# 使用EEM脚本排除间歇性RADIUS服务器故障

## 目录



## 简介

本文档介绍如何对ASA中标记为故障的RADIUS服务器进行故障排除，以及这如何导致客户端基础设施中断。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco ASA上的基本感知或EEM脚本

### 使用的组件

本文档不限于特定的软件和硬件版本。

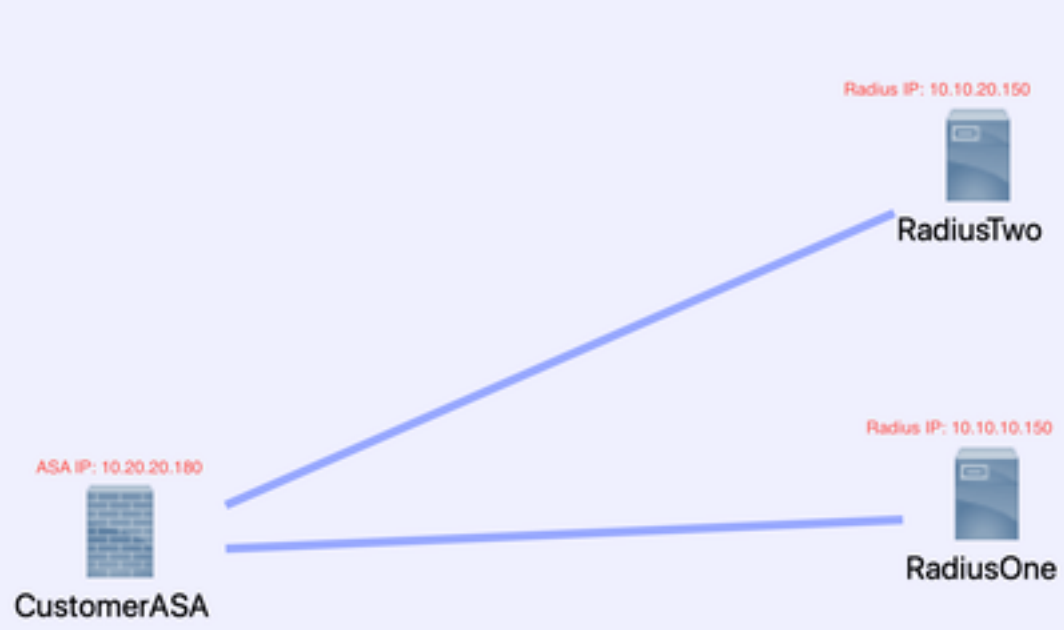
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 问题

RADIUS服务器在思科ASA中标记为发生故障/停机。问题是间歇性的，但会导致客户端基础设施中断。TAC必须区分这是ASA问题、数据路径问题还是Radius服务器问题。如果在发生故障时捕获数据包，它会排除Cisco ASA，因为Cisco ASA会识别ASA是否将数据包发送到RADIUS服务器，以及是否收到这些数据包。

**拓扑**

在本例中，使用的拓扑如下：




要解决此问题，请执行以下步骤。

## 第1步：配置数据包捕获和适用的访问列表以捕获服务器之间的数据包

第一步是配置数据包捕获和适用的访问列表，以捕获ASA和RADIUS服务器之间的数据包。

如果需要有关数据包捕获的帮助，请参阅数据包捕获配置生成器和分析器。

access-list TAC extended permit ip host 10.20.20.180 host 10.10.10.150

access-list TAC extended permit ip host 10.10.10.150 host 10.20.20.180

access-list TAC extended permit ip host 10.20.20.180 host 10.10.20.150

access-list TAC extended permit ip host 10.10.20.150host 10.20.20.180

捕获RADIUS类型原始数据访问列表TAC缓冲区30000000接口内部循环缓冲区

> **注**：您需要检查缓冲区大小，以确保它不会过满并处理数据。缓冲区大小1000000足够。请注意，示例缓冲区是3000000。

## 第2步：配置EEM脚本

接下来，配置EEM脚本。

此示例使用系统日志ID 113022，并且可以在许多其他系统日志消息中触发EEM:

ASA的消息类型可在Cisco Secure Firewall ASA Series Syslog Messages中找到。

此场景中的触发因素是：

**Error Message** %ASA-113022: AAA Marking RADIUS server servername in aaa-server group AAA-Using-DNS as FAILED

此 ASA 已尝试向AAA服务器发送身份验证、授权或记帐请求，并且在配置的超时窗口中未收到响应。然后，AAA服务器被标记为发生故障，并从服务中删除。

事件管理器小程序ISE_Radius_Check

event syslog id 113022

action 0 cli命令“show clock”

action 1 cli命令“show aaa-server ISE”

action 2 cli命令“aaa-server ISE active host 10.10.10.150”

action 3 cli命令“aaa-server ISE active host 10.10.20.150”

action 4 cli命令“show aaa-server ISE”

操作5 cli命令“show capture radius decode dump”

输出文件append disk0:/ISE_Recover_With_Cap.txt

## EEM脚本说明

事件管理器小程序ISE_Radius_Check。 — *您为eem脚本命名。*

event syslog id 113022 — 您的触发器：（请参阅前面的说明）

action 0 cli命令“show clock” — *在故障排除时捕获准确时间戳的最佳实践，以便与客户端可以拥有的其他日志进行比较。*

action 1 cli命令“show aaa-server ISE” — *显示我们的aaa-server组的状态。在本例中，该组称为ISE。*

action 2 cli命令“aaa-server ISE active host 10.10.10.150” — *此命令用于使用该IP“恢复”aaa服务器。这使您可以继续尝试radius数据包以确定数据路径错误。*

action 3 cli command "aaa-server ISE active host 10.10.20.150" — *请参阅之前的命令说明。*

action 4 cli命令“show aaa-server ISE”。 - — *此命令验证服务器是否已恢复。*

action 5 cli命令“show capture radius decode dump” — *现在可对数据包捕获进行解码/转储。*

输出文件append disk0:/ISE_Recover_With_Cap.txt — *此捕获现在保存在ASA上的文本文件中，新结果将附加到末尾。*

## 最终步骤

最后，您可以将此信息上传到Cisco TAC案例，或者使用该信息分析流中的最新数据包，并弄清楚

RADIUS服务器标记为发生故障的原因。

文本文件可以解码，并在前面提到的数据包捕获配置生成器和分析器处转换为pcap。

## 真实世界示例

在下一个示例中，RADIUS流量的捕获被过滤掉。您会看到ASA是以。180结尾的设备，而RADIUS服务器以。21结尾

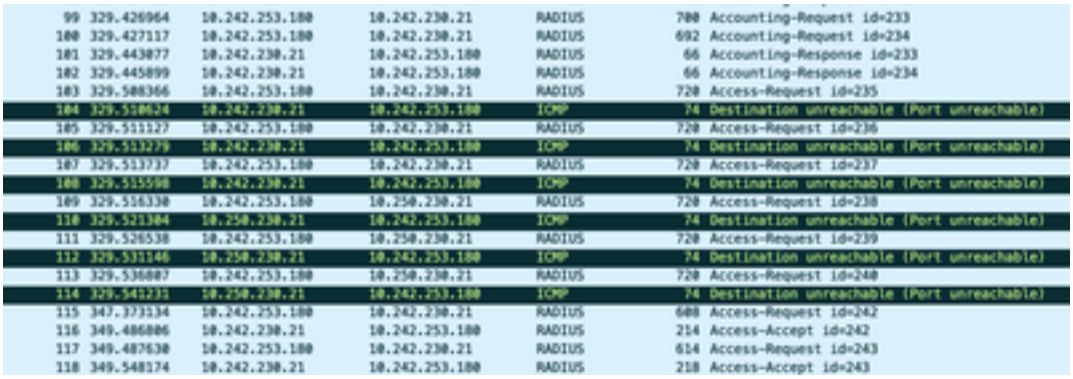
在本示例中，*两个RADIUS*服务器都返回一个“端口无法到达”，每个服务器一行3次。这会触发ASA将*两个RADIUS*服务器标记为彼此之间的停机（以毫秒为单位）。

### 结果

本示例中的每个。21地址都是F5 VIP地址。这意味着VIPS后面是PSN角色中的思科ISE节点集群。

由于F5缺陷，F5返回“端口无法到达”。

在本例中，Cisco TAC团队成功证明ASA按预期工作。也就是说，它发送了radius数据包并接收了3个之前不可达的端口，并影响标记为失败的Radius服务器：




# 相关信息

- **思科技术支持和下载**

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）。