Cisco IOS 路由器：本地、HTTP连接配置示例的TACACS+和RADIUS认证

目录

简介

本文档显示如何配置 HTTP 连接的本地、TACACS+ 和 RADIUS 验证。此外，还提供了一些相关的调试命令。

开始使用前

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

先决条件

本文档没有任何特定的前提条件。

使用的组件

本文档中的信息基于以下软件和硬件版本。

- Cisco IOS软件版本11.2或以上
- 支持这些软件版本的硬件

本文档中的信息都是基于特定实验室环境中的设备创建的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您是在真实网络上操作，请确保您在使用任何命令前已经了解其潜在影响。

背景理论

在 Cisco IOS® 软件版本 11.2 中，添加了通过 HTTP 管理路由器的功能。Cisco IOS配置基本原则命令参考的"Cisco IOS Web 浏览器命令"部分包括有关此功能的下列信息。

“**ip http authentication** 命令允许您为 HTTP 服务器用户指定特定的验证方法。HTTP 服务器使用启用口令方法验证权限级别为 15 的用户。现在，您可使用 **ip http authentication** 命令指定启用、本地、TACACS 或身份验证、授权和记帐 (AAA) HTTP 服务器用户验证。”

配置

本部分提供有关如何配置本文档所述功能的信息。

本文档使用如下所示的配置。

- 为 HTTP 服务器用户配置本地认证
- 为 HTTP 服务器用户配置 TACACS+ 认证
- 为 HTTP 服务器用户配置 RADIUS 验证

注意： 要查找本文档所用命令的其他信息，请使用命令查找工具（仅限注册用户）。

为 HTTP 服务器用户配置本地认证

- 路由器配置
- 用户结果

路由器配置

使用 Cisco IOS 软件版本 11.2 进行本地身份验证

```
!--- This is the part of the configuration related to
local authentication. ! aaa new-model aaa authentication
login default local aaa authorization exec local
username one privilege 15 password one username three
password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

使用 Cisco IOS 软件版本 11.3.3.T 或更高版本进行本地身份验证

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

用户结果

这些结果适用于使用之前路由器配置的用户。

- **User One**如果输入的 URL 为 http://#.#.#.#.通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于启用模式（**show privilege** 将为 15）。如果命令授权添加到路由器中，用户将在所有命令中成功。
- **User Three**由于没有权限级别，用户将无法通过 web 授权。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于非启用模式（**show privilege** 将为 1）。如果命令授权添加到路由器中，用户将在所有命令中成功。
- **User Four**如果输入的 URL 为 http://#.#.#.#/level/7/exec，则用户将通过 web 授权。此时将显示级别 1 命令以及级别 7 clear line 命令。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于权限级别 7（**show privilege** 将为 7）。如果命令授权添加到路由器中，用户将在所有命令中成功。

为 HTTP 服务器用户配置 TACACS+ 认证

路由器配置

使用 Cisco IOS 软件版本 11.2 进行身份验证

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

使用 Cisco IOS 软件版本 11.3.3.T 至 12.0.5.T 进行身份验证

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

使用 Cisco IOS 软件版本 12.0.5.T 及更高版本进行身份验证

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
```

```
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

用户结果

以下结果适用于使用以下服务器配置的用户。

- **User One**如果输入的 URL 为 http://#.#.#.#.通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于启用模式（**show privilege** 将为 15）。如果命令授权添加到路由器中，用户将在所有命令中成功。
- **User Two**如果输入的 URL 为 http://#.#.#.#.通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于启用模式（**show privilege** 将为 15）。如果在该路由器上添加命令授权，用户将会使所有命令出现故障，因为服务器配置不核准。
- **User Three**由于没有权限级别，用户将无法通过 web 授权。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于非启用模式（**show privilege** 将为 1）。如果命令授权添加到路由器中，用户将在所有命令中成功。
- **User Four**如果输入的 URL 为 http://#.#.#.#/level/7/exec，则用户将通过 web 授权。此时将显示级别 1 命令以及级别 7 clear line 命令。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于权限级别 7（**show privilege** 将为 7）。如果命令授权添加到路由器中，用户将在所有命令中成功。

免费软件后台程序服务器配置

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

用于 UNIX 服务器配置的 Cisco Secure ACS

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

[用于 Windows 服务器配置的 Cisco Secure ACS]

User One in Group One

- 组设置选中 **shell (exec)**。选中 **privilege level=15**。选中 **Default (Undefined) Services**。**注意**：如果此选项没出现，请到接口配置中，选择TACACS+以及高级配置选项。选择 **Display enable default (undefined) service** 配置。
- 用户设置来自任意数据库的口令；输入口令并在顶部区域中确认。

User Two in Group Two

- 组设置选中 **shell (exec)**。选中 **privilege level=15**。请勿选中 **Default (Undefined) Services**。
- 用户设置来自任意数据库的口令；输入口令并在顶部区域中确认。

User Three in Group Three

- 组设置选中 **shell (exec)**。将 **privilege level** 留空。选中 **Default (Undefined) Services**。**注意**：如果此选项没出现，请到接口配置中，选择TACACS+以及高级配置选项。选择 **Display enable default (undefined) service** 配置。

- 用户设置来自任意数据库的口令；输入口令并在顶部区域中确认。

User Four in Group Four

- 组设置选中 **shell (exec)**。选中 **privilege level=7**。选中 **Default (Undefined) Services**。**注意**：如果此选项没出现，请到接口配置中，选择TACACS+以及高级配置选项。选择 **Display enable default (undefined) service** 配置。
- 用户设置来自任意数据库的口令；输入口令并在顶部区域中确认。

为 HTTP 服务器用户配置 RADIUS 验证

- 路由器配置
- 用户结果
- 支持 Cisco AV 对的服务器上的 RADIUS 配置
- 用于 UNIX 服务器配置的 Cisco Secure ACS
- 用于 Windows 服务器配置的 Cisco Secure ACS

路由器配置

使用 Cisco IOS 软件版本 11.2 进行身份验证

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

使用 Cisco IOS 软件版本 11.3.3.T 至 12.0.5.T 进行身份验证

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

使用 Cisco IOS 软件版本 12.0.5.T 及更高版本进行身份验证

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

用户结果

以下结果适用于使用以下服务器配置的用户。

- **User One**如果输入的 URL 为 http://#.#.#.#.通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于启用模式（**show privilege** 将为 15）。
- **User Three**由于没有权限级别，用户将无法通过 web 授权。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于非启用模式（**show privilege** 将为 1）。
- **User Four**如果输入的 URL 为 http://#.#.#.#/level/7/exec，则用户将通过 web 授权。此时将显示级别 1 命令以及级别 7 clear line 命令。通过 Telnet 连接到路由器之后，用户可在登录身份验证之后执行所有命令。登录之后，用户将处于权限级别 7（**show privilege** 将为 7）。

支持 Cisco AV 对的服务器上的 RADIUS 配置

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

用于 UNIX 服务器配置的 Cisco Secure ACS

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
```

```
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

用于 Windows 服务器配置的 Cisco Secure ACS

- 用户 = one，服务类型（属性 6）= administrative
- 用户 = three，服务类型（属性 6）= login
- 用户 = four，服务类型（属性 6）= login，选中 Cisco AV 对框并输入 shell:priv-lvl=7

验证

当前没有可用于此配置的验证过程。

故障排除

本部分提供的信息可用于对配置进行故障排除。

故障排除命令

以下命令对于调试 HTTP 身份验证十分有用。这些命令在路由器上发出。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

- **terminal monitor** - 显示当前终端和会话的 **debug** 命令输出和系统错误消息。
- **debug aaa authentication** - 显示 AAA/TACACS+ 身份验证的信息。
- **debug aaa authorization** -显示关于AAA/TACACS+特权的信息。
- **debug radius** - 显示与 RADIUS 相关的调试详细信息。
- **debug tacacs** - 显示与 TACACS 相关的信息。
- **debug ip http authentication** - 使用此命令对 HTTP 身份验证问题进行故障排除。显示路由器尝试的身份验证方法和身份验证特定的状态消息。

相关信息

- Cisco TACACS+ Access 软件支持页
- RADIUS 支持页
- Cisco Secure ACS for Windows 支持页
- Cisco Secure ACS for UNIX 支持页
- 请求注解 (RFC)
- 技术支持和文档 - Cisco Systems