



Red Hat Advanced Cluster Management for Kubernetes 2.5

Release notes

Read more about Release notes for what's new, errata updates, known issues, deprecations and removals, and product considerations for GDPR and FIPS readiness.

Red Hat Advanced Cluster Management for Kubernetes 2.5 Release notes

Read more about Release notes for what's new, errata updates, known issues, deprecations and removals, and product considerations for GDPR and FIPS readiness.

Legal Notice

Copyright © 2023 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

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

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

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

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

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

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

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

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

All other trademarks are the property of their respective owners.

Abstract

Read more about Release notes for what's new, errata updates, known issues, deprecations and removals, and product considerations for GDPR and FIPS readiness.

Table of Contents

CHAPTER 1. RELEASE NOTES	6
1.1. WHAT'S NEW IN RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES	6
1.1.1. Web console	6
1.1.1.1. Observability	7
1.1.2. Clusters	7
1.1.3. Applications	9
1.1.4. Governance	9
1.1.5. Add-ons	9
1.2. KNOWN ISSUES	10
1.2.1. Documentation known issues	10
1.2.1.1. Documentation links in the Customer Portal might link to a higher-level section	10
1.2.2. Installation known issues	10
1.2.2.1. Pods might not come back up after upgrading Red Hat Advanced Cluster Management	11
1.2.2.2. OpenShift Container Platform cluster upgrade failed status	11
1.2.2.3. Two cluster curator controllers are running at the same time after upgrade	11
1.2.2.4. Create MultiClusterEngine button not working	11
1.2.3. Web console known issues	11
1.2.3.1. Dark mode is not supported on Red Hat Advanced Cluster Management version 2.5.x	11
1.2.3.2. Dark mode is not supported on multicluster engine for Kubernetes operator version 2.0.x	12
1.2.3.3. LDAP user names are case-sensitive	12
1.2.3.4. Console features might not display in Firefox earlier version	12
1.2.3.5. Restrictions for storage size in search customization	12
1.2.3.6. Search query parsing error	12
1.2.3.7. Cannot edit namespace bindings for cluster set	12
1.2.3.8. False scaling alert in cluster details	12
1.2.4. Observability known issues	13
1.2.4.1. Duplicate local-clusters on Service-level Overview dashboard	13
1.2.4.2. Observability endpoint operator fails to pull image	13
1.2.4.3. There is no data from ROKS and HyperShift clusters	13
1.2.4.4. There is no etcd data from ROKS and HyperShift clusters	13
1.2.4.5. High CPU usage by the search-collector pod	13
1.2.4.6. Search pods fail to complete the TLS handshake due to invalid certificates	14
1.2.4.7. Metrics are unavailable in the Grafana console	14
1.2.4.8. Prometheus data loss on managed clusters	14
1.2.4.9. Error ingesting out-of-order samples	14
1.2.4.10. Grafana deployment fails on managed clusters	15
1.2.5. Cluster management known issues	15
1.2.5.1. Disconnected installation settings for cluster creation cannot be entered or are ignored if entered	15
1.2.5.2. Credential with disconnected installer does not distinguish between the certificates	15
1.2.5.3. Manual removal of the VolSync CSV required on managed cluster when removing the add-on	15
1.2.5.4. Provisioning a bare metal managed cluster fails when using sushy-tools	15
1.2.5.5. Provisioning a bare metal cluster on OpenShift Container Platform 4.10 fails on a dual stack hub	16
1.2.5.6. Deleting a managed cluster set does not automatically remove its label	16
1.2.5.7. ClusterClaim error	16
1.2.5.8. The product channel out of sync with provisioned cluster	16
1.2.5.9. Restoring the connection of a managed cluster with custom CA certificates to its restored hub cluster might fail	16
1.2.5.10. The local-cluster might not be automatically recreated	17
1.2.5.11. Selecting a subnet is required when creating an on-premises cluster	17
1.2.5.12. Cluster provisioning on Google Cloud Platform fails	17
1.2.5.13. Cluster provisioning with Infrastructure Operator fails	17

1.2.5.14. Cannot hibernate an Azure Government cluster	18
1.2.5.15. Local-cluster status offline after reimporting with a different name	18
1.2.5.16. Cluster provision with Ansible automation fails in proxy environment	18
1.2.5.17. Version of the klusterlet operator must be the same as the hub cluster	19
1.2.5.18. Cannot delete managed cluster namespace manually	19
1.2.5.19. Cannot change credentials on clusters after upgrading to version 2.3	19
1.2.5.20. Hub cluster and managed clusters clock not synced	19
1.2.5.21. Importing certain versions of IBM OpenShift Container Platform Kubernetes Service clusters is not supported	19
1.2.5.22. Detaching OpenShift Container Platform 3.11 does not remove the open-cluster-management-agent	19
1.2.5.23. Automatic secret updates for provisioned clusters is not supported	19
1.2.5.24. Node information from the managed cluster cannot be viewed in search	20
1.2.5.25. Process to destroy a cluster does not complete	20
1.2.5.26. Cannot upgrade OpenShift Container Platform managed clusters on OpenShift Container Platform Dedicated with the console	21
1.2.5.27. Work manager add-on search details	21
1.2.5.28. Cannot use Ansible Tower integration with an IBM Power or IBM Z system hub cluster	21
1.2.5.29. Non-Red Hat OpenShift Container Platform managed clusters must have LoadBalancer enabled	21
1.2.5.30. Cluster-proxy-addon does not start after upgrade	21
1.2.6. Application management known issues	22
1.2.6.1. Application ObjectBucket channel type cannot use allow and deny lists	22
1.2.6.2. Argo Application cannot be deployed on 3.x OpenShift Container Platform managed clusters	22
1.2.6.3. Changes to the multicluster_operators_subscription image do not take effect automatically	22
1.2.6.4. Application topology displays wrong application	22
1.2.6.5. Policy resource not deployed unless by subscription administrator	22
1.2.6.6. Application Ansible hook stand-alone mode	23
1.2.6.7. Edit role for application error	24
1.2.6.8. Edit role for placement rule error	24
1.2.6.9. Application not deployed after an updated placement rule	24
1.2.6.10. Subscription operator does not create an SCC	24
1.2.6.11. Application channels require unique namespaces	25
1.2.6.12. Ansible Automation Platform job fail	25
1.2.6.13. Ansible Automation Platform operator access Ansible Tower outside of a proxy	25
1.2.6.14. Template information does not show when editing a Helm Argo application in version 2.4	26
1.2.6.15. Application name requirements	26
1.2.6.16. Application console table limitations	26
1.2.6.17. No Application console topology filtering	26
1.2.6.18. ApplicationSet resources do not show status in topology	26
1.2.6.19. Allow and deny list does not work in Object storage applications	26
1.2.6.20. ApplicationSet wizard does not fetch path automatically	26
1.2.7. Governance known issues	27
1.2.7.1. Unable to log out from Red Hat Advanced Cluster Management	27
1.2.7.2. Gatekeeper operator installation fails	27
1.2.7.3. Configuration policy listed complaint when namespace is stuck in Terminating state	27
1.2.7.4. Operators deployed with policies do not support ARM	27
1.2.7.5. Policy template issues	27
1.2.8. Backup and restore known issues	27
1.2.8.1. Backup and restore feature does not work on IBM Power and IBM Z	28
1.2.8.2. Avoid backup collision	28
1.2.8.3. Velero restore limitations	28
1.2.8.4. Imported managed clusters are not displayed	29

1.2.8.5. Cluster backup and restore upgrade limitation	29
1.2.8.6. Managed cluster resource not restored	29
1.2.8.7. prepareForBackup is only called when Velero schedules are first created	30
1.2.8.8. Restored Hive managed clusters might not be able to connect with the new hub cluster	30
1.2.9. Submariner known issues	30
1.2.9.1. Submariner currently only supports OpenShift SDN as a CNI network provider	30
1.2.9.2. Submariner does not support some Red Hat Enterprise Linux nodes as worker nodes	30
1.2.9.3. Submariner does not support all infrastructure providers that Red Hat Advanced Cluster Management can manage	30
1.2.9.4. Submariner does not support preparing the Red Hat OpenStack Platform infrastructure from the Red Hat Advanced Cluster Management console	31
1.2.9.5. Submariner does not support headless services with Globalnet	31
1.2.9.6. Submariner does not support air-gapped clusters	31
1.2.9.7. Numerous gateways cannot be deployed	31
1.2.9.8. Submariner does not support VXLAN when NAT is enabled	31
1.2.9.9. Globalnet limitations	31
1.3. ERRATA UPDATES	31
1.3.1. Errata 2.5.9	31
1.3.2. Errata 2.5.8	32
1.3.3. Errata 2.5.7	32
1.3.4. Errata 2.5.6	32
1.3.5. Errata 2.5.5	32
1.3.6. Errata 2.5.4	32
1.3.7. Errata 2.5.3	32
1.3.8. Errata 2.5.2	32
1.3.9. Errata 2.5.1	33
1.4. DEPRECATIONS AND REMOVALS	33
1.4.1. API deprecations and removals	34
1.4.1.1. API deprecations	34
1.4.2. Red Hat Advanced Cluster Management deprecations	36
1.4.3. Removals	37
1.5. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES PLATFORM CONSIDERATIONS FOR GDPR READINESS	38
1.5.1. Notice	38
1.5.2. Table of Contents	39
1.5.3. GDPR	39
1.5.3.1. Why is GDPR important?	39
1.5.3.2. Read more about GDPR	39
1.5.4. Product Configuration for GDPR	39
1.5.5. Data Life Cycle	39
1.5.5.1. What types of data flow through Red Hat Advanced Cluster Management for Kubernetes platform	40
1.5.5.2. Personal data used for online contact	40
1.5.6. Data Collection	40
1.5.7. Data storage	41
1.5.8. Data access	42
1.5.8.1. Authentication	42
1.5.8.2. Role Mapping	42
1.5.8.3. Authorization	43
1.5.8.4. Pod Security	43
1.5.9. Data Processing	43
1.5.10. Data Deletion	43
1.5.11. Capability for Restricting Use of Personal Data	44

1.5.12. Appendix	44
1.6. FIPS READINESS	44
1.6.1. Limitations	45

CHAPTER 1. RELEASE NOTES

Important: The 2.5 and earlier versions of Red Hat Advanced Cluster Management are removed and no longer supported. Documentation for versions 2.5 and earlier are not updated. The documentation might remain available, but is deprecated without any Errata or other updates available.

Best practice: Upgrade to the most recent version of Red Hat Advanced Cluster Management.

- [What's new in Red Hat Advanced Cluster Management for Kubernetes](#)
- [Errata updates](#)
- [Known issues and limitations](#)
- [Deprecations and removals](#)
- [Red Hat Advanced Cluster Management for Kubernetes considerations for GDPR readiness](#)
- [FIPS readiness](#)

1.1. WHAT'S NEW IN RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES

Red Hat Advanced Cluster Management for Kubernetes provides visibility of your entire Kubernetes domain with built-in governance, cluster lifecycle management, and application lifecycle management, along with observability. With this release, you can move towards managing clusters in more environments, GitOps integration for applications, and more.

Important: Some features and components are identified and released as [Technology Preview](#).

Learn more about what is new this release:

- Get an overview of Red Hat Advanced Cluster Management for Kubernetes from [Welcome to Red Hat Advanced Cluster Management for Kubernetes](#).
- The open source *Open Cluster Management* repository is ready for interaction, growth, and contributions from the open community. To get involved, see [open-cluster-management.io](#). You can access the [GitHub repository](#) for more information, as well.
- See the [Multicluster architecture](#) topic to learn more about major components of the product.
- The [Getting started](#) guide references common tasks that get you started, as well as the *Troubleshooting guide*.
- [Web console](#)
 - [Observability](#)
- [Clusters](#)
- [Applications](#)
- [Governance](#)

1.1.1. Web console

- The console side-bar navigation aligns with other products and offers a better user experience. From the navigation, you can access various product features. Additionally, *Search* is available in the navigation from the *Home* tab and no longer from the header.
- With the [Red Hat OpenShift Container Platform 4.10 release](#) and a more hybrid console, you can use dynamic plug-ins. See the OpenShift Container Platform documentation about [Adding a dynamic plug-in to the OpenShift Container Platform web console](#) to create and deploy a dynamic plug-in on your cluster that is loaded at run-time.
- **Note:** Without plug-ins enabled on OpenShift Container Platform versions 4.8 through 4.10, Red Hat Advanced Cluster Management is available in the *Perspective switcher*. To learn about the Red Hat Advanced Cluster Management console, see [Console overview](#).
- The Red Hat Advanced Cluster Management plug-in is generally available for enablement from the OpenShift Container Platform console. Learn how to enable it in the [Console overview](#).

1.1.1.1. Observability

- Red Hat Advanced Cluster Management supports OpenShift Container Platform version 3.11 Grafana dashboards. See the [Creating the MultiClusterObservability CR](#) section in *Enabling observability* for more details.
- Customize certificates for accessing the object store that you use for the observability service. For more details, see [Customizing certificates for accessing the object store](#).
- Configure the observability service with Security Service Token credentials. For more information about what to configure, see [Observability API](#).
- Using the observability service, you can export metrics to external endpoints. For more details, see [Export metrics to external endpoints](#).
- Dynamic metric collection for single node OpenShift (SNO) clusters is supported. For more information, see [Dynamic metrics for single-node OpenShift clusters](#).

1.1.2. Clusters

- Some features of integrating Submariner multicluster networking service through Red Hat Advanced Cluster Management are generally available. See [Submariner multicluster networking and service discovery](#) for more information.
- Enable the Globalnet controller to resolve overlapping CIDRs when you enable the Submariner add-on. See [Globalnet](#) for more information.
- Host a hub cluster, as well as import and manage clusters on the Advanced RISC Machines (ARM) architecture.
- Central Infrastructure Management now supports Metal3 on the following platforms: bare metal, Red Hat OpenStack Platform, VMware vSphere environments, or when it was installed using the user-provisioned infrastructure (UPI) method and the platform is **None**.
- You can discover and add hosts to your infrastructure environment during the cluster creation process. See [Creating a cluster in an on-premises environment](#) for more information.
- Use **ManagedClusterSet**, which is now generally available, to manage access to all of the managed clusters in the group together. **ManagedClusterSet** creates a **default** managed cluster set for any managed clusters that are not specifically assigned to a set. See [Creating and](#)

[managing ManagedClusterSets](#) for more information.

- Specify a number of clusters in a cluster pool that are immediately available to claim. See [Scaling cluster pools](#) for more information.
- Use Red Hat Advanced Cluster Management to create an OpenShift Container Platform cluster on Red Hat Virtualization. See [Creating a cluster on Red Hat Virtualization](#) for more information.
- Control the placements of your managed clusters and managed cluster sets using taints and tolerations. See [Using taints and tolerations to place managed clusters](#) for more information.
- Use extensible scheduling to control the placement of your clusters. See [Extensible scheduling](#) for more information.
- Learn to recover the backup and restore component by using the **backup-restore-enabled** policy. See [Backup validation using a policy](#) for more information.
- Use Red Hat Advanced Cluster Management discovery to find OpenShift 4 clusters that are available from [OpenShift Cluster Manager](#). Discovery is generally available, and the API is updated from **v1alpha1** to **v1**.
 - After discovery, you can import your clusters to manage. The Discovery service uses the Discover Operator for back-end and console usage. See [Discovery service introduction](#).
- You can now specify properties for a disconnected cluster in the credential when you use the Red Hat Advanced Cluster Management console to create a cluster for VMware vSphere or Red Hat OpenStack Platform. See [Creating a credential for VMware vSphere](#) and [Creating a credential for Red Hat OpenStack](#) for more information.

Specify properties for a proxy connection in the credential. See the credential topic for your infrastructure provider in [Managing credentials overview](#) for more information.

- The *multicluster engine operator* is generally available as a software operator that enhances cluster fleet management. The multicluster engine operator supports Red Hat OpenShift Container Platform and Kubernetes cluster lifecycle management across clouds and data centers. Red Hat OpenShift Container Platform is a prerequisite for the multicluster engine operator.

Technology Preview:

See the following cluster features that are available as Technology Preview:

- The **Managed-ServiceAccount** component allows you to create and delete a Service Account on a managed cluster. The component is disabled by default.
 - See the *multicluster engine operator* documentation at [Enabling ManagedServiceAccount add-ons \(Technology Preview\)](#) to learn more.
 - See the Red Hat Advanced Cluster Management documentation at [MultiClusterHub advanced configuration](#) to learn more.
- The **hypershift** add-on helps you host OpenShift Container Platform control planes at scale, separating management from workloads. The component is disabled by default.
 - See the *multicluster engine operator* documentation at [Hypershift add-on \(Technology Preview\)](#) to learn more.

- See the Red Hat Advanced Cluster Management documentation at [Hypershift add-on \(Technology Preview\)](#) and [Using hosted control plane clusters \(Technology Preview\)](#) to learn more.
- Use HyperShift to manage and provision hosted control plane clusters. See [Using hosted control plane clusters \(Technology Preview\)](#) for more information.

For other Clusters topics, see [Managing your clusters](#).

1.1.3. Applications

- The Placement and Placement decisions API is upgraded from **v1alpha1** to **v1beta1**. Placements define the target clusters that must subscribe to a **ClusterSet** where subscriptions and application sets are delivered. View these in the console from **Advanced configuration**.
- Access Topology from an individual tab in the single application overview so that you can view everything at the same time. Learn about the Topology from **How to read topology** to learn about each topology element.
- **ApplicationSet** is now generally available as a sub-project of Argo CD that adds multicluster support for Argo CD applications. You can create an **ApplicationSet** from the product console editor. See [Application model and definitions](#).
- Statuses on managed clusters and **subscriptionReports** on the hub cluster are lightweight and more scalable. See the following three types of subscription status reports:
 - Package-level **SubscriptionStatus**: This is the application package status on the managed cluster with detailed status for all of the resources that are deployed by the application in the **appsub** namespace.
 - Cluster-level **SubscriptionReport**: This is the overall status report on all of the applications that are deployed to a particular cluster.
 - Application-level **SubscriptionReport**: This is the overall status report on all of the managed clusters to which a particular application is deployed. See [Subscription reports](#) for information.

For other Application topics, see [Managing applications](#).

1.1.4. Governance

- Use the optional YAML field, **metadataComplianceType**, to process labels and annotations of an object differently than the other fields. For more information, see the [Policy API](#).
- Create a policy set to group policies together. See [Policy set controller](#).
- Policy set generation is now supported for the policy generator. See [Policy generator](#).
- You can use the **protect** function to secure sensitive data that is on your hub cluster policy template. Also, the **fromSecret** function is now available in the hub cluster policy templates. See [protect function](#) section for more information

See [Governance](#) to learn more about the dashboard and the policy framework.

1.1.5. Add-ons

- Deploy Submariner on Red Hat OpenStack Platform clusters. See [Preparing Red Hat OpenStack Platform for Submariner](#) for more information.

To see more release note topics, go to the [Release notes](#).

1.2. KNOWN ISSUES

Review the known issues for Red Hat Advanced Cluster Management for Kubernetes. The following list contains known issues for this release, or known issues that continued from the previous release. For your Red Hat OpenShift Container Platform cluster, see [OpenShift Container Platform known issues](#).

- [Documentation known issues](#)
- [Installation known issues](#)
- [Web console known issues](#)
 - [Observability known issues](#)
- [Cluster management known issues](#)
- [Application management known issues](#)
- [Governance known issues](#)
- [Backup and restore known issues](#)
- [Submariner known issues](#)

1.2.1. Documentation known issues

1.2.1.1. Documentation links in the Customer Portal might link to a higher-level section

In some cases, the internal links to other sections of the Red Hat Advanced Cluster Management documentation in the Customer Portal do not link directly to the named section. In some instances, the links resolve to the highest-level section.

If this happens, you can either find the specified section manually or complete the following steps to resolve:

1. Copy the link that is not resolving to the correct section and paste it in your browser address bar. For example, it might be: https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.5/html/clusters/index#volsync.
2. In the link, replace **html** with **html-single**. The new URL should read: https://access.redhat.com/documentation/en-us/red_hat_advanced_cluster_management_for_kubernetes/2.5/html-single/clusters/index#volsync
3. Link to the new URL to find the specified section in the documentation.

1.2.2. Installation known issues

1.2.2.1. Pods might not come back up after upgrading Red Hat Advanced Cluster Management

After upgrading Red Hat Advanced Cluster Management to a new version, a few pods that belong to a **StatefulSet** might remain in a **failed** state. This infrequent event is caused by a known [Kubernetes issue](#).

As a workaround for this problem, delete the failed pod. Kubernetes automatically relaunches it with the correct settings.

1.2.2.2. OpenShift Container Platform cluster upgrade failed status

When an OpenShift Container Platform cluster is in the upgrade stage, the cluster pods are restarted and the cluster might remain in **upgrade failed** status for a variation of 1-5 minutes. This behavior is expected and resolves after a few minutes.

1.2.2.3. Two cluster curator controllers are running at the same time after upgrade

After you upgrade from 2.4.x to 2.5.0, two cluster curator controllers might run at the same time. Two or more **AnsibleJobs** were created for some of the prehooks and posthooks for the Cluster Lifecycle Ansible integration. See the following procedure to resolve this issue:

1. Check to see if there are two cluster curator controllers running. Run the following commands, which contain the **multicluster-engine** namespace from the multicluster engine operator, as well as the **open-cluster-management** namespace:

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

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

2. If two cluster curator controllers are running, delete the **cluster-curator-controller** in the **open-cluster-management** namespace. Run the following command:

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

1.2.2.4. Create MultiClusterEngine button not working

After installing Red Hat Advanced Cluster Management for Kubernetes in the Red Hat OpenShift Container Platform console, a pop-up window with the following message appears:

MultiClusterEngine required

Create a MultiClusterEngine instance to use this Operator.

The **Create MultiClusterEngine** button in the pop-up window message might not work. To work around the issue, select **Create instance** in the MultiClusterEngine tile in the Provided APIs section.

1.2.3. Web console known issues

1.2.3.1. Dark mode is not supported on Red Hat Advanced Cluster Management version 2.5.x

While Red Hat Advanced Cluster Management version 2.5.2, and later 2.5.x versions are supported on Red Hat OpenShift Container Platform version 4.11, dark mode is not supported on Red Hat Advanced Cluster Management 2.5.x. Either disable dark mode in the settings, or upgrade to Red Hat Advanced

Cluster Management version 2.6 to enable dark mode.

1.2.3.2. Dark mode is not supported on multicluster engine for Kubernetes operator version 2.0.x

While multicluster engine for Kubernetes operator version 2.0.2, and later 2.0.x versions are supported on Red Hat OpenShift Container Platform version 4.11, dark mode is not supported on multicluster engine for Kubernetes operator 2.0.x. Either disable dark mode in the settings, or upgrade to multicluster engine for Kubernetes operator version 2.1 to enable dark mode.

1.2.3.3. LDAP user names are case-sensitive

LDAP user names are case-sensitive. You must use the name exactly the way it is configured in your LDAP directory.

1.2.3.4. Console features might not display in Firefox earlier version

The product supports Mozilla Firefox 74.0 or the latest version that is available for Linux, macOS, and Windows. Upgrade to the latest version for the best console compatibility.

1.2.3.5. Restrictions for storage size in search customization

When you update the storage size in the **searchcustomization** CR, the PVC configuration does not change. If you need to update the storage size, update the PVC (**<storageclassname>-search-redisgraph-0**) with the following command:

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

1.2.3.6. Search query parsing error

If an environment becomes large and requires more tests for scaling, the search queries can timeout which results in an parsing error message being displayed. This error is displayed after 30 seconds of waiting for a search query.

Extend the timeout time with the following command:

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

1.2.3.7. Cannot edit namespace bindings for cluster set

When you edit namespace bindings for a cluster set with the **admin** role, you might encounter an error that resembles the following message:

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>".

To resolve the issue, make sure you also have permission to create or delete a **ManagedClusterSetBinding** resource in the namespace you want to bind. The role bindings only allow you to bind the cluster set to the namespace.

1.2.3.8. False scaling alert in cluster details

When you view cluster details in the console, you might see the following message in the *Nodes* or *Machine pools* tab:

Worker nodes are currently being removed from this cluster. Click the View machines button to see the status of the scaling operations (it may take a few minutes for the changes to be reflected on this console).

If there are no machine pools present, which is the case for providers that use User Provisioned Infrastructure (UPI) installation, ignore the false alert. The alert appears when there are worker nodes that are not part of the control plane. The false alert can also appear for clusters that were provisioned by using Installer Provisioned Infrastructure (IPI) installation if worker nodes are added to the cluster directly instead of by scaling the machine pool.

1.2.4. Observability known issues

1.2.4.1. Duplicate local-clusters on Service-level Overview dashboard

When various hub clusters deploy Red Hat Advanced Cluster Management observability using the same S3 storage, *duplicate local-clusters* can be detected and displayed within the *Kubernetes/Service-Level Overview/API Server* dashboard. The duplicate clusters affect the results within the following panels: *Top Clusters*, *Number of clusters that has exceeded the SLO*, and *Number of clusters that are meeting the SLO*. The **local-clusters** are unique clusters associated with the shared S3 storage. To prevent multiple **local-clusters** from displaying within the dashboard, it is recommended for each unique hub cluster to deploy observability with a S3 bucket specifically for the hub cluster.

1.2.4.2. Observability endpoint operator fails to pull image

The observability endpoint operator fails if you create a pull-secret to deploy to the MultiClusterObservability CustomResource (CR) and there is no pull-secret in the **open-cluster-management-observability** namespace. When you import a new cluster, or import a Hive cluster that is created with Red Hat Advanced Cluster Management, you need to manually create a pull-image secret on the managed cluster.

For more information, see [Enabling observability](#).

1.2.4.3. There is no data from ROKS and HyperShift clusters

Red Hat Advanced Cluster Management observability does not display data from an ROKS cluster and HyperShift cluster on some panels within built-in dashboards. This is because ROKS and HyperShift do not expose any API Server metrics from servers they manage. The following Grafana dashboards contain panels that do not support ROKS and HyperShift clusters: **Kubernetes/API server**, **Kubernetes/Compute Resources/Workload**, **Kubernetes/Compute Resources/Namespaces(Workload)**

1.2.4.4. There is no etcd data from ROKS and HyperShift clusters

For ROKS clusters and HyperShift clusters, Red Hat Advanced Cluster Management observability does not display data in the *etcd* panel of the dashboard.

1.2.4.5. High CPU usage by the search-collector pod

When search is disabled on a hub cluster that manages 1000 clusters, the **search-collector** pod crashes due to the out-of-memory error (OOM). Complete the following steps:

1. If search is disabled on the hub cluster, which means the **search-redisgraph-pod** is not deployed, reduce memory usage by scaling down the **search-collector** deployment to **0** replicas.
2. If search is enabled on the hub cluster, which means the **search-redisgraph-pod** is deployed, increase the allocated memory by editing the **search-collector** deployment.

1.2.4.6. Search pods fail to complete the TLS handshake due to invalid certificates

In some rare cases, the search pods are not automatically redeployed after certificates change. This causes a mismatch of certificates across the service pods, which causes the Transfer Layer Security (TLS) handshake to fail. To fix this problem, restart the search pods to reset the certificates.

1.2.4.7. Metrics are unavailable in the Grafana console

- Annotation query failed in the Grafana console:
When you search for a specific annotation in the Grafana console, you might receive the following error message due to an expired token:

"Annotation Query Failed"

Refresh your browser and verify you are logged into your hub cluster.

- Error in *rbac-query-proxy* pod:
Due to unauthorized access to the **managedcluster** resource, you might receive the following error when you query a cluster or project:

no project or cluster found

Check the role permissions and update appropriately. See [Role-based access control](#) for more information.

1.2.4.8. Prometheus data loss on managed clusters

By default, Prometheus on OpenShift uses ephemeral storage. Prometheus loses all metrics data whenever it is restarted.

When observability is enabled or disabled on OpenShift Container Platform managed clusters that are managed by Red Hat Advanced Cluster Management, the observability endpoint operator updates the **cluster-monitoring-config ConfigMap** by adding additional alertmanager configuration that restarts the local Prometheus automatically.

1.2.4.9. Error ingesting out-of-order samples

Observability **receive** pods report the following error message:

Error on ingesting out-of-order samples

The error message means that the time series data sent by a managed cluster, during a metrics collection interval is older than the time series data it sent in the previous collection interval. When this problem happens, data is discarded by the Thanos receivers and this might create a gap in the data shown in Grafana dashboards. If the error is seen frequently, it is recommended to increase the metrics collection interval to a higher value. For example, you can increase the interval to 60 seconds.

The problem is only noticed when the time series interval is set to a lower value, such as 30 seconds. Note, this problem is not seen when the metrics collection interval is set to the default value of 300 seconds.

1.2.4.10. Grafana deployment fails on managed clusters

The Grafana instance does not deploy to the managed cluster if the size of the manifest exceeds 50 thousand bytes. Only the **local-cluster** appears in Grafana after you deploy observability.

1.2.5. Cluster management known issues

See the following known issues and limitations for cluster management:

1.2.5.1. Disconnected installation settings for cluster creation cannot be entered or are ignored if entered

When you create a cluster by using the bare metal provider and a disconnected installation, you must store all your settings in the credential in the *Configuration for disconnected installation* section. You cannot enter them in the cluster create console editor.

When creating a cluster by using the VMware vSphere or Red Hat OpenStack Platform providers and disconnected installation, if a certificate is required to access the mirror registry, you must enter it in the *Additional trust bundle* field of your credential in the *Configuration for disconnected installation* section. If you enter that certificate in the cluster create console editor, it is ignored.

1.2.5.2. Credential with disconnected installer does not distinguish between the certificates

When creating a credential for the bare metal, VMware vSphere, or Red Hat OpenStack Platform provider, note that the *Additional trust bundle* field in the *Proxy and Configuration for disconnected installation* contains the same value since the installer does not distinguish between the certificates. You can still use these features independently, and you can enter multiple certificates in the field if different certificates are required for proxy and disconnected installation.

1.2.5.3. Manual removal of the VolSync CSV required on managed cluster when removing the add-on

When you remove the VolSync **ManagedClusterAddOn** from the hub cluster, it removes the VolSync operator subscription on the managed cluster but does not remove the cluster service version (CSV). To remove the CSV from the managed clusters, run the following command on each managed cluster from which you are removing VolSync:

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

If you have a different version of VolSync installed, replace **v0.4.0** with your installed version.

1.2.5.4. Provisioning a bare metal managed cluster fails when using sushy-tools

When you provision a managed cluster on bare metal with sushy-tools, the provision might fail with a **virtual media cd query return 500** error. Using sushy-tools is not guaranteed to be reliable for long running clusters.

Ensure that you have the latest version of sushy-tools, and restart the sushy emulator to work around the issue.

1.2.5.5. Provisioning a bare metal cluster on OpenShift Container Platform 4.10 fails on a dual stack hub

When you provision a bare metal cluster on a dual stack hub that is running OpenShift Container Platform version 4.10, the provision fails with the following error message: 'timeout reached while inspecting the node'. To bypass this issue, disable the provisioning network in your **install-config.yaml** file, as shown in the following example:

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

See [Deploying with no provisioning network](#) in the OpenShift Container Platform documentation for more information about the provisioning network.

1.2.5.6. Deleting a managed cluster set does not automatically remove its label

After you delete a **ManagedClusterSet**, the label that is added to each managed cluster that associates the cluster to the cluster set is not automatically removed. Manually remove the label from each of the managed clusters that were included in the deleted managed cluster set. The label resembles the following example: **cluster.open-cluster-management.io/clusterSet:<ManagedClusterSet Name>**.

1.2.5.7. ClusterClaim error

If you create a Hive **ClusterClaim** against a **ClusterPool** and manually set the **ClusterClaimsSpec** lifetime field to an invalid go lang time value, Red Hat Advanced Cluster Management stops fulfilling and reconciling all **ClusterClaims**, not just the malformed claim.

If this error occurs, you see the following content in the **clusterclaim-controller** pod logs, which is a specific example with the pool name and invalid lifetime included:

```
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":"C|...
```

You can delete the invalid claim.

If the malformed claim is deleted, claims begin successfully reconciling again without any further interaction.

1.2.5.8. The product channel out of sync with provisioned cluster

The **clusterimageset** is in **fast** channel, but the provisioned cluster is in **stable** channel. Currently the product does not sync the **channel** to the provisioned OpenShift Container Platform cluster.

Change to the right channel in the OpenShift Container Platform console. Click **Administration** > **Cluster Settings** > **Details Channel**.

1.2.5.9. Restoring the connection of a managed cluster with custom CA certificates to its restored hub cluster might fail

After you restore the backup of a hub cluster that managed a cluster with custom CA certificates, the connection between the managed cluster and the hub cluster might fail. This is because the CA certificate was not backed up on the restored hub cluster. To restore the connection, copy the custom CA certificate information that is in the namespace of your managed cluster to the **<managed_cluster>-admin-kubeconfig** secret on the restored hub cluster.

Tip: If you copy this CA certificate to the hub cluster before creating the backup copy, the backup copy includes the secret information. When the backup copy is used to restore in the future, the connection between the hub and managed clusters will automatically complete.

1.2.5.10. The local-cluster might not be automatically recreated

If the local-cluster is deleted while **disableHubSelfManagement** is set to **false**, the local-cluster is recreated by the **MulticlusterHub** operator. After you detach a local-cluster, the local-cluster might not be automatically recreated.

- To resolve this issue, modify a resource that is watched by the **MulticlusterHub** operator. See the following example:

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

- To properly detach the local-cluster, set the **disableHubSelfManagement** to true in the **MultiClusterHub**.

1.2.5.11. Selecting a subnet is required when creating an on-premises cluster

When you create an on-premises cluster using the Red Hat Advanced Cluster Management console, you must select an available subnet for your cluster. It is not marked as a required field.

1.2.5.12. Cluster provisioning on Google Cloud Platform fails

When you try to provision a cluster on Google Cloud Platform (GCP), it might fail with the following error:

```
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
```

You can work around this error by enabling the [Network Security API](#) on the GCP project, which allows your cluster installation to continue.

1.2.5.13. Cluster provisioning with Infrastructure Operator fails

When creating OpenShift Container Platform clusters using the Infrastructure Operator, the file name of the ISO image might be too long. The long image name causes the image provisioning and the cluster provisioning to fail. To determine if this is the problem, complete the following steps:

1. View the bare metal host information for the cluster that you are provisioning by running the following command:

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

2. Run the **describe** command to view the error information:

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

3. An error similar to the following example indicates that the length of the filename is the problem:

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

If this problem occurs, it is typically on the following versions of OpenShift Container Platform, because the infrastructure operator was not using image service:

- 4.8.17 and earlier
- 4.9.6 and earlier

To avoid this error, upgrade your OpenShift Container Platform to version 4.8.18 or later, or 4.9.7 or later.

1.2.5.14. Cannot hibernate an Azure Government cluster

When you try to hibernate an Azure Government cluster, the hibernation fails with the following error that is added to the provision pod log:

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

1.2.5.15. Local-cluster status offline after reimporting with a different name

When you accidentally try to reimport the cluster named **local-cluster** as a cluster with a different name, the status for **local-cluster** and for the reimported cluster display **offline**.

To recover from this case, complete the following steps:

1. Run the following command on the hub cluster to edit the setting for self-management of the hub cluster temporarily:

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

2. Add the setting **spec.disableSelfManagement=true**.
3. Run the following command on the hub cluster to delete and redeploy the local-cluster:

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

4. Enter the following command to remove the **local-cluster** management setting:

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

5. Remove **spec.disableSelfManagement=true** that you previously added.

1.2.5.16. Cluster provision with Ansible automation fails in proxy environment

An AnsibleJob template that is configured to automatically provision a managed cluster might fail when both of the following conditions are met:

- The hub cluster has cluster-wide proxy enabled.
- The Ansible Tower can only be reached through the proxy.

1.2.5.17. Version of the klusterlet operator must be the same as the hub cluster

If you import a managed cluster by installing the klusterlet operator, the version of the klusterlet operator must be the same as the version of the hub cluster or the klusterlet operator will not work.

1.2.5.18. Cannot delete managed cluster namespace manually

You cannot delete the namespace of a managed cluster manually. The managed cluster namespace is automatically deleted after the managed cluster is detached. If you delete the managed cluster namespace manually before the managed cluster is detached, the managed cluster shows a continuous terminating status after you delete the managed cluster. To delete this terminating managed cluster, manually remove the finalizers from the managed cluster that you detached.

1.2.5.19. Cannot change credentials on clusters after upgrading to version 2.3

After you upgrade Red Hat Advanced Cluster Management to version 2.3, you cannot change the credential secret for any of the managed clusters that were created and managed by Red Hat Advanced Cluster Management before the upgrade.

1.2.5.20. Hub cluster and managed clusters clock not synced

Hub cluster and managed cluster time might become out-of-sync, displaying in the console **unknown** and eventually **available** within a few minutes. Ensure that the Red Hat OpenShift Container Platform hub cluster time is configured correctly. See [Customizing nodes](#).

1.2.5.21. Importing certain versions of IBM OpenShift Container Platform Kubernetes Service clusters is not supported

You cannot import IBM OpenShift Container Platform Kubernetes Service version 3.11 clusters. Later versions of IBM OpenShift Kubernetes Service are supported.

1.2.5.22. Detaching OpenShift Container Platform 3.11 does not remove the *open-cluster-management-agent*

When you detach managed clusters on OpenShift Container Platform 3.11, the **open-cluster-management-agent** namespace is not automatically deleted. Manually remove the namespace by running the following command:

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

1.2.5.23. Automatic secret updates for provisioned clusters is not supported

When you change your cloud provider access key, the provisioned cluster access key is not updated in the namespace. This is required when your credentials expire on the cloud provider where the managed cluster is hosted and you try delete the managed cluster. If something like this occurs, run the following command for your cloud provider to update the access key:

- 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)

You can identify this issue by a repeating log error message that reads, **Invalid JWT Signature** when you attempt to destroy the cluster. If your log contains this message, obtain a new Google Cloud Provider service account JSON key and enter the following command:

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

Replace **CLUSTER-NAME** with the name of your cluster.

Replace the path to the file **\$HOME/.gcp/osServiceAccount.json** with the path to the file that contains your new Google Cloud Provider service account JSON key.

- 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. Node information from the managed cluster cannot be viewed in search

Search maps RBAC for resources in the hub cluster. Depending on user RBAC settings for Red Hat Advanced Cluster Management, users might not see node data from the managed cluster. Results from search might be different from what is displayed on the *Nodes* page for a cluster.

1.2.5.25. Process to destroy a cluster does not complete

When you destroy a managed cluster, the status continues to display **Destroying** after one hour, and the cluster is not destroyed. To resolve this issue complete the following steps:

1. Manually ensure that there are no orphaned resources on your cloud, and that all of the provider resources that are associated with the managed cluster are cleaned up.
2. Open the **ClusterDeployment** information for the managed cluster that is being removed by entering the following command:

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

Replace **mycluster** with the name of the managed cluster that you are destroying.

Replace **namespace** with the namespace of the managed cluster.

3. Remove the **hive.openshift.io/deprovision** finalizer to forcefully stop the process that is trying to clean up the cluster resources in the cloud.
4. Save your changes and verify that **ClusterDeployment** is gone.
5. Manually remove the namespace of the managed cluster by running the following command:

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

Replace **namespace** with the namespace of the managed cluster.

1.2.5.26. Cannot upgrade OpenShift Container Platform managed clusters on OpenShift Container Platform Dedicated with the console

You cannot use the Red Hat Advanced Cluster Management console to upgrade OpenShift Container Platform managed clusters that are in the OpenShift Container Platform Dedicated environment.

1.2.5.27. Work manager add-on search details

The search details page for a certain resource on a certain managed cluster might fail. You must ensure that the work-manager add-on in the managed cluster is in **Available** status before you can search.

1.2.5.28. Cannot use Ansible Tower integration with an IBM Power or IBM Z system hub cluster

You cannot use the Ansible Tower integration when the Red Hat Advanced Cluster Management for Kubernetes hub cluster is running on IBM Power or IBM Z systems because the [Ansible Automation Platform Resource Operator](#) does not provide **ppc64le** or **s390x** images.

1.2.5.29. Non-Red Hat OpenShift Container Platform managed clusters must have LoadBalancer enabled

Both Red Hat OpenShift Container Platform and non-OpenShift Container Platform clusters support the pod log feature, however non-OpenShift Container Platform clusters require **LoadBalancer** to be enabled to use the feature. Complete the following steps to enable **LoadBalancer**:

1. Cloud providers have different **LoadBalancer** configurations. Visit your cloud provider documentation for more information.
2. Verify if **LoadBalancer** is enabled on your Red Hat Advanced Cluster Management by checking the **loggingEndpoint** in the status of **managedClusterInfo**.
3. Run the following command to check if the **loggingEndpoint.IP** or **loggingEndpoint.Host** has a valid IP address or host name:

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

For more information about the **LoadBalancer** types, see the [Service](#) page in the [Kubernetes documentation](#).

1.2.5.30. Cluster-proxy-addon does not start after upgrade

After you upgrade from version 2.4.x to 2.5.0, **cluster-proxy-addon** does not start and **cluster-proxy-addon-manager** raises a nil pointer exception.

To work around this issue, complete the following steps:

1. Disable **cluster-proxy-addon**. See [Advanced configuration](#) to learn more.
2. Delete the **cluster-proxy-signer** secret from the **open-cluster-management** namespace.
3. Enable **cluster-proxy-addon**.

1.2.6. Application management known issues

See the following known issues for the application lifecycle component.

1.2.6.1. Application ObjectBucket channel type cannot use allow and deny lists

You cannot specify allow and deny lists with ObjectBucket channel type in the **subscription-admin** role. In other channel types, the allow and deny lists in the subscription indicates which Kubernetes resources can be deployed, and which Kubernetes resources should not be deployed.

1.2.6.2. Argo Application cannot be deployed on 3.x OpenShift Container Platform managed clusters

Argo **ApplicationSet** from the console cannot be deployed on 3.x OpenShift Container Platform managed clusters because the **Infrastructure.config.openshift.io** API is not available on on 3.x.

1.2.6.3. Changes to the multicluster_operators_subscription image do not take effect automatically

The **application-manager** add-on that is running on the managed clusters is now handled by the subscription operator, when it was previously handled by the klusterlet operator. The subscription operator is not managed the **multicluster-hub**, so changes to the **multicluster_operators_subscription** image in the **multicluster-hub** image manifest ConfigMap do not take effect automatically.

If the image that is used by the subscription operator is overridden by changing the **multicluster_operators_subscription** image in the **multicluster-hub** image manifest ConfigMap, the **application-manager** add-on on the managed clusters does not use the new image until the subscription operator pod is restarted. You need to restart the pod.

1.2.6.4. Application topology displays wrong application

The Application topology displays the wrong application if **ApplicationSets** with the same name are created in different Gitops instances. If you have multiple Gitops instances installed, you will have **ApplicationSets** with the same name in each Gitops instance and the topology for the **ApplicationSets** will not display correctly. This is due to the topology not differentiating the namespace for the **ApplicationSets** that are created.

Be sure to create **ApplicationSets** with different names in each of the Gitops instances to display the topology correctly.

1.2.6.5. Policy resource not deployed unless by subscription administrator

The **policy.open-cluster-management.io/v1** resources are no longer deployed by an application subscription by default for Red Hat Advanced Cluster Management version 2.4.

A subscription administrator needs to deploy the application subscription to change this default behavior.

See [Creating an allow and deny list as subscription administrator](#) for information. **policy.open-cluster-management.io/v1** resources that were deployed by existing application subscriptions in previous Red Hat Advanced Cluster Management versions remain, but are no longer reconciled with the source repository unless the application subscriptions are deployed by a subscription administrator.

1.2.6.6. Application Ansible hook stand-alone mode

Ansible hook stand-alone mode is not supported. To deploy Ansible hook on the hub cluster with a subscription, you might use the following subscription 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
```

However, this configuration might never create the Ansible instance, since the **spec.placement.local:true** has the subscription running on **standalone** mode. You need to create the subscription in hub mode.

1. Create a placement rule that deploys to **local-cluster**. See the following sample:

```
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. Reference that placement rule in your subscription. See the following:

```
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

```

After applying both, you should see the Ansible instance created in your hub cluster.

1.2.6.7. Edit role for application error

A user performing in an **Editor** role should only have **read** or **update** authority on an application, but erroneously editor can also **create** and **delete** an application. OpenShift Container Platform Operator Lifecycle Manager default settings change the setting for the product. To workaround the issue, see the following procedure:

1. Run **oc edit clusterrole applications.app.k8s.io-v1beta2-edit -o yaml** to open the application edit cluster role.
2. Remove **create** and **delete** from the verbs list.
3. Save the change.

1.2.6.8. Edit role for placement rule error

A user performing in an **Editor** role should only have **read** or **update** authority on an placement rule, but erroneously editor can also **create** and **delete**, as well. OpenShift Container Platform Operator Lifecycle Manager default settings change the setting for the product. To workaround the issue, see the following procedure:

1. Run **oc edit clusterrole placementrules.apps.open-cluster-management.io-v1-edit** to open the application edit cluster role.
2. Remove **create** and **delete** from the verbs list.
3. Save the change.

1.2.6.9. Application not deployed after an updated placement rule

If applications are not deploying after an update to a placement rule, verify that the **klusterlet-addon-appmgr** pod is running. The **klusterlet-addon-appmgr** is the subscription container that needs to run on endpoint clusters.

You can run **oc get pods -n open-cluster-management-agent-addon** to verify.

You can also search for **kind:pod cluster:yourcluster** in the console and see if the **klusterlet-addon-appmgr** is running.

If you cannot verify, attempt to import the cluster again and verify again.

1.2.6.10. Subscription operator does not create an SCC

Learn about Red Hat OpenShift Container Platform SCC at [Managing Security Context Constraints \(SCC\)](#), which is an additional configuration required on the managed cluster.

Different deployments have different security context and different service accounts. The subscription operator cannot create an SCC automatically. Administrators control permissions for pods. A Security Context Constraints (SCC) CR is required to enable appropriate permissions for the relative service accounts to create pods in the non-default namespace:

To manually create an SCC CR in your namespace, complete the following:

1. Find the service account that is defined in the deployments. For example, see the following **nginx** deployments:

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

2. Create an SCC CR in your namespace to assign the required permissions to the service account or accounts. See the following example where **kind: SecurityContextConstraints** is added:

```
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. Application channels require unique namespaces

Creating more than one channel in the same namespace can cause errors with the hub cluster.

For instance, namespace **charts-v1** is used by the installer as a Helm type channel, so do not create any additional channels in **charts-v1**. Ensure that you create your channel in a unique namespace. All channels need an individual namespace, except GitHub channels, which can share a namespace with another GitHub channel.

1.2.6.12. Ansible Automation Platform job fail

Ansible jobs fail to run when you select an incompatible option. Ansible Automation Platform only works when the **-cluster-scoped** channel options are chosen. This affects all components that need to perform Ansible jobs.

1.2.6.13. Ansible Automation Platform operator access Ansible Tower outside of a proxy

The Ansible Automation Platform (AAP) operator cannot access Ansible Tower outside of a proxy-enabled OpenShift Container Platform cluster. To resolve, you can install the Ansible tower within the proxy. See install steps that are provided by Ansible Tower.

1.2.6.14. Template information does not show when editing a Helm Argo application in version 2.4

When a Helm Argo application is created and then edited, the template information appears empty while the YAML file is correct. Upgrade to Errata 2.4.1 to fix the error.

1.2.6.15. Application name requirements

An application name cannot exceed 37 characters. The application deployment displays the following error if the characters exceed this amount.

```
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. Application console table limitations

See the following limitations to various *Application* tables in the console:

- From the *Applications* table on the *Overview* page and the *Subscriptions* table on the *Advanced configuration* page, the *Clusters* column displays a count of clusters where application resources are deployed. Since applications are defined by resources on the local cluster, the local cluster is included in the search results, whether actual application resources are deployed on the local cluster or not.
- From the *Advanced configuration* table for *Subscriptions*, the *Applications* column displays the total number of applications that use that subscription, but if the subscription deploys child applications, those are included in the search result, as well.
- From the *Advanced configuration* table for *Channels*, the *Subscriptions* column displays the total number of subscriptions on the local cluster that use that channel, but this does not include subscriptions that are deployed by other subscriptions, which are included in the search result.

1.2.6.17. No Application console topology filtering

The *Console* and *Topology* for *Application* changes for the 2.5. There is no filtering capability from the console Topology page.

1.2.6.18. ApplicationSet resources do not show status in topology

When you create **ApplicationSet** applications that deploy resources to a different namespace than the namespace defined in the **ApplicationSet** YAML, the resource status does not appear in the topology.

1.2.6.19. Allow and deny list does not work in Object storage applications

The **allow** and **deny** list feature does not work in Object storage application subscriptions.

1.2.6.20. ApplicationSet wizard does not fetch path automatically

After creating a new **ApplicationSet** with the same URL and branch as a previously created **ApplicationSet**, the ApplicationSet wizard does not fetch the path automatically.

To work around the issue, enter the path manually in the **Path** field.

1.2.7. Governance known issues

1.2.7.1. Unable to log out from Red Hat Advanced Cluster Management

When you use an external identity provider to log in to Red Hat Advanced Cluster Management, you might not be able to log out of Red Hat Advanced Cluster Management. This occurs when you use Red Hat Advanced Cluster Management, installed with IBM Cloud and Keycloak as the identity providers.

You must log out of the external identity provider before you attempt to log out of Red Hat Advanced Cluster Management.

1.2.7.2. Gatekeeper operator installation fails

When you install the gatekeeper operator on Red Hat OpenShift Container Platform version 4.9, the installation fails. Before you upgrade OpenShift Container Platform to version 4.9.0., you must upgrade the gatekeeper operator to version 0.2.0. See [Upgrading gatekeeper and the gatekeeper operator](#) for more information.

1.2.7.3. Configuration policy listed complaint when namespace is stuck in *Terminating* state

When you have a configuration policy that is configured with **mustnohave** for the **complianceType** parameter and **enforce** for the **remediationAction** parameter, the policy is listed as compliant after a deletion request is made to the Kubernetes API. Therefore, the Kubernetes object can be stuck in a **Terminating** state while the policy is listed as compliant.

1.2.7.4. Operators deployed with policies do not support ARM

While installation into an ARM environment is supported, operators that are deployed with policies might not support ARM environments. The following policies that install operators do not support ARM environments:

- [Red Hat Advanced Cluster Management policy for the Quay Container Security Operator](#)
- [Red Hat Advanced Cluster Management policy for the Compliance Operator](#)

1.2.7.5. Policy template issues

You might encounter the following issues when you edit policy templates for configuration policies:

- When you rename your configuration policy to a new name, a copy of the configuration policy with the older name remains.
- If you remove a configuration policy from a policy on your hub cluster, the configuration policy remains on your managed cluster but its status is not provided. To resolve this, disable your policy and reenact it. You can also delete the entire policy.

1.2.8. Backup and restore known issues

1.2.8.1. Backup and restore feature does not work on IBM Power and IBM Z

The backup and restore feature for the hub cluster requires the OpenShift API for Data Protection (OADP) operator. The OADP operator is not available on the IBM Power or IBM Z architectures.

1.2.8.2. Avoid backup collision

As hub clusters change from passive to primary clusters and back, different clusters can backup data at the same storage location. This can result in backup collisions, which means that the latest backups are generated by a passive hub cluster.

The passive hub cluster produces backups because the **BackupSchedule.cluster.open-cluster-management.io** resource is enabled on the hub cluster, but it should no longer write backup data since the hub cluster is no longer a primary hub cluster. Run the following command to check if there is a backup collision:

```
oc get backupschedule -A
```

You might receive the following status:

```

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.
```

Avoid backup collisions by setting the **BackupSchedule.cluster.open-cluster-management.io** resource **status** to **BackupCollision**. The **Schedule.velero.io** resources that are created by the **BackupSchedule** resource are automatically deleted.

The backup collision is reported by the **hub-backup-pod** policy. The administrator must verify which hub cluster writes data to the storage location. Then remove the **BackupSchedule.cluster.open-cluster-management.io** resource from the passive hub cluster, and recreate a new **BackupSchedule.cluster.open-cluster-management.io** resource on the primary hub cluster to resume the backup.

See [Cluster backup and restore operator](#) for more information.

1.2.8.3. Velero restore limitations

View the following restore limitations:

- The new hub cluster is not identical to the initial hub cluster, where the data is restored, when there is an existing policy on the new hub cluster before the backup data is restored on the initial hub cluster. The policy should not be running on the new hub cluster since this is a policy that is unavailable with the backup resources.
- Since Velero skips existing resources, the policy on the new hub cluster is unchanged. Therefore, the policy is not the same as the one backed up on the initial hub cluster.
- The new hub cluster has a different configuration from the active hub cluster when a user reapplies the backup on the new hub cluster. Since there is an existing policy on the hub cluster from a previous restore, it is not restored again. Even when the backup contains the expected updates, the policy contents are not updated by Velero on the new hub cluster.

To address the previously mentioned limitations, when a **restore.cluster.open-cluster-management.io** resource is created, the cluster backup and restore operator runs a set of steps to prepare for restore by cleaning the hub cluster before Velero restore begins. For more information, see [Clean the hub cluster before restore](#).

1.2.8.4. Imported managed clusters are not displayed

Managed clusters that are manually imported on the primary hub cluster show only when the activation data is restored on the passive hub cluster.

1.2.8.5. Cluster backup and restore upgrade limitation

If you upgrade your cluster from 2.4 to 2.5 with the **enableClusterBackup** parameter set to **true**, the following message appears:

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

Before you upgrade your cluster, disable cluster backup and restore by setting the **enableClusterBackup** parameter to **false**. The **components** section in your **MultiClusterHub** resource might resemble the following YAML file:

You can reenble the backup and restore component when the upgrade is complete. View the following sample:

```
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
```

If you have manually installed OADP, you must manually uninstall OADP before you upgrade. After the upgrade is successful and backup and restore is reenbled, OADP is installed automatically.

1.2.8.6. Managed cluster resource not restored

When you restore the settings for the **local-cluster** managed cluster resource and overwrite the **local-cluster** data on a new hub cluster, the settings are misconfigured. Content from the previous hub cluster **local-cluster** is not backed up because the resource contains **local-cluster** specific information, such as the cluster URL details.

You must manually apply any configuration changes that are related to the **local-cluster** resource on the restored cluster. See [Prepare the new hub cluster](#) for more details.

1.2.8.7. **prepareForBackup** is only called when Velero schedules are first created

Any labels defined in the **prepareForBackup** function are not added to resources created after the schedules creation. This affects Hive and Infrastructure Operator for Red Hat OpenShift secrets that are being labeled before the backup is initiated.

View the list of affected resources:

- Secrets that are used by **clusterDeployments** and created by cluster claims
- Cluster pool secrets
- Secrets with the labels, **agent-install.openshift.io/watch** and **environment.metal3.io**

Update the **BackupSchedule**, **veleroSchedule**, or **veleroTTL** values to start a new set of schedules. Then use the resulted backup for a restore, which is defined to label the latest resources for the backup.

1.2.8.8. Restored Hive managed clusters might not be able to connect with the new hub cluster

When you restore the backup of the changed or rotated certificate of authority (CA) for the Hive managed cluster, on a new hub cluster, the managed cluster fails to connect to the new hub cluster. The connection fails because the **admin kubeconfig** secret for this managed cluster, available with the backup, is no longer valid.

You must manually update the restored **admin kubeconfig** secret of the managed cluster on the new hub cluster.

1.2.9. Submariner known issues

1.2.9.1. Submariner currently only supports OpenShift SDN as a CNI network provider

Only OpenShiftSDN is supported as a CNI network provider. OVN is currently not supported.

1.2.9.2. Submariner does not support some Red Hat Enterprise Linux nodes as worker nodes

When deploying Submariner on a cluster that includes Red Hat Enterprise Linux worker nodes with the kernel version between 4.18.0-359.el8.x86_64 and 4.18.0-372.11.1.el8_6.x86_64, application workloads fail to communicate with remote clusters.

1.2.9.3. Submariner does not support all infrastructure providers that Red Hat Advanced Cluster Management can manage

Submariner is not supported with all of the infrastructure providers that Red Hat Advanced Cluster Management can manage. Refer to the [Red Hat Advanced Cluster Management support matrix](#) for a list of supported providers.

1.2.9.4. Submariner does not support preparing the Red Hat OpenStack Platform infrastructure from the Red Hat Advanced Cluster Management console

Automatic cloud preparation for Red Hat OpenStack clusters is not supported for Submariner from the product-title-short} console. You can use the Red Hat Advanced Cluster Management APIs to prepare the clouds manually.

1.2.9.5. Submariner does not support headless services with Globalnet

Submariner supports headless services with Globalnet. However, when you access the exported headless service from a client that resides in the same cluster by using **clusterset.local** domain name, the **globalIP** that is associated with the headless service is returned to the client, which is not routable in the cluster.

You can use **cluster.local** domain name to access the local headless services.

1.2.9.6. Submariner does not support air-gapped clusters

Submariner is not validated for clusters that are provisioned in an air-gapped environment.

1.2.9.7. Numerous gateways cannot be deployed

You cannot deploy multiple gateways.

1.2.9.8. Submariner does not support VXLAN when NAT is enabled

Submariner with the VXLAN cable driver is currently only supported in non-NAT deployments.

1.2.9.9. Globalnet limitations

Globalnet is not supported with Red Hat OpenShift Data Foundation disaster recovery solutions. Make sure to use a non-overlapping range of private IP addresses for the cluster and service networks in each cluster for regional disaster recovery scenarios.

1.3. ERRATA UPDATES

By default, Errata updates are automatically applied when released. See [Upgrading by using the operator](#) for more information.

Important: For reference, [Errata](#) links and GitHub numbers might be added to the content and used internally. Links that require access might not be available for the user.

FIPS notice: If you do not specify your own ciphers in **spec.ingress.sslCiphers**, then the **multiclusterhub-operator** provides a default list of ciphers. For 2.4, this list includes two ciphers that are *not* FIPS approved. If you upgrade from a version 2.4.x or earlier and want FIPS compliance, remove the following two ciphers from the **multiclusterhub** resource: **ECDHE-ECDSA-CHACHA20-POLY1305** and **ECDHE-RSA-CHACHA20-POLY1305**.

1.3.1. Errata 2.5.9

- Delivers updates to one or more of the product container images and security fixes.

1.3.2. Errata 2.5.8

- The **must-gather** command now collects the Red Hat OpenShift Container Platform version number. ([ACM-2857](#))
- Fixes an issue that caused the **max_item_size** setting in the **MEMCACHED** index to not propagate changes to all **MEMCACHED** clients. ([ACM-4683](#))
- The policy status of policies with dots in their names now updates faster. ([ACM-4736](#))

1.3.3. Errata 2.5.7

- Fixes the **Edit time window** link in the console. The link now opens the correct edit page. ([ACM-2647](#))
- Fixes an issue that causes topology nodes to appear in the applications console when creating an application. ([ACM-3340](#))

1.3.4. Errata 2.5.6

- Delivers updates to one or more of the product container images and security fixes.

1.3.5. Errata 2.5.5

- Fixes an issue that causes a service denial for all policies when adding a custom label with a specific key and value to a policy.

1.3.6. Errata 2.5.4

- Delivers updates to one or more of the product container images and security fixes.

1.3.7. Errata 2.5.3

- Fixes a permission issue when using the unsupported **--validate-cluster-security** flag as a **HypershiftDeployment** controller argument. ([Bugzilla 2109544](#))
- Updates the search aggregator logic to avoid concurrent sync requests from a managed cluster. ([Bugzilla 2092863](#))
- Delivers updates to one or more of the product container images and security fixes.

1.3.8. Errata 2.5.2

- Beginning with Red Hat Advanced Cluster Management version 2.5.2, later Red Hat Advanced Cluster Management versions 2.5.x are supported on Red Hat OpenShift Container Platform version 4.11.
- Beginning with multicluster engine for Kubernetes operator version 2.0.2, later multicluster engine for Kubernetes operator versions 2.0.x are supported on Red Hat OpenShift Container Platform version 4.11.

- Fixes an MTU issue that caused Submariner Globalnet to fail to connect across on-premises and public clusters. ([Bugzilla 2074547](#))
- Addresses an issue that prevented the management-ingress pods from being started after installation. ([Bugzilla 2082254](#))
- Fixes a bug that caused an error in the managed clusters log when creating a **ClusterClaim** that had a label that contained an uppercase letter. ([Bugzilla 2095481](#))
- Resolves an issue that could result in the **MultiClusterHub** being stuck in the **installing** phase when installing on Red Hat OpenShift Container Platform. ([Bugzilla 2099503](#))
- Increases the limit of customized metrics in the custom metrics **allowlist** which enables it to collect more metrics from managed clusters. ([Bugzilla 2099808](#))
- Fixes a bug that caused a LimitRange Policy that was set to **enforce** to display and **non-compliant** status after updating the memory value for the policy in the console. ([Bugzilla 2100036](#))
- Fixes an issue that caused the following error when using the **app-of-apps** pattern with subscription applications: **This application has no subscription match selector (spec.selector.matchExpressions)** ([Bugzilla 2101577](#))
- Resolves an issue that caused a cluster to remain in the "unknown" state after recovering the Hub cluster with the Red Hat Advanced Cluster Management cluster backup and restore operator. ([Bugzilla 2103653](#))
- Sets the default value of **NodePool.Release.Image** to the release image that is specified for the **HostedClusterSpec.Release.Image** when it is not specified. ([Bugzilla 2105436](#))
- Resolves an issue that caused an application subscription that connected to a privately hosted Git server by using SSH to fail. The fix enables the SSH connection to a privately hosted Git server. ([Bugzilla 2105885](#))
- Fixes a bug that prevented associated **PolicyAutomation** and **AnsibleJob** objects from being removed when a policy was deleted by using the console. ([Bugzilla 2116060](#))

1.3.9. Errata 2.5.1

- Fixes a bug that removed some applications that were deployed on the managed cluster. ([Bugzilla 2101453](#))
- Resolves a console error in the *Overview* page, which displayed **The backend service is unavailable**. ([Bugzilla 2096389](#))
- Resolves a cluster add-on console issue with unhealthy status or failure for the policy add-on. ([Bugzilla 2088270](#))

1.4. DEPRECATIONS AND REMOVALS

Learn when parts of the product are deprecated or removed from Red Hat Advanced Cluster Management for Kubernetes. Consider the alternative actions in the *Recommended action* and details, which display in the tables for the current release and for two prior releases.

Important:

- The 2.4 and earlier versions of Red Hat Advanced Cluster Management are *removed* and no longer supported. The documentation might remain available, but is deprecated without any Errata or other updates available.
- Upgrading to the most recent version of Red Hat Advanced Cluster Management is the best practice.

1.4.1. API deprecations and removals

Red Hat Advanced Cluster Management follows the Kubernetes deprecation guidelines for APIs. See the [Kubernetes Deprecation Policy](#) for more details about that policy. Red Hat Advanced Cluster Management APIs are only deprecated or removed outside of the following timelines:

- All **V1** APIs are generally available and supported for 12 months or three releases, whichever is greater. V1 APIs are not removed, but can be deprecated outside of that time limit.
- All **beta** APIs are generally available for nine months or three releases, whichever is greater. Beta APIs are not removed outside of that time limit.
- All **alpha** APIs are not required to be supported, but might be listed as deprecated or removed if it benefits users.

1.4.1.1. API deprecations

Product or category	Affected item	Version	Recommended action	More details and links
Discovery	The <code>DiscoveredCluster</code> and <code>DiscoveryConfig</code> v1alpha1 APIs are deprecated. Discovery API is upgraded to V1 .	2.5	Use V1 .	None
Placements	The v1alpha1 API is upgraded to v1beta1 because v1alpha1 is deprecated.	2.5	Use v1beta1 .	The field <code>spec.prioritizerPolicy.configurations.name</code> in <code>Placement</code> API v1alpha1 is removed. Use <code>spec.prioritizerPolicy.configurations.scoreCoordinate.builtIn</code> in v1beta1 .

Product or category	Affected item	Version	Recommended action	More details and links
PlacementDecisions	The v1alpha1 API is upgraded to v1beta1 because v1alpha1 is deprecated.	2.5	Use v1beta1 .	None
Applications	The v1alpha1 API is removed completely. GitOps clusters API is upgraded to V1beta1 .	2.5	Use V1beta1 .	None
Applications	deployables.apps.open-cluster-management.io	2.5	None	The deployable API remains just for upgrade path. Any deployable CR create, update, or delete will not get reconciled.
CertPolicyController	The v1 API is deprecated.	2.5	Do not use this API.	CertPolicyController.agent.open-cluster-management.io
ApplicationManager	The v1 API is deprecated.	2.5	Do not use this API.	ApplicationManager.agent.open-cluster-management.io
IAMPolicyController	The v1 API is deprecated.	2.5	Do not use this API.	IAMPolicyController.agent.open-cluster-management.io
PolicyController	The v1 API is deprecated.	2.5	Do not use this API.	PolicyController.agent.open-cluster-management.io
SearchCollector	The v1 API is deprecated.	2.5	Do not use this API.	SearchCollector.agent.open-cluster-management.io

Product or category	Affected item	Version	Recommended action	More details and links
WorkManager	The v1 API is deprecated.	2.5	Do not use this API.	WorkManager.agent.open-cluster-management.io
ManagedClusterSets	The v1alpha1 API is upgraded to v1beta1 because v1alpha1 is deprecated.	2.4	Use v1beta1 .	None
ManagedClusterSetBindings	The v1alpha1 API is upgraded to v1beta1 because v1alpha1 is deprecated.	2.4	Use v1beta1 .	None

1.4.2. Red Hat Advanced Cluster Management deprecations

A *deprecated* component, feature, or service is supported, but no longer recommended for use and might become obsolete in future releases. Consider the alternative actions in the *Recommended action* and details that are provided in the following table:

Product or category	Affected item	Version	Recommended action	More details and links
Clusters	Cluster creation using bare metal assets	2.5	Create an infrastructure environment with the console	See Creating and modifying bare metal assets and Creating a cluster on bare metal for the affected deprecated areas. See Creating a cluster in an on-premises environment for the preceding process.
Add-on operator	Installation of built-in managed cluster add-ons	2.5	None	None

Product or category	Affected item	Version	Recommended action	More details and links
Observability	data.custom_rules.yaml.groups.rules is deprecated	2.5	Use data.custom_rules.yaml.groups.recording_rules .	See Customizing observability .
Installer	enableClusterProxyAddon and enableClusterBackup fields in operator.open-cluster-management.io_multiclusterhubs_crd.yaml	2.5	None	See Advanced Configuration for configuring install.
klusterlet operator	release-2.4 , release-2.3 channels do not receive updates	2.3 and later	To import and manage Red Hat OpenShift dedicated clusters, you must upgrade to 2.5 to receive updates.	See Upgrading by using the operator .
Applications	Managing secrets	2.4	Use policy hub templates for secrets instead.	See Manage security policies .
Governance console	pod-security-policy	2.4	None	None
Installer	Separate cert-manager settings in operator.open-cluster-management.io_multiclusterhubs_crd.yaml	2.3	None	None
Governance	Custom policy controller	2.3	None	None

1.4.3. Removals

A *removed* item is typically a function that was deprecated in previous releases and is no longer available in the product. You must use alternatives for the removed function. Consider the alternative actions in the *Recommended action* and details that are provided in the following table:

Product or category	Affected item	Version	Recommended action	More details and links
Applications	Deployable controller	2.5	None	The Deployable controller removed.
Red Hat Advanced Cluster Management console	Visual Web Terminal (Technology Preview)	2.4	Use the terminal instead	None
Applications	Single ArgoCD import mode, secrets imported to one ArgoCD server on the hub cluster.	2.3	You can import cluster secrets into multiple ArgoCD servers.	None
Applications	ArgoCD cluster integration: spec.applicationManager.argocdCluster	2.3	Create a GitOps cluster and placement custom resource to register managed clusters.	Configuring GitOps on managed clusters
Governance	cert-manager internal certificate management	2.3	No action is required	None

1.5. RED HAT ADVANCED CLUSTER MANAGEMENT FOR KUBERNETES PLATFORM CONSIDERATIONS FOR GDPR READINESS

1.5.1. Notice

This document is intended to help you in your preparations for General Data Protection Regulation (GDPR) readiness. It provides information about features of the Red Hat Advanced Cluster Management for Kubernetes platform that you can configure, and aspects of the product's use, that you should consider to help your organization with GDPR readiness. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party clusters and systems.

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. Red Hat does not provide legal, accounting, or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

1.5.2. Table of Contents

- [GDPR](#)
- [Product Configuration for GDPR](#)
- [Data Life Cycle](#)
- [Data Collection](#)
- [Data Storage](#)
- [Data Access](#)
- [Data Processing](#)
- [Data Deletion](#)
- [Capability for Restricting Use of Personal Data](#)
- [Appendix](#)

1.5.3. GDPR

General Data Protection Regulation (GDPR) has been adopted by the European Union ("EU") and applies from May 25, 2018.

1.5.3.1. Why is GDPR important?

GDPR establishes a stronger data protection regulatory framework for processing personal data of individuals. GDPR brings:

- New and enhanced rights for individuals
- Widened definition of personal data
- New obligations for processors
- Potential for significant financial penalties for non-compliance
- Compulsory data breach notification

1.5.3.2. Read more about GDPR

- [EU GDPR Information Portal](#)
- [Red Hat GDPR website](#)

1.5.4. Product Configuration for GDPR

The following sections describe aspects of data management within the Red Hat Advanced Cluster Management for Kubernetes platform and provide information on capabilities to help clients with GDPR requirements.

1.5.5. Data Life Cycle

Red Hat Advanced Cluster Management for Kubernetes is an application platform for developing and managing on-premises, containerized applications. It is an integrated environment for managing containers that includes the container orchestrator Kubernetes, cluster lifecycle, application lifecycle, and security frameworks (governance, risk, and compliance).

As such, the Red Hat Advanced Cluster Management for Kubernetes platform deals primarily with technical data that is related to the configuration and management of the platform, some of which might be subject to GDPR. The Red Hat Advanced Cluster Management for Kubernetes platform also deals with information about users who manage the platform. This data will be described throughout this document for the awareness of clients responsible for meeting GDPR requirements.

This data is persisted on the platform on local or remote file systems as configuration files or in databases. Applications that are developed to run on the Red Hat Advanced Cluster Management for Kubernetes platform might deal with other forms of personal data subject to GDPR. The mechanisms that are used to protect and manage platform data are also available to applications that run on the platform. Additional mechanisms might be required to manage and protect personal data that is collected by applications run on the Red Hat Advanced Cluster Management for Kubernetes platform.

To best understand the Red Hat Advanced Cluster Management for Kubernetes platform and its data flows, you must understand how Kubernetes, Docker, and the Operator work. These open source components are fundamental to the Red Hat Advanced Cluster Management for Kubernetes platform. You use Kubernetes deployments to place instances of applications, which are built into Operators that reference Docker images. The Operator contain the details about your application, and the Docker images contain all the software packages that your applications need to run.

1.5.5.1. What types of data flow through Red Hat Advanced Cluster Management for Kubernetes platform

As a platform, Red Hat Advanced Cluster Management for Kubernetes deals with several categories of technical data that could be considered as personal data, such as an administrator user ID and password, service user IDs and passwords, IP addresses, and Kubernetes node names. The Red Hat Advanced Cluster Management for Kubernetes platform also deals with information about users who manage the platform. Applications that run on the platform might introduce other categories of personal data unknown to the platform.

Information on how this technical data is collected/created, stored, accessed, secured, logged, and deleted is described in later sections of this document.

1.5.5.2. Personal data used for online contact

Customers can submit online comments/feedback/requests for information about in a variety of ways, primarily:

- The public Slack community if there is a Slack channel
- The public comments or tickets on the product documentation
- The public conversations in a technical community

Typically, only the client name and email address are used, to enable personal replies for the subject of the contact, and the use of personal data conforms to the [Red Hat Online Privacy Statement](#).

1.5.6. Data Collection

The Red Hat Advanced Cluster Management for Kubernetes platform does not collect sensitive personal data. It does create and manage technical data, such as an administrator user ID and password,

service user IDs and passwords, IP addresses, and Kubernetes node names, which might be considered personal data. The Red Hat Advanced Cluster Management for Kubernetes platform also deals with information about users who manage the platform. All such information is only accessible by the system administrator through a management console with role-based access control or by the system administrator through login to a Red Hat Advanced Cluster Management for Kubernetes platform node.

Applications that run on the Red Hat Advanced Cluster Management for Kubernetes platform might collect personal data.

When you assess the use of the Red Hat Advanced Cluster Management for Kubernetes platform running containerized applications and your need to meet the requirements of GDPR, you must consider the types of personal data that are collected by the application and aspects of how that data is managed, such as:

- How is the data protected as it flows to and from the application? Is the data encrypted in transit?
- How is the data stored by the application? Is the data encrypted at rest?
- How are credentials that are used to access the application collected and stored?
- How are credentials that are used by the application to access data sources collected and stored?
- How is data collected by the application removed as needed?

This is not a definitive list of the types of data that are collected by the Red Hat Advanced Cluster Management for Kubernetes platform. It is provided as an example for consideration. If you have any questions about the types of data, contact Red Hat.

1.5.7. Data storage

The Red Hat Advanced Cluster Management for Kubernetes platform persists technical data that is related to configuration and management of the platform in stateful stores on local or remote file systems as configuration files or in databases. Consideration must be given to securing all data at rest. The Red Hat Advanced Cluster Management for Kubernetes platform supports encryption of data at rest in stateful stores that use **dm-crypt**.

The following items highlight the areas where data is stored, which you might want to consider for GDPR.

- **Platform Configuration Data:** The Red Hat Advanced Cluster Management for Kubernetes platform configuration can be customized by updating a configuration YAML file with properties for general settings, Kubernetes, logs, network, Docker, and other settings. This data is used as input to the Red Hat Advanced Cluster Management for Kubernetes platform installer for deploying one or more nodes. The properties also include an administrator user ID and password that are used for bootstrap.
- **Kubernetes Configuration Data:** Kubernetes cluster state data is stored in a distributed key-value store, **etcd**.
- **User Authentication Data, including User IDs and passwords:** User ID and password management are handled through a client enterprise LDAP directory. Users and groups that are defined in LDAP can be added to Red Hat Advanced Cluster Management for Kubernetes platform teams and assigned access roles. Red Hat Advanced Cluster Management for Kubernetes platform stores the email address and user ID from LDAP, but does not store the password. Red Hat Advanced Cluster Management for Kubernetes platform stores the group

name and upon login, caches the available groups to which a user belongs. Group membership is not persisted in any long-term way. Securing user and group data at rest in the enterprise LDAP must be considered. Red Hat Advanced Cluster Management for Kubernetes platform also includes an authentication service, Open ID Connect (OIDC) that interacts with the enterprise directory and maintains access tokens. This service uses ETCD as a backing store.

- **Service authentication data, including user IDs and passwords.** Credentials that are used by Red Hat Advanced Cluster Management for Kubernetes platform components for inter-component access are defined as Kubernetes Secrets. All Kubernetes resource definitions are persisted in the **etcd** key-value data store. Initial credentials values are defined in the platform configuration data as Kubernetes Secret configuration YAML files. For more information, see [Secrets](#) in the Kubernetes documentation.

1.5.8. Data access

Red Hat Advanced Cluster Management for Kubernetes platform data can be accessed through the following defined set of product interfaces.

- Web user interface (the console)
- Kubernetes **kubectl** CLI
- Red Hat Advanced Cluster Management for Kubernetes CLI
- oc CLI

These interfaces are designed to allow you to make administrative changes to your Red Hat Advanced Cluster Management for Kubernetes cluster. Administration access to Red Hat Advanced Cluster Management for Kubernetes can be secured and involves three logical, ordered stages when a request is made: authentication, role-mapping, and authorization.

1.5.8.1. Authentication

The Red Hat Advanced Cluster Management for Kubernetes platform authentication manager accepts user credentials from the console and forwards the credentials to the backend OIDC provider, which validates the user credentials against the enterprise directory. The OIDC provider then returns an authentication cookie (**auth-cookie**) with the content of a JSON Web Token (**JWT**) to the authentication manager. The JWT token persists information such as the user ID and email address, in addition to group membership at the time of the authentication request. This authentication cookie is then sent back to the console. The cookie is refreshed during the session. It is valid for 12 hours after you sign out of the console or close your web browser.

For all subsequent authentication requests made from the console, the front-end NGINX server decodes the available authentication cookie in the request and validates the request by calling the authentication manager.

The Red Hat Advanced Cluster Management for Kubernetes platform CLI requires the user to provide credentials to log in.

The **kubectl** and **oc** CLI also requires credentials to access the cluster. These credentials can be obtained from the management console and expire after 12 hours. Access through service accounts is supported.

1.5.8.2. Role Mapping

Red Hat Advanced Cluster Management for Kubernetes platform supports role-based access control

(RBAC). In the role mapping stage, the user name that is provided in the authentication stage is mapped to a user or group role. The roles are used when authorizing which administrative activities can be carried out by the authenticated user.

1.5.8.3. Authorization

Red Hat Advanced Cluster Management for Kubernetes platform roles control access to cluster configuration actions, to catalog and Helm resources, and to Kubernetes resources. Several IAM (Identity and Access Management) roles are provided, including Cluster Administrator, Administrator, Operator, Editor, Viewer. A role is assigned to users or user groups when you add them to a team. Team access to resources can be controlled by namespace.

1.5.8.4. Pod Security

Pod security policies are used to set up cluster-level control over what a pod can do or what it can access.

1.5.9. Data Processing

Users of Red Hat Advanced Cluster Management for Kubernetes can control the way that technical data that is related to configuration and management is processed and secured through system configuration.

Role-based access control (RBAC) controls what data and functions can be accessed by users.

Data-in-transit is protected by using **TLS. HTTPS (TLS underlying)** is used for secure data transfer between user client and back end services. Users can specify the root certificate to use during installation.

Data-at-rest protection is supported by using **dm-crypt** to encrypt data.

These same platform mechanisms that are used to manage and secure Red Hat Advanced Cluster Management for Kubernetes platform technical data can be used to manage and secure personal data for user-developed or user-provided applications. Clients can develop their own capabilities to implement further controls.

1.5.10. Data Deletion

Red Hat Advanced Cluster Management for Kubernetes platform provides commands, application programming interfaces (APIs), and user interface actions to delete data that is created or collected by the product. These functions enable users to delete technical data, such as service user IDs and passwords, IP addresses, Kubernetes node names, or any other platform configuration data, as well as information about users who manage the platform.

Areas of Red Hat Advanced Cluster Management for Kubernetes platform to consider for support of data deletion:

- All technical data that is related to platform configuration can be deleted through the management console or the Kubernetes **kubectl** API.

Areas of Red Hat Advanced Cluster Management for Kubernetes platform to consider for support of account data deletion:

- All technical data that is related to platform configuration can be deleted through the Red Hat Advanced Cluster Management for Kubernetes or the Kubernetes **kubectl** API.

Function to remove user ID and password data that is managed through an enterprise LDAP directory would be provided by the LDAP product used with Red Hat Advanced Cluster Management for Kubernetes platform.

1.5.11. Capability for Restricting Use of Personal Data

Using the facilities summarized in this document, Red Hat Advanced Cluster Management for Kubernetes platform enables an end user to restrict usage of any technical data within the platform that is considered personal data.

Under GDPR, users have rights to access, modify, and restrict processing. Refer to other sections of this document to control the following:

- Right to access
 - Red Hat Advanced Cluster Management for Kubernetes platform administrators can use Red Hat Advanced Cluster Management for Kubernetes platform features to provide individuals access to their data.
 - Red Hat Advanced Cluster Management for Kubernetes platform administrators can use Red Hat Advanced Cluster Management for Kubernetes platform features to provide individuals information about what data Red Hat Advanced Cluster Management for Kubernetes platform holds about the individual.
- Right to modify
 - Red Hat Advanced Cluster Management for Kubernetes platform administrators can use Red Hat Advanced Cluster Management for Kubernetes platform features to allow an individual to modify or correct their data.
 - Red Hat Advanced Cluster Management for Kubernetes platform administrators can use Red Hat Advanced Cluster Management for Kubernetes platform features to correct an individual's data for them.
- Right to restrict processing
 - Red Hat Advanced Cluster Management for Kubernetes platform administrators can use Red Hat Advanced Cluster Management for Kubernetes platform features to stop processing an individual's data.

1.5.12. Appendix

As a platform, Red Hat Advanced Cluster Management for Kubernetes deals with several categories of technical data that could be considered as personal data, such as an administrator user ID and password, service user IDs and passwords, IP addresses, and Kubernetes node names. Red Hat Advanced Cluster Management for Kubernetes platform also deals with information about users who manage the platform. Applications that run on the platform might introduce other categories of personal data that are unknown to the platform.

This appendix includes details on data that is logged by the platform services.

1.6. FIPS READINESS

FIPS readiness has been completed for Red Hat Advanced Cluster Management for Kubernetes. Red Hat Advanced Cluster Management uses the same tools to make sure cryptography calls are passed to the Red Hat Enterprise Linux (RHEL) certified cryptographic modules that are used by Red Hat

OpenShift Container Platform. For more details on OpenShift FIPS support see, [Support for FIPS cryptography](#).

1.6.1. Limitations

Read the following limitations with Red Hat Advanced Cluster Management and FIPS.

- Red Hat OpenShift Container Platform only supports FIPS on the **x86_64** architecture.
- Integrity Shield is a Technology Preview component that is not FIPS ready.
- Persistent Volume Claim (PVC) and S3 storage that is used by the search and observability components must be encrypted when you configure the provided storage. Red Hat Advanced Cluster Management does not provide storage encryption, see the OpenShift Container Platform documentation, [Support for FIPS cryptography](#).
- When you provision managed clusters using the Red Hat Advanced Cluster Management console, select the following check box in the *Cluster details* section of the managed cluster creation to enable the FIPS standards:

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.