Enabling Kerberos Authentication Using the Wizard

* openldap-clients on the Cloudera Manager Server host
* krb5-workstation, krb5-libs on ALL hosts

[root@node0 ~]# yum install -y openldap-clients

[root@node0 ~]# yum install -y krb5-workstation krb5-libs

# Step 2: Installing JCE Policy File for AES-256 Encryption

Baixar o arquivo de policies direto do site da Oracle

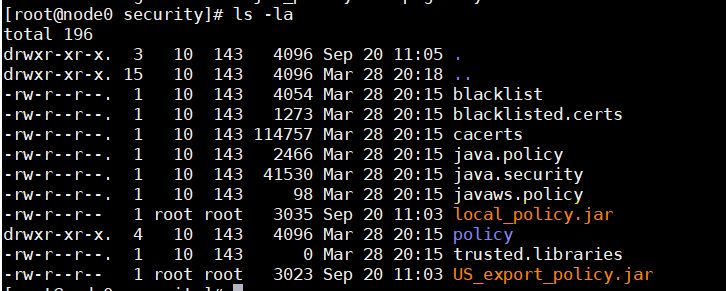
<https://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html>

wget <http://download.oracle.com/otn-pub/java/jce/8/jce_policy-8.zip>

Mover arquivo para pasta:

- local\_policy.jar  
- US\_export\_policy.jar

mv \*policy.jar /usr/java/jdk1.8.0\_171/jre/lib/security



**# Instalar o Kerberos Server**

yum install krb5-server –y

**# Habilitar o serviço do Kerberos krb5 e o kadmin**

[root@node0 security]# systemctl enable krb5kdc

Created symlink from /etc/systemd/system/multi-user.target.wants/krb5kdc.service to /usr/lib/systemd/system/krb5kdc.service.

[root@node0 security]# systemctl enable kadmin

Created symlink from /etc/systemd/system/multi-user.target.wants/kadmin.service to /usr/lib/systemd/system/kadmin.service.

**# Acessar pasta do Kerberos krb5**

[root@node0 krb5kdc]# pwd

/var/kerberos/krb5kdc

[root@node0 krb5kdc]# ls -la

total 16

drwxr-xr-x 2 root root 4096 Sep 20 11:07 .

drwxr-xr-x. 4 root root 4096 Sep 20 11:07 ..

-rw------- 1 root root 22 Apr 10 16:29 kadm5.acl

-rw------- 1 root root 451 Apr 10 16:29 kdc.conf

# Configurar o arquivo krb5.conf

**[root@node0 krb5kdc]# vi /etc/krb5.conf**

[logging]

default = FILE:/var/log/krb5libs.log

kdc = FILE:/var/log/krb5kdc.log

admin\_server = FILE:/var/log/kadmind.log

[libdefaults]

default\_realm = KDC.LAB

dns\_lookup\_realm = false

dns\_lookup\_kdc = false

ticket\_lifetime = 24h

renew\_lifetime = 7d

forwardable = true

udp\_preference\_limit = 1

[realms]

LAB.LOCAL = {

kdc = dc.lab.local:88

admin\_server = dc.lab.local:749

}

KDC.LAB = {

kdc = node0.lab.local:88

admin\_server = node0.lab.local:749

}

[domain\_realm]

.kdc.lab = KDC.LAB

kdc.lab = KDC.LAB

* **copiar krb5.conf para todos os nós.**

**# Configurar arquivo kdc.conf**

cd /var/kerberos/krb5kdc

vi kdc.conf

[kdcdefaults]

kdc\_ports = 88

kdc\_tcp\_ports = 88

[realms]

KDC.LAB = {

kadmind\_port = 749

master\_key\_type = aes256-cts

max\_renewable\_life = 7d 0h 0m 0s

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 rc4-hmac:normal

default\_principal\_flags = +renewable, +forwardable

}

**# Configurar arquivo kadm5.conf**

cd /var/kerberos/krb5kdc

vi kadm5.acl

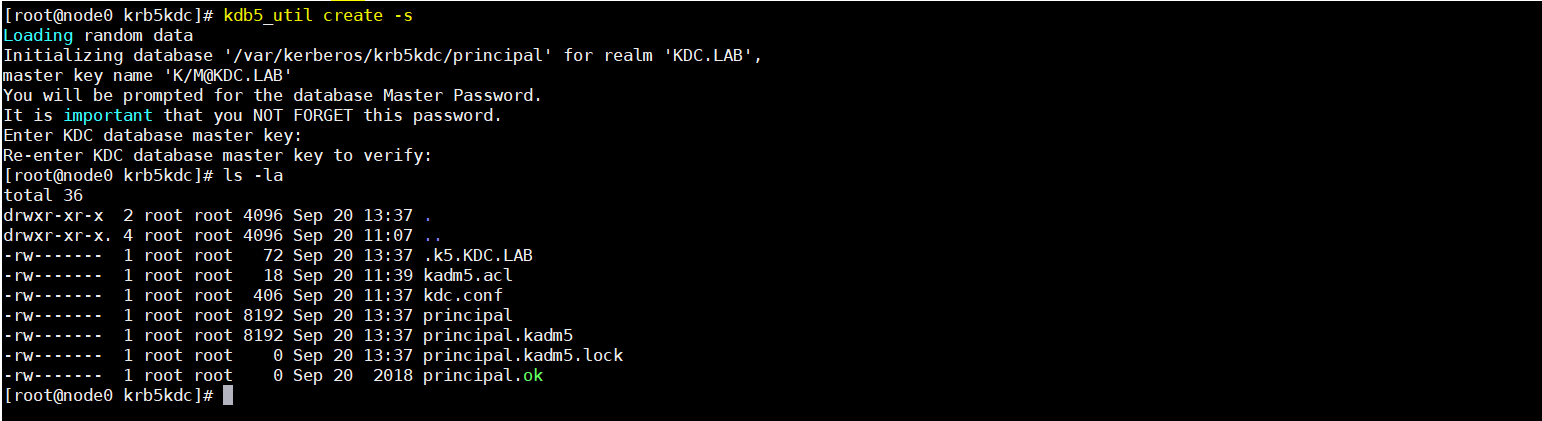
\*/admin@KDC.LAB \*

# Step 3: Create the Kerberos Principal for Cloudera Manager Server

**# Criar o database do Kerberos**

kdb5\_util create –s

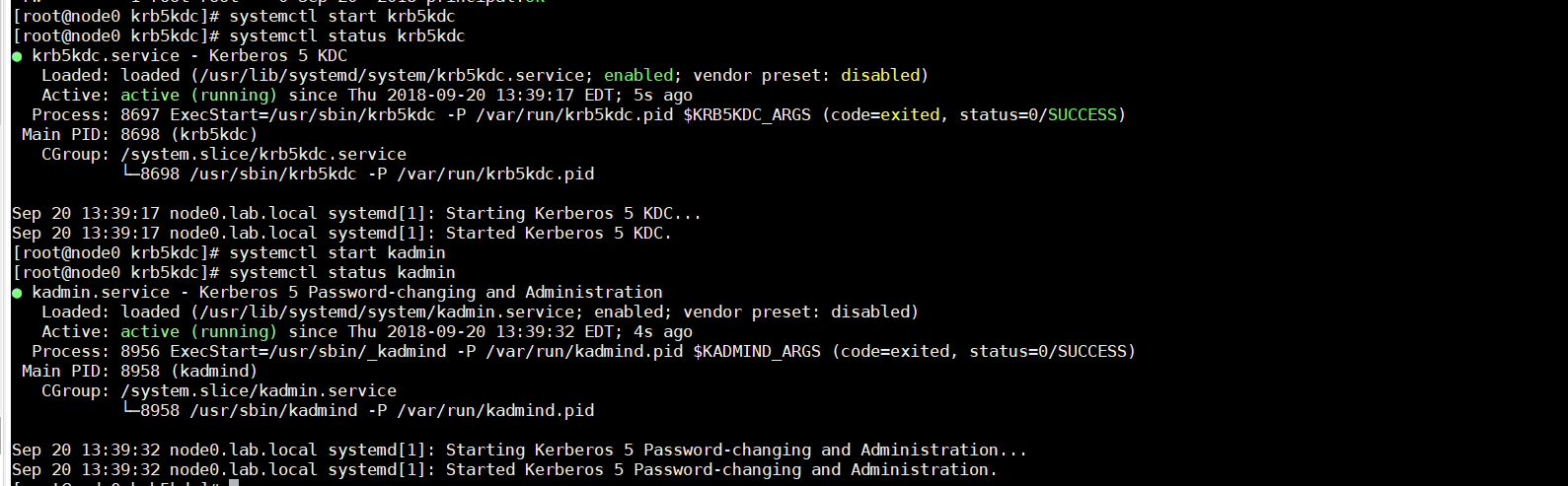
**Defina uma senha para o database do kerberos e depois faça um ls -la para verificar os arquivos criados**



# Iniciando o serviço do kerberos

systemctl start krb5kdc

systemctl start kadmin



# Abrindo o gerenciador de usuários do Kerberos (principals)

Isto abrirá um shell para digitar os comandos do kadmin

**kadmin.local**

**listprincs**

K/M@KDC.LAB

kadmin/admin@KDC.LAB

kadmin/changepw@KDC.LAB

kadmin/node0.lab.local@KDC.LAB

kiprop/node0.lab.local@KDC.LAB

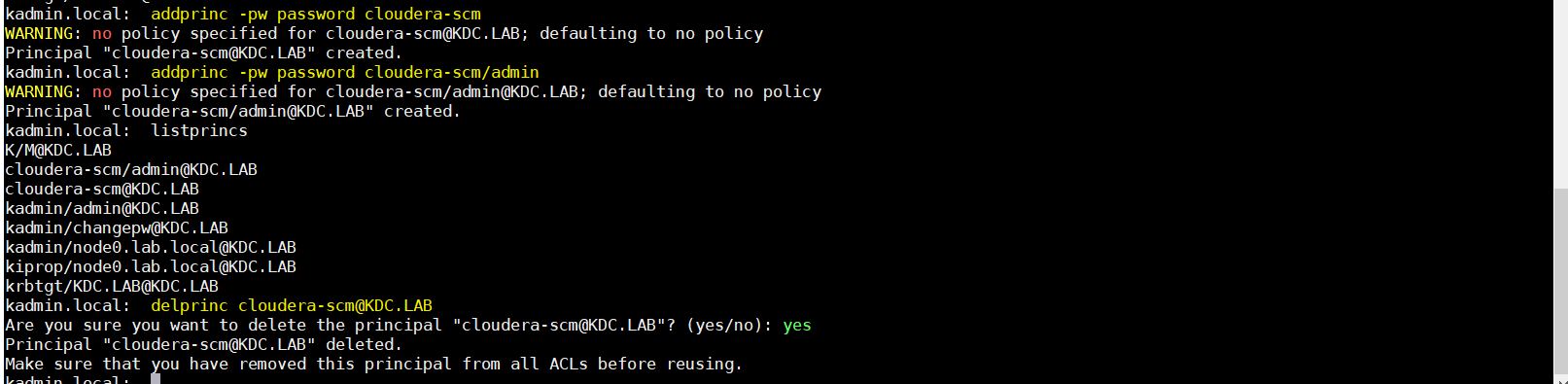
[krbtgt/KDC.LAB@KDC.LAB](mailto:krbtgt/KDC.LAB@KDC.LAB)

# Adicionando um principal

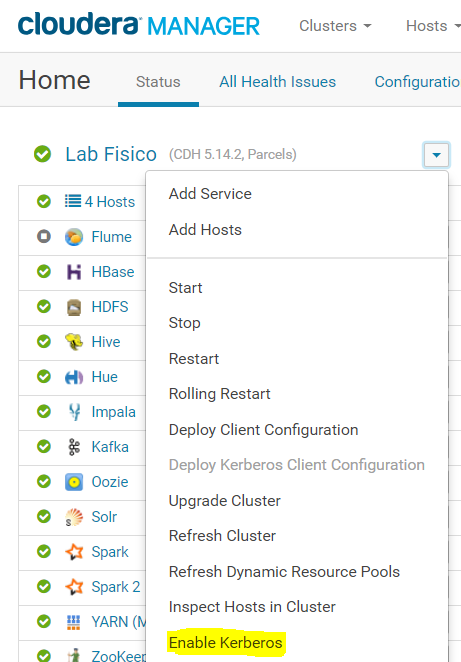
addprinc -pw password cloudera-scm/admin

# Apagando um principal

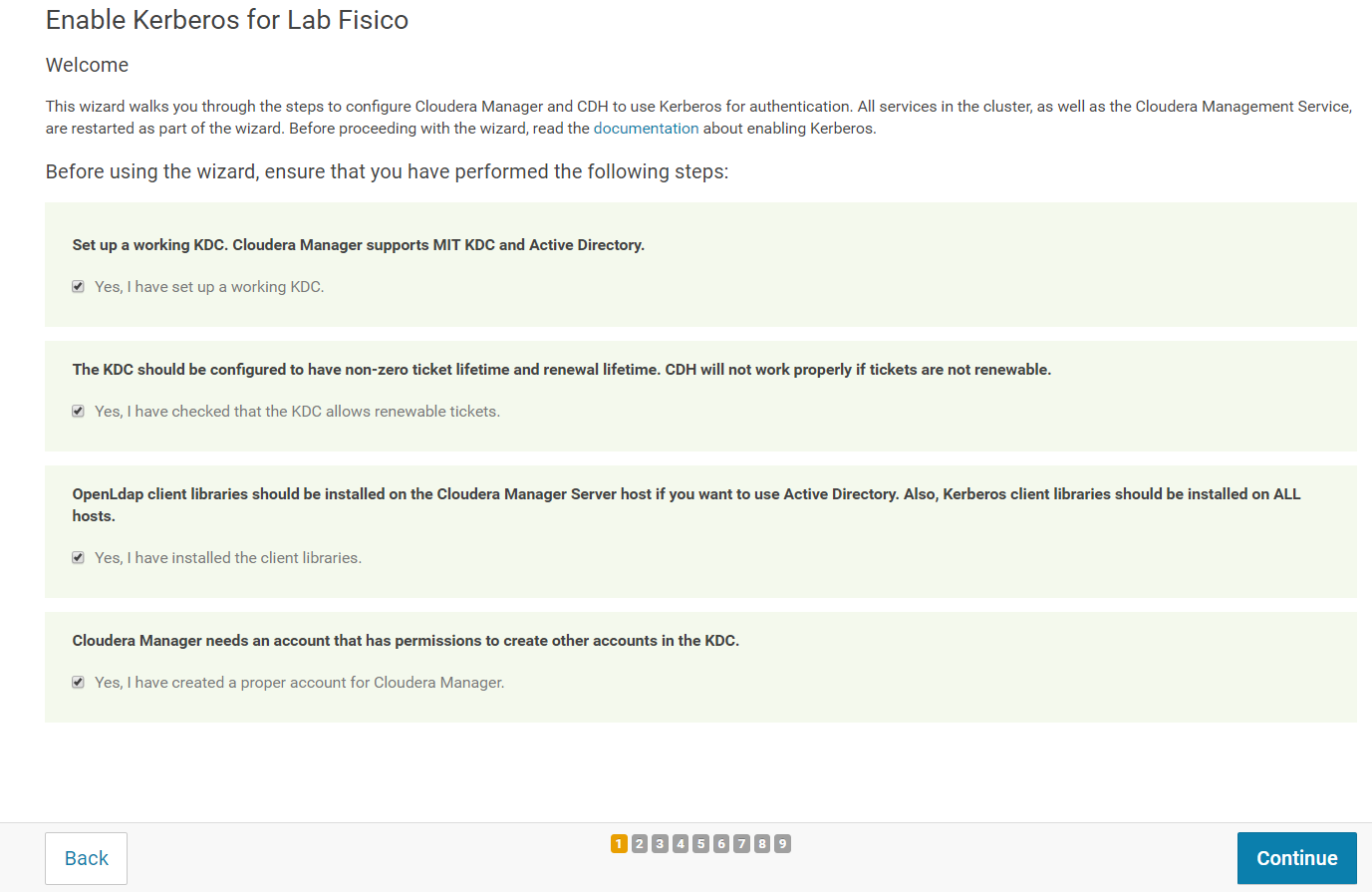
delprinc cloudera-scm@KDC.LAB



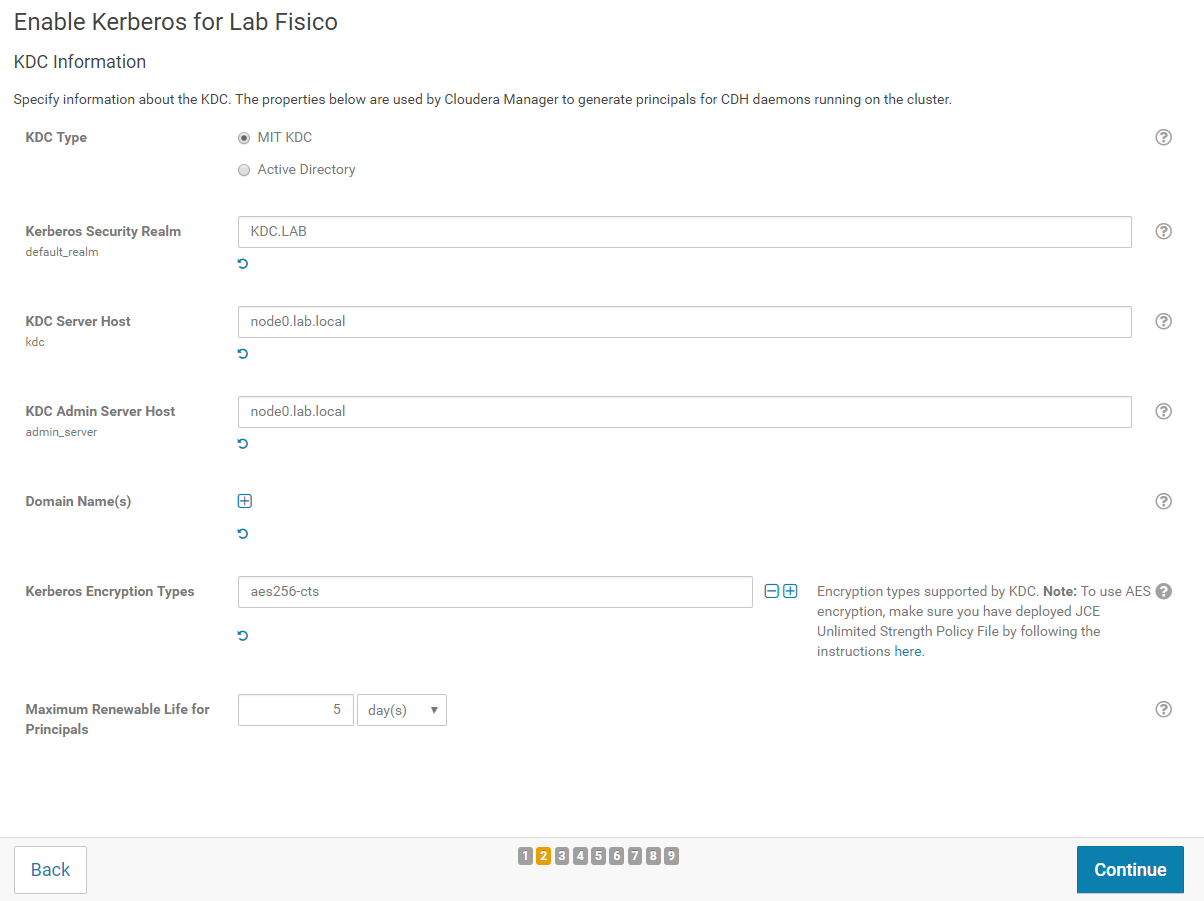
# Step 4: Enabling Kerberos Using the Wizard



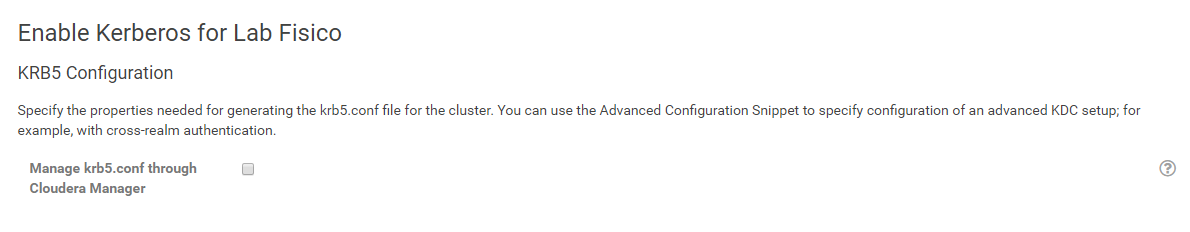
**Marque todas as opções como ‘Yes’ e clique em continuar**



KDC Type : MIT KDC  
Kerberos Security Realm: KDC.LAB   
**# nome do realm criado no arquivo krb5.conf**KDC Server Host: node0.lab.local   
**# nome do host informado no arquivo krb5.conf**KDC Admin Host: node0.lab.local  
**# nome do host informado no arquivo krb5.conf**Kerberos Encryption Types: aes256-cts  
**# nome do realm criado no arquivo kdc.conf**



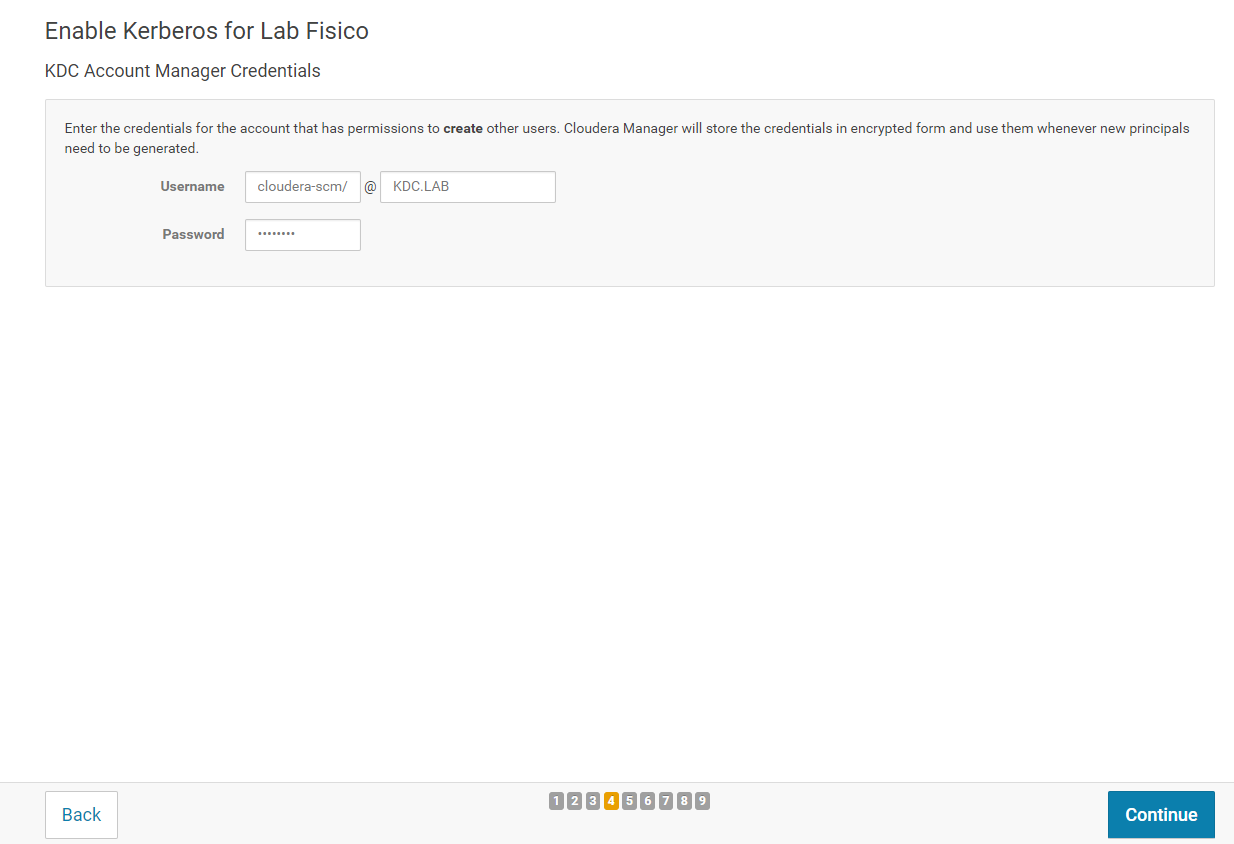
**Caso já tenha configurado manualmente, pule este passo**



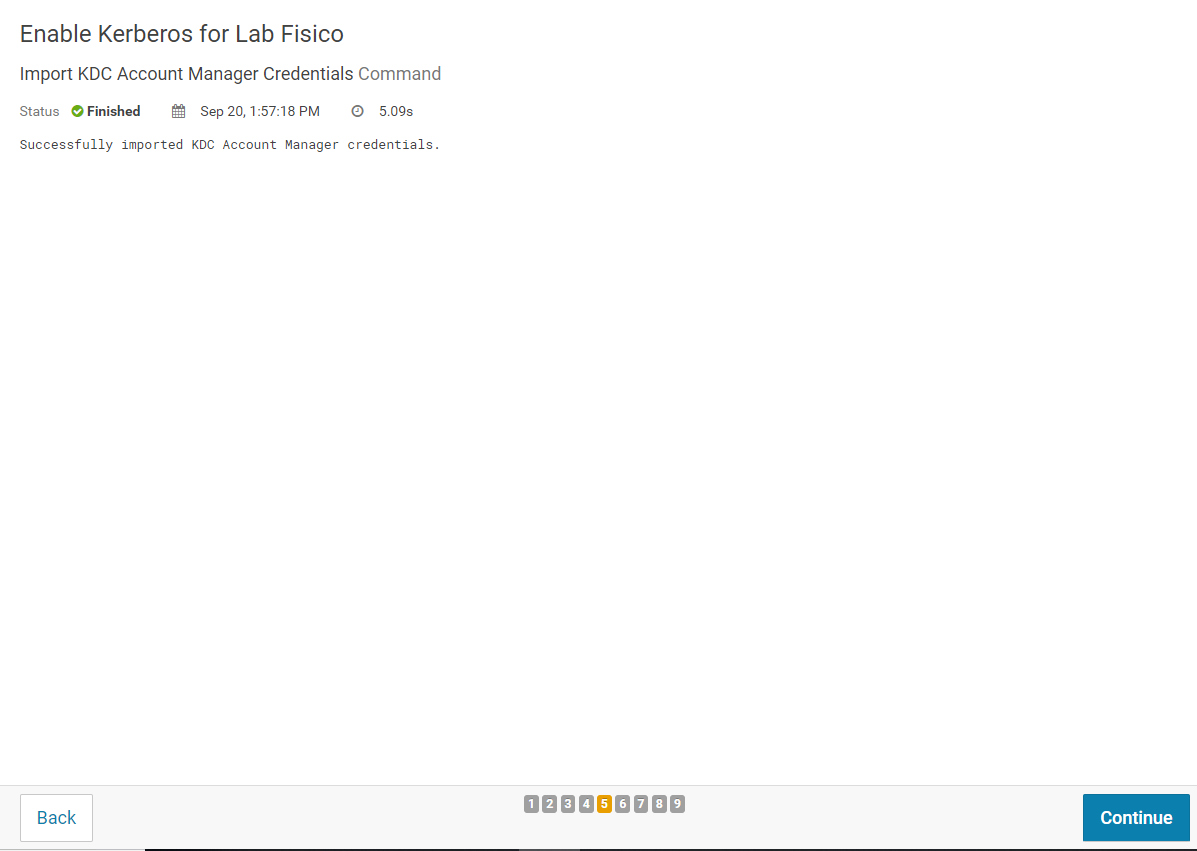
**Username**: cloudera-scm/admin

**Senha**: \*\*\*\*\*\*\*\*\*\*

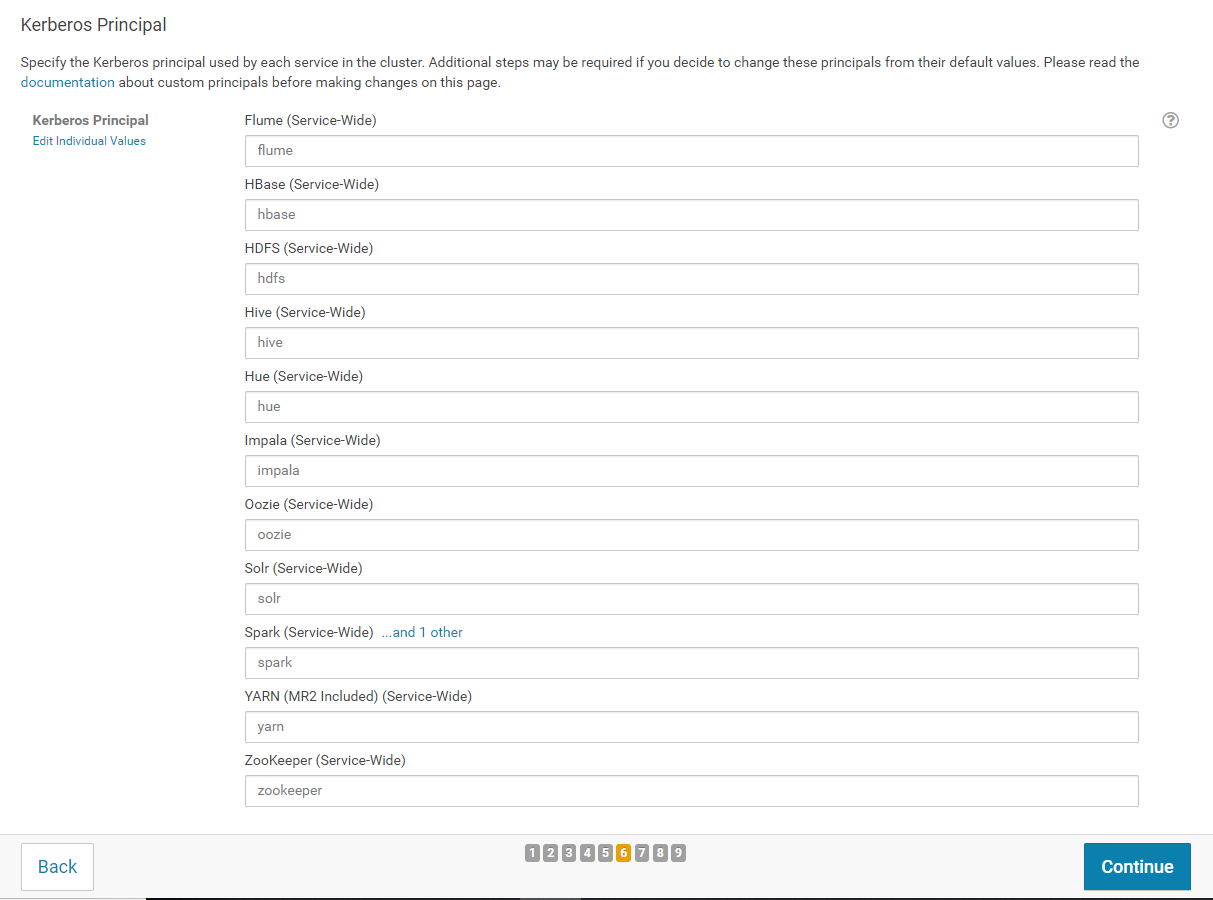
**Informe o usuário e senha e clique em continuar**



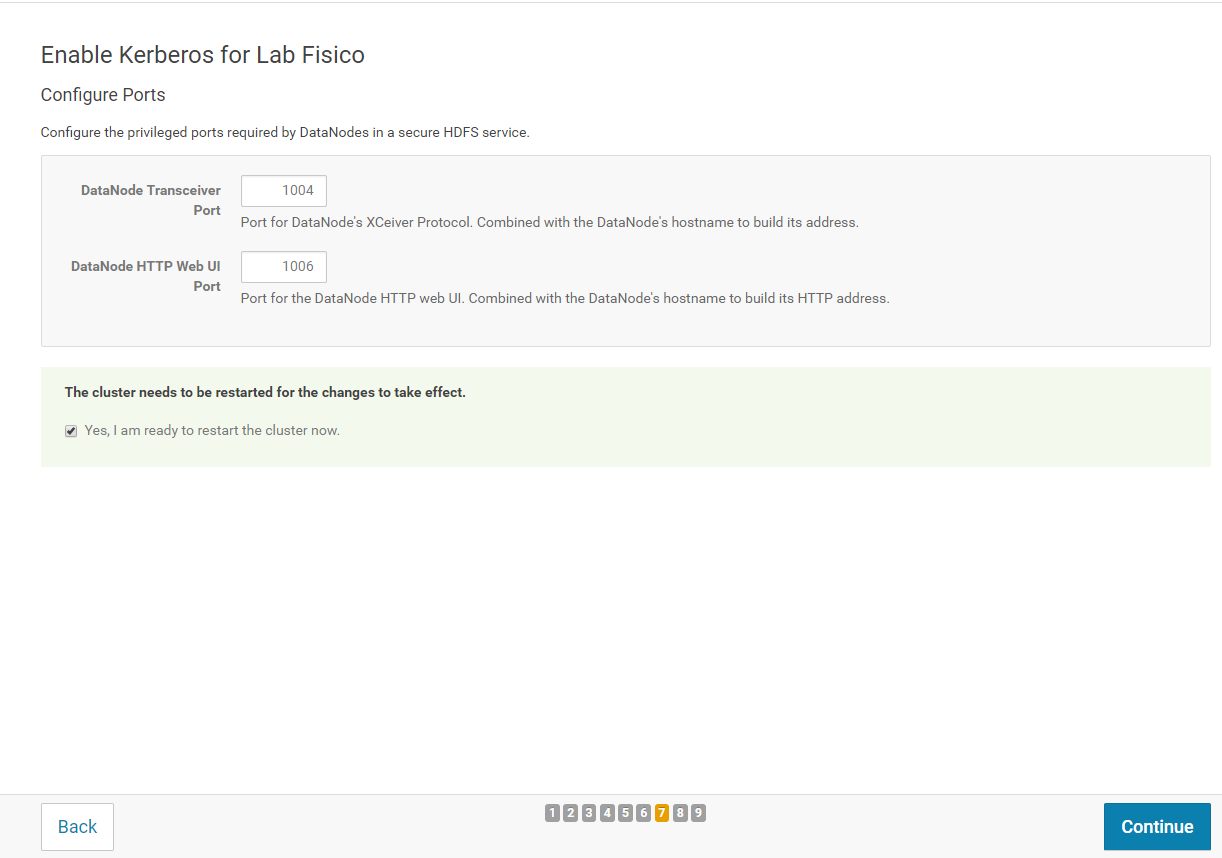
**Aguarde pelo import do KDC, deverá aparecer uma mensagem que a importação das credenciais do KDC Account Manager obtever sucesso. Clique em continuar**



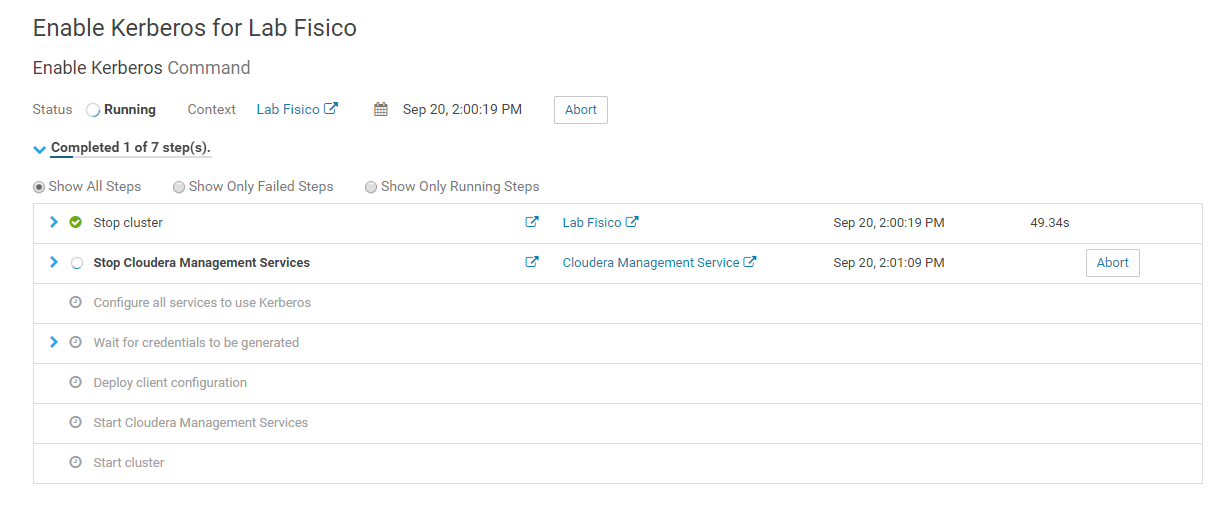
**Agora o Cloudera Manager irá criar os usuários de todos os serviços no Kerberos.**



**Mantenha as mesmas portas especificadas abaixo e clique na opção “Yes, I am ready to restart the cluster now.”**

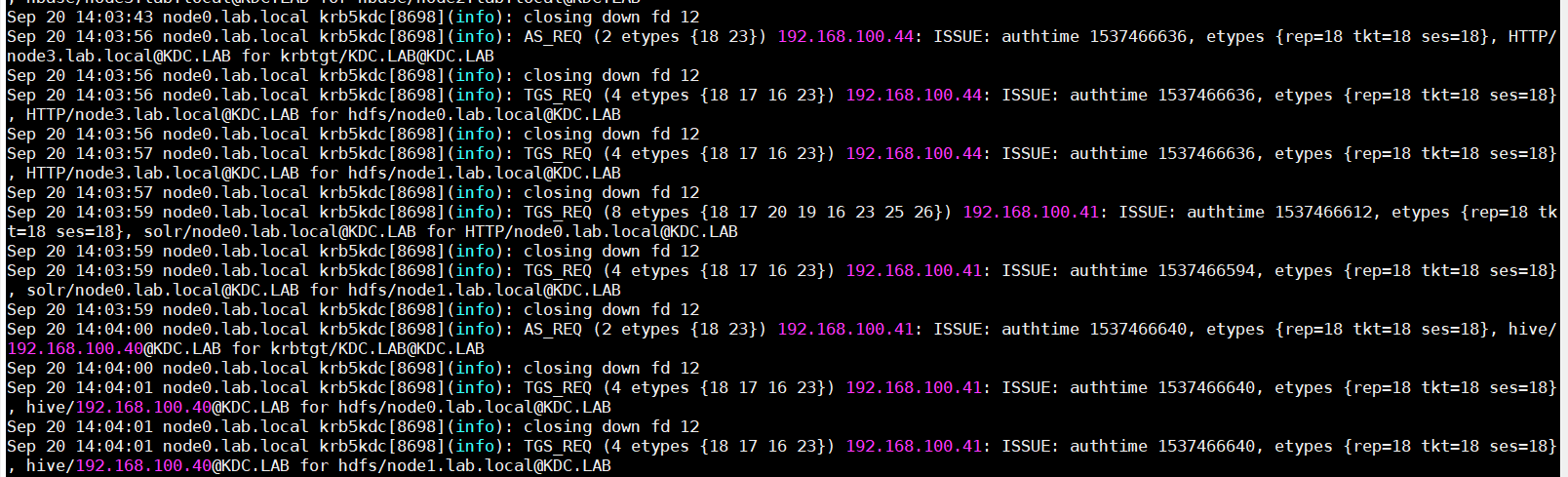


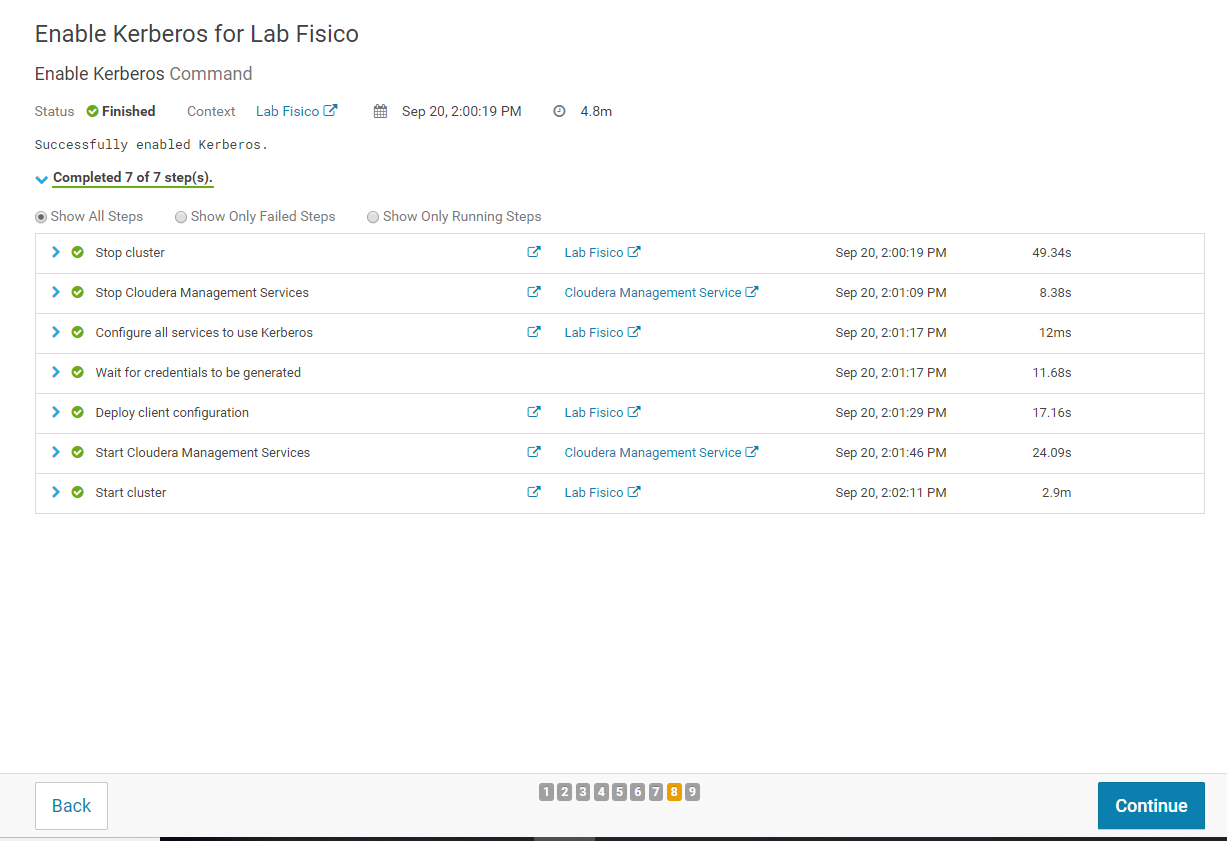
**Aguarde a o reinício do cluster**



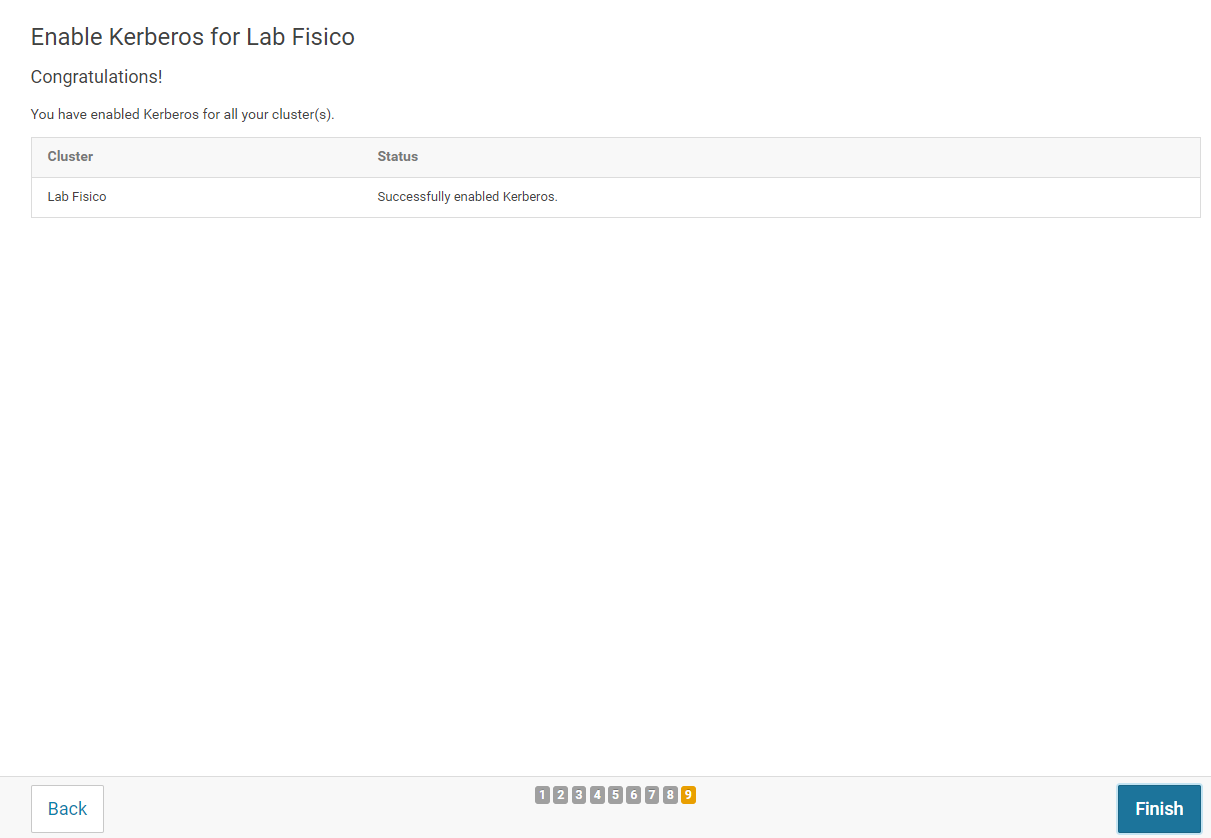
**Enquanto o cluster não reinicia, verifique os logs do krb5kdc na pasta:**

tail –f /var/log/krb5kdc.log

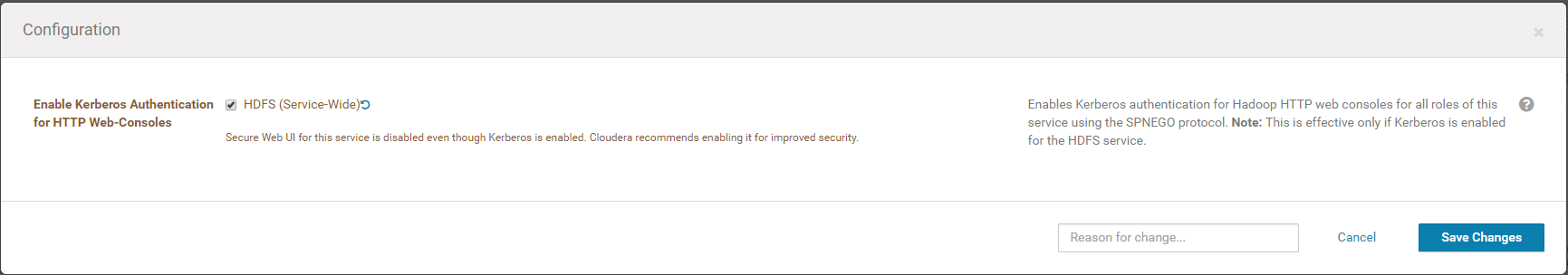


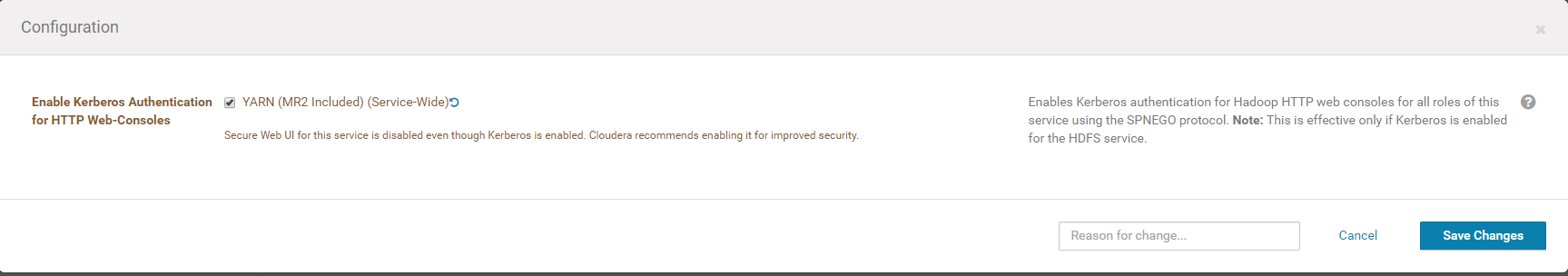


Parabéns você configurou seu primeiro cluster kerberizado!



Habilite a autenticação do Kerberos via HTTP para o HDFS e o YARN e em seguida reinicie os serviços.





# Configuring a Dedicated MIT KDC for Cross-Realm Trust

**PREPARAR CROSS REALM NO AD**

**#Configurar adicionar o trust realm no AD**

NETDOM TRUST KDC.LAB /Domain:LAB.LOCAL /Add /REAlm /passwordT:password

**#Setar criptografia para o trust realm no AD**

ksetup /SetEncTypeAttr KDC.LAB AES256-CTS-HMAC-SHA1-96

**Preparar cross realm no Kerberos**

addprinc -e "aes256-cts:normal" [krbtgt/KDC.LAB@LAB.LOCAL](mailto:krbtgt/KDC.LAB@LAB.LOCAL)

**Digite o comando dentro do kadmin e informe a senha**

kadmin.local: addprinc -e "aes256-cts:normal" krbtgt/KDC.LAB@LAB.LOCAL

WARNING: no policy specified for krbtgt/KDC.LAB@LAB.LOCAL; defaulting to no policy

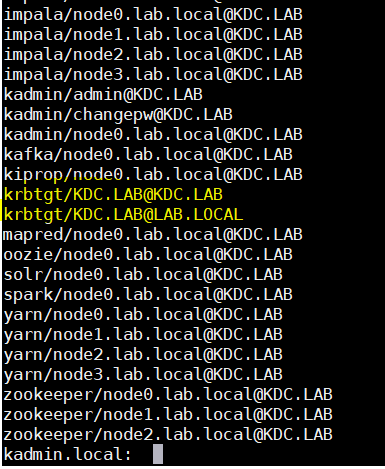
Enter password for principal "krbtgt/KDC.LAB@LAB.LOCAL":

Re-enter password for principal "krbtgt/KDC.LAB@LAB.LOCAL":

Principal "krbtgt/KDC.LAB@LAB.LOCAL" created.

**Digite o comando dentro do kadmin e verifique pelas linhas abaixo, caso elas apareçam, o cross-real foi configurado corretamente.**

**listprincs**



**\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\***

**# Instalar o Sentry, caso não esteja instalado ainda.**

# Instalar os serviços abaixo em todos os nós do cluster

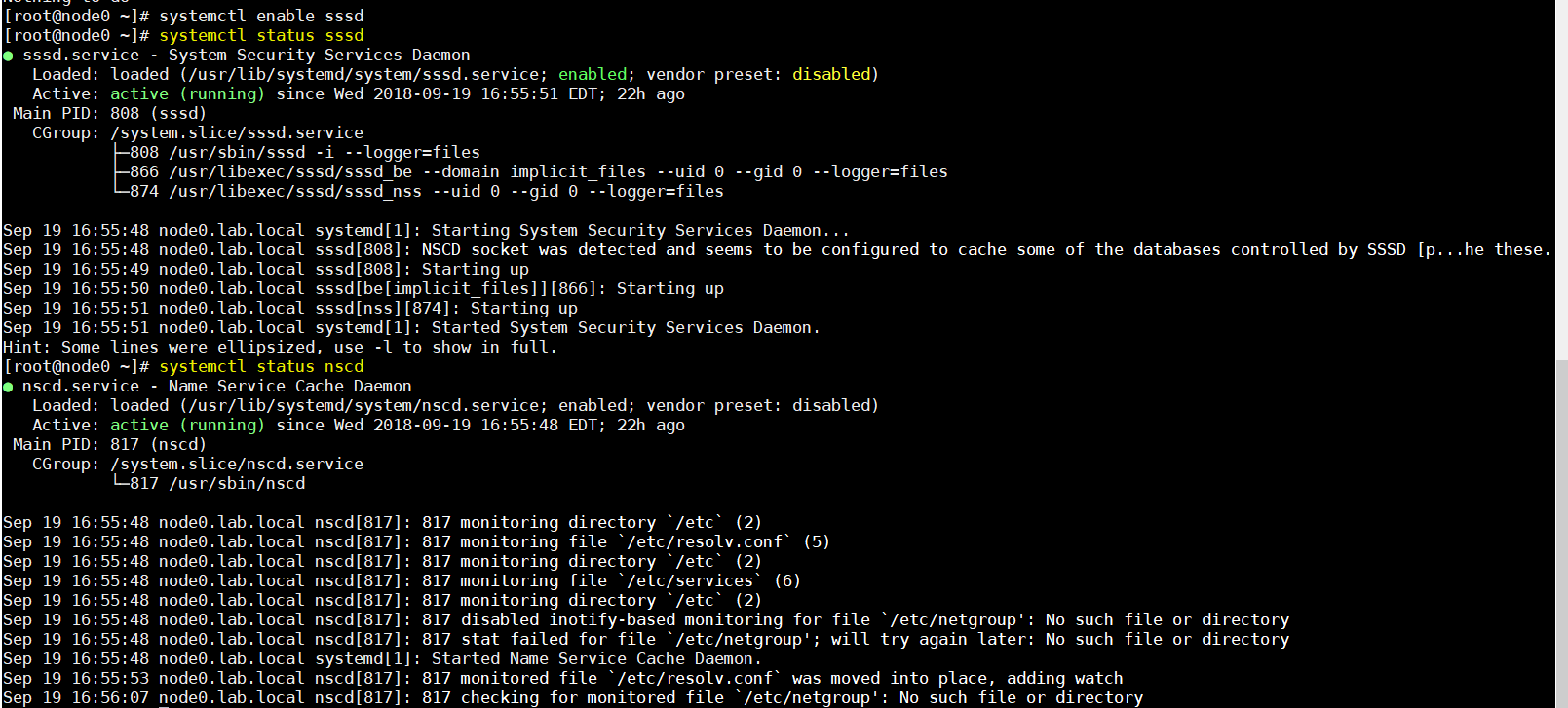
yum install sssd –y

yum install nscd –y

**Habilitar e verificar se os serviços estão rodando**

systemctl enable sssd   
systemctl start sssd

systemctl enable nscd   
systemctl start nscd



**# Criar arquivo sssd.conf**

cd /etc/sssd/

vi sssd.conf

chmod 600 sssd.conf

**# Inserir o texto abaixo e salvar o arquivo**

[sssd]

config\_file\_version = 2

services = nss, pam

domains = lab.local

[domain/LAB.LOCAL]

id\_provider = ad

override\_homedir = /home/%u

default\_shell = /bin/bash

ad\_servers = c2n1.lab.local

[root@node0 ~]# systemctl status sssd

● sssd.service - System Security Services Daemon

Loaded: loaded (/usr/lib/systemd/system/sssd.service; enabled; vendor preset: disabled)

Active: active (running) since Thu 2018-09-20 20:38:27 -03; 53s ago

Main PID: 15787 (sssd)

CGroup: /system.slice/sssd.service

├─15787 /usr/sbin/sssd -i --logger=files

├─15790 /usr/libexec/sssd/sssd\_be --domain LAB.LOCAL --uid 0 --gid 0 --logger=files

├─15791 /usr/libexec/sssd/sssd\_nss --uid 0 --gid 0 --logger=files

└─15792 /usr/libexec/sssd/sssd\_pam --uid 0 --gid 0 --logger=files

Sep 20 20:38:27 node0.lab.local sssd\_be[15790]: GSSAPI client step 2

Sep 20 20:38:27 node0.lab.local systemd[1]: Started System Security Services Daemon.

Sep 20 20:38:28 node0.lab.local sssd[15787]: ; TSIG error with server: tsig verify failure

Sep 20 20:38:28 node0.lab.local sssd[15787]: update failed: REFUSED

Sep 20 20:38:28 node0.lab.local sssd[15787]: ; TSIG error with server: tsig verify failure

Sep 20 20:38:28 node0.lab.local sssd[15787]: update failed: REFUSED

Sep 20 20:38:35 node0.lab.local sssd\_be[15790]: GSSAPI client step 1

Sep 20 20:38:35 node0.lab.local sssd\_be[15790]: GSSAPI client step 1

Sep 20 20:38:35 node0.lab.local sssd\_be[15790]: GSSAPI client step 1

Sep 20 20:38:35 node0.lab.local sssd\_be[15790]: GSSAPI client step 2

**# Rodar o comando authconfig**

authconfig --enablesssd --enablesssdauth --enablemkhomedir --update

**# Instalar o samba em todos os nós**

yum install samba –y

**# Iniciar o serviço em todos os nós**

systemctl start smb

**# Configurar o arquivo smb.conf em todos os nós**

**cd /etc/samba/smb.conf**

[root@node0 ~]# cat /etc/samba/smb.conf

[global]

netbios name = node0

workgroup = LAB

security = ADS

realm = LAB.LOCAL

encrypt passwords = yes

kerberos method = secrets and keytab

dedicated keytab file = /etc/krb5.keytab

**# Adicionar o nó do hadoop no AD em todos os nós**

net ads join createupn=host/node0 createcomputer=ou=cloudera,dc=lab,dc=local -S dc.lab.local -U cloudera%'Compwire@352'

**# Verificar se o krb5.keytab**

klist -kt /etc/krb5.keytab

Keytab name: FILE:/etc/krb5.keytab

KVNO Timestamp Principal

---- ------------------- ------------------------------------------------------

2 09/20/2018 16:40:49 host/node2.lab.local@LAB.LOCAL

2 09/20/2018 16:40:49 host/NODE2.LAB.LOCAL@LAB.LOCAL

2 09/20/2018 16:40:50 host/node2.lab.local@LAB.LOCAL

2 09/20/2018 16:40:50 host/NODE2.LAB.LOCAL@LAB.LOCAL

2 09/20/2018 16:40:50 host/node2.lab.local@LAB.LOCAL

2 09/20/2018 16:40:50 host/NODE2.LAB.LOCAL@LAB.LOCAL

2 09/20/2018 16:40:50 host/node2.lab.local@LAB.LOCAL

2 09/20/2018 16:40:50 host/NODE2.LAB.LOCAL@LAB.LOCAL

2 09/20/2018 16:40:50 host/node2.lab.local@LAB.LOCAL

2 09/20/2018 16:40:50 host/NODE2.LAB.LOCAL@LAB.LOCAL

2 09/20/2018 16:40:50 NODE2.LAB.LOCAL$@LAB.LOCAL

2 09/20/2018 16:40:50 NODE2.LAB.LOCAL$@LAB.LOCAL

2 09/20/2018 16:40:50 NODE2.LAB.LOCAL$@LAB.LOCAL

2 09/20/2018 16:40:50 NODE2.LAB.LOCAL$@LAB.LOCAL

2 09/20/2018 16:40:50 NODE2.LAB.LOCAL$@LAB.LOCAL

2 09/20/2018 16:40:50 host/node2.lab.local@KDC.LAB

2 09/20/2018 16:40:50 host/node2.lab.local@KDC.LAB

2 09/20/2018 16:40:50 host/node2.lab.local@KDC.LAB

2 09/20/2018 16:40:50 host/node2.lab.local@KDC.LAB

2 09/20/2018 16:40:50 [host/node2.lab.local@KDC.LAB](mailto:host/node2.lab.local@KDC.LAB)

# Trocar o timezone do SO

timedatectl set-timezone America/Sao\_Paulo