

Howto Setup Active Directory / SMS One Time Password (SMSOTP) with FreeRADIUS

Thomas Glanzmann
<thomas@glanzmann.de>

May 2012

Thomas Glanzmann

- Strong Unix background including kernel and virtual machine programming
- Linux, VMware, Storage, HP Trainer and Consultant
- Diplom-Informatiker Univ. (bachelor and master degree in computer science)
- Self-employed

Agenda

- Motivation
- Install and Configure Debian squeeze
- Install the build dependencies
- Compile and install FreeRADIUS
- Configure FreeRADIUS
- Test the setup
- Sources

Motivation

- SMSOTP authentication for VMware View 5.1
- SMSOTP authentication for Citrix Netscaler Access Gateway Enterprise
- SMSOTP authentication for Cisco ASA

Install and Configure Debian squeeze

- Can be a virtual or physical system
- In production environments you should have at least two radius servers
- The system needs internet access during installation
- Debian 6.0.5 businesscard CD image
- Make sure your clocks are in sync

Install the build dependencies

```
sudo apt-get install libossp-uuid-perl libfrontier-rpc-perl \  
    libcrypt-ssleay-perl libio-socket-ssl-perl git bzip2 ssh \  
sudo gcc libssl-dev make openssl krb5-user libkrb5-dev \  
libpoe-perl postfix libauthen-radius-perl libberkeleydb-perl \  
ntpdate libterm-readpassword-perl
```

Compile and install FreeRADIUS

```
wget -o /dev/null -O - ftp://ftp.freeradius.org/pub/freeradius/freeradius-server-2.1.12.tar.bz2 | tar xjf -
sudo mkdir /local
sudo chown sithglan /local
cd ~/freeradius-server-2.1.12
./configure --with-openssl --prefix=/local/freeradius-server-2.1.12
make
make install

cd ~/freeradius-server-2.1.12/src/modules/rlm_smsotp
chmod +x configure
./configure --prefix=/local/freeradius-server-2.1.12
make
make install
```

Configure FreeRADIUS: clients.conf

```
client 10.10.20.220 {
    secret = testing123
    shortname = netscaler
}
client 10.10.20.230 {
    secret = testing123
    shortname = cs-01
}
client 127.0.0.1 {
    secret = testing123
    shortname = cs-01
}
```


Configure FreeRADIUS: sites-enabled/default

```
authenticate {  
    Auth-Type smsotp {  
        krb5  
        smsotp  
    }  
  
    Auth-Type smsotp-reply {  
        smsotp  
    }  
}
```

```
authorize {  
    preprocess  
    files  
    smsotp  
}
```

Configure FreeRADIUS: users

```
DEFAULT Auth-Type := smsotp
```

Configure FreeRADIUS: hints

```
DEFAULT User-Name =~ "^directory\\\\\\\\([^\@]+)"
```

```
User-Name := "%{1}@DIRECTORY.GMVL.DE"
```

```
DEFAULT User-Name =~ "^(^\@+)\@directory.gmvl.de"
```

```
User-Name := "%{1}@DIRECTORY.GMVL.DE"
```

Test the setup

```
(minisqueeze) [~/work/smsotpd] ./pap_challenge_request.pl
Enter username: directory\Administrator
Enter password:
server response type = Access-Challenge (11)
Enter otp: 97350
server response type = Access-Accept (2)
```

References

- [FreeRADIUS smsotp documentation](#)
- [PAP followed by a smsotp authentication](#)
- [Radius Wikipedia Entry](#)