在Aironet访问接入点的TACACS+使用GUI登录认证的配置示例

目录

简介

本文解释如何使TACACS加上(TACACS+)在Cisco Aironet接入点(AP)的服务为了进行登录认证与使用TACACS+服务器。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 知识如何配置在Aironet AP的基本参数
- 知识如何配置一个TACACS+服务器类似思科安全访问控制服务器(ACS)
- TACACS+概念知识

关于TACACS+工作，如何的信息参考*了解*配置RADIUS和TACACS+服务器的*TACACS+*部分。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Aironet Cisco Aironet 1240/1140系列接入点

- 运行软件版本4.1的ACS
- 运行软件版本5.2的ACS

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。

配置

此部分说明如何配置Aironet AP和TACACS+服务器(ACS) TACACS+-based登录认证的。

此配置示例使用这些参数：

- ACS的IP地址— 172.16.1.1/255.255.0.0
- AP的IP地址— 172.16.1.30/255.255.0.0
- 在AP和TACACS+服务器使用**—示例的**共享密钥

这些是此示例在ACS配置用户的凭证：

- 用户名— **User1**
- 密码**—思科**
- 组— **Adminuser**

您需要配置TACACS+功能验证设法连接到AP通过Web接口或通过命令行界面(CLI)的用户。为了完成此配置，您必须执行这些任务：

1. 配置登录认证的TACACS+服务器。
2. 配置TACACS+认证的Aironet AP。

注意： 有关本文档所用命令的详细信息，请使用命令查找工具（仅限注册用户）。

网络图

本文档使用以下网络设置：

配置登录认证的TACACS+服务器-使用ACS 4.1

第一步将设置TACACS+守护程序验证设法访问AP的用户。您必须设置TACACS+认证的ACS和创建用户数据库。您能使用所有TACACS+服务器。此示例使用ACS作为TACACS+服务器。完成这些步骤：

1. 完成这些步骤为了添加AP作为验证、授权和统计(AAA)客户端：从ACS GUI，请点击**Network Configuration选项**。在 AAA Clients 下，单击 **Add Entry**。在添加AAA客户端窗口，请输入AP主机名、AP的IP地址和共享密钥。这共享的密钥必须是相同的象您在AP配置的共享密钥。从验证使用下拉菜单，挑选**TACACS+ (Cisco IOS)**。点击**Submit+Restart**为了保存配置。示例如下：此示例使用：AAA客户端主机名**接入点**地址**172.16.1.30/16**作为AAA客户端IP地址共享密钥**示例**
2. 完成这些步骤为了创建包含所有管理的组(admin)用户：点击从菜单的**组建立**在左边。新窗口出现。在GROUP SETUP窗口中，请选择组从下拉菜单配置并且点击**重命名组**。此示例选择

从下拉菜单的Group6并且重命名组Adminuser。单击 **submit**。示例如下：

3. 完成这些步骤为了添加用户到TACACS+数据库：点击**User Setup选项**。为了创建新用户，输入用户名在用户字段和单击**添加/编辑**。这是示例，创建**User1** ：在您单击后请添加/编辑，添加/Edit窗口为此用户出现。
4. 输入是特定对此用户的凭证并且单击**提交**为了保存配置。您能输入的凭证包括：附加用户信息用户设置用户分配的组示例如下：您能看到此示例添加用户User1到组Adminuser。**注意：** 如果不创建一特定组，用户分配到默认组。
5. 完成这些步骤为了定义权限级别：点击**GROUP SETUP选项**。选择您以前分配到此用户并且单击**编辑设置的**组。此示例使用组Adminuser。在TACACS+设置下，请检查**Shell (exec)**复选框并且检查有值为15的**权限级别**复选框。单击 **Submit+ Restart**。**注意：** 必须为GUI和Telnet定义权限级别15为了是可访问作为级别15。否则，默认情况下，用户能只访问作为1级。如果权限级别没有定义，并且用户设法输入在CLI的特权模式(与使用Telnet)， AP显示此错误消息：

```
AccessPoint>enable
% Error in authentication
```

如果想要添加更多用户对TACACS+数据库，请重复步骤2至4此步骤。在您完成这些步骤后，TACACS+服务器准备验证设法登陆到AP的用户。现在，您必须配置TACACS+认证的AP。

配置登录认证的TACACS+服务器-使用ACS 5.2

第一步是添加AP作为ACS的一个AAA客户端并且创建登录的一项TACACS策略。

1. 完成这些步骤为了添加AP作为AAA客户端：从ACS GUI，请点击**网络资源**，然后点击**网络设备和AAA客户端**。在网络设备下，请单击**创建**。进入AP的主机名在**名称的** ，并且提供关于AP的一说明。如果这些类别定义，请选择**位置**和**设备类型**。由于仅单个AP配置，请点击**单个IP地址**。您能通过单击**IP范围**添加多个的AP IP地址范围。然后，请输入AP的IP地址。在**认证选项下**，请检查**TACACS+**方框并且输入**共享塞克雷**。示例如下：
2. 下一步是创建登录用户名和密码：点击**用户和标识存储**，然后点击**用户**。Click **Create**.给用户名在**名称下**，并且提供说明。选择**标识组**，如果其中任一。输入密码在**密码**文本框下，并且重新输入在**确认密码下**。您能通过输入密码修改特权密码在**特权密码下**。重新输入确认。示例如下：
3. 完成这些步骤为了定义权限级别：点击**策略元素>授权和权限>设备Administration > Shell配置文件**。检查**Permit访问检查**复选框并且点击**重复项**。输入**名称**和**说明**。选择普通的任务选项卡并且为最大权限选择**15**。单击 **submit**。
4. 完成这些步骤为了创建授权策略：点击**访问策略**>Access **Services>默认设备Admin >授权**。单击**创建**为了创建一项新的授权策略。新弹出看上去创建授权策略的规则。选择**标识组**，**位置**特定用户名和AAA客户端的(AP)等，如果其中任一。单击**精选**为Shell配置文件选择配置文件创建的自治AP。一旦这执行，请点击**保存更改**。点击**默认设备Admin**，然后点击**允许协议**。检查**允许PAP/ASCII**，然后单击**提交**。点击**服务选择规则**确保那里是指向的规则匹配TACACS和默认设备Admin。

配置TACACS+认证的Aironet AP

您能使用CLI或GUI为了启用在Aironet AP的TACACS+功能。此部分说明如何配置TACACS+登录认证的AP与使用GUI。

完成这些步骤为了配置在AP的TACACS+与使用GUI ：

1. 完成这些步骤为了定义TACACS+服务器参数：从AP GUI，请选择**安全>Server管理器**。安全：Server Manager窗口出现。在公司服务器地区中，从当前服务器列表下拉菜单的挑选**TACACS+**。在此同样区域中，请输入IP地址、共享机密和TACACS+服务器的认证端口端口号。单击 **Apply**。示例如下：**注意：** 默认情况下， TACACS+用途TCP端口49。**注意：** 您在ACS和AP配置的共享密钥必须配比。
2. 选择**默认服务器优先级> Admin验证(TACACS+)**，从Priority1下拉菜单挑选您配置的TACACS+服务器IP地址，并且单击**应用**。示例如下：
3. 选择**安全> Admin访问**和，管理员的验证：请选择**仅认证服务器**并且单击**应用**。此选择保证设法登陆到AP的用户由认证服务器验证。示例如下：

这是配置示例的CLI配置：

接入点

```
AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
!--- Enable AAA. ! ! aaa group server radius rad_eap !
aaa group server radius rad_mac ! aaa group server
radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
cache authentication profile admin_cache ! aaa group
server tacacs+ tac_admin
!--- Configure the server group tac_admin. server
172.16.1.1
!--- Add the TACACS+ server 172.16.1.1 to the server
group. cache expiry 1
!--- Set the expiration time for the local cache as 24
hours. cache authorization profile admin_cache
 cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
!--- Define the AAA login authentication method list to
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
!--- Use TACACS+ for privileged EXEC access
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
```

```
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
!--- Specify the authentication method of HTTP users as
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

注意： 您必须有Cisco IOS软件版本12.3(7)JA或以上为了所有in命令此配置适当地工作。一个初期的Cisco IOS软件版本也许没有所有这些可以使用的命令。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

为了验证配置，请设法登陆到与使用的AP GUI或CLI。当您设法访问AP时， AP提示您输入用户名和密码。

当您提供用户凭证时， AP转发凭证到TACACS+服务器。TACACS+服务器根据是可用的在其数据库和提供访问对AP在成功认证的信息验证凭证。您能选择**报告，并且活动>通过**在ACS的**验证**并且使用合格验证报告为了检查成功认证此用户。示例如下：

您能也使用**show tacacs命令**为了验证TACACS+服务器的正确配置。示例如下：

```
AccessPoint#show tacacs

Tacacs+ Server            : 172.16.1.1/49
              Socket opens:        348
             Socket closes:        348
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
```

```
Failed Connect Attempts:          0
     Total Packets Sent:        525
     Total Packets Recv:        525
```

ACS的5.2验证

您能验证失败/通过登录凭证的尝试从ACS 5.2 ：

1. 点击**监听和报告>启动监听并且报告查看器**。新弹出打开与控制板。
2. 点击认证TACACS**今天**。这显示详细信息失败/通过尝试。

故障排除

您能使用这些调试on命令AP为了排除故障您的配置：

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

- **debug tacacs events** —此命令显示在TACACS认证时发生的事件顺序。这是此命令输出的示例：

```
*Mar  1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for
processing
*Mar  1 00:51:21.113: TPLUS: processing authentication start request id 0
*Mar  1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1)
*Mar  1 00:51:21.114: TPLUS: Using server 172.16.1.1
*Mar  1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
16 bytes data)
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:51:21.121: TPLUS: processing authentication continue request id 0
*Mar  1 00:51:21.122: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout
*Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect
6 bytes data)
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet
*Mar  1 00:51:21.179: TPLUS: Received authen response status PASS (2)
```

- **debug ip http authentication** - 使用此命令对 HTTP 身份验证问题进行故障排除。命令显示路由器尝试和验证特定的状态消息的认证方法。
- **debug aaa authentication** —此命令显示关于AAA TACACS+认证的信息。

如果用户输入不存在于TACACS+服务器的用户名，验证发生故障。这是失败的认证的**debug tacacs authentication命令**输出：

```
*Mar  1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing
```

```
*Mar  1 00:07:26.624: TPLUS: processing authentication start request id 0
*Mar  1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3)
*Mar  1 00:07:26.624: TPLUS: Using server 172.16.1.1
*Mar  1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2
*Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading
*Mar  1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16
bytes data)
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response
*Mar  1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8)
*Mar  1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing
*Mar  1 00:07:26.633: TPLUS: processing authentication continue request id 0
*Mar  1 00:07:26.633: TPLUS: Authentication continue packet generated for 0
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout
*Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6
bytes data)
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1
*Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response
*Mar  1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet
*Mar  1 00:07:26.689: TPLUS: Received authen response status FAIL (3)
```

您能选择**报告和活动>失败的认证**为了看到在ACS的失败的认证尝试。示例如下：

如果使用早于Cisco IOS软件版本12.3(7)JA在AP的一个Cisco IOS软件版本，您可以每次点击您设法登陆到与使用的AP HTTP的bug。Cisco Bug ID是CSCeb52431 (仅限注册用户)。

Cisco IOS软件HTTP/AAA实施要求其中每一的独立验证分开的HTTP连接。无线Cisco IOS软件GUI介入许多数十分离文件参考在单个网页内的(例如Javascript和GIF)。因此，如果装载一单页在无线Cisco IOS软件GUI，十二个和数十独立的认证/授权请求能点击AAA服务器。

对于HTTP验证，请使用RADIUS或本地认证。RADIUS服务器对多次认证请求仍然被服从。但是RADIUS比TACACS+可扩展，和，因此提供less-adverse性能影响可能的。

如果必须使用TACACS+，并且有一Cisco ACS，请以**tacacs-server命令**使用**单连接**关键字。使用此关键字用命令最节省ACS TCP连接建立/卸载开销并且可能某种程度上减少在服务器的负载。

对于Cisco IOS软件版本12.3(7) JA和稍后AP，软件包括修正。此部分剩余描述修正。

请使用AAA认证缓存功能为了缓存TACACS+服务器返回的信息。验证缓存和配置文件功能允许AP缓存用户的认证/授权答复，以便随后的认证/授权请求不需要发送到AAA服务器。为了启用与CLI的此功能，请使用这些命令：

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

关于此功能和命令的更多信息，参考*配置验证缓存并且描出*管理接入点的部分。

为了启用在GUI的此功能，请选择**安全> Admin访问**并且检查**启用认证服务器高速缓冲存储**复选框。由于本文使用Cisco IOS软件版本12.3(7)JA，本文使用修正，正象配置说明。

相关信息

- 配置 RADIUS 和 TACACS+ 服务器
- Field Notice：IOS接入点炮击有请求的TACACS+服务器
- 使用 RADIUS 服务器执行 EAP 身份验证
- 无线产品支持
- 技术支持和文档 - Cisco Systems