Big Data CDH and Cloudera Manager Cluster Installation

Contents

[1 Introduction 5](#_Toc431905254)

[1.1 Assumptions 6](#_Toc431905255)

[1.2 A Word on Repo s 7](#_Toc431905256)

[1.3 Add the Repo File to the server 10](#_Toc431905257)

[1.4 Add THE LATEST COMPATIBLE Citi package for Java to all nodes in the cluster 10](#_Toc431905258)

[1.5 Install & Configure MySQL for the MetaStores Hue/Hive, Oozie and other CDH components 11](#_Toc431905259)

[1.6 Install the Packages and Start Cloudera Manager 13](#_Toc431905260)

[1.6.1 Verify the SSH Keys 13](#_Toc431905261)

[1.6.2 Verify the YUM cache 13](#_Toc431905262)

[1.6.3 Install the latest BD repo Cloudera Manager packages : 13](#_Toc431905263)

[1.6.4 Complete MySQL setup. Some parts of the mysql installation and configuration are dependent on the CDH and CM binaries being present 14](#_Toc431905264)

[1.6.5 Perform Parcel and custom parcel installation s 14](#_Toc431905265)

[1.6.6 Verify your SSH keys 14](#_Toc431905266)

[1.6.7 Start Cloudera manager server: 14](#_Toc431905267)

[1.7 Online configuration of Cloudera Manager and deployment to other nodes 16](#_Toc431905268)

[1.7.1 Supply the License Code for Cloudera Manager 16](#_Toc431905269)

[1.7.2 Add Hosts 20](#_Toc431905270)

[1.7.3 Installation Criteria 27](#_Toc431905271)

[1.7.4 Role Assignments 28](#_Toc431905272)

[1.7.5 Service Configuration and Data Locations 33](#_Toc431905273)

[1.8 Oozie 41](#_Toc431905274)

[1.9 Oozie MySQL database 42](#_Toc431905275)

[1.10 Enable the OOZIE Web Console (web UI) 42](#_Toc431905276)

[1.11 HUE WEB Server 45](#_Toc431905277)

[1.12 Set Heap Sizes for HIVE 45](#_Toc431905278)

[1.13 Using CGroups 46](#_Toc431905279)

[1.14 Total Resources 46](#_Toc431905280)

[1.15 IMPALA 47](#_Toc431905281)

[1.16 HBASE 47](#_Toc431905282)

[1.17 HIVE 47](#_Toc431905283)

[1.18 Configuring HUE to use HS2 instead of Beeswax 48](#_Toc431905284)

[1.19 IDENTIFY The Cluster 49](#_Toc431905285)

[1.19.1 Set the NAME for the new cluster 49](#_Toc431905286)

[1.19.2 Set the Banner Text for the Name and Version 50](#_Toc431905287)

[1.19.3 Set the Alerts Email Header / Footer and recipient list 51](#_Toc431905288)

[1.20 Adding Kerberos Authentication 52](#_Toc431905289)

[1.20.1 Known Issue with Kerberos in nCloudera Manager 52](#_Toc431905290)

[1.21 Uninstall Process 53](#_Toc431905291)

[1.22 Citi SSH keys 56](#_Toc431905292)

[1.23 Notes on HA 58](#_Toc431905293)

[1.24 Other Documents to Reference 58](#_Toc431905294)

[1.24.1 Hadoop Build Catalog Template 58](#_Toc431905295)

[1.24.2 Standard Cluster Installation and Use of Connectors 58](#_Toc431905296)

[1.24.3 CATE Hadoop Reference Architecture 58](#_Toc431905297)

[1.24.4 MySQL Backup & Restore 58](#_Toc431905298)

[1.24.5 MySQL MetaStores 58](#_Toc431905299)

[1.25 Citi Java Package 59](#_Toc431905300)

[1.25.1 Modifying CMF\_AGENT\_JAVA\_HOME 61](#_Toc431905301)

[1.25.2 Modifying Service Settings 61](#_Toc431905302)

[1.26 SAML / SSO for CMS 63](#_Toc431905303)

[1.27 SAML / SSO for HUE 63](#_Toc431905304)

[1.28 Llama 66](#_Toc431905305)

[1.29 SQOOP 71](#_Toc431905306)

[1.30 Accumulo – Ask before installing this 72](#_Toc431905307)

[1.31 Navigator 74](#_Toc431905308)

[1.32 SPARK 74](#_Toc431905309)

[1.32.1 Spark Shell Mode 74](#_Toc431905310)

[1.32.2 Spark Dynamic Resource Allocation 74](#_Toc431905311)

[1.32.3 CM51 Spark History Server 75](#_Toc431905312)

[1.33 HTTPS & LDAP 75](#_Toc431905313)

[2 Additional Configuration Changes for Citi Builds 77](#_Toc431905314)

[2.1 Connectors 77](#_Toc431905315)

[2.2 Changes required by the CIVA audit 77](#_Toc431905316)

[2.2.1 Disable “Remember Me” within Cloudera Manager Administration 77](#_Toc431905317)

[2.2.2 Enable authentication within YARN service’s configuration 78](#_Toc431905318)

[2.2.3 Enable authentication within HDFS1 service’s configuration 78](#_Toc431905319)

[2.2.4 Security Harden Hue 79](#_Toc431905320)

[2.2.5 SET HUE to default to no access 81](#_Toc431905321)

[2.2.6 Disable webhdfs interface 81](#_Toc431905322)

[2.2.7 C4 Only - Disable “debug” ports within Cloudera Manager Administration 83](#_Toc431905323)

[2.2.8 C4 only - To disable Navigator, follow these instructions: 83](#_Toc431905324)

[2.2.9 Restrict access to keystore file 84](#_Toc431905325)

[2.2.10 Default umask for HDFS 84](#_Toc431905326)

[2.2.11 Navigator Metadata Server Switch to HTTPS 85](#_Toc431905327)

[2.2.12 Zookeeper JMX Agent Authentication 85](#_Toc431905328)

[2.2.13 Set Sentry and HDFS ACL synchronization 86](#_Toc431905329)

[2.3 YARN / HUE Logging problems 87](#_Toc431905330)

[2.4 NFS Gateway 89](#_Toc431905331)

[2.5 Cloudera / EMC Isilon 94](#_Toc431905332)

[2.6 Custom Settings IN CMS 95](#_Toc431905333)

[2.7 Setting CMS and CDH logs to use syslog streaming 97](#_Toc431905334)

[2.8 CM 4.5 issue with Talend and Flume starving SMON and HMON services 97](#_Toc431905335)

[2.9 Limiting the use of /tmp 97](#_Toc431905336)

[2.10 HDFS log files 101](#_Toc431905337)

[2.11 HDFS Extended ACL’s 101](#_Toc431905338)

[2.11.1 Enabling HDFS Extended ACLs 101](#_Toc431905339)

[2.11.2 Enabling ACLs 102](#_Toc431905340)

[2.11.3 Commands 102](#_Toc431905341)

[2.12 CMS Monitor Stability Issues 104](#_Toc431905342)

[2.13 Map Reduce MR1 Job Management ID’s 104](#_Toc431905343)

[2.14 Add your custom configurations here – one heading per change 105](#_Toc431905344)

[2.15 Known Issues 106](#_Toc431905345)

[2.15.1 HUE has a known issue that is scheduled to be fixed in HUE 3.8. 106](#_Toc431905346)

[2.15.2 Beeline gives error of hiveconf not found 106](#_Toc431905347)

[2.15.3 C 5.4 known Installation Issues 106](#_Toc431905348)

# Introduction

A package of all the CDH and Cloudera Manager RPMs has been created and will be available once the correct repo locations are added to the server build. The process to follow will be :

1. [Add the repo file to the server](#_Add_the_Repo)
2. [Add or Update Java on the server](#_Citi_Java_Package)
3. [Install and Configure MySQL for ALL component databases](#_Install_&_Configure)
4. [Install the main package and start Cloudera Manager](#_Install_the_Main)
5. [Online configuration of Cloudera Manager and deployment to other nodes](#_Online_configuration_of)
6. [Deployment and configuration of services](#_Service_Configuration_and)
7. [Adding Kerberos authentication](#_Adding_Kerberos_Authentication)

If you’re re installing on a previously used cluster node then make sure to follow the [Uninstal Process](#_Uninstall_Process) before starting a new install

You should be familiar with the [Notes on High Availability](#_Notes_on_HA) and other [Reference materials](#_Reference). Examples of expected outputs are available as guides in the [Appendix](#_Appendix).

## **Assumptions**

1. Root level access is required

Full root access is not required but the following are minimal requirements:

GPACM\_ROOT\_PROD\_CMD\_BIGDATA\_PROD = {"yum","sed","service","chkconfig","id","rm","mv","/sbin/service","chown","install","tail","grep"};

if ( user in GPACM\_ROOT\_PROD\_USERS\_BIGDATA\_PROD && command in GPACM\_ROOT\_PROD\_CMD\_BIGDATA\_PROD && tolower(submithost) in GPACM\_ROOT\_PROD\_HOSTS\_BIGDATA\_PROD ) {

        BATCH\_ROOT\_CMD\_ENV ();

        setenv("PATH", "/usr/bin:/bin:/sbin");

        accept;

}

1. OU groups for servers hostnames and users must be completed before the cluster work starts

All hostnames users and ID’s must be configured within OU groups. Root level access permissions policy example is given above. See the [latest list](https://collaborate.citi.net/docs/DOC-211468) of ID’s and keytabs for verification

1. SSH keys; Kerberos keytabs and SSL certificates must be created before cluster work starts
2. An Install ID with SSH access (keys) to all nodes in the cluster must be availble

## A Word on Repo s

Our packages all come from citi standard repositories (repos)

All machines are build with access to soe-prod and this is the repo that all SA’s pull Linux updates from.

[soe6products]

name=SOE Linux 6 products including VTMs

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6products-x86\_64

enabled=0

gpgcheck=0

We have one package in this repo and it’s called **soe-bigdata-repo**

This package gets installed on all our cluster machines and generates access to our stand alone bigdata repos

The primary repo for Cloudera Manager components and parcels is soe-bigdata-5.

For C4 this repo is soe-bigdata-cm. there are also numerous version specific repos that hold cloudera-manager –server and cloudera-manager-agent packages at different versions. These separate repos allow us to install a specific version of CM when we need to.

YUM commands make use of the repos by naming them explicitly in the ‘enablerepo’ option

So to install cloudera manager components for version 4.5.0 you’d specify the enablerpo option and name the CM repo specific to version 4.5.0. As in:  
🡪yum install cloudera-manager-server --disablerepo=\* --enablerepo=soe-bigdata-cm450

You can also view the contents of these repos in a browser by entering the associated URL that is embedded in each file.

This URL is also specified in the Cloudera Manager web UI when you’re using the add host wizard and it asks for the custom repo to be used.

Here are the main repos for C5

**Note that the cloudera-manager-server and cloudera-manager-agent packages for C5 are only available in the version specific soe-bigdata-cm500 repo not in the soe-bigdata-5 repo which will normally hold only the current version of these packages**

**Note2: even though it has not been removed yet, no one should be using the old soe-bigdata-products repo as it contain vulnerable versions of packages and using these versions will cause conflicts with other required components in the build. This is replaced in all cases by the soe-bigdata-c5 repo.**

# cat soe-bigdata-5.repo

[soe-bigdata-5]

name=soe bigdata5 products

baseurl=http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6c5products-x86\_64

enabled=0

gpgcheck=0

# cat soe-bigdata-c5.repo

[soe-bigdata-c5]

name=soe bigdata c5 products

baseurl=http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6c5bigdataproducts-x86\_64

enabled=0

gpgcheck=0

/etc/yum.repos.d >cat soe-bigdata-cm500.repo

[soe-bigdata-cm500]

name=soe bigdata cm500 products

baseurl=http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6cm500products-x86\_64

enabled=0

gpgcheck=0

/etc/yum.repos.d >cat soe-bigdata-cdh5.repo

[soe-bigdata-cdh5]

name=soe bigdata cdh5 products

baseurl=http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6cdh5products-x86\_64

enabled=0

gpgcheck=0

/etc/yum.repos.d >cat soe-bigdata-at.repo

[soe-bigdata-at]

name=soe bigdata analytical tools products

baseurl=http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6bigdataanalyticaltoolsproducts-x86\_64

enabled=0

gpgcheck=0

**For audit compliance we use the standard Linux engineering repos to source as many packages as possible. Not all SOE Linux repos will be placed on a new build machine but make sure that at least the following repos are available:**

[soe6u4]

name=SOE Linux 6 Update 4

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6u4-x86\_64

enabled=0

gpgcheck=0

[soe6u5]

name=SOE Linux 6 Update 5

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6u5-x86\_64

enabled=0

gpgcheck=0

[soe6products]

name=SOE Linux 6 products including VTMs

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6products-x86\_64

enabled=0

gpgcheck=0

[soe6local]

name=SOE Linux 6 local pacakges

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6local-x86\_64

enabled=0

gpgcheck=0

[soe6iiproducts]

name=soe6iiproducts

baseurl=http://gdsks1/SOELinux/repos/prod/soe6iiproducts-x86\_64/

enabled=0

gpgcheck=0

Standard SOE Linux repos should be present on all servers by default but we also need to add the following optional repos if they’re not already present

>vi /etc/yum.repos.d /ii.repo

[soe6iiproducts]

name=soe6iiproducts

baseurl=http://gdsks1/SOELinux/repos/prod/soe6iiproducts-x86\_64/

enabled=0

gpgcheck=0

>vi /etc/yum.repos.d /soe6local.repo

[soe6local]

name=SOE Linux 6 local pacakges

baseurl=http://gridmstsw1gd.nam.nsroot.net/SOELinux/repos/prod/soe6local-x86\_64

enabled=0

gpgcheck=0

Note that the server name in the URL in repo files that we add manually should match the server name in the standard repo files for the Linux build

For more details on the SOE optional repo see the full documentation at: <https://catecollaboration.citigroup.net/domains/platstor/osunix/stdsrelateddocs/RFP-InstallInfrastructureGuideForSOELinux8.pdf>

## Add the Repo File to the server

After the server build criteria have been completed and verified. Using ‘root’ ID perform the following steps on **all** server:

* Install the latest version of the BigData Repo package “BD\_bigdata\_repo” e.g. BD\_bigdata\_repo-4.2.0-100001.x86\_64.rpm.  
  sudo yum install BD\_bigdata\_repo.x86\_64
* Verify the available contents / packages
* For C4 use :
  + yum list available --disablerepo='\*' --enablerepo='soe-bigdata-c5, soe-bigdata-cm, soe-bigdata-cdh, soe6local, soe6iiproducts'
* For C5 use :
  + yum list available --disablerepo='\*' --enablerepo='soe-bigdata-c5, soe-bigdata-5, soe-bigdata-cdh5, soe6local, soe6iiproducts'
* Run ‘makecache’ to build the yum repo cache for efficiency and to detect any non working yum repos in /etc/yum.repos.d. Disable non working ones if they’re not needed.

## Add THE LATEST COMPATIBLE Citi package for Java to all nodes in the cluster

See the separate section on [java](#_Appendix) later in this doc

## Install & Configure MySQL for the MetaStores Hue/Hive, Oozie and other CDH components

CDH comes with an embedded Postgres DB (cloudera-manager-server-db) We replace this with a MySQL DB for better maintenance.

This process will add the MySQL-server and MySQL-client packages to the server. On stand alone or lab servers you may opt to save space and simplify the install by omitting this step. Configure MySQL defaults and create the necessary databases to be used as metastores.

Some of the MySQL installation steps can not be completed until after you have a CDH image on the machine since that is where some of the installation and configuration details come from.

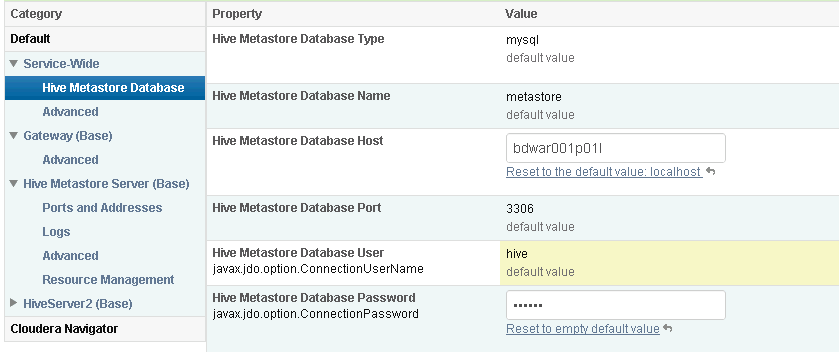
MySQL is required before you can complete the CMS and CDH installation

Since this is a long process and MySQL may be replaced by another RDBMS the whole is documented in a separate location. Refer to that [doc](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/MySQL_DB_For%20Cloudera_Manager_and_CDH.docx) for details:

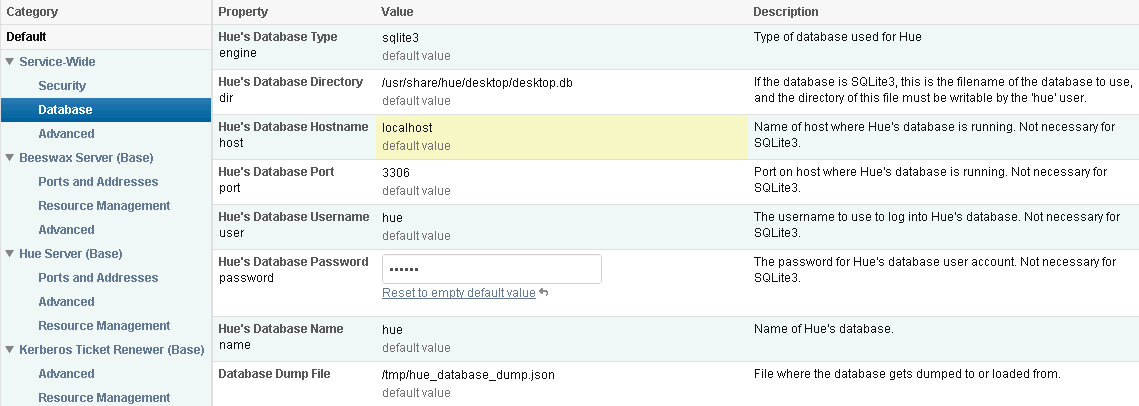
[https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/MySQL\_DB\_For Cloudera\_Manager\_and\_CDH.docx](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/MySQL_DB_For%20Cloudera_Manager_and_CDH.docx)

Once the MysQL databases have been created you must still go through the Cloudera Manager Server web UI configuration pages for the services and change the database type to MysQL - here’s an example of pages for changing Hive.

Hive Configuration:



Hue Configuration:



## Install the Packages and Start Cloudera Manager

Following steps to be done on proxy server

### Verify the SSH Keys

**At the command line of your install / admin machine create an SSH connection to every other machine in the cluster.**

### Verify the YUM cache

**yum clean all;  
yum makecache;**

### Install the latest BD repo Cloudera Manager packages :

pbrun yum -y install fuse redhat-lsb fuse-libs --enablerepo='soe6u5, soe6products, soe6local, soe-bigdata-c5';

pbrun yum -y install cyrus-sasl-gssapi libxslt --enablerepo='soe6u5, soe6products soe6local, soe-bigdata-c5';

For C4

pbrun yum install cloudera-manager-daemons cloudera-manager-agent enterprise-debuginfo cloudera-manager-server --enablerepo=soe-bigdata-cm;

pbrun yum install BD\_cloudera\_cdh\_parcel --enablerepo=soe-bigdata-cm;

pbrun yum install BD\_cloudera\_cdh\_parcel\* BD\_cloudera\_sentry\_parcel\* BD\_cloudera\_impala\_parcel\* BD\_cloudera\_SOLR\_parcel\*--enablerepo=soe-bigdata-cm

For C5

pbrun yum install cloudera-manager-daemons cloudera-manager-agent enterprise-debuginfo cloudera-manager-server --enablerepo=soe-bigdata-5;

pbrun yum install BD\_cloudera\_cdh\_parcel --enablerepo=soe-bigdata-5;

pbrun yum install BD\_cloudera\_cdh\_parcel\* --enablerepo=soe-bigdata-5;

You can also control the yum repos that come into play by specifying them on the command line using enable and disable parameters like the following:  
 --disablerepo='\*' --enablerepo='soe-bigdata,soe-bigdata-cm,soe-bigdata-cdh, soe6iiproducts, soe6u5'

In a pseudo cluster (single node) you may simplify installation by using Postgres embedded DB and so you’ll also want to install that package.  
pbrun yum install cloudera-manager-server-db --disablerepo='\*' --enablerepo='soe-bigdata,soe-bigdata-cm,soe-bigdata-cdh, soe6iiproducts, soe6u5'

Verify that /usr/java/latest (which is a link) points to the correct java installation. It is also recommended that you set an environment variable JAVA\_HOME=/usr/java/latest; and add this to your $PATH

### Complete MySQL setup. Some parts of the mysql installation and configuration are dependent on the CDH and CM binaries being present

Click [here](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/MySQL_DB_For%20Cloudera_Manager_and_CDH.docx) to access doc

~~If you’re using the embedded DB for Cloudera manager server then start the db service:  
service cloudera-scm-server-db start~~ **DON’T USE THE EMBEDDED “CLOUDERA\_MANAGER\_SERVER\_DB” FOR MULTI NODE CLUSTERS**

### Perform Parcel and custom parcel installation s

Add any parcel packages for components that are required for the cluster. BD\_cloudera\_cdh\_parcel is the main cdh components and may contain all that you need for the cluster. However, there may be other parcel packages that are required and they should also be installed at this time e.g. BD\_cloudera\_solr\_parcel or BD\_cloudera\_sentry\_parcel.

In rare cases you will want to install a non standard or custom parcel and details on handling parcels can be found in a separate document .Click [here](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/Cloudera%20manager%20parcels.doc) to access the doc.

### Verify your SSH keys

**Cloudera Manager will deploy binaries to the other nodes in your cluster using and SSH key and password to make connections to those machines. At the command line verify that your SSH connections from your admin machine to all other machines is working.**

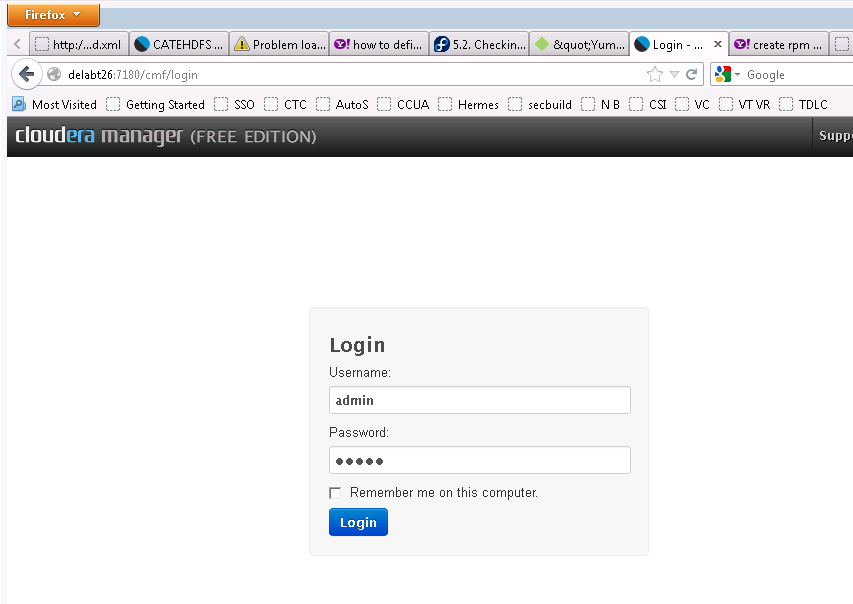
### Start Cloudera manager server:

service cloudera-scm-server start

Wait 1 minute for cloudera-scm-server to be ready. verify status with:service cloudera-scm-server statusservice cloudera-scm-agent status

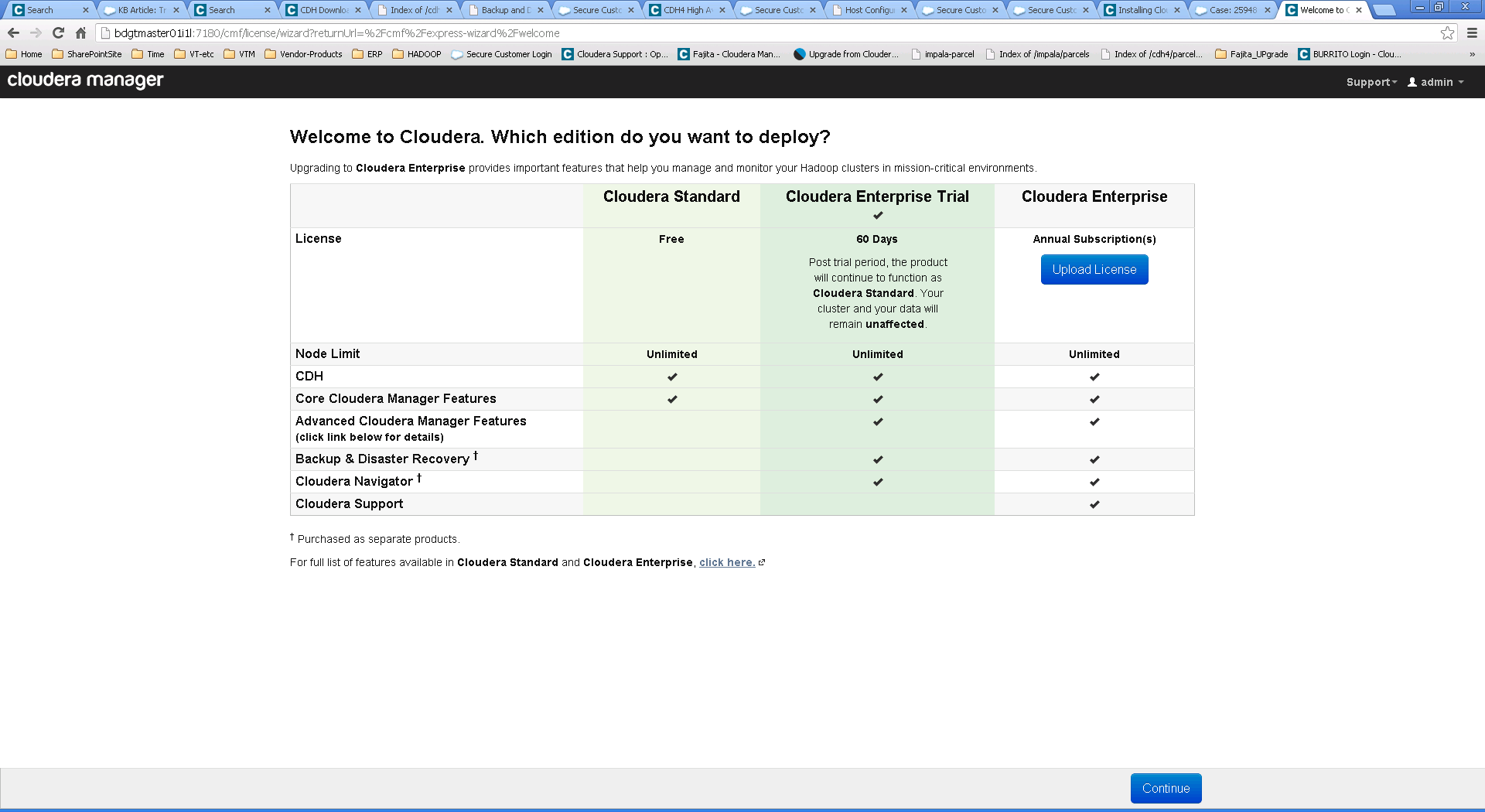
Use the browser to connect to Cloudera Manager. Hostname can be fully qualified or high order name for the installation / proxy server:

http://<hostname>:7180/cmf



Initial login credential is admin/admin.

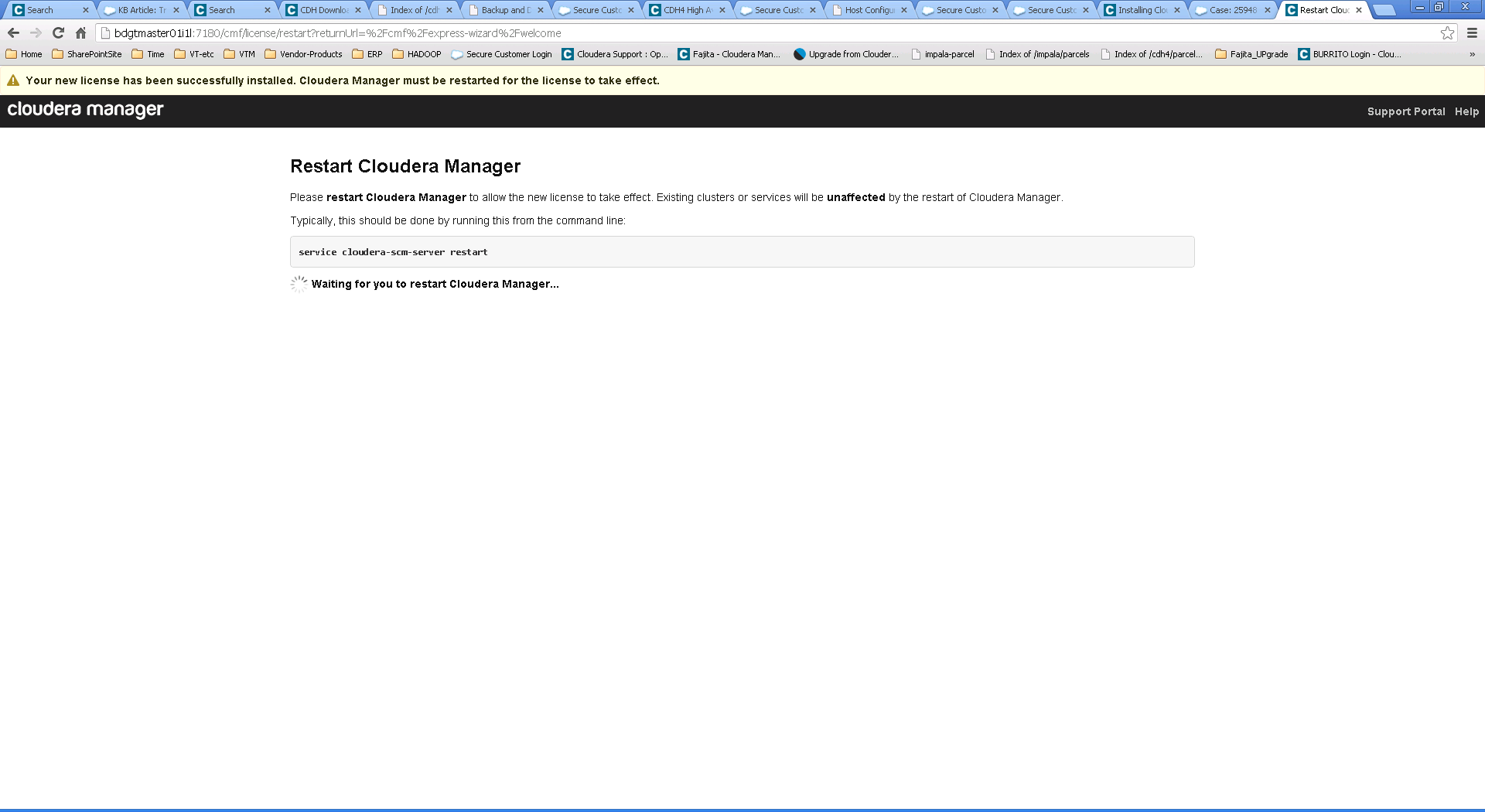
## Online configuration of Cloudera Manager and deployment to other nodes

On first log in you’ll be asked to choose your license strategy and given 3 options. Free Trial or enterprise license. For Cloud and pseudo cluster choose either Free or Trial 

**If you have purchased a license code then enter it and restart the cloudera-scm-server**

### Supply the License Code for Cloudera Manager

The licensed installation will present some additional configuration options and so it’s recommended to enter the license code now if you have it.

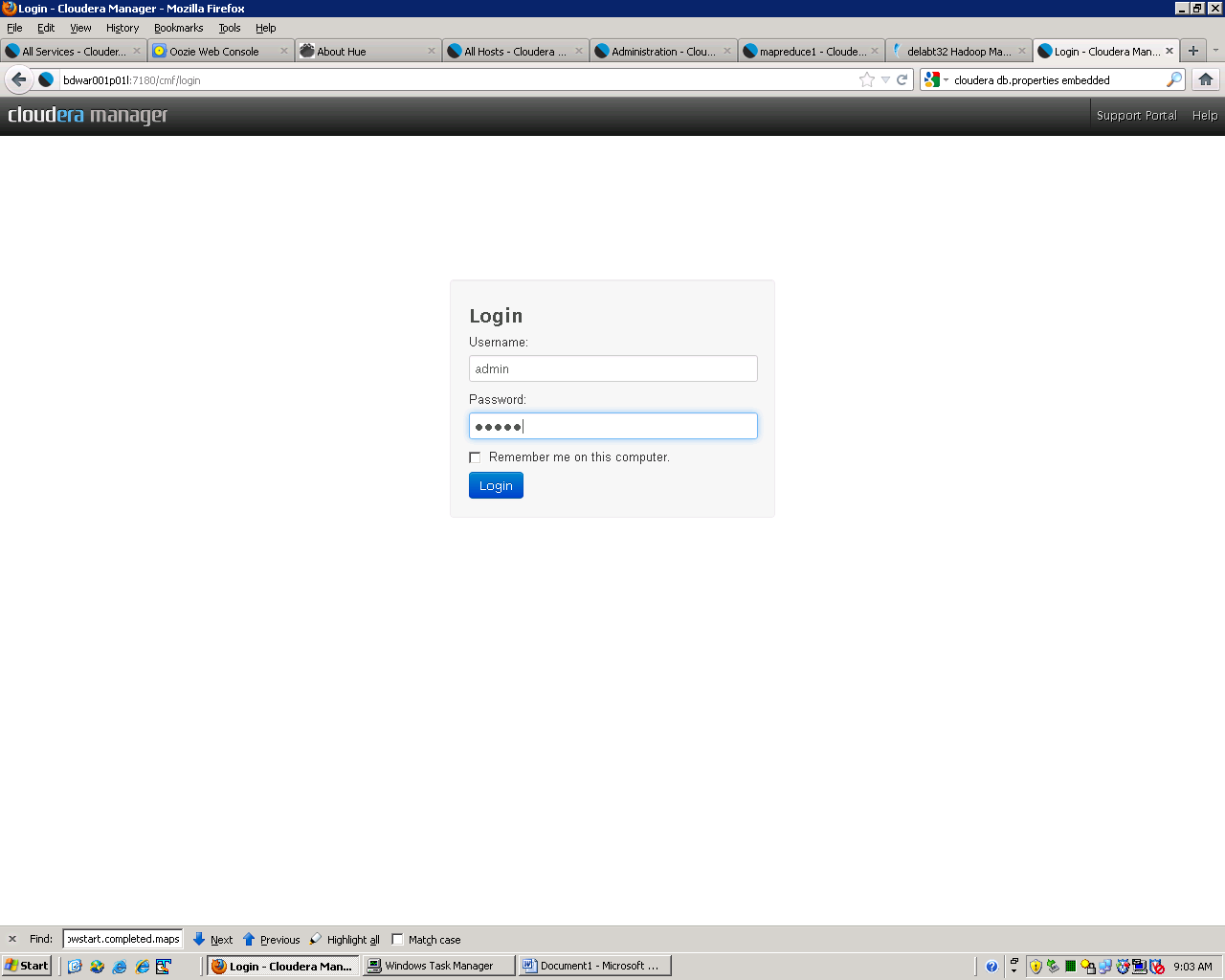
Once the license has been added you’ll be prompted to restart the Cloudera manager server at the linux server. Leave this prompt on screen until the restart has been completed then hit ‘continue’ 

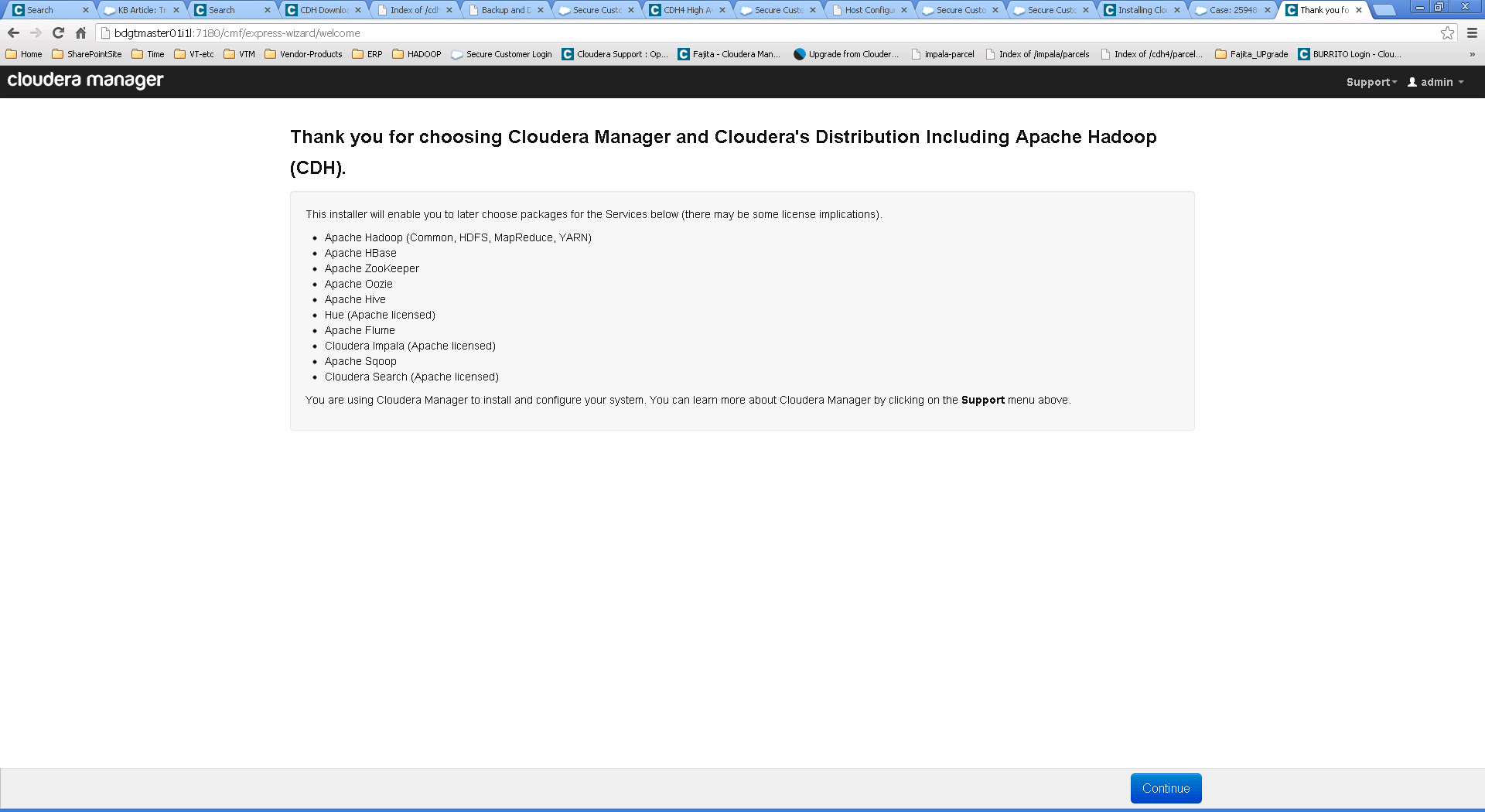
/etc/cloudera-scm-server >pbrun service cloudera-scm-server restart

Stopping cloudera-scm-server: [ OK ]

Starting cloudera-scm-server: [ OK ]

/etc/cloudera-scm-server >

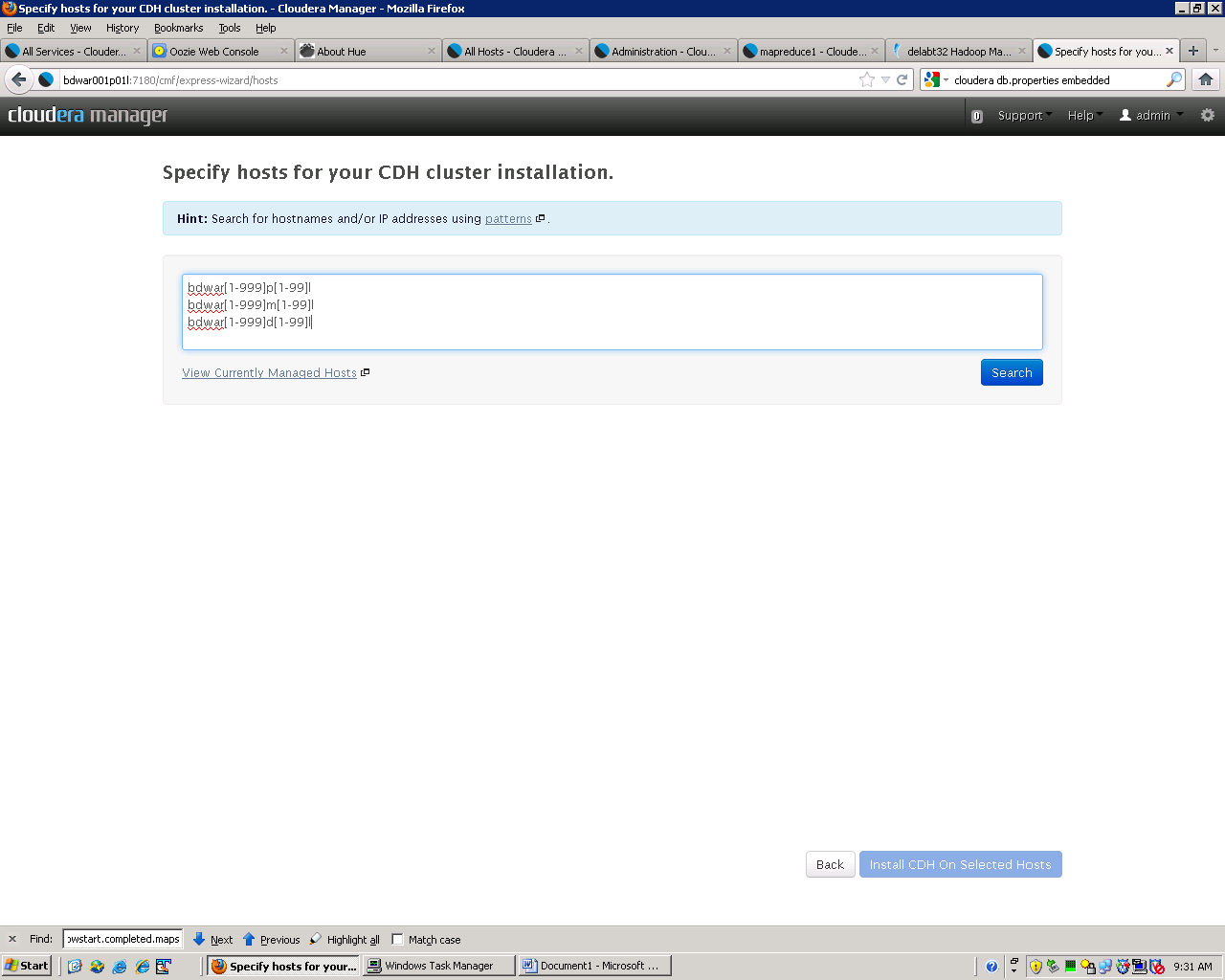
Then log in again  and the wizard will resume

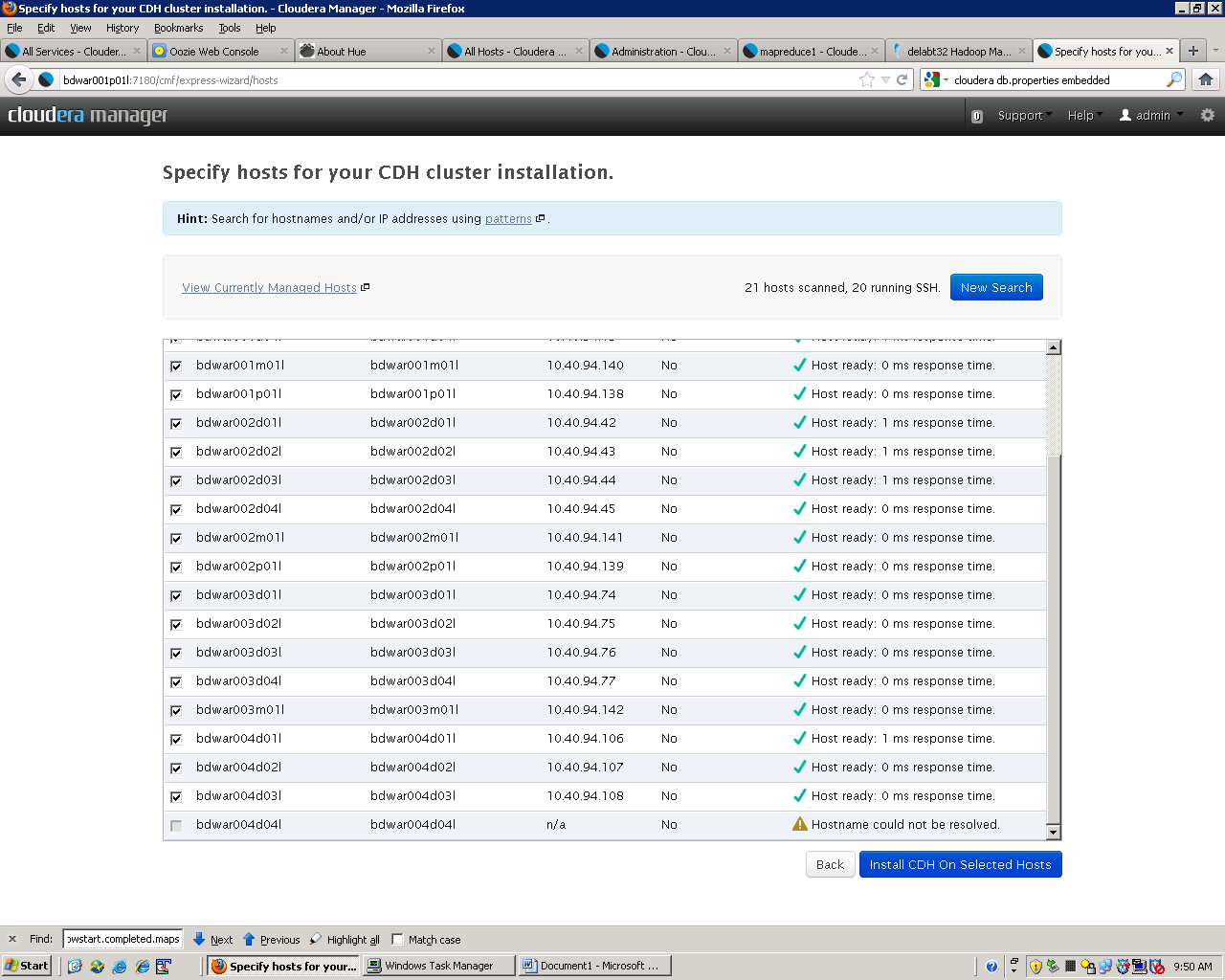
Click Continue

### Add Hosts

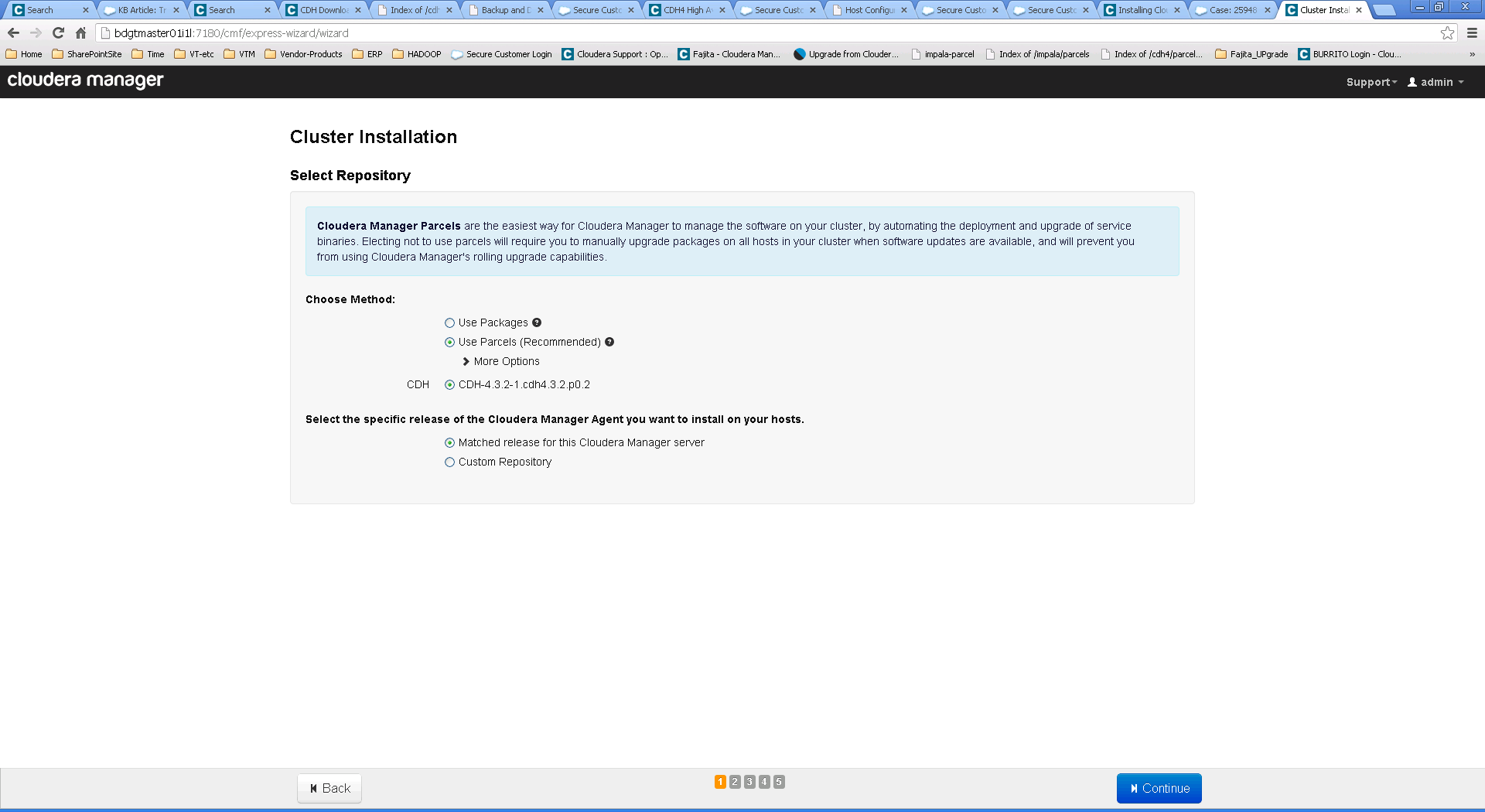
Deployment and configuration of services

Add hosts to the cluster by entering hostnames or search strings e.g. bdgtr00[1-6]d0[1-4]l

then click ‘search’ 

A message of hostname could not be resolved means that the host could not be found and this is typically encountered when a pattern is used that specifies more hosts than exist. 

#### Custom Repos

If you ran the install command to include BD\_cloudera\_cdh\_parcel then you’ll see the parcel version listed under “choose method” (parcel is the default) -- Click on ”Custom Repository” and provide the value as

For c4 use <http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6cm4products-x86_64>

for C5 use <http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6c5products-x86_64>

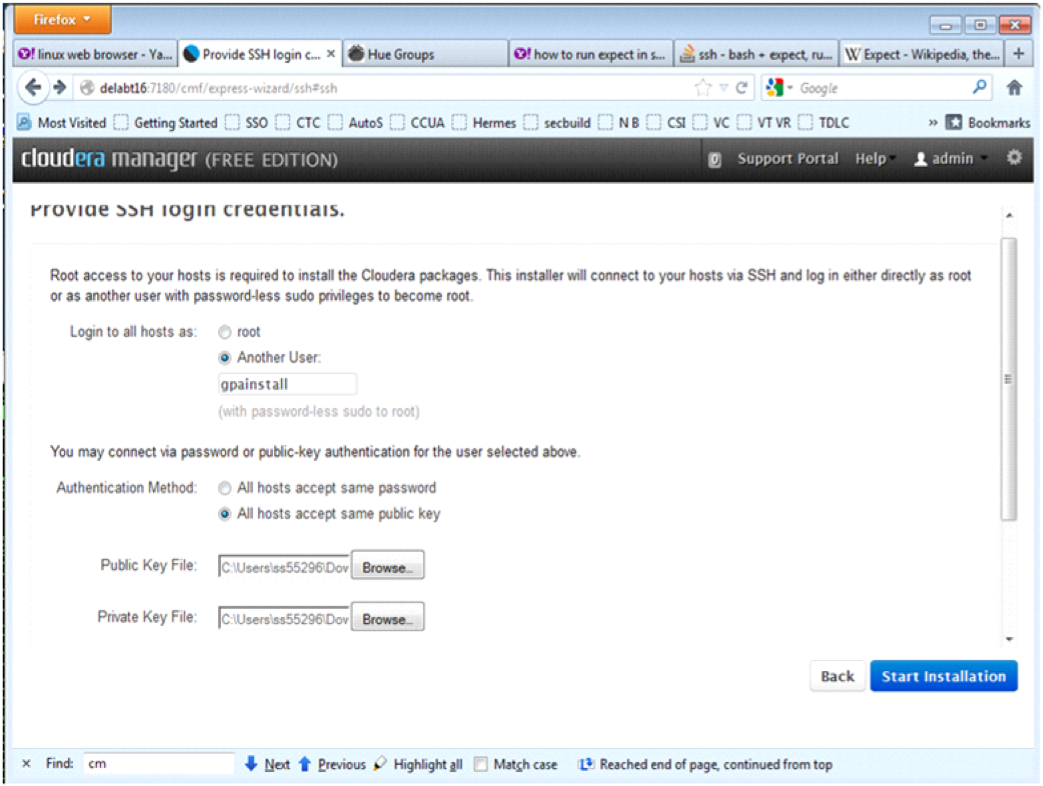
This can also be specified as an exact CM version e.g CM 4.8.0 or cm5.0.0

<http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6cm480products-x86_64>

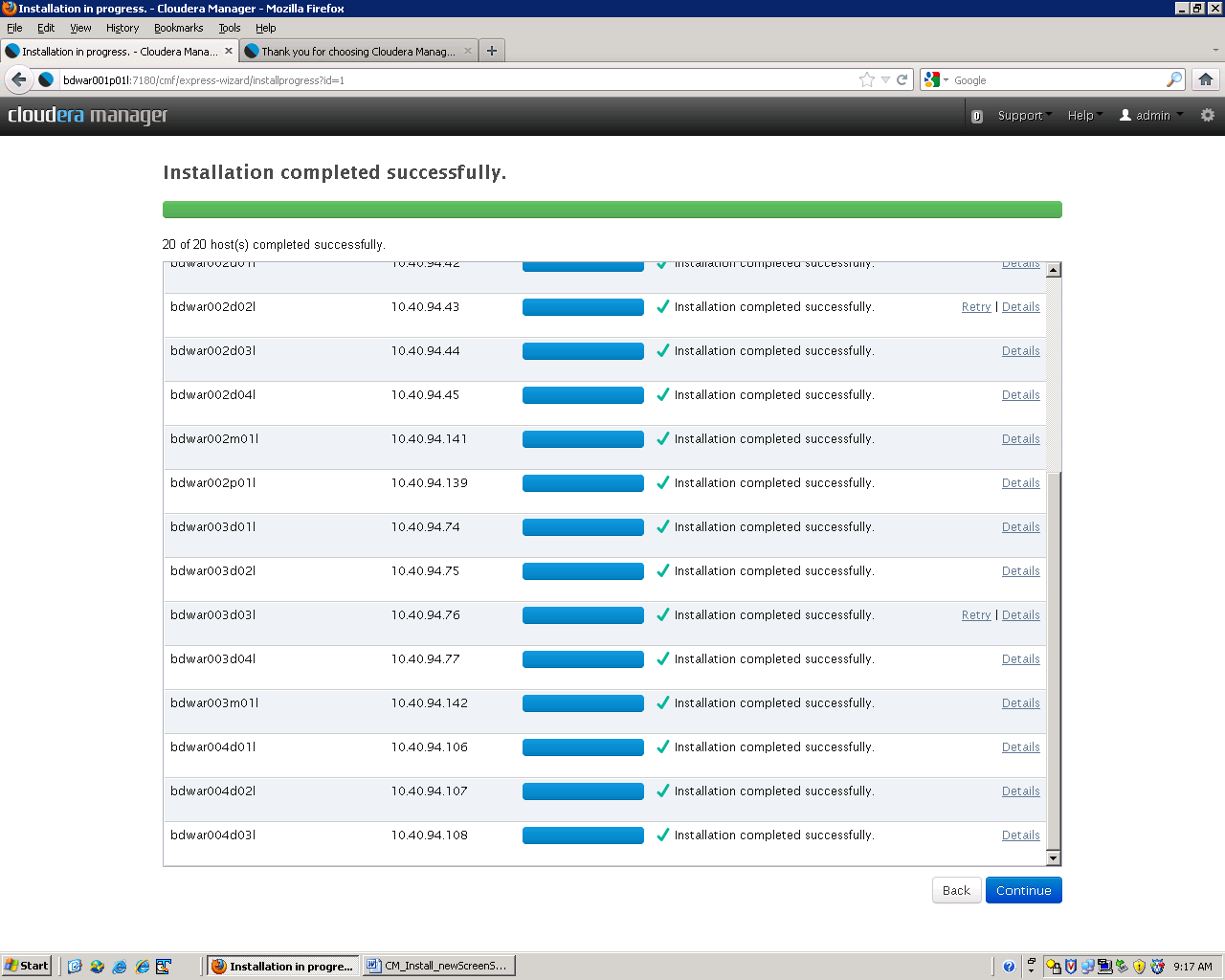
<http://gdsks1.nam.nsroot.net/SOELinux/repos/prod/soe6cm500products-x86_64>

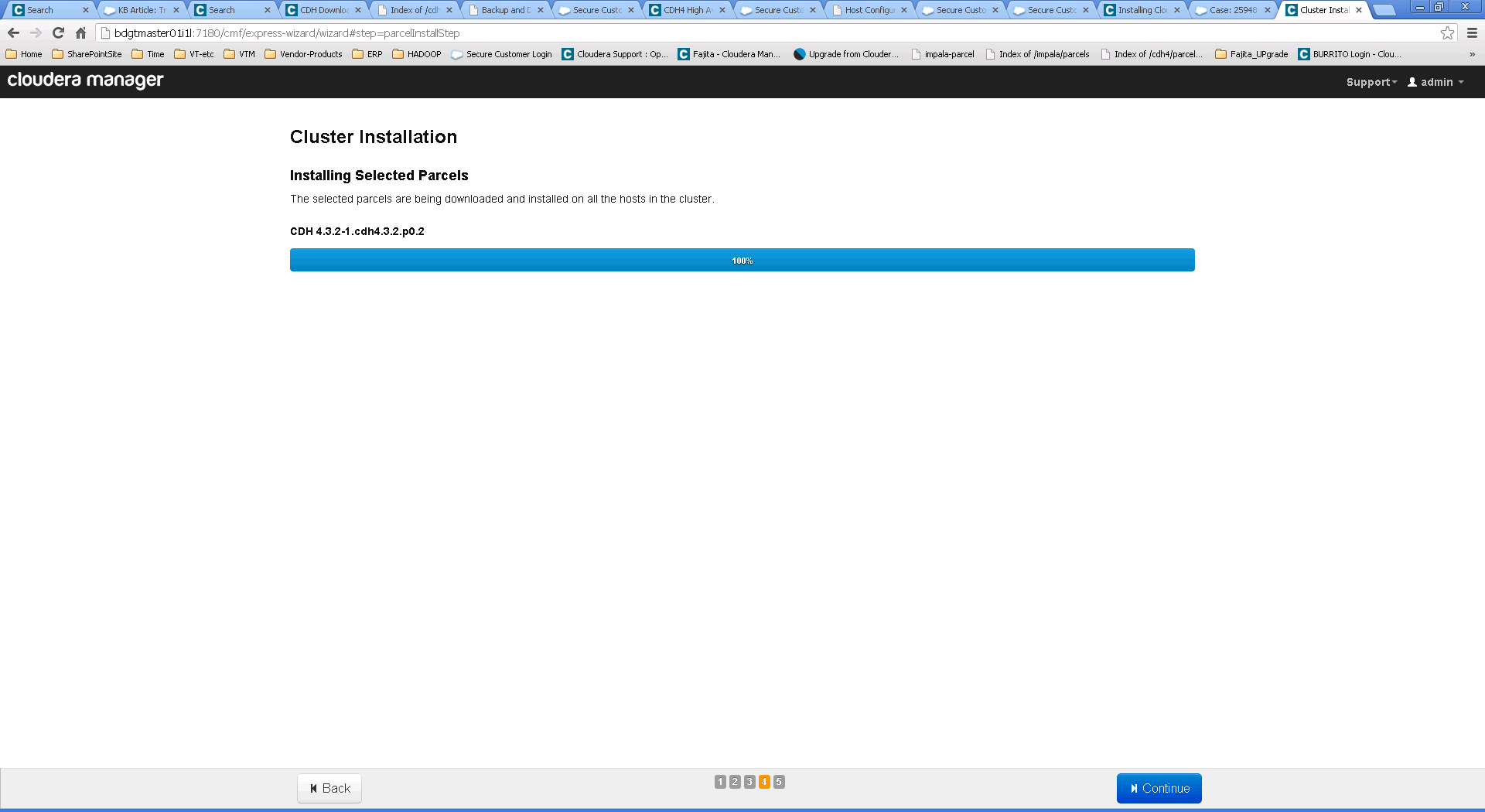
There is no value for “Custom GPG key” leave it blank and Click “Continue”

#### SSH Login Credentials

Enter ‘gpainstall’ (or other ID which has ssh keys enabled) and import the files for both public and private ssh keys    
If you are installing on a Cloud or pseudo cluster just specify the ID (root) and pswd for the server with no value for keys

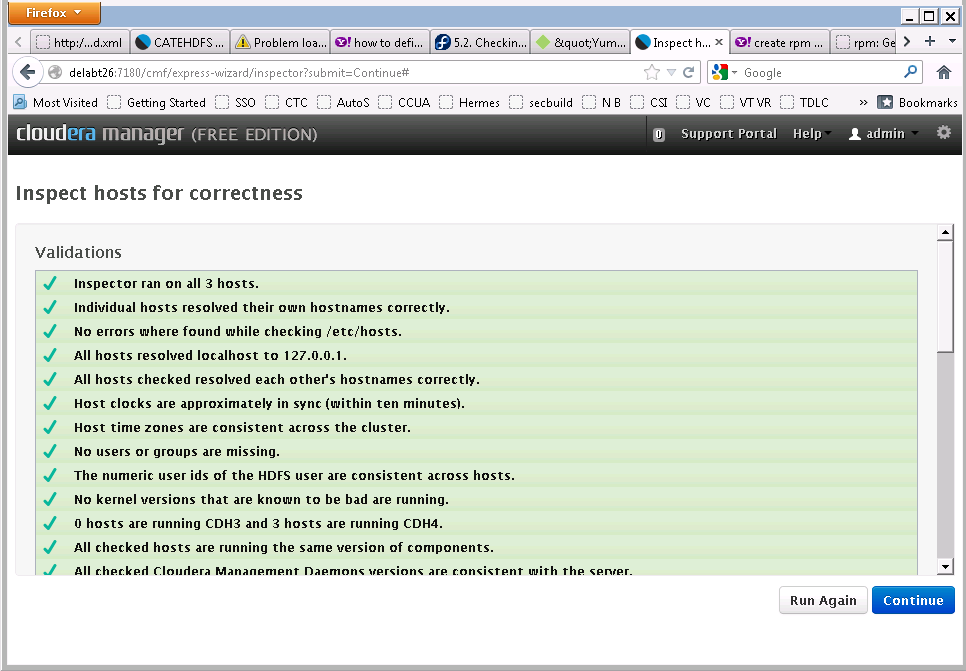
Once the installation is completed then click on Continue.

See the appendix for an example “Details” from a successfully completed installation. 

Once the Nodes are Added to the cluster then the ‘Parcel’ is distributed to them. Once this completes then click “Continue” 

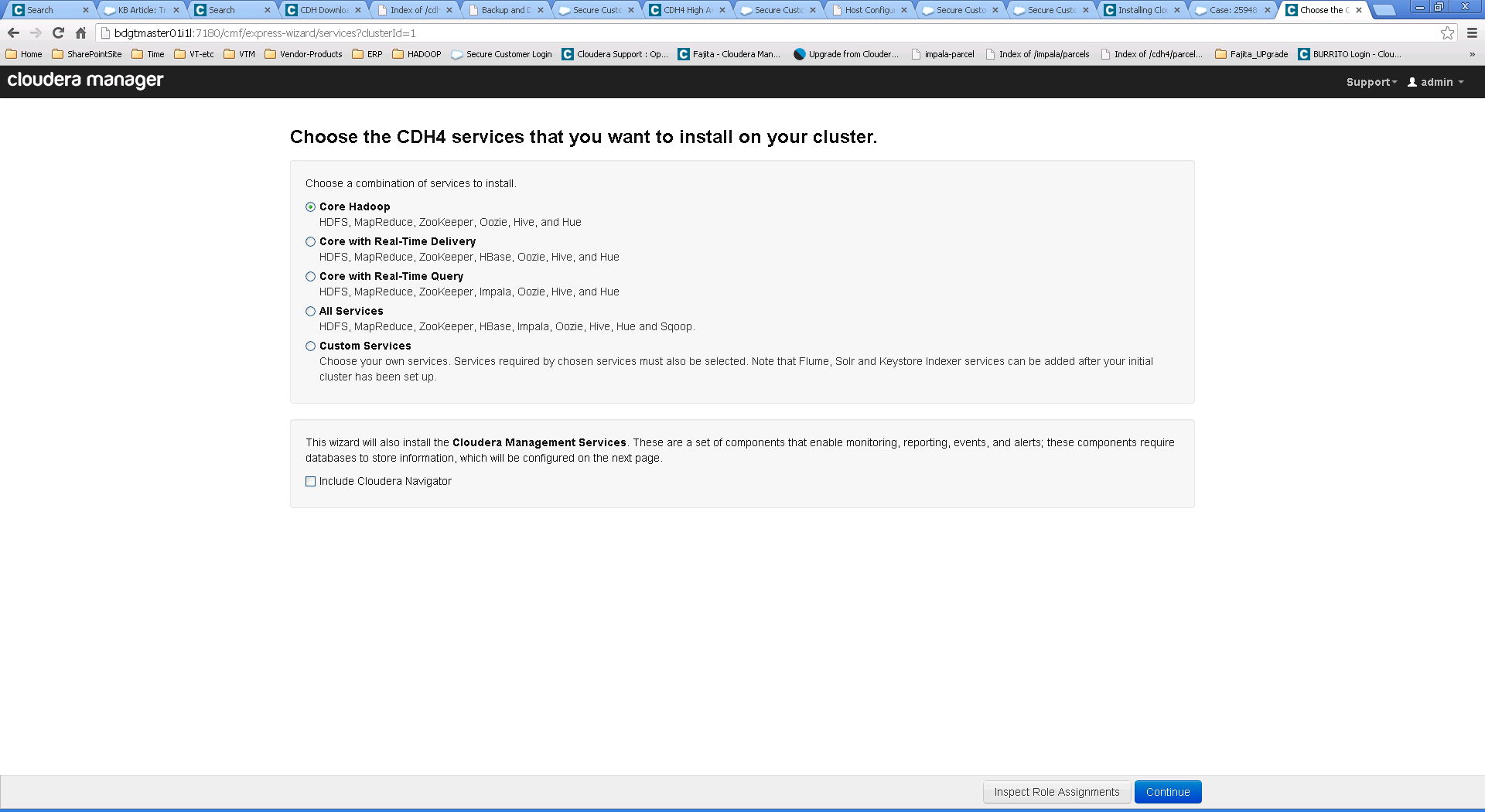
#### Host Inspector

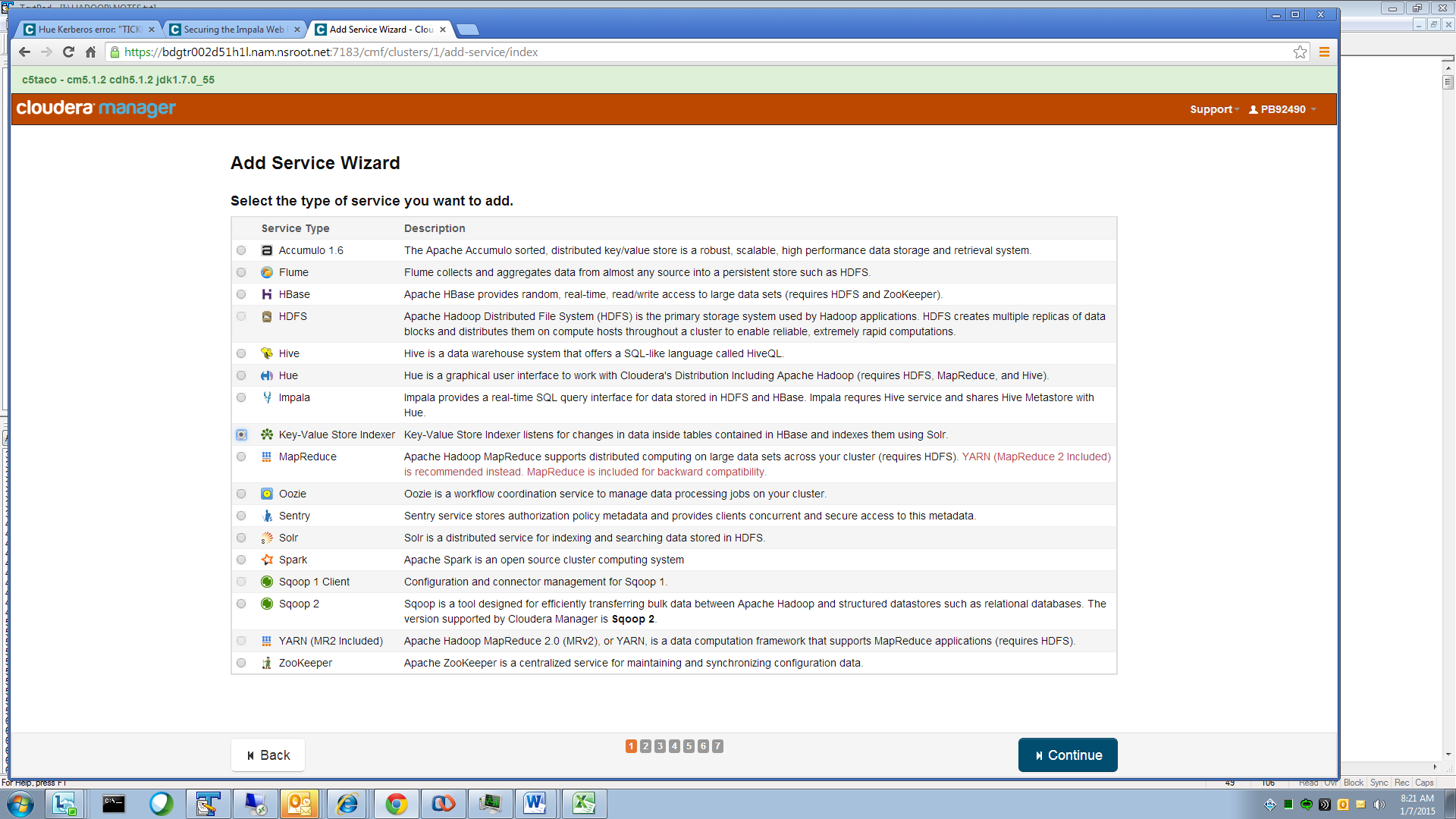
Let the host inspector run to verify the installed nodes

You should see all Validations successful. If not, correct the complaints and Run Again. 

Validation by Cloudera Manager should be all successful. Click Continue.

### Installation Criteria

After the verify report completes (re run if issues are reported) then choose the installation criteria (normally either “Core Hadoop” or “All Services”) 

NOTE: If Both SOLR and HBASE are being used in the cluster then you MUST install and enable the hbase indexing service KSIndexer 

### Role Assignments

Select ‘Inspect Role Assignments’ to verify what nodes will be used in the cluster

Assign the proper roles to the nodes then click Continue.

The cluster consists of multiple software servers (services) that must be assigned to a physical Linux server (machines). There are 3 types of machine; Proxy; master and data nodes. Services must be assigned to the correct type of machine and NOT to the other types. The proxy is also the CM server machine and runs all management services. This list does NOT show HA duplicates except for NN & JT

**Admin – CMS - Proxy machine – Roles – machines running Cloudera Manager Server**

Admin functions These functions are on both **CMS** admin machines

* Activity Monitor
* Alert Publisher
* Event Server
* Host Monitor
* Navigator Server This may require adding the service in CMS before it can be allocated
* Reports Manager
* Service Monitor

**Edge Server** Functions These functions are duplicated on all the **Proxy** and **Analytical Tools Nodes**

* + Flume Agent
  + HBase Gateway
  + HDFS Gateway
  + HDFS NFS Gateway
  + Hive Gateway
  + Solr Gateway
  + Spark Gateway
  + Sqoop1 Gateway
  + YARN (MR2 Included) Gateway
  + Accumulo Gateway 🡨 do not deploy

**Master 1 - Roles**

* Zookeeper Server
* JournalNode
* HttpFS
* Hbase Master
* NameNode
* Failover Controller (NN)
* HBase Thrift Server
* C5 – SentryMaster
* C5 – Spark Master & History Server
* C5 – Yarn Node Manager
* C5 – Hbase Thrift Server
* C5 – Lily Hbasae Indexer
* C5 – Accumulo Master,Tracer, Garbage Collector, Monitor 🡨 do not deploy

**Master 3 - Roles**

* Zookeeper Server
* JournalNode
* HttpFS
* HBase Master
* HBase Thrift Server
* Balancer
* C4 – JobTracker
* C4 – Failover Controller (JT)
* C5 – Yarn history Server
* C5 – Yarn Resource Manager

**Master 2 - Roles**

* Zookeeper Server
* JournalNode
* HttpFS
* Hbase Master
* NameNode (stand by)
* Failover Controller (NN)
* Impala Catalog Server
* Impala StateStore Daemon
* C4 – Job Tracker(standby)
* C4 – Failover Controller (JT)
* C5 – Yarn Resource Manager (Standby)
* C5 – Yarn Node Manager
* Hive Metastore Server

Edge Server Services on Master 2

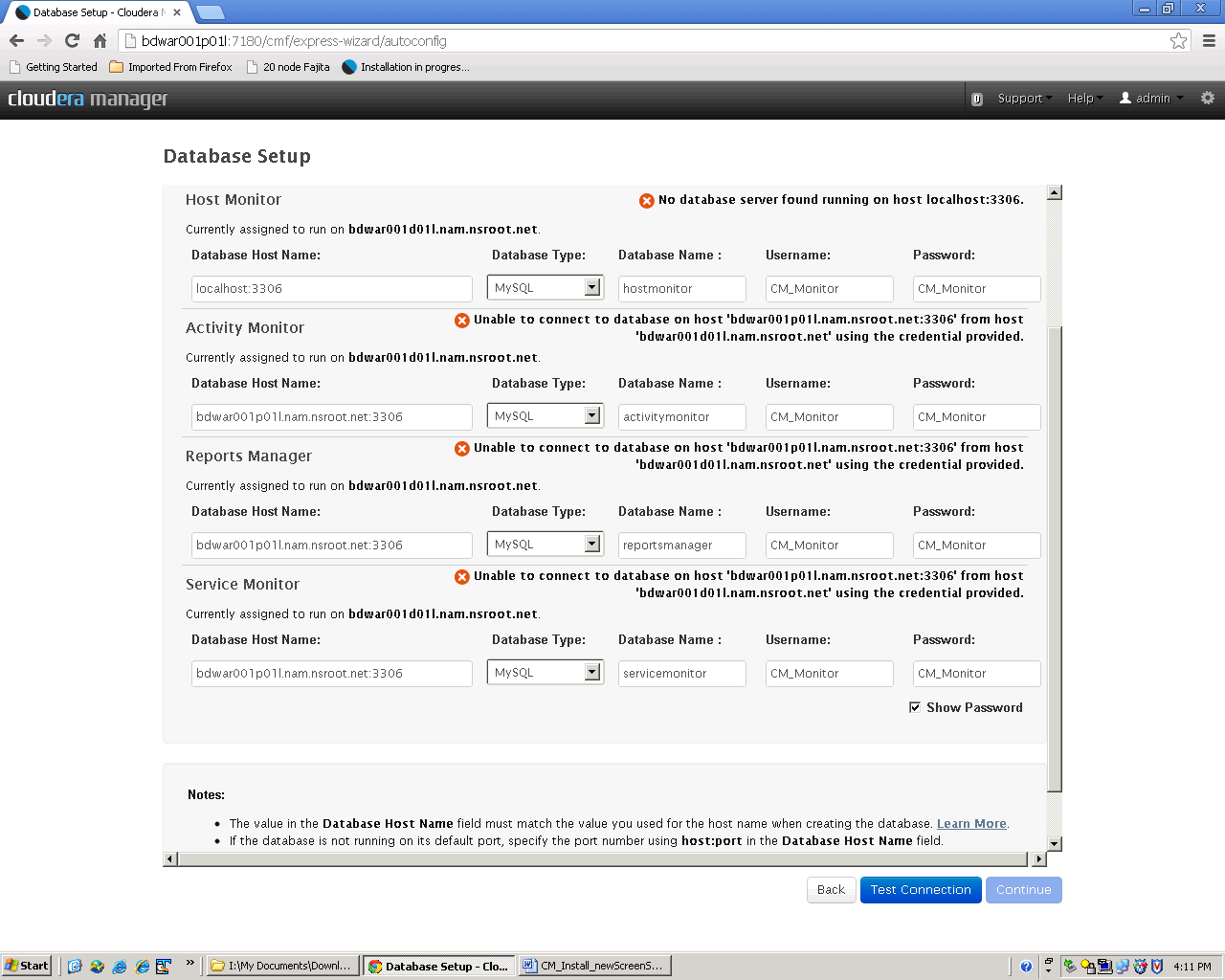
* + Hue Server
  + Hive Server2
  + Hive WebHCat Server
  + (defunct ) Beeswax Server
  + Kerberos Ticket Renewer
  + Oozie Server
  + Sqoop2 Server

**Data Node / Worker - Roles**

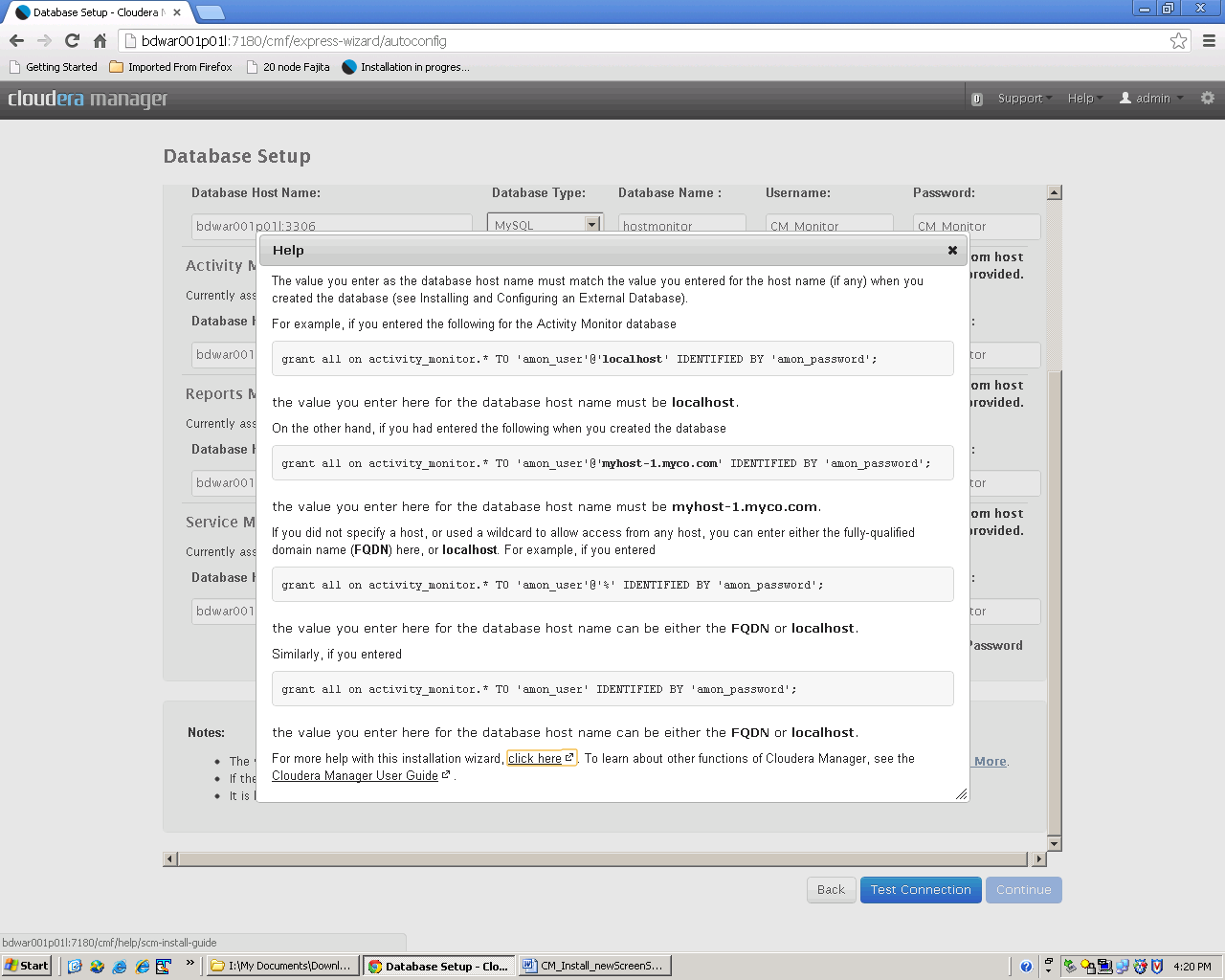
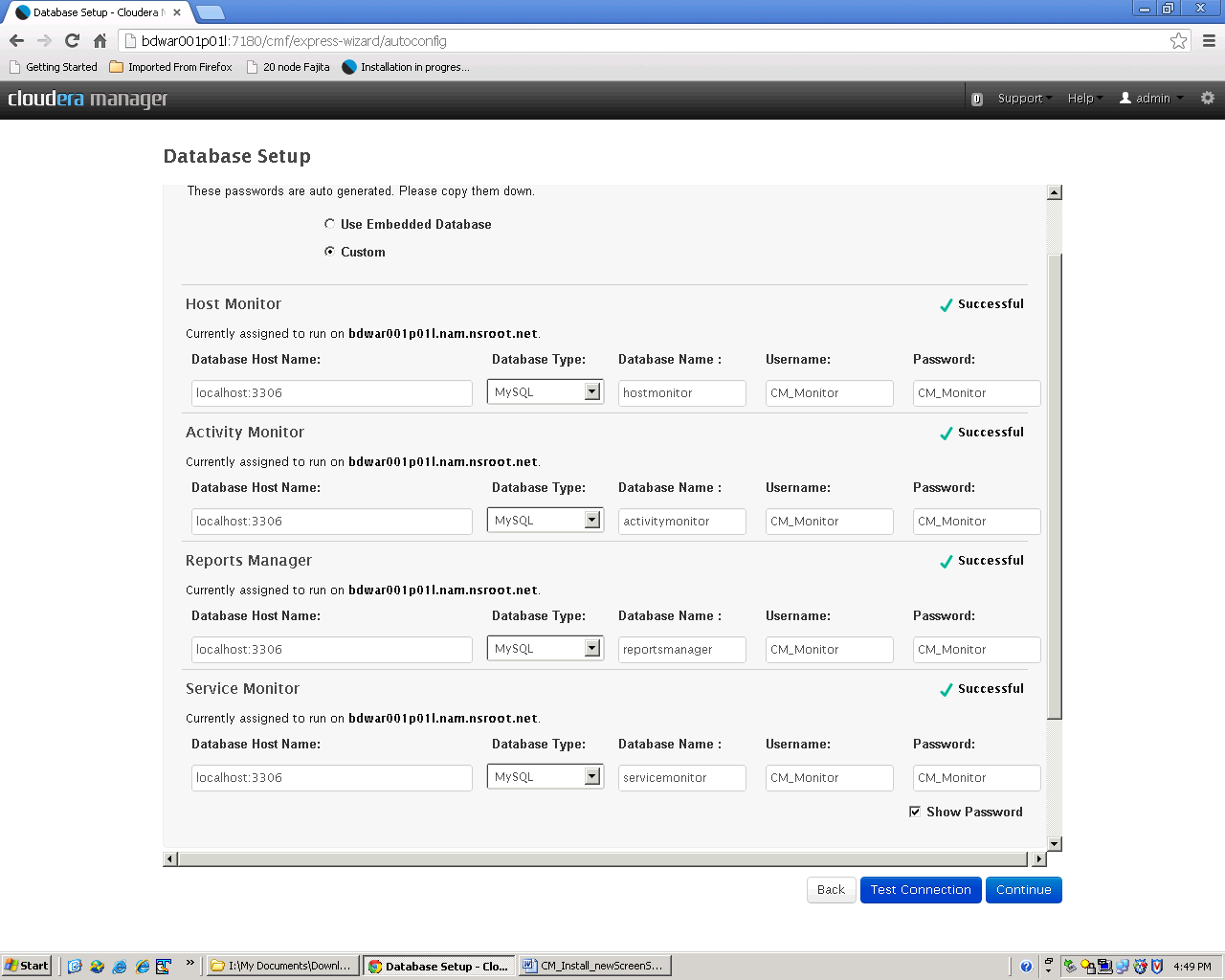
* HDFS Datanode
* HBase RegionServer
* Impala Daemon
* C4 – Map Reduce TaskTracker
* C5 – Yarn Node Manager
* C5 – Spark Worker
* C5 – Accumulo Tablet Server 🡨 do not deploy
* C5 – Solr Server – (not required on all data nodes)

Monitoring Services

You’ll be presented with a default page for monitoring services database values. These values can be used if another RDBMS is not available. You should make note of the pswds listed.

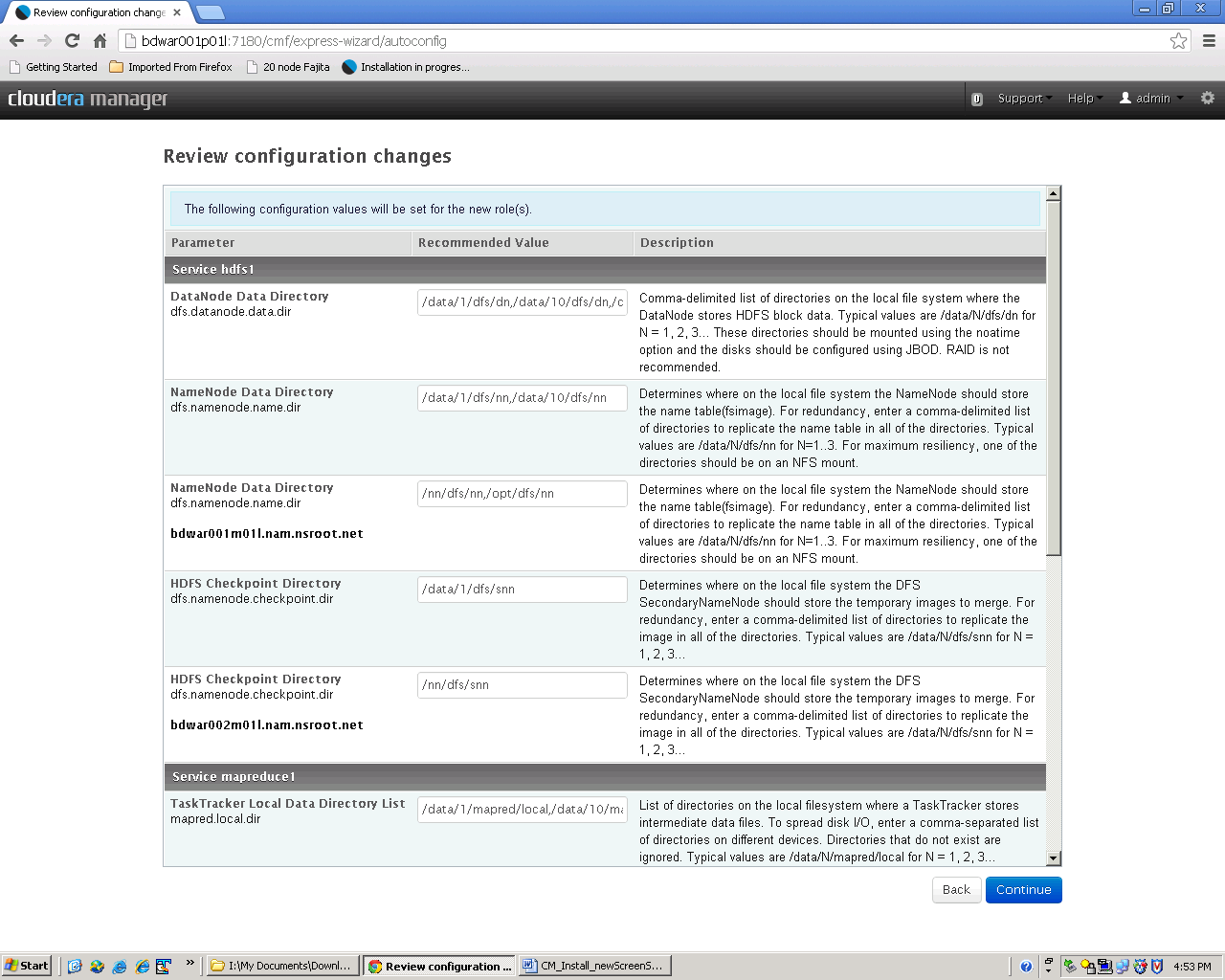
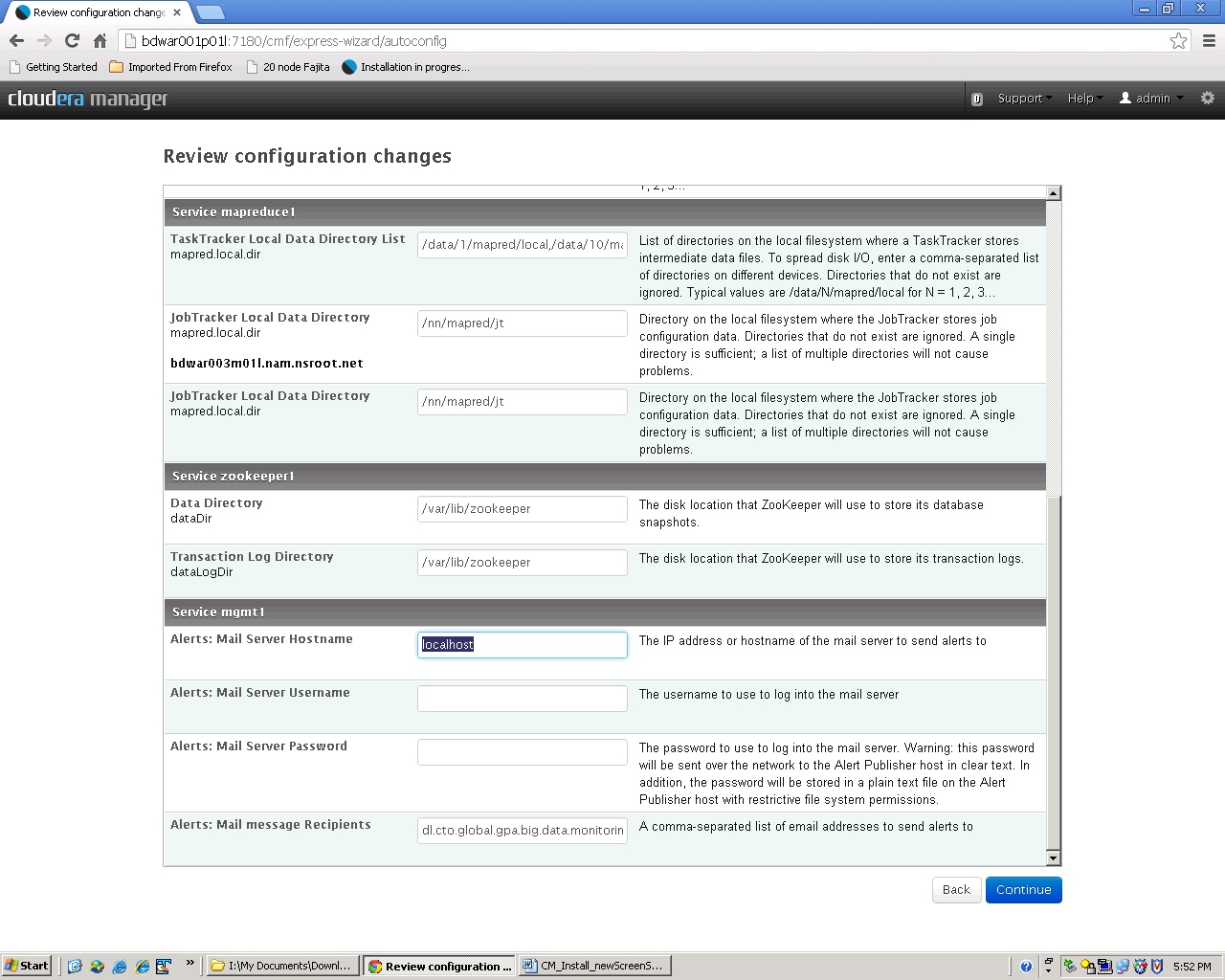
If MySQL or Oracle RDBMS is being used then choose ‘custom’ and add the connection details    
test the connection to make sure that the details are correct before continuing

Make sure that the port number on the connect string matches the “port=” value for the RDBMS – for embedded Postgres that’s 7432; for MySQL that’s 3306, verify in “/etc/my.cnf”

The database host name must match the string that was used in the grant statement: e.g. grant all on activitymonitor.\* TO 'CM\_Monitor'@’%’ IDENTIFIED BY 'CM\_Monitor';since @’%’ was used in this example you can specify any form of the server name or ‘localhost’   
If @’localhost’ or the server name was used here then ‘localhost’ or server name must be used in the connect string.  

### Service Configuration and Data Locations

Next you’ll be asked to verify the default configuration settings including where the data folders will be.   
MAKE SURE THESE ARE ACCURATE!!   
/opt is a default location make sure you replace this with the correct values

   
after verifying the entries then also fill in the email alert fields with localhost for the server name and [dl.cto.global.gpa.big.data.monitoring@imcnam.ssmb.com](mailto:dl.cto.global.gpa.big.data.monitoring@imcnam.ssmb.com) for the mail recipients 

If you need to make any correction then do that in a separate tab or window so that the wizard does not get confused.



HDFS service name node and secondary name node ‘service name’ entry must match and be non blank. Usually we set this to be the same as the cluster name e.g. friedtaco for the Fried Taco cluster.

If Navigator and Impala is being used then make sure that the impala logging directory is not left blank otherwise you’ll get an error starting the service that **/var/log/statestore/statestored.INFO** can’t be created. Set to /var/log/impalad/audit



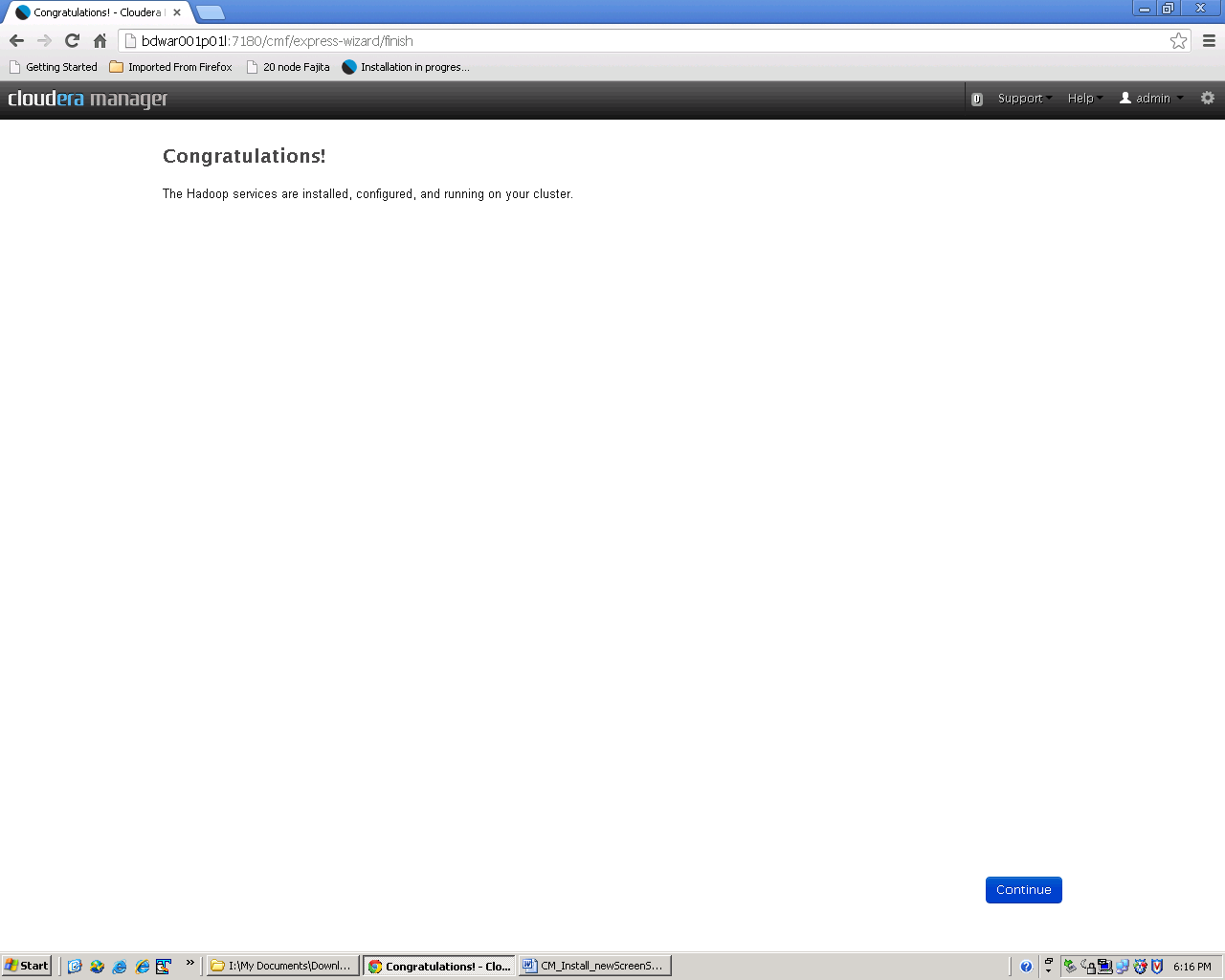
Set to /var/log/impalad/audit

|  |  |  |  |
| --- | --- | --- | --- |
| [**Impala Daemon (Default) / Logs**](https://bdgtmaster01i1l:7183/cmf/services/34/config) | **Impala Daemon Audit Log Directory**  audit\_event\_log\_dir | [Reset to empty default value](https://bdgtmaster01i1l:7183/cmf/services/34/config)  Audit log directory is set when Navigator collection is enabled. |  |

#### Starting the services for the new Cluster

Once all the corrections have been made then the install will continue and services will be started

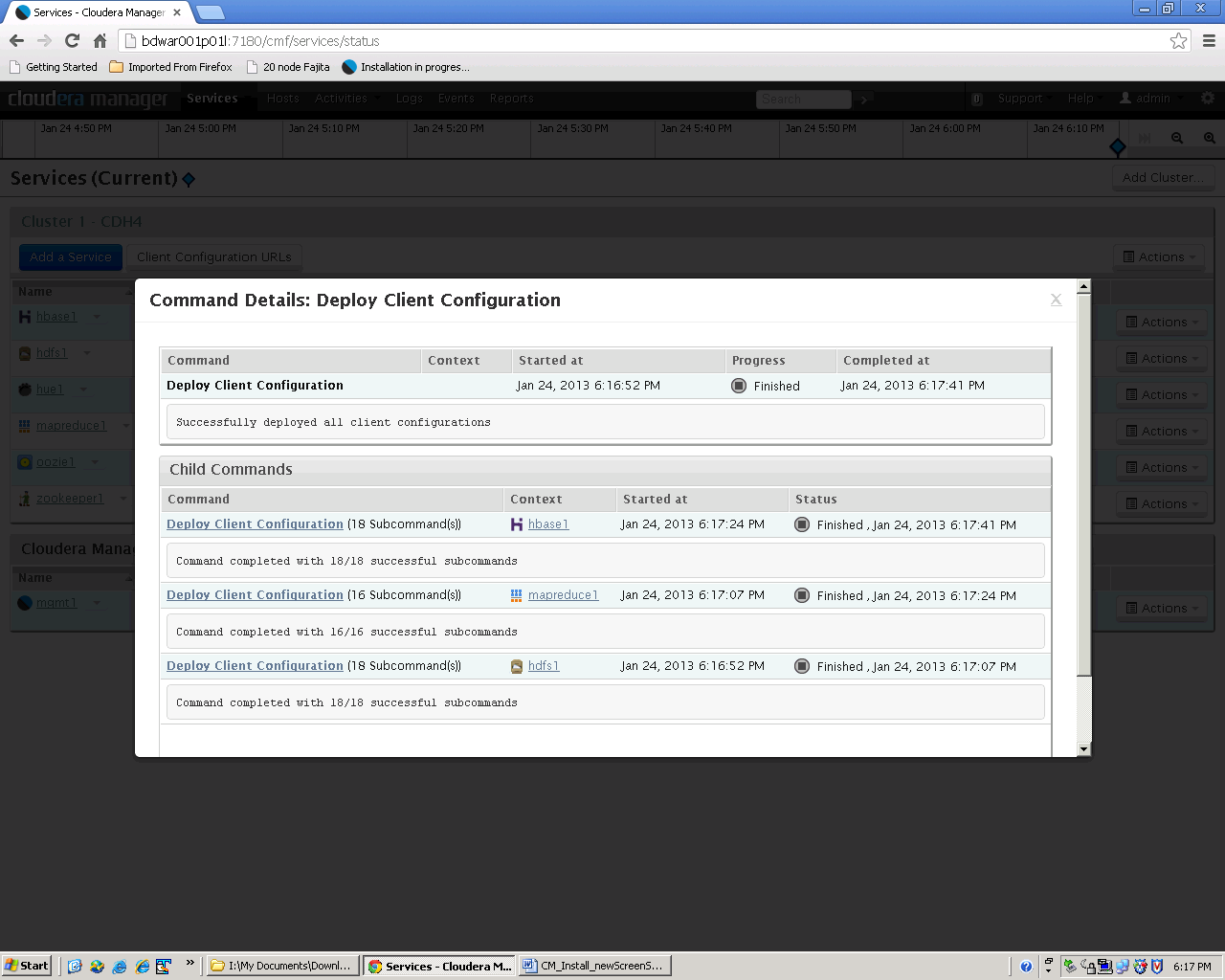
The cluster services should start successfully. If not, connect to Cloudera Manager through another session and correct the issues. Click continue once everything is successful.

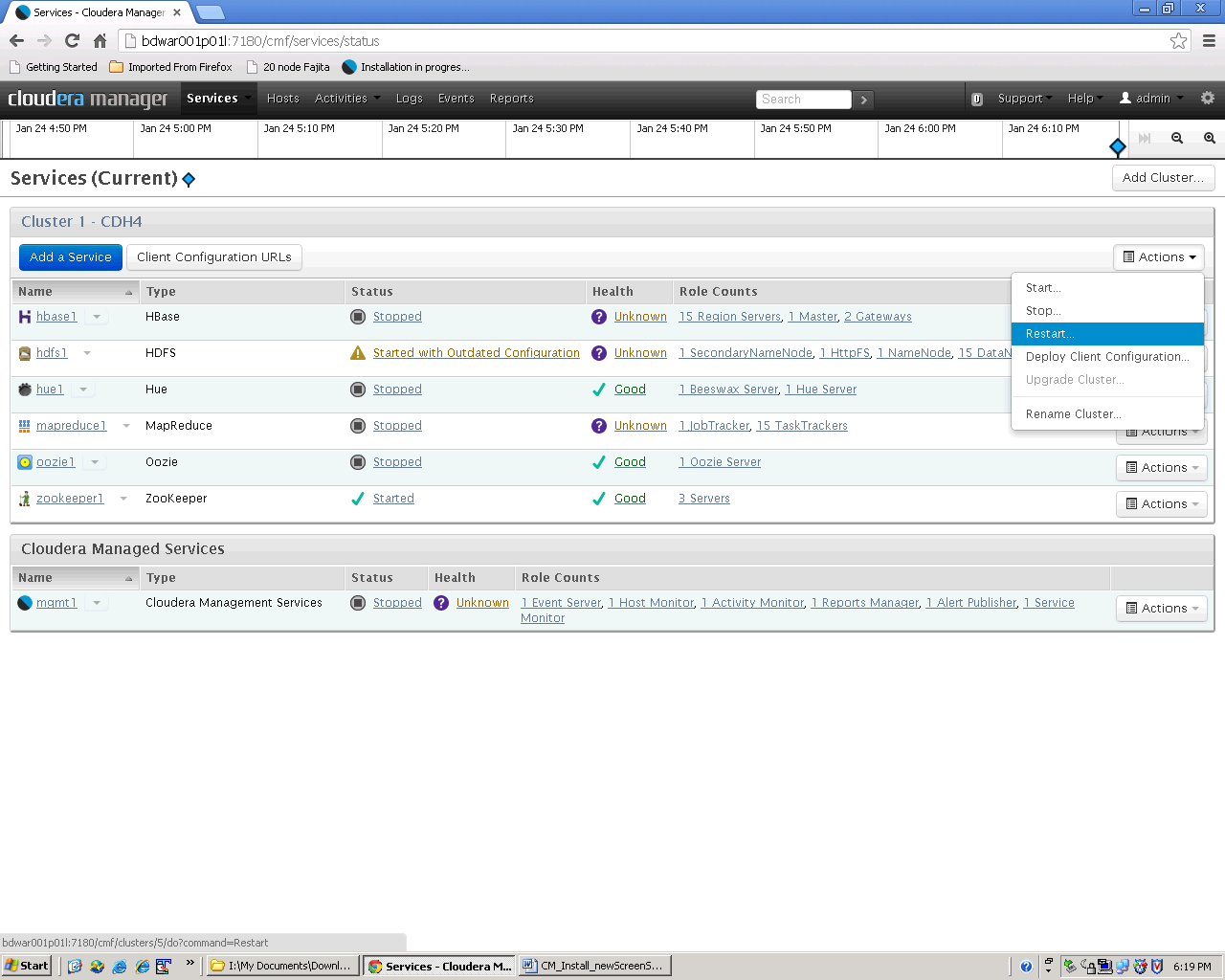


Click Continue to start using the cluster.

**‘Gateway’ is a special service role that must be assigned to nodes in the cluster and this is not done as part of the install wizard from Cloudera. See the configuration check list to determine what action to take for assigning gateway roles in the cluster.**

#### Corrections and alterations

Since we had to make alterations to configuration values during the install wizard- we ran a cluster level ‘deploy client configurations’ command 

And then restarted all cluster services 

## ~~Oozie~~

**~~When Not Using CM to manage the cluster.~~**

~~1. add an Oozie proxy to the core-site.xml for the Hive metastore server:~~

~~Go to, "HDFS Service->Configuration->Service-Wide->Advanced-> Cluster-wide Configuration Safety Valve for core-site.xml" and add:~~

~~<property>~~

~~<name>hadoop.proxyuser.oozie.hosts</name>~~

~~<value>\*</value>~~

~~</property>~~

~~<property>~~

~~<name>hadoop.proxyuser.oozie.groups</name>~~

~~<value>\*</value>~~

~~</property>~~

~~3. Restart the Hive metastore server.~~

~~4. Add the HCat credentials class to oozie-site.xml.~~

~~Edit the file and add:~~

~~<property>~~

~~<name>oozie.credentials.credentialclasses</name>~~

~~<value>hcat=org.apache.oozie.action.hadoop.HCatCredentials</value>~~

~~</property>~~

**~~When using CM~~**~~, go to "Oozie service->Configuration->Oozie Server(default)->Advanced-> Oozie Server Configuration Safety Valve for oozie-site.xml"~~

~~1. Add:~~

~~<property>~~

~~<name>oozie.credentials.credentialclasses</name>~~

~~<value>hcat=org.apache.oozie.action.hadoop.HCatCredentials</value>~~

~~</property>~~

~~2. Restart Oozie.~~

For WorkFlows Using OOZIE

Implementations For the workflow design: [to be completed by the dev teams or operations]

1. At the very top right after the workflow-app line, create HCat credentials:

<workflow-app xmlns="uri:oozie:workflow:0.4" name="hive-wf">

<credentials>

<credential name='hive\_credentials' type='hcat'>

<property>

<name>hcat.metastore.uri</name>

<value>thrift://<thrift\_server>:9083</value>

</property>

<property>

<name>hcat.metastore.principal</name>

<value>hive/\_HOST@<REALM></value>

</property>

</credential>

</credentials>

Note: Make sure to replace <thrift\_server> and <REALM> with the correct values (Make note of the credential name as that has to match in your hive actions).

2. In the hive action, add the credentials from above by setting "cred=". Example:

<action name="hive-node" cred='hive\_credentials'>

<hive xmlns="uri:oozie:hive-action:0.2">

<job-tracker>${jobTracker}</job-tracker>

<name-node>${nameNode}</name-node>

<job-xml>${hiveSite}</job-xml>

3. Run the workflow.

## Oozie MySQL database

Oozie must be configured to use the MySQL database that you created when installing MySQL. Go to the oozie service configuration page for ‘Oozie Server’ and ‘Database’ setting then enter the correct MySQL details as described in the MySQL document.

## Enable the OOZIE Web Console (web UI)

To enable Oozie's web console, you must download and add the ExtJS library to the Oozie server. If you have not already done this, proceed as follows.

yum install BD\_cloudera\_oozie22-2.2-1.x86\_64 -enablerepo=soe-bigdata-c5

Replaces the following manual command line process

#### ~~Step 1: Download the Library~~

~~Download the ExtJS version 2.2 library from~~[**~~http://archive.cloudera.com/gplextras/misc/ext-2.2.zip~~**](http://archive.cloudera.com/gplextras/misc/ext-2.2.zip)~~and place it a convenient location.~~

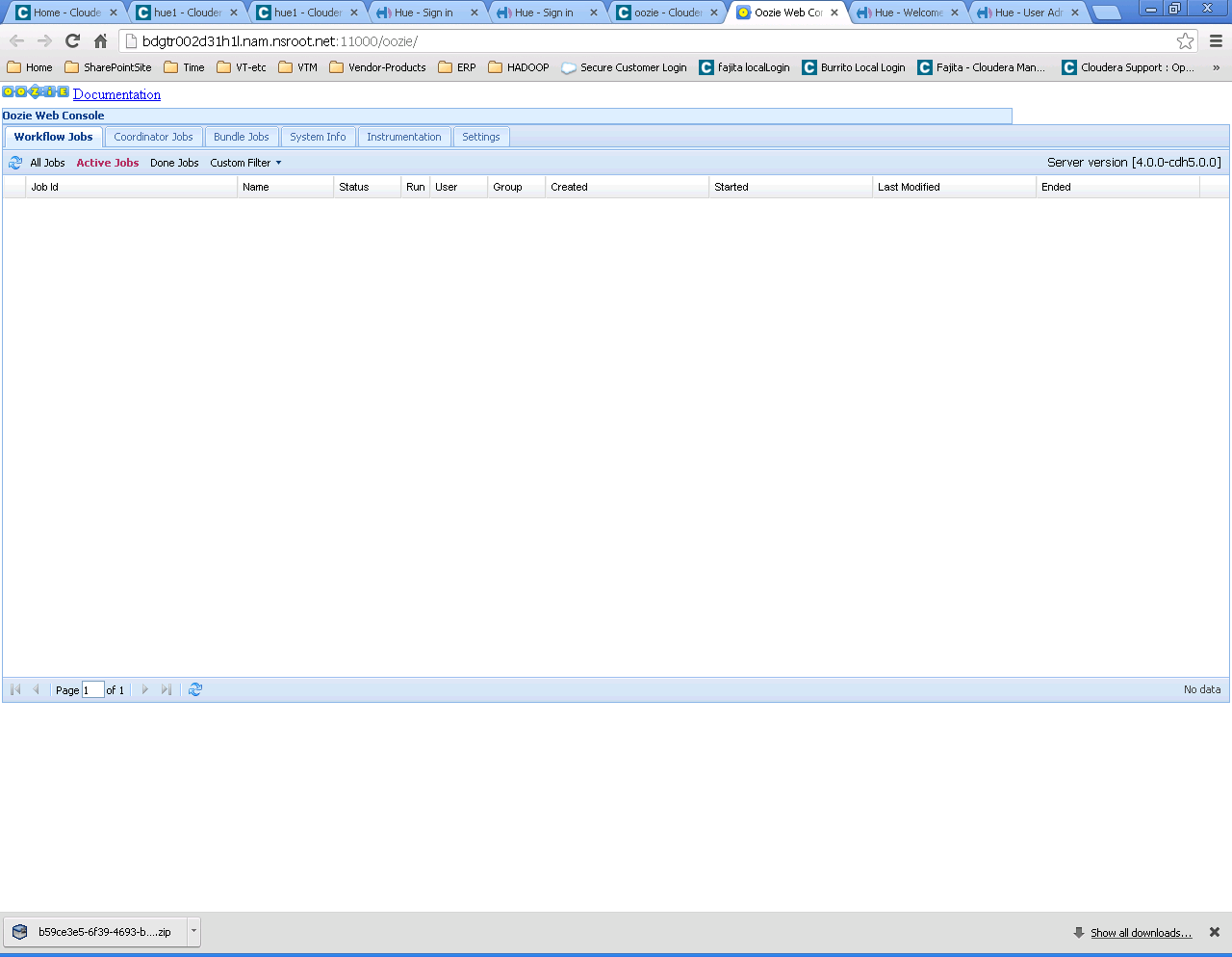
#### ~~Step 2: Install the Library~~

~~Extract the ext-2.2.zip file into /var/lib/oozie.~~

~~Copy ext-2.2.zip to /tmp/oozie/ on all 3 masters where oozie may be placed.~~

* ~~cd /var/lib;mkdir oozie;chown oozie:oozie oozie;cd oozie;~~
* ~~cd /var/lib/oozie;~~
* ~~sudo unzip /tmp/oozie/ext-2.2.zip;~~
* ~~chown –R oozie:oozie ext-2.2;~~

From CM Web UI go to oozie / Configuration / oozie server then select the check box to enable the oozie web console 

* restart the oozie service
* then select ‘oozie Web UI’ from this page to test the oozie console which looks like this 

## HUE WEB Server

For C4 production clusters to increase user throughput and stability , cloudera engineering recommended cherrypy web server for Hue. This should prevent the Hue Web UI from becoming unresponsive.

Under hue1->Configuration->Edit and VIew->Service-Wide->Advanced->Hue Service Configuration Safety Valve for hue\_safety\_valve.ini.

In the [Desktop] section add the following and restart Hue

use\_cherrypy\_server=true

[desktop]

use\_cherrypy\_server = true

cherrypy\_server\_threads=100

This could also be a bad OOZIE web server affecting HUE – so also restart oozie.

Certificates

Set ownership to hue:hue with permissions of 600

/etc/hue/server.crt and /etc/hue/conf/ca-cert.pem

# l /etc/hue/server.crt

-rw------- 1 hue hue 1648 Sep 4 14:58 /etc/hue/server.crt

[IDENbuild root @ bdgtr002d31h1l /var/log/hue]

# l /etc/hue/conf/ca-cert.pem

-rw-r--r-- 1 root root 1375 Sep 24 15:19 /etc/hue/conf/ca-cert.pem

[IDENbuild root @ bdgtr002d31h1l /etc/hue/conf]

# chown hue:hue /etc/hue/conf/ca-cert.pem

[IDENbuild root @ bdgtr002d31h1l /etc/hue/conf]

# chmod 600 /etc/hue/conf/ca-cert.pem

[IDENbuild root @ bdgtr002d31h1l /etc/hue/conf]

# l /etc/hue/conf/ca-cert.pem

-rw------- 1 hue hue 1375 Sep 24 15:19 /etc/hue/conf/ca-cert.pem

## Set Heap Sizes for HIVE

Per case in CDH 4 heap sizes for HIVE should be set as follows:

Documentation [1][2] indicate the servers should be running:

For clusters of 100 nodes or larger, 24 GB of heap is required.   
For clusters of 50 nodes to 99 nodes, 12 GB of heap is required.   
For clusters of 11 nodes to 49 nodes, 6 GB of heap is required.   
For clusters of 2 nodes to 10 nodes, 2GB of heap is required.  
For a single-node node cluster, 256 MB of heap is required.

[1] <http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_hive_metastore_configure.html>   
[2] <http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_hiveserver2_configure.html>

In a case where you have 70 nodes, you need at least 12GB of heap for both HS2 and Hive Metastore.

Increase the heap size for both HS2 and Hive Metastore to 12G at least. Steps are listed below:

1) Navigate to Hive > Configuration > Hive Metastore Server Default Group > Resource Management > Java Heap Size of Hive Metastore Server in Bytes

2) Change the value to 12G

3) Navigate to Hive > Configuration > HiveServer2 Default Group > Resource Management > Java Heap Size of HiveServer2 in Bytes

4) Change the value to 12G

5) Restart Hive

## Using CGroups

So far the cluster recommendations introduce cgroups as a tool to help when HBase is collocated alongside other frameworks, such as MapReduce. However, cgroups can be used to better share resources amongst all the services in the cluster. When using Cloudera Manager 4.5 and later, individual values for cpu.shares and blkio.weight must be set individually for each service. However, with C5 there is a resource management wizard that allows for quick and easy changing of resource allocations in one place, as a percentage of the whole.

A useful example discussing how to use cgroups for a cluster using Impala and MapReduce is at: <http://www.cloudera.com/content/cloudera-content/cloudera-docs/CM4Ent/4.5.4/Cloudera-Manager-Enterprise-Edition-Installation-Guide/cmeeig_impala_res_mgmt.html>

Additionally, C5 documentation for static resource pools is found at: <http://www.cloudera.com/content/cloudera-content/cloudera-docs/CM5/latest/Cloudera-Manager-Managing-Clusters/cm5mc_service_pools.html>

Finally, C5 documentation for dynamic resource pools in the context of Yarn is found at: <http://www.cloudera.com/content/cloudera-content/cloudera-docs/CM5/latest/Cloudera-Manager-Managing-Clusters/cm5mc_resource_pools.html>

## Total Resources

The worker nodes in the cluster have a maximum memory footprint (for Hadoop) of:

* 1 GB – DataNode
* 1 GB – TaskTracker
* 20 GB – MapReduce tasks
* 30 GB – Impala daemon
* 4 GB – RegionServer

Which is a total of 56 GB maximum. This allows for 8 GB for use by the operating system and additional process overhead.

## IMPALA

The default settings in place for the Impala daemon do not constrain the memory that Impala can use. Because the cluster collocates several frameworks, it is necessary to limit the Impala daemon memory to ensure Impala does not starve other frameworks of memory resources.

We accomplish this by setting the memory limit for the Impala daemon to 30 GB, based on the available memory on the worker machines.

## HBASE

HBase services are not normally installed and configured unless specifically requested.

When HBase is installed make sure to add all HBase services on the correct hosts. See role assignments in this doc.

Set the RegionServer heap size to 4 GB at a minimum, with a maximum of 12 GB if needed. If more memory is needed for RegionServers, it may be necessary to reduce the memory limit of the Impala daemons at the same time.

Additionally , RegionServers are prone to bad health reports related to HDFS read latency. HBase is sensitive to latency, and if there is I/O contention due to heavy MapReduce or Impala workloads, HBase can suffer. In order to help mitigate this issue, RegionServers should be given priority over other worker daemon processes to ensure latency does not suffer. This can be done using Linux cgroups.

By default, all processes receive CPU shares of 1024. It is recommended to set cpu.shares to 1536 for RegionServers.

## HIVE

Hive resources for the Hive Metastore Server should be increased from the default (in CM 4.x) of 256 MB to 1 GB (the default in C5). It was found by engineering that 256 MB is not sufficient for most customers with typical workloads, as evidenced by support cases with out-of-memory (OOM) errors showing up in log files.

However, Citi has increased the heap size further to 4 GB 8GB and in some clusters to 12GB and still are encountering OOM errors.

## Configuring HUE to use HS2 instead of Beeswax

Benefits to using HS2 over Beeswax:

HS2 replaces Beeswax in CDH 5 so this step will not be necessary after CDH5.

HS2 is more stable than Beeswax.

Beeswax does not support Sentry (HS2 does).

1. Start Hive Server 2
2. From CM: Go to the Hive Service->Gateway->Advanced->Hive Client Configuration Safety Valve for hive-site.xml and add:

<property>

<name>hive.server2.authentication</name>

<value>KERBEROS</value>

</property>

1. Restart Hive Server 2
2. Configure Hue for HS2.

Using CM, go to the **Hue service->Hue Server->Advanced** and add:

[beeswax]

server\_interface=hiveserver2

beeswax\_server\_port=10000(or HS2 port if diff)

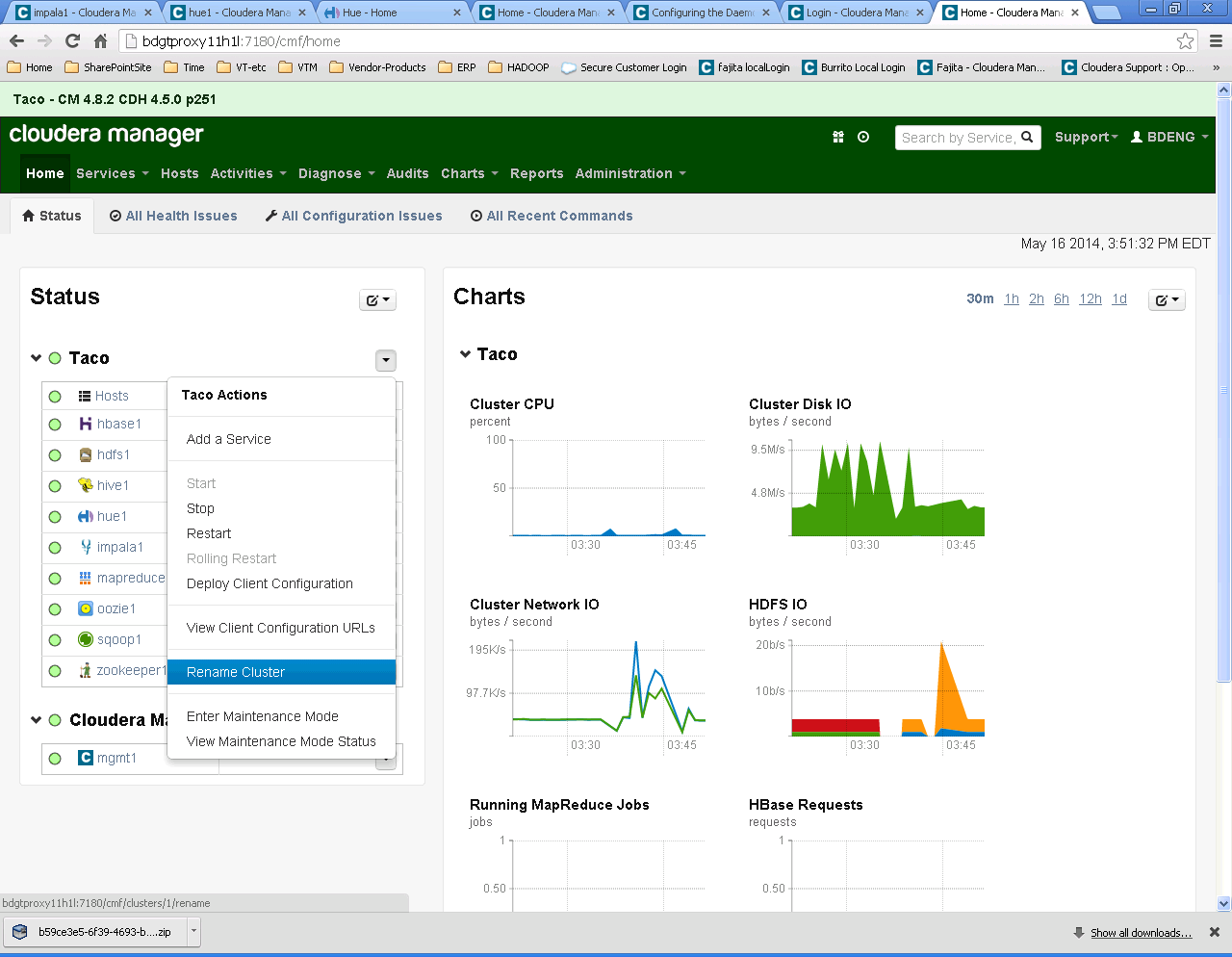
beeswax\_server\_host=<hostname>

1. Using CM:  Restart Hue service. (Beeswax will come up, however you should shut it down to not waste resources. )
2. Test the settings. Hue will now point to HiveServer2.

## IDENTIFY The Cluster

### Set the NAME for the new cluster

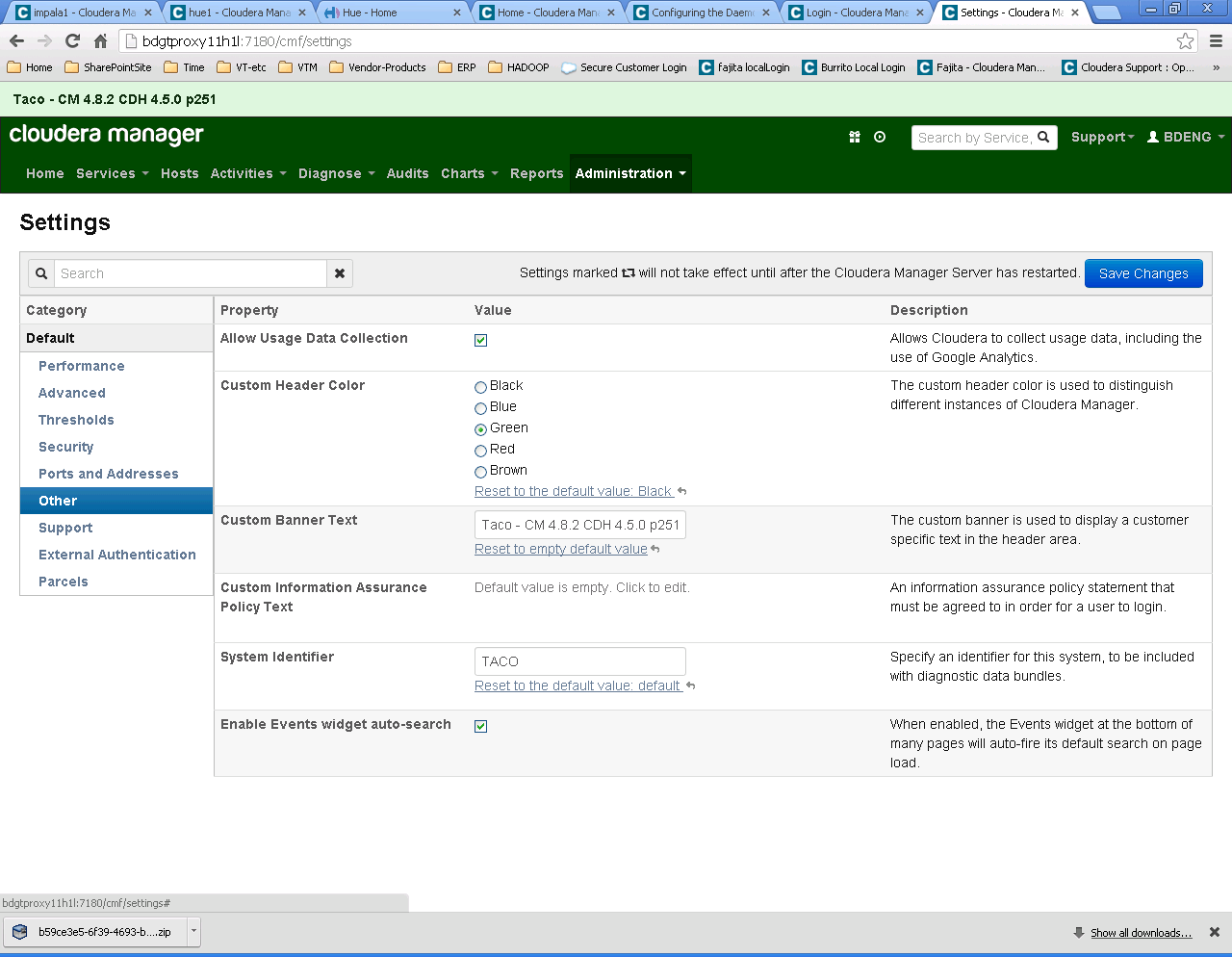
From the main status page select action “rename cluster” and add the name.



Use the same name as the HDFS NN namespace name

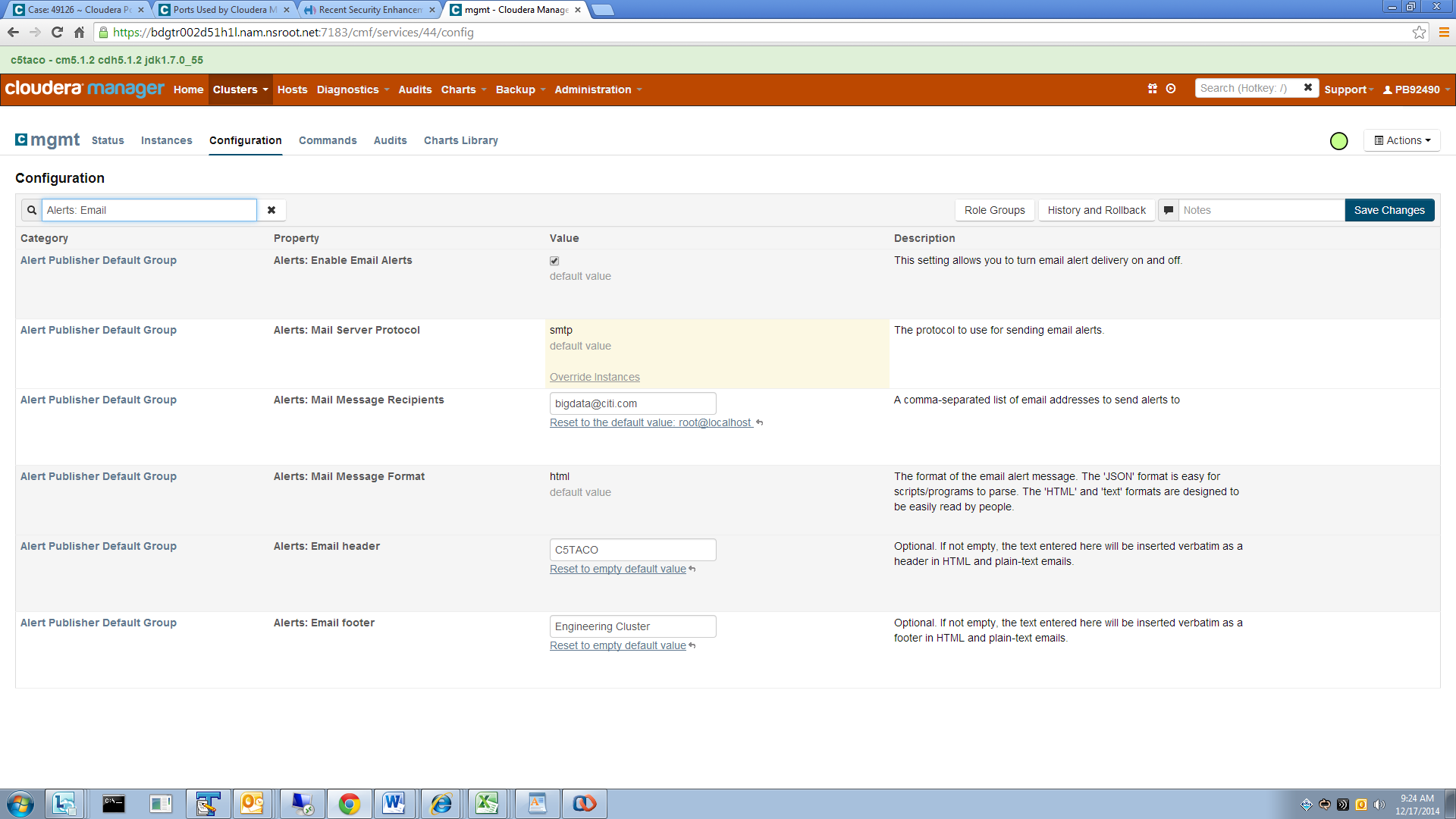
### Set the Banner Text for the Name and Version

Set the display banner to show both the name of the cluster and the versions of the software.

From the main status page select “Administration / Settings” then from the side bar select “Other” and update the fields. In this example I set the Taco cluster banner to reflect the anme and versions as “Taco - CM 4.8.2 CDH 4.5.0 p251” I also set the system Identifier as “Taco”

### Set the Alerts Email Header / Footer and recipient list

When significant events happen in the cluster emails alerts will be sent to the D list that you specify. In the Management service choose configuration and “Alert Publisher” Use the check box to enable email alerts and then fill in the D list of the intended recipients – usually the operations support group. Also add an identifying text to the header and footer to make it easier to identify where the emails are being sent from – usually the cluster name in the header and a short description in the footer.



## Adding Kerberos Authentication

Configure Kerberos / LDAP on the host level. This is necessary for a consistent uid for all the functional ids. Follow instruction from [Kerberos at Citi doc](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Cloudera/TechDocs/KERBEROS_for_Cloudera_Manager_and_CDH.pdf) and also refer to Kerberos engineering wiki page: [http://ewiki.nam.nsroot.net/wiki/KRB5\_LDAP#North\_America](http://ewiki.nam.nsroot.net/wiki/KRB5_LDAP)

See the Kerberos at Citi doc at: <https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Cloudera/TechDocs/KERBEROS_for_Cloudera_Manager_and_CDH.pdf>

### Known Issue with Kerberos in nCloudera Manager

There is a known issue with Cloudera manager and the managemen t of kerberos. The check box for CM to manage Kerberos should not be checked. If it gets checked it will remain in effect even after unchecking it. This causes the cm agent to overlay the machines krb5.conf file every time the agent starts. The effect is kerberos on the machine is broken and communications including local access (ssh) will fail. SA action is required to fix this event.

To prevent this from happening use the following to clean out the bad database settings that control the CM agent.

1) shutdown CM

2) backed up MySQL db

3)logged in as root and run the 2 delete statements –

* mysql –u root –p
* use scm;
* delete from CLIENT\_CONFIGS\_TO\_HOSTS where CLIENT\_CONFIG\_ID IN (select CLIENT\_CONFIG\_ID from CLIENT\_CONFIGS where CLUSTER\_ID IS NOT NULL AND SERVICE\_ID IS NULL);
* delete from CLIENT\_CONFIGS where CLUSTER\_ID IS NOT NULL AND SERVICE\_ID IS NULL;

4) started CM server

## Uninstall Process

When re using a node that was part of another cluster you need to make sure that all links to that other cluster are removed. This means removing configuration files and any data using the following process.  
It is assumed that the nodes were properly removed from the previous cluster using ‘Decommission” and “Delete” operations and that the CM Agent is stopped so that the node does not attempt to rejoin the old cluster.

1. Stop ALL services:
   1. sudo /sbin/service cloudera-scm-server stop
   2. sudo /sbin/service cloudera-scm-server-db stop
   3. sudo /sbin/service cloudera-scm-agent hard\_stop
2. Uninstall the CDH and Cloudera Manager packages:
   1. sudo rpm -e --allmatches $(rpm -qa | grep -ehadoop -ecloudera -ehue -eoozie -ehbase -ehcatalog -eflume -ehive -esqoop -esqoop2 -epig -emahout –ewebhcat –ebigtop –ewhirr -ezookeeper)

OR just the hadoop components (leaving Cloudera Manager intact)

* 1. rpm -e --allmatches $(rpm -qa | grep -ehadoop -ehue -eoozie -ehbase -ehcatalog -eflume -ehive -esqoop -esqoop2 -epig -emahout -ewebhcat -ebigtop -ewhirr -ezookeeper)

1. Clean the YUM CACHE
   1. sudo yum clean all
2. On all Agent hosts, remove all Cloudera Manager data.- Run this command as root
   1. sudo rm -Rf /usr/share/{cmf,hue} /var/lib/cloudera\* /var/cache/yum/cloudera\*
3. On all Agent hosts, kill any running Cloudera Manager and Hadoop processes.

Note: This step should not be necessary if you stopped all the services and the Cloudera Manager agent correctly.

* 1. for u in hdfs mapred cloudera-scm hbase hue zookeeper oozie hive; do sudo kill $(ps -u $u -o pid=); done

1. Remove the Cloudera Manager lock file.

On all Agent hosts, run this command to remove the Cloudera Manager lock file:

* 1. sudo rm /tmp/.scm\_prepare\_node.lock

1. Remove data files and directories:

rm -rf /etc/cloudera-scm-agent;

rm -rf /dfs;

#(Assumes /dfs is where HDFS data is stored.)

#For our main cluster that use /data as the location use these commands on each data node:

rm -rf /data/1/dfs/dn/\*;

rm -rf /data/2/dfs/dn/\*;

rm -rf /data/3/dfs/dn/\*;

rm -rf /data/4/dfs/dn/\*;

rm -rf /data/5/dfs/dn/\*;

rm -rf /data/6/dfs/dn/\*;

rm -rf /data/7/dfs/dn/\*;

rm -rf /data/8/dfs/dn/\*;

rm -rf /data/9/dfs/dn/\*;

rm -rf /data/10/dfs/dn/\*;

if this step gets ommitted and done after re install then you'll also need to re create the HDFS /tmp folder and Hbase root folder

HDFS

In CM go to HDFS service and refresh the node list;

then action- create /tmp directory

then from the physical server command line > hadoop namenode format

HBASE

In CM go to HBASE service and 'action - create root directory'

push the client config to all nodes then restart the service

Uninstalling individual packages

| **Component to remove** | **Command** |
| --- | --- |
| Mahout | $ sudo yum remove mahout |
| Whirr | $ sudo yum remove whirr |
| Hue | $ sudo yum remove hue |
| Pig | $ sudo yum remove pig |
| Sqoop | $ sudo yum remove sqoop |
| Flume | $ sudo yum remove flume |
| Oozie client | $ sudo yum remove oozie-client |
| Oozie server | $ sudo yum remove oozie |
| Hive | $ sudo yum remove hive hive-metastore hive-server hive-server2 |
| HBase | $ sudo yum remove hadoop-hbase |
| ZooKeeper server | $ sudo yum remove hadoop-zookeeper-server |
| ZooKeeper client | $ sudo yum remove hadoop-zookeeper |
| ZooKeeper Failover Controller (ZKFC) | $ sudo yum remove hadoop-hdfs-zkfc |
| HDFS HA Journal Node | $ sudo yum remove hadoop-hdfs-hadoop-hdfs-journalnode |
| Hadoop repository packages | $ sudo yum remove cloudera-cdh3 |
| HttpFS | $ sudo yum remove hadoop-httpfs |
| Hadoop core packages | $ sudo yum remove hadoop-0.20 |

## Citi SSH keys

If keys are required, follow the instructions outlined in the document at  
<https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/Setting_up_passwordless_authentication.docx> 

## Notes on HA

The basic premise of HA for services is to have multiple servers running the same service. However, most services can be configured on multiple servers but can not be running as duplicates as this will cause contention issues.

Some duplicates can be configured and running:

HDFS

MR

GATEWAY

HIVE

For the services that use a metastore (in MySQL) the HA option is achieved by moving (backup & restore) the metastore to the new server and then (re)starting the service.

All master and both proxy servers must be populated with the keytab files so that servers can easily be moved to another machine.

For full details on HA see the document in share point at: <https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/High%20Availability%20and%20Fail%20Over%20For%20Cloudera%20Manager%20and%20CDH.docx>

## Other Documents to Reference

### [Hadoop Build Catalog Template](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Templates/Hadoop-Build-Catalog-Template.xlsx)

### [Standard Cluster Installation and Use of Connectors](https://collaborate.citi.net/docs/DOC-166296)

### [CATE Hadoop Reference Architecture](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Presentations/CATE-Hadoop-Reference-Architecture.pptx)

### [MySQL Backup & Restore](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Cloudera/TechDocs/MySQL_Backup_and_Recovery.pdf)

### [MySQL MetaStores](https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Cloudera/TechDocs/MySQL_DB_For%20Cloudera_Manager_and_Hive.pdf)

## Citi Java Package

If Mysql or Mysql Connectors are to be installed – then do that first.

This process consists of the following steps. More details on some of the steps will follow this overview.

When updating java to the latest supported and patched version of java available in citi packages you must make the same java changes on all nodes in the cluster.

The SA or other root user must make these changes.

Citi Java group maintains packages at: <https://catecollaboration.citigroup.net/domains/deveng/javaappservers/javaj2ee/Lists/Java%20Current%20Supported%20Versions/Supported%20Versions.aspx>

This is normally a network mount in all Linux hosts. You can access the latest rpm from /net/stealth/export1/home1.localhost/sw/Linux/

If you need further Java support, kindly raise an INC in ServiceNow to "CTO GL EX JAVA". cd

This process refers to jdk1.7.0\_51 which was the current latest patch version at writing.   
Use the correct name for the patch package that you’re installing  
cd /net/stealth/export1/home1.localhost/sw/Linux/;l jdk-1.7.0\*l64-linux.x86\_64.rpm;

<--begin green zone activities here -->

1) Remove old jdk versions on all nodes - optional but recommended

To fix older jdk conflicts   
 yum remove jdk;

This also removes several dependencies including mysql-connector-java. A yum install command for mysql-connector-java from soe-bigdata-c5 will re install these after they along with jdk are un installed.

yum install mysql-connector-java --enablerepo=soe-bigdatra-c5;

Now you can install the correct jdk followingthe the jdk install instructions in this section

2) Install new jdk on all nodes

**just yum the latest package**

**yum install jdk-1.7.0\_51l64-linux.x86\_64.rpm**

**Which will create an install at “/opt/jdk/1.7.0\_51164” or “opt/jdk/<version>” where <version> is the same as in the rpm name**

Create a link at /usr/java that points to the location of the latest jdk package

**cd /usr/;mkdir java;**

**cd /usr/java;ln -s /opt/jdk/1.7.0\_51l64 jdk1.7.0\_51**

**Create or Re-Create links:**

**The location of the java jdk install is in red – make sure this is accurate.**

alias l='ls -altrF';

cd /usr/java; rm -f default; ln -s /usr/java/latest default;

cd /usr/java; rm -f latest; ln -s /usr/java/jdk1.7.0\_51 latest;

cd /usr/bin/;l java;rm -f java;ln -s /usr/java/latest/bin/java;l java;

cd /etc/alternatives;l java;rm -f java;ln -s /usr/java/latest/bin/java;l java;

3) remove any 32 bit libraries that exist as they can cause service failures in Impala

rm -f /usr/java/latest/mst/tmp/MSTGenericClient/java/jre/lib/i386/server/libjvm.so;

rm -f /usr/java/latest/mst/tmp/MSTGenericClient/java/jre/lib/i386/client/libjvm.so;

4) Update $JAVA\_HOME to point to the new jdk  
 export JAVA\_HOME=/usr/java/latest;

export PATH=$JAVA\_HOME:$PATH;

alternatives --display java; 🡨 display current configuration

alternatives --config java; 🡨 set /usr/java/latest as active

alternatives --install /usr/bin/java java /usr/java/latest/bin/java 1600;

alternatives --config java 🡨 set /usr/java/latest as active – verify after adding new entry

alternatives --display java 🡨 display current configuration

<--begin downtime here -->

5) Stop all roles/services in CDH via CM Web UI

6) Stop CM management services via CM Web UI

7) Restart all nodes on cluster; Once completed, this will start the CM web UI   
 service cloudera-scm-server restart;

service cloudera-scm-agent restart;

8) SSH to the CM Server node, confirm the updated version of java by running the following:

$java -version

java version "1.7.0\_51"

**This MUST BE the version that you installed**

$ps aux | grep java | awk '{print $11}'

/usr/java/jdk1.7.0\_51/bin/java

9) Login to CM Web UI

10) Start CDH services

11) Start CM Mgmt1 services

<-- end downtime -->

<-- end green zone activities -->

======================================================================================================================================================

**>>>> update Java Version <<<<**

ONCE This process has been completed on a machine then future java upgrades consist of only the following commands – again – make sure that the java version in red is correct and matches in all 3 commands

cd /net/stealth/export1/home1.localhost/sw/Linux/;

yum -y install jdk-1.7.0\_56l64-linux.x86\_64.rpm;

cd /usr/java;ln -s /opt/jdk/1.7.0\_56l64 jdk1.7.0\_56;ls -altrF;

cd /usr/java; rm -f latest; ln -s /usr/java/jdk1.7.0\_56 latest;

>> restart all java processes so that the in memory java version is replaced by the new 'latest' version

======================================================================================================================================================

### Modifying CMF\_AGENT\_JAVA\_HOME

In many cases, modifying the CMF\_AGENT\_JAVA\_HOME environment variable is an effective solution for updating the configuration to accommodate a custom JAVA\_HOME. Modifying the CMF\_AGENT\_JAVA\_HOME environment variable enables all services on the host to find the JDK.   
  
To modify the CMF\_AGENT\_JAVA\_HOME environment variable

* Open /etc/default/cloudera-scm-agent.
* Set the CMF\_AGENT\_JAVA\_HOME environment variable to the java home in your environment. For example, you might modify the file to include the following line:
* export CMF\_AGENT\_JAVA\_HOME=/usr/java/latest/

# v /etc/default/cloudera-scm-agent

#

# Specify any command line arguments for the Cloudera SCM Agent here.

#

CMF\_AGENT\_ARGS=""

export CMF\_AGENT\_JAVA\_HOME=/usr/java/latest/

* Save and close the cloudera-scm-agent file.
* Restart the Cloudera Manager Agent using the following command:
* sudo service cloudera-scm-agent restart

# service cloudera-scm-agent restart

Stopping cloudera-scm-agent: [ OK ]

Starting cloudera-scm-agent: [ OK ]

### Modifying Service Settings

You can modify service settings to use your custom JAVA\_HOME. This is done as an alternative to modifying the CMF\_AGENT\_JAVA\_HOME environment variable. Modifying service settings to use a custom JAVA\_HOME applies to all nodes in the cluster, but you must repeat this process of updating JAVA\_HOME for all services. To modify service settings to use your custom JAVA\_HOME

* Open the Cloudera Manager Admin Console, click any service that fails to start because the JDK location is misconfigured, and click Configuration.
* Under Service-Wide, click Advanced.
* Click the Value cell for the Service Environment Safety Valve and add your custom java home to the property here. For example, you might enter the value JAVA\_HOME=/usr/java/latest/
* Click Save Changes.
* If your deployment includes Cloudera Management services, add your custom JAVA\_HOME value to /usr/share/cmf/bin/cmf-server.
* In the Cloudera Manager Admin Console, for the service you are configuring, click Actions and click Restart.
* Repeat this process for all services that need the updated JAVA\_HOME value.

To see how Cloudera Manager chooses a default JDK, review the contents of /usr/lib64/cmf/service/common/cloudera-config.sh.

## SAML / SSO for CMS

# LOAD ZIP and jar FILES INTO SAML FOLDER - /home/gpainstall/saml

#for C4 repo is bigdata-c5 not c4

yum install BD\_cloudera\_saml\_cdh450 --enablerepo=soe-bigdata-c5

~~#for C5~~

~~yum install BD\_cloudera\_saml\_cdh510 --enablerepo=soe-bigdata-c5~~

The jar file for CM goes in /usr/share/cmf/lib/ and it's size is 215312 - find it in /home/gpainstall/saml

cd /usr/share/cmf/lib;

cp spring-security-saml2-core-1.0.0.RC2.jar spring-security-saml2-core-1.0.0.RC2.jar.original;

cp /home/gpainstall/saml/spring-security-saml2-core-1.0.0.RC2.jar .;

alias l=’ls –altrF’;

cd /usr/share/cmf/lib;

l spring-security-saml\*

-rw-r--r-- 1 root root 215745 Sep 23 2013 spring-security-saml2-core-1.0.0.RC2.jar.original

-rw-r--r-- 1 root root 215312 Aug 1 15:39 spring-security-saml2-core-1.0.0.RC2.jar

When configuring external authentication as SAML there are options in the way to choose the order of authentication. Choose ‘external only’ for CMS as this will still allow ‘local’ admin users to access the local login feature in emergencies

## SAML / SSO for HUE

This process primarily applies to Master 2 but should be done on all master servers to enable fail over of HUE services.

alias l= ‘ls -altrF’;

yum install libtool-ltdl python-setuptools m2crypto python\* --enablerepo='soe6u5, soe6products';

yum install xmlsec1 swig xmlsec1-openssl python-requests python-memcached python-pip --enablerepo='soe6u5, soe6products, soe-bigdata-c5';

🡪 START Debug STEPS for XMLSEC

#Package xmlsec has a bug that requires manual fix at this time but may be fixed in future versions

#Verify xmlsec installation as follows:

# cd /usr/lib64

[IDENbuild root @ bdgtr002d31h1l /usr/lib64]

# l libxml\*

-rwxr-xr-x 1 root root 415208 Jul 19 2010 libxmlsec1.so.1.2.16\*

-rwxr-xr-x 1 root root 225944 Jul 19 2010 libxmlsec1-openssl.so.1.2.16\*

-rwxr-xr-x 1 root root 1383368 Nov 29 2012 libxml2.so.2.7.6\*

lrwxrwxrwx 1 root root 16 Mar 7 2014 libxml2.so.2 -> libxml2.so.2.7.6\*

lrwxrwxrwx 1 root root 20 Jun 10 17:17 libxmlsec1.so.1 -> libxmlsec1.so.1.2.16\*

lrwxrwxrwx 1 root root 28 Jun 10 17:17 libxmlsec1-openssl.so.1 -> libxmlsec1-openssl.so.1.2.16\*

#NOTE that there is no link pointing to

# Create that link and the results will look like this

ln -s libxmlsec1-openssl.so.1 libxmlsec1-openssl.so;

[IDENbuild root @ bdgtmaster12h1l /usr/lib64]

# l libxml\*

-rwxr-xr-x 1 root root 415208 Jul 19 2010 libxmlsec1.so.1.2.16\*

-rwxr-xr-x 1 root root 225944 Jul 19 2010 libxmlsec1-openssl.so.1.2.16\*

-rwxr-xr-x 1 root root 1383368 Nov 29 2012 libxml2.so.2.7.6\*

lrwxrwxrwx 1 root root 16 Mar 7 2014 libxml2.so.2 -> libxml2.so.2.7.6\*

lrwxrwxrwx 1 root root 20 Jun 5 15:37 libxmlsec1.so.1 -> libxmlsec1.so.1.2.16\*

lrwxrwxrwx 1 root root 28 Jun 5 16:26 libxmlsec1-openssl.so.1 -> libxmlsec1-openssl.so.1.2.16\*

lrwxrwxrwx 1 root root 34 Jun 5 16:27 libxmlsec1-openssl.so -> /usr/lib64/libxmlsec1-openssl.so.1\*

#verify the xmlsec command "xmlsec1 --encrypt filename" should return results like this

/usr/bin/xmlsec1 --encrypt 304457l.xml

Error: failed to find default node with name="EncryptedData"

Error: failed to encrypt file with template "304457l.xml"

🡪 END DEBUG STEPS

# FOR C4 cd /opt/cloudera/parcels/CDH/share/hue/build/env/lib64/python2.6/site-packages;

# FOR C5 cd /opt/cloudera/parcels/CDH/lib/hue/build/env/lib64/python2.6/site-packages;

alias l=’ls –altrF’;

l /usr/lib64/python2.6/site-packages/M2Crypto;

l /usr/lib64/python2.6/site-packages;

l /usr/lib64/python2.6/site-packages/M2Crypto-0.20.2-py2.6.egg-info;

ln -s /usr/lib64/python2.6/site-packages/M2Crypto;

ls -altrF M2Crypto\*

ln -s /usr/lib64/python2.6/site-packages/M2Crypto-0.20.2-py2.6.egg-info;

# see CM SAML install (above) for the required “yum” commands

cd /home/gpainstall/saml;

unzip importlib-1.0.2.zip;

unzip pysaml2-master.zip;

unzip djangosaml2-master.zip;

ls -altrF /home/gpainstall/saml;

# IN C4 cd /opt/cloudera/parcels/CDH/share/hue/build/env/bin;

# IN C5 cd /opt/cloudera/parcels/CDH/lib/hue/build/env/bin/; which pip;

pip install /home/gpainstall/saml/importlib-1.0.2

pip install /home/gpainstall/saml/pysaml2-master

pip install /home/gpainstall/saml/djangosaml2-master

grep -A5 assertion\_consumer /usr/lib/python2.6/site-packages/djangosaml2/views.py

## Llama

When adding Impala to a cluster you can optionally add the Llama component to manage long running impala jobs.

From the Impala Instances page select ‘add service’ and select a host for the Llama service to run on. Impala management services usually run on master2 so that’s a good place to select.

Once you’ve selected the Llama host to use then the wizard will attempt to start the service. This will fail if Yarn configurations are not properly selected. Llama MUST be tied to a valid Yarn service and that Yarn service must be configured with certain options to allow Llama to work.

|  |  |  |
| --- | --- | --- |
| **YARN Service for Resource Management** | YARN (MR2 Included)  none  [Reset to empty default value](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/51/config)  For Impala to use YARN for resource management, the YARN configuration "Use CGroups for Resource Management" must be set to true.  For Impala to use YARN for resource management, the YARN configuration "Container Memory Minimum" must be set to 0.  For Impala to use YARN for resource management, the YARN configuration "Container Virtual CPU Cores Minimum" must be set to 0.  Both Llama role and YARN dependency are correctly configured. | Name of YARN service to use for resource management integration between Impala and YARN. This service dependency and the existence of a Llama role is required for using said integration. |

##### YARN Configurations for Llama

Add “Use Cgroups for resource Management” which requires “Linux Container Executor”

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**Service-Wide / Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | **Use CGroups for Resource Management**  yarn.nodemanager.linux-container-executor.resources-handler.class | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | Whether YARN creates a cgroup per container, thereby isolating the CPU usage of containers. When set, yarn.nodemanager.linux-container-executor.resources-handler.class is configured toorg.apache.hadoop.yarn.server.nodemanager.util.CgroupsLCEResourcesHandler. The host (in Cloudera Manager) must have cgroups enabled. The number of shares allocated to all YARN containers is configured by adjusting the CPU shares value of the Node Manager in the Resource Management configuration group. |
| [**Service-Wide / Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | **Always Use Linux Container Executor**  yarn.nodemanager.container-executor.class | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | Whether YARN uses the Linux Container Executor both in secure (Kerberos) and insecure (not Kerberos) environments. Cgroups enforcement only works when the Linux Container Executor is used. |

Hosts must be configured to use Cgroup based resource management otherwise you get this error

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**Service-Wide / Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | **Use CGroups for Resource Management**  yarn.nodemanager.linux-container-executor.resources-handler.class | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config)  Yarn is configured to use cgroups, but 3 hosts do not have "Enable Cgroup-based Resource Management" enabled. Hosts (up to first 10) affected: bdgtr001d52h1l.nam.nsroot.net,bdgtr002d31h1l.nam.nsroot.net,bdgtr003d32h1l.nam.nsroot.net. | Whether YARN creates a cgroup per container, thereby isolating the CPU usage of containers. When set, yarn.nodemanager.linux-container-executor.resources-handler.class is configured toorg.apache.hadoop.yarn.server.nodemanager.util.CgroupsLCEResourcesHandler. The host (in Cloudera Manager) must have cgroups enabled. The number of shares allocated to all YARN containers is configured by adjusting the CPU shares value of the Node Manager in the Resource Management configuration group. |

Fix this in the “Hosts” Configuration pages. Search for CGroup to get the following:

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/hardware/hosts/config) | **Enable Cgroup-based Resource Management** | default value | Enables resource management using control groups (cgroups) for this host. Once toggled, roles on this host must be restarted for cgroups to be enabled or disabled. Per-resource controls can be found in the configuration pages of role configuration groups and individual roles. Cgroups are a feature of the Linux kernel, and as such, support varies by distribution; consult the Cloudera Manager documentation for details. |

Change the YARN Configuration for “Container Memory Minimum” to zero

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**ResourceManager Default Group / Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | **Container Memory Minimum**  yarn.scheduler.minimum-allocation-mb | [Reset to the default value: 1 GiB](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | The smallest amount of physical memory, in MiB, that can be requested for a container. If using the Capacity or FIFO scheduler (or any scheduler, prior to CDH 5), memory requests will be rounded up to the nearest multiple of this number. |

Set to zero(0) the Yarn configuration value of “Container virtual CPU cores minimum”

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**ResourceManager Default Group / Resource Management**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | **Container Virtual CPU Cores Minimum**  yarn.scheduler.minimum-allocation-vcores | [Reset to the default value: 1](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | The smallest number of virtual CPU cores that can be requested for a container. If using the Capacity or FIFO scheduler (or any scheduler, prior to CDH 5), virtual core requests will be rounded up to the nearest multiple of this number. This parameter has no effect prior to CDH 4.4. |

**After making these changes: Deploy Client Configurations AND Restart the cluster**

## SQOOP

In C5 Sqoop may have problems starting – known issues will be fixed by Cloudera in a later release.

Temporary work around is to add values to the sqoop.properties safety valve in Cloudera manager sqoop configuration page :

org.apache.sqoop.connector.autoupgrade=true

org.apache.sqoop.framework.autoupgrade=true

|  |  |  |
| --- | --- | --- |
| **Sqoop 2 Server Advanced Configuration Snippet (Safety Valve) for sqoop.properties** | [Reset to the default value: ...](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/72/config) | For advanced use only, a string to be inserted into **sqoop.properties**for this role only. |

## Accumulo – Ask before installing this

When adding accumulo remember to assign the roles across master and worker / data nodes as defined in the role assignment section.

When adding the Accumulo service you must change the secret that must be known to all nodes in the accumulo cluster as well as the passwords for the root and trace users. By default the root user is used as the trace user so you must use the same password for both root user and trace user.

**Hint set these to the same value using the cluster name as a default before GPA changes them later**

Set the following configuration values for your new role(s). Required values are marked with **\***.

| **Parameter** | **Group** | **Value** | **Description** |
| --- | --- | --- | --- |
| **Service Accumulo 1.6** | | | |
| **Accumulo Instance Secret\*** instance.secret | **Service-Wide** | [Reset to the default value: DEFAULT](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/clusters/1/add-service/index) | A secret unique to a given instance that all servers must know in order to communicate with one another. |
| **HDFS Directory\*** instance.dfs.dir | **Service-Wide** | /accumulo  default value | The directory used in HDFS by Accumulo. |
| **Instance Name\*** accumulo\_instance\_name | **Service-Wide** | accumulo  default value | Name of the Accumulo instance. Used while initializing Accumulo. |
| **Root Password\*** accumulo\_root\_password | **Service-Wide** | [Reset to the default value: \*\*\*\*\*\*](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/clusters/1/add-service/index) | Password for root Accumulo user. Used while initializing Accumulo. If you are chaging this and are using root user for tracing, make sure to set Trace Password to same value. |
| **Trace Password\*** trace.token.property.password | **Service-Wide** | [Reset to the default value: \*\*\*\*\*\*](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/clusters/1/add-service/index) | Trace Password. If you are using root user for tracing, then make sure it is set to same value as Root Password. |
| **Trace User\*** trace.user | **Service-Wide** | root  default value | Trace User |

## Navigator

Per cloudera case 72013 – Increase the Java Heap size for Navigator Metadata Server:   
Currently you are set to the default 2GB. We would like to start with doubling the setting. As it is not trivial to project the number of transactions this may take a few iterations to get the setting correct. We have seen some customers needing as much as 12 GB.

To set this navigate to Management services -> configuration -> Navigator Metadata server -> performance -> Java Heap Size of Navigator Metadata Server in Bytes .

This will require you to restart the Navigator Metadata server.

## SPARK

When installing the spark service the process is the same as other services in that you’ll select add service from the cluster home status page and then select the service and follow the wizard instructions. What you need to know is that there are two spark services that can be added and you only want one of them. The Spark ‘stand alone’ service is not supported and should not be used. Instead, select the spark on yarn service.

### Spark Shell Mode

These changes \***do not**\* require a cluster restart or even a service restart. They affect client configuration only and will be propagated via “Deploy client configuration” action from the Spark service tab.

In gateway default group, Advanced configuration tab:

Spark Client Advanced Configuration Snippet (Safety Valve) for spark-conf/spark-defaults.conf:

spark.master=yarn-client

spark.executor.memory=3g

The reasons are as follows:

1. For some reason, CDH doesn’t default to launching spark through YARN, but rather local. While it can be specified on the command line when launching spark commands, it is unexpected and confusing when people assume things will launch on the cluster rather than locally. For any eventual future release of spark to a cluster, this would be a “good” default.
2. Executor memory defaults to 512Mb, which again can be overridden on the command line, but a good default is in order. In this case, due to Fried Taco’s limitations, I am suggesting 3g. For a real cluster a “reasonable” default would have to be chosen that is balanced to total YARN memory and average cases.

### Spark Dynamic Resource Allocation

### CM51 Spark History Server

The Spark History Server does not start when managed by a Cloudera Manager 5.1 instance when Kerberos authentication is enabled. This is fixed in 5.2 and above.

**Workaround:**

**Keytab files in /opt/Cloudera/keytabs for spark keytabs should be owned by spark: spark not Cloudera-scm**

1. Go to the Spark service.
2. Expand the **History Server Default Group** > **Advanced** category.
3. Add the following configuration to the **History Server Environment Advanced Configuration Snippet** property:

SPARK\_HISTORY\_OPTS=-Dspark.history.kerberos.enabled=true \

-Dspark.history.kerberos.principal=*principal* \

-Dspark.history.kerberos.keytab=*keytab*

where *principal* is (**spark**) the name of the Kerberos principal to use for the History Server, and *keytab* is the path to the principal's keytab file on the local filesystem of the host running the History Server (/opt/Cloudera/keytabs/*file*.)

EXAMPLE:

SPARK\_HISTORY\_OPTS=-Dspark.history.kerberos.enabled=true -Dspark.history.kerberos.principal=spark/bdgtr001d52h1l.nam.nsroot.net@NAMUXDEV.DYN.NSROOT.NET -Dspark.history.kerberos.keytab=/opt/Cloudera/keytabs/spark.bdgtr001d52h1l.keytab

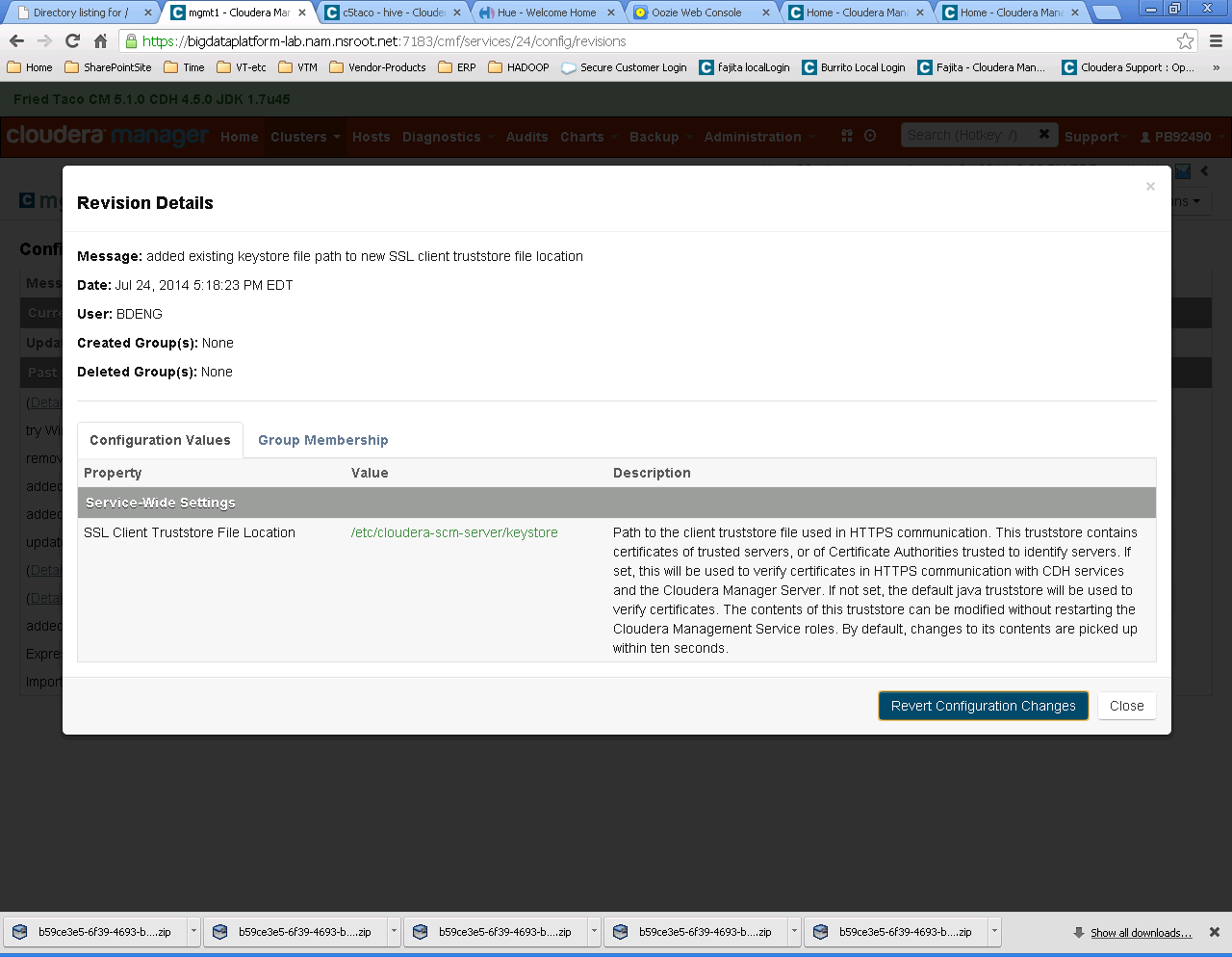
## HTTPS & LDAP

This process consists of the following steps

<https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/BigData_CM_HTTPS_SSL_provisioning.docx>

<https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/BigData_Hue_HTTPS_SSL_provisioning.docx>

<https://catecollaboration.citigroup.net/domains/deveng/debi/BigData/Documents/Engineered-Solutions/Cloudera-Hadoop/BigData_Hue_LDAP_provisioning.docx>

New for CDH 5 and above 

# Additional Configuration Changes for Citi Builds

This is a catch all section intended to include any configuration changes that Citi operations or engineering teams and or Cloudera Support has recommended to be applied to our clusters

## Connectors

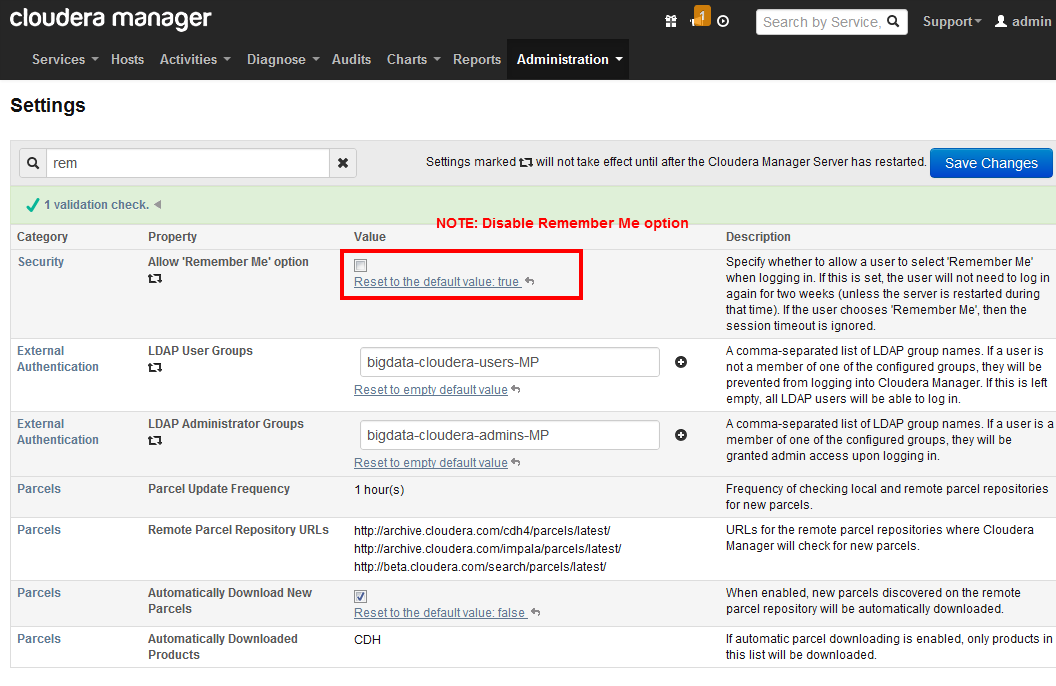
[To see details on loading and using standard connectors see the document on Big Data Connectors](https://collaborate.citi.net/docs/DOC-166296)

## Changes required by the CIVA audit

### Disable “Remember Me” within Cloudera Manager Administration

Administration -> Settings

NOTE: Enter “remember” in search box to locate remember me and disabled/uncheck box.

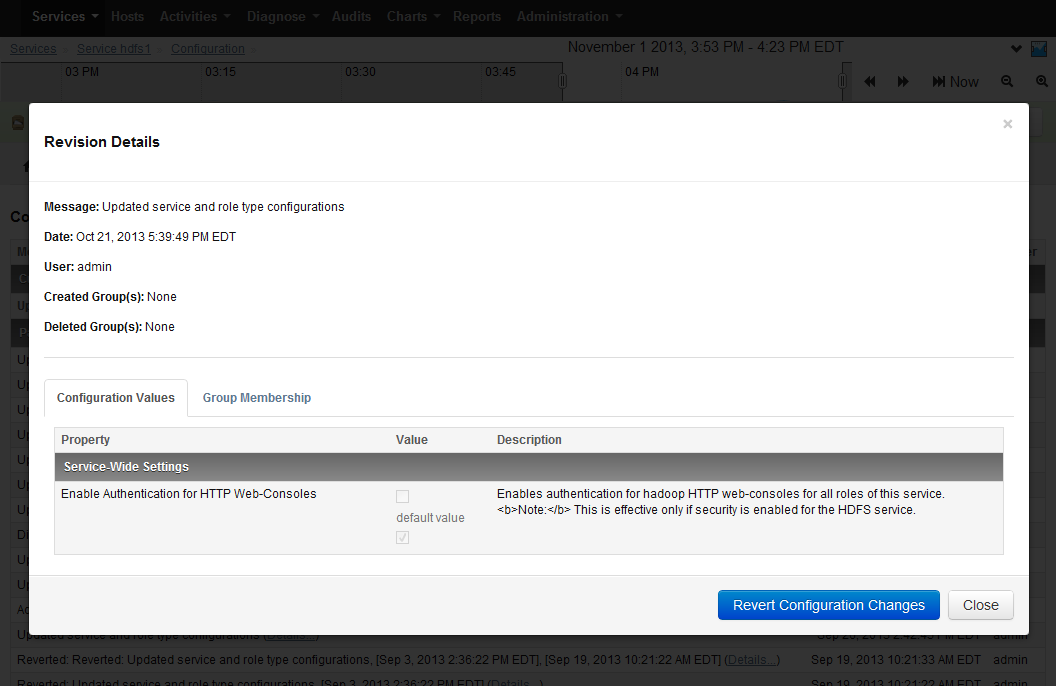


### Enable authentication within YARN service’s configuration

|  |  |  |
| --- | --- | --- |
| **Enable Authentication for HTTP Web-Consoles** | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) | Enables authentication for hadoop HTTP web-consoles for all roles of this service. **Note:** This is effective only if security is enabled for the HDFS service. |

### Enable authentication within HDFS1 service’s configuration

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| | **Category** | **Property** | **Value** | **Description** | | --- | --- | --- | --- | | [**Service-Wide / Security**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/42/config) | **Enable Authentication for HTTP Web-Consoles** | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/42/config) | Enables authentication for hadoop HTTP  web-consoles for all roles of this service.  **Note:** This is effective only if security is  enabled for the HDFS service. | |



### Security Harden Hue

#### Session Timeout

Session timeouts can be set by specifying the ttl configuration property under the [desktop]>[[session]] section in HUE / Srervice-Wide / Advanced / **Hue Service Advanced Configuration Snippet (Safety Valve) for hue\_safety\_valve.ini** Add or update the desktop session section

**[desktop]**

**collect\_usage=false**

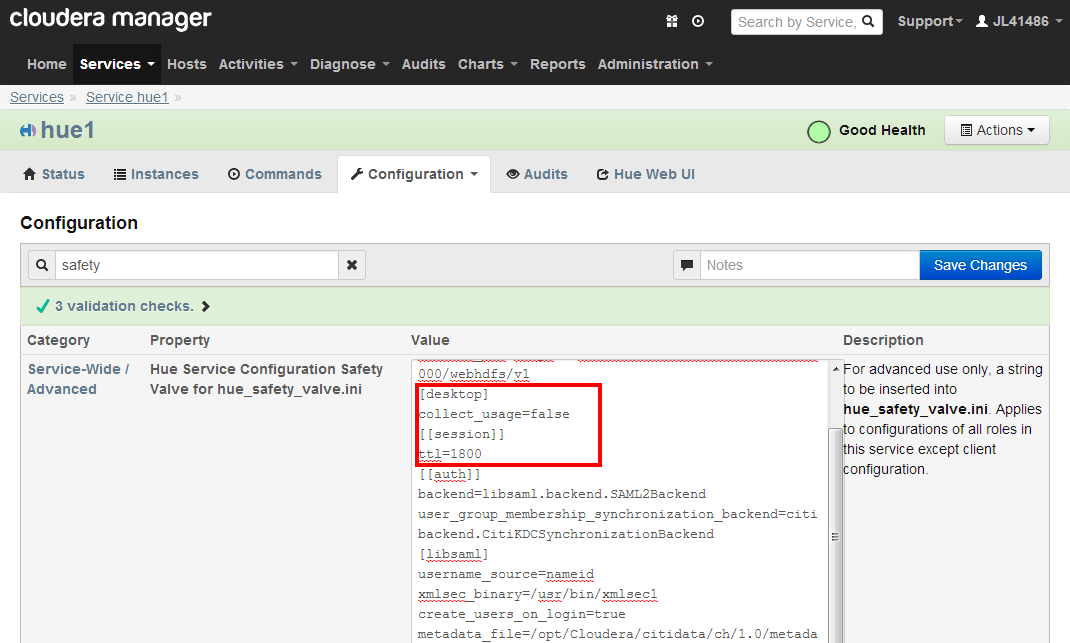
**[[session]]**

**ttl=1800**

**secure=true**

**http-only=true**

|  |  |
| --- | --- |
| Ttl | The cookie containing the users' session ID will expire after this amount of time in seconds.  NOTE: Change to 1800 (30 mins.)  Default: 60\*60\*24\*14 |

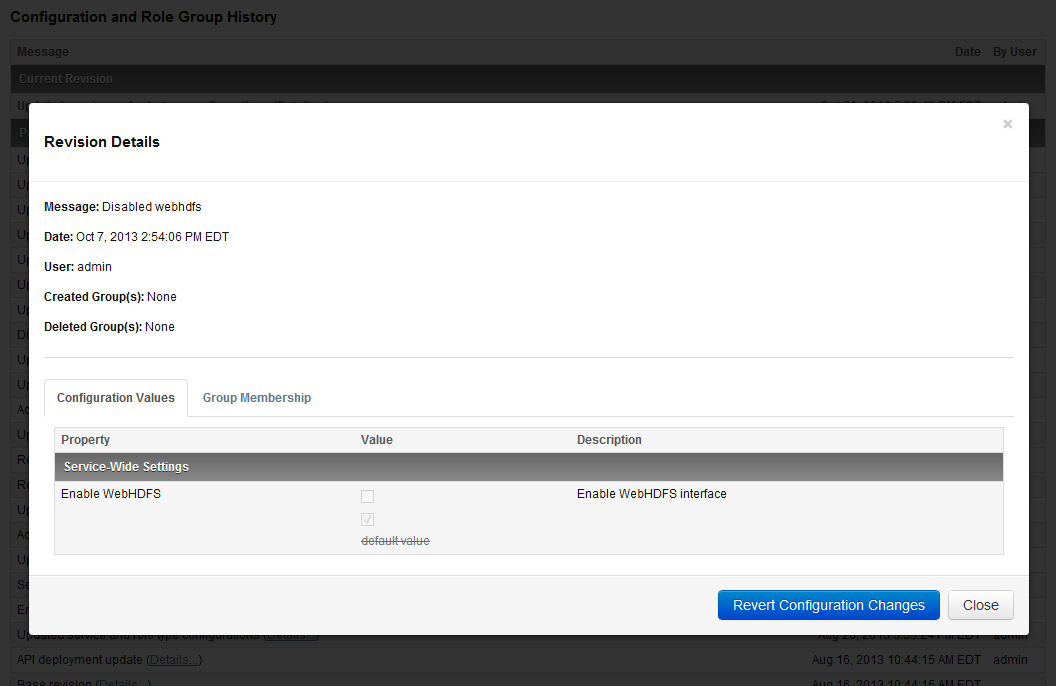


### SET HUE to default to no access

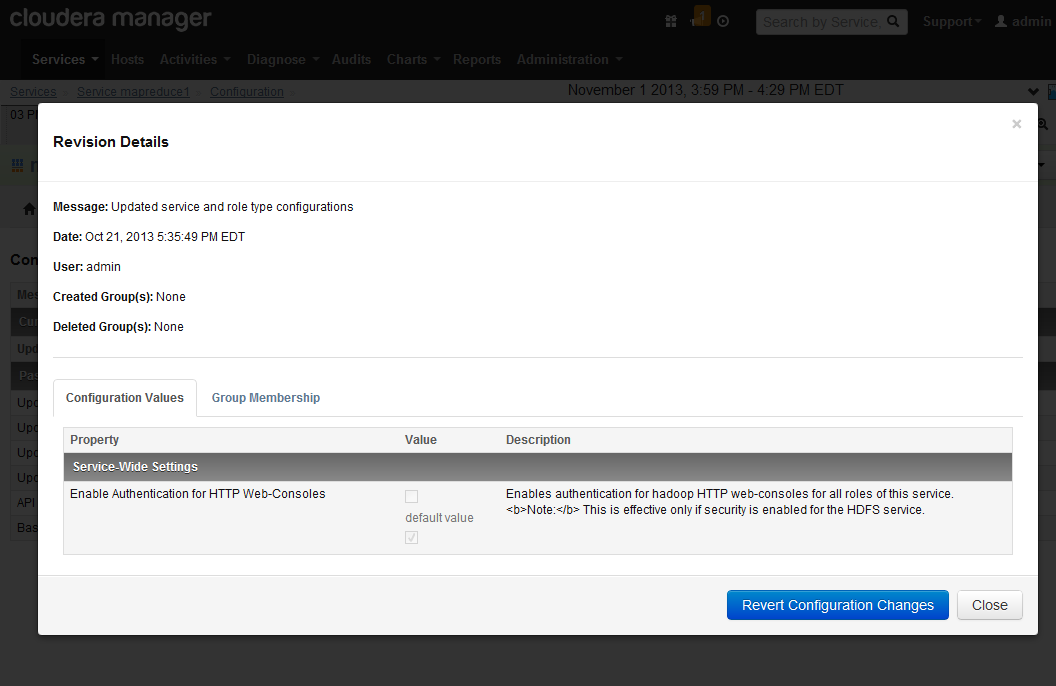
Create a group in HUE with no access permissions and then define this group as the default user group **Default User Group**   
default\_user\_group

|  |  |  |
| --- | --- | --- |
| **Default User Group**  default\_user\_group | [Reset to empty default value](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/49/config) | The name of a default |

### Disable webhdfs interface

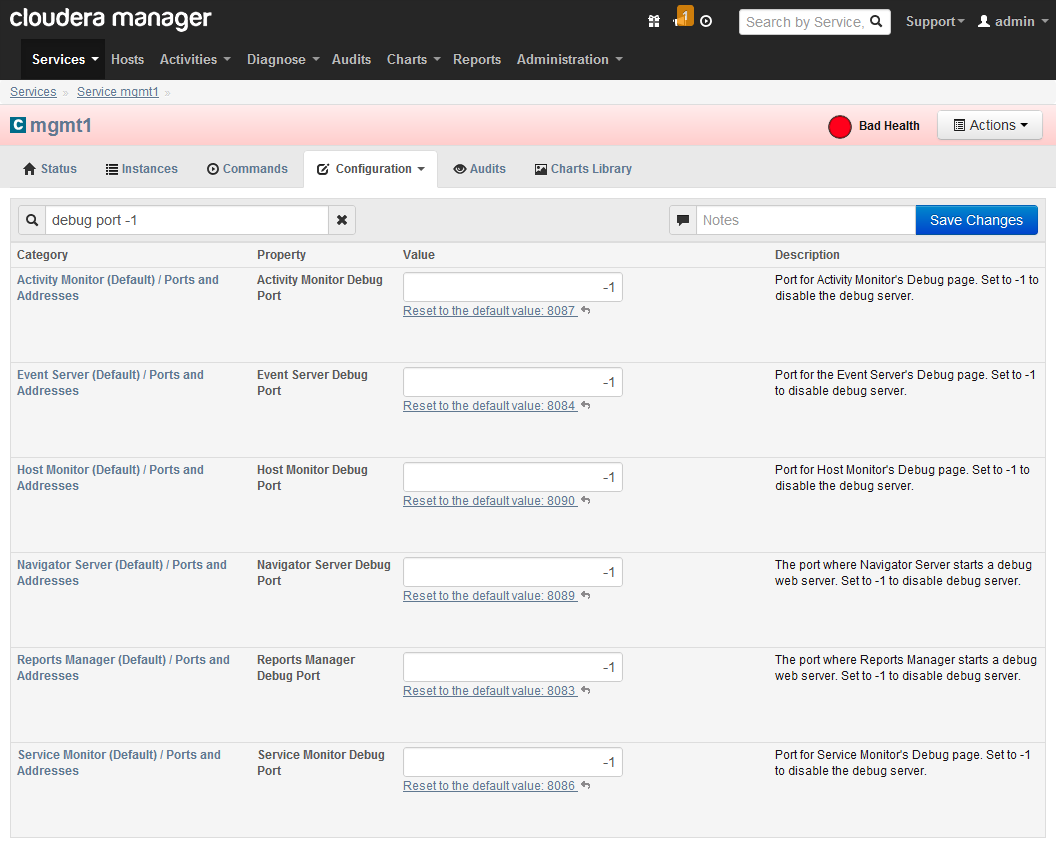


MapReduce1 Service

* Disable WebHDFS from within MapReduce1 service configuration
* 

### C4 Only - Disable “debug” ports within Cloudera Manager Administration

From within the management services configuration, enter “debug port” in the search box. Set all Debug ports to -1 **EXCEPT** Navigator. Then save and restart management services.



### C4 only - To disable Navigator, follow these instructions:

There is a way to disable the debug server on Cloudera Navigator by adding the following property to cloudera-navigator.properties:   
  
navigator.server.debug=false   
  
You can add this in Cloudera Manager by going to;   
  
mgmt > Configuration > View & Edit > Navigator Server > Advanced   
  
and adding the string above to the property entitled, "Navigator Server Configuration Safety Valve for cloudera-navigator.properties." Restart the Navigator server and the debug port will no longer be listening.   
  
We have raised a ticket to have the text in the Manager UI updated to remove the erroneous instructions to set the port to -1 and to document disabling the debug port correctly.

### Restrict access to keystore file

The keystore file (/etc/cloudera-scm-server/keystore) should be owned by Cloudera-scm:Cloudera-scm with permissions of 600

l /etc/cloudera-scm-server/keystore

-rw-r--r-- 1 cloudera-scm cloudera-scm 2924 Sep 3 16:38 /etc/cloudera-scm-server/keystore

# chmod 600 /etc/cloudera-scm-server/keystore

# l /etc/cloudera-scm-server/keystore

-rw------- 1 cloudera-scm cloudera-scm 2924 Sep 3 16:38 /etc/cloudera-scm-server/keystore

### Default umask for HDFS

Change this from 022 to 027 to prevent new files from being created as world readable

|  |  |  |
| --- | --- | --- |
| **Default Umask**  dfs.umaskmode, fs.permissions.umask-mode | [Reset to the default value: 022](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/42/config) | Default umask for file and directory creation, specified in an octal value (with a leading 0) |

### Navigator Metadata Server Switch to HTTPS

The Navigator Metadata Server comes configured as an HTTP service with no option to switch it to HTTPS. Cloudera support offered the following way to change it to HTTPS.

|  |  |  |  |
| --- | --- | --- | --- |
| [**Navigator Metadata Server (beta) Default Group / Advanced**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/44/config) | **Navigator Metadata Server Advanced Configuration Snippet (Safety Valve) for cloudera-navigator.properties** | [Reset to the default value: ...](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/44/config) | For advanced use only, a string to be inserted into**cloudera-navi** |

Use Cloudera Manager to configure the management server for Navigator Metadata Server and edit the advanced property safety valve (snippet) to add a string:

nav.http.enable\_ssl=true

nav.ssl.keyStore=***/etc/cloudera-scm-server/keystore***

nav.ssl.keyStorePassword=***hadoop***

***You must replace the values in this string with valid values for the password and path of the keystore that you’re using.***

### Zookeeper JMX Agent Authentication

CIVA Finding of “RMI Services Exposed - Potential Remote RMI” is fixed as follows:

JMX authentication for ZK is available but is turned off by default. You can set this to true via CM -> ZooKeeper -> Configuration -> "Enable Authenticated Communication with the JMX Agent".

|  |  |  |  |
| --- | --- | --- | --- |
| [**Server Default Group**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/48/config) | **Enable Authenticated Communication with the JMX Agent** | default value | Enables authentication when interacting with the JMX agent on the ZooKeeper server. |

Restart the zookeeper and management services after making this change

### Set Sentry and HDFS ACL synchronization

ACL’s are the way to mimic sentry permissions in HDFS . Set the following propwerties in HDFS configuration so that ACL’s will be automatically set to match sentry permissions at the HDFS layer.

1. Go to the HDFS service.
2. Click the Configuration tab.
3. Navigate to the **Service-Wide** category and check the Check HDFS Permissions checkbox.
4. Under the **Service-Wide** category go to **Security**.
5. Check the **Enable Sentry Synchronization** checkbox.
6. Use the **Sentry Synchronization Path Prefixes** property to list HDFS path prefixes where Sentry permissions should be enforced. Multiple HDFS path prefixes can be specified. By default, this property points to user/hive/warehouse and must always be non-empty. HDFS privilege synchronization will not occur for tables located outside the HDFS regions listed here.
7. Click Save Changes.
8. Restart the cluster. Note that it may take an additional two minutes after cluster restart for privilege synchronization to take effect.

## YARN / HUE Logging problems

|  |  |  |
| --- | --- | --- |
| **Purpose** | |  | | --- | | Configure YARN to allow display of job history logs | |
| **Symptoms** | |  | | --- | | * After job finishes, history server URL for job yields error "java.io.FileNotFoundException:  File /tmp/hadoop-yarn/staging/history/done/2014/06/22/000000 does not exist." * Hitting the history server root URL does not show the successfully completed job in its list of  recently-completed jobs. * YARN command line does not show logs * HUE Job Browser and Pig Dashboard do not show job logs | |

|  |  |  |
| --- | --- | --- |
| **Applies To** | |  | | --- | | * CDH 5 and higher * Cloudera Manager (CM) 5 and higher * YARN * HUE | |
| **Cause** | |  | | --- | | The job history server URL must be configured for the node managers and application manager to be able to  find it and forward the job logs to it. If YARN is not configured correctly the HUE user interface will also not be able to show any logs. | |  | |

In Yarn configuration / Site Wide / Advanced enter the safety vale entrye for yarn-site.xml  
<property>

<name>yarn.log.server.url</name>

<value>http://jobhistoryservername:19888/jobhistory/logs/</value>

</property>

job history server is mstr3 so e.g. bdgtr003d32h1l.nam.nsroot.net

|  |  |
| --- | --- |
| **YARN Service Advanced Configuration Snippet (Safety Valve) for yarn-site.xml** | [Reset to the default value: ...](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/52/config) |

After making the change :

Deploy Client Configurations

Restart the cluster

HUE Debug Messages

Disable debugging messages in HUE unles required for dev team access

Set both of these to ‘OFF”  status

**Enable Django Debug Mode**

django\_debug\_mode

Hue - 1 (Service-Wide)



In debug mode, Django displays a detailed traceback when an exception occurs. Note that the debugging information may contain sensitive data. Note also that Django remembers every SQL query it executes while in debug mode, which will rapidly consume memory.

**Enable Debugging of Internal Server Error Responses**

http\_500\_debug\_mode

Hue - 1 (Service-Wide)



Enable debug output in HTTP Internal Server Error (status 500) responses. Note that the debugging information may contain sensitive data. If Enable Django Debug Mode is set, this is automatically enabled.

Restart the service

## NFS Gateway

##### Create the NFS gateway service on an edge node (proxy1 etc) and this will create the following ports for access

|  |  |  |
| --- | --- | --- |
| **NFS Gateway Server Port**  nfs3.server.port | 2049  default value | The NFS Gateway server port. |
| **NFS Gateway MountD Port**  nfs3.mountd.port | 4242  default value | The port number of the mount daemon implemented inside the NFS Gateway server role. |
| **Portmap (or Rpcbind) Port** | 111  default value | The port number of the system portmap or rpcbind service. This configuration is used by Cloudera Manager to verify if the system portmap or rpcbind service is running before starting NFS Gateway role. Cloudera Manager does not manage the system portmap or rpcbind service. |

##### From linux machines create a folder then a mount point

# id

uid=0(root) gid=0(root) groups=0(root)

# mkdir hadoopnfs

# echo kinit -k -t /opt/Cloudera/keytabs/`whoami`.`hostname -s`.keytab `whoami`/`hostname -f`@NAMUXDEV.DYN.NSROOT.NET

# kinit -k -t /opt/Cloudera/keytabs/hdfs.bdgtr002d31h1l.keytab hdfs/bdgtr002d31h1l.nam.nsroot.net@NAMUXDEV.DYN.NSROOT.NET

# mount -t nfs -o vers=3,proto=tcp,nolock bdgtr002d51h1l.nam.nsroot.net:/tmp /root/hadoopnfs

mount.nfs: mounting bdgtr002d51h1l.nam.nsroot.net:/tmp failed, reason given by server: No such file or directory

# mount -t nfs -o vers=3,proto=tcp,nolock bdgtr002d51h1l.nam.nsroot.net:/ /root/hadoopnfs

# l hadoopnfs

total 9

drwxr-xr-x 3 hdfs supergroup 96 Aug 1 15:14 data/

drwxr-x--x 2 2163130175 2163130175 64 Sep 18 13:27 accumulo/

drwxr-xr-x 9 hdfs supergroup 288 Sep 18 13:27 ./

drwxr-xr-x 8 platfora supergroup 256 Sep 19 12:48 platfora/

drwxrwxr-x 14 solr solr 448 Sep 23 05:43 solr/

drwxrwxrwx 25 hdfs supergroup 800 Sep 24 11:49 user/

drwxrwxrwt 18 hdfs supergroup 576 Sep 24 12:28 tmp/

drwxr-xr-x 10 hbase hbase 320 Sep 24 13:24 hbase/

dr-xr-x--- 6 root root 4096 Sep 24 15:34 ../

# l hadoopnfs/user/hive/warehouse

ls: cannot open directory hadoopnfs/user/hive/warehouse: Permission denied

# l hadoopnfs/user

total 13

drwxrwxrwx 4 mapred hadoop 128 Jun 17 18:24 history/

drwxrwxr-t 3 hive hive 96 Jun 18 17:37 hive/

drwxrwxr-x 3 oozie oozie 96 Jun 18 17:38 oozie/

drwxrwxr-x 2 sqoop2 sqoop 64 Jun 18 17:39 sqoop2/

drwxrwxr-x 2 impala impala 64 Jun 18 17:40 impala/

drwxr-xr-x 2 3385292202 3385292202 64 Jun 18 18:40 sample/

drwxr-xr-x 6 hue hue 192 Jul 2 17:06 hue/

drwxr-xr-x 3 pb92490 3476003296 96 Jul 14 10:22 pb92490/

drwxrwxrwx 4 spark spark 128 Jul 14 10:47 spark/

drwxr-xr-x 4 hdfs supergroup 128 Jul 14 10:50 hdfs/

drwxr-xr-x 2 2886784715 2886784715 64 Jul 14 15:36 c5taco/

drwxr-xr-x 3 tresata tresata 96 Aug 11 17:37 tresata/

drwxr-xr-x 4 63046972 63046972 128 Sep 4 13:14 BDENG/

drwxr-xr-x 2 103662773 103662773 64 Sep 4 15:21 manoj/

drwxr-xr-x 2 3030589694 3030589694 64 Sep 5 09:13 jongkook/

drwxr-xr-x 2 platfora platfora 64 Sep 11 17:14 platfora/

drwxr-xr-x 2 rs89222 1442021808 64 Sep 11 17:14 rs89222/

drwxr-xr-x 2 datameer datameer 64 Sep 11 17:14 datameer/

drwxr-xr-x 9 hdfs supergroup 288 Sep 18 13:27 ../

drwxr-x--- 2 2163130175 2163130175 64 Sep 18 13:28 accumulo/

drwxr-xr-x 2 jk97029 bdegrp 64 Sep 19 10:17 jk97029/

drwx------ 5 tk85776 supergroup 160 Sep 19 12:23 tk85776/

drwxr-xr-x 5 sd33170 supergroup 160 Sep 24 11:13 sd33170/

drwxrwxrwx 25 hdfs supergroup 800 Sep 24 11:49 ./

drwx------ 5 hbase supergroup 160 Sep 24 12:29 hbase/

# l hadoopnfs/user/hive

total 2

drwxrwxr-t 3 hive hive 96 Jun 18 17:37 ./

drwxrwxrwx 25 hdfs supergroup 800 Sep 24 11:49 ../

drwxrwx--x 7 hive hive 224 Sep 24 12:21 warehouse/

#

##### Putting Data to the HDFS system Via NFS Mount Point

To Use the new mount for ‘put’ ing data into the cluster just reference it as a file, so from linux, command >> file.txt will create the file in the HDFS system

l /root/hadoopnfs/user >l

total 17

drwxrwxrwx 4 mapred hadoop 128 Jun 17 18:24 history/

drwxrwxr-x 3 oozie oozie 96 Jun 18 17:38 oozie/

drwxrwxr-x 2 sqoop2 sqoop 64 Jun 18 17:39 sqoop2/

drwxrwxr-x 2 impala impala 64 Jun 18 17:40 impala/

drwxr-xr-x 2 3385292202 3385292202 64 Jun 18 18:40 sample/

drwxr-xr-x 6 hue hue 192 Jul 2 17:06 hue/

drwxrwxrwx 4 spark spark 128 Jul 14 10:47 spark/

drwxr-xr-x 4 hdfs supergroup 128 Jul 14 10:50 hdfs/

drwxr-xr-x 2 2886784715 2886784715 64 Jul 14 15:36 c5taco/

drwxr-xr-x 3 tresata tresata 96 Aug 11 17:37 tresata/

drwxr-xr-x 4 63046972 63046972 128 Sep 4 13:14 BDENG/

drwxr-xr-x 2 103662773 103662773 64 Sep 4 15:21 manoj/

drwxr-xr-x 2 3030589694 3030589694 64 Sep 5 09:13 jongkook/

drwxr-x--- 2 2163130175 2163130175 64 Sep 18 13:28 accumulo/

drwx------ 5 tk85776 supergroup 160 Sep 19 12:23 tk85776/

drwxr-x--- 3 solr solr 96 Sep 24 17:55 solr/

drwxr-x--- 3 sd33170 supergroup 96 Sep 26 11:35 sush/

drwx------ 10 hbase supergroup 320 Sep 26 12:19 hbase/

drwxr-xr-x 4 jk97029 bdegrp 128 Oct 3 10:46 jk97029/

drwxr-xr-x 4 pb92490 3476003296 128 Oct 3 17:43 pb92490/

drwxr-xr-x 6 sd33170 bdegrp 192 Oct 7 08:05 sd33170/

drwxrwxr-t 4 hive hive 128 Oct 16 02:47 hive/

drwxr-xr-x 3 platfora platfora 96 Oct 16 12:40 platfora/

drwxr-x--- 4 rr45795 supergroup 128 Nov 5 13:10 rr45795/

drwx------ 4 revor supergroup 128 Nov 6 14:41 revor/

drwxr-xr-x 10 hdfs supergroup 320 Nov 7 13:13 ../

drwx------ 4 pp85712 supergroup 128 Nov 7 15:54 pp85712/

drwxr-xr-x 4 rs89222 1442021808 128 Nov 7 16:25 rs89222/

drwxrwxr-x 14 datameer datameer 448 Nov 11 11:25 datameer/

drwxrwxrwx 6 hdfs supergroup 192 Nov 12 15:13 RevoShare/

drwxrwxrwx 32 hdfs supergroup 1024 Nov 12 15:15 ./

drwx------ 4 dg25361 supergroup 128 Nov 12 15:17 dg25361/

/root/hadoopnfs/user >l /home/pb92490 >> newtestofNFSput.txt

/root/hadoopnfs/user >l

total 18

drwxrwxrwx 4 mapred hadoop 128 Jun 17 18:24 history/

drwxrwxr-x 3 oozie oozie 96 Jun 18 17:38 oozie/

drwxrwxr-x 2 sqoop2 sqoop 64 Jun 18 17:39 sqoop2/

drwxrwxr-x 2 impala impala 64 Jun 18 17:40 impala/

drwxr-xr-x 2 3385292202 3385292202 64 Jun 18 18:40 sample/

drwxr-xr-x 6 hue hue 192 Jul 2 17:06 hue/

drwxrwxrwx 4 spark spark 128 Jul 14 10:47 spark/

drwxr-xr-x 4 hdfs supergroup 128 Jul 14 10:50 hdfs/

drwxr-xr-x 2 2886784715 2886784715 64 Jul 14 15:36 c5taco/

drwxr-xr-x 3 tresata tresata 96 Aug 11 17:37 tresata/

drwxr-xr-x 4 63046972 63046972 128 Sep 4 13:14 BDENG/

drwxr-xr-x 2 103662773 103662773 64 Sep 4 15:21 manoj/

drwxr-xr-x 2 3030589694 3030589694 64 Sep 5 09:13 jongkook/

drwxr-x--- 2 2163130175 2163130175 64 Sep 18 13:28 accumulo/

drwx------ 5 tk85776 supergroup 160 Sep 19 12:23 tk85776/

drwxr-x--- 3 solr solr 96 Sep 24 17:55 solr/

drwxr-x--- 3 sd33170 supergroup 96 Sep 26 11:35 sush/

drwx------ 10 hbase supergroup 320 Sep 26 12:19 hbase/

drwxr-xr-x 4 jk97029 bdegrp 128 Oct 3 10:46 jk97029/

drwxr-xr-x 4 pb92490 3476003296 128 Oct 3 17:43 pb92490/

drwxr-xr-x 6 sd33170 bdegrp 192 Oct 7 08:05 sd33170/

drwxrwxr-t 4 hive hive 128 Oct 16 02:47 hive/

drwxr-xr-x 3 platfora platfora 96 Oct 16 12:40 platfora/

drwxr-x--- 4 rr45795 supergroup 128 Nov 5 13:10 rr45795/

drwx------ 4 revor supergroup 128 Nov 6 14:41 revor/

drwxr-xr-x 10 hdfs supergroup 320 Nov 7 13:13 ../

drwx------ 4 pp85712 supergroup 128 Nov 7 15:54 pp85712/

drwxr-xr-x 4 rs89222 1442021808 128 Nov 7 16:25 rs89222/

drwxrwxr-x 14 datameer datameer 448 Nov 11 11:25 datameer/

drwxrwxrwx 6 hdfs supergroup 192 Nov 12 15:13 RevoShare/

drwx------ 4 dg25361 supergroup 128 Nov 12 15:17 dg25361/

-rw-r--r-- 1 pb92490 bdegrp 767 Nov 19 12:56 newtestofNFSput.txt

drwxrwxrwx 33 hdfs supergroup 1056 Nov 19 12:56 ./

/root/hadoopnfs/user >

Obviously this is not optimal since users are putting data into the HDFS system outside of their home folders. To remedy this issue we create a linux OS link to the users home folder and have them wite to this location, as follows:

/home/pb92490 >ln -sf /root/hadoopnfs/user/pb92490 hadoopnfspb

/home/pb92490 >l

total 56

-rw-r--r-- 1 pb92490 bdegrp 121 Jun 4 14:50 .kshrc

-rw-r--r-- 1 pb92490 bdegrp 124 Jun 4 14:50 .bashrc

-rw-r--r-- 1 pb92490 bdegrp 176 Jun 4 14:50 .bash\_profile

-rw-r--r-- 1 pb92490 bdegrp 18 Jun 4 14:50 .bash\_logout

-rw------- 1 pb92490 bdegrp 625 Jun 4 15:17 .viminfo

drwxr-xr-x 2 pb92490 bdegrp 4096 Jul 2 15:34 cm51rc2/

-rw-r--r-- 1 pb92490 bdegrp 10240 Jul 11 13:17 HTTP-keytabs.tar

-rw-r--r-- 1 pb92490 bdegrp 1374 Sep 3 13:17 ca-cert.pem

drwxr-xr-x 19 root root 4096 Nov 7 09:09 ../

-rwxr-xr-x 1 pb92490 bdegrp 195 Nov 19 12:46 pab.profile\*

lrwxrwxrwx 1 pb92490 bdegrp 28 Nov 19 13:07 hadoopnfspb -> /root/hadoopnfs/user/pb92490/

drwxr-xr-x 3 pb92490 bdegrp 4096 Nov 19 13:07 ./

-rw------- 1 pb92490 bdegrp 1296 Nov 19 13:07 .sh\_history

/home/pb92490 >cd hadoopnfspb

/home/pb92490/hadoopnfspb >cat /home/pb92490/pab.profile > pab.profile

/home/pb92490/hadoopnfspb >l

total 4

drwxr-xr-x 5 pb92490 3476003296 160 Jul 16 15:48 .sparkStaging/

drwx------ 2 pb92490 3476003296 64 Oct 3 17:43 .staging/

drwxrwxrwx 33 hdfs supergroup 1056 Nov 19 12:56 ../

-rw-r--r-- 1 pb92490 bdegrp 195 Nov 19 13:26 pab.profile

drwxr-xr-x 5 pb92490 3476003296 160 Nov 19 13:26 ./

## Cloudera / EMC Isilon

EMC Isilon is a storage service with a distributed file system that can used in place of HDFS to provide storage for CDH services.

http://www.cloudera.com/content/cloudera/en/documentation/core/latest/static/note.jpg  **Note**: This documentation covers only the Cloudera Manager portion of using EMC Isilon storage with Cloudera Manager. For information about tasks performed on Isilon OneFS, see the information hub for Cloudera on the EMC Community Network: [**https://community.emc.com/docs/DOC-39522**](https://community.emc.com/docs/DOC-39522).

DO NOT INSTALL THIS SERVICE

This service is only to be installed by specific request and with co operation from the storage team

## Custom Settings IN CMS

##### Strong Encryption

When prompted in the install wizard about installing Stong Encryption that requires java compoanents this option should be selected. There are a few coutries where this level of encryption can not or should not be used but these are the exceptions.

AES256 is the current strongest level available and depends on the OS level settings in krb5.conf as to whether its available. Setting CMS to use unlimited strength means that it will use the strongest level that is available from the OS level settings and does not need to be changed when the OS level settings change.

This combines with the level 2 TLS encryption settings fro CMS and agents as well as the ‘HTTP Referer Check’ which should be set on since it’s off by default and helps verify that http addresses are not being spoofed.

##### HOST NAME

Host Name values used by CMS in cluster build and add node operations are taken from “/etc/sysconfig/network” At Citi this value is usually the short name of the hostname which conflicts with the host name used in security certificates at Citi which is always the fully qualified name of the host. This means that when hosts are added they get added using the short name and when we apply security the name in the certificates is NOT the short name so we get a host name mismatch warning.

This is fixed by modifying the hostname value in the agent coinfiguration file. Pro actively we could start using the fully qualified hostname in the /etc/sysconfig/network file.

##### Trusted Kerberos Realm

In the configuration setting for HDFS under system-wide and Security is a value for ‘Trusted Kerberos Realm’ This is the spot to add other realms that you want the cluster to trust. By default it will already trust the realm specified in the krb5.conf file so if only one realm is required then this field can be left blank. If we want to experiment with adding the windows Kerberos realms then this is a place to start.

HDFS default access

All new HDFS content is created using the default umask settings of 022 which means it is “world readable”. Modifying the default umask to 027 will remove the “world readable” property from new creations.

##### HDFS Groups and Group level Access

CMS uses ‘supergroup’ as the default value for Super User Group and membership in this group grants full access to the cluster. This group is intended to grant access for cluster administration purposes. So choose a group that belongs to an appropriate admin ID and that SOE ID’s must pbrun to gain access to.

Similar to the super group are the “Authorized Groups” and “Authorized Admin Groups”. Both of these are in the HDFS configuration under system-wide and Security. These fields are blank by default but could be used to limit access to a cluster by adding a group name that is unique to the cluster like a cluster name for example ‘taco’. By adding this value to the Authorized groups all ID’s that are not members of this group are shut out of the cluster. This is particularly useful when business users are ina specific group that is repeated across all clusters in the SDLC (DEV UAT Prod). We don’t always want members of a business group to have access to all clusters but neither do we want to use different groups to own the same business data that is in all clusters in the SDLC as this would cause migration problems.

Similar to “Authorized Groups” is “Authorized Admin Groups” and adding a group name in this field restricts which users can run admin commands against the cluster.

See the sentry documentation for a more complete discussion on this restriction technique.

## Setting CMS and CDH logs to use syslog streaming

To stream Navigator audit logs to an external syslog server, you need this in the safety valve for Navigator Audit Server logging:

log4j.logger.auditStream = TRACE,SYSLOG

log4j.additivity.auditStream = false

log4j.appender.SYSLOG = org.apache.log4j.net.SyslogAppender

log4j.appender.SYSLOG.SyslogHost = <syslog host>

log4j.appender.SYSLOG.Facility = Local2

log4j.appender.SYSLOG.FacilityPrinting = true

## CM 4.5 issue with Talend and Flume starving SMON and HMON services

In CM 4.5 on Burrito we found the heavy loads of Talend and Flume were effectively starving the service monitor (SMON) and Host Monitor (HMON) services causing them to crash. These admin services should ideally be on a ‘pure’ admin machine where this can not happen. An increased RAM allocation for these services will also help to reduce the crash occurrences. Upgrading to CM 5 should also fix this issue.

Set RAM to 4GB for SMON and HMON services

## Limiting the use of /tmp

AT Citi the use of /tmp is not to be encouraged. Any default use of /tmp should be moved to an alternate location where possible.

Within CMS default locatiosn in /tmp are to be found in multiple configuration locations. These should be replaced with /var/crash /data/1/tmp or some other dedicated space.

Make changes to the configuration of all locations where /tmp is used e.g.   
mgmt. – heap dump directory

**Heap Dump Directory**

Activity Monitor Default Group

Alert Publisher Default Group

Event Server Default Group

Host Monitor Default Group

Navigator Audit Server Default Group

Navigator Metadata Server Default Group

Reports Manager Default Group

Service Monitor Default Group

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it doesn't exist. However, if this directory already exists, role user must have write access to this directory. If this directory is shared amongst multiple roles, it should have 1777 permissions. Note that the heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

HUE – DB Dump file  
HUE – HDFS temp dir

**HDFS Temporary Directory**

temp\_dir

hue1 (Service-Wide)

HDFS directory used for storing temporary files.

**Database Dump File**

hue1 (Service-Wide)

File where the database gets dumped to or loaded from.

HBase – Heap Dump Dir

HBase – Hbase Secure Bulk Loading dir

**Heap Dump Directory**

HBase REST Server Default Group

HBase Thrift Server Default Group

Master Default Group

RegionServer Default Group

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it doesn't exist. However, if this directory already exists, role user must have write access to this directory. If this directory is shared amongst multiple roles, it should have 1777 permissions. Note that the heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

**HBase Secure Bulk Load Directory**

hbase.bulkload.staging.dir

RegionServer Default Group

The directory for HBase secure bulk Load.

HDFS – HDFS Health Canary dir

**Temporary Dump Directory**

dfs.nfs3.dump.dir

NFS Gateway Default Group

NFS clients often reorder writes. As a result, sequential writes can arrive at the NFS Gateway in random order. This directory is used to temporarily save out-of-order writes before writing to HDFS. For each file, the out-of-order writes are dumped after they are accumulated to exceed certain threshold (e.g., 1MB) in memory. Please make sure this directory has enough space. For example, if the application uploads 10 files with each having 100MB, it is recommended that this directory have roughly 1GB of space in case write reorder happens (in the worst case) to every file.

**Heap Dump Directory**

DataNode (h1)

DataNode (i1)

DataNode Default Group

Failover Controller Default Group

HttpFS Default Group

JournalNode Default Group

NFS Gateway Default Group

NameNode Default Group

SecondaryNameNode Default Group

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it doesn't exist. However, if this directory already exists, role user must have write access to this directory. If this directory is shared amongst multiple roles, it should have 1777 permissions. Note that the heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

**Event Filter**

navigator.event.filter

hdfs1 (Service-Wide)

View as JSON

 Action: discard Fields: username: (?:cloudera-scm|hbase|mapred|hive|dr.who|solr|impala)(?:/.+)?

Action: discard Fields: src: /tmp(?:/.\*)?

 Action: discard Fields: operation: listStatus

Default action

Event filters are defined in a JSON object like the following:

{

"defaultAction" : ("accept", "discard"),

"rules" : [

{

"action" : ("accept", "discard"),

"fields" : [

{

"name" : "fieldName",

"match" : "regex"

}

]

}

]

}

A filter has a default action and a list of rules, in order of precedence. Each rule defines an action, and a list of fields to match against the audit event.

A rule is "accepted" if all the listed field entries match the audit event. At that point, the action declared by the rule is taken.

If no rules match the event, the default action is taken. Actions default to "accept" if not defined in the JSON object.

The following is the list of fields that can be filtered for HDFS events:

* username: the user performing the action.
* ipAddress: the IP from where the request originated.
* command: the HDFS operation being performed.
* src: the source path for the operation.
* dest: the destination path for the operation.
* permissions: the permissions associated with the operation.

**HDFS Health Canary Directory**

hdfs1 (Service-Wide)

The service monitor will use this directory to create files to test if the hdfs service is healthy. The directory and files are created with permissions specified by 'HDFS Health Canary Directory Permissions'

YARN – Remote App Log dir  
YARN – Heap Dump dir  
YARN – M/R Task Java Opts Base – if used

**Remote App Log Directory**

yarn.nodemanager.remote-app-log-dir

NODEMANAGER Imported From: TaskTracker (h1)

NODEMANAGER Imported From: TaskTracker (i1)

NODEMANAGER Imported From: TaskTracker (i2)

NODEMANAGER Imported From: TaskTracker Default Group

HDFS directory where application logs are stored when an application completes.

**Heap Dump Directory**

JOBHISTORY Imported From: JobTracker Default Group

NODEMANAGER Imported From: TaskTracker (h1)

NODEMANAGER Imported From: TaskTracker (i1)

NODEMANAGER Imported From: TaskTracker (i2)

NODEMANAGER Imported From: TaskTracker Default Group

RESOURCEMANAGER Imported From: JobTracker Default Group

Path to directory where heap dumps are generated when java.lang.OutOfMemoryError error is thrown. This directory is automatically created if it doesn't exist. However, if this directory already exists, role user must have write access to this directory. If this directory is shared amongst multiple roles, it should have 1777 permissions. Note that the heap dump files are created with 600 permissions and are owned by the role user. The amount of free space in this directory should be greater than the maximum Java Process heap size configured for this role.

## HDFS log files

You can limit the retention of the hdfs audit logs using a safety valve entry. The sample safety valve entry below will set a max of 20 512MB files (10GB). It will auto-purge any overage, which means on a very active system you may want to increase the numbers, for example, in our UAT environment the NN writes about 50GB of audit logs per week. While it is possible to filter Navigator audits, it is not possible to do so with the file system logs.

NameNode (Default) / Advanced / NameNode Logging Safety Valve

hdfs.audit.log.maxfilesize=512MB

hdfs.audit.log.maxbackupindex=20

log4j.logger.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=${log.threshold}, RFAAUDIT, Navigator

log4j.additivity.org.apache.hadoop.hdfs.server.namenode.FSNamesystem.audit=false

log4j.appender.RFAAUDIT=org.apache.log4j.RollingFileAppender

log4j.appender.RFAAUDIT.File=${log.dir}/hdfs-audit.log

log4j.appender.RFAAUDIT.layout=org.apache.log4j.PatternLayout

log4j.appender.RFAAUDIT.layout.ConversionPattern=%d{ISO8601} %p %c{2}: %m%n

log4j.appender.RFAAUDIT.MaxFileSize=${hdfs.audit.log.maxfilesize}

log4j.appender.RFAAUDIT.MaxBackupIndex=${hdfs.audit.log.maxbackupindex}

## HDFS Extended ACL’s

### Enabling HDFS Extended ACLs

As of CDH 5.1, HDFS supports POSIX Access Control Lists (ACLs), in addition to the traditional POSIX permissions model already supported. ACLs provide fine-grained control of permissions for HDFS files by providing a way to set different permissions for specific named users or named groups.

### Enabling ACLs

By default, ACLs are disabled on a cluster. To enable them, set the dfs.namenode.acls.enabled property to true in the NameNode's hdfs-site.xml.

Using Cloudera Manager go to HDFS service configuration and search for ACL then use the check box to select “TRUE”

| **Category** | **Property** | **Value** | **Description** |
| --- | --- | --- | --- |
| [**Service-Wide / Security**](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/42/config) | **Enable Access Control Lists**  dfs.namenode.acls.enabled | [Reset to the default value: false](https://bdgtr002d51h1l.nam.nsroot.net:7183/cmf/services/42/config) | ACLs (Access Control Lists) enhance the existing HDFS permission model to support controlling file access for arbitrary combinations of users and groups instead of a single owner, single group, and all other users. When ACLs are disabled, the NameNode rejects all attempts to set an ACL. |

### Commands

You can use the File System Shell commands, setfacl and getfacl, to modify and retrieve files' ACLs.

#### getfacl

hdfs dfs -getfacl [-R] <path>

<!-- COMMAND OPTIONS

<path>: Path to the file or directory for which ACLs should be listed.

-R: Use this option to recursively list ACLs for all files and directories.

-->

**Examples:**

<!-- To list all ACLs for the file located at /user/hdfs/file -->

hdfs dfs -getfacl /user/hdfs/file

<!-- To recursively list ACLs for /user/hdfs/file -->

hdfs dfs -getfacl -R /user/hdfs/file

#### setfacl

hdfs dfs -setfacl [-R] [-b|-k -m|-x <acl\_spec> <path>]|[--set <acl\_spec> <path>]

<!-- COMMAND OPTIONS

<path>: Path to the file or directory for which ACLs should be set.

-R: Use this option to recursively list ACLs for all files and directories.

-b: Revoke all permissions except the base ACLs for user, groups and others.

-k: Remove the default ACL.

-m: Add new permissions to the ACL with this option. Does not affect existing permissions.

-x: Remove only the ACL specified.

<acl\_spec>: Comma-separated list of ACL permissions.

--set: Use this option to completely replace the existing ACL for the path specified.

Previous ACL entries will no longer apply.

-->

**Examples:**

<!-- To give user ben read & write permission over /user/hdfs/file -->

hdfs dfs -setfacl -m user:ben:rw- /user/hdfs/file

<!-- To remove user alice's ACL entry for /user/hdfs/file -->

hdfs dfs -setfacl -x user:alice /user/hdfs/file

<!-- To give user hadoop read & write access, and group or others read-only access -->

hdfs dfs -setfacl --set user:hadoop:rw-,group::r--,other::r-- /user/hdfs/file

More details about using this feature can be found [**here**](http://hadoop.apache.org/docs/r2.4.0/hadoop-project-dist/hadoop-hdfs/HdfsPermissionsGuide.html#ACLs_Access_Control_Lists).

## CMS Monitor Stability Issues

Cloudera Manager Service Monitor may intermittently ‘lock up’ and show invalid status for HDFS and other services. Extract from Cloudera Support case:

Going by the SMON log, the NN in target appears to lock itself every now and then for a period longer than 1m, such that the /jmx endpoint poller ends up with a read-timed-out issue after a connection is made. What we like you to try is have SMON and agents be more patient with responses by raising its http timeouts. This can be done as below:

**Add a safety valve entry for Service Monitor**

CM -> Management Services -> Configuration -> "Service Monitor Configuration Safety Valve for cmon.conf"

<property>

<name>namenode.jmx.query.timeout</name>

<value>180000</value>

</property>

Restart Service Monitor role

“And for the agent's own poller, within the NameNode's /etc/cloudera-scm-agent/config.ini file, find and raise the metrics\_url\_timeout\_seconds line to:

metrics\_url\_timeout\_seconds=180.0

Restart agent via “service cloudera-scm-agent restart”

## Map Reduce MR1 Job Management ID’s

Set which ID’s can manage jobs by including them in a list of admin ID’s for Job Tracker Jobs.

By default only the owner of the job can manage it.

To change this situation, Enable the check box ‘mapred.acls.enabled’ and update the safety valve entry as follows:

The > < should be replaced with a valid comma delimited list of users who should have admin access on all jobs

<?xml version="1.0"?>

<?xml-stylesheet type="text/xsl" href="configuration.xsl"?>

<configuration>

  <property>

    <name>mapred.queue.default.acl-submit-job</name>

    <value>\*</value>

  </property>

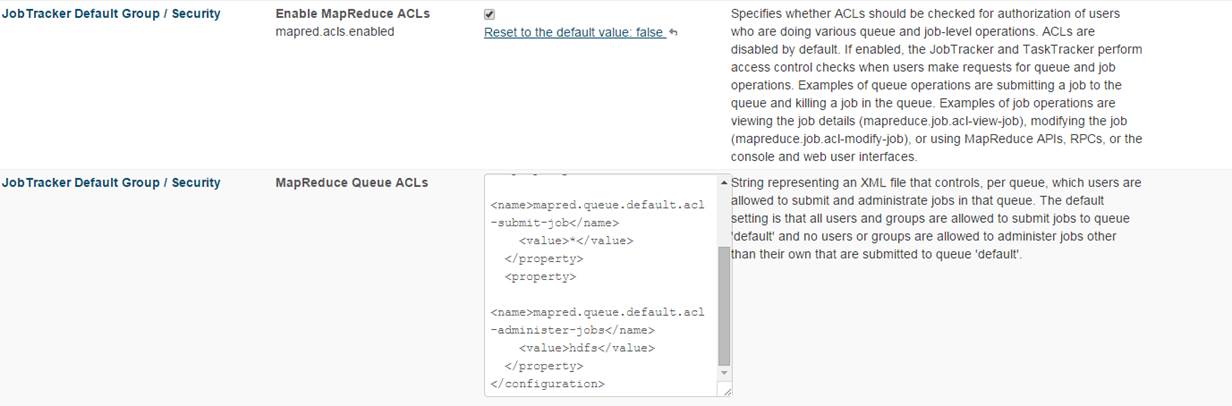
  <property>

    <name>mapred.queue.default.acl-administer-jobs</name>

    <value>hdfs, admin0001, admin0002 </value>

  </property>

</configuration>



## Add your custom configurations here – one heading per change

Details of the change

## Known Issues

### HUE has a known issue that is scheduled to be fixed in HUE 3.8.

HUE logs ‘false positive’ error messages. These error messages can safely be ignored and look something like

kerberos\_ ERROR handle\_other(): Mutual authentication unavailable on 200 response

### Beeline gives error of hiveconf not found

To reproduce:

#beeline

-hiveconf (No such file or directory)

This is related to  (hiveconf option is not supported for beeline), but it has additional problem in hive script where option -hiveconf should be --hiveconf (double dashes).

Fixed in [HIVE-6340.patch](https://issues.apache.org/jira/secure/attachment/12626446/HIVE-6340.patch) 01/Feb/14 03:29

Issue Links

Improvement - An improvement or enhancement to an existing feature or task. [~~HIVE-6173~~](https://issues.apache.org/jira/browse/HIVE-6173) Beeline doesn't accept --hiveconf option as Hive CLI does

* **RESOLVED**

Improvement - An improvement or enhancement to an existing feature or task. [~~HIVE-6173~~](https://issues.apache.org/jira/browse/HIVE-6173) Beeline doesn't accept --hiveconf option as Hive CLI does

* **RESOLVED**

### C 5.4 known Installation Issues

#### — No in-place upgrade to CDH 5 from CDH 4

Cloudera fully supports upgrade from Cloudera Enterprise 4 and CDH 4 to Cloudera Enterprise 5. Upgrade requires uninstalling the CDH 4 packages before installing CDH 5 packages. See the [CDH 5 upgrade documentation](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_cdh4_to_cdh5_upgrade.html#topic_6_unique_2) for instructions.

#### — Upgrading to CDH 5.4 or later requires an HDFS upgrade

Upgrading to CDH 5.4.0 or later from an earlier CDH 5 release requires an HDFS upgrade, and upgrading from a release earlier than CDH 5.2.0 requires additional steps. See [Upgrading from an Earlier CDH 5 Release to the Latest Release](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_upgrade_5_to_latest.html) for further information. See also [What's New in CDH 5.4.0](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_rn_new_in_540.html).

#### — Upgrading from CDH 4 requires an HDFS upgrade

Upgrading from CDH 4 requires an HDFS upgrade. See [Upgrading from CDH 4 to CDH 5](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_cdh4_to_cdh5_upgrade.html#topic_6_unique_2) for further information. See also [What's New in CDH 5.4.0](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_rn_new_in_540.html).

#### — CDH 5 requires JDK 1.7

JDK 1.6 is not supported on any CDH 5 release, but before CDH 5.4.0, CDH libraries have been compatible with JDK 1.6. As of CDH 5.4.0, CDH libraries are no longer compatible with JDK 1.6 and **applications using CDH libraries must use JDK 1.7.**

In addition, you must upgrade your cluster to a [supported version](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_ig_req_supported_versions.html#concept_pdd_kzf_vp_unique_1) of JDK 1.7 before upgrading to CDH 5. See [Upgrading to Oracle JDK 1.7 before Upgrading to CDH 5](http://www.cloudera.com/content/cloudera/en/documentation/core/latest/topics/cdh_cm_upgrading_to_jdk7.html) for instructions.

#### — No upgrade directly from CDH 3 to CDH 5

You must upgrade to CDH 4, then to CDH 5. See the [CDH 4 documentation](http://www.cloudera.com/content/cloudera-content/cloudera-docs/CDH4/latest/CDH4-Installation-Guide/cdh4ig_topic_6.html) for instructions on upgrading from CDH 3 to CDH 4.

#### ***After upgrading from a release earlier than CDH 4.6, you may see reports*** of corrupted files

Some older versions of CDH do not handle DataNodes with a large number of blocks correctly. The problem exists on versions 4.6, 4.7, 4.8, 5.0, and 5.1. The symptom is that the NameNode Web UI and the fsck command incorrectly report missing blocks, even when those blocks are present.

The cause of the problem is that if the DataNode attempts to send a block report that is larger than the maximum RPC buffer size, the NameNode rejects the report. This prevents the NameNode from becoming aware of the blocks on the affected DataNodes. The maximum buffer size is controlled by the ipc.maximum.data.length property, which defaults to 64 MB.

This problem does not exist in CDH 4.5 and earlier because there is no maximum RPC buffer size in these versions. Starting in CDH5.2, DataNodes now send individual block reports for each storage volume, which mitigates the problem.

**Bug:** [HADOOP-9676](https://issues.apache.org/jira/browse/HADOOP-9676)

**Severity:** Medium

**Workaround:** Immediately after upgrading, increase the value of ipc.maximum.data.length; Cloudera recommends doubling the default value, from 64 MB to 128 MB:

<property>

<name>ipc.maximum.data.length</name>

<value>134217728</value>

</property>

* In a Cloudera Manager installation, set this property in the hdfs\_service\_config\_safety\_valve.
* In a command-line-only installation, add and set this property in core-site.xml.

After setting ipc.maximum.data.length, restart the NameNode(s).

#### —Must build native libraries when installing from tarballs

When installing Hadoop from Cloudera tarballs, you must build your own native libraries. The tarballs do not include libraries that are built for the different distributions and architectures.