Configure for KMS

Hadoop KMS is a key management system that enables encrypted transport to and from the Hadoop cluster. This section describes how to configure the Trifacta® platform for integration with KMS.

> **NOTE:** The Trifacta platform supports encryption at rest only through the KMS solution provided with the Hadoop distribution. Generic encryption at rest is not supported.

> **NOTE:** If KMS is enabled on the cluster, you must configure KMS for the Trifacta platform regardless of other security features enabled on the cluster.

- For more information on KMS, see *https://hadoop.apache.org/docs/stable/hadoop-kms/index.html*.

> **NOTE:** The required configuration for integrating with each Hadoop distribution may vary. Please be sure to review the details.

Pre-requisites

1. You have installed the Trifacta software. See *Install*.
2. You have performed the basic configuration steps for Hadoop. See *Configure for Hadoop*.
3. You have enabled any required secure authentication services.
    a. See *Set up for a Kerberos-enabled Hadoop cluster*.
    b. See *Configure for secure impersonation*.

Configure by Distribution Type

> **KMS is a cluster-wide configuration. If you are enabling Kerberos, secure impersonation, or encryption at rest on the cluster, you must perform the KMS site configuration changes in the pages for your specific Hadoop distribution.**

Cloudera/Sentry: See *Configure for KMS for Sentry*.

Hortonworks/Ranger: See *Configure for KMS for Ranger*.

Copyright © 2021 Trifacta Inc.