

基于 LDAP 和动态 VLAN 的 eduroam 配置

Contents

一 .	环境准备	2
二 .	Linux 服务器加 AD 域	2
1.	安装配置 <i>samba</i>	2
2.	修改配置文件	2
3.	<i>samba</i> 加入域并测试	4
4.	测试 NTLM 认证	5
5.	修改 <i>/var/lib/samba/winbindd_privileged</i> 权限	5
三 .	安装 FreeRadius, 并做基本配置测试	5
1.	安装 <i>freeradius</i>	5
2.	编辑 <i>/etc/raddb/clients.conf</i> , 定义客户端	6
3.	编辑 <i>/etc/raddb/users</i> , 编辑用户名和密码	6
4.	自带客户端简单测试	6
四 .	eduroam 的基本配置	7
五 .	基于 LDAP-Group 动态 VLAN 的 eduroam 配置更新	14
六 .	参考文档	21

香港中文大学（深圳）的 eduroam 无线网络，自 2016 年部署以来先已经稳定运行了 3 年，部署之初，为方便我校师生熟悉 802.1x 认证的使用，本校师生和访客在校内均能使用 eduroam 上网，且权限相同。但这也给网络管理带来一定困扰。考虑到即使是同一 AD 域账号，eduroam 的访问权限都需要依据角色而不同，所以本文在 *freeradius* 的基本配置上，添加了 LDAP 模块用于权限分配，认证仍然使用 *eap*，利用 LDAP-Group 实现动态 VLAN 下发，从而实现不同角色权限分离。

一 . 环境准备

两台 Radius 服务器分别模拟校外用户和校内用户认证。

一台校内 AD 域服务器作为 LDAP-Group 授权演示: Windows Server 2016

AD 域服务器集群 : CUHK.EDU.CN 的 AD 域集群做访客登录测试。

radius 系统 : CentOS Linux release 7.7.1908 (Core) 。

无线控制器 : 华为 AC-6805

软件 : freeradius 3.0

二 . Linux 服务器加 AD 域

1. 安装配置 *samba*

安装组件, 关闭防火墙和 selinux

```
yum update -y
yum install samba samba-client samba-winbind krb5-server krb5-workstation samba-winbind-clients -y
```

2. 修改配置文件

配置 /etc/samba/smb.conf

```
[global]
    workgroup = FREETEST           #指定域的 netbios 名称
    security = ads                 #指定 samba 的工作模式
    winbind use default domain = no
    password server = 10.10.9.86  #指定身份认证的服务器必须为域控
    realm = FREETEST.COM          #指定 AD 域名
```

配置/etc/krb5.conf, 这里严格区分大小写

```
[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 = true
    default_realm = FREETEST.COM      #指定 AD 域名
    default_ccache_name = KEYRING:persistent:%{uid}

[realms]
    FREETEST.COM = {
        kdc = 10.10.9.86:88           #指域控为 kdc 服务器及端口
        admin_server = 10.10.9.86:749 #指定域控的管理端口
        default_domain = freetest.com
    }

[domain_realm]
    .freetest.com = FREETEST.COM
    freetest.com = FREETEST.COM

[kdc]
    profile = /var/kerberos/krb5kdc/kdc.conf
```

编辑/etc/nsswitch.conf,在下列行末尾加“winbind”

```
passwd: files sss winbind
shadow: files sss winbind
group: files sss winbind

protocols: files sss winbind

services: files sss winbind

netgroup: files sss winbind

automount: files sss winbind
```

将 samba 和 winbind 服务设置为开机启动，然后重启服务器。

```
systemctl enable smb
systemctl enable winbind
```

3. samba 加入域并测试

重启后测试 samba 与域控的连通性，加入域并测试。

```
kinit user@FREETEST.COM #域名必须大写，输入密码后不返回结果说明没错误
net ads join -U user      #加入域
systemctl restart smb    #重启 smb
systemctl restart winbind #重启 winbind
wbinfo -u                #查看域用户
wbinfo -a user%password  #测试用户认证，最后结尾如下代表成功。
challenge/response password authentication succeeded
```

4. 测试NTLM 认证

```
ntlm_auth --request-nt-key --domain=FREETEST --username=user
NT_STATUS_OK: The operation completed successfully. #表示结果正确
【ntlm 是 windows 域环境下的认证方式】
```

5. 修改/var/lib/samba/winbindd_privileged 权限

```
usermod -G wbpriv radiusd
```

三 . 安装 FreeRadius， 并做基本配置测试

1. 安装 freeradius

```
yum install freeradius freeradius-utils freeradius-ldap -y
```

2. 编辑/etc/raddb/clients.conf，定义客户端

```
client AC {
    ipaddr = *           #定义客户端 IP 地址, *表示任意 IP 地址
    secret = testing123  # 设置预共享密钥
    shortname = AC       #设置客户端项的友好名称
}
```

3. 编辑/etc/raddb/users，编辑用户名和密码

```
testing Cleartext-Password := "testing"
```

4. 自带客户端简单测试

```
firewall-cmd --zone=public --add-port=1812/udp --permanent
```

```
firewall-cmd --zone=public --add-port=1813/udp --permanent
```

```
firewall-cmd --reload
```

```
radius -X # 用 debugging 模式开启 radius 服务
```

```
testing testing localhost 0 testing123 # 第一 testing 是用户名, 第二 testing 是密码,
testing123 客户端对接的共享密码。显示如下表示基本测试成功
Sent Access-Request Id 48 from 0.0.0.0:44835 to 127.0.0.1:1812 length 77
  User-Name = "testing"
  User-Password = "testing"
  NAS-IP-Address = 127.0.0.1
  NAS-Port = 0
  Message-Authenticator = 0x00
  Cleartext-Password = "testing"
Received Access-Accept Id 48 from 127.0.0.1:1812 to 0.0.0.0:0 length 20
```

四 . eduroam 的基本配置

1. 安装测试依赖包

利用 `wpa_supplicant` 下的一个工具 `eapol_test` 用来测试 `eduroam`, 安装依赖包。

```
yum groupinstall "Development Tools"
yum install git openssl-devel pkgconfig libn13-devel
```

2. 设置外虚拟服务器

在 `/etc/raddb/sites-available` 目录下新建 `eduroam` 文件。

```
operator_name = "freetest.com"
server eduroam {
    listen {
        type = "auth"
        ipaddr = *
        port = 0
    }
    listen {
        type = "acct"
        ipaddr = *
        port = 0
    }
    authorize {
        split_username_nai #分离用户名和域名
        if (noop || !&Stripped-User-Domain) {
            reject
        }
        if (Stripped-User-Domain != "${operator_name}") {
            update {
                control:Load-Balance-Key := &Calling-Station-ID
                control:Proxy-To-REALM := 'eduroam_flr'
                #request:Operator-Name,告诉flr 你的信息, 用于 debugging
                request:Operator-Name := "${operator_name}"
            }
            return
        }
        suffix
        eap
    }
    authenticate {
        eap
    }
}
```

```
preacct {
    suffix
}

accounting {
    detail
    exec
    attr_filter.accounting_response
}

post-auth {
    Post-Auth-Type REJECT {
        attr_filter.access_reject
        reply_log
    }
}

pre-proxy {
    if("%{Packet-Type}" != "Accounting-Request") {
        attr_filter.pre-proxy
    }
}

post-proxy {
    attr_filter.post-proxy
}
}
```

3. 配置 *eduroam* 的内虚拟服务器

在 `/etc/raddb/sites-available` 目录下新建 `eduroa-inner-tunnel` 文件。

```
server eduroam-inner-tunnel {
  authorize {
    split_username_nai
    if (noop || (&Stripped-User-Domain && \
      (&outer.Stripped-User-Domain != &Stripped-User-Domain))) {
      reject
    }
    update {
      &outer.session-state:Stripped-User-Name := &Stripped-User-Name
    }

    auth_log
    eap
    files
    mschap
    pap
  }

  authenticate {
    Auth-Type PAP {
      pap
    }
    Auth-Type MS-CHAP {
      mschap
    }
    mschap
    eap
    ntlm_auth
  }

  post-auth {
    reply_log
    Post-Auth-Type REJECT {
      reply_log
    }
  }
}
}
```

4. 配置 EAP 和 mschap

在 `/etc/raddb/mods-available/`, 配置 `eap` 和 `mschap` 文件

```
eap {
    default_eap_type = peap

    timer_expire    = 60

    max_sessions = ${max_requests}

    tls-config tls-common {
        private_key_password = 123456
        private_key_file = ${certdir}/server.pem

        certificate_file = ${certdir}/server.pem

        ca_file = ${cadir}/ca.pem

        fragment_size = 1000
    }

    tls {
        tls = tls-common
    }

    peap {
        tls = tls-common

        default_eap_type = mschapv2

        virtual_server = "eduroam-inner-tunnel"
    }

    mschapv2 {

    }
}
```

修改配置 `mschap`

```
ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}} --challenge=%{%{mschap:Challenge}:-00} --nt-response=%{%{mschap:NT-Response}:-00}--domain=%{%{mschap:NT-Domain}:-FREETEST}"
```

5. *proxy.conf* 配置

在*/etc/raddb/proxy.conf* 下配置

```
home_server antarctica-flr-1 {
    type          = auth+acct
    ipaddr        = 10.21.3.253
    port          = 1812
    secret        = testing123
}
home_server_pool EDUROAM {
    type          = fail-over
    home_server   = antarctica-flr-1
}
realm eduroam_flr {
    nostrip
    auth_pool     = EDUROAM
}
```

6. 配置 *ntlm_auth*

编辑*/etc/raddb/mods-enabled/ntlm_auth*, 修改如下

```
exec ntlm_auth {
    wait = yes
    program = "/usr/bin/ntlm_auth --request-nt-key --domain=MYDOMAIN --username=%{mschap:User-Name} --password=%{User-Password}"
}
```

7. 建立软链接

```
ln -s /etc/raddb/sites-available/eduroam /etc/raddb/sites-enable/eduroam
ln -s /etc/raddb/sites-available/eduroam-inner-tunnel /etc/raddb/sites-enable/eduroam-inner-tunnel
```

8. 配置客户端

```
client AC {
    ipaddr = *           #定义客户端 IP 地址, *表示任意 IP 地址
    secret = testing123 #设置预共享密钥
    shortname = AC      #设置客户端项的友好名称
    virtual_server = eduroam #设置虚拟服务器
}
}
```

9. 配置 `peap-mschap` 测试文件

```
# eapol_test -c peap-mschap.conf -s testing123
network={
    ssid="example"
    key_mgmt=WPA-EAP
    eap=PEAP
    identity="francisco@freetest.com"
    anonymous_identity="francisco@freetest.com"
    password="ITSM@1234"
    phase2="autheap=MSCHAPV2"
}
}
```

运行 `eapol_test -c peap-mschap.conf -s testing123` 返回测试成功。

五 . 基于 LDAP-Group 动态 VLAN 的 eduroam 配置更新

1. /etc/raddb/sites-available/eduroam 更新

```
eduroam_default_guest_vlan = "2156" #客户 vlan
eduroam_default_local_vlan = "2166" #本地账号 vlan
post-auth {
    update reply {

        Tunnel-Type := VLAN
        Tunnel-Medium-Type := IEEE-802
    }
    if (&control:Proxy-To-Realm) {
        update reply {
            Tunnel-Private-Group-ID = ${eduroam_default_guest_vlan}
        }
    }
    if (LDAP-Group == "cn=PAST,dc=freetest,dc=com") {
        update reply {

            Tunnel-Private-Group-ID = ${eduroam_default_local_vlan}
        }
    }
    if (LDAP-Group != "cn=PAST,dc=freetest,dc=com" && Stripped-User-
Domain == "${operator_name}") {

        reject

    } #不在 LDAP-Group 组里就拒绝。

    if (&session-state:Stripped-User-Name) {
        update reply {
            User-Name := "%{session-state:Stripped-User-
Name}@%{Stripped-User-Domain}"
        }
    }

    Post-Auth-Type REJECT {
        attr_filter.access_reject
        reply_log
    }
}
}
```

2. ldap 配置文件更新

```
ldap {
  server = '10.10.9.86'           #LDAP 服务器, AD 域服务器配置参考第三部分

  port = 389

  identity = 'cn=admin,ou=IT,dc=freetest,dc=com' #连接 LDAP 的管理员账号, 密码
  password = password

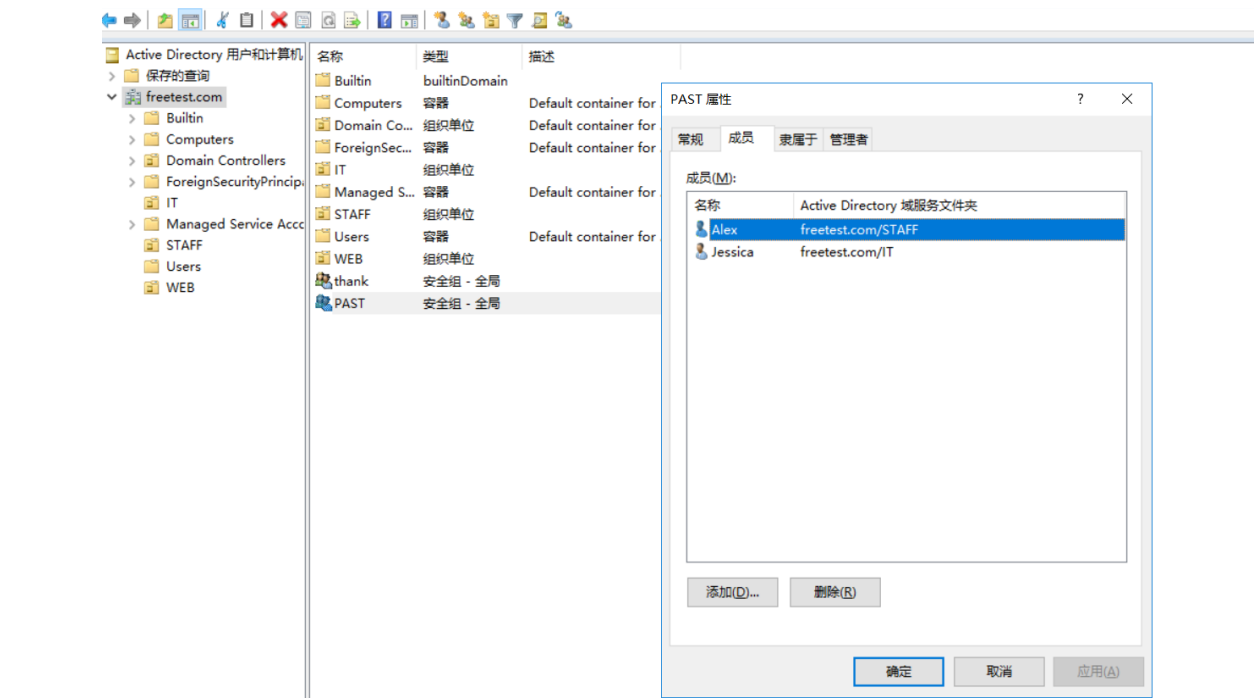
  base_dn = 'dc=freetest,dc=com'

  user {
    base_dn = "${..base_dn}"

    filter = "(samaccountname=%{%{Stripped-User-Name}}:-{%{User-Name}})"
  }

  group {
    base_dn = "${..base_dn}"
    membership_filter = "(|(member=%{control:Ldap-UserDn})(memberUid=%{%{Stripped-User-Name}}:-{%{User-Name}}))"
    membership_attribute = 'memberOf'
  }
}
```

3. AD 域配置



```
PS C:\Users\Administrator> get-adgroup PAST
```

```
DistinguishedName : CN=PAST,DC=freetest,DC=com
GroupCategory     : Security
GroupScope        : Global
Name              : PAST
ObjectClass       : group
ObjectGUID        : 8b622b9d-1b02-4a78-bac0-cf6459806b15
SamAccountName    : PAST
SID               : S-1-5-21-3981203917-699721617-3262906265-1118
```



```
PS C:\Users\Administrator> Get-ADGroupMember PAST

distinguishedName : CN=Alex, OU=STAFF, DC=freetest, DC=com
name               : Alex
objectClass        : user
objectGUID         : a6294fdd-7151-4f5f-b185-ald2dd1fad7
SamAccountName     : Alex
SID                : S-1-5-21-3981203917-699721617-3262906265-1116

distinguishedName : CN=Jessica, OU=IT, DC=freetest, DC=com
name               : Jessica
objectClass        : user
objectGUID         : 54e3854a-98c5-4d00-a782-d3753eee4dd1
SamAccountName     : Jessica
SID                : S-1-5-21-3981203917-699721617-3262906265-1119
```

4. 分别用客户账号，组账号，非组账号测试

测试结果，当用 *francisco@freetest.com* 测试时，因为不在 PAST 组里，被拒绝。

```
(9) Performing search in "cn=PAST,dc=freetest,dc=com" with filter
"(|(member=CN\3dfrancisco\2cOU\3dWEB\2cDC\3dfreetest\2cDC\3dcom)(memberUid=francisco))
", scope "sub"
(9) Waiting for search result...
(9) Search returned no results
(9) Checking user object's memberOf attributes
(9) Performing unfiltered search in "CN=francisco,OU=WEB,DC=freetest,DC=com", scope "base"
(9) Waiting for search result...
(9) No group membership attribute(s) found in user object
rlm_ldap (ldap): Released connection (1)
(9) User is not a member of "cn=PAST,dc=freetest,dc=com"
(9) if (LDAP-Group != "cn=PAST,dc=freetest,dc=com" && Stripped-User-Domain ==
"freetest.com" ) -> TRUE
(9) if (LDAP-Group != "cn=PAST,dc=freetest,dc=com" && Stripped-User-Domain ==
"freetest.com" ) {
(9) [reject] = reject
(9) } # if (LDAP-Group != "cn=PAST,dc=freetest,dc=com" && Stripped-User-Domain ==
"freetest.com" ) = reject
(9) } # post-auth = reject
```


当用 Alex@freetest.com 测试时，因为在 PAST 组里，分配到 2166 动态 VLAN。

Details Identity IPv4 IPv6 Security

Security WPA & WPA2 Enterprise

Authentication Protected EAP (PEAP)

Anonymous identity Alex@freetest.com


CA certificate (None) 

No CA certificate is required

PEAP version Automatic

Inner authentication MSCHAPv2

Username Alex@freetest.com

Password 

Show password

```
Performing search in "cn=PAST,dc=freetest,dc=com" with filter
"(|(member=CN\3dAlex\2cOU\3dSTAFF\2cDC\3dfreetest\2cDC\3dcom)(memberUid=Alex))", scope
"sub"
(9)   Waiting for search result...
(9)   User found in group object "cn=PAST,dc=freetest,dc=com"
rlm_ldap (ldap): Deleting connection (0)
Need 6 more connections to reach 10 spares
rlm_ldap (ldap): Opening additional connection (5), 1 of 28 pending slots used
rlm_ldap (ldap): Connecting to ldap://10.10.9.86:389
TLSMC: MozNSS compatibility interception begins.
tlsmc_convert: INFO: cannot open the NSS DB, expecting PEM configuration is present.
tlsmc_intercept_initialization: INFO: successfully intercepted TLS initialization. Continuing with
OpenSSL only.
TLSMC: MozNSS compatibility interception ends.
rlm_ldap (ldap): Waiting for bind result...
rlm_ldap (ldap): Bind successful
(9)   if (LDAP-Group == "cn=PAST,dc=freetest,dc=com") -> TRUE
(9)   if (LDAP-Group == "cn=PAST,dc=freetest,dc=com") {
(9)     update reply {
(9)       Tunnel-Private-Group-ID = 2166
(9)     }
```

当用 *testfs@cuhk.edu.cn* 测试时，因为这不属于 *freetest.com* 域，属于客户账号，分配到 2156 动态 VLAN。

```
(12) # Executing section post-auth from file /etc/raddb/sites-enabled/eduroam
(12) post-auth {
(12)   update reply {
(12)     Tunnel-Type := VLAN
(12)     Tunnel-Medium-Type := IEEE-802
(12)   } # update reply = noop
(12)   if (&control:Proxy-To-Realm) {
(12)     if (&control:Proxy-To-Realm) -> TRUE
(12)     if (&control:Proxy-To-Realm) {
(12)       update reply {
(12)         Tunnel-Private-Group-ID = 2156
(12)       }
(12)     }
(12)   }
(12) }
```

六 . 参考文档

eduroam 基本配置参考链接 :

<https://wiki.freeradius.org/guide/eduroam>

eduroam samba 加域配置 :

<https://wiki.freeradius.org/guide/FreeRADIUS-Active-Directory-Integration-HOWTO>