Configuring an EasyServer II for use with a RADIUS server

Keywords: EasyServer II RADIUS authentication accounting dialin remote access

Introduction

The purpose of this application note is to outline the configuration options that are available when using a RADIUS server for user authentication with an EasyServer II. A number of different configurations are discussed including simple terminal user login authentication and PPP dialin client authentication.

The examples in this application note are developed using an EasyServer II with the RADIUS option enabled and the Merit RADIUS server software running on a SlackWare Linux system. The Merit RADIUS software is available from the Internet at merit.edu. The version of Merit RADIUS software used in developing these examples is 2.4.23C. Although these examples have been developed using the Merit RADIUS software, the principles of operation will be the same regardless of which RADIUS server is used. Some of the configuration details will differ amongst RADIUS server implementations.

The Merit RADIUS server software is by no means the only RADIUS server software available, nor is it the only RADIUS server software that has been tested with the EasyServer II. Other versions of RADIUS server software tested include the Funk Software Steel Belted RADIUS software for Windows NT and the Livingston RADIUS server.

Requirements

There are only two requirements for installing and configuring RADIUS. Firstly, an EasyServer II with the RADIUS feature enabled and secondly a system on which the RADIUS server software is to be installed. The RADIUS feature is not enabled by default on the EasyServer II and a RADIUS key must be purchased from Stallion Technologies.

Note that the RADIUS feature is only available in those units with Rev 6.0.0 or later firmware. The revision of EasyServer II firmware can be checked using the IDENTIFICATION command.

Figure 1

```
Local 10>> identification

ESII-8  Communications Server V6.0.0  251535-01 revision 0

Local 10>>
```

Configuration

RADIUS Server Configuration

There are three steps to configuring the Merit RADIUS software after it is installed. This Application Note does not go into the details of installing the Merit RADIUS software. This information is available in the documentation that comes with the software. The three steps are:

- creating the *authfile* file which determines the particular authentication mechanism to be used, e.g. Unix password style authentication, Kerberos, TACAS, etc.
- creating the *clients* file which specifies which RADIUS clients are going to be using this RADIUS server and the “secret” that they will be using.
- creating the *users* file that contains information about the individual users and their environment.

In the examples outlined in this Application Note, the *authfile* file appears as follows. The entries in this file indicate that the default authentication mechanism is the Unix password method as opposed to Kerberos, TACAS or another form of authentication.

```
#     The following entry will typically be configured in the authfile for
#     the RADIUS server running on the system with the matching DNS name.
#     It says to use the UNIX password file for authentication.
domain.name.com   UNIX-PW
#     This entry says to pass requests with authentication realm names
#     which didn't appear in this file along to another RADIUS server.
DEFAULT           UNIX-PW
#     This next entry says to handle requests which don't have a realm
#     name appended to the user id as local user ids.
NULL              UNIX-PW
```

The client file appears as follows:

```
# Client Name           Key               user/authfile prefix
# ----------------      ---------------   --------------------

easyserver              secret
```

This file indicates that RADIUS authentication requests can be expected from a client called “easyserver”. As DNS is running on this system, the client name can be used. If DNS was not available, then the IP address of the client would be required. In this example the encryption key or secret used is “secret”. This must, of course, be the same secret as that used on the EasyServer II.

The third file that is created is the *users* file. This file contains information about the users who will be using the EasyServer II and therefore must be authenticated via the RADIUS server. Details of the *users* file entries will be given below, along with the corresponding EasyServer II port configuration.

Basic EasyServer II Configuration

The SHOW SERVER command can be used to determine whether or not the RADIUS feature has been enabled. As can be seen from the output of the command (see Figure 2), the RADIUS optional feature has been enabled. The Dial on Demand feature is enabled by default.

Once the RADIUS feature has been enabled, changes can be made to the EasyServer II to enable RADIUS operation. Whilst initial configuration and testing of the EasyServer II is being performed, the fallback option should be enabled. Once configuration and testing is complete, the fallback option can then be disabled.

To configure the EasyServer II for RADIUS, the following commands need to be executed.

Figure 2

```
Local 10>> show server

ESII-8  Communications Server V6.0.0        Uptime:  20 days 22:17:09

Ethernet:       00-60-1f-00-1a-1f           Internet: 192.168.1.24
Name:           ESII_00601F001A1F           Number:          0

Identification:     None

Console Port:              1        Prompt:          "%N %p>%P "
Inactivity Timer:          30       Password limit:            3
Monitor Timer:             3        Session limit:            64

Startup File:                               ESII-8.CFG
Flash Memory File:                          None

Enabled Optional Features:
  RADIUS Authentication,  Dial On Demand

Enabled Characteristics:
  Broadcast,  Lock,  Heartbeat

Local 10>>
```

```
change radius authentication server 192.168.1.16 port 1812
change radius accounting server 192.168.1.16 port 1813
change radius support enabled
change radius secret "secret"
change radius fallback enabled
```

Figure 3

```
Local 10>> show radius

Radius: Enabled          Fallback: Enabled          Secret: secret
Timeout:        5s               Retry count:       4

Authentication Server    Port    Accounting Server          Port

192.168.1.16             1812    192.168.1.16               1813

Port   Radius

  1    Disabled
  2    Enabled
  3    Enabled
  4    Enabled
  5    Enabled
  6    Enabled
  7    Enabled
  8    Disabled

Local 10>>
```

By default, the EasyServer II uses UDP ports 1812 and 1813, as per RFCs 2138 and 2139, for RADIUS authentication and accounting, rather than ports 1645 and 1646 as used by older RADIUS implementations. It may be necessary to change either the EasyServer II or the RADIUS server software so that the same UDP ports are used by both RADIUS client and server.

RADIUS also has to be enabled for each port. For example, the command to enable RADIUS on ports 2 to 7 only, would be as follows.

```
change port 2-7 radius enabled
```

After RADIUS has been configured for all the required ports of the EasyServer II, the configuration can be verified using the SHOW RADIUS command. The output will appear similar to that displayed in Figure 3.

Creating the Users file

A RADIUS authentication scheme is usually used where there are dial in clients, connecting from outside of the organization, as with an Internet Service Provider (ISP), for example. This is not the only situation where RADIUS might be used. RADIUS can also be used to authenticate terminal users. The entries in the *users* file will relate to the type of user that is being authenticated.

The entry in the *users* file for the system administrator, who may just be using a terminal or telnet session, would appear as follows.

```
admin       Password = admin
            Service-Type = Administrative-User
```

As the password is specified in the *users* file, the default authentication mechanism of Unix-password is not used. If the user being authenticated has an account on the Unix system where the RADIUS server is running, then the user can be authenticated using their Unix password. The *users* entry would appear as follows.

```
username    Authentication-Type = Unix-PW
            Service-Type = Authenticate-Only,
```

For a dedicated, dialin modem PPP connection, the *users* entry would be similar to the next example. This applies to a dedicated PPP connection only. The PPP configuration in the EasyServer II should be configured to use either PAP or CHAP as well. In this example, PAP user authentication is used.

```
pppuser Authentication-Type = Unix-PW
       Service-Type = Framed,
       Framed-Protocol = PPP,
       Framed-IP-Netmask = 255.255.255.0,
       Framed-Routing = None,
       Framed-MTU = 1500
```

The corresponding EasyServer II port configuration would appear as detailed in Figure 4. In this case the user *pppuser* has a Unix user account and is being authenticated using the Unix-PW mechanism. Also, the local and host IP addresses being used, are those configured on the EasyServer II port.

Figure 4

```
DEFINE PORT 4 Autobaud DISABLED
DEFINE PORT 4 Modem Control ENABLED
DEFINE PORT 4 PPP ENABLED
DEFINE PORT 4 Radius ENABLED
DEFINE PORT 4 SPEED 115200
DEFINE PORT 4 STOP BITS 1 FLOW CONTROL CTS
DEFINE PORT 4 PPP COMPRESS ENABLED
DEFINE PORT 4 PPP LOCAL ADDRESS 192.168.1.24
DEFINE PORT 4 PPP HOST ADDRESS 192.168.1.122
DEFINE PORT 4 PPP SUBNET MASK 255.255.255.0
DEFINE PORT 4 PPP PAP USER
DEFINE PORT 4 DEDICATED PPP
```

If it is necessary for some particular reason to associate a particular IP address with a specific user, an IP address can be configured in the *users* file. Any IP addresses configured in the *users* file will then override the host IP address configured on the EasyServer II port.

```
pppuser      Authentication-Type = Unix-PW
             Service-Type = Framed,
             Framed-Protocol = PPP,
             Framed-IP-Address = 192.168.50.2,
             Framed-IP-Netmask = 255.255.255.0,
             Framed-Routing = None,
             Framed-MTU = 1500,
             Framed-Compression = Van-Jacobson-TCP-IP
```

Figure 5

In the output of the

SHOW PORT 4 PPP

command, we can see that the originally configured IP address of 192.168.1.122, as used in the previous example, has now been overridden by the user specific IP address of 192.168.50.2

```
Local 10>> show port 4 ppp

Port  4:          PORT_04          Name:                    PORT_04

Status:           Connected        LCP:open                 IPCP:open
Local Addr:       192.168.1.24     MTU:                     1500
Remote Addr:      192.168.50.2     Compress:                Enabled
Subnet Mask:      255.255.255.0    Character Map:           FFFFFFFF
PAP Security:     User             CHAP Security:           Disabled
CHAP Retry:       0                CHAP Rechallenge Time:   0

Local 10>>
```

For a more generalized dial in user configuration, where the user may or may not be using PPP, the EasyServer II port configuration may appear as follows. The *users* file will not change.

Figure 6

There are three significant changes in the configuration of this port as opposed to port 4 in the previous example.

1) The Login Account characteristic has been enabled
2) The PAP user authentication characteristic has been disabled
3) The port is no longer dedicated to PPP operation

```
DEFINE PORT 5 Autobaud DISABLED
DEFINE PORT 5 Login Account ENABLED
DEFINE PORT 5 Modem Control ENABLED
DEFINE PORT 5 PPP ENABLED
DEFINE PORT 5 Radius ENABLED
DEFINE PORT 5 SPEED 115200
DEFINE PORT 5 STOP BITS 1 FLOW CONTROL CTS
DEFINE PORT 5 PPP COMPRESS ENABLED
DEFINE PORT 5 PPP LOCAL ADDRESS 192.168.1.24
DEFINE PORT 5 PPP HOST ADDRESS 192.168.1.123
DEFINE PORT 5 PPP SUBNET MASK 255.255.255.0
```

When the incoming user connects to the EasyServer II, they will be presented with a username prompt, followed by a password prompt. This username and password prompt will then be authenticated by RADIUS in the usual way. After the authentication phase has been completed, the Service-Type associated with the

user will then commence. This may be a Framed-Protocol, such as PPP, the Administrative-User service, or any other allowable service. No changes to the *users* file examples given above are required for this feature to work, only changes to the EasyServer II configuration.

Conclusions

The RADIUS feature of the EasyServer II, in conjunction with a RADIUS server, provides a very flexible and secure mechanism for authenticating users and providing them with standard user connection profiles. These features are particularly appropriate in situations that involve a large number of dialin users, e.g. an ISP.

This article does not touch on the user accounting features that are available with RADIUS. That will be the subject of a separate Application Note.