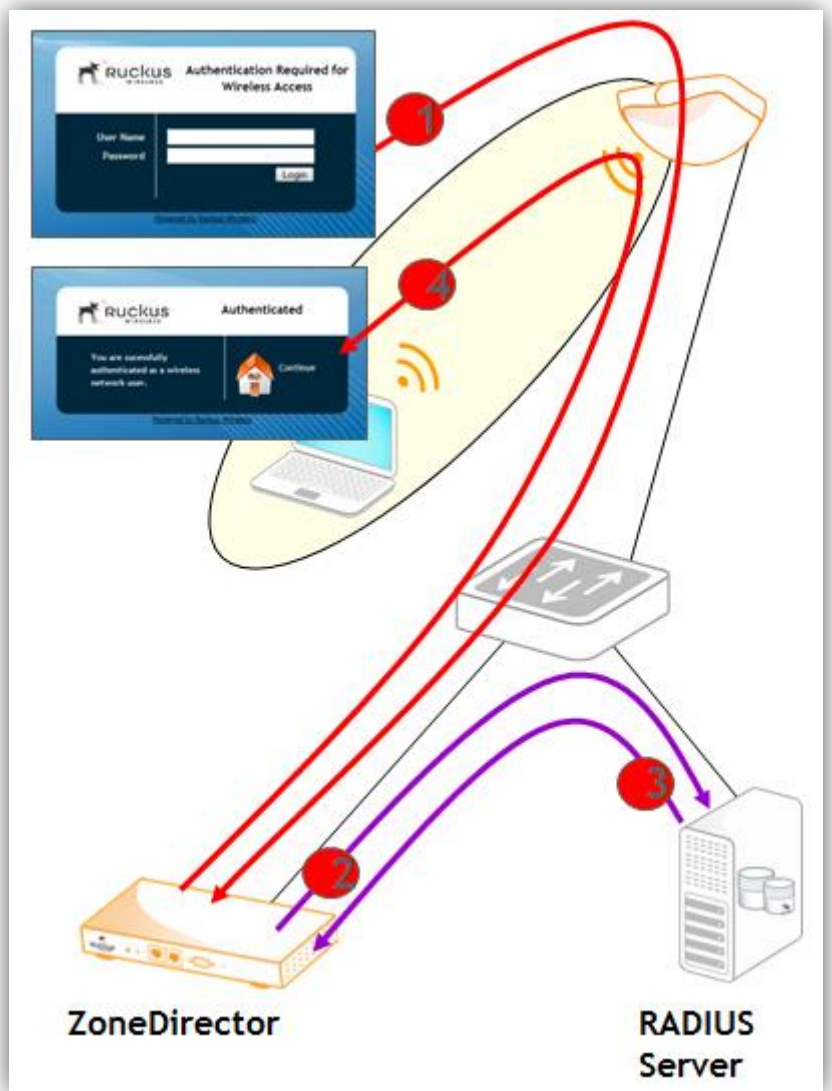

RUCKUS FREERADIUS

Technote

Versie: 1.1
Auteur: Thomas Snijder
Datum: 2-05-2014

Inhoud

1 Inleiding

In dit document wordt beschreven hoe u FreeRadius moet installeren en configureren om een werkende FreeRadius authenticatie server op te zetten. De FreeRadius authenticatie server kunt u gebruiken om gebruikers aan het juiste WLAN te koppelen via het Zero-IT concept van Ruckus Wireless. Na de installatie en configuratie wordt de inrichting besproken van de FreeRadius server, zoals het aanmaken van groepen, gebruikers en clients (ZoneDirectors). Daarnaast wordt beschreven hoe u de ZoneDirector van Ruckus Wireless moet configureren zodat u de juiste WLANs en instellingen heeft voor het Zero-IT concept. Ook wordt beschreven hoe u in de ZoneDirector een AAA profiel kunt aanmaken voor uw FreeRadius server.

In sommige onderdelen van deze technote wordt om gebruikersinvoer gevraagd door middel van de volgende tekens: <…>. Verwijder deze tekens en plaats uw eigen informatie over bijvoorbeeld gebruikersnamen en wachtwoorden.

De technote is gebaseerd en getest op CentOS 6.5 Live CD. Voor het aanpassen van configuratiebestanden hebben wij de grafische teksteditor Gedit gebruikt. Mocht u alleen toegang hebben tot de server via SSH of Telnet, dan moet u “gedit” vervangen voor “vi”.

Let op: Wij hebben de installatie van de Live CD gebruikt. Als u alleen de Live CD opstart zonder te installeren, dan verliest u alle aanpassingen na een herstart. U kunt de installatie direct starten als u de cd opstart. U kunt ook de installatie starten door op de installatie snelkoppeling te klikken op het bureaublad.

Let op: Het kopiëren van command regels uit dit document en vervolgens plakken in de terminal kan tot fouten leiden door verschillen in de gebruikte tekenset. Als u commando’s rechtstreeks in de terminal wilt plakken kunt u de commando’s uit het tekstbestand “Terminal Commands.txt” kopiëren. Eventuele commando’s die om gebruikersinvoer.

2 Installaties

Hieronder wordt beschreven welke installatie mogelijkheden CentOS 6.5 aanbiedt. Daarnaast wordt beschreven hoe u FreeRadius kunt installeren op CentOS 6.5.

2.1 CentOS 6.4 installatie

CentOS biedt meerdere installatiemogelijkheden aan. Voor deze technote is de CentOS 6.5 Live CD installatie gebruikt. Hieronder vindt u een korte toelichting over de verschillende installaties:

- CentOS Bin DVD - Deze installatiemogelijkheid biedt u de optie om tijdens de installatie wizard volledig te specificeren wat voor soort server u wilt gaan opzetten.
- CentOS Minimal - Deze installatiemogelijkheid installeert alleen de pakketten die CentOS nodig heeft om op te starten. U krijgt dus niet de mogelijkheid om tijdens de installatie aan te geven welke extra pakketten u wilt instaleren. Dit na de installatie wel mogelijk via een software beheer programma zoals "yum".
- CentOS Live CD/DVD - De live CD/DVD geeft u de mogelijkheid om een complete CentOS installatie op te starten vanaf de CD/DVD. De live CD/DVD laadt deze installatie in het geheugen van uw server. Wijzigingen die u aanbrengt aan deze installatie zullen verloren gaan na het herstarten van uw server. Daarnaast biedt de live CD/DVD de mogelijkheid om de betreffende installatie te installeren op uw server. Hierdoor zullen wijzigingen niet verloren gaan na het herstarten van uw server.

Via de onderstaande link kunt u één van de installaties downloaden:

Download CentOS 6.5

2.2 FreeRadius installatie

Hieronder wordt beschreven hoe u FreeRadius en de andere benodigde onderdelen kunt installeren. Om FreeRadius te installeren moet u als Root ingelogd zijn op de CentOS server. De commando's voor de installatie moeten via de terminal uitgevoerd worden:

```
[root@localhost ~]# yum -y install freeradius freeradius-utils freeradius-mysql mysql mysql-server
```

Door het bovenstaande command uit te voeren zullen de benodigde onderdelen geïnstalleerd worden die nodig zijn voor de installatie/configuratie van de FreeRadius server.

3 Configuratie

3.1 MySQL configuratie

Voordat u kunt beginnen aan het configureren van FreeRadius moet u eerst MySQL configureren. De onderstaande instructies zullen u helpen met het opzetten van de juiste databasestructuur. Om met de MySQL configuratie te beginnen moet u de MySQL server eerst starten met het volgende command:

```
[root@localhost ~]# service mysqld start
```

Als u de intentie heeft om de FreeRadius server in een productie omgeving te gaan gebruiken, dan raden wij u aan om het onderstaande script uit te voeren. Dit script verzorgt de volgende onderdelen van de MySQL installatie:

- Wachtwoord toekennen voor het MySQL Root account
- Root accounts verwijderen die vanaf buiten de localhost benaderd kunnen worden
- Verwijderen van anonieme gebruikers accounts
- Verwijderen van test database

```
[root@localhost ~]# /usr/bin/mysql_secure_installation
```

Hieronder worden de commando's beschreven voor het creëren van de database en voor het maken van de juiste tabellenstructuur.
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database aanmaken:

```
mysql> create database radiusauth;
```

Gebruiker aanmaken voor de zojuist aangemaakte database:

```
mysql> grant all on radiusauth.* to raduser@localhost identified by
"raduser123";
```

Gebruikersrechten opnieuw doorvoeren:

```
mysql> flush privileges;
```

Database selecteren voor het aanmaken van de tabellen:

```
mysql> use radiusauth;
```

De tabellen-schema's importeren:

```
mysql> source /etc/raddb/sql/mysql/schema.sql;
mysql> source /etc/raddb/sql/mysql/nas.sql;
```

Na het uitvoeren van de bovenstaande commando's is de MySQL configuratie afgerond. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

3.2 FreeRadius configuratie

In dit hoofdstuk wordt de configuratie van FreeRadius behandeld. Om FreeRadius te configureren moet u als Root zijn ingelogd op de CentOS server. De commando's voor de configuratie moeten via de terminal uitgevoerd worden.

3.2.1 SQL configuratiebestand

Hieronder wordt beschreven welke instellingen u moet aanpassen in het SQL configuratiebestand. FeeRadius zal dit configuratiebestand gebruiken voor het opzetten van een verbinding naar de MySQL server. Ook wordt in dit configuratiebestand aangegeven in welke database FreeRadius de gebruikers moet gaan authentiseren. Daarnaast wordt nog aangegeven dat FreeRadius de database moet gebruiken voor het uitlezen van zijn clients. Het configuratiebestand opent u als volgt:

```
[root@localhost ~]# gedit /etc/raddb/sql.conf
```

In dit configuratiebestand past u de volgende gegevens aan:

```
server = "localhost"     Mocht de MySQL server die u wilt gebruiken niet
                         actief zijn op de localhost, dan dient u hier het
                         IP adres op te geven van de externe MySQL server.

port = 3306              Mocht de MySQL server actief zijn op een andere
                         poort, dan dient u hier het poort nummer te
                         wijzigen.

login = "raduser"        Hier vult u de gebruikersnaam in die u heeft
                         aangemaakt voor de database radiusauth.

password = "raduser123"  Hier vult u het bijbehorende wachtwoord in van de
                         opgegeven gebruikersnaam.

radius_db = "radiusauth"     Dit is de naam van de database die FreeRadius
                         moet gebruiken voor het authentiseren van de
                         gebruikers. Mocht u een database aangemaakt hebben
                         met een andere naam, dan moet u hier die naam in
                         vullen.

readclients = yes        Door de comment (#) weg te halen zal FreeRadius
                         voortaan de database gebruiken voor het uitlezen
                         van zijn clients (ZoneDirectors).
```

Als u de bovenstaande aanpassingen heeft gedaan, dan kunt u het bestand opslaan en sluiten door middel van de keuzeopties van de editor.

3.2.2 Radiusd configuratiebestand

Hieronder wordt beschreven welke instellingen u moet aanpassen in het radiusd configuratiebestand. Radiusd is het hoofd configuratiebestand van de FreeRadius installatie. In dit configuratiebestand moet worden aangegeven dat clients.conf niet gebruikt mag worden voor het uitlezen van de clients. Daarnaast moet worden aangegeven dat FreeRadius het sql.conf bestand moet gebruiken voor het opzetten van de verbinding met de MySQL server. Het configuratiebestand opent u als volgt:

```
[root@localhost ~]# gedit /etc/raddb/radiusd.conf
```

In het configuratiebestand past u de volgende gegevens aan:

```
#$INCLUDE clients.conf  Door een comment (#) te plaatsen voor deze regel
                        zal FreeRadius het clients.conf bestand negeren
                        tijdens het opstarten.

$INCLUDE sql.conf       Door de comment (#) weg te halen zal FreeRadius
                        het sql.conf bestand uitlezen tijdens het
                        opstarten.
```

Als u bovenstaande aanpassingen heeft gedaan, dan kunt u het bestand opslaan en sluiten door middel van de keuzeopties van de editor.

Hieronder wordt beschreven hoe u twee bestanden op de server moet vervangen. Deze bestanden bevatten instellingen over de authenticatiemogelijkheden van de client (ZoneDirector). Omdat deze bestanden te lang zijn om in een Word document weer te geven, vindt u twee voorgeconfigureerde bestanden in de map “Files”. De map Files vindt u in het gedownloade .zip bestand van de Alcadis support site. De bestanden hebben de volgende naam:

- default
- inner-tunnel

Deze twee bestanden moet u naar het bureaublad van de server kopiëren. Na het kopiëren van de bestanden gebruikt u de volgende twee commando’s om de bestanden op de juiste plek te zetten:

```
[root@localhost ~]# cp /root/Desktop/default /etc/raddb/sites-enabled/
```

Op de vraag of u dit bestand wilt overschrijven antwoord u: “**y**”.

```
[root@localhost ~]# cp /root/Desktop/inner-tunnel /etc/raddb/sites-
enabled/
```

Op de vraag of u dit bestand wilt overschrijven antwoord u: “**y**”.

Wilt u graag de inhoud van deze bestanden bekijken, dan kunt u deze bestanden als volgt openen:

```
[root@localhost ~]# gedit /etc/raddb/sites-enabled/default
[root@localhost ~]# gedit /etc/raddb/sites-enabled/inner-tunnel
```

3.2.3 Ruckus dictionary

Hieronder wordt beschreven hoe u een Ruckus dictionary bestand kunt aanmaken. Dit bestand is nodig omdat FreeRadius anders geen groepsattributen kan sturen naar de ZoneDirector. De gegevens die in dit bestand worden geplaatst komen van de Ruckus support site. Elke vendor zal deze gegevens beschikbaar stellen omdat dit "Vendor Specific Attributes" zijn. Het dictionary bestand maakt u als volgt aan:

```
[root@localhost ~]# gedit /usr/share/freeradius/dictionary.ruckus
```

U heeft nu een leeg tekst bestand geopend. In dit lege tekstbestand plaatst u de onderstaande gegevens:

```
#########################################################################
# -*- text -*-
#
#             dictionary.ruckus
#
#             place the following line into the "dictionary" file of your
FreeRadius installation
#             $INCLUDE dictionary.ruckus
#
#             For use with FreeRadius and ZoneDirector
#
#             Vendor-ID:         25053
#
VENDOR Ruckus 25053

BEGIN-VENDOR Ruckus

ATTRIBUTE Ruckus-User-Groups 1 string
ATTRIBUTE Ruckus-Sta-RSSI 2 integer
ATTRIBUTE Ruckus-SSID 3 string
ATTRIBUTE Ruckus-WlanID 4 integer
ATTRIBUTE Ruckus-Location 5 string
ATTRIBUTE Ruckus-Grace-Period  6 integer
ATTRIBUTE Ruckus-SCG-CBlade-IP 7 integer
ATTRIBUTE Ruckus-SCG-DBlade-IP 8 integer
ATTRIBUTE Ruckus-Session-Type 125 integer
ATTRIBUTE Ruckus-Acct-Status 126 integer

END-VENDOR Ruckus
#########################################################################
```

Na het invoeren van bovenstaande informatie kunt u het bestand opslaan en sluiten via de keuzeopties van de editor.

Hieronder wordt beschreven hoe u het Ruckus dictionary bestand kunt toevoegen aan het hoofd dictionary bestand. Door het Ruckus dictionary bestand toe te voegen zal FreeRadius kunnen omgaan met de "Vendor Specific Attributes" van Ruckus. Het hoofd dictionary bestand opent u als volgt:

```
[root@localhost ~]# gedit /etc/raddb/dictionary
```

In het dictionary bestand voegt u de volgende dik gedrukte regel toe onder het aangegeven stukje tekst:

```
#
#     Place additional attributes or $INCLUDEs here.
#     …….
#     the format of the dictionary files.
#
$INCLUDE    /usr/share/freeradius/dictionary.ruckus
```

Na het toevoegen van de dik gedrukte regel kunt u het bestand opslaan en sluiten via de keuzeopties van de editor.

Alle configuratie aanpassingen zijn nu gedaan. In hoofdstuk 4 is beschreven hoe u de FreeRadius installatie kunt testen. Mocht u tijdens het testen tegen problemen aanlopen, dan is in hoofdstuk 5 beschreven hoe u deze problemen kunt troubleshooten.

In hoofdstuk 6 is beschreven hoe u de FreeRadius server kunt inrichten, zoals het aanmaken van groepen, gebruikers en clients (ZoneDirectors).

In hoofdstuk 7 is beschreven welke beveiligingsaanpassingen u moet maken zodat de clients (ZoneDirectors) kunnen communiceren met uw FreeRadius server.

In hoofdstuk 8 vindt u een toelichting over de commando's die gebruikt zijn in deze technote. Hierin is beschreven welke commando's u eventueel kunt aanpassen om de FreeRadius installatie naar uw eigen hand te zetten.

In hoofdstuk 10 is beschreven hoe u de ZoneDirector moet configureren voor het authentiseren van gebruikers tegen de zojuist aangemaakte FreeRadius server.

4 Testen

Na het configureren van zowel MySQL als FreeRadius, kunt u gaan testen of de FreeRadius server goed geconfigureerd is. Voor het testen kunt u gebruikmaken van het programma Radtest. Dit programma kan lokaal op de server gebruikt worden. U hoeft dus niet eerst de ZoneDirector te configureren om de werking van de FreeRadius server te testen.

4.1 Loopback client

Om lokaal de testen te kunnen uitvoeren moet u een client aanmaken voor het loopback adres van de FreeRadius server. Dit moet u doen omdat anders de FreeRadius server de aanvraag van het loopback adres niet zal accepteren. Het toevoegen van een client voor het loopback adres gaat als volgt.
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Client aanmaken:

```
mysql> insert into nas (nasname,shortname,type,secret) values
("127.0.0.1","<omschrijving>","other","<secret>");
```

Na het uitvoeren van de bovenstaande commando's is de loopback client toegevoegd. Sluit MySQL nog niet af, u moet nog een testgebruiker aanmaken.

4.2 Testgebruiker

Nu de client is aangemaakt voor het loopback adres moet u ook een testgebruiker aanmaken. De aangemaakte gebruiker kunt u dan gaan authentiseren met het programma Radtest. Het toevoegen van een gebruiker gaat als volgt.
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Gebruiker aanmaken:

```
mysql> insert into radcheck (username,attribute,op,value) values
("<gebruikersnaam>","Cleartext-Password",":=","<wachtwoord>");
```

Na het uitvoeren van de bovenstaande commando's is de testgebruiker toegevoegd. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

4.3 Radtest

De client voor het loopback adres en de testgebruiker zijn nu aangemaakt. Nu kunt u de FreeRadius server starten:

```
[root@localhost ~]# service radiusd start
```

Na het starten van de server kunt u het programma Radtest gebruiken om deze gebruiker te authentiseren. Het programma Radtest moet u als volgt aanroepen:

```
[root@localhost ~]# radtest <gebruikersnaam> <wachtwoord> 127.0.0.1 0
<secret>
```

Het programma Radtest zal nu proberen om de opgegeven gebruiker te authentiseren tegen de zojuist opgezette FreeRadius server. Als u in de output van het programma "rad_recv: Access-Accept" terug ziet komen dan is de FreeRadius server goed geconfigureerd. Mocht u deze uitkomst niet krijgen, dan kunt u het beste hoofdstuk 5 "Troubleshooting" raadplegen.

De installatie en configuratie is nu voltooid. Het laatste wat u nu nog moet doen is het inrichten van de FreeRadius server. In hoofdstuk 6 wordt beschreven hoe u groepen, gebruikers en de ZoneDirector kunt toevoegen aan de MySQL database.

5 Troubleshooting

Hieronder wordt beschreven hoe u te werk kunt gaan als u tegen problemen aanloopt met de FreeRadius installatie. Mocht u na de radtest geen "rad_recv: Access-Accept" terug krijgen, dan is het verstandig om FreeRadius in debug mode op te starten. FreeRadius debug mode laat u exact zien waar het mis gaat met het laden van de configuratiebestanden. Op de server kan maar 1 FreeRadius service tegelijk actief zijn. Omdat u voor het testen de FreeRadius server heeft gestart, moet u deze eerst afsluiten. Pas daarna kan de FreeRadius service opnieuw opgestart worden in de debug mode.

FreeRadius service stoppen:

```
[root@localhost ~]# service radiusd stop
```

FreeRadius in debug mode starten:

```
[root@localhost ~]# radiusd -X
```

FreeRadius zal nu in debug mode opstarten. Aan de hand van deze debug output kunt u gaan controleren waar het precies mis gaat. Mocht FreeRadius zonder problemen opstarten in debug mode dan kunt u dit herkennen aan de volgende regel in de terminal: **Ready to process requests**.

Als FreeRadius zonder problemen opstart in debug mode, maar u krijgt niet de melding "rad_recv: Access-Accept" als u radtest uitvoert, dan kunt u het beste de FreeRadius service in debug mode laten staan en een nieuwe terminal openen. In de nieuwe terminal voert u nog een keer het programma radtest uit. In de debug terminal van FreeRadius kunt u dan zien hoe het verzoek behandeld wordt door de FreeRadius server. Aan de hand van deze debug output kunt u gaan controleren waar het precies mis gaat.

Om FreeRadius weer normaal te starten doet u het volgende:

FreeRadius debug mode afsluiten:
Ctrl + c in de FreeRadius debug terminal

FreeRadius normaal starten:

```
[root@localhost ~]# service radiusd start
```

6 FreeRadius inrichting

In de onderstaande hoofdstukken wordt beschreven hoe u groepen, gebruikers en clients (ZoneDirectors) kunt toevoegen aan de MySQL server. Het is verstandig om met de groepen te beginnen, omdat u daarna de gebruikers direct aan deze groepen kunt koppelen.

6.1 Groepen

Via de onderstaande commando's kunt u groepen aanmaken. U kunt deze handeling herhalen om nog meer groepen toe te voegen:
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Groep aanmaken:

```
mysql> insert into radgroupreply (groupname,attribute,op,value) values
("<groepnaam>","Ruckus-User-Groups",":=","<groepnaam>");
```

Na het uitvoeren van de bovenstaande commando's is de groep toegevoegd. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

6.2 Gebruikers (handmatig)

Via de onderstaande commando's kunt u een gebruiker aanmaken. U kunt deze handeling herhalen om nog meer gebruikers toe te voegen:
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Gebruikers aanmaken:

```
mysql> insert into radcheck (username,attribute,op,value) values
("<gebruikersnaam>","Cleartext-Password",":=","<wachtwoord>");
```

Na het uitvoeren van de bovenstaande commando's is de gebruiker toegevoegd. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

Via de onderstaande commando's kunt u een gebruiker toekennen aan een groep. U kunt deze handeling herhalen om nog meer gebruikers toe te kennen aan een groep:

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Gebruikers toekennen aan groepen:

```
mysql> insert into radusergroup (username,groupname) values
("<gebruikersnaam>","<groepnaam>");
```

Na het uitvoeren van de bovenstaande commando's is de gebruiker toegekend aan een groep. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

6.3 Gebruikers (.csv)

Gebruikers kunnen geïmporteerd worden via een .csv bestand. Ook kunnen gebruikers aan een groep gekoppeld worden via een .csv bestand. De .csv bestanden kunt u vinden in de map "Files". De map Files vindt u in het gedownloade .zip bestand van de Alcadis support site. De bestanden hebben de volgende naam:

- Gebruiker_Sjabloon.csv - Bedoeld voor het aanmaken van gebruikers.
- Groep_Sjabloon.csv - Bedoeld voor het koppelen van gebruikers aan groepen.

Beide bestanden zijn te openen met Excel zodat de inhoud aangepast kan worden. Als u de bestanden heeft aangepast moet u de bestanden naar het bureaublad van de server kopiëren.

Na het kopiëren van de bestanden naar het bureaublad van de server, kunt u de volgende twee commando's gebruiken om de bestanden op de juiste plek te zetten:

```
[root@localhost ~]# cp /root/Desktop/Gebruiker_Sjabloon.csv
/var/lib/mysql/<database>/
[root@localhost ~]# cp /root/Desktop/Groep_Sjabloon.csv
/var/lib/mysql/<database>/
```

Via de hieronder beschreven commando's kunt u gebruikers importeren met behulp van het .csv bestand.
Let op: Alle commando's die u uitvoert in de MySQL prompt moeten worden afgesloten met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Gebruikers importeren via .csv bestand:

```
mysql> load data infile 'Gebruiker_Sjabloon.csv' into table radcheck
fields terminated by ';' lines terminated by '\r\n' ignore 1 lines
(username,attribute,op,value);
```

Na het uitvoeren van de bovenstaande commando's zijn de gebruikers geïmporteerd. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

Via de hieronder beschreven commando's kunt u gebruikers toekennen aan een groep met behulp van het .csv bestand.

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

Gebruikers toekennen aan groepen via .csv bestand:

```
mysql> load data infile 'Groep_Sjabloon.csv' into table radusergroup
fields terminated by ';' lines terminated by '\r\n' ignore 1 lines
(username,groupname);
```

Na het uitvoeren van de bovenstaande commando's zijn de gebruikers toegekend aan een groep. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

6.4 ZoneDirector

Via de onderstaande commando's wordt de ZoneDirector toegevoegd aan de MySQL database. De gegevens die u hier invoert heeft u later nodig als u een AAA server aanmaakt in uw ZoneDirector.
Let op: Alle commando's die u uitvoert in de MySQL prompt dienen afgesloten te worden met ";".

Inloggen op MySQL:

```
[root@localhost ~]# mysql -uroot -p<root wachtwoord>
```

Database selecteren:

```
mysql> use radiusauth;
```

ZoneDirector aanmaken:

```
mysql> insert into nas (nasname,shortname,type,secret) values
("<zdip>","<omschrijving>","Wireless-802.11","<secret>");
```

Na het uitvoeren van de bovenstaande commando's is de ZoneDirector toegevoegd. U kunt MySQL afsluiten met het volgende commando:

```
mysql> exit
```

Mocht u op een later tijdstip nog meer "Clients" toevoegen, dan dient u na het toevoegen de FreeRadius server te herstarten:

```
[root@localhost ~]# service radiusd restart
```

7 Beveiliging

Hieronder wordt beschreven welke aanpassingen u moet maken in het iptables configuratiebestand. Het iptables configuratiebestand bevatten de firewall regels voor uw CentOS server. Via dit configuratiebestand kunt u specificeren welke diensten (poorten) toegang mogen hebben tot uw CentOS server. Standaard worden de poorten voor FreeRadius en de in hoofdstuk 11 beschreven GUI geblokkeerd. Het configuratiebestand opent u als volgt:

```
[root@localhost ~]# gedit /etc/sysconfig/iptables
```

In dit configuratiebestand voegt u de volgende dikgedrukte regels toe:
Let op: Plaats de dikgedrukte regels boven eventuele REJECT regels anders worden deze alsnog genegeerd.

```
#FreeRadius
-A INPUT -p udp --dport 1812 -j ACCEPT
```

Als u de bovenstaande aanpassingen heeft gedaan, dan kunt u het bestand opslaan en sluiten door middel van de keuzeopties van de editor.

Na het opslaan van de iptables moet u de iptables service herstarten om de nieuwe regels actief te maken:

```
[root@localhost ~]# service iptables restart
```

Wilt u geen gebruik maken van iptables dan kunt deze service helemaal uitzetten op uw CentOS server via het volgende commando:

```
[root@localhost ~]# service iptables stop
```

Hieronder vindt u een voorbeeld van het iptables configuratiebestand met daarin de firewall regels voor FreeRadius en de DaloRadius GUI.

```
# Firewall configuration written by system-config-firewall
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
#FreeRadius
-A INPUT -p udp --dport 1812 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

8 Commando toelichting

In de commando's die wij in deze technote gebruikt hebben zijn consequent voorbeelden gebruikt om te kunnen laten zien waar bepaalde gegevens op andere locaties weer opnieuw van toepassing zijn. Wij zullen hieronder beschrijven welke commando's u kunt aanpassen om de FreeRadius installatie naar uw eigen hand te zetten.

Tijdens de MySQL configuratie maken wij een database aan en een gebruiker met toegang tot deze database. De aangemaakte database en de gebruiker moet u later aanpassen in het sql.conf bestand. Aan de hand van de informatie in het sql.conf bestand zal FreeRadius een verbinding proberen op te zetten met de MySQL server. De onderstaande commando's kunt u zelf aanpassen zolang u de wijzigingen ook doorvoert in het sql.conf bestand.

```
mysql> create database <databasenaam>;
mysql> grant all on <databasenaam>.* to <gebruikersnaam>@localhost
identified by "<wachtwoord>";
```

Mocht u tijdens de MySQL configuratie gebruik maken van een andere databasenaam dan in deze technote wordt beschreven, dan moet u bij het selecteren van de database er rekening mee houden dat u de juiste databasenaam gebruikt.

```
mysql> use <databasenaam>;
```

9 MySQL commando's

Hieronder worden MySQL commando's beschreven die u kunt gebruiken voor het beheren van uw MySQL database.

Commando	Omschrijving
mysql> show databases;	Alle databases weergeven
mysql> use <database>;	Database selecteren
mysql> show tables;	Alle tabellen weergeven van database
mysql> describe <tabel>;	Tabel format weergeven
mysql> drop <database>;	Database verwijderen
mysql> drop table <tabel>;	Tabel verwijderen
mysql> select * from <tabel>;	Inhoud van tabel tonen
mysql> delete from <tabel> where <veld naam> = '<waarde>';	Regel verwijderen uit tabel
mysql> flush privileges;	Update gebruikersrechten

10 ZoneDirector configuratie

Hieronder wordt beschreven hoe u een WLAN kunt aanmaken die gebruikt kan worden voor het Zero-IT concept. Deze handeling kunt u herhalen voor het toevoegen van nog meer WLANs met Zero-IT functionaliteit. Verder in dit hoofdstuk wordt beschreven hoe u verschillende rollen kunt aanmaken voor deze WLANs. Met deze rollen kunt u aangegeven welke gebruikersgroep toegang heeft tot dit WLAN. Om het Zero-IT concept goed te kunnen uitvoeren moet u eerst een gasten netwerk aanmaken. Het aanmaken van een gasten netwerk gaat als volgt:

1. Login op de webinterface van uw ZoneDirector
2. Navigeer naar Configure > WLANs
3. Klik op "Create new" en vul de volgende informatie in:
    - Name/SSID - Naam van uw WLAN
    - Descprition - Omschrijving van uw WLAN
    - Type - Hier kiest u voor Guest Access
4. De rest van de instellingen kunt u default laten staan. Klik op "Ok" om de ingevulde informatie op te slaan

Hieronder wordt beschreven hoe u de captive portal voor het gasten netwerk kunt activeren:

1. Login op de webinterface van uw ZoneDirector
2. Navigeer naar Configure > Guest Access
3. Op deze pagina past u de volgende instellingen aan:
    - Plaats een vinkje bij: Enable Zero-IT device registration from the Guest Portal
    - Plaats het bolletje bij: Use guest pass authentication
4. Klik op "Ok" om de instellingen op te slaan

Nu het gasten netwerk is aangemaakt en de captive portal geactiveerd is, kunt u een WLAN aanmaken voor het Zero-IT concept. Het aanmaken van een WLAN met Zero-IT functionaliteit gaat als volgt:

1. Login op de webinterface van uw ZoneDirector
2. Navigeer naar Configure > WLANs
3. Klik op "Create new" en vul de volgende informatie in:
    - Name/SSID - Naam van uw WLAN
    - Description - Omschrijving van uw WLAN
    - Type - Standard Usage
    - Authentication Method - Open
    - Ecryption Method - WPA2
    - Algorithm - AES
    - Passpharse - Hier vult u het wachtwoord in van het WLAN. U heeft dit wachtwoord later niet meer nodig omdat elke client een uniek wachtwoord zal hebben. Wij raden dan ook aan om dit wachtwoord zolang mogelijk te maken.
    - Plaats een vinkje bij: Enable Zero-IT Activation
    - Plaats een vinkje bij: Enable Dynamic PSK with 62 characters passphrase
    - Wilt u dat gebruikers maar een beperkt aantal apparaten kunnen aanmelden, dan moet u een vinkje plaatsen bij: Limit D-PSK generation per user to X devices.
4. De rest van de instellingen kunt u default laten staan. Klik op "Ok" om de ingevulde informatie op te slaan

Hieronder wordt beschreven hoe u een authenticatieserver moet aanmaken op de ZoneDirector. Na het aanmaken van de authenticatieserver, kunt u de test functie gebruiken om te controleren of de ZoneDirector daadwerkelijk met de FreeRadius server kan communiceren. Het aanmaken van een authenticatieserver gaat als volgt:

1. Login op de webinterface van uw ZoneDirector
2. Navigeer naar Configure > AAA Servers
3. Klik op "Create new" en vul de volgende informatie in:
    - Name – <Naam voor deze authenticatie server>
    - Type – RADIUS
    - Auth Method – PAP
    - IP Address – <IP adres van uw FreeRadius server>
    - Port – 1812
    - Shared Secret – <Secret van de betreffende ZoneDirector>
    - Confirm Secret – <Secret van de betreffende ZoneDirector>
4. Klik op "Ok" om de ingevulde informatie op te slaan

De authenticatieserver is nu aangemaakt. Nu kunt u bij "Test Authentication Settings" de FreeRadius server selecteren en testen of u gebruikers via de ZoneDirector kunt authentiseren op uw FreeRadius server.