在无线局域网控制器上配置RADIUS服务器回退功能

目录

简介

先决条件

- 要求
- 使用的组件

背景信息

- RADIUS服务器回退功能
- 回退模式
  - 主动模式
  - 被动模式
  - 关闭模式

配置

- 使用CLI配置RADIUS服务器回退功能
- 使用GUI配置RADIUS服务器回退功能

验证

故障排除

相关信息

简介

本文档介绍如何使用无线局域网控制器(WLC)配置RADIUS服务器回退功能。

先决条件

要求

Cisco 建议您了解以下主题：

- 了解轻量接入点 (LAP) 和 Cisco WLC 配置的基础知识
- 无线接入点协议(CAPWAP)的控制和调配基础知识
- 无线安全解决方案基础知识

使用的组件

本文档中的信息基于Cisco 5508/5520控制器。

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。

背景信息

RADIUS服务器回退功能

低于5.0的WLC软件版本不支持RADIUS服务器回退机制。当主RADIUS服务器变得不可用时，WLC将故障切换到下一个主用 — 备份RADIUS服务器。即使主服务器可用，WLC仍将继续使用辅助RADIUS服务器。通常，主服务器是高性能和首选服务器。

在WLC 5.0及更高版本中，WLC支持RADIUS服务器回退功能。通过此功能，可以将WLC配置为检查主服务器是否可用，并在主服务器可用后切换回主RADIUS服务器。为此，WLC支持两种新模式（被动和主动），以便检查RADIUS服务器的状态。在指定的超时值之后，WLC返回至最首选的服务器。

回退模式

主动模式

在主动模式下，当服务器不响应WLC身份验证请求时，WLC会将服务器标记为停机，然后将服务器移至非主动服务器池，并开始定期发送探测消息，直到该服务器响应为止。如果服务器响应，则WLC将停用的服务器移至活动池，并停止发送探测消息。在此模式中，当身份验证请求到来时，WLC始终从RADIUS服务器的活动池中选择最低索引（最高优先级）服务器。

WLC在超时后发送探测数据包（默认值为300秒），以确定服务器状态，以防之前服务器无响应。

被动模式

在被动模式下，如果服务器没有响应WLC身份验证请求，则WLC将服务器移至非活动队列并设置计时器。当计时器到期时，WLC会将服务器移动到活动队列，而不考虑服务器的实际状态。当收到身份验证请求时，WLC从活动队列（可能包括非活动服务器）中选择最低索引（最高优先级）服务器。 如果服务器没有响应，则WLC会将其标记为非活动状态，设置计时器，并移至下一个优先级最高的服务器。此过程将一直持续到WLC找到活动RADIUS服务器或活动服务器池耗尽。

WLC假定服务器在超时后处于活动状态（默认值为300秒），以防服务器之前无响应。如果仍然无响应，WLC会等待另一个超时，并在身份验证请求传入时再次尝试。

关闭模式

在关闭模式下，WLC仅支持故障切换。换句话说，回退被禁用。当主RADIUS服务器关闭时，WLC将故障切换到下一个主用 — 备份RADIUS服务器。WLC继续永远使用辅助RADIUS服务器，即使主服务器可用。

配置

使用CLI配置RADIUS服务器回退功能

注意：使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

从WLC CLI使用这些命令以在WLC上启用RADIUS服务器回退功能。

第一步是选择RADIUS服务器回退模式。如前所述，WLC支持主动和被动的回退模式。

要选择回退模式，请输入以下命令：

```
<#root>

WLC1 >

config radius fallback-test mode {active/passive/off}
```

- active — 将探测功能发送到失效服务器以测试状态。
- passive — 根据上一个事务设置服务器状态。
- off — 禁用服务器回退测试（默认）。

下一步是选择指定主动模式的探测间隔或被动操作模式的非活动时间的间隔。

要设置间隔，请输入以下命令：

```
<#root>

WLC1 >

config radius fallback-test mode interval {180 - 3600}
```

<180到3600> — 以秒为单位输入探测间隔或非活动时间（默认值为300秒）。

时间间隔指定在主动模式回退情况下的探测时间或在被动模式回退情况下的非活动时间。

对于主动操作模式，您需要配置一个用户名，该用户名将用于发送到RADIUS服务器的探测请求。

要配置用户名，请输入以下命令：

```
<#root>

WLC1 >

config radius fallback-test username {username}
```

<username> — 输入最多16个字母数字字符的名称（默认值为cisco-probe）。

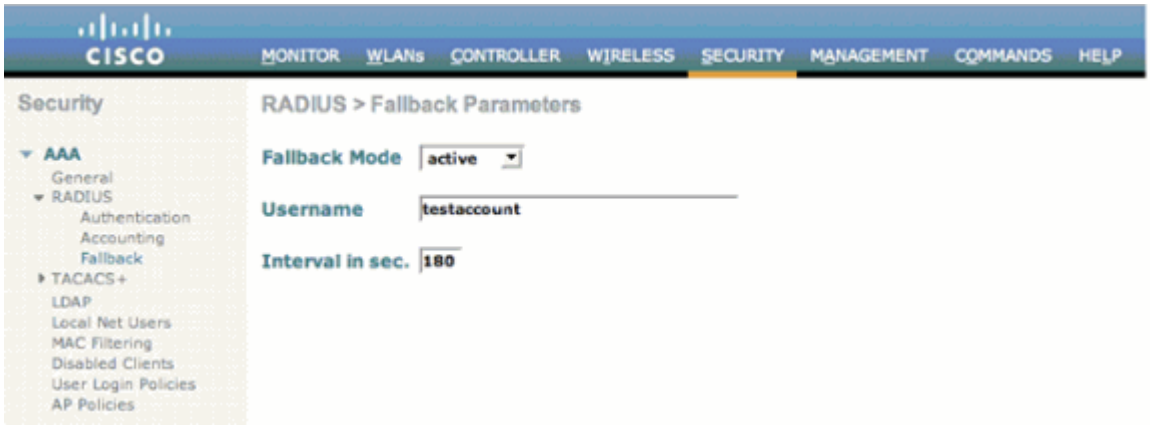
注意：您可以输入自己的用户名或保留默认值。默认用户名是“cisco-probe”。 由于此用户名用于发送探测消息，因此无需配置密码。

使用GUI配置RADIUS服务器回退功能

要使用GUI配置WLC，请完成以下步骤：

1. 配置RADIUS服务器回退模式。为此，请从WLC GUI中选择Security > RADIUS > Fallback。系统将显示RADIUS > Fallback Parameters页。
2. 从Fallback Mode下拉列表中，选择回退模式。可用选项包括active、passive和off。

   以下是活动回退模式配置的示例截图，如图所示。



3. 对于活动操作模式，请在用户名字段中输入用户名。
4. 在Interval in sec中输入探测间隔值。字段。
5. 单击 Apply。

如果在WLC中启用了主动故障切换功能，则WLC过于主动，无法将AAA服务器标记为“无响应”。 但是，不应执行此操作，因为如果您执行静默丢弃，则AAA服务器可能仅对该特定客户端不作出响应。它可以是对其他具有有效证书的有效客户端的响应。WLC仍然可以将AAA服务器标记为“不响应”和“无法正常工作”。

为了克服这种情况，请禁用主动故障切换功能。从控制器GUI输入config radius aggressive-failover disable命令以执行此操作。如果禁用了此操作，则当连续三个客户端都未能从 RADIUS 服务器收到响应时，控制器将只会故障切换到下一个 AAA 服务器。

注意：版本8.5.140、8.8.100、8.10.105及更高版本中引入的功能更改：当禁用控制器的RADIUS主动故障切换时：数据包重试六次，除非从客户端中止。RADIUS服务器（AUTH和ACCT）在来自多个客户端（之前仅来自三个客户端）的三个超时事件（18次连续重试）后被标记为不可达。 启用控制器的RADIUS主动故障切换时：数据包重试六次，除非从客户端中止。RADIUS服务器（身份验证和ACCT）在来自多个客户端（之前仅来自一个客户端）的一个

超时事件（6次连续重试）后被标记为不可达。 这意味着每个RADIUS服务器（AUTH或ACCT）可以从多个客户端连续重试18次。因此，并不总是保证每个数据包将重试六次。

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。

输入show radius summary命令以验证回退配置。例如：

```
<#root>

WLC1 >

show radius summary



Vendor Id Backward Compatibility..... Disabled
Call Station Id Type..... IP Address
Aggressive Failover..... Enabled
Keywrap..... Disabled

Fallback Test:
Test Mode.....

Active


 Probe User Name.....

testaccount


 Interval (in seconds).....

180



Authentication Servers

Idx Type Server Address Port State   Tout RFC3576  IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
--- ---- -------------- ---- ------- ---- -------  ---------------------------------------------
1   NM   10.1.1.12      1812 Enabled 2    Disabled Disabled-none/unknown/group-0/0 none/none

Accounting Servers

Idx Type Server Address Port  State   Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
--- ---- -------------- ----  ------- ---- ------- ----------------------------------------
1   N    10.1.1.12      1813  Enabled 2    N/A     Disabled-none/unknown/group-0/0 none/nonen
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

注意：使用 debug 命令之前，请参阅有关 Debug 命令的重要信息。

- debug dot1x events enable — 配置802.1X事件的调试。
- debug aaa events enable — 配置所有AAA事件的调试。

相关信息

- WLAN 控制器 (WLC) 中 EAP 身份验证的配置示例
- 轻量 AP (LAP) 注册到无线 LAN 控制器 (WLC)
- 配置安全解决方案
- 带有RADIUS服务器的动态VLAN分配和无线局域网控制器的配置示例
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。