Cloudera Manager 7.13.1

Unified Cloudera Manager Release Notes

Date published: 2024-05-15
Date modified: 2024-05-15

CLOUDERA

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

Cloudera Manager 7.13.3 Release Notes 4
What's New in Cloudera Manager 4
What's new in Platform Support 7
Release Matrix 7
Fixed Issues 8
Known Issues 9
Behavioral Changes 10
Cloudera Manager API Compatibility Matrix 12
Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.13.3 13
Deprecation notices in Cloudera Manager 7.13.3 16
Deprecation Notices for Cloudera Manager 17
Platform, OS, and Environment Support 17

Cloudera Manager 7.13.3 Release Notes

This document provides a summary of the latest updates in Cloudera Manager 7.13.3 and its Cumulative hotfixes. You can review the Release Notes of Cloudera Manager 7.13.3 associated with unified Cloudera Runtime 7.3.3 (includes Cloudera Base on premises and Cloudera on cloud) for release-specific information related to new features and improvements, bug fixes, deprecated features and components, known issues, and changed features that can affect product behavior.

Important:

Note the following requirements and platform support changes before proceeding:

Cloudera Runtime compatibility

Cloudera Manager 7.13.3.0 supports the following Cloudera Runtime versions:

- Cloudera Runtime 7.3.3.0
- Cloudera Runtime 7.3.2 SP2 (7.3.2.20000)
- Cloudera Runtime 7.3.2 SP1 (7.3.2.10000)
- Cloudera Runtime 7.3.2.0
- Cloudera Runtime 7.3.1.600 and higher
- Cloudera Runtime 7.1.9 SP2, including Cumulative Hotfix 2 and subsequent cumulative hotfixes (CHFx)
- Cloudera Runtime 7.1.7 SP3 CHF10

Upgrade instructions

For complete upgrade procedures, see Upgrading Cloudera Manager 7.

Feature and behavior changes

Feature updates, configuration changes, and behavioral updates in Cloudera Manager 7.13.3 directly impact the unified Cloudera Runtime 7.3.3.

Platform support matrix

Platform support changes in Cloudera Manager 7.13.3 apply across the unified Cloudera Runtime 7.3.3. To review supported infrastructure combinations, see the Cloudera support matrix.

What's New in Cloudera Manager

Learn about the new features and changed behavior of Cloudera Manager in Cloudera Manager 7.13.3 and its cumulative hotfixes.

You must be aware of the additional functionalities and improvements to features of Cloudera Manager in Cloudera Manager 7.13.3 and its cumulative hotfixes. Learn how the new features and improvements benefit you.

Cloudera Manager 7.13.3 introduces new features and includes all cumulative hotfixes from 7.13.2.100 through 7.13.2.20000. For a comprehensive record of all updates in Cloudera Manager 7.13.2.x, see What's New in Cloudera Manager 7.13.2.x.

Cloudera Manager 7.13.3.0

System and Security Improvements - Upgraded logging framework to Apache Log4j 2

Cloudera Manager now utilizes Apache Log4j 2 for internal logging and system communications, replacing the legacy Reload4J framework. This architectural upgrade eliminates false-positive security vulnerability reports and provides modern logging capabilities. For configuration migration

steps and file path changes, see Cloudera Manager upgrades the internal logging framework to Apache Log4j 2.

New REST API support for Configuration Change Auditing

Cloudera Manager now introduces a dedicated Representational State Transfer (REST) Application Programming Interface (API) endpoint that retrieves configuration audit history programmatically:

```
GET /api/v58/audits/configChanges
```

External security, compliance, and Security Information and Event Management (SIEM) systems can now query structured configuration change records across clusters, services, roles, and Role Config Groups without manually aggregating raw audit events.

Key Capabilities and Enhancements

- Granular Audit Details: Exposes who changed a setting, the change timestamp, the revision ID, the affected cluster, service, or role, and the previous and new configuration values.
- Flexible Filtering: Supports exact-match filtering by cluster name, service name, configuration parameter name, and specific revision ID point lookups.
- Advanced FIQL Expressions: Supports Feed Item Query Language (FIQL) operators to query by username, role, source (API or Admin Console), and configuration parameters using asterisk (*) wildcard syntax.
- Revision-Level Pagination: Paginates results by complete revision units rather than individual records, which prevents configuration changes from fragmenting across API pages.
- Role-Based Security: Controls access through the AUTH_AUDITS authority (granted to ROLE_ADMIN and ROLE_AUDITOR) and automatically redacts sensitive parameter values, matching the behavior in the Config History user interface.

For more information about request parameters, pagination, and query examples, see Configuration Change Audit API.

Load balancer support for Livy for Spark 3

The Livy for Spark 3 service now has a Livy Load Balancer Address property (livy.lb.uri). When you place a load balancer, such as HAProxy, in front of several Livy for Spark 3 service instances, set this property to the client-facing URL of the load balancer on every instance. Cloudera Manager passes the address to each Livy Server role and adds the load balancer principal to the Livy keytabs when you regenerate them, so that every instance accepts requests and Kerberos authentication for the load balancer hostname. For more information, see Livy load balancing with HAProxyLivy load balancing with HAProxy.

Livy version in the Host Inspector

The Host Inspector now shows the Livy and Livy for Spark 3 versions together with the versions of the other Cloudera Runtime components. To view them, go to Hosts All Hosts Inspect All Hosts , and then click Show Inspector Results.

Health check monitoring for HiveServer2 query compilation

Cloudera Manager now monitors HiveServer2 query compilation performance by tracking the hive_waiting_compile_ops metric. When threads waiting to compile queries reach configured thresholds, Cloudera Manager raises health alerts on HiveServer2 roles:

- **CONCERNING health status:** Raised when the CONCERNING threshold is reached
- **BAD health status:** Raised when the BAD threshold is reached

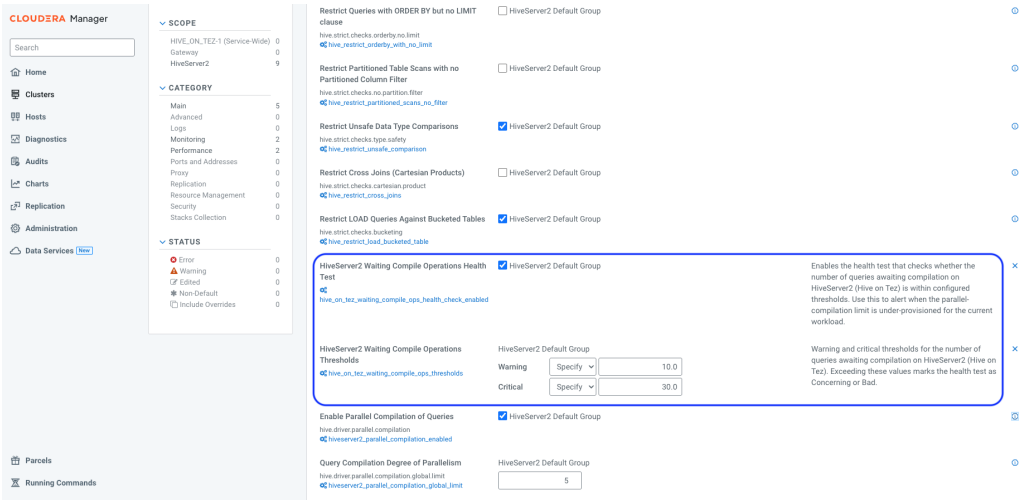
You can configure the CONCERNING and BAD threshold values separately for your environment.

If you experience frequent health alerts, increase the hive.driver.parallel.compilation.global.limit configuration value (default: 5) to allow more concurrent query compilations.

To configure thresholds:

1. In Cloudera Manager, navigate to Clusters Hive Configuration .
2. Search for HiveServer2 Waiting Compile Operations Thresholds.
3. Set the Warning threshold (CONCERNING state) and Critical threshold (BAD state) values:

Figure 1: Compilation thresholds and parallelism settings

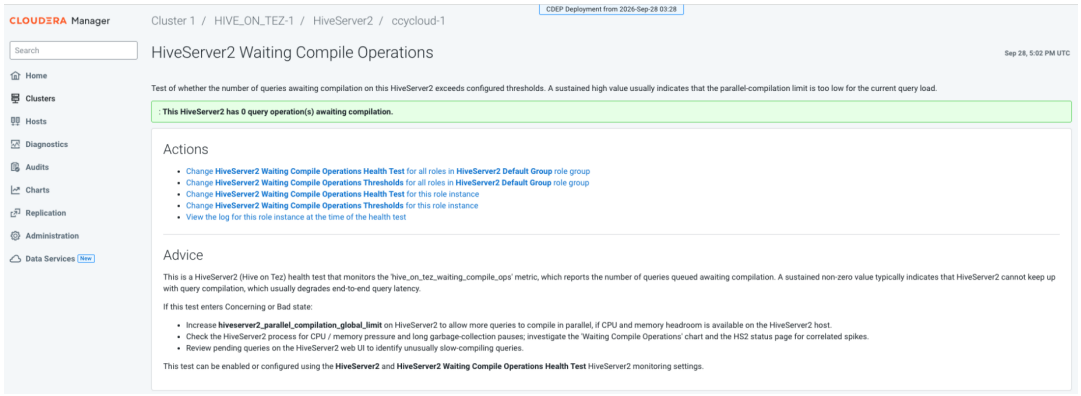


Default values: Warning threshold is 10.0 queries, Critical threshold is 30.0 queries. The Query Compilation Degree of Parallelism defaults to 5.

4. Optionally, increase the Query Compilation Degree of Parallelism value to allow more concurrent query compilations.

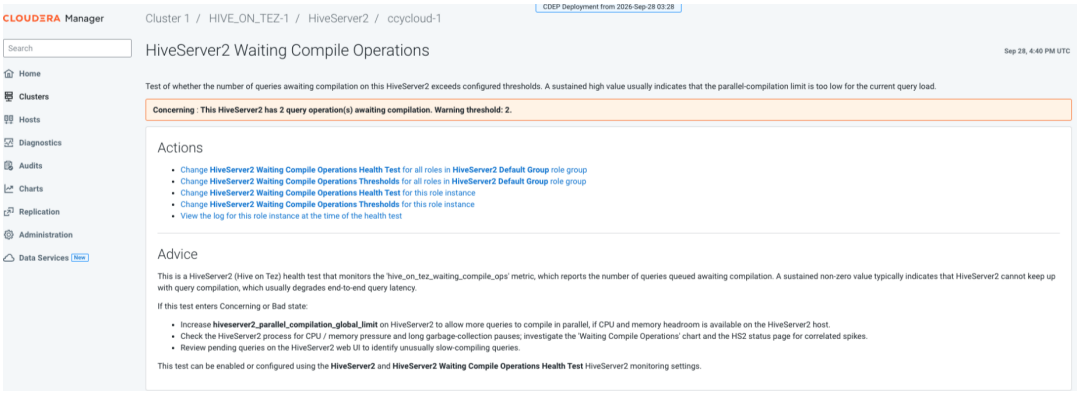
Health check displays: Health check results are displayed on the HiveServer2 role page.

Figure 2: Normal status



When no queries are waiting for compilation, the health test shows green status with 0 operations awaiting compilation.

Figure 3: CONCERNING status



When queries exceed the warning threshold, the health test shows orange status. A sustained high value indicates that the parallel-compilation limit is too low for the current query load.

What's new in Platform Support

Cloudera Manager 7.13.3 release and its cumulative hotfixes introduce expanded platform support across Cloudera Runtime 7.3.3 and its cumulative hotfix releases. Review these additions to plan your infrastructure upgrades and take advantage of newly supported operating systems, databases, Python versions, and Java Development Kits (JDKs).

Cloudera Manager 7.13.3.0

Platform Support Enhancements

New OS support

None

New Database support

None

New Python support

None

New JDK support

None

Release Matrix

You must be familiar with the versions of all the cumulative hotfixes for Cloudera Manager 7.13.3.

The Release build number has two parts, the [*Cloudera Manager release version number*] and the [*Cloudera Manager Build number*]. For example, in 7.13.3.100-69, 7.13.3.100 is the release version number and 69 is the build number.

Table 1: Cloudera Manager versions certified with Cloudera Base on premises

Cloudera Manager 7.13.3 Release Series	Cloudera Manager Release Build Number	GBN	Release Date	Download URL
7.13.3.0	7.13.3.0-49	84934162	November 13, 2026	https://archive.cloudera.com/p/cm7/7.13.3.0/

Fixed Issues

Review the list of Cloudera Manager issues that are resolved in Cloudera Manager 7.13.3 and its cumulative hotfixes.

Cloudera Manager 7.13.3 resolves issues and incorporates fixes from the cumulative hotfixes from 7.13.2.100 through 7.13.2.20000. For a comprehensive record of all fixes in Cloudera Manager 7.13.2.x, see Fixed Issues 7.13.2.x.

Cloudera Manager 7.13.3.0

OPSAPS-79698: ATLAS is not accessible for GCP cluster with LIGHT_DUTY_WITHOUT_HBASE

7.13.2.30000

Previously, when database SSL was enabled for Atlas on a GCP cluster using PostgreSQL RDS, Cloudera Manager configured the JanusGraph JDBC URL with sslmode=verify-full. This caused hostname verification to fail because only an IP address was available, preventing Atlas from starting. This issue is now resolved. When atlas.db.ssl.verifyServerCertificate is true and atlas.db.ssl .certificateFile is set, Cloudera Manager uses sslmode=verify-ca instead.

OPSAPS-81307: Ozone refresh cluster command fails due to missing Kerberos configuration

7.13.3.0

Previously, the Ozone `refresh cluster` command failed in Kerberos-enabled environments because the refresh handlers did not include the moveConfigs operation. This caused the Ozone client to fall back to simple authentication, which resulted in access control errors. This issue is now resolved by adding the moveConfigs operation to all Ozone refresh handlers, which ensured that the necessary Kerberos settings were correctly applied during a cluster refresh.

OPSAPS-76171: Cloudera Manager skips the INVALIDATE METADATA step when an Impala Daemon reports a warning status

7.13.3.0

Previously, during Hive external table replication with Replication Manager, Cloudera Manager silently skipped the INVALIDATE METADATA step if an Impala Daemon reported any health test warning, such as an upcoming certificate expiration. Cloudera Manager did not run the command and did not provide an explanation in the command history or server logs.

This issue is now resolved by introducing the Impala Health Threshold For Skipping Invalidate Metadata setting. The default value is now Red, which skips metadata invalidation only when an Impala Daemon experiences a critical failure. Health test warnings no longer prevent Cloudera Manager from executing the step. When Cloudera Manager skips the step, it documents the reason in the command history and records the event in the Cloudera Manager server log.

OPSAPS-78574, OPSAPS-80536: Cloudera Manager skips scheduled commands when the scheduler is unavailable or overloaded

7.13.3.0

Previously, Cloudera Manager omitted scheduled commands (such as replication policies and snapshot policies) when administrators scheduled more than approximately 30 commands to run simultaneously. Because Cloudera Manager initiated commands sequentially within a single minute, commands that could not start within that minute failed to run. Additionally, when Cloudera Manager shut down or heavy workloads overloaded the scheduler during a scheduled execution window, the scheduler skipped those commands entirely and did not execute them later.

Cloudera Manager now triggers missed commands immediately when the scheduler becomes available. Even if an outage or period of heavy load spans multiple scheduled intervals, Cloudera Manager triggers only a single execution upon recovery. For example, if you schedule a command to run every two hours, and the scheduler remains unavailable for seven hours, Cloudera Manager executes that command once immediately when the scheduler recovers, and runs the subsequent execution at its next regular scheduled time. This issue is now resolved by setting the scheduler misfire policy to FIRE_ONCE_NOW by default.

OPSAPS-79524: Improved Replications page performance when loading Hive ACID policies

7.13.3.0

Previously, the Replications page took more than a minute to load in environments with more than 100 Apache Hive ACID policies. For each Hive ACID policy, the service issued two sequential remote calls to the source, which slowed down the page load time for all policies.

This issue is now resolved by consolidating the queries into a single remote call per source. The Replications page now loads faster without initiating multiple remote calls per policy.

Known Issues

You must be aware of the known issues and limitations, the areas of impact, and workaround in Cloudera Manager 7.13.3 and its cumulative hotfixes.

Known issues identified in Cloudera Manager 7.13.3.0

OPSAPS-81194: Cloudera Manager Server experiences memory leaks and potential Out Of Memory (OOM) errors due to unclosed NettyTransceiver connections

7.13.3.0

In Cloudera Manager 7.13.3.0, Cloudera Manager Server leaks Avro RPC publisher connections (NettyTransceiver) to the Event Server approximately once every minute. Over time, these unclosed connections accumulate threads, connections, and heap memory, eventually causing Cloudera Manager Server to run out of memory (OOM) and crash.

This issue affects installations running Cloudera Manager 7.13.3.0.



Important: Increasing the Cloudera Manager Server Java heap size only delays the failure. Restarting the Event Server, restarting the Cloudera Management Service, or disabling Enable Log Event Capture does not resolve this issue.

Periodically restart the Cloudera Manager Server before JVM memory usage reaches its limit. Restarting the server releases all leaked threads, active network connections, and consumed memory.

1. Check the current thread and Event Server connection counts on the Cloudera Manager Server host:

   ```
   ps -o nlwp=,rss= -p $(pgrep -f com.cloudera.server.cmf.Main)
   ss -tn | grep -c ':7184'
   ```

   While this issue persists, both values increase by approximately 1,440 per day.
2. Restart the Cloudera Manager Server:

   ```
   sudo systemctl restart cloudera-scm-server
   ```

3. Schedule a recurring restart interval based on your observed resource growth rate. For example, a server using the default 8 GB Java heap typically requires a restart every 5 to 7 days to maintain an adequate memory buffer.

CDPD-99324: Livy gateway role is available only on the first Livy for Spark 3 service

7.13.3.0

When a cluster has more than one Livy for Spark 3 service, for example to place several Livy for Spark 3 service instances behind a load balancer, Cloudera Manager supports the Livy gateway role only on the first Livy for Spark 3 service. You cannot add the gateway role to the second or any later Livy for Spark 3 service.

Add the Livy gateway role only to the first Livy for Spark 3 service. Point clients to the client-facing URL of the load balancer, or to Knox, instead of to an individual Livy for Spark 3 service. For more information, see Livy load balancing with HAProxyLivy load balancing with HAProxy.

Behavioral Changes

You can review the changes in certain features or functionalities of Cloudera Manager that have resulted in a change in behavior from the previously released version to this version of Cloudera Manager 7.13.3.

Cloudera Manager 7.13.3 introduces functional adjustments, behavioral updates, and includes all cumulative hotfixes from 7.13.2.100 through 7.13.2.20000. For a comprehensive record of all functional adjustments in Cloudera Manager 7.13.2.x, see Behavioral Changes 7.13.2.x.

Cloudera Manager 7.13.3.0

Summary: Cloudera Manager updates the health threshold and visibility for skipping the INVALIDATE METADATA step during Hive external table replication

Starting in Cloudera Manager 7.13.3.0, Cloudera Manager updates how it evaluates Impala Daemon health when deciding whether to execute the INVALIDATE METADATA step during Hive external table replication with Replication Manager. Previously, Cloudera Manager skipped this step whenever an Impala Daemon reported any warning, even when the daemon remained operational. This behavior caused out-of-synchronization Impala metadata and occurred without explanatory status updates or log messages.

To prevent unnecessary skips while maintaining cluster stability, Cloudera Manager introduces the Impala Health Threshold For Skipping Invalidate Metadata parameter. The default threshold is now less strict (Red), which allows metadata invalidation to run when daemons report minor warnings. Additionally, Cloudera Manager now logs the specific reason whenever it skips this step and displays the cause on the command details page.

Previous behavior:

In Cloudera Manager versions earlier than 7.13.3.0, during Hive external table replication with Replication Manager, Cloudera Manager skipped the INVALIDATE METADATA step if any health check on the destination Impala Daemons generated a warning status or worse. Cloudera Manager skipped the step silently without recording the reason in the command execution history or the Cloudera Manager server logs.

New behavior:

Starting in Cloudera Manager 7.13.3.0, the new Impala Health Threshold For Skipping Invalidate Metadata configuration parameter controls when the INVALIDATE METADATA step runs.

The parameter supports the following values:

- Red: (Default) Cloudera Manager skips the step only if an Impala Daemon reports a bad or critical health state. Health check warnings do not prevent the step from running.
- Yellow: Cloudera Manager skips the step if an Impala Daemon reports any warning or critical health state. This option preserves the previous behavior.
- None: Cloudera Manager always runs the step regardless of the Impala Daemon health state.

When Cloudera Manager skips the INVALIDATE METADATA step, it adds an explanatory message to the command execution details and records the reason in the Cloudera Manager server log.

Summary: Cloudera Manager upgrades the internal logging framework to Apache Log4j 2

In Cloudera Manager 7.13.3.0, the logging framework transitions from Reload4J (a Log4j 1 fork) to Apache Log4j 2. Cloudera Manager continues to utilize Simple Logging Facade for Java (SLF4J) for log routing but replaces the active configuration file path and format. Existing custom logging

configurations do not migrate automatically to the new Log4j 2 file format. If you customized logging settings in prior versions, you must manually apply those changes to the new configuration file.

Previous behavior:

In Cloudera Manager 7.13.2 and earlier releases, Cloudera Manager used Reload4J (a fork of Log4J version 1) for system logging and internal communications. This framework triggered false-positive vulnerability reports in automated security scanning tools. Cloudera Manager read logging properties from the /etc/cloudera-scm-server/log4j.properties file.

New behavior:

Cloudera Manager no longer packages or uses Reload4J. Cloudera Manager now uses Apache Log4j 2 for internal communications and system logging:

- Cloudera Manager now reads logging configurations from the /etc/cloudera-scm-server/log4j2.properties file.
- Cloudera Manager ignores the previous /etc/cloudera-scm-server/log4j.properties file.



Important: Cloudera Manager does not automatically migrate prior custom logging configurations to the new file. You must manually port any custom settings from the legacy file to the new /etc/cloudera-scm-server/log4j2.properties file using standard Apache Log4j 2 syntax.

Summary: Cloudera Manager validates the location argument in addCustomCerts requests against the configured CMCA storage mode

Cloudera Manager now validates the location parameter in addCustomCerts API requests against the inferred Cloudera Manager Certificate Authority (CMCA) storage mode (derived from the HOST_CERT_GENERATOR setting) before issuing the command. Invalid requests fail immediately with an HTTP 400 error (IllegalArgumentException), and Cloudera Manager does not create or persist a database command. You can bypass this validation by setting the new optional parameter disableLocationValidation to true.

Previous behavior:

Previously, Cloudera Manager did not validate the location parameter against HOST_CERT_GENERATOR or inferred CMCA storage mode before issuing addCustomCerts. The API accepted the request, persisted the command, and showed it under Recent Commands.

At command execution, Cloudera Manager resolved location as follows:

- Non-empty location: Used the supplied path directly. Cloudera Manager did not compare it to the configured CMCA directory or to database-backed storage.
- Omitted or blank location:
  - If there was no ROOT CA certificate in the Auto-TLS certificate database, Cloudera Manager used the legacy default filesystem path /var/lib/cloudera-scm-server/certmanager.
  - If a ROOT CA certificate existed in that database, Cloudera Manager extracted the CMCA archive from the database into a temporary directory, ran certmanager there, and (on success) persisted updated host certificates back to the database. This path did not use HOST_CERT_GENERATOR to locate an on-disk CMCA tree.

If callers supplied an incorrect location, the command failed asynchronously during execution with generic errors or stack traces instead of rejecting the request at submission time.

New behavior:

By default (disableLocationValidation: false), Cloudera Manager validates the location argument against the inferred CMCA storage mode before assembling command steps:

- Filesystem-backed CMCA: When HOST_CERT_GENERATOR ends with /generate_host_cert, you must pass a location argument that matches the parent CMCA directory (for example, if

HOST_CERT_GENERATOR is /opt/cloudera/CMCA/generate_host_cert, pass "location": "/opt/cloudera/CMCA"). Cloudera Manager compares normalized paths. Requests fail with an HTTP 400 error if you omit location or if location does not match the configured CMCA directory.

- Database-backed CMCA: When HOST_CERT_GENERATOR equals the temporary directory marker, you must omit the location parameter entirely. If you provide a location parameter, Cloudera Manager rejects the request with an HTTP 400 error.
- Legacy or Non-standard Setups: When HOST_CERT_GENERATOR uses a pattern from which Cloudera Manager cannot infer the CMCA location, Cloudera Manager skips validation and retains the previous flexibility for passing or omitting location.

When validation fails, Cloudera Manager rejects the request before persisting the command, which prevents generating a command ID or displaying an entry under Recent Commands.

Important:

If existing automations rely on the previous behavior, set disableLocationValidation to true to skip validation and restore previous acceptance rules.

Summary: Cloudera Manager 7.13.3 removes legacy API endpoints for end-of-support CDH 3.x, 4.x, and 5.x releases. API requests to these endpoints now return HTTP 404 Not Found instead of HTTP 400 Bad Request or HTTP 410 Gone.

Previous behavior:

Cloudera Manager returned the following HTTP status codes when calling deprecated CDH 5 API endpoints:

- POST /{serviceName}/commands/hbaseUpgrade # HTTP 400 Bad Request
- POST /{serviceName}/commands/impalaEnableLlamaRm # HTTP 410 Gone
- POST /{serviceName}/commands/impalaDisableLlamaRm # HTTP 410 Gone
- POST /{serviceName}/commands/impalaEnableLlamaHa # HTTP 410 Gone
- POST /{serviceName}/commands/impalaDisableLlamaHa # HTTP 410 Gone

New behavior:

Cloudera Manager returns an HTTP 404 Not Found status code for all requests to these unsupported API endpoints:

- POST /{serviceName}/commands/hbaseUpgrade # HTTP 404 Not Found
- POST /{serviceName}/commands/impalaEnableLlamaRm # HTTP 404 Not Found
- POST /{serviceName}/commands/impalaDisableLlamaRm # HTTP 404 Not Found
- POST /{serviceName}/commands/impalaEnableLlamaHa # HTTP 404 Not Found
- POST /{serviceName}/commands/impalaDisableLlamaHa # HTTP 404 Not Found

Cloudera Manager API Compatibility Matrix

This document provides the Cloudera Manager API Compatibility Matrix to ensure seamless communication between automated clients and the Cloudera Manager server. This matrix defines the required Python environments and minimum Cloudera Manager versions necessary for specific API client versions and REST endpoints to function correctly.

To maintain system stability and avoid breaking changes, Cloudera Manager enforces strict versioning for its API clients and REST interfaces. This compatibility framework allows administrators to upgrade Cloudera Manager while understanding the impact on existing automation scripts and custom integrations.

- Python Support: Each cm-client version requires a specific Python runtime to execute successfully.
- Version Alignment: Upgrading to a newer REST API version (for example, v57 to v58) typically requires a corresponding minimum Cloudera Manager backend version to support the newer features and data structures.
- Backward Compatibility: While newer Cloudera Manager versions generally support older API clients, using an outdated cm-client with a modern Cloudera Manager server might limit access to the latest platform capabilities.

Cloudera Manager Client Compatibility

The following table identifies the supported Python environments and the minimum Cloudera Manager version required for each cm-client release.

cm-client Version	Supported Python Versions	Minimum Cloudera Manager / Runtime Versions Supported
58.0.2	3.11	7.13.2 / 7.3.2.0

REST API Version Support

This table maps the REST API endpoint versions to the minimum Cloudera Manager version required to host them.

REST API Version	Minimum Cloudera Manager Version Supported
v58	7.13.2.0
v57	7.13.1.0
v54	7.11.3.0

Fixed Common Vulnerabilities and Exposures in Cloudera Manager 7.13.3

Common Vulnerabilities and Exposures (CVE) that are fixed in Cloudera Manager 7.13.3.

Cloudera Manager 7.13.3.0

CVEs	Package Name
CVE-2025-68121	stdlib
CVE-2026-33701	io.opentelemetry.javaagent:opentelemetry-javaagent
CVE-2026-27459	pyOpenSSL
CVE-2026-27727	com.mchange:mchange-commons-java
CVE-2026-33454	org.apache.camel:camel-mail
CVE-2026-33186	google.golang.org/grpc
CVE-2025-14813	org.bouncycastle:bcprov-jdk18on
CVE-2025-47273	setuptools
CVE-2026-0603	org.hibernate:hibernate-core
CVE-2026-33997	github.com/docker/docker
CVE-2026-34040	github.com/docker/docker
CVE-2026-3505	org.bouncycastle:bcpg-jdk18on
CVE-2025-66471	urllib3
CVE-2026-50645	org.apache.cxf:cxf-core
CVE-2026-39836	stdlib
CVE-2026-32283	stdlib
CVE-2025-7962	com.sun.mail:jakarta.mail
CVE-2026-21441	urllib3
CVE-2026-41205	Mako
CVE-2025-68156	github.com/expr-lang/expr
CVE-2026-33811	stdlib
CVE-2026-42198	org.postgresql:postgresql

CVEs	Package Name
CVE-2026-32287	github.com/antchfx/xpath
CVE-2026-39820	stdlib
CVE-2026-34480	org.apache.logging.log4j:log4j-core
CVE-2026-32281	stdlib
CVE-2026-34478	org.apache.logging.log4j:log4j-core
CVE-2025-66418	urllib3
CVE-2026-42306	github.com/docker/docker
CVE-2026-39883	go.opentelemetry.io/otel/sdk
CVE-2024-45338	golang.org/x/net
CVE-2026-25679	stdlib
CVE-2026-69249	cryptography
CVE-2026-41567	github.com/docker/docker
CVE-2026-55153	com.mchange:mchange-commons-java
CVE-2026-41720	org.springframework.ldap:spring-ldap-core
CVE-2026-27145	stdlib
CVE-2024-34156	stdlib
CVE-2025-61729	stdlib
CVE-2026-44307	Mako
CVE-2026-42504	stdlib
CVE-2026-27830	com.mchange:c3p0
CVE-2026-24051	go.opentelemetry.io/otel/sdk
CVE-2025-47913	golang.org/x/crypto
CVE-2026-45300	org.asynchttpclient:async-http-client
GHSA-537c-gmf6-5ccf	cryptography
CVE-2024-45337	golang.org/x/crypto
CVE-2026-32280	stdlib
CVE-2026-42499	stdlib
CVE-2025-61726	stdlib
CVE-2026-39822	stdlib
CVE-2026-68494	com.fasterxml.jackson.core:jackson-core
CVE-2025-22869	golang.org/x/crypto
CVE-2026-26007	cryptography
CVE-2026-32282	stdlib
CVE-2025-50181	urllib3
CVE-2025-50182	urllib3
CVE-2026-32289	stdlib
CVE-2026-49844	org.apache.logging.log4j:log4j-api
CVE-2026-34477	org.apache.logging.log4j:log4j-core
CVE-2025-53864	com.nimbusds:nimbus-jose-jwt

CVEs	Package Name
CVE-2026-32288	stdlib
CVE-2026-34073	cryptography
CVE-2026-44431	urllib3
CVE-2025-58190	golang.org/x/net
CVE-2025-47911	golang.org/x/net
CVE-2024-47081	requests
CVE-2026-27448	pyOpenSSL
CVE-2025-54388	github.com/docker/docker
CVE-2025-58188	stdlib
CVE-2026-42507	stdlib
CVE-2025-47906	stdlib
CVE-2026-5588	org.bouncycastle:bcpkix-jdk18on
CVE-2025-61730	stdlib
CVE-2026-59230	org.apache.camel:camel-mail
CVE-2025-58185	stdlib
CVE-2025-47912	stdlib
CVE-2025-61724	stdlib
CVE-2026-27142	stdlib
CVE-2026-18401	com.fasterxml.jackson.core:jackson-core
CVE-2024-45336	stdlib
CVE-2025-71405	github.com/go-chi/chi/v5
CVE-2024-34155	stdlib
CVE-2026-39823	stdlib
CVE-2025-47914	golang.org/x/crypto
CVE-2026-40490	org.asynchttpclient:async-http-client
CVE-2025-22870	golang.org/x/net; stdlib
CVE-2025-0913	stdlib
CVE-2026-39826	stdlib
CVE-2024-34158	stdlib
CVE-2025-22866	stdlib
CVE-2025-47907	stdlib
CVE-2025-61727	stdlib
CVE-2026-39882	go.opentelemetry.io/otel/exporters/otlp/otlplog/otlploghttp; go.opentelemetry.io/otel/exporters/otlp/otlpmetric/otlpmetrichttp; go.opentelemetry.io/otel/exporters/otlp/otlptrace/otlptracehttp
CVE-2025-22872	golang.org/x/net
CVE-2026-42505	stdlib
CVE-2025-22871	stdlib
CVE-2026-55688	org.asynchttpclient:async-http-client
CVE-2026-0636	org.bouncycastle:bcprov-jdk18on

CVEs	Package Name
CVE-2025-58187	stdlib
CVE-2025-58189	stdlib
CVE-2026-39825	stdlib
CVE-2025-58183	stdlib
GHSA-h4gh-qq45-vh27	cryptography
CVE-2025-22873	stdlib
CVE-2025-8869	pip
CVE-2025-61723	stdlib
CVE-2026-41568	github.com/docker/docker
CVE-2026-2303	go.mongodb.org/mongo-driver
CVE-2025-58181	golang.org/x/crypto
CVE-2025-61728	stdlib
CVE-2025-4673	stdlib
CVE-2025-61725	stdlib
CVE-2025-58186	stdlib
CVE-2024-45341	stdlib
CVE-2024-12797	cryptography
CVE-2026-27139	stdlib
CVE-2026-69248	cryptography
CVE-2025-66566	at.yawk.lz4:lz4-java

Deprecation notices in Cloudera Manager 7.13.3

Certain features and functionalities have been removed or deprecated in Cloudera Manager 7.13.3. You must review these items to understand whether you must modify your existing configuration. You can also learn about the features that will be removed or deprecated in the future release to plan for the required changes.

Terminology

Items in this section are designated as follows:

Deprecated

Technology that Cloudera is removing in a future Cloudera Manager release. Marking an item as deprecated gives you time to plan for removal in a future Cloudera Manager release.

Moving

Technology that Cloudera is moving from a future Cloudera Manager release and is making available through an alternative Cloudera offering or subscription. Marking an item as moving gives you time to plan for removal in a future Cloudera Manager release and plan for the alternative Cloudera offering or subscription for the technology.

Removed

Technology that Cloudera has removed from Cloudera Manager and is no longer available or supported as of this release. Take note of technology marked as removed since it can potentially affect your upgrade plans.

Deprecation Notices for Cloudera Manager

Certain features and functionality are deprecated or removed in Cloudera Manager 7.13.3. You must review these changes along with the information about the features in Cloudera Manager that will be removed or deprecated in a future release.

Removal of legacy CDH 3.x, 4.x, and 5.x cluster management support and API endpoints

Cloudera Manager 7.13.3 removes all legacy code paths, management workflows, and REST API endpoints associated with end-of-support CDH 3.x, 4.x, and 5.x releases. Because CDH 3.x, 4.x, and 5.x reached end-of-support status previously, Cloudera Manager no longer supports managing, monitoring, or configuring these legacy releases.

This change cleans up obsolete code paths and does not impact supported target platforms, such as CDP Private Cloud Base or Cloudera Runtime 7.x.

Affected components and services

Cloudera Manager 7.13.3 removes the following API endpoints and legacy services:

- HBase Upgrade API:
  - POST /{serviceName}/commands/hbaseUpgrade
- Low Latency Application Master (LLAMA) Service APIs:
  - POST /{serviceName}/commands/impalaEnableLlamaRm
  - POST /{serviceName}/commands/impalaDisableLlamaRm
  - POST /{serviceName}/commands/impalaEnableLlamaHa
  - POST /{serviceName}/commands/impalaDisableLlamaHa
- Legacy Services:
  - Sqoop 2 service integration and configuration.

Impact and behavioral changes

- Management capabilities: Upgrading Cloudera Manager to version 7.13.3 removes all functionality required to manage, monitor, or configure existing CDH 3.x, 4.x, or 5.x clusters.
- REST API status code changes: Automated scripts or API clients calling removed endpoints now receive an HTTP 404 Not Found response code instead of the previously returned HTTP 400 Bad Request or HTTP 410 Gone status codes.

Action required

Before upgrading Cloudera Manager to version 7.13.3, migrate any remaining CDH 3.x, 4.x, or 5.x workloads and clusters to a supported Cloudera Base on premises release line. Additionally, update any custom automation scripts to remove references to the deprecated LLAMA, Sqoop 2, and HBase upgrade API endpoints.

Platform, OS, and Environment Support

Cloudera Manager 7.13.3 and its cumulative hotfixes remove support for several operating systems, databases, Python versions, and Java Development Kits (JDKs). To ensure a successful upgrade, verify that your environment meets these new requirements.

Cloudera Manager 7.13.3.0

Database Support

None

Operating System

None

Python Support

None

JDK Support

None