Guide

Introduction

eduroam Virtual Appliance (VA) is an image based implementation tool for eduroam . The appliance helps organizations to set up eduroam identity provider (idp) in very reasonable time so that they immediately can participate in the global federation for Internet without having to worry about the complexity to set up eduroam idp. The VA has been customized with pre-configuration to get connected with eduroam Malaysia Federation Level Radius (FLR). The VA image is developed by Academic Grid Malaysia.

Requirement

The EduShib VA requires (minimum):

1. 25GB Storage
2. 2GB Rams
3. 1 Network Interface
4. 2 CPU Cores
5. Firewall: Allow connection from internet to port 80 (tcp), 443 (tcp), 1812 (tcp and udp), 1813 (tcp and udp), 2083 (tcp and udp)
6. 1 IPv4 Public IP address
7. 1 FQDN hostname (e.g. eduroam-idp.university.edu.my)
8. 1 Production level host (SSL) certificate

Info

- The VA should works as-it-is with minimum customization.
- Despite the VA was developed in KVM hypervisor, it could be run at another hypervisor too (tested: VMWare ESXi).
- To improve its performance, simply increase the computer resources (e.g. number of cores, RAM).
- Since this workshop is more focus on deploying eduroam IdP instead of SAML IdP, hence the shibboleth functionality will be removed.
- Despite the EduShib VA comes with pre-configured LDAP server, shall the organization already has directory service installed (e.g. AD, LDAP), it is recommended to connect EduShib VA to the existing directory service instead of using the pre-configured LDAP.
- This VA and tutorial assume that the eduroam users will join the existing network users (same VLAN). Should you need to assign eduroam users to a separate VLAN, you may need to modify the radius config by hand and it's not covered in this tutorial.
- The VA needs to be accessible from the Internet, hence an IPv4 public IP address and FQDN hostname are required. In case you are using NAT, please ensure that inbound and outbound traffic from the VA should be identified from the same IP address (1:1 NAT).
- A Production level host (SSL) certificate is required. You could get it from any SSL certificate reseller. In this tutorial, we are going to get one from letsencrypt.org. The minimum requirement is a domain validation (assurance) based SSL certificate. WARNING: Do not use a wildcard SSL certificate! it won't work!

Installation Instruction

Warning
The steps given below are must be in order! Failed to do so, may cause unsuccessful deployment.

Due to recent OpenSSL vulnerability, please update the openssl library to the latest version before you start to configure the system. To update, please type: yum update -y openssl

1. Download EduShib VA image [Raw Format][OVA Format][VMWare Image Format]
2. Extract the EduShib VA image (For VMWare Image Format, please use the 7-Zip software to extract the image)

```
# tar -jxvf edushib-(version).tar.bz2
```

3. Deploy it to your Virtualization Server
4. Login to the VA (the root password is: eduroamshibboleth)
5. Change the root password:

```
[root@eduroam-idp /root]# passwd
```

6. Configure the network interface according to your network setup. Make sure that the vm can access the Internet
7. Update the OS software

```
[root@eduroam-idp /root]# yum update -y
```

8. Install the certbot software and request a host certificate from letsencrypt:

```
[root@eduroam-idp /root]# yum install -y git
[root@eduroam-idp /root]# git clone https://github.com/letsencrypt/letsencrypt
[root@eduroam-idp /root]# cd letsencrypt
[root@eduroam-idp letsencrypt]# ./letsencrypt-auto certonly -d
eduroam-idp.university.edu.my  (replace eduroam-idp.university.edu.my with your
hostname)
```

9. Download the configuration tool update:

```
[root@eduroam-idp /root]# wget http://sifulan.my/download/runconfig_v2 -O
/opt/installer/bin/runconfig
```

10. Run the configuration tool:

```
[root@eduroam-idp /root]# runconfig --hostname eduroam-idp.university.edu.my --ip
192.168.10.175  (replace eduroam-idp.university.edu.my with your hostname and
192.168.10.175 with the ip address of the vm)
```

11. Download the root CA certificate file

```
[root@eduroam-idp /root]# wget http://sifulan.my/download/tls-ca-bundle.pem -O
/etc/certs/ca/tls-ca-bundle.pem
```

12. Open **/opt/radsecproxy-1.6.5/etc/radsecproxy.conf** file and edit the following lines:

```
Line:

CACertificatePath /etc/certs/ca/

change to:

CACertificateFile /etc/certs/ca/tls-ca-bundle.pem

Line:

CertificateFile /etc/certs/host.pem
CertificateKeyFile /etc/certs/host.key

change to:

CertificateFile /etc/letsencrypt/live/eduroam-idp.university.edu.my/cert.pem
CertificateKeyFile
/etc/letsencrypt/live/eduroam-idp.university.edu.my/privkey.pem

Line:

LogDestination xsyslog:///LOG_LOCAL0

change to:

LogDestination file:///var/log/radsecproxy.log
```

13. Edit **/opt/radsecproxy-1.6.5/etc/conf.d/realms.conf** . Replace: **/edushib\.sifulan\.my$** with your realm (e.g. **/university\.edu\.my$**) and **mytlr.myren.net.my** with **nro1.eduroam.my**
14. Edit **/opt/radsecproxy-1.6.5/etc/conf.d/realms.conf** , Replace: **mytlr.myren.net.my** with **nro1.eduroam.my**
15. Edit **/opt/radsecproxy-1.6.5/etc/conf.d/client.conf .** Replace:

```
client mytlr.myren.net.my {

 host mytlr.myren.net.my

 type tls

 tls defaultClient

 secret xxxx

}
```

with

```
client nro1.eduroam.my {
 host nro1.eduroam.my
 type tls
 tls defaultClient
 secret xxxx
}
```

16. Edit **/opt/radsecproxy-1.6.5/etc/conf.d/server.conf .** Replace:

```
server mytlr.myren.net.my {
 host mytlr.myren.net.my
 type tls
 tls defaultServer
 secret xxxx
}
```

with

```
server nro1.eduroam.my {
        host    nro1.eduroam.my
        type    tls
        tls     defaultServer
        secret  xxxxx
        statusserver on
}
```

17. Edit **/etc/raddb/proxy.conf** . Replace: **edushib\\.sifulan\\.my$** with your realm (e.g. university\\.edu\\.my$)
18. Edit **/opt/radsecproxy-1.6.5/etc/conf.d/clients.conf** . Add your wireless access point IP address/network information to this file by using these syntaxes:

in the case of a standalone/unmanageable wireless access point:

```
client ap-access-point {
 host 192.168.0.0/24  (replace 192.168.0.0/24 with your wireless access point ip
address range)
 type udp
 secret eduroamap  (replace with a good secret password)
}
```

in the case of a controlled/manageable access point:

```
client ap-access-point {
 host 192.168.0.254  (replace 192.168.0.254 with your wireless controller ip
address)
 type udp
 secret eduroamap  (replace with a good secret password)
}
```

19. Restart the radsecproxy service:

```
[root@eduroam-idp /root]# service radsecproxy restart
```

20. Edit /etc/raddb/eap.conf , replace private_key_file, certificate_file and CA_file with the following:

```
private_key_file =
/etc/letsencrypt/live/eduroam-idp.university.edu.my/privkey.pem
certificate_file = /etc/letsencrypt/live/eduroam-idp.university.edu.my/cert.pem
CA_file = /etc/letsencrypt/live/eduroam-idp.university.edu.my/chain.pem
```

21. Restart the radius service:

```
[root@eduroam-idp /root]# service radiusd restart
```

22. Please contact Eduroam Malaysia (support@eduroam.my) to test your EduShib VA installation. Please mention the hostname of your EduShib VA as well.

Installation Guide