内容分发网络技术要求 日志留存

1 范围

本文件规定了内容分发网络（CDN）日志留存的留存场景、留存内容、日志查询要求、技术性能要求及安全保密要求。

本文件适用于基础电信运营企业、CDN服务提供商对CDN业务的日志留存以及行业监管部门对日志留存信息的查询、溯源。

2 规范性引用文件

本文件没有规范性引用文件。

3 术语和定义

下列术语和定义适用于本文件。

3.1

数据流 data flow

源IP、目的IP、源端口、目的端口均相同，速率大于1帧/秒且持续时间大于10秒的数据流量。

4 缩略语

下列缩略语适用于本文件。

CDN	内容分发网络	Content Delivery Network
DNS	域名系统	Domain Name System
GSLB	全局负载均衡集群	Global Server Load Balancer
IDC	互联网数据中心	Internet Data Center
IP	互联网协议	Internet Protocol

5 日志留存场景

5.1 概述

依据CDN不同场景下的日志留存内容不同，CDN留存日志分为访问日志、调度日志、回源日志和系统日志四类。其中：

-- 调度日志包括DNS域名解析日志、应用层重定向调度日志。

-- 系统日志包括系统操作日志、系统运行日志。

CDN日志留存示意图如图1所示。

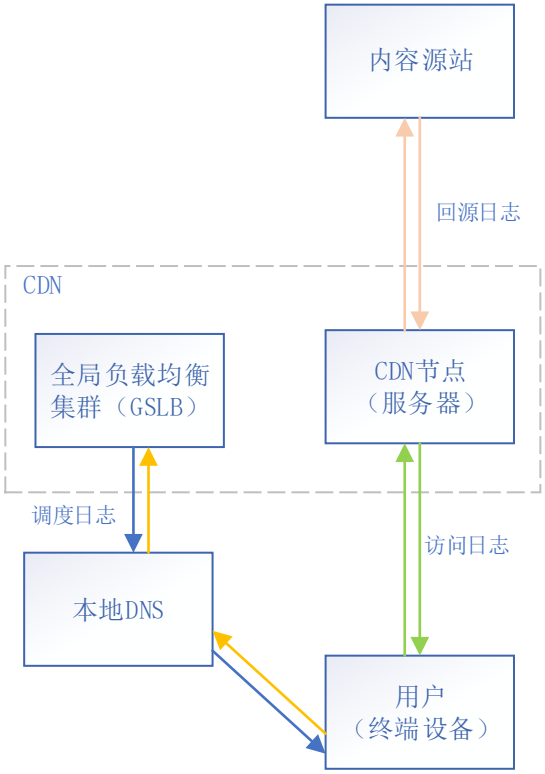

图1　CDN 日志留存示意图

5.2　访问场景

用户向CDN最佳访问节点发送请求内容，CDN最佳访问节点将用户请求内容传送给用户终端设备，该过程产生的日志为访问日志。

访问场景如下：

a）用户输入要访问的网站域名；

b）终端设备向本地DNS服务器请求对该域名的解析；

c）若本地DNS服务器中缓存有该域名的解析结果，则直接响应用户的解析请求，响应地址为CDN最佳访问节点的IP地址；

d）用户向CDN最佳访问节点发送请求内容；

e）CDN最佳访问节点将用户请求内容传送给用户终端设备。

5.3　调度场景

全局负载均衡集群（GSLB）接收到通过别名记录（CNAME）机制转发来的DNS请求，进行调度决策，最终将最佳CDN访问节点的IP地址送达用户所在地的DNS服务器，该过程产生的日志为调度日志。

调度场景：

a）用户的域名解析请求被发往本地DNS服务器，经过迭代解析后，回到该域名的注册服务器进行解析；

b）该URL所属主体的DNS解析服务器通过别名记录（CNAME）机制将用户的域名解析请求解析到另一个域名，而这个域名最终会被指向CDN全局负载均衡集群（GSLB）；

c) 负载均衡集群具有智能调度决策功能，为用户提供最佳的CDN访问节点，该节点的IP地址会送达用户所在地的DNS服务器；
d) 本地DNS服务器将CDN最佳访问节点的IP地址返回给用户，用户根据IP地址来访问该节点完成业务流程。

5.4 回源场景

CDN 节点向内容源站发出请求，并从内容源站获取最新数据，更新本地缓存，该过程产生的日志为回源日志。

回源场景：

a) 当用户访问某一个URL时，被解析的CDN节点判断缓存数据是否过期，若缓存数据没有过期，则直接将缓存数据返回给用户；
b) 如果该CDN节点没有缓存相应的内容，或者该内容的缓存已经到期，该CDN节点则向内容源站发出回源请求，从内容源站获取最新数据，更新本地缓存，并将最新数据返回给用户。

6 日志留存内容

6.1 访问日志

CDN节点应记录用户发起的访问请求信息，并生成用户访问日志。访问日志留存内容见表1。

访问日志留存内容包括：

a) 对于可通过传输层协议或应用层协议头信息区分会话特征的数据流量，以会话为单位记录访问日志，记录信息至少应包括源 IP、目的 IP、源端口、目的端口、访问开始时间、访问结束时间、用户访问 URL；
b) 对于采用加密方式的会话，记录的访问日志应至少包括源 IP、目的 IP、源端口、目的端口、访问开始时间、访问结束时间；
c) 对于无法通过传输层协议或应用层协议报文头内容区分会话特征的数据流量，应以数据流为单位记录访问日志，记录信息至少应包括源 IP、目的 IP、源端口、目的端口、访问开始时间、访问结束时间。

表1 访问日志留存内容

字段名称	说明
源 IP	发起访问请求的用户的源 IP 地址
目的 IP	发起访问请求的用户的目的 IP 地址
源端口	发起访问请求的用户的源端口
目的端口	发起访问请求的用户的目的端口
用户访问 URL	浏览类协议的访问需留存
访问开始时间	起始时间，精确到秒
访问结束时间	结束时间，精确到秒

6.2 调度日志

6.2.1 DNS 域名解析日志

DNS域名解析日志留存内容至少应包括请求处理时间、请求源IP、目标域名、解析结果、生存时间，见表2。

表2　DNS 域名解析日志留存内容

字段名称	说明
请求处理时间	接收到域名解析请求的时间戳
请求源 IP	发起 DNS 解析的源 IP 地址
目标域名	需要进行解析的目标域名
解析结果	返回给用户的域名解析结果
生存时间（TTL）	域名解析的生命周期

6.2.2　重定向调度日志

应用层重定向调度日志留存内容至少应包括请求处理时间、用户 IP 地址、用户请求 IP 地址、用户请求 URL、重定向 IP、重定向 URL，见表 3。

表3　应用层重定向调度日志留存内容

字段名称	说明
请求处理时间	接收到重定向请求的时间戳
用户 IP 地址	发起请求的用户的源 IP 地址
用户请求 IP 地址	用户请求的目的 IP 地址
用户请求 URL	用户请求的目标 URL
重定向 IP	重定向的目标 IP 地址
重定向 URL	返回给用户的重定向后的 URL

6.3　回源日志

当下级节点向汇聚节点或内容中心发起回源请求时，节点应根据回源信息生成回源日志。

回源日志留存内容至少应包括源IP地址、源端口、目的IP地址，目的端口、访问开始时间、访问结束时间、用户访问URL、业务类型（可选），见表4。

表4　回源日志留存内容

字段名称	说明
源 IP 地址	本次请求回源使用的源 IP 地址
源端口	本次请求回源使用的源端口
目的 IP 地址	本次请求回源访问的目的 IP 地址
目的端口	本次请求回源访问的目的端口
访问开始时间	起始时间，精确到秒
访问结束时间	结束时间，精确到秒
用户访问 URL	浏览类协议需要留存
业务类型（可选）	业务类型：音/视频、文本等

6.4　系统日志

6.4.1　系统操作日志

系统操作日志留存内容至少应包括：用户名、用户IP地址、操作描述、操作结果、日志等级、操作时间。

系统操作日志留存内容见表5。

表5　系统操作日志留存内容

字段名称	说明
用户名	需要查看的用户的名称
用户 IP 地址	需要查看的用户的 IP 地址
操作描述	描述该用户进行的操作
操作结果	描述用户执行该操作后的结果
日志等级	需要查看的日志的级别 日志级别由高到低为：关键、重要、普通
操作时间	需要查看的日志的操作时间

6.4.2　系统运行日志

系统运行日志留存内容至少应包括：服务器ID、服务器IP、应用软件版本号、操作系统版本号、告警等级。

系统运行日志留存内容见表6。

表6　系统运行日志留存内容

字段名称	说明
服务器 ID	系统所属服务器唯一标识
服务器 IP	系统所属服务器 IP 地址
应用软件版本号	应用软件版本号
操作系统版本号	操作系统版本号
告警等级	告警级别由高到低为：严重、普通

7　日志留存查询要求

7.1　访问日志

7.1.1　查询方式

访问日志查询方式见表 7。其中，“M”为必须支持，“O”为可选支持。

表7　访问日志留存查询方式

访问日志留存查询方式	属性	查询流程
源IP地址、查询时间	M	7.1.2.1
源IP地址、目的IP地址、查询时间	M	7.1.2.2
源IP地址、用户访问URL、查询时间	M	7.1.2.3
源IP地址、用户访问URL、目的IP地址、查询时间	M	7.1.2.4
目的IP地址、查询时间	M	7.1.2.5
用户访问URL、查询时间	M	7.1.2.6
目的IP地址、用户访问URL、查询时间	M	7.1.2.7
注：查询时间指明确起止时间点的查询时段（单次查询的时间跨度以不大于30分钟为宜）。		

7.1.2　查询流程

7.1.2.1　源 IP 地址+查询时间

用户访问日志查询采用“源IP地址+查询时间”组合查询方式，查询流程见图2。

源IP地址+查询时间组合查询流程如下：

a) 用户源IP地址+查询时间组合查询留存日志信息；

b) 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：目的IP地址、目的端口、用户访问URL、访问开始时间、访问结束时间。

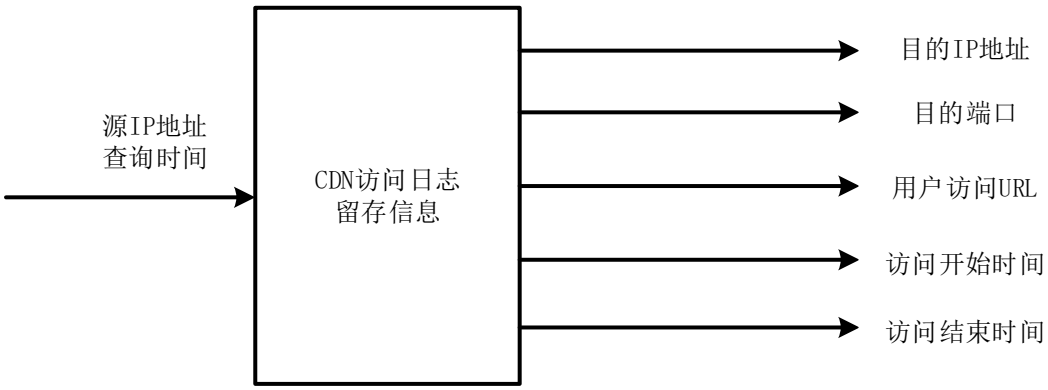

图2 源 IP 地址+查询时间组合查询流程图

7.1.2.2 源 IP 地址+目的 IP 地址+查询时间

用户访问日志查询采用“源IP地址+目的IP地址+查询时间”组合查询方式，查询流程见图3。

源IP地址+目的IP地址+查询时间组合查询流程如下：

a) 用户源IP地址+目的IP地址+查询时间组合查询留存日志信息；

b) 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：用户访问URL、源端口、目的端口、访问开始时间、访问结束时间。

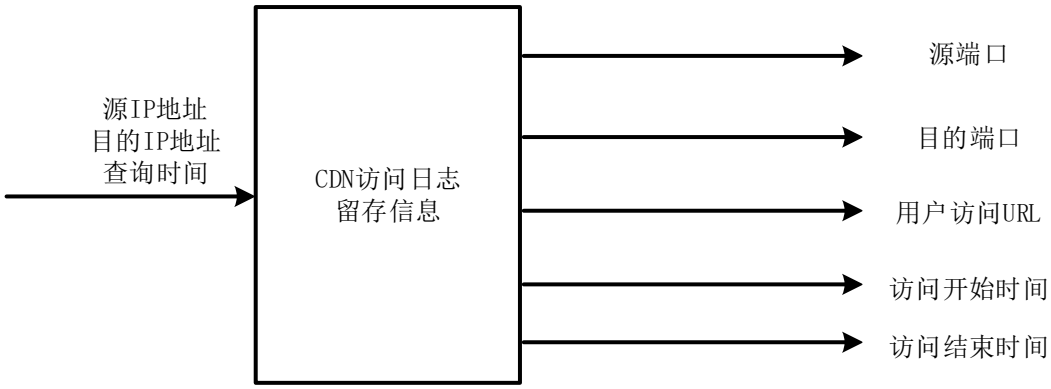

图3 源 IP 地址+目的 IP 地址+查询时间组合查询流程图

7.1.2.3 源 IP 地址+用户访问 URL+查询时间

用户访问日志查询采用“源IP地址+用户访问URL+查询时间”组合查询方式，查询流程见图4。

源IP地址+用户访问URL+查询时间组合查询流程如下：

a) 用户源IP地址+目的IP地址+查询时间组合查询留存日志信息；

b) 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：目的IP地址、目的端口、源端口、访问开始时间、访问结束时间。

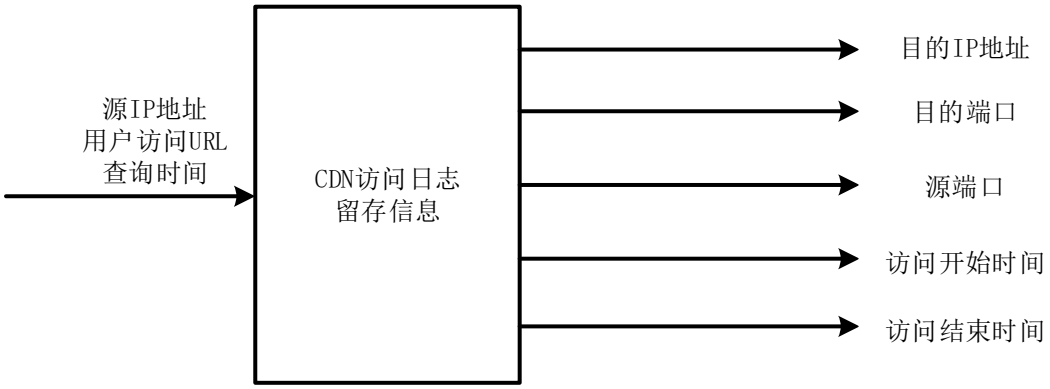

图4　源 IP 地址+用户访问 URL+查询时间组合查询流程图

7.1.2.4　源 IP 地址+用户访问 URL+目的 IP 地址+查询时间

用户访问日志查询采用“源IP地址+目的IP地址+用户访问URL+查询时间”组合查询方式，查询流程见图5。

源IP地址+目的IP地址+用户访问URL+查询时间组合查询流程如下：

a)　用户源IP地址+目的IP地址+用户访问URL+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：目的端口、源端口、访问开始时间、访问结束时间。

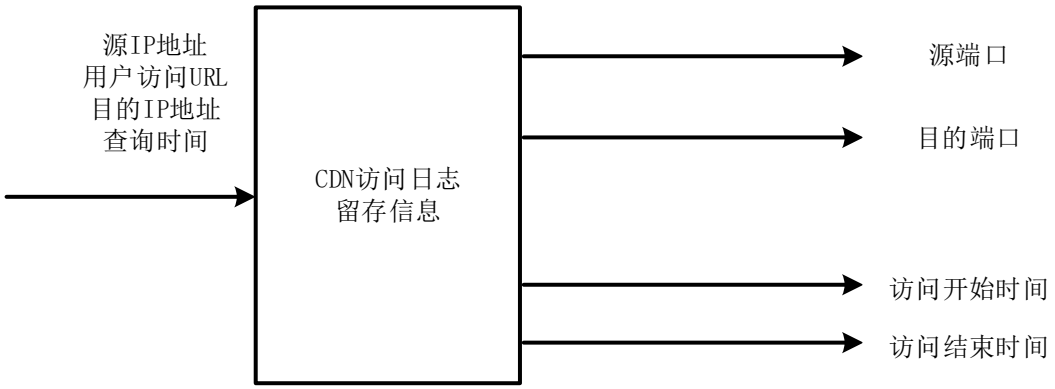

图5　源 IP 地址+用户访问 URL+目的 IP 地址+查询时间组合查询流程图

7.1.2.5　目的 IP 地址+查询时间

用户访问日志查询采用“目的IP地址+查询时间”组合查询方式，查询流程见图6。

目的IP地址+查询时间组合查询流程如下：

a)　用户目的IP地址+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：源IP地址、目的端口、用户访问URL、访问开始时间、访问结束时间。

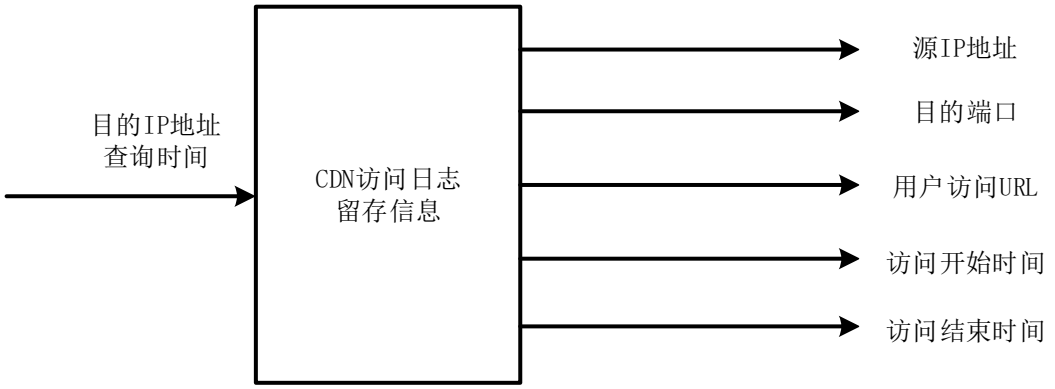

图6　目的 IP 地址+查询时间组合查询流程图

7.1.2.6　用户访问 URL+查询时间

用户访问日志查询采用“用户访问URL+查询时间”组合查询方式，查询流程见图7。

用户访问URL+查询时间组合查询流程如下：

a)　用户访问URL +查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：源IP地址、目的端口、目的IP地址、访问开始时间、访问结束时间。

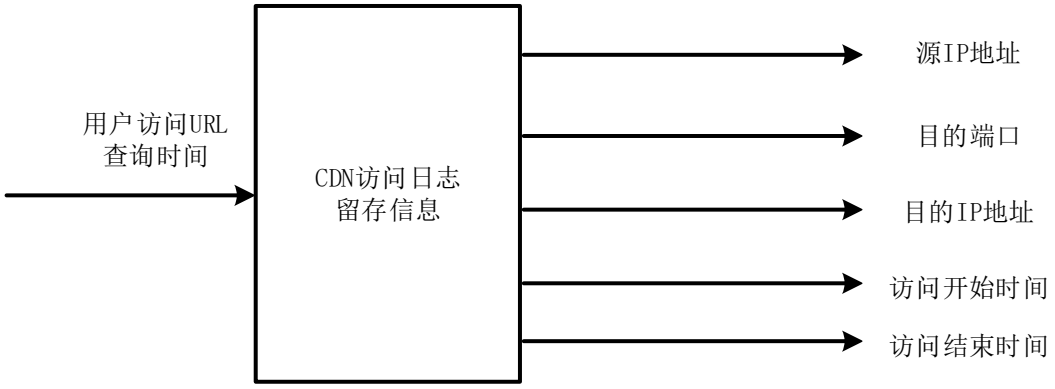

图7　用户访问 URL+查询时间组合查询流程图

7.1.2.7　目的 IP 地址+用户访问 URL+查询时间

用户访问日志查询采用“用户访问URL+目的IP地址+查询时间”组合查询方式，查询流程见图8。

用户访问URL+目的IP地址+查询时间组合查询流程如下：

a)　用户访问URL+目的IP地址+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：源IP地址、目的端口、访问开始时间、访问结束时间。

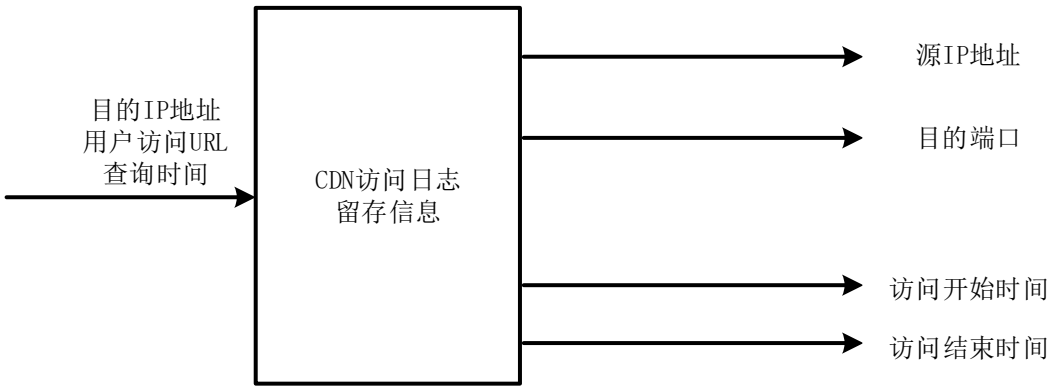

图8　目的 IP 地址+用户访问 URL+查询时间组合查询流程图

7.1.3　查询要求

查询用户访问日志留存信息时，应在2小时后可对用户访问日志信息进行查询，查询时间跨度不超过30分钟，且查询响应时间不大于10分钟。

7.2　调度日志

7.2.1　DNS 域名解析日志

7.2.1.1　查询方式

DNS 域名解析日志查询方式见表 8。其中，“M”为必须支持，“O”为可选支持。

表8　DNS 域名解析日志留存查询方式

访问日志留存查询方式	属性	查询流程
请求源IP、查询时间	M	7.2.1.2.1
请求源IP、目标域名、查询时间	M	7.2.1.2.2
请求源IP、解析结果、查询时间	M	7.2.1.2.3
请求源IP、生存时间、查询时间	M	7.2.1.2.4
目标域名、解析结果、查询时间	M	7.2.1.2.5
目标域名、查询时间	M	7.2.1.2.6
解析结果、查询时间	O	7.2.1.2.7
生存时间、查询时间	O	7.2.1.2.8
注：查询时间指明确起止时间点的查询时段（单次查询的时间跨度以不大于30分钟为宜）。		

7.2.1.2　查询流程

7.2.1.2.1　请求源 IP+查询时间

DNS域名解析日志查询采用“请求源IP+查询时间”组合查询方式，查询流程见图9。

请求源IP+查询时间组合查询流程如下：

a)　请求源IP+查询时间组合查询留存日志信息；

b） 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求处理时间、目标域名、解析结果、生存时间。

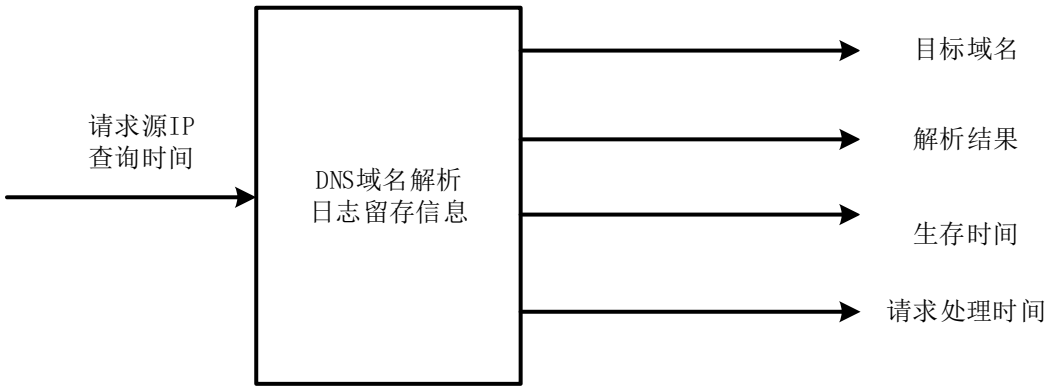

图9 请求源 IP+查询时间 流程图

7.2.1.2.2 请求源 IP+目标域名+查询时间

DNS域名解析日志查询采用“请求源IP+目标域名+查询时间”组合查询方式，查询流程见图10。

请求源IP+目标域名+查询时间组合查询流程如下：

a） 请求源IP+目标域名+查询时间组合查询留存日志信息；

b） 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求处理时间、解析结果、生存时间。

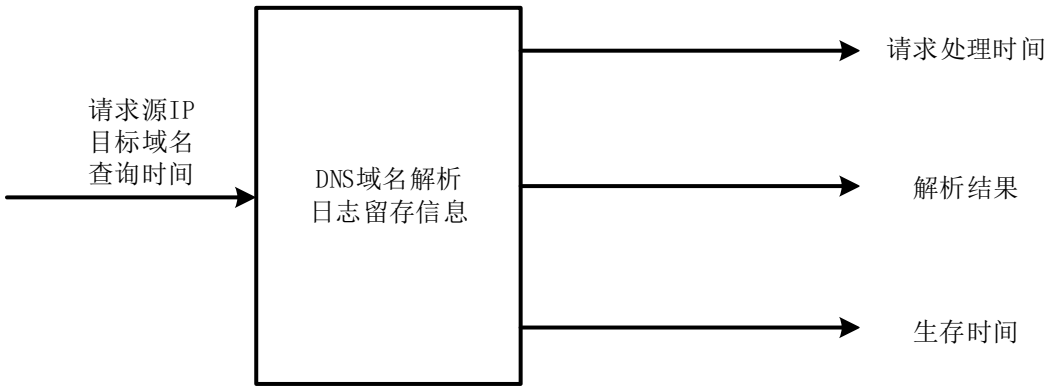

图10 请求源 IP+目标域名生存时间+查询时间组合查询流程图

7.2.1.2.3 请求源 IP+解析结果+查询时间

DNS域名解析日志查询采用“请求源IP+解析结果+查询时间”组合查询方式，查询流程见图11。

请求源IP+解析结果+查询时间组合查询流程如下：

a） 请求源IP+解析结果+查询时间组合查询留存日志信息；

b） 基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求处理时间、目标域名、生存时间。

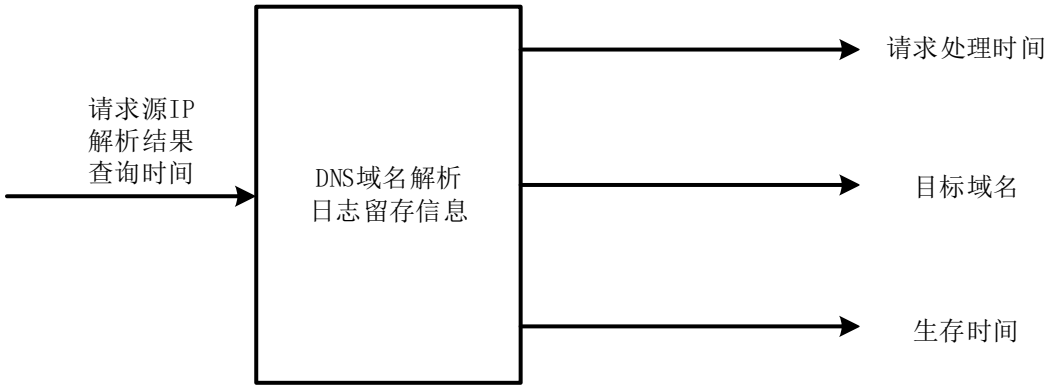

图11　请求源 IP+解析结果+查询时间组合查询流程图

7.2.1.2.4　请求源 IP+生存时间+查询时间

DNS域名解析日志查询采用“请求源IP+生存时间+查询时间”组合查询方式，查询流程见图12。

请求源IP+生存时间+查询时间组合查询流程如下：

a)　请求源IP+生存时间+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求处理时间、目标域名、解析结果。

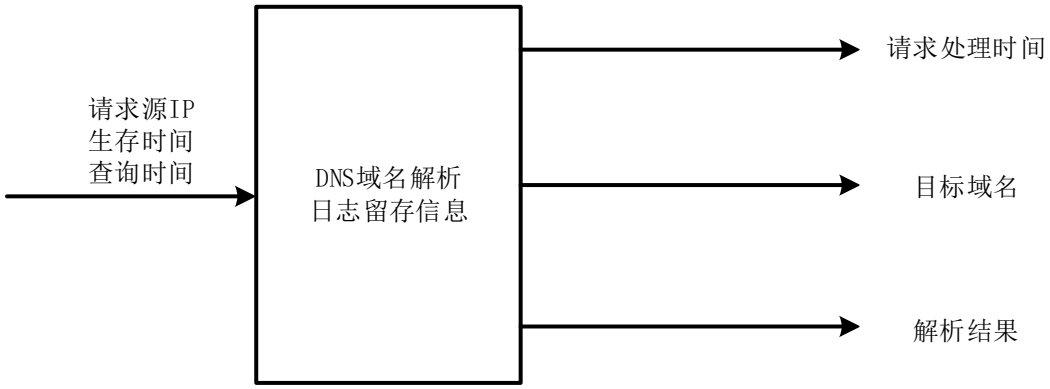

图12　请求源 IP+生存时间+查询时间组合查询流程图

7.2.1.2.5　目标域名+解析结果+查询时间

DNS域名解析日志查询采用“目标域名+解析结果+查询时间”组合查询方式，查询流程见图13。

目标域名+解析结果+查询时间组合查询流程如下：

a)　目标域名+解析结果+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求处理时间、请求源IP、生存时间。

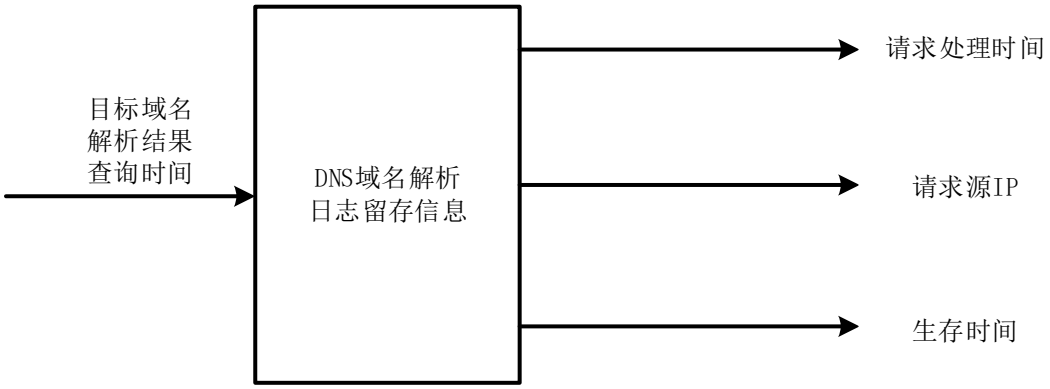

图13　目标域名+解析结果+查询时间组合查询流程图

7.2.1.2.6　目标域名+查询时间

DNS域名解析日志查询采用“目标域名+查询时间”组合查询方式，查询流程见图14。

目标域名+查询时间组合查询流程如下：

a)　目标域名+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求源IP、解析结果、生存时间、请求处理时间。

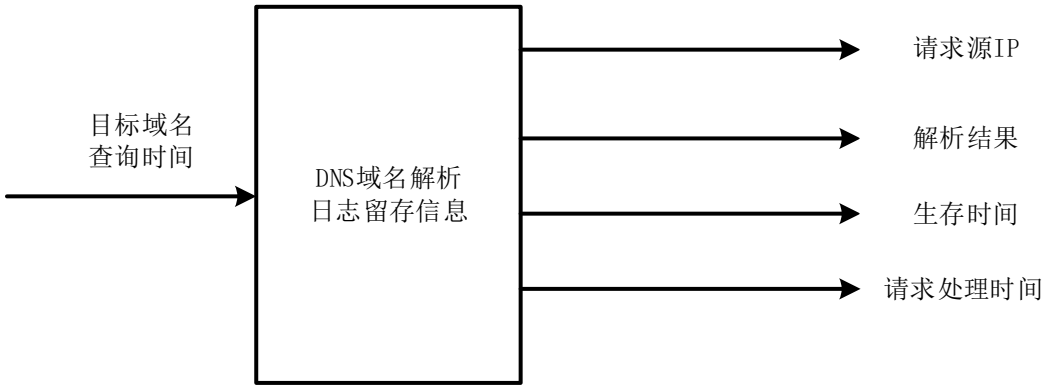

图14　目标域名+查询时间组合查询流程图

7.2.1.2.7　解析结果+查询时间

DNS域名解析日志查询采用“解析结果+查询时间”组合查询方式，查询流程见图15。

解析结果+查询时间组合查询流程如下：

a)　解析结果+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求源IP、目标域名、生存时间、请求处理时间。

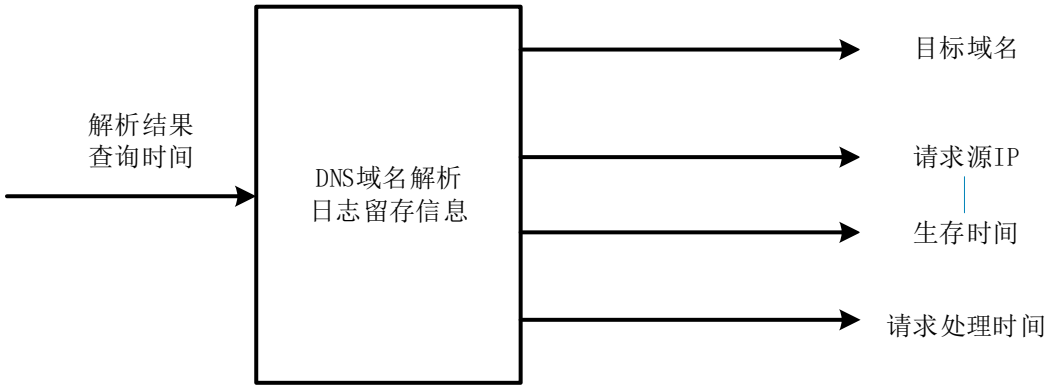

图15　解析结果+查询时间组合查询流程图

7.2.1.2.8　生存时间+查询时间

DNS域名解析日志查询采用“生存时间+查询时间”组合查询方式，查询流程如16。

生存时间+查询时间组合查询流程如下：

a)　解析结果+查询时间组合查询留存日志信息；

b)　基于该组合查询方式，用户可查询到的日志留存信息包括但不限于：请求源IP、目标域名、请求处理时间、解析结果。

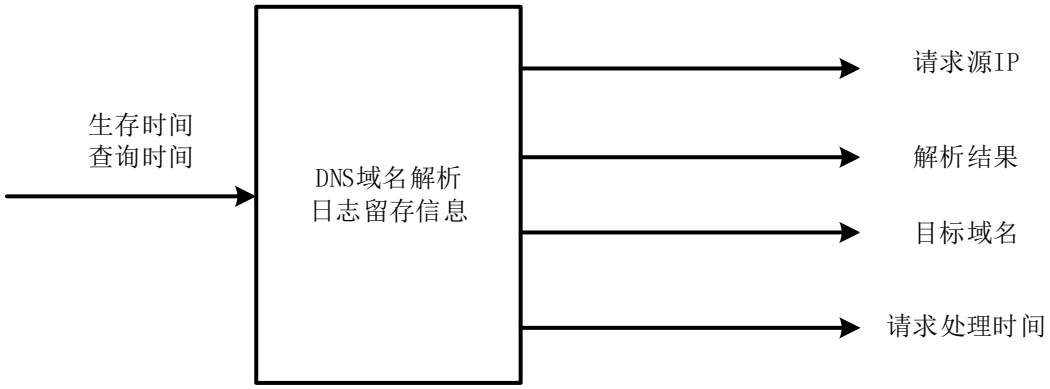

图16　生存时间+查询时间组合查询流程图

7.2.1.3　查询要求

查询DNS域名解析日志留存信息时，应在2小时后可对DNS域名解析日志信息进行查询，查询时间跨度不超过30分钟，且查询响应时间不大于10分钟。

7.2.2　重定向调度日志

7.2.2.1　查询方式

应用层重定向调度日志查询方式见表 9。其中，“M”为必须支持，“O”为可选支持。

表9　应用层重定向调度日志留存查询方式

访问日志留存查询方式	属性	查询流程