安全数据库审计没有日志的排查和理解

数据库审计 **孔梦龙** 2022-06-10 发表

组网及说明

数据库获得流量的两种方式：

方式一：直接将流量镜像给数据口的口，此时不需要在网卡上配置IP，但是需要勾选监听；

方式二：通过探针的方式，探针镜像数据库上网卡的流量然后通过三层发给数据库审计系统；

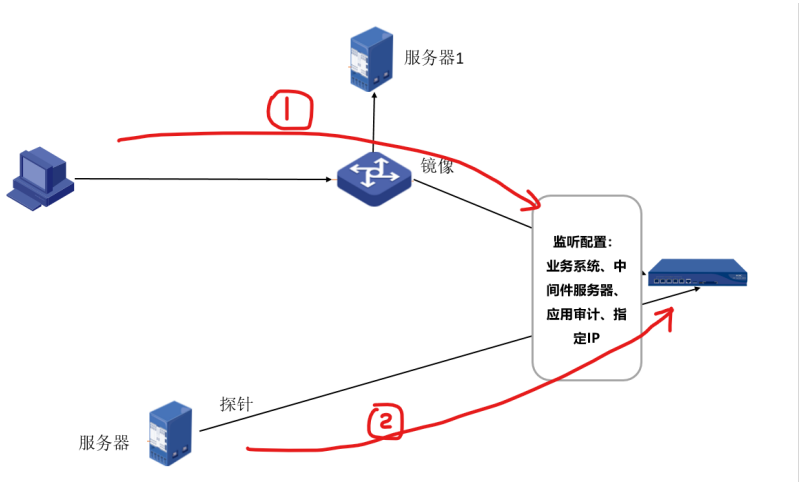
不管哪一种方式，都需要配置【监听配置】来审计流量，简单来理解四种方式：

（1）业务系统：正常的审计流量，需要配置服务器的IP和端口

（2）中间件服务器：一般用在HTTP类型的流量

（3）应用审计：针对telnet、FTP之类的

（3）指定IP审计：对收到的流量过滤；虽然接受的是全集流量，但是审计之选其中指定的IP统计



告警信息

无

告警信息

问题描述

无日志的时候怎么排查：

此问题一般是因为配置问题导致不能正常审计到数据。请按照如下操作检查处理：

(1)　确认镜像流量是否正确（是否包含目标审计对象的双向流量）；

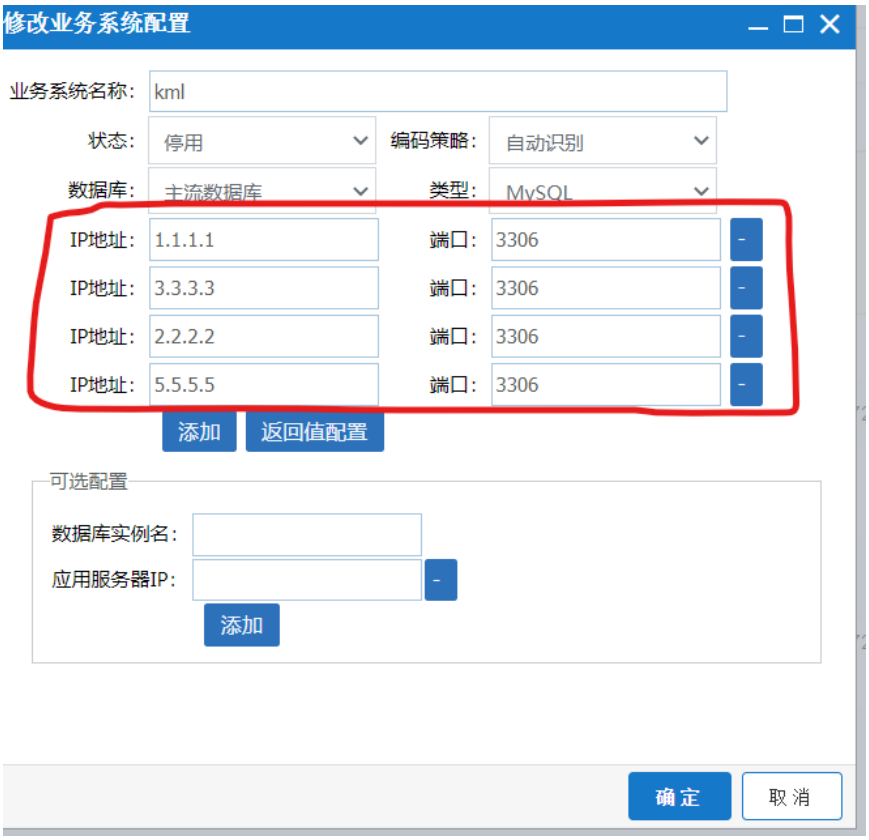
(2)　“策略中心”-“网络配置”页面中的监听网卡是否正常设置并接入镜像数据；

方式一：镜像的口要连接，勾选监听，开启网卡

方式二：要配置地址，到流量探针的3层路由可达；

(3)　“策略中心”- “监听配置”页面中的各项配置是否按照实际情况正确配置；

一定要填写争取的IP和端口



(4)　“策略中心”- “监听配置”-“指定IP审计”页面中的配置是否正确；

//这里尽量勾选上vlan，万一来的流量带有vlan

(5)　“运行状态”或者“系统服务”页面中的监听服务是否启动；

(6)　“策略中心”-“事件定义”页面中的规则中的规则动作是否设置为丢弃；

(7)　“审计中心”-“SQL模板”页面中的SQL模板是否大量或者全部设置为“丢弃此类语句”。

(8)　将流量发到电脑上，然后抓包看，真实的流量的IP和端口，看配置的和目标是否一致；

过程分析

排查过程如上

解决方法

排查过程如上