Red Hat OpenShift GitOps 1.11

Release notes

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

Last Updated: 2023-12-22
Red Hat OpenShift GitOps 1.11 Release notes

Highlights of what is new and what has changed with this OpenShift GitOps release
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 OPENSIFT GITOPS RELEASE NOTES ........................................... 3
   1.1. COMPATIBILITY AND SUPPORT MATRIX ............................................. 3
      1.1.1. Technology Preview features ................................................... 4
   1.2. MAKING OPEN SOURCE MORE INCLUSIVE ........................................ 4
   1.3. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.11.0 .................... 4
      1.3.1. New features ............................................................................. 5
      1.3.2. Fixed issues ............................................................................. 5
   1.4. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.10.1 .................... 5
      1.4.1. Errata updates ........................................................................... 5
         1.4.1.1. RHSA-2023:6220 - Red Hat OpenShift GitOps 1.10.1 security update advisory
   1.5. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.10.0 .................... 6
      1.5.1. Errata updates ........................................................................... 6
         1.5.1.1. RHSA-2023:5407 and RHEA-2023:5408 - Red Hat OpenShift GitOps 1.10.0 security update advisory
   1.6. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.9.3 ....................... 9
      1.6.1. Errata updates ........................................................................... 9
         1.6.1.1. RHSA-2023:7345 - Red Hat OpenShift GitOps 1.9.3 security update advisory
   1.7. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.9.2 ....................... 9
      1.7.1. Errata updates ........................................................................... 9
         1.7.1.1. RHSA-2023:5029 - Red Hat OpenShift GitOps 1.9.2 security update advisory
   1.8. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.9.1 ....................... 10
      1.8.1. Errata updates .......................................................................... 10
         1.8.1.1. RHSA-2023:3591 and RHBA-2023:4117 - Red Hat OpenShift GitOps 1.9.1 security update advisory
      1.8.2. New features ............................................................................. 10
      1.8.3. Fixed issues ............................................................................. 10
   1.9. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.9.0 ....................... 11
      1.9.1. Errata updates .......................................................................... 11
         1.9.1.1. RHSA-2023:3557 - Red Hat OpenShift GitOps 1.9.0 security update advisory
      1.9.2. New features ............................................................................. 11
      1.9.3. Deprecated and removed features .............................................. 11
      1.9.4. Fixed issues ............................................................................. 12
      1.9.5. Known issues .......................................................................... 12
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.

<table>
<thead>
<tr>
<th>OpenShift GitOps Component Versions</th>
<th>OpenShift Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version</strong></td>
<td><strong>kam</strong></td>
</tr>
<tr>
<td>1.11.0</td>
<td>0.0.51</td>
</tr>
<tr>
<td>1.10.0</td>
<td>0.0.50</td>
</tr>
</tbody>
</table>
1.9.0
0.0.49
3.11.2
5.0.1
2.7.2
1.5.0
NA
2.35.1
7.5.1
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

<table>
<thead>
<tr>
<th>Feature</th>
<th>TP in Red Hat OpenShift GitOps versions</th>
<th>GA in Red Hat OpenShift GitOps versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Argo Rollouts</td>
<td>1.9.0</td>
<td>NA</td>
</tr>
<tr>
<td>ApplicationSet Progressive Rollout Strategy</td>
<td>1.8.0</td>
<td>NA</td>
</tr>
<tr>
<td>Multiple sources for an application</td>
<td>1.8.0</td>
<td>NA</td>
</tr>
<tr>
<td>Argo CD applications in non-control plane namespaces</td>
<td>1.7.0</td>
<td>NA</td>
</tr>
<tr>
<td>Argo CD Notifications controller</td>
<td>1.6.0</td>
<td>NA</td>
</tr>
<tr>
<td>The Red Hat OpenShift GitOps Environments page in the Developer perspective of the OpenShift Container Platform web console</td>
<td>1.1.0</td>
<td>NA</td>
</tr>
</tbody>
</table>

### 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 1.11.0

Red Hat OpenShift GitOps 1.11.0 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.
1.3.1. 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.

1.3.2. 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

1.4. 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.

1.4.1. Errata updates

1.4.1.1. 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
```

### 1.5. 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.

#### 1.5.1. Errata updates

**1.5.1.1. 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
```

#### 1.5.2. 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 accommodate 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**

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**

### Additional resources

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

### 1.5.3. 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**

### 1.5.4. 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

1.6. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.9.3

Red Hat OpenShift GitOps 1.9.3 is now available on OpenShift Container Platform 4.12, 4.13, and 4.14.

1.6.1. Errata updates

1.6.1.1. RHSA-2023:7345 - Red Hat OpenShift GitOps 1.9.3 security update advisory

Issued: 2023-11-20

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

- RHSA-2023:7345

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

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

1.7. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.9.2

Red Hat OpenShift GitOps 1.9.2 is now available on OpenShift Container Platform 4.12 and 4.13.

1.7.1. Errata updates

1.7.1.1. RHSA-2023:5029 - Red Hat OpenShift GitOps 1.9.2 security update advisory

Issued: 2023-09-08

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

- RHSA-2023:5029

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

The following issue has been resolved in the current release:

- Before this update, an old Redis image version was used when deploying the Red Hat OpenShift
1.8. RELEASE NOTES FOR RED HAT OPENSSHIFT GITOPS 1.9.1

Red Hat OpenShift GitOps 1.9.1 is now available on OpenShift Container Platform 4.12 and 4.13.

1.8.1. Errata updates

1.8.1.1. RHSA-2023:3591 and RHBA-2023:4117 - Red Hat OpenShift GitOps 1.9.1 security update advisory

Issued: 2023-07-17

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

- RHSA-2023:3591
- RHBA-2023:4117

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. New features

The current release adds the following improvements:

- With this update, the bundled Argo CD has been updated to version 2.7.6.

1.8.3. Fixed issues

The following issues have been resolved in the current release:

- Before this update, Argo CD was becoming unresponsive when there was an increase in namespaces and applications. This update fixes the issue by removing a deadlock. Deadlock occurs when two functions are competing for resources. Now, you should not experience crashes or unresponsiveness when there is an increase in namespaces or applications. GITOPS-2782

- Before this update, the Argo CD application controller resource could suddenly stop working when resynchronizing applications. This update fixes the issue by adding logic to prevent a cluster cache deadlock. Now, you should not experience the deadlock situation, and applications should resynchronize successfully. GITOPS-2880

- Before this update, there was a mismatch in the RSA key for known hosts in the argocd-ssh-known-hosts-cm config map. This update fixes the issue by matching the RSA key with the upstream project. Now, you can use the default RSA keys on default deployments. GITOPS-3042

- Before this update, the reconciliation timeout setting in the argocd-cm config map was not being correctly applied to the Argo CD application controller resource. This update fixes the
issue by correctly reading and applying the reconciliation timeout setting from the `argocd-cm` config map. Now, you can modify the reconciliation timeout value from the `AppSync` setting without a problem. GITOPS-2810

1.9. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.9.0

Red Hat OpenShift GitOps 1.9.0 is now available on OpenShift Container Platform 4.12 and 4.13.

1.9.1. Errata updates

1.9.1.1. RHSA-2023:3557 - Red Hat OpenShift GitOps 1.9.0 security update advisory

Issued: 2023-06-09

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

- RHSA-2023:3557

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
```

1.9.2. New features

The current release adds the following improvements:

- With this update, you can use a custom `must-gather` tool to collect diagnostic information for project-level resources, cluster-level resources, and Red Hat OpenShift GitOps components. This tool provides the debugging information about the cluster associated with Red Hat OpenShift GitOps, which you can share with the Red Hat Support team for analysis. GITOPS-2797

- With this update, you can add support to progressive delivery using Argo Rollouts. Currently, the supported traffic manager is only Red Hat OpenShift Service Mesh. GITOPS-959

IMPORTANT

Argo Rollouts is a Technology Preview feature.

Additional resources

- Using Argo Rollouts

1.9.3. Deprecated and removed features

- In Red Hat OpenShift GitOps 1.7.0, the `.spec.resourceCustomizations` parameter was deprecated. The deprecated `.spec.resourceCustomizations` parameter is planned to be removed in the upcoming Red Hat OpenShift GitOps GA v1.10.0 release. You can use the new formats `spec.ResourceHealthChecks`, `spec.ResourceIgnoreDifferences`, and `spec.ResourceActions` instead. GITOPS-2890
• With this update, the support for the following deprecated sso and dex fields extends until the upcoming Red Hat OpenShift GitOps GA v1.10.0 release:
  o The .spec.sso.image, .spec.sso.version, .spec.sso.resources, and .spec.sso.verifyTLS fields.
  o The .spec.dex parameter along with DISABLE_DEX.

The deprecated previous sso and dex fields were earlier scheduled for removal in the Red Hat OpenShift GitOps v1.9.0 release but are now planned to be removed in the upcoming Red Hat OpenShift GitOps GA v1.10.0 release. GITOPS-2904

1.9.4. Fixed issues

The following issues have been resolved in the current release:

• Before this update, when the argocd-server-tls secret was updated with a new certificate Argo CD was not always picking up this secret. As a result, the old expired certificate was presented. This update fixes the issue with a new GetCertificate function and ensures that the latest version of certificates is in use. When adding new certificates, now Argo CD picks them up automatically without the user having to restart the argocd-server pod. GITOPS-2375

• Before this update, when enforcing GPG signature verification against a targetRevision integer pointing to a signed Git tag, users got a Target revision in Git is not signed error. This update fixes the issue and lets users enforce GPG signature verification against signed Git tags. GITOPS-2418

• Before this update, users could not connect to Microsoft Team Foundation Server (TFS) type Git repositories through Argo CD deployed by the Operator. This update fixes the issue by updating the Git version to 2.39.3 in the Operator. GITOPS-2768

• Before this update, when the Operator was deployed and running with the High availability (HA) feature enabled, setting resource limits under the .spec.ha.resources field did not affect Redis HA pods. This update fixes the reconciliation by adding checks in the Redis reconciliation code. These checks ensure whether the spec.ha.resources field in the Argo CD custom resource (CR) is updated. When the Argo CD CR is updated with new CPU and memory requests or limit values for HA, now these changes are applied to the Redis HA pods. GITOPS-2404

• Before this update, if a namespace-scoped Argo CD instance was managing multiple namespaces by using the managed-by label and one of those managed namespaces was in a Terminating state, the Argo CD instance could not deploy resources to all other managed namespaces. This update fixes the issue by enabling the Operator to remove the managed-by label from any previously managed now terminating namespace. Now, a terminating namespace managed by a namespace-scoped Argo CD instance does not block the deployment of resources to other managed namespaces. GITOPS-2627

1.9.5. Known issues

• Currently, the Argo CD does not read the Transport Layer Security (TLS) certificates from the path specified in the argocd-tls-certs-cm config map resulting in the x509: certificate signed by unknown authority error. Workaround: Perform the following steps:

  1. Add the SSL_CERT_DIR environment variable:

     Example Argo CD custom resource
Create an empty config map in the namespace where the subscription for your Operator exists and include the following label:

Example config map

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd
  labels:
    example: repo
spec:
  # ...
  repo:
    env:
      - name: SSL_CERT_DIR
        value: /tmp/sslcertdir
    volumeMounts:
      - name: ssl
        mountPath: /tmp/sslcertdir
    volumes:
      - name: ssl
        configMap:
          name: user-ca-bundle
          # ...
```

2. Create an empty config map in the namespace where the subscription for your Operator exists and include the following label:

Example config map

```yaml
apiVersion: v1
kind: ConfigMap
metadata:
  name: user-ca-bundle
  labels:
    config.openshift.io/inject-trusted-cabundle: "true"
```

1. Name of the config map.
2. Requests the Cluster Network Operator to inject the merged bundle.

After creating this config map, the `user-ca-bundle` content from the `openshift-config` namespace automatically gets injected into this config map, even merged with the system ca-bundle. GITOPS-1482

Additional resources

- Injecting a custom CA certificate