86-64"
in namespace "" exists and cannot be imported into the current release: invalid
ownership metadata; label validation error: missing key "app.kubernetes.io/managed-by":
must be set to "Helm"; annotation validation error: missing key "meta.helm.sh/release-name":
must be set to "console-chart-c4cb5"; annotation validation error: missing key
"meta.helm.sh/release-namespace": must be set to "open-cluster-management"
```

当现有版本中的一个或多个 ClusterImageSet 的名称与升级时添加的版本的名称相同时会出现这种情况，这会导致冲突。要临时解决这个问题，请完成以下步骤：

1. 停止正在运行的升级。
2. 从您在错误消息中标识的本地环境中删除 ClusterImageSet 或 ClusterImageSets。
3. 重启升级。

1.3.1.5. 升级到 2.1.1 禁用 klusterletaddonconfig CRD

当您的 Red Hat Advanced Cluster Management 从 2.1.0 升级到 2.1.1 时，在升级过程中可能会重新安装 **klusterletaddonconfig** 自定义资源定义（CRD）。如果发生了这种情况，所有的附加组件在 *集群设置* 页面中都会显示为 **Disabled** 状态。完成以下步骤以诊断问题并恢复 klusterletaddonconfig CRD：

1. 使用 **oc login** 命令登录到 hub 集群。
2. 运行以下命令，以确认因为重新安装了 CRD 而导致 **klusterletaddonconfig** CRD 被删除：

   ```
   % oc get klusterletaddonconfig --all-namespaces
   ```

   如果返回的内容为 **No resources found**，则问题就可能是因为重新安装造成的。继续第 3 步。

3. 将以下脚本保存到文件中。在这个示例中，文件名是 **restore-addons.sh**：

   ```
   KUBECTL=oc
   ACM_NAMESPACE=open-cluster-management

   ACM_VERSION=$(${KUBECTL} get -n ${ACM_NAMESPACE} `${KUBECTL} get mch -
   oname -n ${ACM_NAMESPACE} | head -n1` -ojsonpath='{.status.desiredVersion}')
   if [ "${ACM_VERSION}" = ""  ]; then
   ACM_VERSION=2.1.1
   ```

```
fi

echo "ACM version: ${ACM_VERSION}"

for clusterName in `${KUBECTL} get managedcluster --ignore-not-found | grep -v "NAME" |
awk '{ print $1 }'`; do
    echo "Checking klusterletaddonconfig in ${clusterName} namespace."
    ${KUBECTL} get klusterletaddonconfig ${clusterName} -n ${clusterName} >/dev/null 2>&1
    if [ "$?" != "0"  ]; then
        echo "  klusterletaddonconfig in ${clusterName} is missing."
        echo "  Creating..."
        printf "  "
        cat <<EOF | ${KUBECTL}  apply -f -
apiVersion: agent.open-cluster-management.io/v1
kind: KlusterletAddonConfig
metadata:
  name: ${clusterName}
  namespace: ${clusterName}
spec:
  clusterLabels:
    cloud: auto-detect
    vendor: auto-detect
  clusterName: ${clusterName}
  clusterNamespace: ${clusterName}
  applicationManager:
    enabled: true
  certPolicyController:
    enabled: true
  iamPolicyController:
    enabled: true
  policyController:
    enabled: true
  searchCollector:
    enabled: true
  version: ${ACM_VERSION}
EOF

    fi
    echo "  Done."
done
```

如果您没有在 **open-cluster-management** 命名空间中安装 Red Hat Advanced Cluster Management，请将 **ACM_NAMESPACE** 的值替换为您的命名空间名称。

4. 通过 CLI 运行脚本。您的命令应类似以下命令：

```
chmod +x restore-addons.sh && ./restore-addons.sh
```

运行该脚本会在每个受管集群命名空间中重新创建缺少的 **klusterletaddonconfig** CRD。

1.3.1.6. 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。

1.3.1.7. 从 2.0.4 升级到 2.1 版会使 ClusterServiceVersion 处于待处理状态

从 Red Hat Advanced Cluster Management 版本 2.0.4 升级到 2.1 后，运行 **oc get csv** 命令。在输出中，Red Hat Advanced Cluster Management ClusterServiceVersion（CSV）的 **PHASE** 为 **Pending**，但 **NAME** 被更新至 **advanced-cluster-management.v2.1.0**。

要解决这个问题，请按照以下步骤查找并创建缺少的 **clusterRole** 自定义资源：

1. 输入以下命令查找由 Red Hat Advanced Cluster Management 2.1 CSV 部署的所有 **clusterrolebinding** 资源：

   ```
   oc get clusterrolebinding |grep advanced-cluster-management
   ```

   您的输出应类似以下内容：

   ```
   advanced-cluster-management.v2.1.0-86dfdf7c5d          ClusterRole/advanced-cluster-
   management.v2.1.0-86dfdf7c5d       9h
   advanced-cluster-management.v2.1.0-cd8d57f64           ClusterRole/advanced-cluster-
   management.v2.1.0-cd8d57f64        9h
   ```

2. 打开每个 **clusterrolebinding**，找到与 **open-cluster-management** 服务帐户关联的 **clusterRole** 名称。输入类似以下的命令：

   ```
   oc get clusterrolebinding advanced-cluster-management.v2.1.0-cd8d57f64 -o yaml
   ```

   您的输出应类似以下内容：

   ```
   apiVersion: rbac.authorization.k8s.io/v1
   kind: ClusterRoleBinding
   metadata:
     name: advanced-cluster-management.v2.1.0-cd8d57f64
   roleRef:
     apiGroup: rbac.authorization.k8s.io
     kind: ClusterRole
     name: advanced-cluster-management.v2.1.0-cd8d57f64
   subjects:
   - kind: ServiceAccount
     name: multicluster-operators
     namespace: open-cluster-management
   ```

3. 通过在 **.yaml** 文件中添加类似以下内容的内容来手动创建任何缺少的 **clusterRole** 条目：

   ```
   apiVersion: rbac.authorization.k8s.io/v1
   kind: ClusterRole
   metadata:
     name: advanced-cluster-management.v2.1.0-cd8d57f64
   rules:
   - apiGroups:
     - '*'
     resources:
     - '*'
     verbs:
     - '*'
   ```

1.3.2. 已知的与安装相关的问题

1.3.2.1. 安装过程中必须不存在证书管理器

在安装 Red Hat Advanced Cluster Management for Kubernetes 时，不能存在证书管理器。

当集群中已存在证书管理器时，Red Hat Advanced Cluster Management for Kubernetes 安装会失败。

要解决这个问题，请运行以下命令确认集群中是否存在证书管理器：

```
kubectl get crd | grep certificates.certmanager
```

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. 无法使用带有空空格的值搜索

在控制台和 Visual Web 终端中，用户无法搜索包括一个空空格的值。

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

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

1.3.3.6. 不再显示 Secret 的内容

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

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

1.3.3.7. 由于 *MultiClusterObservability* CR 名称，Observability 无法正常工作

当您使用唯一名称部署 **MultiClusterObservability** 自定义资源(CR)，则不会收集指标数据。指标不会被收集，因为 **metrics-collector** 不会被创建。当您部署可观察性时，Red Hat Advanced Cluster Management 只支持为 **MultiClusterObservability** CR 使用默认名称 **observability**。

1.3.4. 已知的与集群管理相关的问题

1.3.4.1. 可能不会显示新的裸机资产选项

创建并保存裸机资产后，您可以在表中选择裸机资产并应用所选操作。在这个版本中，在选择新的裸机资产后您可能不会看到可用的操作。刷新浏览器窗口，以便在表开始时恢复操作。

1.3.4.2. 无法在 OpenShift Container Platform 版本 4.7 上创建裸机受管集群

当 hub 集群在 OpenShift Container Platform 版本 4.7 上托管时，您无法使用 Red Hat Advanced Cluster Management hub 集群创建裸机受管集群。

1.3.4.3. 创建资源下拉菜单错误

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

> Error occurred while retrieving clusters info. Not found.

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

1.3.4.4. hub 集群和受管集群的时钟未同步

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

1.3.4.5. 控制台可能会报告受管集群策略不一致

导入集群后，请登录导入的集群，确保 Klusterlet 部署的所有 pod 都在运行。否则，在控制台中看到的数据可能不一致。

例如，如果策略控制器没有运行，您可能无法在 *监管和风险*以及*集群状态*页中得到同样的结果。

例如，您可能会看到 *Overview* 状态中没有（0 个）违反的情况，但可能会在 *监管和风险*页面中报告有 12 个违反情况。

在这种情况下，页面间不一致表示受管集群的 **policy-controller-addon** 和 hub 集群上的策略控制器之间断开连接。另外，受管集群可能没有足够的资源来运行所有 Klusterlet 组件。

因此，不会向受管集群传播该策略，或者未向受管集群报告违反情况。

1.3.4.6. 导入集群可能需要两次尝试

当您导入一个之前由 Red Hat Advanced Cluster Management hub 集群管理并分离的集群时，第一次导入过程可能会失败。集群状态为 **pending import**。再次运行命令，导入应可以成功。

1.3.4.7. 不支持导入 IBM OpenShift Kubernetes Service 集群的特定版本

您不能导入 IBM Red Hat OpenShift Kubernetes Service 版本 3.11 集群。支持 IBM OpenShift Kubernetes Service 的更新的版本。

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

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

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

1.3.4.9. 不支持为置备的集群进行自动 secret 更新

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

- Amazon Web Services (AWS)

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

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

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

  将 **CLUSTER-NAME** 替换为集群的名称。

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

- Microsoft Azure

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

- VMware vSphere

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

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

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

1.3.4.11. 无法在搜索中查看受管集群的节点信息

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

1.3.4.12. 销毁集群的进程没有完成

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

1. 手动确保云中没有孤立的资源，且清理与受管集群关联的所有供应商资源。

2. 输入以下命令为正在删除的受管集群打开 **ClusterDeployment**：

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

将 *mycluster* 替换为您要销毁的受管集群的名称。使用受管集群的命名空间替换 *namespace*。

3. 删除 **hive.openshift.io/deprovision** finalizer，以强制停止尝试清理云中的集群资源的进程。
4. 保存您的更改，验证 **ClusterDeployment** 是否已不存在。
5. 运行以下命令手动删除受管集群的命名空间：

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

使用受管集群的命名空间替换 *namespace*。

1.3.4.13. Grafana 控制台中没有指标数据

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

  "Annotation Query Failed"

  重新刷新浏览器，验证您是否已登录到 hub 集群。

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

  no project or cluster found

  检查角色权限并进行相应的更新。如需更多信息，请参阅基于角色的访问控制。

1.3.5. 已知的与应用程序管理相关的问题

1.3.5.1. 应用程序部署窗口错误

当您创建带有**在指定间隔内**设置为 **Active** 的部署窗口的应用程序时，可能无法正确计算部署窗口，从而导致应用程序在未定义时间部署。

1.3.5.2. 未部署资源拓扑状态

如果您的 Helm 订阅没有定义 **packageAlias**，则资源拓扑会将远程集群资源显示为 **Not deployed**。

请参阅配置软件包覆盖以定义正确的 **packageName** 和 **packageAlias**。

1.3.5.3. 在本地集群限制时部署应用程序

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

要解决这个问题，请执行以下步骤：

1. 在控制台中取消选择 **Deploy on local cluster**选项。

2. 选择 **Deploy application resources only on clusters matching specified labels**选项。

3. 创建以下标签：**local-cluster : 'true'**

1.3.5.4. 编辑应用程序时，控制台中的合并更新选项会取消选择

在应用程序控制台中，当您编辑应用程序时，**Merge updates（合并更新）**不会被取消选择。如果您之前选择了该选项且仍需要合并您的更新，则需要再次选择该选项。

要验证合并更新是否成功，请确保 **reconcile-option: merge** 在 YAML 订阅注解中。在控制台中完成以下步骤：

1. 单控制台中资源拓扑图中的 **Subscription** 节点。

2. 在弹出的订阅详情窗口中，点 **View Resource YAML** 按钮。

3. 确认 **apps.open-cluster-management.io/reconcile-option: merge** 注解在订阅 **.yaml** 文件中创建。

1.3.5.5. 如果存在私有 Git URL，则 Git 分支和 URL 路径字段不会被填充

如果您使用*私有* Git 仓库创建应用程序，点 **Create application** 创建另一个 Git 类型，以前的 URL 不会被填充到控制台的字段中。

应用程序编辑器在此例中不显示频道凭证详情。如果您更改了现有频道仓库的仓库身份验证信息，则该产品无法管理订阅该仓库的现有应用程序。

要解决这个问题，您可以更新频道资源的凭证信息，也可以删除并重新创建频道。

使用 YAML 编辑器使用最新凭证更新频道资源。请参阅链接的示例部分：../manage_applications#manage-apps-with-git-repositories[管理使用 Git 仓库的应用程序]。

1.3.5.6. 控制台管道卡可能会显示不同的数据

管道的搜索结果会返回准确数量的资源，但该数字在管道卡中可能会不同，因为在卡中显示的资源还没有被应用程序使用。

例如，在搜索 **kind:channel** 后，您可能会看到有 10 个频道，但控制台上的管道卡可能只会显示它使用的 5 个频道。

1.3.5.7. 命名空间频道

命名空间频道可以在代码中正常工作，但目前在文档中还没有包括这个选项。

1.3.5.8. 命名空间频道订阅处于失败状态

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

要强制订阅再次进行协调以退出 **FAILED** 状态，完成以下步骤：

1. 登录到您的 hub 集群。

2. 使用以下命令手动在订阅中添加一个标签：

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

1.3.5.9. 在一个命名空间频道中可部署的资源

您需要在频道命名空间中手动创建可部署的资源。

要正确创建可部署资源，将可部署资源所需的以下两个标签添加到订阅控制器中用于标识需要添加哪些可部署资源：

```
labels:
  apps.open-cluster-management.io/channel: <channel name>
  apps.open-cluster-management.io/channel-type: Namespace
```

不要在每个可部署 **spec.template.metadata.namespace** 中指定模板命名空间。

对于命名空间类型频道和订阅，所有可部署的模板都部署到受管集群的订阅命名空间中。因此，会跳过在订阅命名空间之外定义的可部署模板。

1.3.5.10. 为应用程序编辑角色错误

具有 **Editor** 角色的用户应只拥有应用程序的 **read** 或 **update** 授权。但这样的用户会错误地具有应用程序的 **create** 和 **delete** 的权限。Red Hat OpenShift Operator Lifecycle Manager 默认设置更改产品的设置。要解决这个问题，请遵循以下步骤：

1. 运行 **oc edit clusterrole applications.app.k8s.io-v1beta1-edit -o yaml** 以打开应用程序编辑集群角色。
2. 从 verbs 列表中删除 **create** 和 **delete**。
3. 保存更改。

1.3.5.11. 编辑放置规则错误的角色

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

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

1.3.5.12. 在更新的放置规则后没有部署应用程序

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

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

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

如果无法验证，请尝试再次导入集群并重新验证。

1.3.5.13. Subscription operator 不会创建一个 SCC

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

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

要手动在命名空间中创建 SCC CR，完成以下操作：

1. 找到在部署中定义的服务帐户。例如，查看以下 **nginx** 部署：

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

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

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

1.3.5.14. 应用程序频道需要唯一的命名空间

在同一命名空间中创建多个频道可能会导致 hub 集群出现错误。

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

1.3.6. 已知的与安全相关的问题

1.3.6.1. 在登录到控制台时出现内部错误 500

当安装了 Red Hat Advanced Cluster Management for Kubernetes，而且 OpenShift Container Platform 使用一个自定义的 ingress 证书，则会出现一个 **500 Internal Error** 信息。您无法访问控制台，因为 OpenShift Container Platform 证书没有包括在 Red Hat Advanced Cluster Management for Kubernetes management ingress 中。通过以下步骤添加 OpenShift Container Platform 证书：

1. 创建包含用于签发新证书的证书颁发机构的 ConfigMap：ConfigMap 必须与在 **openshift-config** 命名空间中创建的一样。运行以下命令：

```
oc create configmap custom-ca \
    --from-file=ca-bundle.crt=</path/to/example-ca.crt> \
    -n open-cluster-management
```

2. 运行以下命令来编辑 **multiclusterhub** YAML 文件：

```
oc edit multiclusterhub multiclusterhub
```

   a. 通过为 **customCAConfigmap** 编辑参数值来更新 **spec** 部分。参数可能类似以下内容：

```
customCAConfigmap: custom-ca
```

完成这些步骤后，请等待几分钟以使更新生效，然后重新登录。OpenShift Container Platform 证书被添加。

1.3.6.2. 在删除 helm 发行版本后恢复 *cert-manager*

如果您删除了 **cert-manager** 和 **cert-manager-webhook-helmreleases**，则会触发 Helm 发行版本自动重新部署 chart 并生成新证书。新证书必须与创建其他 Red Hat Advanced Cluster Management 组件的其他 helm chart 同步。要从 hub 集群中恢复证书组件，请完成以下步骤：

1. 运行以下命令删除 **cert-manager** 的 helm 发行版本：

```
oc delete helmrelease cert-manager-5ffd5
oc delete helmrelease cert-manager-webhook-5ca82
```

2. 验证 helm 发行版本是否已重新创建且 pod 正在运行。

3. 运行以下命令，确保证书的生成：

```
oc get certificates.certmanager.k8s.io
```

   您可能会收到以下响应：

```
(base) ➜  cert-manager git:(master) ✗ oc get certificates.certmanager.k8s.io
NAME                          READY   SECRET                        AGE
EXPIRATION
multicloud-ca-cert            True    multicloud-ca-cert            61m   2025-
09-27T17:10:47Z
```

4. 通过下载并运行 **generate-update-issuer-cert-manifest.sh** 脚本来更新这个证书的其他组件。

5. 验证 **oc get certificate.certmanager.k8s.io** 中的所有 secret 的就绪状态是否是 **True**。

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

1.4.1. 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。

1.4.2. 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

1.4.3. GDPR

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

1.4.3.1. 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

1.4.3.2. 更多关于 GDPR 的信息

- EU GDPR Information Portal

- Red Hat GDPR website

1.4.4. 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。

1.4.5. 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。

1.4.5.1. 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。

1.4.5.2. 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。

1.4.6. 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。

1.4.7. 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 集群状态数据存储在分布式键值存储 **etcd** 中。
- **用户身份验证数据，包括用户 ID 和密码：**用户 ID 和密码管理通过客户端企业 LDAP 目录进行处理。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 平台组件用于组件间访问的凭证定义为 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。

1.4.8. 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。

1.4.8.1. 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。

1.4.8.2. 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。

1.4.8.3. 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。

1.4.8.4. 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。

1.4.9. 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。

1.4.10. 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。

1.4.11. 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。

1.4.12. 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。