Red Hat OpenShift GitOps 1.12

Release notes

Highlights of what is new and what has changed with this OpenShift GitOps release

Last Updated: 2024-06-04

Red Hat OpenShift GitOps 1.12 Release notes

Highlights of what is new and what has changed with this OpenShift GitOps release

Legal Notice

Abstract

The release notes for OpenShift GitOps summarize all new features and enhancements, notable technical changes, major corrections from the previous version, and any known bugs upon general availability.

Table of Contents

CHAPTER 1. RED HAT OPENSHIFT GITOPS RELEASE NOTES

Red Hat OpenShift GitOps is a declarative way to implement continuous deployment for cloud native applications. Red Hat OpenShift GitOps ensures consistency in applications when you deploy them to different clusters in different environments, such as: development, staging, and production. Red Hat OpenShift GitOps helps you automate the following tasks:

- Ensure that the clusters have similar states for configuration, monitoring, and storage
- Recover or recreate clusters from a known state
- Apply or revert configuration changes to multiple OpenShift Container Platform clusters
- Associate templated configuration with different environments
- Promote applications across clusters, from staging to production

For an overview of Red Hat OpenShift GitOps, see About Red Hat OpenShift GitOps .

1.1. COMPATIBILITY AND SUPPORT MATRIX

Some features in this release are currently in Technology Preview. These experimental features are not intended for production use.

In the table, features are marked with the following statuses:

- **TP**: *Technology Preview*
- **GA**: *General Availability*
- **NA**: *Not Applicable*

IMPORTANT

In OpenShift Container Platform 4.13, the **stable** channel has been removed. Before upgrading to OpenShift Container Platform 4.13, if you are already on the **stable** channel, choose the appropriate channel and switch to it.

OpenShift GitOps	Component Versions								OpenShift Versions
Version	kam	Argo CD CLI	Helm	Kustomize	Argo CD	Argo Rollouts	Dex	RH SSO	
1.12.0	0.0.51 TP	2.10.3 TP	3.14.0 GA	5.2.1 GA	2.10.3 GA	1.6.0 TP	2.36.0 GA	7.6.0 GA	4.12-4.15
1.11.0	0.0.51 TP	NA	3.13.2 GA	5.2.1 GA	2.9.2 GA	1.6.0 TP	2.36.0 GA	7.6.0 GA	4.12-4.14

OpenShift GitOps	Component Versions								OpenShift Versions
1.10.0	0.0.50 TP	NA	3.12.1 GA	5.1.0 GA	2.8.3 GA	1.5.0 TP	2.35.1 GA	7.5.1 GA	4.12-4.14

- **kam** is the Red Hat OpenShift GitOps Application Manager command-line interface (CLI).
- RH SSO is an abbreviation for Red Hat SSO.

1.1.1. Technology Preview features

The features mentioned in the following table are currently in Technology Preview (TP). These experimental features are not intended for production use.

Table 1.1. Technology Preview tracker

Feature	TP in Red Hat OpenShift GitOps versions	GA in Red Hat OpenShift GitOps versions
The GitOps **argocd** CLI tool	1.12.0	NA
Argo CD application sets in non-control plane namespaces	1.12.0	NA
The **round-robin** cluster sharding algorithm	1.10.0	NA
Dynamic scaling of shards	1.10.0	NA
Argo Rollouts	1.9.0	NA
ApplicationSet Progressive Rollout Strategy	1.8.0	NA
Multiple sources for an application	1.8.0	NA
Argo CD applications in non-control plane namespaces	1.7.0	NA
The Red Hat OpenShift GitOps **Environments** page in the **Developer** perspective of the OpenShift Container Platform web console	1.1.0	NA

1.2. MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. We are beginning with these four terms: master, slave, blacklist, and whitelist. Because of the enormity of this endeavor, these changes will be implemented gradually over several upcoming releases.

For more details, see our CTO Chris Wright's message .

1.3. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.12.3

Red Hat OpenShift GitOps 1.12.3 is now available on OpenShift Container Platform 4.12, 4.13, 4.14, and 4.15.

1.3.1. Errata updates

1.3.1.1. RHSA-2024:3368 - Red Hat OpenShift GitOps 1.12.3 security update advisory

Issued: 2024-05-28

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:3368

If you have installed the Red Hat OpenShift GitOps Operator in the default namespace, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-gitops-operator
```

1.3.2. Fixed issues

- Before this update, pods in a different namespace could access the Redis server on port **6379** to obtain read and write access to the data. This update fixes the issue by enabling secure authentication.

1.4. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.12.2

Red Hat OpenShift GitOps 1.12.2 is now available on OpenShift Container Platform 4.12, 4.13, 4.14, and 4.15.

1.4.1. Errata updates

1.4.1.1. RHSA-2024:2816 - Red Hat OpenShift GitOps 1.12.2 security update advisory

Issued: 2024-05-10

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:2816

If you have installed the Red Hat OpenShift GitOps Operator in the default namespace, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-gitops-operator
```

1.4.2. New features

- With this update, support has been provided for the **must-gather** tool in the Argo Rollouts Operator. This update provides support for the following enhancements:

- Logs for Argo Rollouts Operator pods and Argo Rollouts pods.
- Contents of Argo Rollouts Manager and Argo Rollouts custom resources (CRs).
- Contents of **Deployment**, **Statefulset**, and **ConfigMaps** CRs created by the **must-gather** tool in the Argo Rollouts Operator. GITOPS-3947

1.4.3. Fixed issues

- Before this update, users could not use the **argocd-k8s-auth** binary to add Google Kubernetes Engine (GKE) and Amazon Elastic Kubernetes Service (EKS) clusters because this binary was not available in the GitOps container. This update fixes the issue by adding the **argocd-k8s-auth** binary in the GitOps container. GITOPS-4226
- Before this update, attempts to connect to Azure DevOps with Argo CD would result in an error due to the deprecation of the **rsa-ssh** host key algorithm by the Azure DevOps Repository service. This update fixes the issue by providing support for the **rsa-ssh** host key algorithms during the communication process between Argo CD and Azure DevOps Repository service. GITOPS-4543
- Before this update, GitOps console plugin workloads did not schedule on infrastructure nodes when the **runOnInfra** field was enabled in the **GitOpsService** custom resource (CR). This update fixes the issue by adding the infrastructure **node-selector** on the GitOps console plugin workloads. This enables users to configure custom node-selectors and tolerations on the **gitops-console** pod. As a result, when the **runOnInfra** field is enabled, the GitOps console plugin pod is placed on the infrastructure nodes like the other default workloads. GITOPS-4496
- Before this update, the **ignoreDifferences** sync option in Argo CD did not work for array fields. This update fixes the issue by modifying the merge strategy of the **ignoreDifferences** sync option used in the upstream project to handle array fields. As a result, the sync option now functions correctly by allowing users to ignore specific elements in the array during sync. GITOPS-2962
- Before this update, users were unable to include context for notifications in the **NotificationsConfiguration** custom resource (CR). With this update, users can now add context for notifications by using the **context** field in the **NotificationsConfiguration** CR. This field can also be used to establish shared context across all templates defined in the **NotificationsConfiguration** CR. GITOPS-4303

  Example of the context field in the NotificationsConfiguration CR

  ```
  spec:
    context:
      region: east (1)
  ```

  (1) Context among all notification templates is in **key-value** pairs

- Before this update, users accessing a Red Hat OpenShift on AWS (ROSA) cluster after hibernation were unable to log in to the Argo CD web console due to an error indicating an invalid redirect URI in the Dex configuration. With this update, users can now log in to the Argo CD web console without facing any errors when the ROSA cluster is operational post-hibernation. GITOPS-4358
- Before this update, users were unable to log in to the Argo CD web console if the availability of the **openshift-gitops** route was delayed while the Red Hat OpenShift GitOps Operator

processed an Argo CD custom resource instance. An error message was displayed indicating an invalid redirect URI in the Dex configuration. With this update, users can now log in to the Argo CD web console without facing any errors. GITOPS-3736

- Before this update, users could not create custom resources for Argo CD from the **Add** page on the **Developer** perspective of the Red Hat OpenShift GitOps web console. This issue has been observed from Red Hat OpenShift GitOps 1.10 and later releases. This update fixes the issue because Operator-backed resources with the correct versions are included in the **ClusterServiceVersion** manifest file. GITOPS-4513

1.5. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.12.1

Red Hat OpenShift GitOps 1.12.1 is now available on OpenShift Container Platform 4.12, 4.13, 4.14, and 4.15.

1.5.1. Errata updates

1.5.1.1. RHSA-2024:1753 - Red Hat OpenShift GitOps 1.12.1 security update advisory

Issued: 2024-04-10

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1753

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.6. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.12.0

Red Hat OpenShift GitOps 1.12.0 is now available on OpenShift Container Platform 4.12, 4.13, 4.14, and 4.15.

1.6.1. Errata updates

1.6.1.1. RHSA-2024:1441 - Red Hat OpenShift GitOps 1.12.0 security update advisory

Issued: 2024-03-20

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1441

If you have installed the Red Hat OpenShift GitOps Operator in the default namespace, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-gitops-operator
```

1.6.2. New features

- With this update, the GitOps **argocd** CLI is supported and accessible as a productized component of Red Hat OpenShift GitOps. The GitOps **argocd** CLI tool is available through RPMs in RHEL. You can download it through the OpenShift mirror registry.

WARNING

The GitOps **argocd** CLI tool is a Technology Preview feature.

By using the GitOps **argocd** CLI tool, you can complete the following tasks:

  - Manage Red Hat OpenShift GitOps from a terminal.
  - Manage ArgoCD resources, such as **Applications**, **ApplicationSets**, **AppProjects**, **User accounts**, and **GPG keys** from a client terminal. GITOPS-3389

NOTE

The **argocd** executable binary file is included in the archive and RPM formats.

- With this update, **NotificationsConfiguration** custom resource (CR) is now supported. Before this update, you had to update the **argocd-notifications-cm** ConfigMap to manage templates, triggers, services and subscriptions. With this release, you cannot modify the **argocd-notifications-cm** ConfigMap. A new Custom Resource definition **NotificationsConfiguration** is introduced to manage the **argocd-notifications-cm** ConfigMap. GITOPS-4130

NOTE

This update removes any configuration added to **argocd-notifications-cm** ConfigMap. You must take a backup of your configuration and update the configuration/backup in the **default-notifications-configuration** custom resource of **kind:NotificationsConfiguration** after upgrading to the new version. Also, with this update, any modifications to **argocd-notifications-cm** ConfigMap are not allowed.

- With this update, two new fields **.spec.applicationSet.sourceNamespaces** and **.spec.applicationSet.scmProviders** are introduced in the **ArgoCD** CRD to support **ApplicationSet** in any non-control plane namespaces. Administrators can use these fields to define certain namespaces that manage **ApplicationSet** resources. GITOPS-3754

WARNING

Argo CD application sets in non-control plane namespaces is a Technology Preview feature.

- With this update, Argo CD server has the required permissions to manage **ApplicationSet** resources. GITOPS-3762

- With this update, you can configure log levels, such as **debug**, **info**, **warn**, **error**, **panic** and **fatal**. The default log level set for the output is **info**. To change the log level, add the environment variable **LOG_LEVEL** in the **.spec.config.env** field of the **Subscription** CR. GITOPS-4016

  Example output

```
apiVersion: operators.coreos.com/v1alpha1
kind: Subscription
metadata:
  name: gitops-operator
  namespace: openshift-gitops-operator
spec:
  ...
  config:
    env:
    - name: LOG_LEVEL
      value: "error"
```

- With this update, Argo CD accepts the wildcard values in the **sourceNamespaces** field so that you can specify multiple namespaces or patterns for namespaces. To use this feature, specify the namespaces where Argo CD can manage applications in the **.spec.sourceNamespaces** field of the **ArgoCD** CR. GITOPS-3935

  Example

```
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd-wildcard-pattern
spec:
  sourceNamespaces:
    - app-team-*
    - namespace-2
```

  In the previous example, permissions are granted to namespaces that match the pattern **app-team-***, such as **app-team-1**, **app-team-2**, and namespace-2, which does not use wildcard values.

  To grant permissions for all the namespaces on the Argo CD cluster using the * wildcard pattern, configure the **ArgoCD** CR in the following manner:

  Example

```
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd-all-namespaces
spec:
  sourceNamespaces:
    - '*'
```

1.6.3. Fixed issues

- Before this update, the notifications controller could not use built-in functions in notification templates to obtain information about applications because of an incorrect repository server address. This update fixes the issue by initializing the notification controller to use the correct repository server address. GITOPS-2867

- Before this update, when a user created a **Job** from a **CronJob** resource, an error is displayed. With this update, users can create **Job** executions from a **CronJob** resource defined in a deployed Argo CD application. GITOPS-3617

- Before this update, in some instance when applications are deleted, their application environment card would remain in a half-deleted state until the page was refreshed. With this update, the application environment card is removed from the UI automatically after the Argo CD application is deleted. GITOPS-2677

- Before this update, when a user deleted apps and namespaces in Argo CD, in some cases, the Red Hat OpenShift GitOps plugin would display an error message. This update fixes the issue by updating some components from the dynamic plugin SDK and provides better error handling. As a result, the error message is not displayed after deleting apps or namespaces. GITOPS-2746

- Before this update, the password for the **admin** role was used to reset to the default password when it was updated by the GitOps **argocd** CLI or the Argo CD UI. This update fixes the issue and the user can now update the admin password and the password is no longer set to default. GITOPS-3581

1.6.4. Known Issues

- There is currently a known issue that changes the functionality of routing in the OpenShift Console Dynamic plugin, **dynamic-console-sdk**, that is used by the Red Hat OpenShift GitOps Dynamic Plugin. This issue causes the horizontal navigation bar, which is used to switch between the **Application Overview** page and the **Deployment History** page for an application, on the **Application Overview** page to not function correctly. GITOPS-4232
  Workaround: To view the **Deployment History** page of an application, use the **Deployment History** link on the application instead of the link on the horizontal navigation bar on the **Application Overview** page. This issue has been observed on all supported cluster versions that use the Red Hat OpenShift GitOps Dynamic Plugin.

- There is currently a known issue on the OpenShift Container Platform cluster for the console Red Hat OpenShift GitOps Dynamic Plugin where users can experience some delay when fetching application data. GITOPS-4234
  Workaround: No workaround currently exists for this issue, so you must wait for the fetching of the application data to complete.

- There is currently a known issue that causes the Red Hat OpenShift GitOps Dynamic Plugin to be disabled on the OpenShift Container Platform 4.15 cluster. GITOPS-4231
  Workaround: Perform the following steps:

  1. Install the Red Hat OpenShift GitOps Operator on your cluster.
  2. In the **Administrator** perspective of the web console, navigate to **Home → Overview**.
  3. On the **Overview** tab, click the **Dynamic plugins** link in the **Status** section.
  4. To enable the Red Hat OpenShift GitOps Dynamic Plugin, click **gitops-plugin** and then click **Enabled**.

After some time, a notification with the message “Web console update is available” is displayed.

1.7. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.5

Red Hat OpenShift GitOps 1.11.5 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.7.1. Errata updates

1.7.1.1. RHSA-2024:3475 - Red Hat OpenShift GitOps 1.11.5 security update advisory

Issued: 2024-05-29

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:3475

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.7.2. Fixed issues

- Before this update, pods in a different namespace could access the Redis server on port **6379** to obtain read and write access to the data. This issue has been fixed in this release by enabling secure authentication.

1.8. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.4

Red Hat OpenShift GitOps 1.11.4 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.8.1. Errata updates

1.8.1.1. RHSA-2024:2815 - Red Hat OpenShift GitOps 1.11.4 security update advisory

Issued: 2024-05-10

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:2815

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.8.2. Fixed issues

- Before this update, users could not use the **argocd-k8s-auth** binary to add Google Kubernetes Engine (GKE) and Amazon Elastic Kubernetes Service (EKS) clusters because this binary was not available in the GitOps container. This update fixes the issue by adding the **argocd-k8s-**

auth binary in the GitOps container. GITOPS-4226

- Before this update, attempts to connect to Azure DevOps with Argo CD would result in an error due to the deprecation of the **rsa-ssh** host key algorithm by the Azure DevOps Repository service. This update fixes the issue by providing support for the **rsa-ssh** host key algorithms during the communication process between Argo CD and Azure DevOps Repository service. GITOPS-4543

- Before this update, the **ignoreDifferences** sync option in Argo CD did not work for array fields. This update fixes the issue by modifying the merge strategy of the **ignoreDifferences** sync option used in the upstream project to handle array fields. As a result, the sync option now functions correctly by allowing users to ignore specific elements in the array during sync. GITOPS-2962

- Before this update, users accessing a Red Hat OpenShift on AWS (ROSA) cluster after hibernation were unable to log in to the Argo CD web console due to an error indicating an invalid redirect URI in the Dex configuration. With this update, users can now log in to the Argo CD web console without facing any errors when the ROSA cluster is operational post-hibernation. GITOPS-4358

- Before this update, users were unable to log in to the Argo CD web console if the availability of the **openshift-gitops** route was delayed while the Red Hat OpenShift GitOps Operator processed an Argo CD custom resource instance. An error message was displayed indicating an invalid redirect URI in the Dex configuration. With this update, users can now log in to the Argo CD web console without facing any errors. GITOPS-3736

- Before this update, users could not create custom resources for Argo CD from the **Add** page on the **Developer** perspective of the Red Hat OpenShift GitOps web console. This issue has been observed from Red Hat OpenShift GitOps 1.10 and later releases. This update fixes the issue because Operator-backed resources with the correct versions are included in the **ClusterServiceVersion** manifest file. GITOPS-4513

1.9. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.3

Red Hat OpenShift GitOps 1.11.3 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.9.1. Errata updates

1.9.1.1. RHSA-2024:1697 - Red Hat OpenShift GitOps 1.11.3 security update advisory

Issued: 2024-04-08

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1697

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.10. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.2

Red Hat OpenShift GitOps 1.11.2 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.10.1. Errata updates

1.10.1.1. RHSA-2024:1346 - Red Hat OpenShift GitOps 1.11.2 security update advisory

Issued: 2023-03-15

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1346

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.10.2. Fixed issues

Before this update, due to the incorrect filtering of URL protocols in the Argo CD application summary component, an attacker could use cross-site scripting with permission to edit the application. This update fixes the issue by upgrading the Argo CD version to 2.9.8, which patches this vulnerability. GITOPS-4210

1.11. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.1

Red Hat OpenShift GitOps 1.11.1 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.11.1. Errata updates

1.11.1.1. RHSA-2024-0689 - Red Hat OpenShift GitOps 1.11.1 security update advisory

Issued: 2024-02-05

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024-0689

If you have installed the Red Hat OpenShift GitOps Operator, view the container images in this release by running the following command:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.12. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.11.0

Red Hat OpenShift GitOps 1.11.0 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.12.1. New features

The current release adds the following improvement:

- With this update, you can selectively disable the **redis** and **application-controller** components for an Argo CD instance in a specified namespace. These components are enabled by default. To disable a component, set the **enabled** flag to **false** in the **.spec.<component>.enabled** field

of the Argo CD Custom Resource (CR). GITOPS-3723
For example:

```
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd
spec:
  controller:
    enabled: false
  redis:
    enabled: false
```

NOTE

This feature is currently limited to the **redis** and **application-controller** components. It is expected that support for other components will be included in a future Red Hat OpenShift GitOps release.

1.12.2. Fixed issues

The following issues have been resolved in the current release:

- Before this update, the Argo CD Notifications Controller did not support custom certificates added to the **argocd-tls-certs-cm** config map. As a result, notification services with custom certificates did not receive notifications due to the **x509: certificate signed by unknown authority** error message. This update fixes the issue by correctly initializing the cert resolver function in the Argo CD Notifications Controller to load all certificates stored in the **argocd-tls-certs-cm** config map. Now, notification services with custom certificates can successfully receive notifications. GITOPS-2809

- Before this update, users would face **PrometheusOperatorRejectedResources** alerts when the Red Hat OpenShift GitOps Operator was not installed in the **openshift-gitops-operator** namespace. The problem affected users who upgraded from earlier versions of the Red Hat OpenShift GitOps Operator to v1.10. This update fixes the issue by updating the Operator's **serverName** metrics service to reflect the correct installation namespace. Now, users who upgrade or install the Red Hat OpenShift GitOps Operator in namespaces other than **openshift-gitops-operator** should not see these alerts. GITOPS-3424

1.13. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.6

Red Hat OpenShift GitOps 1.10.6 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.13.1. Errata updates

1.13.1.1. RHSA-2024:3369 - Red Hat OpenShift GitOps 1.10.6 security update advisory

Issued: 2024-05-28

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:3369

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.13.2. Fixed issues

- Before this update, pods in a different namespace could access the Redis server on port **6379** to obtain read and write access to the data. This update fixes the issue by enabling secure authentication.

1.14. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.5

Red Hat OpenShift GitOps 1.10.5 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.14.1. Errata updates

1.14.1.1. RHSA-2024:2817 - Red Hat OpenShift GitOps 1.10.5 security update advisory

Issued: 2024-05-10

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:2817

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.14.2. Fixed issues

- Before this update, users could not use the **argocd-k8s-auth** binary to add Google Kubernetes Engine (GKE) and Amazon Elastic Kubernetes Service (EKS) clusters because this binary was not available in the GitOps container. This update fixes the issue by adding the **argocd-k8s-auth** binary in the GitOps container. GITOPS-4226

- Before this update, attempts to connect to Azure DevOps with Argo CD would result in an error due to the deprecation of the **rsa-ssh** host key algorithm by the Azure DevOps Repository service. This update fixes the issue by providing support for the **rsa-ssh** host key algorithms during the communication process between Argo CD and Azure DevOps Repository service. GITOPS-4543

- Before this update, the **ignoreDifferences** sync option in Argo CD did not work for array fields. This update fixes the issue by modifying the merge strategy of the **ignoreDifferences** sync option used in the upstream project to handle array fields. As a result, the sync option now functions correctly by allowing users to ignore specific elements in the array during sync. GITOPS-2962

- Before this update, users could not create custom resources for Argo CD from the **Add** page on the **Developer** perspective of the Red Hat OpenShift GitOps web console. This issue has been observed from Red Hat OpenShift GitOps 1.10 and later releases. This update fixes the issue

because Operator-backed resources with the correct versions are included in the **ClusterServiceVersion** manifest file. GITOPS-4513

1.15. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.4

Red Hat OpenShift GitOps 1.10.4 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.15.1. Errata updates

1.15.1.1. RHSA-2024:1700 - Red Hat OpenShift GitOps 1.10.4 security update advisory

Issued: 2024-04-08

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1700

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.16. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.3

Red Hat OpenShift GitOps 1.10.3 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.16.1. Errata updates

1.16.1.1. RHSA-2024:1345 - Red Hat OpenShift GitOps 1.10.3 security update advisory

Issued: 2024-03-15

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024:1345

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.16.2. Fixed issues

Before this update, due to the incorrect filtering of URL protocols in the Argo CD application summary component, an attacker could use cross-site scripting with permission to edit the application. This update fixes the issue by upgrading the Argo CD version to 2.8.12, which patches this vulnerability. GITOPS-4209

1.17. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.2

Red Hat OpenShift GitOps 1.10.2 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.17.1. Errata updates

1.17.1.1. RHSA-2024-0692 - Red Hat OpenShift GitOps 1.10.2 security update advisory

Issued: 2024-02-05

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2024-0692

If you have installed the Red Hat OpenShift GitOps Operator, view the container images in this release by running the following command:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-operators
```

1.18. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.1

Red Hat OpenShift GitOps 1.10.1 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.18.1. Errata updates

1.18.1.1. RHSA-2023:6220 - Red Hat OpenShift GitOps 1.10.1 security update advisory

Issued: 2023-10-31

The list of security fixes that are included in this release is documented in the following advisory:

- RHSA-2023:6220

If you have installed the Red Hat OpenShift GitOps Operator in the default namespace, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-gitops-operator
```

1.19. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.10.0

Red Hat OpenShift GitOps 1.10.0 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.19.1. Errata updates

1.19.1.1. RHSA-2023:5407 and RHEA-2023:5408 - Red Hat OpenShift GitOps 1.10.0 security update advisory

Issued: 2023-09-29

The list of security fixes and enhancements that are included in this release is documented in the following advisories:

- RHSA-2023:5407
- RHEA-2023:5408

If you have installed the Red Hat OpenShift GitOps Operator in the default namespace, run the following command to view the container images in this release:

```
$ oc describe deployment gitops-operator-controller-manager -n openshift-gitops-operator
```

1.19.2. New features

The current release adds the following improvements:

- With this update, the Argo CD CRD API version is upgraded from **v1alpha1** to **v1beta1** to accomodate the breaking changes resulting from the deprecation of **.spec.dex** and certain **.spec.sso** fields. To streamline the automatic migration of existing **v1alpha1** Argo CD CRs to **v1beta1**, conversion webhook support is implemented. GITOPS-3040

NOTE

By default, the conversion webhook is enabled only for OLM-installed Operators. For non-OLM installations of the Operator, enabling the webhook is optional. However, without conversion webhook support, you have to manually migrate any existing Argo CD **v1alpha1** CRs to **v1beta1**.

- With this update, the Red Hat OpenShift GitOps Operator deploys three monitoring dashboards in the Administrator perspective of the web console. The three dashboards are **GitOps Overview**, **GitOps Components**, and **GitOps gRPC**. To access these dashboards, go to **Observe → Monitoring**. GITOPS-1767

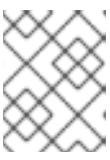
NOTE

Disabling or changing the content of the dashboards is not supported.

- Previously, timestamps were presented in a Unix epoch format. With this update, the timestamps are changed to RFC3339 format, for example: 2023-06-27T07:12:48-04:00, to improve overall readability. GITOPS-2898

- With this update, the default Argo CD instance in the **openshift-gitops** namespace has restricted permissions for non-admin users by default. This improves security because non-admin users no longer have access to sensitive information. However, as an administrator, you can set permissions and grant non-admin users access to the resources managed by the default **openshift-gitops** Argo CD instance by configuring your Argo CD RBAC. This change only applies to the default **openshift-gitops** Argo CD instance. GITOPS-3032

- With this update, the default installation namespace for Red Hat OpenShift GitOps Operator is changed to its own namespace called **openshift-gitops-operator**. You can still choose the old default installation namespace, **openshift-operators**, through a drop-down menu available in the OperatorHub UI at installation time. You can also enable cluster monitoring on the new namespace by selecting the check box, which makes the Operator's performance metrics accessible within the OpenShift Container Platform web console. GITOPS-3073



NOTE

The Red Hat OpenShift GitOps Operator's metrics are only available when the Operator is installed in the default namespace, **openshift-gitops-operator**.

- With this update, the Red Hat OpenShift GitOps Operator exports custom metrics that allow you to track the performance of the Operator. The following are the exported metrics:
  - **active_argocd_instances_total**: This shows the number of Argo CD instances currently managed across the cluster.
  - **active_argocd_instances_by_phase{phase="<_PHASE>"}**: This shows the number of Argo CD instances in a given phase, such as pending, available, among others.
  - **active_argocd_instance_reconciliation_count{namespace="<_YOUR-DEFINED-NAMESPACE>"}**: This shows the number of times the instance in a given namespace is reconciled.
  - **controller_runtime_reconcile_time_seconds_per_instance{namespace="<_YOUR-DEFINED-NAMESPACE>"}**: This metric displays the distribution of reconciliation cycles by their duration for the instance in a given namespace.
    To access these metrics, go to the **Observe** tab on the web console, and run queries against the monitoring stack. GITOPS-2645

NOTE

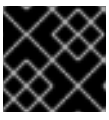
You need to install the Red Hat OpenShift GitOps Operator in the default **openshift-gitops-operator** namespace with monitoring enabled to have these metrics automatically available.

- Before this update, there was no option for choosing an algorithm for distributing the destination clusters equally across the different application controller shards. Now, you can set the sharding algorithm to the **round-robin** parameter, which distributes clusters equally across the different application controller shards so that the synchronization load is spread equally among the shards. GITOPS-3288

IMPORTANT

The **round-robin** sharding algorithm is a Technology Preview feature.

- Before this update, there was no option for scaling the application controller replicas dynamically. Now, you can dynamically scale the number of application controllers based on the number of clusters managed by each application controller. GITOPS-3287



IMPORTANT

Dynamic scaling of shards is a Technology Preview feature.

Additional resources

- Dynamically scale the Argo CD application controller with Red Hat OpenShift GitOps 1.10.0

1.19.3. Deprecated and removed features

- With this release, the following deprecated **sso** and **dex** fields are removed from Argo CD CR:
  - The **.spec.sso.image**, **.spec.sso.version**, **.spec.sso.resources**, and **.spec.sso.verifyTLS** fields for keycloak SSO configurations

- The **.spec.dex** fields, along with **DISABLE_DEX** environment variable Additionally, the **.status.dex** and **.status.ssoConfig** fields are also removed, and a new status field, **.status.sso**, is introduced. The new field reflects the workload status of the SSO provider (dex or keycloak) configured through the **.spec.sso.provider** field. GITOPS-2473

IMPORTANT

To configure dex or keycloak SSO, use the equivalent fields under **.spec.sso**.

- With this update, the deprecated **.spec.resourceCustomizations** field is removed from Argo CD CR. Bug fixes and support are only provided through the end of the Red Hat OpenShift GitOps v1.9 lifecycle. As an alternative to **.spec.resourceCustomizations**, you can use **.spec.resourceHealthChecks**, **.spec.resourceIgnoreDifferences**, and **.spec.resourceActions** fields instead. GITOPS-3041

IMPORTANT

To prevent data loss during upgrade to Red Hat OpenShift GitOps Operator v1.10.0, ensure that you backup **.spec.resourceCustomization** value if it is used in your Argo CD CRs.

- With this update, the deprecated legacy Configuration Management Plugins (CMPs) feature, specified in the **argocd-cm** config map or the Operator through the **.spec.configManagementPlugins** field in Argo CD CR, has been removed in Argo CD v2.8. To continue using your legacy plugins, consider migrating them to the new sidecar available in the Operator through the **.spec.repo.sidecarContainers** field in Argo CD CR. GITOPS-3462

1.19.4. Fixed issues

The following issues have been resolved in the current release:

- Before this update, there were vulnerabilities on Redis. This update fixes the issue by upgrading Redis to the latest version of **registry.redhat.io/rhel-8/redis-6**. GITOPS-3069

- Before this update, users were facing an "x509: certificate signed by unknown authority" error when using scmProvider with GitLab. This update fixes the issue by adding support for the **Insecure** flag for scmProvider with GitLab, and an option for mounting TLS certificate on the applicationSet controller. This certificate can then be utilized for scmProvider interactions with GitLab. GITOPS-3107