



# 统一告警 产品文档





# 文档目录

## 产品简介

什么是统一告警

产品架构

物理架构

逻辑架构

功能特性

告警接入

告警的生命周期管理

告警聚合和关联分析

告警通知

维护期

## 常见问题

Alert产品权限申请

Alert告警接入规范

调用示例

告警规则分类说明

## 词汇表



# 产品简介

## 什么是统一告警

最近更新时间: 2023-02-16 09:47:51

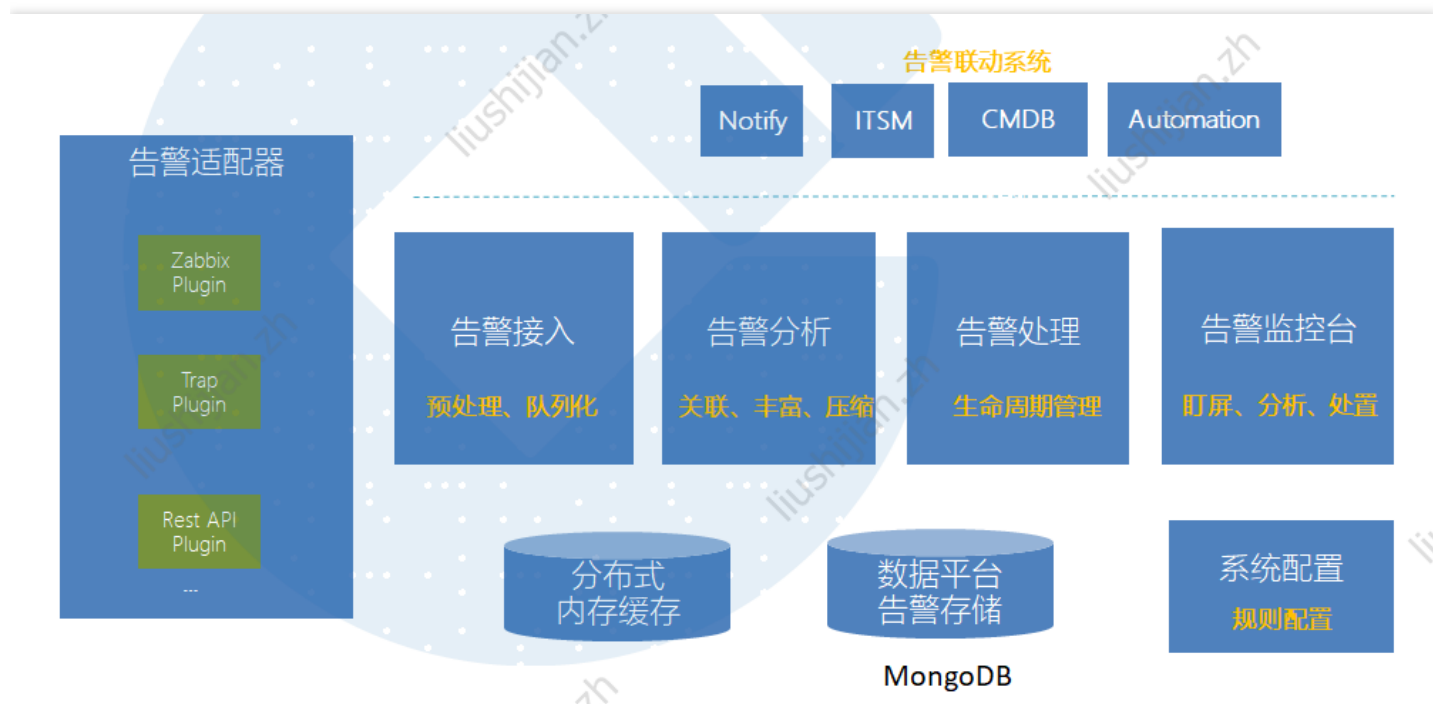
统一告警管理平台(Alert)，面向运维中最关键的日常值班与故障处理场景，提供多种告警管理能力，包括超强的性能、告警标签化、分析可视化、关联自动化、便于扩展等等。让建行云客户利用集中告警管理平台，对告警信息进行快速、高效处置。



# 产品架构

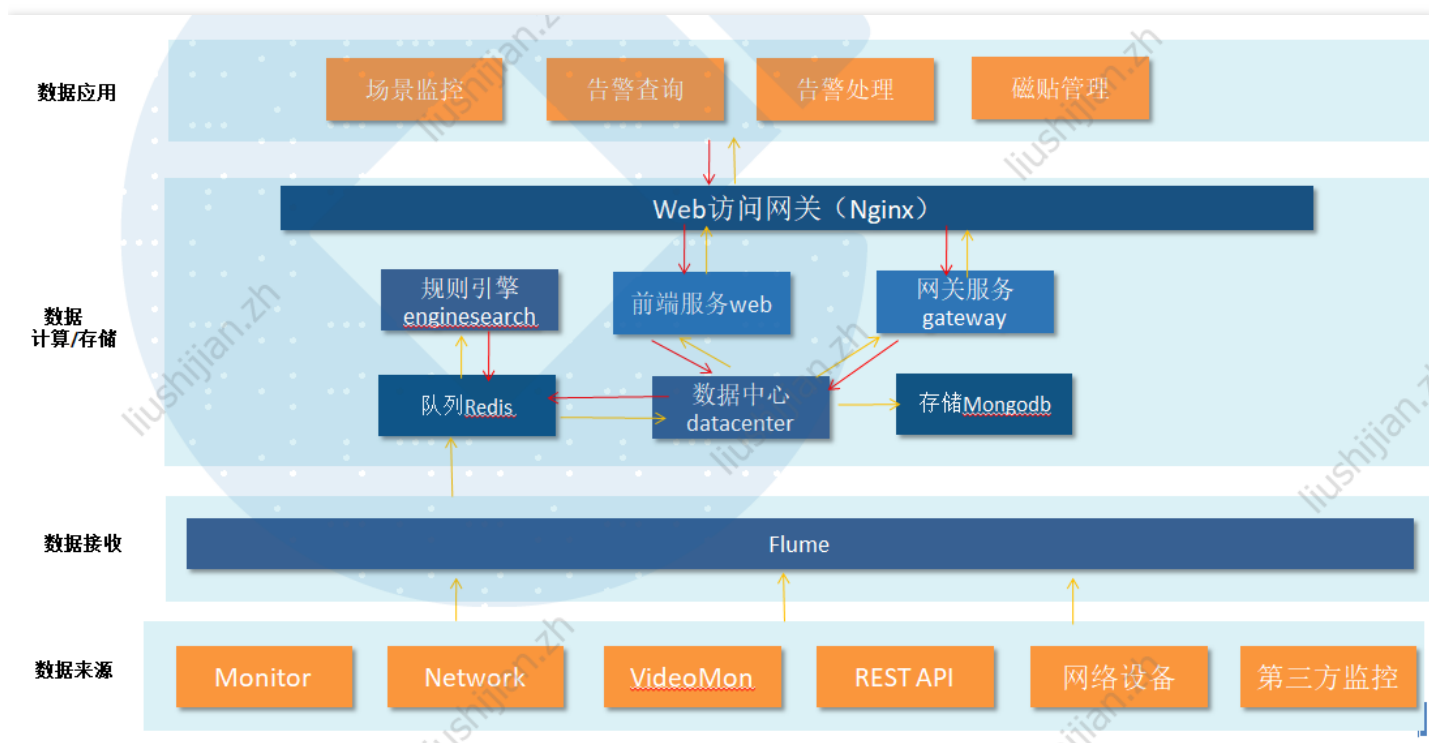
## 物理架构

最近更新时间: 2023-02-16 09:51:32



# 逻辑架构

最近更新时间: 2023-02-16 10:06:33





# 功能特性

## 告警接入

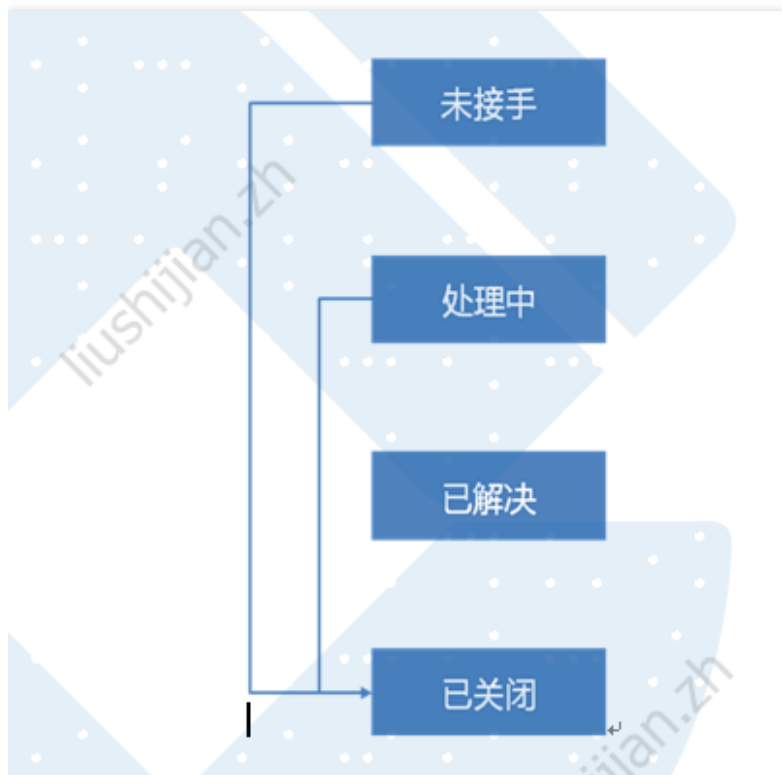
最近更新时间: 2023-02-16 10:06:33

Alert系统提供连接各式各样监控工具的能力，可直接接入相关告警数据，只需要配界面置即可完成，具有灵活的告警事件收集方式，提供标准化、高性能的Rest API接口，支持SNMP Trap、Syslog等多种标准协议接入，告警接入之后，结合CMDB可以对告警属性进一步丰富。一般来说，告警信息自带有特征和几个特征字段，通过这些字段将查询到告警对应的CI，并把CI中的某些重要字段作为告警的附加属性。

告警通过REST API或SNMPTrap接入Alert告警平台。Alert通过flume插件接收本系统或第三方系统发送的原告警。Alert业务程序将满足接入条件的原告警进行告警丰富、告警归并操作。然后规则引擎程序将满足条件的告警执行相关动作之后展示在Alert告警平台中。

# 告警的生命周期管理

最近更新时间: 2023-02-16 10:06:33



告警生命周期状态有：未接手、处理中、已解决、已关闭。

- 未接手：首次创建即此状态
- 处理中：告警经过接手后，告警状态变成处理中
- 已解决：ITSM工单完成回调/界面触发/API调用解决动作即此状态
- 已关闭：界面触发/API调用关闭动作即此状态（关闭后代表告警的生命周期结束，相同的告警进来会重新生成一条告警）

# 告警聚合和关联分析

最近更新时间: 2023-02-16 10:06:33

告警接入之后，通过告警引擎进行分析处理。告警关联引擎是集中告警平台的核心部分，告警经过丰富后，依赖Alert关联引擎的计算能力，可以最大限度减少无效告警噪音，只关注可操作性的故障；告警关联引擎也是协同和自动化的基础，允许定义上下文规则执行不同的动作处理，减少无效告警的噪音干扰，避免告警风暴。



支持多种动作，动作支持扩展：

- 归并
- 接手
- 派单
- 关闭
- 通知
- 抑制
- 升级
- 分享
- .....

提供动作插件二次开发能力，支持插件包热部署





Alert 集中告警管理平台

告警配置 > 动作管理

+ 添加动作 导入 导出 动作总数: 16

<input type="checkbox"/>	动作名称	描述	适用范围	是否内置	是否开启	操作
<input type="checkbox"/>	告警关闭/删除	对告警进行关闭/删除操作	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	告警升级/通知	对告警进行邮件、短信、ChatOps私聊窗口、Web弹窗通知	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	告警派单	将告警派发为工单到优云TSM系统	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	告警抑制	对告警进行抑制操作	新产生的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	分享到ChatOps	将告警分享到优云ChatOps群组	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	修改告警级别	修改告警到固定级别或升降级	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	告警接手	自动接手告警	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除
<input type="checkbox"/>	告警自动修复	自动修复告警	新产生的告警/已存在的告警	是	<input checked="" type="checkbox"/>	编辑 删除



# 告警通知

最近更新时间: 2023-02-16 10:06:33

可以灵活配置规则来实现告警自动通知，通知方式可以选择电子邮件，短消息，分享到ChatOps私聊窗口，弹窗声音提醒。选择通知对象和通知方式，填写相关信息，其中支持插入变量形式。可勾选“当且仅当告警级别改变时再次提醒”，“是否开启告警升级”，开启告警升级可以设置条件再次通知。

The screenshot shows the 'Alert Management Platform' interface. The main content area is titled '告警配置 > 关联配置 > 编辑规则'. Under the '设置动作' (Set Action) section, there is a sub-section for '告警升级/通知' (Alert Upgrade/Notification). The '通知对象' (Notification Object) is set to '用户组' (User Group). The '通知方式' (Notification Method) is set to '短信息' (Short Message). The '邮件标题' (Email Subject) is '\$\${entityName}:\${name}' and the '邮件内容' (Email Content) is '\$\${severity},\$\${entityName},\$\${lastOccurTime},\$\${description}'. There are checkboxes for '当且仅当告警级别改变时再次提醒' (checked), '是否开启告警升级' (unchecked), '是否开启告警恢复提醒检查' (unchecked), and '是否开启告警周期通知' (checked). A '当满足以下条件时, 周期通知:' (When the following conditions are met, periodic notification:) section shows a condition: '等待 15 分钟, 如果告警等级不是恢复状态, 进行周期通知' (Wait 15 minutes, if the alert level is not the recovery state, perform periodic notification).

## 告警通知：

- 通知方式 包括 邮件、短信、 ChatOps；
- 通知对象 可选择用户或用户组；
- 短信内容自定义，支持插入变量形式；

- 升级提醒；恢复提醒；周期通知条件设置



- 告警用户组：
  - 自定义添加告警用户组，关联相关用户；
  - 告警通知可直接选择用户组；



# 维护期

最近更新时间: 2023-02-16 10:06:33

Alert可以对相关的资源设置维护期，在变更期间引起的告警则不再进行告警通知。

The screenshot displays the 'Alert 集中告警管理平台' (Alert Central Alert Management Platform) interface. The main section is titled '维护期管理' (Maintenance Period Management). It features a search bar with the placeholder '请输入名称' (Please enter name) and a status filter section with checkboxes for '待执行' (Pending), '进行中' (In Progress), '已撤销' (Cancelled), and '已结束' (Completed). A '新增维护' (Add Maintenance) button is located on the right. Below the filter is a table with the following data:

名称	描述	状态	开始时间	结束时间	更新时间	操作
123	asd	已结束	2019-08-21 11:26:24	2019-08-21 12:58:10	2019-08-21 12:58:10	
测试	测试	已结束	2019-08-19 10:35:17	2019-08-19 10:59:01	2019-08-19 10:49:46	

At the bottom right of the table area, it shows '共 2 条' (Total 2 items) and a pagination control for '10 条/页' (10 items per page).

告警维护期：

- 关联相关资源对象；设置维护期时间段；
- 修改、撤销、新建维护期；
- 维护期状态自检测



## 常见问题

# Alert产品权限申请

最近更新时间: 2023-02-14 10:23:11

首先确认内容:

1. 可以访问龙舟统一运维平台;
2. 拥有平台登录uass账号和ITSM流程平台权限;
3. 通过ITSM工单申请统一告警平台方案。



# Alert告警接入规范

最近更新时间: 2023-02-16 09:36:37

如果需要接入第三方的告警，Alert可以通过 REST API的方式接入的告警，需要按照接口的接入规范和告警字段设置进行告警接入Alert。

## 调用方式

url	http://oss.yun.ccb.com/alert/openapi/v2/create? apikey=7e6c9715ab394722a51706b68cbdb9c6&app_key=b0p38x7pco66iunjhquujnriwe230ck2 apikey 用于标识租户， app_key用于标识应用
调用方式	post
header	Content-Type、application/json;charset=utf-8
body	<pre>{   "severity": 3,   "name": "system.mem.pct_usage-CPU利用率",   "description": "内存使用率超过80%",   "occur_time": 1490251916807,   "entity_name": "PC Server",   "entity_addr": "10.2.1.2",   "merge_key": "entity_name,name",   "identify_key": "entity_name,entity_addr",   "type": "metric",   "networkDomain": "defaultZone",   "properties": [     {       "val": "system.mem.pct_usage",       "code": "metricname",       "name": "METRIC_NAME"     }   ] }</pre>
返回码	500 apikey错误 Deserializer threw unexpected exception. 1 400 appkey错误 Bad request from client. Event authed failed 200 接收成功

### ## 参数说明

--	--	--	--



参数	是否必须	是否可为空	备注
severity	可选	可为空	告警级别: 严重:3, 错误:2,警告: 1, 恢复: 0
name	可选	可为空	告警名称
description	必须	不可为空	告警描述
occur_time	可选	可为空	发生时间,不填默认现在时间
entity_name	必须	不可为空	告警对象, 比如X86服务器(PCServer); 虚拟机(VM); Linux ;Windows; Mysql ;Oracle等等
entity_addr	可选	可为空	告警对象地址
merge_key	可选	可为空	指定用于告警合并的字段, 如果有多个字段请用逗号隔开。可选范围: entity_name,entity_addr,app_key,name,properties中的字段的code
identify_key	可选	可为空	用于定位统一资源库(cmdb)的资源, 如果有多个字段请用逗号隔开。默认设置: entity_addr这个字段就可
networkDomain	可选	可为空	网络域: defaultZone 为默认域的Code信息, 为了更好的区分告警所属的网络域信息,此信息可以在ANT产品中查询, 查看设备纳管所分配的网络域信息, 不填写的情况, 默认把告警划分到默认域。
Type	可选	可为空	告警类型: event 事件告警, metric 指标告警, 默认为event(不传或为空都可以)
properties	可选	可为	告警的扩展字段, 请使用 name,code,val的形式, 当 type 为 metric时, 如果可以传递指标编码, 可增加 name为METRIC_NAME, code 填metricname, val



---

		空   填写报警指标的code
--	--	-----------------





# 调用示例

最近更新时间: 2023-02-16 09:47:51

## python

```
1 | # -*- coding:utf8 -*-
2 | import requests
3 | import json
4 | import sys
5 | reload(sys)
6 | sys.setdefaultencoding("utf8")
7 |
8 | if __name__ == "__main__":
9 |     url_oss = " http://oss.yun.ccb.com/alert/openapi/v2/create?apikey=e10adc
10 |     headers = {'Content-Type': 'application/json;charset=utf-8'}
11 |     payload = {
12 |         "name": "LZ-Alert-健康巡检",
13 |         "description": "测试告警 >0个, 接入正常",
14 |         "entity_name": "龙舟Alert巡检", # 告警对象
15 |         "entity_addr": "10.253.253.253",
16 |         "severity": 2,
17 |     }
18 |     data_json = json.dumps(payload)
19 |     r = requests.post(url=url_oss, headers=headers, data=data_json)
20 |     print("龙舟告警健康检查推送结果%s" % (r.status_code))
21 |
```

## shell

```
curl -X POST -H 'Content-Type: application/json' -i --data '{"severity": 3, "name":
"system.mem.pct_usage-CPU利用率", "description": "内存使用率超过80%", "occur_time": 1490251916807,
"entity_name": "Linux", "entity_addr": "10.2.1.2", "merge_key": "entity_name,name", "identify_key":
"entity_name,entity_addr", "networkDomain": "defaultZone", "type": "metric", "properties": [ { "val":
"system.mem.pct_usage", "code": "metricname", "name": "METRIC_NAME" } ]}'
"http://oss.yun.ccb.com/alert/openapi/v2/create?
apikey=7e6c9715ab394722a51706b68cbdb9c6&app_key=umtck7jutguornycya5b1l2bzezdnb"'
```



# 告警规则分类说明

最近更新时间: 2023-02-16 09:47:51

告警动作	描述	范围
告警通知	通知方式有电子邮件、短信息	实时、历史
告警关闭	关闭将告警状态改为已恢复	实时、历史
告警派单	需要选择工单类别和填写映射配置，在选择工单类别后，填写工单映射配置。	实时、历史
告警抑制	告警白名单功能，在白名单里的告警将不再接入Alert进行处理	实时
告警级别更改	对告警级别进行自动修改	实时、历史
告警压缩	设置告警压缩字段，字段相同的告警会压缩为一条告警信息，叠加告警次数	实时、历史
定位与丰富	根据定位字段，定位告警信息，插入从CMDB中丰富过来的告警信息	实时、历史
临时合并	临时将告警合并成一条	实时
故障自愈		实时



# 词汇表

最近更新时间: 2023-02-13 15:52:59

术语	定义
告警	从第三方系统接入的告警或原始事件经过Monitor、Alert处理形成的需要关注的信息为告警；
告警严重等级	<p>根据告警的严重程度，告警级别在alert中从高到低依次为：</p> <p>【紧急】（对应《中国建设银行信息系统监控管理规程（2020年版）》中的严重告警）：提示信息系统完全停止服务或部分服务中断，必须立即处理的告警</p> <p>【错误】（对应《中国建设银行信息系统监控管理规程（2020年版）》中的主要告警）：提示可能影响信息系统运行，产生潜在业务影响，需要立即处理的告警。</p> <p>【警告】（对应《中国建设银行信息系统监控管理规程（2020年版）》中的次要告警）：提示可能影响信息系统运行，但不产生潜在业务影响，可以在24小时内处理的告警。</p> <p>【恢复】（对应《中国建设银行信息系统监控管理规程（2020年版）》中的通知告警）：不影响信息系统运行，需要关注的告警。</p>
标签	告警除了自身的属性外，Alert还支持为告警添加标签，通常标签是从CMDB系统丰富而来，系统也支持通过一定的规则为告警打标签。
动作	对告警处置均定义为动作，如接手、关闭、派发工单、分享、抑制、通知等。
告警规则	指在Alert中配置关联规则，在定义的时间点或者时间段对符合条件的告警执行某个动作的配置。在Alert磁贴中定义的规则为私有规则，只在磁贴中生效，在Alert->设置->告警关联规则中配置的为全局规则，对全局告警生效。
告警抑制	若因变更或者故障，出现大量无效告警时，可以创建规则抑制告警风暴。告警被抑制之后，将会在接入层面直接过滤掉告警，即告警不会出现所有告警列表中，亦不会发送短信通知。
告警聚合	多条告警聚合成一条告警显示。可以配置规则指定告警压缩字段，配置告警压缩字段之后，压缩字段相同的告警会被聚合成一条告警。告警被聚合的情况，可以通过点击告警次数进行查看。如果在告警通知中没有勾选“当且仅当告警等级改变时再次提醒”，则每条告警都会发送短信通知；如果在告警通知中勾选“当且仅当告警等级改变时再次提醒”，则等级相同的告警只会发送一次短信，直到告警等级改变时才会重新发送短信。
告警关闭	告警接入到Alert中后，满足条件的告警会自动关闭,结束告警生命周期。
告	维护期用于变更期间触发的告警，处于维护期的告警不会通过Alert发送告警通知，但是告警会在Alert中有记



警维护期	录。
告警生命周期状态	<p>未接手：首次创建即此状态；</p> <p>已关闭：界面点击关闭或者触发关闭规则后告警置为关闭状态。告警未关闭前，所有新接入的相同告警将会聚合到当前告警，如果在告警通知中没有勾选“当且仅当告警等级改变时再次提醒”，则每条告警都会发送短信通知；如果在告警通知中勾选“当且仅当告警等级改变时再次提醒”，则等级相同的告警只会发送一次短信，直到告警等级改变时才会重新发送短信。告警关闭后代表告警的生命周期结束，相同的告警进来会重新生成一条告警。</p>