Apache Ambari Release Notes

Date of Publish: 2019-08-26

Contents

Apache Ambari Release Notes

This document provides you with the latest information about the Apache Ambari 2.7.4 release.

Descriptions of New Features

Following is the new feature introduced in the Ambari 2.7.4 release.

Table 1: Apache Ambari 2.7.4 New Features

Feature	Description
Password policy for Ambari users	This version of Ambari supports a feature that enables you to configure password policy for Ambari users.

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.

Table 2: Apache Ambari 2.7.4 Behavioral Changes

Hortonworks Bug ID	Apache Component	Apache JIRA	Summary	Details
BUG-105818	Ambari	AMBARI-9016	Ambari API uses HTTP Header Content-Type:text/plain when the content is JSON	Scenario: Ambari REST API is expecting "Content-Type" HTTP header set to "text/plain" even though content is in JSON format. If client specified the same header with the value of "application/json", Ambari threw HTTP 500 error. Previous Behavior:Ambari behaviour was misleading forcing the user to use "text/plain" Content-Type header in HTTP clients. New Behavior: Ambari expects "application/json" Content-Type header. Expected Customer Action:Revise any custom code which uses the Ambari REST API and take actions if needed

Common Vulnerabilities and Exposures

No Common Vulnerabilities and Exposures (CVEs) fixes apply to Ambari 2.7.4.

Fixed Issues

Fixed issues represents selected issues that were previously logged via Hortonworks 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 Hortonworks Quality Engineering team.

Incorrect-results

Bug ID	Apache JIRA	Summary
BUG-120097	AMBARI-25278	Fix aggregate metric in Kafka's Grafana dashboard
BUG-100002	AMBARI-23478	YARN Cluster CPU Usage Graph Always Shows High CPU Usage

Other

Bug ID	Apache JIRA	Summary
BUG-120711	AMBARI-25320	NIFI-Hosts dashboard does not show any metrics in Grafana
BUG-120503	AMBARI-25293	Logsearch: logfeeder throws NPE when updating checkpoint
BUG-120353	AMBARI-25305	Ambari UI gets into corrupt state after installing a cluster
BUG-120078	AMBARI-25275	Changes in Yarn Capacity Scheduler is requesting for restart of Resource Manager
BUG-119973	AMBARI-24950	Logsearch: use os timezone in Logfeeder
BUG-119367	Ambari-25234	Ambari audit log shows "null" user when executing an API call as admin
BUG-119103	AMBARI-25093	Spark2 Thrift Server alert does not work with HTTPS/SSL
BUG-118993	AMBARI-25210	ONEFS installation via blueprint fails
BUG-118727	AMBARI-25196	HDFS Service Checking with an ClassNotFound Error in Ambari WFManager view
BUG-118660	AMBARI-25080AMBARI-25080	CLONE - Unable to install Hive service
BUG-118561	AMBARI-25187	Kerberos operations are shown in service action dropdown when not needed
BUG-118559	AMBARI-25186	Kerberos Client is unnecessarily installed via Blueprints when kerberos-env/kdc-type is none
BUG-117935	AMBARI-25165	Oozie service check fails due to import error
BUG-117930	AMBARI-25164	Rack "Config Refresh" behaviour is different in Ambari 2.6 and 2.7.3
BUG-117882	AMBARI-25159	http.strict-transport-security change does not take affect in 2.7.x
BUG-117868	AMBARI-25158	Dashboard is unable to load . Common console error : "SEVERE TypeError: widgetGroups is undefined"
BUG-117414	AMBARI-25168	Leader for a topic is assigned 'None'
BUG-117246	AMBARI-25151	HDFS running with root user has process limitation of 512 in SLES 12.2 when agent is started by SystemD
BUG-116898	AMBARI-25114	Login to Logsearch UI not possible if Ambari Server is configured with https
BUG-116328	AMBARI-25069	Empty baseurl values written to Repo Files when using a local repository causing stack installation failure
BUG-116216	AMBARI-25052	Unable to Add Services Due to toMapByProperty()
BUG-113969	AMBARI-25102	Dasboard metrics will not load for ambari user which has dot in their username.
BUG-113526	AMBARI-24848AMBARI-25306	Satellite repo cluster installation Issues
BUG-112761	AMBARI-24767	CLONE - Error while starting Timeline v2 Reader during Move operation
BUG-111201	AMBARI-24652	Grafana failed to show data for custom metrics
BUG-105818	AMBARI-9016	Ambari API uses HTTP Header Content-Type:text/plain when the content is JSON.

Bug ID	Apache JIRA	Summary
BUG-120905	AMBARI-25328	When spark_transport_mode is set to 'http' then STS server fails to start in Ambari 2.7 .

Performance

Bug ID	Apache JIRA	Summary
BUG-119395	AMBARI-25235	Add a sysprep configurations to run conf-selects only a single time

Security

Bug ID	Apache JIRA	Summary
BUG-120219	AMBARI-25280	improper error handling when adding non-existent LDAP user
BUG-120086	AMBARI-25277	Security Concern as ambari-server.log and ambari-agent.log shows cleartext passwords.
BUG-118907	AMBARI-25204	Ambari returns stack trace in HTML doc when an error occurs retrieving details for an Ambari View resource that does not exist
BUG-118849	AMBARI-25201	Updating a user's password does not validate the administrator's current password.
BUG-118750	AMBARI-25200	Ambari returns stack trace in HTML doc when an error occurs retrieving details for a user resource that does not exist
BUG-118562	AMBARI-25283	Ambari UI evaluates Javascript embedded in user input when adding hosts, adding remote clusters, and renaming the cluster
BUG-117996	AMBARI-25169	Upgrade Apache Solr version to 7.7.0 or later in Ambari
BUG-116897	AMBARI-25141	LDAP password in cleartext in ldap-password.dat file after encrypting passwords

Stability

Bug ID	Apache JIRA	Summary
BUG-119942	AMBARI-25272	Ambari UI default Ajax Timeout is 3 minutes but some operations in server can take more than that
BUG-118554	AMBARI-25185	Chrome and Firefox browsers are crashing while opening Ambari UI
BUG-116973	AMBARI-25123	/var/lib/ambari-agent/cache not updating (Ambari 2.7)

Supportability

Bug ID	Apache JIRA	Summary
BUG-119871	AMBARI-25269	Hive Server Interactive process alert triggered in HA setup

Usability

Bug ID	Apache JIRA	Summary
BUG-120730	AMBARI-25311	FinalizeKerberosServerAction timeout has to be configurable
BUG-116406	AMBARI-25090	Logsearch should index keywords without the ending periods(.)
BUG-113845	AMBARI-24879	The kadmin service principal name should be configurable for MIT KDC interactions
BUG-113488	AMBARI-24847	[Logsearch Backend] I cannot search for a term that includes spaces or dashes

Known Issues

Ambari 2.7.4 has the following known issues, scheduled for resolution in a future release.

Table 3: Ambari 2.7.4 Known Issues

Apache Jira	Hortonworks 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 | 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:<br><br>• Login to any node with ZooKeeper Client and create digest for selected user:password pair:<br><br>```
export ZK_CLASSPATH=/etc/zookeeper/conf/:/usr/
hdp/current/zookeeper-server/lib/*:/usr/hdp/
current/zookeeper-server/*
java -cp $ZK_CLASSPATH
 org.apache.zookeeper.server.
auth.DigestAuthenticationProvider
 super:super123
```<br><br>where super:super123 is the user:password pair. We will get digest in output:<br><br>super:super123->super:UdxDQl4f9v5oITwcAsO9bmWgHSI=<br><br>• Update "zookeeper-env template" property on ZooKeeper service page with adding following line:<br><br>```
export SERVER_JVMFLAGS="$SERVER_JVMFLAGS -
Dzookeeper.
DigestAuthenticationProvider.superDigest=super:UdxDQl4f9v5
```<br><br>User should replace proposed digest with got one in previous step.<br><br>• Restart all required services.<br><br>• Login to any node with ZooKeeper Client and connect to ZooKeeper console:<br><br>```
/usr/hdp/current/zookeeper-client/bin/zkCli.sh
 -server <zookeeperServerHostFQDN>:2181
```<br><br>• Remove/change permissions for credential znode. User should use value of Storm's storm.zookeeper.root property instead <stormRoot>:<br><br>```
delete /<stormRoot>/credentials
```<br><br>or update permissions to available-to-all:<br><br>```
setAcl /<stormRoot>/credentials
 world:anyone:cdrwa
```<br><br>After following the steps mentioned above Storm service check starts to pass. |
| N/A | BUG-120925 | Hbase Service check fails after upgrading to Ambari 2.7.4.0 | Make sure HDFS service is fully started and then restart the HBase service. |

Apache Jira	Hortonworks Bug ID	Problem	Solution
N/A	BUG-113993	Document known issue with disabling security in AMS. 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-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.

Documentation Errata

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

Legal Information

Apache Ambari 2.7.4

Copyright information for Apache Ambari components may be found within the documentation accompanying each component in a particular release.

Apache Ambari incorporates software from various open source projects released primarily under the Apache Software License 2.0 ("ASLv2"). Other software included may be released under the terms of alternative ASLv2 compatible open source licenses. Please review the license and notice files accompanying the software for additional licensing information.

Please visit the Apache Ambari page for more information on Apache Ambari technology. For more information on Hortonworks support services, please visit either the Support or Sales page. Feel free to contact us directly to discuss your specific needs.

Hortonworks reserves the right to change any products described herein at any time, and without notice. Hortonworks assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Hortonworks.

Trademark: Apache Ambari is/are trademark/s of Hortonworks, Inc. 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 HORTONWORKS, HORTONWORKS DOES NOT MAKE OR GIVE ANY REPRESENTATION, WARRANTY, OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, IN CONNECTION WITH HORTONWORKS TECHNOLOGY OR RELATED SUPPORT PROVIDED IN CONNECTION THEREWITH. HORTONWORKS DOES NOT WARRANT THAT Apache Ambari WILL OPERATE UNINTERRUPTED OR THAT IT WILL BE FREE FROM DEFECTS OR ERRORS, THAT IT WILL PROTECT YOUR DATA FROM LOSS, CORRUPTION OR UNAVAILABILITY, OR THAT # WILL MEET ALL OF CUSTOMER'S BUSINESS REQUIREMENTS. WITHOUT LIMITING THE FOREGOING, AND TO THE MAXIMUM EXTENT PERMITTED BY

APPLICABLE LAW, HORTONWORKS 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.