TACACS +和RADIUS比较

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Conventions](#)
[RADIUS背景](#)
[客户端/服务器模型](#)
[网络安全](#)
[灵活的认证机制](#)
[服务器代码可用性](#)
[比较TACACS+和RADIUS](#)
[UDP和TCP](#)
[信息包加密](#)
[认证和授权](#)
[多协议支持](#)
[路由器管理](#)
[互通性](#)
[数据流](#)
[设备支持](#)
[Related Information](#)

Introduction

两个用于控制网络访问的典型安全协议是 Cisco TACACS+ 和 RADIUS。RADIUS规格在RFC 2865描述 ，废弃RFC 2138 。Cisco做对支持与最佳的两个协议组提供。它不是Cisco的目的与RADIUS竞争或影响用户使用TACACS+。您应该选择该最佳适应您的需要的解决方案。本文讨论在TACACS+和RADIUS之间的区别，因此您能使一个通告选择做出。

Cisco在1996年2月支持RADIUS协议从Cisco IOS软件版本11.1。Cisco继续提高有新功能和功能的RADIUS客户端，支持RADIUS作为标准。

在开发了TACACS+前， Cisco严重评估了RADIUS作为安全协议。许多功能在TACACS+协议包括适应生长安全市场的需要。协议设计扩展，当网络增长和适应新的安全技术，当市场成熟。TACACS+协议的底层体系结构补全独立验证、授权和统计(AAA)体系结构。

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

This document is not restricted to specific software and hardware versions.

Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

RADIUS背景

RADIUS是使用AAA协议的接入服务器。它是获取对网络和网络服务的远程访问未被授权的访问分布式安全的系统。RADIUS包括三个组件：

- 与使用用户数据报协议(UDP) /IP的帧格式的一个协议。
- 一个服务器。
- 一个客户端。

而客户端在拨号接入服务器驻留，并且可以被分配在网络中，服务器在中央计算机典型地运行在客户站点。Cisco合并RADIUS客户端到Cisco IOS软件版本11.1及以上版本和其它设备软件里。

客户端/服务器模型

网络接入服务器(NAS)运行作为RADIUS的客户端。客户端负责传递用户信息给选定的RADIUS服务器，然后操作在返回的回应。RADIUS服务器对收到用户连接请求，验证用户和返回所有配置信息负责必要为了客户端能提供服务到用户。RADIUS服务器能作为代理客户端到其他认证服务器。

网络安全

客户端和 RADIUS 服务器之间的事务通过使用从未在网络上发送的共享密钥进行身份验证。另外，发送所有用户密码被加密在客户端和RADIUS服务器之间。这排除监听在一个不安全的网络的某人可能确定用户密码的可能性。

灵活的认证机制

RADIUS服务器支持各种各样的方法验证用户。当带有用户时和原始密码产生的用户名，可以支持PPP，密码认证协议或者质询握手验证协议(CHAP)、UNIX登录和其他认证机制。

服务器代码可用性

有商业和免费提供服务器编码的一定数量的分配。Cisco服务器包括Windows的UNIX的Cisco Secure ACS， Cisco Secure ACS和Cisco Access Registrar。

比较TACACS+和RADIUS

这些部分比较TACACS+和RADIUS几个功能。

UDP和TCP

RADIUS用途UDP，当TACACS+使用TCP时。TCP提供几个优点超过UDP。而UDP提供最佳效果发送， TCP提供面向连接的传输。RADIUS要求另外的可编程变量例如重新传输尝试和超时补尝尽力而为传输，但是缺乏TCP传输提供内置支持的级别：

- TCP使用方法提供单独确认请求如何在(近似)网络Round-Trip Time (RTT)内收到了，不管装载并且减慢后端验证机制(TCP确认)也许是。
- TCP提供一失败或者不的立即指示，服务器由重置(RST)负责。您能确定，当服务器失败并且返回服务时，如果使用长寿的TCP连接。UDP不能说出发生故障的服务器，慢速服务器和一个不存在的服务器之间的差别。
- 使用TCP Keepalive，服务器失败可以发现带外与实际请求。与多个服务器的连接可以同时被维护，并且您只需要传送信息到知道是正在运行的那个。
- TCP是更加可升级的并且适应生长，以及拥塞，网络。

信息包加密

RADIUS加密在访问请求信息包的仅密码，从客户端到服务器。信息包的剩下的事末加密。其他信息，例如用户名，核准的服务和认为，可以由第三方获取。

TACACS+加密信息包的整个正文，但是留下一个标准的TACACS+报头。在报头内是指示的字段是否正文被加密。为调试目的，是有用的有末加密的信息包的正文。然而，在正常运行时，信息包的正文为更多安全通信充分地被加密。

认证和授权

RADIUS结合认证和授权。RADIUS服务器发送的访问接受信息包到客户端包含授权信息。这使困难分离认证和授权。

TACACS+使用AAA体系结构，分离AAA。这允许能仍然使用TACACS+授权和记帐的独立的身份验证解决方案。例如，与TACACS+，使用Kerberos认证和TACACS+授权和记帐是可能的。在NAS在Kerberos服务器后验证，请求从TACACS+服务器的授权信息，而不必重新鉴别。NAS通知TACACS+服务器在Kerberos服务器成功验证，并且服务器然后提供授权信息。

在会话期间，如果另外的授权检查是需要的，接入服务器检查以TACACS+服务器确定是否同意用户权限使用一个特定命令。这提供对在接入服务器可以被执行，当分离从认证机制时的命令的更加巨大的控制。

多协议支持

RADIUS不支持这些协议：

- AppleTalk远程访问(ARA)协议
- NetBIOS帧协议控制协议
- Novell异步服务接口(NASI)
- X.25 PAD连接

TACACS+提供多协议支持。

路由器管理

RADIUS不允许用户控制哪些命令在路由器可以被执行，并且哪些不能。所以， RADIUS不是如有用为路由器管理或如灵活为终端服务。

TACACS+提供两个方法控制路由器on命令的授权一个单个用户或基于组。第一种方法是指定权限级别到命令和安排路由器用TACACS+服务器验证用户是否被认证在指定的权限级别。第二种方法是明确地指定在TACACS+服务器，在一个单个用户或基于组，允许的命令。

互通性

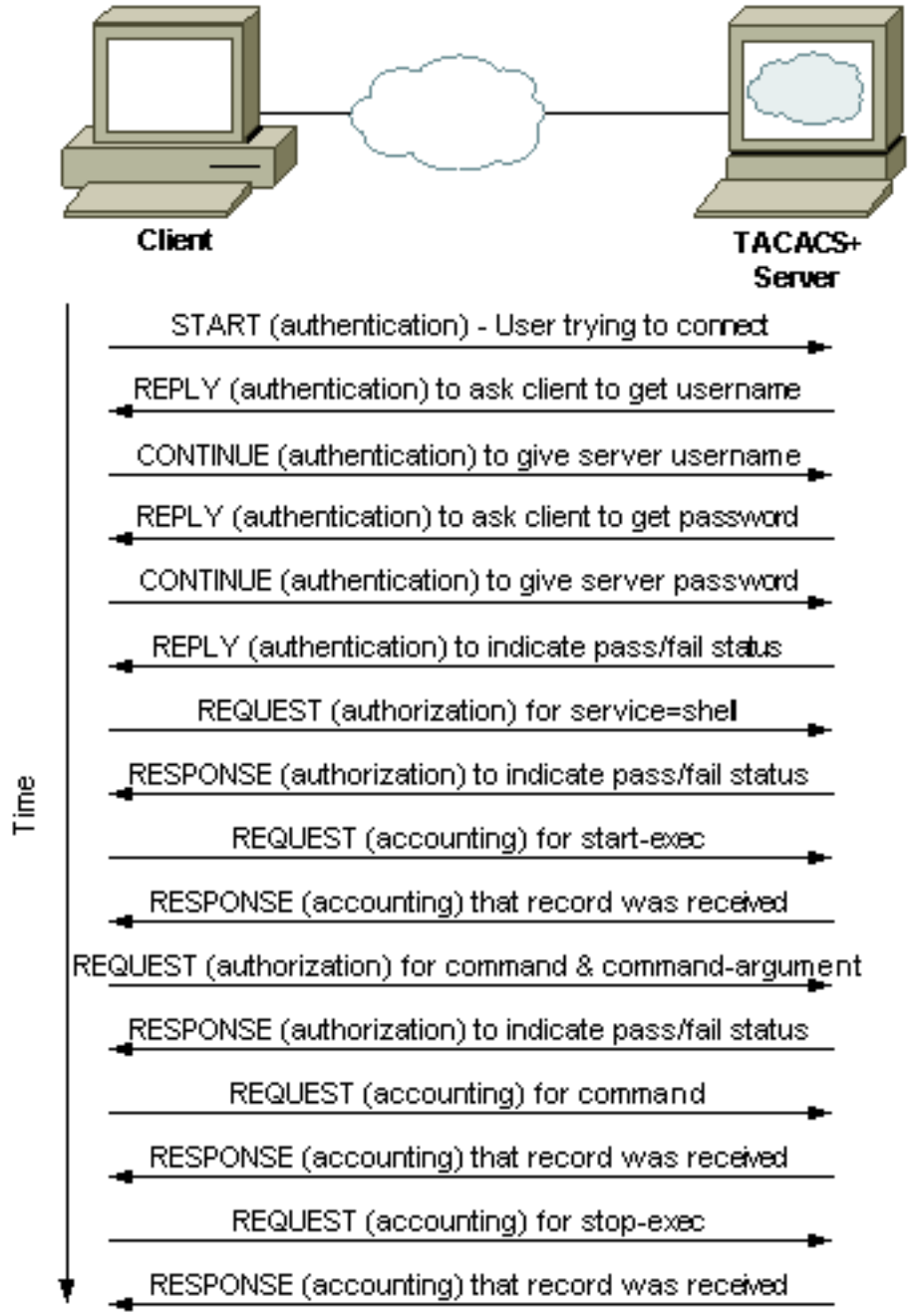
由于RADIUS请求注释(RFC)的多种解释，遵照RADIUS RFC不保证互通性。即使几个供应商实现RADIUS客户端，这不意味着他们是相互可操作的。Cisco实现多数RADIUS属性和一致添加更多。如果用户在他们的服务器使用仅标准RADIUS属性，他们能兼容在几个供应商之间，只要这些供应商实现同样属性。然而，许多供应商实现是专有属性的扩展。如果用户使用这些特定供应商的扩展属性之一，互通性不是可能的。

数据流

由于在TACACS+和RADIUS之间的以前被援引的区别，流量总量生成在客户端和服务器之间有所不同。这些示例说明客户端和服务器TACACS+的和RADIUS之间的数据流，当使用路由器管理与RADIUS不能执行)的认证、exec授权， authorization命令(exec认为和RADIUS不能执行)的命令记帐(。

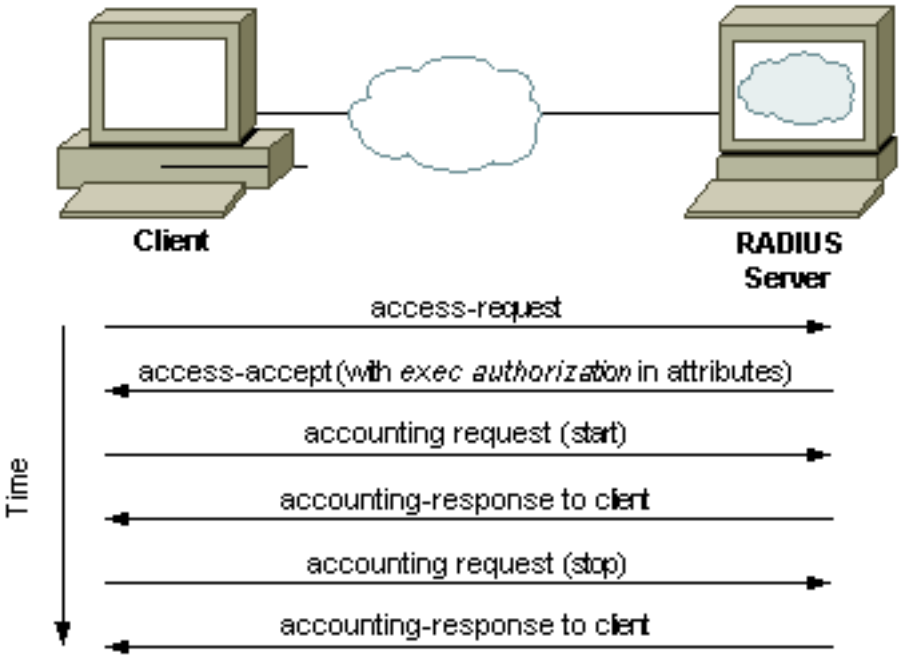
TACACS+数据流示例

当用户远程登录到路由器，执行命令，并且退出路由器时，此示例假设登录认证、exec授权， authorization命令， start-stop exec认为和命令记帐实现与TACACS+ ：



RADIUS数据流示例

此示例假设登录认证， exec授权，并且start-stop exec认为实现与RADIUS，当用户远程登录到路由器，执行命令，并且退出路由器时(其他管理服务不是可用的) ：



设备支持

此表由所选平台的设备类型列出TACACS+和RADIUS AAA技术支持。这包括技术支持被添加的软件版本。如果您的产品不在此列表，欲知详情检查产品版本注释。

Cisco设备	TACACS+认证	TACACS+授权	TACACS+认为	RADIUS认证	RADIUS授权	RADIUS认为
Cisco Aironet 1	12.2(4)JA	12.2(4)JA	12.2(4)JA	所有接入点	所有接入点	所有接入点
Cisco IOS Software2	10.33	10.33	10.33[3]	11.1.1	11.1.1[4]	11.1.1[5]
Cisco缓存引擎	--	--	--	1.5	1.5[6]	--
Cisco Catalyst交换机	2.2	5.4.1	5.4.1	5.1	5.4.1[4]	5.4.1[5]
Cisco CSS 11000内容服务交换机	5.03	5.03	5.03	5.0	5.0[4]	--
Cisco CSS 11500 Content Services交换机	5.20	5.20	5.20	5.20	5.20[4]	--
Cisco PIX防火墙	4.0	4.0[7]	4.2[8,5]	4.0	5.2[7]	4.2[8,5]
Cisco Catalyst	8.x enterp	--	--	--	--	--

1900/2820交换机	rise9					
Cisco Catalyst 2900XL/3500XL交换机	11.2.(8)SA6[10]	11.2.(8)SA6[10]	11.2.(8)SA6[10]	12.0(5)WC5[11]	12.0(5)WC5[11，4]	12.0(5)WC5[11，5]
Cisco VPN 3000 Concentrator [6]	3.0	3.0	--	2.0[12]	2.0	2.0[12]
Cisco VPN 5000 Concentrator	--	--	--	5.2X[12]	5.2X[12]	5.2X[12]

表注释

1. 只有无线客户端的终端，在版本的不是管理数据流除Cisco IOS Software Release 12.2(4)JA或以上之外。在Cisco IOS Software Release 12.2.(4)JA或以上，无线客户端和管理数据流的终端的认证是可能的。
2. 检查功能导航(当前由软件顾问(仅限注册用户)的)已废弃的在Cisco IOS软件内的平台支持。
3. 命令记帐不是被实施的直到Cisco IOS Software Release 11.1.6.3。
4. no命令授权。
5. no命令记帐。
6. URL阻塞仅，不管理数据流。
7. 非VPN数据流的授权通过PIX。**Note:** 版本5.2 -访问控制表(ACL) RADIUS供应商专用属性(VSA)的访问列表终止在PIX可下载的ACLs的版本6.1 -为ACL VPN流量的RADIUS属性11授权请支持终止在PIX版本6.2.2 -技术支持的VPN流量的技术支持或TACACS+授权与终止在PIX版本6.2的VPN流量的RADIUS授权-授权的技术支持PIX管理数据流的通过TACACS+。
8. 占非VPN数据流通过仅PIX，不是管理数据流。**Note:** 版本5.2 -占的技术支持VPN客户端TCP信息包通过PIX。
9. 仅企业软件。
10. 镜像的需要8M闪存。
11. 仅VPN终端。

Related Information

- RADIUS 支持页
- 在IOS文档的TACACS+
- TACACS/TACACS+ 支持页面
- 请求注解 (RFC)
- Technical Support & Documentation - Cisco Systems