

告警模块设计创新 点举例说明

作者：朱菁菁
时间：20190719

目录

1

背景及目的

2

告警主页优化

3

自定义告警指标配置



背景及目的

阐述背景及目的

背景及目的

背景

告警是监管系统及软件本身运行异常情况的一种展现方式，为运维人员快速定位排除故障提供参考与帮助，提升排查处理效率。运管中心提供了告警展示、查询、处理、策略配置功能，实现了对告警的全生命周期管理。您可以在“告警处理”模块，进行异常告警的查看和处理。为了帮助用户提供解决告警的工作效率，需要对告警处理模块进行改版优化。

Program Title

Sub Title

首页

告警处理

状态监控

系统维护

日志分析

知识库

系统管理

sysadmin

11:05

2018/6/27

☐ 全部

☒ 未处理

☐ 已解决

☐ 已忽略

搜索告警

导出全部

批量解决

批量忽略

当前搜索结果：

紧急：1

一般：0

提醒：4

<input type="checkbox"/>	告警等级	最新告警时间	告警来源	告警策略	告警次数	状态	操作
<input type="checkbox"/>	<div><div></div>紧急</div>	2018-06-25 02:00:00	中心管理服务器>设备接入框架 (1.3.1)	高负载	2	未处理	详情
<input type="checkbox"/>	<div><div></div>提醒</div>	2018-06-25 02:00:00	中心管理服务器>设备接入框架 (1.3.1)	Text1	23	未处理	详情
<input type="checkbox"/>	<div><div></div>提醒</div>	2018-06-25 02:00:00	中心管理服务器>设备接入框架 (1.3.1)	Text2	23	未处理	详情
<input type="checkbox"/>	<div><div></div>提醒</div>	2018-06-25 02:00:00	中心管理服务器>设备接入框架 (1.3.1)	Text3	23	未处理	详情
<input type="checkbox"/>	<div><div></div>提醒</div>	2018-06-25 02:00:00	中心管理服务器>设备接入框架 (1.3.1)	Text4	23	未处理	详情

目的

- 提高用户查看、处理告警的工作效率；
- 帮助用户有效配置告警策略；

下面将介绍部分我在根据需求思考设计的过程中产出的一些设计重点、疑难点和亮点。



告警主页优化

阐述疑难/重点、分析及最终方案亮点设计



设计优化前

重点/疑难点

当前组件的告警页面无法及时看到告警详情，而告警处理对于技术支持来说是每天必做的繁重的工作，提高用户操作高效性非常关键。

场景分析

【场景1】

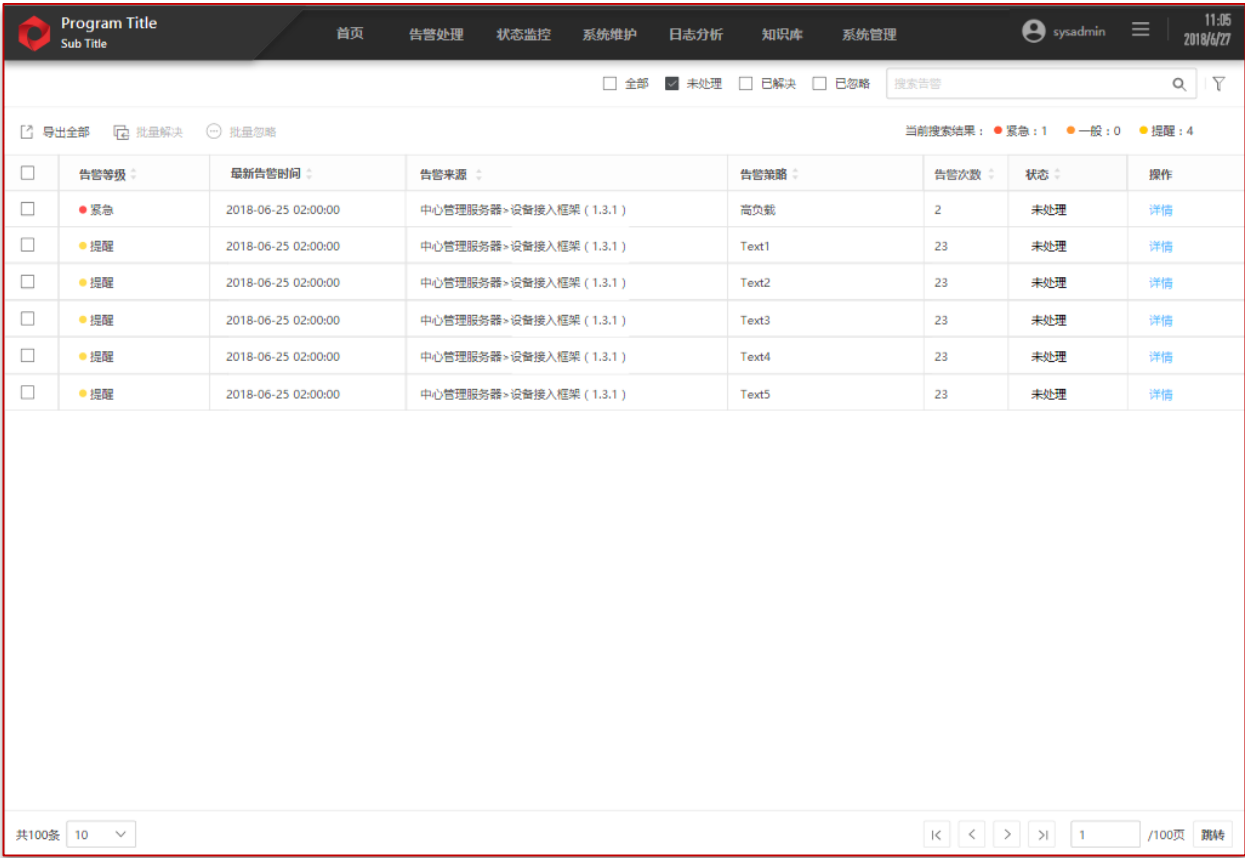
用户每天都要检查是否有新告警产生，严重程度是什么，什么时候产生的报警，是什么告警，以前是否出现过相同告警。

分析：需要给予用户更为便捷的查看模式，减少繁复的操作。

【场景2】

某些组件的告警频繁触发，而对于用户来说紧急程度低，数量多，每天进入模块查看的时候，容易将其他等级的告警数据淹没，无法在当前模块进行配置修改。

分析：告警模块缺少告警配置功能，与参数配置的告警配置模块关联性弱，可以通过提供修改告警阈值功能较少一些无效告警。

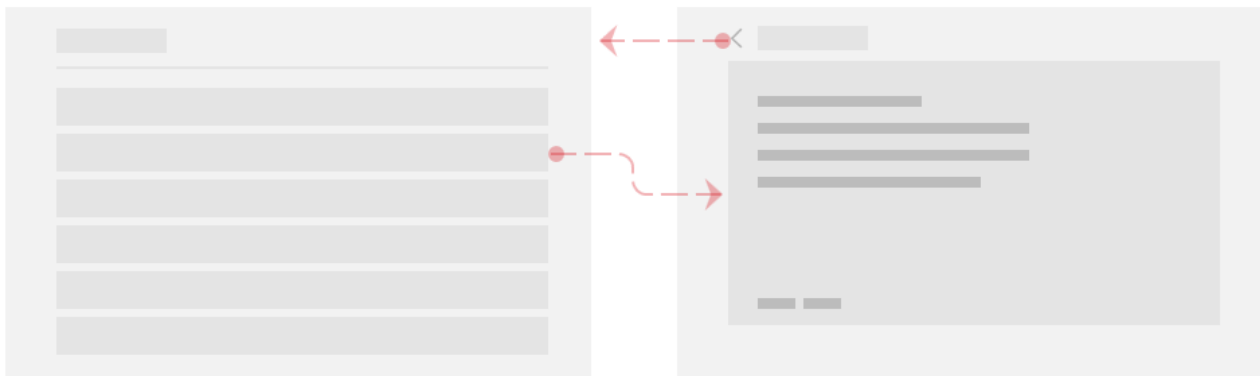


操作布局分析

- 优化前列表布局及操作拆解：

表格每一行告警数据都需要查看具体详情，切换查看是高频操作，而要查看详情需要点击打开二级页面，查看完详情后关闭页面再回到主页，才能继续切换另一条告警打开详情页查看详情。

繁琐的两步操作，不利于这类列表数据高频切换的用户使用场景。



- 优化思考：

将“两步操作”简化为“一步到位”。
表格的告警选中后即在右侧查看它的详情，即点即看即操作。

切换查看流畅无阻碍，节省操作成本，帮助提高查阅和操作效率。



同时，“C位”显示重点内容，更容易让我们的用户关注到。

优化查看详情的交互方式

将内置的详情页前置到主页显示，切换表格告警数据的同时联动查看该告警的详情信息，帮助用户在一个界面完成查看和处理，提高工作效率。

The screenshot displays the Hikvision alarm management interface. The top navigation bar includes links for 首页 (Home), 告警处理 (Alarm Processing), 状态监控 (Status Monitoring), 系统维护 (System Maintenance), 日志分析 (Log Analysis), 知识库 (Knowledge Base), and 系统管理 (System Management). The user is logged in as sysadmin on 2018/6/27 at 11:05.

The main content area is divided into two sections. The left section shows a table of alerts with columns for 告警等级 (Alert Level), 最新告警时间 (Latest Alert Time), 告警描述 (Alert Description), 告警策略 (Alert Strategy), 告警次数 (Alert Count), and 状态 (Status). The right section provides a detailed view of a selected alert, including 告警来源 (Alert Source), 告警时间 (Alert Time), 告警描述 (Alert Description), and 处理建议 (Handling Suggestions).

告警等级	最新告警时间	告警描述	告警策略	告警次数	状态
紧急	2018-06-25 02:00:00	关键进程devSearch.exe已停止	高负载	2	未处理
一般	2018-06-25 02:00:00	C: D: E: F: 磁盘持续300s队列长度68以...	Text1	23	未处理
一般	2018-06-24 02:00:00	关键进程VsHub.exe已停止	Text2	23	未处理
提醒	2018-06-25 02:00:00	内存占用38MB, 高于1MB	Text2	33	已解决
提醒	2018-06-24 02:00:00	内存占用39MB, 高于2MB	Text2	23	已忽略
提醒	2018-06-23 02:00:00	剩余内存低于1024MB	Text2	23	已忽略
提醒	2018-06-22 02:00:00	服务已停止, 依赖于该组件的服务无法...	Text2	23	未处理
提醒	2018-06-21 02:00:00	服务器与授时服务器时间差为28803s...	Text2	23	已解决

The detailed view on the right shows the following information:

- 告警来源:** 中心管理服务器 > 消息推送 > mpms监控数据分析
- 告警时间:** 2018-06-01 12:00:00 (首次告警时间)
2018-06-25 02:00:00 (最新告警时间)
- 告警描述:** 持续5分钟CPU占用率超过90%, 持续5分钟CPU占用率超过90%, 持续5分钟CPU占用率超过90%持续5分钟CPU占用率超过90%, 就持续5分钟CPU占用率超过90%, 持续5分钟CPU占用率超过90%。率超...
- 处理建议:**
 1. 进入日志分析页面查看该组件的系统日志进行分析。
 2. 如果超出研发给出的最大句柄数, 手动创建该进程的堆dump, 并将日志和dump交与研发分析。
 3. 重启服务

告警来源支持点击跳转到告警源页面

将对用户来说最需要了解的告警描述和处理建议放置在页面中心位置，加强视觉焦点，引导用户查看。

底部操作常驻方便操作，当详情内容过多的时候，不随滚动条滚动而消失。

优化追加处理建议功能

在系统提供的处理建议基础上，支持用户针对当前告警人工录入经过实战得出的更优的解决建议，一方面，扩充系统建议库，弥补系统所提供建议的不足，另一方面，为其他用户解决同类告警时提供解决参考。



- 处理建议展示全部建议方法；
- 若该建议中关联到支持查看日志，则出现【查看日志】功能入口，帮助用户快速点击查看相关日志；
- 提取处理建议中的标签类型，关联【知识库】模块，支持点击，帮助用户直接过滤出标签类相关文章和经验案例，帮助综合解决告警。



- 若针对该条未解决的告警，有用户曾填过的处理记录，则显示 添加的时间、添加人、记录描述；
- 记录按上新下旧排序显示；
- 由于面板空间有限，记录默认显示近3条数据，支持查看更多。



根据使用场景优化告警操作记录

根据业务需求，告警的操作有解决和忽略两种

场景一：查询这条告警之前是被谁忽略的

● 紧急

服务器线程数超限

告警来源
中心管理服务器 > 消息推送 > mpms监控数据分析

告警时间
2018-06-01 12:00:00 (首次告警时间)
2018-06-25 02:00:00 (最新告警时间)

告警描述
持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%持续5分钟CPU占用率超过90%，就持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%。率超...
[查看更多](#)

处理建议

【忽略】记录

2019-02-02 15:11:32 张三

追加处理建议...

【忽略】记录

2019-02-02 15:11:32 张三

解决

场景二：查询这条告警之前的解决人和方法

● 紧急

服务器关键进程停止

告警来源
中心管理服务器 > 消息推送 > mpms监控数据分析

告警时间
2018-06-01 12:00:00 (首次告警时间)
2018-06-25 02:00:00 (最新告警时间)

告警描述
持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%持续5分钟CPU占用率超过90%，就持续5分钟CPU占用率超过90%，持续5分钟CPU占用率超过90%。率超...
[查看更多](#)

处理建议
1、进入日志分析页面查看该组件的系统日志进行分析。
2、如果超出研发给出的最大句柄数，手动创建该进程的堆dump，并将日志和dump交与研发分析。
3、重启服务
[查看日志](#)

句柄数 dump 标签1 标签2

追加处理建议...

【解决】记录

2019-02-02 15:11:32 Administrator
系统自动处理

【解决】记录

2019-02-02 15:11:32 Administrator
系统自动处理

若解决人是系统，系统对于该告警做了自动化处理，则“处理人”显示为【Administrator】，使用户清楚是【系统自动处理】的结果。

【解决】记录

2019-02-02 15:11:32 张三

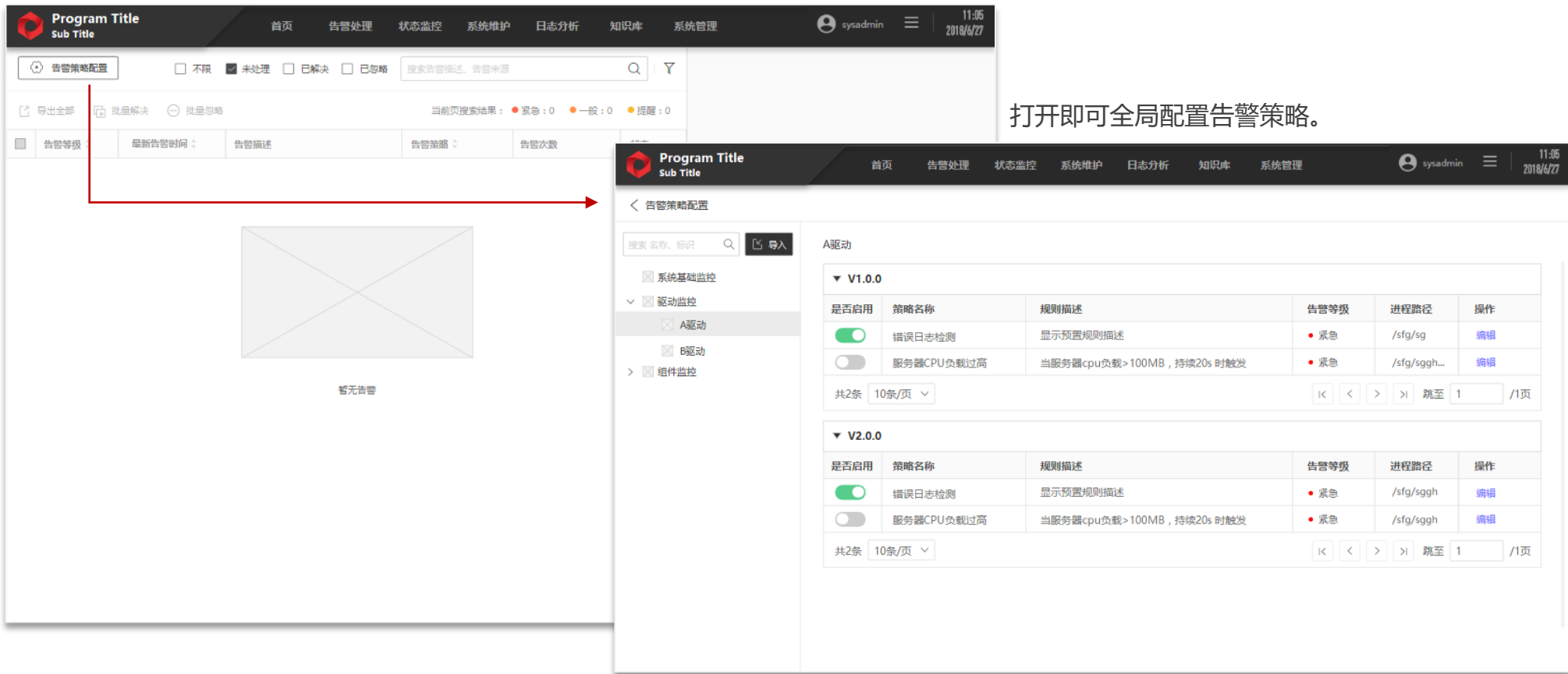
【解决】记录

2019-02-02 15:11:32 张三
按照系统提供的处理建议完美解决了告警问题。

若解决人是用户，且在解决时写过“处理建议”，则“处理意见”的内容为用户所写的最新的处理建议；若解决人为用户，且在解决时从未写过“处理建议”，则“处理意见”的内容为空，不显示。

增强功能模块操作关联性

将告警策略配置入口新增到告警处理模块中，增强功能与模块的关联性，贴合用户使用场景，方便用户在处理告警时即时配置告警策略。





自定义告警策略配置

阐述疑难/重点、分析及最终方案亮点设计

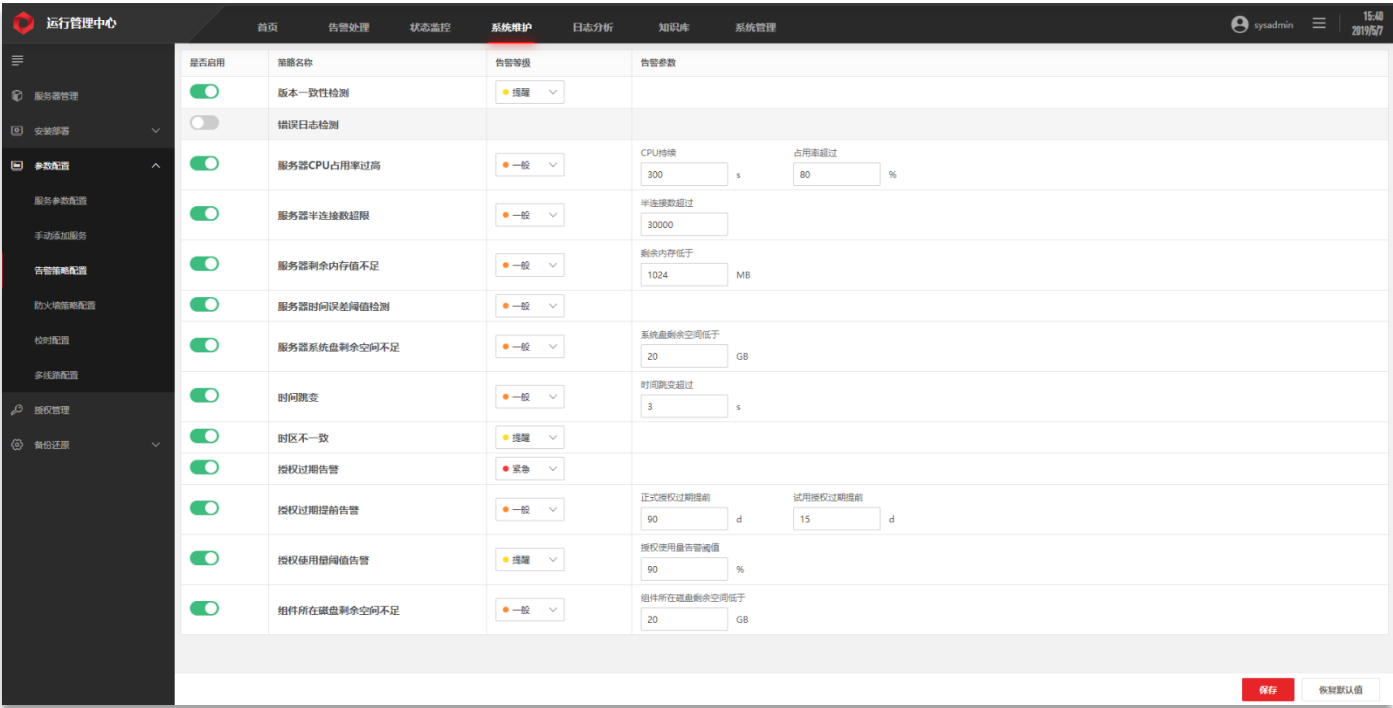


设计优化前

重点/疑难点

系统存在不同类型的告警，具有多样的告警规则，如何清晰的展示，帮助用户直观的找到不同对象的某个告警策略并进行修改呢？

- 从布局上来说，目前这种平铺不利于定位目标，同时在编辑时其他信息也会对用户视觉上造成干扰，根据告警策略特性，可以考虑将策略按不同对象分类展示。
- 从场景和功能上来说，全局保存适合批量操作，操作完后进行统一保存，但是用户往往是遇到某类告警后需要重新配置触发告警的阈值参数，而不是积累汇总所有需要修改的告警策略再来统一修改的，因此根据场景考虑提供即时生效的功能。



优化告警策略结果展示

按照系统基础监控、驱动监控、组件监控分为三类，并使用树结构进行展示，方便用户切换和搜索具体对象，同时详情页中通过卡片将告警策略继续归类，帮助用户培养对告警策略的概念认知，也帮助用户快速定位查看。

左侧树结构分类，帮助用户快速筛选定位

Program Title
Sub Title

首页告警处理状态监控系统维护日志分析知识库系统管理

sysadmin11:05
2018/6/27

< 告警策略配置

搜索名称、标识

导入

系统基础监控

驱动监控

组件监控

ActiveAAaaa

Bewrebbb

C数据库服务ccc

安保区域管理ddd

采集上报eee

存储接入服务xxx

ActiveAA

业务监控

针对该规则项显示对应的解释说明，比如所选规则为“下级域在线数”，则tip显示提示语：下级域离线将会导致级联预览、回放均失败。

是否启用	策略名称	规则描述	告警等级	操作
<input type="checkbox"/>	组件预置的业务监控策略名称	当xx下级域在线数=0，立即触发	一般	编辑删除
<input checked="" type="checkbox"/>	服务器CPU负载过高	当xxxx连接数<20，持续2s，出现2次时触发	紧急	编辑

共2条10条每页

错误码监控

+ 错误码监控告警策略

是否启用	策略名称	规则描述	告警等级	操作
<input checked="" type="checkbox"/>	错误码告警名称	当{XX错误码}，持续{x}s，触发{y}次 时触发	紧急	编辑删除

共1条10条每页

基础监控

是否启用	策略名称	规则描述	告警等级	操作
<input type="checkbox"/>	组件名（标识）占用磁盘空间超限	当磁盘占用 > 450MB，立即触发	紧急	编辑
<input checked="" type="checkbox"/>	进程服务名（进程服务标识）占用内存超限	当磁盘占用 > 450MB，立即触发	紧急	编辑

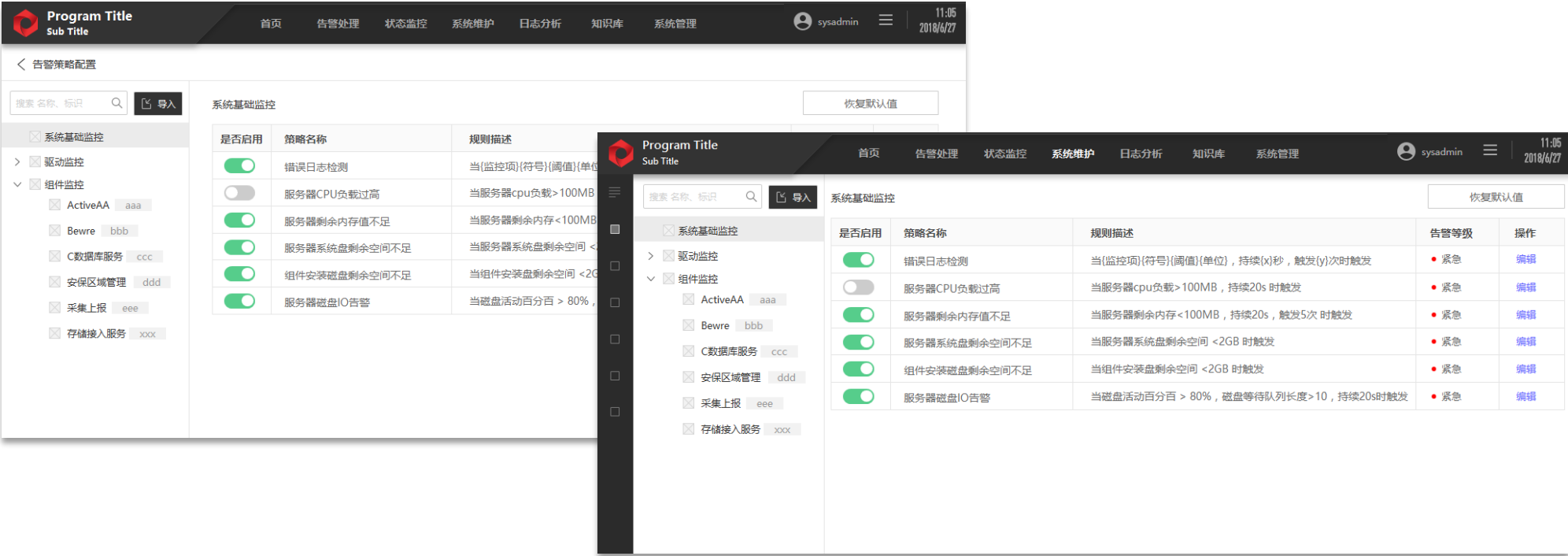
共2条10条每页

右侧根据每种对象的属性，将告警策略再进行归类展示。



加强告警策略配置页的一致性

保持告警策略配置页面的统一，对用户来说，可以有效降低认知成本，利于操作，对研发来说，可以做到开发复用，降低同类功能维护成本。



从其他模块入口打开告警策略配置的界面与 参数配置>告警策略配置模块主页的界面布局结构功能均保持一致。

对用户来说，相同功能的界面不一致容易引起困惑，且增加认知成本，不利于操作，对研发来说，同类功能多套界面将增加维护成本。

根据用户使用场景增加告警策略导入功能

新增告警策略导入功能，提高用户配置操作的便捷性。

- 1 呈现上突出按钮，鼠标移入按钮tip提示，引导用户进行导入的操作，支持导入告警策略模板Excel文件；
- 2 根据目前业务，不支持线上下载模板，只直接通过线下提供安全准确的告警策略文档，支持用户一键导入所有策略帮助解决业务问题；
- 3 导入文档适用全局，导入的数据需要自动检测找到数据匹配的节点，导入到对应节点表格数据中，提高系统智能性；



加强反馈结果有用性

导入告警策略文档进行检测后，异常的结果中把异常项对应到Excel表格的具体所在行，方便用户识别和定位Excel中异常的内容，进行针对性的修改。

导入失败的提示：



- 模板文档导入时，先扫描整个文档，若文档中不存在错误项（比如必填项数据为空），仅存在策略名称有重复的情况，则显示重复的数量，重复项所在行，以及对应的告警策略名称，方便用户寻找和定位修改。



- 扫描整个文档，若文档中存在错误项，则视为整份文档导入失败，需要显示文档中错误项：所在第几行，对应名称，错误原因。
 - 1) 文档中只要有一条有错误即视为整个文档导入失败。
 - 2) 若同时存在导入的策略重复的情况，则将重复的策略也纳入表格展示出来，异常原因固定为【告警策略已存在】。

导入成功的提示：



- 操作成功，需要告知用户成功的结果：成功的数量、开启的状态。



优化配置文案描述的可读性

将影响告警触发的配置项串联成一句话进行“人话”表达，帮助用户更好的理解策略触发的规则。

编辑系统基础监控告警策略

策略名称* 服务器系统盘剩余空间不足

告警规则* 当服务器系统盘剩余空间 < 80 GB 时触发。

告警等级*

提醒

一般

紧急

保存 取消

编辑业务监控

策略名称* A服务 (aa) 下级域在线个数为0

告警规则* 当 空余线程数 Number of free threads > 500

立即触发

满足以下规则触发

持续 86401 s, 出现 2222 次时触发。

告警等级*

提醒

一般

紧急

告警描述* 显示所选告警规则下拉项对应的默认告警描述。支持修改

- 告警规则描述中，将后端传入的各字段调整为一句连贯可配置的语句：“当.....时触发”。
- 显示格式为“当{监控项}{符号}{阈值}{单位}，持续{x}s，出现{y}次时触发。”

Program Title
Sub Title

首页 告警处理 状态监控 系统维护 日志分析 知识库 系统管理

sysadmin 11:06 2018/4/27

告警策略配置

搜索名称、标识 导入

系统基础监控

驱动监控

组件监控

ActiveAA aaa

Bewre bbb

C数据库服务 ccc

安保区域管理 ddd

采集上报 eee

存储接入服务 xxx

是否启用	策略名称	规则描述	告警等级	操作
<input checked="" type="checkbox"/>	错误日志检测	当(监控项){符号}{阈值}{单位}，持续(x)s，触发(y)次时触发	紧急	编辑
<input type="checkbox"/>	服务器CPU负载过高	当服务器cpu负载>100MB，持续20s 时触发	紧急	编辑
<input checked="" type="checkbox"/>	服务器剩余内存不足	当服务器剩余内存<100MB，持续20s，触发5次 时触发	紧急	编辑
<input checked="" type="checkbox"/>	服务器系统盘剩余空间不足	当服务器系统盘剩余空间 <2GB 时触发	紧急	编辑
<input checked="" type="checkbox"/>	组件安装磁盘剩余空间不足	当组件安装磁盘剩余空间 <2GB 时触发	紧急	编辑
<input checked="" type="checkbox"/>	服务器磁盘IO告警	当磁盘活动百分比 > 80%，磁盘等待队列长度>10，持续20s时触发	紧急	编辑

将以上规则格式同步显示到表格中的“规则描述”列，提高用户对规则的理解。

THANKS