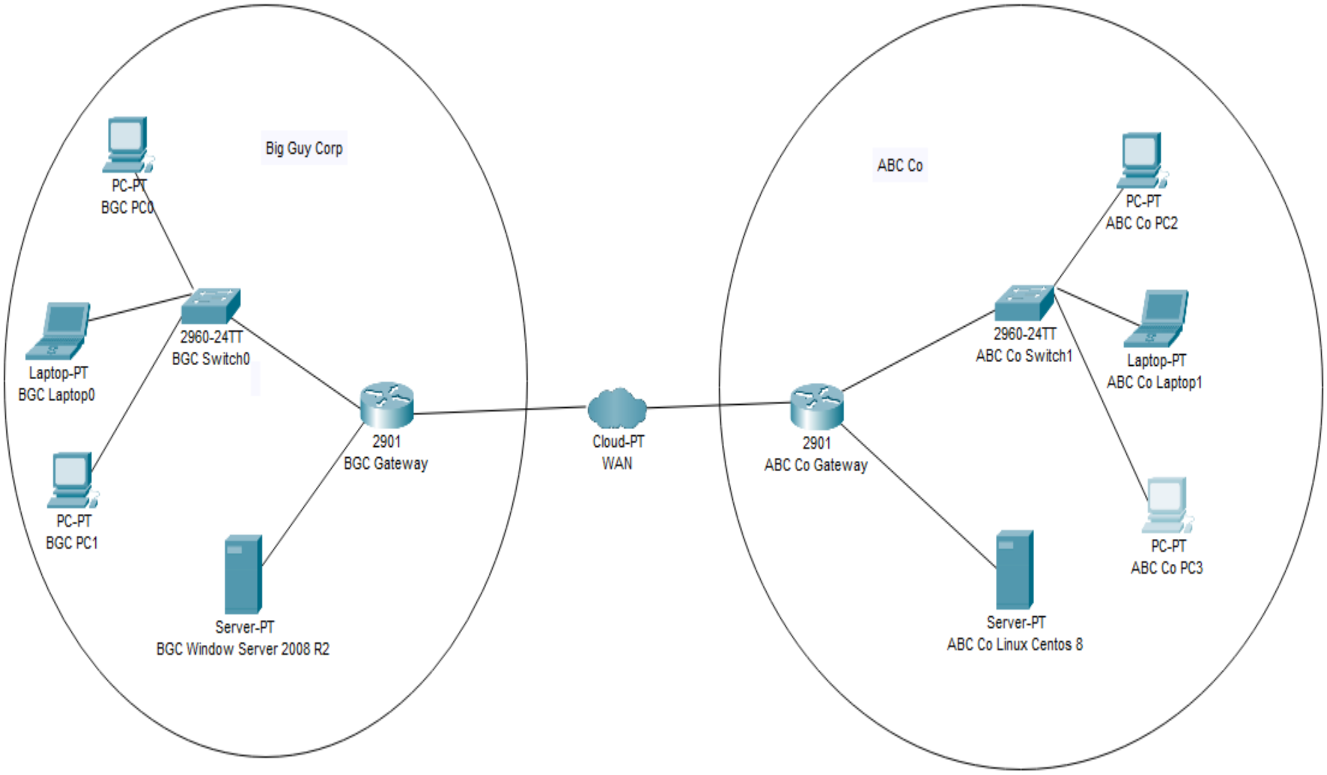
MULTIPLE LOGIN ACCESS DIRECTORY WITH OPENLDAP AND KERBEROS

Project Network Flow Diagram



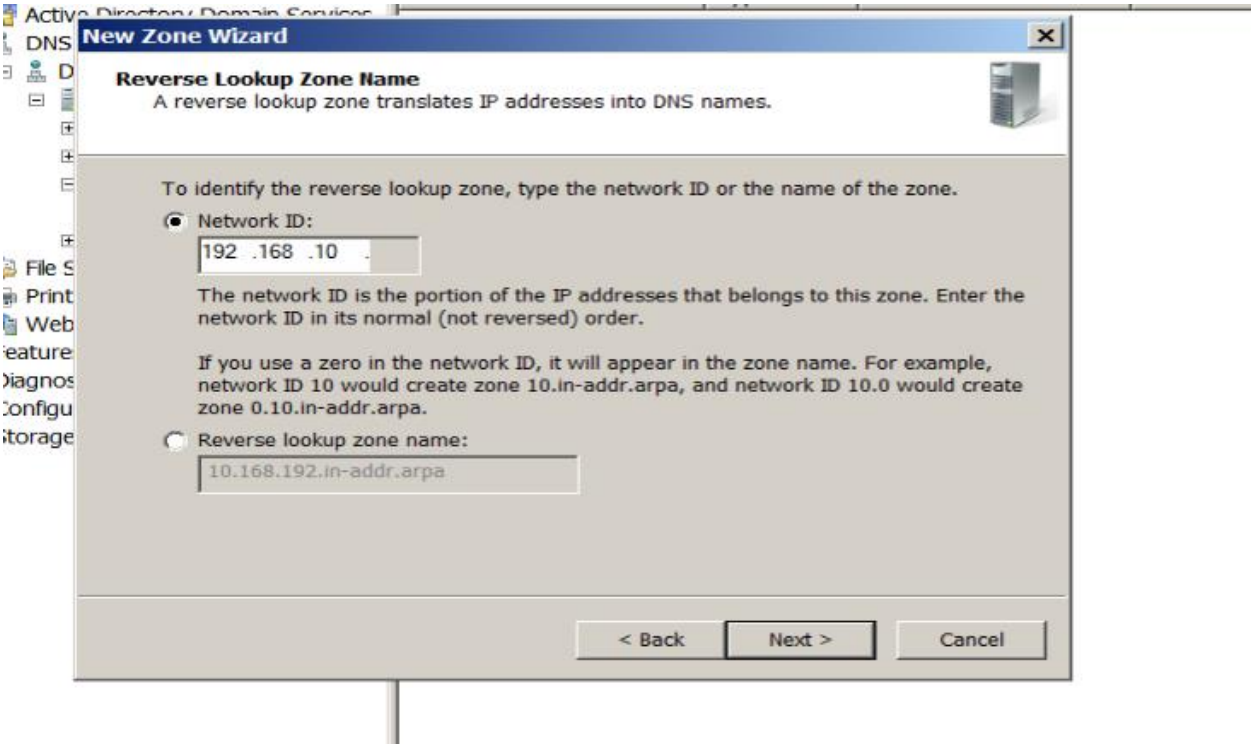
This figure above is the simple diagram of the network flow in the project. The network administrator will configure and implement necessary services and gateway in order to allow Window Server to communicate with Linux Operating system.

Configuration

Install the DNS service on Window Server 2008 R2

REVERSE LOOKUP ZONES

- Click into the Server Manager
- Then click to Roles -> DNS Server (Choose no if the warning message display)
- Click into the DNS -> Your Domain name -> Right Click Reverse Lookup Zones -> New Zone -> Next -> Primary Zone -> Next -> Choose second option (To all DNS servers running on domain controllers in this domain bigguycorp.com) -> Next -> IPv4 Reverse Lookup Zones
- Then Fill like the table below



Reverse Lookup Zone Name

A reverse lookup zone translates IP addresses into DNS names.

To identify the reverse lookup zone, type the network ID or the name of the zone.

● Network ID:

192 .168 .10 .

The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order.

If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.

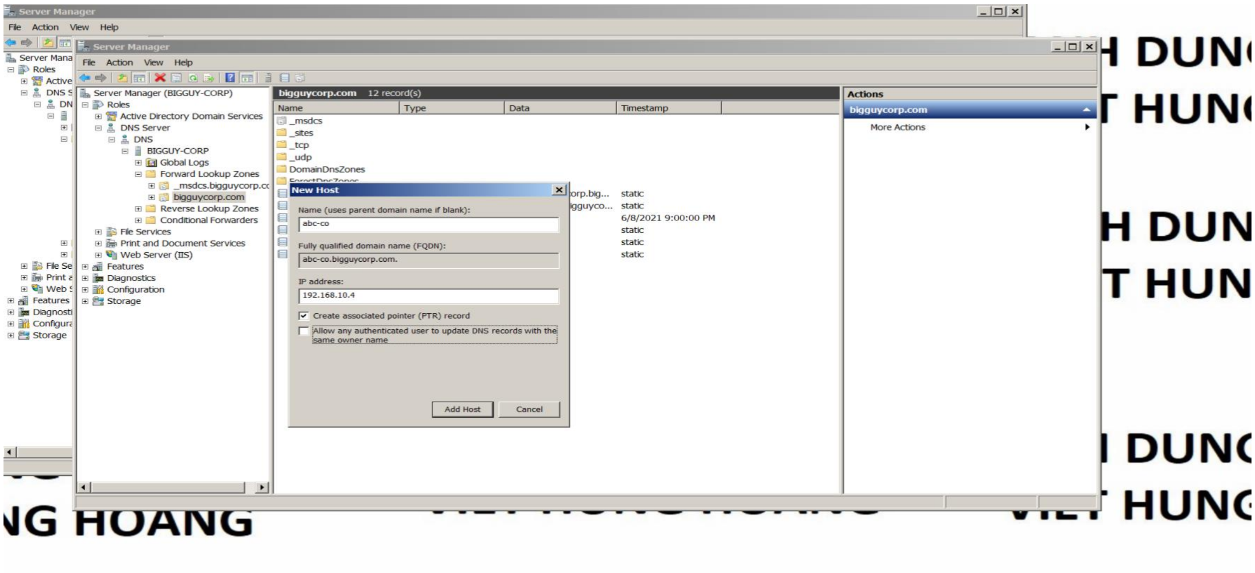
○ Reverse lookup zone name:

10.168.192.in-addr.arpa

FORWARD LOOKUP ZONES

- Then click to Roles -> DNS Server (Choose no if the warning message display)
- Click into the DNS -> Your Domain name -> Forward Lookup Zones -> choose domain (bigguycorp.com)
- Right Click to the Domain name, then choose New Host AAA…

- Then fill the information of Linux machine (abc-co) with proper IP address 192.168.10.4



New Host

Name (uses parent domain name if blank):
abc-co

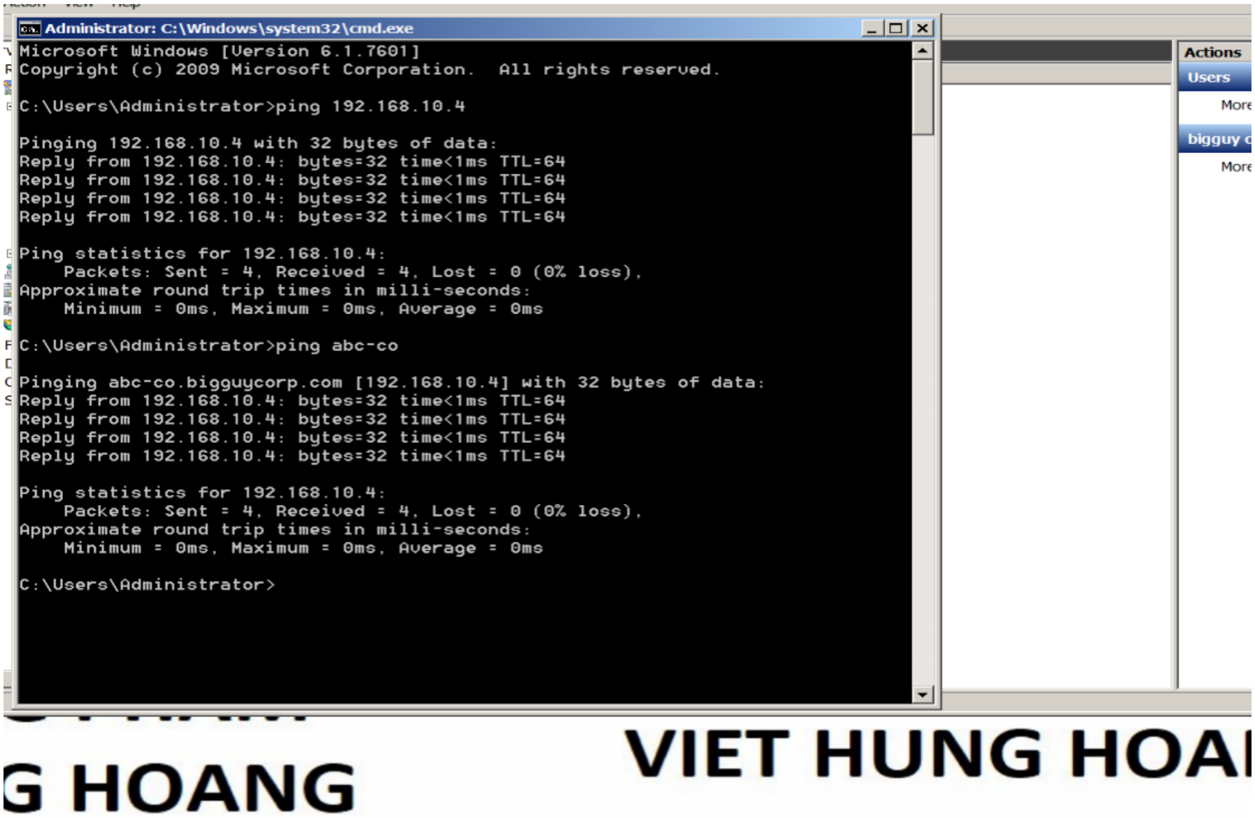
Fully qualified domain name (FQDN):
abc-co.bigguycorp.com.

IP address:
192.168.10.4

☑ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

- **Verify the connection by pinging to ABC linux machine by:**
  - ping abc-co
  - ping 192.168.10.4



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator>ping 192.168.10.4

Pinging 192.168.10.4 with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>ping abc-co

Pinging abc-co.bigguycorp.com [192.168.10.4] with 32 bytes of data:
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64
Reply from 192.168.10.4: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

Install OpenLDAP service on CentOS 8

- **On centos machine, configure the hostname with command**
  - hostnamectl set-hostname abc-co.abc.com

- **Install OpenLDAP service**
  - yum install yum-utils -y
  - yum-config-manager --add-repo=https://repo.symas.com/configs/SOFL/rhel8/sofl.repo
  - yum install openldap openldap-clients openldap-servers symas-openldap-clients symas-openldap-servers perl tar openssl --skip-broken

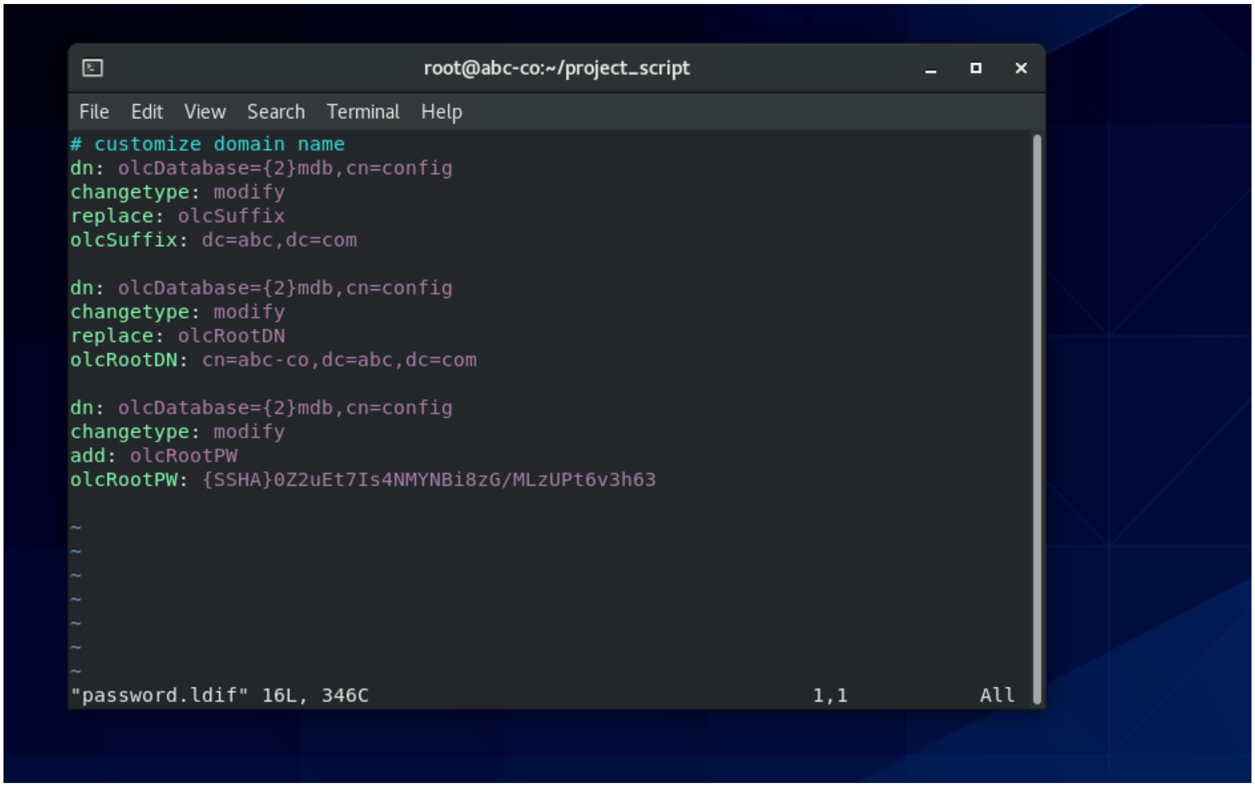
- **Configure OpenLDAP service**
  - Issue the command “slappasswd” to generate the password for ldap administrator

```
{SSHA}0Z2uEt7Is4NMYNBi8zG/MLzUPt6v3h63
```

  - systemctl enable slapd
  - systemctl start slapd

- **Configure OpenLDAP via the extension .ldif**
  - Before doing that, we have to issue these commands to setup the LDAP database
  - ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif
  - ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif
  - ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

- **Configure domain name, make the root account for the domain and generate the password**
  - Create the empty folder named “project_script” on /root
  - Create the password for ldap server with this content below

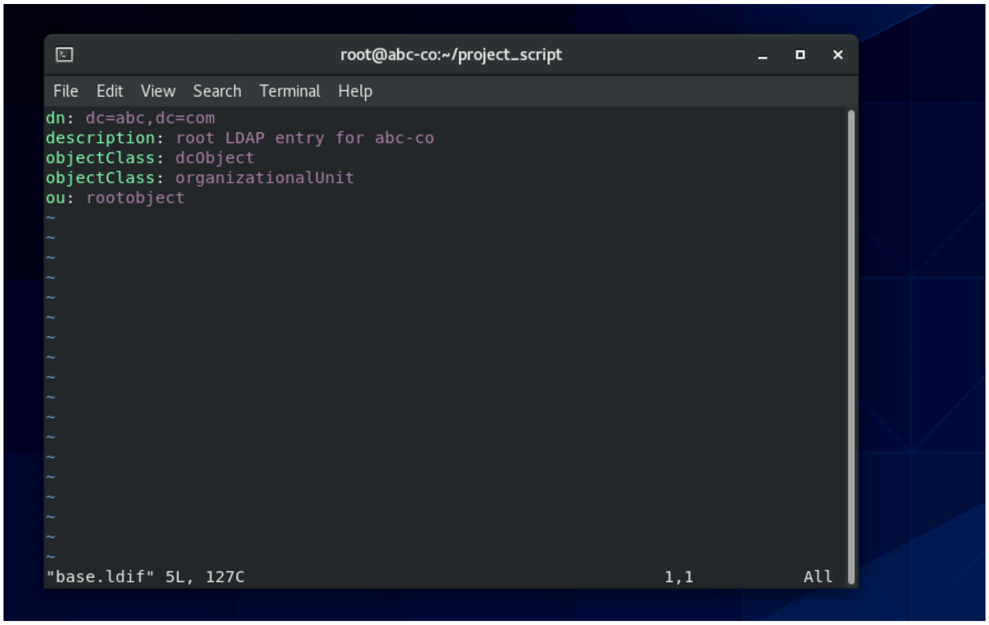

root@abc-co:~/project_script
File Edit View Search Terminal Help

```
# customize domain name
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=abc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=abc-co,dc=abc,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
add: olcRootPW
olcRootPW: {SSHA}0Z2uEt7Is4NMYNBi8zG/MLzUPt6v3h63

~
~
~
~
~
~
~
"password.ldif" 16L, 346C                                    1,1           All
```

- Save and exit the file, then run the command below:

⇨ **ldapmodify -Y EXTERNAL -H ldapi:/// -f password.ldif**

- Create the file named base.ldif with the specific content:

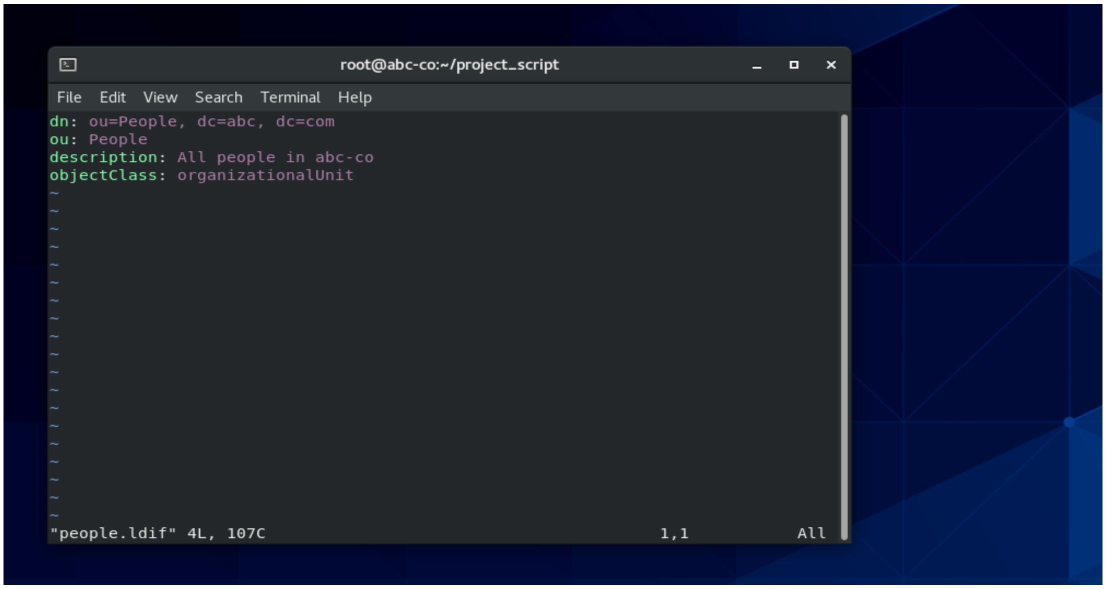

root@abc-co:~/project_script
File Edit View Search Terminal Help

```
dn: dc=abc,dc=com
description: root LDAP entry for abc-co
objectClass: dcObject
objectClass: organizationalUnit
ou: rootobject
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"base.ldif" 5L, 127C                                         1,1           All
```

- Save and exit the file, then run the command below

⇨ **ldapadd -H ldapi:/// -x -D "cn=abc-co,dc=abc,dc=com" -W -f base.ldif**

- Create the file called people.ldif to store all of the people on Organization Units (OU), it helps to store the user on the abc.com network.

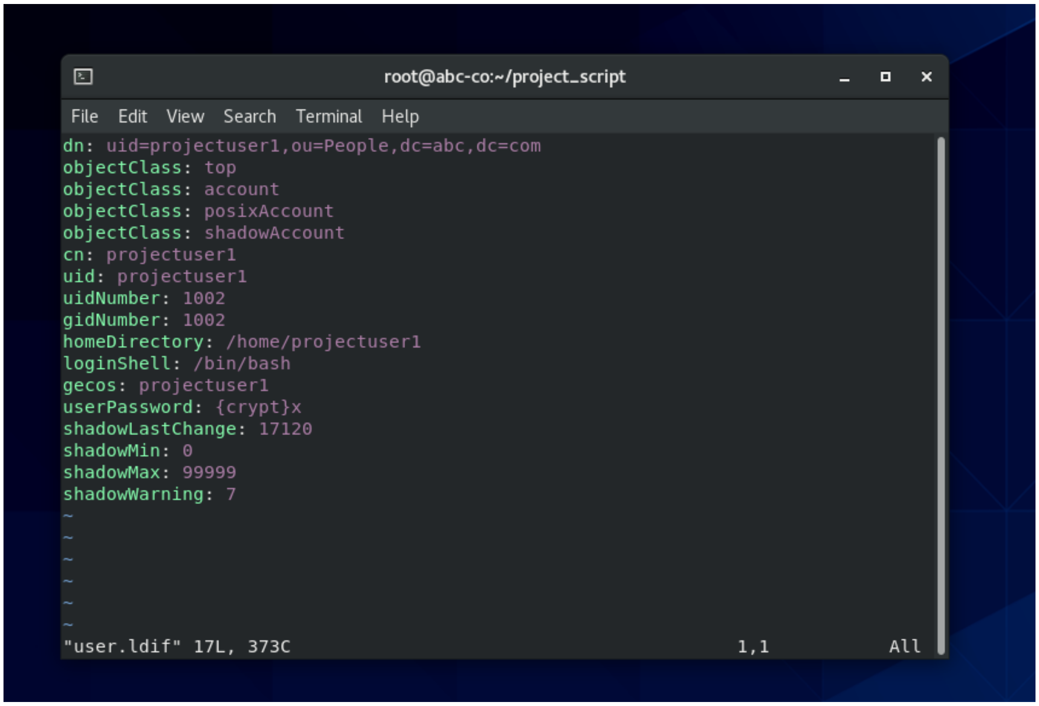

root@abc-co:~/project_script
File Edit View Search Terminal Help

```
dn: ou=People, dc=abc, dc=com
ou: People
description: All people in abc-co
objectClass: organizationalUnit
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"people.ldif" 4L, 107C                                    1,1           All
```

- Save and exit the file, then run the command below

⇨ **ldapadd -H ldapi:/// -x -D "cn=abc-co,dc=abc,dc=com" -W -f people.ldif**

- **Create LDAP user allows login to the system and put this user into the OU People:**
  - Create the file named user.ldif with the content below:



root@abc-co:~/project_script
File Edit View Search Terminal Help

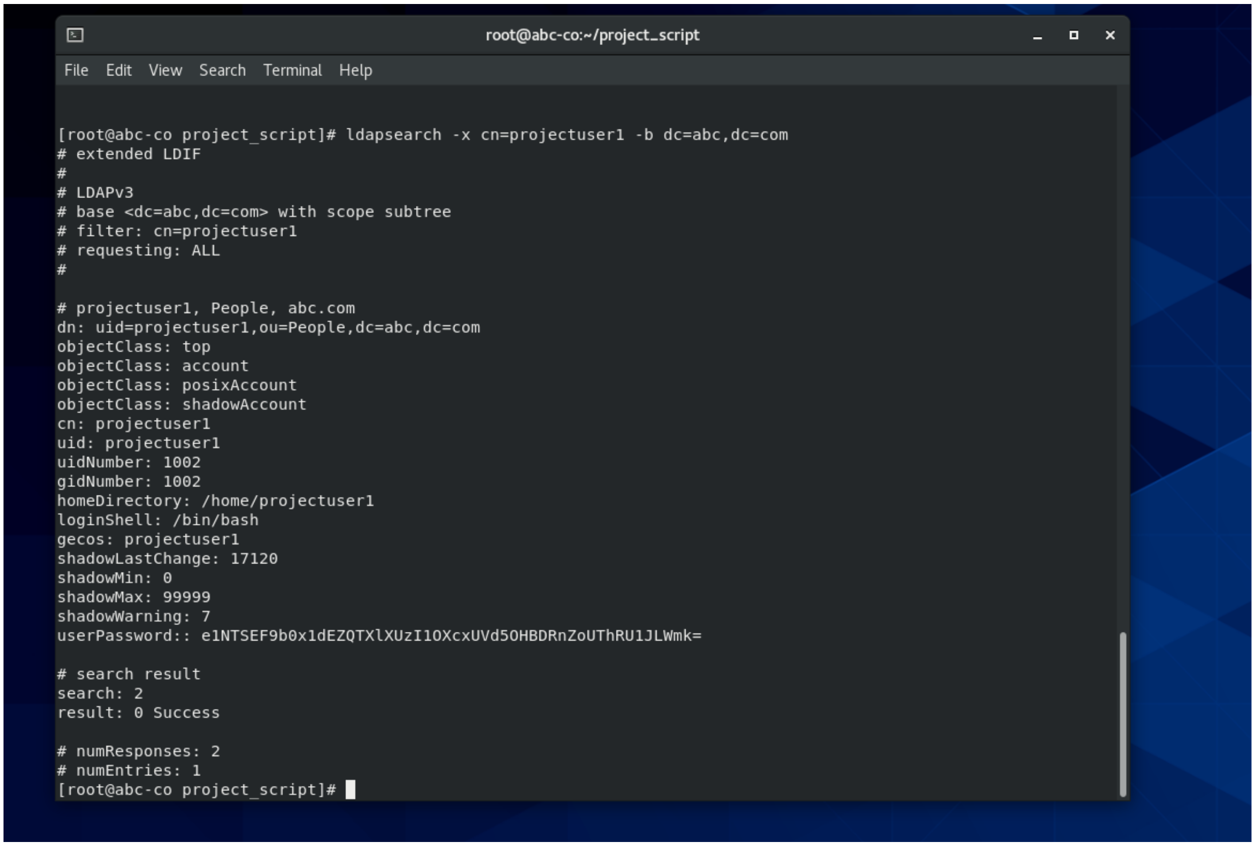
```
dn: uid=projectuser1,ou=People,dc=abc,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: projectuser1
uid: projectuser1
uidNumber: 1002
gidNumber: 1002
homeDirectory: /home/projectuser1
loginShell: /bin/bash
gecos: projectuser1
userPassword: {crypt}x
shadowLastChange: 17120
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
~
~
~
~
~
~
"user.ldif" 17L, 373C                                1,1           All
```

- Save and exit the file. Then issue this command to add new user into the database:

⇨ **ldapadd -H ldapi:/// -x -D "cn=abc-co,dc=abc,dc=com" -W -f user.ldif**

- **Verify the user added into the LDAP by using these commands:**

⇨ **ldapsearch -x cn=projectuser1 -b dc=abc,dc=com**


root@abc-co:~/project_script
File Edit View Search Terminal Help

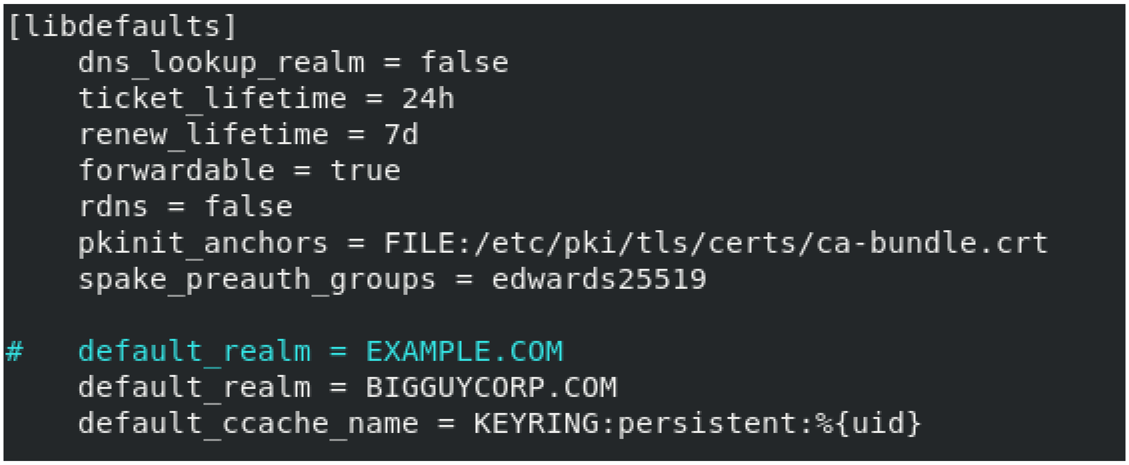
```
[root@abc-co project_script]# ldapsearch -x cn=projectuser1 -b dc=abc,dc=com
# extended LDIF
#
# LDAPv3
# base <dc=abc,dc=com> with scope subtree
# filter: cn=projectuser1
# requesting: ALL
#

# projectuser1, People, abc.com
dn: uid=projectuser1,ou=People,dc=abc,dc=com
objectClass: top
objectClass: account
objectClass: posixAccount
objectClass: shadowAccount
cn: projectuser1
uid: projectuser1
uidNumber: 1002
gidNumber: 1002
homeDirectory: /home/projectuser1
loginShell: /bin/bash
gecos: projectuser1
shadowLastChange: 17120
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
userPassword:: e1NTSEF9b0x1dEZQTXlXUzI1OXcxUVd5OHBDRnZoUThRU1JLWmk=

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
[root@abc-co project_script]# 
```

- Then issue the command below to generate the LDAP password for projectuser1:

⇨ **ldappasswd -x -D "cn=abc-co,dc=abc,dc=com" -W -S "uid=projectuser1,ou=People,dc=abc,dc=com"**

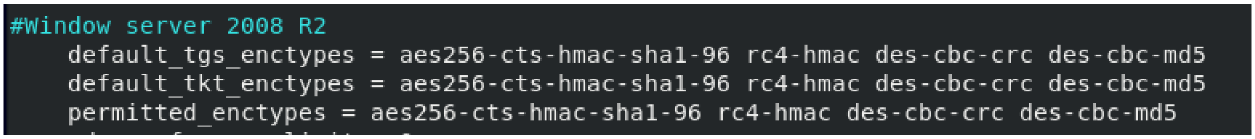
Configure the Kerberos Service

- yum install -y realmd sssd oddjob-mkhomedir adcli samba-common samba-common-tools krb5-workstation
- Open the /etc/krb5.conf
- Then forward into the [libdefaults], and add these line below:



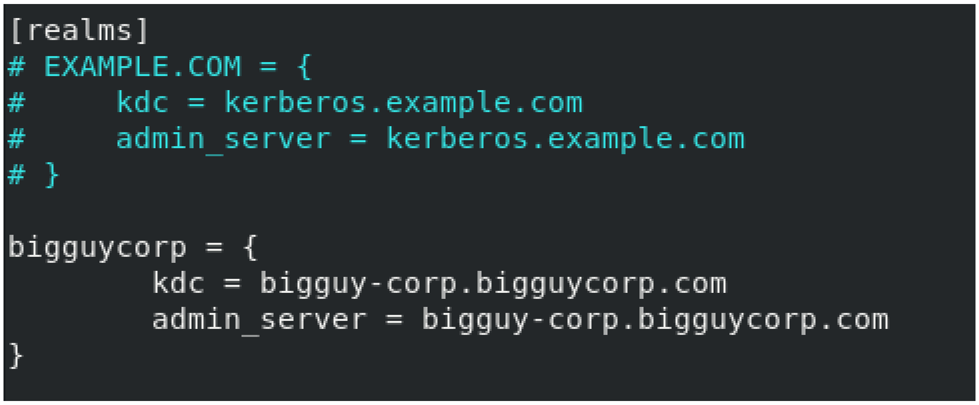
```
[libdefaults]
    dns_lookup_realm = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519

#   default_realm = EXAMPLE.COM
    default_realm = BIGGUYCORP.COM
    default_ccache_name = KEYRING:persistent:%{uid}
```

- Then adding the different encryption method to connect Kerberos and realmd service.



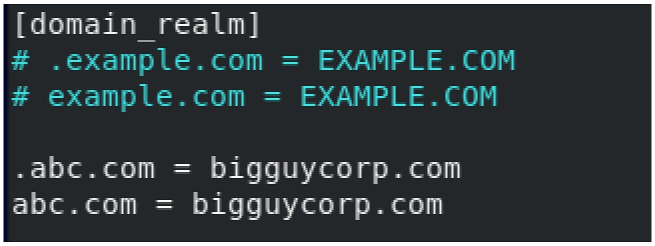
```
#Window server 2008 R2
    default_tgs_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
    default_tkt_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
    permitted_enctypes = aes256-cts-hmac-sha1-96 rc4-hmac des-cbc-crc des-cbc-md5
```

- Forward into the [realms] section, then add the following content below:



```
[realms]
# EXAMPLE.COM = {
#     kdc = kerberos.example.com
#     admin_server = kerberos.example.com
# }

bigguycorp = {
        kdc = bigguy-corp.bigguycorp.com
        admin_server = bigguy-corp.bigguycorp.com
}
```

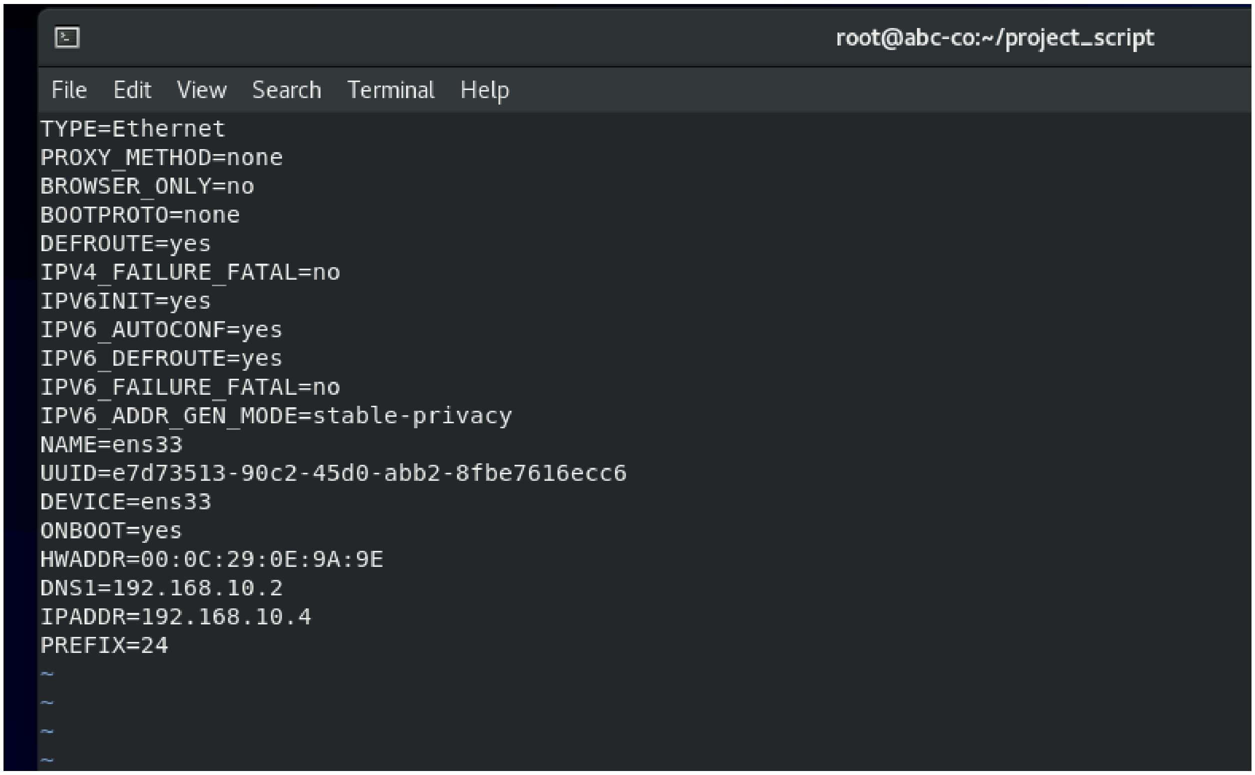
- Then next to the [domain_realm] section, add these content below:



```
[domain_realm]
# .example.com = EXAMPLE.COM
# example.com = EXAMPLE.COM

.abc.com = bigguycorp.com
abc.com = bigguycorp.com
```

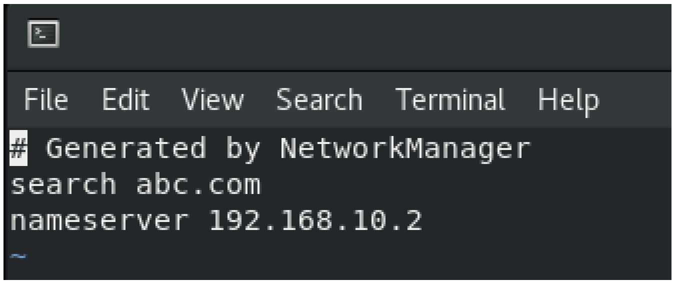
Connect Linux CentOS 8 to Window server 2008 R2

- Disable firewall if necessary
- Add All machine to the Active Directory Domain via realmd service
- Check the network configuration to make sure that DNS1 forward to Window Server 2008 R2



```
TYPE=Ethernet
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=none
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=ens33
UUID=e7d73513-90c2-45d0-abb2-8fbe7616ecc6
DEVICE=ens33
ONBOOT=yes
HWADDR=00:0C:29:0E:9A:9E
DNS1=192.168.10.2
IPADDR=192.168.10.4
PREFIX=24
~
~
~
~
```

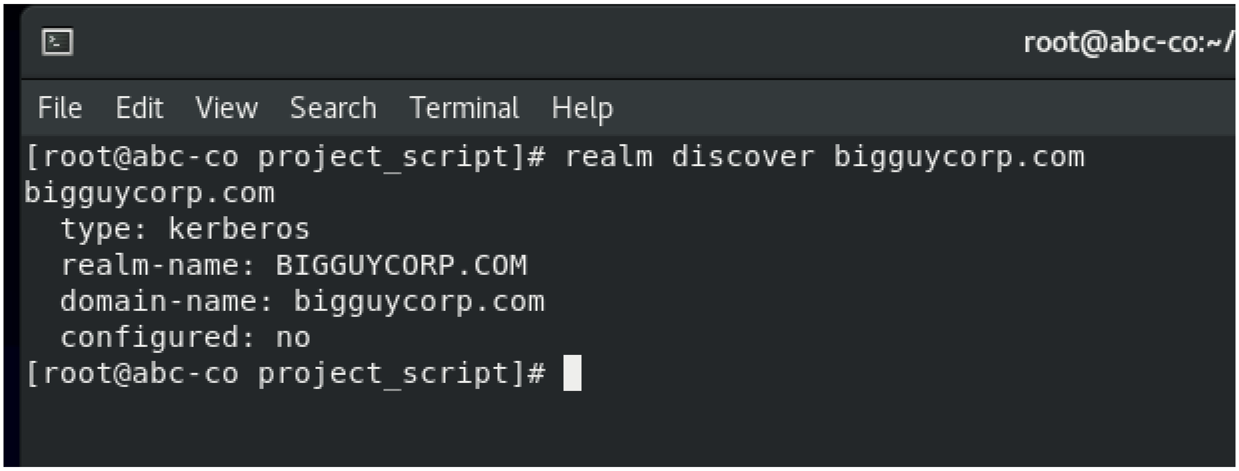
- Then issues these command to restart the network
  - ifdown ens33
  - ifup ens33
- Check /etc/resolv.conf



```
# Generated by NetworkManager
search abc.com
nameserver 192.168.10.2
~
```

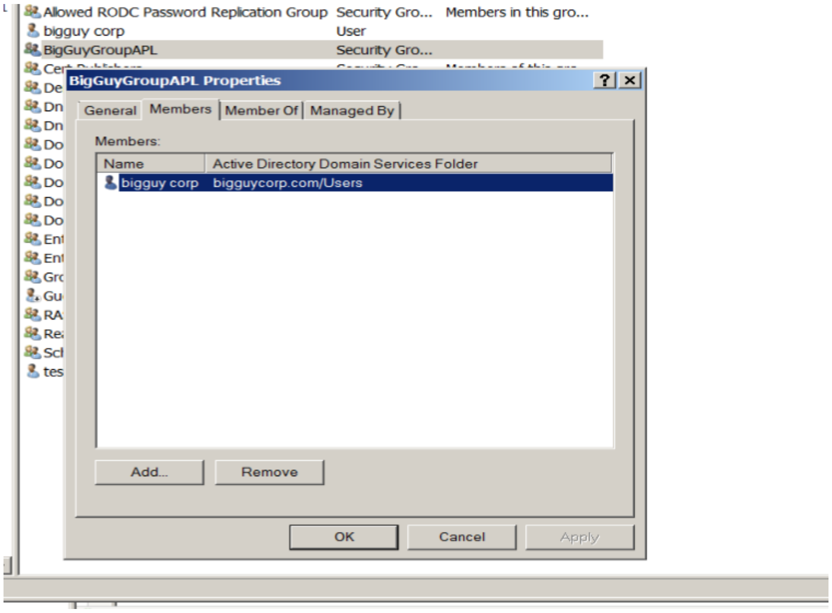
Verify the connection into Window Server (bigguycorp.com)

- **Issue the command below to search the available connection to bigguycorp.com**



```
[root@abc-co project_script]# realm discover bigguycorp.com
bigguycorp.com
  type: kerberos
  realm-name: BIGGUYCORP.COM
  domain-name: bigguycorp.com
  configured: no
[root@abc-co project_script]# 
```

- **After that, issue this command to join to the bigguycorp.com**
  ⇨ realm join bigguycorp.com
- **Go back to Window Server 2008 R2 to create ADDS user and group**
  - Open Server Manager -> Roles -> Active Directory Domain Services -> Active Directory Users and Computers -> Click into the domain name.
  - Right Click into Users -> New -> User -> Then create the User (bigguycorp)
  - Repeat the same step to create second user (testuser)
  - Right Click into Users, Create a Group called 'BigGuyGroupAPL'
  - Then Right Click the the BigGuyGroupAPL created before, choose Properties -> Members -> Click Add -> and Add the user 'bigguycorp' created before into group.

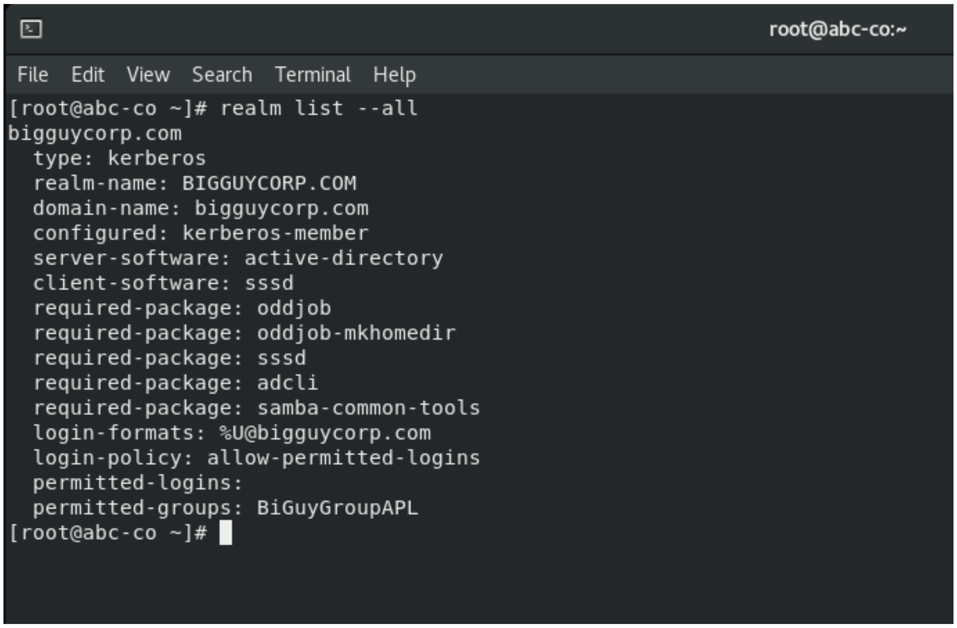

Allowed RODC Password Replication Group Security Gro... Members in this gro...
bigguy corp User
BigGuyGroupAPL Security Gro...
Cer
De
Dn
Dn
Do
Do
Do
Do
Do
Ent
Ent
Grc
Gu
RA
Rea
Scl
tes
BigGuyGroupAPL Properties
General
Members
Member Of
Managed By
Members:
Add...
Remove
OK
Cancel
Apply

Name	Active Directory Domain Services Folder
bigguy corp	bigguycorp.com/Users

- **Go back to CentOS 8 machine to set the permission**
  - realm deny --all
  - realm permit –groups BigGuyGroupAPL

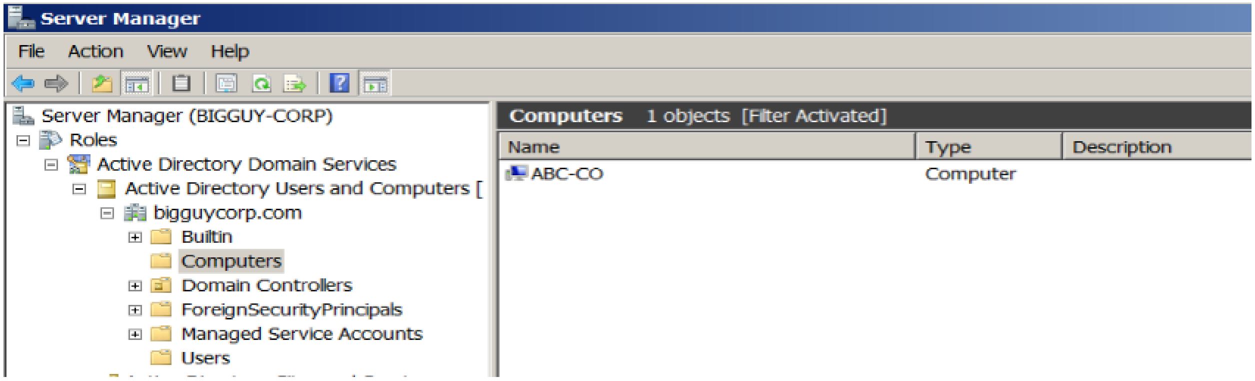
  ⇨ Allow only users who exist on BigGuyGroupAPL, and deny everything.

Then using the realm list --all to check the configuration:



```
[root@abc-co ~]# realm list --all
bigguycorp.com
  type: kerberos
  realm-name: BIGGUYCORP.COM
  domain-name: bigguycorp.com
  configured: kerberos-member
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
  login-formats: %U@bigguycorp.com
  login-policy: allow-permitted-logins
  permitted-logins:
  permitted-groups: BiGuyGroupAPL
[root@abc-co ~]#
```

- On Window Server 2008 R2, we can check Linux machine connected via ADDS on Computers


Server Manager
File
Action
View
Help
Server Manager (BIGGUY-CORP)
Roles
Active Directory Domain Services
Active Directory Users and Computers [
bigguycorp.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

Computers 1 objects [Filter Activated]

Name	Type	Description
ABC-CO	Computer	

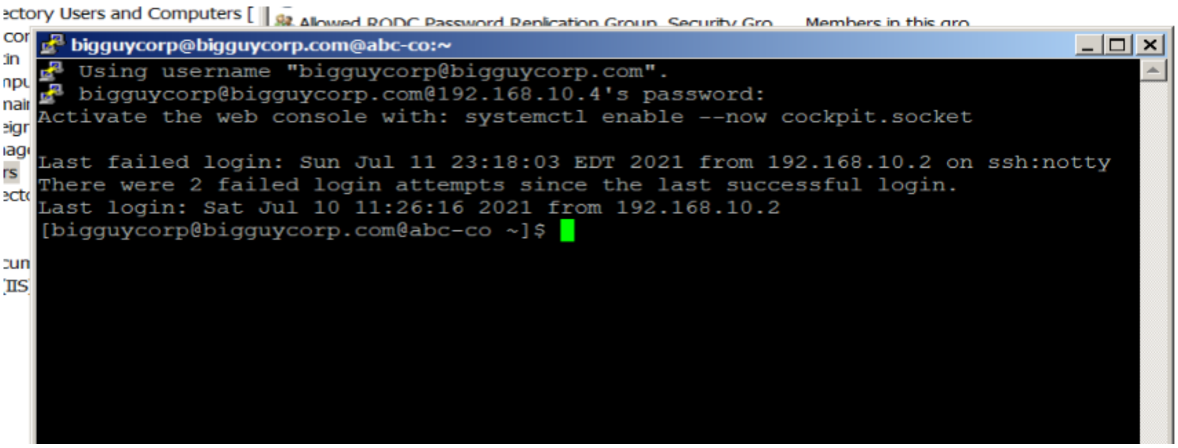
Testing Login permission for Domain users

ALLOW

- On Window Server 2008 R2, Download Putty and Install.
- Then open Putty and write the command below to test the connection

bigguycorp@bigguycorp.com@192.168.10.4

⇨ Because “bigguycorp” user is currently in BigGuyGroupAPL, it allows the connect via Putty


ectory Users and Computers [
Allowed RODC Password Replication Group Security Gro
Members in this gro
bigguycorp@bigguycorp.com@abc-co:~

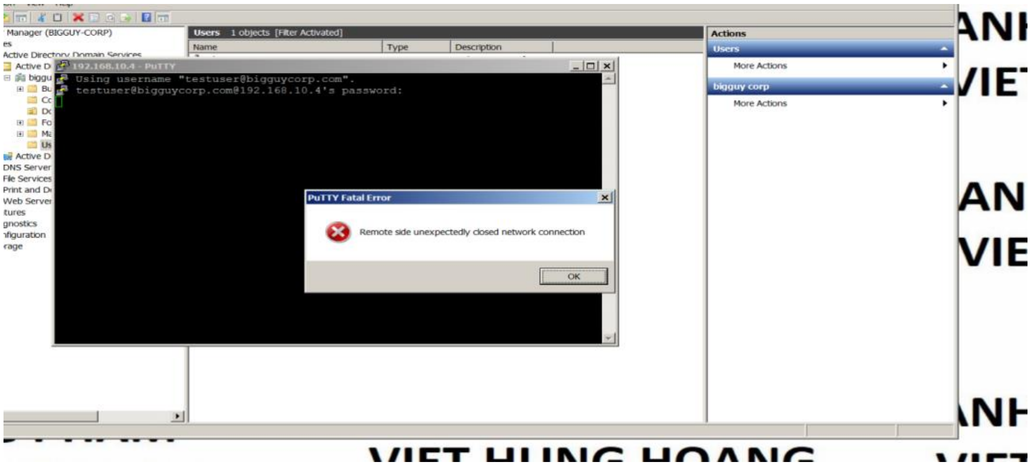
```
Using username "bigguycorp@bigguycorp.com".
bigguycorp@bigguycorp.com@192.168.10.4's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sun Jul 11 23:18:03 EDT 2021 from 192.168.10.2 on ssh:notty
There were 2 failed login attempts since the last successful login.
Last login: Sat Jul 10 11:26:16 2021 from 192.168.10.2
[bigguycorp@bigguycorp.com@abc-co ~]$
```

DENY

- On Window Server 2008 R2, Download Putty and Install.
- Then open Putty and write the command below to test the connection

testuser@bigguycorp.com@192.168.10.4

⇨ Because “testuser” user is currently NOT in BigGuyGroupAPL, it doesn’t connect via Putty

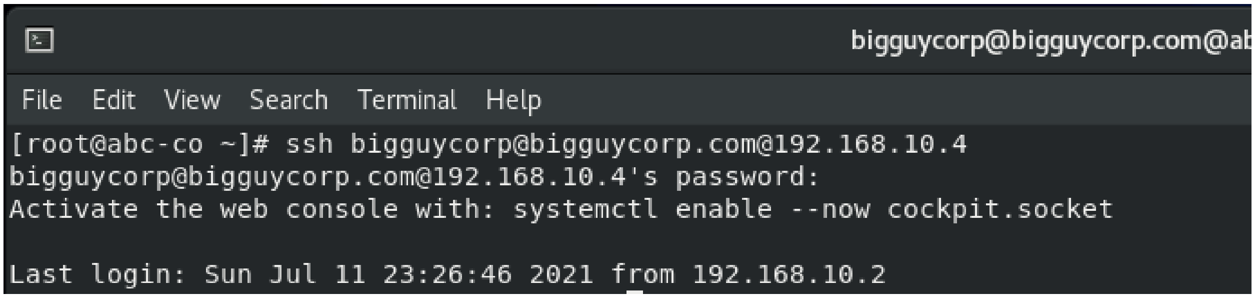


```
Using username "testuser@bigguycorp.com".
testuser@bigguycorp.com@192.168.10.4's password:
```

Remote side unexpectedly closed network connection

We can also verify the connection on Linux CentOS 8 machine

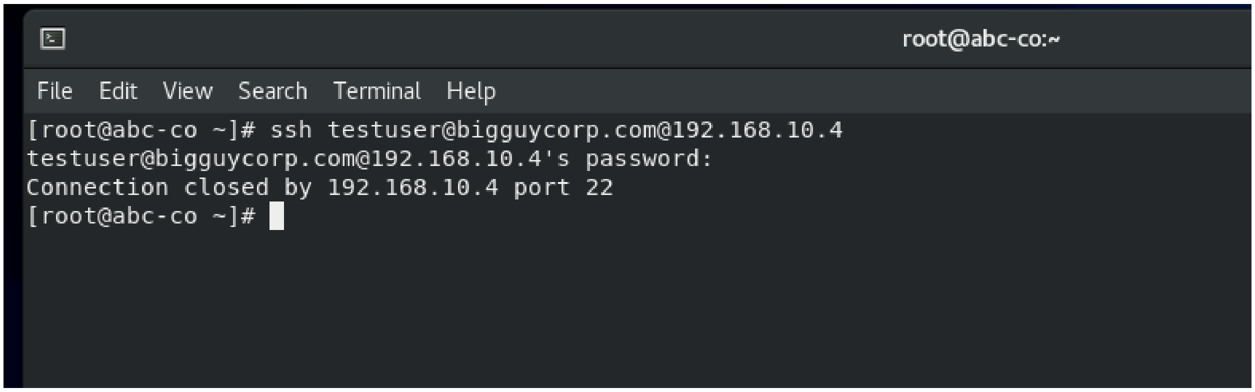
ALLOW



bigguycorp@bigguycorp.com@ab
File Edit View Search Terminal Help

```
[root@abc-co ~]# ssh bigguycorp@bigguycorp.com@192.168.10.4
bigguycorp@bigguycorp.com@192.168.10.4's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun Jul 11 23:26:46 2021 from 192.168.10.2
```

DENY



```
[root@abc-co ~]# ssh testuser@bigguycorp.com@192.168.10.4
testuser@bigguycorp.com@192.168.10.4's password:
Connection closed by 192.168.10.4 port 22
[root@abc-co ~]#
```