漫遊連線機制建置說明手冊

Freeradius+ Active Directory

無線網路漫遊交換中心 | 桃園啟英高級中學

共同建置 2017/05/15 版本 1.0

一、 安裝前準備

Windows sever 環境

IP：192.168.1.10
主機名稱：winad
網域：aaa.bbb.edu.tw
FQDN：winad. aaa.bbb.edu.tw

CentOS7 環境

IP：192.168.1.20
主機名稱：centos
網域：aaa.bbb.edu.tw
FQDN：centos. aaa.bbb.edu.tw

使用工具

Samba
Winbind
Kerbros

1. 修改 centos 伺服器相對應 IP 與名稱

```
[root@tanetroaming]#    vim /etc/hosts

127.0.0.1     localhost localhost.localdomain localhost4 localhost4.localdomain4
::1           localhost localhost.localdomain localhost6 localhost6.localdomain6
192.168.1.10    winad. aaa.bbb.edu.tw    aaa.bbb.edu.tw winad
#AD→IP、FQDN、網域名稱、電腦名稱
192.168.1.20 centos. aaa.bbb.edu.tw    centos
# Centos7→IP、FQDN、網域名稱、電腦名稱
192.168.7.100
#AP    IP
```

2. 修改 selinux 將他關閉

```
[root@tanetroaming]# vim /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=disabled        #關閉 selinux 功能
```

一、 安裝 samba

```
[root@tanetroaming]# yum install samba.x86_64
```

1. 備份設定 samba 設定檔

```
[root@tanetroaming]# cp /etc/samba/smb.conf.exmple /etc/samba/smb.conf
```

2. 修改 samba 設定檔

```
[root@tanetroaming]# vim /etc/samba/smb.conf

[global]
   workgroup = winad     #Domain 最左邊的名稱
   server string = Samba Server Version %v
   netbios name = centos     #Centos7 名稱
   log file = /var/log/samba/log.%m
   max log size = 50
   security = ads     #使用 AD 驗證方式
   passdb backend = tdbsam
   realm =    aaa.bbb.edu.tw    #網域名稱
   password server = 192.168.1.10     #AD 伺服器 IP
   load printers = yes
   cups options = raw
[homes]
   comment = Home Directories
   browseable = no
   writable = yes
[printers]
    comment = All Printers
    path = /var/spool/samba
    browseable = no
    guest ok = no
    writable = no
    printable = yes
```

二、 安裝 Kerberos

1. 安裝 Kerberos

```
[root@tanetroaming]# yum install  krb5-server.x86_64
```

2. 修改/etc/krb5.conf 設定檔

```
[root@tanetroaming]# vim /etc/krb5.conf

includedir /etc/krb5.conf.d/

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

[libdefaults]
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = AAA.BBB.EDU.TW       #新增網域名稱(大寫)
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
AAA.BBB.EDU.TW = {     #新增網域名稱(大寫)
   kdc = 192.168.1.10:88
   admin_server = 192.168.1.10.749
   default_domain = aaa.bbb.edu.tw
}
```

```
[domain_realm]     #新增網域名稱，注意大小寫
.aaa.bbb.edu.tw = AAA.BBB.EDU.TW
aaa.bbb.edu.tw = AAA.BBB.EDU.TW

[kdc]     #增加 kdc 認證路徑
  profile = /var/kerberos/krb5kdc/kdc.conf
```

3. 修改/var/kerberos/krb5kdc/kdc.conf

```
   [root@tanetroaming]# vim   /var/kerberos/krb5kdc/kdc.conf

   [kdcdefaults]
     kdc_ports = 88
     kdc_tcp_ports = 88
   [realms]
       AAA.BBB.EDU.TW = {     #修改 realm 部份(大寫)
       #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 camellia256-cts:normal camellia128-cts:normal des-hmac-sha1:normal
des-cbc-md5:normal des-cbc-crc:normal
     }
```

4. 重啟 samba 服服務開機自動啟動服務

```
[root@tanetroaming]# systemctl    restart    smb.service
[root@tanetroaming]# chkconfig    smb    on
```

5. 測試 samba 與 kdc 溝通

```
[root@tanetroaming]# kinit    administrator @AAA.BBB.EDU.TW    #輸入 AD 管理者帳號
@DOMAIN
Password for administrator@AAA.BBB.EDU.TW: *********              #輸入 AD 管理者帳號密碼
                                                                  #無出現錯誤代表正常
```

6. 將 centos 加入 windows AD 網域

```
[root@tanetroaming]#net rpc join -U administrator      #輸入管理者帳號
Enter admin's password: ******          #輸入管理者密碼
Using short domain name -- WINAD
Joined 'CENTOS' to realm 'aaa.bbb.edu.tw'          #出現這個代表加入成功!!!
```

三、 安裝 winbind

1. 安裝 winbind

```
[root@tanetroaming]#yum  install  samba-winbind.x86_64
```

2. 修改/etc/nsswitch.conf

```
[root@tanetroaming]# vim  /etc/nsswitch.conf

# Example:
#passwd:       db files nisplus nis
#shadow:       db files nisplus nis
#group:        db files nisplus nis

passwd:        files sss winbind          # 新增 winbind
shadow:        files sss winbind
group:         files sss winbind
#initgroups: files

#hosts:        db files nisplus nis dns
hosts:         files dns myhostname
```

3. 重啟 winbind 服務開機自動啟動服務

```
[root@tanetroaming]# systemctl  restart  winbind.service
[root@tanetroaming]# chkconfig  winbind  on
```

4. 測試 ntlm_auth 連接 AD 帳號

```
[root@tanetroaming]# ntlm_auth --request-nt-key --domain=DOMAIN(大寫)–username=AD 帳號  --password=AD 帳號密碼
```

```
[root@tanetroaming]# ntlm_auth --request-nt-key --domain=AAA.BBB.EDU.TW --username=AAAAAA  --password=XXXXXX
NT_STATUS_OK: Success (0x0)        #出現這個代表成功了!!!
```

四、 修改 freeradius

1. 修改 ntlm_auth 模組

```
[root@tanetroaming]# vim /etc/raddb/mods-available/ntlm_auth

exec ntlm_auth {
        wait = yes
        #program = "/path/to/ntlm_auth --request-nt-key --domain=MYDOMAIN --
username=%{mschap:User-Name} --password=%{User-Password}"
         program = "/usr/bin/ntlm_auth --request-nt-key --domain=aaa.bbb.edu.tw --
username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --password=%{User-
Password}"      #修改執行路徑和 NULL 認證方式
}
```

2. 修改 default 檔案

```
[root@tanetroaming]# vim /etc/raddb/sites-available/default

authorize {
。。。略。。。
files
ntlm_auth
。。。略。。。
}
```

3. 重啟 freeradius 服務

```
[root@tanetroaming]# systemctl   restart   radiusd.service
```

4. 測試 freeradius+AD 認證

```
[root@tanetroaming]# radtest   AD 帳號   AD 帳號密碼   127.0.0.1 0 testing123
Sending Access-Request Id 152 from 0.0.0.0:50068 to 127.0.0.1:1812
        User-Name = ' AD 帳號'
        User-Password = ' AD 帳號密碼'
```

```
        NAS-IP-Address = 192.168.1.20
        NAS-Port = 0
        Message-Authenticator = 0x00
Received Access-Accept Id 152 from 127.0.0.1:1812 to 127.0.0.1:50068 length 40
        Reply-Message = 'AD CONECT SUCCESS'      #代表認證成功
```

五、 參考資料

1. Freeradius+AD

http://deployingradius.com/documents/configuration/active_directory.html

https://sam198214.blogspot.tw/2015/02/freeradius-v2-with-active-directory-on.html

http://a810162.blogspot.tw/2010/12/freeradius-ad.html

http://keynes0918.tian.yam.com/posts/31351174

2. ntlm_auth

https://wiki.freeradius.org/guide/NTLM-Auth-with-PAP-HOWTO