Red Hat Advanced Cluster Management for Kubernetes 2.7

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: 2024-09-05

Red Hat Advanced Cluster Management for Kubernetes 2.7 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

了解当前版本。

弃用： 不再支持 Red Hat Advanced Cluster Management 的 2.7 及更早的版本。文档可能仍然可用，但没有任何可用的勘误或其他更新。

- 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

如果您在当前支持的某个版本或产品文档时遇到问题，请访问 红帽支持，您可以在其中进行故障排除、查看知识库文章、与支持团队连接，或者创建一个问题单。您必须使用您的凭证登录。您还可以访问红帽客户门户文档，Red Hat Customer Portal FAQ 。

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。

- Web 控制台
- 集群
- 应用程序
- 监管
- 附加组件
- 备份和恢复

1.1.1. Web 控制台

- 使用搜索可配置的集合来管理您要由 hub 集群和受管集群收集的 Kubernetes 资源。如需了解更多详细信息，请参阅创建搜索可配置的集合。
- 使用 OpenShift Container Platform 监控来收集用户定义的指标。如需了解更多详细信息，请参阅添加用户工作负载指标。
- 在搜索功能中添加了一个新的自定义资源定义，名为 **searches.search.open-cluster-management.io**。要进一步自定义搜索，请参阅搜索自定义和配置以了解更多详细信息。
- 通过编辑 PostgreSQL 数据库存储和配置来优化搜索。请参阅搜索自定义和配置。

- 现在，您可以在 Grafana 中使用受管集群标签。请参阅在Grafana 中使用受管集群标签。

1.1.2. 集群

集群生命周期文档记录在 multicluster engine operator 中，它是一个软件 operator，用于增强集群群管理。

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，而 Red Hat Advanced Cluster Management 不是。

查看发行注记，以及 集群生命周期概述 中的任务和支持信息。

1.1.3. 应用程序

现在，您可以使用 **LeaderElection** 来更改控制器在故障时请求选择新领导者的方式，这样可确保一个领导实例一次处理协调。您可以增加或减少控制器获取 **LeaderElection** 所需的时间。请参阅配置领导选举机制。

现在，您可以使用 **AnsibleJob** 自定义资源启动 Ansible Automation Platform 工作流。将 **job_template_name** 字段替换为 **workflow_template_name** 来跟踪一组作业。请参阅配置 Ansible Automation Platform。

有关其他应用程序主题，请参阅管理应用程序。

1.1.4. 监管

- 您可以从自动化接收策略违反详情。请参阅监管自动化配置。
- 现在，日志由策略控制器名称与 **ManagedClusterAddOn** 资源区分。请参阅配置调试日志。
- 策略框架现在支持使用依赖项激活策略或策略模板。请参阅策略依赖项。
- 策略生成器现在引用本地和远程 Kustomize 配置，以提高灵活性。如需了解更多详细信息，请参阅策略生成器。
- 配置 hub 集群模板，以自动协调模板处理。例如，将 secret 和其他资源从 hub 集群同步到受管集群。请参阅重新处理的特殊注解。
- 在处理模板字符串后，使用 **toLiteral** 函数删除模板字符串的任何引号。如需了解更多详细信息，请参阅 *toLiteral* 功能。
- 您可以使用 OpenShift GitOps (ArgoCD) 管理策略定义。请参阅使用 OpenShift GitOps (ArgoCD) 管理策略定义。
- 现在，您在 *History* 列中收到一个策略补丁对象的状态事件。如需更多信息，请参阅监管页面。

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

- restic 和 rclone mover 现在默认以非 root 身份运行，且不再有 SE Linux 功能。如果 Pod 安全标准要求命名空间中的 pod 使用受限权限，则 restic 和 rclone 的 mover pod 不需要提升命名空间的权限。
- 您可以使用新的 Submariner **LoadBalancer** 模式来简化 Microsoft Azure Red Hat OpenShift 集

群和 Red Hat OpenShift Service on AWS 集群的部署。如需更多信息，请参阅 Preparing Microsoft Azure Red Hat OpenShift for Submariner by using the console (Technology Preview) 和 Preparing Red Hat OpenShift Service on AWS for Submariner by using the console (Technology Preview)。

- Submariner 现在支持断开连接的集群，以便减少安全问题。如需更多信息，请参阅在断开连接的集群中部署 Submariner。

1.1.6. 备份和恢复

- 您可以使用 Managed Service Account 组件自动将导入的集群连接到新的 hub 集群。如需了解更多详细信息，请参阅使用受管服务帐户自动连接集群。

1.1.7. 了解有关此发行版本的更多信息

- 欢迎使用 Red Hat Advanced Cluster Management for Kubernetes 包括了 Red Hat Advanced Cluster Management for Kubernetes 的概述。
- 请参阅 Red Hat Advanced Cluster Management 发行注记中的*已知问题和限制*。
- 多集群架构包括了与该产品主要组件相关的详细信息。
- 请参阅 Red Hat Advanced Cluster Management 故障排除指南中的支持信息和更多信息。
- 访问开源的 *Open Cluster Management* 存储库，以获取开源社区的交互、增长和贡献。要参与，请参阅 open-cluster-management.io。如需更多信息，请访问 GitHub 存储库。

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。

有关弃用和删除的更多信息，请参阅发行注记中的弃用和删除。

- 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/2.7/html/add-ons/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/2.7/html-single/add-ons/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. RBAC 用户需要额外的角色和角色绑定来查看升级后部署的资源

升级到 Red Hat Advanced Cluster Management 版本 2.7 后，**apps.open-cluster-management.io** 组中的资源的用户权限不可用。从 Red Hat Advanced Cluster Management 版本 2.7 开始，这些自定义资源定义不再由 OLM 部署，并会产生以下更改：

1. Red Hat Advanced Cluster Management 订阅控制台视图中不再提供资源类型，作为您可以选择创建资源的卡。
2. 分配给默认角色的聚合规则的 **clusterroles** 不适用于 API 资源类型。

如果 RBAC 用户需要访问这些资源，您必须授予正确的权限。

1.2.2.2. 在升级到勘误发行版本后，已弃用的资源会保留

从 2.4.x 升级到 2.5.x，然后再升级到 2.6.x，受管集群命名空间中的已弃用资源可能会被保留。如果版本 2.6.x 从 2.4.x 升级，则需要手动删除这些已弃用的资源：

注： 在从 2.5.x 升级到 2.6.x 版本前，您需要等待 30 分钟或更长时间。

您可以从控制台中删除，也可以运行类似以下示例的命令，用于您要删除的资源：

```
oc delete -n <managed cluster namespace> managedclusteraddons.addon.open-cluster-management.io <resource-name>
```

查看可能保留的已弃用资源列表：

```
managedclusteraddons.addon.open-cluster-management.io:
policy-controller
manifestworks.work.open-cluster-management.io:
-klusterlet-addon-appmgr
-klusterlet-addon-certpolicyctrl
-klusterlet-addon-crds
-klusterlet-addon-iampolicyctrl
```

```
-klusterlet-addon-operator
-klusterlet-addon-policyctrl
-klusterlet-addon-workmgr
```

1.2.2.3. 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。

1.2.2.4. 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。

1.2.2.5. 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. 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。

1.2.3.2. Firefox 的较老版本可能无法显示控制台的功能

对于旧版本的 Firefox，有模糊处理的问题。为了获得最好的兼容性，请升级至最新版本。

如需更多信息，请参阅支持的浏览器。

1.2.3.3. 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
```

1.2.3.4. 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
```

1.2.3.5. 无法编辑集群集的命名空间绑定

当使用 **admin** 角色或 **bind** 角色编辑集群集的命名空间绑定时，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。

1.2.3.6. 在置备托管的 control plane 集群后，水平滚动无法正常工作

置备托管的 control plane 集群后，如果 **ClusterVersionUpgradeable** 参数太长，您可能无法在 Red Hat Advanced Cluster Management 控制台的集群概述中水平滚动。因此，您无法查看隐藏的数据。

要临时解决这个问题，请使用浏览器缩放控制来缩放，增加 Red Hat Advanced Cluster Management 控制台窗口大小，或者复制文本并将其粘贴到不同的位置。

1.2.3.7. 使用与 Red Hat Ansible Automation Platform Operator 集成时出错

如果您使用依赖于 Ansible Automation Platform Operator 的集成，且没有在 Red Hat OpenShift Container Platform 集群上查看已安装的 Operator 的权限，您可能会看到类似如下的错误消息：

Ansible Automation Platform Operator 需要使用自动化模板。在自动化模板中使用工作流作业模板需要 2.2.1 或更高版本。

如果您使用已安装 Operator 的系统管理员确认，您可以安全地忽略错误消息。

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 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)**

1.2.4.4. 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。

1.2.4.5. 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。

1.2.4.6. 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**。

1.2.4.7. 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。

1.2.4.8. 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。

1.2.4.9. 升级后 Grafana 部署失败

如果您在 2.6 之前的系统中部署了 **grafana-dev** 实例，并将环境升级到 2.6，**grafana-dev** 无法正常工作。您必须运行以下命令来删除现有 **grafana-dev** 实例：

```
./setup-grafana-dev.sh --clean
```

使用以下命令重新创建实例：

```
./setup-grafana-dev.sh --deploy
```

1.2.4.10. *klusterlet-addon-search* pod 失败

klusterlet-addon-search pod 失败，因为达到内存限制。您必须通过自定义受管集群中的 **klusterlet-addon-search** 部署来更新内存请求和限制。在 hub 集群中编辑名为 **search-collector** 的 **ManagedclusterAddon** 自定义资源。在 **search-collector** 中添加以下注解并更新内存 **addon.open-cluster-management.io/search_memory_request=512Mi** 和 **addon.open-cluster-management.io/search_memory_limit=1024Mi**。

例如，如果您有一个名为 **foobar** 的受管集群，请运行以下命令将内存请求更改为 **512Mi**，内存限值为 **1024Mi** ：

```
oc annotate managedclusteraddon search-collector -n foobar \
addon.open-cluster-management.io/search_memory_request=512Mi \
addon.open-cluster-management.io/search_memory_limit=1024Mi
```

1.2.4.11. 启用 *disableHubSelfManagement* 在 Grafana 仪表板中会导致空列表

如果在 **mulitclusterengine** 自定义资源中将 **disableHubSelfManagement** 参数设置为 **true** 时，Grafana 仪表板会显示一个空标签列表。您必须将参数设置为 **false** 或删除参数来查看标签列表。如需了解更多详细信息，请参阅 disableHubSelfManagement。

1.2.4.12. 端点 URL 无法具有完全限定域名 (FQDN)

当您将 FQDN 或协议用于 **endpoint** 参数时，您的可观察性 pod 不会被启用。此时会显示以下出错信息：

```
Endpoint url cannot have fully qualified paths
```

输入没有协议部分的 URL。您的 **endpoint** 值必须类似您的 secret 的以下 URL：

```
endpoint: example.com:443
```

1.2.4.13. Grafana downsampled 数据不匹配

当您尝试查询历史数据时，计算的步骤值和 downsampled 数据之间存在差异，结果为空。例如，如果计算的步骤值为 **5m**，并且 downsampled 数据处于一小时的间隔，则数据不会出现在 Grafana 中。

此差异发生，因为 URL 查询参数必须通过 Thanos Query 前端数据源进行传递。之后，当数据缺失时，URL 查询可以对其他降级级别执行额外的查询。

您必须手动更新 Thanos Query 前端数据源配置。完成以下步骤：

1. 进入 Query 前端数据源。

2. 要更新您的查询参数，请点击 *Misc* 部分。
3. 在 *Custom query parameters* 字段中，选择 **max_source_resolution=auto**。
4. 要验证是否显示数据，请刷新 Grafana 页面。

您的查询数据会出现在 Grafana 仪表板中。

1.2.5. 已知的与集群管理相关的问题

集群管理或 *集群生命周期* 由带有或没有 Red Hat Advanced Cluster Management 的多集群引擎 operator 提供。请参阅以下已知问题和限制适用于 Red Hat Advanced Cluster Management 的集群管理。大多数已知的与集群管理相关的问题包括在 集群生命周期文档中。

1.2.5.1. 无法使用 Ansible Automation Platform 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 Automation Platform 集成，因为 Ansible Automation Platform Resource Operator 不提供 **ppc64le** 或 **s390x** 镜像。

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. 处于阻塞状态的应用程序

如果应用程序处于 **blocked** 状态，订阅会显示集群离线，但集群处于 **healthy** 和 **ready** 状态。

1.2.6.2. 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。

1.2.6.3. 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。

1.2.6.4. 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。

1.2.6.5. 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，请验证 **application-manager** pod 是否正在运行。**application-manager** 是需要在受管集群上运行的订阅容器。

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

您还可以在控制台中搜索 **kind:pod cluster:yourcluster** 来查看 **application-manager** 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 SCC CR。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 **kind: 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 Automation Platform

Red Hat Ansible Automation Platform Operator 无法访问启用了代理的 OpenShift Container Platform 集群之外的 Ansible Automation Platform。要解决这个问题，您可以在代理中安装 Ansible Automation Platform。请参阅 Ansible Automation Platform 提供的安装步骤。

1.2.6.14. 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'
```

1.2.6.15. 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。

1.2.6.16. 没有应用程序控制台拓扑过滤

2.7 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。

1.2.6.17. 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。

1.2.7. 已知的监管问题

1.2.8. 策略生成器会忽略 *ignorePending* 标志

如果您在策略生成器中设置 **consolidateManifests: true**，则 **ignorePending** 标志会被忽略。

如果需要实现 **ignorePending** 功能，您可以设置 **consolidateManifests: false**。

1.2.8.1. 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。

1.2.8.2. 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。

1.2.8.3. 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。

1.2.8.4. 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

1.2.8.5. ConfigurationPolicy CRD 处于终止状态

当您通过在 **KlusterletAddonConfig** 或分离集群中禁用策略控制器，或从受管集群中删除 **config-policy-controller** 附加组件时，**ConfigurationPolicy** CRD 可能会处于终止状态。如果 **ConfigurationPolicy** CRD 处于终止状态，如果稍后重新安装附加组件，则可能不会添加新策略。您还可以收到以下错误：

```
template-error; Failed to create policy template: create not allowed while custom resource definition is terminating
```

使用以下命令检查 CRD 是否卡住：

```
oc get crd configurationpolicies.policy.open-cluster-management.io -o=jsonpath='{.metadata.deletionTimestamp}'
```

如果删除时间戳位于资源上，则 CRD 会卡住。要解决这个问题，从集群中保留的配置策略中删除所有终结器。在受管集群中使用以下命令，将 **<cluster-namespace>** 替换为受管集群命名空间：

```
oc get configurationpolicy -n <cluster-namespace> -o name | xargs oc patch -n <cluster-namespace> --type=merge -p '{"metadata":{"finalizers": []}}'
```

配置策略资源会自动从集群中移除，CRD 会退出其终止状态。如果已经重新安装了附加组件，则在没有删除时间戳的情况下自动重新创建 CRD。

1.2.9. 在修改现有配置策略时，*pruneObjectBehavior* 无法正常工作

当您修改现有配置策略时，**pruneObjectBehavior** 无法正常工作。查看 **pruneObjectBehavior** 可能无法正常工作的原因：

- 如果您在配置策略中将 **pruneObjectBehavior** 设置为 **DeleteAll** 或 **DeleteIfCreated**，则不会正确清理修改前创建的旧资源。当您删除配置策略时，只有策略创建和策略更新中的新资源才会被跟踪和删除。
- 如果将 **pruneObjectBehavior** 设置为 **None** 或没有设置参数值，则可能会在受管集群上意外删除旧对象。具体来说，当用户更改模板中的 **name**, **namespace**, **kind**, or **apiversion** 时这会发生。当 **object-templates-raw** 或 **namespaceSelector** 参数更改时，参数字段可以动态更改。

1.2.9.1. 强制时策略状态显示重复的更新

如果策略被设置为 **remediationAction: enforce** 并重复更新，Red Hat Advanced Cluster Management 控制台会显示重复违反情况，并成功更新。这可能会在以下两个情况下发生：

- 另一个控制器或进程也使用不同的值更新对象。
  要解决这个问题，请禁用策略并比较策略和受管集群上的 **objectDefinition** 之间的不同。如果值不同，则可能会更新另一个控制器或进程。检查对象的**元数据**，以帮助识别值的不同原因。
- **ConfigurationPolicy** 中的 **objectDefinition** 不匹配，因为 Kubernetes 在应用策略时处理对象。
  要解决这个问题，请禁用策略并比较策略和受管集群上的 **objectDefinition** 之间的不同。如果键不同或缺失，Kubernetes 可能会在将密钥应用到对象之前处理密钥，如删除包含默认值或空值的键。

已知示例：

Kind	问题描述
PodSecurityPolicy	Kubernetes 删除值为 **false** 的键，您可以在受管集群上看到生成的对象。在本例中，从策略中的 **objectDefinition** 中删除密钥。
Secret	**stringData** 映射由 Kubernetes 处理，到使用 **base64** 编码值的**数据**。不使用 **stringData**，而是直接使用 **base64** 编码值的**数据**，而不是字符串。

1.2.9.2. 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。

1.2.9.3. OpenShift 4.12 及更新的版本不支持 Pod 安全策略

对 Pod 安全策略的支持已从 OpenShift Container Platform 4.12 及更新的版本中删除，并从 Kubernetes v1.25 及之后的版本中删除。如果应用 **PodSecurityPolicy** 资源，您可能会收到以下不合规的信息：

```
violation - couldn't find mapping resource with kind PodSecurityPolicy, please check if you have CRD deployed
```

1.2.10. 为策略自动化创建重复的 Ansible 作业

如果您有一个设置为 *Run once* mode 并禁用的 **PolicyAutomation**，则会创建额外的 Ansible 作业。您可以删除额外的 Ansible 作业。完成以下步骤：

1. 运行以下命令来查看 Ansible 作业列表：

```
oc get ansiblejob -n {namespace}
```

2. 使用以下命令删除重复的 Ansible 作业：

```
oc delete ansiblejob {ansiblejob name} -n {namespace}
```

1.2.11. 备份和恢复已知问题

1.2.11.1. *BackupSchedule* 在使用 OADP 1.1.2 或更高版本时显示 *FailedValidation* 状态

启用 Red Hat Advanced Cluster Management 备份和恢复组件并成功创建 **DataProtectionApplication** 资源后，会创建一个 **BackupStorageLocation** 资源，状态为 **Available**。当您使用 OADP 版本 1.1.2 或更高版本时，您可能会在创建 **BackupSchedule** 资源后收到以下信息，其状态为 **FailedValidation** ：

```
oc get backupschedule -n open-cluster-management-backup
NAME PHASE MESSAGE
rosa-backup-schedule FailedValidation Backup storage location is not available. Check
velero.io.BackupStorageLocation and validate storage credentials.
```

此错误是由 **BackupStorageLocation** 资源中的 **ownerReference** 缺少的值造成的。**DataProtectionApplication** 资源的值应用作 **ownerReference** 的值。

要临时解决这个问题，请手动将 **ownerReference** 添加到 **BackupStorageLocation** 中：

1. 运行以下命令，打开 **oadp-operator.v1.1.2** 文件：

```
oc edit csv -n open-cluster-management-backup oadp-operator.v1.1.2
```

2. 通过将 **1** 替换为 OADP operator CSV 中的 **0** 来编辑 **spec.deployments.label.spec.replicas** 的值。

3. 对 YAML 脚本中的 **ownerReference** 注解进行补丁，如下例所示：

```
metadata:
resourceVersion: '273482'
name: dpa-sample-1
uid: 4701599a-cdf5-48ac-9264-695a95b935a0
namespace: open-cluster-management-backup
ownerReferences: <<

apiVersion: oadp.openshift.io/v1alpha1
blockOwnerDeletion: true
controller: true
kind: DataProtectionApplication
name: dpa-sample
uid: 52acd151-52fd-440a-a846-95a0d7368ff7
```

4. 将 **spec.deployments.label.spec.replicas** 的值改回到 **1**，以使用新设置启动数据保护应用进程。

1.2.11.2. Velero 恢复限制

如果在其中恢复数据的新 hub 集群有用户创建的资源，则这个新的 hub 集群可能会有与活跃的 hub 集群不同的配置。例如，在将备份的数据恢复到新的 hub 集群中之前，在这个新的 hub 集群上可能已包括了一个现存的策略。

如果不是恢复的备份的一部分，Velero 会跳过现存的资源，因此新 hub 集群上的策略不会改变，这会导致新 hub 集群和活跃 hub 集群之间的不同配置。

为解决这个问题，集群备份和恢复 Operator 可以运行一个恢复后的操作以清理由用户创建的资源，或在 **restore.cluster.open-cluster-management.io** 资源时执行不同的恢复操作。

如需更多信息，请参阅管理备份和恢复 operator 中的 *在恢复前清理 hub 集群* 部分。

1.2.11.3. 被动配置不显示受管集群

只有在被动 hub 集群上恢复激活数据时，才会显示受管集群。

1.2.11.4. 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。请参阅管理备份和恢复 operator 主题中的*准备新的 hub 集群*。

1.2.11.5. 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。

1.2.11.6. 导入的受管集群显示 *Pending Import* 状态

在主 hub 集群上手动导入的受管集群会在被动 hub 集群上恢复激活数据时显示一个 **Pending Import** 状态。如需更多信息，请参阅使用受管服务帐户自动连接集群。

1.2.11.7. 恢复 hub 集群后，*appliedmanifestwork* 不会被从受管集群中删除

当在新 hub 集群上恢复 hub 集群数据时，**appliedmanifestwork** 不会从没有固定集群集的应用程序订阅的放置规则的受管集群中删除。

有关不是固定集群集的应用程序订阅，请参阅以下放置规则示例：

```
spec:
  clusterReplicas: 1
  clusterSelector:
    matchLabels:
      environment: dev
```

因此，当受管集群从恢复的 hub 集群分离时，应用程序会被孤立。

要避免这个问题，请在放置规则中指定固定的集群集。请参见以下示例：

```
spec:
  clusterSelector:
    matchLabels:
      environment: dev
```

您还可以通过运行以下命令来手动删除剩余的 **appliedmanifestwork** ：

```
oc delete appliedmanifestwork <the-left-appliedmanifestwork-name>
```

1.2.11.8. *appliedmanifestwork* 不会被删除，hub 集群放置规则没有固定的集群集

当在新 hub 集群上恢复 hub 集群数据时，**appliedmanifestwork** 不会从没有固定集群集的应用程序订阅的放置规则的受管集群中删除。因此，当受管集群从恢复的 hub 集群分离时，应用程序会被孤立。

有关不是固定集群集的应用程序订阅，请参阅以下放置规则示例：

+

```
spec:
  clusterReplicas: 1
  clusterSelector:
    matchLabels:
      environment: dev
```

要避免这个问题，请在放置规则中指定固定的集群集。请参见以下示例：

+

```
spec:
  clusterSelector:
    matchLabels:
      environment: dev
```

您还可以通过运行以下命令来手动删除剩余的 **appliedmanifestwork** ：

```
oc delete appliedmanifestwork <the-left-appliedmanifestwork-name>
```

1.2.11.9. *appliedmanifestwork* 不会被删除，规格中缺少 *agentID*

当您将 Red Hat Advanced Cluster Management 2.6 用作主 hub 集群时，但您的恢复 hub 集群位于 2.7 或更高版本的版本时，**appliedmanifestworks** 规格中缺少 **agentID**，因为此字段在 2.7 发行版本中引入。这会为受管集群上的主 hub 生成额外的 **appliedmanifestworks**。

要避免这个问题，请将主 hub 集群升级到 Red Hat Advanced Cluster Management 2.7，然后在新的 hub 集群中恢复备份。

通过为每个 **appliedmanifestwork** 手动设置 **spec.agentID** 来修复受管集群。

1. 运行以下命令来获取 **agentID** ：

   ```
   oc get klusterlet klusterlet -o jsonpath='{.metadata.uid}'
   ```

2. 运行以下命令，为每个 **appliedmanifestwork** 设置 **spec.agentID** ：

   ```
   oc patch appliedmanifestwork <appliedmanifestwork_name> --type=merge -p '{"spec":
   {"agentID": "'$AGENT_ID'"}}'
   ```

1.2.11.10. *managed-serviceaccount* add-on 状态显示 *Unknown*

如果您使用 Managed Service Account，则受管集群 **appliedmanifestwork addon-managed-serviceaccount-deploy** 会从导入的受管集群中删除，而无需在新 hub 集群的 multicluster engine for Kubernetes operator 资源中启用它。

受管集群仍然导入到新的 hub 集群，但 **managed-serviceaccount** add-on 状态显示 **Unknown**。

在 multicluster engine operator 资源中启用 Managed Service Account 后，您可以恢复 **managed-serviceaccount** 附加组件。请参阅启用自动导入以了解如何启用受管服务帐户。

1.2.12. Submariner 已知问题

1.2.12.1. 没有 *ClusterManagementAddon* submariner 附加组件失败

对于版本 2.8 及更早版本，在安装 Red Hat Advanced Cluster Management 时，您还可以使用 Operator Lifecycle Manager 部署 **submariner-addon** 组件。如果您没有创建 **MultiClusterHub** 自定义资源，**submariner-addon** pod 会发送错误，并阻止 Operator 安装。

发生以下通知，因为缺少 **ClusterManagementAddon** 自定义资源定义：

```
graceful termination failed, controllers failed with error: the server could not find the requested resource (post clustermanagementaddons.addon.open-cluster-management.io)
```

ClusterManagementAddon 资源由 **cluster-manager** 部署创建，但当集群中安装 **MultiClusterEngine** 组件时，此部署将可用。

如果在创建 **MultiClusterHub** 自定义资源时没有在集群中可用的 **MultiClusterEngine** 资源，**MultiClusterHub** operator 会部署 **MultiClusterEngine** 实例，以及所需的 Operator，用于解决前面的错误。

1.2.12.2. 不是 Red Hat Advanced Cluster Management 可以管理的所有基础架构供应商都被支持

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 。

1.2.12.3. 有限的无头服务支持

在使用 Globalnet 时，在没有选择器的情况下的无头服务不支持服务发现。

1.2.12.4. 不支持在启用 NAT 时使用 VXLAN 的部署

只有非 NAT 部署支持使用 VXLAN 电缆驱动程序的 Submariner 部署。

1.2.12.5. OVN Kubernetes 需要 OCP 4.11 及更新的版本

如果使用 OVN Kubernetes CNI 网络，则需要 Red Hat OpenShift 4.11 或更高版本。

1.2.12.6. 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。

1.2.12.7. 自签名证书可能会阻止到代理的连接

代理上的自签名证书可能会阻止加入集群连接到代理。连接失败并显示证书验证错误。您可以通过在相关 **SubmarinerConfig** 对象中将 **InsecureBrokerConnection** 设置为 **true** 来禁用代理证书验证。请参见以下示例：

```
apiVersion: submarineraddon.open-cluster-management.io/v1alpha1
kind: SubmarinerConfig
metadata:
  name: submariner
```

```
    namespace: <managed-cluster-namespace>
spec:
    insecureBrokerConnection: true
```

1.2.12.8. Submariner 只支持 OpenShift SDN 或 OVN Kubernetes

Submariner 只支持使用 OpenShift SDN 或 OVN-Kubernetes Container Network Interface (CNI) 网络供应商的 Red Hat OpenShift Container Platform 集群。

1.2.12.9. Microsoft Azure 集群的命令限制

subctl diagnose firewall inter-cluster 命令无法在 Microsoft Azure 集群中工作。

1.2.13. *EditApplicationSet* 扩展功能重复

当您添加多个标签表达式或尝试为 **ApplicationSet** 输入集群选择器时，您可能会重复收到以下信息，"Expand to enter expression"。尽管出现这个问题，您可以输入集群选择。

1.2.13.1. 自动升级无法使用自定义 *CatalogSource* 或 *Subscription*

当 Red Hat Advanced Cluster Management for Kubernetes 升级时，Submariner 会被自动升级。如果您使用自定义 **CatalogSource** 或 **Subscription**，则自动升级可能会失败。

为确保在受管集群上安装 Submariner 时自动升级可以正常工作，您必须在每个受管集群的 **SubmarinerConfig** 自定义资源中将 **spec.subscriptionConfig.channel** 字段设置为 **stable-0.14**。

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 2.7.13

- 为一个或多个产品容器镜像提供更新。

1.3.2. Errata 2.7.12

- 修复了在为外部端点创建 Kubernetes secret 时阻止 **tlsSecretMountPath** 正常工作的问题。(ACM-7717)
- 为一个或多个产品容器镜像提供更新。

1.3.3. Errata 2.7.11

- 为一个或多个产品容器镜像提供更新。

1.3.4. Errata 2.7.10

- 为一个或多个产品容器镜像提供更新。
- 修复了导致 pod 从不正确的 registry 中拉取镜像的问题。(ACM-6615)
- 修复了导致策略因为空 标签 参数而无法识别的问题。(ACM-7055)
- 修复了策略模板更改导致合并不一致或控制器不响应的问题。(ACM-7799)

1.3.5. Errata 2.7.9

- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.6. Errata 2.7.8

- 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 2.7.7

- 为一个或多个产品容器镜像和安全修复提供更新。
- 修复了在将受管集群添加到 Red Hat Advanced Cluster Management for Kubernetes 时导致 **enableUserWorkload: true** 设置被删除的问题。(ACM-3938)
- 修复了导致管理 pod 没有固定到保留内核并缺少正确的注解的问题。(ACM-5110)
- 修复导致搜索索引程序报告错误的问题。(ACM-5168)
- 修复了在删除 **enableUserWorkload: true** 设置时导致 **uwl-metrics-controller** 部署不会被自动删除的问题。(ACM-5268)
- 修复了一个 **APIService** 问题，它在控制台中禁用 **Create cluster** 和 **Import cluster** 按钮。(ACM-5460)
- 修复了在禁用警报转发时删除了 **hub-alertmanager-router-ca** 和 **observability-alertmanager-accessor** secret 的问题。(ACM-5623)
- 修复了在 hub 集群恢复过程中删除与基于订阅的工作负载关联的受管资源的问题。(ACM-5795)

1.3.8. Errata 2.7.6

- 更正使用 hub 集群模板功能的策略的根策略状态以及受管集群自定义资源。(ACM-5547)
- 修复了在 hub 集群中策略和策略之间造成不匹配状态的问题。(ACM-6042)

1.3.9. Errata 2.7.5

- 为一个或多个产品容器镜像提供更新。

1.3.10. Errata 2.7.4

- 为一个或多个产品容器镜像和安全修复提供更新。

1.3.11. Errata 2.7.3

- 现在，*Applications* 侧边栏可以更快地加载，即使有大量应用程序。(ACM-2503)
- 修复了在启用 Red Hat OpenShift Container Platform 集群范围代理时阻止使用 **cluster-proxy-addon** 的问题。(ACM-3208)
- 修复了导致在没有空字段的情况下创建监管资源以及合规状态不一致的问题。(ACM-3424)
- **ClusterIP** 服务现在仅在它们就绪后解决。(ACM-3751)
- 修复了导致 **MEMCACHED** 索引中的 **max_item_size** 设置不会对所有 **MEMCACHED** 客户端传播更改的问题。(ACM-4685)

1.3.12. Errata 2.7.2

- 添加了对在 Microsoft Azure 上使用 Red Hat OpenShift Container Platform 4.12 的支持。(ACM-3223)
- 添加了对 YAML 内容的支持，以扩展到策略模板中的一行。(ACM-3517)

1.3.13. Errata 2.7.1

- 修复了导致受管集群在 Topology 中离线的控制台问题，即使受管集群在线也是如此。(ACM-3466)

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。

弃用： 不再支持 Red Hat Advanced Cluster Management 的 2.7 及更早的版本。文档可能仍然可用，但没有任何可用的勘误或其他更新。

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

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 已正式发布（GA），提供 12 个月或跨三个发行版本（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 通常在九个月或跨三个发行版本（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
应用程序	**v1alpha1** API 已完全删除。GitOps 集群 API 升级至 **V1beta1**。	2.5	使用 **V1beta1**。	无
应用程序	**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。
ManagedClusterSets	**v1beta1** API 升级到 **v1beta2**，因为 **v1beta1** 已被弃用。	2.7	使用 **v1beta2**。	无
ManagedClusterSetBindings	**v1beta1** API 升级到 **v1beta2**，因为 **v1beta1** 已被弃用。	2.7	使用 **v1beta2**。	无

产品或类别	受影响的项	Version	推荐的操作	详情和链接
ClusterManagementAddOn	字段 **addOnConfiguration** 在 **ClusterManagementAddOn** spec 中已弃用。	2.7	使用 **supportedConfigs** 字段。	无
ManagedClusterAddOn	字段 **addOnConfiguration** 在 **ManagedClusterAddOn** spec 中已弃用。	2.7	使用 **supportedConfigs** 字段。	无

1.4.1.2. API 删除

产品或类别	受影响的项	Version	推荐的操作	详情和链接
HypershiftDeployment	**HypershiftDeployment** API 已被删除。	2.7	不要使用这个 API。	
BareMetalAssets	**v1alpha1** API 被删除。	2.7	不要使用这个 API。	Baremetalassets.inventory.open-cluster-management.io
放置	**v1alpha1** API 被删除。	2.7	使用 **v1beta1** 替代。	Placements.cluster.open-cluster-management.io
PlacementDecisions	**v1alpha1** API 被删除。	2.7	使用 **v1beta1** 替代。	PlacementDecisions.cluster.open-cluster-management.io
ManagedClusterSets	**v1alpha1** API 被删除。	2.7	使用 **v1beta1** 替代。	ManagedClusterSets.cluster.open-cluster-management.io
ManagedClusterSetBindings	**v1alpha1** API 被删除。	2.7	使用 **v1beta1** 替代。	ManagedClusterSetBindings.cluster.open-cluster-management.io

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。	2.6	不要使用这个 API。	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	**v1** API 已被弃用。	2.6	不要使用这个 API。	ApplicationManager.agent.open-cluster-management.io
IAMPolicyController	**v1** API 已被弃用。	2.6	不要使用这个 API。	IAMPolicyController.agent.open-cluster-management.io
PolicyController	**v1** API 已被弃用。	2.6	不要使用这个 API。	PolicyController.agent.open-cluster-management.io
SearchCollector	**v1** API 已被弃用。	2.6	不要使用这个 API。	SearchCollector.agent.open-cluster-management.io
WorkManager	**v1** API 已被弃用。	2.6	不要使用这个 API。	WorkManager.agent.open-cluster-management.io

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
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。

产品或类别	受影响的项	Version	推荐的操作	详情和链接
安装程序	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 中的 **ingress.sslCiphers** 字段	2.7	无	请参阅高级配置来配置安装。
安装程序	**operator.open-cluster-management.io_multiclusterhubs_crd.yaml** 中的 **customCAConfigmap** 字段	2.7	无	请参阅高级配置来配置安装。
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。
应用程序	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

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
监管	之前的版本中使用的管理入口已被删除。	2.7	您无法自定义管理入口证书。如果您将自己的证书与管理入口搭配使用，则必须使用以下命令删除证书：**oc -n open-cluster-management delete secret byo-ca-cert byo-ingress-tls-secret**	None
搜索	**SearchCustomizations.open-cluster-management.io** 自定义资源定义已被删除。	2.7	使用 **search.open-cluster-management.io/v1alpha1** 自定义搜索。	None
搜索	RedisGraph 被 PostgreSQL 替代作为内部数据库。	2.7	不需要更改。	使用 PostgreSQL 作为内部数据库重新实施搜索组件。
控制台（Console）	独立 Web 控制台	2.7	使用集成的 Web 控制台。	如需更多信息，请参阅访问您的控制台。
监管	完整性盾牌 （技术预览）	2.7	您可以继续使用完整性盾牌作为社区提供的签名解决方案。如需了解更多详细信息，请参阅 Integrity Shield 文档。Getting Started documentation	None
集群	使用标签配置 Red Hat Ansible 作业	2.6	使用控制台配置 Red Hat Ansible 作业。	如需更多信息，请参阅使用控制台将 Automation 模板配置为在集群中运行。
集群	使用裸机资产创建集群	2.6	使用控制台创建基础架构环境	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	2.6	None	None

产品或类别	受影响的项	Version	推荐的操作	详情和链接
监管	自定义策略控制器	2.6	不需要操作	None
监管	未使用的 **LabelSelector** 参数已从配置策略中删除。	2.6	None	请参阅 Kubernetes 配置策略控制器文档。
应用程序	可部署控制器	2.5	None	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	None
应用程序	单个 ArgoCD 导入模式，导入至 hub 集群中的一个 ArgoCD 服务器的 secret。	2.3	您可以将集群 secret 导入到多个 ArgoCD 服务器中	None
应用程序	ArgoCD 集群集成：**spec.applicationManager.argocdCluster**	2.3	创建 GitOps 集群和放置自定义资源以注册受管集群。	在受管集群中配置 GitOps
监管	**cert-manager** 内部证书管理	2.3	不需要操作	None
监管	自定义策略控制器	2.6	不需要操作	None
监管	未使用的 **LabelSelector** 参数已从配置策略中删除。	2.6	None	请参阅 Kubernetes 配置策略控制器文档。
监管	完整性盾牌 （技术预览）	2.7	None	您可以继续使用完整性盾牌作为社区提供的签名解决方案。如需了解更多详细信息，请参阅 Integrity Shield 文档。Getting Started documentation

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

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

Red Hat Advanced Cluster Management for Kubernetes 为 FIPS 设计。当以 FIPS 模式在 Red Hat OpenShift Container Platform 上运行时，OpenShift Container Platform 会使用 Red Hat Enterprise Linux 加密库提交给 NIST 进行 OpenShift Container Platform 支持的架构。有关 NIST 验证程序的更多信息，请参阅加密模块验证程序。有关为验证提交的 RHEL 加密库的单独版本的最新 NIST 状态，请参阅 Compliance Activities 和 Government Standards。

如果您计划管理启用了 FIPS 的集群，则必须在配置为以 FIPS 模式操作的 OpenShift Container Platform 集群上安装 Red Hat Advanced Cluster Management。hub 集群必须处于 FIPS 模式，因为在受管集群中使用在 hub 集群中创建的加密。

要在受管集群中启用 FIPS 模式，请在置备 OpenShift Container Platform 受管集群时设置 **fips: true**。置备集群后您无法启用 FIPS。如需更多信息，请参阅 OpenShift Container Platform 文档，是否需要额外的安全集群？

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 只支持 x86_64 架构上的 FIPS。
- 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.

1.6.2. 其他资源

- 有关 NIST 验证程序的更多信息，请参阅加密模块验证程序。

- 有关为验证提交的 RHEL 加密库的单独版本的最新 NIST 状态，请参阅 Compliance Activities 和 Government Standards。