

# Configuring SELinux for Cloudera environments (Preview)

Date published: 2025-02-07

Date modified: 2025-02-07

## Legal Notice

© Cludera Inc. 2024. All rights reserved.

The documentation is and contains Cludera 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 Cludera software may be found within the documentation accompanying each component in a particular release.

Cludera 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 Cludera software product page for more information on Cludera software. For more information on Cludera support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Cludera reserves the right to change any products at any time, and without notice. Cludera assumes no responsibility nor liability arising from the use of products, except as expressly agreed to in writing by Cludera.

Cludera, Cludera Altus, HUE, Impala, Cludera Impala, and other Cludera 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.

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cludera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## Contents

<b>Legal Notice</b>	<b>2</b>
<b>Contents</b>	<b>3</b>
<b>Overview</b>	<b>3</b>
<b>Before you begin</b>	<b>4</b>
<b>Configuring SELinux for new environments using CDP CLI</b>	<b>5</b>
<b>Reference list of security policies</b>	<b>6</b>

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## Overview

Security-Enhanced Linux (SELinux) security architecture allows you to control access to applications, processes, and files using security policies. Cludera images have permissive and enforced modes. You can use the permissive mode to log the security violations, and enforced mode to block the logged security violations. You can enable SELinux with enforced mode for Cludera environments and its services during environment creation, or you can configure your existing environments to use enforced mode for higher security.

### Important!

Currently, only third-party softwares, such as PostgreSQL, Nginx and FreeIPA is supported for SELinux.

You can set the following modes for SELinux:

- Enforcing: enforcing mode actively applies security policies
- Permissive: permissive mode logs any security violations without enforcing policies

For the list of security policies covered in SELinux, see [Reference list of SELinux security policies](#).

You can configure SELinux mode for Cludera environments during environment creation. If no parameter is specified for SELinux, the permissive mode will be used by default for new environments. If no value is specified for SELinux when updating existing environments, a **BadRequest** exception is thrown.

SELinux related logs are included in the default log collection of an environment. This means that the logs regarding SELinux are included in the diagnostic bundle that can be sent to Cludera Support for case resolution. For more information, see the [Sending diagnostic bundle to Cludera Support](#) documentation.

### Important!

Configuring SELinux is currently available as a preview feature for AWS. You need to have **CDP\_SECURITY\_ENFORCING\_SELINUX** entitlement to use this feature. For more information about how to obtain the entitlement, contact Cludera Customer Support.

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cludera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## Before you begin

- You need to install beta CDP CLI to configure SELinux for your environments. For more information, see the [Installing beta CDP CLI documentation](#).

## Configuring SELinux for new environments using CDP CLI

You can set the SELinux mode for FreeIPA, Data Lake and Cloudera Data Hub using the `selinux` parameter:

- FreeIPA

```
Unset
cdp environments create-aws-environment \
  --environment-name [***ENVIRONMENT NAME***] \
  --credential-name [***CREDENTIAL NAME***] \
  --region [***CONTROL PLANE REGION***] \
  --free-ipa selinux=ENFORCING,instanceCountByGroup=[***NUMBER OF FREEIPA INSTANCE***]
```

- Data Lake

```
Unset
cdp datalake create-aws-datalake \
  --datalake-name [***ENVIRONMENT NAME***]-dl \
  --environment-name [***ENVIRONMENT NAME***] \
  --selinux ENFORCING
```

- Cloudera Data Hub

```
Unset
cdp datahub create-aws-cluster \
  --cluster-name [***DATA HUB NAME***] \
  --environment-name [***ENVIRONMENT NAME***] \
```

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

```
--cluster-definition [***CLUSTER DEFINITION***] \  
--selinux ENFORCING
```

## Reference list of security policies

The following list details the default security policies that are logged or enforced based on the SELinux mode setting:

- abrt
- accountsd
- acct
- afs
- aiccu
- aide
- ajaxterm
- alsa
- amanda
- amtu
- anaconda
- antivirus
- apache
- apcupsd
- apm
- application
- arpwatch
- asterisk
- auditadm
- authconfig
- authlogin
- automount
- avahi
- awstats
- bacula
- base
- bcfg2
- bind
- bitlbee
- blkmapd
- icecast
- inetd
- init
- inn
- insights\_client
- iodine
- iotop
- ipa
- ipmievd
- ipsec
- iptables
- irc
- irqbalance
- iscsi
- isns
- jabber
- jetty
- jockey
- journalctl
- kdbus
- kdump
- kdumpgui
- keepalived
- kerberos
- keyboardd
- keystone
- kismet
- kmscon
- kpatch
- ksmtuned

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## CLLOUDERA TECHNICAL PREVIEW DOCUMENTATION

- blueman
- bluetooth
- boinc
- bolt
- bootloader
- brctl
- brlty
- bugzilla
- bumblebee
- cachefilesd
- calamaris
- callweaver
- canna
- ccs
- cdrecord
- certmaster
- certmonger
- certwatch
- cfengine
- cgdb
- cgroup
- chrome
- chronyd
- cinder
- cipe
- clock
- clogd
- cloudform
- cmirrord
- cobbler
- cockpit
- collectd
- colord
- comsat
- condor
- conman
- conntrackd
- consolekit
- couchdb
- courier
- cpucontrol
- ktalk
- l2tp
- ldap
- libraries
- likewise
- linuxptp
- lircd
- livedcd
- lldpad
- loadkeys
- locallogin
- lockdev
- logadm
- logging
- logrotate
- logwatch
- lpd
- lsm
- lttng-tools
- lvm
- mailman
- mailscanner
- man2html
- mandb
- mcelog
- mediawiki
- memcached
- milter
- minidlna
- minissdpd
- mip6d
- mirrormanager
- miscfiles
- mock
- modemmanager
- modutils
- mojomojo
- mon\_statd
- mongod
- motion
- mount

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*

## CLUDERA TECHNICAL PREVIEW DOCUMENTATION

- cpufreqselector
- cpuplug
- cron
- ctdb
- cups
- cvs
- cyphesis
- cyrus
- daemontools
- dbadm
- dbskk
- dbus
- dcc
- ddclient
- denyhosts
- devicekit
- dhcp
- dictd
- dirsrv
- dirsrv-admin
- dmesg
- dmidecode
- dnsmasq
- dnssec
- dovecot
- drbd
- dspam
- entropyd
- exim
- fail2ban
- fcoe
- fetchmail
- finger
- firewallld
- firewallgui
- firstboot
- fprintd
- freeipmi
- freqset
- fstools
- ftp
- mozilla
- mpd
- mplayer
- mrtg
- mta
- munin
- mysql
- mythtv
- naemon
- nagios
- namespace
- ncftool
- netlabel
- netutils
- networkmanager
- ninfod
- nis
- nova
- nscd
- nsd
- nslcd
- ntop
- ntp
- numad
- nut
- nx
- obex
- oddjob
- opafm
- openct
- opensnssec
- openfortivpn
- openhpid
- openshift
- openshift-origin
- opensm
- openvpn
- openvswitch
- opensman
- oracleasm
- osad

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*



## CLOUDERA TECHNICAL PREVIEW DOCUMENTATION

- fwupd
- games
- gdomap
- geoclue
- getty
- git
- gitosis
- glance
- gnome
- gpg
- gpm
- gpsd
- gssproxy
- guest
- hddtemp
- hostapd
- hostname
- hsqlldb
- hwloc
- hypervkvp
- ibacm
- pads
- passenger
- pcmcia
- pcp
- pcscd
- pdns
- pegasus
- permissivedomains
- pesign
- pingd
- piranha
- pkcs
- pkcs11proxyd
- pki
- plymouthd
- podsleuth
- policykit
- polipo
- portmap
- portreserve
- pos

*This document has been released as part of a technical preview for features described herein. Technical preview components are provided as a convenience to our customers for their evaluation and trial usage. These components are provided 'as is' without warranty or support. Further, Cloudera assumes no liability for the usage of technical preview components, which should be used by customers at their own risk.*