**管理系统前后台接口文档**

2017年10月

1. 设备监控

1.1监控器页面

1.1.1 监控器管理页面跳转

url: eqpMonitor/monitorManage

请求方式：post

参数：无

返回结果：eqpMonitor/monitorManage (即指定跳转页面为monitorManage.jsp)

1.2设备监控页面

1.2.1设备监控页面跳转

[url: eqpMonitor/eqpMonitor](url:monitor/eqpMonitor%20)

请求方式：post

参数：无

返回结果：eqpMonitor/eqpMonitor (即指定跳转页面为eqpMonitor.jsp)

1.2.2设备监控初始化列表（左边的preview）

url: eqpMonitor/preMonitor

请求方式：post

参数：type（树形结构的类型，1代表资产类型，2代表安全域）

返回结果： 示例，{

"result": true,

"assetPreviewList": [{

"name": "天基骨干卫星安全接入网关(1)",

"id": 1,

"parentId": -1

},

{

"name": "管理服务器(1)",

"id": 25,

"parentId":- 3

},

{

"name": "三层交换机(5)",

"id": 20,

"parentId": -1

},

{

"name": "二层交换机(8)",

"id": 21,

"parentId": -1

},

{

"name": "网络设备",

"id": -1,

"parentId": "root"

},

{

"name": "服务器",

"id": -3,

"parentId": "root"

},

{

"name": "资产类型",

"id": "root",

"parentId": "null"

}]

}

1.2.3 显示同一类型的监控设备列表（右侧详细列表）

url: eqpMonitor/delMonitor

请求方式：post

参数：

type: 值有3种“root”，“class”,“type”,其中当值为“root”时，则显示所有类型的列表，这时id值为-1

id: 设备类型的id

currentPage：当前页数

numPerPage：每页大小

返回结果：{

"result": true,

" assetDetailsList ": [{

"eqpNo": "0001-00002",

"eqpID": "3",

"name": "天基接入网关",

"assetType": 1,

"assetValue": 1,

"securityDomain": "3",

"workMode": 1,

"manageMode": 1,

"os": "Linux",

"account": null,

"pass": null,

"ip": "10.224.1.25",

"location": "管理平台",

"serial": null,

"contaction": null},

{ "eqpNo": "0001-00004",

"eqpID": "14",

"name": "路由器1",

"assetType": 20,

"assetValue": 1,

"securityDomain": "1",

"workMode": 1,

"manageMode": 1,

"os": "Linux",

"account": null,

"pass": null,

"ip": "10.224.11.25",

"location": "管理平台",

"serial": null,

"contaction": null}]}

1.2.4 点击加号显示某一设备上的监控属性(CPU，内存等信息)

url: eqpMonitor/plusPreInfo

请求方式：post

参数：eqpNo(设备编号)

返回结果：示例

{

"result": true,

"typeList": [{

"type": "系统信息代理",

"infoList": [{

"picName": "HARDWARE\_MEMORY\_TYPE",

"infoName": "内存信息",

"infoType": "TBLVALUESMEMORY"

},{

"picName": "HARDWARE\_MEMORY\_TYPE",

"infoName": "内存信息",

"infoType": "TBLVALUESMEMORY"

}]

},{

"type": "系统信息代理",

"infoList": [{

"picName": "HARDWARE\_MEMORY\_TYPE",

"infoName": "内存信息",

"infoType": "TBLVALUESMEMORY"

},{

"picName": "HARDWARE\_MEMORY\_TYPE",

"infoName": "内存信息",

"infoType": "TBLVALUESMEMORY"

}]

}]

}

1.2.5 点击设备上的某一监控属性(CPU，内存等)，弹框显示具体信息

url: eqpMonitor/plusDelInfo

请求方式：post

参数：eqpNo(设备编号), infoType(监控属性的类型，eg: TBLVALUESDISKS)

返回结果：示例

{

"result": true,

"infoList": [{

"valueIndex": 4,

"dskAvail": 13512156,

"eqpNo": "0001-00001",

"collectTime": "2017-05-17 18:01:00",

"dskUsed": 4953568,

"dskTotal": 19478204,

"dskPercent": 27,

"dskPath": "/",

"dskDevice": "/dev/sda1"

}]

}

1. 设备管理

2.1设备类型页面

2.1.1设备类型页面跳转

url: eqpManage/eqpTypeInit

请求方式：post

参数：无

返回结果：eqpManage/eqpType(即指定跳转页面为eqpType.jsp)

2.1.2设备类型列表

url: eqpManage/eqpTypeList

请求方式：post

参数：

currentPage：当前页数

numPerPage：每页大小

返回结果：{

"result": true,

"totalRows": 22,

"infoList": [{

"id": 1,

"typeName": "天基骨干卫星安全接入网关",

"pic": "",

"className": "网络设备"

},

{

"id": 2,

"typeName": "宽带卫星安全接入网关",

"pic": "",

"className": "网络设备"

},

{

"id": 3,

"typeName": "卫星移动安全接入网关",

"pic": "",

"className": "网络设备"

},

{

"id": 4,

"typeName": "异构网间安全互联网关",

"pic": "",

"className": "网络设备"

},

{

"id": 5,

"typeName": "地面网间安全互联网关",

"pic": "",

"className": "网络设备"

}]

}

2.1.3获取设备所属大类class的下拉列表

url: eqpManage/eqpClassList

请求方式：post

参数：无

返回结果：{

"result": true,

"infoList": [{

"id": 1,

"name": "网络设备",

"pic": ""

},

{

"id": 2,

"name": "安全设备",

"pic": ""

},

{

"id": 3,

"name": "服务器",

"pic": ""

},

{

"id": 4,

"name": "终端",

"pic": ""

}]

}

2.1.3设备类型新增,编辑和删除

url: eqpManage/eqpTypeModify

请求方式：post

参数：包括3种操作方式，根据不同的操作方式传入相应的参数

operateType:1(新增), eqpClassId:1(网络设备，即下拉选择所属大类)，eqpTypeName: 宽带卫星安全接入网关，文件

operateType:2(编辑), eqpTypeId:2，eqpClassId:1(网络设备，即下拉选择所属大类)，eqpTypeName: 宽带卫星安全接入网关，文件

operateType:3(删除,包括批量删除), eqpTypeIdList:1,2,3,4(id组成的字符串，以英文的“，”分隔多个id)

返回结果：{"result": true,

}

2.2设备安全域页面

2.2.1设备安全域类型页面跳转

url: eqpManage/eqpSecDomInit

请求方式：post

参数：无

返回结果：eqpManage/eqpSecDom (即指定跳转页面为eqpSecDom.jsp)

2.2.2设备安全域列表

url: eqpManage/eqpSecDomList

请求方式：post

参数：

currentPage：当前页数

numPerPage：每页大小

返回结果示例：{

"result": true,

"totalRows": 4,

"infoList": [{

"secDomId": 1,

"secDomName": "安全域1",

"description": null

},

{

"secDomId": 2,

"secDomName": "安全域2",

"description": null

},

{

"secDomId": 3,

"secDomName": "安全域3",

"description": null

},

{

"secDomId": 4,

"secDomName": "安全域4",

"description": null

}]

}

2.2.3设备安全域新增,编辑和删除

url: eqpManage/eqpSecDomModify

请求方式：post

参数：包括3种操作方式，根据不同的操作方式传入相应的参数

operateType:1(新增), eqpSecDomName: 安全域1（安全域Name），eqpSecDomDesc: 安全域描述语句；

operateType:2(编辑), eqpSecDomId:1(安全域id)，eqpSecDomName: 安全域1（安全域Name），eqpSecDomDesc: 安全域描述语句；

operateType:3(删除，以及批量删除), eqpSecDomIdList:1,2,3,4(多个安全域id组成的字符串，以英文的“，”分隔开) 。

返回结果：{"result": true}

2.3设备登记页面

2.3.1设备登记页面跳转

url: eqpManage/eqpRegInit

请求方式：post。

参数：无。

返回结果：eqpManage/eqpRegInit(即指定跳转页面为eqpReg.jsp)。

2.3.2设备信息列表（显示已有的设备列表）

url: eqpManage/eqpRegList

请求方式：post。

参数：

currentPage：当前页数

numPerPage：每页大小

返回结果：{

"result": true,

"totalRows": 15,

"infoList": [{

"account": "",

"assetType": "管理服务器",

"assetValue": 1,

"contaction": "",

"eqpID": "1",

"eqpNo": "0001-00001",

"ip": "10.224.0.25",

"location": "管理平台",

"manageMode": 1,

"name": "管理服务器",

"os": "Linux",

"pass": "",

"securityDomain": "安全域1",

"serial": "",

"workMode": 1

},{

"account": "",

"assetType": "天基骨干卫星安全接入网关",

"assetValue": 1,

"contaction": "",

"eqpID": "3",

"eqpNo": "0001-00002",

"ip": "10.224.1.25",

"location": "管理平台",

"manageMode": 1,

"name": "天基接入网关",

"os": "Linux",

"pass": "",

"securityDomain": "安全域3",

"serial": "",

"workMode": 1

}]}

2.3.3手动登记设备(安全域和设备类型以下拉选择的方式进行，接口分别调用2.1.2和2.2.2)

url: eqpManage/eqpRegManualAdd

请求方式：post。

参数：eqpNo:“0001-00001”,eqpID:“”，name:“管理服务器”,assetType:25,assetValue:1.0,securityDomain:1,workMode:1,manageMode:1,os:“Linux”,account:“”,pass:“”,ip:”10.224.0.25”, location:“管理平台”,serial: “”,contaction:“”(注意：eqpNo, name, assetType, assetValue, securityDomain, os, ip必须要有值)。

返回结果：成功：{"result": true}；失败：{"result": false}

2.3.4下载Excel模板

url: eqpManage/templateDownload

请求方式：post。

参数：“fileName”：“Template”(模板的名字固定为Template,

eg: <a href="eqpManage/templateDownload?fileName=Template.xlsx">下载模板</a>)

返回结果：浏览器下载文件。

2.3.5 Excel批量登记设备

url: eqpManage/excelUpload

请求方式：post。

参数：excel文件。(使用form表单。eg:

<input id=*"excelFile"* type=*"file"* name=*"fileName"* accept=*"xlsx"*/>)

返回结果示例：

成功：{"result": true}；

失败：{"result": false,"msg": “文件格式不正确！请使用.xls或.xlsx后缀文档” }

2.3.6自动扫描新增设备

url: eqpManage/eqpRegAutoAdd

请求方式：post。

参数：无

返回结果：{"result": true}

1. 告警管理

3.1告警类型页面

3.1.1告警类型页面跳转

url: alertManage/alertTypeInit

请求方式：post。

参数：无。

返回结果：alertManage/alertType (即指定跳转页面为alertType.jsp)。

3.1.2告警类型列表

url: alertManage/ alertTypeList

请求方式：post。

参数：

currentPage：当前页数

numPerPage：每页大小

operateType：1表示显示所有的告警类型列表；2表示只显示基本告警类型列表

返回结果：示例

{

"result": true,

"infoList": {

"result": true,

"totalRows": 13,

"infoList": [{

"id": 1,

"typeName": "拒绝服务",

"description": "通过向服务器发送大量垃圾信息或干扰信息的方式，导致服务器无法向正常用户提供服务的现象。",

"mixType": "否",

"mixTypeValue": ""

},

{

"id": 2,

"typeName": "扫描探测",

"description": "扫描探测是在攻击开始前必需的情报收集工作，攻击者在这个过程中尽可能的了解被攻击目标安全方面的信息。",

"mixType": "否",

"mixTypeValue": ""

},

{

"id": 3,

"typeName": "认证/授权/访问",

"description": "识别用户身份，允许特定的用户访问特定的区域或信息。",

"mixType": "否",

"mixTypeValue": ""

},

{

"id": 4,

"typeName": "利用漏洞",

"description": "利用系统安全方面的缺陷，控制或破坏受害系统。",

"mixType": "否",

"mixTypeValue": ""

},

{

"id": 5,

"typeName": "逃避行为",

"description": "在不被检测的情况下，绕过信息安全设备进行攻击的方式。",

"mixType": "否",

"mixTypeValue": ""

}]

}

}

3.1.3告警类型新增，编辑和修改

url: alertManage/alertTypeModify

请求方式：post。

参数：包括3种操作方式，任选其1，根据不同的操作方式传入相应的参数

方式一：operateType:1(新增), typeName(告警类型)，description，mixType(0表示基本类型，1表示混合告警类型): mixTypeValue(混合告警类型的值以英文逗号“,”隔开)；

方式二：operateType:2(编辑), typeName(告警类型)，alertTypeId(告警类型id),description，mixType(0表示基本告警类型，1表示混合告警类型): mixTypeValue(混合告警类型的值以英文逗号“,”隔开)；

方式三：operateType:3(删除，以及批量删除), alertTypeIdList(多个告警类型id组成的字符串，以英文的“，”分隔开) 。

返回结果：{"result": true}

3.2告警统计页面

3.2.1告警统计页面跳转

url: alertManage/alertStatistics

请求方式：post。

参数：无。

返回结果：alertManage/alertStatistics (即指定跳转页面为alertStatistics.jsp)。

* + 1. 告警类别统计（柱状图）

url: alertManage/alertTypeStatistics

请求方式：post。

参数：无。

返回结果：{

"result": true,

"valueList": [21,22,20,23,14,18,15,16,22,17,12],

"nameList": ["病毒/木马","违背策略","自定义类型","关联事件","利用漏洞","逃避行为","认证/授权/访问","扫描探测","系统状况/配置","可疑活动","拒绝服务"]}

* + 1. 告警紧急程度统计（饼状图）

url: alertManage/alertUrgentStatistics

请求方式：post。

参数：无。

返回结果：{

{"result": true,

"typeList": ["待定告警",

"警告告警",

"次要告警",

"重大告警",

"严重告警"],

"dataList": [{

"name": "次要告警",

"value": 38

},

{

"name": "重大告警",

"value": 54

},

{

"name": "警告告警",

"value": 41

},

{

"name": "待定告警",

"value": 38

},

{

"name": "严重告警",

"value": 29

}]}

* + 1. 基于时间的告警统计（折线图）

url: alertManage/alertTimeStatistics

请求方式：post。

参数：无。

返回结果：{

"result": true,

"statisticsDataValues": [13,10,8,8,6,12,6,6,6,5,8,7,11,8,11,8,4,6,15,14,9,7,7,5],

"statisticsDataName": [

"00:00时","01:00时","02:00时","03:00时",

"04:00时","05:00时","06:00时","07;00时",

"08:00时","09:00时","10:00时","11:00时",

"12:00时","13:00时","14:00时","15:00时",

"16:00时","17:00时","18:00时","19:00时",

"20:00时","21:00时","22:00时","23:00时"]

}

* + 1. 事件类别统计（饼状图）

url: alertManage/eventTypeStatistics

请求方式：post。

参数：无。

返回结果：{"result": true,

"valueList": [{

"name": "操作系统事件",

"value": 2901

},

{

"name": "应用软件",

"value": 4917

},

{

"name": "其他",

"value": 1088

},

{

"name": "网络 设备",

"value": 671

},

{

"name": "链路告警",

"value": 423

}],

"nameList": ["操作系统事件",

"应用软件",

"网络设备",

"链路告警",

"其他"]}

3.2.6 事件级别统计（饼状图）

url: alertManage/eventRankStatistics

请求方式：post。

参数：无。

返回结果：{

"result": true,

"valueList": [{

"name": "一般故障",

"value": 1982

},

{

"name": "致命故障",

"value": 2029

},

{

"name": "严重故障",

"value": 2052

},

{

"name": "较大故障",

"value": 1941

},

{

"name": "一般信息",

"value": 1996

}],

"nameList": ["一般信息",

"一般故障",

"较大故障",

"严重故障",

"致命故障"]

}

* + 1. 基于时间的事件统计（折线图）

url: alertManage/eventTimeStatistics

请求方式：post。

参数：无。

返回结果：{

"result": true,

"statisticsDataValues": [13,10,8,8,6,12,6,6,6,5,8,7,11,8,11,8,4,6,15,14,9,7,7,5],

"statisticsDataName": [

"00:00时","01:00时","02:00时","03:00时",

"04:00时","05:00时","06:00时","07;00时",

"08:00时","09:00时","10:00时","11:00时",

"12:00时","13:00时","14:00时","15:00时",

"16:00时","17:00时","18:00时","19:00时",

"20:00时","21:00时","22:00时","23:00时"]

}

3.3告警列表页面

3.3.1 告警列表页面跳转

url: alertManage/alertInfoInit

请求方式：post。

参数：无。

返回结果：alertManage/alertInfoInit (即指定跳转页面为alertInfoInit.jsp)。

3.3.2 告警信息列表展示

url: alertManage/ alertTypeList

请求方式：post。

参数：

currentPage：当前页数

numPerPage：每页大小

返回结果：示例

{

"result": true,

"totalRows": 200,

"infoList": [{

"id": 1,

"reportTime": "2017-02-01 00:00:00",

"startTime": null,

"lastTime": null,

"reportLevel": 5,

"confidence": 0.05,

"seriousLevel": 4,

"ugentLevel": 3,

"assetType": 3,

"targetAssets": "3E",

"alertTypeID": 6,

"alertProc": 4,

"attackSource": "154.73.43.19",

"alertRegion": "210.84..72.11",

"strategy": "",

"isSolve": 0,

"alertTypeName": "病毒/木马"

},

{

"id": 2,

"reportTime": "2017-02-01 15:00:00",

"startTime": null,

"lastTime": null,

"reportLevel": 3,

"confidence": 0.49,

"seriousLevel": 1,

"ugentLevel": 4,

"assetType": 4,

"targetAssets": "4E",

"alertTypeID": 9,

"alertProc": 4,

"attackSource": "210.73.43.120",

"alertRegion": "202.44.21.0/25",

"strategy": "",

"isSolve": 1,

"alertTypeName": "违背策略"

},

{

"id": 3,

"reportTime": "2017-02-02 13:00:00",

"startTime": null,

"lastTime": null,

"reportLevel": 5,

"confidence": 0.27,

"seriousLevel": 3,

"ugentLevel": 2,

"assetType": 5,

"targetAssets": "3E",

"alertTypeID": 11,

"alertProc": 2,

"attackSource": "154.45.31.12",

"alertRegion": "196.232.12.0/24",

"strategy": "",

"isSolve": 1,

"alertTypeName": "自定义类型"

},

{

"id": 4,

"reportTime": "2017-02-03 10:00:00",

"startTime": null,

"lastTime": null,

"reportLevel": 5,

"confidence": 0.41,

"seriousLevel": 1,

"ugentLevel": 1,

"assetType": 4,

"targetAssets": "4E",

"alertTypeID": 10,

"alertProc": 1,

"attackSource": "212.23.32.108",

"alertRegion": "10.10.32.0/24",

"strategy": "",

"isSolve": 0,

"alertTypeName": "关联事件"

},

{

"id": 5,

"reportTime": "2017-02-04 09:00:00",

"startTime": null,

"lastTime": null,

"reportLevel": 2,

"confidence": 0.08,

"seriousLevel": 2,

"ugentLevel": 2,

"assetType": 4,

"targetAssets": "2E",

"alertTypeID": 4,

"alertProc": 4,

"attackSource": "219.73.54.23",

"alertRegion": "174.23.42.0/25",

"strategy": "",

"isSolve": 1,

"alertTypeName": "利用漏洞"

}]

}

3.3.3 告警所包含的详细事件列表

url: alertManage/ alertTypeList

请求方式：post。

参数：

currentPage：当前页数

numPerPage：每页大小

alertID：报警id

返回结果：示例

{

"result": true,

"totalRows": 10,

"infoList": [{

"Event\_id": 8338,

"Alert\_id": 1,

"relevancyStrength": 0.95,

"id": 8338,

"time": "2017-01-15 09:41:00",

"priority": 4,

"eventTypeID": 50,

"eqpNo": "0001-00001",

"pluginID": null,

"rank": 2,

"category": 2

},

{

"Event\_id": 2514,

"Alert\_id": 1,

"relevancyStrength": 0.41,

"id": 2514,

"time": "2017-01-05 07:51:00",

"priority": 5,

"eventTypeID": 78,

"eqpNo": "0001-00001",

"pluginID": null,

"rank": 1,

"category": 2

},

{

"Event\_id": 2730,

"Alert\_id": 1,

"relevancyStrength": 0.15,

"id": 2730,

"time": "2017-01-05 17:12:00",

"priority": 1,

"eventTypeID": 28,

"eqpNo": "0001-00001",

"pluginID": null,

"rank": 2,

"category": 1

},

{

"Event\_id": 9244,

"Alert\_id": 1,

"relevancyStrength": 0.18,

"id": 9244,

"time": "2017-01-17 00:41:00",

"priority": 5,

"eventTypeID": 133,

"eqpNo": "0001-00001",

"pluginID": null,

"rank": 1,

"category": 2

},

{

"Event\_id": 1051,

"Alert\_id": 1,

"relevancyStrength": 1.0,

"id": 1051,

"time": "2017-01-02 19:58:00",

"priority": 2,

"eventTypeID": 155,

"eqpNo": "0001-00001",

"pluginID": null,

"rank": 1,

"category": 2

}]

}

3.3.4 告警事件处理（点击3.3.2 告警信息列表展示中，每条告警中预留操作/处理按钮，弹框/页面来进行下一步的处理）