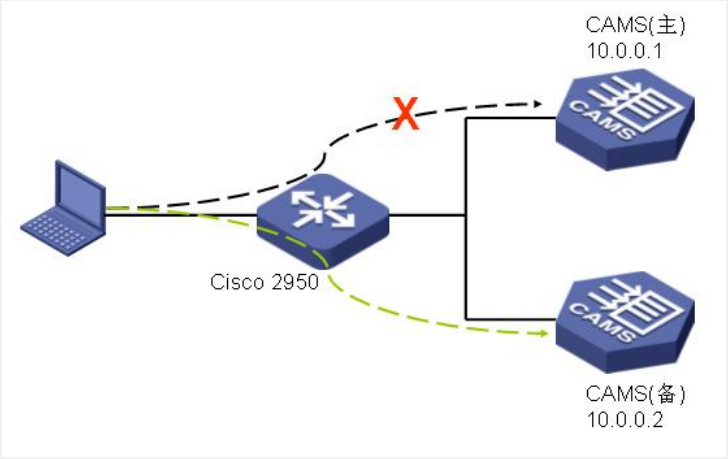
CAMS与Cisco交换机配合实现EAD时CAMS主机故障切换至备机认证用户身份认证通过后被策略服务器强制下线的问题

王涛1 2007-08-13 发表

CAMS与Cisco交换机配合实现EAD时CAMS主机故障切换至备机认证，用户身份认证通过后被策略服务器强制下线的问题

一、 组网：



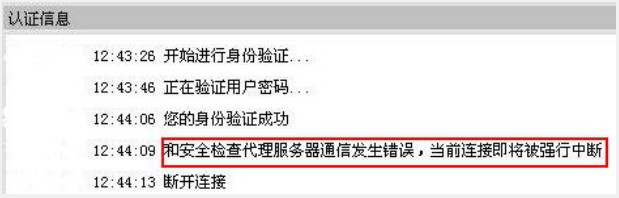
Cisco软件版本：C2950 Software (C2950-I6Q4L2-M), Version 12.1(22)EA4, RELEASE SOFTWARE (fc1)

CAMS软件版本：2.10-R0208P02

iNode客户端版本:2.40-F0326

二、 问题描述：

当主CAMS服务器发生故障不响应交换机发来的Radius报文时，Cisco交换机将根据其配置切换到备机认证。此时iNode客户端的认证信息中显示身份认证已通过，但三秒钟后提示“和安全检查代理服务器通信发生错误，当前连接即将被强行中断”，随后用户被强制下线。



三、 过程分析：

按照EAD的实现流程，安全检查在身份认证通过之后，此时策略服务器认为既然客户端已经主动发起安全检查请求，身份认证应该已经通过了，即能够在CAMS上查询到该用户在线。仅从客户端提示的报错信息推测下线原因为策略服务器在对某用户执行安全检查时，没有在CAMS配置台的在线用户列表中查询到该用户，故认为这是一种异常现象并立即强制用户下线。

CAMS配置台上显示用户是否在线完全依赖于该用户的计费开始报文，若交换机不支持发送计费开始报文或没有使能发送，则会造成用户身份认证通过但CAMS配置台的在线用户列表中查询不到该用户。

Cisco交换机使能发送计费开始/停止报文的配置命令为：

aaa accounting dot1x default start-stop group radius

首先查看Cisco交换机的配置，确认设备软件版本支持配置发送计费开始/停止报文，并确认配置无误。

Cisco交换机在实现Radius服务器的冗余时，在命令行下体现为指定多台Radius服务器的配置，如：

radius-server host 10.0.0.1 auth-port 1812 acct-port 1813 key cams

radius-server host 10.0.0.2 auth-port 1812 acct-port 1813 key cams

交换机发送认证请求时采用从上到下逐一尝试的方法，以上面的配置为例，先将认证请求发往主CAMS（10.0.0.1），若在可配置的重试次数内没有收到响应则再发往CAMS备机（10.0.0.2）。

那么我们首先需要确认的是当主机故障时，CAMS备机是否收到交换机发送的计费开始报文。

通过在CAMS备机上抓包分析，找到了问题原因在于Cisco交换机的Radius重发配置不仅对认证请求报文生效，对同一个用户同一个认证会话中的计费开始报文同样生效。

还是以上面的配置为例，Cisco 2950首先发认证请求至主CAMS，发现主CAMS没有响应，经过缺省3次的重试后，再将认证请求发往CAMS备机。CAMS备机正常回应认证成功报文后，交换机应该接着发送计费开始报文，但此时Cisco 2950交换机仍旧将计费开始报文首先发送至主CAMS。该计费开始报文同样需要重试缺省的3次后才会尝试发往CAMS备机。而此时iNode客户端早已经收到了认证成功的报文，计费报文的交互和客户端没有关系。按照EAD的流程，客户端收到认证成功报文后即发起与CAMS备机的策略服务器的会话。但此时CAMS备机还没有来得及收到计费开始报文（发往主CAMS的计费开始报文还没有重试完毕），导致CAMS备机上查询不到在线用户。该用户请求安全检查，但策略服务器查询不到该用户在线，于是客户端报“和安全检查代理服务器通信发生错误，当前连接即将被强行中断”，用户被强制下线。

四、　　解决方法：

更改Cisco 2950的配置，全局下增加一条命令：

radius-server deadtime *

增加该命令后，当主CAMS服务器发生故障不响应交换机发来的Radius报文时，交换机第一次尝试之后，将把主CAMS标记为dead，在之后的*分钟内，交换机再收到认证请求则直接跳过主CAMS，发送到下一个Radius服务器地址（即CAMS备机）。当超过*分钟后，交换机会再次尝试将Radius报文发往主CAMS。

增加此配置后，主CAMS服务器发生故障后，每*分钟内，第一个发起认证的用户将会被强制下线，其他用户正常。当然，这第一个用户再次发起认证也能够通过安全检查正常上线。用户数量越大则该影响越小。

另外，如果更改Radius报文的缺省重试次数以及重试间隔，也可以解决该问题。身份认证结束到安全检查开始之间大约间隔3秒钟。我们需要更改配置，使得计费开始报文在3秒内重试完毕并发往CAMS备机。

可以更改为如下形式，全局下增加两条命令：

radius-server retransmit 1 //Radius报文只重试一次

radius-server timeout 1　//发送间隔1秒钟

或

radius-server retransmit 0 //Radius报文不重试

radius-server timeout 2　//发送间隔2秒钟

更改Radius报文的缺省重试次数所带来的弊端是当网络状态不太好时，CAMS主备机切换过于频繁。当有计费需求时，对费用的准确性影响很大。另外，CAMS冷备方案中主备机的数据库同步不是实时的，主备机切换过于频繁对数据库同步的事实性要求就非常高了。

首先建议配置radius-server deadtime *，这样能够最大程度上免去不必要的报文重试，提高CAMS主备机切换后用户上线的速度。

如果用户的网络状况很好（不会出现Radius报文在发送过程中被丢弃的情况），并且希望当CAMS主备机切换后，每一个用户都能正常通过EAD认证（不牺牲deadtime时间内处理的第一次认证请求），那么可以考虑更改Radius报文的缺省重试次数以及重试间隔。