云查相关梳理

- 云查相关梳理
  - 云查接口
    - 当前云查接口
    - 内容格式区别
  - 证书权限
    - 证书匹配权限规格
    - License 与 API KEY 权限的对应关系
    - 当前证书对应云查规格
  - 权限控制框架
  - 云查业务提供方式
    - 设备获取 API KEY
    - 防火墙使用云查
    - 云查逻辑
  - 设备查询统计
    - 接入设备数量统计
    - 设备查询量 TOP20
  - IOC 查询统计
    - 在线查询响应时间统计
    - IOC 查询量统计
    - IOC 查询判定结果统计
    - IOC 查询量 TOP20

云查接口

当前云查接口

URI	API 版本	内容格式	权限控制对象	描述
/api/c2/domain/reputation	1.0.0	`List<ReputationModel>`	USER	第一版云查，用户登录云瞻获取 APIKEY 后手动粘贴至防火墙开启，该接口支持所有类型查询
/api/c2/domain/shortlisted-tests/reputation	1.0.0	`List<ReputationModel>`	USER	提供给江西威胁情报入围测试，只支持域名，查询时同步查询第三方，优先采用第三方结果
/device/ioc/reputation	1.1.0	`List<ReputationModel>`	DEVICE	第二版云查，由设备证书来控制权限，该接口支持所有类型查询
/device/ioc/{type: ip/domain/url/file}/reputation	1.1.0	`List<ReputationModelV2>`	DEVICE	第三版云查，由设备证书来控制权限，根据不同类型细分为四个接口，根据证书来实现更加细致的权限控制
/api/permission/quota	1.0.0		USER	用户获取其下接口配额信息，只查询以下方案组下的 URI：api、reputation、quota
/device/permission/quota	1.1.0		DEVICE	设备获取其下接口配额信息，只查询以下方案组下的 URI：device-quota、device-reputation、device-query-ip、device-query-domain、device-query-url、device-query-file

内容格式区别

ReputationModel				ReputationModelV2			
一级字段	二级字段	类型	描述	一级字段	二级字段	类型	描述
result		int	0: white, 1: black, 2: unknown	result		int	0: none; 1: white; 2: suspicious; 3: black
iocType		int	ioc_type 0: ip (type=0), ip+port (type=port); 1: domain (FQDN (type=0), SLD (type=1)); 2: url (type=0); 3: File (md5 (type=0), sha1 (type=1), sha256 (type=2), sha512 (type=3))	type		int	ioc_type 0: ip (subtype=0), ip+port (subtype=port); 1: domain (FQDN (subtype=0), SLD (subtype=1)); 2: url (subtype=0); 3: File (md5 (subtype=0), sha1 (subtype=1), sha256 (subtype=2), sha512 (subtype=3))
type		int	子类型	subtype		int	子类型
ioc		String		ioc		int	
tags		array	分类标签英文名称列表	tags		array	分类标签列表
					nameEn	String	

ReputationModel				ReputationModelV2			
					nameCn	String	
				familyTags		array	家族标签列表
					nameEn	String	
					nameCn	String	
				groupTags		array	团伙标签列表
					nameEn	String	
					nameCn	String	

证书权限

证书匹配权限规格

```
permission:
  # 该配置只针对于 DEVICE 角色组下方案
  license_cases:
    # 没有 license 时需要分配的权限
    -1:
      # 方案组: 规格
      device-quota: 云查配额查询规格
    # 僵尸网络C&C防御 license key
    57:
      device-quota: 云查配额查询规格
      device-reputation: C2证书规格
      device-query-ip: C2证书规格
```

```
    device-query-domain: C2证书规格
  # 安全DNS服务 license key
  91:
    device-quota: 云查配额查询规格
    device-reputation: 安全DNS证书规格
    device-query-ip: 安全DNS证书规格
    device-query-domain: 安全DNS证书规格
# 规格优先级，数字越大优先级越高，可随意设置整数，只比大小，！！！需要覆盖license_cases下的所有规格！！！
specification_priority:
  0: 云查配额查询规格
  1: C2证书规格
  2: 安全DNS证书规格
```

License 与 API KEY 权限的对应关系

> *IF 有安全 DNS 服务的 License*
> *权限过期时间与该 License 过期时间一致，且查询配额无限制（安全 DNS 授权）*
> *ELSE IF 有 C2 的license*
> *权限过期时间与该 License 过期时间一致，查询配额 10k/天（C2 授权）*
> *ELSE*
> *权限过期时间为一百年后，仅允许查询配额*

如果云端已存在该 SN 的 API KEY 信息，则根据上述规则重置过期时间和配额，并下发已存在的 API KEY（无论该 API KEY 是否与原来的相同，设备收到后直接替换即可）

当前证书对应云查规格

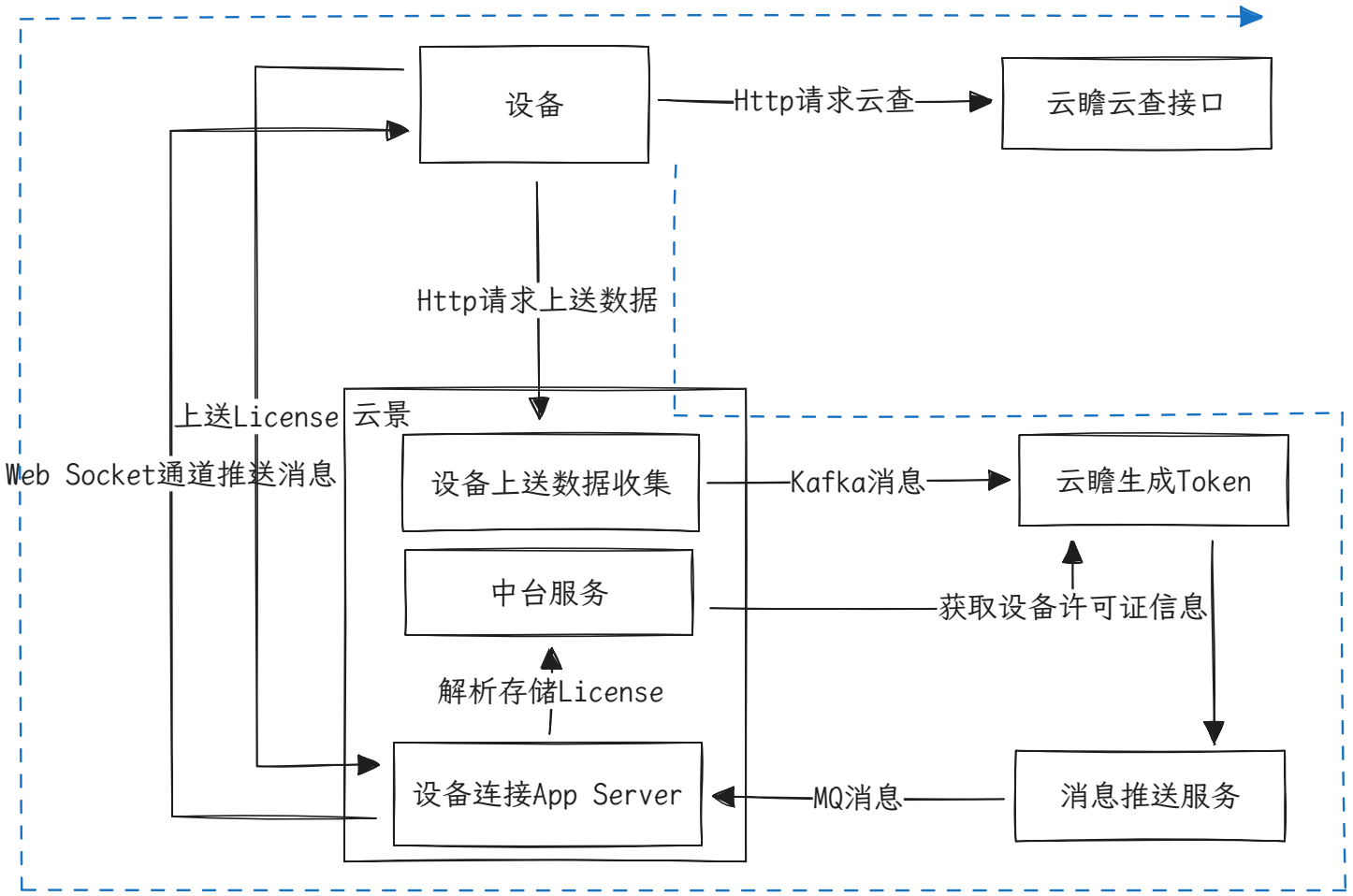
规格名称	资源配额/天	资源配额/分钟
云查配额查询规格	20 K	20
C2证书规格	10 K	无限制
安全DNS证书规格	无限制	无限制

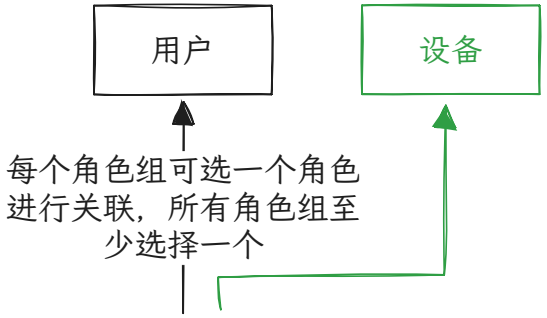
权限控制框架

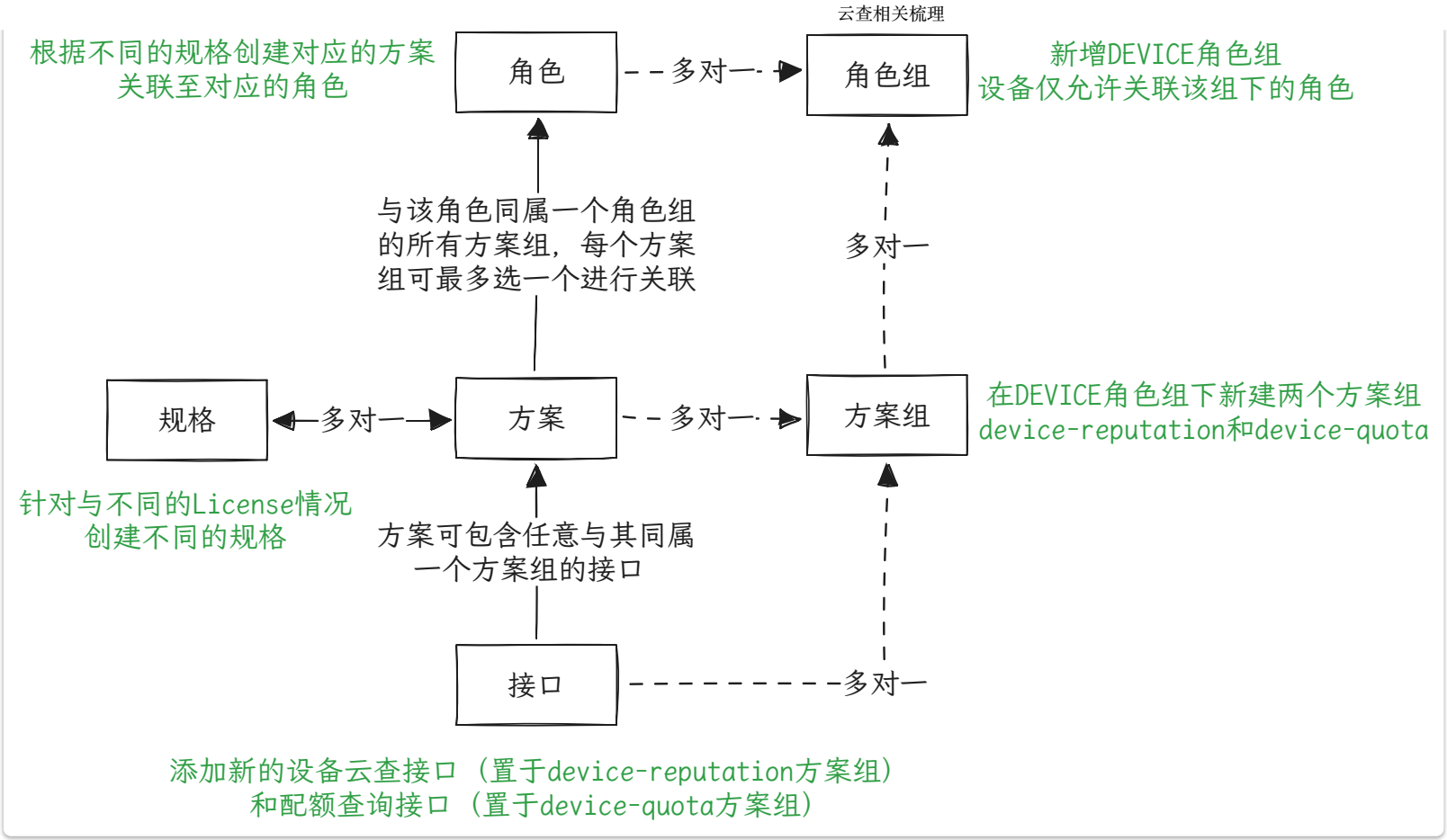
云查业务提供方式

设备获取 API KEY

FR48832 防监管通报 - 云瞻配合实现云查token自动分发 FD


设备
Http请求云查
云瞻云查接口
Http请求上送数据
上送License
云景
Web Socket通道推送消息
设备上送数据收集
Kafka消息
云瞻生成Token
中台服务
获取设备许可证信息
解析存储License
设备连接App Server
MQ消息
消息推送服务


用户
设备
每个角色组可选一个角色
进行关联，所有角色组至
少选择一个



防火墙使用云查

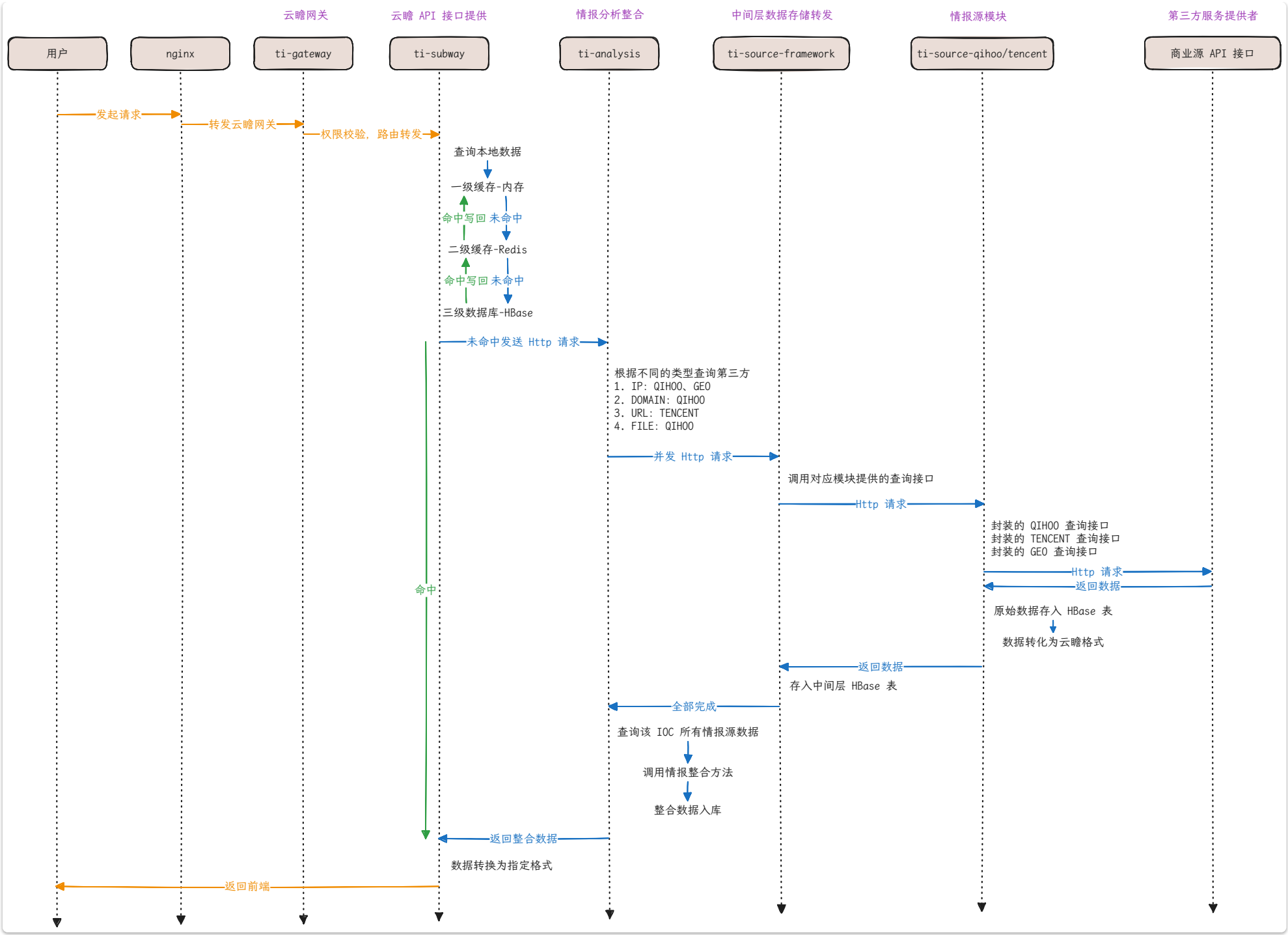
FR48345-针对预防监管通报方案的云查方案优化，优化DNS查询效率、扩大查询缓存-FD

1. 新增布隆过滤器打包进 C2 特征库，设备加载 C2 特征库时也会将布隆过滤器加载至内存中，若命中才进行云查
2. 目前云瞻提供的云查接口实际上是查询云瞻全库，通过上述方式，云瞻可以修改布隆过滤器制作的条件来控制设备实际云查的范围

云查逻辑

> *以下为云瞻首页查询的逻辑，去掉第三方源查询的部分即为设备云查的逻辑*

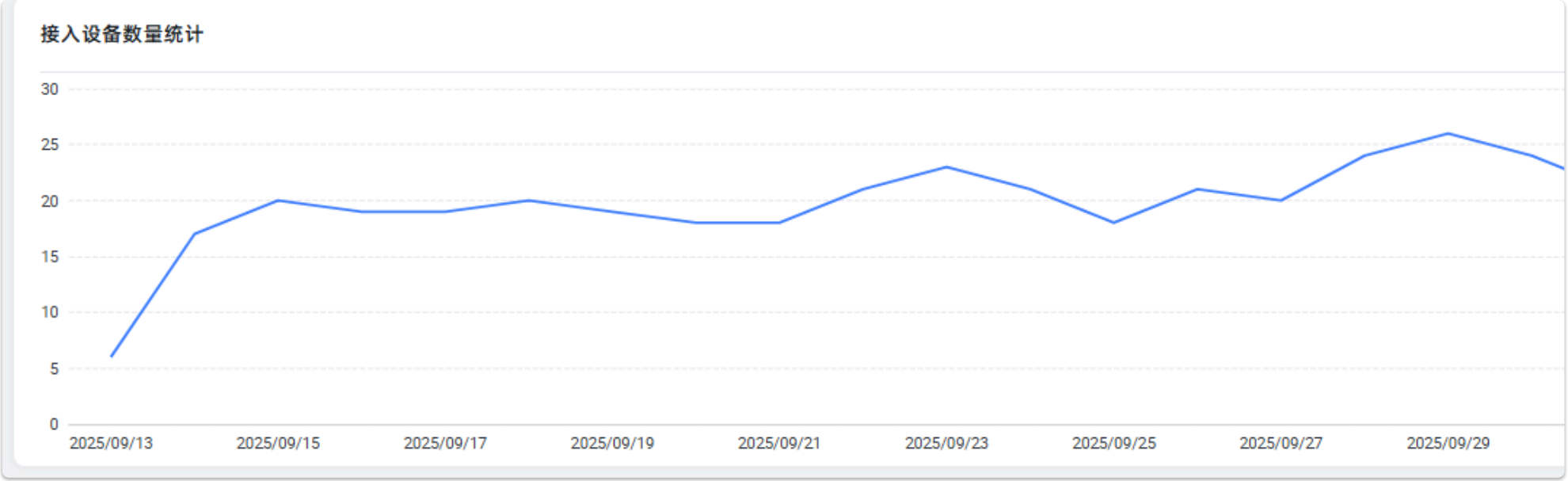
云查相关梳理


云瞻网关
云瞻 API 接口提供
情报分析整合
中间层数据存储转发
情报源模块
第三方服务提供者
用户
nginx
ti-gateway
ti-subway
ti-analysis
ti-source-framework
ti-source-qihoo/tencent
商业源 API 接口
发起请求
转发云瞻网关
权限校验，路由转发
查询本地数据
一级缓存-内存
命中写回
未命中
二级缓存-Redis
命中写回
未命中
三级数据库-HBase
未命中发送 Http 请求
根据不同的类型查询第三方
1. IP: QIHOO、GEO
2. DOMAIN: QIHOO
3. URL: TENCENT
4. FILE: QIHOO
并发 Http 请求
调用对应模块提供的查询接口
Http 请求
封装的 QIHOO 查询接口
封装的 TENCENT 查询接口
封装的 GEO 查询接口
Http 请求
返回数据
命中
原始数据存入 HBase 表
数据转化为云瞻格式
返回数据
存入中间层 HBase 表
全部完成
查询该 IOC 所有情报源数据
调用情报整合方法
整合数据入库
返回整合数据
数据转换为指定格式
返回前端

设备查询统计

接入设备数量统计

- 在时间范围内，各时间粒度接入云查并查询的设备数量统计



设备查询量 TOP20

- 在时间范围内，接入云查的设备按查询量降序排列的 TOP20
  - 总查询次数 = 单词查询次数 + 批量查询次数
  - 总数量 = 单词查询数量 + 批量查询数量

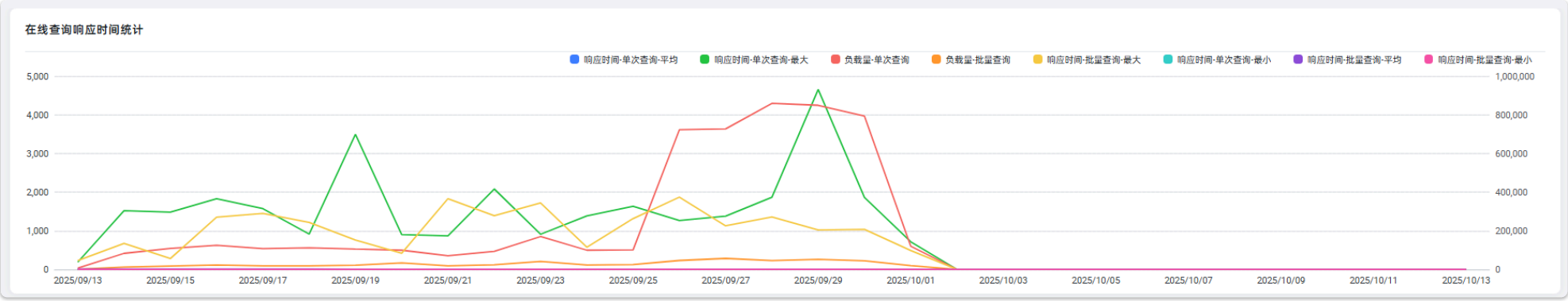
设备查询量TOP20

	设备SN	客户信息	单次查询次数	批量查询次数	总查询次数	批量查询数量	总数量
1	6031616232000333		2039871	40878	2080749	103556	2143427
2	5932441245000645		1357578	85658	1443236	312260	1669838
3	5926447225003857	中国电信股份有限公司重庆分公司	74836	62558	137394	700144	774980
4	5026613242001941	石河子大学	193435	129344	322779	547036	740471
5	HDDGHS2503247866		395112	87933	483045	257009	652121
6	5827638225014760	张家港市医疗保障局	258088	0	258088	0	258088
7	5026627222000943	西安工业大学	83497	41187	124684	115795	199292
8	26LSHW1703240298		164375	15458	179833	34657	199032
9	5823634225002850		94938	28653	123591	75826	170764
10	5828208225000547		92235	18815	111050	59971	152206

IOC 查询统计

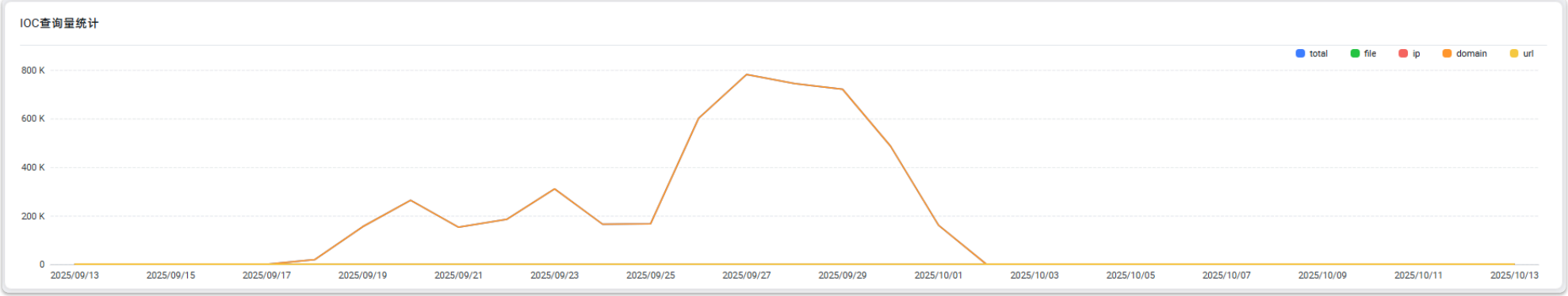
在线查询响应时间统计

- 时间范围内，使用云查接口查询的响应时间、接口负载量统计趋势
  - 响应时间
    - 分单次、批量查询
    - 每种查询又分别统计了最小、平均、最大值
  - 负载量
    - 即使用云查接口查询的查询量



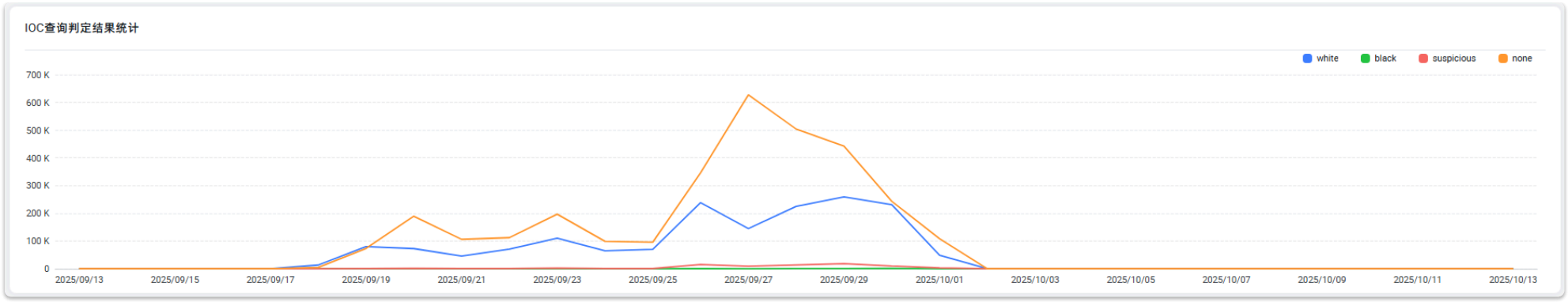
IOC 查询量统计

- 时间范围内，各时间粒度查询的 ioc 数量统计
  - 按照不同 IOC 类型维度划分



IOC 查询判定结果统计

- 时间范围内，各时间粒度查询的 ioc 数量统计
  - 按照 ioc 结果维度划分



IOC 查询量 TOP20

- 时间范围内，查询数量最多的 20 个 IOC

IOC查询量TOP20

	IOC	ioc类型	数量
1	h.root-servers.net	domain	87702
2	k.root-servers.net	domain	87695
3	j.root-servers.net	domain	87692
4	e.root-servers.net	domain	87691
5	l.root-servers.net	domain	87689
6	c.root-servers.net	domain	87687
7	d.root-servers.net	domain	87687
8	f.root-servers.net	domain	87684
9	i.root-servers.net	domain	87682
10	g.root-servers.net	domain	87680