

Cloudera Private Cloud Experiences 1.3.3

# Cloudera Private Cloud Experiences Release Notes

Date published: 2020-12-15

Date modified: 2022-01-12

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 a horizontal bar extending to the right.

<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>Data Services Release Notes.....</b>	<b>4</b>
<b>CVE-2021-44228 remediation for CDP Private Cloud Data Services</b>	
<b>1.4.0.....</b>	<b>4</b>

## Data Services Release Notes

CDP Private Cloud Data Services includes Management Console, Cloudera Data Warehouse (CDW), Cloudera Machine Learning (CML) and Cloudera Data Engineering (CDE). Learn about the new features and improvements in each of these experiences.

Learn about the new features and improvements in:

- [Management Console](#)
- [Cloudera Data Warehouse \(CDW\)](#)
- [Cloudera Machine Learning \(CML\)](#)
- [Cloudera Data Engineering \(CDE\)](#)

log4j Remediation: [CVE-2021-44228 remediation for CDP Private Cloud Data Services 1.4.0](#) on page 4

In addition, learn about the new features and improvements in Cloudera Manager 7.6.5 supported with this version of CDP Private Cloud Experiences.

[Cloudera Manager](#)

## CVE-2021-44228 remediation for CDP Private Cloud Data Services 1.4.0

CDP Private Cloud Data Services 1.4.0 contains mitigation for the Apache Log4j vulnerability tracked at CVE-2021-44228. The mitigation is achieved either by upgrading the embedded Log4j version to 2.17.1 or by removing the affected classes.



**Note:** This release does *not* contain fixes for the subsequent Log4j CVEs including CVE-2021-44832, CVE-2021-45046, and CVE-2021-45105 (denial of service attack using specially crafted log entries with custom Log4j configuration settings). Cloudera is continuing to update product lines as newer versions of Log4j are made available.

### Dependencies

CDP Private Cloud Data Services 1.4.0 requires that you upgrade Cloudera Manager (CM) to version 7.5.5 which contains the mitigation for the Log4j vulnerability.

### Remediation for Management Console

CVE-2021-44228 has been addressed in the Management Console on CDP Private Cloud Data Services 1.4.0 by upgrading Apache Log4j 2 to version 2.17.1

### Remediation for Cloudera Machine Learning (CML)

The CML engine image engine:15-cml-2021.09-2 removes the JndiLookup class from all Log4j versions in the engine image. This update addresses the issue found in CVE-2021-44228. An inaccessible log4j2 jar is also present in /root but the jar file is not reachable by CML sessions. Therefore, the jar file does not pose a security threat.



**Note:** You can upgrade CML workspaces only on OpenShift deployments. On ECS deployments, you cannot upgrade existing CML workspaces. Therefore, you must launch new workspaces.

### Remediation for Cloudera Data Engineering (CDE)

CVE-2021-44228 has been addressed in CDE on CDP Private Cloud Data Services 1.4.0 by upgrading Apache Log4j 2 to version 2.17.1.



**Note:** In-place upgrade is still not supported for CDE virtual clusters. You must back up the job details from the running virtual clusters, and restore the jobs after creating virtual clusters based on version 1.4.0.

### Remediation for Cloudera Data Warehousing (CDW)

CVE-2021-44228 has been addressed in CDW on CDP Private Cloud Data Services 1.4.0 by upgrading Apache Log4j 2 to version 2.17.1.



**Note:** After upgrading to CDP Private Cloud Data Services 1.4.0, you must recreate the database catalogs and warehouses.