Red Hat OpenShift GitOps 1.10

Release notes

Highlights of what is new and what has changed with this OpenShift GitOps release
Red Hat OpenShift GitOps 1.10 Release notes

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

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 OPENSHEF GITOPS RELEASE NOTES

- 1.1. COMPATIBILITY AND SUPPORT MATRIX ........................................ 4
- 1.1.1. Technology Preview features .............................................. 4
- 1.2. MAKING OPEN SOURCE MORE INCLUSIVE .................................... 5
- 1.3. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.10.1 ............... 5
- 1.3.1. Errata updates ....................................................................... 6
- 1.3.1.1. RHSA-2023:6220 - Red Hat OpenShift GitOps 1.10.1 security update advisory ........................................ 6
- 1.4. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.10.0 ............... 6
- 1.4.1. Errata updates ....................................................................... 6
- 1.4.1.1. RHSA-2023:5407 and RHEA-2023:5408 - Red Hat OpenShift GitOps 1.10.0 security update advisory ......................... 6
- 1.4.2. New features ......................................................................... 6
- 1.4.3. Deprecated and removed features ......................................... 8
- 1.4.4. Fixed issues .......................................................................... 9
- 1.5. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.9.3 ............... 9
- 1.5.1. Errata updates ....................................................................... 9
- 1.5.1.1. RHSA-2023:7345 - Red Hat OpenShift GitOps 1.9.3 security update advisory ........................................ 9
- 1.6. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.9.2 ............... 9
- 1.6.1. Errata updates ....................................................................... 9
- 1.6.1.1. RHSA-2023:5029 - Red Hat OpenShift GitOps 1.9.2 security update advisory ........................................ 9
- 1.6.2. Fixed issues .......................................................................... 10
- 1.7. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.9.1 ............... 10
- 1.7.1. Errata updates ....................................................................... 10
- 1.7.1.1. RHSA-2023:3591 and RHBA-2023:4117 - Red Hat OpenShift GitOps 1.9.1 security update advisory ......................... 10
- 1.7.2. New features ......................................................................... 10
- 1.7.3. Fixed issues .......................................................................... 10
- 1.8. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.9.0 ............... 11
- 1.8.1. Errata updates ....................................................................... 11
- 1.8.1.1. RHSA-2023:3557 - Red Hat OpenShift GitOps 1.9.0 security update advisory ........................................ 11
- 1.8.2. New features ......................................................................... 11
- 1.8.3. Deprecated and removed features ......................................... 12
- 1.8.4. Fixed issues .......................................................................... 12
- 1.8.5. Known issues ....................................................................... 13
- 1.9. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.8.6 ............... 14
- 1.9.1. Errata updates ....................................................................... 14
- 1.9.1.1. RHSA-2023:6788 - Red Hat OpenShift GitOps 1.8.6 security update advisory ........................................ 14
- 1.10. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.8.5 ............. 14
- 1.10.1. Errata updates ..................................................................... 14
- 1.10.1.1. RHSA-2023:5030 - Red Hat OpenShift GitOps 1.8.5 security update advisory ........................................ 14
- 1.10.2. Fixed issues ....................................................................... 14
- 1.11. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.8.4 ............. 15
- 1.11.1. New features ...................................................................... 15
- 1.11.2. Fixed issues ....................................................................... 15
- 1.11.3. Known issues ..................................................................... 15
- 1.12. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.8.3 ............. 15
- 1.12.1. Errata updates ..................................................................... 15
- 1.12.1.1. RHBA-2023:3206 and RHSA-2023:3229 - Red Hat OpenShift GitOps 1.8.3 security update advisory ......................... 16
- 1.12.2. Fixed issues ....................................................................... 16
- 1.13. RELEASE NOTES FOR RED HAT OPENSHEF GITOPS 1.8.2 ............. 16
- 1.13.1. Fixed issues ....................................................................... 16
<table>
<thead>
<tr>
<th>Section</th>
<th>Red Hat OpenShift GitOps 1.7.4 Release Notes</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.14.1.</td>
<td>Errata updates</td>
<td>17</td>
</tr>
<tr>
<td>1.14.1.1.</td>
<td>RHSA-2023:1452 - Red Hat OpenShift GitOps 1.8.1 security update advisory</td>
<td>17</td>
</tr>
<tr>
<td>1.15.</td>
<td>RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.8.0</td>
<td>17</td>
</tr>
<tr>
<td>1.15.1.</td>
<td>New features</td>
<td>17</td>
</tr>
<tr>
<td>1.15.2.</td>
<td>Fixed issues</td>
<td>18</td>
</tr>
<tr>
<td>1.15.3.</td>
<td>Known issues</td>
<td>18</td>
</tr>
<tr>
<td>1.16.</td>
<td>RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.4</td>
<td>19</td>
</tr>
<tr>
<td>1.16.1.</td>
<td>Errata updates</td>
<td>19</td>
</tr>
<tr>
<td>1.16.1.1.</td>
<td>RHSA-2023:1454 - Red Hat OpenShift GitOps 1.7.4 security update advisory</td>
<td>19</td>
</tr>
<tr>
<td>1.17.</td>
<td>RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.3</td>
<td>19</td>
</tr>
<tr>
<td>1.17.1.</td>
<td>Errata updates</td>
<td>19</td>
</tr>
<tr>
<td>1.17.1.1.</td>
<td>RHSA-2023:1454 - Red Hat OpenShift GitOps 1.7.3 security update advisory</td>
<td>19</td>
</tr>
<tr>
<td>1.18.</td>
<td>RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.1</td>
<td>19</td>
</tr>
<tr>
<td>1.18.1.</td>
<td>Errata updates</td>
<td>19</td>
</tr>
<tr>
<td>1.18.1.1.</td>
<td>RHSA-2023:0467 - Red Hat OpenShift GitOps 1.7.1 security update advisory</td>
<td>19</td>
</tr>
<tr>
<td>1.19.</td>
<td>RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.0</td>
<td>20</td>
</tr>
<tr>
<td>1.19.1.</td>
<td>New features</td>
<td>20</td>
</tr>
<tr>
<td>1.19.2.</td>
<td>Fixed issues</td>
<td>21</td>
</tr>
<tr>
<td>1.19.3.</td>
<td>Known issues</td>
<td>22</td>
</tr>
</tbody>
</table>
CHAPTER 1. RED HAT OPENS SHIFT 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>kam</td>
</tr>
<tr>
<td>-------------</td>
<td>-----</td>
</tr>
<tr>
<td>1.10.0</td>
<td>0.0.50 TP</td>
</tr>
<tr>
<td>1.9.0</td>
<td>0.0.49 TP</td>
</tr>
</tbody>
</table>
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>The custom <strong>must-gather</strong> tool</td>
<td>1.9.0</td>
<td>NA</td>
</tr>
<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 <strong>Environments</strong> page in the Developer perspective of the OpenShift Container Platform web console</td>
<td>1.1.0</td>
<td>NA</td>
</tr>
</tbody>
</table>

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

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

1.3.1. Errata updates

1.3.1.1. 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:

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

1.4. 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.

1.4.1. Errata updates

1.4.1.1. 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:

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

1.4.2. 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.

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.

- 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.

- 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.

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

1.4.3. 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
1.4.4. 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**

1.5. 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.

1.5.1. Errata updates

1.5.1.1. 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
```

1.6. 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.

1.6.1. Errata updates

1.6.1.1. 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:
1.6.2. 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 GitOps Operator, which resulted in vulnerabilities. This update fixes the vulnerabilities on Redis by upgrading it to the latest version of the registry.redhat.io/rhel-8/redis-6 image. GITOPS-3069

1.7. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.9.1

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

1.7.1. Errata updates

1.7.1.1. 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:

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

1.7.2. New features

The current release adds the following improvements:

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

1.7.3. 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

1.8. 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.

1.8.1. Errata updates

1.8.1.1. 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
```

1.8.2. 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

**IMPORTANT**

The custom `must-gather` tool is a Technology Preview feature.

- 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
1.8.3. 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:
  - The `.spec.sso.image`, `.spec.sso.version`, `.spec.sso.resources`, and `.spec.sso.verifyTLS` fields.
  - 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

1.8.4. 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
1.8.5. 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**

   ```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

1.9. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.8.6

Red Hat OpenShift GitOps 1.8.6 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.9.1. Errata updates

1.9.1.1. RHSA-2023:6788 - Red Hat OpenShift GitOps 1.8.6 security update advisory

Issued: 2023-11-08

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

- RHSA-2023:6788

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:

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

1.10. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.8.5

Red Hat OpenShift GitOps 1.8.5 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.10.1. Errata updates

1.10.1.1. RHSA-2023:5030 - Red Hat OpenShift GitOps 1.8.5 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-2023:5030

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

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

1.10.2. Fixed issues

The following issue has been resolved in the current release:

- Before this update, there was a mismatch in the RSA key for known hosts in the `argocd-sshs-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-3248
1.11. RELEASE NOTES FOR RED HAT OPENShift GITOPS 1.8.4

Red Hat OpenShift GitOps 1.8.4 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.11.1. New features

The current release adds the following improvements:

- With this update, the bundled Argo CD has been updated to version 2.6.13.

1.11.2. 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. The functions competing for resources caused a deadlock. This update fixes the issue by removing the deadlock. Now, you should not experience crashes or unresponsiveness when there is an increase in namespaces or applications. GITOPS-3192

- 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, applications should resynchronize successfully. GITOPS-3052

- 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-3144

- Before this update, an old Redis image version was used when deploying the Red Hat OpenShift GitOps Operator, which resulted in vulnerabilities. This update fixes the vulnerabilities on Redis by upgrading it to the latest version of the `registry.redhat.io/rhel-8/redis-6` image. GITOPS-3069

- 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. Now, you can set the `Force HTTP basic auth` flag during repository configurations to connect with the TFS type Git repositories. GITOPS-1315

1.11.3. Known issues

- Currently, Red Hat OpenShift GitOps 1.8.4 is not available in the `latest` channel of OpenShift Container Platform 4.10 and 4.11. The `latest` channel is taken by GitOps 1.9.z, which is only released on OpenShift Container Platform 4.12 and later versions. As a workaround, switch to the `gitops-1.8` channel to get the new update. GITOPS-3158

1.12. RELEASE NOTES FOR RED HAT OPENShift GITOPS 1.8.3

Red Hat OpenShift GitOps 1.8.3 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.12.1. Errata updates
1.12.1. RHBA-2023:3206 and RHSA-2023:3229 - Red Hat OpenShift GitOps 1.8.3 security update advisory

Issued: 2023-05-18

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

- RHBA-2023:3206
- RHSA-2023:3229

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
```

1.12.2. Fixed issues

- Before this update, when Autoscale was enabled and the horizontal pod autoscaler (HPA) controller tried to edit the replica settings in server deployment, the Operator overwrote it. In addition, any changes specified to the autoscaler parameters were not propagated correctly to the HPA on the cluster. This update fixes the issue. Now the Operator reconciles on replica drift only if Autoscale is disabled and the HPA parameters are updated correctly. GITOPS-2629

1.13. RELEASE NOTES FOR RED HAT OPENSOURCE GITOPS 1.8.2

Red Hat OpenShift GitOps 1.8.2 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.13.1. Fixed issues

The following issues have been resolved in the current release:

- Before this update, when you configured Dex using the .spec.dex parameter and tried to log in to the Argo CD UI by using the LOG IN VIA OPENSHIFT option, you were not able to log in. This update fixes the issue.

  IMPORTANT

  The spec.dex parameter in the ArgoCD CR is deprecated. In a future release of Red Hat OpenShift GitOps v1.9, configuring Dex using the spec.dex parameter in the ArgoCD CR is planned to be removed. Consider using the .spec.sso parameter instead. See "Enabling or disabling Dex using .spec.sso". GITOPS-2761

- Before this update, the cluster and kam CLI pods failed to start with a new installation of Red Hat OpenShift GitOps v1.8.0 on the OpenShift Container Platform 4.10 cluster. This update fixes the issue and now all pods run as expected. GITOPS-2762

1.14. RELEASE NOTES FOR RED HAT OPENSOURCE GITOPS 1.8.1

Red Hat OpenShift GitOps 1.8.1 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.
1.14.1. Errata updates

1.14.1.1. RHSA-2023:1452 - Red Hat OpenShift GitOps 1.8.1 security update advisory

Issued: 2023-03-23

The list of security fixes that are included in this release is documented in the RHSA-2023:1452 advisory.

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

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

1.15. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.8.0

Red Hat OpenShift GitOps 1.8.0 is now available on OpenShift Container Platform 4.10, 4.11, 4.12, and 4.13.

1.15.1. New features

The current release adds the following improvements:

- With this update, you can add support for the ApplicationSet Progressive Rollout Strategy feature. Using this feature, you can enhance the ArgoCD ApplicationSet resource to embed a rollout strategy for a progressive application resource update after you modify the ApplicationSet spec or Application templates. When you enable this feature, applications are updated in a declarative order instead of simultaneously. GITOPS-956

  IMPORTANT

  ApplicationSet Progressive Rollout Strategy is a Technology Preview feature.

- With this update, the Application environments page in the Developer perspective of the OpenShift Container Platform web console is decoupled from the Red Hat OpenShift GitOps Application Manager command-line interface (CLI), kam. You do not have to use the kam CLI to generate Application Environment manifests for the environments to show up in the Developer perspective of the OpenShift Container Platform web console. You can use your own manifests, but the environments must still be represented by namespaces. In addition, specific labels and annotations are still needed. GITOPS-1785

- With this update, the Red Hat OpenShift GitOps Operator and the kam CLI are now available to use on ARM architecture on OpenShift Container Platform. GITOPS-1688

  IMPORTANT

  spec.sso.provider: keycloak is not yet supported on ARM.

- With this update, you can enable workload monitoring for specific Argo CD instances by setting the .spec.monitoring.enabled flag value to true. As a result, the Operator creates a PrometheusRule object that contains alert rules for each Argo CD component. These alert rules trigger an alert when the replica count of the corresponding component has drifted from the desired state for a certain amount of time. The Operator will not overwrite the changes made to the PrometheusRule object by the users. GITOPS-2459
With this update, you can pass command arguments to the repo server deployment using the Argo CD CR. GITOPS-2445

For example:

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd
spec:
  repo:
    extraRepoCommandArgs:
      - --max.combined.directory.manifests.size
      - 10M
```

### 1.15.2. Fixed issues

The following issues have been resolved in the current release:

- Before this update, you could set the `ARGOCD_GIT_MODULES_ENABLED` environment variable only on the `openshift-gitops-repo-server` pod and not on the `ApplicationSet Controller` pod. As a result, when using the Git generator, Git submodules were cloned during the generation of child applications because the variable was missing from the `ApplicationSet Controller` environment. In addition, if the credentials required to clone these submodules were not configured in ArgoCD, the application generation failed. This update fixes the issue; you can now add any environment variables such as `ARGOCD_GIT_MODULES_ENABLED` to the `ApplicationSet Controller` pod using the Argo CD CR. The `ApplicationSet Controller` pod then successfully generates child applications from the cloned repository and no submodule is cloned in the process. GITOPS-2399

For example:

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd
labels:
  example: basic
spec:
  applicationSet:
    env:
      - name: ARGOMODULES_ENABLED
        value: "true"
```

- Before this update, while installing the Red Hat OpenShift GitOps Operator v1.7.0, the default `argocd-cm.yml` config map file created for authenticating Dex contained the base64-encoded client secret in the format of a `key:value` pair. This update fixes this issue by not storing the client secret in the default `argocd-cm.yml` config map file. Instead, the client secret is inside an `argocd-secret` object now, and you can reference it inside the configuration map as a secret name. GITOPS-2570

### 1.15.3. Known issues

- When you deploy applications using your manifests without using the `kam` CLI and view the applications in the `Application environments` page in the `Developer` perspective of the OpenShift Container Platform web console, the Argo CD URL to the corresponding application
1.16. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.4

Red Hat OpenShift GitOps 1.7.4 is now available on OpenShift Container Platform 4.10, 4.11, and 4.12.

1.16.1. Errata updates

1.16.1.1. RHSA-2023:1454 - Red Hat OpenShift GitOps 1.7.4 security update advisory

Issued: 2023-03-23

The list of security fixes that are included in this release is documented in the RHSA-2023:1454 advisory.

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
```

1.17. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.3

Red Hat OpenShift GitOps 1.7.3 is now available on OpenShift Container Platform 4.10, 4.11, and 4.12.

1.17.1. Errata updates

1.17.1.1. RHSA-2023:1454 - Red Hat OpenShift GitOps 1.7.3 security update advisory

Issued: 2023-03-23

The list of security fixes that are included in this release is documented in the RHSA-2023:1454 advisory.

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
```

1.18. RELEASE NOTES FOR RED HAT OPENSHIFT GITOPS 1.7.1

Red Hat OpenShift GitOps 1.7.1 is now available on OpenShift Container Platform 4.10, 4.11, and 4.12.

1.18.1. Errata updates

1.18.1.1. RHSA-2023:0467 - Red Hat OpenShift GitOps 1.7.1 security update advisory

Issued: 2023-01-25

The list of security fixes that are included in this release is documented in the RHSA-2023:0467 advisory.

If you have installed the Red Hat OpenShift GitOps Operator, run the following command to view the container images in this release:
1.19. RELEASE NOTES FOR RED HAT OPENSIFT GITOPS 1.7.0

Red Hat OpenShift GitOps 1.7.0 is now available on OpenShift Container Platform 4.10, 4.11, and 4.12.

1.19.1. New features

The current release adds the following improvements:

- With this update, you can add environment variables to the Notifications controller. GITOPS-2313

- With this update, the default nodeSelector "kubernetes.io/os": "linux" key-value pair is added to all workloads such that they only schedule on Linux nodes. In addition, any custom node selectors are added to the default and take precedence if they have the same key. GITOPS-2215

- With this update, you can set custom node selectors in the Operator workloads by editing their GitopsService custom resource. GITOPS-2164

- With this update, you can use the RBAC policy matcher mode to select from the following options: glob (default) and regex. GITOPS-1975

- With this update, you can customize resource behavior using the following additional subkeys:

<table>
<thead>
<tr>
<th>Subkey</th>
<th>Key form</th>
<th>Mapped field in argocd-cm</th>
</tr>
</thead>
<tbody>
<tr>
<td>resourceHealthChecks</td>
<td>resource.customizations.health.&lt;group_kind&gt;</td>
<td>resource.customizations.health</td>
</tr>
<tr>
<td>resourceIgnoreDifferences</td>
<td>resource.customizations.ignore Differences.&lt;group_kind&gt;</td>
<td>resource.customizations.ignore Differences</td>
</tr>
<tr>
<td>resourceActions</td>
<td>resource.customizations.action.&lt;group_kind&gt;</td>
<td>resource.customizations.action</td>
</tr>
</tbody>
</table>

GITOPS-1561

**NOTE**

In future releases, there is a possibility to deprecate the old method of customizing resource behavior by using only resourceCustomization and not subkeys.

- With this update, to use the Environments page in the Developer perspective, you must upgrade if you are using a Red Hat OpenShift GitOps version prior to 1.7 and OpenShift Container Platform 4.15 or above. GITOPS-2415

- With this update, you can create applications, which are managed by the same control plane Argo CD instance, in any namespace in the same cluster. As an administrator, perform the following actions to enable this update:
- Add the namespace to the `.spec.sourceNamespaces` attribute for a cluster-scoped Argo CD instance that manages the application.

- Add the namespace to the `.spec.sourceNamespaces` attribute in the `AppProject` custom resource that is associated with the application.

**GITOPS-2341**

**IMPORTANT**

Argo CD applications in non-control plane namespaces is a Technology Preview feature only. Technology Preview features are not supported with Red Hat production service level agreements (SLAs) and might not be functionally complete. Red Hat does not recommend using them in production. These features provide early access to upcoming product features, enabling customers to test functionality and provide feedback during the development process.

For more information about the support scope of Red Hat Technology Preview features, see [Technology Preview Features Support Scope](#).

- With this update, Argo CD supports the Server-Side Apply feature, which helps users to perform the following tasks:
  - Manage large resources which are too big for the allowed annotation size of 262144 bytes.
  - Patch an existing resource that is not managed or deployed by Argo CD.

You can configure this feature at application or resource level. **GITOPS-2340**

### 1.19.2. Fixed issues

The following issues have been resolved in the current release:

- Before this update, Red Hat OpenShift GitOps releases were affected by an issue of Dex pods failing with `CreateContainerConfigError` error when the `anyuid` SCC was assigned to the Dex service account. This update fixes the issue by assigning a default user id to the Dex container. **GITOPS-2235**

- Before this update, Red Hat OpenShift GitOps used the RHSSO (Keycloak) through OIDC in addition to Dex. However, with a recent security fix, the certificate of RHSSO could not be validated when configured with a certificate not signed by one of the well-known certificate authorities. This update fixes the issue; you can now provide a custom certificate to verify the KeyCloak’s TLS certificate while communicating with it. In addition, you can add `rootCA` to the Argo CD custom resource `.spec.keycloak.rootCA` field. The Operator reconciles such changes and updates the `oidc.config in argocd-cm` config map with the PEM encoded root certificate. **GITOPS-2214**

Example Argo CD with Keycloak configuration:

```yaml
apiVersion: argoproj.io/v1alpha1
kind: ArgoCD
metadata:
  name: example-argocd
spec:
  sso:
    keycloak:
      rootCA: '<PEM encoded root certificate>'
```
provider: keycloak

- Before this update, the application controllers restarted multiple times due to the unresponsiveness of liveness probes. This update fixes the issue by removing the liveness probe in the `statefulset` application controller. GITOPS-2153

1.19.3. Known issues

- Before this update, the Operator did not reconcile the `mountsatoken` and `ServiceAccount` settings for the repository server. While this has been fixed, deletion of the service account does not revert to the default. GITOPS-1873

- Workaround: Manually set the `spec.repo.serviceaccountfield` to the default service account. GITOPS-2452