Cloudera Flow Management - Kubernetes Operator 2.10.0

CFM Operator Release Notes

Date published: 2024-06-11
Date modified: 2025-04-28

https://docs.cloudera.com/

Legal Notice

Contents

What's new

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

Release 2.10.0

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

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

- 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 - Kubernetes Operator.

A Cloudera Flow Management - Kubernetes Operator 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 - Kubernetes Operator 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 - Kubernetes Operator.

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 - Kubernetes Operator.

Cloudera Flow Management - Kubernetes Operator 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 - Kubernetes Operator and its typical deployment architecture, see the Cloudera Flow Management - Kubernetes Operator 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.

Vulnerability Details:

Exploiting this vulnerability is only possible by modifying the accepted schema used for translating Parquet files and subsequently submitting a specifically crafted malicious file.

CVE-2025-30065 | Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code.

CVE:

NVD - CVE-2025-30065

Severity (Critical):

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

Impact:

Schema parsing in the parquet-avro module of Apache Parquet 1.15.0 and previous versions allows bad actors to execute arbitrary code. Attackers may be able to modify unexpected objects or data that was assumed to be safe from modification. Deserialized data or code could be modified without using the provided accessor functions, or unexpected functions could be invoked.

Deserialization vulnerabilities most commonly lead to undefined behavior, such as memory modification or remote code execution.

Mitigation:

Until Cloudera has released a product version with the Apache Parquet vulnerability fix, please continue to use the mitigations listed below:

Customers with their own FIM Solution:

1. Utilize a File Integrity Monitoring (FIM) solution. This allows administrators to monitor files at the filesystem level and receive alerts on any unexpected or suspicious activity in the schema configuration.

General advisory:

1. Use network segmentation and traffic monitoring with a device capable of deep packet inspection, such as a network firewall or web application firewall, to inspect all traffic sent to the affected endpoints.
2. Configure alerts for any suspicious or unexpected activity. You may also configure sample analysis parameters to include:
   - Parquet file format “magic bytes” = PAR1
   - Connections from sending hosts that are not expected source IP ranges.
3. Be cautious with Parquet files from unknown or untrusted sources. If possible, do not process files with uncertain origins or that can be ingested from outside the organization.
4. Ensure that only authorized users have access to endpoints that ingest Parquet files.

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

Known issues

Learn about the known issues in this release of Cloudera Flow Management - Kubernetes Operator

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.

Until Cloudera has released a product version with the Apache Parquet vulnerability fix, please continue to use the mitigations listed below:

Customers with their own FIM Solution:

1. Utilize a File Integrity Monitoring (FIM) solution. This allows administrators to monitor files at the filesystem level and receive alerts on any unexpected or suspicious activity in the schema configuration.

General advisory:

1. Use network segmentation and traffic monitoring with a device capable of deep packet inspection, such as a network firewall or web application firewall, to inspect all traffic sent to the affected endpoints.
2. Configure alerts for any suspicious or unexpected activity. You may also configure sample analysis parameters to include:
   - Parquet file format “magic bytes” = PAR1
   - Connections from sending hosts that are not expected source IP ranges.
3. Be cautious with Parquet files from unknown or untrusted sources. If possible, do not process files with uncertain origins or that can be ingested from outside the organization.
4. Ensure that only authorized users have access to endpoints that ingest Parquet files.

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

CDPDFX-10225: Cloudera Flow Management - Kubernetes Operator crashes once when creating a NiFi Registry (Standalone)

When first creating a NifiRegistry resource, the Cloudera Flow Management - Kubernetes Operator may crash once before recovering. No impact to functionality.

None.

Supported component versions

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

Table 1: Cloudera Flow Management - Kubernetes Operator component versions

Component	Version
Cloudera Flow Management - Kubernetes Operator and cfmctl	2.10.0
NiFi	1.28.0 / 2.3.0
NiFi Registry	1.28.0

System requirements

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

- Kubernetes cluster
  - Version 1.23 or later
  - OpenShift 4.10 or later

  

  Note: Cloudera Flow Management - Kubernetes Operator 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 - Kubernetes Operator 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 - Kubernetes Operator. Prometheus is used for collecting and monitoring NiFi metrics.