Release Notes for Ambari 2

Apache Ambari Release Notes

Date of Publish: 2019-12-17

https://docs.hortonworks.com

Contents

Apache Ambari Release Notes

This document provides you with the latest information about the Apache Ambari 2.7.5 release and all the cumulative fixes until Ambari 2.7.5.27 including log4j-2.16.0. For more information, see Fixed Issues for Ambari 2.7.5.27.

CVE 2021-44228 Remediation for HDP 3.1.5 and Ambari 2.7.5

As mentioned in Cloudera Technical Service Bulletin 2021-545 (Critical vulnerability in log4j2 CVE-2021-44228), the Hortonworks Data Platform (HDP) and Ambari are impacted by the recent Apache Log4j2 vulnerability.

As per that bulletin: The Apache Security team has released a security advisory for CVE-2021-44228 which affects Apache Log4j2. A malicious user could exploit this vulnerability to run arbitrary code as the user or service account running the affected software. Software products using log4j versions 2.0 through 2.14.1 are affected and log4j 1.x is not affected. Cloudera is making short-term workarounds available for affected software and is in the process of creating new releases containing fixes for this CVE.

Short Term Resolution

Remediation steps are outlined in the TSB-545 documentation. Be aware that the following actions are pulling the vulnerable jar back in action again:

- Adding service
- Scaling up cluster
- Enabling features like: LZO, HDFS HA

Long Term Resolution - HDP 3.1.5.6178 and Ambari 2.7.5.27

Please follow the upgrade instructions for minor upgrades to replace the vulnerable HDP and Ambari bits. The instruction for updating the JDBC driver (affected by this vulnerability) can be followed here.

HDP bits are built on top of the GA'd HDP 3.1.5.6091 with log4j-2.16.0 and the Ambari bits include 2.7.5.0 plus all cumulative fixes so far including log4j-2.16.0. For more information, see Fixed Issues for Ambari 2.7.5.27.

Ambari Repositories

Use the link appropriate for your OS family to download a repository file that contains the software for setting up Ambari.

OS	Format	URL
RedHat 7 CentOS 7 Oracle Linux 7	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/centos7
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/centos7/ambari.repo
	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/centos7/ambari-2.7.5.29-5-centos7.tar.gz
amazonlinux 2	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/amazonlinux2
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/amazonlinux2/ambari.repo

	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/amazonlinux2/ambari-2.7.5.29-5-amazonlinux2.tar.gz
SLES 12	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/sles12/
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/sles12/ambari.repo
	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/sles12/ambari-2.7.5.29-5-sles12.tar.gz
Ubuntu 16	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu16
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu16/ambari.list
	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu16/ambari-2.7.5.29-5-ubuntu16.tar.gz
Ubuntu 18	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu18
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu18/ambari.list
	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/ubuntu18/ambari-2.7.5.29-5-ubuntu18.tar.gz
Debian 9	Base URL	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/debian9
	Repo File	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/debian9/ambari.list
	Tarball md5 | asc	https://archive.cloudera.com/p/ambari/patch/2.x/2.7.5.29-5/debian9/ambari-2.7.5.29-5-debian9.tar.gz

Descriptions of New Features

Following is the new feature introduced in the Ambari 2.7.5 release.

Table 1: Apache Ambari 2.7.5 New Features

Feature	Description
Secured Ambari repositories	Access to Ambari repositories for production purposes requires authentication. The release package repositories are secured with Basic Authentication and Ambari supports the handling of username and password for these repositories. For more information, see "Accessing Ambari Repositories" topic in the Ambari installation guide.

Behavioral Changes

Behavioral changes denote a marked change in behavior from the previously released version to this version of Ambari. There are no behavioral changes in this version when compared to the previously released version.

Common Vulnerabilities and Exposures

No Common Vulnerabilities and Exposures (CVEs) fixes apply to Ambari 2.7.5.

Fixed Issues

Fixed issues represents selected issues that were previously logged through Cloudera Support, but are now addressed in the current release. These issues may have been reported in previous versions within the Known Issues section; meaning they were reported by customers or identified by the Cloudera Quality Engineering team. See Fixed Issues for Ambari 2.7.5.27 section to know more about the cumulative fixes until Ambari 2.7.5.27.

Incorrect-results

Bug ID	Apache JIRA	Summary
BUG-121927	N/A	Configuring YARN with custom queues leads to misleading errors in Stack Advisor
BUG-107724	AMBARI-24302	(Tracking JIRA for 2.6.x) - Dhdp.version shows blank value in process output for Datanodes

Other

Bug ID	Apache JIRA	Summary
BUG-122369	AMBARI-25412	Remove all tags from logger service methods in ambari-contrib
BUG-122337	N/A	HiveServer2 JDBC URL is incorrectly configured in Zeppelin JDBC interpreter
BUG-122165	Ambari-25400	Issue while determining live collector in case of HA
BUG-122125	AMBARI-14526	Ambari Agent SUSE12 Systemd service is not auto starting Ambari agent on system reboot.
BUG-122035	AMBARI-25394	Ambari Metrics whitelisting is failing on * wildcard for HBase Tables
BUG-122032	AMBARI-25397	Upgrading ambari-logsearch-logfeeder to 2.7.4 rpm gives warnings
BUG-121976	AMBARI-25378	500 advisor error with ambari metrics mode set to distributed with OneFS
BUG-121926	N/A	Remove hardcoded number of retries from Hive script
BUG-121911	AMBARI-25379	Upgrade AMS Grafana version to 6.4.2
BUG-121898	AMBARI-25399	Add Hive PAM support for service check and alerts
BUG-121879	N/A	HDP Stack does not set oozie.server.authentication.type=kerberos resulting in conflicts when KnoxSSO enabled
BUG-121218	N/A	Use hdfs resource instead of execute in hive_server_interactive.py
BUG-121024	AMBARI-25333	Regenerate keytab generates empty keytab file if no file is present in cache
BUG-120861	AMBARI-25326	AMS - no HBase and Hive metrics post-upgrade when using 2 collectors
BUG-120603	AMBARI-25395	Update help text in Hive install to reflect an actual JAR file name or provide a clearly formatted example

Performance

Bug ID	Apache JIRA	Summary
BUG-121889	AMBARI-25385	Reduce cluster creation request processing time
BUG-120989	AMBARI-25332	Kerberos keytab regeneration working slow
BUG-122244	AMBARI-21935	Hive Vectorization: Degraded performance with vectorize UDF
BUG-122079	AMBARI-25156	ClientComponentHasNoStatus exception clutters Operating System's /var/log/messages
BUG-122239	AMBARI-25408	Upgrade Infra Solr to 7.7.2

Security

Bug ID	Apache JIRA	Summary
BUG-121464	AMBARI-25396	Cross-site scripting vulnerability on Ambari hosts
BUG-122087	N/A	Stored XSS vulnerability in rack_info using API
BUG-121361	AMBARI-25384	Cross-site scripting vulnerability in Files View
BUG-122015	AMBARI-25391	Ambari logging Grafana Password in ActionQueue.py
BUG-121801	AMBARI-25390	Disable indexing in /resources endpoint and sub-directories

Stability

Bug ID	Apache JIRA	Summary
BUG-122238	AMBARI-25403	Ambari Management Pack: Ambari throws 500 error while downloading OneFS client configuration

Supportability

Bug ID	Apache JIRA	Summary
BUG-121600	N/A	For HDP 3.1 HS (container mode) hive.merge.nway.joins is not set to false

Usability

Bug ID	Apache JIRA	Summary
BUG-121804	AMBARI-25380	UI does not reflect/update task logs

Fixed issues for Ambari 2.7.5.27

Bug ID	Apache JIRA	Summary
BUG-123914		Fix curator 4.2 to support zookeeper 3.4.x (#3108)
BUG-125601		Secure Atlas executable search path is hardcoded to default (kinit)
BUG-125601		Secure Atlas executable search path is hardcoded to default (kinit)
BUG-125281		Ambari fails to kill datanode processes properly
BUG-125490		Add always_replace flag to HdfsResource
BUG-125325		Make DBConnectionVerification for HiveServer2 optional for users with least privilege mode cluster model.
BUG-125298		Ambari alert for HMS checks fails for hosts not is "hive.metastore.uris"
BUG-124388	AMBARI-25547	AMBARI-25547 Update Grafana version to 6.7.4 to avoid CVE-2020-13379
BUG-124898		Resource Manager not starting with permissions issues
BUG-124464		NodeManager doesn't work after adding a new host to a patch upgraded cluster.
BUG-124066		YARN Timeline Service coprocessor JAR locations incorrect.
BUG-119732		Stack advisor fails because of accessible-node-labels
BUG-122926		Ambari reads incorrect stack version while starting Nodemanager
BUG-122928		HBase master fails to start if it has older hbase-client on the node.
BUG-123951		Rack awareness for Kafka
BUG-123920		Rolling upgrade From 3.1.5.28 to 3.1.5.51 fails with fs.defaultFS viewfs://.
BUG-123609		Custom kinit path not taking effect. Additional patch

Bug ID	Apache JIRA	Summary
	AMBARI-25511	hive auth fallback to SIMPLE because startup script fail to do kerberos login
BUG-125775		log4j2 vulnerability fix - transitive dependencies exclusions
BUG-125775		Ambari - log4j2 zero day vulnerability fix - 2.16
BUG-125775		replacing vulnerable log4j2 jars with patched log4j2 jars in apache-solr
BUG-125775		Ambari - log4j2 zero day vulnerability fix
BUG-125281		Ambari fails to kill datanode processes properly
BUG-125490		Add always_replace flag to HdfsResource
BUG-125488		"Loading" pop-up does not disappear after bulk delete hosts.
BUG-125510		Prepare delete identities never triggers 'Remove Keytab Kerberos Client' task.
BUG-125501		[ISILON] [HDP7.1.7] HDP 2.6 to HDP7.1.7 is stuck with "CHECK_KEYTABS KERBEROS/KERBEROS_CLIENT".
BUG-125443		NullPointerException after host deleting
BUG-125400		Deleting identites fails with DB constraint violation after host removal from kerberized cluster
BUG-125374		During host removal, removal of obsolete identities produces null pointer exception
BUG-125328		Optimize getActiveIdentities call and fix the issue with not updating the database with cached identities
BUG-125360		Warning "llap" is not available in the list of valid values.
BUG-125348		Group permission being revoked when associated user permission is modified
BUG-125325		Make DBConnectionVerification for HiveServer2 optional for users with least privilege mode cluster model.
BUG-125282		ConcurrentModificationException during stomp subscriptions processing.
BUG-125291		StackOverflowError appears on MethodArgument*Exception during stomp message handling.
BUG-123485		Add a step during keytabs regeneration to select the config update policy
BUG-124754		Kerberization of the big cluster using Blueprints takes too much time
	AMBARI-25533	Delete redundant phantomjs dependency
BUG-124980		Timezone data is outdated
	AMBARI-25547	Update Grafana version to 6.7.4 to avoid CVE-2020-13379 (#3279)
	AMBARI-25604	During blueprint deploy tasks sometimes fail due to KeyError
	AMBARI-25589	When hearbeat is lost sometimes start/stop tasks can hang for a long time.
BUG-123485		Add a step during keytabs regeneration to select the config update policy
BUG-124994		No warning message at changing repo name to an invalid one
BUG-124784		Configs XSS issues
BUG-124715		Ambari UI is taking time to update new IP address
BUG-124612		Primary key duplication error during flushing alerts from alerts cache.
	AMBARI-25469	Bad UTF encoding on Alert listener receiver
BUG-124464		NodeManager doesn't work after adding a new host to a patch upgraded cluster.
	AMBARI-25571	Vulnerable Spring components in Ambari - CVE-2020">CVE-2020-5398, CVE-2020">CVE-2020-5421
	AMBARI-25506	Upgrade Apache Solr version to 7.7.3 in Ambari Infra
	AMBARI-25485	Change authentication method from get to post. (#3182)

Bug ID	Apache JIRA	Summary
	AMBARI-25265	upgrade AngularJS to v1.7.5 in ambari-admin ui
	AMBARI-25472	Disable autocomplete on login screen (#3177)
	AMBARI-25477	Add autocomplete off to all forms
	AMBARI-25495	Extend the set of headers from server's response.
BUG-123303		Ambari - Path and Domain attribute not set on session cookie
	AMBARI-25487	AMBARI-25487.Change authentication method from get to post (#3185)
BUG-124087		File upload/download validation method should be configurable
BUG-124055		Add hosts via Ambari fails during installation of Hive/Spark/other clients.
BUG-122926		Ambari reads incorrect stack version while starting Nodemanager
BUG-123428		ambari upgrade (2.7.4 -> 2.7.5) overwrite infra-solr-xml and infra-solr-env
BUG-123644		Yarn Configs are getting removed by changes in Yarn Queue Manager
BUG-123609		Custom kinit path not taking effect. Additional patch
BUG-123807		Ambari builds are failing with a bower error
BUG-123340		Ambari server should provide HI leader state via API
BUG-123609		Custom kinit path not taking effect
BUG-123228		Ambari's HDFS resource should use hashing to decide if file resources are identical
BUG-123607		Encryption method to AES256 from 3DES on Ambari keystore.
BUG-123544		Ambari UI host Tooltip not showing for some services
BUG-123381		ambari-admin build failed because of the issue with transitive "q" dependency of bower
	AMBARI-25457	Hive 3 Grafana dashboards showing outdated metrics (#3168)
	AMBARI-25479	Set Keytab: Kerberos Client operation takes lot of time and timing out

Known Issues

Ambari 2.7.5 has the following known issues, scheduled for resolution in a future release.

Table 2: Ambari 2.7.5 Known Issues

<table>
<tr><th>Apache Jira</th><th>Cloudera Bug ID</th><th>Problem</th><th>Solution</th></tr>
<tr><td>N/A</td><td>BUG-123500</td><td>During the HDP stack upgrade, the existing configurations are merged with the default configurations of the upgraded HDP stack. Properties that have default values are overwritten by new default values from the target stack.</td><td>Move the affected keystore files to different location or non-default location and change the property values accordingly.
<table>
<tr><th>Affected property</th><th>Default value</th></tr>
<tr><td>Atlas:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /usr/hdp/current/atlas-server/conf/ranger-plugin-keystore.jks
• /usr/hdp/current/atlas-server/conf/ranger-plugin-truststore.jks</td></tr>
<tr><td>HDFS:
• Advanced ranger-hdfs-policymgr-ssl xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore
• Advanced ssl-client ssl.client.keystore.location
• ssl.client.truststore.location</td><td>• /usr/hdp/current/hadoop-client/conf/ranger-plugin-keystore.jks
• /usr/hdp/current/hadoop-client/conf/ranger-plugin-truststore.jks
• /etc/security/clientKeys/keystore.jks
• /etc/security/clientKeys/all.jks</td></tr>
<tr><td>Hive:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /usr/hdp/current/hive-server2/conf/ranger-plugin-keystore.jks
• /usr/hdp/current/hive-server2/conf/ranger-plugin-truststore.jks</td></tr>
<tr><td>HBase:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /usr/hdp/current/hbase-client/conf/ranger-plugin-keystore.jks
• /usr/hdp/current/hbase-client/conf/ranger-plugin-truststore.jks</td></tr>
<tr><td>Kafka:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /usr/hdp/current/kafka-broker/config/ranger-plugin-keystore.jks
• /usr/hdp/current/kafka-broker/config/ranger-plugin-truststore.jks</td></tr>
<tr><td>Knox:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /usr/hdp/current/knox-server/conf/ranger-plugin-keystore.jks
• /usr/hdp/current/knox-server/conf/ranger-plugin-truststore.jks</td></tr>
<tr><td>Ranger:
• Advanced atlas-tagsync-ssl xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore
• Advanced ranger-tagsync-policymgr-ssl xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /etc/security/serverKeys/atlas-tagsync-keystore.jks
• /etc/security/serverKeys/atlas-tagsync-mytruststore.jks
• /etc/security/serverKeys/ranger-tagsync-keystore.jks
• /etc/security/serverKeys/ranger-tagsync-mytruststore.jks</td></tr>
<tr><td>Ranger KMS:
• xasecure.policymgr.clientssl.keystore
• xasecure.policymgr.clientssl.truststore</td><td>• /etc/security/serverKeys/ranger-plugin-keystore.jks
• /etc/security/serverKeys/ranger-plugin-truststore.jks</td></tr>
<tr><td>Storm:</td><td>• hadoopdev-clientcert.jks</td></tr>
</table>
</td></tr>
</table>

Apache Jira	Cloudera Bug ID	Problem	Solution
N/A	BUG-120773	EU: Oozie SC fails java.io.IOException: Error while connecting Oozie server	If Ranger HA and/or Oozie Server HA is configured and a custom composite keytab file is being used, service checks for Ranger and Oozie will fail during the HDP 2.6 to HDP 3.1 Upgrade. Re-create the custom Ranger and/or Oozie Server keytab files and re-try the service check, or ignore and proceed past the service check.
N/A	N/A	Unable to install HDF over HDP when HDF URL is not behind the paywall.	If HDF URL is not behind the paywall, then you must select the disableCredentialsAutocompleteForRepoUrls option on http://$AMBARI_SERVER:8080/#/experimental

N/A	BUG-121044	Storm service check failed after disabling kerberos	We should create ZooKeeper superuser and remove/change permissions for credentials znode. Here are the detailed steps:
			• Login to any node with ZooKeeper Client and create digest for selected user:password pair:
			`export ZK_CLASSPATH=/etc/zookeeper/conf/:/usr/hdp/current/zookeeper-server/lib/*:/usr/hdp/current/zookeeper-server/*`
			`java -cp $ZK_CLASSPATH org.apache.zookeeper.server.auth.DigestAuthenticationProvider super:super123`
			where super:super123 is the user:password pair. We will get digest in output:
			super:super123->super:UdxDQl4f9v5oITwcAsO9bmWgHSI=
			• Update "zookeeper-env template" property on ZooKeeper service page with adding following line:
			`export SERVER_JVMFLAGS="$SERVER_JVMFLAGS -Dzookeeper.DigestAuthenticationProvider.superDigest=super:UdxDQl4f9v5`
			User should replace proposed digest with got one in previous step.
			• Restart all required services.
			• Login to any node with ZooKeeper Client and connect to ZooKeeper console:
			`/usr/hdp/current/zookeeper-client/bin/zkCli.sh -server <zookeeperServerHostFQDN>:2181`
			• Remove/change permissions for credential znode. User should use value of Storm's storm.zookeeper.root property instead <stormRoot>:
			`delete /<stormRoot>/credentials`
			or update permissions to available-to-all:
			`setAcl /<stormRoot>/credentials world:anyone:cdrwa`
			After following the steps mentioned above Storm service check starts to pass.

N/A	BUG-120925	Hbase Service check fails after upgrading to Ambari 2.7.5.0	Make sure HDFS service is fully started and then restart the HBase service.
N/A	BUG-105092	Oozie service check failure on HA cluster during EU	If Ranger HA and/or Oozie Server HA is configured and a custom composite keytab file is being used, service checks for Ranger and Oozie will fail during the HDP 2.6 to HDP 3.0 Upgrade.

Apache Jira	Cloudera Bug ID	Problem	Solution
N/A	BUG-113993	On a cluster on which security was enabled in the past, if it is disabled, metrics collector start fails with an error.	Clear out the data on the znode specified in ams-hbase-site:zookeeper.znode.parent. • If AMS is in embedded mode, this can be done by deleting the directory as specified in the ams-hbase-site property 'HBase ZooKeeper Property DataDir'. • If AMS is in distributed mode, this can be done by deleting the znode in cluster zookeeper using zkCli. Instead of deleting the znode, changing the value of the znode from /ams-hbase-unsecure to something like /ams-hbase-unsecure-new is also OK.
N/A	BUG-121151	Smartsense service does not start when upgrading from Ambari 2.7.1 (or older) to 2.7.4 on Debian 9 with openssl 1.1.0k installed.	Disable starting of SmartSense services pre-upgrade. SmartSense services can only be started once upgrade to Ambari 2.7.4.0 is successful.
N/A	BUG-113753	YARN Application Timeline Server (ATSV2) fails when restarting after making any configuration changes on a viewfs enabled cluster.	Restart Timeline Service V2.0 Reader if HDFS is restarted.
N/A	BUG-122551	Submitting the storm-starter-topologies*.jar script might fail because the storm starter script tries to transform the JAR according to the client.jartransformer.class configuration parameter. The starter script does not handle the failure as expected.	When the transformation fails, the client.jartransformer.class configuration parameter must be changed or set to be empty.
N/A	BUG-122408	Oozie is found to be down post downgrade after a non finalized upgrade from HDP-3.0.1.0 to HDP-3.1.5.0. Downgrade completes succesfully but Oozie is down post downgrade.	N/A

Apache Jira	Cloudera Bug ID	Problem	Solution
N/A	BUG-122579	Disable HSI and Enable HSI is failing. Enable HSI on any host using Hive Configs -> Enable Interactive Query, HSI is installed and it starts. Restart services with stale configurations. Next, disable HSI by toggling the Interactive Query button. Enable HSI on another host. HSI fails to start.	Use to following procedure to enable HIS: **1.** su hdfs. **2.** Authenticate with hdfs principal: kinit -k -t /etc/security/keytabs/hdfs.headless.keytab hdfs@EXAMPLE.COM **3.** Delete the Keytab from HDFS: hdfs dfs -rm /user/hive/.yarn/keytabs/hive/hive.service.keytab **4.** Restart Hive.
N/A	BUG-123417	The no_proxy='.example.com' format (starting with .) does not work and causes <urlopen error Tunnel connection failed: 403 Tunnel Forbidden> error. This error can show up in multiple places of the product in multiple forms, like an alert of Grafana accessibility, or LDAP configuration error at Ambari setup, and so on.	Set the no_proxy env var accordingly.

Documentation Errata

This section contains late additions or corrections to the product documentation.

Legal Information