**DNS拨测逻辑、拨测数据说明**

数据库表：见附件



**adns\_collect**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| 序号 | 字段名 | 类型 | 主键 | NULL | 默认值 | 说明 | 示例 |
| 1 | 开始时间 | varchar2(100) |  |  |  | DNS解析请求发起时间 | 2022-10-15 10:09:56.901512291 |
| 2 | 客户端地理位置 | varchar2(20) |  |  |  | DNS解析请求发起位置 | 浙江 |
| 3 | 请求发起端 | varchar2(100) |  |  |  | DNS解析请求发起端IP（出口递归解析器） | 211.140.11.69 |
| 4 | 请求接收端 | varchar2(100) |  |  |  | 工行权威服务器IP | 211.95.81.245 |
| 5 | cName | varchar2(300) |  |  |  | DNS解析请求的域名 | 2409:8c28:2808:4:800:0:0:52x8478xmapsystm.icbc.com.cn |
|  |  |  |  |  |  |  |  |

**a\_query**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 字段名 | 类型 | 主键 | NULL | 默认值 | 说明 | 示例 |
| 1 | ldns | varchar2(100) |  |  |  | 本地解析器IP | '222.85.85.85' |
| 2 | adns | varchar2(100) |  |  |  | 目标工行权威域名服务器hostname | 'bjtns2.icbc.com.cn.' |
| 3 | domain | varchar2(100) |  |  |  | 目标检测域名 | 'fee.icbc.com.cn' |
| 5 | q\_type | varchar2(100) |  |  |  | 查询类型query\_type | 'A' |
|  | answers | varchar2(500) |  |  |  | DNS回答记录 base64字符串 | 'ZmVlLmljYmMuY29tLmNuLgk5MDAJSU4JQQkyMTkuMTQyLjkxLjE4Ngo=' |
|  | query\_time | number(4) |  |  |  | 查询用时 单位ms | 5 |
|  | msgsize | number(4) |  |  |  | DNS响应大小，单位字节 | 432 |
|  | monitor | varchar2(100) |  |  |  | 拨测探针/客户端IP | '36.99.184.104' |
|  | dns\_ip | varchar2(100) |  |  |  | 目标工行权威域名服务器IP | '60.247.99.245' |
|  | collect\_time | number(15) |  |  |  | 拨测时间 | 1669814092000 |
|  | answer\_num | number(3) |  |  |  | DNS回答个数 | 1 |
|  | nxd\_1 | number(3) |  |  |  | 一阶段测量响应时延，需要直接求平均值 | ';8;8;16;3;8' |
|  | adns\_2\_latency | number(4) |  |  |  | 二阶段测量响应时延，需要直接求平均值 | ';28;15;28;16;15' |
|  | ips | varchar2(100) |  |  |  | 目标待测域名解析出的IP地址 字符串，一次查询可能有多个 | '219.142.91.186;' |
|  | collect\_date | date |  |  |  | 拨测日期 | '2022-11-30' |

**环境要求**

精简版linux系统会发现没有dig命令，这时系统需要安装dig相关工具

|  |
| --- |
| Python debian系  apt-get install dnsutils  centos系 yum install bind-utils pip3 install xlrd |

**DNS拨测逻辑**

设工行有6台ADNS（权威域名服务器），和N个受监控域名。

**IPv4**

|  |
| --- |
| Python for adns in ADNS\_list:  ipdomain = clientip + 'x' + random + 'xmapsystm' + '.icbc.com.cn'#拨测端将自己的ip硬编码到域名d1(d1是字符串变量，编码规则见后文详述)  'dig ipdomain' #将拨测端硬编码域名发送到工行DNS服务器    adnsip = 'dig A adns' 命令传回ADNS的解析IP  localdns = 'dig .' 命令传回的信息最后的 ';; SERVER: ' 字段    'dig MX icbc.com.cn @adnsip' #查MX记录  'dig SOA icbc.com.cn @adnsip' #查SOA记录  'dig TXT icbc.com.cn @adnsip' #查TXT记录    #查A记录或者AAAA记录，根据IPv4和IPv6需求  for domain in domain\_list:  'dig .'\*5次  '''5次查询取平均时延。向LDNS询问根服务器的解析记录，由于LDNS一定会缓存这个记录，所以LDNS作递归查询的时间=0。phase1的最终DNS查询时间等于client和LDNS之间的网络时延。可用于检测LDNS是否宕机、不能正常提供服务'''  'dig A domain @adnsip'\*5次  '''5次查询取平均时延。直接向ADNS的IP发起DNS查询，ADNS的递归查询时间=0。phase2的最终DNS查询时间等于client和ADNS之间的网络时延。可用于检测ADNS是否宕机、不能正常提供服务。'''  'dig A domain'  '''模拟真实用户因业务查询工行域名，phase3的最终DNS查询时间。可用于检测工行的DNS解析服务（包括CDN厂商的DNS服务器）质量。'''    sleep 300秒（目前测量粒度是300秒） |

**IPv6**

|  |
| --- |
| Python for adns in ADNS\_list:  ipdomain = clientip + 'x' + random + 'xmapsystm' + '.icbc.com.cn'  'dig ipdomain'     adnsip = 'dig AAAA adns' 命令传回ADNS的解析IP  localdns = 'dig .' 命令传回的信息最后的 ';; SERVER: ' 字段    'dig MX icbc.com.cn @adnsip'   'dig SOA icbc.com.cn @adnsip'   'dig TXT icbc.com.cn @adnsip'       for domain in domain\_list:  'dig .'\*5次  'dig AAAA domain @adnsip'\*5次  'dig AAAA domain'    sleep 300秒（测量粒度是300秒） |

**拨测端IP硬编码到域名 编码规则**

示例1：2409:8c28:2808:4:800:0:0:52x8478xmapsystm.icbc.com.cn

示例2：222-12-8-145x1998xmapsystm.icbc.com.cn

前三种颜色用 'x' 字符分割，因为IPv6地址中不存在 'x'，可防止分隔字符串时出现问题/

2409:8c28:2808:4:800:0:0:52 和 222-12-8-145：硬编码的IPv6地址和IPv4（v4地址要把'.'改为'-'，因为'.'是DNS域名系统的官方分隔符，会引起DNS服务器歧义）

8478：随机值，任意长度都可以，示例里是4位随机值

mapsystm：硬编码关键词，作为工行权威服务器端的日志提取关键词

icbc.com.cn：工行父域名

**拨测收集数据**

**IPv4**

|  |
| --- |
| Python for adns in ADNS\_list:  ipdomain = clientip + 'x' + random + 'xmapsystm' + '.icbc.com.cn'  'dig ipdomain' #拨测端无需收集数据    adnsip = 'dig A adns' 命令传回ADNS的解析IP  localdns = 'dig .' 命令传回的信息最后的 ';; SERVER: ' 字段    'dig MX icbc.com.cn @adnsip' # 对应数据库表 mx\_query  'dig SOA icbc.com.cn @adnsip' # 对应数据库表 soa\_query  'dig TXT icbc.com.cn @adnsip' # 对应数据库表 txt\_query    for domain in domain\_list:  #每循环一次 记录一条数据，对应数据库表 a\_query  'dig .' \*5次 #5次查询取平均时延。对应数据库表 a\_query 的 nxd\_1 字段  'dig A domain @adnsip' \*5次 #5次查询取平均时延。对应数据库表 a\_query 的 adns\_2\_latency 字段。  'dig A domain' # 对应数据库表 a\_query 的 query\_time 字段    sleep 300秒（目前测量粒度是300秒） |

**IPv6**

|  |
| --- |
| Python for adns in ADNS\_list:  ipdomain = clientip + 'x' + random + 'xmapsystm' + '.icbc.com.cn'  'dig ipdomain' #拨测端无需收集数据    adnsip = 'dig AAAA adns' 命令传回ADNS的解析IP  localdns = 'dig .' 命令传回的信息最后的 ';; SERVER: ' 字段    'dig MX icbc.com.cn @adnsip' # 对应数据库表 mx\_query\_v6  'dig SOA icbc.com.cn @adnsip' # 对应数据库表 soa\_query\_v6  'dig TXT icbc.com.cn @adnsip' # 对应数据库表 txt\_query\_v6    for domain in domain\_list:  #每循环一次 记录一条数据，对应数据库表 aaaa\_query\_v6  'dig .' \*5次 #5次查询取平均时延。对应数据库表 aaaa\_query\_v6 的 nxd\_1 字段  'dig AAAA domain @adnsip' \*5次 #5次查询取平均时延。对应数据库表 aaaa\_query\_v6 的 adns\_2\_latency 字段  'dig AAAA domain' # 对应数据库表 aaaa\_query\_v6 的 query\_time 字段    sleep 300秒（目前测量粒度是300秒） |