漫遊連線機制建置說明手冊

Freeradius+ Active Directory

For 802.1X

無線網路漫遊交換中心 | 桃園啟英高級中學 | 霧峰農工
共同建置 2019/07/30 版本 1.2

一、 安裝前準備

Windows sever 環境

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

CentOS7 環境

IP：192.168.1.20
主機名稱：centos
網域(domain)：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
```

3. 重新開機

一、 安裝及設定 samba + winbind + Kerberos

```
[root@tanetroaming]# yum install authconfig samba samba-winbind samba-client samba-winbind-clients krb5-server krb5-workstation pam_krb5 -y
```

1. 使用 authconfig 工具設定並加入 AD 網域

```
[root@tanetroaming]# authconfig-tui
```

2. 認證設定：「使用者資訊」勾選”使用 Winbind” ；「認證」勾選”使用 Shadow” 、” 使用 Kerberos” 、” 使用 Winbind 認證” 、” 本機認證即可” ，之後按下一步。

3. Kerberos 設定值：「領域」填入”AAA.BBB.EDU.TW” ；「Kerberos 機碼配送中心(KDC)」填

入” 192.168.1.10:88” ;「管理伺服器」填入”192.168.1.10:749” ，下一步

4. Winbind 設定值 :「安全模型」勾選” ads” 、 「網域」填入” AAA” 、「網域控制器」填入” winad. aaa.bbb.edu.tw” 、「ADS 領域」填入” AAA.BBB.EDU.TW” 、「模板 Shell」勾選” /bin/bash” ，選「結合網域」


authconfig-tui - (c) 1999-2005 Red Hat, Inc.
Winbind 設定值
安全模型：
(*) ads
( ) domain
網域：
AAA
網域控制器：
winad.aaa.bbb.edu.tw
ADS 領域：
AAA.BBB.EDU.TW
模板 Shell：
( ) /sbin/nologin
( ) /bin/sh
(*) /bin/bash
上一步
結合網域
確定
<Tab>/<Alt-Tab> 移動游標 | <Space> 選取 | <F12> 下一個畫面

5. 儲存設定值：勾選”是”

6. 結合設定值：「網域管理員」填入”Administrator”(或其他管理者帳號)；「密碼」填入網域管理員密碼(輸入密碼時螢幕不會顯示任何字元)，之後按確定

7. 之後會跳回 Winbind 設定值畫面，再按確定即可。

8. 重啟 samba 服服務開機自動啟動服務

```
[root@tanetroaming]# systemctl  restart  smb
[root@tanetroaming]# systemctl  enable  smb
```

9. 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!!!
```

net ads info 查看伺服器狀態

wbinfo –u 查看伺服器帳號

二、 修改/var/lib/samba/winbindd_privileged 目錄權限

這裡需要把 radiusd 這個使用者加入 wbpriv 群組裡，不然 Freeradius 是無法透過使用

winbind 與 ntlm_auth 來溝通 AD

```
[root@tanetroaming]# usermod -G wbpriv radiusd
```

三、 修改 freeradius(PAP 驗證)

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. 新增 policy 規則(設定 ntlm_auth 驗證)

```
[root@tanetroaming]# vim /etc/raddb/policy.d/ntlm_auth

ntlm_auth.authorize {
    if (!control:Auth-Type && User-Password) {
        update control {
            Auth-Type := ntlm_auth
```

```
        }
    }
}
```

3. 修改 default 檔案

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

authorize {
        。。。略。。。
        files
        ntlm_auth               #新增 ntlm_auth 驗證
        。。。略。。。
}
authenticate {
        。。。略。。。
        Auth-Type MS-CHAP {
                mschap
        }
        Auth-Type ntlm_auth {               #新增 ntlm_auth 驗證
                ntlm_auth
        }
        。。。略。。。
}
```

4. 重啟 freeradius 服務

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

5. 測試 freeradius+AD 認證

```
[root@tanetroaming]# radtest  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
```

↑代表認證成功

四、　修改 freeradius(802.1X 方式)

1. 修改 mschap 模組

```
[root@tanetroaming]#    vim /etc/raddb/mods-enabled/mschap

mschap {
            。。。略。。。
            use_mppe = yes
            with_ntdomain_hack = yes
            #ntlm_auth = "/path/to/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"
            ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --domain=AAA.BBB.EDU.TW --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}"
            ntlm_auth_timeout = 10
            。。。略。。。
}
```

2. 重啟 freeradius 服務

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

3. 測試 freeradius+AD 認證(802.1X 驗證)

```
[root@tanetroaming /]# radtest    -t    mschap    AD 帳號    密碼    127.0.0.1    0    testing123
Sending Access-Request Id 25 from 0.0.0.0:43887 to 127.0.0.1:1812
            User-Name = ' AD 帳號'
            NAS-IP-Address = 192.168.1.20
            NAS-Port = 0
            Message-Authenticator = 0x00
            MS-CHAP-Challenge = 0x71b41b4fadc65ac4
            MS-CHAP-Response fds20sd9501e9223b838e5fed449e62ac84ccdfbe322b37229
Received Access-Accept Id 25 from 127.0.0.1:1812 to 127.0.0.1:43887 length 84
                        ↑代表認證成功
```

```
MS-CHAP-MPPE-Keys = 0x
MS-MPPE-Encryption-Policy = Encryption-Allowed
MS-MPPE-Encryption-Types = RC4-40or128-bit-Allowed
```

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