



(12)发明专利申请

(10)申请公布号 CN 110113178 A

(43)申请公布日 2019.08.09

(21)申请号 201811329498.0

(22)申请日 2018.11.09

(71)申请人 深圳互联先锋科技有限公司
地址 518000 广东省深圳市福田区深南中路2008号华联大厦2楼(203-212)

(72)发明人 杨海滨

(51)Int.Cl.

H04L 12/24(2006.01)

H04L 29/08(2006.01)

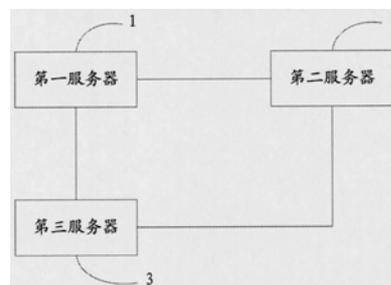
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种网络设备监控主备装置、方法及系统

(57)摘要

本发明公开一种网络设备监控主备装置、方法及系统,所述装置包括:第一服务器、第二服务器和第三服务器,所述第一服务器与所述第二服务器连接,所述第三服务器分别与所述第一服务器和所述第二服务器连接,所述第一服务器和所述第二服务器用于互相监控对方服务器的存活状态,所述第三服务器用于接收所述第一服务器和所述第二服务器的数据并将所述数据进行校对后发送至客户端。采用本发明的上述装置能够减少网络监控误报的情况发生。



1. 一种网络设备监控主备装置,其特征在于,所述装置包括:第一服务器、第二服务器和第三服务器,所述第一服务器与所述第二服务器连接,所述第三服务器分别与所述第一服务器和所述第二服务器连接,所述第一服务器和所述第二服务器用于互相监控对方服务器的存活状态,所述第三服务器用于接收所述第一服务器和所述第二服务器的数据并将所述数据进行校对后发送至客户端。

2. 根据权利要求1所述的网络设备监控主备装置,其特征在于,所述第一服务器采用PRTG监控服务器。

3. 根据权利要求1所述的网络设备监控主备装置,其特征在于,所述第二台服务器采用CACTI监控服务器。

4. 根据权利要求1所述的网络设备监控主备装置,其特征在于,所述第一服务器和所述第二台服务器采用SNMP协议获取被监控设备的状态。

5. 根据权利要求1所述的网络设备监控主备装置,其特征在于,所述第三服务器采用日志服务器。

6. 根据权利要求1所述的网络设备监控主备装置,其特征在于,所述第一服务器和所述第二服务器内部包含报警灯,所述存活状态通过所述报警灯的状态进行显示。

7. 一种网络设备监控主备方法,其特征在于,所述方法包括:

获取第一服务器的第一报警灯数据状态;

获取第二服务器的第二报警灯数据状态;

对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

将所述报警信息发送至客户端。

8. 根据权利要求7所述的网络设备监控主备方法,其特征在于,所述将所述报警信息发送至客户端,具体包括:

将所述报警信息采用短信形式或者邮件形式发送至客户端。

9. 一种网络设备监控主备系统,其特征在于,所述系统包括:

第一获取模块,用于获取第一服务器的第一报警灯数据状态;

第二获取模块,用于获取第二服务器的第二报警灯数据状态;

校正模块,用于对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

发送模块,用于将所述报警信息发送至客户端。

10. 根据权利要求9所述的网络设备监控主备系统,其特征在于,所述发送模块,具体包括:

发送单元,用于将所述报警信息采用短信形式或者邮件形式发送至客户端。

一种网络设备监控主备装置、方法及系统

技术领域

[0001] 本发明涉及网络监控领域,特别是涉及一种网络设备监控主备装置、方法及系统。

背景技术

[0002] 随着IDC机房机柜的增加,服务器及交换机数量的增多,网络设备的监控相当重要,可以先知道服务器是不是被入侵了或者攻击别人,是否发垃圾邮件等违规行为,也可以控制服务器的流量。但是目前的监控系统非常单一,经常出现误报的问题,而且如果监控服务器出现意外了,那什么监控信息都没有了。

发明内容

[0003] 本发明的目的是提供一种网络设备监控主备装置、方法及系统,能够避免网络监控误报。

[0004] 为实现上述目的,本发明提供了如下方案:

[0005] 一种网络设备监控主备装置,所述装置包括:第一服务器、第二服务器和第三服务器,所述第一服务器与所述第二服务器连接,所述第三服务器分别与所述第一服务器和所述第二服务器连接,所述第一服务器和所述第二服务器用于互相监控对方服务器的存活状态,所述第三服务器用于接收所述第一服务器和所述第二服务器的数据并将所述数据进行校对后发送至客户端。

[0006] 可选的,所述第一服务器采用PRTG监控服务器。

[0007] 可选的,所述第二台服务器采用CACTI监控服务器。

[0008] 可选的,所述第一服务器和所述第二台服务器采用SNMP协议获取被监控设备的状态。

[0009] 可选的,所述第三服务器采用日志服务器。

[0010] 可选的,所述第一服务器和所述第二服务器内部包含报警灯,所述存活状态通过所述报警灯的状态进行显示。

[0011] 一种网络设备监控主备方法,所述方法包括:

[0012] 获取第一服务器的第一报警灯数据状态;

[0013] 获取第二服务器的第二报警灯数据状态;

[0014] 对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

[0015] 将所述报警信息发送至客户端。

[0016] 可选的,所述将所述报警信息发送至客户端,具体包括:

[0017] 将所述报警信息采用短信形式或者邮件形式发送至客户端。

[0018] 一种网络设备监控主备系统,所述系统包括:

[0019] 第一获取模块,用于获取第一服务器的第一报警灯数据状态;

[0020] 第二获取模块,用于获取第二服务器的第二报警灯数据状态;

[0021] 校正模块,用于对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

[0022] 发送模块,用于将所述报警信息发送至客户端。

[0023] 可选的,所述发送模块,具体包括:

[0024] 发送单元,用于将所述报警信息采用短信形式或者邮件形式发送至客户端。

[0025] 根据本发明提供的具体实施例,本发明公开了以下技术效果:本发明提供一种网络设备监控主备装置,所述装置包括:第一服务器、第二服务器和第三服务器,所述第一服务器与所述第二服务器连接,所述第三服务器分别与所述第一服务器和所述第二服务器连接,所述第一服务器和所述第二服务器用于互相监控对方服务器的存活状态,所述第三服务器用于接收所述第一服务器和所述第二服务器的数据并将所述数据进行校对后发送至客户端。采用本发明的上述装置能够减少网络监控误报的情况发生。

附图说明

[0026] 为了更清楚地说明本发明实施例或现有技术中的技术方案,下面将对实施例中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0027] 图1为本发明实施例网络设备监控主备装置组成模块图;

[0028] 图2为本发明实施例PRTG配置的页面图;

[0029] 图3为本发明实施例网络设备监控主备方法流程图;

[0030] 图4为本发明实施例网络设备监控主备系统结构图;

[0031] 图5为本发明实施例网络设备监控主备装置示意图。

具体实施方式

[0032] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0033] 本发明的目的是提供一种网络设备监控主备装置、方法及系统,能够避免网络监控误报。

[0034] 为使本发明的上述目的、特征和优点能够更加明显易懂,下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0035] 图1为本发明实施例网络设备监控主备装置组成模块图。如图1所示,一种网络设备监控主备装置,所述装置包括:第一服务器1、第二服务器2和第三服务器3,所述第一服务器与所述第二服务器2连接,所述第三服务器3分别与所述第一服务器1和所述第二服务器2连接,所述第一服务器1和所述第二服务器2用于互相监控对方服务器的存活状态,所述第三服务器3用于接收所述第一服务器和所述第二服务器2的数据并将所述数据进行校对后发送至客户端。

[0036] 所述第一服务器1采用PRTG监控服务器。所述第二服务器2采用CACTI 监控服务

器。所述第一服务器和所述第二服务器采用SNMP协议获取被监控设备的状态。所述第三服务器3采用日志服务器。

[0037] 所述第一服务器1和所述第二服务器2内部包含报警灯,所述存活状态通过所述报警灯的状态进行显示。

[0038] 软件介绍:

[0039] PRTG全称为Paessler Router Traffic Grapher,是一款功能强大的免费且可以通过路由器等设备上的SNMP协议取得流量资讯并产生图形报表的软件,可以产生企业内部网络包括服务器,路由器,交换机,员工计算机等多种设备的网络流量图形化报表,并能够对这些报表进行统计和绘制,帮助网络管理员找到企业网络的问题所在,分析网络的升级方向。当然该软件可以在绘制完毕后将图形图表以页面的形式反馈给我们,这样网络管理员可以通过网络中的任何一台计算机访问配置了PRTG的计算机,实现远程管理,查看和维护网络流量的目的。

[0040] CACTI是一套基于PHP、MySQL、SNMP和RRDtool开发的网络流量监测图形分析工具,它通过snmpget来获取数据使用RRDtool绘图,简化RRDtool 使用。提供了非常强大的数据和用户管理功能,可以指定每一个用户能查看树状结构、主机设备以及任何一张图,还可以与LDAP结合进行用户认证,同时也能自定义模板。在历史数据展示监控方面,其功能相当不错。

[0041] CACTI通过添加模板,使不同设备的监控添加具有可复用性,并且具备可自定义绘图的功能,具有强大的运算能力(数据的叠加功能)。

[0042] 安装3台服务器的软件后,把监控的服务器、交换机端口全部用SNMP协议录入软件的模板,形成监控拓扑图。做好阈值报警设置,短信或者邮箱设置报警。

[0043] 图5为本发明实施例网络设备监控主备装置示意图。如图5所示,PRTG服务器和CACTI服务器通过SNMP协议获取监控的服务器、交换机端口的流量,CPU内存值,当网络中断或者超过阈值主设备会自动告警。当其中任何一个设备出现故障,另外一台会发生报警并替代其功能。所有监控的日志会发送到第三服务器的日志服务器。日志服务器会收到两个不同软件的警告,对警告过滤后进行校对数据,并生产报表,来参考设置的模板和阈值是否正常。两台监控服务器可以分别监控到信息,分别报警,并且把监控信息发到日志服务器。

[0044] 当所述第一服务器和所述第二服务器中一台监控服务器出现故障了,另外一台可以马上使用,建议两台服务器放置不同的机房。

[0045] 使用日志服务器的日志分析功能,可以同时收到信息告警后才发送短信或者邮件警告。

[0046] 两台监控服务器互相监控对方的状态,当其中一台故障了,另外一台会报警,避免监控服务器发生故障后无法知道信息。

[0047] 图2为本发明实施例PRTG配置的页面图。

[0048] 本发明的优点是:

[0049] 本发明的装置具有高可用性、操作方便、稳定性好、安全性高的特点。

[0050] 本发明中的第一服务器和第二服务器之间可以互相备份。

[0051] 图3为本发明实施例网络设备监控主备方法流程图。如图3所示,一种网络设备监

控主备方法,所述方法包括:

[0052] 步骤101:获取第一服务器的第一报警灯数据状态;

[0053] 步骤102:获取第二服务器的第二报警灯数据状态;

[0054] 步骤103:对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

[0055] 步骤104:将所述报警信息发送至客户端。

[0056] 步骤104,具体包括:

[0057] 将所述报警信息采用短信形式或者邮件形式发送至客户端。

[0058] 图4为本发明实施例网络设备监控主备系统结构图。如图4所示,一种网络设备监控主备系统,所述系统包括:

[0059] 第一获取模块201,用于获取第一服务器的第一报警灯数据状态;

[0060] 第二获取模块202,用于获取第二服务器的第二报警灯数据状态;

[0061] 校正模块203,用于对所述第一报警灯数据状态和所述第二报警灯数据状态进行校正,得到报警信息;

[0062] 发送模块204,用于将所述报警信息发送至客户端。

[0063] 所述发送模块204,具体包括:

[0064] 发送单元,用于将所述报警信息采用短信形式或者邮件形式发送至客户端。

[0065] 本说明书中各个实施例采用递进的方式描述,每个实施例重点说明的都是与其他实施例的不同之处,各个实施例之间相同相似部分互相参见即可。对于实施例公开的系统而言,由于其与实施例公开的方法相对应,所以描述的比较简单,相关之处参见方法部分说明即可。

[0066] 本文中应用了具体个例对本发明的原理及实施方式进行了阐述,以上实施例的说明只是用于帮助理解本发明的方法及其核心思想;同时,对于本领域的一般技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处。综上所述,本说明书内容不应理解为对本发明的限制。

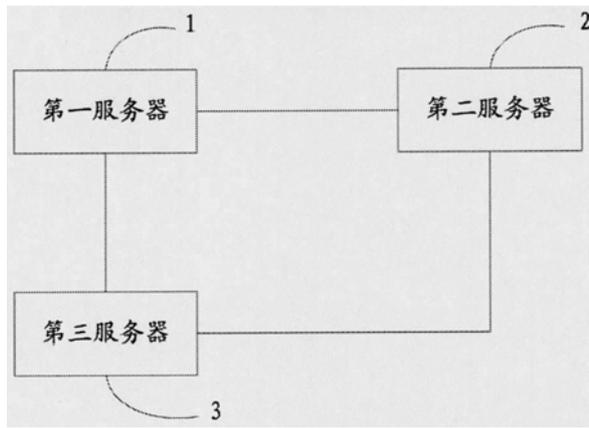


图1

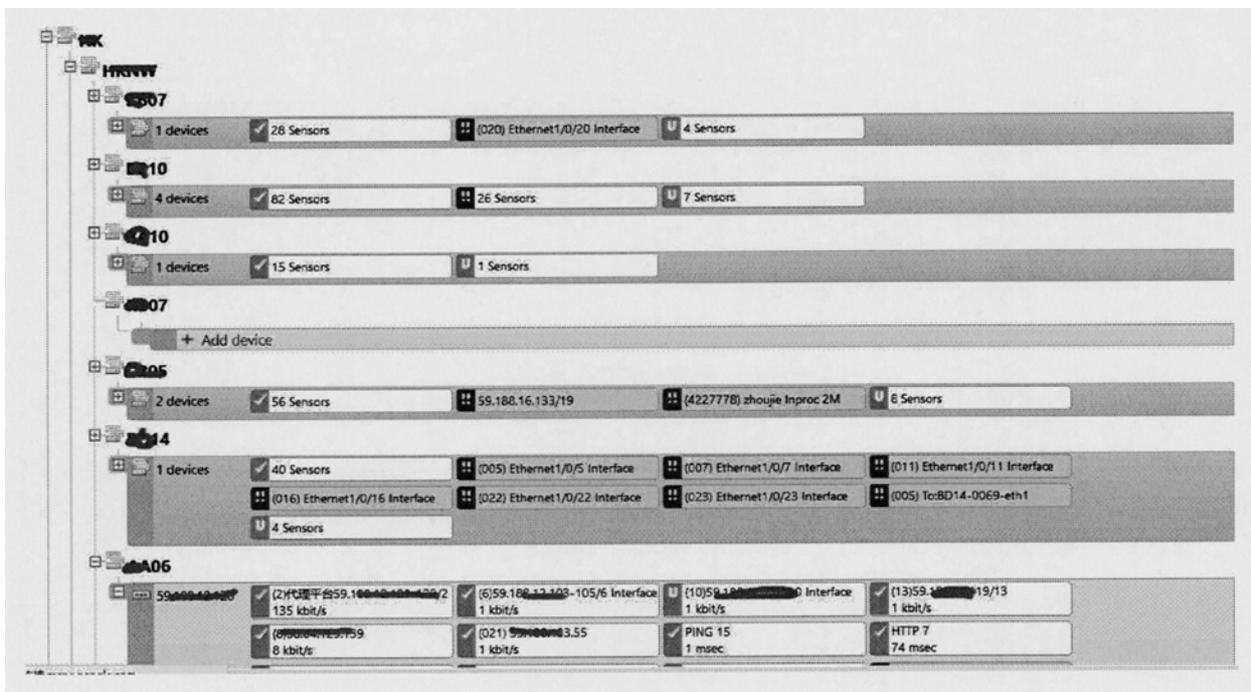


图2

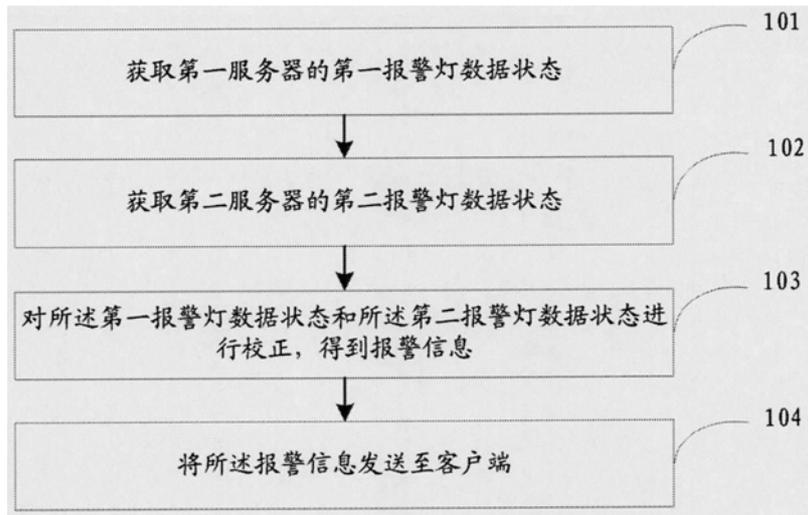


图3

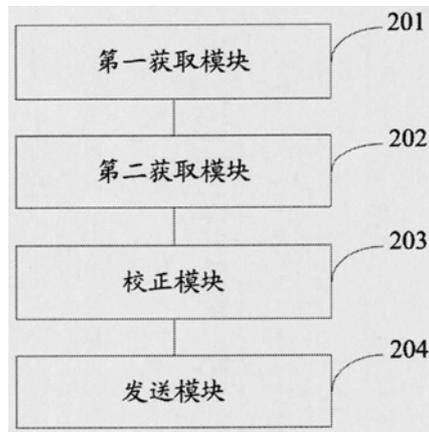


图4

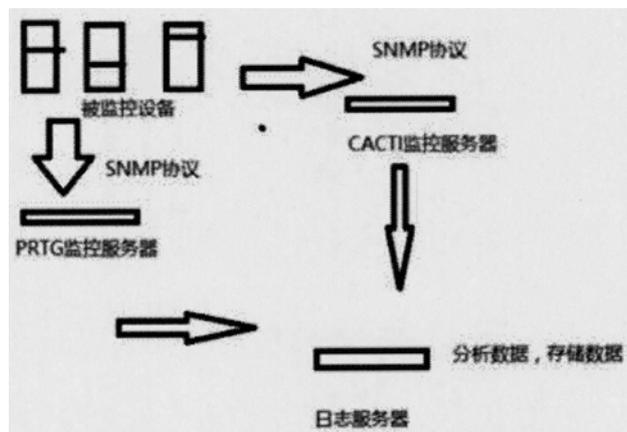


图5