神州云科
Yunke China

DCYK 身份认证服务器手册

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

认证服务器

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

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

- 了解身份认证服务器最佳实践和例外；
- 了解服务器和服务器组。

配置身份认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认证服务器和服务器组的过程。

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

了解身份认证服务器最佳实践和例外

要使外部身份认证服务器处理来自 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 支持以下外部身份认证服务器:

- RADIUS
- LDAP
- TACACS+
- Windows(用于有状态 NTLM 身份认证)

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认证。

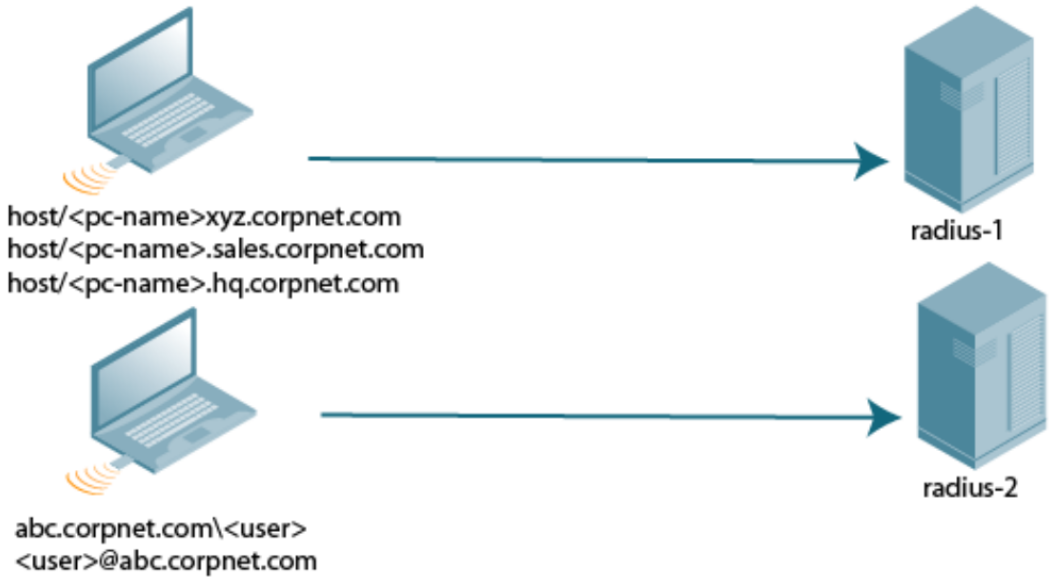
您可以为特定类型的身份认证创建服务器组。例如，您可以指定要用于 802.1X 身份认证的一个或多个 RADIUS 服务器。 服务器组中的服务器列表是有序列表。这意味着，除非列表中的第一台服务器不可用，否则将始终使用该服务器，在这种 情况下，将使用列表中的下一台服务器。

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 身份认证的服务器组。

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认证，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。

配置身份认证服务器

本节介绍如何配置 RADIUS、LDAP、TACACS+ 和 Windows 外部身份认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 身份认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>身份认证”>“身份认证服务器”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”复选框以激活身份认证服务器。

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 上的管理身份认证，而不用于用户 或设备(有线或无线)身份认证。/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

RADIUS 服务类型属性

托管设备为 RADIUS 身份认证请求发送以下服务类型属性值。

无论身份认证类型如何，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) 上进行的身份认证，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 身份认证和记帐数据在 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认证、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认证。对于要对 Radsec 服务器进行身份认证的受管设备:

- 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 身份认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。

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]