**SAS Enable Kerberos**

**安裝說明**

**章節**

1. **OverAll**
2. **Environment Validation**
3. **Server Configuration**
4. **Cloudera Manager Software download**
5. **Install Cloudera Manger**
6. **Install Hadoop CDH**
7. **Enable High Availability**
8. **Installed Validation**
9. **Enable Kerberos**
10. **Remark**
11. **Enable Kerberos**
    1. **check iptables is closed**

#> service iptables status

#> service iptables stop

* 1. **backup Database**

#> pg\_dump -h 10.67.67.93 -p 5432 -U amon > /tmp/db\_backup3.txt

* 1. **pre chek JCE is installed**

|  |
| --- |
| #> cd $JAVA\_HOME/jre/lib/security/  #> ls local\_policy.jar  #> ls US\_export\_policy.jar  如果沒有發現上述兩檔案則須到oracle 官網下載JCE jar files，並放置至$JAVA\_HOME/jre/lib/security/目錄 |

* 1. **install kerberos server**

|  |
| --- |
| 1. install server packages by yum   #> sudo yum install krb5-server 5krb-libs krb5-auth-dialog   1. config /etc/krb5.conf, 將EXAMPLE.COM換成HADOOP.AEGON.COM.TW   #> sudo vi /etc/krb5.conf  [libdefaults]  default\_realm = HADOOP.AEGON.COM.TW  dns\_lookup\_realm = false  dns\_lookup\_kdc = false  ticket\_lifetime = 24h  renew\_lifetime = 7d  forwardable = true  [realms]  HADOOP.AEGON.COM.TW = {  kdc = urlsasnode1.aegon.com.tw  admin\_server = urlsasnode1.aegon.com.tw  }  [domain\_realm]  .hadoop.aegon.com.tw = HADOOP.AEGON.COM.TW  hadoop.aegon.com.tw = HADOOP.AEGON.COM.TW   1. config /var/kerberos/krb5kdc/kdc.conf, 將EXAMPLE.COM換成HADOOP.AEGON.COM.TW，並加入max\_life, max\_renewable\_life, kdc\_tcp\_ports   #> sudo vi /var/kerberos/krb5kdc/kdc.conf  [realms]  HADOOP.AEGON.COM.TW = {  #master\_key\_type = aes256-cts  max\_life = 1d  max\_renewable\_life = 7d  kdc\_tcp\_ports = 88  acl\_file = /var/kerberos/krb5kdc/kadm5.acl  dict\_file = /usr/share/dict/words  admin\_keytab = /var/kerberos/krb5kdc/kadm5.keytab  supported\_enctypes = aes256-cts:normal aes128-cts:normal des3-hmac-sha1:normal arcfour-hmac:normal des-hmac-sha1:normal des-cbc-md5:normal des-cbc-crc:normal  }   1. create kerberos database   #> sudo /usr/sbin/kdb5\_util create -s   1. config the /var/kerberos/krb5kdc/kadm5.acl file   #> sudo vi /var/kerberos/krb5kdc/kadm5.acl  \*/admin@HADOOP.AEGON.COM.TW \*   1. create first principal using kadmin.local   #> sudo /usr/sbin/kadmin.local -q "addprinc cloudera-scm/admin"   1. start kerberos   #> sudo service krb5kdc start  #> sudo service kadmin start  #> sudo chkconfig krb5kdc on  #> sudo chkconfig kadmin on |

* 1. **install openldap-clients on Cloudera-Manager-Sever host**

|  |
| --- |
| #> sudo yum install openldap-clients |

* 1. **install kerberos client on all hosts**

|  |
| --- |
| #> sudo yum install -y krb5-workstation krb5-libs krb5-auth-dialog |

* 1. **If you have enabled YARN Resource Manager HA, you should clear the StateStore znode in ZooKeeper before enabling Kerberos**

|  |
| --- |
| 1. Go to the Cloudera Manager Admin Console home page, click to the right of the YARN service and select Stop. 2. When you see a Finished status, the service has stopped. 3. Go to the YARN service and select Actions > Format State Store.  1. When the command completes, click Close. |

* 1. **install kerberos from GUI**

|  |
| --- |
| 1. Go to the Cloudera Manager Admin Console and click to the right of the cluster for which you want to enable Kerberos authentication. 2. Select Enable Kerberos  1. double check the following steps  1. input kdc information  1. KRB5 Configuration  1. Input KDC account manager Credential   userName:cloudera-scm**/admin**   1. Import KDC account Manager Credentials Command  1. Create Kerberos Principal  1. Configure Ports  1. Enable Kerberos Commands  1. Finished |

* 1. **Add principal and keytab file at KDC server**

|  |
| --- |
| #> sudo /usr/sbin/kadmin.local  #> kadmin.local: addprinc sasetlt  #> Enter password for principal " sasetlt @HADOOP.AEGON.COM.TW":  #> Re-enter password for principal " sasetlt @HADOOP.AEGON.COM.TW":  #> Principal " sasetlt @HADOOP.AEGON.COM.TW" created.  #> kadmin.local: xst -k sasetlt.keytab sasetlt |

* 1. **Copy sasetlt.keytab to sas node(**

|  |
| --- |
| #> sudo /usr/sbin/kadmin.local  #> kadmin.local: xst -k sasdemo.keytab sasdemo |

* 1. **SAS Node operation**

1. install Kerberos client libraries

|  |
| --- |
| #> yum install krb5-workstation krb5-libs krb5-auth-dialog |

1. copy hadoop’s krb5.conf to sas node

|  |
| --- |
| #> scp /etc/krb5.conf root@ URLSASNAME1:/etc/kerb5.conf |

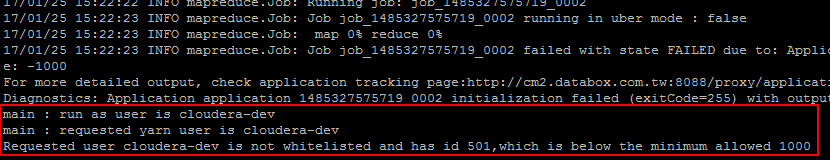
1. copy hadoop’s krb5.conf to sas node

|  |
| --- |
| #> scp /etc/krb5.conf root@ URLSASNAME1:/etc/kerb5.conf |

1. In yarn Configuration search : “min.user.id” and “allowed System Users”，then restart yarn

|  |
| --- |
| 1. change min.user.id to 500  1. add cloudera-dev to allowed System Users |

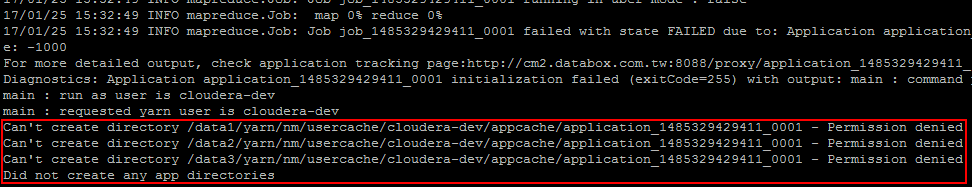
否則會出現下列錯誤



1. 執行MapReduce程式

|  |
| --- |
| #> sudo su - cloudera-dev  #> kinit cloudera-dev  #> echo “Hello Hadoop, Bye Hadoop” > file3  #> hadoop fs -put file3 /user/cloudera-dev/wordcount/input  #> hadoop fs -rmr /user/cloudera-dev/wordcount/output  #> yarn jar /opt/cloudera/parcels/CDH/jars/hadoop-examples.jar wordcount wordcount/input wordcount/output  #> hadoop fs -getmerge wordcount/output output.txt  #> cat output.txt |

若執行時發生下列錯誤，



則執行下列動作

|  |
| --- |
| #> pssh -h nodes.txt -x "-t -t" -i "sudo rm -rf /data1/yarn/nm/usercache/\*"  #> pssh -h nodes.txt -x "-t -t" -i "sudo rm -rf /data2/yarn/nm/usercache/\*"  #> pssh -h nodes.txt -x "-t -t" -i "sudo rm -rf /data3/yarn/nm/usercache/\*" |

1. **Remark**
2. **mount new disk**

若有新的hard disk加入Hadoop Cluster內，則需要做下列動作

|  |
| --- |
| 1. 找出尚未格式化的hd   #> fdisk -l   1. 以/dev/sdb為例，對/dev/sdc執行fdisk   #> sudo fdisk /dev/sdb   * 1. n   2. p   3. 1   4. Enter   5. Enter   6. w  1. 對/dev/sdc1進行格式化，並取個label name /data2   #> sudo /sbin/mkfs.ext4 -L /data2 /dev/sdc1   1. 建立掛載點   #> sudo mkdir /data2  #> sudo mount /dev/sdc1 /data2   1. 建立永久掛載點   #> sudo vi /etc/fstab  LABEL=/data2 /data2 ext4 defaults 1 2   1. 更改掛載點權限   #> sudo chown -R cloudera-scm:cloudera-scm /data2  #> sudo chmod -R 777 /data2 |

1. **bash shell commands to multi nodes**

* **use pssh**

**on line install psshl**

|  |
| --- |
| #> sudo yum install epel-release  #> sudo yum install python-pip  #> sudo pip install --upgrade pip  #> sudo pip install pssh |

**off line install psshl**

|  |
| --- |
| #> sudo yum install python-setuptools  #> wget https://storage.googleapis.ocm/google-code-archive-downloads/v2/code.google.com/parallel-ssh/pssh-2.3.1.tar.gz  #> tar zxvf pssh-2.3.1.tar.gz  #> cd pssh-2.3.1/  #> sudo python setup.py install |

**使用範例**

|  |
| --- |
| #> pssh -h nodes.txt -i "date"  ##若使用sudo 須加入 -x "-tt" 參數  #> pssh -h nodes.txt -x "-tt" -i "sudo service cloudera-scm-agent status"  ## run as root -l:ssh user -A:input password  #> pssh -h nodes.txt -l root -A -i "date"  ##copy file to remote hosts  #> pscp -h hosts.txt foo.txt /home/foo.txt  ## copy remote hosts files to local directory  #> pslurp -h hosts.txt /etc/hosts local\_dir |

* **write script by myself**

|  |
| --- |
| [bdmgr@cmgui ~]$ **cat nodes.txt**  cms  cm1  cm2  cm3  cm4  cm5  [bdmgr@cmgui ~]$ **cat mncmd.sh**  **#!/bin/bash**  **for i in $(cat nodes.txt);**  **do**  **echo "server:"$i;**  **# do your stuff here**  **ssh bdmgr@$i "hostname; date;"**  **done**  [bdmgr@cmgui ~]$ **sh mncmd.sh**  server:cms  cms.aegon.com.tw  Thu Jan 19 14:23:26 CST 2017  server:cm1  cm1.aegon.com.tw  Thu Jan 19 14:23:26 CST 2017  server:cm2  cm2.aegon.com.tw  Thu Jan 19 14:23:26 CST 2017  server:cm3  cm3.databox.com.tw  Thu Jan 19 14:23:26 CST 2017  server:cm4  cm4.databox.com.tw  Thu Jan 19 14:23:26 CST 2017  server:cm5  cm5.databox.com.tw  Thu Jan 19 14:23:27 CST 2017  [bdmgr@cmgui ~]$ |

1. **On line MySQL Install**

此步驟使用線上安裝方式

|  |
| --- |
| ##download mysql57-community-release-el6-9.noarch.rpm to /tmp  #> sudo yum localinstall /tmp/mysql57-community-release-el6-9.noarch.rpm  #> sudo yum install mysql-server  #> sudo service mysqld start  ##從/var/log/mysqld.log找出預設的密碼  #> sudo grep 'temporary password' /var/log/mysqld.log  ##root密碼改為P@ssw0rd  #> sudo mysql\_secure\_installation  #> sudo /sbin/chkconfig mysqld on |

1. **Red Hat Enterprise 試用版註冊方式**

此步驟需access internet

|  |
| --- |
| 1. 若重新安裝另一台VM，則須在原安裝VM先刪除之前的subscribe   root #> subscription-manager remove --all   1. 在新安裝的VM，重新subscribe   root #> subscription-manager clean  root #> subscription-manager register   1. 須執行attach，才算註冊完成   root #> subscription-manager attach |

1. **failing to install Oozie ShareLib on service Oozie**

因為是使用VM，所以IO特別慢，若在first time Sartup Cluster 發生'failing to install Oozie ShareLib on service Oozie'，可將預設值得timeout時間調高

|  |
| --- |
| open another browser tab, go to console, oozie, configuration, search for oozie\_upload\_sharelib\_cmd\_timeout parameter and change it to something bigger then 270. I entered 600 |

1. **How to add new network Interface**

因為是使用VM，所以IO特別慢，若在first time Sartup Clust

|  |
| --- |
| 1. 取得network interface name   root #> nmcli   1. 在/etc/sysconfig/network-scripts/內建立一個新的ifcfg-enpXX，並且以新的interface name作為命名   root #> cp ifcfg-enps0 ifcfg-enpXXX   1. 重啟network service   root #> systemctl restart network |