

配置 Livingston 服务器的 RADIUS

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[身份验证](#)

[增加记账功能](#)

[测试文件](#)

[相关信息](#)

简介

本文档旨在帮助首次RADIUS用户设置和调试Livingston RADIUS服务器的RADIUS配置。它并非对Cisco IOS® RADIUS功能的详尽描述。Livingston文档可从Lucent Technologies网站获取。

无论使用什么服务器，路由器配置都是相同的。思科以课程NA、课程UNIX或Cisco Access Registrar提供商业可用的RADIUS代码。

此路由器配置是在运行Cisco IOS软件版本11.3.3的路由器上开发的；版本12.0.5.T及更高版本使用组radius而不是radius，因此aaa authentication login default radius enable等语句显示为aaa authentication login default group radius enable。

有关RADIUS路由器[命令的](#)详细信息，请参阅Cisco IOS文档中的RADIUS信息。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

规则

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

身份验证

请完成以下步骤：

1. 确保在UNIX服务器上编译了RADIUS代码。服务器配置假设您使用Livingston RADIUS服务器代码。路由器配置需要与其他服务器代码配合使用，但服务器配置不同。代码radiusd必须以root身份运行。
2. Livingston RADIUS代码附带三个要为系统定制的示例文件：clients.example、users.example和dictionary。这些都通常在raddb目录中找到。您可以修改这些文件或本文档末尾的用户和客户端文件。所有三个文件都需要放在工作目录中。测试以确保RADIUS服务器以三个文件启动：

```
radiusd -x -d (directory_containing_3_files)
```

启动错误需要打印到屏幕或directory_containing_3_files_logfile。检查以确保从另一个服务器窗口启动RADIUS:

```
ps -aux | grep radiusd  
(or ps -ef | grep radiusd)
```

您看到两个放射性进程。

3. 终止RADIUS进程：

```
kill -9 highest_radiusd_pid
```

4. 在路由器控制台端口上，开始配置RADIUS。在命令集前输入 enable mode 和 **configure terminal**。此语法可确保在RADIUS不在服务器上运行的情况下，您最初不会被锁定在路由器之外：

```
!--- Turn on RADIUS aaa new-model enable password whatever !--- These are lists of authentication methods, !--- that is, "linmethod", "vtymethod", "conmethod" are !--- names of lists, and the methods listed on the same !--- lines are the methods in the order to be tried. As !--- used here, if authentication fails due to the radiusd !--- not being started, the enable password will be !--- accepted because it is in each list. aaa authentication login default radius enable aaa authentication login linmethod radius enable aaa authentication login vtymethod radius enable aaa authentication login conmethod radius enable !--- Point the router to the server, that is, !--- #.#.#.# is the server IP address. radius-server host #.#.#.# !--- Enter a key for handshaking !--- with the RADIUS server: radius-server key cisco line con 0 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication conmethod line 1 8 login authentication linmethod modem InOut transport input all rxspeed 38400 txspeed 38400 password whatever flowcontrol hardware line vty 0 4 password whatever !--- No time-out to prevent being !--- locked out during debugging. exec-timeout 0 0 login authentication vtymethod
```

5. 在检查时，请通过控制台端口保持登录到路由器，以确保您仍可以通过Telnet访问路由器，然后再继续。由于radiusd未运行，因此需要使用任何用户ID接受使能密码。**注意：**保持控制台端口会话处于活动状态并保持启用模式。确保此会话不超时。在更改配置时，请勿将自己锁定。发出以下命令，以查看路由器上服务器与路由器之间的交互：

```
terminal monitor  
debug aaa authentication
```

6. 作为根用户，在服务器上启动RADIUS:

```
radiusd -x -d (directory_containing_3_files)
```

启动错误会打印到屏幕或directory_containing_3_files_logfile。检查以确保RADIUS从另一个服务器窗口启动：

```
Ps -aux | grep radiusd  
(or Ps -ef | grep radiusd)
```

您需要看到两个放射性进程。

7. Telnet(vty)用户现在必须通过RADIUS进行身份验证。在路由器和服务器上执行调试 (步骤5和6) 后，从网络的另一部分Telnet至路由器。路由器会生成您回复的用户名和密码提示：

```
ciscour (username from users file)
```

```
ciscopas (password from users file)
```

观察需要查看RADIUS交互的服务器和路由器，例如，在何处发送什么、响应和请求等。在您继续前，请更正所有问题。

8. 如果您还希望用户通过RADIUS进行身份验证以进入启用模式，请确保您的控制台端口会话仍处于活动状态并将此命令添加到路由器。

```
!--- For enable mode, list "default" looks to RADIUS !--- then enable password if RADIUS not running. aaa authentication enable default radius enable
```

9. 用户现在需要通过RADIUS启用。在路由器和服务器上执行调试（步骤5和6）后，从网络的另一部分Telnet至路由器。路由器需要生成您回复的用户名和密码提示：

```
ciscoursr (username from users file)
ciscopas (password from users file)
```

当您进入启用模式时，路由器会发送用户名\$enable15\$并请求密码，您会回复：

```
shared
```

观察需要查看RADIUS交互的服务器和路由器，例如，在何处发送什么、响应和请求等。在您继续前，请更正所有问题。

10. 通过建立到路由器的Telnet会话，检查控制台端口用户通过RADIUS的身份验证，该会话需要通过RADIUS进行身份验证。保持Telnetted到路由器并处于启用模式，直到您确定可以通过控制台端口登录路由器，通过控制台端口注销到路由器的原始连接，然后重新连接到控制台端口。通过使用步骤9中的用户ID和密码登录和启用的控制台端口身份验证现在需要通过RADIUS。
11. 当您通过Telnet会话或控制台端口保持连接，并在路由器和服务器上进行调试时，步骤5和6建立与线路1的调制解调器连接。线路用户现在需要登录并通过RADIUS启用。路由器需要生成您回复的用户名和密码提示：

```
ciscoursr (username from users file)
ciscopas (password from users file)
```

当您进入启用模式时，路由器会发送用户名\$enable15\$并请求密码，您会回复：

```
shared
```

观察需要查看RADIUS交互的服务器和路由器，例如，在何处发送什么、响应和请求等。在您继续前，请更正所有问题。

增加记账功能

添加记帐是可选的。

1. 除非在路由器中配置，否则不会进行记账。在路由器中启用记帐，如以下示例所示：

```
aaa accounting exec default start-stop radius
aaa accounting connection default start-stop radius
aaa accounting network default start-stop radius
aaa accounting system default start-stop radius
```

2. 使用记帐选项在服务器上启动RADIUS:

Start RADIUS on the server with the accounting option:

3. 要查看路由器上服务器与路由器之间的交互，请执行以下操作：

```
terminal monitor
debug aaa accounting
```

4. 通过调试观察服务器与路由器的交互过程，访问路由器，然后检查日志文件的记帐目录。

测试文件

以下是用户测试文件：

```
ciscousr      Password = "ciscopas"  
              User-Service-Type = Login-User,  
              Login-Host = 1.2.3.4,  
              Login-Service = Telnet  
  
$enable15$    Password = "shared"  
              User-Service-Type = Shell-User
```

以下是客户端测试文件：

```
# 1.2.3.4 is the ip address of the client router and cisco is the key  
1.2.3.4      cisco
```

[相关信息](#)

- [远程用户拨入认证系统\(RADIUS\)](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)