Module 5: Ambari Advance Topics and Security

Assignment Solution

Version 1.0

Module 5: Assignment Solution

Perform this Assignment on your Node for Ambari Security Task:

→ Logs Checking and reviewing

Solution:

a. Ambari server logs
   i. Go to your server where you have installed ambari server.
   ii. Cd /var/log/ambari-server/
   iii. Now you will find ambari-server.log

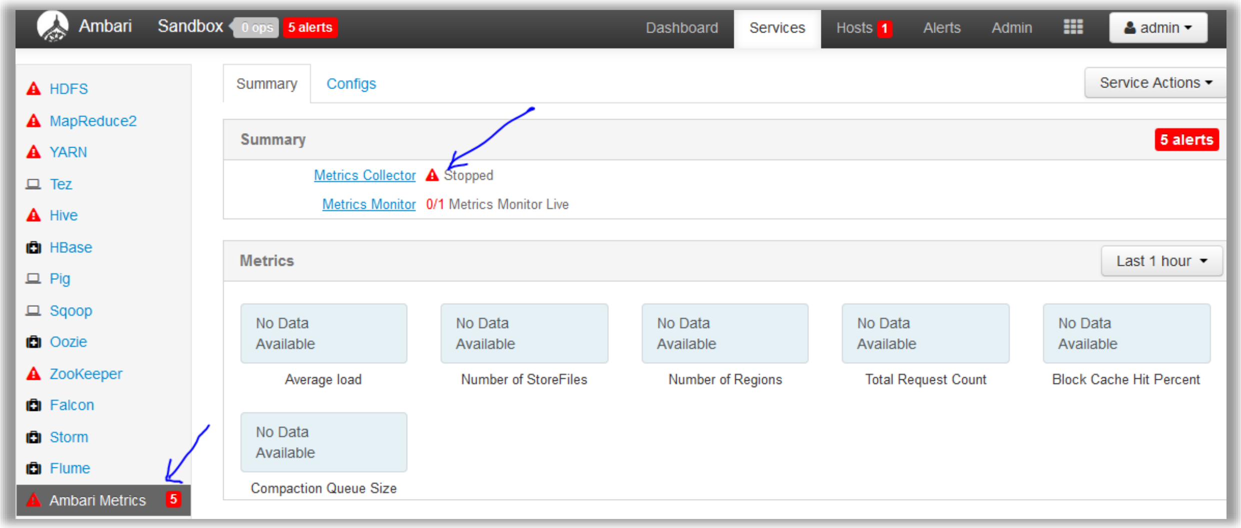
b. Ambari agent log
   i. Go to your server where you have installed ambari agent.
   ii. Cd /var/log/ambari-agent/
   iii. Now you will find ambari-agent.log

c. Ambari tasks logs
   i. Go to your server where you have installed ambari agent.
   ii. Cd /var/log/ambari-agent/data
   iii. Here you will find all the logs related to tasks
   iv. Files are below
      1. command-N.json
      2. output-N.txt
      3. errors-N.txt

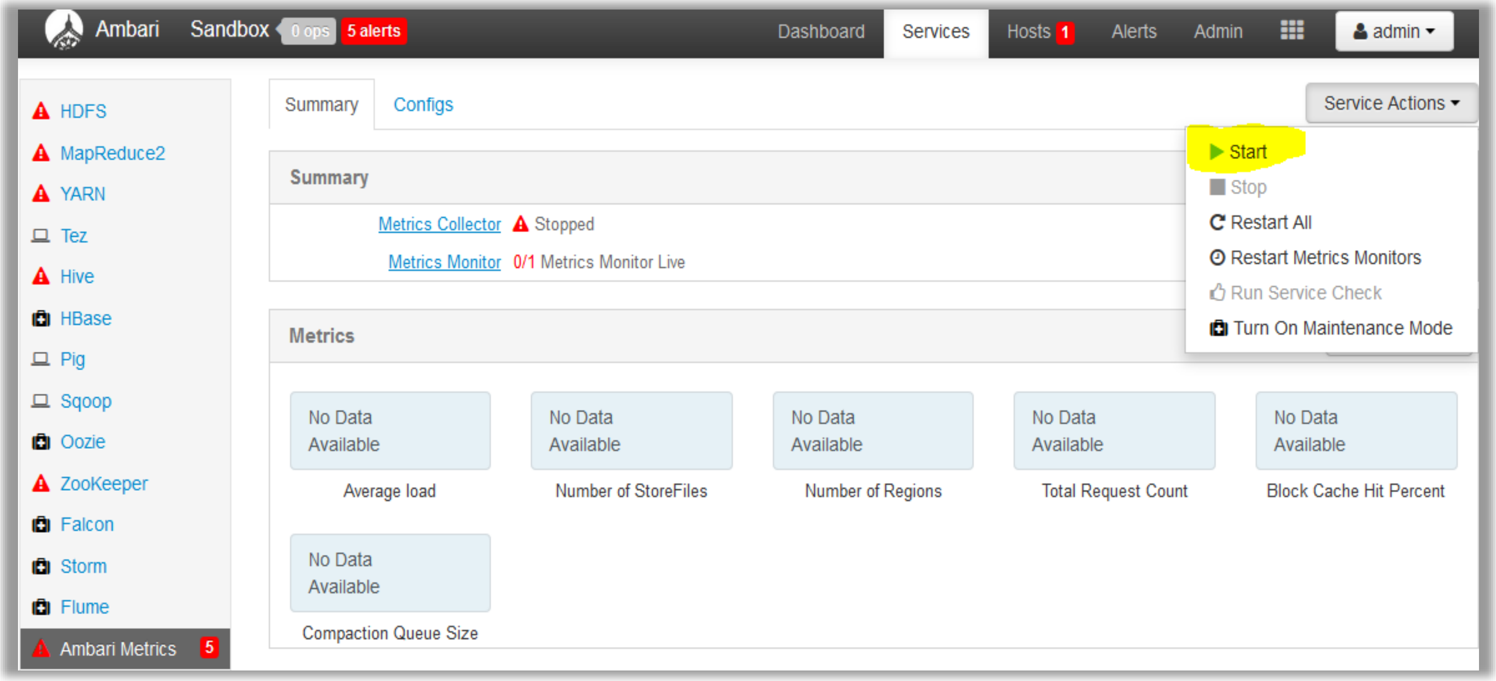
→ Error Checking

Solution:

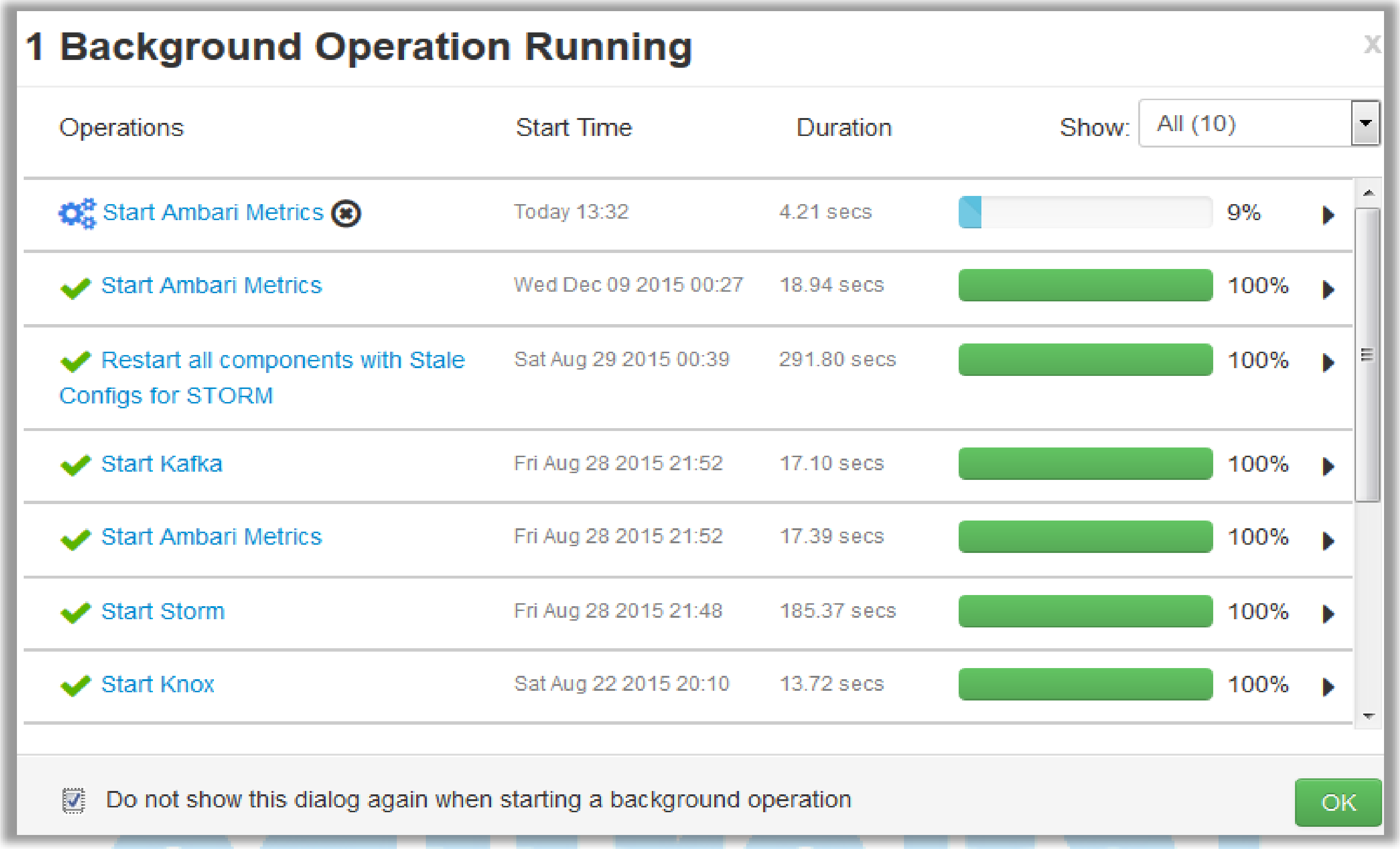
Step 1: Red marks beside service name shows that it's not running like in below image



Step 2: Just go to Service action and click on start



Step 3: You can click on gray field where it will show 1 opt as soon you click on start services



1 Background Operation Running

Operations	Start Time	Duration	Show: All (10)	
Start Ambari Metrics	Today 13:32	4.21 secs	9%	▸
✓ Start Ambari Metrics	Wed Dec 09 2015 00:27	18.94 secs	100%	▸
✓ Restart all components with Stale Configs for STORM	Sat Aug 29 2015 00:39	291.80 secs	100%	▸
✓ Start Kafka	Fri Aug 28 2015 21:52	17.10 secs	100%	▸
✓ Start Ambari Metrics	Fri Aug 28 2015 21:52	17.39 secs	100%	▸
✓ Start Storm	Fri Aug 28 2015 21:48	185.37 secs	100%	▸
✓ Start Knox	Sat Aug 22 2015 20:10	13.72 secs	100%	▸

☑ Do not show this dialog again when starting a background operation

→ Performance tuning

Solution:

» Calculate the new, larger cache size, using the following relationship:

ecCacheSizeValue=60*<cluster_size>

» On the Ambari Server host, in /etc/ambari-server/conf/ambari-properties, add the following property:

server.ecCacheSize=<ecCacheSizeValue>

where <ecCacheSizeValue> is the value calculated previously, based on the number of nodes in the cluster.

» Add the following properties to adjust the JDBC connection pool settings:

server.jdbc.connection-pool.acquisition-size=5

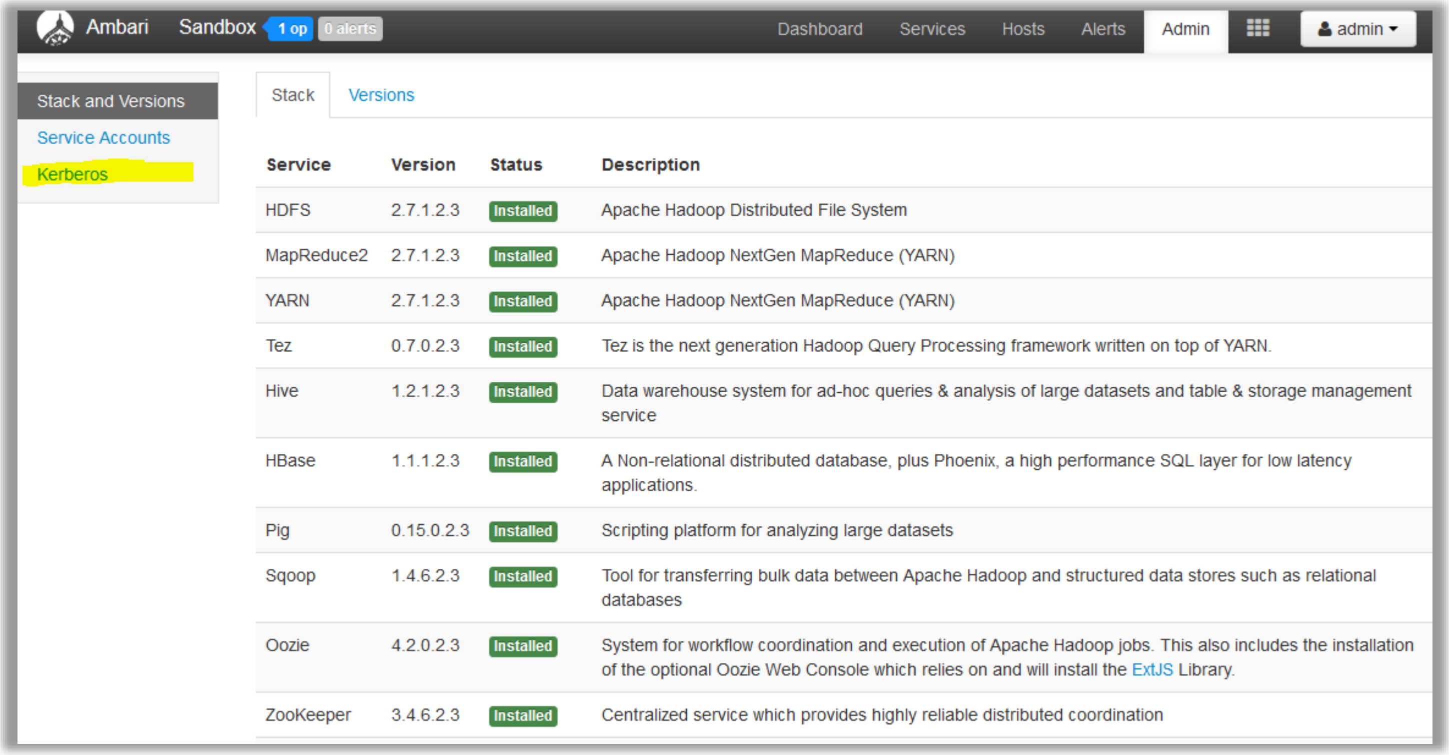
server.jdbc.connection-pool.max-age=0

```
server.jdbc.connection-pool.max-idle-time=14400

server.jdbc.connection-pool.max-idle-time-excess=0

server.jdbc.connection-pool.idle-test-interval=7200
```

If using MySQL as the Ambari database, increase the timeout in MySQL from 15 minutes to 8 hours and the max connections from 32 to 128.

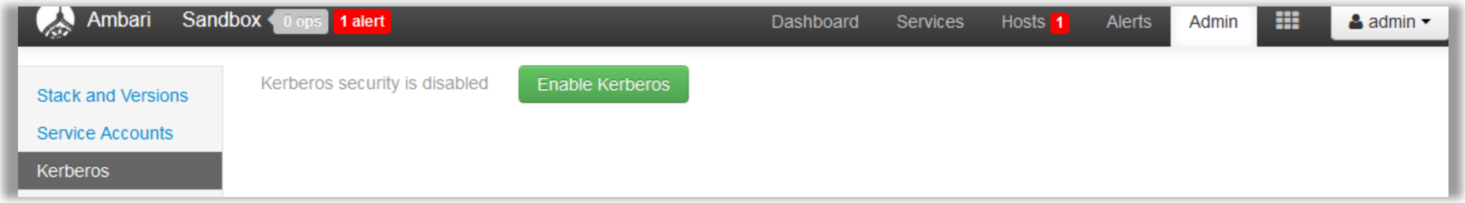
→ Security Implementation

Step 1: Click on Admins



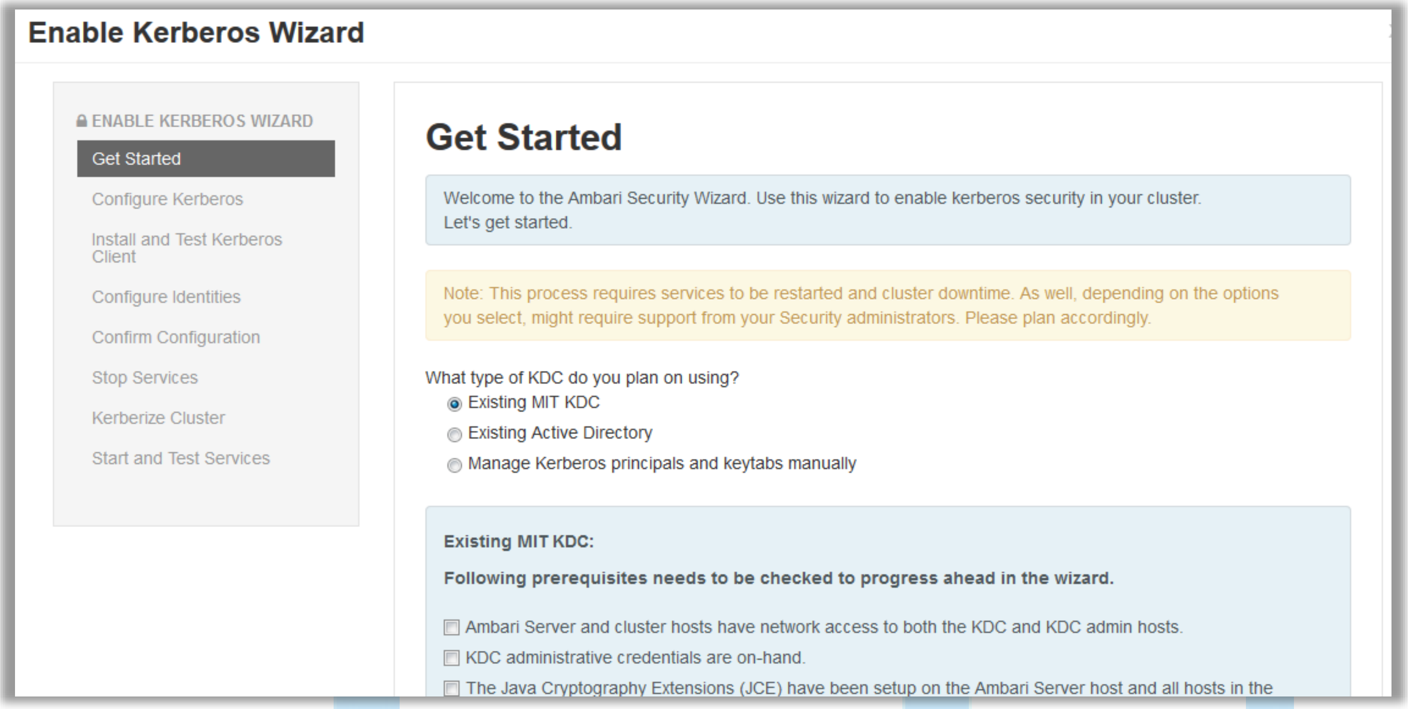
Service	Version	Status	Description
HDFS	2.7.1.2.3	Installed	Apache Hadoop Distributed File System
MapReduce2	2.7.1.2.3	Installed	Apache Hadoop NextGen MapReduce (YARN)
YARN	2.7.1.2.3	Installed	Apache Hadoop NextGen MapReduce (YARN)
Tez	0.7.0.2.3	Installed	Tez is the next generation Hadoop Query Processing framework written on top of YARN.
Hive	1.2.1.2.3	Installed	Data warehouse system for ad-hoc queries & analysis of large datasets and table & storage management service
HBase	1.1.1.2.3	Installed	A Non-relational distributed database, plus Phoenix, a high performance SQL layer for low latency applications.
Pig	0.15.0.2.3	Installed	Scripting platform for analyzing large datasets
Sqoop	1.4.6.2.3	Installed	Tool for transferring bulk data between Apache Hadoop and structured data stores such as relational databases
Oozie	4.2.0.2.3	Installed	System for workflow coordination and execution of Apache Hadoop jobs. This also includes the installation of the optional Oozie Web Console which relies on and will install the ExtJS Library.
ZooKeeper	3.4.6.2.3	Installed	Centralized service which provides highly reliable distributed coordination

Step 2: Now Click on Kerberos



Kerberos security is disabled

Step 3: After that you will see a form to fill up app the information regarding realm, principal, hostname etc.



Enable Kerberos Wizard

Get Started

Welcome to the Ambari Security Wizard. Use this wizard to enable kerberos security in your cluster. Let's get started.

Note: This process requires services to be restarted and cluster downtime. As well, depending on the options you select, might require support from your Security administrators. Please plan accordingly.

What type of KDC do you plan on using?

● Existing MIT KDC
○ Existing Active Directory
○ Manage Kerberos principals and keytabs manually

Existing MIT KDC:

Following prerequisites needs to be checked to progress ahead in the wizard.

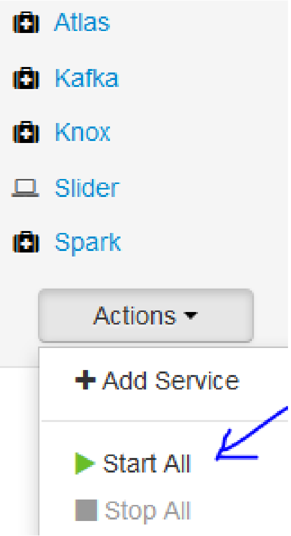
□ Ambari Server and cluster hosts have network access to both the KDC and KDC admin hosts.
□ KDC administrative credentials are on-hand.
□ The Java Cryptography Extensions (JCE) have been setup on the Ambari Server host and all hosts in the

Step 4: You need to setup Kerberos server and principal before connecting Ambari to it.

- Creating KDC server
- Creating principal and realms
- Creating keytabs

Step 5: Once you fill the form you need to restart the services.

- Stop-all
- Start-all



→ LDAP Integration

Solution: On the Ambari Server host, open /etc/ambari-server/conf/ambari.properties with a text editor

Make the following edits:

Step 1: Add the client security property and set it to LDAP

```
client.security=ldap
```

Step 2: Add the following properties for the LDAP server, including whether to use SSL, whether you can bind to the server anonymously or if you need to provide manager credentials, the base DN, and so forth.

Property	Values	Description
authentication.ldap.useSSL	true or false	If true, use SSL when connecting to the LDAP server.
authentication.ldap.primaryUrl	server:port	The hostname and port for the LDAP server. Example: my.ldap.server:389
authentication.ldap.secondaryUrl	server:port	The hostname and port for the secondary LDAP server. Example: my.secondary.ldap.server:389
authentication.ldap.baseDn	[Distinguished Name]	The base Distinguished Name to search in the directory for users. Example: ou=people,dc=hadoop,dc=apache,dc=org

authentication.ldap.bindAnonymously	true or false	If true, bind to the LDAP server anonymously
authentication.ldap.managerDn	[Full Distinguished Name]	If Bind anonymous is set to false, the Distinguished Name ("DN") for the manager. Example: uid=hdfs,ou=people,dc=hadoop,dc=apache,dc=org
authentication.ldap.managerPassword	[password]	If Bind anonymous is set to false, the password for the manager
authentication.ldap.usernameAttribute	[LDAP attribute]	The attribute for username Example: uid

When you have made the necessary edits to the properties file, you can go on to start (or re-start) the server. Initially the users you have enabled will all have User privileges. Users can read metrics, view service status and configuration, and browse job information. For these new users to be able to start or stop services, modify configurations, and run smoke tests, they need to be Admins. To make this change, use the Ambari Web Admin View.

Start the Ambari Server

- To start the Ambari Server: `ambari-server start`
- To check the Ambari Server processes: `ps -ef | grep Ambari`