HDP 2.3.x -  AD Kerberos

Monday, January 25, 2016

1:48 PM

version1.1

russ stevenson

[russ.stevenson@emc.com](mailto:russ.stevenson@emc.com)

Document detailing how to enable AD Kerborization against ambari/HDP Isilon HDFS cluster:

ambari 2.1.1

HDP 2.3.4.0

Isilon 7.2.1.1 + patch-164059

|  |  |
| --- | --- |
| link to hdp ambari  doc | <http://docs.hortonworks.com/HDPDocuments/Ambari-2.1.0.0/bk_Ambari_Security_Guide/content/ch_amb_sec_guide.html>    <http://hortonworks.com/hadoop-tutorial/integrating-hadoop-cluster-microsoft-active-directory-authentication/> |
| * 1. start the Kerberos wizard   2. Approve all the prerequisites; complete if needed     some of these steps are covered in other blog posts: <https://inside.emc.com/blogs/russ_stevenson> | Machine generated alternative text: Enable Kerberos Wizard  ENABLE KERBEROS WIZARD  Get Started  Configure Kerberos  Install and Test Kerberos  Configure Identities  Confirm Configuration  Stop Services  Kerberize Cluster  Start and Test Services  Get Started  Welcome to the Ambari Security' WizarcL Use this wizard to enable kerberos security' in your cluster  Let's get started  Note: This process requires services to be restarted and cluster downtirnæ As well, depending on the options  you select, might require support trom your Security' Please plan accordinglyn  What tvpe ot KDC do you plan on using?  O  existing MIT KOC  Existing Active Directory  O  Manage Kerberos principals and keytaös manually      Machine generated alternative text: Existing Active Directory:  Following prerequisites needs to be checked to progress ahead in the wizard.  Ambari Server and cluster hosts have network access to the Domain Controllers  Active Directory secure LDAP (LDAPS) connectivity' has been configured  Active Directory User container tor principals has been created and is on-hand (e g  OlJzHadoop IOU-People ,dczapache ,dczorg)  Active Directory administrative credentials with delegated control ot "Create, delete, and rnanage user  accounts" on the previously mentioned User container are on-hand  The Java Cryptography Extensions (JOE) have been setup on the Ambari Server host and all hosts in the      <http://docs.hortonworks.com/HDPDocuments/Ambari-2.1.0.0/bk_Ambari_Security_Guide/content/_distribute_and_install_the_jce.html> |
| 2a. create the AD account with delegated control for ambari to use (prereq4 above) | Machine generated alternative text: Active Directory Certificate  Services  E  ActiveDirectOryDornainServices  r 。 硪 「 鹹 卜 r  Active Directory users and computers  E ; fw.  〕 8 n  匚 〕 Computers  〔 介 , CM 〔 r $  〔 〕 Foreignsecurltyprincipals  bbs  〔 卜 dse co.          Machine generated alternative text: server Manager (RS-2008R2-DC)  Active Directory Certificate Services  Active Directory Domain Services  Microsoft Identity Management For LINI  hdp I objects (Filter Activated)  Name  ambari-krbS  Description        Machine generated alternative text: Delegation of Control Wizard  Welcome to the Delegation of  Control Wizard  This wizard helps you delegate control of Active Directory  obiects You can grant users permission to manage users,  groups, computers, organizational units, and other obiects  stored in Active Directory Domain Services  To continue, click Next  Cancel      Machine generated alternative text: Delegation of Control Wizard  Users 01 Groups  Select one or more users or groups to whom you want to delegate control  Selected users and groups:  ambari-krb5 (ambari-krb5@foocom  Cancel  Remove      Machine generated alternative text: Delegation of Control Wizard  T asks to Delegate  You can select common tasks custmize yotA own.  @ Delegate the following common tasks:  Create, delete and manage usel accounts  Reset user passwords and force password next boon  Read all user information  Create. delete and  Modify the membership Of a group  Manage "s  Generate Resultant Set of Policy (Planning)  Create a cust«n task to  Back  Next      Machine generated alternative text: Delegation of Control Wizard  Completing the Delegation of  Control Wizard  You have successfully completed the Delegation of Control  wizard  You chose to delegate control of obiects  in the following Active Directory folder:  foo corn/hdp  The groups, users, or computers to which you  have given control are:  ambari-krb5 (ambari-krb5@foocoml  You chose to delegate the following tasks:  To close this wizard, click Finish  Cancel |
| 2b. Validate the DNS    DNS A & PTR | every compute node needs DNS A & PTR record    Machine generated alternative text: hdp6  hdpS  hdp4  Host (A)  Host (A)  Host (A)  172 - 16 - 201 - 1 12  172 - 16 - 201 - 1 1 1  172 - 16 - 201 - 1 10    Machine generated alternative text:      SmartConnect DNS NS delegation for zone is correct    Machine generated alternative text: Delete pool  Basic settings Edi  IP range (low-high): 17216101 72 - 17216101 74  Access zone:  honon2  SmartConnect settings  Zone name:  Connection policy:  SmartConnect service subnet:  IP allocation method:  Rebalance policy:  IP failover policy:  Pool members Edi  Edi  Round Robin  subnetO  Dynamic  Automatic Failback  Round Robin  Aggregation mode: Link Aggregation Control Protocol (L ACP)  o  ext-I Node 01 (17216101 72, 17216101 73, 17216101 74)          every isilon IP assigned to the Smartconnect zone needs PTR record    Machine generated alternative text: |
| * 1. Place the Isilon host in Maintenance Mode, this allows the wizard to run with attempting to deploy the kerberos libraries | select the isilon host      Machine generated alternative text: moby.foo.com  Back  Summary  Components  NameNode /  SNarneNode  DataNode /  Alerts  Versions  + Add  Started  Started  Started  Host Metrics  No Data Available  CPU usage  No Data Available  Host Actions  No Data Available  Disk Usage  No Data Available    Machine generated alternative text: Host Actions  Start All Components  Stop All Components  C Restart All Components  Turn On Maintenance Mode  Delete Host  Set Rack  Download Client Contigs      Machine generated alternative text: Back  Summary  Components  NameNode /  SNarneNode  DataNode /  Alerts  Versions  + Add  Started  Started  Started  Clients / Kerberos Client  Summary  Hostname: mobyfoocorn  IP Address:  Rack.  • 'default-rack  OS: centos6 ()  cores (CPU): O (0)  Disk:  Data Unavailable  Memory:  Load Avg:  Heartbeat: a moment ago  Current Version.  Host Metrics  No Data Available  CPU usage  No Data Available  Load  No Data Available  Network Usage  191 Maintenance Mode  Host Actions  No Data Available  Disk Usage  No Data Available  Memory Usage  No Data Available  Processes |
| * + Select the KDC type - AD | Machine generated alternative text: Enable Kerberos Wizard  Stop Services  Kerberize Cluster  Start and Test Services  What tvpe ot KDC do you plan on using?  O  existing MIT KOC  Existing Active Directory  O  Manage Kerberos principals and keytaös manually  Existing Active Directory:  Following prerequisites needs to be checked to progress ahead in the wizard.  Ambari Server and cluster hosts have network access to the Domain Controllers  Active Directory secure LDAP (LDAPS) connectivity' has been configured  Active Directory User container tor principals has been created and is on-hand (e g  OlJzHadoop IOU-People ,dczapache ,dczorg)  Active Directory administrative credentials with delegated control ot "Create, delete, and rnanage user  accounts" on the previously mentioned User container are on-hand  The Java Cryptography Extensions (JOE) have been setup on the Ambari Server host and all hosts in the |
| 5. enter the KDC info and test | Change the ldap url to use the ldaps port 636    Machine generated alternative text: Kerberos  KOC  KOC type  KOC nost  Realm name  LDAP un  Container DN  Domains  Existing Active Directory  rs-200Br2-dc foo torn  FOOCOM  Idap://rs-200Br2-dc foo torn: 636/DC=too IDC-corn  ou=hdp  too corn  -rest KOC  Connection  Connection OK        Machine generated alternative text: Kadrnin  Kadrnin host  Admin principal  Admin password  rs-2DDBr2-dc too corn  ambari-krö5@FOOcorn      modify the Encryption types if needed  rc4-hmac  - Isilon only supports rc4-hma c encryption currently, onefs 7.x code    aes des3-cbc-sha1 rc4 des-cbc-md5  - the default      Machine generated alternative text: Encryption Types  aes desa-cnc-snal rc4 des-cnc-rndî      OR    Machine generated alternative text: Advanced kerberos-env  Install OS-specitic  Kerberos client  package(s)  Executable Search Paths  Encryption Types  /usr/bin, /usr/kerberos/bin, /usr/sbin, /usr/Iib/rnitJbin, /usr/Iib/rnitJ:  rc4-hrnac |
| * 1. Install and test clients       install complete on all hosts as no Isilon deploy is attempted due to maintenance mode | Machine generated alternative text: Enable Kerberos Wizard  ENABLE KERBEROS WIZARD  Get Started  Configure Kerberos  Install and Test Kerberos  Configure Identities  Confirm Configuration  Stop Services  Kerberize Cluster  Start and Test Services  Install and Test Kerberos Client  Please wait while the Kerberos clients are being installed and tested  Install Kerberos Client  Test Kerberos Client  x      Machine generated alternative text: Install and Test Kerberos Client  Kerberos service has been installed and tested successfully%  Install Kerberos Client  Test Kerberos Client |
| * 1. review  Result | Machine generated alternative text: Install Kerberos Client  Hosts  hdp4foocorn  hdp5foocorn  hdp6foocorn  Do not show this dialog again when starting a background operation  Show  x  All (3)        Machine generated alternative text: Test Kerberos Client  Hosts  hdp4foocorn  hdp5foocorn  hdp6foocorn  Do not show this dialog again when starting a background operation  Show  x  All (3) |
| 8a. Under the Configure Identities tab, we need to edit a few of the principals that ambari wants to create | Machine generated alternative text: Configure Identities  Configure principal name and key-tab location tor serice users and hadoop service components,  General Actvanced       * 1. (Remove -${cluster\_name} suffixes from principals.)   2. Smoke user principal   3. HDFS user principal   4. HBase user principal   5. Accumulo user principal   6. Spark user principal   7. trace.user       Advanced   * 1. (Replace alias principals.)   2. HDFS > dfs.namenode.kerberos.principal = hdfs/\_HOST@${realm}   3. HDFS > dfs.namenode.keytab.file = ${keytab\_dir}/hdfs.service.keytab        * 1. HDFS > dfs.secondary.namenode.kerberos.principal = hdfs/\_HOST@${realm}   2. HDFS > dfs.secondary.namenode.keytab.file = ${keytab\_dir}/hdfs.service.keytab        * 1. HDFS > dfs.datanode.kerberos.principal = hdfs/\_HOST@${realm}   2. HDFS > dfs.datanode.keytab.file = ${keytab\_dir}/hdfs.service.keytab        * 1. MapReduce2 > mapreduce.jobhistory.principal = mapred/\_HOST@${realm}   2. MapReduce2 > mapreduce.jobhistory.keytab =${keytab\_dir}/mapred.service.keytab          * 1. YARN > yarn.nodemanager.principal = yarn/\_HOST@${realm}   2. YARN > yarn.nodemanager.keytab = ${keytab\_dir}/yarn.service.keytab        * 1. YARN > yarn.resourcemanager.principal = yarn/\_HOST@${realm}   2. YARN > yarn.resourcemanager.keytab = ${keytab\_dir}/yarn.service.keytab        * 1. Falcon > \*.dfs.namenode.kerberos.principal = hdfs/\_HOST@${realm} |
| 8b. | Machine generated alternative text: Configure Identities  Configure principal narne and keytaö location tor service users and hadoop service components  General  Advanced  /etc/securitWkeytaös  FOOCOM  $(keytaö dir)/spnegoservicekeytaö  Global  Keytaö Dir  Spnego Principal  Spnego Keytaö      Machine generated alternative text: Ambari Principals  Smoke user principal  Smoke user keytab  HOFS user principal  HOFS user keytab  Spark user principal  Spark user keytab  I-leadless keytab  ${spark-env/spark_user}-${cluster_name}@${realm}        Machine generated alternative text: Ambari Principals  Smoke user principal  Smoke user keytab  HOFS user principal  HOFS user keytab  Spark user principal  Spark user keytab  I-leadless keytab  ${spark-env/spark_user}@${realm}      Advanced    Machine generated alternative text: MapReduce2  mapreduce Jobhistorb&  principal  mapreduce Jobhistorb&  keytab  mapreduce Jobhistorb&  webapp spnego-principal  mapreduce Jobhistorb&  webappspnego-keytab-  maored/ HOST $ realm  service keytab  service keytab        Machine generated alternative text: Configure Identities  Configure principal narne and keytaö location tor service users and hadoop service components  General  Advanced  Global  Ambari Principals  1M All configurations have been addressed |
| * 1. Next     download of the csv is shown | Machine generated alternative text: Confirm Configuration  Please review the configuration before continuing the setup process  Using the Download CSV button, you can download a csv tile which contains a list ot the principals and  keytabs that will automatically be created by AmbarL  KDC Type: Existing Active Directory  KDC Host: rs-200Br2-dcfoocorn  Realm Name: FOOCOM  LDAP URL:  Container DN: OU=hdp  Executable path: /usr/bin, /usr/kerberos/bin, /usr/sbin, /usr/Iib/rnitJbin, /usr/Iib/rnitJsbin  Exit Wizard  Download CSV        A dump of the csv, of principals created    host,description,principal name,principal type,local username,keytab file path,keytab file owner,keytab file owner access,keytab file group,keytab file group access,keytab file mode,keytab file installed    hdp4.foo.com,/spnego,HTTP/hdp4.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/spnego.service.keytab,root,r,hadoop,r,440,unknown  hdp4.foo.com,/smokeuser,ambari-qa@FOO.COM,USER,ambari-qa,/etc/security/keytabs/smokeuser.headless.keytab,ambari-qa,r,hadoop,r,440,unknown  hdp4.foo.com,hdfs,hdfs@FOO.COM,USER,hdfs,/etc/security/keytabs/hdfs.headless.keytab,hdfs,r,hadoop,r,440,unknown  hdp4.foo.com,sparkuser,spark@FOO.COM,USER,spark,/etc/security/keytabs/spark.headless.keytab,spark,r,hadoop,,400,unknown  hdp4.foo.com,nodemanager\_nm,yarn/hdp4.foo.com@FOO.COM,SERVICE,yarn,/etc/security/keytabs/yarn.service.keytab,yarn,r,hadoop,,400,unknown  hdp4.foo.com,zookeeper\_zk,zookeeper/hdp4.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/zk.service.keytab,zookeeper,r,hadoop,,400,unknown  hdp5.foo.com,/spnego,HTTP/hdp5.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/spnego.service.keytab,root,r,hadoop,r,440,unknown  hdp5.foo.com,/smokeuser,ambari-qa@FOO.COM,USER,ambari-qa,/etc/security/keytabs/smokeuser.headless.keytab,ambari-qa,r,hadoop,r,440,unknown  hdp5.foo.com,hdfs,hdfs@FOO.COM,USER,hdfs,/etc/security/keytabs/hdfs.headless.keytab,hdfs,r,hadoop,r,440,unknown  hdp5.foo.com,history\_server\_jhs,mapred/hdp5.foo.com@FOO.COM,SERVICE,mapred,/etc/security/keytabs/mapred.service.keytab,mapred,r,hadoop,,400,unknown  hdp5.foo.com,sparkuser,spark@FOO.COM,USER,spark,/etc/security/keytabs/spark.headless.keytab,spark,r,hadoop,,400,unknown  hdp5.foo.com,nodemanager\_nm,yarn/hdp5.foo.com@FOO.COM,SERVICE,yarn,/etc/security/keytabs/yarn.service.keytab,yarn,r,hadoop,,400,unknown  hdp5.foo.com,zookeeper\_zk,zookeeper/hdp5.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/zk.service.keytab,zookeeper,r,hadoop,,400,unknown  hdp6.foo.com,/spnego,HTTP/hdp6.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/spnego.service.keytab,root,r,hadoop,r,440,unknown  hdp6.foo.com,/smokeuser,ambari-qa@FOO.COM,USER,ambari-qa,/etc/security/keytabs/smokeuser.headless.keytab,ambari-qa,r,hadoop,r,440,unknown  hdp6.foo.com,hdfs,hdfs@FOO.COM,USER,hdfs,/etc/security/keytabs/hdfs.headless.keytab,hdfs,r,hadoop,r,440,unknown  hdp6.foo.com,sparkuser,spark@FOO.COM,USER,spark,/etc/security/keytabs/spark.headless.keytab,spark,r,hadoop,,400,unknown  hdp6.foo.com,nodemanager\_nm,yarn/hdp6.foo.com@FOO.COM,SERVICE,yarn,/etc/security/keytabs/yarn.service.keytab,yarn,r,hadoop,,400,unknown  hdp6.foo.com,zookeeper\_zk,zookeeper/hdp6.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/zk.service.keytab,zookeeper,r,hadoop,,400,unknown  moby.foo.com,/spnego,HTTP/moby.foo.com@FOO.COM,SERVICE,,/etc/security/keytabs/spnego.service.keytab,root,r,hadoop,r,440,unknown  moby.foo.com,/smokeuser,ambari-qa@FOO.COM,USER,ambari-qa,/etc/security/keytabs/smokeuser.headless.keytab,ambari-qa,r,hadoop,r,440,unknown  moby.foo.com,secondary\_namenode\_nn,hdfs/moby.foo.com@FOO.COM,SERVICE,hdfs,/etc/security/keytabs/hdfs.service.keytab,hdfs,r,hadoop,,400,unknown  moby.foo.com,hdfs,hdfs@FOO.COM,USER,hdfs,/etc/security/keytabs/hdfs.headless.keytab,hdfs,r,hadoop,r,440,unknown |
| * 1. stop the service | Machine generated alternative text: Stop Services  Please wait while services are being stopped  Stop Services      Machine generated alternative text: Stop Services  Services have been successfully stoppel  Stop Services |
| * 1. next | Machine generated alternative text: Kerberize Cluster  Please wait while cluster is being kerberizec[  Preparing Operations  Create Principals  Create Keytabs  Distribute Keytabs  Update Configurations  Finalize Operations |
| * 1. it will complete | Machine generated alternative text: Kerberize Cluster  Kerberos has successfully been enabled on the cluster  Preparing Operations  Create Principals  Create Keytabs  Distribute Keytabs  Update Configurations  Finalize Operations |
| * 1. service start will fail, will fix later     one reason service may fail is isilon is set to kerberos\_only athentication, by changing this to ALL services can be started and then reset back to kerberos\_only | Machine generated alternative text: Start and Test Services  Please wait while services are being started and testec[  Start and Test Services  Complete    Machine generated alternative text: Start and Test Services  Hosts  hdp4 footorn  hdp5 footorn  hdp6foocorn  Do not show this dialog again when starting a background operation  Show  x  All (3) |
| * 1. example of failing services | Machine generated alternative text: hdp4.foo.com  Tasks  Install  Client Install  Client Install  Install  Install  Client Install  Server Start  Show  x  All (15)    Machine generated alternative text: cnetk HOFS  Spark History Server Start  Check ZooKeeper  NodeManager Start  Check Spark  Check YARN  Check MapReduce2  Do not show this dialog again when starting a background operation |
| * 1. validate AD for principal creation | Machine generated alternative text: hdp 18 objects [Filter Activated]  Name  ambari-krbS  ambari-qa  hdFslmoby.Eoo.com  hdpuserl  HTTP/hdp4.Foo.com  HTTP/hdpS.Foo.com  HTTP/hdp6.Foo.com  HTTP/moby.Foo.com  isilon-12101S  mapredlhdpS.Foo.com  yarnlhdp4.Foo.com  yarnlhdpS.Foo.com  yarnlhdp6.Foo.com  zookEeperlhdp4. com  zookEeperlhdpS.Foo com  zookEeperlhdp6.Foo com |
| * 1. remove the isilon host from maintenance mode                               kerberos client installed -------->  needs removing, its isilon its not installed                                                                                                                                                                  Start the HDFS services                    kerberos client gone  ----------------> | Machine generated alternative text: Back  Summary  Components  NameNode /  SNarneNode  DataNode /  Alerts  Versions  + Add  Started  Started  Started  Clients / Kerberos Client  Summary  Hostname: mobyfoocorn  IP Address:  Rack.  • 'default-rack  OS: centos6 ()  cores (CPU): O (0)  Disk:  Data Unavailable  Memory:  Load Avg:  Heartbeat: a moment ago  Current Version.  Host Metrics  No Data Available  CPU usage  No Data Available  Load  No Data Available  Network Usage  191 Maintenance Mode  Host Actions  Start All Components  Stop All Components  C Restart All Components  191 Maintenance Mode  Delete Host  Set Rack  Download Client Contigs  Memory Usage  No Data Available  Processes        Machine generated alternative text: moby.foo.com  Back  Summary  Components  NameNode /  SNarneNode  Alerts  Versions  + Add  Started  Started  Started  DataNode  Clients /  Kerberos Client A  Host Metrics  No Data Available  CPU usage  No Data Available  Host Actions  No Data Available  Disk Usage  No Data Available      <!--------------    if the ambari install tried/failed to add the kerberos client to the Isilon HDFS service in Ambari, it can be deleted by using the following command against ambari    -----------------!>    curl -i -v -X DELETE -u admin:admin -H "X-Requested-By: Ambari" "<http://172.16.201.110:8080/api/v1/clusters/isilon/hosts/moby.foo.com/host_components/KERBEROS_CLIENT>"      Machine generated alternative text: [root@hdp4 — ] #  ://172.16.201.110:  ts/KERBERos CLIENT"  i -v -X DELETE -u  admin: admin —H  port BOBO (#0)  Ambar i "  "http  8080/ ap i/ VI/ c lusters/ isi Ion/ hosts/moby . foo . com/ host  Iibssh2/I.4  compone  About to connect() to  172.16. 201.110  Trying 172.16. 201.110...  connected  connected to 172.16. 201.110 (172.16. 201.110) port BOBO  Server auth using Basic with user admin'  DELETE / api/vl/clusters/ isilon/hosts/moby.foo.com/ host  Authorization: Basic YWRtaW46YWRtaW4=  components/ KERBEROS CLIENT HTTP/I.I  User —Agent: cur 1/7. lg. 7 (x86 IibcurI/7. lg. 7 NSS/3.14.O.O z lib/ 1.2 .3  Host: 172.16.201.110:8080  Accept:  Ambari  HTTP/I.1 200 0K  HTTP/I.1 200 0K  < User: admin  User: admin  < Set—Cookie: ; HttpOnIy  Set—Cookie: AMBARISESSIONID=Itg7jdOxtnpkzvnhv3 Path=/ ; HttpOnIy  < Expires: Thu, 01 Jan 1970 GMT  libidn/l.  Expires: Thu, 01 Jan 1970  < Content—Type: text/ plain  Content—Type: text/ plain  < Content—Length: O  Content—Length: O  < server: Jetty (B. 1.17.v20150415)  server: Jetty (B. 1.17.v20150415)  Connection #0 to host 172.16. 201.  Closing connection #0  [root@hdp4 — ] #  GMT  110  left  intact      kerberos client gone from isilon host!      Machine generated alternative text: moby.foo.com  Back  Summary  Components  NameNode /  SNarneNode  DataNode /  Alerts  Versions  + Add  Started  Started  Started  Host Metrics  No Data Available  CPU usage  No Data Available  Host Actions  No Data Available  Disk Usage  No Data Available |
| * 1. start  remaining services         notes:  History Server fails to start while isilon is in kerberos\_only, service will start if simple only or all is set on the zone    Spark service also has the same issue      Cannot figure this issue out yet! | Machine generated alternative text: Quick Links •  MapReduce2  YARN  ZooKeeper  Actions  Summary  Summary  Contigs  History Server A  Service Actions  2 alerts  MapReduce2 3 MapReduce2 Clients Installed    Machine generated alternative text: Summary  Heatmaps  Contigs  Quick Links •  A  YARN  ZooKeeper  Actions  Restart Required: 3 Components  Summary  App Timeline Server  ResourceManager  NodeManagers  NodeManagers Status  YARN Clients  ResourceManager Uptime  Started  Started  O active / O lost / O unhealthy / O rebooted / O  decommissioned  3 YARN Clients Installed  3767B secs  ResourceManager Heap  Containers  Applications  Cluster Memory  aueues  Service Actions  Restart  8 alerts  153 Ma / Ma (1 used)  O allocated / O pending / O reserved  O submitted / O running / O pending / O  completed / O killed / O failed  O Bytes used / O Bytes reserved / O Bytes  1 aueues |
| 16a. | get all the services started, you may need to work a little to get some of these started.      Machine generated alternative text: Ambari isilon O HDFS O MapReduce2 O YARN O Dozie O ZooKeeper .. Kerberos O Spark Actions — |
| 16b. | Kerberos user principals typically have the format username@REALM, whereas Hadoop usernames are typically just username. To translate Kerberos principals to Hadoop usernames,  Hadoop uses rules defined in the hadoop.security.auth\_to\_local property. The default setting strips the @REALM portion from the Kerberos principal, where REALM  is the Kerberos  realm defined by the default\_realm setting in the NameNode krb5.conf file.  Cloudera's default rule handled this while within  HDP specific rules exist and required the addition of a specific rule to handle the AD usernames, added:  RULE:[<1:$1@$0>]([.\*@AD.COM)s/@.\*//](mailto:.*@AD.COM)s/@.*//)    RULE:[<1:$1@$0>]([ambari-qa@FOO.COM](mailto:ambari-qa@FOO.COM))s/.\*/ambari-qa/ RULE:[<1:$1@$0>]([hdfs@FOO.COM](mailto:hdfs@FOO.COM))s/.\*/hdfs/ RULE:[<1:$1@$0>]([spark@FOO.COM](mailto:spark@FOO.COM))s/.\*/spark/ RULE:[<2:$1@$0>]([amshbase@FOO.COM](mailto:amshbase@FOO.COM))s/.\*/ams/ RULE:[<2:$1@$0>]([amszk@FOO.COM](mailto:amszk@FOO.COM))s/.\*/ams/ RULE:[<2:$1@$0>]([hdfs@FOO.COM](mailto:hdfs@FOO.COM))s/.\*/hdfs/ RULE:[<2:$1@$0>]([hdfs@FOO.COM](mailto:hdfs@FOO.COM))s/.\*/mapred/ RULE:[<2:$1@$0>]([jn@FOO.COM](mailto:jn@FOO.COM))s/.\*/hdfs/ RULE:[<2:$1@$0>]([nfs@FOO.COM](mailto:nfs@FOO.COM))s/.\*/hdfs/ RULE:[<2:$1@$0>]([oozie@FOO.COM](mailto:oozie@FOO.COM))s/.\*/oozie/ RULE:[<2:$1@$0>]([yarn@FOO.COM](mailto:yarn@FOO.COM))s/.\*/yarn/ RULE:[<1:$1@$0>]([.\*@AD.COM)s/@.\*//](mailto:.*@AD.COM)s/@.*//) DEFAULT    find hadoop.security.auth\_to\_local  property under the hdfs advanced configuration and add or modify the rule    Machine generated alternative text: hadoop.security. RULE:[1 :$  auth to local  RULE:[1:$1@$O](fl@FOD.CDM)s/.*/flfl/ RULE:[1 :$1@$O](spark@FOO.CDM)s/.t/spark/ RULE: [2:$ 1 @$U1(amshbase@FOO .COM)s/.t/ams/ RULE:[2:$ 1 @$O1(amszk@FOO .COM)s/.*/ams/ RULE:[2:$ 1 @$O1(hdfs@FOO .CDM)s/.*/hdfs/ RULE:[2:$ 1 @$Q1(hdts@FOO .CDM)s/.t/mapred/ RULE:[2:$ 1 @$Oljn@FOO .COM)s/.*/hdfs/ RULE:[2:$ 1 @$U1(nfs@FOO .COM)s/*/hdfs/ RULE:[2:$ 1 @$O1(oozie@FDO .COM)s/.*/oozie/ RULE:[2:$1$Oj(yarnFOO ,00M’ls/.t/yarn/ I:IiIIti!j[cl!]LW[€L DEFAULT      The error seen when this is not done is as follows:  -sh-4.1$ yarn jar hadoop-mapreduce-examples.jar teragen 10000 /user/hdpuser1/teragenOUT 16/01/14 14:30:17 INFO impl.TimelineClientImpl: Timeline service address: <http://hdp5.foo.com:8188/ws/v1/timeline/> 16/01/14 14:30:17 INFO client.RMProxy: Connecting to ResourceManager at hdp5.foo.com/172.16.201.111:8050 16/01/14 14:30:18 INFO hdfs.DFSClient: Created HDFS\_DELEGATION\_TOKEN token 4 for hdpuser1 on moby.foo.com:8020 16/01/14 14:30:18 INFO security.TokenCache: Got dt for hdfs://moby.foo.com:8020; Kind: HDFS\_DELEGATION\_TOKEN, Service: moby.foo.com:8020, Ident: (HDFS\_DELEGATION\_TOKEN token 4 for hdpuser1) java.io.IOException: The ownership on the staging directory /user/hdpuser1/.staging is not as expected. It is owned by FOO\hdpuser1. The directory must be owned by the submitter hdpuser1 or by hdpuser1 |
| * 1. Isilon Config  setup and validation (same as all other krb/isilon configs) | Validate Isilon for Kerberos    SPN  Zone Configuration  users  permissions |
| * 1. SPN - create hdfs/  spn's and additional | moby1-1# isi auth ads spn create --domain=foo.com --spn=HTTP/moby.foo.com --user=foo\\administrator  Enter password for [administrator@FOO.COM](mailto:administrator@FOO.COM):  Successfully added SPN(s).  moby1-1# isi auth ads spn create --domain=foo.com --spn=mapred/moby.foo.com --user=foo\\administrator  Enter password for [administrator@FOO.COM](mailto:administrator@FOO.COM):  The username or password entered is invalid  moby1-1# isi auth ads spn create --domain=foo.com --spn=mapred/moby.foo.com --user=foo\\administrator  Enter password for [administrator@FOO.COM](mailto:administrator@FOO.COM):  Successfully added SPN(s).  moby1-1# isi auth ads spn create --domain=foo.com --spn=yarn/moby.foo.com --user=foo\\administrator  Enter password for [administrator@FOO.COM](mailto:administrator@FOO.COM):  Successfully added SPN(s).  moby1-1# isi auth ads spn list --domain=foo.com  SPNs registered for MOBY1$:          yarn/moby.foo.com          mapred/moby.foo.com        moby1-1# isi auth ads spn list --domain=foo.com  SPNs registered for MOBY1$:          hdfs/moby.foo.com          HOST/moby.foo.com          HOST/moby    maybe add a yarn/domain.com SPN - not sure if this is needed yet |
| * 1. Change the HDFS auth to kerberos\_only | Machine generated alternative text: mob y I—I #  • poo. COM,  ISI  —zone=horton2  zone zones VI ew  Name :  Path:  Cache Size:  Map Untrusted:  Auth Providers:  NetBIOS Name:  All Auth Providers:  User Mapping Rules:  Home Directory Umask:  Skeleton Directory:  Audit Success:  Audit Failure:  HDFS Authentication:  HDFS Root Directory:  IdebHDFS Enabled:  HDFS Ambari Server:  HDFS Ambari Namenode:  Sys log Forwarding Enabled:  Sys log Audit Events:  Zone ID:  horton2  / ifs/ horton2  g. 54M  No  0077  / usr/ share/ skel  create, delete,  create, delete,  simple only  rename ,  rename ,  Isa— local—provider : horton2  close  close  / ifs/ horton2/ hadoop  Yes  hdp4 . foo . com  moby. foo . com  No  create, delete,  rename ,  set  set  set  security,  security,  security        Machine generated alternative text: mob y I—I #  mob y I—I #  • poo. COM,  ISI  ISI  zone  zone  zones modify  —zone=horton2  —zone=horton2  zones VI ew  —hdfs—authent i cat ion=kerberos  only  Name :  Path:  Cache Size:  Map Untrusted:  Auth Providers:  NetBIOS Name:  All Auth Providers:  User Mapping Rules:  Home Directory Umask:  Skeleton Directory:  Audit Success:  Audit Failure:  HDFS Authentication:  HDFS Root Directory:  IdebHDFS Enabled:  HDFS Ambari Server:  HDFS Ambari Namenode:  Sys log Forwarding Enabled:  Sys log Audit Events:  Zone ID:  horton2  / ifs/ horton2  g. 54M  No  0077  / usr/ share/ skel  create, delete,  create, delete,  kerberos only  rename ,  rename ,  Isa— local—provider : horton2  close  close  / ifs/ horton2/ hadoop  Yes  hdp4 . foo . com  moby. foo . com  No  create, delete,  rename ,  set  set  set  security,  security,  security |
| * 1. Create user in AD to run job | create AD user  create home directory for user on isilon hdfs root:  /ifs/hdfs-root/user/<AD user>  set permissions on isilon |
| * 1. access the compute cluster   2. validate user doesn't exist      1. cat /etc/passwd      2. create a user home directory         1. mkdir /home/<AD user>         2. chown it         3. chmod it      * 1. su - <AD user>   2. kinit   3. hadoop fs -ls /   4. cd /usr/hdp/2.3.2.0-2950/hadoop-mapreduce/ | Machine generated alternative text: [root@hdp4 — ] # su  hdpuserl  —sh—4.I$ kin it  Password for hdpuserI@FOO. COM:  —sh—4.I$ k list  Ticket cache: FILE  Default principal:  Valid starting  12/14/15  :/tmp/krb5cc 49002  hdpuser1@F00. COM  Expires  12/15/15  Service principal  krbtgt/FOO. COM@FOO.COM  renew until 12/21/15        Machine generated alternative text: [root@hdp4 — ] # su  hdpuserl  [hdpuserI@hdp4 — ] $ kin it  Password for hdpuserI@FOO. COM:  0 2014-12-15  0 2015-10-15  0 2015-07-06  0 2015-10-15  0 2015-10-15  0 2015-10-14  0 2015-11-02  0 2014-12-12  0 2015-01-20  0 2015-11-02  18:13  0 2015-11-02  0 2015-07-31  0 2015-12-07  0 2015-07-07  0 2014-12-18  [hdpuserI@hdp4  Found 15 items  drwxrwxrwx  drwxrwxrwx  drwxrwxr—x  drwxrwxr—x  drwxrwxr—x  drwxrwxrwx  drwxrwxrwx  drwxrwxr—x  drwxrwxrwx  drwxrwxr—x  drwxrwxrwx  — ] $ hadoop f s  —Is  root  hdfs  hdfs  root  hdfs  map red  map red  hdfs  root  root  hdfs  hdfs  hdfs  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  hadoop  03 •  .00  11:  03 •  .03  04  : 22  03 •  .57  12 •  .27  1B:  16:  03  1B:  15.  •55  13 •  .29  10  1B.  •03  / Thislslsilon. txt  / app— logs  / apps  / hdfs  / hdp  / home  / map red  /mr—history  / temp  / terasoRT  / teragenOUT  / tmp  / user  / webhdfs  / wiki |
| * 1. Create the users home directory on isilon hdfs root | hadoop fs -mkdir  /user/hdpuser1    Machine generated alternative text: 2015—07—06 09:34 2015—07—01 14:56 2014—12—15 19:13 2016—01—1219 :32 2015—07—01 15:04 2015—07—07 09:29 2015—07—01 10:58 2015—07—06 14:12 2015—06—29 13:44 2015—10—14 04:23 2015—07—06 09:34 2015—03—19 14:05 / usen hbase / usen heat / usen hdf s /user/h’Jpuserl / user/hive / user/hue / user/niapred / us e r /00 z je / user/root / user/spark / us e r / t e z / user/yarn [hdpuserl@hdp6 hadoop—niapreduce] $ kinlt Password for hdpuser1@F00.COM: [hdpuserl@hdp6 hadoop—niapreduce] $ hadoop fs —Is /user Found 12 itenis drwxrwxr—x — hbase hadoop O drwxrwxrwx — heat hadoop O drwxrwxrwx — hdf s hadoop O [lrwxr—xr—x — FOO\hdpuserl haduup O drwxrwxr—x — tez hadoop O drwxrwxr—x — cloudera hadoop O drwxrwxr—x — niapred hadoop O drwxrwxr—x — 1003 hadoop O drwxrwxr—x — root hadoop O drwxrwxr—x — spark hadoop O drwxrwxr—x — tez hadoop O drwxrwxr—x — yarn hadoop O |
| * 1. run an example job | -sh-4.1$ cd /usr/hdp/2.3.4.0-3485/hadoop-mapreduce/  -sh-4.1$ yarn jar hadoop-mapreduce-examples.jar teragen 10000 /user/hdpuser1/teragenOUT  16/01/21 19:11:07 INFO impl.TimelineClientImpl: Timeline service address: <http://hdp5.foo.com:8188/ws/v1/timeline/>  16/01/21 19:11:08 INFO client.RMProxy: Connecting to ResourceManager at hdp5.foo.com/172.16.201.111:8050  16/01/21 19:11:10 INFO hdfs.DFSClient: Created HDFS\_DELEGATION\_TOKEN token 5 for hdpuser1 on 172.16.201.74:8020  16/01/21 19:11:10 INFO security.TokenCache: Got dt for hdfs://moby.foo.com:8020; Kind: HDFS\_DELEGATION\_TOKEN, Service: 172.16.201.7                         4:8020, Ident: (HDFS\_DELEGATION\_TOKEN token 5 for hdpuser1)  16/01/21 19:11:11 INFO terasort.TeraSort: Generating 10000 using 2  16/01/21 19:11:11 INFO mapreduce.JobSubmitter: number of splits:2  16/01/21 19:11:11 INFO mapreduce.JobSubmitter: Submitting tokens for job: job\_1453328250692\_0004  16/01/21 19:11:11 INFO mapreduce.JobSubmitter: Kind: HDFS\_DELEGATION\_TOKEN, Service: 172.16.201.74:8020, Ident: (HDFS\_DELEGATION\_TO                         KEN token 5 for hdpuser1)  16/01/21 19:11:13 INFO impl.YarnClientImpl: Submitted application application\_1453328250692\_0004  16/01/21 19:11:13 INFO mapreduce.Job: The url to track the job: <http://hdp5.foo.com:8088/proxy/application_1453328250692_0004/>  16/01/21 19:11:13 INFO mapreduce.Job: Running job: job\_1453328250692\_0004  16/01/21 19:11:31 INFO mapreduce.Job: Job job\_1453328250692\_0004 running in uber mode : false  16/01/21 19:11:31 INFO mapreduce.Job:  map 0% reduce 0%  16/01/21 19:11:39 INFO mapreduce.Job:  map 50% reduce 0%  16/01/21 19:11:45 INFO mapreduce.Job:  map 100% reduce 0%  16/01/21 19:11:46 INFO mapreduce.Job: Job job\_1453328250692\_0004 completed successfully  16/01/21 19:11:46 INFO mapreduce.Job: Counters: 31          File System Counters                  FILE: Number of bytes read=0                  FILE: Number of bytes written=263942                  FILE: Number of read operations=0                  FILE: Number of large read operations=0                  FILE: Number of write operations=0                  HDFS: Number of bytes read=164                  HDFS: Number of bytes written=1000000                  HDFS: Number of read operations=8                 HDFS: Number of large read operations=0                  HDFS: Number of write operations=4          Job Counters                  Launched map tasks=2                  Other local map tasks=2                  Total time spent by all maps in occupied slots (ms)=18332                  Total time spent by all reduces in occupied slots (ms)=0                  Total time spent by all map tasks (ms)=18332                  Total vcore-seconds taken by all map tasks=18332                  Total megabyte-seconds taken by all map tasks=28157952          Map-Reduce Framework                  Map input records=10000                  Map output records=10000                  Input split bytes=164                  Spilled Records=0                  Failed Shuffles=0                  Merged Map outputs=0                  GC time elapsed (ms)=188                  CPU time spent (ms)=1820                  Physical memory (bytes) snapshot=225046528                  Virtual memory (bytes) snapshot=6327631872                  Total committed heap usage (bytes)=257294336          org.apache.hadoop.examples.terasort.TeraGen$Counters                  CHECKSUM=21555350172850          File Input Format Counters                  Bytes Read=0          File Output Format Counters                  Bytes Written=1000000 |
| * 1. the end | enjoy! |