NTA&UBA基于采集器创建用户行为审计任务

NTA UBA 马永鸿 2020-11-27 发表

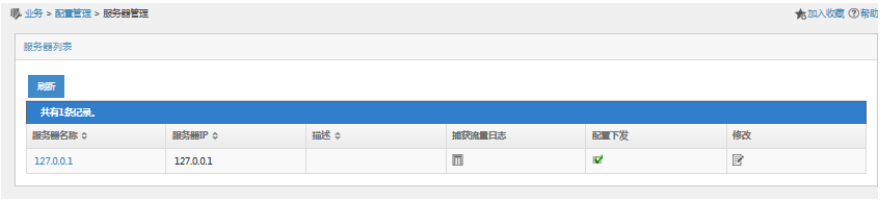
组网及说明

不涉及

配置步骤

1. 下发服务器配置

(1) 在配置管理页面，单击“服务器管理”链接，进入服务器管理页面



(2) 单击修改图标，进入服务器配置页面

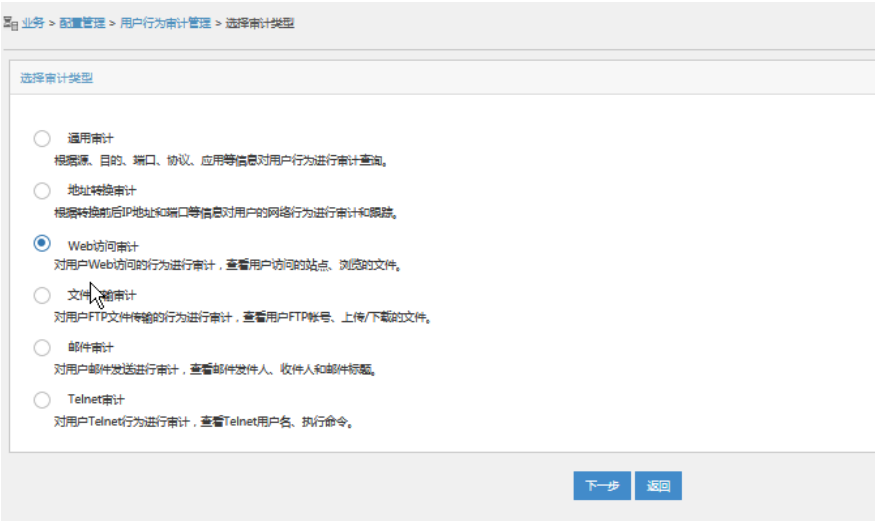
(3)配置服务器参数。

在上图的基本信息中各项均保持默认配置即可。在用户行为审计中的设备信息列表中选中采集器“2.2.2.1”并启用四类特殊应用监控。内网信息中增加内网用户的三个网段。单击<下发>按钮保存并下发服务器配置。

2. 增加审计任务

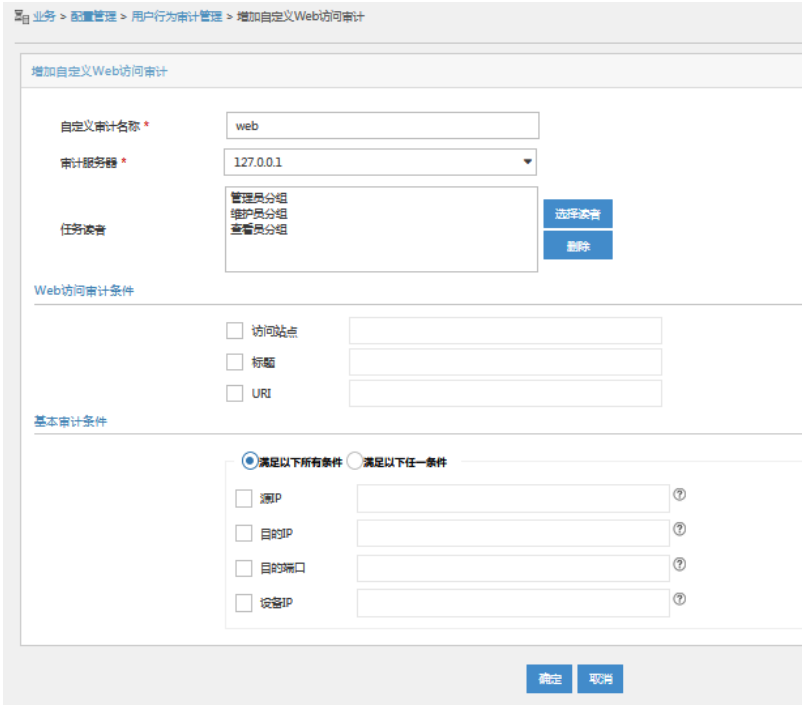
点击“网络流量分析与审计快速配置向导”中“用户行为审计管理”链接，进入自定义行为审计页面，增加一个用户行为审计任务。

单击<增加>按钮，进入选择审计类型界面。

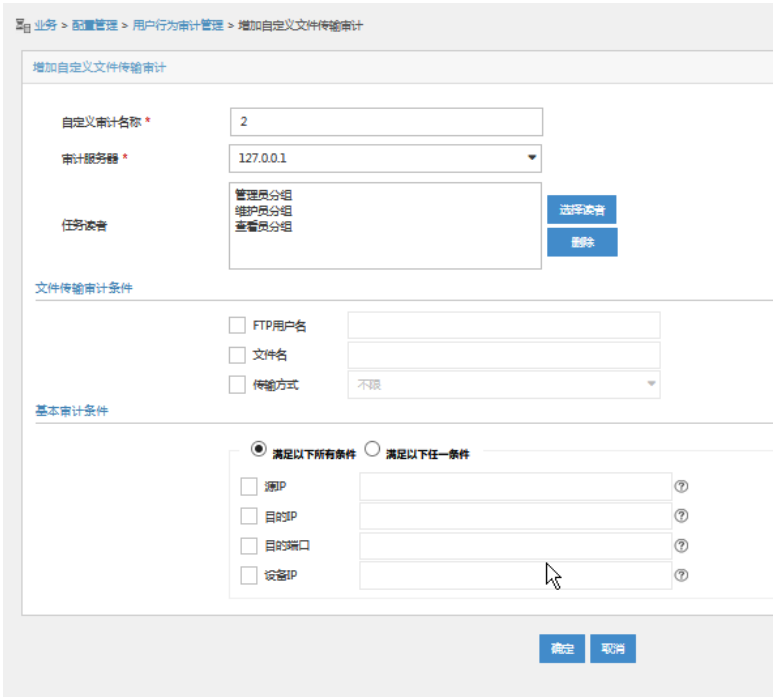


选择任务类型后单击<下一步>按钮，进入相应的任务配置页面

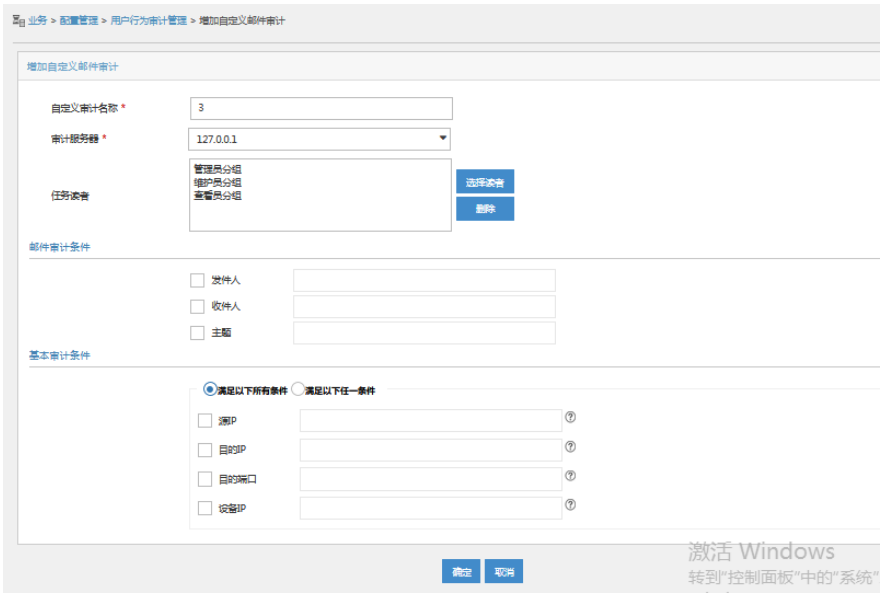
Web 访问审计配置页面



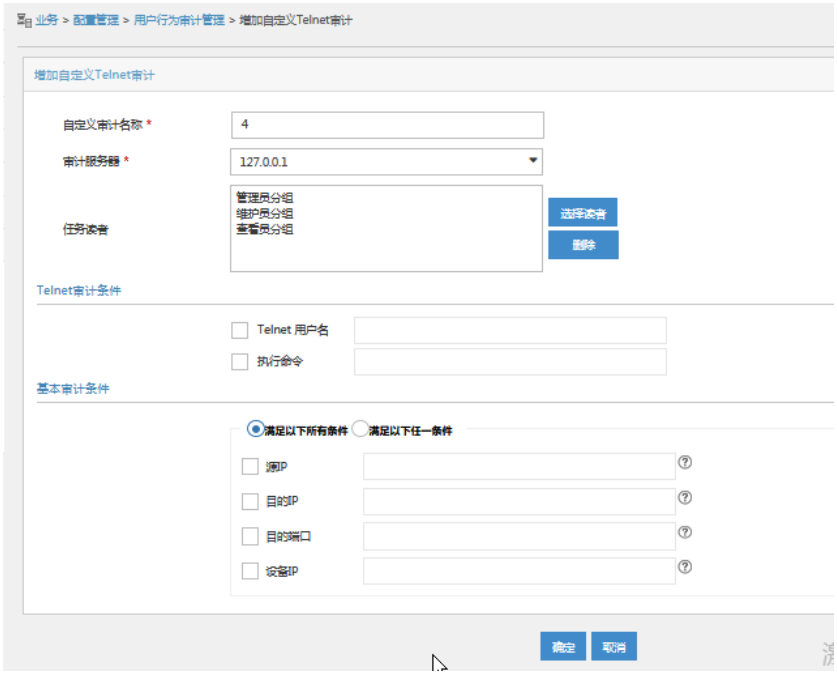
文件传输审计任务配置页面



邮件审计任务配置页面



Telnet 审计任务配置页面



根据任务类型，完成如下操作：

• 根据审计内容，输入自定义通用审计名称。

• 选择设备所属的流量分析服务器，本例中选择 127.0.0.1。

• 选择查询条件，本例中选中“满足以下所有条件”。

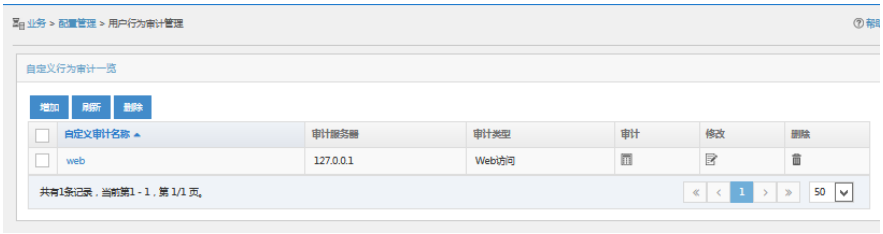
单击<确定>按钮，完成增加审计任务的操作。

3. 验证结果

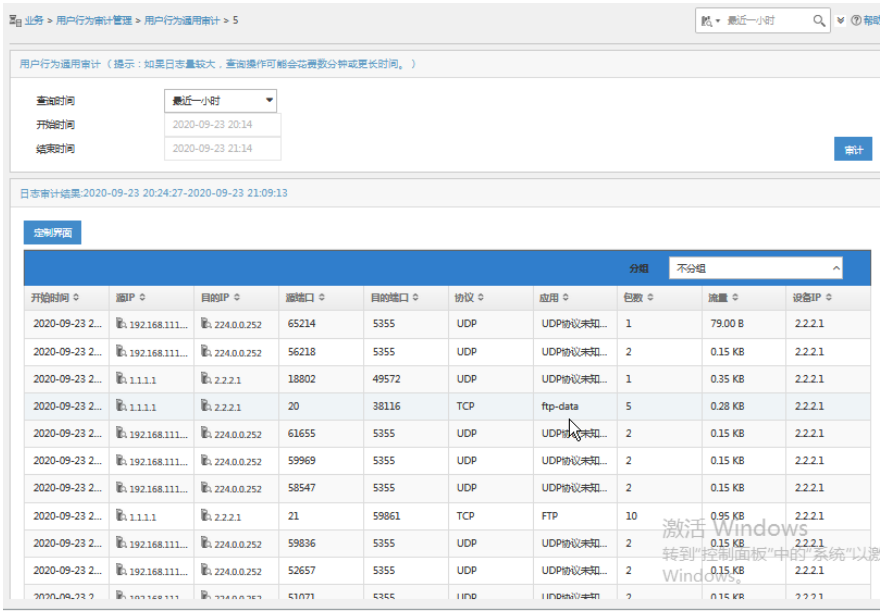
(1) 查看已创建的任务

完成任务增加后，在左导航树中出现四类审计任务菜单项

分别单击上述四个菜单项，进入相应的审计任务列表。例如，查看Web访问审计任务如图所示。



数据不会立即产生，请等待一段时间后，点击“Web 访问审计”对应的图标，可以查看到审计结果。



配置关键点

无