Cloudera Flow Management Operator for Kubernetes 3.4.1

CFM Operator Release Notes

Date published: 2024-06-11
Date modified: 2026-10-28



https://docs.cloudera.com/

Legal Notice

© Cloudera Inc. 2026. All rights reserved.

The documentation is and contains Cloudera proprietary information protected by copyright and other intellectual property rights. No license under copyright or any other intellectual property right is granted herein.

Unless otherwise noted, scripts and sample code are licensed under the Apache License, Version 2.0.

Copyright information for Cloudera software may be found within the documentation accompanying each component in a particular release.

Cloudera software includes software from various open source or other third party projects, and may be released under the Apache Software License 2.0 (“ASLv2”), the Affero General Public License version 3 (AGPLv3), or other license terms. Other software included may be released under the terms of alternative open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Cloudera software product page for more information on Cloudera software. For more information on Cloudera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cloudera reserves the right to change any products at any time, and without notice. Cloudera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cloudera.

Cloudera, Cloudera Altus, HUE, Impala, Cloudera Impala, and other Cloudera marks are registered or unregistered trademarks in the United States and other countries. All other trademarks are the property of their respective owners.

Disclaimer: EXCEPT AS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT WITH CLOUDERA, CLOUDERA DOES NOT MAKE NOR GIVE ANY REPRESENTATION, WARRANTY, NOR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH CLOUDERA TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. CLOUDERA DOES NOT WARRANT THAT CLOUDERA PRODUCTS NOR SOFTWARE WILL OPERATE UNINTERRUPTED NOR THAT IT WILL BE FREE FROM DEFECTS NOR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION NOR UNAVAILABILITY, NOR THAT IT WILL MEET ALL OF CUSTOMER’S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CLOUDERA EXPRESSLY DISCLAIMS ANY AND ALL IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, QUALITY, NON-INFRINGEMENT, TITLE, AND FITNESS FOR A PARTICULAR PURPOSE AND ANY REPRESENTATION, WARRANTY, OR COVENANT BASED ON COURSE OF DEALING OR USAGE IN TRADE.

Contents

What's new **4**
- Release 3.4.1 4
- Release 3.4.0 4
- Release 3.3.3 5
- Older releases 5
  - Release 3.3.2 6
  - Release 3.3.1 6
  - Release 3.3.0 6
  - Release 3.2.2 7
  - Release 3.2.1 7
  - Release 3.2.0 8
  - Release 3.1.0 8
  - Release 3.0.0 8
  - Release 2.11.0 9
  - Release 2.10.0 9
  - Release 2.9.1 10
  - Release 2.9.0 10
  - Release 2.8.0 11

Apache Parquet CVE-2025-30065 ..... **11**

Supported component versions **12**

System requirements **12**

What's new

Learn about the new features and notable changes throughout releases of Cloudera Flow Management Operator for Kubernetes.

Release 3.4.1

Release 3.4.1 of Cloudera Flow Management Operator for Kubernetes delivers security and functionality fixes.

Security updates

Compromised eMudhra intermediate CA removal

All affected certificates were removed from the Cloudera Flow Management Operator for Kubernetes images.

All wild card role-based access control (RBAC) permissions replaced with explicit list

Cloudera Flow Management Operator for Kubernetes now only deploys resources without wildcard RBAC, supporting security policies which block wild card permissions.

Fixed issues

CFMOP-332: SSL Context Property name mismatch

Fixes an issue where in a previous release the SSL Context property names changed, rendering Cloudera Flow Management Operator for Kubernetes unable to correctly configure the Default Node SSL Context Service.

Release 3.4.0

Release 3.4.0 of Cloudera Flow Management Operator for Kubernetes promotes the Nifi custom resource to v1, supports NiFi 2.11 images, and adds install-time namespace and role-based access control (RBAC) controls.

New features

Promotion of the Nifi custom resource to v1

The Nifi custom resource is now available at API version cfm.cloudera.com/v1, reflecting its maturity as the default version for new deployments. Version v1alpha1 remains supported for existing clusters, but new spec fields are added only to v1.

For more information, see Group, version, kind, meta.

NiFi 2.11 support

Cloudera Flow Management Operator for Kubernetes supports deploying NiFi 2.11 container images. For supported component versions, see Component versions.

Limit the namespaces the operator watches

You can configure a list of namespaces for Cloudera Flow Management Operator for Kubernetes to reconcile during installation. When you do not set this list, the operator continues to watch all namespaces, which is the default behavior.

For more information, see the watchNamespaces property in Helm chart reference.

Optional creation of operator RBAC resources

Creation of RBAC resources for the operator, including ClusterRoles, ServiceAccounts, and bindings, can be turned off at install time. You can then define a stricter RBAC model and supply the roles and service account that the operator uses.

For more information, see the rbac.create and serviceAccount.create properties in Helm chart reference.

Per-cluster Cloudera Flow Management Operator for Kubernetes user identity

As a cluster administrator, you can assign a distinct Cloudera Flow Management Operator for Kubernetes user identity to each NiFi cluster. This scopes the operator identity that performs NiFi API management in that cluster.

Deprecations and removals

Cross-namespace references

The User, UserGroup, and ProcessGroup custom resources can no longer target a NiFi cluster in a different namespace. This preserves namespace permission boundaries that cluster administrators define, so principals without access to a namespace cannot use these resources to manage NiFi clusters or flows in that namespace.

Fixed issues

CFMOP-239: Nil user ID in policy updates

The operator now guards against a nil user ID when adding or removing users from policies.

Release 3.3.3

Release 3.3.3 of Cloudera Flow Management Operator for Kubernetes introduces automatic, zero downtime certificate reload, and delivers various fixes.

New features

Automatic, zero downtime certificate reload

Cloudera Flow Management Operator for Kubernetes now configures NiFi to auto reload its default keystore and truststore. A new subshell process in the nifi container watches the node certificates created by Cloudera Flow Management Operator for Kubernetes and recompiles the keystore and truststore for NiFi to consume, without a restart of the NiFi runtime.

Fixed issues

CFMOP-31: Block changes to NiFi instance target for Users

A new validation guardrail was added to prevent the unsupported action of changing the instance target of a User custom resource.

CFMOP-268: Proxy certificate missing common name

The proxy certificate created by Cloudera Flow Management Operator for Kubernetes now contains its common name, preventing potential issues with cert-manager DNS name length validation.

CFMOP-269: Pod Security Context customization missing in v1 spec

The v1 NiFi CRD specification now contains the Pod Security Context configuration fields.

Older releases

Overview of new features, enhancements, and changed behavior introduced in earlier releases of Cloudera Flow Management Operator for Kubernetes.

Release 3.3.2

Release 3.3.2 of Cloudera Flow Management Operator for Kubernetes delivers improvements to configuring access to ProcessGroups, and on condition handling.

Improvements

Configure user/group access to ProcessGroups

You can now configure access policies on User and UserGroup resources that reference ProcessGroup custom resources. This allows for deploying a ProcessGroup and configuring access to that ProcessGroup in a single yaml update, without having to wait for NiFi to provide an identifier for the created process group.

Improved condition handling

Conditions are now always updated, even when there are unanticipated errors in the reconciliation of resources.

Release 3.3.1

Release 3.3.1 of Cloudera Flow Management Operator for Kubernetes provides two observability improvements: NiFi custom resource status conditions that report the state of operator connectedness to the target NiFi and improved error surfacing for existing offloading conditions.

Improvements

Attempting nifi-client interactions with custom authorizer

Cloudera Flow Management Operator for Kubernetes now attempts a best effort connection to the NiFi cluster when custom authorizers are configured, setting status conditions on the NiFi resource explaining when the operator has insufficient permissions to perform its API heavy management of NiFi, such as process group or SSL Context Service creation.

Surfacing error texts encountered during offloading

Any errors encountered during offloading are now surfaced in the NiFi status conditions for easier discovery.

Release 3.3.0

Learn about the new features and notable changes in release 3.3.0 of Cloudera Flow Management Operator for Kubernetes.

New features

Automatic SSL context provisioning for secure inter-cluster communication

Cloudera Flow Management Operator for Kubernetes now automatically provisions a DefaultNodeSSLContextService in the root process group of each NiFi cluster. The service uses the existing node keystore and truststore, enabling secure TLS communication between NiFi clusters managed by the same operator without requiring manual SSL configuration.

Apache Ranger authorization support for NiFi

You can now configure NiFi deployments managed by Cloudera Flow Management Operator for Kubernetes to use Apache Ranger for centralized, policy-based access control.

Rolling upgrades for NiFi 2 version upgrades

Cloudera Flow Management Operator for Kubernetes now supports rolling upgrades between NiFi 2 versions. During the upgrade, at least one NiFi node remains running at all times to maintain service availability.

The upgrade behavior varies by scenario:

- Upgrades between NiFi 2 versions: Configuration changes and version upgrades, such as 2.3.1 to 2.6.0, use a rolling upgrade.
- Upgrades between NiFi 1 versions: Configuration changes that do not change the NiFi version use a rolling upgrade. Version changes require a non-rolling upgrade, during which all nodes are taken offline simultaneously.
- Migration from NiFi 1 to NiFi 2: The migration always uses a non-rolling upgrade.

Declarative flow deployment using the ProcessGroup custom resource

The Cloudera Flow Management Operator for Kubernetes introduces the ProcessGroup custom resource for deploying NiFi flows declaratively. It imports a Flow Definition JSON from a Kubernetes ConfigMap or Secret into a root-level process group, starts the flow automatically, and records the process group identifier in the custom resource status.

Limitations:

- Deployed flows cannot be updated.
- Changes to the source ConfigMap or Secret are not applied after deployment.
- External parameter contexts are not supported. Parameters must be defined within the Flow Definition JSON.

Automatic cleanup of unused operator-managed resources

Cloudera Flow Management Operator for Kubernetes now automatically removes Kubernetes resources that are owned by a NiFi or NiFi Registry instance but are no longer required after an operator upgrade or configuration change. During reconciliation, the operator identifies and removes these obsolete resources, helping maintain a clean cluster state.

Release 3.2.2

Release 3.2.2 of Cloudera Flow Management Operator for Kubernetes fixes an issue related to NiFi conversion webhook misconfiguration.

Fixed issues

CFMOP-187 - Incorrect conversion webhook configuration

A misconfiguration of the Nifi conversion webhook caused issues with retrieving newly introduced v1 instances of the Nifi resource.

Release 3.2.1

Learn about the new features and notable changes in release 3.2.1 of Cloudera Flow Management Operator for Kubernetes.

New features

Configurable NiFi security context.

Provides the ability to customize the Pod and Container security contexts for pods in the Nifi and NifiRegistry custom resources.

For more information, see Security context configuration for Nifi and Security context configuration for NifiRegistry.

Support restrictive Pod Security Standard out-of-the-box

The default security context on NiFi Pods now aligns with the requirements to fit the restricted Pod Security Standard.

Fixed issues

CFMOP-143 Routes and Connection conflict across namespaces

When two Nifi custom resources, in different namespaces, have the same name, there is a conflict that occurs in the Cloudera Flow Management Operator for Kubernetes that results in the Services and Routes created to serve the Connection being terminated continuously.

Release 3.2.0

Learn about the new features and notable changes in release 3.2.0 of Cloudera Flow Management Operator for Kubernetes.

Improvements

AccessPolicyProfiles are now supported by the UserGroup CRD

For more information, see Configuring user groups.

Deprecations and removals

proxyAccessNamespaces removed

The proxyAccessNamespaces CRD has been removed from the NifiRegistrySpec. Use the NifiRegistryBindings CRD instead.

For more information, see Configuring NiFi Registry binding.

Release 3.1.0

Learn about the new features and notable changes in release 3.1.0 of Cloudera Flow Management Operator for Kubernetes.

New features

UserGroup

This CRD allows for NiFi user group configuration in YAML.

For more information, see Configuring user groups

AccessPolicyProfile

This CRD allows for defining sets of access policies, roles, for Users.

For more information, see Configuring NiFi access policy profiles

User CRD supports certificate generation

User CRD now supports generating certificates which can be used to authenticate as that user.

For more information, see Configuring NiFi image

NiFi version detection

Cloudera Flow Management Operator for Kubernetes now can detect NiFi version based on image tag.

For more information, see Configuring NiFi image

Release 3.0.0

Learn about the new features and notable changes in release 3.0.0 of Cloudera Flow Management Operator for Kubernetes.

New features

User CRD

This release introduces a new Custom Resource Definition (CRD) that represents a NiFi user and allows for defining a user identity and associated access policies.

NiFi deployments secure by default

NiFi deployed by Cloudera Flow Management Operator for Kubernetes is now secure by default. When no authorization method is provided, NiFi will be configured in single user auth mode with username "demonstration-user" and password "demonstration-password". When no Node Certificate Generation is specified, node certificates will be generated using a self-signed Cluster Issuer nifi-node-certs that is deployed with the operator.

Fixed issues

Lost flow during zero leader scale up

If a NiFi cluster lost all viable leaders during scale up (usually a single node cluster scaling to two nodes), the new Node would begin waiting for leader election, eventually time out, and declare itself the leader with an empty flow definition. When the old leader finally recovered, it would take the empty flow of the leader, assuming it had no data in queues. Cloudera Flow Management Operator for Kubernetes now temporarily reverts the scale up if there is no viable leader at any point in the scale up process.

Release 2.11.0

Learn about the new features and notable changes in release 2.11.0 of Cloudera Flow Management Operator for Kubernetes.

New features

NifiRegistryBinding

Connect a NiFi and NiFi Registry instance using the NifiRegistryBinding custom resource.

Initial Admin Canvas Access Policies

The initial admin user specified in the NiFi custom resource's spec.security.initialAdminIdentity field now has immediate access to the NiFi canvas on first startup, making getting up and running with a new NiFi cluster much faster.

Fixed issues

OOM Recovery did not maintain QoS of Pods

OOM Recovery would increase resource limits but not requests, resulting in a changed quality of service of Pods, i.e. changing from Guaranteed (request == limit) to Burstable (request < limit).

Operational Changes

cfm-operator NiFi User

A default 'cfm-operator.cfm-operator-system.svc' user was added to give Cloudera Flow Management - Kubernetes Operator the permissions it needs to manage the NiFi cluster. Do not remove this user or any of its permissions, as it will render the operator unable to manage that NiFi Cluster.

Release 2.10.0

Learn about the new features and notable changes in release 2.10.0 of Cloudera Flow Management Operator for Kubernetes.

New features

Cluster scheduling

The NiFi custom resource now contains a schedule spec that can be used to define the times during which the NiFi cluster should be running.

Security providers

In order to support FIPS compliant operation, a method of providing and declaring additional Java security providers, such as CryptoComply for Java and Bouncy Castle, has been added to the NiFi spec.

OIDC authentication

Support for OpenID Connect authentication has been added to the NiFi Registry spec.

Out of memory (OOM) recovery

An OOM Recovery function has been added to the NiFi controller. When configured, the CFM Operator will detect OOM events in NiFi and increase the memory of the Pod by a configurable step.

Additional proxy hosts

A NiFi spec field has been added such that multiple hostnames can be provided to NiFi. This allows configuration of alternate DNS names for the NiFi service beyond the hostName spec field.

NAR volume providers

Provide NiFi NARs through Kubernetes volumes. NARs can be landed in a networked filesystem or object storage and provided to NiFi by way of a CSI driver, i.e. EFS or S3.

Additional CA bundles reference

Additional CA certificates can now be provided by a Secret or ConfigMap reference instead of in-line in the NiFi spec yaml, greatly reducing file length and improving readability.

Environment variables

An environment variable override has been provided in the NiFi spec. This allows for setting custom environment variables on the NiFi container for use in Flows or Python scripts.

Fixed issues

- This release of Cloudera Flow Management Operator for Kubernetes is shipped with NiFi 1 and 2 versions that contain the remediation for CVE-2025-30065.
- NiFi Registry resources not cleaned up on delete, i.e. PVCs and Certificate Secrets.
- NiFi Registry hostname not added to Node Certificate.
- NiFi Registry users and authorizations incorrectly persisted.
- NiFi not restarting when additional CA bundles are provided.

Release 2.9.1

Learn about the new features and notable changes in release 2.9.1 of Cloudera Flow Management Operator for Kubernetes.

A Cloudera Flow Management Operator for Kubernetes 2.9.1 bundle for RedHat OpenShift OperatorHub is released. This is not a functional release, deployed images are still at 2.9.0-b96.

Fixed issues

- Cloudera Flow Management Operator for Kubernetes running out of memory when deploying NiFis
- Missing role permissions

Release 2.9.0

Learn about the new features and notable changes in release 2.9.0 of Cloudera Flow Management Operator for Kubernetes.

Improvements

- Cluster domains other than the default 'cluster.local' are now supported.

- Kubernetes replaced ZooKeeper as the default state management and leader election option.
- JVM memory settings are now calculated based on Pod memory.
- A NiFi CR config for Single User Authentication is now available.
- Pod and Node affinity are now configurable.
- The cfmctl CLI utility lists resources that block uninstallation of a cluster.

Fixed issues

- Node Cert alt names for proper SNI resolution
- NiFi Registry StatefulSet not updated on spec change
- OIDC did not use NiFi truststore
- CFM Operator continually overwriting default sensitive properties key
- Incorrect port configuration for non secure NiFi

Release 2.8.0

Learn about the new features and notable changes in release 2.8.0 of Cloudera Flow Management Operator for Kubernetes.

Cloudera Flow Management Operator for Kubernetes 2.8.0 is the first release of the CFM Kubernetes operator, which provides a way to deploy, manage, and operate NiFi clusters on Kubernetes application platforms. This release comes with container images based on Apache NiFi 1.25 and Apache NiFi 2.0 (milestone release). To learn more about the Cloudera Flow Management Operator for Kubernetes and its typical deployment architecture, see the Cloudera Flow Management Operator for Kubernetes Overview. To get started with installing the operator, see Installation overview.

Apache Parquet CVE-2025-30065

A critical vulnerability (CVE-2025-30065) in Apache Parquet's parquet-avro module allows arbitrary code execution through schema manipulation and crafted files. Cloudera advises upgrading to supported versions with fixes once they become available and implementing mitigations in the meantime.

Background:

On April 1, 2025, a critical vulnerability in the parquet-avro module of Apache Parquet (CVE-2025-30065, CVSS score 10.0) was announced.

Cloudera has determined the list of affected products, and is issuing this TSB to provide details of remediation for affected versions.

Upgraded versions are being released for all currently affected supported releases of Cloudera products. Customers using older versions are advised to upgrade to a supported release that has the remediation, once it becomes available.

Addressed in release/refresh/patch:

Upgrade your NiFi clusters to one of the NiFi Runtime versions that contain the fix:

- 1.28.0 or higher
- 1.27.0.2.3.14.2-2
- 1.25.0.2.3.13.2-3
- 1.24.0.2.3.12.4-4
- 1.23.2.2.3.11.1-4
- 1.21.0.2.3.9.3-5
- 1.20.0.2.3.8.3-3

For more information on upgrading a NiFi cluster to a newer Runtime version, see Configuring NiFi image.

For the latest updates on this issue, see the corresponding Knowledge article.

Supported component versions

Cloudera Flow Management Operator for Kubernetes components and their versions delivered in this release of the product.

Table 1: Cloudera Flow Management Operator for Kubernetes component versions

Component	Version
Cloudera Flow Management Operator for Kubernetes and cfmctl	3.4.1
NiFi	1.28.1 /2.11
NiFi Registry	1.28.1/2.11

System requirements

To install and use Cloudera Flow Management Operator for Kubernetes and its components, your Kubernetes cluster environment must meet the following system requirements and prerequisites.

- Kubernetes cluster
  - Version 1.30 or later
  - OpenShift 4.19 or later

  Note: Cloudera Flow Management Operator for Kubernetes complies with Cloud Native Computing Foundation (CNCF) standards and is compatible with CNCF-compliant Kubernetes distributions. For supporting your specific Kubernetes distribution, contact Cloudera.
- Administrative rights on the Kubernetes cluster
- Access to kubectl or oc, configured to connect to your running cluster
- Access to helm
- cert-manager installed on the Kubernetes cluster
- Log collection enabled for the Kubernetes cluster
- Cloudera requires that the logs of Cloudera Flow Management Operator for Kubernetes components are stored long term for diagnostic and supportability purposes.
- Persistent storage class configured on the Kubernetes cluster that satisfies the durability and low-latency requirements for operating NiFi. The ideal storage class configuration can vary depending on the environment and use case, and it is determined by the Kubernetes platform where the product is deployed.
- (Optional): Prometheus installation running in the same Kubernetes cluster where you install Cloudera Flow Management Operator for Kubernetes. Prometheus is used for collecting and monitoring NiFi metrics.