**简介**

本文将介绍aTrust Syslog配置方法、日志格式以及日志中各字段的含义。

**配置说明**

配置路径：审计中心-外置日志中心-第三方Syslog

**Syslog服务器配置**



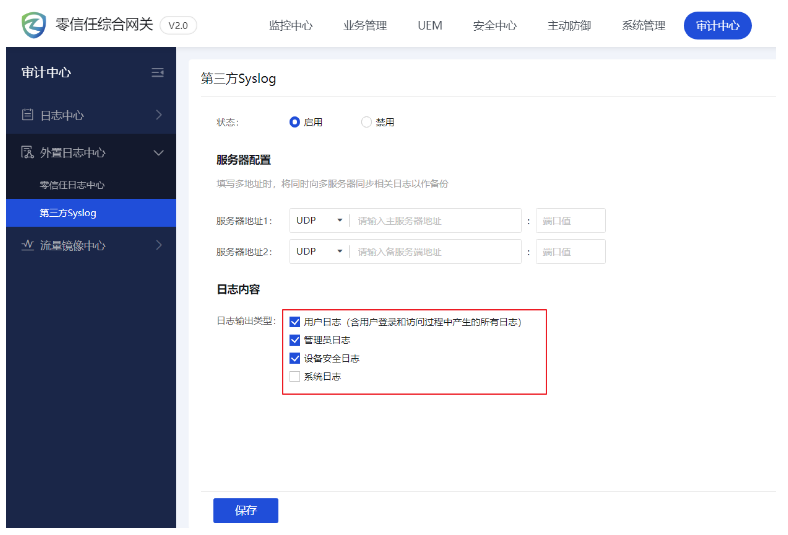
配置说明：

1.支持TCP、UDP传输方式

2.服务器名称、服务器地址、端口为必填项

3.服务器地址只支持填写IP

**日志类型配置**



配置说明：

1.具有用户日志（含用户登录和访问过程中产生的所有日志）、管理员日志、设备安全日志、系统日志四种日志类型

**集群部署环境下配置**

在集群部署下只有主节点能够配置Syslog，从节点服务器无法配置。主节点上的Syslog配置会**同步到从节点服务器上**。

**日志格式说明**

日志使用RFC 3164syslog协议标准：(<https://www.rfc-editor.org/info/rfc3164>)

具体格式示例请见后续章节

**2.3.10 日志字段调整说明**

您可以直接查看对应日志的【字段说明】章节阅读完整的字段解释

**通用调整：**

| **调整前字段名** | **调整后字段名** | **备注** |
| --- | --- | --- |
| event.isRiskEvent | \_isRisk | 值调整为1/0 |
| actor.username | actor.name |  |
| actor.label |  | 废弃 |
| actor.phone | actor.phoneNumber |  |
| actor.sessionId | actor.sTraceId | 含义改变，不输出真正的会话ID，输出会话跟踪码 |
|  | actor.externalId | 新增，用户外部ID |
|  | actor.directoryName | 新增，用户目录名称 |
| actor其他字段保持不变 | actor其他字段保持不变 |  |
| client.id | src.dvc.id |  |
| client.ip | src.ip |  |
| client.preProxyIP | src.preProxyIP |  |
| client.addr |  | 废弃此字段，按国家省市分开处理 |
| client.mac | src.dvc.mac |  |
| client.deviceName | src.dvc.hostname |  |
|  | src.dvc.modelName | 新增，品牌型号 |
| client.userAgent.browser | src.client.browser |  |
|  | src.client.browserVersion | 新增，暂未实现 |
|  | src.client.version | 新增，客户端版本 |
|  | src.client.type | 新增，值的范围'SDPClient'， 'SDPBrowserClient'， 'SangforIdClient'， 'ECClient'， 'SDKClient'， 'MobileClient' |
| client.userAgent.os | src.dvc.os |  |
| client.userAgent.rawUserAgent | src.client.httpUserAgent |  |
| client.virtualIp | src.virtualIp |  |
| client.country | src.geo.country |  |
| client.city | src.geo.city |  |
| client.province | src.geo.province |  |
|  | src.geo.organization |  |
| client.edrAgentId | src.edrAgentId |  |
| clinet.externalId | src.dvc.externalId |  |
| source.id | vendor.dvcId |  |
| source.type | vendor.productType |  |
| source.displayName |  | 废弃 |
|  | vendor.dvcIp | 新增，设备IP |
|  | vendor.sourceName | 新增，客户名称 |
|  | vendor.product | 新增，产品名称 |
|  | vendor.productVersion | 新增，产品版本号 |
| target.dispalyName | target.name |  |
| target其他字段不变 | target其他字段不变 |  |
| event.timestamp | event.timestamp | 值调整为13位整数时间戳 |
|  | event.startTime | 新增，事件开始时间 |
|  | event.endTime | 新增，事件结束时间 |
| event其他字段不变 | event其他字段不变 |  |
|  | security | 新增安全字段，具体见【用户日志-字段说明-安全信息】 |
|  | acl | 新增ACL字段，具体见【用户日志-字段说明-ACL】 |

**访问日志调整：**

各字段调整到了network，具体见【访问日志-字段说明-访问信息】

| **调整前字段名** | **调整后字段名** | **备注** |
| --- | --- | --- |
| target.dispalyName | network.app.name | 应用名称，以前放在target，现在移动到network.app下（仅访问日志调整，其他日志的target不变） |
| target.id | network.app.id | 应用ID，以前放在target，现在移动到network.app下（仅访问日志调整，其他日志的target不变） |
| target.type | network.app.type | 应用类型，以前放在target，现在移动到network.app下（仅访问日志调整，其他日志的target不变） |
|  | network.app.groupId | 新增，应用分类ID |
|  | network.app.groupName | 新增，应用分类名称 |
|  | network.protocol | 新增，访问协议 |
| target.details.app.status.recvBytes | network.recvBytes |  |
| target.details.app.status.sendBytes | network.sendBytes |  |
| target.details.app.status.responseTime | network.responseTime |  |
|  | network.conn.dstHost | 新增，目标主机 |
| target.details.app.upstream.host | network.conn.dstIp |  |
| target.details.app.upstream.port | network.conn.dstPort |  |
| target.details.app.upstream.srcIp | network.conn.srcIp |  |
| target.details.app.upstream.srcPort | network.conn.srcPort |  |
|  | network.debug.connId | 新增， tcp连接唯一标识符，调试用 |
| target.details.app.status.authTime | network.debug.authTime |  |
| target.details.app.status.resolveTime | network.debug.upstreamResolveTime |  |
| target.details.app.status.upstreamConnectTime | network.debug.upstreamConnectTime |  |
| target.details.app.status.upstreamHeaderTime | network.debug.upstreamHeaderTime |  |
| target.details.app.status.upstreamResponseTime | network.debug.upstreamResponseTime |  |
| target.details.web.request.url | network.web.reqUrl |  |
|  | network.web.reqHost | 新增，前端访问主机名 |
|  | network.web.reqHttpHost | 新增，前端访问地址httpHost |
|  | network.web.reqHttpUserAgent | 新增，userAgent |
| target.details.web.request.backendUrl | network.web.reqBackendUrl |  |
|  | network.web.reqBackendHost | 新增，后端访问主机名 |
| target.details.web.request.refer | network.web.reqRefer |  |
| target.details.web.request.xForwardedFor | network.web.reqXff |  |
| target.details.web.request.query | network.web.reqQuery |  |
| target.details.web.request.method | network.web.reqMethod |  |
| target.details.web.request.body | network.web.reqBody |  |
|  | network.web.reqSchema | 新增，WEB协议 |
| target.details.web.response.redirectUri | network.web.resRedirectUri |  |
| target.details.web.response.server | network.web.resServer |  |
| target.details.web.response.status | network.web.resStatusCode |  |
| target.details.web.response.contentType | network.web.resContentType |  |
| target.details.web.response.contentLength | network.web.resContentLength |  |
| target.details.web.response.contentDisposition | network.web.resContentDisposition |  |
| target.details.web.response.attachment |  | 废弃 |
| target.flowLimit |  | 废弃 |
| client.userAgent.processName | src.process.name |  |
| client.userAgent.processPath | src.process.path |  |
| client.userAgent.processDigtalSignature |  | 废弃 |
| client.userAgent.processFingerprint |  | 废弃 |

**设备安全日志调整：**

请求的API相关信息移动到了API节点下，具体见【设备安全日志-字段说明-API信息】

**1.用户日志**

**1.1 示例**

用户日志的programname包含：@userCtrlLog

完整报文示例如下：

<150>Aug 14 10:42:46 localhost sdp-controller@userCtrlLog[128]: { "actor": { "id": "9f8146c0-8aeb-11ec-b30f-e50f6db6d9d6", "externalId": "", "directoryName": "本地用户目录", "type": "user", "name": "user", "description": "描述", "displayName": "张三", "groupPath": "\/test\/99", "domain": "local", "phoneNumber": "185\*\*\*\*0000", "email": "881\*\*\*\*988@qq.com", "sTraceId": "8de0bdf2-fa99-46a2-b618-580ec74e27a4", "tags": [ ] }, "src": { "dvc": { "id": "", "os": "Windows 10", "mac": "", "hostname": "", "modelName": "", "tags": [ ], "externalId": "" }, "geo": { "tags": [ ], "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" }, "loginGeo": { "tags": [ ], "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" }, "client": { "type": "SDPBrowserClient", "version": "", "httpUserAgent": "Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/115.0.0.0 Safari\/537.36", "browser": "Chrome\/115.0.0.0", "browserVersion": "" }, "ip": "1.1.1.1", "ipTags": [ ], "loginIp": "1.1.1.1", "loginIpTags": [ ], "preProxyIp": "1.1.1.1" }, "event": { "id": "408ad571-3a4c-11ee-961b-1fea8304b102", "subType": "user.try\_primary\_bruteforce", "mainType": "auth", "reason": "连续登陆失败4次", "result": "-", "timestamp": 1691980966983, "\_vSchema": "risk" }, "security": { "engine": "IDP", "confidence": 3, "riskLevel": 1, "firstDefense": "IdDefense", "secondDefense": "PrimaryAuthDefense", "severity": 1, "attTactic": [ "TA0006" ], "attTechnique": [ "T1110.001" ], "threatCategory": "AccountBruteForce", "threatType": "AccountBruteForce", "d3Tactic": "Detect", "d3Technique": "D3-ANET", "engineVersion": "1.4.3", "engineRuleVersion": "1.6.1", "ruleName": "IDP\_USER\_TRY\_PRIMARY\_BRUTE\_FORCE" }, "traceId": "4953bd3b", "\_isRisk": 1, "\_logId": "1122419", "vendor": { "product": "aTrust", "productType": "hybrid", "productVersion": "2.3.10", "dvcId": "A14C0E10", "sourceName": "A14C0E10", "dvcIp": "1.1.1.1" } }

Copy

其中正文为：

{

"actor": {

"id": "9f8146c0-8aeb-11ec-b30f-e50f6db6d9d6",

"externalId": "",

"directoryName": "本地用户目录",

"type": "user",

"name": "user",

"description": "描述",

"displayName": "张三",

"groupPath": "/test/99",

"domain": "local",

"phoneNumber": "185\*\*\*\*0000",

"email": "881\*\*\*\*988@qq.com",

"sTraceId": "8de0bdf2-fa99-46a2-b618-580ec74e27a4",

"tags": []

},

"src": {

"dvc": {

"id": "",

"os": "Windows 10",

"mac": "",

"hostname": "",

"modelName": "",

"tags": [],

"externalId": ""

},

"geo": {

"tags": [],

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

},

"loginGeo": {

"tags": [],

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

},

"client": {

"type": "SDPBrowserClient",

"version": "",

"httpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36",

"browser": "Chrome/115.0.0.0",

"browserVersion": ""

},

"ip": "1.1.1.1",

"ipTags": [],

"loginIp": "1.1.1.1",

"loginIpTags": [],

"preProxyIp": "1.1.1.1"

},

"event": {

"id": "408ad571-3a4c-11ee-961b-1fea8304b102",

"subType": "user.try\_primary\_bruteforce",

"mainType": "auth",

"reason": "连续登陆失败4次",

"result": "-",

"timestamp": 1691980966983,

"\_vSchema": "risk"

},

"security": {

"engine": "IDP",

"confidence": 3,

"riskLevel": 1,

"firstDefense": "IdDefense",

"secondDefense": "PrimaryAuthDefense",

"severity": 1,

"attTactic": [

"TA0006"

],

"attTechnique": [

"T1110.001"

],

"threatCategory": "AccountBruteForce",

"threatType": "AccountBruteForce",

"d3Tactic": "Detect",

"d3Technique": "D3-ANET",

"engineVersion": "1.4.3",

"engineRuleVersion": "1.6.1",

"ruleName": "IDP\_USER\_TRY\_PRIMARY\_BRUTE\_FORCE"

},

"traceId": "4953bd3b",

"\_isRisk": 1,

"\_logId": "1122419",

"vendor": {

"product": "aTrust",

"productType": "hybrid",

"productVersion": "2.3.10",

"dvcId": "A14C0E10",

"sourceName": "A14C0E10",

"dvcIp": "1.1.1.1"

}

}

**1.2 字段说明**

**1.2.1 主体（actor）**

主体信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 用户ID，一般为UUID，外部未导入用户可以没有ID |
| externalId | string | 用户外部ID，可空 |
| type | string | 用户类型，可选值：user（用户）、admin（管理员） |
| name | string | 用户名 |
| directoryName | string | 所属用户目录名称 |
| domain | string | 所属用户目录域 |
| description | string | 用户描述 |
| displayName | string | 显示名 |
| groupPath | string | 所属组织架构 |
| phoneNumber | string | 手机号码，输出到日志中的已经掩码 |
| email | string | 电子邮箱，输出到日志中的已经掩码 |
| details | string | 用户详情，可空，一般为JSON，外部服务器登录时，会输出角色和组织架构信息 |
| tags | []string | 用户分析，可选值：FirstLoginAccount（首次登录账号）、IdleAccount（闲置账号） |
| sTraceId | string | 会话ID，用于跟踪用户会话，这里不是真正起作用的会话ID |

**JSON格式**

"actor": {

"id": "2616cbd2-d4d8-47f7-93cd-44d4b5a09e35",

"externalId": "996dccd9-2a5c-42cb-971f-205e9801ff5d",

"type": "user",

"name": "zhangsan",

"directoryName": "本地用户目录",

"domain": "local",

"description": "",

"displayName": "张三",

"groupPath": "/",

"phoneNumber": "188\*\*\*\*8888",

"email": "188\*\*\*\*88@qq.com",

"details": "",

"tags": [],

"sTraceId": "6d7b6a7f-364b-4fbe-bae1-4329553a5e05"

}

**1.2.2 源（src）**

来源信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| dvc |  | 设备，设备信息 |
| .id | string | 终端ID，由硬件特征码计算出来的ID，不更换硬件一般不会变。注：如果没有安装客户端使用浏览器登录，则由浏览器随机生成终端ID（清除缓存会更换ID） |
| .os | string | 操作系统 |
| .mac | string | MAC地址，需要安装客户端方可取到 |
| .assetType | string | 资产类型，需要安装客户端方可取到 |
| .hostname | string | 终端名称，需要安装客户端方可取到 |
| .modelName | string | 品牌型号，需要安装客户端方可取到 |
| .externalId | string | 外部ID，导入终端时可以指定的外部ID，用于第三方联动审计 |
| .edrAgentId | string | EDR客户端ID，需要安装EDR客户端方可取到 |
| .tags | []string | 终端分析，可选值：FirstDvc（首次登录终端）、NewDvc（新终端）、CommonlyDvc（非常用终端）、UncommonlyDvc（常用终端） |
| geo |  | 地理信息，实时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| loginGeo |  | 登录地理信息，登录时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| .tags | []string | 登录归属地分析，可选值：FirstLocation（首次登录地点）、NewLocation（新地点）、UncommonlyLocation（非常用地点）、CommonlyLocation（常用地点） |
| client |  | 客户端信息 |
| .type | string | 客户端类型，可选值：SDPBrowserClient（浏览器客户端）、SDPClient（客户端）、SDKClient（SDK）、SangforIdClient（移动端）、MobileClient（移动端） |
| .version | string | 客户端版本 |
| .httpUserAgent | string | userAgent |
| .browser | string | 浏览器 |
| preProxyIp | string | 代理IP |
| ip | string | 客户端源IP |
| ipTags | []string | IP分析 |
| loginIp | string | 登录IP |
| loginIpTags | []string | 登录IP分析 |

**JSON格式**

"src": {

"dvc": {

"id": "6cdbe1f3-6abf-427a-b378-8b4da5162534",

"os": "Windows",

"mac": "AA:BB:CC:DD:EE:FF",

"assetType": "",

"hostname": "DESKTOP-123456",

"modelName": "",

"externalId": "",

"edrAgentId": "",

"tags": []

},

"geo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南"

},

"loginGeo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南",

"tags": []

},

"client": {

"type": "",

"version": "2.3.10.10",

"httpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",

"browser": "Chrome/118.0.0.0"

},

"preProxyIp": "1.1.1.1",

"ip": "1.1.1.1",

"ipTags": [],

"loginIp": "1.1.1.1",

"loginIpTags": []

}

**1.2.3 事件（event）**

事件信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 日志ID，日志唯一ID |
| mainType | string | 操作类型 |
| subType | string | 操作子类型 |
| timestamp | number | 时间，13位时间戳（无时区概念），精确到毫秒 |
| result | string | 结果，可选值：SUCCESS（成功）、FAILED（失败）、-（无） |
| reason | string | 原因 |
| action | string | 处置动作，可选值：DENY（已拦截）、ALLOW（已通过）、-（无） |
| startTime | number | 事件开始时间，可空，13位时间戳（无时区概念），精确到毫秒 |
| endTime | number | 事件结束时间，可空，13位时间戳（无时区概念），精确到毫秒 |
| \_vSchema | string | schema，用于动态控制控制台展示某些字段，可选值：management（显示target字段）、apiGuard（显示api字段）、risk（显示security字段）、acl（显示acl字段）、proxy（显示target、network字段） |
| details | string | 日志描述，可空，一般为JSON，为日志的附加信息 |

**JSON格式**

"event": {

"id": "67f48a04-7961-44af-a693-1833decff4f0",

"mainType": "user",

"subType": "user.login",

"timestamp": 1689606221501,

"result": "SUCCESS",

"reason": "",

"action": "",

"startTime": 0,

"endTime": 0,

"\_vSchema": "",

"details": ""

}

**1.2.4 客体（target）**

客体信息：涉及到操作对象的日志会有客体信息：如应用鉴权日志（客体信息为应用信息）、授信终端（客体信息为终端信息）等

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 客体ID |
| type | string | 操作对象 |
| name | string | 操作内容 |
| details | string | 操作详情，可空，一般为JSON，为客体的附加信息 |

**JSON格式**

"target": {

"id": "54bad20a-488d-4923-84d5-cec6834799cf",

"type": "local\_user",

"name": "张三",

"details": ""

}

**1.2.5 安全信息（security）**

安全信息，当日志中的\_isRisk=1时为安全日志，会有安全日志节点

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| ruleName | string | 防护规则名称 |
| firstDefense | string | SDP防线，可选值：DvcDefense（设备防线）、IdDefense（账号防线）、AppDefense（终端防线） |
| secondDefense | string | SDP子防线，可选值：PrimaryAuthDefense（主认证防线）、ApiDefense（API防线）、SecondaryAuthDefense（从认证防线）、UdpSpaDefense（UDP SPA防线）、TcpSpaDefense（TCP SPA防线）、TrapDefense（诱捕防线）、SessionDefense（会话防线） |
| attTactic | []string | ATT&CK战术 |
| attTechnique | []string | ATT&CK技术 |
| d3Tactic | string | D3Fend防御战术 |
| d3Technique | string | D3Fend防御技术 |
| engine | string | 安全引擎名称 |
| engineVersion | string | 安全引擎版本 |
| engineRuleVersion | string | 防护规则版本 |
| severity | number | 严重程度，1~3，分别代表低中高 |
| riskLevel | number | 风险等级，1~3，分别代表低中高 |
| confidence | number | 威胁置信度，1~3，分别代表低中高 |
| threatCategory | string | 威胁分类 |
| threatType | string | 威胁类型 |

**JSON格式**

"security": {

"ruleName": "RASP\_API\_SCAN",

"firstDefense": "DvcDefense",

"secondDefense": "ApiDefense",

"attTactic": [

"TA0043"

],

"attTechnique": [

"T1595"

],

"d3Tactic": "Detect",

"d3Technique": "D3-PMAD",

"engine": "RASP",

"engineVersion": "1.0.0",

"engineRuleVersion": "1.0.0",

"severity": 1,

"riskLevel": 1,

"confidence": 1,

"threatCategory": "HackingTool",

"threatType": "ScanningTool"

}

**1.2.6 ACL（acl）**

ACL信息，由于ACL失败的应用鉴权日志、ACL阻断用户上线、ACL阻断访问应用会有ACL节点

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | ACL策略ID |
| code | string | ACL策略编号，P开头为应用防护策略、L开头为上线准入策略、A开头为威胁处置策略 |
| name | string | ACL策略名称 |
| timing | string | ACL策略类型，可选值：auth-app（应用防护）、pre-login（上线准入） |
| action | string | 处置动作 |
| actionType | string | 处置类型，可选值：prevEffect（补救）、effect（处置） |

**JSON格式**

"acl": {

"id": "713cac16-a114-4706-a926-4d015da0adf5",

"code": "P000001",

"name": "ACL防护策略",

"timing": "auth-app",

"action": "auth/sms",

"actionType": "prevEffect"

}

**1.2.7 设备（vendor）**

设备信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| sourceName | string | 客户名称，取自授权客户名称 |
| product | string | 产品名称，可选值：aTrust、VPN |
| productVersion | string | 产品版本号 |
| productType | string | 产品类型，可选值：hybrid（综合网关）、sdp（控制中心）、proxy（代理网关） |
| dvcId | string | 设备ID |
| dvcIp | string | 设备IP |

**JSON格式**

"vendor": {

"sourceName": "",

"product": "aTrust",

"productVersion": "2.3.6",

"productType": "hybrid",

"dvcId": "ABCDEF",

"dvcIp": "1.1.1.1"

}

**1.2.8 是否安全日志（\_isRisk）**

可选值：0（否），1（是）

**1.2.9 TraceID（traceId）**

请求接口跟踪码

**1.2.10 日志对账ID（\_logId）**

rsyslog自动生成的自增ID，用于排查是否丢失日志

**1.3.日志类型**

**1.3.1 登录**

此类事件的主类型（mainType）为login，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.login | 登录 |  |

**1.3.2 登录事件**

此类事件的主类型（mainType）为auth，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.abnormal\_login\_sms | 异常登录事件短信通知 |  |
| user.abnormal\_period\_login | 异常时间段登录 | √ |
| user.first\_login | 账号首次登录 | √ |
| user.idle\_account\_login | 闲置账号登录 | √ |
| user.login\_in\_first\_location | 账号在该地点首次登录 | √ |
| user.login\_in\_new\_location\_v2 | 账号在新地点登录 | √ |
| user.login\_in\_uncommonly\_location | 账号在非常用地点登录 | √ |
| user.mitm\_req\_complete | 中间人检测 |  |
| user.new\_device\_login | 账号在该终端首次登录 | √ |
| user.remote\_login\_tia | 账号多会话异地登录 | √ |
| user.weak\_psw\_login | 弱密码登录 |  |

**1.3.3 认证**

此类事件的主类型（mainType）为auth/auth\_primary/auth\_secondary/auth\_trust\_device/auth\_enhance\_acl\_pre\_login/auth\_enhance\_acl\_auth\_app，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| uem\_author.auth | UEM授权准入认证 |  |
| user.access\_check.auth | 准入认证 |  |
| user.alert.auth | 安全警示认证 |  |
| user.auth\_check.auth | 用户认证策略匹配 |  |
| user.cas.auth | CAS认证 |  |
| user.cert.auth | 证书认证 |  |
| user.check\_code.auth | 短信验证码校验 |  |
| user.dingtalk.auth | 钉钉认证 |  |
| user.feishu.auth | 飞书认证 |  |
| user.govDingtalk.auth | 浙政钉认证 |  |
| user.https\_oauth2.auth | 自定义oauth2认证 |  |
| user.https\_psw.auth | https密码认证 |  |
| user.https\_sms.auth | 短信认证 |  |
| user.https\_token.auth | HTTP(S)令牌认证 |  |
| user.ldap.auth | LDAP认证 |  |
| user.local\_psw.auth | 本地密码认证 |  |
| user.oauth2.auth | oauth2认证 |  |
| user.passport\_token\_online.auth | 客户端免密认证 |  |
| user.passport\_token\_verify.auth | 免密校验认证 |  |
| user.qrcode.auth | 扫码认证 |  |
| user.qywechat.auth | 企业微信认证 |  |
| user.radius.auth | radius认证 |  |
| user.sangfor\_id.auth | 手机令牌免密认证 |  |
| user.secondaryCert.auth | 证书二次认证 |  |
| user.send\_sms | 发送短信 |  |
| user.skip\_second\_auth | 免辅认证 |  |
| user.token.auth | 令牌认证 |  |
| user.totp\_token.auth | totp令牌认证 |  |
| user.totp\_token.bind | 绑定totp密钥 |  |
| user.trust\_device.auth | 授信终端认证 |  |

**1.3.4 注销**

此类事件的主类型（mainType）为logout，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.ac\_linkage.logout | AC联动下线 |  |
| user.logout | 注销 |  |
| user.logout\_by\_acl | ACL注销 |  |
| user.logout\_by\_admin | 被管理员强制注销 |  |
| user.logout\_by\_config\_change | 配置变更注销 |  |
| user.logout\_by\_cookie\_hijacking | 发生会话劫持被注销 |  |
| user.logout\_by\_forget\_pwd | 忘记密码并重置成功后下线其他会话 |  |
| user.logout\_by\_mod\_pwd | 密码失效注销 |  |
| user.logout\_by\_no\_operation\_timeout | 无鼠标键盘操作超时注销 |  |
| user.logout\_by\_relogin | 上线抢占注销 |  |
| user.logout\_by\_self | 主动注销 |  |
| user.logout\_by\_session\_timeout | 无业务访问流量超时注销 |  |
| user.logout\_by\_time\_plan | 时间计划注销 |  |
| user.logout\_by\_token\_client | 注销免密登录令牌（token） |  |
| user.logout\_by\_uem\_auth\_forbid | UEM授权失败注销 |  |
| user.timeout\_offline | 无业务访问流量超时注销 |  |

**1.3.5 修改密码**

此类事件的主类型（mainType）为modify\_pwd/forget\_pwd，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.forget\_pwd | 忘记密码 |  |
| user.modify\_pwd | 登录后修改密码 |  |
| user.modify\_pwd.auth | 强制修改密码 |  |
| user.reset\_pwd\_by\_forget\_pwd | 通过忘记密码重置密码 |  |
| user.skip\_modify\_pwd.auth | 跳过强制修改密码 |  |
| user.try\_to\_reset\_pwd\_by\_forget\_pwd | 尝试通过忘记密码重置密码 |  |

**1.3.6 ACL动态访问控制**

此类事件的主类型（mainType）为acl，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.access\_denied\_by\_acl | ACL阻断访问应用 |  |
| user.acl\_event\_by\_uem\_sandbox | 工作空间准入策略被执行 |  |
| user.acl\_passed | ACL校验通过 |  |
| user.disabled\_by\_acl | ACL策略锁定 |  |
| user.disabled\_by\_security\_risk | 威胁诱捕锁定 | √ |
| user.log\_by\_acl | ACL记录风险事件日志 |  |
| user.login\_denied\_by\_acl | ACL阻断用户上线 |  |
| user.passed\_by\_rescued | ACL灰度处置成功通过授权 |  |
| user.rescue\_by\_acl | ACL灰度处置 |  |
| user.revoke\_app\_token\_by\_acl | ACL吊销应用访问凭据 |  |

**1.3.7 授信终端**

此类事件的主类型（mainType）为trust\_device/untrust\_device/user，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| device.logout\_by\_user | 授信终端注销在线用户 |  |
| device.trust\_by\_user | 添加授信终端 |  |
| device.untrust\_by\_user | 移除授信终端 |  |
| user.bind\_authorized\_device | 添加授信终端 |  |
| user.delete\_redundancy\_devices | 自动清理多余的临时终端 |  |
| user.trust\_device | 用户可信终端 |  |
| user.untrust\_device | 用户取消可信终端 |  |

**1.3.8 终端诱饵**

此类事件的主类型（mainType）为deviceDecoy，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.device.decoy.distribute | 终端诱饵下发 |  |
| user.device.decoy.write | 终端诱饵写入 |  |

**1.3.9 SPA**

此类事件的主类型（mainType）为spa，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.spa.exchange\_seed | SPA激活码交换安全码 |  |
| user.spa.steal\_seed | SPA安全码泄露 | √ |
| user.spa.steal\_tmp\_seed | SPA激活码泄露 | √ |
| user.spa.tcp | TCP SPA敲门 |  |
| user.spa.tcp.compat\_check | TCP SPA安全码兼容性检查 |  |
| user.spa.tcp.exhaustive\_attack | TCP SPA爆破攻击 | √ |
| user.spa.tcp.format\_check\_failed | TCP SPA格式检查 |  |
| user.spa.tcp.inconsistent\_system\_time | TCP SPA终端时间同步检查 |  |
| user.spa.tcp.passpord\_failed | TCP SPA口令检查 |  |
| user.spa.tcp.seed\_expire | TCP SPA安全码有效期检查 |  |
| user.spa.tcp.seed\_not\_exist | TCP SPA安全码不存在 |  |
| user.spa.tcp.tmp\_seed\_expired | TCP SPA激活码有效期检查 |  |
| user.spa.tcp.tmp\_seed\_not\_exist | TCP SPA激活码不存在 |  |
| user.spa.tcp.tmp\_seed\_revoked | TCP SPA激活码有效性检查 |  |
| user.spa.udp | UDP SPA敲门 |  |
| user.spa.udp.compat\_check | UDP SPA安全码兼容性检查 |  |
| user.spa.udp.exhaustive\_attack | UDP SPA爆破攻击 | √ |
| user.spa.udp.forgery\_attack | UDP SPA敲门伪造 | √ |
| user.spa.udp.inconsistent\_system\_time | UDP SPA终端时间同步检查 |  |
| user.spa.udp.replay\_attack | UDP SPA重放攻击 | √ |
| user.spa.udp.seed\_expire | UDP SPA安全码有效期检查 |  |
| user.spa.udp.seed\_not\_exist | UDP SPA安全码不存在 |  |
| user.spa.udp.sniffers\_attack | SPA Fuzz攻击 | √ |
| user.spa.udp.tmp\_seed\_expired | UDP SPA激活码有效期检查 |  |
| user.spa.udp.tmp\_seed\_not\_exist | UDP SPA激活码不存在 |  |
| user.spa.udp.tmp\_seed\_revoked | UDP SPA激活码有效性检查 |  |

**1.3.10 违反客户端防护规则**

此类事件的主类型（mainType）为uem\_client\_protection，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.apihookRevert.unknown.uemProcess | 移除客户端安全钩子 | √ |
| user.apihookRevert.unknown.workspaceProcess | 移除工作空间内进程安全钩子 | √ |
| user.crossSpaceDataTrans.process.process | 跨空间进程通信 | √ |
| user.debug.personalProcess.clientProcess | 在个人空间调试客户端进程 | √ |
| user.debug.personalProcess.workspaceProcess | 在个人空间调试工作空间内进程 | √ |
| user.debug.workspaceProcess.clientProcess | 在工作空间调试客户端进程 | √ |
| user.debug.workspaceProcess.workspaceProcess | 在工作空间调试工作空间内进程 | √ |
| user.violating\_client\_protection\_rules\_lock | 违反客户端防护规则被锁定 | √ |

**1.3.11 uem**

此类事件的子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| uem\_app\_store.markMsgAsRead | 标记控制台消息已读 |  |
| uem\_app\_store.pkg\_exists | 获取ABM应用兑换码 |  |
| uem\_app\_store.report\_install | 上报安装信息 |  |
| uem\_audit\_task.approved\_task | 审批任务批准 |  |
| uem\_audit\_task.complete\_task | 审批任务完结 |  |
| uem\_audit\_task.new\_task | 新建审批任务 |  |
| uem\_audit\_task.reject\_task | 审批任务拒绝 |  |
| uem\_audit\_task.terminate\_task | 审批任务终止 |  |
| uem\_audit\_task.update\_task | 更新审批任务 |  |
| uem\_audit\_task.withdraw\_task | 审批任务撤销 |  |
| uem\_author.clear | UEM授权清理 |  |

**1.3.12 爆破登录**

此类事件的主类型（mainType）为auth，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| ip.enhance\_bruteforce\_locked | 增强认证爆破锁定IP | √ |
| ip.primary\_bruteforce\_locked | 首次认证爆破锁定IP | √ |
| ip.secondary\_bruteforce\_locked | 二次认证爆破锁定IP | √ |
| user.enhance\_bruteforce\_locked | 增强认证爆破锁定账号 | √ |
| user.primary\_bruteforce\_locked | 首次认证爆破锁定账号 | √ |
| user.secondary\_bruteforce\_locked | 二次认证爆破锁定账号 | √ |
| user.try\_enhance\_bruteforce | 增强认证爆破 | √ |
| user.try\_primary\_bruteforce | 首次认证爆破 | √ |
| user.try\_secondary\_bruteforce | 二次认证爆破 | √ |

**1.3.13 其他**

其余未归类事件的子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.ac\_linkage.login | AC联动上线 |  |
| user.active.scanning | 用户恶意侦察 |  |
| user.app.permission | 应用鉴权 |  |
| user.cookie\_hijacking | 会话劫持 | √ |
| user.device\_log\_upload | 终端日志上传 |  |
| user.disabled\_by\_active\_scan | 恶意侦察锁定 | √ |
| user.disabled\_by\_admin | 管理员禁用用户 |  |
| user.disabled\_by\_browser\_app\_type\_abnormal | 浏览器访问应用类型异常锁定 | √ |
| user.disabled\_by\_browser\_ua\_abnormal | 浏览器访问UA信息异常锁定 | √ |
| user.disabled\_by\_intermediary\_agency | 中间人锁定 | √ |
| user.disabled\_by\_new\_process\_app\_type\_abnormal | 孤立进程访问应用类型异常锁定 | √ |
| user.disabled\_by\_web\_credential\_steal | 会话劫持锁定 | √ |
| user.honeypot.access | 访问蜜罐 | √ |
| user.intermediary\_agency | 中间人 | √ |
| user.l3app.access | 隧道应用访问 |  |
| user.login\_address\_change\_within\_session | 同一会话IP归属地变更 |  |
| user.trust\_cookie | 校验可信cookie |  |
| user.update\_sso\_config | 编辑单点登录配置 |  |
| user.web\_credential\_steal | 会话劫持 | √ |
| user.webapp.access | web应用访问 |  |

**2.访问日志**

**2.1 示例**

访问日志的programname包含：@userProxyLog

完整报文示例如下：

<150>Sep 7 11:09:15 localhost sdp-proxy@userProxyLog[1238]: { "network": { "sendBytes": 488, "debug": { "upstreamConnectTime": 3, "upstreamHeaderTime": 7, "upstreamResponseTime": 14 }, "responseTime": 14, "conn": { "srcPort": 52002, "dstHost": "1.1.1.1", "dstIp": "1.1.1.1", "dstPort": 80, "srcIp": "1.1.1.1" }, "protocol": "http", "app": { "type": "webapp", "id": "ee8782a0-0125-11ee-b353-0527bf15439e", "name": "企业网盘", "groupId": "default", "groupName": "默认分类" }, "recvBytes": 7397, "web": { "resContentType": "text\/html", "reqHttpHost": "webapp.com", "reqSchema": "http", "reqUrl": "http:\/\/webapp.com:80\/", "reqMethod": "GET", "reqHost": "webapp.com", "reqBackendUrl": "http:\/\/1.1.1.1:80\/", "reqBackendHost": "1.1.1.1", "reqReferer": "http:\/\/webapp.com\/", "reqXff": "1.1.1.1", "resStatusCode": 200, "resServer": "Everything HTTP Server", "reqHttpUserAgent": "Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/118.0.0.0 Safari\/537.36" } }, "actor": { "phoneNumber": "18\*\*\*\*\*\*000", "id": "9f8146c0-8aeb-11ec-b30f-e50f6db6d9d6", "tags": [ "IdleAccount" ], "email": "8\*\*\*\*\*\*\*\*8@qq.com", "displayName": "张三", "name": "zhangsan", "externalId": "", "directoryName": "本地用户目录", "domain": "local", "groupPath": "\/test\/99", "type": "user", "sTraceId": "cea93c87-4973-49cb-aecf-48b4a1524e94" }, "traceId": "010e9f6163fa96b9", "event": { "timestamp": 1694056155867, "\_vSchema": "proxy", "subType": "user.webapp.access", "reason": "", "result": "SUCCESS", "id": "4ca64f41-ab3c-4892-9217-86e846e3dfa5", "mainType": "app" }, "src": { "preProxyIp": "1.1.1.1", "client": { "type": "SDPBrowserClient" }, "ip": "1.1.1.1", "dvc": { "os": "Windows 10", "id": "0011945c35df39ee2476394a3679968e8ac5697cf808a04bf2", "hostname": "Chrome", "modelName": "", "assetType": "", "externalId": "bb370a11-1bd8-4ebd-9f65-2944af25c426", "tags": [ "FirstDvc" ], "mac": "", "edrAgentId": "" }, "port": 63695, "loginGeo": { "tags": [ "UncommonlyLocation" ], "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" }, "loginIp": "1.1.1.1", "geo": { "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" } }, "\_logId": "2545", "version": "2.0", "vendor": { "product": "aTrust", "productType": "hybrid", "productVersion": "2.3.10", "dvcId": "A14C0E10", "sourceName": "A14C0E10", "dvcIp": "1.1.1.1" } }

Copy

其中正文为：

{

"network": {

"sendBytes": 488,

"debug": {

"upstreamConnectTime": 3,

"upstreamHeaderTime": 7,

"upstreamResponseTime": 14

},

"responseTime": 14,

"conn": {

"srcPort": 52002,

"dstHost": "1.1.1.1",

"dstIp": "1.1.1.1",

"dstPort": 80,

"srcIp": "1.1.1.1"

},

"protocol": "http",

"app": {

"type": "webapp",

"id": "ee8782a0-0125-11ee-b353-0527bf15439e",

"name": "企业网盘",

"groupId": "default",

"groupName": "默认分类"

},

"recvBytes": 7397,

"web": {

"resContentType": "text/html",

"reqHttpHost": "webapp.com",

"reqSchema": "http",

"reqUrl": "http://webapp.com:80/",

"reqMethod": "GET",

"reqHost": "webapp.com",

"reqBackendUrl": "http://1.1.1.1:80/",

"reqBackendHost": "1.1.1.1",

"reqReferer": "http://webapp.com/",

"reqXff": "1.1.1.1",

"resStatusCode": 200,

"resServer": "Everything HTTP Server",

"reqHttpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36"

}

},

"actor": {

"phoneNumber": "18\*\*\*\*\*\*000",

"id": "9f8146c0-8aeb-11ec-b30f-e50f6db6d9d6",

"tags": [

"IdleAccount"

],

"email": "8\*\*\*\*\*\*\*\*8@qq.com",

"displayName": "张三",

"name": "zhangsan",

"externalId": "",

"directoryName": "本地用户目录",

"domain": "local",

"groupPath": "/test/99",

"type": "user",

"sTraceId": "cea93c87-4973-49cb-aecf-48b4a1524e94"

},

"traceId": "010e9f6163fa96b9",

"event": {

"timestamp": 1694056155867,

"\_vSchema": "proxy",

"subType": "user.webapp.access",

"reason": "",

"result": "SUCCESS",

"id": "4ca64f41-ab3c-4892-9217-86e846e3dfa5",

"mainType": "app"

},

"src": {

"preProxyIp": "1.1.1.1",

"client": {

"type": "SDPBrowserClient"

},

"ip": "1.1.1.1",

"dvc": {

"os": "Windows 10",

"id": "0011945c35df39ee2476394a3679968e8ac5697cf808a04bf2",

"hostname": "Chrome",

"modelName": "",

"assetType": "",

"externalId": "bb370a11-1bd8-4ebd-9f65-2944af25c426",

"tags": [

"FirstDvc"

],

"mac": "",

"edrAgentId": ""

},

"port": 63695,

"loginGeo": {

"tags": [

"UncommonlyLocation"

],

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

},

"loginIp": "1.1.1.1",

"geo": {

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

}

},

"\_logId": "2545",

"version": "2.0",

"vendor": {

"product": "aTrust",

"productType": "hybrid",

"productVersion": "2.3.10",

"dvcId": "A14C0E10",

"sourceName": "A14C0E10",

"dvcIp": "1.1.1.1"

}

}

**2.2 字段说明**

**2.2.1 主体（actor）**

主体信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 用户ID，一般为UUID，外部未导入用户可以没有ID |
| externalId | string | 用户外部ID，可空 |
| type | string | 用户类型，可选值：user（用户）、admin（管理员） |
| name | string | 用户名 |
| directoryName | string | 所属用户目录名称 |
| domain | string | 所属用户目录域 |
| displayName | string | 显示名 |
| groupPath | string | 所属组织架构 |
| phoneNumber | string | 手机号码，输出到日志中的已经掩码 |
| email | string | 电子邮箱，输出到日志中的已经掩码 |
| details | string | 用户详情，可空，一般为JSON，外部服务器登录时，会输出角色和组织架构信息 |
| tags | []string | 用户分析，可选值：FirstLoginAccount（首次登录账号）、IdleAccount（闲置账号） |
| sTraceId | string | 会话ID，用于跟踪用户会话，这里不是真正起作用的会话ID |

**JSON格式**

"actor": {

"id": "2616cbd2-d4d8-47f7-93cd-44d4b5a09e35",

"externalId": "996dccd9-2a5c-42cb-971f-205e9801ff5d",

"type": "user",

"name": "zhangsan",

"directoryName": "本地用户目录",

"domain": "local",

"displayName": "张三",

"groupPath": "/",

"phoneNumber": "188\*\*\*\*8888",

"email": "188\*\*\*\*88@qq.com",

"details": "",

"tags": [],

"sTraceId": "6d7b6a7f-364b-4fbe-bae1-4329553a5e05"

}

**2.2.2 源（src）**

来源信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| dvc |  | 设备，设备信息 |
| .id | string | 终端ID，由硬件特征码计算出来的ID，不更换硬件一般不会变。注：如果没有安装客户端使用浏览器登录，则由浏览器随机生成终端ID（清除缓存会更换ID） |
| .os | string | 操作系统 |
| .mac | string | MAC地址，需要安装客户端方可取到 |
| .assetType | string | 资产类型，需要安装客户端方可取到 |
| .hostname | string | 终端名称，需要安装客户端方可取到 |
| .modelName | string | 品牌型号，需要安装客户端方可取到 |
| .externalId | string | 外部ID，导入终端时可以指定的外部ID，用于第三方联动审计 |
| .edrAgentId | string | EDR客户端ID，需要安装EDR客户端方可取到 |
| .tags | []string | 终端分析，可选值：FirstDvc（首次登录终端）、NewDvc（新终端）、CommonlyDvc（非常用终端）、UncommonlyDvc（常用终端） |
| geo |  | 地理信息，实时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| loginGeo |  | 登录地理信息，登录时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| .tags | []string | 登录归属地分析，可选值：FirstLocation（首次登录地点）、NewLocation（新地点）、UncommonlyLocation（非常用地点）、CommonlyLocation（常用地点） |
| process |  | 进程信息，进程信息 |
| .name | string | 进程名称，需要安装客户端方可取到 |
| .path | string | 进程路径，需要安装客户端方可取到 |
| client |  | 客户端信息 |
| .type | string | 客户端类型，可选值：SDPBrowserClient（浏览器客户端）、SDPClient（客户端）、SDKClient（SDK）、SangforIdClient（移动端）、MobileClient（移动端） |
| preProxyIp | string | 代理IP |
| port | number | 客户端源端口 |
| ip | string | 客户端源IP |
| ipTags | []string | IP分析 |
| loginIp | string | 登录IP |
| loginIpTags | []string | 登录IP分析 |
| virtualIp | string | 虚拟IP |

**JSON格式**

"src": {

"dvc": {

"id": "6cdbe1f3-6abf-427a-b378-8b4da5162534",

"os": "Windows",

"mac": "AA:BB:CC:DD:EE:FF",

"assetType": "",

"hostname": "DESKTOP-123456",

"modelName": "",

"externalId": "",

"edrAgentId": "",

"tags": []

},

"geo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南"

},

"loginGeo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南",

"tags": []

},

"process": {

"name": "chrome.exe",

"path": ""

},

"client": {

"type": ""

},

"preProxyIp": "1.1.1.1",

"port": 50076,

"ip": "1.1.1.1",

"ipTags": [],

"loginIp": "1.1.1.1",

"loginIpTags": [],

"virtualIp": "1.1.1.1"

}

**2.2.3 事件（event）**

事件信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 日志ID，日志唯一ID |
| mainType | string | 操作类型 |
| subType | string | 操作子类型 |
| timestamp | number | 时间，13位时间戳（无时区概念），精确到毫秒 |
| result | string | 结果，可选值：SUCCESS（成功）、FAILED（失败）、-（无） |
| reason | string | 原因 |
| action | string | 处置动作，可选值：DENY（已拦截）、ALLOW（已通过）、-（无） |
| startTime | number | 事件开始时间，可空，13位时间戳（无时区概念），精确到毫秒 |
| endTime | number | 事件结束时间，可空，13位时间戳（无时区概念），精确到毫秒 |
| \_vSchema | string | schema，用于动态控制控制台展示某些字段，可选值：management（显示target字段）、apiGuard（显示api字段）、risk（显示security字段）、acl（显示acl字段）、proxy（显示target、network字段） |
| details | string | 日志描述，可空，一般为JSON，为日志的附加信息 |

**JSON格式**

"event": {

"id": "67f48a04-7961-44af-a693-1833decff4f0",

"mainType": "user",

"subType": "user.login",

"timestamp": 1689606221501,

"result": "SUCCESS",

"reason": "",

"action": "",

"startTime": 0,

"endTime": 0,

"\_vSchema": "",

"details": ""

}

**2.2.4 客体（target）**

客体信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 客体ID |
| type | string | 操作对象 |
| name | string | 操作内容 |
| details | string | 操作详情，可空，一般为JSON，为客体的附加信息 |

**JSON格式**

"target": {

"id": "54bad20a-488d-4923-84d5-cec6834799cf",

"type": "local\_user",

"name": "张三",

"details": ""

}

**2.2.5 安全信息（security）**

安全信息，当日志中的\_isRisk=1时为安全日志，会有安全日志节点

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| ruleName | string | 防护规则名称 |
| firstDefense | string | SDP防线，可选值：DvcDefense（设备防线）、IdDefense（账号防线）、AppDefense（终端防线） |
| secondDefense | string | SDP子防线，可选值：PrimaryAuthDefense（主认证防线）、ApiDefense（API防线）、SecondaryAuthDefense（从认证防线）、UdpSpaDefense（UDP SPA防线）、TcpSpaDefense（TCP SPA防线）、TrapDefense（诱捕防线）、SessionDefense（会话防线） |
| attTactic | []string | ATT&CK战术 |
| attTechnique | []string | ATT&CK技术 |
| d3Tactic | string | D3Fend防御战术 |
| d3Technique | string | D3Fend防御技术 |
| engine | string | 安全引擎名称 |
| engineVersion | string | 安全引擎版本 |
| engineRuleVersion | string | 防护规则版本 |
| severity | number | 严重程度，1~3，分别代表低中高 |
| riskLevel | number | 风险等级，1~3，分别代表低中高 |
| confidence | number | 威胁置信度，1~3，分别代表低中高 |
| threatCategory | string | 威胁分类 |
| threatType | string | 威胁类型 |

**JSON格式**

"security": {

"ruleName": "RASP\_API\_SCAN",

"firstDefense": "DvcDefense",

"secondDefense": "ApiDefense",

"attTactic": [

"TA0043"

],

"attTechnique": [

"T1595"

],

"d3Tactic": "Detect",

"d3Technique": "D3-PMAD",

"engine": "RASP",

"engineVersion": "1.0.0",

"engineRuleVersion": "1.0.0",

"severity": 1,

"riskLevel": 1,

"confidence": 1,

"threatCategory": "HackingTool",

"threatType": "ScanningTool"

}

**2.2.6 访问信息（network）**

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| protocol | string | 访问协议 |
| recvBytes | number | 接收的字节数 |
| sendBytes | number | 发送的字节数 |
| responseTime | number | 回给客户端响应时间 |
| app |  | 应用信息 |
| .id | string | 应用ID |
| .type | string | 应用类型，可选值：l3app（隧道应用，包含隧道转WEB）、webapp（WEB应用）、authfreewebapp（免认证应用） |
| .name | string | 应用名称 |
| .groupId | string | 应用分类ID |
| .groupName | string | 应用分类名称 |
| conn |  | 连接信息 |
| .dstHost | string | 目标主机 |
| .dstIp | string | 目标主机IP |
| .dstPort | number | 目标主机端口 |
| .srcIp | string | 代理网关源IP |
| .srcPort | number | 代理网关源端口 |
| debug |  | 调试信息 |
| .connId | string | tcp连接唯一标识符 |
| .authTime | number | 资源鉴权耗时 |
| .upstreamResolveTime | number | dns解析时间 |
| .upstreamConnectTime | number | 上游服务器新建耗时 |
| .upstreamHeaderTime | number | 上游服务器header返回耗时 |
| .upstreamResponseTime | number | 上游服务器响应耗时 |
| web |  | Web信息 |
| .reqUrl | string | 前端访问地址 |
| .reqHost | string | 前端访问主机名 |
| .reqHttpHost | string | 前端访问地址httpHost |
| .reqHttpUserAgent | string | userAgent |
| .reqBackendUrl | string | 后端访问地址 |
| .reqBackendHost | string | 后端访问主机名 |
| .reqRefer | string | Referer |
| .reqXff | string | XFF |
| .reqQuery | string | 请求参数 |
| .reqMethod | string | 请求方法 |
| .reqBody | string | 请求数据 |
| .reqHeader | string | 请求头部 |
| .reqUri | string | 请求uri |
| .reqContentType | string | 请求体类型 |
| .reqSchema | string | WEB协议 |
| .resRedirectUri | string | 上游服务器302回跳地址 |
| .resServer | string | 响应服务器 |
| .resStatusCode | number | 响应状态码 |
| .resContentType | string | 响应Content-Type |
| .resContentLength | number | 响应报文长度 |
| .resContentDisposition | string | 下载文件名称 |
| .resBody | string | 响应体 |
| .resHeader | string | 响应头部 |

**JSON格式**

"network": {

"protocol": "https",

"recvBytes": 567,

"sendBytes": 123,

"responseTime": 10,

"app": {

"id": "29a8ad31-de9d-462a-abfd-383035ea4fd8",

"type": "webapp",

"name": "邮箱应用",

"groupId": "default",

"groupName": "默认分类"

},

"conn": {

"dstHost": "1.1.1.1",

"dstIp": "1.1.1.1",

"dstPort": 80,

"srcIp": "1.1.1.1",

"srcPort": 42449

},

"debug": {

"connId": "EE57617F87A220FECE7F4B38AAEAF88F-981145",

"authTime": 100,

"upstreamResolveTime": 100,

"upstreamConnectTime": 100,

"upstreamHeaderTime": 100,

"upstreamResponseTime": 100

},

"web": {

"reqUrl": "https://sdp.com",

"reqHost": "sdp.com",

"reqHttpHost": "sdp.com",

"reqHttpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.0.0 Safari/537.36",

"reqBackendUrl": "https://sdp-backend.com",

"reqBackendHost": "1.1.1.1",

"reqRefer": "https://sdp.com",

"reqXff": "1.1.1.1",

"reqQuery": "name=1&type=1",

"reqMethod": "GET",

"reqBody": "\\\"{\\\\\\\"name\\\\\\\":\\\\\\\"app1\\\\\\\",\\\\\\\"attr\\\\\\\":\\\\\\\"type1\\\\\\\"}\\\"",

"reqHeader": "\"{\\\"accept\\\":\\\"application/json, text/javascript, \*/\*; q=0.01\\\",\\\"accept-encoding\\\":\\\"gzip, deflate, br\\\"}\"",

"reqUri": "/rest/quickreload/latest/381994897",

"reqContentType": "application/x-www-form-urlencoded; charset=utf-8",

"reqSchema": "https",

"resRedirectUri": "",

"resServer": "",

"resStatusCode": 200,

"resContentType": "text/html",

"resContentLength": 500,

"resContentDisposition": "",

"resBody": "\"{\\\"name\\\":\\\"app1\\\",\\\"attr\\\":\\\"type1\\\"}\"",

"resHeader": "{\\\"cache-control\\\":\\\"private, no-cache\\\",\\\"content-length\\\":\\\"101\\\"}"

}

}

**2.2.7 设备（vendor）**

设备信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| sourceName | string | 客户名称，取自授权客户名称 |
| product | string | 产品名称，可选值：aTrust、VPN |
| productVersion | string | 产品版本号 |
| productType | string | 产品类型，可选值：hybrid（综合网关）、sdp（控制中心）、proxy（代理网关） |
| dvcId | string | 设备ID |
| dvcIp | string | 设备IP |

**JSON格式**

"vendor": {

"sourceName": "",

"product": "aTrust",

"productVersion": "2.3.6",

"productType": "hybrid",

"dvcId": "ABCDEF",

"dvcIp": "1.1.1.1"

}

**2.2.8 是否安全日志（\_isRisk）**

可选值：0（否），1（是）

**2.2.9 TraceID（traceId）**

请求接口跟踪码

**2.2.10 日志对账ID（\_logId）**

rsyslog自动生成的自增ID，用于排查是否丢失日志

**2.3 日志类型**

**2.3.1 应用访问日志**

此类事件的主类型（mainType）为app，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.authfreewebapp.access | 免认证web应用访问 |  |
| user.l3app.access | 隧道应用访问 |  |
| user.l3app.access\_decoy | 隧道应用诱饵访问 |  |
| user.l3app.conn\_decoy\_establish | 短隧道应用诱饵连接建立 |  |
| user.l3app.conn\_establish | 短隧道应用连接建立 |  |
| user.webapp.access | web应用访问 |  |
| user.webapp.redirecting | 应用访问重定向 |  |

**2.3.2 蜜罐访问日志**

此类事件的主类型（mainType）为app，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.honeypot.access | 访问蜜罐 | √ |

**2.3.3 虚拟IP申请/释放**

此类事件的主类型（mainType）为vip，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.apply\_private\_vip | 申请IPv4虚拟IP(独享) |  |
| user.apply\_private\_vipv6 | 申请IPv6虚拟IP(独享) |  |
| user.apply\_virtual\_ip | 申请IPv4虚拟IP(共享) |  |
| user.apply\_virtual\_ipv6 | 申请IPv6虚拟IP(共享) |  |
| user.revoke\_all\_private\_vip | 释放所有独享虚拟IP |  |
| user.revoke\_private\_vip | 释放IPv4虚拟IP(独享) |  |
| user.revoke\_private\_vipv6 | 释放IPv6虚拟IP(独享) |  |
| user.revoke\_virtual\_ip | 释放IPv4虚拟IP(共享) |  |
| user.revoke\_virtual\_ipv6 | 释放IPv6虚拟IP(共享) |  |

**2.3.4 SPA**

此类事件的主类型（mainType）为spa，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.spa.tcp | TCP SPA敲门 |  |
| user.spa.tcp.compat\_check | TCP SPA安全码兼容性检查 |  |
| user.spa.tcp.exhaustive\_attack | TCP SPA爆破攻击 | √ |
| user.spa.tcp.format\_check\_failed | TCP SPA格式检查 |  |
| user.spa.tcp.inconsistent\_system\_time | TCP SPA终端时间同步检查 |  |
| user.spa.tcp.passpord\_failed | TCP SPA口令检查 |  |
| user.spa.tcp.seed\_expire | TCP SPA安全码有效期检查 |  |
| user.spa.tcp.seed\_not\_exist | TCP SPA安全码不存在 |  |
| user.spa.tcp.tmp\_seed\_expired | TCP SPA激活码有效期检查 |  |
| user.spa.tcp.tmp\_seed\_not\_exist | TCP SPA激活码不存在 |  |
| user.spa.tcp.tmp\_seed\_revoked | TCP SPA激活码有效性检查 |  |
| user.spa.udp | UDP SPA敲门 |  |
| user.spa.udp.compat\_check | UDP SPA安全码兼容性检查 |  |
| user.spa.udp.exhaustive\_attack | UDP SPA爆破攻击 | √ |
| user.spa.udp.forgery\_attack | UDP SPA敲门伪造 | √ |
| user.spa.udp.inconsistent\_system\_time | UDP SPA终端时间同步检查 |  |
| user.spa.udp.replay\_attack | UDP SPA重放攻击 | √ |
| user.spa.udp.seed\_expire | UDP SPA安全码有效期检查 |  |
| user.spa.udp.seed\_not\_exist | UDP SPA安全码不存在 |  |
| user.spa.udp.sniffers\_attack | SPA Fuzz攻击 | √ |
| user.spa.udp.tmp\_seed\_expired | UDP SPA激活码有效期检查 |  |
| user.spa.udp.tmp\_seed\_not\_exist | UDP SPA激活码不存在 |  |
| user.spa.udp.tmp\_seed\_revoked | UDP SPA激活码有效性检查 |  |

**2.3.5 其他**

其余未归类事件的子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| user.browser\_app\_type\_abnormal | 浏览器访问应用类型异常 | √ |
| user.browser\_ua\_abnormal | 浏览器访问UA信息异常 | √ |
| user.new\_process\_app\_type\_abnormal | 孤立进程访问应用类型异常 | √ |
| user.port.scan | 全端口侦察 | √ |
| user.sensitive.port.scan | 知名端口侦察 | √ |
| user.sensitive.web.path.scan | 敏感目录侦察 | √ |
| user.web.path.scan | 全目录侦察 | √ |
| user.web\_credential\_steal | 会话劫持 | √ |

**3.管理员日志**

**3.1 示例**

管理员日志的programname包含：@adminAuditLog

完整报文示例如下：

<158>Aug 14 10:55:01 localhost sdp-console@adminAuditLog[116]: { "actor": { "id": "1", "type": "admin", "name": "admin", "displayName": "", "groupPath": "\/", "sTraceId": "7cb5da2d-861f-403a-ba3a-ec1155709973", "tags": [ ], "details": "" }, "src": { "dvc": { "os": "Windows 10" }, "geo": { "tags": [ ], "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" }, "client": { "type": "SDPBrowserClient", "browser": "Chrome\/115.0.0.0", "browserVersion": "", "httpUserAgent": "Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/115.0.0.0 Safari\/537.36" }, "preProxyIp": "", "ip": "1.1.1.1", "ipTags": [ ] }, "event": { "id": "f6144380-3a4d-11ee-8e1b-afac54098405", "mainType": "admin", "subType": "user.logout", "timestamp": 1691981701048, "result": "SUCCESS", "reason": "user.logout\_by\_self" }, "\_isRisk": 0, "target": { "id": "1", "type": "admin", "name": "admin", "details": "admin: [empty] -> [empty]" }, "traceId": "01520bbd044c2037", "\_logId": "4407", "vendor": { "product": "aTrust", "productType": "hybrid", "productVersion": "2.3.10", "dvcId": "A14C0E10", "sourceName": "A14C0E10", "dvcIp": "1.1.1.1" } }

Copy

其中正文为：

{

"actor": {

"id": "1",

"type": "admin",

"name": "admin",

"displayName": "",

"groupPath": "/",

"sTraceId": "7cb5da2d-861f-403a-ba3a-ec1155709973",

"tags": [],

"details": ""

},

"src": {

"dvc": {

"os": "Windows 10"

},

"geo": {

"tags": [],

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

},

"client": {

"type": "SDPBrowserClient",

"browser": "Chrome/115.0.0.0",

"browserVersion": "",

"httpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"

},

"preProxyIp": "",

"ip": "1.1.1.1",

"ipTags": []

},

"event": {

"id": "f6144380-3a4d-11ee-8e1b-afac54098405",

"mainType": "admin",

"subType": "user.logout",

"timestamp": 1691981701048,

"result": "SUCCESS",

"reason": "user.logout\_by\_self"

},

"\_isRisk": 0,

"target": {

"id": "1",

"type": "admin",

"name": "admin",

"details": "admin: [empty] -> [empty]"

},

"traceId": "01520bbd044c2037",

"\_logId": "4407",

"vendor": {

"product": "aTrust",

"productType": "hybrid",

"productVersion": "2.3.10",

"dvcId": "A14C0E10",

"sourceName": "A14C0E10",

"dvcIp": "1.1.1.1"

}

}

**3.2字段说明**

**3.2.1 主体（actor）**

主体信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 管理员用户ID，为UUID |
| type | string | 用户类型，可选值：user（用户）、admin（管理员） |
| name | string | 用户名 |
| groupPath | string | 所属管理组 |
| details | string | 用户详情，可空，一般为JSON |
| sTraceId | string | 会话ID，用于跟踪用户会话，这里不是真正起作用的会话ID |

**JSON格式**

"actor": {

"id": "2616cbd2-d4d8-47f7-93cd-44d4b5a09e35",

"type": "user",

"name": "zhangsan",

"groupPath": "/",

"details": "",

"sTraceId": "6d7b6a7f-364b-4fbe-bae1-4329553a5e05"

}

**3.2.2 源（src）**

来源信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| dvc |  | 设备，设备信息 |
| .os | string | 操作系统 |
| geo |  | 地理信息，实时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| client |  | 客户端信息 |
| .type | string | 客户端类型，可选值：SDPBrowserClient（浏览器客户端）、SDPClient（客户端）、SDKClient（SDK）、SangforIdClient（移动端）、MobileClient（移动端） |
| .httpUserAgent | string | userAgent |
| .browser | string | 浏览器 |
| preProxyIp | string | 代理IP |
| ip | string | 客户端源IP |
| ipTags | []string | IP分析 |

**JSON格式**

"src": {

"dvc": {

"os": "Windows"

},

"geo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南"

},

"client": {

"type": "",

"httpUserAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/118.0.0.0 Safari/537.36",

"browser": "Chrome/118.0.0.0"

},

"preProxyIp": "1.1.1.1",

"ip": "1.1.1.1",

"ipTags": []

}

**3.2.3 事件（event）**

事件信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 日志ID，日志唯一ID |
| mainType | string | 操作类型 |
| subType | string | 操作子类型 |
| timestamp | number | 时间，13位时间戳（无时区概念），精确到毫秒 |
| result | string | 结果，可选值：SUCCESS（成功）、FAILED（失败）、-（无） |
| reason | string | 原因 |
| action | string | 处置动作，可选值：DENY（已拦截）、ALLOW（已通过）、-（无） |
| \_vSchema | string | schema，用于动态控制控制台展示某些字段，可选值：management（显示target字段）、apiGuard（显示api字段）、risk（显示security字段）、acl（显示acl字段）、proxy（显示target、network字段） |
| details | string | 日志描述，可空，一般为JSON，为日志的附加信息 |

**JSON格式**

"event": {

"id": "67f48a04-7961-44af-a693-1833decff4f0",

"mainType": "user",

"subType": "user.login",

"timestamp": 1689606221501,

"result": "SUCCESS",

"reason": "",

"action": "",

"\_vSchema": "",

"details": ""

}

**3.2.4 客体（target）**

客体信息，即管理员操作对象的信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 客体ID |
| type | string | 操作对象 |
| name | string | 操作内容 |
| details | string | 操作详情，可空，一般为JSON，为客体的附加信息 |

**JSON格式**

"target": {

"id": "54bad20a-488d-4923-84d5-cec6834799cf",

"type": "local\_user",

"name": "张三",

"details": ""

}

**3.2.5 设备（vendor）**

设备信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| sourceName | string | 客户名称，取自授权客户名称 |
| product | string | 产品名称，可选值：aTrust、VPN |
| productVersion | string | 产品版本号 |
| productType | string | 产品类型，可选值：hybrid（综合网关）、sdp（控制中心）、proxy（代理网关） |
| dvcId | string | 设备ID |
| dvcIp | string | 设备IP |

**JSON格式**

"vendor": {

"sourceName": "",

"product": "aTrust",

"productVersion": "2.3.6",

"productType": "hybrid",

"dvcId": "ABCDEF",

"dvcIp": "1.1.1.1"

}

**3.2.6 是否安全日志（\_isRisk）**

可选值：0（否），1（是）

**3.2.7 TraceID（traceId）**

请求接口跟踪码

**3.2.8 日志对账ID（\_logId）**

rsyslog自动生成的自增ID，用于排查是否丢失日志

**3.3日志类型**

**3.3.1 管理员登录**

此类事件的主类型（mainType）为login，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user.login | 登录 |

**3.3.2 管理员认证**

此类事件的主类型（mainType）为auth/auth\_primary/auth\_secondary，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user.access\_check.auth | 准入认证 |
| user.auth\_check.auth | 管理员认证策略匹配 |
| user.cert.auth | 证书认证 |
| user.https\_sms.auth | 短信认证 |
| user.local\_psw.auth | 本地密码认证 |
| user.modify\_pwd.auth | 强制修改密码 |
| user.modify\_pwd\_and\_ssh.auth | 强制修改账号密码及SSH密码 |
| user.secondaryCert.auth | 证书二次认证 |
| user.send\_sms | 发送短信 |
| user.skip\_modify\_pwd.auth | 跳过强制修改密码 |
| user.skip\_second\_auth | 免辅认证 |
| user.test\_device.auth | 测试设备认证 |

**3.3.3 管理员爆破锁定**

此类事件的主类型（mainType）为auth，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| ip.primary\_bruteforce\_locked | 首次认证爆破锁定IP |
| ip.secondary\_bruteforce\_locked | 二次认证爆破锁定IP |

**3.3.4 管理员注销**

此类事件的主类型（mainType）为admin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user.logout | 注销 |

**3.3.5 管理员注销在线用户**

此类事件的主类型（mainType）为admin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin.logout\_online\_user | 管理员强制注销在线用户 |

**3.3.6 管理员角色**

此类事件的主类型（mainType）为admin\_role，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin.admin\_role.edit | 编辑管理员账户的管理员角色 |

**3.3.7 管理员账号**

此类事件的主类型（mainType）为admin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin.get\_config | 管理员查看加密的敏感信息 |
| admin.lifecycle.activate | 启用管理员账户 |
| admin.lifecycle.create | 创建管理员账户 |
| admin.lifecycle.delete | 删除管理员账户 |
| admin.lifecycle.edit | 编辑管理员账户 |
| admin.lifecycle.forbidden | 禁用管理员账户 |
| admin.lifecycle.reset | 重置管理员账户 |
| admin.password.edit | 编辑管理员账户的密码 |
| admin.password.resetssh | 重置管理员SSH密码 |
| admin.password\_and\_ssh.edit | 编辑管理员账户及SSH的密码 |

**3.3.8 管理员认证服务器**

此类事件的主类型（mainType）为admin\_auth\_plugin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin\_auth\_plugin.config.edit | 编辑管理员认证服务器配置 |
| admin\_auth\_plugin.https.test | 发送http(s)测试请求 |
| admin\_auth\_plugin.https.token.test | 发送HTTP(S)令牌测试请求 |
| admin\_auth\_plugin.lifecycle.activate | 启用管理员认证服务器 |
| admin\_auth\_plugin.lifecycle.create | 创建管理员认证服务器 |
| admin\_auth\_plugin.lifecycle.delete | 删除管理员认证服务器 |
| admin\_auth\_plugin.lifecycle.edit | 编辑管理员认证服务器 |
| admin\_auth\_plugin.lifecycle.forbidden | 禁用管理员认证服务器 |

**3.3.9 管理员认证策略**

此类事件的主类型（mainType）为admin\_auth\_compose，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin\_auth\_compose.lifecycle.create | 创建管理员认证策略 |
| admin\_auth\_compose.lifecycle.delete | 删除管理员认证策略 |
| admin\_auth\_compose.lifecycle.edit | 编辑管理员认证策略 |
| admin\_auth\_compose.lifecycle.reset | 重置超级管理员认证策略 |
| admin\_auth\_compose.user\_membership.edit | 编辑管理员认证策略适用对象 |

**3.3.10 用户目录**

此类事件的主类型（mainType）为user\_directory，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user\_directory.band.import | 导入用户目录的角色 |
| user\_directory.cleanDeleted.edit | 编辑用户目录自动清理配置 |
| user\_directory.config.edit | 编辑用户目录配置 |
| user\_directory.entity.import | 导入用户目录的用户和组 |
| user\_directory.lifecycle.create | 创建用户目录 |
| user\_directory.lifecycle.delete | 删除用户目录 |
| user\_directory.lifecycle.edit | 编辑用户目录 |
| user\_directory.lifecycle.sync | 创建用户同步任务成功 |
| user\_directory.name.edit | 编辑用户目录名 |
| user\_directory.pagesize.edit | 编辑用户目录同步分页大小 |
| user\_directory.resource\_group\_membership.edit | 编辑用户目录关联授权应用分类 |
| user\_directory.resource\_membership.edit | 编辑用户目录关联授权应用 |
| user\_directory.synctime.edit | 编辑用户目录同步周期 |

**3.3.11 本地组织架构**

此类事件的主类型（mainType）为local\_user\_group，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| local\_user\_group.auth\_compose.edit | 编辑本地组织架构的认证策略 |
| local\_user\_group.band.edit | 编辑本地组织架构关联的角色 |
| local\_user\_group.lifecycle.create | 创建本地组织架构 |
| local\_user\_group.lifecycle.delete | 删除本地组织架构 |
| local\_user\_group.lifecycle.edit | 编辑本地组织架构 |
| local\_user\_group.resource\_group\_membership.edit | 编辑本地组织架构关联的应用分类 |
| local\_user\_group.resource\_membership.edit | 编辑本地组织架构关联的应用 |
| local\_user\_group.user\_policy.edit | 编辑本地组织架构的用户策略 |
| user\_attr\_import.group | 批量导入组织架构 |
| user\_attr\_upload.group | 上传待导入组织架构文件 |

**3.3.12 本地用户角色**

在2.2.4之前这里的本地用户角色名字叫本地用户群组。此类事件的主类型（mainType）为local\_user\_band，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| local\_user\_band.group\_membership.edit | 编辑角色关联的组织架构 |
| local\_user\_band.lifecycle.create | 创建角色 |
| local\_user\_band.lifecycle.delete | 删除角色 |
| local\_user\_band.lifecycle.edit | 编辑角色 |
| local\_user\_band.resource\_group\_membership.edit | 编辑角色关联的资源组 |
| local\_user\_band.resource\_membership.edit | 编辑角色关联的资源 |
| local\_user\_band.user\_membership.delete | 移除角色关联的用户 |
| local\_user\_band.user\_membership.edit | 编辑角色关联的用户 |

**3.3.13 本地用户**

此类事件的主类型（mainType）为local\_user，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| local\_user.auth\_compose.edit | 编辑本地用户的认证策略 |
| local\_user.band\_membership.edit | 编辑本地用户关联的角色 |
| local\_user.description.edit | 编辑本地用户的描述 |
| local\_user.display\_name.edit | 编辑本地用户的显示名 |
| local\_user.email.edit | 编辑本地用户的电子邮箱 |
| local\_user.expired\_time.edit | 编辑本地用户的过期时间 |
| local\_user.export | 导出本地用户 |
| local\_user.inherit\_band.edit | 编辑角色继承 |
| local\_user.inherit\_group.edit | 编辑本地用户组织架构授权设置 |
| local\_user.lifecycle.activate | 启用本地用户 |
| local\_user.lifecycle.create | 创建本地用户 |
| local\_user.lifecycle.createbyImport | 批量导入本地用户 |
| local\_user.lifecycle.delete | 删除本地用户 |
| local\_user.lifecycle.edit | 编辑本地用户 |
| local\_user.lifecycle.forbidden | 禁用本地用户 |
| local\_user.lifecycle.uploadUserFile | 上传批量导入本地用户的文件 |
| local\_user.local\_user\_group.edit | 编辑本地用户的所属组织架构 |
| local\_user.password.edit | 编辑本地用户的密码 |
| local\_user.phone.edit | 编辑本地用户的手机号码 |
| local\_user.resource\_group\_membership.edit | 编辑本地用户关联的应用分类 |
| local\_user.resource\_membership.edit | 编辑本地用户关联的应用 |
| local\_user.role\_membership.edit | 编辑本地用户关联的应用集 |
| local\_user.user\_policy.edit | 编辑本地用户的用户策略 |

**3.3.14 外部用户组织架构**

此类事件的主类型（mainType）为external\_user\_group，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| external\_user\_group.auth\_compose.edit | 编辑外部组织架构的认证策略 |
| external\_user\_group.band.edit | 编辑外部组织架构关联的角色 |
| external\_user\_group.inherit\_group.edit | 编辑外部用户组织架构授权设置 |
| external\_user\_group.lifecycle.create | 创建外部组织架构 |
| external\_user\_group.lifecycle.delete | 删除外部组织架构 |
| external\_user\_group.lifecycle.edit | 编辑外部组织架构 |
| external\_user\_group.lifecycle.recursiveDelete | 递归删除外部组织架构 |
| external\_user\_group.resource\_group\_membership.edit | 编辑外部组织架构关联的应用分类 |
| external\_user\_group.resource\_membership.edit | 编辑外部组织架构关联的应用 |
| external\_user\_group.user\_policy.edit | 编辑外部组织架构的用户策略 |

**3.3.15 外部用户角色**

此类事件的主类型（mainType）为external\_user\_band，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| external\_user\_band.group\_membership.edit | 编辑角色关联的组织架构 |
| external\_user\_band.lifecycle.create | 创建角色 |
| external\_user\_band.lifecycle.delete | 删除角色 |
| external\_user\_band.lifecycle.edit | 编辑角色 |
| external\_user\_band.resource\_group\_membership.edit | 编辑角色关联的资源组 |
| external\_user\_band.resource\_membership.edit | 编辑角色关联的资源 |
| external\_user\_band.user\_membership.delete | 移除角色关联的用户 |
| external\_user\_band.user\_membership.edit | 编辑角色关联的用户 |

**3.3.16 外部用户**

此类事件的主类型（mainType）为external\_user，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| external\_user.auth\_compose.edit | 编辑外部用户的认证策略 |
| external\_user.band\_membership.edit | 编辑外部用户关联的角色 |
| external\_user.description.edit | 编辑外部用户的描述 |
| external\_user.display\_name.edit | 编辑外部用户显示名 |
| external\_user.email.edit | 编辑外部用户的电子邮箱 |
| external\_user.expired\_time.edit | 编辑外部用户的过期时间 |
| external\_user.export | 导出外部用户 |
| external\_user.external\_id.edit | 编辑外部用户外部ID |
| external\_user.external\_user\_group.edit | 编辑外部用户的所属组织架构 |
| external\_user.inherit\_band.edit | 编辑角色继承 |
| external\_user.inherit\_group.edit | 编辑外部用户组织架构授权设置 |
| external\_user.lifecycle.activate | 启用外部用户 |
| external\_user.lifecycle.create | 创建外部用户 |
| external\_user.lifecycle.createbyImport | 批量导入外部用户 |
| external\_user.lifecycle.delete | 删除外部用户 |
| external\_user.lifecycle.edit | 编辑外部用户 |
| external\_user.lifecycle.forbidden | 禁用外部用户 |
| external\_user.phone.edit | 编辑外部用户的手机号码 |
| external\_user.resource\_group\_membership.edit | 编辑外部用户关联的应用分类 |
| external\_user.resource\_membership.edit | 编辑外部用户关联的应用 |
| external\_user.role\_membership.edit | 编辑外部用户关联的应用集 |
| external\_user.user\_policy.edit | 编辑外部用户的用户策略 |

**3.3.17 认证服务器**

此类事件的主类型（mainType）为auth\_plugin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| auth\_plugin.config.edit | 编辑认证服务器的配置 |
| auth\_plugin.create\_trusted\_domain\_file.edit | 创建可信域名校验文件 |
| auth\_plugin.lifecycle.activate | 启用认证服务器 |
| auth\_plugin.lifecycle.create | 创建认证服务器 |
| auth\_plugin.lifecycle.delete | 删除认证服务器 |
| auth\_plugin.lifecycle.edit | 编辑认证服务器 |
| auth\_plugin.lifecycle.forbidden | 禁用认证服务器 |
| auth\_plugin.lifecycle.sort | 更新认证服务器排序 |
| auth\_plugin.resource\_group\_membership.edit | 编辑认证服务器关联应用分类 |
| auth\_plugin.resource\_membership.edit | 编辑认证服务器关联的应用 |
| auth\_plugin.user\_config.edit | 编辑认证服务器用户配置 |
| auth\_plugin\_template.config.edit | 编辑https认证服务器模板配置 |
| auth\_plugin\_template.info.edit | 编辑https认证服务器模板信息 |
| auth\_plugin\_template.lifecycle.create | 创建https认证服务器模板 |
| auth\_plugin\_template.lifecycle.delete | 删除https认证服务器模板 |
| auth\_plugin\_template.lifecycle.edit | 编辑https认证服务器模板 |

**3.3.18 认证策略**

此类事件的主类型（mainType）为auth\_compose，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| auth\_compose.lifecycle.create | 创建认证策略 |
| auth\_compose.lifecycle.delete | 删除认证策略 |
| auth\_compose.lifecycle.edit | 编辑认证策略 |
| auth\_compose.user\_membership.edit | 编辑认证策略适用对象 |

**3.3.19 应用分类**

此类事件的主类型（mainType）为resource\_group，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| resource\_group.grant.append | 追加应用分类授权 |
| resource\_group.grant.delete | 移除应用分类授权 |
| resource\_group.grant.reset | 应用分类授权 |
| resource\_group.lifecycle.create | 创建应用分类 |
| resource\_group.lifecycle.delete | 删除应用分类 |
| resource\_group.lifecycle.edit | 编辑应用分类 |
| resource\_group.lifecycle.sort | 排序应用分类 |

**3.3.20 应用**

此类事件的主类型（mainType）为resource，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| app\_icon.upload | 上传应用图标 |
| depend\_site\_record.edit | 编辑依赖站点采集工具配置 |
| resource.grant.append | 追加应用授权 |
| resource.grant.delete | 移除应用授权 |
| resource.grant.reset | 应用授权 |
| resource.lifecycle.activate | 启用应用 |
| resource.lifecycle.batchEdit | 批量编辑 |
| resource.lifecycle.create | 创建应用 |
| resource.lifecycle.createbyImport | 批量导入应用 |
| resource.lifecycle.delete | 删除应用 |
| resource.lifecycle.delete\_template | 删除应用授权告警模板 |
| resource.lifecycle.edit | 编辑应用 |
| resource.lifecycle.export | 导出应用 |
| resource.lifecycle.forbidden | 禁用应用 |
| resource.lifecycle.save\_template | 保存应用授权告警模板 |
| resource.lifecycle.update\_template | 编辑应用授权告警模板 |
| resource.lifecycle.uploadResourceFile | 上传批量导入应用的文件 |
| resource\_access\_address.lifecycle.activate | 启用应用前端地址别名 |
| resource\_access\_address.lifecycle.create | 创建应用前端地址别名 |
| resource\_access\_address.lifecycle.delete | 删除应用前端地址别名 |
| resource\_access\_address.lifecycle.edit | 编辑应用前端地址别名 |
| resource\_access\_address.lifecycle.forbidden | 禁用应用前端地址别名 |
| tp\_resource.lifecycle.activate | 启用免认证应用 |
| tp\_resource.lifecycle.create | 创建免认证应用 |
| tp\_resource.lifecycle.delete | 删除免认证应用 |
| tp\_resource.lifecycle.edit | 编辑免认证应用 |
| tp\_resource.lifecycle.forbidden | 禁用免认证应用 |
| web\_config\_tool\_edit | 编辑应用调试选项配置 |

**3.3.21 授信终端**

此类事件的主类型（mainType）为trust\_device，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| trust\_device.lifecycle.batchDelete | 批量解绑授信终端 |
| trust\_device.lifecycle.create | 绑定授信终端 |
| trust\_device.lifecycle.delete | 解绑授信终端 |
| trust\_device.lifecycle.edit | 定义授信终端 |
| trust\_device\_approval.agree | 通过授信终端申请 |
| trust\_device\_approval.batchAgree | 批量通过授信终端申请 |
| trust\_device\_approval.batchReject | 批量驳回授信终端申请 |
| trust\_device\_approval.reject | 驳回授信终端申请 |
| trust\_device\_config.lifecycle.edit | 编辑授信终端配置 |

**3.3.22 终端管理**

此类事件的主类型（mainType）为device/device\_match\_rule\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| device.lifecycle.batchDelete | 批量删除终端 |
| device.lifecycle.batchUpdate | 批量编辑终端 |
| device.lifecycle.create | 新增终端 |
| device.lifecycle.delete | 删除终端 |
| device.lifecycle.export | 导出终端列表 |
| device.lifecycle.import | 导入终端列表 |
| device.lifecycle.setTag | 终端设置标签 |
| device.lifecycle.unsetTag | 终端取消标签 |
| device.lifecycle.update | 编辑终端 |
| device.lifecycle.upload | 上传导入文件 |
| device.superCode.query | 查看超级卸载码 |
| device.superCode.reset | 重置超级卸载码 |
| device.uniqueCode.query | 查看终端卸载码 |
| device\_match\_rule\_config.lifecycle.update | 编辑终端匹配规则 |
| device\_tag.lifecycle.create | 创建标签 |
| device\_tag.lifecycle.delete | 删除标签 |
| device\_tag.lifecycle.update | 更新标签 |
| device\_tag.lifecycle.update\_name | 更新标签名 |

**3.3.23 应用权限**

此类事件的主类型（mainType）为user\_permission\_approval，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user\_permission\_approval.lifecycle.edit | 编辑应用权限审批 |

**3.3.24 应用集**

此类事件的主类型（mainType）为role，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| role.lifecycle.create | 创建应用集 |
| role.lifecycle.delete | 删除应用集 |
| role.lifecycle.edit | 编辑应用集 |
| role.resource\_group\_membership.edit | 编辑应用集关联的应用分类 |
| role.resource\_membership.edit | 编辑应用集关联的应用 |

**3.3.25 权限基线**

此类事件的主类型（mainType）为baseline\_permission\_resource，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| baseline\_permission\_resource.access\_permission.auth | 授予权限基线应用的访问权限 |
| baseline\_permission\_resource.access\_permission.ignore | 忽略权限基线应用的访问权限 |
| baseline\_permission\_resource.access\_permission.reject | 拒绝权限基线应用的访问权限 |
| baseline\_permission\_resource.access\_permission.unauth | 取消权限基线应用的访问权限 |
| baseline\_permission\_resource.access\_permission.unignore | 取消忽略权限基线应用的访问权限 |
| baseline\_permission\_resource.access\_permission.unreject | 取消拒绝权限基线应用的访问权限 |
| baseline\_permission\_resource.lifecycle.add | 添加权限基线应用 |
| baseline\_permission\_resource.state.edit | 编辑权限基线应用状态 |

**3.3.26 全局策略**

此类事件的主类型（mainType）为global\_strategy，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| global\_strategy.access\_restriction.edit | 编辑全局策略接入限制选项 |
| global\_strategy.client\_config.edit | 编辑全局策略客户端选项 |
| global\_strategy.client\_download\_rate\_limit.edit | 编辑全局策略客户端下载限流限速 |
| global\_strategy.cookie\_hijacking.edit | 编辑全局策略会话劫持配置 |
| global\_strategy.edit | 编辑全局策略 |
| global\_strategy.enable\_client\_force\_update.edit | 编辑全局策略强制升级至最新版本客户端 |
| global\_strategy.login\_config.edit | 编辑全局策略登录安全配置 |
| global\_strategy.psw.edit | 编辑全局策略密码安全配置 |
| global\_strategy.skip\_app\_center.edit | 编辑全局策略登录成功后最小化客户端配置 |
| global\_strategy.sslvpn\_config.edit | 编辑全局策略深信服 VPN 客户端升级配置 |
| global\_strategy.uncommon\_location\_limit.edit | 设置非常用地点判断条件 |
| global\_strategy.web\_diagnosis\_config.edit | 编辑全局策略WEB诊断工具配置 |

**3.3.27 应用防护策略**

此类事件的主类型（mainType）为auth\_app\_acl，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| auth\_app\_acl.lifecycle.create | 创建应用防护策略 |
| auth\_app\_acl.lifecycle.delete | 删除应用防护策略 |
| auth\_app\_acl.lifecycle.edit | 编辑应用防护策略 |
| auth\_app\_acl.resource\_group\_membership.edit | 编辑应用防护策略关联的应用分类 |
| auth\_app\_acl.resource\_membership.edit | 编辑应用防护策略关联的应用 |
| auth\_app\_acl.user\_membership.edit | 编辑应用防护策略关联的用户 |

**3.3.28 上线准入策略**

此类事件的主类型（mainType）为pre\_login\_acl，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| pre\_login\_acl.lifecycle.create | 创建上线准入策略 |
| pre\_login\_acl.lifecycle.delete | 删除上线准入策略 |
| pre\_login\_acl.lifecycle.edit | 编辑上线准入策略 |
| pre\_login\_acl.user\_membership.edit | 编辑上线准入策略关联的用户 |

**3.3.29 安全策略**

此类事件的主类型（mainType）为security\_policy，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| security\_policy.lifecycle.create | 创建安全策略 |
| security\_policy.lifecycle.delete | 删除安全策略 |
| security\_policy.lifecycle.edit | 编辑安全策略 |
| security\_policy.resource\_membership.edit | 编辑安全策略关联的应用 |
| security\_policy.user\_membership.edit | 编辑安全策略关联的用户 |
| security\_policy\_ext\_cond.lifecycle.create | 创建安全基线扩展条件 |
| security\_policy\_ext\_cond.lifecycle.delete | 删除安全基线扩展条件 |
| security\_policy\_ext\_cond.lifecycle.edit | 编辑安全基线扩展条件 |

**3.3.30 网路区域**

此类事件的主类型（mainType）为net\_zone，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| net\_zone.lifecycle.create | 创建网络区域扩展条件 |
| net\_zone.lifecycle.delete | 删除网络区域扩展条件 |
| net\_zone.lifecycle.edit | 编辑网络区域扩展条件 |

**3.3.31 第三方设备**

此类事件的主类型（mainType）为third\_device，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| third\_device.lifecycle.activate | 启用第三方设备 |
| third\_device.lifecycle.create | 创建第三方设备 |
| third\_device.lifecycle.delete | 删除第三方设备 |
| third\_device.lifecycle.edit | 编辑第三方设备 |
| third\_device.lifecycle.forbidden | 禁用第三方设备 |
| third\_device.third\_device\_key\_membership.edit | 编辑第三方设备关联的第三方设备自定义key |
| third\_device\_key.lifecycle.create | 创建第三方设备自定义key |
| third\_device\_key.lifecycle.delete | 删除第三方设备自定义key |
| third\_device\_key.lifecycle.edit | 编辑第三方设备自定义key |

**3.3.32 可信应用**

此类事件的主类型（mainType）为trust\_app/not\_trust\_app，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| application.lifecycle.create | 创建可信进程 |
| application.lifecycle.delete | 删除可信进程 |
| application.lifecycle.edit | 编辑可信进程 |
| application.lifecycle.update\_status | 切换开关状态 |
| application.process\_rule\_membership.edit | 编辑可信进程关联的可信进程匹配规则 |
| not\_trust\_app.lifecycle.create | 创建不可信进程 |
| not\_trust\_app.lifecycle.delete | 删除不可信进程 |
| not\_trust\_app.lifecycle.edit | 编辑不可信进程 |
| not\_trust\_app.process\_rule\_membership.edit | 编辑不可信进程关联的不可信进程匹配规则 |
| process.hack\_tool.edit | 编辑攻击工具 |
| process.hack\_tool.rollback | 回滚攻击工具 |
| process.lifecycle.not\_trust | 不信任进程 |
| process.lifecycle.trust | 信任进程 |
| trust\_app.lifecycle.create | 创建可信进程 |
| trust\_app.lifecycle.delete | 删除可信进程 |
| trust\_app.lifecycle.edit | 编辑可信进程 |
| trust\_app.process\_rule\_membership.edit | 编辑可信进程关联的可信进程匹配规则 |

**3.3.33 NTP时间同步**

此类事件的主类型（mainType）为time\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| time\_config.edit | 编辑日期与时间配置 |
| time\_config.net\_time\_sync.edit | 编辑NTP时间同步配置 |
| time\_config.net\_time\_sync.sync | 立即同步时间 |

**3.3.34 客户端接入设置**

此类事件的主类型（mainType）为client\_access\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| client\_access\_config.cdn\_node\_whitelist.edit | 编辑客户端接入设置的CDN节点白名单 |
| client\_access\_config.cert\_port.edit | 编辑客户端接入设置的证书认证端口设置 |
| client\_access\_config.client\_access\_address.edit | 编辑客户端接入设置的客户端接入地址 |
| client\_access\_config.edit | 编辑客户端接入设置 |
| client\_access\_config.ssl\_tls.edit | 编辑客户端接入设置的SSL/TLS协议设置 |
| client\_access\_config.vnic\_running\_type.edit | 编辑客户端接入设置的网卡常驻状态 |
| client\_access\_config.vnic\_type.edit | 编辑客户端接入设置的虚拟网卡设置 |

**3.3.35 控制台选项**

此类事件的主类型（mainType）为console\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| console\_config.access\_console\_host.edit | 编辑控制台接入地址限制 |
| console\_config.anti\_brute.edit | 编辑控制台选项的防爆破设置 |
| console\_config.cert\_port.edit | 编辑控制台选项的控制台证书认证端口 |
| console\_config.cert\_port\_status.edit | 编辑控制台选项的控制台证书认证端口开关 |
| console\_config.cipher\_method.edit | 编辑控制台选项的加密方式 |
| console\_config.edit | 编辑控制台选项 |
| console\_config.ip\_limit.edit | 编辑接入源ip限制 |
| console\_config.ping.edit\_activate | 启用控制台选项的ping命令连接设备 |
| console\_config.session\_timeout.edit | 编辑控制台选项的会话超时配置 |
| console\_config.ssh.edit | 启用控制台选项的远程维护 |
| console\_config.ssh.edit\_activate | 启用控制台选项的远程维护 |
| console\_config.ssh.edit\_forbidden | 禁用控制台选项的远程维护 |
| console\_config.ssh.edit\_port | 修改控制台选项的远程维护的端口 |

**3.3.36 隐私设置**

此类事件的主类型（mainType）为console\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| privacy\_config.disable | 关闭隐私设置 |
| privacy\_config.enable | 开启隐私设置 |

**3.3.37 系统主题**

此类事件的主类型（mainType）为portal\_theme，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| login\_portal.update\_pri | 更新登录门户 |
| portal\_theme.lifecycle.activate | 启用系统主题 |
| portal\_theme.lifecycle.delete | 删除系统主题 |
| portal\_theme.lifecycle.download | 下载系统主题 |
| portal\_theme.lifecycle.edit | 编辑系统主题 |
| portal\_theme.lifecycle.upload | 上传系统主题 |

**3.3.38 设备证书**

此类事件的主类型（mainType）为device\_cert，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| device\_cert.lifecycle.download | 下载设备证书 |
| device\_cert.lifecycle.generate\_req | 生成设备证书请求 |
| device\_cert.lifecycle.req\_download | 下载设备证书请求 |
| device\_cert.lifecycle.update | 更新设备证书 |
| device\_cert.lifecycle.updateByupload | 通过手动导入更新设备证书 |

**3.3.39 web应用证书**

此类事件的主类型（mainType）为web\_cert，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| web\_cert.lifecycle.delete | 删除web应用证书 |
| web\_cert.lifecycle.update | 更新web应用证书 |
| web\_cert.lifecycle.update\_builtin | 更新内置web应用证书 |
| web\_cert.lifecycle.upload | 上传web应用证书 |

**3.3.40 授权文件**

此类事件的主类型（mainType）为license，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| license.export\_dev\_info | 导出设备信息 |
| license.lifecycle.check | 检查授权文件 |
| license.lifecycle.update | 更新授权文件 |

**3.3.41 CA证书**

此类事件的主类型（mainType）为ca\_cert，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| ca\_cert.lifecycle.create | 创建CA证书 |
| ca\_cert.lifecycle.delete | 删除CA证书 |
| ca\_cert.lifecycle.edit | 编辑CA证书 |

**3.3.42 CA证书吊销列表**

此类事件的主类型（mainType）为ca\_cert\_crl，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| ca\_cert\_crl.lifecycle.create | 上传证书CRL列表 |
| ca\_cert\_crl.lifecycle.delete | 删除证书CRL列表 |

**3.3.43 网络配置**

此类事件的主类型（mainType）为network\_interface/route/host/bond\_interface，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| bond\_interface.lifecycle.create | 新增聚合网口 |
| bond\_interface.lifecycle.delete | 删除聚合网口 |
| bond\_interface.lifecycle.edit | 编辑聚合网口 |
| host.lifecycle.create | 创建HOST |
| host.lifecycle.delete | 删除HOST |
| host.lifecycle.edit | 编辑HOST |
| network\_interface.lifecycle.create | 新增链路IP |
| network\_interface.lifecycle.delete | 删除链路IP |
| network\_interface.lifecycle.edit | 编辑链路IP |
| network\_interface.proxy.create | 新增proxy的链路IP |
| network\_interface.proxy.delete | 删除proxy的链路IP |
| network\_interface.proxy.edit | 编辑proxy的链路IP |
| route.lifecycle.create | 创建路由 |
| route.lifecycle.delete | 删除路由 |
| route.lifecycle.edit | 编辑路由 |
| route.proxy.create | 创建proxy的路由 |
| route.proxy.delete | 删除proxy的路由 |
| route.proxy.edit | 编辑proxy的路由 |

**3.3.44 集群**

此类事件的主类型（mainType）为cluster，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| cluster.lifecycle.add\_node | 增加集群节点 |
| cluster.lifecycle.create | 创建集群 |
| cluster.lifecycle.del\_node | 删除集群节点 |
| cluster.lifecycle.delete | 删除集群节点 |
| cluster.lifecycle.destroy | 拆除集群 |
| cluster.lifecycle.edit | 编辑集群 |
| cluster.node.state\_changed | 集群节点状态切换 |
| cluster.role.changed | 集群角色切换 |
| cluster.role.switch\_to\_master | 切换为主节点 |

**3.3.45 分布式**

此类事件的主类型（mainType）为distributed\_cluster，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| distributed\_cluster.activeunit | 激活分支单元 |
| distributed\_cluster.addunit | 创建分支单元加入分布式集群 |
| distributed\_cluster.create | 创建分布式集群 |
| distributed\_cluster.deleteunit | 移除单元 |
| distributed\_cluster.destroy | 解散分布式集群 |
| distributed\_cluster.setmasterunit | 设置分支单元为中心单元 |
| distributed\_cluster.unitstatechanged | 分布式单元状态切换 |
| distributed\_cluster.updateMultilineBaseConfig | 更新多线路基础配置 |
| distributed\_cluster.updateunit | 更新单元配置 |
| distributed\_secret.query | 查询分布式集群接入密钥 |
| distributed\_secret.update | 更新分布式集群接入密钥 |

**3.3.46 SNMP**

此类事件的主类型（mainType）为snmp\*，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| snmp.edit | 编辑SNMP配置 |
| snmp.sdpc\_sync\_edit | 编辑SNMP的控制中心同步配置 |
| snmp\_mib.download | 下载MIB库 |
| snmp\_trap.activate | 启用SNMP TRAP |
| snmp\_trap.edit | 编辑SNMP trap配置 |
| snmp\_trap.forbidden | 禁用SNMP TRAP |
| snmp\_v1\_v2.activate | 启用SNMP v1/v2 |
| snmp\_v1\_v2.edit | 编辑SNMP v1/v2配置 |
| snmp\_v1\_v2.forbidden | 禁用SNMP v1/v2 |
| snmp\_v3.activate | 启用SNMP v3 |
| snmp\_v3.edit | 编辑SNMP v3配置 |
| snmp\_v3.forbidden | 禁用SNMP v3 |

**.3.47 配置备份**

此类事件的主类型（mainType）为backup\_file/backup\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| backup\_config.edit | 编辑自动备份配置 |
| backup\_config.sdpc\_sync\_edit | 编辑自动备份的控制中心同步配置 |
| backup\_file.lifecycle.backup | 创建备份文件 |
| backup\_file.lifecycle.backup\_start | 开始备份 |
| backup\_file.lifecycle.create | 创建备份文件 |
| backup\_file.lifecycle.delete | 删除备份文件 |
| backup\_file.lifecycle.download | 导出备份文件 |
| backup\_file.lifecycle.import | 导入备份文件恢复配置 |
| backup\_file.lifecycle.import\_start | 开始恢复导入备份文件 |
| backup\_file.lifecycle.mod\_sm1\_to\_sm4 | 转换ipsec加密算法SM1为SM4 |
| backup\_file.lifecycle.reset | 重置配置 |
| backup\_file.lifecycle.restore | 使用备份文件恢复配置 |
| backup\_file.lifecycle.restore\_start | 开始恢复本机备份文件 |

**3.3.48 设备节点**

此类事件的主类型（mainType）为node/node\_group/proxy\_secret，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| node.lifecycle.activate | 启用单机节点 |
| node.lifecycle.delete | 删除单机节点 |
| node.lifecycle.edit | 编辑单机节点信息 |
| node.lifecycle.join | 申请加入控制中心 |
| node.lifecycle.leave | 解除加入控制中心 |
| node\_group.lifecycle.create | 创建区域分组 |
| node\_group.lifecycle.delete | 删除区域分组 |
| node\_group.lifecycle.edit | 编辑区域分组 |
| proxy\_secret.query | 查询proxy接入密钥 |
| proxy\_secret.update | 更新proxy接入密钥 |

**3.3.49 日志**

此类事件的子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| actor\_security\_log.download | 导出用户安全日志 |
| admin\_log.download | 导出管理员日志 |
| client\_log.lifecycle.check\_collect | 终端日志任务定时监测 |
| client\_log.lifecycle.dispatch | 终端日志定时采集 |
| client\_log\_file.collect | 收集终端运维日志 |
| client\_log\_file.delete | 删除终端运维日志 |
| client\_log\_file.download | 下载终端运维日志文件 |
| log.download | 下载日志 |
| log\_config.edit | 编辑日志配置 |
| mock\_log.generate | 生成演示日志 |
| network\_log.download | 导出访问日志 |
| security\_log.download | 导出设备安全日志 |
| syslog.activate | 启用syslog |
| syslog.edit | 编辑syslog配置 |
| syslog.forbidden | 禁用syslog |
| syslog.log\_content.edit | 编辑syslog的日志内容配置 |
| syslog.sdpc\_sync\_edit | 编辑syslog的控制中心同步配置 |
| syslog.server\_config.edit | 编辑syslog的服务器配置 |
| system\_log.download | 导出系统日志 |
| user\_log.download | 导出用户日志 |
| vendor\_security\_log.download | 导出设备安全日志 |

**3.3.50 用户策略**

此类事件的主类型（mainType）为user\_policy，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user\_policy.lifecycle.create | 创建用户策略 |
| user\_policy.lifecycle.delete | 删除用户策略 |
| user\_policy.lifecycle.edit | 编辑用户策略 |
| user\_policy.user\_membership.edit | 编辑用户策略适用对象 |

**3.3.51 webconsole**

此类事件的主类型（mainType）为webconsole，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| webconsole.login | webconsole登录 |
| webconsole\_file.delete | 删除web控制台文件 |
| webconsole\_file.download | 下载web控制台文件 |

**3.3.52 虚拟IP**

此类事件的主类型（mainType）为vip，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| vip.detect | 虚拟IP连通性检测 |
| vip.lifecycle.add | 加入单机节点的虚拟IP池 |
| vip.lifecycle.clear | 清理虚拟IP |
| vip.lifecycle.create | 创建单机节点的虚拟IP池 |
| vip.lifecycle.create\_private | 创建独享虚拟IP绑定 |
| vip.lifecycle.delete | 删除单机节点的虚拟IP池 |
| vip.lifecycle.delete\_private | 删除独享虚拟IP绑定 |
| vip.lifecycle.delete\_temp\_private | 删除待导入的独享虚拟IP绑定 |
| vip.lifecycle.disable | 禁用单机节点的虚拟ip池 |
| vip.lifecycle.disableV6 | 禁用单机节点的虚拟ip池启用IPV6 |
| vip.lifecycle.edit | 编辑单机节点的虚拟IP池 |
| vip.lifecycle.edit\_act\_conn\_alloc\_ip\_type | 编辑虚拟IP分配策略 |
| vip.lifecycle.edit\_private | 编辑独享虚拟IP绑定 |
| vip.lifecycle.edit\_usage\_mode | 编辑虚拟IP使用模式 |
| vip.lifecycle.enable | 启用单机节点的虚拟ip池 |
| vip.lifecycle.enableV6 | 单机节点虚拟ip池启用IPV6 |
| vip.lifecycle.export\_private | 独享虚拟IP绑定关系导出 |
| vip.lifecycle.import\_private | 独享虚拟IP绑定关系导入 |
| vip.lifecycle.session | 启用按终端分配虚拟ip |
| vip.lifecycle.upload\_private | 独享虚拟IP绑定关系上传 |
| vip.lifecycle.user | 启用按用户分配虚拟ip |

**3.3.53 特性中心**

此类事件的主类型（mainType）为feature\_center，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| feature\_center.activate | 特性中心启用 |
| feature\_center.delete | 特性中心删除 |
| feature\_center.forbidden | 特性中心禁用 |
| feature\_center.lifecycle.create | 特性中心创建 |
| feature\_center.lifecycle.update | 特性中心更新 |

**3.3.54 客户端灰度**

此类事件的主类型（mainType）为grayscale\_upgrade，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| grayscale\_upgrade.edit | 编辑客户端灰度升级策略 |

**3.3.55 邮件服务器**

此类事件的主类型（mainType）为mail，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| mail.report.edit | 编辑邮件通知 |
| mail.server.edit | 编辑邮件服务器 |
| mail.server.test\_mail | 发送测试邮件 |
| mail.server\_password.get | 查看邮件服务器用户密码 |

**3.3.56 事件告警**

此类事件的主类型（mainType）为alert，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| alert.event.edit | 编辑告警事件 |
| alert.history.ignored | 设置告警状态为已忽略 |
| alert.mail.edit | 编辑告警通知 |

**3.3.57 系统升级**

此类事件的主类型（mainType）为system\_upgrade，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| linkage\_device.create | 创建联动设备 |
| linkage\_device.delete | 删除联动设备 |
| linkage\_device.lifecycle.activate | 启用联动设备 |
| linkage\_device.lifecycle.forbidden | 禁用联动设备 |
| linkage\_device.update | 更新联动设备 |
| sdp\_updated.auto\_update.finish | 自动升级 |
| sdp\_updated.update.cancel | 取消升级 |
| sdp\_updated.update.finish | 安装升级包 |
| sdp\_updated.update.force\_cancel | 强制取消升级 |
| sdp\_updated.uploadpkg.failed | 上传升级包失败 |
| sdp\_updated.uploadpkg.success | 上传升级包成功 |
| snapshot.delete | 删除快照 |
| sp.rollback | 回滚升级包 |
| sp.update | 安装升级包 |
| system\_upgrade.begin | 开始升级 |
| system\_upgrade.enter\_maintenance | 进入运维模式 |
| system\_upgrade.exit | 取消升级 |
| system\_upgrade\_package.upload | 升级包上传 |
| system\_upgrade\_seettings.edit | 编辑升级设置 |
| upgrade\_config.autoupgrade.disabled | 关闭自动下载并安装补丁包 |
| upgrade\_config.autoupgrade.edit | 编辑自动下载并安装时间 |
| upgrade\_config.autoupgrade.enabled | 开启自动下载并安装补丁包 |
| upgrade\_config.browser.disabled | 关闭浏览器代理访问在线升级平台 |
| upgrade\_config.browser.enabled | 开启浏览器代理访问在线升级平台 |
| upgrade\_config.edit | 修改升级设置 |
| upgrade\_config.emergencycontact.edit | 编辑紧急联系人 |
| upgrade\_config.proxy.disabled | 关闭第三方代理服务器访问在线升级平台 |
| upgrade\_config.proxy.edit | 编辑第三方代理服务器配置 |
| upgrade\_config.proxy.enabled | 开启第三方代理服务器访问在线升级平台 |

**3.3.58 用户帐号解锁**

此类事件的主类型（mainType）为user\_account\_status，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user\_account\_status.batchUnlock | 用户帐号批量解锁 |
| user\_account\_status.unlock | 用户帐号解锁 |

**3.3.59 闲置账号**

此类事件的主类型（mainType）为idle\_account，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| idle\_account\_config.lifecycle.edit\_enable | 编辑闲置账号清理开关 |
| idle\_account\_config.lifecycle.edit\_idle\_time | 编辑允许闲置时长 |
| idle\_account\_config.lifecycle.edit\_proposal | 编辑处置动作 |
| idle\_account\_config.lifecycle.update | 编辑闲置账号配置 |
| idle\_account\_cron\_tab.lifecycle.lock | 定时锁定闲置账号 |
| idle\_account\_list.lifecycle.edit | 编辑闲置账号 |
| idle\_account\_list.lifecycle.edit\_lock | 锁定闲置账号 |
| idle\_account\_list.lifecycle.edit\_unlock | 解锁闲置账号 |

**3.3.60 open API**

此类事件的主类型（mainType）为console\_open\_api\_device，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| console\_open\_api\_device.lifecycle.activate | 启用开放第三方设备 |
| console\_open\_api\_device.lifecycle.create | 创建开放第三方设备 |
| console\_open\_api\_device.lifecycle.delete | 删除开放第三方设备 |
| console\_open\_api\_device.lifecycle.edit | 编辑开放第三方设备 |
| console\_open\_api\_device.lifecycle.forbidden | 禁用开放第三方设备 |
| console\_open\_api\_device.lifecycle.getsec | 查询开放第三方设备的密钥 |
| console\_open\_api\_device.lifecycle.resetsec | 重置开放第三方设备的密钥 |

**3.3.61 设备健康检查**

此类事件的主类型（mainType）为acheck/acheck\_res/health\_check，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| acheck\_res.download | 下载acheck巡检报告 |
| acheck\_secret.disable | 关闭acheck巡检授权 |
| acheck\_secret.enable | 开启acheck巡检授权 |
| acheck\_secret.query | 查看acheck巡检密钥 |
| health\_check.start | 启动设备安全检查 |

**3.3.62 流量镜像**

此类事件的主类型（mainType）为traffic\_mirror，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| traffic\_mirror.disable | 关闭流量镜像 |
| traffic\_mirror.enable | 开启流量镜像 |

**3.3.63 加密卡**

此类事件的主类型（mainType）为crypto\_card，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| crypto\_card.activate | 激活密码卡 |
| crypto\_card.backup\_enc\_key | 备份密码卡密钥 |
| crypto\_card.deactivate | 取消激活密码卡 |
| crypto\_card.modify\_pin | 更改管理Key口令 |
| crypto\_card.recover\_enc\_key | 恢复密码卡密钥 |
| crypto\_card.reset\_ukey | 重置管理Key |
| crypto\_card.self\_check | 进行算法自检 |

**3.3.64 测试设备找回**

此类事件的主类型（mainType）为test\_device，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| user.test\_device.qrcode.get | 获取测试设备认证二维码 |

**3.3.65 GRE隧道**

此类事件的主类型（mainType）为gre\_ip\_tunnel，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| gre\_ip\_tunnel.lifecycle.create | 创建GRE隧道 |
| gre\_ip\_tunnel.lifecycle.delete | 删除GRE隧道 |
| gre\_ip\_tunnel.lifecycle.edit | 编辑GRE隧道 |
| gre\_ip\_tunnel.proxy.create | 创建proxy的GRE隧道 |
| gre\_ip\_tunnel.proxy.delete | 删除proxy的GRE隧道 |
| gre\_ip\_tunnel.proxy.edit | 编辑proxy的GRE隧道 |
| gre\_ip\_tunnel\_secret.lifecycle.query | 查询GRE密钥 |
| gre\_ip\_tunnel\_secret.proxy.query | 查询proxy的GRE密钥 |

**3.3.66 SPA**

此类事件的主类型（mainType）为spa，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| spa.edit | 编辑服务隐身配置 |
| spa.enable\_fakeip.edit | 编辑服务隐身配置的客户端引流设置 |
| spa.ip\_white\_policy.add | 新增SPA白名单策略 |
| spa.ip\_white\_policy.delete | 删除SPA白名单策略 |
| spa.ip\_white\_policy.edit | 编辑SPA白名单策略 |
| spa.seed.expiredtime.reset | 重置用户安全码有效期 |
| spa.seed.query | 查看用户安全码 |
| spa.seed.reset | 重置用户安全码 |
| spa.seed.retry\_send\_task | 重试发送失败的用户安全码 |
| spa.seed.send | 发送用户安全码 |
| spa.seed.send\_result | 更新用户安全码分发进度 |
| spa.sharedseed.expiredtime.reset | 重置共享安全码有效期 |
| spa.sharedseed.query | 查看共享安全码 |
| spa.sharedseed.reset | 重置共享安全码 |
| spa.sharedseed.retry\_send\_task | 重试发送失败的共享安全码 |
| spa.sharedseed.send | 发送共享安全码 |
| spa.sharedseed.send\_result | 更新共享安全码分发进度 |
| spa.tmpseed.query | 查看用户激活码 |
| spa.tmpseed.reset | 重置用户激活码 |
| spa.tmpseed.retry\_send\_task | 重试发送失败的用户激活码 |
| spa.tmpseed.send | 发送用户激活码 |
| spa.tmpseed.send\_result | 更新用户激活码分发进度 |
| spa\_client.download | 下载SPA客户端 |

**3.3.67 UEM**

此类事件的主类型（mainType）为uem，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| emm\_app\_policy.create | 创建移动应用授权与策略 |
| emm\_app\_policy.delete | 删除移动应用授权与策略 |
| emm\_app\_policy.update | 更新移动应用授权与策略 |
| emm\_app\_watermark.update | 更新移动应用全局水印 |
| emm\_policy\_template.update | 更新应用默认策略 |
| uem\_app\_advancedConfig.update | 更新应用高级配置 |
| uem\_app\_appExport.cancel | 取消应用压缩任务 |
| uem\_app\_appExport.compress | 提交应用压缩任务 |
| uem\_app\_appExport.download | 下载应用压缩包 |
| uem\_app\_authConfig.update | 更新移动授权高级配置 |
| uem\_app\_group.create | 创建应用分组 |
| uem\_app\_group.delete | 删除应用分组 |
| uem\_app\_group.update | 更新应用分组 |
| uem\_app\_installer\_config.create | 创建程序安装配置数据 |
| uem\_app\_installer\_config.delete | 删除程序安装配置数据 |
| uem\_app\_installer\_config.update | 更新程序安装配置数据 |
| uem\_app\_installer\_list.create | 创建程序安装名单数据 |
| uem\_app\_installer\_list.delete | 删除程序安装名单数据 |
| uem\_app\_installer\_list.update | 更新程序安装名单数据 |
| uem\_app\_net\_policy.update | 更新应用网络隔离策略 |
| uem\_app\_sso.delete | 删除录制信息 |
| uem\_app\_sso.genRandCode | 生成验证码 |
| uem\_app\_sso.update | 保存录制信息 |
| uem\_app\_store.betaToRel | 将测试版本转为正式版本 |
| uem\_app\_store.cancel | 取消发布任务 |
| uem\_app\_store.configure | 提交封装配置 |
| uem\_app\_store.configureBasic | 提交基础配置 |
| uem\_app\_store.create | 开始创建应用发布任务 |
| uem\_app\_store.createBetaApp | 开始创建Beta应用发布任务 |
| uem\_app\_store.delHistoryVersion | 删除历史版本 |
| uem\_app\_store.delete | 删除发布应用 |
| uem\_app\_store.download | 下载应用包 |
| uem\_app\_store.exportAppInstallCancel | 取消已安装用户详情导出任务 |
| uem\_app\_store.exportAppInstallCompress | 提交已安装用户详情导出任务 |
| uem\_app\_store.exportAppInstallDownload | 下载已安装用户详情导出结果 |
| uem\_app\_store.importRedeemCode | 添加兑换码 |
| uem\_app\_store.markMsgAsRead | 移动应用中心消息置为已读 |
| uem\_app\_store.publish | 提交发布任务 |
| uem\_app\_store.update | 开始更新发布应用 |
| uem\_app\_store.updateExclude | 更新排除用户配置 |
| uem\_app\_store.upload | 上传发布应用包 |
| uem\_app\_store.uploadRedeemCode | 上传兑换码文件 |
| uem\_audit\_center.commitConfig | 零信任分析中心的保存配置 |
| uem\_audit\_flow.terminate | 终止审批流程 |
| uem\_audit\_standard.update | 更新文件审批规范配置 |
| uem\_audit\_standard.upload | 上传安全规定文档 |
| uem\_audit\_task.complete\_task | 审批任务完结 |
| uem\_audit\_tpl.create | 新建审批模板 |
| uem\_audit\_tpl.delete | 删除审批模板 |
| uem\_audit\_tpl.update | 更新审批模板 |
| uem\_auth\_sharing.update | 更新UEM授权共享状态 |
| uem\_cert\_store.create | 添加移动应用证书 |
| uem\_cert\_store.getAlias | 获取移动应用证书别名 |
| uem\_cert\_store.update | 更新移动应用证书 |
| uem\_helpGuide.update | 更新工作空间帮助向导 |
| uem\_installer\_list.lifecycle.create | 创建安装文件记录 |
| uem\_installer\_list.lifecycle.delete | 删除安装文件记录 |
| uem\_installer\_list.lifecycle.edit | 编辑安装文件记录 |
| uem\_net\_policy.create | 创建网络访问策略 |
| uem\_net\_policy.delete | 删除网络访问策略 |
| uem\_net\_policy.move | 调整网络访问策略优先级 |
| uem\_net\_policy.update | 更新网络访问策略 |
| uem\_program\_list.lifecycle.create | 创建被管控程序 |
| uem\_program\_list.lifecycle.delete | 删除被管控程序 |
| uem\_program\_list.lifecycle.edit | 编辑被管控程序 |
| uem\_sandbox.create | 创建工作空间 |
| uem\_sandbox.delete | 删除工作空间 |
| uem\_sandbox.publish | 发布工作空间 |
| uem\_sandbox.update | 更新工作空间 |
| uem\_sandbox.updateExclude | 更新排除用户配置 |
| uem\_sandbox.upload | 上传工作空间图标 |
| uem\_sandboxACL.create | 新增工作空间准入策略 |
| uem\_sandboxACL.delete | 删除工作空间准入策略 |
| uem\_sandboxACL.update | 更新工作空间准入策略 |
| uem\_sandbox\_advance\_config.update | 更新工作空间高级设置 |
| uem\_sandbox\_dataPolicy.create | 创建工作空间发布与策略 |
| uem\_sandbox\_dataPolicy.delete | 删除工作空间发布与策略 |
| uem\_sandbox\_dataPolicy.update | 更新工作空间发布与策略 |
| uem\_sandbox\_dns\_rule.create | 新增DNS规则 |
| uem\_sandbox\_dns\_rule.delete | 删除DNS规则 |
| uem\_sandbox\_dns\_rule.move | 移动DNS规则优先级 |
| uem\_sandbox\_dns\_rule.update | 更新DNS规则 |
| uem\_sandbox\_linux\_program\_repository.create | 创建统信UOS/麒麟Kylin程序仓库名单 |
| uem\_sandbox\_linux\_program\_repository.delete | 删除统信UOS/麒麟Kylin程序仓库名单 |
| uem\_sandbox\_linux\_program\_repository.update | 更新统信UOS/麒麟Kylin程序仓库名单 |
| uem\_sandbox\_mac\_program\_repository.create | 创建Mac程序仓库名单 |
| uem\_sandbox\_mac\_program\_repository.delete | 删除Mac程序仓库名单 |
| uem\_sandbox\_mac\_program\_repository.update | 更新Mac程序仓库名单 |
| uem\_sandbox\_netAccessPolicy.create | 创建工作空间网络访问控制策略 |
| uem\_sandbox\_netAccessPolicy.delete | 删除工作空间网络访问控制策略 |
| uem\_sandbox\_netAccessPolicy.move | 调整工作空间网络访问控制策略优先级 |
| uem\_sandbox\_netAccessPolicy.update | 更新工作空间网络访问控制策略 |
| uem\_sandbox\_programList.delete | 删除工作空间程序运行限制策略 |
| uem\_sandbox\_programList.setChildProcessPerm | 子进程运行权限开关 |
| uem\_sandbox\_programList.setStatus | 设置工作空间程序运行限制策略开关 |
| uem\_sandbox\_programList.update | 更新工作空间程序运行限制策略 |
| uem\_sandbox\_program\_repository.create | 创建程序仓库名单 |
| uem\_sandbox\_program\_repository.delete | 删除程序仓库名单 |
| uem\_sandbox\_program\_repository.update | 更新程序仓库名单 |
| uem\_sandbox\_safe\_module.create | 创建安全模块定制配置策略 |
| uem\_sandbox\_safe\_module.delete | 删除安全模块定制配置策略 |
| uem\_sandbox\_safe\_module.move | 移动安全模块定制配置策略优先级 |
| uem\_sandbox\_safe\_module.update | 更新安全模块定制配置策略 |
| uem\_sandbox\_watermark.update | 更新工作空间水印策略 |
| uem\_virtual\_net\_domain.copy | 复制虚拟网络域 |
| uem\_virtual\_net\_domain.create | 新建虚拟网络域 |
| uem\_virtual\_net\_domain.delete | 删除虚拟网络域 |
| uem\_virtual\_net\_domain.preCreate | 准备新建或编辑虚拟网络域 |
| uem\_virtual\_net\_domain.save | 虚拟网络域保存 |
| uem\_virtual\_net\_domain.update | 更新虚拟网络域 |
| uem\_virtual\_net\_domain.updateConfig | 更新虚拟网络域高级配置 |
| uem\_virtual\_net\_domain.uploadIcon | 上传虚拟网络域图标 |
| uem\_virtual\_net\_domain\_net\_policy.create | 新建虚拟网络域网络策略 |
| uem\_virtual\_net\_domain\_net\_policy.delete | 删除虚拟网络域网络策略 |
| uem\_virtual\_net\_domain\_net\_policy.move | 调整虚拟网络域网络策略优先级 |
| uem\_virtual\_net\_domain\_net\_policy.update | 更新虚拟网络域网络策略 |
| uem\_virtual\_net\_policy.create | 新建虚拟专网策略 |
| uem\_virtual\_net\_policy.delete | 删除虚拟专网策略 |
| uem\_virtual\_net\_policy.update | 更新虚拟专网策略 |
| uem\_virtual\_net\_policy.updateExcludeUsers | 更新排除用户配置 |
| uem\_web\_app\_store.configure | 配置web应用商店选项 |
| uem\_windowTag.update | 更新工作空间窗口标记 |
| uem\_workspace.lifecycle.edit | 编辑可用程序限制 |
| uem\_wp\_warning\_message.disableReceiveMessage | 关闭订阅信息 |
| uem\_wp\_warning\_message.enableReceiveMessage | 开启订阅信息 |
| uem\_wp\_warning\_message.viewMessage | 阅读产品预警信息 |

**3.3.68 管理组**

此类事件的主类型（mainType）为admin，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| admin.admin\_group.edit | 编辑管理员账户的所属管理组 |
| admin\_group.data\_perm.edit | 编辑管理组内容权限 |
| admin\_group.func\_perm.edit | 编辑管理组模块权限 |
| admin\_group.lifecycle.create | 创建管理组 |
| admin\_group.lifecycle.delete | 删除管理组 |
| admin\_group.lifecycle.edit | 编辑管理组 |

**3.3.69 短信网关**

此类事件的主类型（mainType）为sms\_gateway，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| auth\_plugin.sms.test | 发送测试短信 |
| sms\_gateway.connect\_test | 网关连通性测试 |
| sms\_gateway.lifecycle.DELETE | 删除短信网关 |
| sms\_gateway.lifecycle.create | 创建短信网关 |
| sms\_gateway.lifecycle.update | 编辑短信网关 |
| sms\_gateway.query\_secret | 查看短信网关密钥 |

**3.3.70 定制配置**

此类事件的主类型（mainType）为custom\_config，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| custom\_config.backup | 备份定制通用配置 |
| custom\_config.edit | 编辑定制通用配置 |
| custom\_config.recover\_default | 恢复默认定制通用配置 |
| custom\_config.recover\_last | 恢复最近定制通用配置 |

**3.3.71 灰度升级策略**

此类事件的主类型（mainType）为upgrade\_policy，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| upgrade\_policy.lifecycle.create | 新增灰度升级策略 |
| upgrade\_policy.lifecycle.delete | 删除灰度升级策略 |
| upgrade\_policy.lifecycle.deletePkg | 删除安装包 |
| upgrade\_policy.lifecycle.setChangelog | 设置版本信息 |
| upgrade\_policy.lifecycle.setStableVersion | 设置灰度升级稳定版本 |
| upgrade\_policy.lifecycle.update | 修改灰度升级策略 |

**3.3.72 诱饵**

此类事件的主类型（mainType）为honeypot/device\_decoy/decoy\_task，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| decoy\_resource\_probe.create | 创建应用诱饵引流规则 |
| decoy\_resource\_probe.edit | 更新应用诱饵探针引流规则 |
| decoy\_task.create | 创建诱饵发布任务 |
| decoy\_task.delete | 删除诱饵发布任务 |
| decoy\_task.edit | 终止诱饵发布任务 |
| device\_decoy.create | 创建终端诱饵 |
| device\_decoy.custom\_info\_dict.edit | 更新终端诱饵自定义字典 |
| device\_decoy.delete | 删除终端诱饵 |
| device\_decoy.edit | 编辑终端诱饵 |

**3.3.73 蜜罐**

此类事件的主类型（mainType）为honeypot，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| honeypot.create | 新建蜜罐 |
| honeypot.delete | 删除蜜罐 |
| honeypot.edit | 编辑蜜罐 |

**3.3.74 威胁处置策略**

此类事件的主类型（mainType）为security\_response，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| security\_response.edit | 编辑威胁处置策略 |

**3.3.75 移动推送服务**

此类事件的主类型（mainType）为mobile\_push\_server，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| mobile\_push\_server.disable | 关闭移动推送服务器 |
| mobile\_push\_server.enable | 开启移动推送服务器 |
| mobile\_push\_server.push\_test | 移动端推送服务测试 |

**3.3.76 图标**

此类事件的主类型（mainType）为common\_icon，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| common\_icon.update\_pri | 更新图标关联顺序 |
| common\_icon.upload | 上传图标 |

**3.3.77 IP爆破管理**

此类事件的主类型（mainType）为ip\_brute\_status，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| ip\_brute\_status.lifecycle.auto\_unlock | 自动解锁爆破IP |
| ip\_brute\_status.lifecycle.unlock | 解锁爆破IP |

**3.3.78 配置向导**

此类事件的主类型（mainType）为config\_wizard，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| config\_wizard.update | 更新配置向导数据 |

**3.3.79 弱密码库**

此类事件的主类型（mainType）为weakpwd，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| weakpwd.lifecycle.clear | 清空弱密码库 |
| weakpwd.lifecycle.upload | 上传弱密码库 |

**3.3.80 更新客户端文案**

此类事件的主类型（mainType）为client\_copywriting/err\_feedback\_copywriting，子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| client\_copywriting.update | 更新客户端通用文案 |
| err\_feedback\_copywriting.update | 更新客户端错误反馈文案 |

**3.3.81 其他**

其余未归类事件的子类型（subType）列举如下：

| **事件子类型** | **事件说明** |
| --- | --- |
| DEFAULT\_POLICY\_NAME\_PREDEF\_EE4129 | 默认策略 |
| DEFAULT\_POLICY\_PREDEF\_EE4129 | 默认策略 |
| DEFAULT\_THEME\_PREDEF\_EE4129 | 默认主题 |
| DEFAULT\_VITUAL\_IP\_POOL\_PREDEF\_EE4129 | 默认虚拟IP池 |
| LOCAL\_PWD\_AUTH\_PREDEF\_EE4129 | 本地密码认证 |
| LOCAL\_USER\_DIRECTORY\_PREDEF\_EE4129 | 本地用户目录 |
| RESOURCE\_GROUP\_DEFAULT\_CATEGORY\_PREDEF\_EE4129 | 默认分类 |
| ac\_linkage.query\_appSecret | 查询AC联动配置中的APPSECRET |
| ac\_linkage.query\_shareSecret | 查询AC联动配置中的共享秘钥 |
| ac\_linkage.update | 更新AC联动认证配置 |
| ac\_linkage.update\_appid\_appSecret | 更新AC联动的APPID和APPSECRET |
| admin.logout\_by\_delete | 删除账户注销 |
| admin.logout\_by\_forbidden | 禁用账户注销 |
| admin.logout\_by\_pwd\_change | 密码修改注销 |
| admin.logout\_by\_relogin | 上线抢占注销 |
| admin.logout\_by\_session\_timeout | 超时注销 |
| auto\_unlock\_bruteforce\_status.unlock | 用户账号批量自动解锁 |
| client\_zip.release | 发布客户端压缩包 |
| credential\_theft.intermediary.edit | 更新中间人检测配置 |
| credential\_theft.web\_credential\_steal.edit | 更新会话劫持检测配置 |
| entity\_score.reset | 重置分数 |
| fw\_nat.lifecycle.create | 创建地址转换配置 |
| fw\_nat.lifecycle.delete | 删除地址转换配置 |
| fw\_nat.lifecycle.edit | 编辑地址转换配置 |
| govdingtalk\_auth\_server.h5download | 下载浙政钉H5代码包 |
| ipsec\_iptable\_rules.lifecycle.add | 增加ipsec防火墙规则 |
| ipsec\_iptable\_rules.lifecycle.delete | 删除ipsec防火墙规则 |
| ipsec\_process.lifecycle.disable | 禁用ipsec服务 |
| ipsec\_process.lifecycle.enable | 启用ipsec服务 |
| node\_group\_global\_config.update | 更新网关区域配置 |
| resource\_scan.activate | 启用恶意侦察 |
| resource\_scan.custom\_path.edit | 更新自定义敏感目录 |
| resource\_scan.custom\_port.edit | 更新自定义知名端口 |
| resource\_scan.edit | 更新恶意侦察配置 |
| resource\_scan.exclude\_resource.edit | 更新恶意侦察排除应用 |
| resource\_scan.forbidden | 禁用恶意用侦察 |
| route\_forward.lifecycle.add | 创建路由转发规则 |
| route\_forward.lifecycle.delete | 删除路由转发规则 |
| route\_forward.lifecycle.update | 编辑路由转发规则 |
| sdp\_multiline.changed | 多线路中最优线路发生变化 |
| secuirty\_event.dispose | 标记事件状态 |
| security\_response.create | 新增威胁处置策略 |
| security\_response.delete | 删除威胁处置策略 |
| ssh\_knock.openssh | 开启SSH端口 |
| task.lifecycle.clear | 清理任务 |
| task.lifecycle.edit | 编辑任务 |
| task.nextRunTime.edit | 更新下次同步时间 |
| terminal\_phishing.app\_type\_baseline.creat | 新建应用和进程访问关系 |
| terminal\_phishing.app\_type\_baseline.delete | 删除应用和进程访问关系 |
| terminal\_phishing.app\_type\_baseline.edit | 修改应用和进程访问关系 |
| terminal\_phishing.new\_process\_access\_check.edit | 更新孤立进程访问应用类型异常检测配置 |
| terminal\_phishing.process\_host\_port\_baseline\_check.edit | 更新浏览器访问应用类型异常检测配置 |
| terminal\_phishing.ua\_baseline.creat | 新建本地UA特征库 |
| terminal\_phishing.ua\_baseline.delete | 删除本地UA特征库 |
| terminal\_phishing.ua\_baseline.edit | 更新本地UA特征库 |
| terminal\_phishing.ua\_baseline\_check.edit | 更新浏览器访问UA信息异常检测配置 |
| time\_plan.lifecycle.create | 创建时间计划 |
| time\_plan.lifecycle.delete | 删除时间计划 |
| time\_plan.lifecycle.edit | 更新时间计划 |
| totp.unbind\_user | totp解除绑定 |
| upcoming\_expire\_reminder\_time.update | 更新授权过期提醒配置 |
| upload\_file.lifecycle.upload | 上传备份文件 |
| user.logout\_by\_admin | 强制注销 |
| user.logout\_by\_config\_change | 配置变更注销 |
| user.logout\_by\_relogin | 上线抢占注销 |
| user.logout\_by\_self | 主动注销 |
| user.logout\_by\_session\_timeout | 会话超时注销 |
| user.modify\_pwd | 登录后修改密码 |
| user.trust\_cookie | 校验可信cookie |
| user\_or\_auth\_policy.clear | 清空组织架构的用户策略或认证策略 |
| user\_permission\_approval\_notice.send.sms | 审批结果短信通知 |
| user\_permission\_approval\_notice.update | 编辑应用权限审批通知配置 |
| vpn\_config.import | VPN配置转换 |
| watermark\_template.lifecycle.create | 创建水印模板 |
| watermark\_template.lifecycle.delete | 删除水印模板 |
| watermark\_template.lifecycle.edit | 更新水印模板 |

**4设备安全日志**

**4.1 示例**

设备安全日志的programname包含：@vendorSecurityLog

完整报文示例如下：

<150>Aug 14 10:56:05 localhost apiguard@vendorSecurityLog[149]: { "\_isRisk": 1, "traceId": "0131412b2cb8aff8", "security": { "confidence": 3, "riskLevel": 1, "firstDefense": "DvcDefense", "engineVersion": "1.4.4", "engine": "RASP", "engineRuleVersion": "1.5.0", "severity": 1, "attTactic": [ "TA0043" ], "attTechnique": [ "T1595" ], "ruleName": "RASP\_API\_SCAN", "threatCategory": "HackingTool", "d3Technique": "D3-PMAD", "threatType": "ScanningTool", "secondDefense": "ApiDefense", "d3Tactic": "Detect" }, "src": { "port": 50762, "ip": "1.1.1.1", "geo": { "country": "内网IP", "province": "-", "city": "-", "organization": "内网IP" } }, "api": { "query": "status[]=1", "url": "https:\/\/1.1.1.1:4433\/api\/v1\/securityEvent\/getSecurityEvent", "method": "GET", "userAgent": "Mozilla\/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit\/537.36 (KHTML, like Gecko) Chrome\/115.0.0.0 Safari\/537.36" }, "event": { "action": "", "timestamp": 1691981765314, "id": "4c08c0db-801b-43d1-8c86-b73aae189240", "reason": "[QUERY\_NAME]invalid arg name in query: status[]", "\_vSchema": "apiGuard,risk", "subType": "security.api\_guard.ngswaf.query\_name\_check", "result": "-", "mainType": "security.ngswaf" }, "\_logId": "244", "vendor": { "product": "aTrust", "productType": "hybrid", "productVersion": "2.3.10", "dvcId": "A14C0E10", "sourceName": "A14C0E10", "dvcIp": "1.1.1.1" } }

Copy

其中正文为：

{

"\_isRisk": 1,

"traceId": "0131412b2cb8aff8",

"security": {

"confidence": 3,

"riskLevel": 1,

"firstDefense": "DvcDefense",

"engineVersion": "1.4.4",

"engine": "RASP",

"engineRuleVersion": "1.5.0",

"severity": 1,

"attTactic": [

"TA0043"

],

"attTechnique": [

"T1595"

],

"ruleName": "RASP\_API\_SCAN",

"threatCategory": "HackingTool",

"d3Technique": "D3-PMAD",

"threatType": "ScanningTool",

"secondDefense": "ApiDefense",

"d3Tactic": "Detect"

},

"src": {

"port": 50762,

"ip": "1.1.1.1",

"geo": {

"country": "内网IP",

"province": "-",

"city": "-",

"organization": "内网IP"

}

},

"api": {

"query": "status[]=1",

"url": "https://1.1.1.1:4433/api/v1/securityEvent/getSecurityEvent",

"method": "GET",

"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/115.0.0.0 Safari/537.36"

},

"event": {

"action": "",

"timestamp": 1691981765314,

"id": "4c08c0db-801b-43d1-8c86-b73aae189240",

"reason": "[QUERY\_NAME]invalid arg name in query: status[]",

"\_vSchema": "apiGuard,risk",

"subType": "security.api\_guard.ngswaf.query\_name\_check",

"result": "-",

"mainType": "security.ngswaf"

},

"\_logId": "244",

"vendor": {

"product": "aTrust",

"productType": "hybrid",

"productVersion": "2.3.10",

"dvcId": "A14C0E10",

"sourceName": "A14C0E10",

"dvcIp": "1.1.1.1"

}

}

**4.2字段说明**

**4.2.1 源（src）**

来源信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| geo |  | 地理信息，实时地理位置信息 |
| .city | string | IP归属城市 |
| .organization | string | 所属运营商 |
| .country | string | IP归属国家 |
| .province | string | IP归属省份 |
| preProxyIp | string | 代理IP |
| port | number | 客户端源端口 |
| ip | string | 客户端源IP |
| ipTags | []string | IP分析 |

**JSON格式**

"src": {

"geo": {

"city": "长沙",

"organization": "",

"country": "中国",

"province": "湖南"

},

"preProxyIp": "1.1.1.1",

"port": 50076,

"ip": "1.1.1.1",

"ipTags": []

}

**4.2.2 事件（event）**

事件信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| id | string | 日志ID，日志唯一ID |
| mainType | string | 操作类型 |
| subType | string | 操作子类型 |
| timestamp | number | 时间，13位时间戳（无时区概念），精确到毫秒 |
| result | string | 结果，可选值：SUCCESS（成功）、FAILED（失败）、-（无） |
| reason | string | 原因 |
| action | string | 处置动作，可选值：DENY（已拦截）、ALLOW（已通过）、-（无） |
| \_vSchema | string | schema，用于动态控制控制台展示某些字段，可选值：management（显示target字段）、apiGuard（显示api字段）、risk（显示security字段）、acl（显示acl字段）、proxy（显示target、network字段） |
| details | string | 日志描述，可空，一般为JSON，为日志的附加信息 |

**JSON格式**

"event": {

"id": "67f48a04-7961-44af-a693-1833decff4f0",

"mainType": "user",

"subType": "user.login",

"timestamp": 1689606221501,

"result": "SUCCESS",

"reason": "",

"action": "",

"\_vSchema": "",

"details": ""

}

**4.2.3 安全信息（security）**

安全信息，当日志中的\_isRisk=1时为安全日志，会有安全日志节点

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| ruleName | string | 防护规则名称 |
| firstDefense | string | SDP防线，可选值：DvcDefense（设备防线）、IdDefense（账号防线）、AppDefense（终端防线） |
| secondDefense | string | SDP子防线，可选值：PrimaryAuthDefense（主认证防线）、ApiDefense（API防线）、SecondaryAuthDefense（从认证防线）、UdpSpaDefense（UDP SPA防线）、TcpSpaDefense（TCP SPA防线）、TrapDefense（诱捕防线）、SessionDefense（会话防线） |
| attTactic | []string | ATT&CK战术 |
| attTechnique | []string | ATT&CK技术 |
| d3Tactic | string | D3Fend防御战术 |
| d3Technique | string | D3Fend防御技术 |
| engine | string | 安全引擎名称 |
| engineVersion | string | 安全引擎版本 |
| engineRuleVersion | string | 防护规则版本 |
| severity | number | 严重程度，1~3，分别代表低中高 |
| riskLevel | number | 风险等级，1~3，分别代表低中高 |
| confidence | number | 威胁置信度，1~3，分别代表低中高 |
| threatCategory | string | 威胁分类 |
| threatType | string | 威胁类型 |

**JSON格式**

"security": {

"ruleName": "RASP\_API\_SCAN",

"firstDefense": "DvcDefense",

"secondDefense": "ApiDefense",

"attTactic": [

"TA0043"

],

"attTechnique": [

"T1595"

],

"d3Tactic": "Detect",

"d3Technique": "D3-PMAD",

"engine": "RASP",

"engineVersion": "1.0.0",

"engineRuleVersion": "1.0.0",

"severity": 1,

"riskLevel": 1,

"confidence": 1,

"threatCategory": "HackingTool",

"threatType": "ScanningTool"

}

**4.2.4 API信息（api）**

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| url | string | 请求地址 |
| query | string | 请求参数 |
| method | string | 请求方法 |
| body | string | 请求body |
| statusCode | string | 响应状态码 |
| referer | string | Referer |

**JSON格式**

"api": {

"url": "https://sdp.com",

"query": "",

"method": "POST",

"body": "",

"statusCode": 200,

"referer": ""

}

**4.2.5 设备（vendor）**

设备信息

**字段定义**

| **字段** | **类型** | **说明** |
| --- | --- | --- |
| sourceName | string | 客户名称，取自授权客户名称 |
| product | string | 产品名称，可选值：aTrust、VPN |
| productVersion | string | 产品版本号 |
| productType | string | 产品类型，可选值：hybrid（综合网关）、sdp（控制中心）、proxy（代理网关） |
| dvcId | string | 设备ID |
| dvcIp | string | 设备IP |

**JSON格式**

"vendor": {

"sourceName": "",

"product": "aTrust",

"productVersion": "2.3.6",

"productType": "hybrid",

"dvcId": "ABCDEF",

"dvcIp": "1.1.1.1"

}

**4.2.6 是否安全日志（\_isRisk）**

可选值：0（否），1（是）

**4.2.7 TraceID（traceId）**

请求接口跟踪码

**4.2.8 日志对账ID（\_logId）**

rsyslog自动生成的自增ID，用于排查是否丢失日志

**4.3日志类型**

**4.3.1 API防护（apiguard日志）**

此类事件的主类型（mainType）为api\_guard，子类型（subType）列举如下：

| **事件子类型** | **事件说明** | **是否为安全日志** |
| --- | --- | --- |
| security.api\_guard.ngswaf.header\_check | 接口头部检测 | √ |
| security.api\_guard.ngswaf.query\_name\_check | 接口参数名检测 | √ |
| security.api\_guard.ngswaf.snort | 接口攻击行为检测 | √ |
| security.api\_guard.request\_validation.api\_not\_found | 接口扫描 | √ |
| security.api\_guard.request\_validation.invalid\_data | 接口参数爆破 | √ |
| security.api\_guard.request\_validation.need\_online | 接口越权调用 | √ |
| security.api\_guard.request\_validation.tia\_api\_brute\_scan | 接口暴力扫描 | √ |
| security.api\_guard.request\_validation.tia\_api\_param\_brute\_scan | 接口参数暴力爆破 | √ |
| security.api\_guard.shellcheck.failed | 接口webshell攻击 | √ |

**5.系统日志**

**5.1 示例**

系统日志的programname包含：@systemLog

完整报文示例如下：

<142>Aug 14 10:52:19 localhost sdp-passport@systemLog[128]: sess: 822728bc-99f6-466c-81ed-bd7a9cfd9a8c\_0793f2c8-062e-4e2, user: user@local, auth: auth/psw is success, code: 0, msg: 密码认证成功 |AUTHZ|url=/passport/v1/auth/psw?clientType=SDPBrowserClient&platform=Windows&lang=zh-CN, username=user, sessid=822728bc-99f6-466c-81ed-bd7a9cfd9a8c\_aab2b86d-f161-472, sTraceId=810908a5-d2c9-437a-aadf-0b9, traceid=ad985062, ip=1.1.1.1#end#

Copy

其中正文为：

sess: 822728bc-99f6-466c-81ed-bd7a9cfd9a8c\_0793f2c8-062e-4e2, user: user@local, auth: auth/psw is success, code: 0, msg: 密码认证成功 |AUTHZ|url=/passport/v1/auth/psw?clientType=SDPBrowserClient&platform=Windows&lang=zh-CN, username=user, sessid=822728bc-99f6-466c-81ed-bd7a9cfd9a8c\_aab2b86d-f161-472, sTraceId=810908a5-d2c9-437a-aadf-0b9, traceid=ad985062, ip=1.1.1.1#end#