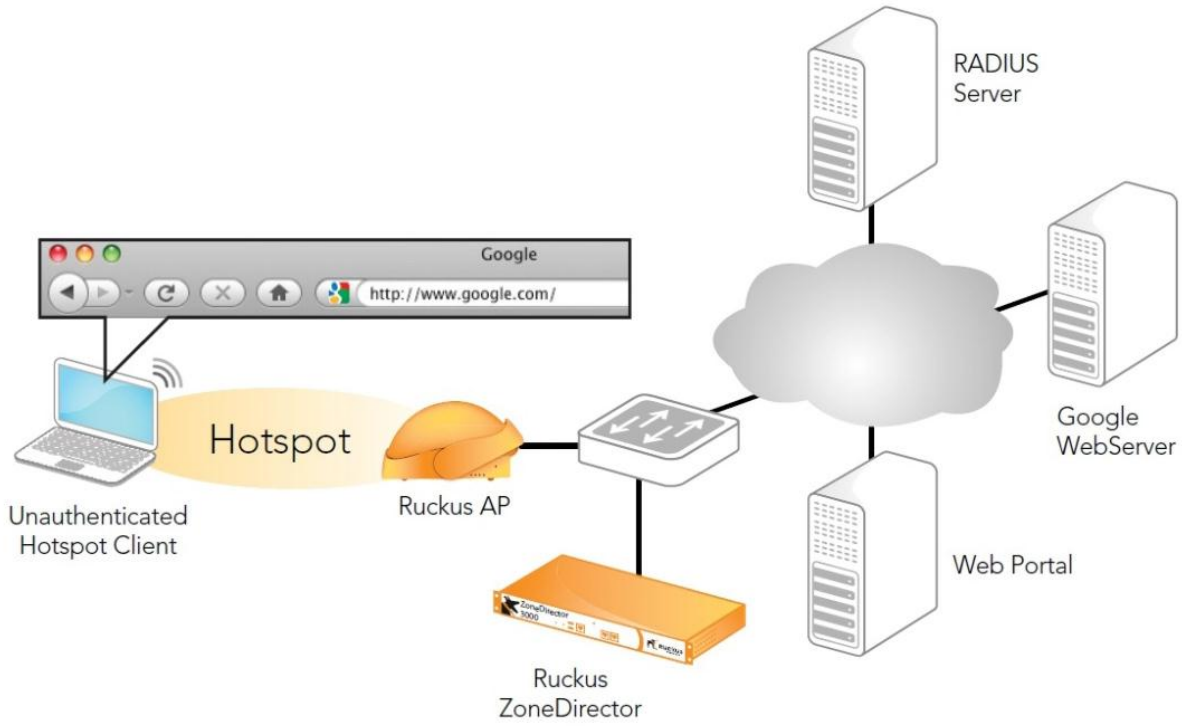


WISPR

Technote

Versie: 1.0
Auteur: Thomas Snijder
Datum: 24-02-2014

Inhoud

1 Inleiding

In dit document wordt beschreven hoe u een WISPr-omgeving kunt opzetten met de bijbehorende webserver en radius server. WISPr maakt het mogelijk om meerdere netwerken te koppelen aan één en dezelfde captive portal. Hierdoor kunnen gebruikers van dit netwerk op meerdere plekken inloggen met hun eigen credentials.

Als voorbeeld voor een WISPr-omgeving kunt u denken aan een scholengemeenschap die op meerdere locaties vestigingen heeft. Via een WISPr-omgeving kunnen dan bijvoorbeeld de leerlingen op een centrale captive portal inloggen om toegang te krijgen tot het internet. Dit heeft als voordeel dat niet op elke locatie een captive portal opgezet hoeft te worden voor het authentiseren van de leerlingen. Een ander voordeel van WISPr is het gebruik van een centrale authenticatie-server. Dit kan een Active Directory, Radius of LDAP-server zijn. Voor deze technote maken wij gebruik van FreeRadius.

Voor het opzetten van een WISPr-omgeving heeft u een ZoneDirector en op zijn minst één access point nodig. Ook heeft u een server nodig, deze server zal gebruikt worden als webserver en als radiusserver. Dit document beschrijft de configuratie van de ZoneDirector en de installatie en configuratie van Apache en FreeRadius op de server.

De installatie van het besturingssysteem op de betreffende server wordt niet behandeld in deze technote. Om de technote goed te kunnen uitvoeren moet een u de server voorzien van CentOS 6.4 Minimal.

Deze technote is bedoeld als hulpmiddel voor het opzetten van een basis WISPr-omgeving. Deze technote gaat niet in op de beveiliging van de webserver en de radiusserver. Ook wordt het maken van een lay-out voor de captive portal niet behandeld in deze technote. Wel wordt er een basistemplate verstrekt met eenvoudige inlogfunctionaliteit om uw WISPr-omgeving te testen.

Voor het opzetten van een WISPr-omgeving is basiskennis van de ZoneDirector vereist. Zoals het verschil weten tussen de verschillende tabs en waar de verschillende configuratie-opties zich bevinden. Daarnaast is het ook goed om basiskennis van netwerken te hebben voor het inrichten van het WISPr-WLAN. Ook is basiskennis van CentOS 6.4 vereist zoals het navigeren tussen mappen en het aanpassen van bestanden.

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 instructies die in dit document gegeven worden met betrekking tot de ZoneDirector configuratie gaan uit van een Engelstalige web interface. Mocht u de web interface ingesteld hebben op de Nederlandse taal, dan zullen de stappen hetzelfde zijn, maar de benaming van de menu’s zullen verschillen.

De instructies die in dit document gegeven worden zijn op basis van firmware versie 9.6.1.0.15. Mocht u een lagere firmware hebben dan heeft u kans dat sommige functionaliteiten nog niet aanwezig zijn. Wanneer u een hogere firmware versie heeft, dan zullen de stappen nagenoeg hetzelfde zijn.

Het kopiëren van commando regels uit dit document en vervolgens plakken in de terminal van CentOs 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 Commandos.txt” kopiëren. Eventuele commando’s die om gebruikersinvoer vragen kunt u in het tekstbestand al aanpassen naar uw eigen waardes.

2 Installaties

In dit hoofdstuk vindt u alle informatie omtrent de installatie van CentOS 6.4. Daarnaast wordt beschreven hoe u FreeRadius en Apache kunt installeren op CentOS 6.4.

2.1 CentOS 6.4 installatie

CentOS biedt meerdere installatiemogelijkheden aan. Voor deze technote is de CentOS 6.4 Minimal installatie gebruikt. Hieronder vindt u een korte toelichting over de verschillende installaties:

- CentOS Bin DVD: deze installatiemogelijkheid biedt u de optie om tijdens de installatiewizard 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 installeren. Dit is na de installatie wel mogelijk via een software 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 uit te voeren 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: [CentOS 6.4 Download]

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 zijn ingelogd 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.

2.3 Apache installatie

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

```
[root@localhost ~]# yum -y install httpd php php-mysql
```

3 Configuratie

3.1 FreeRadius 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 configuratie te beginnen moet u de MySQL-server eerst starten met het volgende commando:

```
[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 gebruikersaccounts
- Verwijderen van testdatabase

```
[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, vervang <databasenaam> met de eerder aangemaakte database.

```
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 aangegeven dat FreeRadius de database moet gebruiken voor het uitlezen van zijn clients. Het configuratiebestand opent u als volgt:

```
[root@localhost ~]# vi /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
                              poortnummer 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 ~]# vi /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 supportsite. De bestanden hebben de volgende naam:

- default
- inner-tunnel

Deze twee bestanden moet u naar de “root” map 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/default /etc/raddb/sites-enabled/
```

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

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

3.2.3 FreeRadius 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.

3.2.3.1 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.

3.2.3.2 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
```

3.2.3.3 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 3.2.4 "FreeRadius troubleshooting" raadplegen.

De installatie en configuratie van FreeRadius is nu voltooid. Wat u nu nog moet doen met betrekking tot de configuratie van FreeRadius is het inrichten van de FreeRadius-server. In hoofdstuk 4 wordt beschreven hoe u gebruikers en clients (ZoneDirectors) kunt toevoegen aan de MySQL-database. De gebruikers die u toevoegt aan de database kunnen via de WISPr-portal geauthentiseerd worden. Het toevoegen van een client (ZoneDirector) is nodig omdat anders de verzoeken van de betreffende ZoneDirector genegeerd worden door FreeRadius-server. Het toevoegen van gebruikers en ZoneDirectors kan ook op een later moment gedaan worden.

3.2.4 FreeRadius 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
```

3.3 Apache configuratie

3.3.1 Lay-out

Hieronder wordt beschreven hoe u een standaard inlogformulier op uw webserver kunt plaatsen. Via dit inlogformulier kunt u gebruikers authentiseren via het WISPr WLAN. Het inlogformulier is heel basic en heeft geen bijzondere layout. Het betreffende inlog formulier is alleen bedoeld voor het testen van uw WISPr-omgeving.

Uiteindelijk kunt u de lay-out van uw inlogpagina compleet aanpassen naar uw eigen wensen. Het is wel belangrijk dat uw ontwerp te alle tijde een gebruikersnaam en wachtwoord terugstuurt naar de ZoneDirector voor de authenticatie. Dit kan zo ingericht worden dat de gebruikers alleen een button hoeven aan te klikken voor het inloggen. Of dat u om een gebruikersnaam en wachtwoord vraagt die u daarna doorstuurt naar de ZoneDirector.

Het sturen van een gebruikersnaam en wachtwoord naar de ZoneDirector kan gedaan worden via de volgende HTML code:

```
<form method=POST action=”http://<ZD-IP>:9997/login”>
      <input type=”” name=”username”>
      <input type=”” name=”password”>
      <input type=”submit” value=””>
</form>
```

Mocht u vragen hebben over het opzetten van een WISPr-pagina, dan kunt contact opnemen met Alcadis. U kunt eventueel ook nog extra informatie vinden via de volgende URL: [WISPr informatie]

De HTML-code voor het standaard inlogformulier ziet er als volgt uit:

```
<html>
      <head><title>Wireless Internet Service</title></head>
      <body>
            <br/>
            <center>
                  <h2>Wireless Internet Service</h2>
                  <br/>
                  <form method=POST action=”http://<ZD-IP>:9997/login”>
                        Username:<input type=”text” name=”username”>
                        Password:<input type=”password” name=”password”>
                        <input type=”submit” value=”Login”>
                  </form>
            </center>
      </body>
</html>
```

In de map "Files" vindt u een .html bestand genaamd index.html. De map Files vindt u in het gedownloade .zip bestand van de Alcadis support site. Het index.html bestand bevat de standaard HTML-code voor het inlogformulier.

Het index.html bestand kunt u kopiëren naar de "root" map van uw server. Na het kopiëren van het bestand naar de "root" map van de server, kunt u het volgende commando gebruiken om het bestand op de juiste plek te zetten:

```
[root@localhost ~]# cp /root/index.html /var/www/html/
```

Na het uitvoeren van het commando staat het index.html bestand in de webroot van uw webserver. U moet nu alleen nog het IP-adres van uw ZoneDirector in het formulier plaatsen. Het openen van het index.html bestand gaat als volgt:

```
[root@localhost ~]# vi /var/www/html/index.html
```

In het index.html bestand verandert u <ZD-IP> voor uw ZoneDirector IP-adres.

3.3.2 Apache testen

In het vorige hoofdstuk staat beschreven hoe u een basis inlogformulier kunt maken. In dit hoofdstuk wordt beschreven hoe u de Apache webserver kunt starten en kunt controleren of het index.html bestand goed wordt weergegeven.

U kunt de Apache webserver starten via het volgende commando:

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

Na het starten van de Apache webserver en het aanpassen van de iptables (Hoofdstuk 5), kunt u een webbrowser openen en navigeren naar het IP-adres van uw Apache webserver. U krijgt nu het standaard inlogformulier te zien van uw WISPr-omgeving.

Figuur 1: Standaard inlogformulier

Het opzetten van de lay-out en het starten van de webserver is nu voltooid. Wat u nu nog moet doen is het aanpassen van de iptables zoals beschreven staat in hoofdstuk 5. En het aanmaken van een WISPr-WLAN in de ZoneDirector. Het aanmaken van een WISPr-WLAN staat beschreven in hoofdstuk 7. Na het aanmaken kunt u gaan testen of u kunt inloggen via uw WISPr-portal. De gebruiker waarmee u inlogt, moet wel bekend zijn in de MySQL-database. Voor het aanmaken van gebruikers kunt u hoofdstuk 4 raadplegen.

3.3.3 Apache troubleshooting

Zodra de Apache webserver gestart is houdt deze verschillende logs bij. De logs kunt u vinden op de volgende locatie:

```
[root@localhost ~]# cd /var/log/httpd/
```

Mocht u tegen problemen aanlopen tijdens het laden van het inlogformulier dan kunt u deze logbestanden raadplegen. Het weergeven van het error logbestand gaat als volgt:

```
[root@localhost ~]# cat /var/log/httpd/error_log
```

Het weergeven van het access logbestand gaat als volgt:

```
[root@localhost ~]# cat /var/log/httpd/access_log
```

Tijdens het starten van de Apache webserver wordt automatisch het configuratie bestand van Apache gecontroleerd. Mochten hier fouten in zitten dan krijgt u deze direct te zien tijdens het starten. Het configuratie bestand van Apache kunt u als volgt openen:

```
[root@localhost ~]# vi /etc/httpd/conf/httpd.conf
```

4 Gebruikers & ZoneDirectors

In de onderstaande hoofdstukken wordt beschreven hoe u gebruikers en clients (ZoneDirectors) kunt toevoegen aan de MySQL-server.

4.1 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
```

4.2 Gebruikers (.csv)

Gebruikers kunnen geïmporteerd worden via een .csv bestand. Het .csv bestand kunt u vinden in de map "Files". De map Files vindt u in het gedownloade .zip bestand van de Alcadis support site. Het bestand heeft de volgende naam:

- Gebruiker_Sjabloon.csv - Bedoeld voor het aanmaken van gebruikers.

Het bestand is te openen met Excel waarmee de inhoud aangepast kan worden. Als u het bestand heeft aangepast moet u het bestand naar de "root" map van de server kopiëren.

Na het kopiëren van het bestand naar de "root" map van de server, kunt u het volgende commando gebruiken om het bestand op de juiste plek te zetten:

```
[root@localhost ~]# cp /root/Gebruiker_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
```

4.3 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
```

5 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 Apache geblokkeerd. Het configuratiebestand opent u als volgt:

```
[root@localhost ~]# vi /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
-A INPUT -p udp --dport 1813 -j ACCEPT
#Apache
-A INPUT -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 443 -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 Apache.

```
*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 -p udp --dport 1813 -j ACCEPT
#Apache
-A INPUT -p tcp --dport 80 -j ACCEPT
-A INPUT -p tcp --dport 443 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

6 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 moeten later aangepast worden 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 gebruikmaken 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>;
```

Dit geldt ook als u gebruikers wilt importeren via een .csv bestand. U moet het .csv bestand naar de directory kopiëren van de betreffende database. Anders gaat het importeren van gebruikers fout.

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

7 ZoneDirector configuratie

In de onderstaande hoofdstukken wordt beschreven hoe u een authenticatieserver, een Hotspot (WISPr) profiel en een WLAN kunt aanmaken op de ZoneDirector.

7.1 Authenticatieserver

Hieronder wordt beschreven hoe u een authenticatiserver 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. Voor het aanmaken van een authenticatieserver navigeert u naar **Configure -> AAA Servers**. Op deze pagina vindt u twee categorieën.

- Authentication/Accounting Servers
- Test Authentication Settings

Om een nieuwe authenticatieserver aan te maken klikt u in de categorie **Authentication/Accounting Servers** op **Create New**.

In het veld **Name** geeft u de naam op voor de betreffende authenticatieserver.

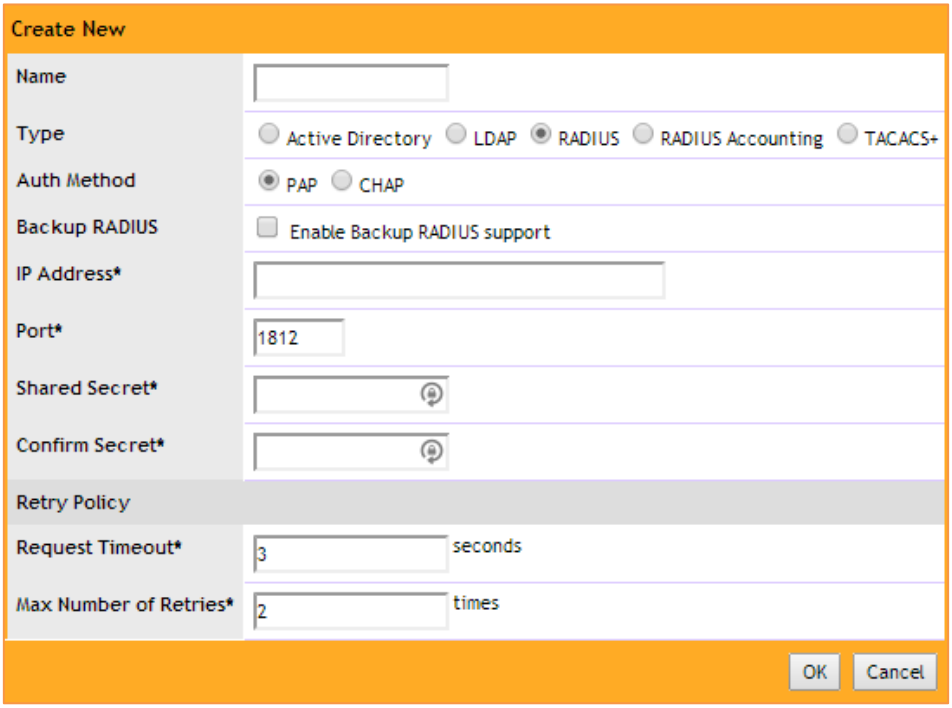
Bij **Type** selecteert u **RADIUS**.

In het veld **IP Address** geeft u het IP-adres op van betreffende FreeRadius-server.

Het veld **Port** kunt u op **1812** laten staan, tenzij u een andere poort heeft gespecificeerd op uw FreeRadius-server.

In het veld **Shared Secret** vult u het betreffende wachtwoord in voor de ZoneDirector die u heeft aangemaakt als "Client" in de MySQL-database.

In het veld **Confirm Secret** vult u nogmaals het wachtwoord in voor de ZoneDirector die u heeft aangemaakt als "Client" in de MySQL-database.



Figuur 2: Create New AAA server

7.2 WISPr-profiel

Hieronder wordt beschreven hoe u een Hotspot (WISPr) profiel moet aanmaken op de ZoneDirector. Voor het aanmaken van een Hotspot (WISPr) profiel navigeert u naar **Configure -> Hotspot Services**. Op deze pagina vindt u één categorieën.

- Hotspot Services

Om een nieuwe authenticatieserver aan te maken klikt u in de categorie **Hotspot Services** op **Create New**.

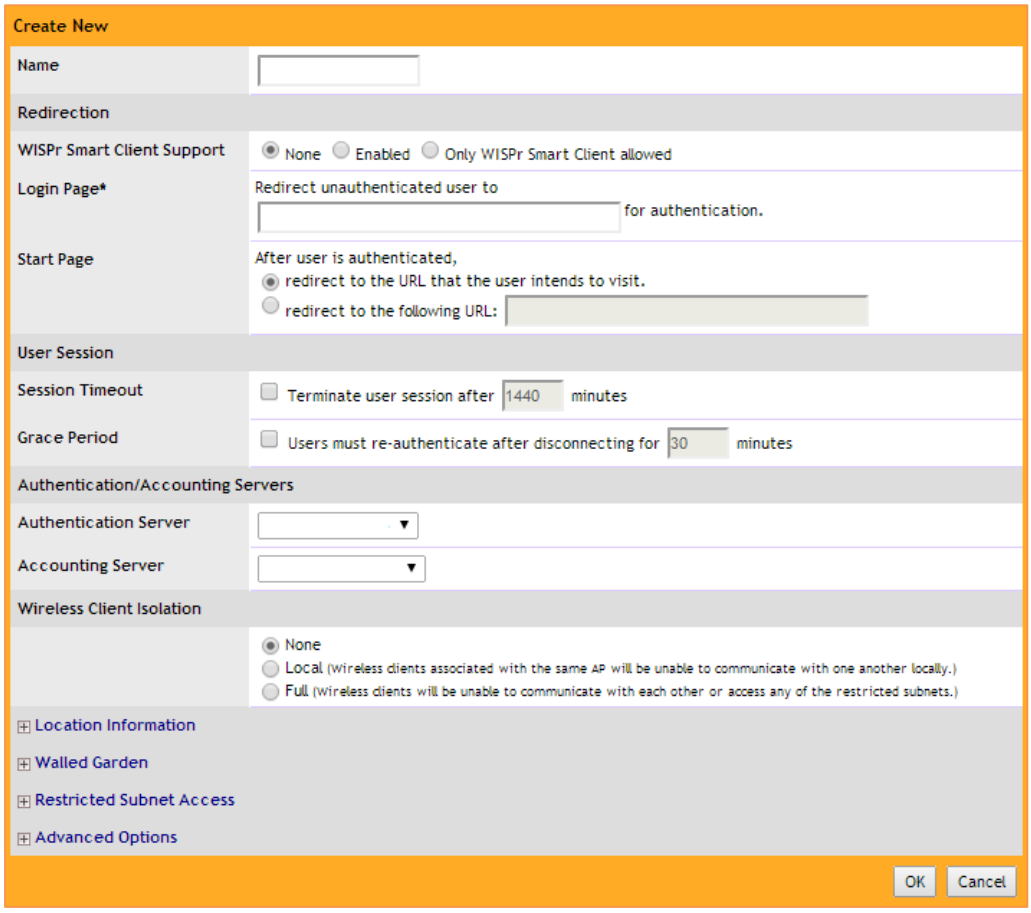
In het veld **Name** geeft u de naam op voor het betreffende WISPr-profiel.

In het veld **Login Page** geeft u het IP-adres op van uw webserver waar de WISPr-portal op draait.

Start Page geeft u de optie om gebruikers te redirecten of om gebruiker door te sturen naar de pagina die zij wilde bezoeken.

Bij **Authentication Server** selecteert u de eerder aangemaakte FreeRadius-server.

De bovenstaande instellingen zijn de basisinstellingen voor een WISPr-profiel. Alle andere instellingen zijn aanvullende instellingen voor het WISPr-profiel, deze zijn niet verplicht.



Figuur 3: Create New Hotspot

7.3 WISPr WLAN

In de bovenstaande hoofdstuken hebben wij uitgelegd hoe u een AAA server en een WISPr-profiel kunt aanmaken. In dit hoofdstuk beschrijven wij hoe u een WLAN kunt aanmaken dat gebruik maakt van het WISPr-profiel. Om een WLAN aan te maken navigeert u naar **Configure -> WLANs**.

Op deze pagina klikt u in de categorie WLANs op **Create New**. Er zal een scherm openklappen voor het aanmaken van een nieuw WLAN.

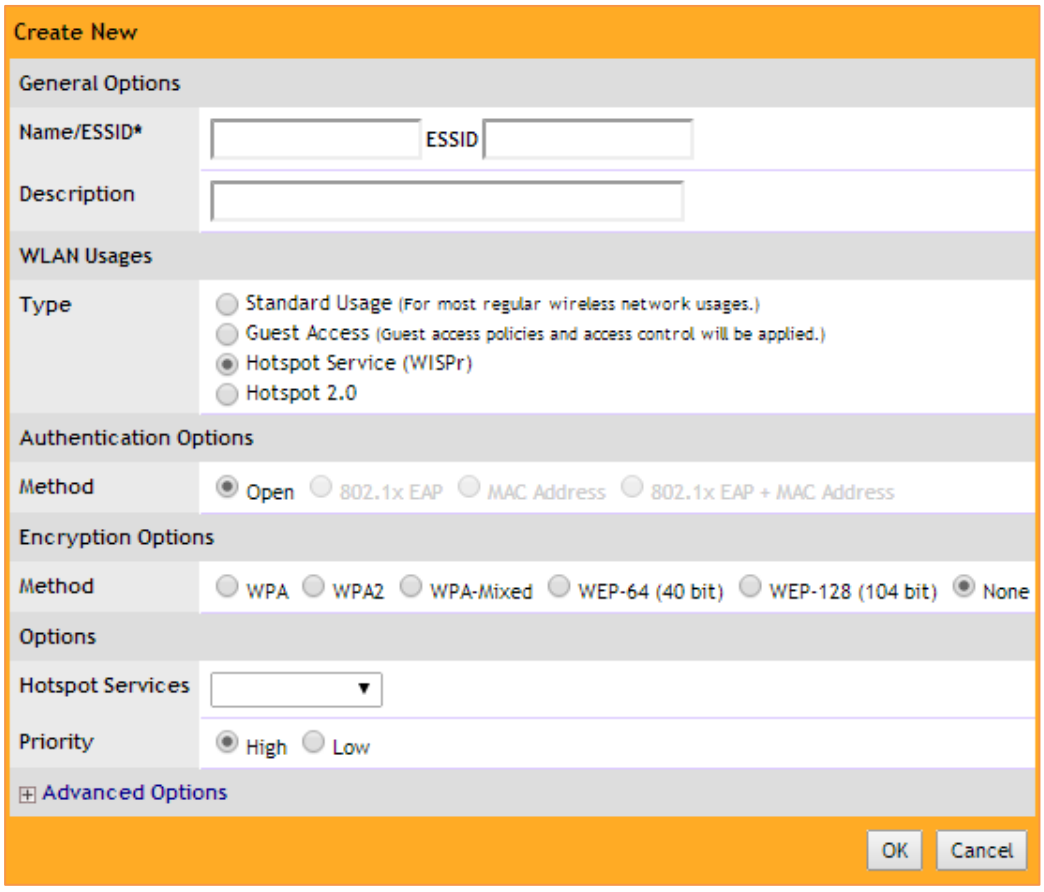
In de velden **Name** en **ESSID** geeft u de naam op van uw WISPr-netwerk. De naam die u invult in het veld **ESSID** zal de naam zijn die zichtbaar is voor uw gebruikers.

In het veld **Description** kunt u een omschrijving invullen van het betreffende WLAN. Het invullen van een omschrijving is niet verplicht.

Bij **Type** selecteert u **Hotspot Service (WISPr)**.

Onder **Options Hostpot Services** selecteert u het WISPr-profiel dat u eerder heeft aangemaakt.

De basisinstellingen voor het WISPr-WLAN zijn nu gedaan, eventueel kunt u nog onder **Advanced Options** extra instellingen doen voor het WISPr-WLAN. Onder advanced options kunt u bijvoorbeeld een bandbreedte beperking activeren. Ook heeft u de mogelijkheid om onder de advanced options het WISPr-WLAN in een apart VLAN te laten opereren.



Figuur 4: Create New WLAN