ocdp开启kerberos操作文档

执行以下操作时最好能将集群所有组件停掉，可以大大节省时间。

1. kerberos server安装（选择一个可靠主机）：

```
yum - y install krb5-libs
yum - y install krb5-server
yum - y install krb5-workstation
yum - y install krb5-auth-dialog
```

集群其它节点需要安装kerberos client

```
yum - y install krb5-workstation
```

2. 配置kerberos

vi kerb5.conf

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = ocdp
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true

[realms]
 ocdp = {
  kdc = ochadoop09:88
  admin_server = ochadoop09:749
 }

[domain_realm]
 .ocdp = ocdp
 ocdp = ocdp

[kdc]
profile=/var/kerberos/krb5kdc/kdc.conf
```

修改完成后同步以上配置文件到集群其它节点。

```
scp /etc/krb5.conf   ochadoop10:/etc
```

```
cd  /var/kerberos/krb5kdc
```

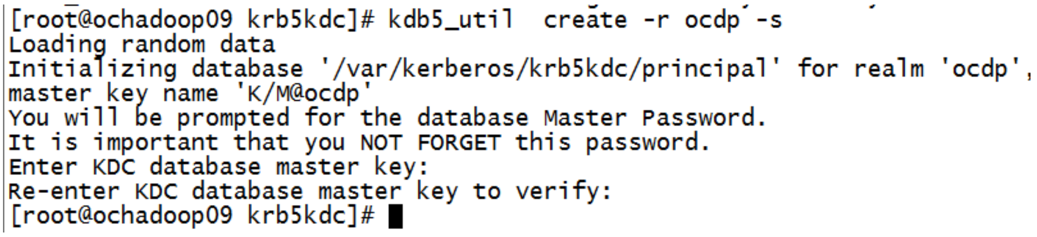
```
vi  kadm5.acl
*/admin@ocdp    *
vi kdc.conf
```

```
[kdcdefaults]
 kdc_ports = 88
 kdc_tcp_ports = 88

[realms]
 ocdp = {
  #master_key_type = aes256-cts
  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
 }
```

3. kerberos初始化

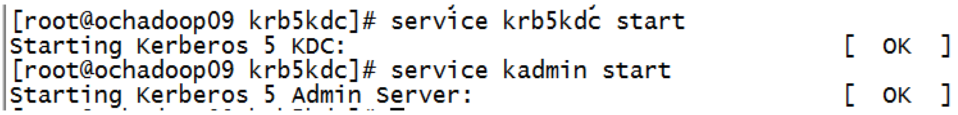
```
kdb5_util  create -r ocdp -s
```



```
[root@ochadoop09 krb5kdc]# kdb5_util  create -r ocdp -s
Loading random data
Initializing database '/var/kerberos/krb5kdc/principal' for realm 'ocdp',
master key name 'K/M@ocdp'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
[root@ochadoop09 krb5kdc]#
```

4.启动kerberos

```
service krb5kdc start
service kadmin start
```

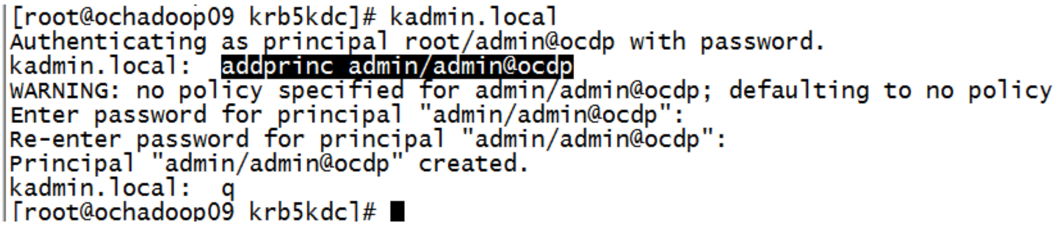


```
[root@ochadoop09 krb5kdc]# service krb5kdc start
Starting Kerberos 5 KDC:                                   [  OK  ]
[root@ochadoop09 krb5kdc]# service kadmin start
Starting Kerberos 5 Admin Server:                          [  OK  ]
```

5.测试kerberos是否可用

```
kadmin.local
```

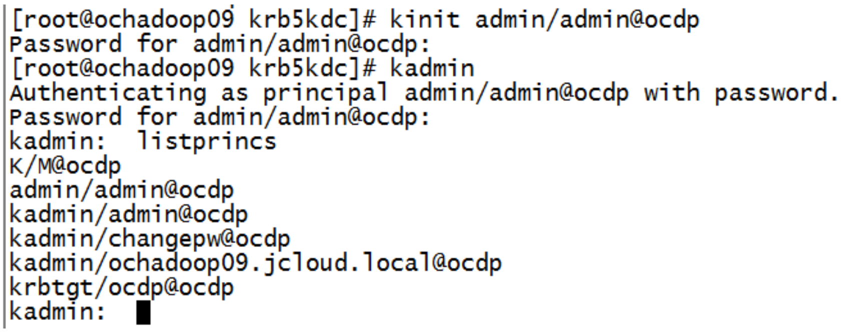
```
addprinc admin/admin@ocdp
```



```
[root@ochadoop09 krb5kdc]# kadmin.local
Authenticating as principal root/admin@ocdp with password.
kadmin.local:  addprinc admin/admin@ocdp
WARNING: no policy specified for admin/admin@ocdp; defaulting to no policy
Enter password for principal "admin/admin@ocdp":
Re-enter password for principal "admin/admin@ocdp":
Principal "admin/admin@ocdp" created.
kadmin.local:  q
[root@ochadoop09 krb5kdc]#
```

```
 kinit admin/admin@ocdp
```

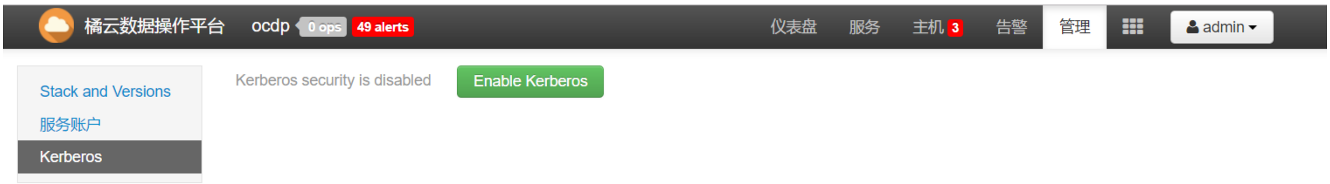
```
kadmin
listprincs
```



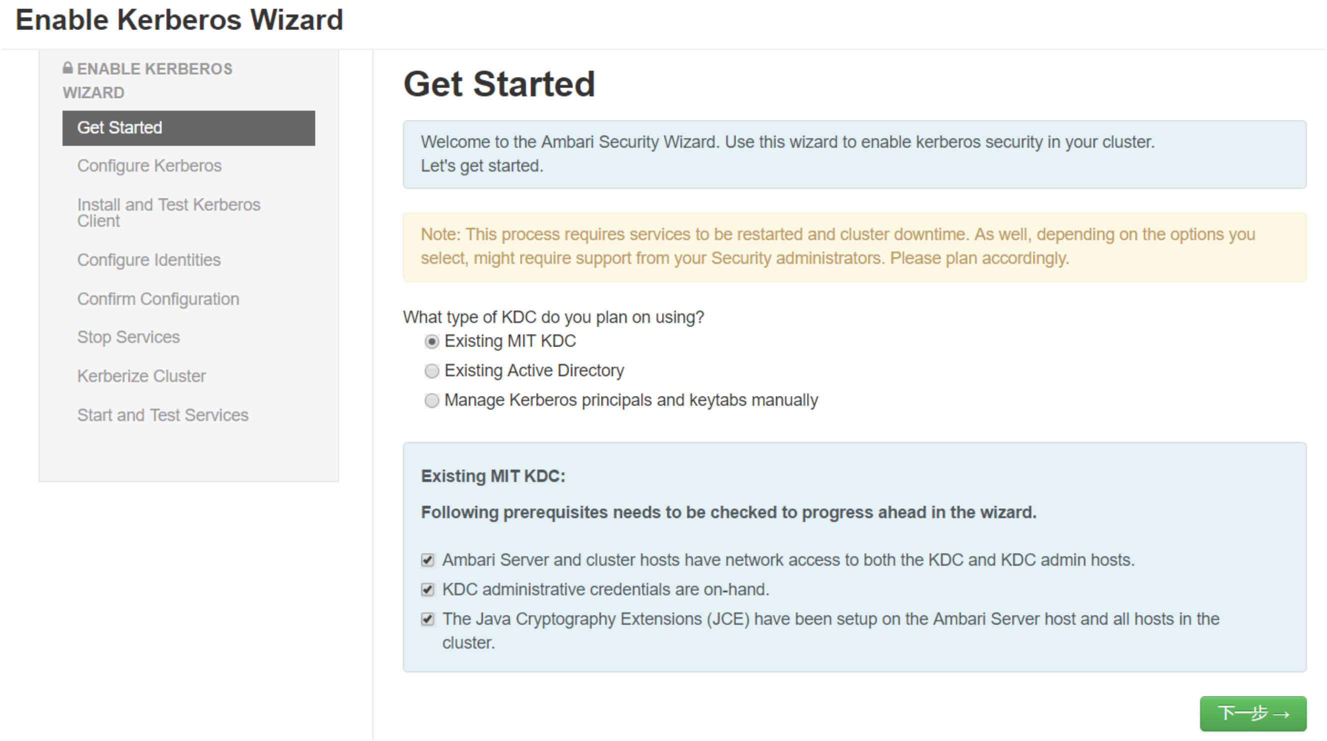
```
[root@ochadoop09 krb5kdc]# kinit admin/admin@ocdp
Password for admin/admin@ocdp:
[root@ochadoop09 krb5kdc]# kadmin
Authenticating as principal admin/admin@ocdp with password.
Password for admin/admin@ocdp:
kadmin:  listprincs
K/M@ocdp
admin/admin@ocdp
kadmin/admin@ocdp
kadmin/changepw@ocdp
kadmin/ochadoop09.jcloud.local@ocdp
krbtgt/ocdp@ocdp
kadmin:  █
```

如果集群所有节点都可以正常登陆则kerberos安装成功。

6. ambari开启kerberos：



Kerberos security is disabled



Enable Kerberos Wizard

Get Started

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

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

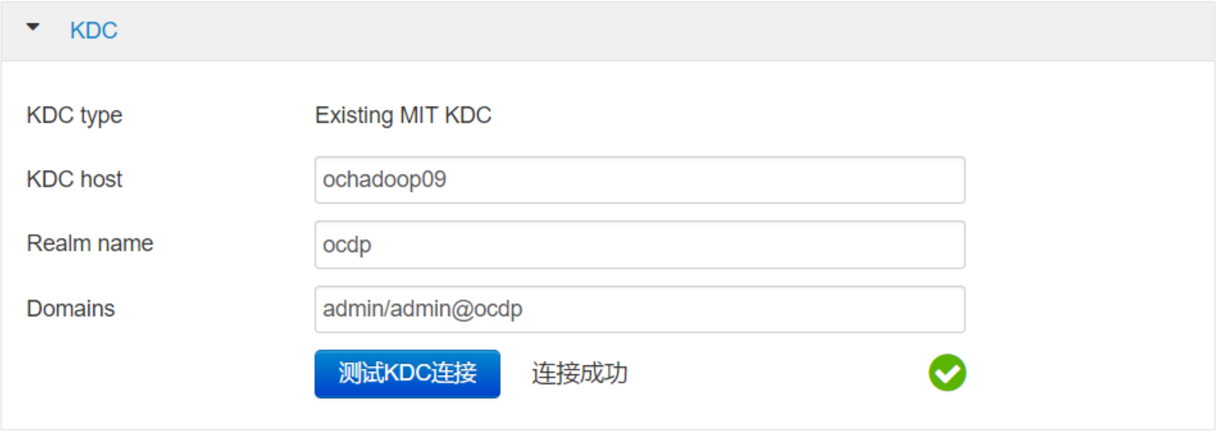
What type of KDC do you plan on using?

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

Existing MIT KDC:

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

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



▾ KDC

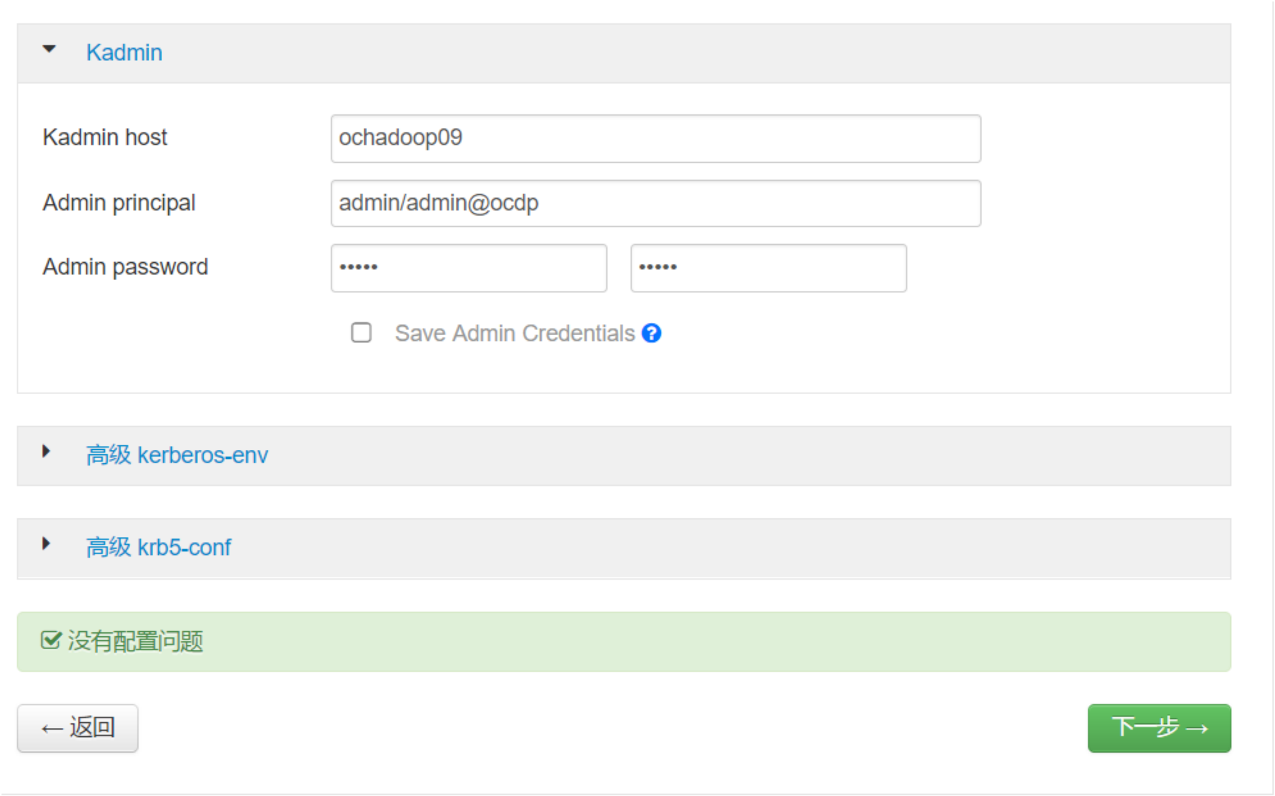
KDC type: Existing MIT KDC

KDC host: ochadoop09

Realm name: ocdp

Domains: admin/admin@ocdp

连接成功 ✓



▾ Kadmin

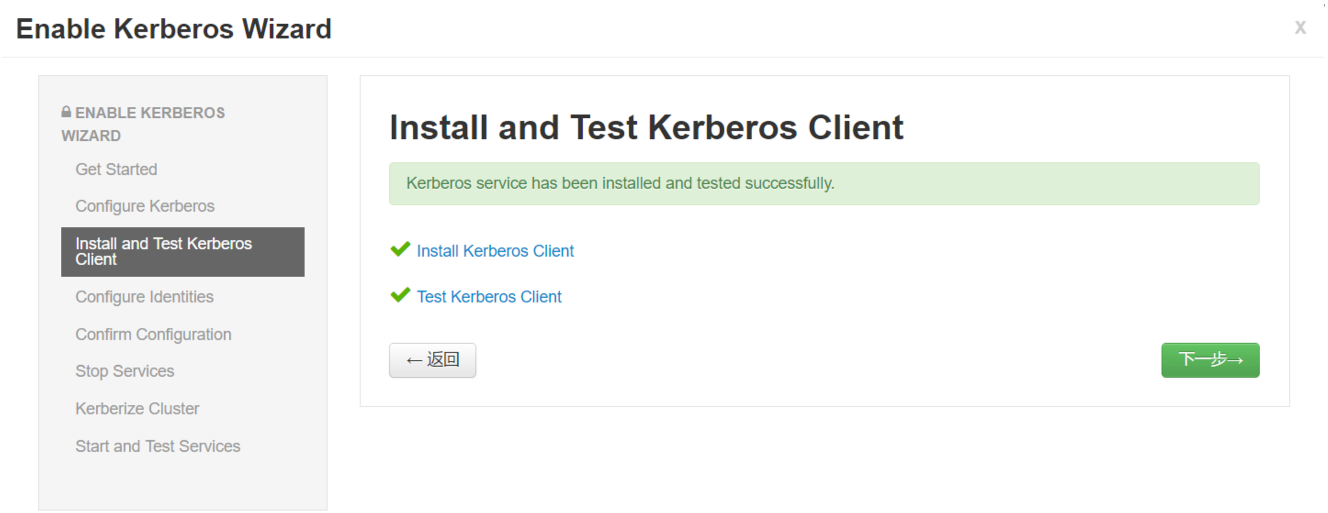
Kadmin host: ochadoop09

Admin principal: admin/admin@ocdp

Admin password: ••••• •••••

□ Save Admin Credentials

☑ 没有配置问题



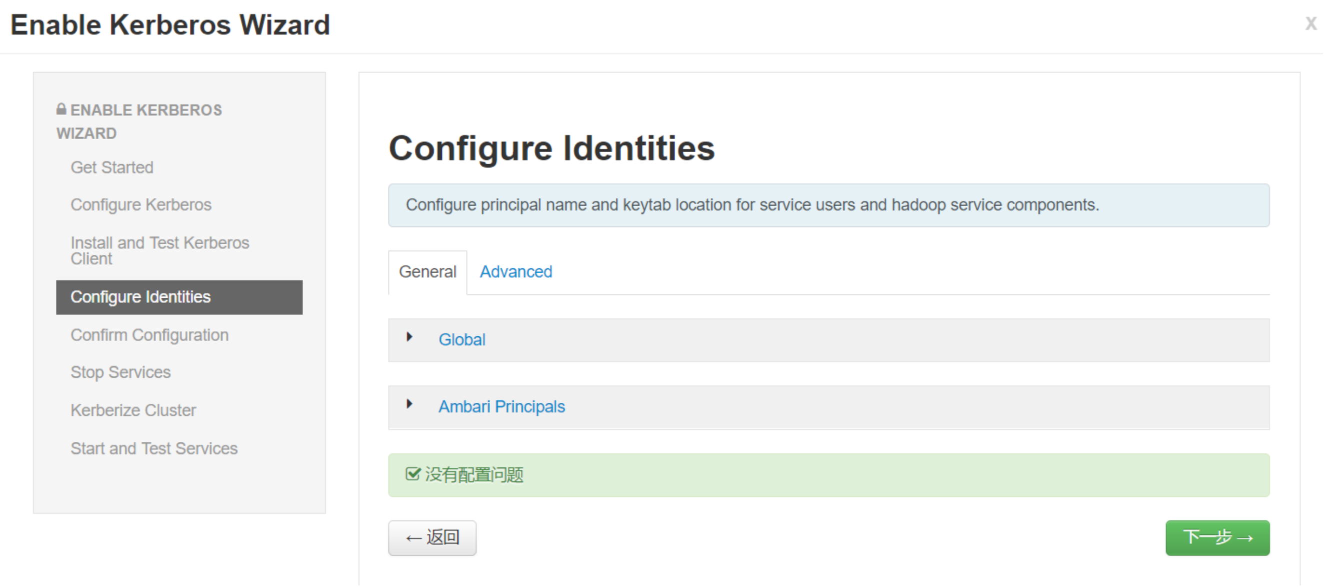
Enable Kerberos Wizard

Install and Test Kerberos Client

Kerberos service has been installed and tested successfully.

✓ Install Kerberos Client

✓ Test Kerberos Client

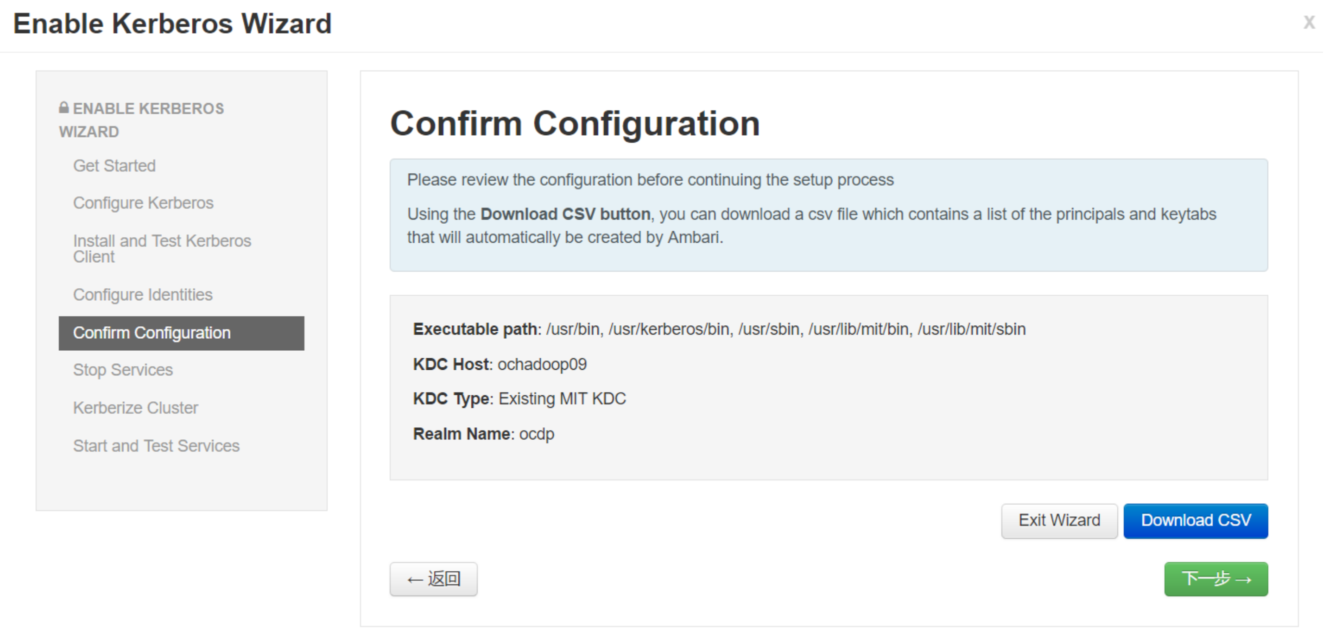


Enable Kerberos Wizard

Configure Identities

Configure principal name and keytab location for service users and hadoop service components.

☑ 没有配置问题



Enable Kerberos Wizard

Confirm Configuration

Please review the configuration before continuing the setup process

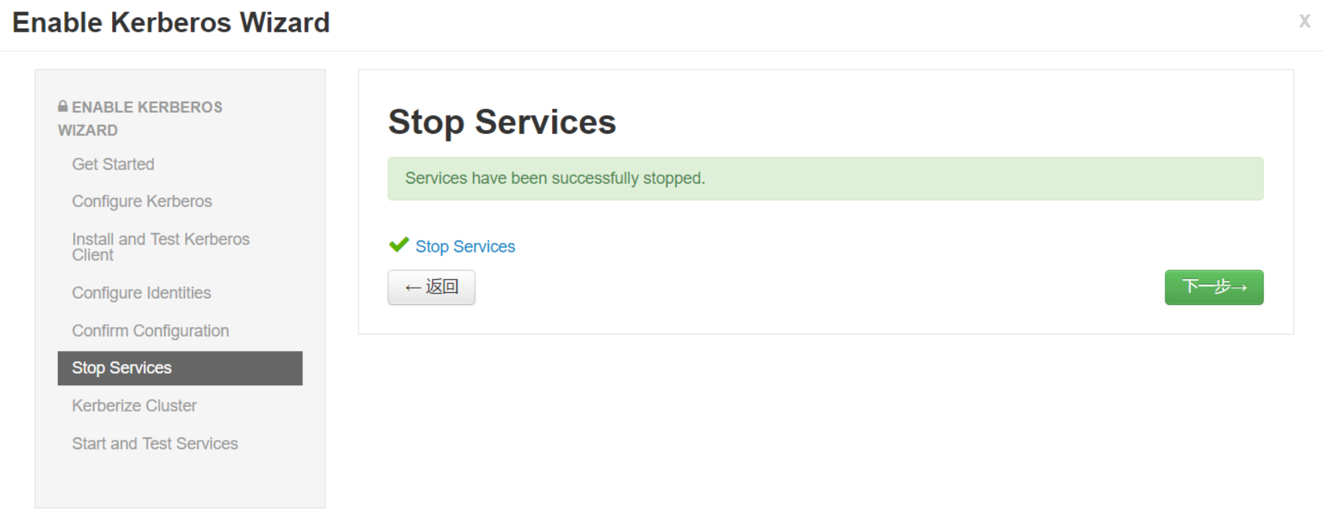
Using the **Download CSV button**, you can download a csv file which contains a list of the principals and keytabs that will automatically be created by Ambari.

Executable path: /usr/bin, /usr/kerberos/bin, /usr/sbin, /usr/lib/mit/bin, /usr/lib/mit/sbin

KDC Host: ochadoop09

KDC Type: Existing MIT KDC

Realm Name: ocdp

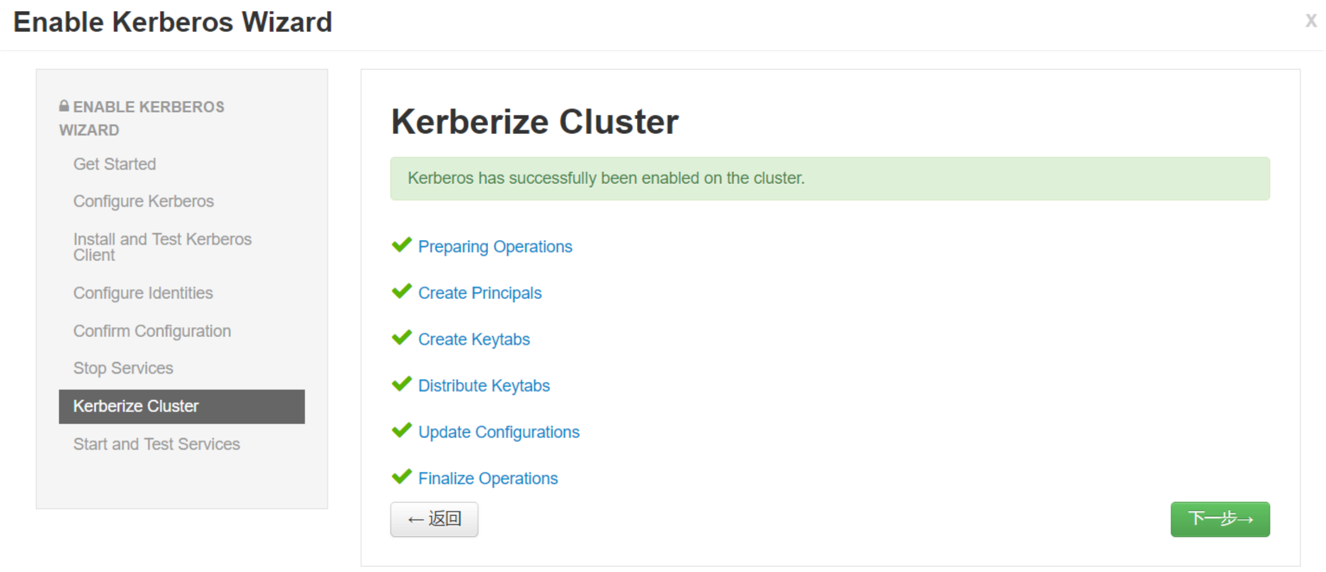


Enable Kerberos Wizard

Stop Services

Services have been successfully stopped.

✓ Stop Services



Enable Kerberos Wizard

ENABLE KERBEROS WIZARD
- Get Started
- Configure Kerberos
- Install and Test Kerberos Client
- Configure Identities
- Confirm Configuration
- Stop Services
- Kerberize Cluster
- Start and Test Services

Kerberize Cluster

Kerberos has successfully been enabled on the cluster.

✓ Preparing Operations

✓ Create Principals

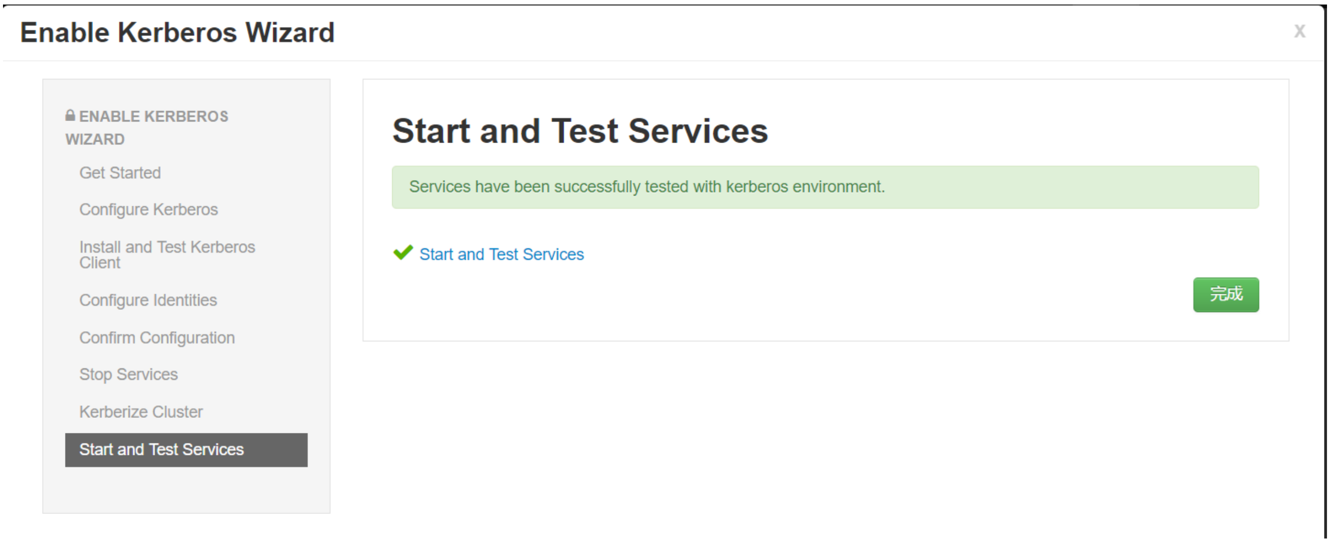
✓ Create Keytabs

✓ Distribute Keytabs

✓ Update Configurations

✓ Finalize Operations

←返回 下一步→



Enable Kerberos Wizard

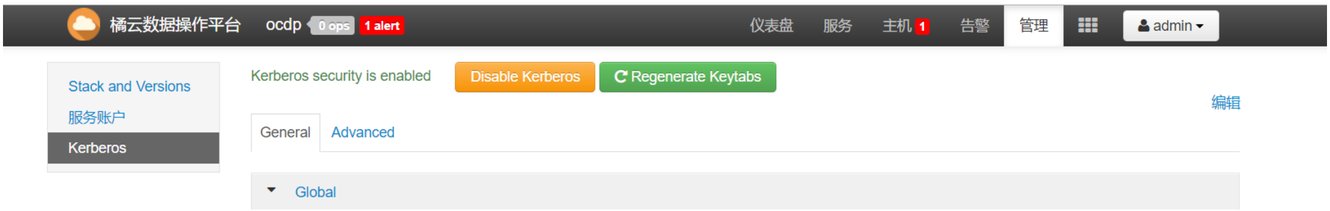
ENABLE KERBEROS WIZARD
- Get Started
- Configure Kerberos
- Install and Test Kerberos Client
- Configure Identities
- Confirm Configuration
- Stop Services
- Kerberize Cluster
- Start and Test Services

Start and Test Services

Services have been successfully tested with kerberos environment.

✓ Start and Test Services

完成



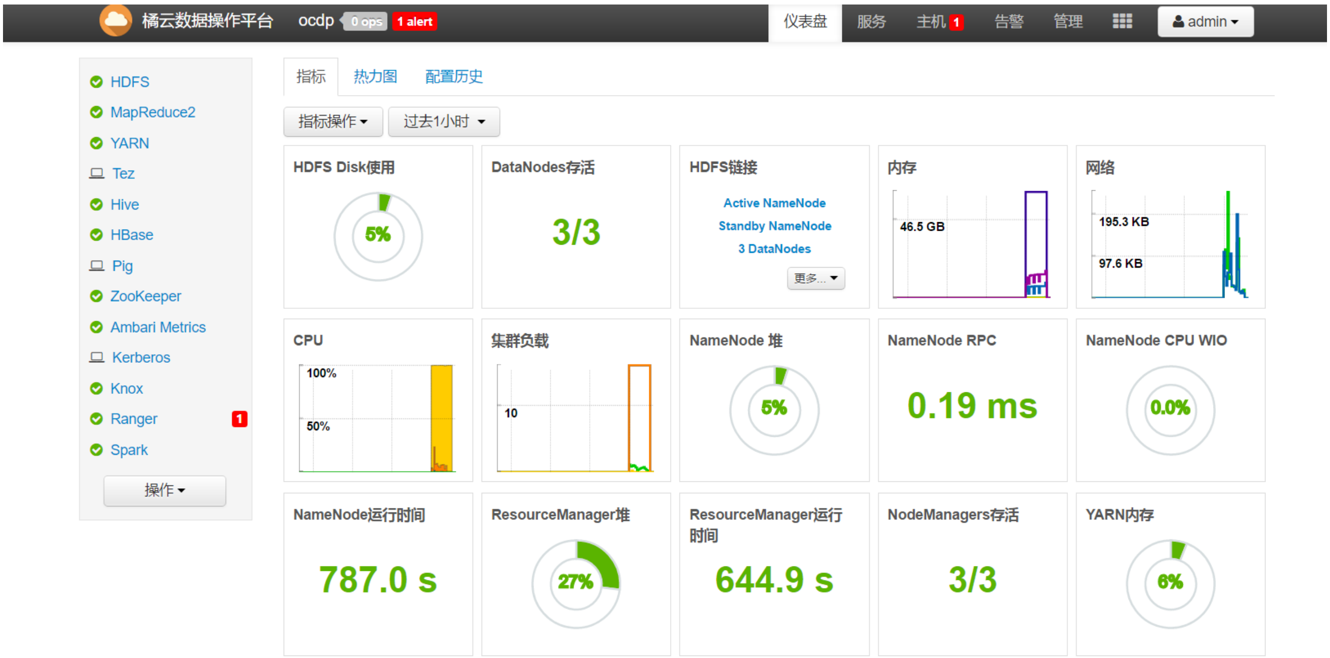
橘云数据操作平台 ocdp 0 ops 1 alert
仪表盘 服务 主机 1 告警 管理 admin
Stack and Versions
服务账户
Kerberos

Kerberos security is enabled Disable Kerberos Regenerate Keytabs

编辑

General Advanced

Global



HDFS Disk使用: 5%

DataNodes存活: 3/3

HDFS链接: Active NameNode, Standby NameNode, 3 DataNodes

内存: 46.5 GB

网络: 195.3 KB, 97.6 KB

CPU: 100%, 50%

集群负载: 10

NameNode 堆: 5%

NameNode RPC: 0.19 ms

NameNode CPU WIO: 0.0%

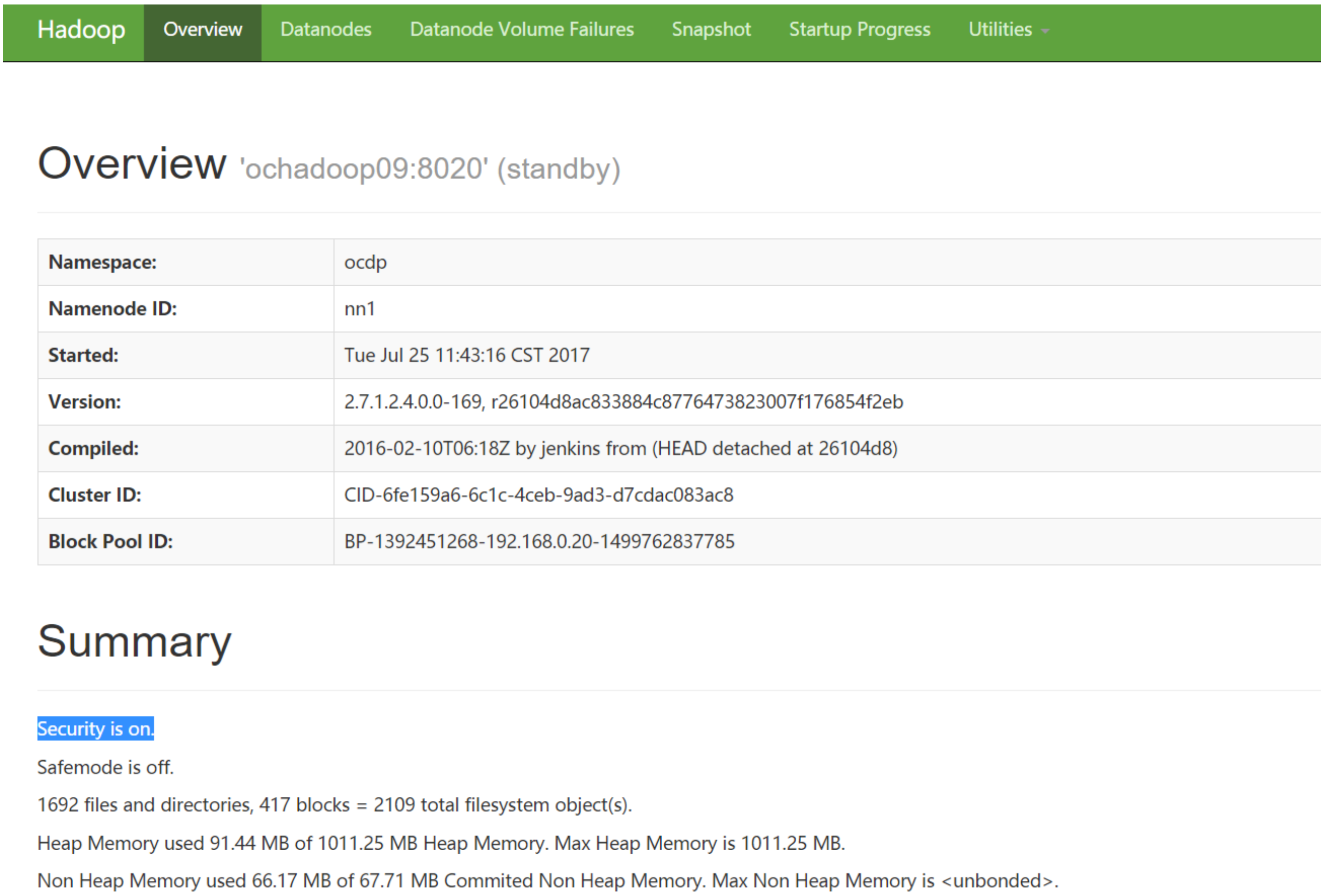
NameNode运行时间: 787.0 s

ResourceManager堆: 27%

ResourceManager运行时间: 644.9 s

NodeManagers存活: 3/3

YARN内存: 6%



Overview 'ochadoop09:8020' (standby)

Namespace:	ocdp
Namenode ID:	nn1
Started:	Tue Jul 25 11:43:16 CST 2017
Version:	2.7.1.2.4.0.0-169, r26104d8ac833884c8776473823007f176854f2eb
Compiled:	2016-02-10T06:18Z by jenkins from (HEAD detached at 26104d8)
Cluster ID:	CID-6fe159a6-6c1c-4ceb-9ad3-d7cdac083ac8
Block Pool ID:	BP-1392451268-192.168.0.20-1499762837785

Summary

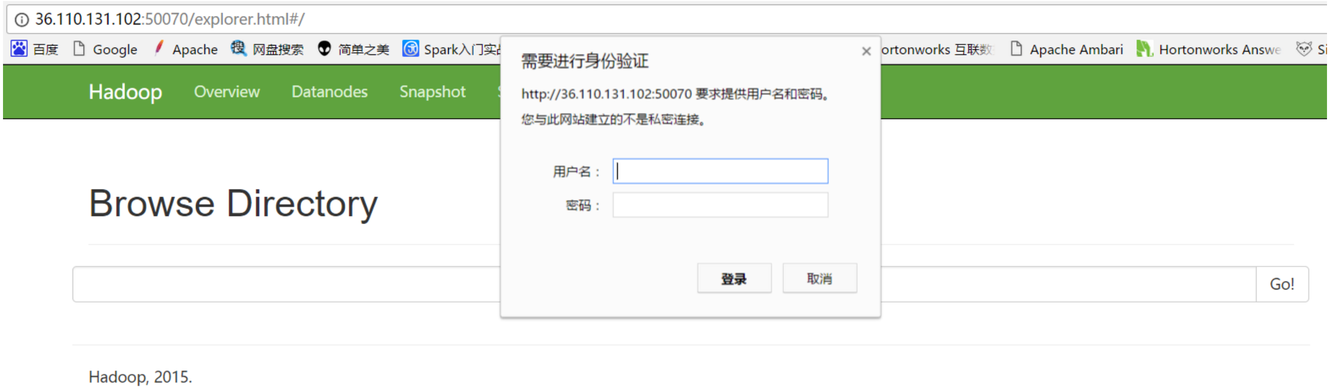
Security is on.

Safemode is off.

1692 files and directories, 417 blocks = 2109 total filesystem object(s).

Heap Memory used 91.44 MB of 1011.25 MB Heap Memory. Max Heap Memory is 1011.25 MB.

Non Heap Memory used 66.17 MB of 67.71 MB Commited Non Heap Memory. Max Non Heap Memory is <unbonded>.



需要进行身份验证

http://36.110.131.102:50070 要求提供用户名和密码。

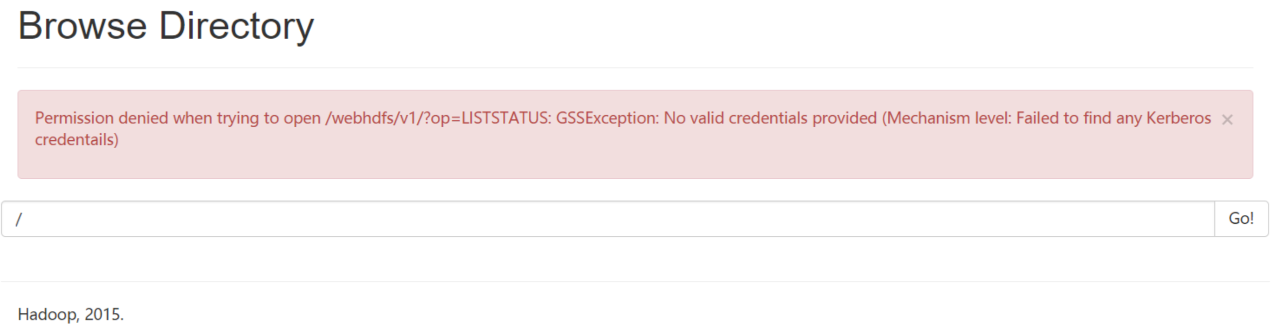
您与此网站建立的不是私密连接。

用户名：

密码：

Browse Directory

Hadoop, 2015.



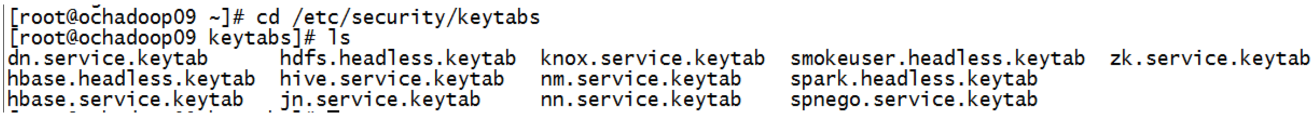
Browse Directory

Permission denied when trying to open /webhdfs/v1/?op=LISTSTATUS: GSSException: No valid credentials provided (Mechanism level: Failed to find any Kerberos credentails)

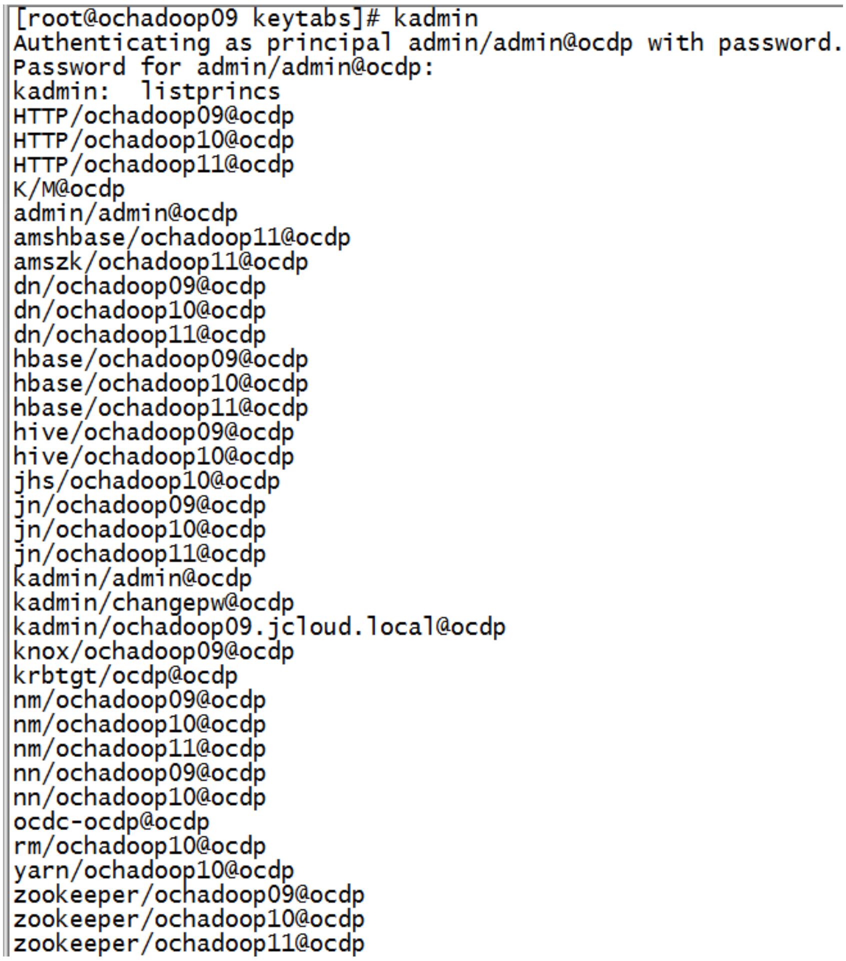
Hadoop, 2015.

7. kerberos集群使用

集群默认的ktb目录： /etc/security/keytabs

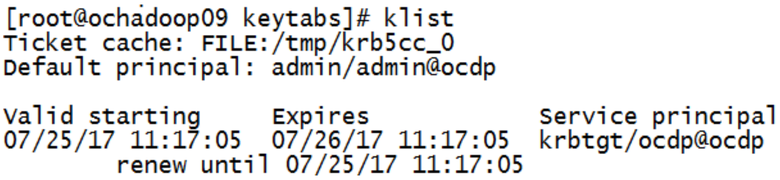


```
[root@ochadoop09 ~]# cd /etc/security/keytabs
[root@ochadoop09 keytabs]# ls
dn.service.keytab       hdfs.headless.keytab   knox.service.keytab   smokeuser.headless.keytab   zk.service.keytab
hbase.headless.keytab   hive.service.keytab    nm.service.keytab     spark.headless.keytab
hbase.service.keytab    jn.service.keytab      nn.service.keytab     spnego.service.keytab
```



```
[root@ochadoop09 keytabs]# kadmin
Authenticating as principal admin/admin@ocdp with password.
Password for admin/admin@ocdp:
kadmin:  listprincs
HTTP/ochadoop09@ocdp
HTTP/ochadoop10@ocdp
HTTP/ochadoop11@ocdp
K/M@ocdp
admin/admin@ocdp
amshbase/ochadoop11@ocdp
amszk/ochadoop11@ocdp
dn/ochadoop09@ocdp
dn/ochadoop10@ocdp
dn/ochadoop11@ocdp
hbase/ochadoop09@ocdp
hbase/ochadoop10@ocdp
hbase/ochadoop11@ocdp
hive/ochadoop09@ocdp
hive/ochadoop10@ocdp
jhs/ochadoop10@ocdp
jn/ochadoop09@ocdp
jn/ochadoop10@ocdp
jn/ochadoop11@ocdp
kadmin/admin@ocdp
kadmin/changepw@ocdp
kadmin/ochadoop09.jcloud.local@ocdp
knox/ochadoop09@ocdp
krbtgt/ocdp@ocdp
nm/ochadoop09@ocdp
nm/ochadoop10@ocdp
nm/ochadoop11@ocdp
nn/ochadoop09@ocdp
nn/ochadoop10@ocdp
ocdc-ocdp@ocdp
rm/ochadoop10@ocdp
yarn/ochadoop10@ocdp
zookeeper/ochadoop09@ocdp
zookeeper/ochadoop10@ocdp
zookeeper/ochadoop11@ocdp
```

列出本机kerberos当前用户信息：klist



```
[root@ochadoop09 keytabs]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: admin/admin@ocdp

Valid starting     Expires            Service principal
07/25/17 11:17:05  07/26/17 11:17:05  krbtgt/ocdp@ocdp
        renew until 07/25/17 11:17:05
```

总结：

1. 默认集群管理员用户（ocdc）拥有访问集群的权限。

2. kinit test/host@ocdp 这种初始化方式是需要输入密码的，仅限于集群管理员使用。

3.集群租户使用如下方式初始化（不需要密码）：

```
kinit -k -t  test.keytab  test/host@ocdp
```

keytab 文件如下方式生成：

```
kadmin.local -q "addprinc -randkey test/host@ocdp"
kadmin.local -q "xst  -k test-unmerged.keytab  test/host@ocdp"
ktutil
 rkt test-unmerged.keytab
 wkt test.keytab
 exit
```

hdfs使用

执行相关命令前需要使用kinit初始化keytab

hive使用：

```
beeline -u "jdbc:hive2://ochadoop10:10000/default;principal=hive/ochadoop10@ocdp" -n  test/host@ocdp  -p  test
```

```
beeline -u "jdbc:hive2://ochadoop10:10000/default;principal=hive/ochadoop10@ocdp" -n  yinkp/ochadoop09@ocdp  -p  yinkp
```

Hbase使用：

进入Hbase shell 前需要执行相关命令前需要使用kinit初始化keytab

kerberos 用户失效时间配置:

http://www.cnblogs.com/morvenhuang/p/4607790.html