Cloudera Data Science Workbench

Restricting User-Controlled Kubernetes Pods

Date published: 2020-02-28
Date modified:

https://docs.cloudera.com/

Legal Notice

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.

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

Restricting User-Controlled Kubernetes Pods

Cloudera Data Science Workbench 1.6.0 (and higher) includes three properties that allow you to control the permissions granted to user-controlled Kubernetes pods.

Required Role: Site Administrator

An example of a user-controlled pod is the engine pod, which provides the environment for sessions, jobs, etc. These pods are launched in a per-user Kubernetes namespace. Since the user has the ability to launch arbitrary pods, these settings restrict what those pods can do.

They are available under the site administrator panel at Admin Security under the Control of User-Created Kubernetes Pods section.

Do not modify these settings unless you need to run pods that require special privileges. Enabling any of these properties puts CDSW user data at risk.

Allow containers to run as root

Security best practices dictate that engine containers should not run as the root user. Previously, engines (v7 and lower) would briefly initialize as the root user and then run as the cdsw user. With engine v8 (and higher), engines now follow the best practice and run only as the cdsw user.

Use the following sections to determine whether you need to perform any steps to take advantage of this feature.

New Deployments - Version 1.6.0 (or higher)

Cloudera Data Science Workbench 1.6 (and higher) ships with engine v8 (and higher). On such deployments, all projects should already be using the latest engine versions. Therefore, this property should be left disabled .

Upgrades from Version 1.5.x (and lower) to 1.6.0 (or higher)

For deployments that have upgraded from Cloudera Data Science Workbench 1.5 (or lower), it is likely that projects on your deployment are still using base engine v7 (or lower). On such deployments, this property will be enabled by default.

Perform the following steps so that you can disable this property to take advantage of the security fix:

1. Upgrade to Cloudera Data Science Workbench 1.6 (or higher).
2. Test and upgrade all projects to engine v8 (or higher). If you are using custom engines, you will need to rebuild these engines using engine v8 or higher as the base image.
3. Go to Admin Security . Under the Control of User-Created Kubernetes Pods section, disable the Allow containers to run as root checkbox.

Allow "privileged" pod containers

Pod containers that are "privileged" are extraordinarily powerful. Processes within such containers get almost the same privileges that are available to processes outside the container. If this property is enabled, a privileged container could potentially access all data on the host.

This property is disabled by default .

Allow pod containers to mount unsupported volume types

The volumes that can be mounted inside a container in a Kubernetes pod are already heavily restricted. Access is normally denied to volume types that are unfamiliar, such as GlusterFS, Cinder, Fibre Channel, etc. If this property is enabled, pods will be able to mount all unsupported volume types.

This property is disabled by default .