

Ranger and Observability Integration

Date published: 2020-07-28

Date modified: 2026-03-31



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

Overview of Ranger and Observability integration.....	4
Configuration details of supported Ranger modules.....	4
Ranger Admin.....	4

Overview of Ranger and Observability integration

This guide provides the foundational knowledge and structured processes necessary to connect Apache Ranger with Cloudera's OpenTelemetry-native telemetry framework.

Modern enterprise data platforms face severe reputational and brand risks if data is exposed or left unmonitored. Regulated organizations demand total operational visibility alongside strict adherence to compliance standards like FIPS 140-3 and FedRAMP High. Meeting these requirements necessitates a standardized approach to tracking platform security compliance, ensuring that every security policy evaluation and audit event is captured efficiently and securely.

To achieve this, the Cloudera Observability framework leverages the `cdp-opentelemetry-collector`, a custom distribution of the OpenTelemetry Collector. This component acts as the unified telemetry pipeline across both virtual machine (VM) and Kubernetes (K8s) cluster form factors. By onboarding Apache Ranger into this architecture, platform administrators can seamlessly collect system metrics and stream vital security log records directly to Cloudera-managed data storages and backend analytical engines.

By following this guide, service teams can successfully establish deep security observability for Apache Ranger, reinforcing the data platform's perimeter security with high-performance and compliant monitoring.

Configuration details of supported Ranger modules

The integration between Cloudera Observability and Apache Ranger is modularly designed around specific platform roles and telemetry types to ensure comprehensive security monitoring and system visibility.

The initial scope of this integration officially supports the following modules:

- Ranger Admin

The integration modules are natively supported across all primary Cloudera deployment footprints managed through Cloudera Manager, including:

- DataHub
- Data Lake
- Cloudera Base on premises clusters

This modular approach ensures that regardless of where Ranger Admin is running, their telemetry data can be seamlessly pulled and routed to the backend analytical engines.

Ranger Admin

The integration between Observability and Ranger Admin is enabled by default. Based on your requirements, you can disable it.

Ranger Admin is the centralized management component of Apache Ranger, an open-source framework used to enable, monitor, and manage data security across big data platforms and cloud storage environments. It serves as the core user interface and control center where security administrators define, coordinate, and track data access policies.

A configuration property called `ranger.admin.observability.metrics.enabled` in the `ranger-admin-site.xml` enables the integration between Observability and Ranger Admin. The property is enabled by default with the value set to `true`. If you want to disable the integration between Observability and Ranger Admin, set its value to `false` as follows:

1. Log in to Cloudera Manager.
2. Navigate to Ranger Configuration .
3. Search for Ranger Admin Advanced Configuration Snippet (Safety Valve) for `conf/ranger-admin-site.xml`.
4. Set the value of the `ranger.admin.observability.metrics.enabled` property to `false`.

5. Save changes.