HDP Security Advanced Ambari Options 3

Configuring Advanced Security Options for Ambari

Date of Publish: 2018-07-15

http://docs.hortonworks.com

Contents

Advanced Security Options for Ambari

This section describes several security options for an Ambari-monitored-and-managed Hadoop cluster.

Configure Ciphers and Protocols for Ambari Server

Ambari provides control of ciphers and protocols that are exposed via Ambari Server.

Procedure

1. To disable specific ciphers, you can optionally add a list of the following format to ambari.properties. If you specify multiple ciphers, separate each cipher using a vertical bar |.
   security.server.disabled.ciphers=TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
2. To disable specific protocols, you can optionally add a list of the following format to ambari.properties. If you specify multiple protocols, separate each protocol using a vertical bar |.
   security.server.disabled.protocols=SSL|SSLv2|SSLv3

Configure Ambari Web Inactivity Timeout

Ambari is capable of automatically logging a user out of Ambari Web after a period of inactivity. After a configurable amount of time, the user's session will be terminated and they will be redirected to the login page.

About this task

This capability can be separately configured for Operators and Read-Only users. This allows you to distinguish a read-only user (useful when Ambari Web is used as a monitoring dashboard) from other operators. Alternatively, you can set both inactivity timeout values to be the same so that regardless of the user type, automatic logout will occur after a set period of time.

By default, the Ambari Web inactivity timeout is not enabled (i.e. is set to 0). The following instructions should be used to enable inactivity timeout and set as the amount of time in seconds before users are automatically logged out.

Before you begin

Ensure the Ambari Server is completely stopped before making changes to the inactivity timeout. Either make these changes before you start Ambari Server the first time, or bring the server down before making these changes.

Procedure

1. On the Ambari Server host, open /etc/ambari-server/conf/ambari.properties with a text editor.
2. There are two properties for the inactivity timeout setting. Both are initially set to 0 (which means this capability is disabled).
   a) user.inactivity.timeout.default: Sets the inactivity timeout (in seconds) for all users except Read-Only users.
   b) user.inactivity.timeout.role.readonly.default: Sets the inactivity timeout (in seconds) for all Read-Only users.
3. Modify the values to enable the capability. The values are in seconds.
4. Save changes and restart Ambari Server.
5. After a user logs into Ambari Web, once a period of inactivity occurs, the user will be presented with an Automatic Logout dialog 60 seconds from logout. The user can click to remain logged in or if no activity occurs, Ambari Web will automatically log the user out and redirect the application to the login page.