云平台DNS安全体系研究

Security Framework for Cloud DNS

宋林健/SONG Linjian，马永/MA Yong，梁卓/LIANG Zhuo
（阿里云计算有限公司，中国 北京 100102）
(Alibaba Cloud Computing Co. Ltd., Beijing 100102, China)

DOI：10.12142/ZTETJ.202301007
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20230301.1441.002.html
网络出版日期：2023-02-28
收稿日期：2022-12-05

摘要：域名系统（DNS）是互联网的基础设施服务，对数字经济发展的安全和稳定至关重要。结合阿里云DNS的安全实践，提出了适应融合云时代发展的DNS安全体系，包括全链路和融合云DNS的应用场景，DNS南北向、东西向服务接口能力，以及在数据保密性、数据一致性、服务高可用、软件质量、安全运维、服务测量等多个维度的安全能力框架。

关键词：DNS；安全体系；互联网基础设施

Abstract: The domain name system (DNS) is the infrastructure service of the Internet and is crucial to the continuous security and stability of the digital economy. Based on the security practice of Alibaba Cloud DNS, a DNS security framework suitable for the development of a converged cloud era is proposed, including the application scenarios of the all-link and converged cloud DNS, the south-north and east-west service interface capabilities of DNS, as well as a security capability framework in multiple dimensions such as confidentiality, Integrity, availability, software quality, operation, and service measurement.

Keywords: DNS; security framework; Internet infrastructure

互联网域名系统（DNS）提供了互联网域名和互联网协议（IP）地址两种网络标识符体系之间的衔接转换。随着新技术新场景新模式的涌现，企业信息架构在持续升级，数字化建设朝着云管边端一体化演进，万物互联格局已然显现。有IP的地方就有DNS寻址。寻址的形态渗透在云管边端各个场景中，从以南北流量为主的互联网通用互联场景到以东西流量为主的企业机房场景，再到云技术服务的云内IP寻地和多云的云间寻址。作为互联网的中枢神经，DNS在网络安全和企业数字化治理体系中扮演至关重要的角色，例如：2021年6月，美国政府要求域名注册局对36个伊朗媒体域名进行“查封”[1]，引起了国际社会的关注。2021年10月，Facebook DNS服务不可用导致其旗下很多应用发生了故障，持续了6个多小时[2]。“十四五”是中国推进信息通信行业高质量发展、建设网络强国和数字中国的关键时期，DNS作为核心网络基础设施的重要地位也正在得到业界愈发广泛的认可。

随着互联网发展和技术演进，DNS技术和产品形态不断丰富，机遇与挑战并存。一方面，通过安全扩展协议和新技术的引入，DNS不断增强安全能力。互联网工程任务组（IETF）不断发布新的DNS安全扩展协议，从底层协议标准层面完善DNS安全，如DNS Cookie、DNS安全扩展（DNSSEC）。加密传输技术开始广泛应用在DNS领域，增强了数据一致性和隐私保护。进入现代的互联网时代，新型的移动互联网服务模式为DNS提供了新的服务架构，大型云计算平台为DNS服务提供了全链路自研的更可控的服务、更高的弹性、更高的可用能力，以及更及时的软件和服务漏洞更新。新技术、新模式提高了DNS抗攻击的安全加固能力。

另一方面，进入云计算时代，云平台DNS的服务架构和形态正在发生变化，以适应复杂的多应用场景的互联互通和新业务形态的规模化增长。尤其是在多云异构的融合场景下，DNS成为部署在公有云、私有云、本地互联网数据中心（IDC）、应用和智能终端等多场景的IP地址寻址和统一调度平台服务。这对DNS软件质量、安全运维和体系化服务能力提出了新的挑战。

1 DNS的演进和各阶段特征

1.1 网络协议和分布式IP数据库

传输控制协议（TCP）/IP被发明并普及后，互联网规模迅速扩展。基于Host.txt集中式的名字解析已无法满足日益扩大的网络规模和主机名字解析的需要。20世纪80年代初，为了解决名字解析服务的扩展性问题，DNS的基本概念和实现框架（RFC882/883）被提出。DNS引入了树状的域名空间，按照分层的域名结构划分管理域，数据和管理权限的下

放实现了分级的分布式结构。该时期，DNS支撑了TCP/IP初期的互联网商业化。

在该阶段，作为网络基础组件和协议，DNS提供了分布式“查询-响应”的IP查找。域名拥有者或网络管理员在自己的网络中独立部署和运行DNS解析服务，并依赖开源的DNS软件，如BIND（软件名）。该阶段，DNS安全能力依赖于DNS协议的安全和开源DNS软件的质量，任何DNS协议漏洞或开源DNS软件的漏洞都会影响DNS服务。所以该时期大部分DNS安全的讨论集中在DNS协议标准层面，例如DNS安全扩展（DNSSEC）。但DNSSEC安全扩展协议未能快速进行全球部署，一些例如DNS劫持之类的安全风险到今天仍然普遍存在[5]。

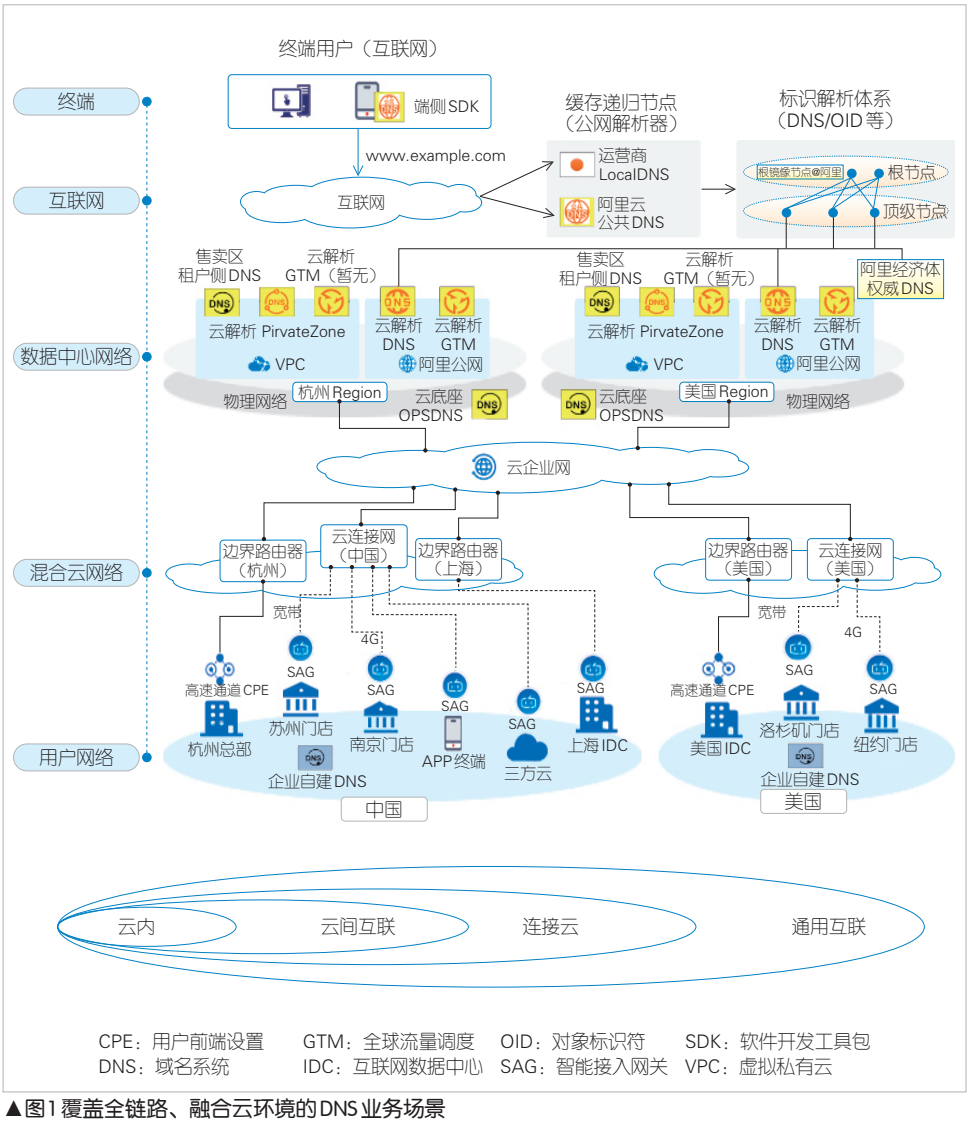
1.2 平台型IP寻址和流量调度服务（SaaS/PaaS）

随着移动互联网、在线视频服务的兴起，金融、民生、政务等重要行业加速了数字化进程，通用DNS IP解析功能已无法满足不同应用的性能、功能和安全需求。DNS服务对象和服务部署模式发生了改变：用户从PC转移到智能手机、智能终端物联网（IoT）；应用服务开始共享超大型第三方公共域名解析平台，并出现了超过百万级别的DNS权威解析托管服务，如Amazon Route 53、Alibaba Cloud DNS；公共递归DNS的出现也让用户流量集中在少数DNS递归服务平台，如Google的8.8.8.8和Cloudflare的1.1.1.1。

从业务功能上看，DNS不仅是一个简单查询静态的域名IP地址库，更是一个基于用户位置、资源状态、容灾等需求的动态智能的流量调度系统。从业务形态上看，DNS不再只是网络协议和基础组件，而是面向业务和应用，对外提供软件即服务（SaaS）或应用程序编程接口（API）的平台即服务（PaaS），具有更强的智能化、安全性和可扩展性。大型企业和云平台将更多的网络、研发运维资源投入到DNS服务，增强了服务的高可用和安全性。从全球范围来看DNS的故障变少了，但少数的故障的影响却更大了。平台型DNS的稳定和高可用仍然是挑战。

1.3 融合云DNS：面向IT数字资产的DNS融合管理架构

针对信息技术（IT）数字资产，出于服务高可用、风险控制和数据治理的考虑，越来越多的企业采用融合云部署的方式，即将企业的数字化业务资产同时部署在公有云、私有云、本地IDC、应用和智能终端等多场景（如图1所示）。在融合云场景下，IT数字资产高效管理和运维成为一个痛点。融合云DNS也应运而生，开始承担面向融合云的IT数字资产融合管理的角色。用户可以跨平台地统一管理、配置、维护DNS，达到统管、统维、统防的目标。



▲图1 覆盖全链路、融合云环境的DNS业务场景

在该阶段，平台型DNS企业已经具备全链路解析资源和信息，包括APP/智能终端解析器、递归解析、云上/云下权威解析、网络质量探测，提供DNS全链路安全可控的服务，同时，平台型DNS企业还采用IT视角用软件定义DNS服务，提供端-递归-权威融合的云端一体技术架构，摆脱了DNS协议固有安全限制。

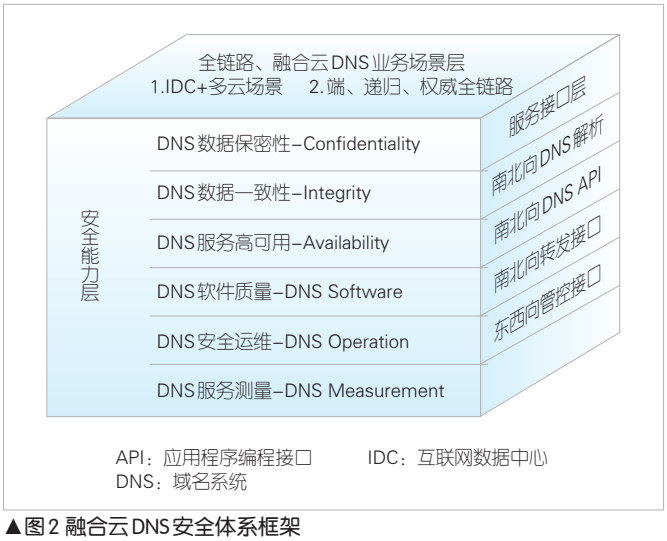
2 融合云DNS安全体系研究

结合该领域的相关工作和阿里云在融合云DNS方面的实践，我们提出了一个融合云DNS安全体系框架，如图2所示。该框架具体包括全链路的融合云DNS业务场景层、DNS业务服务接口层，以及最重要的安全能力层。融合云DNS的安全能力应该充分考虑南北向、东西向的业务和管控接口，覆盖多个融合云DNS业务场景。

2.1 DNS数据保密性

近年来，人们也提高了对DNS的关注度。如RFC9076所描述，DNS甚至被认为是互联网隐私泄露最严重的领域。传统DNS协议没有专门的安全机制来保障隐私安全。DNS查询响应数据揭示了特定用户和设备访问的网络行为，包括所访问域名和和位置信息。参考文献[11]指出，IoT设备会查询少数固定的域名，而DNS查询数据包信息的泄露会暴露智能的厂家、信号以及潜在的设备漏洞。

针对DNS隐私的安全防护，目前有两种基本思路：一种是尽量减少对外发送的信息，如RFC7816中提到的QNAME Minimization技术，该技术可以通过递归服务器修改查询的名字，以达到减少信息泄露的目的；另一类是将DNS数据通过安全传输层协议（TLS）加密信道进行传输，以达到数据隐私保护的效果，例如RFC7858中提到的基于TLS的DNS（DoT）、RFC8484中提到的基于安全超文本传送协议的DNS（DoH）。近几年，业界主流的浏览器、操作系统平台都已对外宣布支持DoT和DoH。



▲图2 融合云DNS安全体系框架

另外，在融合云场景下，除了DNS查询过程中的数据具有保密性以外，有研究表明DNS zone数据也可能包含敏感信息，因此也需要考虑数据保密性[12]。例如，在递归、权威服务器存储、与多个服务器通过完全区域传输（AXFR）/增量区域传输（IXFR）同步zone数据场景下，zone数据信息都有可能被泄露。因此，在融合云DNS设计和使用中，需要充分考虑必要的传输和存储的加密，为各个功能接口和应用场景预留DNS数据保密能力。

针对DNS数据保密性，仍有如下的3个方面内容需要进一步关注：

1）除了静态配置服务外，如何在家庭、企业不同场景下支持动态DoH/DoT地址和加密证书服务发现机制。目前，IETF的ADD工作组正在讨论制定新的技术标准。

2）当DNS递归成为数据加密传输的中心化节点后，如何保证递归服务商不泄露数据。曾经有Oblivious DNS和Oblivious DoH（ODoH）方案，隔离查询域名和用户地址的对应关系，但是并没有得到技术社群的一致认可。

3）递归-权威的加密传输机制研究。递归需要在面对大量权威服务器具备加密证书服务发现的能力。

2.2 DNS数据一致性

DNS协议固有的缺陷会使DNS易遭受缓存数据篡改，从而引导用户访问攻击者设置的恶意网站和文件内容。典型的有Kaminsky攻击[13]，以及2020年出现的因DNS侧信道漏洞带来的缓存“投毒”[14]。早在2000年，DNSSEC的概念被提出，旨在通过携带签名保障数据传输的一致性和可验证性。然而，直到2023年1月，全球递归支持DNSSEC校验的比例仅有31%。

除了缓存投毒攻击以外，数据一致性的安全风险也会发生在数据源头。网络黑客可以攻陷域名注册账号，通过域名注册商平台直接给DNS zone文件注入恶意数据，这类攻击也被称为“注册劫持”。例如：2019年发生的海龟攻击[16]，即攻击者通过系统漏洞获取用户权限后，恶意篡改用户的DNS注册信息。在融合云环境中，需要引入“域名注册锁”或者双因子认证机制来保护DNS注册信息不被攻击者单方面篡改。

DNS数据一致性的挑战在于：DNSSEC由于其复杂性难以大规模部署，也没有新的签名保障机制。另外，由于大规

模量子计算的发展，现在广泛使用的加密算法如RSA（算法名）和椭圆曲线加密（ECC）会更容易破解。因此，我们需要考虑量子安全算法的研究，以进行快速替换。更大的密钥和签名可能会给现有的DNSSEC和DNS数据的传输带来挑战。

2.3 DNS服务高可用

DNS是互联网基础服务，在互联网业务的高可用和稳定性方面起到至关重要的作用。互联网中心化的趋势也体现在DNS领域中，因此越来越多的网络应用与服务共享超大型第三方公共域名解析平台。研究表明，在全球排名前10万的流行域名之中，有89%的域名使用了公共域名解析服务[3-4]。为了高效管理，基于云平台的DNS域名托管服务往往为其托管的大量域名配置共用的解析服务和统一的安全策略。一旦域名托管服务遭遇大型分布式拒绝服务（DDoS）攻击，则会导致服务不可用[17]。还有一些研究表明，域名托管服务所管理的域名存在被攻击者接管的风险[9-10]。因此，平台型DNS需要具备应对各种故障的弹性能力，以提供极致的高可用服务，也就是说能够在任意时间、任何地方都能提供间断的服务。

DNS的高可用能力可以从表1中的7个方面来加强。

2.4 DNS软件质量

《“十四五”软件和信息技术服务业发展规划》要求强化基础组件供给，推进域名、标识等基础资源管理与服务的软件研发。然而，中国仍有不少企业和网络运维人员使用和集成其他国家开源软件，为国家数字经济基础设施安全带来潜在软件供应链安全风险。

中国互联网信息中心2021年发布的《中国域名服务安全状况与态势分析报告》[8]指出，中国二级以下权威域名服务器主要使用互联网系统联盟（ISC）维护的开源软件BIND，占比达到59%。其中，超过40%的BIND开源软件仍旧开启版本应答功能，为漏洞扫描和针对性攻击留下安全隐患。据互联网安全大会（ISC）官网统计，2016—2021年的5年，BIND共有69个软件bug被曝出，仅2022年就新增11个软件漏洞，这些漏洞主要为DDoS安全威胁漏洞[18]。

大型的商业化DNS公司和机构出于高性能和高安全性的考虑，都会专注于自主研发DNS软件和安全测试技术。这样可以在保障DNS软件质量的同时，在遇到问题时能够快速定位软件故障并进行服务恢复。为了缓解一款软件带来的质量和安全风险，企业通常也会考虑采用至少两个不同开发者的DNS软件来增加系统的多样性[20]，避免单一软件可能带来的漏洞，但相应的代价是需要增加运营和维护成本。总归DNS软件的质量对服务安全至关重要。

DNS软件安全风险主要体现在两个方面：一方面，从软件开发的角度看，很难100%保证软件没有漏洞。对此，业界有通用的软件自动化测试方法，例如Fuzz测试和symbolic测试，但是它们很难对复杂的语意和交互式行为的DNS软件进行可扩展的测试。另一方面，从网络通信软件方面看，DNS软件的实现需要严格遵守协议，对于协议定义不明确的领域DNS软件，要考虑安全异常的情况。目前，业界有不少针对域名协议的安全漏洞分析，如缓存投毒、DNSSEC等。然而，对于域名协议的载体、域名解析软件实现代码的安全性和正确性研究工作不多，在最近一两年才逐渐引起研究者的重视[19]。

2.5 DNS安全运维

超大规模的分布式、平台型的DNS安全运维是DNS服务中至关重要的一环，直接影响用户体验和服务质量。当云平台DNS进入融合云DNS阶段时，安全运维场景更加复杂。

▼表1 提升DNS高可用能力的7种方案

机制	权威	递归/缓存	需求描述
性能/资源	适用	适用	在DNS服务器处理能力和网络带宽两个方面预留足够的资源来抵御超过3～10倍的攻击流量。对于无差别网络洪泛攻击，可结合特殊的DDoS防御机制做流量清洗
多个NS	适用	不适用	权威设置多组NS，通过zone文件分发同步数据
组播Anycast	适用	适用	每个NS可以在不同的地理位置的站点通过Anycast组播机制设置镜像和备份服务器
服务检测	适用	适用	大规模的DNS服务需要对多站点部署的服务可用性进行监控，如服务器状态、业务流量、数据一致性等
缓存	不适用	适用	当某一权威服务器不可达时，可以采用本地历史或缓存数据来应答服务（RFC8767）
安全控制	适用	适用	当遭遇攻击时，可以采用RRL以及ACL安全控制等手段来减少应答长度，降低高可用风险
多样性	适用	适用	在网络部署、软件硬件选型方面充分考虑多样性，增加系统性的冗余

注：表1中的方案能够增强DNS的服务能力，但是无法百分之百保证DNS服务的高可用。在互联网中心化趋势的背景下，超大规模的DDoS攻击一直会是DNS服务可用性的挑战之一。

ACL：访问控制列表　DDoS：分布式拒绝服务　DNS：域名系统　NS：名字服务器　RRL：响应速率限制

有研究认为，大量的DNS故障来自于DNS配置变更[22]。例如：2019年，微软因NS配置变更错误导致了其在线服务全球故障，微软Azure云宕机3个小时[21]；2021年Facebook自动化运维漏洞导致了路由故障和DNS服务不可用，引起了其旗下的各种应用故障，持续6个多小时[2]。

学术和产业界都很重视DNS安全运维的研究和建设。针对潜在的运维漏洞和DNS变更故障，微软开发了GRooT工具[22]，通过分析DNS配置文件来排查潜在的DNS服务风险[22]；作为中国最大的DNS云平台，阿里云也从管理保障、设计与开发、测试与评估、发布与变更、监控与应急、基础设施保障等各方面保障DNS服务安全稳定[23]。

2.6 DNS测量

域名解析服务异常有可能隐藏在正常业务中，虽没有造成大规模故障但却存在安全隐患，因此我们需要对DNS服务进行安全测量来揭示中国乃至全球DNS运行的规律和安全风险。近期一项研究工作表明，互联网中13.5%的域名解析查询均会以失败告终[6]。另外，引发域名解析服务异常的原因不尽相同，其中包括域名权威服务器配置错误、网络通信链路存在劫持、网络中间件缓存不一致性等等[5,7]，这些都需要通过DNS安全测量来定位根因。

DNS安全测量通常有主动发探测包的主动测量和收集DNS业务数据的被动测量两种方案。但由于探测节点的广度、测量手段的局限，现有测量方法还很难还原完整的DNS解析链路全局信息。尤其是对复杂的云平台DNS，以及融合云DNS而言，当域名解析发生故障时，通常难以准确获知用户终端网络、IDC侧网络的环境信息，也难以有效排查并追溯故障原因。总之，DNS服务测量、故障定位一直是业界的难点。

3 阿里云DNS的安全实践

面对融合云DNS的发展趋势和安全挑战，阿里云在业界首次提出了全链路安全可控的融合云DNS技术。该技术不再局限于单一设备、单一服务运行场景，而是从DNS业务的全局视角出发，实现融合云环境下的统一管理、统一运维、统一防护。技术服务覆盖了公网域名解析、内网域名解析、全球流量调度、移动解析、专有云和客户IDC的域名解析场景。

为了提供高可用的永远在线解析服务，同时保障云生用户的域名解析安全稳定，阿里云DNS将安全实践主要在下面集中于以下几个方面：

1）基础资源和能力：基于阿里云全球覆盖的基础设施，阿里云在全球28个地理区域内运营着86个可用区，部署了243个DNS集群，日解析量超过2万亿次。

2）安全攻击防护：基于云计算的弹性和安全运维体保障了DNS服务的弹性和安全抗攻击能力，具备全球10T+带宽储备和多个大型流量清洗中心，提供大规模DDoS流量攻击防护。

3）自研软件：具备全链路的融合云DNS软件自研能力，能够自研高性能解析服务器集群，且单集群每秒过亿防护能力。

4）安全研究：对DNS服务异常测量、软件安全漏洞测试、正确性验证进行深入研究。

5）数据一致性：提供DNSSEC在线签名服务，避免DNS劫持/缓存投毒，保障网站访问安全。

6）数据隐私：提供了DoT、DoH和HTTP(s) DNS件开发工具包（SDK）服务，保障DNS传输的数据隐私性。

7）数据本地化：引入了DNS根镜像、.CN./.COM/.NET镜像，以及本地备份重要的热点DNS数据，预防因网络中断导致的DNS服务不可达故障。

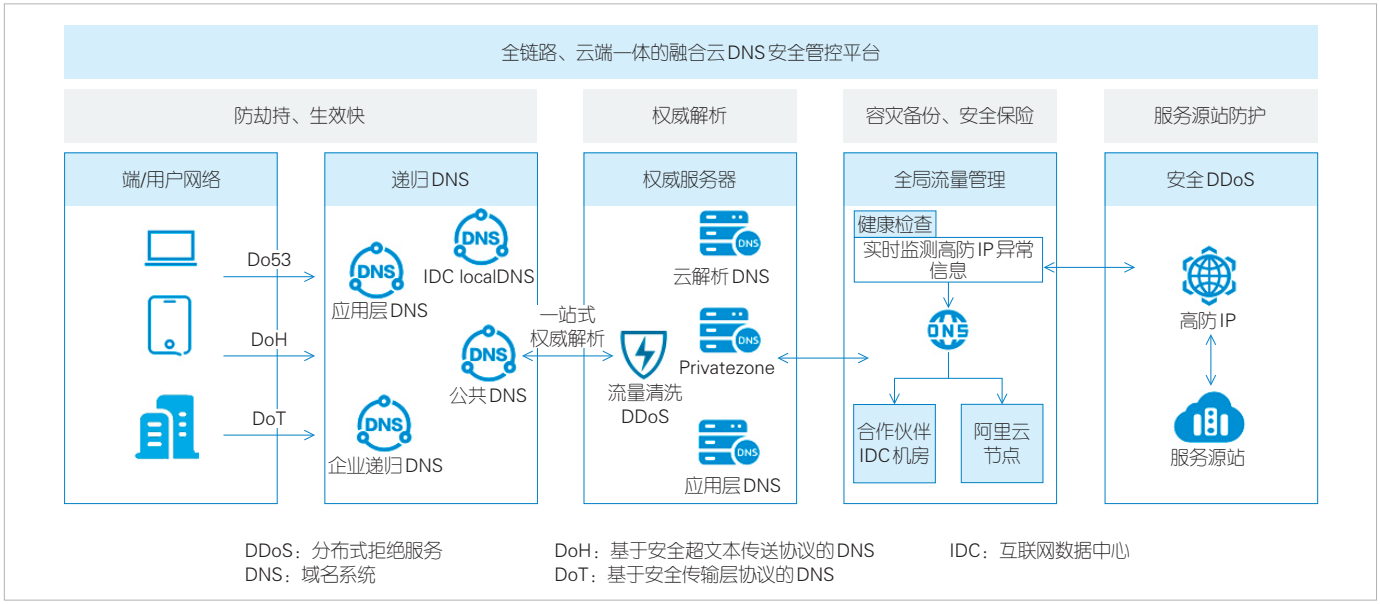
8）云端一体安全运维体系：阿里云全系列的DNS产品和技术能力覆盖了用户端（通过软件和SDK部署）、企业/公共递归解析、权威解析、DNS服务检测和调度、DDoS防护，从而能够从全链路视角来服务客户，减少中间链路的不确定性，保障DNS业务的安全可控、可预期，具体信息如图3所示。

4 结束语

DNS是全球互联网也是中国数字经济的重要基础设施，其安全稳定至关重要。DNS从一个简单的网络IP数据查找的基础组件，发展到智能算力和流量调度的平台型服务（SaaS/PaaS）。步入融合云时代，DNS在网络协议和平台型服务的基础上，又增加了新的功能场景，成为更高效的现代企业IT数字资产和流量调度管理平台。DNS的功能和应用场景更加丰富，承担的流量也进一步集中化和平台化，这其中机遇和挑战并存。

基于阿里云的DNS安全研究和运维经验，本文提出了融合云DNS安全体系框架，也介绍了我们在安全和稳定性方面所做工作。我们虽然在该领域收获了一些成果，但对DNS的安全和稳定性心存敬畏，因为一个小的故障就可能引发大量用户、大面积的业务受损。

DNS是国家关键信息基础设施的组成部分。当前，中国仍存在依赖外部关键域名解析资源（根和顶级服务器）、开源软件核心组件，DNS软件国产化水平不足，安全运维总体



▲图3 全链路、云端一体的融合云DNS安全运维体系

能力不高，对DNS安全体系缺少顶层设计等一系列问题。DNS是一个生态，需要全产业链参与其中，共同分享、协作，并统筹行动，应对各种安全风险。

参考文献

[1] The United States Department of Justice. United States seizes websites used by the Iranian Islamic radio and television union and Kata'ib hizballah [EB/OL]. [2022-12-04]. https://www. justice. gov/opa/pr/united-states-seizes-websites-used-iranian-islamic-radio-and-television-union-and-kata-ib

[2] Facebook. Update about the October 4th outage [EB/OL]. [2022-11-22]. https://engineering.fb.com/2021/10/04/networking-traffic/outage/

[3] KASHAF A, SEKAR V, AGARWAL Y. Analyzing third party service dependencies in modern web services: have we learned from the mirai-dyn incident? [C]//Proceedings of the ACM Internet Measurement Conference. ACM, 2020: 634-647. DOI: 10.1145/3419394.3423664

[4] MOURA G C M, CASTRO S, HARDAKER W, et al. Clouding up the Internet: how centralized is DNS traffic becoming? [C]//Proceedings of the ACM Internet Measurement Conference. ACM, 2020: 42-49. DOI: 10.1145/3419394.3423625

[5] LIU B J, LU C Y, DUAN H X, et al. Who is answering my queries: understanding and characterizing interception of the DNS resolution path [C]//Proceedings of the Applied Networking Research Workshop. ACM, 2019: 15-16. DOI: 10.1145/3340301.3341122

[6] LU C Y, LIU B J, ZHANG Y M, et al. From WHOIS to WHOWAS: a large-scale measurement study of domain registration privacy under the GDPR [EB/OL]. [2022-12-03]. https://www. researchgate. net/publication/349216875_From_WHOIS_to_WHOWAS_A_Large-Scale_Measurement_Study_of_Domain_Registration_Privacy_under_the_GDPR

[7] LU C Y, LIU B J, LI Z, et al. An end-to-end, large-scale measurement of DNS-over-encryption: how far have we come? [C]//Proceedings of the Internet Measurement Conference. ACM, 2019: 22-35. DOI: 10.1145/3355369.3355580

[8] 中国互联网络信息中心. 中国域名服务安全状况与态势分析报告[R/OL]. [2022-12-03]. https://www.cnnic.cn/NMediaFile/2022/0827/MAIN16615908654649L2MS5ZEJS.pdf

[9] LIU D P, HAO S, WANG H N. All your DNS records point to us: understanding the security threats of dangling DNS records [C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2016: 1414-1425. DOI: 10.1145/2976749.2978387

[10] ALOWAISHEQ E, TANG S Y, WANG Z H, et al. Zombie awakening: stealthy hijacking of active domains through DNS hosting referral [C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2020: 1307-1322. DOI: 10.1145/3372297.3417864

[11] RASMUSSEN R. ICANN SAC105: The DNS and the Internet of things: opportunities, risks, and challenges [EB/OL]. [2022-11-18]. https://www.icann. org/en/blogs/details/dns-and-the-internet-of-things-opportunities-risks-and-challenges-18-7-2019-en

[12] SKWAREK M, KORCZYNSKI M, MAZURCZYK W, et al. Characterizing vulnerability of DNS AXFR transfers with global-scale scanning [C]//Proceedings of 2019 IEEE Security and Privacy Workshops (SPW). IEEE, 2019: 193-198. DOI: 10.1109/SPW.2019.00044

[13] KAMINSKY D. Black ops 2008: it's the end of the cache as we know it, in: Black Hat USA, 2008 [EB/OL]. [2022-11-15]. https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf

[14] MAN K Y, QIAN Z Y, WANG Z J, et al. DNS cache poisoning attack reloaded: revolutions with side channels [C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2020: 1337-1350. DOI: 10.1145/3372297.3417280

[15] WWDC. Improve DNS security for apps and servers [EB/OL]. [2022-11-16].https://developer.apple.com/videos/play/wwdc2022/10079/

[16] Cisico Talos. A DNS hijacking called sea turtle [EB/OL]. [2022-12-03]. https://blog.talosintelligence.com/seaturtle/

[17] ABHISHTA A, VAN RIJSWIJK-DEIJ R, NIEUWENHUIS L J M. Measuring the impact of a successful DDoS attack on the customer behaviour of managed DNS service providers [J]. ACM SIGCOMM computer communication review, 2019, 48(5): 70-76. DOI: 10.1145/3310165.3310175

[18] CVE. ISC BIND CEV 漏洞库 [EB/OL]. [2022-12-04]. https://www.cvedetails.com/product/144/ISC-Bind.html?vendor_id=64

[19] KAKARLA S K R, BECKETT R, MILLSTEIN T, et al. SCALE: automatically finding RFC compliance bugs in DNS nameservers [EB/OL]. [2022-12-28]. https://www.usenix.org/conference/nsdi22/presentation/kakarla

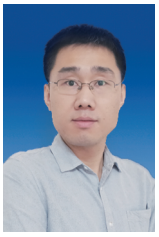
[20] SIGARAM A. Implementing dual stack recursive DNS at Microsoft: challenges and learning [EB/OL]. [2022-12-04]. https://indico. dns-oarc.net/event/42/contributions/904/

[21] TUNG L. Azure global outage: our DNS update mangled domain records, says Microsoft [EB/OL]. [2022-11-15]. https://www. zdnet. com/article/azure-global-outage-our-dns-update-mangled-domain-records-says-microsoft/

[22] KAKARLA S K R, BECKETT R, ARZANI B, et al. GRooT: proactive verification of DNS configurations [EB/OL]. [2022-11-25]. https://dl.acm.org/doi/10.1145/3387514.3405871
[23] 阿里云基础设施. 阿里云DNS荣获信通院2022首批“分布式系统稳定性保障能力评估”最高等级证书 [EB/OL]. (2022-04-28)[2022-12-01]. https://mp.weixin.qq.com/s/f8AFlr8EyModp_C78e7_CA

作 者 简 介

宋林健，阿里云计算有限公司高级技术架构师、ICANN根服务器咨询委员会专家组ICANN TEG技术专家、国家OID注册中心受邀专家；长期从事互联网体系架构、互联网地址标识领域等研究工作；曾参与多个下一代网络体系结构国家“973”和“863”计划项目，参与制定IETF RFC8483、ITU-T X.672等；发表多篇论文，拥有发明专利20项。



马永，阿里云计算有限公司基础设施网络研发高级技术专家、阿里云DNS解析研发&运维负责人；负责阿里DNS解析服务平台的技术架构设计、功能研发、建设运维工作，主导了阿里DNS系统的多次架构升级。

梁卓，阿里云计算有限公司基础设施网络研发技术总监、DNS产研负责人；长期从事网络基础服务关键技术和应用体系开发和设计工作；曾先后负责和参与工业和信息化部的相关项目、国家“863”计划项目等，并积极参与物联网标识解析国际标准ISO/IEC 29168-2的制定。