HORTONWORKS HDP WITH ECS CONFIGURATION AND BEST PRACTICES GUIDE

ABSTRACT

This white paper describes the configuration and best practices for using Hortonworks HDP with EMC ECS.

August, 2015

REDEFINE

EMC WHITE

EMC²

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller, visit www.emc.com, or explore and compare products in the EMC Store

Part Number HXXXXX <required, see Part numbers below for more info>

TABLE OF CONTENTS

PRODUCT VERSIONS

This document applies to following product versions.

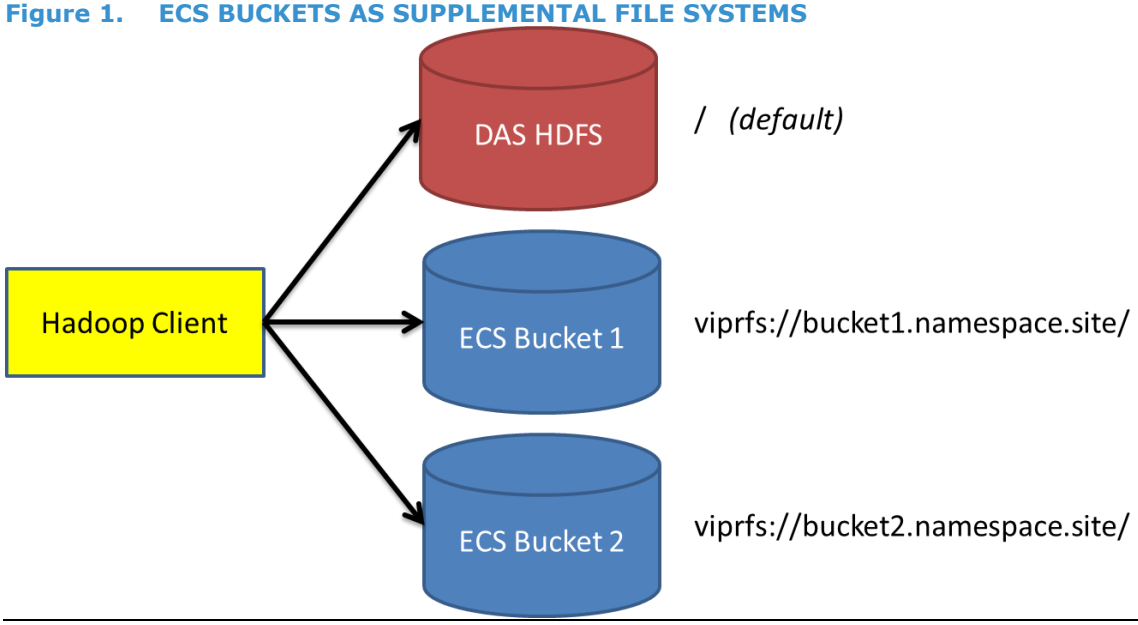
Table 1 PRODUCT VERSIONS

PRODUCT	VERSION
Hortonworks HDP	2.2.6.0-2800
Ambari	2.0.1
CentOS	6.6
ECS	2.0.1.0-427.6d6535a
ViPRFS Client	1.2.0.0-hadoop-2.3

DEPLOYMENT OPTIONS

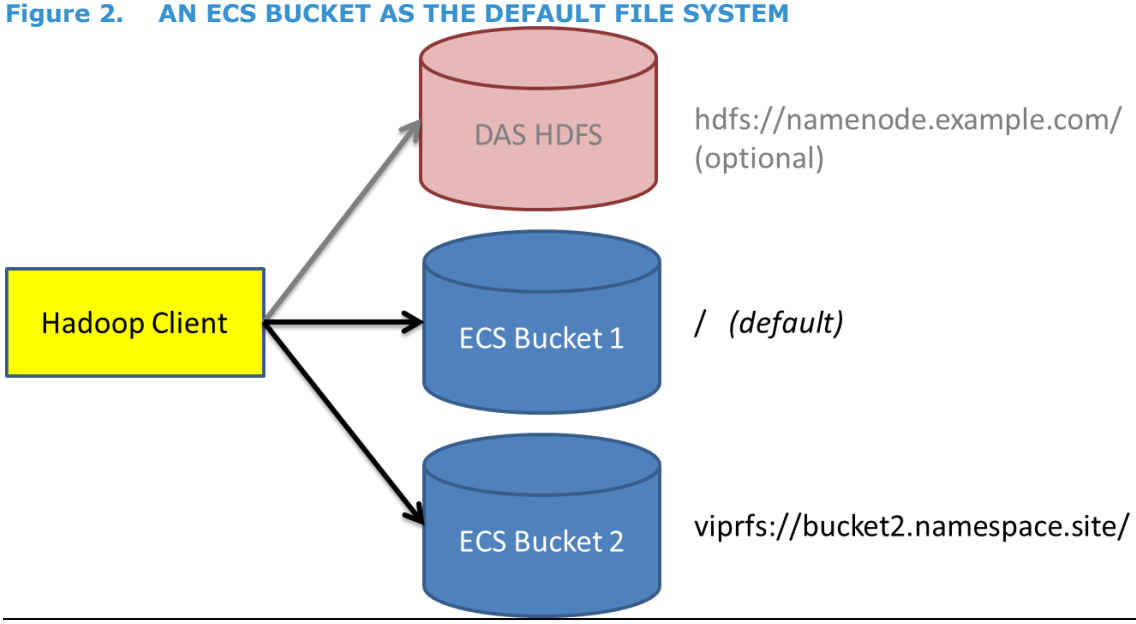
ECS buckets can be used as supplemental or auxiliary file systems. In this scenario, fs.defaultFS in core-site.xml remains as the default and references the HDFS NameNode. Applications can access data in any ECS bucket by using fully-qualified paths in the format "viprfs://bucket.namespace.site/". Jobs and applications may need to be reconfigured or updated to use a fully-qualified path. This is the recommended configuration and is what this document describes.

Figure 1. ECS BUCKETS AS SUPPLEMENTAL FILE SYSTEMS



An ECS bucket can be used as the default file system in Hadoop, in which all Hadoop paths without an explicit URI prefix such as "hdfs://" refer to objects in a single ECS bucket. In this scenario, fs.defaultFS in core-site.xml is set to "viprfs://bucket.namespace.site/". Data on the traditional HDFS NameNode and DataNodes will be accessible by using the fully-qualified URI such as "hdfs://namenode.example.com/". Some applications that require the Apache HDFS implementation will not work in this Hadoop cluster.

Figure 2. AN ECS BUCKET AS THE DEFAULT FILE SYSTEM



The default authentication in Hadoop is called standard authentication. Standard authentication provides minimal security and is intended to run in an environment where everyone with network access to the Hadoop nodes can be trusted. Environments with untrusted users should use Kerberos to protect access to sensitive data.

COMPATIBLE HADOOP COMPONENTS

The following matrix lists the compatible Hadoop components for the product versions that this document applies to.

Table 2 COMPATIBLE HADOOP COMPONENTS

	NON-KERBEROS	KERBEROS
ECS AS DEFAULT FILE SYSTEM	MapReduce, Pig, Hive, HBase	MapReduce
ECS AS SUPPLEMENTAL FILE SYSTEM	MapReduce, Pig, Hive, HBase	MapReduce, Pig

INSTALLATION OVERVIEW (NON-KERBEROS)

The installation of Hortonworks HDP in an ECS environment with standard Hadoop authentication (non-Kerberos) is composed of the following general steps.

1. Deploy a standard HDP cluster. This will use local disks (DAS), not ECS storage, for HDFS.
2. Configure users and buckets on ECS.
3. Configure the ECS client on the HDP nodes.
4. Optionally relocate selected Hadoop services from DAS HDFS to ECS storage.

INSTALLATION PROCEDURE (NON-KERBEROS)

DEPLOY HORTONWORKS HDP

Complete details for this procedure can be found at http://docs.hortonworks.com/HDPDocuments/Ambari-2.0.1.0/bk_Installing_HDP_AMB/content/_download_the_ambari_repo.html. A concise list of steps is shown below.

```
[root@mycluster1-master-0 ~]#
```

```
wget -nv http://public-repo-1.hortonworks.com/ambari/centos6/2.x/updates/2.0.1/ambari.repo -O
/etc/yum.repos.d/ambari.repo

yum install -y ambari-server

ambari-server setup

ambari-server start
```

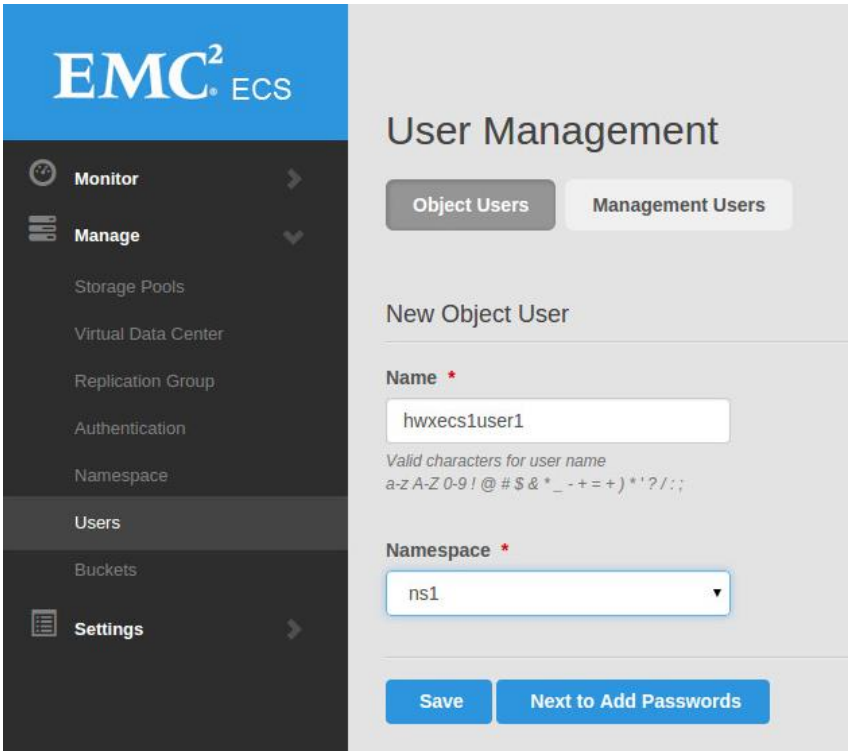
Complete the installation using the Ambari Install Wizard as documented at http://docs.hortonworks.com/HDPDocuments/Ambari-2.0.1.0/bk_Installing_HDP_AMB/content/ch_Deploy_and_Configure_a_HDP_Cluster.html.

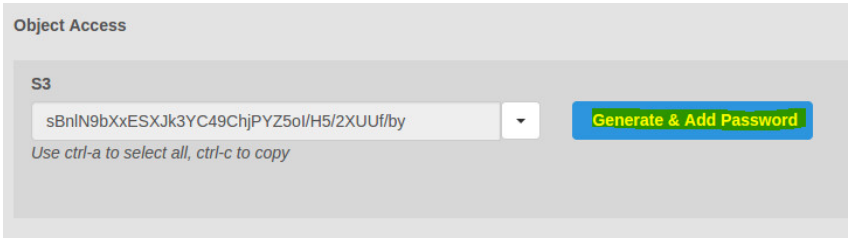
CONFIGURE ECS (NON-KERBEROS)

This document assumes that an ECS cluster has been installed and configured, and is ready for users and buckets to be created. For complete details, refer to ECS Step-by-Step (https://community.emc.com/docs/DOC-45299). Additional details are available at http://www.emc.com/techpubs/ecs/ecs_hdfs_configure-1.htm.

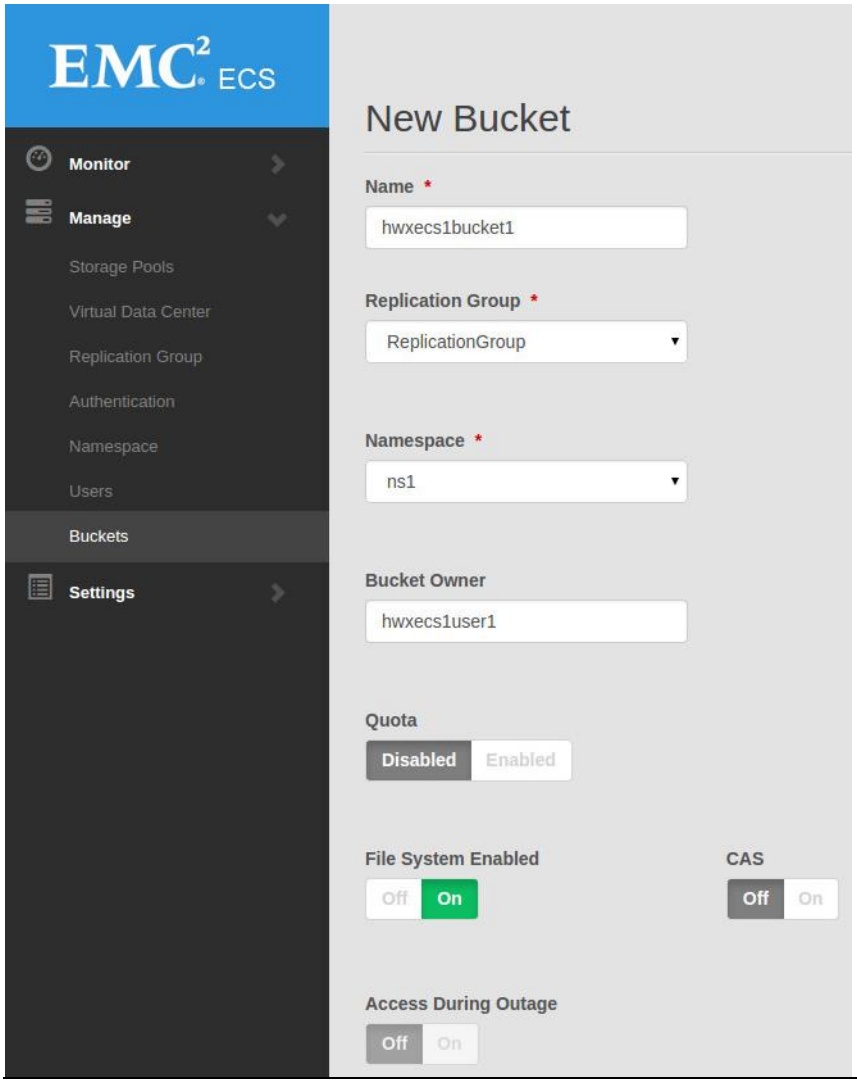
This section describes the process when using a Hadoop cluster with standard authentication, not Kerberos.

First, create an object user that will be the owner of the ECS bucket that we will use for our Hadoop data. Generate and add an S3 password. For complete details, refer to http://www.emc.com/techpubs/ecs/users_authprov_and_mapping-1.htm.

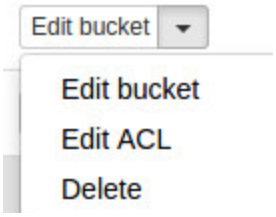


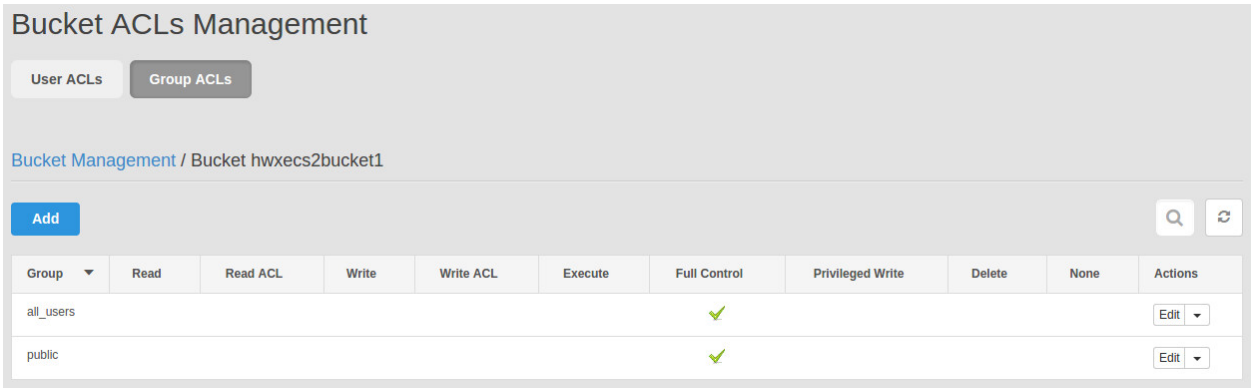


Next, create a bucket owned by the new object user. To allow HDFS access, you must set *File System Enabled* to On.



Next, edit the bucket ACL to allow the all_users and public groups Full Control. This is required for non-Kerberos access.





CONFIGURE ECS CLIENT ON HDP NODES

The ECS client is a JAR library that allows Hadoop applications access the bucket on an ECS cluster. It is implemented as a Hadoop Compatible File System and uses the prefix "viprfs://". Installation of the ECS client consist of copying the .jar file to each Hadoop node and adding properties to the Hadoop configuration files.

Additional details are available at http://www.emc.com/techpubs/ecs/ecs_hdfs_configure-1.htm.

The following Hadoop properties should be set.

Table 3 Hadoop configuration and tuning recommendations relevant to the validation process

LOCATION	PROPERTY	VALUE
core-site	fs.viprfs.impl	com.emc.hadoop.fs.vipr.ViPRFileSystem
core-site	fs.AbstractFileSystem.viprfs.impl	com.emc.hadoop.fs.vipr.ViPRAbstractFileSystem
hdfs-site	fs.permissions.umask-mode	022
core-site	fs.viprfs.auth.identity_translation	NONE
core-site	fs.viprfs.auth.anonymous_translation	CURRENT_USER
core-site	fs.vipr.installations	site1 (this can be any name and will be referred to as $SITE)
core-site	fs.vipr.installation.$SITE.hosts	(comma-separated list of FQDN or IP address of each ECS host)
core-site	fs.vipr.installation.$SITE.hosts.resolution	dynamic
core-site	fs.vipr.installation.$SITE.resolution.dynamic.time_to_live_ms	900000
yarn-site	yarn.application.classpath	Append the following: /usr/lib/hadoop/lib/*
mapred-site	mapreduce.application.classpath	Append the following: /usr/lib/hadoop/lib/*
tez-site	tez.cluster.additional.classpath.prefix	Append the following: /usr/lib/hadoop/lib/*
HDFS	hadoop-env template	Append the following: export HADOOP_CLASSPATH=${HADOOP_CLASSPATH}:/usr/lib/hadoop/lib/*

These properties can be set using the Ambari UI or by running the following commands on the host running Ambari.

```
[root@mycluster1-master-0 ~]#
```

```
CLUSTER_NAME=mycluster1

ECS_HOSTS=ecs1-1.example.com,ecs1-2.example.com,ecs1-3.example.com,ecs1-4.example.com

SITE=site1

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.viprfs.impl com.emc.hadoop.fs.vipr.ViPRFileSystem

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.AbstractFileSystem.viprfs.impl com.emc.hadoop.fs.vipr.ViPRAbstractFileSystem

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME hdfs-site
fs.permissions.umask-mode 022

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.viprfs.auth.identity_translation NONE

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.viprfs.auth.anonymous_translation CURRENT_USER

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.vipr.installations $SITE

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.vipr.installation.$SITE.hosts $ECS_HOSTS

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.vipr.installation.$SITE.hosts.resolution dynamic

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.vipr.installation.$SITE.resolution.dynamic.time_to_live_ms 900000

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.application.classpath \

'$HADOOP_CONF_DIR,/usr/hdp/current/hadoop-client/*,/usr/hdp/current/hadoop-
client/lib/*,/usr/hdp/current/hadoop-hdfs-client/*,/usr/hdp/current/hadoop-hdfs-
client/lib/*,/usr/hdp/current/hadoop-yarn-client/*,/usr/hdp/current/hadoop-yarn-
client/lib/*,/usr/lib/hadoop/lib/*'

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME mapred-site
mapreduce.application.classpath \

'$PWD/mr-framework/hadoop/share/hadoop/mapreduce/*:$PWD/mr-
framework/hadoop/share/hadoop/mapreduce/lib/*:$PWD/mr-framework/hadoop/share/hadoop/common/*:$PWD/mr-
framework/hadoop/share/hadoop/common/lib/*:$PWD/mr-framework/hadoop/share/hadoop/yarn/*:$PWD/mr-
framework/hadoop/share/hadoop/yarn/lib/*:$PWD/mr-framework/hadoop/share/hadoop/hdfs/*:$PWD/mr-
framework/hadoop/share/hadoop/hdfs/lib/*:/usr/hdp/${hdp.version}/hadoop/lib/hadoop-lzo-
0.6.0.${hdp.version}.jar:/etc/hadoop/conf/secure:/usr/lib/hadoop/lib/*'

/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME tez-site
tez.cluster.additional.classpath.prefix \

'/usr/hdp/${hdp.version}/hadoop/lib/hadoop-lzo-
0.6.0.${hdp.version}.jar:/etc/hadoop/conf/secure:/usr/lib/hadoop/lib/*'
```

Note that the property change for hadoop-env template is not in the script above. This property should be edited using the Ambari UI.

Next, extract the contents of hdfsclient-1.2.0.0-1380.zip. Copy the files viprfs-client-1.2.0.0-hadoop-2.3.jar and libvipr-1.2.0.0.so to /usr/lib/hadoop/lib on all HDP nodes. Note that this destination directory was added to all relevant class paths.

Finally, use Ambari to stop all services and then start them.

At this point, all Hadoop applications will have the ability to access ECS using the viprfs prefix, although no applications or services will attempt to yet. So far, all data remains on the DAS HDFS that was created during the HDP installation.

CHECK HDFS ACCESS TO ECS

Once all Hadoop services have started (actually just the client configurations need to be refreshed), ensure that the ECS bucket can be accessed using the Hadoop CLI. The URI will be of the form viprfs://*bucket*.*namespace*.*site*/. In the example commands below, first, a directory listing is attempted. A new bucket will be empty and nothing will be returned. Then an empty file is created, followed by another directory listing.

```
[root@mycluster1-master-0 ~]# hdfs dfs -ls viprfs://mycluster1bucket1.ns1.ecs1/
[root@mycluster1-master-0 ~]# hdfs dfs -touchz
viprfs://mycluster1bucket1.ns1.ecs1/THIS_IS_mycluster1bucket1
[root@mycluster1-master-0 ~]# hdfs dfs -ls viprfs://mycluster1bucket1.ns1.ecs1/
Found 1 items
-rw-------   1 root          0 2015-08-26 19:05
viprfs://mycluster1bucket1.ns1.ecs1/THIS_IS_mycluster1bucket1
```

RELOCATE HADOOP SERVICES TO ECS

In this configuration, the default file system (fs.defaultFS in core-site.xml) remains as the DAS HDFS NameNode. To access data on ECS, the fully-qualified path with the viprfs prefix must be specified in the application. This section provides details on specific applications.

RELOCATE HIVE TO ECS

To have existing Hive tables on the default file system and other tables on ECS, the only requirement is to use an external table with a fully-qualified path as the table's location. However, to have the default Hive warehouse located on ECS, the configuration steps below can be used. This will direct all new non-external Hive tables to be created on ECS.

```
[root@mycluster1-master-0 ~]# CLUSTER_NAME=mycluster1
[root@mycluster1-master-0 ~]# FS=viprfs://mycluster1bucket1.ns1.ecs1
[root@mycluster1-master-0 ~]# /var/lib/ambari-server/resources/scripts/configs.sh set localhost
$CLUSTER_NAME hive-site hive.metastore.warehouse.dir $FS/apps/hive/warehouse
```

For the change to take effect, use Ambari to restart all Hive services.

RELOCATE HBASE TO ECS

Unlike MapReduce and Hive, the HBase service stores its data in a single Hadoop directory tree. The steps below will configure HBase to use ECS for its data.

WARNING!!! DO NOT USE THIS PROCEDURE IF YOU ALREADY HAVE DATA IN HBASE. ANY EXISTING DATA WILL BECOME INACCESSIBLE AND POSSIBLY LOST FORVER USING THIS PROCEDURE.

Using Ambari, Stop HBase services.

```
[root@mycluster1-master-0~]# CLUSTER_NAME=mycluster1
[root@mycluster1-master-0~]# FS=viprfs://mycluster1bucket1.ns1.ecs1
[root@mycluster1-master-0~]# /var/lib/ambari-server/resources/scripts/configs.sh set localhost
$CLUSTER_NAME hbase-site hbase.rootdir $FS/apps/hbase/data
[root@mycluster1-master-0~]# hbase zkcli
[zk] rmr /hbase-unsecure
[zk] quit
```

Using Ambari, Start HBase services.

INSTALLATION OVERVIEW (KERBEROS)

This section is intended for the following deployment scenario:

- An MIT KDC server will be used to authenticate all Hadoop services and built-in accounts such as hdfs and ambari-qa.
- A Windows 2008 R2 Active Directory will be used to authenticate all other user accounts.
- The MIT KDC server will delegate user authentication requests to Active Directory.

The installation of Hortonworks HDP in an ECS environment with Kerberos authentication is composed of the following general steps.

1. Deploy a non-Kerberos Hadoop cluster with ECS
2. Deploy an MIT KDC server.
3. Configure Active Directory.
4. Enable Kerberos using Ambari.
5. Configure ECS for Kerberos and Active Directory.
6. Create users and buckets on ECS.
7. Reconfigure the ECS client on the HDP nodes for Kerberos.

In the subsequent sections, the environment-specific settings listed below should be changed to match the desired target environment.

Table 4 Kerberos-related Example Environment

DESCRIPTION	EXAMPLE VALUE
AD (Active Directory) Domain	solarch.local
AD domain controller host name	dc-01.solarch.local
AD Kerberos Realm	SOLARCH.LOCAL
MIT KDC Kerberos Realm	KR.SOLARCH.LOCAL
MIT KDC host name	kdc-1.solarch.local
Kerberos Encryption Types	aes256-cts-hmac-sha1-96

INSTALLATION PROCEDURE (KERBEROS)

DEPLOY A NON-KERBEROS CLUSTER WITH ECS

Due to the significant complexity of a Kerberos environment, it is highly recommended to get a complete environment running without Kerberos prior to enabling it.

Perform all steps in the following sub-sections of **Installation Procedure (Non-Kerberos)**:

- Deploy Hortonworks HDP
- Configure ECS
- Configure ECS Client on HDP Nodes
- Check HDFS Access to ECS

DEPLOY AN MIT KDC SERVER

Complete details for this procedure can be found at http://docs.hortonworks.com/HDPDocuments/Ambari-2.0.1.0/bk_Ambari_Security_Guide/content/_optional_install_a_new_mit_kdc.html. A concise list of steps is shown below.

On the server that will be the MIT KDC server:

```
[root@kdc-1 ~]#
yum install krb5-server krb5-libs krb5-auth-dialog krb5-workstation
```

Create the file /etc/krb5.conf with contents shown:

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log
[libdefaults]
 default_realm = KR.SOLARCH.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 1000d
 renew_lifetime = 1000d
 forwardable = true
 default_tkt_enctypes = aes256-cts-hmac-sha1-96
 default_tgs_enctypes = aes256-cts-hmac-sha1-96
[realms]
 KR.SOLARCH.LOCAL = {
  kdc = kdc-1.solarch.local
  admin_server = kdc-1.solarch.local
 }
 SOLARCH.LOCAL = {
  kdc = dc-01.solarch.local
  admin_server = dc-01.solarch.local
 }
[domain_realm]
kr.solarch.local = KR.SOLARCH.LOCAL
.kr.solarch.local = KR.SOLARCH.LOCAL
```

Create the file /var/kerberos/krb5kdc/kdc.conf with contents shown:

```
[kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88
[realms]
 KR.SOLARCH.LOCAL = {
  acl_file = /var/kerberos/krb5kdc/kadm5.acl
```

```
  dict_file = /usr/share/dict/words
  admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
  supported_enctypes = aes256-cts-hmac-sha1-96:normal
 }
```

Create the file /var/kerberos/krb5kdc/kadm5.acl with contents shown:

```
*/admin@KR.SOLARCH.LOCAL    *
```

Initialize the MIT KDC.

```
[root@kdc-1 ~]#
mv /dev/random /dev/random.orig
ln -s /dev/urandom /dev/random
kdb5_util create -s
KDC database master password: <enter new KDC master password>
service krb5kdc start
service kadmin start
chkconfig krb5kdc on
chkconfig kadmin on
kadmin.local -q "addprinc admin/admin"
admin/admin password: <enter new admin/admin password>
```

Test admin/admin access to the MIT KDC.

```
[root@kdc-1 ~]#
kadmin -p admin/admin
Authenticating as principal admin/admin with password.
Password for admin/admin@KR.SOLARCH.LOCAL: <enter admin/admin password>
kadmin:  listprincs
K/M@KR.SOLARCH.LOCAL
admin/admin@KR.SOLARCH.LOCAL
kadmin/admin@KR.SOLARCH.LOCAL
kadmin/changepw@KR.SOLARCH.LOCAL
kadmin/kdc-1.solarch.local@KR.SOLARCH.LOCAL
krbtgt/KR.SOLARCH.LOCAL@KR.SOLARCH.LOCAL
kadmin:  exit
```

CONFIGURE ACTIVE DIRECTORY

This assumes that an Active Directory domain has already been created and is functioning normally.

Let Active Directory know about the MIT KDC.

```
C:\Windows\system32>
```

```
ksetup /addkdc KR.SOLARCH.LOCAL kdc-1.solarch.local
```

Create an account for the MIT KDC to authenticate users in AD.

```
C:\Windows\system32>
netdom trust KR.SOLARCH.LOCAL /Domain: solarch.local /add /realm /passwordt:<enter new trust password>
```

Set the Kerberos encryption type used by this account.

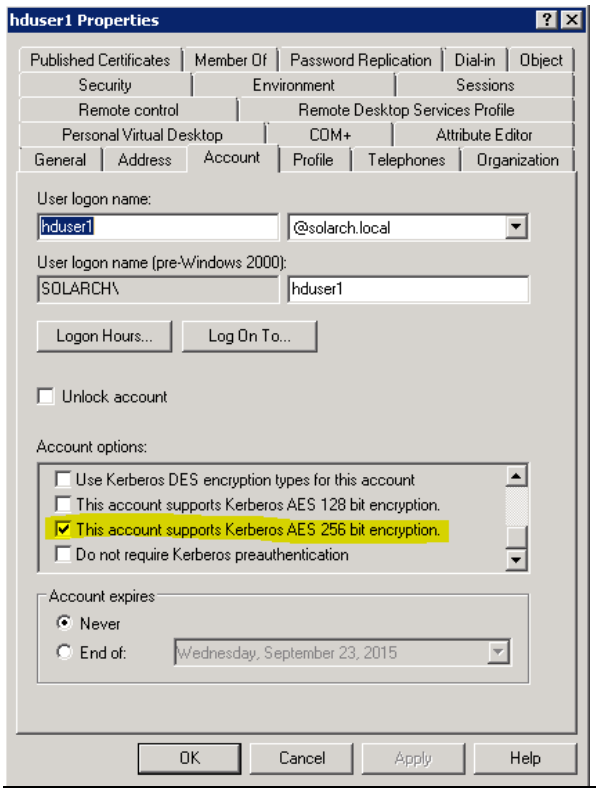
```
C:\Windows\system32>
ksetup /SetEncTypeAttr KR.SOLARCH.LOCAL AES256-CTS-HMAC-SHA1-96
```

Create the principal on MIT KDC to access the AD KDC.

```
[root@kdc-1 ~]# kadmin.local
kadmin.local: addprinc -e "aes256-cts-hmac-sha1-96:normal" krbtgt/KR.SOLARCH.LOCAL@SOLARCH.LOCAL
admin/admin password: <enter trust password>
```

ECS uses an AD account to lookup users and group. Create a normal AD user that will be used by ECS for this purpose. It is assumed that this user will be named "Manager".

Create or Enable User Accounts in Active Directory. Unless enabled by AD policies, each user account needs to be enabled to authenticate with Kerberos. This is done by checking the box "This account supports Kerberos AES 256 bit encryption" in the AD User Account properties.



CONFIRM KERBEROS AUTHENTICATION OF AD ACCOUNTS

Use the steps below to confirm that an AD user can be authenticated using Kerberos. Additionally, ensure that the encryption types match the expected value (aes256-cts-hmac-sha1-96 in this case).

```
[hduser1@kdc-1 ~]# kinit hduser1@SOLARCH.LOCAL
Password for hduser1@SOLARCH.LOCAL: <enter password for hduser1 as defined in AD>
[hduser1@kdc-1 ~]# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: hduser1@SOLARCH.LOCAL
Valid starting     Expires            Service principal
08/24/15 22:35:26  08/25/15 08:35:18  krbtgt/SOLARCH.LOCAL@SOLARCH.LOCAL
        renew until 08/31/15 22:35:26, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-
sha1-96
```

ENABLE KERBEROS USING AMBARI

Follow the procedure at http://docs.hortonworks.com/HDPDocuments/Ambari-2.0.1.0/bk_Ambari_Security_Guide/content/_running_the_kerberos_wizard.html.

The settings below have been tested successfully.

Table 5 Kerberos Settings in Ambari

PROPERTY	VALUE
KDC type	Existing MIT KDC
KDC host	kdc-1.solarch.local
Realm name	KR.SOLARCH.LOCAL
Domains	.kr.solarch.local,kr.solarch.local
Kadmin host	kdc-1.solarch.local
Admin principal	admin/admin@KR.SOLARCH.LOCAL
Encryption Types	aes256-cts-hmac-sha1-96
krb5-conf template	Add to [realms] section: **SOLARCH.LOCAL = {** **kdc = dc-01.solarch.local** **admin_server = dc-01.solarch.local** **}**
hadoop.security.auth_to_local	Add rule for @SOLARCH.LOCAL at appropriate position. Final value should be: RULE:[1:$1@$0](ambari-qa@KR.SOLARCH.LOCAL)s/.*/ambari-qa/ RULE:[1:$1@$0](hdfs@KR.SOLARCH.LOCAL)s/.*/hdfs/ RULE:[1:$1@$0](.*@KR.SOLARCH.LOCAL)s/@.*// **RULE:[1:$1@$0](.*@SOLARCH.LOCAL)s/@.*//** RULE:[2:$1@$0](dn@KR.SOLARCH.LOCAL)s/.*/hdfs/ RULE:[2:$1@$0](jhs@KR.SOLARCH.LOCAL)s/.*/mapred/ RULE:[2:$1@$0](jn@KR.SOLARCH.LOCAL)s/.*/hdfs/ RULE:[2:$1@$0](nm@KR.SOLARCH.LOCAL)s/.*/yarn/ RULE:[2:$1@$0](nn@KR.SOLARCH.LOCAL)s/.*/hdfs/ RULE:[2:$1@$0](rm@KR.SOLARCH.LOCAL)s/.*/yarn/ RULE:[2:$1@$0](yarn@KR.SOLARCH.LOCAL)s/.*/yarn/ DEFAULT

CONFIRM ACCESS TO DAS HDFS USING KERBEROS

Use the steps below to authenticate as the ambari-qa user and perform a directory listing of the DAS HDFS.

```
[ambari-qa@mycluster1-master-0 ~]# kinit -kt /etc/security/keytabs/smokeuser.headless.keytab ambari-qa
[ambari-qa@mycluster1-master-0 ~]# klist -e
Ticket cache: FILE:/tmp/krb5cc_1001
Default principal: ambari-qa@KR.SOLARCH.LOCAL
Valid starting     Expires            Service principal
08/24/15 23:42:42  08/25/15 23:42:42  krbtgt/KR.SOLARCH.LOCAL@KR.SOLARCH.LOCAL
        renew until 08/24/15 23:42:42, Etype (skey, tkt): aes256-cts-hmac-sha1-96, aes256-cts-hmac-
sha1-96
[ambari-qa@mycluster1-master-0 ~]# hdfs dfs -ls /
```

CONFIGURE ECS FOR KERBEROS

Complete details for this procedure can be found at http://www.emc.com/techpubs/ecs/ecs_hdfs_configure-1.htm#GUID-6BB4F312-628A-422F-9E41-A949CA7FBE44. A concise list of steps follows.

To enable Kerberos on the ECS nodes, the Ansible automation tool is used. Ansible can be installed on any CentOS server using the following steps.

```
[root@kdc-1 ~]#
yum-config-manager --enable base
yum-config-manager --enable extras
yum-config-manager --enable updates
yum clean all
yum install epel-release
yum install ansible
yum install sshpass
cd viprfs-client-1.2.0.0-1380/playbooks
ansible-galaxy install -r requirements.txt -f
mkdir mycluster1
cp samples/* mycluster1/
cd mycluster1/
unzip /path/to/UnlimitedJCEPolicyJDK7.zip
cp /etc/krb5.conf .
```

Create a file named **inventory.txt** with the following contents:

```
[data_nodes]
ecs1-[1:4].solarch.local   ansible_ssh_pass=ChangeMe

[kdc]
kdc-1.solarch.local   ansible_ssh_pass=ChangeMe
```

Edit the file **generate-vipr-keytabs.yml** to contain the following:

```
---
###
# Generates keytabs for ViPR/ECS data nodes.
###

- hosts: data_nodes
  serial: 1

  roles:
    - role: vipr_kerberos_principal
      kdc: "{{ groups.kdc | first }}"
      principals:
        - name: vipr/_HOST@KR.SOLARCH.LOCAL
          keytab: keytabs/_HOST@KR.SOLARCH.LOCAL.keytab
```

Edit the file **setup-vipr-kerberos.yml** to contain the following:

```
---
###
# Configures ViPR/ECS for Kerberos authentication.
# - Configures krb5 client
# - Installs keytabs
# - Installs JCE policy
###

 - hosts: data_nodes


   roles:
     - role: vipr_kerberos_config
       krb5:
         config_file: krb5.conf
       service_principal:
         name: vipr/_HOST@KR.SOLARCH.LOCAL
         keytab: keytabs/_HOST@KR.SOLARCH.LOCAL.keytab


     - role: vipr_jce_config
       jce_policy:
         name: unlimited
         src: UnlimitedJCEPolicy/
```

Run the Ansible playbooks.

```
[root@kdc-1 mycluster1]#
ansible-playbook -v -i inventory.txt generate-vipr-keytabs.yml
ansible-playbook -v -i inventory.txt setup-vipr-kerberos.yml
```

Confirm that vipr service principals were generated on the KDC.

```
[root@kdc-1 mycluster1]#
kadmin.local -q "list_principals" | grep vipr
vipr/ecs1-1.solarch.local@KR.SOLARCH.LOCAL
vipr/ecs1-2.solarch.local@KR.SOLARCH.LOCAL
vipr/ecs1-3.solarch.local@KR.SOLARCH.LOCAL
vipr/ecs1-4.solarch.local@KR.SOLARCH.LOCAL
```

Finally, restart the ECS Storage OS Data Services. Refer to the Troubleshooting section of this document for details.

ADD ACTIVE DIRECTORY TO ECS

Complete details for this procedure can be found at http://www.emc.com/techpubs/ecs/users_authprov_and_mapping-1.htm#GUID-78D7D61D-F774-4DE2-B8DE-69DD164E68DE. A concise list of steps follows.

In the ECS UI, click Manager -> New Authentication Provider and enter the following values.

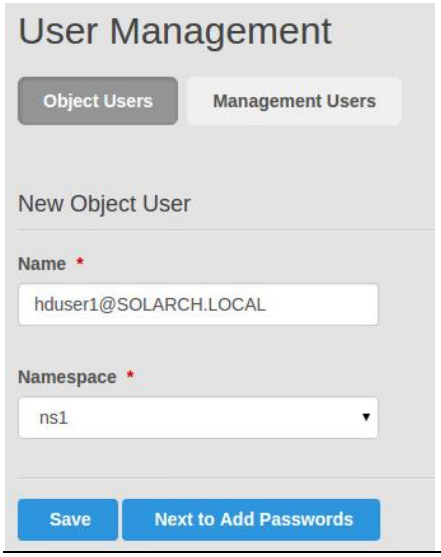
Table 6 ECS Authentication Provider Settings

PROPERTY	VALUE
Name	solarch.local
Description	solarch.local AD
Type	Active Directory
Domains	solarch.local
Server URLs	ldap://dc-01.solarch.local
Manager DN	CN=Manager,CN=Users,DC=solarch,DC=local
Search Scope	One Level
Search Base	DC=solarch,DC=local
Search Filter	userPrincipalName=%u

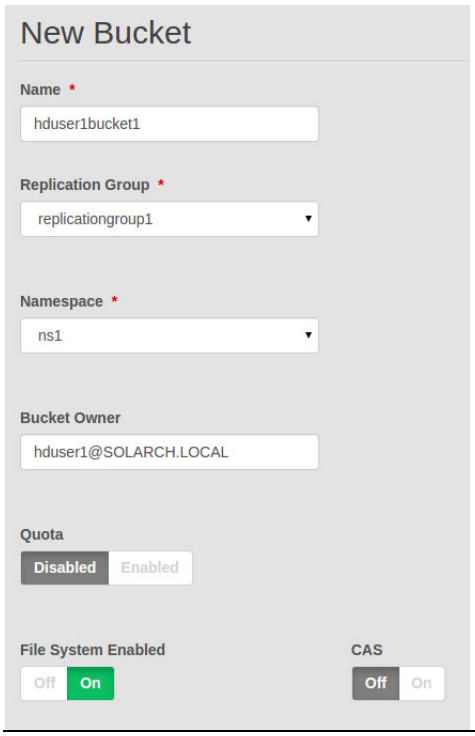
CREATE ECS USER AND BUCKET

ECS refers to AD users using the format user@REALM. For instance, the user named "hduser1" in the AD Users group of the solarch.local AD domain will be referred to as hduser1@SOLARCH.LOCAL. The upper-case realm is important.

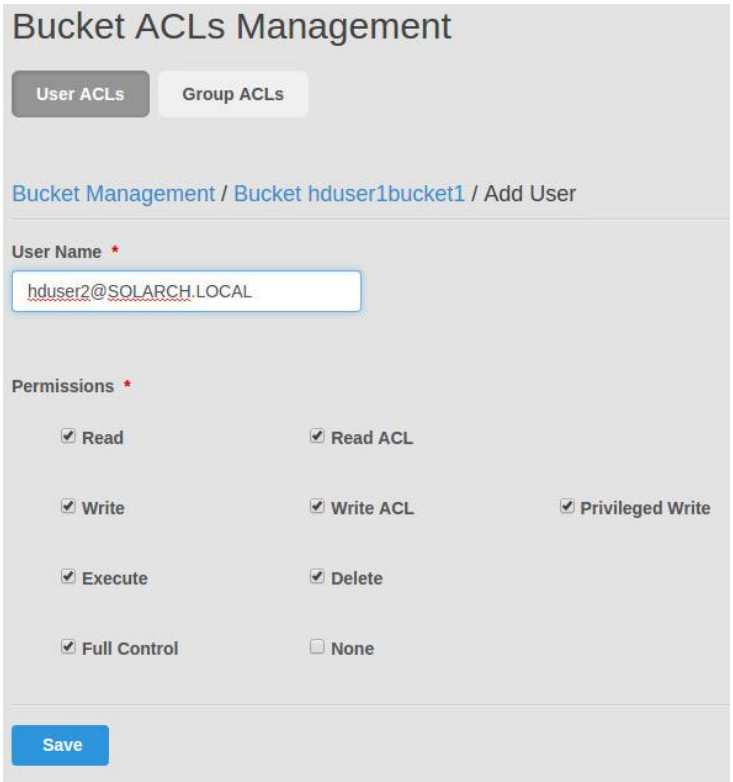
Create a ECS object user account for each AD account that will access ECS.



Next, create a bucket owned by the new object user. To allow HDFS access, you must set *File System Enabled* to On.



Next, edit the bucket ACL to allow the appropriate AD users. You must make sure that all users, including the bucket owner, are listed in the ACL using the correct case of user@REALM. To ensure a secure bucket, remove all permissions from all_users and public.



RECONFIGURE THE ECS CLIENT ON HDP NODES FOR KERBEROS

Using Ambari, make changes to the following Hadoop configuration properties.

Additional details are available at http://www.emc.com/techpubs/ecs/ecs_hdfs_configure-1.htm.

Table 7 Hadoop Properties for Kerberos on ECS

LOCATION	PROPERTY	VALUE
hdfs-site	fs.permissions.umask-mode	027
core-site	fs.viprfs.auth.identity_translation	CURRENT_USER_REALM
core-site	viprfs.security.principal	vipr/_HOST@KR.SOLARCH.LOCAL

Finally, use Ambari to stop all services and then start them.

CONFIRM ACCESS TO ECS USING KERBEROS

Use the steps below to authenticate as the AD user hduser1 and perform a directory listing of the secure ECS bucket.

```
[hduser1@mycluster1-master-0 ~]# kinit hduser1@SOLARCH.LOCAL
Password for hduser1@SOLARCH.LOCAL: <enter password for hduser1 as defined in AD>
[hduser1@mycluster1-master-0 ~]# hdfs dfs -ls viprfs://hduser1bucket1.ns1.ecs1/
[hduser1@mycluster1-master-0 ~]# hdfs dfs -touchz
viprfs://hduser1bucket1.ns1.ecs1/THIS_IS_hduser1bucket1
[hduser1@mycluster1-master-0 ~]# hdfs dfs -ls viprfs://hduser1bucket1.ns1.ecs1/
Found 1 items
-rw-------   1 hduser1          0 2015-08-26 19:05
viprfs://hduser1bucket1.ns1.ecs1/THIS_IS_hduser1bucket1
```

TESTING THE HADOOP INSTALLATION

To ensure that all required Hadoop components are functional, it is recommended that the functional and performance tests as documented in the related validation brief (**EMC Technical Validation of Hortonworks HDP with ECS**) be performed.

TROUBLESHOOTING

ENTER DOCKER CONTAINERS

The ECS system is built using Docker containers. Most command-line operations for ECS will be performed within the object-main Docker container. To "enter" this container, SSH to the Docker container host and run the following command.

```
ecs1-1:~ # docker exec -it object-main bash
ecs1-1:/ # # Enter your command here.
ecs1-1:/ # exit
```

RESTART ECS STORAGE OS DATA SERVICES

Use the Bash script below to restart the Storage OS Data Services on all ECS nodes. Note that it may take up to 10 minutes after this script runs for the services to be ready to accept requests.

```
#!/bin/bash
HOSTS="ecs1-1 ecs1-2 ecs1-3 ecs1-4"
for h in $HOSTS
        do
```

```
        ssh root@$h docker exec object-main service storageos-dataservice restart &
        done
```

UPDATE FILES ON ECS

Use the Bash script below to copy configuration files or patches to each ECS node. Before running the script, create a directory called *template* with the desired directory structure and files.

```
#!/bin/bash
HOSTS="ecs1-1 ecs1-2 ecs1-3 ecs1-4"
tar -cvf template.tar -C template/ .
tar -tvf template.tar
for h in $HOSTS
        do
        ssh root@$h docker exec -i object-main tar --overwrite -xvf - < template.tar
        done
```

ECS LOG FILES

The following log files contain useful information regarding HDFS access on ECS. These are in the Docker object-main container.

/opt/storageos/logs/hdfssvc-error.log
/opt/storageos/logs/hdfssvc.log

S3 BROWSER

In addition to accessing the ECS bucket using HDFS, an S3-compatible browser may also be used to edit bucket objects and object ACLs. For instance, S3 Browser (http://s3browser.com/) may be used. To configure S3 Browser to access ECS, create an account with the following settings.

Table 8 S3 Browser Settings

FIELD	VALUE
Storage Type	S3 Compatible Storage
REST Endpoint	9021
Access Key ID	(This should match the name of the object user defined in ECS)
Secret Access Key	(This should match the Object Access S3 password defined in ECS)

HADOOP DEBUG LOGGING

To troubleshoot issues with Hadoop CLI commands such as "hdfs dfs -ls", use the following commands.

```
[root@mycluster1-master-0~]#
export HADOOP_ROOT_LOGGER="TRACE,console"
export HADOOP_OPTS="-Dsun.security.krb5.debug=true"
hdfs dfs -ls $FS/ 2>&1 | tee log
```

For more details, refer to https://community.emc.com/docs/DOC-45698.

PERFORMANCE OPTIMIZATION

The table below lists the most commonly used Hadoop parameters and recommended initial values for good MapReduce performance.

Table 9 Hadoop performance-related parameters for MapReduce

LOCATION	PROPERTY	VALUE	NOTES
yarn-site	yarn.nodemanager.resource.cpu-vcores	(Number of CPU cores - 1)	Set this to the number of CPU cores on each of your Node Manager servers minus 1. By default, this is the maximum number of map or reduce tasks that will run on each Node Manager. This is a per-NodeManager setting.
yarn-site	yarn.nodemanager.resource.memory-mb	(Physical or Virtual Machine RAM minus 12 GiB)	In general, leave 12-16 GiB of RAM for use by the OS and Hadoop services. The remainder can be use by the map and reduce tasks. This is a per-NodeManager setting.
yarn-site	yarn.resourcemanager.scheduler.class	org.apache.hadoop.yarn.server.resourcemanager.scheduler.fair.FairSchedule	Although the default Capacity Scheduler has many more features and is more commonly used, the Fair Scheduler does a better job of running simple MapReduce jobs such as Terasort on remote Hadoop storage.
yarn-site	yarn.scheduler.maximum-allocation-mb	65536	In case the default is too small, allow a large memory allocation by the map and reduce tasks.
yarn-site	yarn.scheduler.minimum-allocation-mb	(yarn.nodemanager.resource.memory-mb / yarn.nodemanager.resource.cpu-vcores)	To achieve an even balance of CPU and memory usage for a homogoneous workload of MapReduce tasks, use this calculated value. Increase if memory errors are encountered.
yarn-site	yarn.scheduler.increment-allocation-mb	(yarn.scheduler.minimum-allocation-mb)	When using the Fair Scheduler, set this to the same value as the miminum.
mapred-site	mapreduce.map.memory.mb	(yarn.scheduler.minimum-allocation-mb)	This is a per-job setting but the default value can be specified globally.
mapred-site	mapreduce.reduce.memory.mb	(yarn.scheduler.minimum-allocation-mb)	This is a per-job setting but the default value can be specified globally.
mapred-site	mapreduce.map.java.opts	(mapreduce.map.memory.mb * 0.75 in format -Xmx1536m)	This is a per-job setting but the default value can be specified globally.
mapred-site	mapreduce.reduce.java.opts	(mapreduce.reduce.memory.mb * 0.75 in format -Xmx1536m)	This is a per-job setting but the default value can be specified globally.

For additional details, see https://community.emc.com/docs/DOC-41843.

AUTOMATING CONFIGURATION CHANGES WITH AMBARI

Hadoop configuration changes should be made using Ambari. In addition to making changes using the Ambari UI, the following *example* commands can be used to make configuration changes. The CLUSTER_NAME environment variable should be set to the name of your Hadoop cluster as defined in Ambari. Note that the values listed below are *examples* only.

```
[root@mycluster1-master-0 ~]#
```

```
CLUSTER_NAME=mycluster1
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.nodemanager.resource.memory-mb 229376
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.scheduler.minimum-allocation-mb 5881
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.scheduler.increment-allocation-mb 1
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.scheduler.maximum-allocation-mb 1000000
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.nodemanager.resource.cpu-vcores 39
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site
yarn.resourcemanager.scheduler.class
org.apache.hadoop.yarn.server.resourcemanager.scheduler.fair.FairScheduler
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME yarn-site yarn.log-
aggregation.retain-seconds -1
/var/lib/ambari-server/resources/scripts/configs.sh set localhost $CLUSTER_NAME core-site
fs.trash.interval 0
```

Just as when making configuration changes using the Ambari UI, the affected services will need to be restarted for the configuration changes to take effect.