目录

简介

本文档介绍如何通过在 UNIX 上运行的 TACACS+ 配置 Cisco 路由器进行认证。TACACS+ 提供的功能没有商用 Cisco Secure ACS for Windows 或 Cisco Secure ACS UNIX 提供的多。

Cisco Systems 以前提供的 TACACS+ 软件已停产并且不再受 Cisco Systems 支持。

今天，当您在您最喜爱的 Internet 搜索引擎上搜索“TACACS+ 免费软件”时，您可以找到许多可用的 TACACS+ 免费软件版本。Cisco 并不具体推荐任何特定的 TACACS+ 免费软件版本实施。

Cisco 安全访问控制服务器 (ACS) 可通过世界范围内的常规 Cisco 销售和分销渠道购买。Cisco Secure ACS for Windows 包括在 Microsoft Windows 工作站实施独立安装所需的全部必要组件。Cisco Secure ACS 解决方案引擎随附有预先安装的 Cisco Secure ACS 软件许可证。访问 Cisco 订购主页（仅限注册用户）下订单。

注意： 您需要一个签署了相关服务合同的 CCO 帐户来获得 Cisco Secure ACS for Windows 的 90 天试用版本。

本文档中的路由器配置是根据运行 Cisco IOS® 软件版本 11.3.3 的路由器制定的。Cisco IOS 软件版本 12.0.5.T 及以上版本使用 **group tacacs+** 代替 **tacacs+**，因此，**aaa authentication login default tacacs+ enable** 等语句将显示为 **aaa authentication login default group tacacs+ enable**。

有关路由器命令的详细信息，请参阅 Cisco IOS 软件文档。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息以 Cisco IOS 软件版本 11.3.3 和 Cisco IOS 软件版本 12.0.5.T 及以上版本为基础

。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

验证

完成这些步骤：

1. 确保您在 UNIX 服务器上已编译了 TACACS+ (TAC+) 代码。此处的服务器配置假设您使用 Cisco TAC+ 服务器代码。无论服务器编码是否为 Cisco 服务器编码，该路由器配置都应工作。TAC+ 必须作为根而运行；如有必要，将 su 作为根。
2. 复制本文档末的 test_file，放到 TAC+ 服务器上，并将其命名为 **test_file**。检查以确定 **tac_plus_executable** 守护进程从 **test_file** 开始。此命令中，**-P** 选项用于检查编译错误，但不会启动守护进程：您可能会看到 test_file 的内容在窗口中向下滚动，但您应该不会看到以下消息：cannot find file、cleartext expected--found cleartext 或 unexpected }。如果出现错误，请检查 test_file 的路径、重新核对您的输入并重新测试，然后才能继续下一步。
3. 开始在路由器上配置 TAC+。在命令集前输入 **enable mode** 和 **configure terminal**。此命令语法可确保您开始时不会锁定路由器，但前提是 **tac_plus_executable** 并未运行：

   ```
   !--- Turn on
   TAC+. aaa new-model enable password whatever !--- These are lists of authentication
   methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- tac_plus_executable not being
   started, the !--- enable password is accepted because !--- it is in each list.        !
   aaa authentication login linmethod tacacs+ enable   aaa authentication login vtymethod
   tacacs+ enable   aaa authentication login conmethod tacacs+ enable   !   !--- Point the
   router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host
   #.#.#.# 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
   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
   ```
4. 测试以确定您仍可在继续下一步前通过 Telnet 和控制台端口访问路由器。由于 **tac_plus_executable** 并未运行，所以会接受**启用口令。注意：** 使控制台端口会话保持在活动状态并保持在启用模式。此会话不应超时。对路由器的访问限制在某一点上，并且您需要能够在无需锁定您自己的情况下进行配置更改。发出这些命令，以查看该路由器上的服务器对路由器的交互。

   ```
   !--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists
   of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---
   tac_plus_executable not being started, the !--- enable password is accepted because !--- it
   is in each list.        !        aaa authentication login linmethod tacacs+ enable   aaa
   authentication login vtymethod tacacs+ enable   aaa authentication login conmethod tacacs+
   enable   !   !--- Point the router to the server, where #.#.#.# !--- is the server IP
   address. ! tacacs-server host #.#.#.# 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 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. 作为根用户，请在服务器上启动 TAC+：!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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
6. 检查以确定 TAC+ 已启动：!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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或!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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如果 TAC+ 未启动，那么通常是 test_file 中的语法有问题。返回步骤 1 更正此问题。
7. 键入 **tail -f /var/tmp/tac_plus.log** 查看该服务器上路由器对服务器的交互。**注意：** 步骤 5 中的 -d 16 选项可将所有事务的输出发送到 /var/tmp/tac_plus.log。
8. 现在，Telnet (VTY) 用户必须通过 TAC+ 进行认证。当 debug 接近路由器和服务器（步骤 4 和 7）时，Telnet 将从网络的另一个部分进入路由器。路由器将生成用户名和口令提示符，您应对它们做出回复：!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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用户 authenuser 在组 admin 中，口令为 admin。观察服务器和您能看到TAC+交互

作用的路由器？什么发送，答复，请求，等等的地方。在您继续前，请更正所有问题。

9. 如果您还希望通过 TAC+ 认证您的用户，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以下命令添加到路由器：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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现在，用户必须通过 TAC+ 启用。
10. 当 debug 接近路由器和服务器（步骤 4 和 7）时，Telnet 将从网络的另一个部分进入路由器。路由器将生成用户名和口令提示符，您应对它们做出回复：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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当您进入启用模式时，路由器将请求输入口令，您应对此其做出回复：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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观察服务器和您应该看到TAC+交互作用的路由器？什么发送，答复，请求，等等的地方。在您继续前，请更正所有问题。
11. 终止服务器上的 TAC+ 进程时仍将服务器连接到控制台端口，以确保在 TAC+ 被终止的情况下您的用户仍能访问路由器。*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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或*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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重复前面的 Telnet 和启用步骤。然后，路由器会意识到 TAC+ 进程没有响应并允许用户使用默认口令登录和启用。

12. 检查通过 TAC+ 进行的控制台端口用户认证。为实现这一目标，请再次启动 TAC+ 服务器（步骤 5 和 6）并建立到达路由器的 Telnet 会话（应通过 TAC+ 进行认证）。在启用模式下保持 Telnet 到路由器的连接，直到您确定您可以通过控制台端口登录到路由器。注销您通过控制台端口到路由器的原始连接，然后重新连接到控制台端口。使用用户 ID 和口令进行登录和启用的控制台端口认证（如步骤 10 所示）现在应通过 TAC+ 进行。
13. 当您通过 Telnet 会话或控制台端口保持连接以及在 debug 接近路由器和服务器时（步骤 4 和 7），建立到线路 1 的调制解调器连接。线路用户现在必须通过 TAC+ 登录和启用。路由器将生成用户名和口令提示符，您应对它们做出回复：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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当您进入启用模式时，路由器将请求输入口令。回复：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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观察服务器和您看到TAC+交互作用的路由器？什么发送，答复，请求，等等的地方。在您继续前，请更正所有问题。现在，用户必须通过 TAC+ 启用。

添加授权

添加授权是可选的。

默认情况下，路由器上有三个命令级别：

- 权限级别 0，包括禁用、启用、退出、帮助和注销
- 权限级别 1 - Telnet 上的正常级别 - 提示符为 router>
- 权限级别 15 - 启用级别 - 提示符为 router#

由于可用命令取决于 IOS 功能集、Cisco IOS 版本、路由器型号等等，因此不存在级别 1 和 15 的所有命令的完整列表。例如，**show ipx route** 不存在于仅 IP 的功能集中，**show ip nat trans** 不存在于 Cisco IOS 软件版本 10.2.x 中，因为当时并未引入 NAT，而 **show environment** 不存在于没有电源和温度监测功能的路由器型号中。特定路由器的特定级别的命令，可以在您位于该权限级别时，在路由器提示符下输入 **?**，即可获得。

控制台端口授权不会作为功能添加，直到实施 Cisco bug ID CSCdi82030（仅限注册用户）。默认情况下，控制台端口授权是关闭的，以降低您意外锁定路由器的可能性。如果用户通过控制台对路由器进行物理访问，则控制台端口授权并不十分有效。不过，控制台端口授权可在某个镜像中的线路 con 0 下打开，在该镜像中，Cisco bug ID CSCdi82030 （仅限注册用户）通过以下命令实施：

```
!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication
methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- tac_plus_executable not being started, the !-
-- enable password is accepted because !--- it is in each list.          !          aaa
authentication login linmethod tacacs+ enable    aaa authentication login vtymethod tacacs+
enable    aaa authentication login conmethod tacacs+ enable    !    !--- Point the router to the
server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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
```

1. 可将路由器配置为在所有或一些级别通过 TAC+ 授权命令。此路由器配置允许所有用户在服务器上设置每个命令授权。这里我们通过 TAC+ 授权所有命令，但是，如果服务器发生故障，则无需进行授权。

   ```
   !--- Turn on TAC+. aaa new-model enable password whatever !--- These are
   lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on
   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 !---
   tac_plus_executable not being started, the !--- enable password is accepted because !--- it
   is in each list.          !          aaa authentication login linmethod tacacs+ enable    aaa
   authentication login vtymethod tacacs+ enable    aaa authentication login conmethod tacacs+
   enable    !    !--- Point the router to the server, where #.#.#.# !--- is the server IP
   address. ! tacacs-server host #.#.#.# 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 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
   ```

2. 当 TAC+ 服务器运行时，Telnet 将进入具有 userid **authenuser** 的路由器中。由于 authenuser 有默认服务 = permit in test_file，因此该用户应该能够执行所有功能。当在路由器中时，请进入**启用模式**，并打开授权调试：

   ```
   !--- Turn on TAC+. aaa new-model enable password whatever !-
   -- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod",
   and !--- so on 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 !--- tac_plus_executable not being started, the !--- enable password is accepted
   because !--- it is in each list.          !          aaa authentication login linmethod
   tacacs+ enable    aaa authentication login vtymethod tacacs+ enable    aaa authentication
   login conmethod tacacs+ enable    !    !--- Point the router to the server, where #.#.#.# !--
   - is the server IP address. ! tacacs-server host #.#.#.# 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 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

3. Telnet 将进入具有 userid **authoruser** 和口令**操作员**的路由器。该用户不能执行以下两个 show 命令：**traceroute** 和 **logout**（请参阅 test_file）。观察服务器和路由器，其中您应看到 TAC+ 交互（比如，发送地点、回复、请求等等）。在您继续前，请更正所有问题。
4. 如果您想配置 autocommand 用户，请消除 test_file 中的备注用户瞬态，并用有效的 IP 地址目标代替 #.#.#.#。停止并启动 TAC+ 服务器。在路由器上：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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使用用户 ID **transient** 和口令 **transient** 远程登录到路由器。**telnet #.#.#.#** 将执行，而用户瞬态将发送到另一个位置。

添加记帐

添加记帐是可选的。

对记帐文件的参考在test_file ？记帐文件= /var/log/tac.log。但是记帐不会发生，除非在路由器中进行了配置（假设该路由器运行比 Cisco IOS 软件版本 11.0 更高的软件）。

1. 在路由器中启用记帐：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host #.#.#.# 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 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**注意：** 有些版本中的 AAA 记帐不会执行每个命令记帐。应急方案是使用每个命令授权并将出现的情况记录在记帐文件中。（请参阅 Cisco bug ID CSCdi44140。）如果您使用用过这种解决方法的镜像 [Cisco IOS 软件版本 11.2(1.3)F、11.2(1.2)、11.1(6.3)、11.1(6.3)AA01、从 1997 年 9 月 24 日开始发行的 11.1(6.3)CA]，您也能启用命令记帐。
2. 当 TAC+ 在服务器上运行时，请在服务器上输入此命令，以查看进入记帐文件的条目：*!--- Turn on TAC+.* aaa new-model enable password whatever *!--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !---* **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! *!--- Point the router to the server, where #.#.#.# !--- is the server IP address.* ! tacacs-server host

#.#.#.# 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 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然后登录路由器，再从路由器注销，注销路由器的远程登录等等。如有必要，在路由器上输入：!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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

测试文件

!--- Turn on TAC+. aaa new-model enable password whatever !--- These are lists of authentication methods. !--- "linmethod", "vtymethod", "conmethod", and !--- so on 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 !--- **tac_plus_executable** not being started, the !--- enable password is accepted because !--- it is in each list. ! aaa authentication login linmethod tacacs+ enable aaa authentication login vtymethod tacacs+ enable aaa authentication login conmethod tacacs+ enable ! !--- Point the router to the server, where #.#.#.# !--- is the server IP address. ! tacacs-server host #.#.#.# 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 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

注意： 如果您的 TACACS 服务器无法到达，则会生成以下错误消息：%AAAA-3-DROPACCTSNDFAIL accounting record dropped,send to server failed:system-start。验证 TACACS+ 服务器是否可以运行。

相关信息

- 单用户的网络接入安全 TACACS+
- 终端访问控制器访问控制系统 (TACACS+)
- 用于 Windows 的 Cisco 安全访问控制服务器
- 技术支持和文档 - Cisco Systems