

Cloudera Flow Management 2.1.1

Cloudera Flow Management Release Notes

Date published: 2019-06-26

Date modified: 2021-04-28

CLOUDERA

<https://docs.cloudera.com/>

Legal Notice

© Cloudera Inc. 2024. 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 in this release?	4
Component support	5
Unsupported Features	5
Technical Preview Features	5
Unsupported Customizations	6
Apache Patches	6
NiFi Patches	6
NiFi Registry Patches	7
Behavioral Changes	7
Known Issues	8
Fixed Issues	9
Common Vulnerabilities and Exposures	9
Download from the CFM Repository	10

What's new in this release?

Cloudera Flow Management (CFM) 2.1.1 is a major release of CFM on CDP Private Cloud Base. It is the first version based on Apache NiFi 1.13.2. In addition, CFM 2.1.1 also includes bug fixes and improvements on top of the Apache NiFi release.



Note: CFM 2.1.1 is the first release in the CFM 2.1.x family. There is no CFM 2.1.0 version.

CDP Private Cloud Base support

CFM 2.1.1 supports CDP Private Cloud Base 7.1.6.

If you are upgrading to CFM 2.1.1, see *CFM upgrade and migration paths*.

SAML authentication

NiFi now supports user authentication through a Security Assertion Markup Language (SAML).

For more information, see *SAML Authentication*.

Restricted-component policy is more granular

Fine-tune access by a restricted component to the localhost filesystem data by specifying the restricted component and type of permission in the policy that you assign to the user or user group. This also makes a distinction between processors that can access the local filesystem where NiFi is running and the processors that can access a distributed file system like the Hadoop related processors.

For more information, see *NiFi Restricted Components*.

Ability to install NiFi clusters with Ranger/Solr but no HDFS

Starting with CFM 2.1.1 and CDP 7.1.6, you can now deploy NiFi clusters that use Ranger for authorization, but do not require HDFS. If you are a legacy Hortonworks customer and have NiFi from HDF with Ranger but did not install HDFS to store audit logs with Ranger, you now have two options:

- Use HDFS for long-term audit log archive and Solr for indexing and searching
- Keep using only Solr as in HDFS

FIPS compliance

You can encrypt NiFi sensitive properties with a secret key generated by the FIPS 140-2 approved PBKDF2 algorithm. For more information, see *FIPS 140-2 Compliance*.

NiFi-Ozone integration

If Ozone is installed in your CDP cluster, you can use the HDFS processors in NiFi to interact with the Ozone storage layer.

NiFi node status history and status repository

Starting with CFM 2.1.1, it is now possible to access a Node Status History view from the hamburger menu. This provides useful monitoring data about the NiFi nodes in the cluster over time. Just like Status History data at the component level, Node History data is stored in memory by default and removed after a NiFi restart.

It is now possible to persist both Node and Status history data by setting the `nifi.components.status.repository.implementation` property in the `nifi.properties` file.

For more information, see the *Status History Repository* topic in the *Apache NiFi Administration Guide*.

Related Information

[SAML Authentication](#)

[NiFi Restricted Components](#)
[FIPS 140-2 Compliance](#)
[Status History Repository](#)
[CFM upgrade and migration paths](#)

Component support

List of the official component versions for Cloudera Flow Management. To know the component versions for compatibility with other applications, you must be familiar with the latest component versions in CFM.

**Note:**

NiFi works with the version of NiFi Registry shipped with your version of CFM or later.

CFM 2.1.1

- Apache NiFi 1.13.2.2.1.1.0
- Apache NiFi Registry 0.8.0.2.1.1.0

CFM 2.0.4

- Apache NiFi 1.11.4
- Apache NiFi Registry 0.6.0

For more information, see the *CFM 2.0.4 Release Notes*.

CFM 2.0.1

- Apache NiFi 1.11.4
- Apache NiFi Registry 0.6.0

For more information, see the *CFM 2.0.1 Release Notes*.

Related Information

[CFM 2.0.4 Release Notes](#)

[CFM 2.0.1 Release Notes](#)

Unsupported Features

The following features are developed and tested by the Cloudera community but are not officially supported by Cloudera. These features are excluded for a variety of reasons, including insufficient reliability or incomplete test case coverage, declaration of non-production readiness by the community at large, and feature deviation from Cloudera best practices. Do not use these features in your production environments.

Technical Preview Features

The following features are available within CFM 2.1.1 but are not ready for production deployment. Cloudera encourages you to explore these technical preview features in non-production environments and provide feedback on your experiences through the [Cloudera Community Forums](#).

- The following rules engine and handlers controller services:
 - EasyRulesEngineService
 - EasyRulesEngineProvider
 - ScriptedRulesEngine
 - ActionHandlerLookup
 - AlertHandler
 - ExpressionHandler
 - LogHandler
 - RecordSinkHandler
 - ScriptedActionHandler

Unsupported Customizations

Cloudera cannot guarantee that default NiFi processors are compatible with proprietary protocol implementations or proprietary interface extensions. For example, we support interfaces like JMS and JDBC that are built around standards, specifications, or open protocols. But we do not support customizations of those interfaces, or proprietary extensions built on top of those interfaces.

Apache Patches

The following sections list patches in each CFM component beyond what was fixed in the base version of the Apache component.

NiFi Patches

In addition to what is available with Apache NiFi 1.13.2, CFM 2.1.1 includes the patches listed here.

CFM 2.1.1

- [NIFI-8430](#) - Fix ReportLineageToAtlas Truststore Loader Thread Leak
- [NIFI-8405](#) - Add debug logging around request replication
- [NIFI-8404](#) - Support "Rollback on Failure" for PublishKafka(Record) processors
- [NIFI-8387](#) - UI - render bulletins for referencing components from new data model
- [NIFI-8386](#) - When fetching Parameter Context/Variable Registry/Controller Services, referencing components should include bulletins
- [NIFI-8368](#) - Avro decimal logical type fails if scale > precision
- [NIFI-8360](#) - SplitContent does not find any 'splits' that occur after about 2 GB into FlowFile
- [NIFI-8357](#) - ConsumeKafka(Record)_2_0, ConsumeKafka(Record)_2_6 do not reconnect if using statically assigned partitions
- [NIFI-8353](#) - When node is offloaded, it may still receive data from load-balanced connections
- [NIFI-8346](#) - PutAzureBlobStorage doesn't route to failure despite the exception during upload
- [NIFI-8344](#) - Allow TailFile to continue tailing a file for some time after it has been rolled over
- [NIFI-8319](#) - EncryptContent should support decrypting AES/CBC/NoPadding
- [NIFI-8314](#) - Generate warning for any long-running tasks
- [NIFI-8313](#) - Upgrade zip4j to 2.7.0
- [NIFI-8312](#) - Support PKCS12 and BCFKS truststores in Atlas reporting task
- [NIFI-8307](#) - Controller Services not fully enabling on startup, preventing NiFi from completing startup
- [NIFI-8302](#) - Correct Sensitive Value Encoding in FingerprintFactory
- [NIFI-8296](#) - Integration with API to retrieve all subjects associated with a schema id for Confluent Schema Registry v5.3.1+

- [NIFI-8289](#) - EmbeddedQuestDbRolloverHandlerTest tests fail when local date and UTC date differ
- [NIFI-8286](#) - CertificateUtils do not support embedded emailAddress in CN
- [NIFI-8283](#) - Value handling in ScanAccumulo processor
- [NIFI-8263](#) - ListenHTTP - thread pool size
- [NIFI-8260](#) - Process Group Import JSON file
- [NIFI-8258](#) - Add support for Service Principal authentication in ADLS processors
- [NIFI-8224](#) - Add LoggingRecordSink controller service
- [NIFI-8212](#) - Improve startup times for Stateless
- [NIFI-8188](#) - Processors: right click / run once
- [NIFI-8132](#) - Replace Framework Uses of MD5 with Modern Algorithm
- [NIFI-8113](#) - Persisting status history
- [NIFI-8030](#) - Improve Atlas lineage when using PutHDFS to push data accessed through Hive
- [NIFI-7912](#) - Site-to-Site over HTTP fails for FlowFiles over 100MB
- [NIFI-7668](#) - Add configurable PBE AEAD algorithms to flow encryption
- [NIFI-7127](#) - Allow injection of SecureHasher into FingerprintFactory
- [NIFI-6752](#) - Create ASN.1 RecordReader

For more information on fixed Apache NiFi patches, see the *Apache NiFi Release Notes*.

Related Information

[Apache NiFi Release Notes](#)

NiFi Registry Patches

This release includes Apache NiFi Registry 0.8.0 and the following patches.

- [NIFIREG-434](#) - Support BCFKS Keystore Type
- [NIFIREG-429](#) - Flyway error when upgrading from older release to 0.8.0

For more information on fixed Apache NiFi Registry patches, see the *Apache NiFi Registry Release Notes*.

Related Information

[Apache NiFi Registry Release Notes](#)

Behavioral Changes

Learn about the change in behavior in this version of CFM 2.1.1.

DOCS-9193: After upgrade, update header value for X-ProxiedEntitiesChain

If you are upgrading from CFM 2.0.4 to CFM 2.1.1, then you are upgrading from Apache NiFi version 1.11.4 to 1.13.2. In this case, after you upgrade, if you want an authorized proxy to make a web request on behalf of another authenticated user, then you must enclose the X-ProxiedEntitiesChain header value in < >.

Previous behavior:

There was no need to add an outermost < > to the X-ProxiedEntitiesChain header value.

New behavior:

The handling of the X-ProxiedEntitiesChain header for secure proxy requests is now more strict, requiring the outermost < > in the value.

For example, a value of `%{SSL_CLIENT_S_DN}` (Apache httpd) or `$ssl_client_s_dn` (NGINX) that was previously valid must now be formatted as: `<%{SSL_CLIENT_S_DN}>` or `<$ssl_client_s_dn>`.

For other migration information, review the *Apache NiFi Migration Guidance* to be aware of changes made between versions and the impact they may have on your existing dataflows.

DOCS-8537: Granular Restricted Component Policy in Ranger

You can now use the Ranger policy `/restricted-components` to differentiate permissions between processors. For instance, previously, the `/restricted-components/read-filesystem` policy covered both a processor like `FetchFile` and a processor like `FetchHDFS`.

In this release, you can differentiate between the processors by specifying the following levels of the `/restricted-components` policy for Hadoop related processors:

- `/restricted-components/read-distributed-filesystem`
- `/restricted-components/write-distributed-filesystem`



Important: After upgrading, if a user who was not able to drag and drop a `PutHDFS` processor on the canvas because of the `/restricted-components/read-filesystem` policy, will now be able to drag and drop the `PutHDFS` processor until the new policy is added.

For more information, see *NiFi Restricted Components*.

Related Information

[Apache NiFi Migration Guidance](#)

[NiFi Restricted Components](#)

Known Issues

Summarizes known issues for this release.

- **Special characters in Keystore/Truststore passwords:** If there are special characters in the passwords of the truststores/keystores, the normal operation of NiFi and its integration with Cloudera Manager (command and control, monitoring, etc) is affected.

Workaround: Update the passwords using only [A-Z a-z 0-9] characters or upgrade to CFM 2.1.5. You can also file a support case to get a hotfix from Cloudera Support.

- **NiFi UI Performance considerations:** A known issue in Chrome 92.x causes significant slowness in the NiFi UI and may lead to high CPU consumption. For more information, see the Chrome Known Issues documentation at [1235045](#).

Workaround: Use another version of Chrome or a different browser.

- **JDK limitation:** JDK 8u271, JDK 8u281, and JDK 8u291 may cause socket leak issues in NiFi due to JDK-8245417 and JDK-8256818. Pay attention to the build version of your JDK because some later builds are fixed as described in [JDK-8256818](#).

Workaround: Consider using a more recent version of the JDK like 8u282, or builds of the JDK where the issue is fixed.

- [NIFI-8387](#): UI - render bulletins for referencing components from new data model
- [NIFI-8386](#): When fetching Parameter Context/Variable Registry/Controller Services, referencing components should include bulletins
- [NIFI-8330](#): JythonScriptEngineConfigurator needs to recompile on init()
- [NIFI-8326](#): KafkaRecordSink puts multiple records in one message
- [NIFI-7912](#): Site to Site may fail if data exchange takes more than 30 seconds

Technical Service Bulletins

TSB 2022-580: NiFi Processors cannot write to content repository

If the content repository disk is filled more than 50% (or any other value that is set in `nifi.properties` for `nifi.content.repository.archive.max.usage.percentage`), and if there is no data in the content

repository archive, the following warning message can be found in the logs: "Unable to write flowfile content to content repository container default due to archive file size constraints; waiting for archive cleanup". This would block the processors and no more data is processed.

This appears to only happen if there is already data in the content repository on startup that needs to be archived, or if the following message is logged: "Found unknown file XYZ in the File System Repository; archiving file".

Upstream JIRA

- [NIFI-10023](#)
- [NIFI-9993](#)

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2022-580: NiFi Processors cannot write to content repository](#)

TSB 2022-589: CVE-2022-33140 Apache NiFi ShellUserGroupProvider Vulnerability

The optional ShellUserGroupProvider in Apache NiFi 1.10.0 to 1.16.2 and Apache NiFi Registry 0.6.0 to 1.16.2 does not neutralize arguments for group resolution commands, allowing injection of operating system commands on Linux and macOS platforms. The ShellUserGroupProvider is not included in the default configuration. Command injection requires ShellUserGroupProvider to be one of the enabled User Group Providers (UGP) in the Authorizers configuration. Command injection also requires an authenticated user with elevated privileges. Apache NiFi requires an authenticated user with authorization to modify access policies in order to execute the command. Apache NiFi Registry requires an authenticated user with authorization to read user groups in order to execute the command. The resolution removes command formatting based on user-provided arguments.

Knowledge article

For the latest update on this issue see the corresponding Knowledge article: [TSB 2022-589: CVE-2022-33140 Apache NiFi ShellUserGroupProvider Vulnerability](#)

Fixed Issues

CFM 2.1.1 is a major release. Fixed issues information will be added in maintenance releases of CFM 2.1.x.

Common Vulnerabilities and Exposures

Lists common vulnerabilities and exposures fixed in CFM 2.1.1.

CVE-2020-27218: Apache NiFi's use of Jetty server

Severity: Low

Versions Affected: Apache NiFi 1.2.0 - 1.12.1

Description: The Jetty server dependency had a HTTP Request Smuggling vulnerability. See [NIST NVD CVE-2020-27218](#) for more information.

Mitigation: Jetty server was upgraded from 9.4.26.v20200117 to 9.4.35.v20201120 for the Apache NiFi 1.13.0 release.

CVE Link: [Mitre Database: CVE-2020-27218](#)

NiFi Jira: [NIFI-8098](#)

NiFi PR: [PR 4731](#)

CVE-2021-20190; CVE-2019-12086: Apache NiFi's jackson-databind usage

Severity: Low

Versions Affected: Apache 1.7.0 - 1.12.1

Description: The com.fasterxml.jackson.core;jackson-databind dependency had various serialization vulnerabilities. See [NIST NVD CVE-2021-20190](#) for more information.

Mitigation: jackson-databind was upgraded from 2.9.10.5 to 2.9.10.8 for the Apache NiFi 1.13.0 release.

CVE Link: [Mitre Database: CVE-2021-20190](#)

NiFi Jira: [NIFI-8166](#)

NiFi PR: [PR 4777](#)

CVE-2020-7676: Apache NiFi's angular.js usage

Severity: Low

Versions Affected: Apache NiFi 1.8.0 - 1.11.4

Description: The angular.js dependency had an XSS vulnerability. See [NIST NVD CVE-2020-7676-9658](#) for more information.

Mitigation: angular.js was upgraded from 1.7.9 to 1.8.0 for the Apache NiFi 1.12.0 release.

CVE Link: [Mitre Database: CVE-2020-7676](#)

NiFi Jira: [NIFI-7577](#)

NiFi PR: [PR 4357](#)

Download from the CFM Repository

Use the following tables to identify the Cloudera Flow Management (CFM) repository location for your operating system and operational objectives.



Note:

You must have credentials to download CFM files. Your download credential is not the same as the credential you use to access the support portal.

You can get download credentials in the following ways:

- Contact your Cloudera sales representative.
- View the Welcome email for your Flow Management account.
- File a non-technical case within the [Cloudera support portal](#) for our Support team to assist you.

Table 1: CentOS 7

File	Location
Manifest	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/parcel/manifest.json
Parcel	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/parcel/CFM-2.1.1.0-13-el7.parcel
Parcel sha file	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/parcel/CFM-2.1.1.0-13-el7.parcel.sha

Table 2: SLES 12

File	Location
Manifest	https://archive.cloudera.com/p/cfm2/2.1.1.0/sles12/yum/tars/parcel/manifest.json
Parcel	https://archive.cloudera.com/p/cfm2/2.1.1.0/sles12/yum/tars/parcel/CFM-2.1.1.0-13-sles12.parcel

File	Location
Parcel sha file	https://archive.cloudera.com/p/cfm2/2.1.1.0/sles12/yum/tars/parcel/CFM-2.1.1.0-13-sles12.parcel.sha

Table 3: Ubuntu 18

File	Location
Manifest	https://archive.cloudera.com/p/cfm2/2.1.1.0/ubuntu18/apt/tars/parcel/manifest.json
Parcel	https://archive.cloudera.com/p/cfm2/2.1.1.0/ubuntu18/apt/tars/parcel/CFM-2.1.1.0-13-bionic.parcel
Parcel sha file	https://archive.cloudera.com/p/cfm2/2.1.1.0/ubuntu18/apt/tars/parcel/CFM-2.1.1.0-13-bionic.parcel.sha

Table 4: CSD files

File	Location
NiFi	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/parcel/NIFI-1.13.2.2.1.0-13.jar
NiFi Registry	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/parcel/NIFIREGISTRY-0.8.0.2.1.0-13.jar

Table 5: Standalone components

File	Location
NiFi (.tar.gz)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-1.13.2.2.1.0-13-bin.tar.gz
NiFi (.zip)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-1.13.2.2.1.0-13-bin.zip
NiFi (.zip.sha256)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-1.13.2.2.1.0-13-bin.zip.sha256
NiFi Registry (.tar.gz)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi_registry/nifi-registry-0.8.0.2.1.0-13-bin.tar.gz
NiFi Toolkit (.tar.gz)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-toolkit-1.13.2.2.1.0-13-bin.tar.gz
NiFi Toolkit (.zip)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-toolkit-1.13.2.2.1.0-13-bin.zip
NiFi Toolkit (.zip.sha256)	https://archive.cloudera.com/p/cfm2/2.1.1.0/redhat7/yum/tars/nifi/nifi-toolkit-1.13.2.2.1.0-13-bin.zip.sha256

Table 6: Windows files

File	Location
NiFi MSI	https://archive.cloudera.com/p/cfm2/2.1.1.0/windows/nifi-2.1.1.0-13.msi
NiFi MSI sha file	https://archive.cloudera.com/p/cfm2/2.1.1.0/windows/nifi-2.1.1.0-13.msi.sha