用于 AAA 的 RADIUS 服务器

本章介绍如何配置用于 AAA 的 RADIUS 服务器。

- 关于用于 AAA 的 RADIUS 服务器， 第 1 页
- AAA 的 RADIUS 服务器准则， 第 12 页
- 配置用于 AAA 的 RADIUS 服务器， 第 13 页
- 测试 RADIUS 服务器身份验证和授权， 第 18 页
- 为 AAA 监控 RADIUS 服务器， 第 18 页
- 用于 AAA 的 RADIUS 服务器历史记录， 第 19 页

关于用于 AAA 的 RADIUS 服务器

ASA 支持以下符合 RFC 标准的用于 AAA 的 RADIUS 服务器：

- 思科安全 ACS 3.2、4.0、4.1、4.2 和 5.x
- 思科身份服务引擎 (ISE)
- RSA 身份验证管理器 5.2、6.1 和 7.x 中的 RSA RADIUS
- Microsoft

受支持的身份验证方法

ASA 支持为 RADIUS 服务器使用以下身份验证方法：

- PAP - 适用于所有连接类型。
- CHAP 和 MS-CHAPv1 - 适用于 L2TP-over-IPsec 连接。
- MS-CHAPv2 - 适用于 L2TP-over-IPsec 连接和常规 IPsec 远程访问连接（当启用密码管理功能时）。您也可以通过无客户端连接使用 MS-CHAPv2。
- 身份验证代理模式 - 适用于 RADIUS-to-Active-Directory、RADIUS-to-RSA/SDI、RADIUS-to-Token 服务器和 RSA/SDI-to-RADIUS 连接。

注释 要启用 MS-CHAPv2 作为 ASA 与 RADIUS 服务器之间进行 VPN 连接所用的协议，则必须在隧道组常规属性中启用密码管理。启用密码管理会生成一个从 ASA 向 RADIUS 服务器的 MS-CHAPv2 身份验证请求。有关详细信息，请参阅 **password-management** 命令的描述。

如果在隧道组中使用双重身份验证并启用密码管理，则主身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则可以通过使用 **no mschapv2-capable** 命令将该服务器配置为发送非 MS-CHAPv2 身份验证请求。

VPN 连接的用户授权

ASA 可以使用 RADIUS 服务器进行 VPN 远程访问和防火墙直接转发代理会话的用户授权（按用户使用动态 ACL 或 ACL 名称）。要实施动态 ACL，必须将 RADIUS 服务器配置为支持动态 ACL。在用户进行身份验证时，RADIUS 服务器向 ASA 发送可下载的 ACL 或 ACL 名称。设备会根据 ACL 允许或拒绝对指定服务的访问。当身份验证会话到期时，ASA 会删除 ACL。

除了 ACL 以外，ASA 还支持 VPN 远程访问和防火墙直接转发代理会话的权限授权与设置的许多其他属性。

支持的 RADIUS 属性集

ASA 支持以下 RADIUS 属性集：

- RFC 2138 和 2865 中定义的身份验证属性。
- RFC 2139 和 2866 中定义的记帐属性。
- RFC 2868 和 6929 中定义的用于隧道协议支持的 RADIUS 属性。
- RADIUS 供应商 ID 9 确定的思科 IOS 供应商特定属性 (VSA)。
- RADIUS 供应商 ID 3076 确定的思科 VPN 相关 VSA。
- RFC 2548 中定义的 Microsoft VSA。

支持的 RADIUS 授权属性

授权是指执行权限或属性的过程。如果已配置权限或属性，则定义为身份验证服务器的 RADIUS 服务器会执行权限或属性。这些属性具有供应商 ID 3076。

下表列出了可用于用户授权的受支持 RADIUS 属性。

注释 RADIUS 属性名称不包含 cVPN3000 前缀。思科安全 ACS 4.x 支持这一新的命名法，但 ACS 4.0 之前版本中的属性名称仍然包含 cVPN3000 前缀。ASA 基于属性数字 ID（而非属性名称）实施 RADIUS 属性。

下表中列出的所有属性均为从 RADIUS 服务器发送到 ASA 的下游属性，但以下属性除外：146、150、151 和 152。这些属性编号是从 ASA 发送到 RADIUS 服务器的上游属性。RADIUS 属性 146 和 150 是从 ASA 发送到 RADIUS 服务器，以提出身份验证和请求授权。前面列出的所有四个属性都是从 ASA 发送到 RADIUS 服务器，以提出开始记账、临时更新和停止请求。8.4(3) 版本引入了上游 RADIUS 属性 146、150、151 和 152。

表 *1:* 支持的 *RADIUS* 授权属性

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Access-Hours	支持	1	字符串	单值	时间范围的名称，例如工作时间
Access-List-Inbound	支持	86	字符串	单值	ACL ID
Access-List-Outbound	支持	87	字符串	单值	ACL ID
Address-Pools	支持	217	字符串	单值	IP 本地池的名称
Allow-Network-Extension-Mode	支持	64	布尔值	单值	0 = 已禁用 1 = 已启用
Authenticated-User-Idle-Timeout	支持	50	整数	单值	1-35791394 分钟
Authorization-DN-Field	支持	67	字符串	单值	可能的值：UID、OU、O、CN、L、SP、T、N、GN、SN、I、GENQ、DNQ、SE use-entire-name
Authorization-Required		66	整数	单值	0 = 否 1 = 是
Authorization-Type	支持	65	整数	单值	0 = 无 1 = RADIUS 2 = LDAP
Banner1	支持	15	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 Secure Client SSL TLS/DTL Clientless SSL。
Banner2	支持	36	字符串	单值	要为思科 VPN 远程访问会话显示的横幅 IPsec IKEv1、 Secure Client SSL TLS/DTL Clientless SSL。如果进行了相应的配置，字符串会连接到 Banner1 字符串。
Cisco-IP-Phone-Bypass	支持	51	整数	单值	0 = 已禁用 1 = 已启用
Cisco-LEAP-Bypass	支持	75	整数	单值	0 = 已禁用 1 = 已启用

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Client Type	支持	150	整数	单值	1 = 思科 VPN 客户端 (IKEv1) 2 = Secure Clie VPN 3 = 无客户端 SSL VPN 4 = 直接转发代 L2TP/IPsec SSL VPN 6 = Secure Client IPsec (IKEv2)
Client-Type-Version-Limiting	支持	77	字符串	单值	IPsec VPN 版本号字符串
DHCP-Network-Scope	支持	61	字符串	单值	IP 地址
Extended-Authentication-On-Rekey	支持	122	整数	单值	0 = 已禁用 1 = 已启用
Framed-Interface-Id	支持	96	字符串	单值	分配的 IPv6 接口 ID。与 Framed-IPv6-Prefix 用以创建完整的已分配 IPv6 地址。例如：Framed-Interface-ID =1:1:1:1与 Framed-IPv6-P =2001:0db8::/64 组合可提供分配的IP地址 2001:0db8::1:1:1:1。
Framed-IPv6-Prefix	支持	97	字符串	单值	分配的 IPv6 前缀和长度。与 Framed-Interfac 合以创建完整的已分配 IPv6 地址。例如：前 2001:0db8::/64 与 Framed-Interface-Id=1:1:1:1 提供IP地址 2001:0db8::1:1:1:1。通过分配前缀 为/128 的完整 IPv6 地址（例如，Framed-IPv6-Prefix=2001:0db8::1/128），可以 属性分配IP地址而不使用 Framed-Interface-Id
Group-Policy	支持	25	字符串	单值	为远程访问 VPN 会话设置组策略。对于 8.2. 及更高版本，请改用此属性而非 IETF-Radius- 您可以使用以下其中一种格式： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称；
IE-Proxy-Bypass-Local		83	整数	单值	0 = 无 1 = 本地
IE-Proxy-Exception-List		82	字符串	单值	换行符 (\n) 分隔的 DNS 域列表
IE-Proxy-PAC-URL	支持	133	字符串	单值	PAC 地址字符串
IE-Proxy-Server		80	字符串	单值	IP 地址
IE-Proxy-Server-Policy		81	整数	单值	1 = 无修改 2 = 无代理 3 = 自动检测 4 = 使用 设置
IKE-KeepAlive-Confidence-Interval	支持	68	整数	单值	10 到 300 秒

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IKE-Keepalive-Retry-Interval	支持	84	整数	单值	2 到 10 秒
IKE-Keep-Alives	支持	41	布尔值	单值	0 = 已禁用 1 = 已启用
Intercept-DHCP-Configure-Msg	支持	62	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Allow-Passwd-Store	支持	16	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Authentication		13	整数	单值	0 = 无 1 = RADIUS 2 = LDAP（仅适用于 = NT 域 4 = SDI 5 = 内部 6 = RADIUS 到 Kerberos/Active Directory
IPsec-Auth-On-Rekey	支持	42	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Backup-Server-List	支持	60	字符串	单值	服务器地址（以空格分隔）
IPsec-Backup-Servers	支持	59	字符串	单值	1 = 使用客户端配置的列表 2 = 禁用并清除 表 3 = 使用备份服务器列表
IPsec-Client-Firewall-Filter-Name		57	字符串	单值	指定要作为防火墙策略推送到客户端的过 称
IPsec-Client-Firewall-Filter-Optional	支持	58	整数	单值	0 = 必需 1 = 可选
IPsec-Default-Domain	支持	28	字符串	单值	指定要发送到客户端的单个默认域名（1 符）。
IPsec-IKE-Peer-ID-Check	支持	40	整数	单值	1 = 必需 2 = 如果对等证书支持 3 = 不检
IPsec-IP-Compression	支持	39	整数	单值	0 = 已禁用 1 = 已启用
IPsec-Mode-Config	支持	31	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP	支持	34	布尔值	单值	0 = 已禁用 1 = 已启用
IPsec-Over-UDP-Port	支持	35	整数	单值	4001 到 49151。默认值为 10000。
IPsec-Required-Client-Firewall-Capability	支持	56	整数	单值	0 = 无 1 = 远程 FW Are-You-There (AYT) 略 2 = 策略推送的 CPP 4 = 来自服务器的
IPsec-Sec-Association		12	字符串	单值	安全关联的名称
IPsec-Split-DNS-Names	支持	29	字符串	单值	指定要发送到客户端的辅助域名列表（1 符）。
IPsec-Split-Tunneling-Policy	支持	55	整数	单值	0 = 无拆分隧道 1 = 拆分隧道 2 = 允许本

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IPsec-Split-Tunnel-List	支持	27	字符串	单值	指定用于描述分割隧道包含列表的网络或 AC 称。
IPsec-Tunnel-Type	支持	30	整数	单值	1 = LAN 到 LAN 2 = 远程访问
IPsec-User-Group-Lock		33	布尔值	单值	0 = 已禁用 1 = 已启用
IPv6-Address-Pools	支持	218	字符串	单值	IP 本地池 IPv6 的名称
IPv6-VPN-Filter	支持	219	字符串	单值	ACL 值
L2TP-Encryption		21	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
L2TP-MPPC-Compression		38	整数	单值	0 = 已禁用 1 = 已启用
Member-Of	支持	145	字符串	单值	逗号分隔的字符串，例如： `Engineering, Sales` 可在动态访问策略里使用的管理属性。不设 略。
MS-Client-Subnet-Mask	支持	63	布尔值	单值	IP 地址
NAC-Default-ACL		92	字符串		ACL
NAC-Enable		89	整数	单值	0 = 否 1 = 是
NAC-Revalidation-Timer		91	整数	单值	300 到 86400 秒
NAC-Settings	支持	141	字符串	单值	NAC 策略名称
NAC-Status-Query-Timer		90	整数	单值	30 到 1800 秒
Perfect-Forward-Secrecy-Enable	支持	88	布尔值	单值	0 = 否 1 = 是
PPTP-Encryption		20	整数	单值	位图： 1 = 需要加密 2 = 40 位 4 = 128 位 8 无状态 15= 40/128 位加密/需要无状态
PPTP-MPPC-Compression		37	整数	单值	0 = 已禁用 1 = 已启用
Primary-DNS	支持	5	字符串	单值	IP 地址
Primary-WINS	支持	7	字符串	单值	IP 地址
Privilege-Level	支持	220	整数	单值	介于 0 和 15 之间的整数。

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
Required-Client- Firewall-Vendor-Code	支持	45	整数	单值	1 = 思科系统（使用思科集成客户端） 2 = 3 = NetworkICE 4 = Sygate 5 = 思科系统 入侵防御安全代理）
Required-Client-Firewall-Description	支持	47	字符串	单值	字符串
Required-Client-Firewall-Product-Code	支持	46	整数	单值	思科系统公司产品： 1 = 思科入侵防御安全代理或思科集成客 Zone Labs 产品： 1 = Zone Alarm 2 = Zon 3 = Zone Labs Integrity NetworkICE 产品： 1 = BlackIce Defende Sygate 产品： 1 = Personal Firewall 2 = P Firewall Pro 3 = 安全代理
Required-Individual-User-Auth	支持	49	整数	单值	0 = 已禁用 1 = 已启用
Require-HW-Client-Auth	支持	48	布尔值	单值	0 = 已禁用 1 = 已启用
Secondary-DNS	支持	6	字符串	单值	IP 地址
Secondary-WINS	支持	8	字符串	单值	IP 地址
SEP-Card-Assignment		9	整数	单值	未使用
Session Subtype	支持	152	整数	单值	0 = 无 1 = 无客户端 2 = 客户端 3 = 仅客 Session Subtype 的适用条件是 Session Typ 性仅具有以下值：1、2、3 和 4。
Session Type	支持	151	整数	单值	0 = 无1 = Secure Client SSL VPN 2 = Secu IPSec VPN (IKEv2) 3 = 无客户端 SSL VP 户端邮件代理5 = 思科 VPN 客户端 (IKEv1) LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN
Simultaneous-Logins	支持	2	整数	单值	0 到 2147483647
Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
Smart-Tunnel-Auto	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
Smart-Tunnel-Auto-Signon-Enable	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
Strip-Realm	支持	135	布尔值	单值	0 = 已禁用 1 = 已启用
SVC-Ask	支持	131	字符串	单值	0 = 已禁用 1 = 已启用 3 = 启用默认服务 认无客户端 （未使用 2 和 4）

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
SVC-Ask-Timeout	支持	132	整数	单值	5 到 120 秒
SVC-DPD-Interval-Client	支持	108	整数	单值	0 = 关 5-3600 秒
SVC-DPD-Interval-Gateway	支持	109	整数	单值	0 = 关） 5-3600 秒
SVC-DTLS	支持	123	整数	单值	0 = 错误 1 = 正确
SVC-Keepalive	支持	107	整数	单值	0 = 关 15-600 秒
SVC-Modules	支持	127	字符串	单值	字符串（模块的名称）
SVC-MTU	支持	125	整数	单值	MTU 值 256-1406 字节
SVC-Profiles	支持	128	字符串	单值	字符串（配置文件的名称）
SVC-Rekey-Time	支持	110	整数	单值	0 = 已禁用 1-10080 分钟
Tunnel Group Name	支持	146	字符串	单值	1 到 253 个字符
Tunnel-Group-Lock	支持	85	字符串	单值	隧道组的名称或“none”
Tunneling-Protocols	支持	11	整数	单值	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2T 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2) 互斥。 0 - 11、16 - 27、32 - 43、48 - 59 是合
Use-Client-Address		17	布尔值	单值	0 = 已禁用 1 = 已启用
VLAN	支持	140	整数	单值	0 到 4094
WebVPN-Access-List	支持	73	字符串	单值	访问列表名称
WebVPN ACL	支持	73	字符串	单值	设备上的 WebVPN ACL 的名称
WebVPN-ActiveX-Relay	支持	137	整数	单值	0 = 已禁用 Otherwise = 已启用
WebVPN-Apply-ACL	支持	102	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Auto-HTTP-Signon	支持	124	字符串	单值	保留
WebVPN-Citrix-Metaframe-Enable	支持	101	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Content-Filter-Parameters	支持	69	整数	单值	1 = Java ActiveX 2 = Java 脚本 4 = 映像 8 = 的 Cookie
WebVPN-Customization	支持	113	字符串	单值	自定义的名称
WebVPN-Default-Homepage	支持	76	字符串	单值	URL，例如 http://example-example.com

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-Deny-Message	支持	116	字符串	单值	有效字符串（最多 500 个字符）
WebVPN-Download_Max-Size	支持	157	整数	单值	0x7fffffff
WebVPN-File-Access-Enable	支持	94	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Browsing-Enable	支持	96	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-File-Server-Entry-Enable	支持	95	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	支持	78	字符串	单值	带可选通配符 (*) 的逗号分隔的 DNS/IP（ *.cisco.com、192.168.1.*、wwwin.cisco.co
WebVPN-Hidden-Shares	支持	126	整数	单值	0 = 无 1 = 可见
WebVPN-Home-Page-Use-Smart-Tunnel	支持	228	布尔值	单值	已启用（如果无客户端主页将通过智能隧道
WebVPN-HTML-Filter	支持	69	位图	单值	1 = Java ActiveX 2 = 脚本 4 = 映像 8 = C
WebVPN-HTTP-Compression	支持	120	整数	单值	0 = 关 1 = Deflate 压缩
WebVPN-HTTP-Proxy-IP-Address	支持	74	字符串	单值	逗号分隔的 DNS/IP:端口，带 http= 或 https 如 http=10.10.10.10:80、https=11.11.11.11:
WebVPN-Idle-Timeout-Alert-Interval	支持	148	整数	单值	0 到 30 0 = 已禁用。
WebVPN-Keepalive-Ignore	支持	121	整数	单值	0 到 900
WebVPN-Macro-Substitution	有	223	字符串	单值	无限制。
WebVPN-Macro-Substitution	有	224	字符串	单值	无限制。
WebVPN-Port-Forwarding-Enable	支持	97	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	支持	98	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-HTTP-Proxy	支持	99	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-Port-Forwarding-List	支持	72	字符串	单值	端口转发列表名称
WebVPN-Port-Forwarding-Name	支持	79	字符串	单值	字符串名称（例如，“Corporate-Apps”） 此文本将替换无客户端门户主页上的默认 “Application Access”。
WebVPN-Post-Max-Size	支持	159	整数	单值	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	支持	149	整数	单值	0 到 30 0 = 已禁用。

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN Smart-Card-Removal-Disconnect	支持	225	布尔值	单值	0 = 已禁用 1 = 已启用
WebVPN-Smart-Tunnel	支持	136	字符串	单值	智能隧道的名称
WebVPN-Smart-Tunnel-Auto-Sign-On	支持	139	字符串	单值	智能隧道自动登录名称列表（附带域名）
WebVPN-Smart-Tunnel-Auto-Start	支持	138	整数	单值	0 = 已禁用 1 = 已启用 2 = 自动启动
WebVPN-Smart-Tunnel-Tunnel-Policy	支持	227	字符串	单值	“e networkname”、“i networkname”或“a 一，其中 networkname 是指智能隧道网络列表 称，e表示不包含的隧道，i表示指定的隧道， 所有隧道。
WebVPN-SSL-VPN-Client-Enable	支持	103	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Keep- Installation	支持	105	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSL-VPN-Client-Required	支持	104	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SSO-Server-Name	支持	114	字符串	单值	有效字符串
WebVPN-Storage-Key	支持	162	字符串	单值	
WebVPN-Storage-Objects	支持	161	字符串	单值	
WebVPN-SVC-Keepalive-Frequency	支持	107	整数	单值	15 到 600 秒，0 = 关闭
WebVPN-SVC-Client-DPD-Frequency	支持	108	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-DTLS-Enable	支持	123	整数	单值	0 = 已禁用 1 = 已启用
WebVPN-SVC-DTLS-MTU	支持	125	整数	单值	MTU 值为 256 到 1406 个字节。
WebVPN-SVC-Gateway-DPD-Frequency	支持	109	整数	单值	5 到 3600 秒，0 = 关闭
WebVPN-SVC-Rekey-Time	支持	110	整数	单值	4 到 10080 分钟，0 = 关闭
WebVPN-SVC-Rekey-Method	支持	111	整数	单值	0（关闭）、1 (SSL)、2（新隧道）
WebVPN-SVC-Compression	支持	112	整数	单值	0（关闭）、1（Deflate 压缩）
WebVPN-UNIX-Group-ID (GID)	支持	222	整数	单值	有效 UNIX 组 ID
WebVPN-UNIX-User-ID (UID)	支持	221	整数	单值	有效 UNIX 用户 ID
WebVPN-Upload-Max-Size	支持	158	整数	单值	0x7fffffff
WebVPN-URL-Entry-Enable	支持	93	整数	单值	0 = 已禁用 1 = 已启用

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
WebVPN-URL-List	支持	71	字符串	单值	URL 列表名称
WebVPN-User-Storage	支持	160	字符串	单值	
WebVPN-VDI	支持	163	字符串	单值	设置列表

支持的 IETF RADIUS 授权属性

下表列出了支持的 IETF RADIUS 属性。

表 *2:* 支持的 *IETF RADIUS* 属性

属性名称	ASA	属性编号	语法/类型	单值或多值	说明或值
IETF-Radius-Class	支持	25		单值	对于 8.2.x 版本及更高版本，我们建议使用 Group-Policy 属性 (VSA 3076，#25)： • 组策略名称 • OU = 组策略名称 • OU = 组策略名称
IETF-Radius-Filter-Id	支持	11	字符串	单值	在 ASA 中定义的 ACL 名称，仅适用于全隧道 IPs 和 SSL VPN 客户端。
IETF-Radius-Framed-IP-Address	支持	n/a	字符串	单值	IP 地址
IETF-Radius-Framed-IP-Netmask	支持	n/a	字符串	单值	IP 地址掩码
IETF-Radius-Idle-Timeout	支持	28	整数	单值	秒
IETF-Radius-Service-Type	支持	6	整数	单值	秒。可能的 Service Type 值： • .Administrative - 允许用户访问配置提示符。 • .NAS-Prompt - 允许用户访问 exec 提示符。 • .remote-access - 允许用户访问网络
IETF-Radius-Session-Timeout	支持	27	整数	单值	秒

RADIUS 记帐连接断开原因代码

如果 ASA 在发送数据包时遇到连接断开问题，则会返回以下代码：

连接断开原因代码
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA 的 RADIUS 服务器准则

本节介绍您在配置用于 AAA 的 RADIUS 服务器之前应检查的准则和限制。

- 在单模式下可以有最多 200 个服务器组，在多模式下每个情景可以有 4 个服务器组。

- 在单模式下每个组可以有最多 16 个服务器，在多模式下每个组可以有 8 个服务器。
- RADIUS 负载的最大长度为 4096 字节。

配置用于 AAA 的 RADIUS 服务器

本节介绍如何配置用于 AAA 的 RADIUS 服务器。

过程

步骤 1 将 ASA 属性加载到 RADIUS 服务器。用于加载属性的方法取决于您使用的 RADIUS 服务器类型：

- 对于思科 ACS：服务器已集成这些属性。您可以跳过此步骤。
- 对于来自其他供应商的 RADIUS 服务器（例如 Microsoft 互联网身份验证服务）：必须手动定义每个 ASA 属性。要定义属性，请使用属性名称或编号、类型、值和供应商代码 (3076)。

步骤 2 配置 RADIUS 服务器组，第 13 页。

步骤 3 向组中添加 RADIUS 服务器，第 15 页。

步骤 4 （可选） 添加身份验证提示，第 17 页。

配置 RADIUS 服务器组

如果您要将外部 RADIUS 服务器用于身份验证、授权或记帐，则必须先为每个 AAA 协议创建至少一个 RADIUS 服务器组，然后向每个服务器组添加一个或多个服务器。

过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**。

步骤 2 在 **AAA Server Groups** 区域中，点击 **Add**。

系统将显示 **Add AAA Server Group** 对话框。

步骤 3 在 **AAA Server Group** 字段中输入组的名称。

步骤 4 从 **Protocol** 下拉列表中选择 RADIUS 服务器类型。

步骤 5 选择 **Accounting Mode**。

- **Simultaneous** - 将记帐数据发送到组中的所有服务器。
- **Single** - 仅将记帐数据发送到一个服务器。

步骤 6 配置用于重新激活组中出现故障的服务器的方法 (**Reactivation Mode**)。

- **Depletion**, **Dead Time** - 仅在组中的所有服务器都处于非活动状态后才重新激活出现故障的服务器。这是默认重新激活模式。指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时长（0 到 1440 分钟之间）。仅当配置回退到本地数据库时，失效时间时间才适用；身份验证将在本地尝试，直到失效时间结束。默认值为 10 分钟。
- **Timed** - 在 30 秒钟的停机时间后重新激活出现故障的服务器。

步骤 7 在**最大失败尝试次数**，指定会向组中带有 RADIUS 服务器的失败的 AAA 事务最大数量发送的请求的最大数量。

范围为 1 至 5。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，或者其响应无效，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（如果您使用默认重新激活模式和停顿时间）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要将无响应时段从默认值改为其他值，请参阅更改 **Dead Time**。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

步骤 8 （可选。）通过选择所需选项，启用 RADIUS 临时记帐更新消息的定期生成。

仅当您将此服务器组用于 Secure Client 或无客户端 SSL VPN 时，这些选项才相关。

- **Enable interim accounting update** - 如果您使用此命令而不选择 **Update Interval** 选项，则 ASA 仅会在将 VPN 隧道连接添加到无客户端 VPN 会话时发送临时记帐更新消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。
- **Update Interval** - 允许为每个被配置为向有关服务器组发送记帐记录的 VPN 会话定期生成和传输记帐记录。可以更改发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。

注释 对于包含 ISE 的服务器的服务器组，请同时选择这两个选项。ISE 将基于其从 NAS 设备（如 ASA）收到的记帐记录，保留一个活动会话的目录。不过，如果 ISE 为期 5 天没有接收到该会话仍处于活动状态的任何指示（记帐消息或终端安全评估事务处理），则它将删除从其数据库中删除该会话记录。为了确保长期VPN连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记帐更新消息。

步骤 9 （可选。）如果此组仅包含 AD 代理或思科目录代理 (CDA) 服务器，则请选择 **Enable Active Directory Agent Mode**。

CDA 或 AD 代理用于身份防火墙，而且并非全功能 RADIUS 服务器。如果选择此选项，则只能将此组用于身份防火墙用途。

步骤 10 （可选）如果您将此服务器用于远程访问 VPN 中的 ISE 策略实施，则请配置以下选项：

- **Enable dynamic authorization** - 为 AAA 服务器组启用 RADIUS 动态授权（ISE 授权更改，CoA）服务。当您在 VPN 隧道中使用服务器组时，RADIUS 服务器组将注册接收 CoA 通知，并且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口。仅当您在远程访问 VPN 中结合 ISE 使用此服务器组时，才能启用动态授权。

- **Dynamic Authorization Port** - 如果您启用动态授权，则可指定用于 RADIUS CoA 请求的侦听端口。默认值为 1700。有效范围为 1024 至 65535。
- **Use authorization only mode** - 如果您不想将 ISE 用于身份验证，请为 RADIUS 服务器组启用仅授权模式。这表示当此服务器组用于授权时，RADIUS 访问请求消息将会构建为“仅授权”请求，而不是为 AAA 服务器定义的已配置的密码方法。如果您为 RADIUS 服务器配置公用密码，则它将被忽略。

  例如，如果您想将证书用于身份验证而不是此服务器组，则应使用仅授权模式。您仍可将此服务器组用于授权和在 VPN 隧道中记帐。

步骤 11 （可选。）配置 **VPN3K Compatibility Option** 以指定是否应将从 RADIUS 数据包获得的可下载 ACL 与思科 AV 对 ACL 合并。

此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。

- **不合并** - 可下载 ACL 将不与思科 AV 对 ACL 合并。如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。这是默认选项。
- **Place the downloadable ACL after Cisco AV-pair ACL**
- **Place the downloadable ACL before Cisco AV-pair ACL**

步骤 12 点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并将新服务器组添加到 **AAA Server Groups** 表。

步骤 13 点击 **Apply** 以将更改保存到运行配置。

向组中添加 RADIUS 服务器

要向组中添加 RADIUS 服务器，请执行以下步骤：

过程

步骤 1 依次选择 **Configuration** > **Device Management** > **Users/AAA** > **AAA Server Groups**，然后在 **AAA Server Groups** 区域中，点击要向其添加服务器的服务器组。

步骤 2 在 **Servers in the Selected Group** 区域（下部窗格）中，点击 **Add**。

系统将为该服务器组显示 **Add AAA Server Group** 对话框。

步骤 3 选择身份验证服务器所在接口的名称。

步骤 4 为正添加到组中的服务器添加名称或 IP 地址。

步骤 5 指定与服务器的连接尝试超时值。

指定服务器的超时间隔（1-300 秒）；默认值为 10 秒。对于每个 AAA 事务，ASA 将重试连接尝试（基于重试间隔），直到达到超时。如果连续失败事务的数量达到 AAA 服务器组中指定的 maximum-failed-attempts 上限，则将会停用 AAA 服务器，并且 ASA 开始向另一台 AAA 服务器（如果已配置）发送请求。

步骤 6 指定您希望 ASA 如何处理可下载 ACL 中接收的网络掩码。从以下选项中选择：

- **Detect automatically** - ASA 尝试确定使用的网络掩码表达式的类型。如果 ASA 检测到通配符网络掩码表达式，ASA 会将其转换为标准网络掩码表达式。

  注释 由于难以明确检测这些通配符表达式，此设置可能会误将通配符网络掩码表达式当作标准网络掩码表达式。

- **Standard** - ASA 假定从 RADIUS 服务器接收的可下载 ACL 中仅包含标准网络掩码表达式。因而不会对通配符网络掩码表达式进行转换。
- **Wildcard** - ASA 假定从 RADIUS 服务器接收的可下载 ACL 中仅包含通配符网络掩码表达式，并会在下载 ACL 时将所有通配符网络掩码表达式转换为标准网络掩码表达式。

步骤 7 指定一个区分大小写的密码，该密码对于通过此 ASA 访问 RADIUS 授权服务器的用户是公用的。请务必将此信息提供给 RADIUS 服务器管理员。

注释 对于身份验证 RADIUS 服务器（而非授权服务器），请勿配置公用密码。

如果将此字段留空，则用户名即是用于访问此 RADIUS 授权服务器的密码。

请勿使用 RADIUS 授权服务器进行身份验证。公用密码或使用用户名作为密码不如指定唯一的用户密码安全。

虽然 RADIUS 协议和 RADIUS 服务器要求密码，但用户并不需要知道该密码。

步骤 8 如果在隧道组中使用双重身份验证并启用密码管理，则主身份验证请求和辅助身份验证请求包含 MS-CHAPv2 请求属性。如果 RADIUS 服务器不支持 MS-CHAPv2，则可以通过取消选中此复选框，将该服务器配置为发送非 MS-CHAPv2 的身份验证请求。

步骤 9 指定 ASA 在尝试联系服务器之间等待的时长，范围介于 1 到 10 秒之间。

注释 对于 RADIUS 协议，如果服务器回复“无法访问 ICMP 端口”消息，则系统会忽略 retry-interval 设置，并且 AAA 服务器会立即进入故障状态。如果这是 AAA 组中的唯一服务器，则会重新激活该服务器并向其发送另一个请求。这是预期行为。

步骤 10 点击 **Simultaneous** 或 **Single**。

在 Single 模式下，ASA 仅向一台服务器发送记账数据。

在 Simultaneous 模式下，ASA 将向组中的所有服务器发送记账数据。

步骤 11 指定用于用户记帐的服务器端口。默认端口为 1646。

步骤 12 指定用于用户身份验证的服务器端口。默认端口为 1645。

步骤 13 指定用于向 ASA 验证 RADIUS 服务器的共享密钥值。您配置的服务器密钥应与在 RADIUS 服务器中配置的密钥相匹配。如果您不知道服务器密钥，请询问 RADIUS 服务器管理员。最大字段长度为 64 个字符。

步骤 14 点击 **OK**。

系统将关闭 **Add AAA Server Group** 对话框，并会将 AAA 服务器添加到 AAA 服务器组。

步骤 15 在 **AAA Server Groups** 窗格中，点击 **Apply** 以将更改保存到运行配置。

添加身份验证提示

当要求通过 RADIUS 服务器进行用户身份验证时，您可以通过 ASA 为 HTTP、FTP 和 Telnet 访问指定质询文本。此文本是主要用于修饰目的，并且显示在用户登录时看到的用户名和密码提示符上方。如果不指定身份验证提示，则用户在使用 RADIUS 服务器进行身份验证时会看到以下信息：

连接类型	默认提示
FTP	FTP 身份验证
HTTP	HTTP 身份验证
Telnet	无

要添加身份验证提示，请执行以下操作：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **身份验证提示**。

步骤 2 在**Prompt**字段中输入文本，以将其添加为用户登录时看到的用户名和密码提示符上方显示的消息。

下表显示身份验证提示的允许字符数限制：

应用	字符限制
Microsoft Internet Explorer	37
Telnet	235
FTP	235

步骤 3 在 **User accepted message** 和 **User rejected message** 字段中添加消息。

如果通过 Telnet 进行用户身份验证，则可以使用 **User accepted message** 和 **User rejected message** 选项来显示不同的状态提示，以表明 RADIUS 服务器接受还是拒绝身份验证尝试。

如果 RADIUS 服务器对用户进行身份验证，则 ASA 会向用户显示 **User accepted message** 文本（如果指定）；否则，ASA 显示 **User rejected message** 文本（如果指定）。HTTP 和 FTP 会话的身份验

证仅在提示时才会显示质询文本。系统不会显示 **User accepted message** 和 **User rejected message** 文本。

步骤 4 点击 **Apply** 以将更改保存到运行配置。

测试 RADIUS 服务器身份验证和授权

要确认 ASA 是否能够联系 RADIUS 服务器并对用户进行身份验证或授权，请执行以下步骤：

过程

步骤 1 依次选择**配置** > **设备管理** > **用户/AAA** > **AAA 服务器组**。

步骤 2 在 **AAA Server Groups** 表中点击服务器所在的服务器组。

步骤 3 在 **Servers in the Selected Group** 表中点击要测试的服务器。

步骤 4 点击 **Test**。

系统将针对所选服务器显示 **Test AAA Server** 对话框。

步骤 5 点击要执行的测试的类型 - **Authentication** 或 **Authorization**。

步骤 6 输入用户名。

步骤 7 如果测试的是身份验证，请输入与用户名对应的密码。

步骤 8 点击 **OK**。

ASA 将向服务器发送身份验证或授权测试消息。如果测试失败，系统会显示错误消息。

为 AAA 监控 RADIUS 服务器

请参阅以下命令来为 AAA 监控 RADIUS 服务器的状态：

- **Monitoring > Properties > AAA Servers**

  此窗格显示 RADIUS 服务器运行配置。

- **Tools > Command Line Interface**

  您可以在此窗格中发出各种非交互式命令并查看结果。

用于 AAA 的 RADIUS 服务器历史记录

表 3: 用于 AAA 的 RADIUS 服务器历史记录

功能名称	平台版本	说明
用于 AAA 的 RADIUS 服务器	7.0(1)	说明如何配置用于 AAA 的 RADIUS 服务器。 引入了以下屏幕： Configuration > Device Management > Users/AAA > AAA Server Groups Configuration > Device Management > Users/AAA > Authentication Prompt。
在来自 ASA 的 RADIUS 访问请求和计费请求数据包中发送主要的供应商特有属性 (VSA)	8.4(3)	四个新 VSA - 通过来自 ASA 的 RADIUS 访问请求数据包发送 Tunnel Group Name (146) 和 Client Type (150)。通过来自 ASA 的 RADIUS 记帐请求数据包发送 Session Type (151) 和 Session Subtype (152)。为所有类型的记帐请求数据包（Start、Interim-Update 和 Stop）发送全部四个属性。RADIUS 服务器（例如 ACS 和 ISE）可以执行授权和策略属性，或者将这些属性用于记帐和收费。
每个组的 AAA 服务器组和服务器的数量上限都增加了。	9.13(1)	您可以配置更多 AAA 服务器组。在单情景模式下，您可以配置 200 AAA 服务器组（前一个限制为100）。在多情景模式下，您可以配置 8（前一个限制为4个）。 此外，在多情景模式下，您可以每组配置8个服务器（每个组的前一个限制为 4 个服务器）。单情景模式的每组限制 16，保持不变。 修改了 AAA 屏幕以接受这些新的限制。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。