DCYK 角色和策略手册

目录

修订记录

本文档修订内容列表.

修订	修订说明
Rev 01	初始发布

身份验证服务器

DCYKOS 软件允许您使用外部身份验证服务器或 Mobility Conductor 的内部用户数据库来验证需要访问无线网络的客户 端。

以下各节提供了 Mobility Conductor 身份验证服务器管理的一般概述:

- 了解身份验证服务器最佳实践和例外;
- 了解服务器和服务器组。

配置身份验证服务器和服务器组

以下主题介绍创建和管理外部和内部身份验证服务器和服务器组的过程。

- 配置身份验证服务器
- 管理内部数据库
- 配置服务器组
- 分配服务器组
- 配置身份验证计时器
- 认证服务器负载均衡
- 测试已配置的身份验证服务器

了解身份验证服务器最佳实践和例外

要使外部身份验证服务器处理来自 Mobility Conductor 的请求，必须将服务器配置为识别 Mobility Conductor。

了解服务器和服务器组

Mobility Conductor 支持以下外部身份验证服务器:

- RADIUS
- LDAP
- TACACS+
- Windows(用于有状态 NTLM 身份验证)

提示:最多可以在受管设备上配置 128 个 LDAP、RADIUS 和 TACACS 服务器，每个服务器都可以配置。

此外，还可以使用内部数据库通过为用户、其密码和默认角色创建条目来对用户进行身份验证。

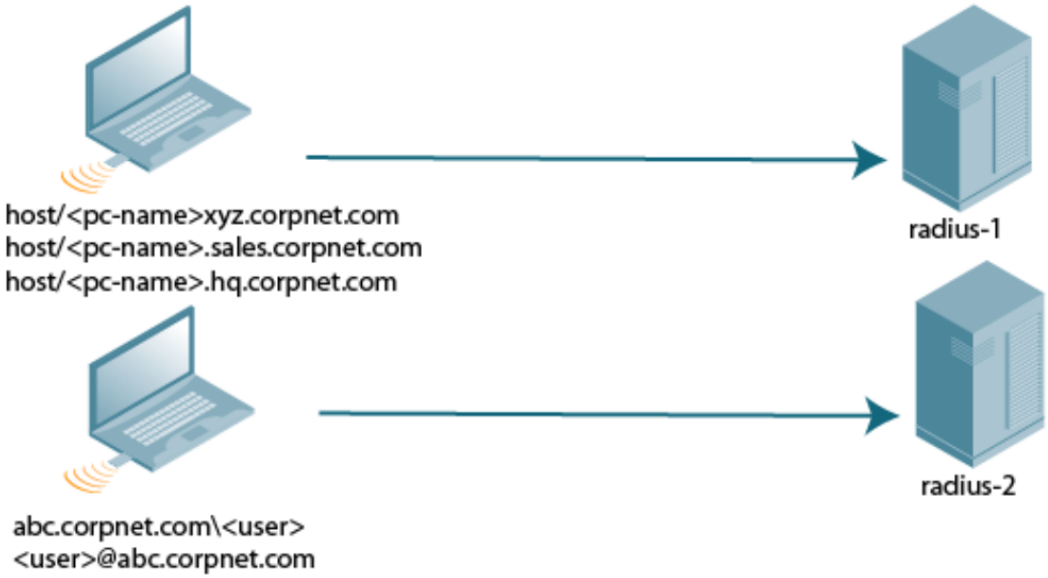
您可以为特定类型的身份验证创建服务器组。例如，您可以指定要用于 802.1X 身份验证的一个或多个 RADIUS 服务器。 服务器组中的服务器列表是有序列表。这意味着，除非列表中的第一台服务器不可用，否则将始终使用该服务器，在这种 情况下，将使用列表中的下一台服务器。

提示:如果在服务器组中配置内部服务器，则负载平衡不适用于内部服务器。当组中的所有其他服务器都关闭时，内部服务器将用作回退。

您可以在一个组中配置不同类型的服务器。例如，您可以将内部数据库作为 RADIUS 服务器的备份包含在内。

表示一个名为“Radii”的服务器组，该服务器组由两个 RADIUS 服务器 Radius-1 和 Radius-2 组成。服务器组分配给用于 802.1X 身份验证的服务器组。

服务器组



服务器名称是唯一的。您可以在多个服务器组中配置同一台服务器。必须先配置服务器，然后才能将其添加到服务器组。

提示:如果使用内部数据库进行用户身份验证，请使用预定义的“内部”服务器组。

您还可以在服务器组配置中包括服务器派生用户角色或 VLAN 的条件。服务器派生规则适用于组中的所有 服务器。

配置身份验证服务器

本节介绍如何配置 RADIUS、LDAP、TACACS+ 和 Windows 外部身份验证服务器和内部数据库。

本部分包括以下信息:

- 配置 RADIUS 服务器
- RADIUS 服务类型属性
- RADIUS 服务器上启用 Radsec
- ClearPass Policy Manager 身份验证的配置用户名和密码
- 配置 RFC-3576 RADIUS 服务器
- 配置 LDAP 服务器

- 配置 TACACS+服务器
- 配置 Windows Server

配置 RADIUS 服务器

以下过程介绍如何配置 RADIUS 服务器:

1.在“托管网络”节点层次结构中，导航到“配置>身份验证”>“身份验证服务器”选项卡。

2.在“所有服务器”表中，单击“+”添加新服务器。配置以下参数:

a. ”名称-输入新服务器的名称。

b. "IP 地址/主机名一输入新服务器的 IP 地址/主机名。

c. 类型-将服务器类型设置为 RADIUS。

3.点击提交。

4.在“所有服务器”(All Servers) 表中，选择为配置服务器参数而创建的服务器。

5.输入参数。选中“模式”复选框以激活身份验证服务器。

6.点击提交。

7.单击“挂起的更改”。

8.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

提示:/mm 节点下的 Mobility Conductor 上的 RADIUS 配置仅用于 Mobility Conductor 上的管理身份验证，而不用于用户 或设备(有线或无线)身份验证。/mm 节点下的配置仅推送到冗余 Mobility Conductor 中，而不推送到受管设备。应在/md 节点上或/md 节点下为客户端或受管设备配置 RADIUS 服务器。

以 下 CLI 命令配置 RADIUS 服务器:

```
(host) [mynode] (config) #aaa authentication-server radius <name>
    host <ipaddr>
    key <psk>
    Enable
```

参数说明	描述
Name	RADIUS 服务器的名称。

IP 地址/ 主机名	身份验证服务器的 IP 地址或 FQDN。支持的最大 FQDN 长度为 63 个字符。默认值： N/A
身份验证端口	此服务器的身份验证端口。默认值：1812
计费端口	此服务器的记帐端口。默认值：1813
共享密钥	受管设备和身份验证服务器之间的共享密钥。 最大长度为 128 个字符。默认值：N/A
重新键入键	重新输入共享密钥。
超时	受管设备在超时请求并重新发送请求之前等待的最长时间(以秒为单位)。范围：1-120 秒 默认值：5 秒
重新传输	在服务器标记为关闭之前，受管设备发送到服务器的最大重试次数。默认值：3
NAS ID	用于 RADIUS 数据包的 NAS 标识符。
NAS IP	要从该服务器以 RADIUS 数据包形式发送的 NAS IP 地址。 如果使用“配置”>“安全性”>“身份验证>服务器”页面定义本地 NAS IP,并使 用“配置>安全性”>“身份验证>高级”页面定义全局 NAS IP,则全局 NAS IP 地址优 先。
启用 IPv6	为此服务器启用或禁用 IPv6。默认值：禁用
NAS IPv6	要在 RADIUS 数据包中发送的 NAS IPv6 地址。
使用 MD5	使用明文密码的 MD5 哈希。默认值：禁用
Mode	启用或禁用服务器。默认值：已启用
小写 MAC 地址	将身份验证和记帐请求中的小写 MAC 地址发送到此服务器。默认值：禁用
将 IP 地址用于呼叫站 ID	启用或禁用使用呼叫站 ID 的 IP 地址。默认值：禁用

MAC 地址分隔符	在身份验证中使用以下分隔符发送 MAC 地址，并且 此服务器的记帐请求： ● colon：发送 MAC 地址为 XX:XX:XX:XX:XX:XX " ● dash:发送 MAC 地址为 XX-XX-XX-XX-XX-XX ● none:将 MAC 地址发送为 XXXXXXXXXXXX ● oul-nlc:发送 MAC 地址为 XXXXXX-XXXXXX 默认值：无
FRAMED-USER 的服务类型	将服务类型发送为 FRAMED-USER 而不是 LOGIN-USER。有关详细信息，请参阅第 195 页的 RADIUS 服务类型属性。默认值：禁用
CPPM 凭据	使用 ClearPass Policy Manager 服务器身份验证。
CPPM 用户名	输入 ClearPass Policy Manager 用户名。
CPPM 密码	输入 ClearPass Policy Manager 密码。
重新输入密码	重新输入 ClearPass Policy Manager 密码。
工作站 ID 类型	选择要使用 RADIUS 属性发送的以下工作站 ID 类型之一，即身份验证和记帐请求的被叫 工作站 ID: ● AP 组 ● APMAC 地址 ● AP 名称 ● IP 地址 ● MAC 地址 ● VLAN ID
工作站 ID 分隔符	选择以下分隔符选项之一: ● Colon ● Dash ● None
包括 SSID	选中该复选框以在被叫站 ID 属性中包含 SSID 名称。

RADIUS 服务类型属性

托管设备为 RADIUS 身份验证请求发送以下服务类型属性值。

RADIUS 服务类型属性

RADIUS 属性	身份验证类型	属性值
服务类型	MAC	Call-Check
	802.1X	Framed
	Captive Portal	Login

无论身份验证类型如何，RADIUS 服务器的 service-type-framed-user 配置都会将所有属性值覆盖到 Framed。依赖于 此属性进行第三方 RADIUS 集成的现有部署应进行更改以支持这些新服务类型。

在 RADIUS 服务器上启用 Radsec

传统的 RADIUS 协议提供有限的安全性。对于在不安全的网络(如 Internet) 上进行的身份验证，这种有限的安全级别 是不够的。为了解决这个问题，引入了 RADIUS over TLS 或 Radsec 增强功能，以确保 RADIUS 身份验证和记帐数据在 不安全的网络中安全可靠地传输。RADIUS over TLS 的默认目标端口是 TCP/2083。单独的端口不用于身份验证、记帐和 动态授权更改。

在 TLS 连接中，受管设备 (TLS 客户端)和 Radsec 服务器 (TLS 服务器)都需要使用证书相互验证。对于要对 Radsec 服务器进行身份验证的受管设备：

- 如果 Radsec 服务器使用由 CA 签名的证书，则 CA 证书应作为受信任的 CA 上传。
- 如果 Radsec 服务器使用自签名证书，则应将自签名证书作为 PublicCert 上传。

提示:如果这两个证书均未配置，则受管设备不会尝试与 Radsec 服务器建立任何连接，即使启用了 Radsec。

受管设备还必须将 TLS 客户端证书发送到 Radsec 服务器，方法是将 Mobility Conductor 上的证书作为 ServerCert 上 传，并将 Radsec 配置为接受和使用该证书。如果未配置证书，Mobility Conductor 将在其 TPM 中使用设备证书。在这种情况下，签署证书的神州云科设备 CA 应配置为 Radsec 服务器上的受信任 CA。

提示:启用 Radsec 支持后，默认 RADIUS 共享密钥为 radsec,即使用户配置了不同的共享密

钥，该密钥也保持不变。

以下 CLI 命令在 RADIUS 服务器上配置 Radsec:

```
(host) [mynode] (config) #aaa authentication-server radius <rad_server_name>
    enable-radsec
    radsec-client-cert-name <name>
    radsec-port <radsec-port>
    radsec-trusted-cacert-name <radsec-trusted-ca>
    radsec-trusted-servercert-name <name>
```

RADIUS 服务器 VSA

VSA 是一种在网络访问服务器和 RADIUS 服务器之间通信供应商特定信息的方法，允许供应商支持自己的扩展属性。您可 以使用神州云科 VSA 为经过 RADIUS 身份验证的客户端派生用户角色和 VLAN; 但是，VSA 必须存在于 RADIUS 服务器上。

这要求您使用供应商名称 (神州云科) 和/或特定于供应商的代码(14823)、供应商分配的属性编号以及每个 VSA 的属性 格式(如字符串或整数)更新 RADIUS 字典文件。

从 DCYKOS 8.4.0.0 开始，RADIUS 服务器 VSA 支持神州云科-Captive-Portal-VSA 属性。

有关当前在 Mobility Conductor 上运行的 ArubaOS 版本中可用的所有 RADIUS VSA 的当前完整列表，请访问命令行界面并发出命令 show aaa radius-attributes。

通过 COA （RFC3576）可接收更新以下的 VSA 属性

Value	Description	Data Type	Reference
1	User-Name	text	[RFC2865]
2	User-Password	string	[RFC2865]
3	CHAP-Password	string	[RFC2865]
4	NAS-IP-Address	ipv4addr	[RFC2865]
5	NAS-Port	integer	[RFC2865]
6	Service-Type	enum	[RFC2865]
7	Framed-Protocol	enum	[RFC2865]
8	Framed-IP-Address	ipv4addr	[RFC2865]

9	Framed-IP-Netmask	ipv4addr	[RFC2865]
10	Framed-Routing	enum	[RFC2865]
11	Filter-Id	text	[RFC2865]
12	Framed-MTU	integer	[RFC2865]
13	Framed-Compression	enum	[RFC2865]
14	Login-IP-Host	ipv4addr	[RFC2865]
15	Login-Service	enum	[RFC2865]
16	Login-TCP-Port	integer	[RFC2865]
17	Unassigned		
18	Reply-Message	text	[RFC2865]
19	Callback-Number	text	[RFC2865]
20	Callback-Id	text	[RFC2865]
21	Unassigned		
22	Framed-Route	text	[RFC2865]
23	Framed-IPX-Network	ipv4addr	[RFC2865]
24	State	string	[RFC2865]
25	Class	string	[RFC2865]
26	**Vendor-Specific**	**vsa**	**[RFC2865]**
27	Session-Timeout	integer	[RFC2865]
28	Idle-Timeout	integer	[RFC2865]
29	Termination-Action	enum	[RFC2865]
30	Called-Station-Id	text	[RFC2865]
31	Calling-Station-Id	text	[RFC2865]
32	NAS-Identifier	text	[RFC2865]
33	Proxy-State	string	[RFC2865]
34	Login-LAT-Service	text	[RFC2865]
35	Login-LAT-Node	text	[RFC2865]
36	Login-LAT-Group	string	[RFC2865]

37	Framed-AppleTalk-Link	integer	[RFC2865]
38	Framed-AppleTalk-Network	integer	[RFC2865]
39	Framed-AppleTalk-Zone	text	[RFC2865]
40	Acct-Status-Type	enum	[RFC2866]
41	Acct-Delay-Time	integer	[RFC2866]
42	Acct-Input-Octets	integer	[RFC2866]
43	Acct-Output-Octets	integer	[RFC2866]
44	Acct-Session-Id	text	[RFC2866]
45	Acct-Authentic	enum	[RFC2866]
46	Acct-Session-Time	integer	[RFC2866]
47	Acct-Input-Packets	integer	[RFC2866]
48	Acct-Output-Packets	integer	[RFC2866]
49	Acct-Terminate-Cause	enum	[RFC2866]
50	Acct-Multi-Session-Id	text	[RFC2866]
51	Acct-Link-Count	integer	[RFC2866]
52	Acct-Input-Gigawords	integer	[RFC2869]
53	Acct-Output-Gigawords	integer	[RFC2869]
54	Unassigned		
55	Event-Timestamp	time	[RFC2869]
56	Egress-VLANID	integer	[RFC4675]
57	Ingress-Filters	enum	[RFC4675]
58	Egress-VLAN-Name	text	[RFC4675]
59	User-Priority-Table	string	[RFC4675]
60	CHAP-Challenge	string	[RFC2865]
61	NAS-Port-Type	enum	[RFC2865]
62	Port-Limit	integer	[RFC2865]
63	Login-LAT-Port	text	[RFC2865]

带宽 VSA

从 ArubaOS 8.2.0.0 开始，受管设备可以根据 RADIUS 服务器的方向，在第 3 层身份验证客户端上动态分配每用户或每 组带宽速率。为了指示受管设备在强制网络门户身份验证成功后对特定客户端强制实施带宽速率，将在 RADIUS 访问-接 受数据包中添加三个名为 Bandwidth-VSA 的 RADIUS 供应商特定属性。

带宽 VSA

VSA	类型	Value	描述
Nomadix-Group-Bw-Policy-ID	整数	19	将每个客户端设置为零，否则将每个组的 group-ID 设置为零。
WISPr-Bandwidth-Max-Up	整数	7	上行带宽速率(以比特/秒为单位)。
WISPr-Bandwidth-Max-Down	整数	8	下行带宽速率(以比特/秒为单位)。
Vendor ID	整数	8	供应商的 ID。

服务器重定向带宽控制功能仅支持 D 隧道和控制器有线客户端。

以下 CLI 命令检查当前分配的动态带宽协定：

```
(host) # show aaa bandwidth-contracts dynamic
```

自定义 RADIUS 属性

从 ArubaOS8.1.0.0 开始，用户现在可以配置 RADIUS 修饰符配置文件，以自定义 RADIUS 请求中包含、排除和修改的属性，然后再将其发送到身份验证服务器。RADIUS 修饰符配置文件可以配置并应用于 RADIUS 身份验证或记帐服务器上的 AccessRequest 或 Accounting-Request 或两者。

此配置文件最多可以包含 64 个具有静态值的 RADIUS 属性，这些属性用于在请求中添加或更新，另外 64 个 RADIUS 属性要从请求中排除。

在 RADIUS 修改器配置文件中添加了两个新参数：

- auth-modifier:分配时，它引用 RADIUS 修饰符配置文件，该配置文件应用于发送到此 RADIUS 身份验证服务器的所有访问请求。

- acct-modifier:分配时，它引用 RADIUS 修饰符配置文件，该配置文件应用于发送到此 RADIUS 记帐服务器的 所有记帐请求。

您可以创建 RADIUS 修饰符配置文件，以自定义 RADIUS 请求中包含、排除和修改的属性，然后再将其发送到身份验 证或记帐服务器。

以下过程介绍如何创建 RADIUS 修饰符配置文件并自定义 RADIUS 属性：

1.在 Mobility Conductor 节点层次结构中，导航到配置>系统>配置文件选项卡。

2.在“所有配置文件”下，展开“无线局域网”。

3.单击 Radius Modifier。

4.在“半径修改器配置文件：新建配置文件”下，单击“+”添加半径修改器配置文件。

- 配置文件名称 (Profile name)-输入配置文件的名称。

5.在“+属性”字段中，单击“+”,然后从“名称”下拉列表框中选择一个名称，然后将“类型”设置为“静态”，然后输入 Static_val。单击“确定”。当我们配置命令时，name 字段应该在属性列表中可用，show aaa radius-attribute 命令。

6.在-Attr 字段中，单击+,然后选择要从-attr 下拉列表框中排除的属性的名称，然后单击确定。

7.点击提交。

8.单击“挂起的更改”。

9.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令创建 RADIUS 修饰符配置文件并自定义 RADIUS 属性：

```
(host) [md] (config) #aaa authentication-server radius radius1

(host) [md] (RADIUS Server "radius1) #

acct-modifier

acctport

auth-modifier

authport

...

...

(host) [md] (config) #aaa radius modifier <profile_name>

clone
```

exclude

include

no

(host) [md] #show aaa radius modifier <profile_name>

动态数据支持

从 ArubaOS 8.2.0.0 开始，支持对 RADIUS 属性修饰符中包含的属性的动态数据的支持。用户可以将 RADIUS 修饰符 中包含的每个属性的动态值配置为一个或两个数据项。可以选择以下数据项来形成每个包含属性的动态值:

- AP-Name:客户端当前关联的 AP 的名称。
- AP-MAC-Address:客户端当前关联的 AP 的 MAC 地址。
- AP-Group: 客户端当前关联的 AP 的组名。
- ESSID:客户端当前关联到的 ESSID。

Field1 和 Field2 具有相同的值，但这些值可用于与分隔符的不同组合。此包含的属性类型为 String,最多可包含 128 个字节。

以下过程介绍如何使用单项动态数据配置 RADIUS 修饰符配置文件:

1.在 Mobility Conductor 节点层次结构中，导航到配置>Systems> 配置文件选项卡。

2.在“所有配置文件”下，展开“无线局域网”。

3.单击 Radius Modifier。

4.在“半径修改器配置文件: 新建配置文件”中，单击“+”添加新的半径修改器配置文件。

- 配置文件名称 (Profile name)-输入配置文件的名称。

5.单击“+Attr”字段中的“+”,然后从“名称”下拉列表中选择一个名称，然后将“类型”设置为“动态”。

6.从 D_field1 下拉列表中选择第一个动态字段。

7 . (可选)从 D_field2 下拉列表中选择第二个动态字段。

8. 从 D_delimiter 下拉列表中选择分隔符。

9.单击“确定”。

10.点击提交

11.单击“挂起的更改”。

12.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令使用单项动态数据配置 RADIUS 修饰符配置文件:

(host)(config) #aaa radius modifier dynamic-mod

(host) (Radius Modifier Profile "dynamic-mod") #?

clone Copy data from another Radius Modifier Profile

exclude Attribute to be excluded in RADIUS request

include Attribute/Value to be included in RADIUS request

no Delete Command

(host) (Radius Modifier Profile "dynamic-mod") #include ?

<name> RADIUS Attribute Name

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id ?

dynamic First dynamic field

static Static Data

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic ?

ap-group1 Use AP group as first dynamic field

ap-macaddr1 Use AP mac address as first dynamic field

ap-name1 Use AP name as first dynamic field

essid1 Use essid as first dynamic field

user-vlan1 Use user's current VLAN-ID as first dynamic field

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic ap-

name1

To configure a RADIUS modifier profile with two-item dynamic data

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic ?

ap-group1 Use AP group as first dynamic field

ap-macaddr1 Use AP mac address as first dynamic field

ap-name1 Use AP name as first dynamic field

essid1 Use essid as first dynamic field

user-vlan1 Use user's current VLAN-ID as first dynamic field

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic essid1

?

with Optional second dynamic field

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic essid1

with ?

ap-group2 Use AP group as second dynamic field

ap-macaddr2 Use AP mac address as second dynamic field

ap-name2 Use AP name as second dynamic field

essid2 Use essid as second dynamic field

user-vlan2 Use user's current VLAN-ID as first dynamic field

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic essid1

with ap-macaddr2 ?

delimiter Delimiter between fields

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic essid1

with ap-macaddr2 delimiter ?

at Use '@' as delimiter between fields

colon Use ':' as delimiter between fields

dash Use '-' as delimiter between fields

dollar Use '$' as delimiter between fields

hash Use '#' as delimiter between fields

none NULL

percent Use '%' as delimiter between fields

semicolon Use ';' as delimiter between fields

slash Use '/' as delimiter between fields

space Use ' ' as delimiter between fields

(host) (Radius Modifier Profile "dynamic-mod") #include Aruba-Location-Id dynamic essid1

with ap-macaddr2 delimiter at ?

以下 CLI 命令显示了混合了静态和动态数据的 RADIUS 修饰符配置文件:

(host) (config) #show aaa radius modifier dynamic-mod

Radius Modifier Profile

Action Attribute Name Data Type Data Value

------ -------------- --------- ----------

+Attr Aruba-Location-Id dynamic essid1 with ap-macaddr2 delimiter at

+Attr BW-Area-Code static "212"

+Attr BW-City-Name static "San Jose"

+Attr Aruba-AP-Group dynamic ap-group1

-Attr Aruba-Device-Type

动态分配 VLAN-ID 到 NAS 端口

以下 CLI 命令配置 RADIUS 修饰符，以将客户端的 VLAN-ID 分配给 NAS-Port RADIUS 属性：

(host) [mode] (config) # aaa radius modifier "Hilton-Eleven"

include "NAS-Port-ID" dynamic user-vlan1

!

以下 CLI 命令将 RADIUS 修饰符分配给 RADIUS 身份验证服务器：

(host) [mode] (config) #aaa authentication-server radius "eleven-server"

.....

auth-modifier "Hilton-Eleven"

.....

!

RADIUS 服务器验证码

配置的 RADIUS 服务器返回以下标准响应代码。

RADIUS 身份验证响应代码

代码	描述
0	身份验证正常。
1	身份验证失败：用户/密码组合不正确
2	身份验证请求超时：服务器无响应。
3	内部身份验证错误。
4	来自 RADIUS 服务器的错误响应：验证共享密钥是否正确。

5	未配置 RADIUS 身份验证服务器。
6	来自服务器的质询(这并不一定表示错误情况)。

RADIUS 服务器完全限定域名

如果使用服务器的 FQDN 而不是其 IP 地址定义 RADIUS 服务器，则受管设备会定期生成 DNS 请求并缓存 DNS 响应中返回的 IP 地址。要查看当前与每个 RADIUS 服务器 FQDN 关联的 IP 地址，请在配置模式下访问命令行界面，然后发出 show aaa fqdn-server-names 命令。

DNS 查询间隔

如果使用服务器的 FQDN 而不是其 IP 地址定义 RADIUS 服务器，则受管设备会定期生成 DNS 请求并缓存 DNS 响应中返回的 IP 地址。

默认情况下，DNS 请求每 15 分钟发送一次。

可以使用 WebUI 或 CLI 来配置生成 DNS 请求的频率，以缓存通过其 FQDN 标识的 RADIUS 服务器的 IP 地址。

以下过程介绍如何配置 DNS 查询间隔：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>“高级”页面。

2.展开 DNS 查询间隔可折叠，在 DNS 查询间隔(分钟)字段中输入 1-1440 分钟的新 DNS 查询间隔。

3.点击提交。

4.单击“挂起的更改”。

5.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置 DNS 查询间隔：

```
(host) [mynode] (config) #aaa dns-query-interval <minutes>
```

配置 ClearPass Policy Manager 身份验证的用户名和密码

增强了对 ClearPass Policy Manager 的身份验证，以使用可配置的用户名和密码而不是支持密码。由于 ClearPass Policy Manager 服务器提供的服务器证书未经过验证，因此支持密码容易受到攻击。

配置 RFC-3576 RADIUS 服务器

您可以将 RADIUS 服务器配置为发送用户断开连接、CoA 和会话超时消息，如 RFC3576“远程拨入用户服务 (RADIUS)的动态授权扩展”中所述。

对于远程 AP,RADIUS CoA 仅在隧道和拆分隧道转发模式下受支持。

对于园区 AP,RADIUS CoA 仅在隧道和解密隧道转发模式下受支持。

从服务器发送到受管设备的断开连接、会话超时和 CoA 消息包含用于标识消息发送对象的用户的信息。从 ArubaOS8.5.0.0 开始，受管设备还接受来自基于 IPv6 地址的 DAC 的断开连接、会话超时和 CoA 请求，并根据用户的 IPv6 地址识 别用户会话。Mobility Conductor 支持以下属性，用于标识使用 RFC 3576 服务器进行身份验证的用户：

- user-name: 要认证的用户的名称
- framed-ip-address:用户 IPv4 地址
- framed-ipv6-address:用户 IPv6 地址
- calling-station-id:发起呼叫的工作站的电话号码
- accounting-session-id:用户会话的唯一记帐 ID。

IPv4 地址在标识用户会话方面比 IPv6 地址具有更高的优先级。

如果身份验证服务器将受支持和不支持的属性发送到受管设备，则将忽略未知或不支持的属性。如果未找到匹配的用户，则 会将 503:未找到会话错误消息发送回 RFC 3576 服务器。

以下过程介绍如何配置 RFC-3576 RADIUS 服务器：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.要定义新的 RFC3576 RADIUS 服务器，请单击“所有服务器”下的“+”。配置以下参数：

- 类型—从下拉列表中选择动态授权。
- IP 地址版本-根据您的偏好选择 IPv4 或 IPv6 单选按钮。
- IP 地址-输入 IPv4 或 IPv6 地址。

3.点击提交。

4.从“所有服务器”列表中，选择您创建的服务器来配置服务器参数。

5.在“服务器选项”下，在“密钥”和“重新键入密钥”字段中输入服务器身份验证密钥。

6.点击提交。

7.单击“挂起的更改”。

8.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置 RFC-3576 RADIUS 服务器:

```
(host) [mynode] (config) #aaa rfc-3576-server <ipaddr>
clone <source>
key <psk>
no ..
```

使用 Radsec 配置 RFC 3576 RADIUS 服务器

从 ArubaOS 8.2.0.0 开始，RFC 3576 中的新增强功能将使来自 RADIUS 服务器和受管设备的断开连接请求之间的通信更 加全面。此版本还支持检测来自 RADIUS 服务器的重复断开连接请求。此更改可确保:

1.系统不易受到数据包重放攻击。

2.受管设备不会多次处理来自 RADIUS 服务器的重复断开连接请求。

从 ArubaOS 8.5.0.0 开始，您还可以使用 IPv6 地址配置带有 Radsec 的 RFC3576 RADIUS 服务器。

以下 CLI 命令使用 Radsec 配置 RFC 3576 RADIUS 服务器:

```
(host) [mynode] (config) #aaa rfc-3576-server <ipaddr>
clone <source>
enable-radsec
event-timestamp-requi..
key <psk>
no ...
replay-protection
window-duration
enable-radsec
no ...
```

RFC 5176 中引入了以下增强功能:

状态属性

状态属性是 CoA 请求的一部分，而不是断开连接请求的一部分。断开来自 RADIUS 服务器的请求具有许多可选属性，

服务类型属性就是这样一种属性。如果此属性的值为“仅授权”,则 RFC 5176 已强制要求在断开连接请求中具有状态 属性，如果缺少状态属性，则报告错误原因 402。

错误原因 407

RFC 5176 为断开连接请求响应引入了这个新的错误原因。407-通知 DAC 与任何属性关联的无效属性值。

重复请求检测

断开连接请求检测来自同一 RADIUS 服务器 IP 地址或源端口的重复请求，适用于具有相同序列号的数据包。可以配置来自 同一源的两个断开连接请求之间的最小时间跨度，并且此时间窗口内的任何两个请求都被视为重复请求，这将被拒绝。

服务类型属性：仅授权

如 果 Network Access Service 收到来自 Dynamic Authorization Client 的断开连接请求，并且 service-type 属性为 Authorize Only,则 Network Access Service 应向动态授权客户端发送动态授权客户端否定确认，因为 service-type 属性只能是 CoA 请求的一部分，而不能是断开连接请求的一部分。

配置 LDAP 服务器

下表描述了您为 LDAP 服务器配置的参数。

LDAP 服务器配置参数

参数	说明
Host	LDAP 服务器的 IP 地址。默认值： N/A
管理员-dn	对 LDAP 数据库中的所有条目具有读取/搜索权限的管理员用户的可分辨名称(用户确实需要写入权限，但能够搜索数据库，并读取数据库中其他用户的属性)。
admin-passwd	管理员用户的密码。 默认值：NAAN
重新输入 admin-passwd	重新输入管理员密码。

允许明文	允许与 LDAP 服务器进行明文(未加密)通信。 默认值：禁用
身份验证端口	用于身份验证的端口号。默认值：389
Base-dn	包含整个用户数据库的节点的可分辨名称。默认值：N/A
Filter	字符串在 LDAP 数据库中搜索用户。默认筛选器字符串为：(objectclass=*)。 默认值：N/A
键属性	字符串搜索 LDAP 服务器。对于 Active Directory,该值为 sAMAccountName。 默认值：sAMAccountName
超时	LDAP 请求的超时期限(以秒为单位)。默认值：20 秒
Mode	启用或禁用服务器。默认值： enabled
首选连接类型	受管设备和 LDAP 服务器之间的首选连接类型。连接类型的默认顺序为： 1.明文 2.ldap-s 3.start-tls 受管设备首先尝试使用首选连接类型联系 LDAP 服务器，并且仅在第一次尝试不成功时才 尝试使用优先级较低的连接类型。 注意：如果选择明文作为首选连接类型，则还必须启用允许明文选项。
最大非管理员连接数量	配置与服务器的最大非管理员连接数。默认值：4
Chase 推荐	Chase 匿名推荐。

以下过程介绍如何配置 LDAP 服务器：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.要配置 LDAP 服务器，请单击“所有服务器”下的“+”。配置以下参数：

- 名称-输入服务器的名称。

- IP 地址—设置服务器的 IP 地址。
- 类型-将服务器类型设置为 Ldap。

3.点击提交。

4.选择为配置服务器参数而创建的服务器的名称。输入如上表所示的参数。选中“模式”复选框以激活身份验证服务器。

5.点击提交。

6.单击“挂起的更改”。

7.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

在执行此步骤之前，配置不会生效。

以下 CLI 命令配置 LDAP 服务器:

(host) [mynode] (config) #aaa authentication-server ldap <name>

host <ipaddr>

(enter parameters as described in Table 35)

enable

配置 TACACS+服务器表

下表定义了 TACACS+服务器参数。

TACACS+服务器配置参数

参数	说明
Host	服务器的 IP 地址。默认值： N/A
Key	用于验证 TACACS+客户端和服务器之间通信的共享密钥。默认值：N/A
重新键入密钥	重新输入密钥。
TCP 端口	服务器使用的 TCP 端口。默认 值：49
重新传输	请求的最大重试次数。默认值：3
超时	TACACS+请求的超时期限，以秒为单位。默认值：20 秒

Mode	启用或禁用服务器。默认值：enabled
会期授权	启用或禁用会话授权。会话授权为管理员用户启用可选授权会话。默认值：禁用

以下过程介绍如何配置 TACACS+服务器：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.要配置 TACACS+服务器，请单击“所有服务器”下的“+”。配置以下参数：

- 名称-输入服务器的名称。
- IP 地址/主机名—设置服务器的 IP 地址/主机名。
- 类型-将服务器类型设置为 TACACS。

3.选择创建的服务器以配置服务器参数。输入如表 36 所示的参数。选中“模式”复选框以激活身份验证服务器。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

在执行此步骤之前，配置不会生效。

以下 CLI 命令配置 TACACS+ 服务器和会话授权：

```
(host) [mynode] (config) #aaa authentication-server tacacs <name>

clone default

host <ipaddr>

key <psk>

enable

session-authorization
```

配置 Windows Server

下表定义了用于有状态 NTLM 身份验证的 Windows 服务器的参数。

Windows Server 配置参数

参数	说明

Host	服务器的 IP 地址。默认值： N/A
Mode	启用或禁用服务器。默认值： enabled
Windows Domain	分配给服务器的 Windows 域名。

以下过程介绍如何配置 Windows 服务器:

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.若要配置 Windows 服务器，请单击“所有服务器”下的“+”。配置以下参数:

- 名称-输入服务器的名称。
- IP 地址/主机名—设置服务器的 IP 地址/主机名。
- 类型-将服务器类型设置为 Windows。

3.选择创建的服务器以配置服务器参数。输入如上表所示的参数。

4.选中“模式”复选框以激活身份验证服务器。

5.点击提交。

6.单击“挂起的更改”。

7.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

在执行此步骤之前，配置不会生效。

以下 CLI 命令配置 Windows 服务器:

```
(host) [mynode] (config) #aaa authentication-server windows <windows-server-name>
    host <ipaddr>
    enable
```

使用强制 portal 验证配置 MAC 身份验证

以下配置条件适用于 MAC +强制 portal 身份验证方法:

如果强制门户启动页面类型为“内部认证”或“外部 RADIUS 服务器”，则 MAC 认证将重用服务器配置。

如果强制 portal 启动页面类型为“内部确认”或“外部身份验证文本”，并且启用了 MAC 身份验证，则会显示服务器配置页面。

您可以使用 WebUI 或 CLI 为网络配置文件配置带有强制 portal 身份验证的 MAC 身份验证。

在 WebUI 中

1.在配置>网络部分中，单击+以创建新的网络配置文件或选择现有配置文件，为其配置 WLAN SSID 或有线配置文件的内部强制 portal 身份验证，然后单击编辑。

要在新的 WLAN SSID 或有线配置文件上启用带有强制 portal 身份验证的 MAC 身份验证，请单击“创建新网络”窗口上的“安全”选项卡。

2.选择“安全”选项卡并指定以下参数：

a.开启 MAC 认证开关，开启强制 portal 用户的 MAC 认证，如果 MAC 认证失败，则将强制 portal 认证角色分配给客户端。

b.如果是有线配置文件供员工访问，请切换 802.1X 身份验证开关以启用。这是对启用 MAC 身份验证的补充。

c.如果有线配置文件用于猜测访问，请从强制 portal 配置文件下拉列表中选择一个配置文件。这是对启用 MAC 身份验证的补充。

d.要强制实施 MAC 身份验证，请转至“访问”选项卡，从“访问规则”下拉列表中选择“基于角色”，然后将“仅实施 MAC 身份验证”角色开关切换为启用。

3.单击“下一步”，然后单击“完成”以应用更改。

员工访问的 WLAN 配置文件不支持“强制 MAC 身份验证唯一角色”参数。

在 CLI 中

要为无线配置文件配置 MAC 身份验证和强制 portal 身份验证：

(host)(config)# wlan ssid-profile <name>

(host)(SSID Profile <name>)# type <guest>

(host)(SSID Profile <name>)# mac-authentication

(host)(SSID Profile <name>)# captive-portal {<type> [exclude-uplink <types>]|external [Profile <name>] [exclude-uplink <types>]}

(host)(SSID Profile <name>)# set-role-mac-auth <mac-only>

To configure MAC authentication with captive portal authentication for a wired profile:

(host)(config)# wired-port-profile <name>

(host)(wired ap profile <name>)# type <guest>

(host)(wired ap profile <name>)# mac-authentication

(host)(wired ap profile <name>)# captive-portal <type>

(host)(wired ap profile <name>)# captive-portal {<type> [exclude-uplink <types>]external [Profile <name>] [exclude-uplink <types>]}

(host)(wired ap profile <name>)# set-role-mac-auth <mac-only>

管理内部数据库

您可以在内部数据库中创建条目来验证客户端。内部数据库包含客户端列表，以及每个客户端的密码和默认角色。将内部数 据库配置为身份验证服务器时，将在针对内部数据库的传入身份验证请求中检查客户端信息。

配置内部数据库

默认情况下，Mobility Conductor 使用内部数据库进行身份验证。您可以通过输入 CLI 命令 aaa authentication-server internal use-local-switch 来选择使用受管设备中的内部数据库。如果在受管设备中使用内部数据库，则需要在受管设备上添加客户端。

以下 CLI 命令配置内部数据库：

(host) [mynode] #local-userdb add {generate-username|username <name>}{

generate-password|password <password>}

管理内部数据库文件

Mobility Conductor 允许您在内部数据库中导入和导出用户信息表。这些文件一旦导出，就不应进行编辑。Mobility Conductor 仅支持导入在导出过程中创建的数据库文件。请注意，将文件导入内部数据库会覆盖并删除所有现有条目。

以下 CLI 命令配置内部数据库文件的导入和导出：

(host) [mynode] #local-userdb export <filename>

(host) [mynode] #local-userdb import <filename>

配置服务器组

您可以为特定类型的身份验证创建服务器组。例如，您可以指定要用于 802.1X 身份验证的

一个或多个 RADIUS 服务器。您可以在一个组中配置不同类型的服务器。例如，您可以将内部数据库作为 RADIUS 服务器的备份包含在内。您还可以在多个服务器组中配置同一台服务器。但是，必须先配置服务器，然后才能使用 WebUI 或 CLI 将其包含在服务器组中。

以下过程介绍如何配置服务器组：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.“服务器组”（Server Groups）表格显示服务器组列表。

3.单击服务器组中的+。输入新服务器组的名称，然后单击提交。

4.选择创建的新服务器组。

5.在“服务器组<”服务器组名称>中，单击“服务器”选项卡，然后单击“+”将服务器添加到该组。

- 若要添加现有服务器，请选择“添加现有服务器”,然后从列表中选择一个服务器。点击提交。
- 若要添加新服务器，请选择“添加新服务器”。配置以下参数，然后单击提交：
  - 类型（Type）- 从下拉列表中指定服务器类型。
  - 名称-输入服务器的名称。
  - IP 地址/主机名一设置服务器的 IP 地址/主机名。
- 重复上述步骤，将其他服务器添加到组中。

6.点击提交。

7.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

8.单击“挂起的更改”。

```
(host) [mynode] (config) #aaa server-group <name>

       auth-server <name>
```

配置服务器列表顺序和故障传递

服务器组中的服务器是有序列表的一部分。默认情况下，始终使用列表中的第一台服务器，除非它不可用，在这种情况下， 将使用列表中的下一台服务器。您可以使用向上或向下箭头通过 WebUI 配置服务器组中服务器的顺序(顶部服务器是列表 中的第一个服务器)。在 CLI 中 ， position 参数指定列表中服务器的相对顺序(最低值表示列表中的第一台服务器)。如前所述，列表中的第一个可用服务器用于身份验证。如果服务器响应身份验证失败，则不会对身份验证请求失败的用户或 客户端进行进一步处理。还可以为服务器组启用故障传递

身份验证，以便在列表中的第一台服务器返回身份验证拒绝时，受 管设备将尝试使用有序列表中的下一台服务器进行身份验证。受管设备尝试对列表中的每台服务器进行身份验证，直到身份 验证成功或组中的服务器列表用尽为止。此功能在具有多个独立身份验证服务器的环境中非常有用；用户可能在一台服务器 上无法通过身份验证，但可以在另一台服务器上进行身份验证。

在启用故障传递身份验证之前，请注意以下事项：

- 对于由符合 EAP 的外部 EAP 的 RADIUS 服务器组成的服务器组的 802.1X 身份验证，不支持此功能。但是，当 802.1X 身份验证在受管设备 (AAA FastConnect)上终止时，可以使用故障传递身份验证。
- 为大型服务器组列表启用此功能可能会导致受管设备上的处理负载过大。建议您尽可能使用基于域匹配的服务器选择 (请参阅第 209 页上的配置动态服务器选择)。
- 如果出现多个身份验证失败，某些服务器(如 RSA RADIUS 服务器)会锁定受管设备。因此，不应使用这些服务器 启用故障传递身份验证。

在以下示例中，您将创建一个服务器组“corp-serv”,其中包含两个 LDAP 服务器 (ldap-1 和 ldap2)，每个服务器都 包含网络中使用的用户名和密码的子集。启用故障传递身份验证后，未通过列表中第一台服务器进行身份验证的用户将使用 第二台服务器进行身份验证。

以下过程介绍如何配置服务器列表顺序和故障传递：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.单击“+”,配置以下参数：

- 名称-输入 ldap-1 作为服务器的名称。
- IP 地址/主机名-输入服务器的 IP 地址/主机名。
- 类型(Type)-将类型设置为 LDAP。

3.点击提交。

4.单击“+”,配置以下参数：

- 名称-输入 ldap-2 作为服务器的名称。
- IP 地址/主机名-输入服务器的 IP 地址/主机名。
- 类型 (Type)-将类型设置为 LDAP。

5.点击提交。

6.在“所有服务器”下，选择“ldap-1”以配置服务器参数。选中“模式”复选框以激活身份验证服务器。

7.点击提交。

8.重复以上的步骤以配置 ldap-2。

9.单击“服务器组”(Server Groups)表格下的“+”(+)以添加新的服务器组。将服务器组名称设置为 corp- serv， 然后单击“提交”。

10.从“服务器组” (Server Groups) 表中选择 corp-serv 以配置服务器组设置。

11.在“服务器组”<corp-serv>中，选择“选项”选项卡。

12.选中“失败”复选框。

13.点击提交。

14.导航到“服务器”选项卡。

15.单击+将服务器添加到组中。

- 选择“ldap-1”,然后单击“提交”。
- 重复上述步骤，将 ldap-2 添加到服务器组。

16.点击提交。

17.单击“挂起的更改”。

18.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置服务器列表顺序和故障传递:

```
(host)[mynode] (config) #aaa authentication-server ldap ldap-1
        host 10.1.1.234
(host) [mynode] (config) #aaa authentication-server ldap ldap-2
        host 10.2.2.234
(host) [mynode] (config) #aaa server-group corp-serv
        auth-server ldap-1 position 1
        auth-server ldap-2 position 2
        allow-fail-through
```

配置动态服务器选择

受管设备可以根据客户端在身份验证请求中发送的用户信息，从服务器组中动态选择身份验

证服务器。例如，身份验证请求 可以包含以下格式之一的客户端或用户信息：

- <domain>\<user>:例如，corpnet.com\Darwin
- <user>@<domain>:例如 darwin@corpnet.com
- host/<pc-name>.<domain>:例如，host/darwin-g.finance.corpnet.com(此格式用于 Windows 环境中的 802.1X 计算机身份验证)

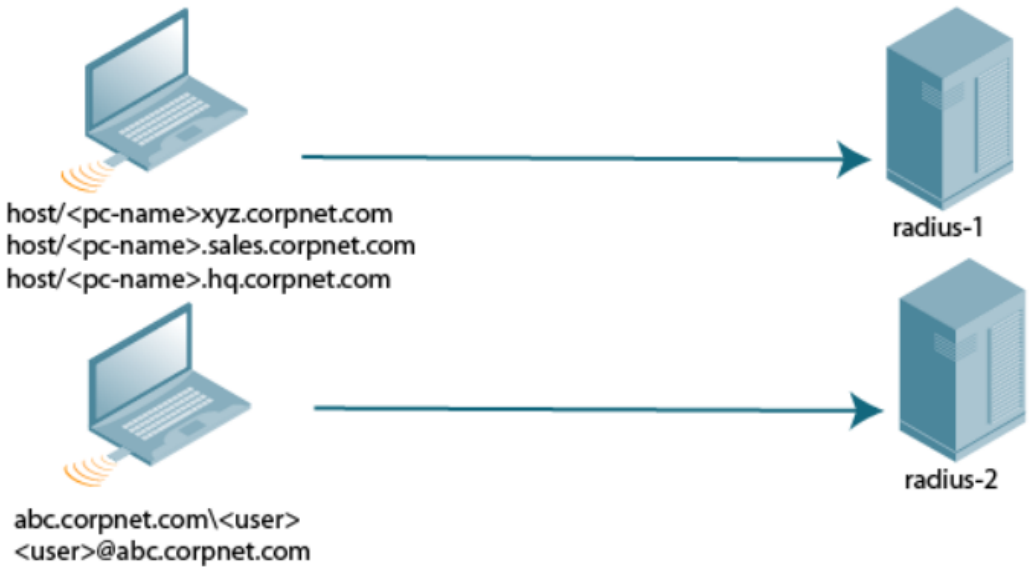
在服务器组中配置服务器时，可以选择将服务器与一个或多个匹配规则相关联。服务器的匹配规则可以是以下规则之一：

- 如果客户端/用户信息包含指定的字符串，则选择服务器。
- 如果客户端/用户信息以指定的字符串开头，则选择服务器。
- 如果客户端/用户信息与指定的字符串完全匹配，则选择服务器。

您可以为同一台服务器配置多个匹配规则。托管设备将客户端/用户信息与为每个服务器配置的匹配规则进行比较，从服务 器组中的第一台服务器开始。如果找到匹配项，托管设备会使用匹配规则将身份验证请求发送到服务器。如果在到达服务器 列表末尾之前未找到匹配项，则返回错误，并且不会发送客户端/用户的身份验证请求。

下图描绘了一个由 corpnet.com 中的多个子域组成的网络。服务器 radius-1 为 xyz.corpnet.com、 sales.corpnet.com 和 hq.corpnet.com 的 PC 客户端提供 802.1X 机器身份验证。服务器 radius-2 为 abc.corpnet.com 中的用户提供身份验证。

基于域的服务器选择示例



以下过程介绍如何配置动态服务器选择：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.从“服务器组”(Server Groups) 表格中选择一个服务器组。

3.在“服务器组<”服务器组名称>中，选择“服务器规则”选项卡，单击“+”。

- 属性(Attribute)-从下拉列表中选择一个属性。
- 操作(Operation)-选择一个操作以将条件应用于属性。
- 操作数—将操作数值设置为客户端或用户信息。
- 动作(Action)-将操作应用于属性。
- 角色(Role)-为属性设置角色。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置动态服务器选择：

host) [mynode] (config) #aaa server-group <group>

auth-server <name> [match-authstring contains|equals|starts-with <string>] [match-fqdn <string>] [position <number>] [trim-fqdn]

配置匹配 FQDN 选项

还可以对服务器规则使用“匹配 FQDN (域名)”选项。使用此规则时，如果<domain> 格式<domain>为\或@的用户信息部分<user><user><domain>与指定的字符串完全匹配，则选择服务器。使用匹配 FQDN 规则时，请注意以下注意事项：

- 此规则不支持 host/. 格式的客户端信息<pc-name><domain>， 因此它对 802.1X 计算机身份验证没有用。
- FQDN 选项仅对<domain>身份验证请求中发送的用户信息部分执行匹配。match-authstring 选项(如前所述)允许您匹配身份验证请求中发送的全部或部分用户信息。

以下过程介绍如何配置匹配 FQDN 选项：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器页面。

2.从“服务器组” (Server Groups) 表格中选择一个服务器组。

3.在“服务器组<”服务器组名称>中，选择“服务器规则”选项卡，然后单击“+”。

- 域名-从属性下拉列表中选择域名。
- 操作(Operation)-将操作设置为等于。
- 操作数(Operand)-将操作数值设置为客户端或用户信息。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置匹配 FQDN 选项:

(host) [mynode] (config) #aaa server-group <group>

auth-server <name> match-fqdn <string>

从请求中剪裁域信息

在受管设备将身份验证请求转发到指定服务器之前，它可以截断用户信息中特定于域的部分。当身份验证服务器上的用户 条目不包括域信息时，这很有用。您可以使用任何服务器匹配规则指定此选项。仅当用户信息以下列格式发送到受管设备 时，此选项才适用:

<domain>\<user>: <domain>\部分被截断

<user>@<domain>: @<domain>部分被截断

此选项不支持以 host/.格式发送的客户端信息<pc-name><domain>。

以下过程介绍如何配置请求中的修整域信息:

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.从“服务器组” (Server Groups) 表格中选择一个服务器组。

3.在“服务器组<”>“下，单击”服务器“选项卡并选择一个服务器，或单击”+“将新服务器添加到该组。

- 若要添加现有服务器，请选择“添加现有服务器”,然后从列表中选择一个服务器。点击提交。
- 若要添加新服务器，请选择“添加新服务器”。配置以下参数，然后单击提交:

- 类型 (Type)-从下拉列表中指定服务器类型。
- 名称-输入服务器的名称。
- IP 地址/主机名—设置服务器的 IP 地址/主机名。

4.选择新服务器。

5.在“服务器组<”服务器组名称><“服务器名称>中，单击”服务器组修剪 FQDN “选项卡。

6.选中“修剪 FQDN” 复选框。

7.点击提交。

8.单击“挂起的更改”。

9.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以 CLI 命令配置来自请求的修整域信息：

(host) [mynode] (config) #aaa server-group <group>

auth-server <name> trim-fqdn

配置服务器派生规则

配置服务器组时，可以根据服务器在认证期间为客户端返回的属性设置客户端的 VLAN 或角色。服务器派生规则适用于组 中的所有服务器。通过服务器派生规则分配的用户角色或 VLAN 优先于为身份验证方法配置的默认角色和 VLAN。

身份验证服务器必须配置为在身份验证期间返回客户端的属性。

服务器规则基于第一个匹配原则应用。适用于服务器和返回的属性的第一个规则将应用于客户端，并且是从服务器规则 应用的唯一规则。这些规则统一应用于服务器组中的所有服务器。可配置的服务器规则参数如下表 38 所示。

服务器规则配置参数

参数	说明
属性	这是身份验证服务器返回的属性，用于检查操作和操作数匹配。
操作	这是将 Operand 中的字符串与身份验证服务器返回的属性值进行匹配的匹配方法。

	● contains :当且仅当属性值包含参数 Operand 中的字符串时，才会应用规则。 ● starts-with:当且仅当返回的属性值以参数 Operand 中的字符串开头时，才会应用规则。 ● ends-with:当且仅当返回的属性值以参数Operand 中的字符串结尾时，才会应用规 则。 ● equals:当且仅当返回的属性值等于参数 Operand 中的字符串时，才会应用规则。 ● not-equals:当且仅当返回的属性值不等于参数 Operand 中的字符串时，才会应用该规则。 ● value-of:这是一个特殊条件。这意味着角色或 VLAN 设置为返回的属性的值。要成功执行此操作，应将角色和 VLAN ID 作为所选属性的值返回应用规则时，必须已在受管设备上配置。
操作数	这是返回属性的值与之匹配的字符串。
行动	定义在规则匹配时是向用户分配角色还是 VLAN。
角色或 VLAN	服务器派生规则适用于用户角色或 VLAN 分配。跟 角色分配，可以根据返回的属性为客户端分配特定角色。在 VLAN 分配中，可以根据返回的属 性将客户端放置在特定的 VLAN 中。

以下过程介绍如何配置服务器派生规则:

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>身份验证服务器选项卡。

2.从“服务器组” (Server Groups) 表格中选择一个服务器组。

3.在“服务器组<”服务器组名称>“中，选择”服务器“选项卡并选择一个服务器，或单击”+“将新服务器添加到该组。

- 若要添加现有服务器，请选择“添加现有服务器”,然后从列表中选择一个服务器。点击提交
- 要添加新服务器，请选择“添加新服务器”。配置以下参数，然后单击提交:
  - 类型 (Type)-从下拉列表中指定服务器类型。
  - 名称-输入服务器的名称。

- IP 地址/主机名—设置服务器的 IP 地址/主机名。

4.在“服务器规则”选项卡中，单击“+”以添加用于分配用户角色或 VLAN 的服务器派生规则。

属性(Attribute)-从下拉列表中选择一个属性。

- 操作(Operation)-选择一个操作以将条件应用于属性。
- 操作数—将操作数值设置为客户端或用户信息。
- set role -从操作下拉列表中设置角色。从“角色”下拉列表中选择要分配的角色。
- set vlan 从操作下拉列表中设置 vlan。从 Vlan 下拉列表中选择 VLAN 名称或 ID。

5.点击提交。

6.重复上述步骤，为服务器组添加其他规则。

7.单击“挂起的更改”。

8.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令配置服务器派生规则：

(host) [mynode] (config) #aaa server-group <name>

(host) [mynode] (Server Group name) #set {role|vlan} condition <attribute> contains|ends-with|equals|not-equals|starts-with <operand> set-value <set-value-str> position <number>

为内部数据库配置角色派生规则

将用户条目添加到内部数据库时，可以指定用户角色。在要分配给经过身份验证的客户端的内部数据库条目中指定的角色，必须配置服务器派生规则，如下所示：

以下 CLI 命令为内部数据库配置服务器派生规则：

(host) [mynode] (config) #aaa server-group internal

set role condition Role value-of

分配服务器组

您可以出于以下目的创建服务器组：

- 用户身份验证
- 管理身份验证
- 计费

您可以为用户和管理身份验证配置所有类型的服务器(请参见下表)。仅当使用 RADIUS 或 TACACS+进行身份验证时，RADIUS 和 TACACS+服务器才支持记帐。

服务器类型和用途

	RADIUS	TACACS+	LDAP	内部数据库
用户身份验证	Yes	Yes	Yes	Yes
管理身份验证	Yes	Yes	Yes	Yes
计费	Yes	Yes	Yes	Yes

以下部分介绍用户身份验证、管理身份验证和记帐：

用户身份验证

有关为用户身份验证分配服务器组的信息，请参阅“角色和策略”一章。

管理身份验证

需要访问 Mobility Conductor 以监控、管理或配置 Aruba 以用户为中心的网络的用户可以通过 RADIUS、TACACS+或 LDAP 服务器或内部数据库进行身份验证。

身份验证成功后，仅返回用户记录属性。因此，要派生除默认管理身份验证角色之外的管理角色，请根据用户属性。

以下 CLI 命令启用管理身份验证：

```
(host)[mynode] (config) #aaa authentication mgmt
server-group <group>
enable
```

计费

您可以为 RADIUS 和 TACACS+服务器组配置记帐。

仅当使用 RADIUS 或 TACACS+ 进行身份验证时，才支持 RADIUS 或 TACACS+ 记帐。

以下部分介绍 RADIUS 记帐、漫游 RADIUS 记帐服务、多服务器上的 RADIUS 记帐和 TACACS+记帐：

RADIUS 计费

RADIUS 记帐允许将用户活动和统计信息从托管设备报告到 RADIUS 服务器:

1.受管设备在用户登录时生成记帐开始数据包。传输的 RADIUS 数据包的代码字段设置为 4 (Accounting-Request) 。 请注意，敏感信息(如用户密码)不会发送到记帐服务器。RADIUS 服务器发送数据包的确认。

2.当用户注销时，受管设备会发送记帐停止数据包；数据包信息包括各种统计信息，例如经过的时间、输入和输出字节以及数据包。RADIUS 服务器发送数据包的确认。

可以将以下属性发送到 RADIUS 记帐服务器:

- Acct-Status-Type:此属性标记用户的记帐记录的开始或结束。当前值为“开始”、“停止”和“临时更新”。
- User-Name:用户名。
- Acct-Session-Id: 唯一标识符，用于方便用户的记帐记录匹配。它派生自用户名、IP 地址和 MAC 地址。这是在 所有记帐数据包中设置的。
- Acct-Authentic:这指示如何对用户进行身份验证。当前值为 1 (RADIUS)、2(本地)和 3 (LDAP)。
- Acct-Session-Time:端登录到受管设备所经过的时间(以秒为单位)。这仅在 Accounting-Request 记录中发 送，其中 Acct-Status-Type
- Acct-Terminate-Cause: 指示会话是如何终止的，以及如何在 Acct-Status-Type 为 Stop 的 Accounting-Request 记 录中发送。可能的值为:
  - 1: 用户注销
  - 4: 空闲超时
  - 5: 会话超时。最大会话长度计时器已过期。
  - 7: 管理员重新启动: 管理员正在结束服务，例如在重新启动 Mobiity Conductor 之前。

- NAS-Identifier: 这是在 RADIUS 服务器配置中设置的。
  - 在 WebUI 的 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>“高级”页面。在 “RADIUS 客户端”下，输入 IPv4 或 IPv6 地址。
- NAS-IP-Address:受管设备的 IP 地址。您可以配置“全局”NAS IP 地址: 在 CLI 中，使用 ip radius nas-ip 命令。

- NAS-Port:用户流量通过该端口(隧道)进入受管设备的物理或虚拟端口(隧道)号。
- NAS-Port-Type:连接中使用的端口类型。这设置为以下选项之一:
  - 5: 管理员登录
  - 15: 有线用户类型
  - 19: 无线用户
- Framed-IP-Address:用户的 IP 地址。
- Calling-Station-ID: 用户的 MAC 地址。
- Called-station-ID:受管设备的 MAC 地址。

当 Acct-Status-Type 值为 Start 时，将在 Accounting-Request 数据包中发送以下属性:

- Acct-Status-Type
- User-Name
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- NAS-Identifier
- Framed-IP-Address
- Calling-Station-ID
- Called-station-ID
- Acct-Session-ID
- Acct-Authentic

当 Acct-Status-Type 值为 Stop 时，将在 Accounting-Request 数据包中发送以下属性:

- Acct-Status-Type
- User-Name
- NAS-IP-Address
- NAS-Port
- NAS-Port-Type
- NAS-Identifier
- Framed-IP-Address
- Calling-Station-ID

- Called-station-ID
- Acct-Session-ID
- Acct-Authentic

以下统计属性仅在 Interim-Update 和 Accounting Stop 数据包中发送(它们不在 Accounting Start 数据包中发送):

- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Input-Packets
- Acct-Output-Packets
- Acct-Input-Gigawords
- Acct-Output-Gigawords

处于拆分隧道模式的远程 AP 现在支持 RADIUS 记帐。如果在拆分隧道远程 AP AAA 配置文件中启用 RADIUS 记帐，则当 用户与远程 AP 关联时，受管设备会向 RADIUS 服务器发送 RADIUS 记帐开始记录，并在用户注销或从用户数据库中删除 时发送停止记录。如果启用了临时记帐，受管设备会定期发送更新。每个临时记录都包括累积用户统计信息，包括接收的字 节数和数据包计数器。

以下过程介绍如何为 RADIUS 记帐分配服务器组：

1.在“托管网络”节点层次结构中，导航到“配置>身份验证”>“AAA 配置文件”选项卡。

2.展开 AAA 配置文件窗格，然后选择默认配置文件实例。

3.(可选)在 AAA 配置文件：默认窗格中，选择 RADIUS 临时记帐以允许受管设备，用于定期向服务器发送包含当前用户统计信息的临时更新消息。默认情况下，此选项处于禁用状态，允许受管设备仅发送启动和停止消息 RADIUS 记帐服务器。

4.选择 AAA 配置文件，然后向下滚动以选择 AAA 配置文件的 RADIUS 记帐服务器组。从下拉列表中选择“服务器”组。

您可以向组添加其他服务器或配置服务器规则。

5.单击提交。

6.单击“挂起的更改”(Pending Changes)。

7.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令为 RADIUS 记帐配置服务器组：

(host) [mynode] (config) #aaa profile <profile>

radius-accounting <group>

radius-interim-accounting

漫游 RADIUS 计费服务

从 ArubaOS 8.1 开始，漫游 RADIUS 记帐服务为每个无线客户端创建一个记帐会话。与基于计时器的 RADIUS 临时更新记 帐记录相比，会话中的记录包含相同的 RADIUS 属性集，但统计属性除外。每当无线客户端漫游到其他 AP 时，漫游触发的 RADIUS 临时更新记帐记录都会发送到配置的 RADIUS 记帐服务器。此记录用于跟踪无线客户端的当前位置。目前，群集和 非群集环境中的无线客户端都支持此功能，但有线、VPN/VIA 和 L3 移动客户端不支持此功能。

以下过程介绍如何启用漫游 RADIUS 记帐服务：

1.在“托管网络”节点层次结构中，导航到“配置>身份验证”> “AAA 配置文件”选项卡。

2.展开 AAA 配置文件并选择 AAA 配置文件实例。

3.在 “AAA 配置文件：“<配置文件的名称>窗格中，选中“RADIUS 漫游记帐”复选框。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令启用漫游 RADIUS 记帐服务：

(host) [mynode] (config) # aaa profile <profile_name>

radius-accounting <group>

radius-roam-accounting

以下 CLI 命令检查是否启用了漫游触发的 RADIUS 记帐：

(host) #show aaa profile <profile_name>

在多台服务器上配置 RADIUS 计费

ArubaOS 支持将 RADIUS 记帐发送到多个 RADIUS 服务器。Mobility Conductor 通知所有 RADIUS 服务器以跟踪经过 身份验证的用户的状态。记帐消息按顺序发送到服务器组中配

置的所有服务器。

以下过程介绍如何启用多个服务器帐户功能：

1.在“托管网络”节点层次结构中，导航到“配置>身份验证”>“AAA 配置文件”选项卡。

2.展开 AAA 配置文件并选择 AAA 配置文件实例。

3.在“AAA 配置文件：“<配置文件的名称>窗格中，选中“多服务器记帐”复选框。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

以下 CLI 命令启用多服务器上的 RADIUS 记帐功能：

```
(host) [mynode] (config) # aaa profile <profile_name>

multiple-server-accounting
```

TACACS+计费

TACACS+记帐允许将在 Mobility Conductor 或受管设备上发出的命令报告给 TACACS+服务器。您可以指定报告的命令类型(操作、配置或显示命令),或报告所有命令。

您只能使用 CLI 配置 TACACS+记帐。

以下 CLI 命令配置 TACACS+记帐：

```
(host) [mm] (config) #aaa tacacs-accounting

(host) ^[mm] (config-submode) #command {action|all|configuration|show}

(host) ^[mm] (config-submode) #server-group <name of the TACACS server>

(host) ^[mm] (config-submode) #write memory
```

配置身份验证计时器

以下过程介绍如何配置身份验证计时器：

1.在 Mobility Conductor 节点层次结构中，导航到“配置>身份验证”>“高级”选项卡。

2.展开身份验证计时器。

3.如下表中所述配置计时器。

4.点击提交。

5.单击“挂起的更改”。

6.在“挂起的更改”窗口中，选中该复选框，然后单击“部署更改”。

身份验证计时器

定时器	描述
用户空闲超时(User Idle Timeout)	如果客户端没有空闲，则客户端被视为空闲的最长时间来自客户端的无线流量。如果存在无线流量，则超时期限将重置。如果在超时期限内 没有无线流量，则客户端已过期。超时期限到期后，将删除用户。如果未指定关键字seconds,则该值在命令行中默认为 minutes。范围：1-255 分钟(30-15300 秒)默认值：5 分钟(300 秒)
身份验证服务器死亡时间	受管设备将无响应的身份验证服务器视为“停止服务”的最长时间(以分钟为单位)。仅当受管设备上配置了两个或多个身份验证服务器时，此计时器才适用。如果只配置了一个身份验证服务器，则该服务器永远不会被视为停止服务，并且所有请求 都将发送到该服务器。如果配置了一个或多个备份服务器，并且服务器无响应，则该 服务器将被标记为在死时间内停止服务；后续请求将在死时间期间发送到优先级列表中 的下一个服务器。如果服务器在死区时间过后响应，则它可以接管来自低优先级服务 器的服务请求；如果服务器仍然没有响应，则在死区时间内将其标记为关闭。范围：0- 50 分钟默认值：10 分钟
登录用户生存期	允许未经身份验证的客户端保持登录状态的最长时间(以分钟为单位)。范围：0-255 分钟默认 值：5 分钟
用户临时统计信息频率	设置用户统计信息的超时值，以分钟或秒为单位进行报告。范围：300-3600 秒，或 5-60 分钟默认值：600 秒

以下 CLI 命令配置可应用于客户端的计时器。如果未为 idle-timeout 和 stats-timeout 参

数指定可选的 seconds 关 键字，则该值默认为 minutes:

```
(host)[mynode] (config) #aaa timers

dead-time <minutes>

idle-timeout <time> [seconds]

logon-lifetime <0-255>

stats-timeout <time> [seconds]
```

身份验证服务器负载平衡

身份验证服务器的负载平衡可确保身份验证负载在多个身份验证服务器之间拆分，从而避免任何一个特定的身份验证服务 器过载。身份验证服务器负载平衡功能使 Mobility Conductor 能够对发往外部身份验证服务器(RADIUS 或 LDAP) 的 身份验证请求执行负载平衡。这样可以防止任何一个身份验证服务器在繁重的身份验证期间(例如在工作日开始时)处理全部负载。

以前，控制器使用服务器组列表中的第一个身份验证服务器。仅当身份验证服务器关闭时，该组中的其余服务器才会按顺 序使用。

因此，控制器执行故障转移，而不是对身份验证服务器进行负载平衡。

负载平衡算法计算对每个身份验证服务器的新客户端进行身份验证所需的预期时间，并选择预期身份验证时间最短的身份验 证服务器。负载平衡算法保持重新身份验证粘性，这意味着在重新身份验证时，请求将转发到最初进行身份验证的同一服务器。

启用身份验证服务器负载平衡功能

以下 CLI 命令启用身份验证服务器负载平衡功能：

```
(host) [mynode] (config) #aaa server-group <group>

    load-balance

    auth-server s1

    auth-server s2
```

以下 CLI 命令禁用负载平衡：

```
(host) [mynode] (config) #aaa server-group <group>
```

```
no load-balance
```

如果在服务器组中配置内部服务器，则负载平衡不适用于内部服务器。当组中的所有其他服务器都关闭时，内部服务器将用作回退。

测试已配置的身份验证服务器

您可以在 WebUI 或 CLI 中测试配置的 RADIUS 身份验证服务器。此功能允许您检查配置的 RADIUS 身份验证服务器或 内部数据库。您可以使用此功能检查 RADIUS 服务器是否“停止服务”。

以下 CLI 命令在内部数据库中配置用户：

```
(host)(mynode)# local-userdb add kgreen lkjHGfds

(host)(mynode)# aaa test-server pap internal kgreen lkjHGfds
```

从 ArubaOS 8.1.0.0 开 始 ， aaa test-server 命令包含 verbose 选项。详细选项有助于显示 RADIUS 服务器在身份验证 成功或失败时的响应。这样可以简化对活动网络进行故障排除。此增强功能适用于 WebUI 和 CLI。

以下过程介绍如何在身份验证成功或失败时获取 RADIUS 服务器响应：

1.在 Mobility Conductor 节点层次结构中，转到“诊断>工具”>AAA 服务器测试选项卡。

2.从“服务器名称”下拉列表中选择服务器。

3.为“身份验证方法”选择一个选项。您可以选择 MSCHAPv2 或 PAP。

4.在“用户名”和“密码”文本框中输入用户凭据。

5.单击“测试”。将显示身份验证状态以及 RADIUS 服务器响应。

以下 CLI 命令显示服务器返回的 RADIUS 服务器属性：

```
(host)(mynode) # aaa test-server mschapv2 internal raduser1 raduser verbose

Authentication Successful

Processing time (ms) : 1.397

Attribute value pairs in response

---------------------------------

Vendor Attribute Value
```

------ --------- -----

MS-CHAPv2

Role guest