

Cloudera Flow Management 2.0.4

# Cloudera Flow Management Release Notes

Date published: 2019-06-26

Date modified: 2021-01-06

The Cloudera logo is displayed in a bold, orange, sans-serif font. The word "CLOUDERA" is written in all caps, with a stylized 'E' that has three horizontal bars.

<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

<b>What's New in This Release?</b> .....	<b>4</b>
<b>Component support</b> .....	<b>4</b>
<b>Unsupported Features</b> .....	<b>4</b>
Technical Preview Features.....	5
Unsupported Customizations.....	5
<b>Apache Patches</b> .....	<b>5</b>
NiFi Patches.....	5
NiFi Registry Patches.....	6
<b>Known Issues</b> .....	<b>6</b>
<b>Fixed Issues</b> .....	<b>7</b>
<b>Common Vulnerabilities and Exposures</b> .....	<b>8</b>
<b>Download from the CFM Repository</b> .....	<b>12</b>

## What's New in This Release?

Cloudera Flow Management (CFM) 2.0.4 is the first maintenance release CFM on CDP Private Cloud Base. It includes new Apache NiFi features and improvements.

**Note:**

The NiFi version in CFM 2.0.4 is NiFi 1.11.4.2.0.4.0. It means that CFM 2.0.4 is based on Apache NiFi 1.11.4 but it also includes additional features, improvements, and fixes.

Bug fixes

- CFM 2.0.4 includes a fix for the NiFi `ReplaceText` processor. See the [Known Issues documentation](#) in the CFM 2.0.1 Release Notes.
- It also includes fixes for the integration with Cloudera Manager and the CDP components.

CDP Private Cloud Base support

CFM 2.0.4 supports the following versions of CDP Private Cloud Base:

- 7.1.1
- 7.1.2
- 7.1.3
- 7.1.4
- 7.1.5

**Note:**

CDP 7.1.5 is supported provided you have met the following two conditions:

- You have not enabled FIPS on your CDP CDP Private Cloud Base cluster.
- You are installing CFM 2.0.4 on CentOS/RHEL.

## 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 2.0.4

- Apache NiFi 1.11.4
- Apache NiFi Registry 0.6.0

CFM 2.0.1

- Apache NiFi 1.11.4
- Apache NiFi Registry 0.6.0

## 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 2.0.4 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](#).

- Encrypted flow file repository
- Encrypted content repository
- 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

This release includes Apache NiFi 1.11.4 and the following patches.

CFM 2.0.4

- [NIFI-7183](#): ReplaceText with multiple concurrency tasks can result in data corruption

CFM 2.0.1

- [NIFI-4792](#): Allow QueryRecord processor to query nested arrays.
- [NIFI-6064](#): MockComponentLog misplaces reported exceptions.
- [NIFI-6491](#): Improve installation documentation.
- [NIFI-6551](#): Improve timestamp handling for PutKudu processor.
- [NIFI-6867](#): PutKudu operation type parameter allows bad values.
- [NIFI-6927](#): PutElasticsearchHttp 1.10.0 with java 11 Fails to initialize due to "clientBuilder.sslSocketFactory(SSLSocketFactory) not supported on JDK 9+.
- [NIFI-6958](#): Disabled State in Registry (in Sub PG) breaks Flow Update on Nifi Side.

- [NIFI-6968](#): Create Connection Modal Allows Multiple Adds.
- [NIFI-7049](#): SFTP processors shouldn't silently try to access known hosts file of the user.
- [NIFI-7053](#): Update Toolkit Guide with macOS 10.15 trusted certificate requirements (2048 bit key and max of 825 days of validity).
- [NIFI-7067](#): Allow a user and group with the same name/identity to exist.
- [NIFI-7075](#): Update list of flowfile core attributes in Developer Guide.
- [NIFI-7082](#): In tls-toolkit, change default validity of to 825 days or less.
- [NIFI-7095](#): ResetSetRecordSet: handle java.sql.Array Types in normalizeValue method.
- [NIFI-7105](#): NPE in SiteToSiteStatusReportingTask for counters.
- [NIFI-7106](#): Add parent name and parent path in SiteToSiteStatusReportingTask.
- [NIFI-7108](#): Upgrade com.puppycrawl.tools:checkstyle.
- [NIFI-7109](#): Unit tests should be able to determine if item validator was called.
- [NIFI-7114](#): NiFi not closing file handles.
- [NIFI-7117](#): Load Balance is not working.
- [NIFI-7132](#): PutCassandraQL is handling UUIDs as Strings.
- [NIFI-7135](#): Fix Java 11 build with com.puppycrawl.tools:checkstyle:jar:8.29 dependency.
- [NIFI-7136](#): Set the autocomplete HTML5 tag to false for username/password login fields.
- [NIFI-7142](#): Automatically handle schema drift in the PutKudu processor.
- [NIFI-7143](#): Upgrade GCP dependency.
- [NIFI-7157](#): Investigate adoption of Github Workflow - Actions - CI.
- [NIFI-7165](#): Update documentation for Toolkit certificate validity period to 825 days.
- [NIFI-7175](#): Fix formatting of core attributes in docs.

For more information on fixed Apache NiFi patches, see the [Apache NiFi Release Notes](#).

## NiFi Registry Patches

This release includes Apache NiFi Registry 0.6.0 and the following patches.

- [NIFIREG-252](#): Add docker maven image and build profile.
- [NIFIREG-320](#): Add standard HTTP security headers.
- [NIFIREG-323](#): Updated bootstrap port handling causes restarts to fail.
- [NIFIREG-325](#): Support for node identity group.
- [NIFIREG-334](#): Changes to support Java 11.
- [NIFIREG-336](#): Enable Integration Tests by Default.
- [NIFIREG-353](#): Add ShellUserGroupProvider to NiFi Registry.
- [NIFIREG-355](#): Include profiles for hadoop libs in ranger plugin.
- [NIFIREG-356](#): Fixing additional classpath resources for Authorizers.
- [NIFIREG-358](#): Proxy authorization not working with groups.

For more information on fixed Apache NiFi Registry patches, see the [Apache NiFi Registry Release Notes](#).

## Known Issues

Summarizes known issues for this release.

- **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

Provides a summary of the issues fixed in this release.

- [CFM-1325](#): Incomplete NiFi and NiFi Registry URLs in Knox configuration
- [CFM-1446](#): Creation of HDFS directory for Ranger audits

## Common Vulnerabilities and Exposures

Lists common vulnerabilities and exposures fixed in CFM 2.0.4.

### CVE-2020-9486

Component: Apache NiFi

Description: The NiFi stateless execution engine produced log output which included sensitive property values. When a flow was triggered, the flow definition configuration JSON was printed, potentially containing sensitive values in plaintext.

Severity: Important

Versions Affected: Apache NiFi 1.10.0 - 1.11.4

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-9486>

Apache JIRA: [NIFI-7377](#)

### CVE-2020-9487

Component: Apache NiFi

Description: The NiFi download token (one-time password) mechanism used a fixed cache size and did not authenticate a request to create a download token, only when attempting to use the token to access the content. An unauthenticated user could repeatedly request download tokens, preventing legitimate users from requesting download tokens.

Severity: Important

Versions Affected: Apache NiFi 1.10.0 - 1.11.4

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-9487>

Apache JIRA: [NIFI-7385](#)

### CVE-2020-9491

Component: Apache NiFi

Description: The NiFi UI and API were protected by mandating TLS v1.2, as well as listening connections established by processors like ListenHTTP, HandleHttpRequest, etc. However intracluster communication such as cluster request replication, Site-to-Site, and load balanced queues continued to support TLS v1.0 or v1.1.

Severity: Critical

Versions Affected: Apache NiFi 1.2.0 - 1.11.4

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-9491>

Apache JIRA: [NIFI-7407](#)

### CVE-2020-11023

Component: Apache NiFi

Description: The jquery dependency had an XSS vulnerability. See [NIST NVD CVE-2020-11023](#) for more information.

Severity: Low

Versions Affected: Apache NiFi 1.8.0 - 1.11.4

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-11023>

Apache JIRA: [NIFI-7423](#)

### **CVE-2019-9658**

Component: Apache NiFi

Description: The com.puppycrawl.tools:checkstyle dependency had a XXE vulnerability. See [NIST NVD CVE-2019-9658](#) for more information.

Severity: Low

Versions Affected: Apache NiFi 1.8.0 - 1.11.4

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-9658>

Apache JIRA: [NIFI-7108](#)

### **CVE-2019-11358**

Component: Apache NiFi

Description: Various vulnerabilities existed within the JQuery dependency used by NiFi. See [NIST NVD CVE-2019-11358](#) for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.6.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-11358>

Apache JIRA: [NIFI-6316](#)

### **CVE-2019-10247, CVE-2019-10246**

Component: Apache NiFi

Description: Various vulnerabilities existed within the Jetty dependency used by NiFi. See [NIST NVD CVE-2019-10247](#), [NIST NVD CVE-2019-10246](#) for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.8.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-10247>

Apache JIRA: [NIFI-6330](#)

### **CVE-2019-16335, CVE-2019-14540, CVE-2019-14439, CVE-2019-12814, CVE-2019-12384, CVE-2018-1000873, CVE-2018-19362, CVE-2018-19361, CVE-2018-19360**

Component: Apache NiFi

Description: Various vulnerabilities existed within the Jackson Core: Databind dependency used by NiFi. See [NIST NVD CVE-2019-16335](#), [NIST NVD CVE-2019-14540](#), [NIST NVD CVE-2019-14439](#), [NIST NVD CVE-2019-12814](#), [NIST NVD CVE-2019-12384](#), [NIST NVD CVE-2018-1000873](#), [NIST NVD CVE-2018-19362](#), [NIST NVD CVE-2018-19361](#), [NIST NVD CVE-2018-19360](#) for more information.

Severity: Medium

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-16335>

Apache JIRA: [NIFI-6709](#)

**CVE-2019-0193, CVE-2019-0192, CVE-2017-3164**

Component: Apache NiFi

Description: Various vulnerabilities existed within the Solr dependency used by NiFi. See [NIST NVD CVE-2019-0193](#), [NIST NVD CVE-2019-0192](#), [NIST NVD CVE-2017-3164](#) for more information.

Severity: Critical

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-0193>

Apache JIRA: [NIFI-6516](#)

**CVE-2017-5637, CVE-2016-5017, CVE-2018-8012**

Component: Apache NiFi

Description: Various vulnerabilities existed within the Zookeeper dependency used by NiFi. See [NIST NVD CVE-2018-8012](#), [NIST NVD CVE-2017-5637](#), [NIST NVD CVE-2016-5017](#) for more information.

Severity: Important

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2017-5637>

Apache JIRA: [NIFI-6578](#)

**CVE-2019-10083**

Component: Apache NiFi

Description: When updating a Process Group via the API, the response to the request includes all of its contents (at the top most level, not recursively). The response included details about processors and controller services which the user may not have had read access to.

Severity: Low

Versions Affected: Apache NiFi 1.3.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-10083>

Apache JIRA: [NIFI-6302](#)

**CVE-2019-12421**

Component: Apache NiFi

Description: If NiFi uses an authentication mechanism other than PKI, when the user clicks Log Out, NiFi invalidates the authentication token on the client side but not on the server side. This permits the user's client-side token to be used for up to 12 hours after logging out to make API requests to NiFi.

Severity: Moderate

Versions Affected: Apache NiFi 1.0.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-12421>

Apache JIRA: [NIFI-6085](#)

**CVE-2019-10080**

Component: Apache NiFi

Description: The XMLFileLookupService allowed trusted users to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE) and reveal information such as the versions of Java, Jersey, and Apache that the NiFi instance uses.

Severity: Low

Versions Affected: Apache NiFi 1.3.0 - 1.9.2

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-10080>

Apache JIRA: [NIFI-6301](#)

### **CVE-2019-10768**

Component: Apache NiFi

Description: An Object.prototype pollution vulnerability existed within the AngularJS dependency used by NiFi. See [NIST NVD CVE-2019-10768](#) for more information.

Severity: Important

Versions Affected: Apache NiFi 1.8.0 - 1.10.0

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2019-10768>

Apache JIRA: [NIFI-6893](#)

### **CVE-2020-1933**

Component: Apache NiFi

Description: Malicious scripts could be injected to the UI through action by an unaware authenticated user in Firefox. Did not appear to occur in other browsers.

Severity: Important

Versions Affected: Apache NiFi 1.0.0 - 1.10.0

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-1933>

Apache JIRA: [NIFI-7023](#)

### **CVE-2020-1928**

Component: Apache NiFi

Description: The sensitive parameter parser would log parsed property descriptor values for debugging purposes. This would expose literal values entered in a sensitive property when no parameter was present.

Severity: Moderate

Versions Affected: Apache NiFi 1.10.0

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-1928>

Apache JIRA: [NIFI-6948](#)

### **CVE-2020-1942**

Component: Apache NiFi

Description: The flow fingerprint factory generated flow fingerprints which included sensitive property descriptor values. In the event a node attempted to join a cluster and the cluster flow was not inheritable, the flow fingerprint of both the cluster and local flow was printed, potentially containing sensitive values in plaintext.

Severity: Important

Versions Affected: Apache NiFi 0.0.1 - 1.11.0

Apache CVE Report Link: <https://nifi.apache.org/security.html#CVE-2020-1942>

Apache JIRA: [NIFI-7079](#)

## 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	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/manifest.json">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/manifest.json</a>
Parcel	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/CFM-2.0.4.0-80-el7.parcel">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/CFM-2.0.4.0-80-el7.parcel</a>
Sha File	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/CFM-2.0.4.0-80-el7.parcel.sha">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/CFM-2.0.4.0-80-el7.parcel.sha</a>

**Table 2: SLES 12**

File	Location
Manifest	<a href="https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/manifest.json">https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/manifest.json</a>
Parcel	<a href="https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/CFM-2.0.4.0-80-sles12.parcel">https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/CFM-2.0.4.0-80-sles12.parcel</a>
Sha File	<a href="https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/CFM-2.0.4.0-80-sles12.parcel.sha">https://archive.cloudera.com/p/CFM/2.x/sles12/yum/tars/parcel/CFM-2.0.4.0-80-sles12.parcel.sha</a>

**Table 3: Ubuntu 18**

File	Location
Manifest	<a href="https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/manifest.json">https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/manifest.json</a>
Parcel	<a href="https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/CFM-2.0.4.0-80-bionic.parcel">https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/CFM-2.0.4.0-80-bionic.parcel</a>
Sha File	<a href="https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/CFM-2.0.4.0-80-bionic.parcel.sha">https://archive.cloudera.com/p/CFM/2.x/ubuntu18/apt/tars/parcel/CFM-2.0.4.0-80-bionic.parcel.sha</a>

**Table 4: CSD Files**

File	Location
NiFi CSD File	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/NIFI-1.11.4.2.0.4.0-80.jar">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/NIFI-1.11.4.2.0.4.0-80.jar</a>
NiFi Registry CSD File	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/NIFIREGISTRY-0.6.0.2.0.4.0-80.jar">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/parcel/NIFIREGISTRY-0.6.0.2.0.4.0-80.jar</a>

**Table 5: Standalone components**

File	Location
NiFi (.tar.gz)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.tar.gz">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.tar.gz</a>

File	Location
NiFi (.zip)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.zip">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.zip</a>
NiFi (.zip SHA256)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.zip.sha256">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-1.11.4.2.0.4.0-80-bin.zip.sha256</a>
NiFi Registry (.tar.gz)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi_registry/nifi-registry-0.6.0.2.0.4.0-80-bin.tar.gz">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi_registry/nifi-registry-0.6.0.2.0.4.0-80-bin.tar.gz</a>
NiFi Toolkit (.zip)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-toolkit-1.11.4.2.0.4.0-80-bin.zip">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-toolkit-1.11.4.2.0.4.0-80-bin.zip</a>
NiFi Toolkit (zip SHA256)	<a href="https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-toolkit-1.11.4.2.0.4.0-80-bin.zip.sha256">https://archive.cloudera.com/p/CFM/2.x/redhat7/yum/tars/nifi/nifi-toolkit-1.11.4.2.0.4.0-80-bin.zip.sha256</a>

**Table 6: Windows Files**

File	Location
NiFi MSI	<a href="https://archive.cloudera.com/p/CFM/2.x/nifi-2.0.4.0-80.msi">https://archive.cloudera.com/p/CFM/2.x/nifi-2.0.4.0-80.msi</a>
NiFi MSI Sha	<a href="https://archive.cloudera.com/p/CFM/2.x/nifi-2.0.4.0-80.msi.sha">https://archive.cloudera.com/p/CFM/2.x/nifi-2.0.4.0-80.msi.sha</a>