**Инструкция за работа с CentOS 7.9.x core**

**Работни часове по изграждането на цялостното специализирано решение - 76.  
Екип, отговорен по изпълнението:  
1. Мениджър проект  
2. Супервайзер  
3. Линукс системен администратор  
4. Линукс системен администратор  
Реализирано: Юли месец, 2021г.**

**1. Инсталиране на CentOS 7.9.x core**

**2. Добавяне на Epel-Release**

# yum -y install epel-release

# yum update

**3. Инсталиране на допълнителни програми**

# yum -y install mc nano wget curl zip unzip

**4. Смяна да името на сървъра**

# hostnamectl set-hostname ldap.obs-02.local

**5. Инсталиране на пакети за Ldap 2.4.x**

# yum -y install openldap compat-openldap openldap-clients openldap-servers openldap-servers-sql openldap-devel

**6. Инсталиране на Пакет Samba и Name сървър**

# yum -y install samba samba-common bind bind-utils

**7. Инсталиране на Пакет smbldap-tools**

# yum -y install smbldap-tools

**8. Настройка name server:**

**Копиране на файл bpk.tar.gz (ще бъде предоставен) /root/**

**Експортиране на базата от стартият сървър:**

**#** slapcat -n 1 -l data.ldif

# scp data.ldif root@new\_server:/root/bkp/ldif

# cd /root/

# tar -xf bkp.tar.gz

**8.1 Копиране на Зона от Предоставеният архив : obs-02.local.zone в /etc/named**

**8.2 Сменя на IP адрес според новият хост file obs-02.local.zone :**

A 192.168.10.70

srv-pdc-01 192.168.10.70

**8.3 Смяна на IP адрес според новият хост file /etc/named.conf :**

listen-on port 53 { 192.168.10.70; };

allow-query { localhost;192.168.0.0/16; };

**8.4 Добавяне на зона**

zone "obs-02.local" IN {

type master;

file "/etc/named/obs-02.local.zone";

allow-update { none; };

};

**8.5 Стартиране на услугата на BIND**

# systemctl enable named

# systemctl start named

# systemctl status named

**9. Описване на новият Name сървър в /etc/resolv.conf (според IP адрес)**

search obs-02.local

nameserver 192.168.10.70

-------------- Ldap --------------

**9.1 Копиране на OBS tools**

**# cp -r /root/bkp/etc/obs /etc/**

**9.2 Копират се схемите на OBS в /etc/openldap/schema**

**# cp -r /root/bkp/etc/openldap/\* /etc/openldap/**

**9.3 Импортиране на базата:**

**# rm -rf /etc/openldap/slapd.d/\***

**# cp /usr/share/openldap-servers/DB\_CONFIG.example /var/lib/ldap/DB\_CONFIG**

**# slapadd -n 0 -F /etc/openldap/slapd.d -l /root/bkp/ldif/config.ldif**

**# slapadd -n 1 -F /etc/openldap/slapd.d -l /root/bkp/ldif/data.ldif**

**9.4 Смяна на правата**

# chown -R ldap:ldap /var/lib/ldap/.

# chown -R ldap:ldap /etc/openldap/slapd.d/.

**9.5 Стартиране на LDAP**

# systemctl start slapd

# systemctl status slapd

# systemctl enable slapd.service

**9.6 Проверка на конфигурацията:**

[root@ldap ~]# ldapsearch -Y EXTERNAL -Q -H ldapi:/// -LLL -o ldif-wrap=no -b cn=config '(objectClass=olcDatabaseConfig)' ''

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}bdb,cn=config

dn: olcDatabase={1}monitor,cn=config

**9.6.1 Фикс монитор ( Ако е нужно)**

vi monitor.ldif

dn: olcDatabase={1}monitor,cn=config

changetype: modify

replace: olcAccess

olcAccess: {0}to \* by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external, cn=auth" read by dn.base="cn=ldaproot,dc=obs,dc=local" read by \* none

# ldapmodify -Y EXTERNAL -H ldapi:/// -f monitor.ldif

**9.7 Проверка на инпортирани схеми:**

[root@ldap ~]# ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=config" '(objectClass=\*)' dn -LLL

SASL/EXTERNAL authentication started

SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth

SASL SSF: 0

dn: cn=config

dn: cn=schema,cn=config

dn: cn={0}core,cn=schema,cn=config

dn: cn={1}cosine,cn=schema,cn=config

dn: cn={2}inetorgperson,cn=schema,cn=config

dn: cn={3}nis,cn=schema,cn=config

dn: cn={4}samba,cn=schema,cn=config

dn: cn={5}outlook,cn=schema,cn=config

dn: cn={6}mozilla,cn=schema,cn=config

dn: cn={7}obs,cn=schema,cn=config

dn: cn={8}authldap,cn=schema,cn=config

dn: olcDatabase={-1}frontend,cn=config

dn: olcDatabase={0}config,cn=config

dn: olcDatabase={1}bdb,cn=config

dn: olcDatabase={1}monitor,cn=config

**9.8 Проверка на Администраторски профил:**

[root@ldap ~]# slapcat -n 0 -a '(olcRootDN=\*)' | egrep '^dn:|olcRootDN|olcRootPW'

dn: olcDatabase={1}bdb,cn=config

olcRootDN: cn=ldaproot,dc=obs,dc=local

olcRootPW:: \*\*\*\*NTSEF9cTdydk\*\*\*\*\*\*\*\*\*\*TZTRV\*\*\*GV2NT\*\*\*

**9.8.1 Проверка Админ парола.**

**[root@ldap ~]# ldapwhoami -x -w "3esti1mld@p3" -D cn=ldaproot,dc=obs,dc=local -ZZ -H ldap://ldap.obs-02.local/**

**dn:cn=ldaproot,dc=obs,dc=local**

**\*\* Ако даде това :**

**ldap\_bind: Invalid credentials (49)**

**трябва да смени админ паса:**

ldapsearch -H ldapi:// -LLL -Q -Y EXTERNAL -b "cn=config" "(olcRootDN=\*)" dn olcRootDN olcRootPW | tee ~/newpasswd.ldif

sudo slappasswd -h {SSHA} >> newpasswd.ldif

**file newpasswd.ldif – трябва да изглежда така.**

**dn: olcDatabase={1}bdb,cn=config**

**#olcRootDN: cn=ldaproot,dc=obs,dc=local**

**changetype: modify**

**replace: olcRootPW**

**olcRootPW: ?!?!?!new-passwd!?!?!**

**\*\* update password \*\***

# ldapmodify -H ldapi:// -Y EXTERNAL -f ~/newpasswd.ldif

**Check again**

**[root@ldap ~]# ldapwhoami -x -w "\*\*админ-пасс\*\*" -D cn=ldaproot,dc=obs,dc=local -ZZ -H ldap://ldap.obs-02.local/**

**Result: dn:cn=ldaproot,dc=obs,dc=local**

**Проверка на ldapsearch**

**# ldapsearch -h localhost -LLL -l 3 -x -b "ou=Users,dc=obs,dc=local" "uid=agalipienso"**

**dn: uid=agalipienso,ou=Users,dc=obs,dc=local**

**objectClass: top**

**objectClass: person**

**objectClass: organizationalPerson**

**objectClass: inetOrgPerson**

**objectClass: posixAccount**

**objectClass: shadowAccount**

**objectClass: sambaSamAccount**

**objectClass: obsPerson**

**objectClass: officePerson**

**objectClass: CourierMailAccount**

**objectClass: mozillaAbPersonAlpha**

**sn: agalipienso**

**9.9 Инсталиране на програми за да работят предоставените скриптове за добавяне/изтриване на потребител в Ldap/Samba**

# yum -y install perl-Unicode-MapUTF8 perl-Digest-SHA1

**9.9.1 – Копиране на старите файлове в /etc/samba и генериране на парола**

**# cp /root/bpk/samba/\* /etc/samba/**

**# the ldap admin dn password is stored in secrets.tdb and is set using "smbpasswd -w passphrase**

**# smbpasswd -w (ldaproot account password)**

**9.9.2 – Създаване на директории използвани от SAMBA**

# mkdir -p /home/ACCOUNTING\_DATA/accounting\_owl

# mkdir -p /var/cache/samba/shares/drivers

# mkdir -p /var/cache/samba/shares/drivers/{color,PCC,W32ALPHA,W32MIPS,W32PPC,W32X86,WIN40,x64}

# mkdir -p /var/cache/samba/shares/drivers/W32X86/PCC

# mkdir -p /var/cache/samba/shares/drivers/x64/PCC

# mkdir /var/cache/samba/shares/drivers/IA64

**9.9.3 Промени в файла на самба разлика в версиите.**

**Old: guest account = guests**

**NEW: guest account = nobody**

**\*\*\* Ако е нужно**

**9.10 Стартиране на SAMBA**

# systemctl start nmb.service

# systemctl start smb.service

# systemctl enable nmb.service

# systemctl enable smb.service

**\*\*\* /var/log/samba/ - Ако има грешки да се отстранят \*\*\***

**9.11** **Тест на скрипта за добавяне на потребител:**

[root@ldap smbldap-tools]# ./owlbg\_usermgnt test2207

[root@ldap smbldap-tools]# ./owlbg\_usermgnt -a test2207

Enter user 'test2207' fullname [Example: Ivan Ivanov Ivanov]: Test on 22072021

setting LAN password "b\*\*\*\*\*"

[root@ldap smbldap-tools]# ./owlbg\_usermgnt test2207

dn: uid=test2207,ou=Users,dc=obs,dc=local

objectClass: top

objectClass: person

objectClass: organizationalPerson

objectClass: posixAccount

objectClass: shadowAccount

objectClass: inetOrgPerson

objectClass: sambaSamAccount

objectClass: obsPerson

objectClass: officePerson

objectClass: CourierMailAccount

objectClass: mozillaAbPersonAlpha

sn: test2207

uid: test2207

uidNumber: 2469

gidNumber: 513

homeDirectory: /home/test2207

loginShell: /bin/bash

givenName: test2207

sambaLogonTime: 0

sambaLogoffTime: 2147483647

sambaKickoffTime: 2147483647

sambaPwdCanChange: 0

sambaPwdMustChange: 2147483647

sambaAcctFlags: '[UX]'

sambaSID: S-1-5-21-3341649654-3636416974-85384702-1007

sambaPrimaryGroupSID: S-1-5-21-3341649654-3636416974-85384702-513

sambaLogonScript: startup.cmd

sambaProfilePath: \\SRV-PDC-01\profiles\test2207

sambaHomePath: \\SRV-PDC-01\test2207

sambaHomeDrive: X:

gecos: Test on 22072021

displayName: Test on 22072021

cn: Test on 22072021

mail: test2207@estiym.com

sambaLMPassword: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

sambaNTPassword: 046224DCA3E87FF15A86A3AC53021804

sambaPwdLastSet: 1626984613

userPassword:: e1NTSEF9QkdyNmJyK3JCNmRDanp1elNONHRNeDQ4dFdGWFRDNUM=

shadowLastChange: 18830

[root@ldap smbldap-tools]# smbldap-passwd test2207

Changing UNIX and samba passwords for test2207

New password:

Retype new password:

**9.12 Тест Клиент на LDAP**

**# yum install -y openldap-clients nss-pam-ldapd**

# authconfig --enableldap --enableldapauth --ldapserver=192.168.10.70 --ldapbasedn="dc=obs,dc=local" --enablemkhomedir --update

# getent passwd

….. …. …

kstefanova:x:1070:513:Kamelia Ivanova Stefanova:/home/kstefanova:/bin/bash

nnedyalkova:x:1073:513:Nadezhda Dimitrova Nedyalkova:/home/nnedyalkova:/bin/bash

dsvilenova:x:1075:513:Daniela Grigorova Svilenova:/home/dsvilenova:/bin/bash

slyamova:x:1077:513:Sonia Toneva Lyamova:/home/slyamova:/bin/bash

ndyankova:x:1086:513:Nina Nikolova Dyankova:/home/ndyankova:/bin/bash

bzlatanova:x:1087:513:Borislava Tsvetanova Zlatanova:/home/bzlatanova:/bin/bash

dchalakova:x:1021:513:Daniela Angelova Chalakova:/home/dchalakova:/bin/bash

nnikolova:x:1023:513:Nadezhda Stoyanova Nikolova:/home/nnikolova:/bin/bash

ws-acc-01$:\*:1031:515:Computer:/dev/null:/bin/false

ws-acc-02$:\*:1032:515:Computer:/dev/null:/bin/false

ws-test1$:\*:1033:515:Computer:/dev/null:/bin/false

….. …. …

getent passwd test2207

test2207:x:2469:513:Test on 22072021:/home/test2207:/bin/bash

login as: test2207

test2207@192.168.10.51's password:

Creating directory '/home/test2207'.

[test2207@cln ~]$ pwd

/home/test2207

[test2207@cln ~]$ id

uid=2469(test2207) gid=513(Domain Users) groups=513(Domain Users) context=unconfined\_u:unconfined\_r:unconfined\_t:s0-s0:c0.c1023

**9.13 Изтриване на потребител**

[root@ldap smbldap-tools]# ./owlbg\_usermgnt -d test2207

[root@ldap smbldap-tools]# ./owlbg\_usermgnt test2207