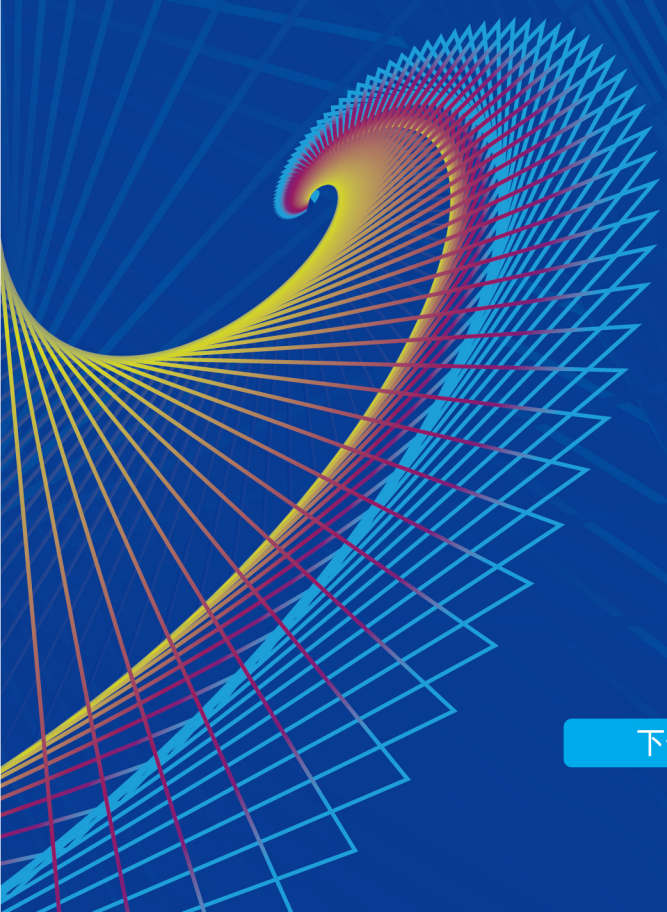
下一代DNS发展论坛
Next Generation DNS Summit

NEXT GENERATION DNS

# 下一代DNS

## 优秀实践案例

2023/北京



下一代DNS发展论坛

下一代DNS发展论坛
Next Generation DNS Summit

NEXT GENERATION DNS

# 下一代DNS

## 优秀实践案例

2023/北京


**编委会：** 吴　琦　池慧斌　苏　钰
程智强　郭晓东　郭　磊　何　铅　何黎明　贾爱军
蒯　磊　李宏涛　仇一泓　唐　洁　王丰刚　王　东
王承晖　王　亮　王　健　吴有文　夏超俊　徐　巍
甄　彬　周　珂　周剑涛

（以姓氏首字拼音为序）

# CONTENTS 目录

以下排名不分先后

## 01 【金融】



## 02 【政务】

## 03 【教育】



## 04 【大型企业】



## 05 【运营商 & 广电】

# 01 金融

根据《国民经济和社会发展第十四个五年规划和2035年远景目标纲要》有关要求，IPv6规模部署和应用进入全面推进阶段。金融是国民经济的重要组成部分，金融行业积极响应国家IPv6政策要求，基于IPv6研究规划新一代核心骨干网建设，实现网络架构升级，构建高速泛在、融合互联、灵活调度、弹性部署、云网一体、算力调度的网络体系。金融机构持续优化网络架构，不断融入IPv6+新技术元素，助力金融科技不断发展。

数字化转型，业务线上化，使得域名系统成为互联网业务的核心入口，其服务可靠性、安全性亟需优化和提升。为提升业务连续性，基于域名系统的应用多活调度方案成为理想方式，做好应用域名化改造的顶层设计和场景化解决方案成为当务之急，同时确保方案可落地、可执行、可持续成为关键。海量访问、交易背景下传统域名技术架构面临瓶颈，域名系统同样需要从基础解析寻址向“数据赋能、全面感知、可靠传输、智能处理、精准决策”的新模式升级。

基于域名化建设、改造、升级金融行业的业务系统，为金融科技构建基础支撑，成为金融科技不断发展的重要网络根基。自主可控的下一代DNS正在推动IPv6快速应用，为互联网体系架构升级筑牢更安全、更高效、更智能的网络根基。

# 中信银行：域名服务体系支撑金融业务高质量运行

通过采用云地协同的服务架构、优化解析流程与服务模式，中信银行构建了一套具备强大生命力的互联网域名服务体系，有效支撑了互联网金融业务的高质量运行。

## 中信银行金融科技蓬勃发展，DNS 成为互联网业务的第一入口

现如今，互联网银行、线上金融服务成为金融行业的主流，离柜率逐年提升，金融 IT 基础设施的可靠性、安全性成为了银行业的生命线。为保障金融业务的可靠性，中信银行目前已建成标准的两地三中心架构，并且利用智能 DNS 实现了业务服务体验的优化和业务连续性保障能力的提升，DNS 已经成为了客户与金融机构数据中心连接的“核心枢纽”。

为了确保互联网域名系统的可靠性，中信银行采用了跨中心自建集群、多运营商接入的冗余架构，虽可保证一定程度的高可用性，但在极端情况下，如遭遇针对其 DNS 集群的大流量 DDOS 攻击时，自建集群并发处理性能和网络带宽均存在瓶颈，且灵活性较差，很难实现快速的性能容量的横向扩容，极易出现资源耗尽、网络拥塞、金融服务中断的生产事故。

## 构建云地协同、天地互备的互联网域名服务体系

为了进一步提升互联网域名服务的抗攻击能力，支撑金融服务安全访问，中信银行携手 ZDNS 基于“云地协同、天地互备”的方案对其互联网域名体系进行了全面升级。方案中将 ZDNS Cloud 云服务强大的抗 DDOS 攻击能力、智能高效的解析能力纳入到了中信银行互联网域名服务体系中，该方案并不改变中信银行自建域名服务集群的整体架构，融合过程平滑透明，如同给中信银行自建 DNS 集群穿了一层“防弹衣”，即使本地集群全部故障，云端依然可以承载解析服务，大大提升了中信银行互联网域名系统的抗毁能力，保障互联网金融业务的高效、可靠运行。

# 民生银行：建立稳定、可靠、高质量金融服务信息化平台

中国人民银行在《金融科技（FinTech）发展规划（2019-2021 年）》中提出“建立健全我国金融科技发展的‘四梁八柱’，进一步增强金融业科技应用能力，实现金融与科技深度融合、协调发展。”随着云计算、大数据、人工智能、区块链等信息技术的发展和应用，极大地促进了金融科技创新，加快了金融数字化转型的进程。

近年来，民生银行聚焦金融数字化转型建设的发展方向，围绕金融业务安全，以业务线上化、服务智能化、运营自动化为抓手，打造稳定、可靠、高质量的金融服务信息化平台。

## 构建安全可靠、智能高效的互联网 DNS 系统

在互联网信息技术日新月异的变革周期内，业务线上化作为连接广大互联网用户的纽带，如何以稳态运营为基石，拓展金融数字化视野，全面迭代安全维度，成为银行业进行数字科技创新破局的关键路径。

ZDNS 围绕民生银行互联网业务体系下的平台化需求，基于全球云化域名服务平台，与客户共建基于域名的互联网业务流量调度、风险感知与管控、资产管理的整体化能力。

通过云地协同能力融合客户本地 GSLB 节点，打通云上云下异构壁垒，保障数据秒级同步，实现一致化的互联网域名查询服务，规避单一自建平台故障风险，全球分布式云化解析节点，满足客户对于多运营商多线路解析服务智能化调度要求，实现本地化的高效解析查询；云高防为客户解析服务串联数十 G 以上的抗 D 带宽吞吐服务，有效过滤面向 DNS 系统的 DDOS 攻击，消除服务安全隐患；云监测通过对民生银行域名解析服务链条端到端的全过程感知，开拓了系统风险感知视野，快速定位金融业务各解异常所在环节，利用配套技术服务工具，使业务得以快速恢复正常。

## 满足金融级多中心业务冗灾的智能解析系统

民生银行持续建设并形成多地多中心信息化业务运营模式，金融业务在运维运营层面的差异化需求突显，对银行数字技术支撑能力提出更高要求的同时，在网络关键基础设施层面持续加大智能化敏捷冗灾能力建设，成为金融服务质量实现突破的发力点。

ZDNS 帮助客户梳理当前多中心网络分区和业务关联逻辑，遵循“多中心统一规划、生产办公分离”原则，建设跨主中心、同城中心和异地中心的平台化域名解析系统，通过集中管控平台实现 DNS 服务节点的统一管理和配置；复用客户负载均衡完成 DNS 服务节点跨中心集群架构部署，保障解析服务高可用性和一致性；

民生银行协同 ZDNS 重新拆解多地多中心的智能解析需求，实现了不同网络区域间生产终端和办公终端解析流量精细化调度，提升了业务连续性和用户体验，改善金融服务质量。

未来，民生银行还将不断开拓和深入智能解析系统在金融信息化服务体系中的应用，最终建成基于国产品牌的“根、权威、递归”三层域名体系架构，扩大在金融科技创新领域的影响力。ZDNS 也将积极助力客户在金融科技领域的探索，为中国金融科技的发展贡献自己的力量。

# 光大银行：分布式智能 DNS 筑牢新一代信息基础设施

全栈云作为光大银行新一代基础设施，采用“双栈并举、一栈多芯”的建设思路，为全行系统上云及分布式系统提供能力支撑，分布式智能 DNS 服务作为全栈云提供的基本服务能力之一，需要同时满足海量高并发的域名查询和安全可控及分布式系统稳定性两项要求，本文分享了光大银行全栈云 - 分布式智能 DNS 服务建设的信创方案和实践经验。

## 建设背景及需求

### 三层网络架构

为了适应云时代的敏捷开发和迭代，应用架构与网络架构解耦，跨中心的数据访问从大二层网络改为三层网络。

### 统一域名访问

在三层网络下，没有全局可用的浮动 IP 地址作为统一出入口，全栈云应用需要转变为统一采用域名方式提供服务和访问。

### 应用多活架构、分布式改造

全栈云采用多可用区架构建设，为应用多活、分布式系统提供跨数据中心、跨异地的多活部署能力，其中分布式域名解析能力作为全栈云平台的基础核心能力之一，提供区域就近访问、轮询等多种智能域名解析算法，贴近应用需求。域名解析服务在用户与服务端之间、在应用与底层网络架构之间加了一层缓冲，所有的访问请求流量第一步先到达 DNS 进行域名解析，由 DNS 给予其对应的 IP 资源，之后才是真正的业务数据流量的交互；数据中心灾备、多活数据中心可依托于分布式智能 DNS 系统的智能解析与流量调度指引。

### 自主可控

当前我国各领域使用的 DNS 软件多为基于开源 DNS 版本进行的二次研发，存在较大的信息安全风险。全栈云作为光大银行下一代基础设施，域名解析服务必须搭建在安全可控的基础上，并具备完全自主可控的能力。

## 建设目标

随着分布式成为主流的系统架构设计方案，大规模分布式系统的稳定性保障能力越来越成为业界关注的重点，稳定性工作贯穿软件生命周期的全过程，从故障的视角来看，稳定性建设的最终目标是“降发生”和“降影响”，即降低故障发生的概率、降低故障发生后的影响范围。围绕稳定性建设目标，稳定性建设思路主要包括了四大建设模式：良好的系统架构和实现、合理的容量规划设计、完备的运维方案设计，以及规范的安全设计。

结合背景及全栈云应用需求，分布式智能 DNS 主要建设目标如下：

- 分布式智能 DNS 系统稳定性，提供分布式智能解析能力；
- 采用分布式系统稳定性建设模式，“降发生”和“降影响”；

- 良好的系统架构和容量设计；
- 具备自主可控能力和安全设计；
- 完备的运维方案设计。

## 选型及部署架构

通过结合业界技术产品情况，具备采用自主可控 DNS 作为全栈云 - 分布式智能 DNS 服务的条件（见图 1）。

| 与传统 DNS 对比 | 自主可控 DNS 能力情况 |
| --- | --- |
| 数据中心 | 基本相当 |
| 服务成员 | 基本相当 |
| 地址池 | 基本相当 |
| 记录类型 | 基本相当 |
| pool 内负载均衡算法 | 只具备最基本、常用的算法。如：轮询 / 加权轮询 / 备用 ip/ 全局可用 / 到 DNS 解析 / 基于服务器性能 / 静态就近性等 |
| 域名到 pool 负载算法 | 基本相当 |
| 健康检测 | 基本相当 |
| 健康检测类型 | 只具备最基本、常用的类型。如 ftp/http/https/tcp/tcp 半开连接 /udp 等 |

图 1　传统 DNS 与自主可控 DNS 对比

作为分布式智能 DNS 系统，需要考虑关乎分布式系统稳定性的核心要素，影响分布式系统稳定性的核心要素主要有以下几点。

1. 去除单点

全栈云分布式智能 DNS 系统采用多机房、多可用区 (AZ)、多节点，两套独立分布式智能 DNS 系统 ( 另一套待建设 ) 等设计方案，避免了包括硬件单点、存储单点、网络单点、机房单点、基础技术单点、内部服务单点等隐患。

2. 依赖设计

高等级服务不允许强依赖于低等级的服务或资源。全栈云分布式智能 DNS 系统作为行内的二级 DNS，面向全栈云应用提供域名解析服务，向上只依赖于全行 DNS 根节点，纳入全行 DNS 统一管理序列。

3. 数据保护设计

具备两级数据保护能力：

一是通过部署探测节点可以自动对业务数据（应用域名）进行一致性校验，并自动备份为 hosts 文件，可保证业务数据完整性、一致性。

二是具备定期系统级整体数据备份，单机房灾难情况下可分钟级整体恢复。

分布式智能 DNS 系统是全栈云关键基础设施，采用两级灾备 + 逃生方案设计。

第一级灾备：

系统内分 DNS 管理节点、DNS 解析节点角色。DNS 管理节点负责配置、分发系统配置给解析节点，自身具备解析能力但不做解析服务。管理节点采用同城热备 + 异地热备灾备架构。

某台管理节点出现故障既不影响系统管理能力也不影响应用解析服务。

全部管理节点出现故障只影响系统管理能力（无法新增应用域名配置），但不影响应用解析服务（不影响为存量应用域名提供解析服务）。

DNS 解析节点接受来自于管理节点的配置数据，专门负责应用域名的解析服务，并且在全栈云每个数据中心的每个可用区都有部署，只要有 1 台解析节点正常就能保证应用域名解析服务能正常进行。

第二级灾备（待建设）：

在设计阶段，考虑极端情况下系统整体出现问题，所有 DNS 管理节点、DNS 解析节点全部故障的情况下，除系统整体恢复方案外，在不考虑成本的情况下，可在全栈云内再建设一个独立分布式智能 DNS 系统 B（已建设的为系统 A），A、B 两系统完全独立，具备故障隔离并随时独立为全栈云应用提供分布式智能域名解析能力。

日常只用系统 A 提供分布式智能域名服务，系统 B 只做热备不提供服务。通过云管平台同时对 A、B 两个系统同步做变更和管理。在灾备演练或 A 系统出现问题时，可分钟级平滑切换到 B 系统，接管 A 系统继续提供分布式智能域名解析服务。

逃生方案设计：

在 A、B 两套分布式智能 DNS 系统全部出现问题时，应用域名解析服务仍然需要最后的手段来保障，上文数据保护设计中提到的 hosts 文件，可以直接用来下发到应用系统中，把所有域名记录追加到系统 /etc/hosts 文件后，仍然可以最大限度保障应用域名解析服务不受影响（除某些需要特殊算法的域名外）。

5. 弹性设计和安全设计

系统 / 组件间不具有强依赖关系，也不具有共享资源的场景，具备防止故障从一个系统 / 组件传播到另一个系统 / 组件的能力。通过 IP 解析限速、域名解析限速、缓存安全防护、黑名单、白名单、最小权限访问等机制可实现系统自身的安全保障，在需要时实现域名解析服务降级、限流与熔断能力。

6. 容量设计

容量设计的目的是根据业务优先级、资源消耗情况等合理评估及分配资源，良好的容量设计可以提升核心业务稳定同时带来成本节约。

根据业务发展需要，综合考虑单台 DNS 解析节点能力、域名查询请求数（QPS）、域名查询并发递归能力，DNS 解析节点的分布式部署方式可以在不影响现有域名解析的情况下实现单台或多台 DNS 解析节点透明扩容（管理节点只做简单的管理配置，不做解析服务），满足海量高并发的域名查询要求。

全栈云 - 分布式智能 DNS 系统整体架构设计和部署示意图详见图 2。

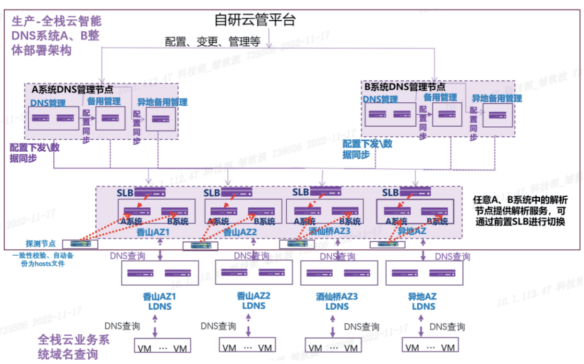



图 2　全栈云 - 分布式智能 DNS 系统整体架构设计和部署示意图

## 运维方案设计

考虑系统上线后持续迭代发布变更以及运维诉求，做到变更可控、流程可控、演练到位、可观测性 & 监控应急处置等能力。

### 1. 变更可控

全栈云 - 分布式智能 DNS 系统自身通过自研工具变更，已实现多个原子封装变更工具，可以实现包括新增、修改、删除动态 / 静态域名记录配置、全局地址池、健康检测、数据中心服务、解析同步组、远程认证策略、用户权限管理、域名记录用户授权、用户区域、就近访问策略等约 50 种类型变更。

### 2. 流程可控

通过自研云管平台，对分布式智能 DNS 系统进行纳管，云管平台作为统一入口，对所有平台操作流程进行管控，后端调用上述的变更工具进行标准化、模板化操作。在 A、B 两套独立分布式智能域名解析系统的情况下，云管平台可对 A、B 两套独立系统分别进行单立配置，实现 A、B 系统具备独立的操作逻辑，从入口即实现 A、B 系统配置独立，这样从部署实体到操作配置均实现 A、B 两套分布式智能 DNS 系统完全独立，完全解耦，真正实现系统级冗余。

### 3. 系统软件版本升级

DNS 管理节点域 DNS 解析节点角色分离设计，以及 DNS 解析节点全局服务能力可以实现系统内的 DNS 解析节点灰度变更 / 升级 / 回滚（管理节点只做简单的管理配置，不做解析服务，升级时不影响应用域名解析）。

A/B 两个独立部署系统设计方案，可以支持系统间灰度变更 / 升级 / 回滚。

### 4. 可观测性 & 监控应急处置

DNS 产品自身具备完善的日志、监控指标等基础的可观测性手段，全面分析架构特点后，梳理出 60 余项监控能力及 11 种应急处置场景。另外通过在 DNS 管理节点、DNS 解析节点部署全栈云流量采集分析工具，充分复用全栈云自身的可视化流量分析能力，补充了全栈云平台内 DNS 流量全链路追踪能力，可及时掌握域名解析请求实时运行情况并及时定位处理问题。

## 总结与展望

全栈云平台作为光大银行最重要的基础设施之一，自身的安全稳定性至关重要。作为全栈云平台服务能力之一的分布式智能 DNS 系统，在考虑使用需求和全面自主可控的前提下，基于分布式系统稳定性建设目标、建设模式指引下设计并完成了系统的建设，已正式上线并全面提供服务，经过模拟演练圆满实现了预期的效果。接下来将继续探索全栈云上智能 DNS 的高阶应用，通过智能 DNS 实现云上应用的引流、隔离等场景，无需通过应用启停实现云上应用优雅的切换。

# 华夏银行：构建涵盖全业务场景的 DNS 服务体系，建成两地三中心标准金融 IT 架构

华夏银行构建涵盖全业务场景的 DNS 服务体系，制定标准化改造流程，统一域名生命周期管理过程中的运营模式，加速应用域名化改造进程，目前已建成两地三中心的标准金融 IT 架构。

## 加速域名化改造，构建两地三中心 IT 架构

在谋求“大而强”、“稳而优”发展目标过程中，华夏银行在产业端率先起步，基于云原生技术自主研发，构建了一套完备的产业数字金融理论和实践体系，搭建了产业数字金融科技平台，助力华夏银行实现数字化授信、智能风控技术突破和落地应用，通过内部业务系统直联核心企业，实现批量获客、批量授信，为客户提供全流程线上化、数字化融资服务。伴随数字化转型逐渐步入深水区，华夏银行愈加认识到金融企业对信息技术和数据的应用应多方面强化信息安全管理；作为互联网所有服务的入口，域名系统（DNS）是信息技术关键基础资源，对信息安全发挥基础支撑作用。聚焦基础安全支撑，华夏银行携手互联网域名和 IP 地址专业服务机构，构建涵盖全业务场景的 DNS 服务体系，包含生产网（各业务区）、办公网，提供动态及静态的域名解析服务；实现两地三中心的业务多活、冗余灾备，构建灾难应急保障能力，优化业务交互逻辑，提升金融服务质量；基于统一管控、分布部署的 DNS 服务架构，实现管理集中化、平台化、可视化，提质增效、智简运维；依靠集群化部署，实现自身灾难快速迁移，解析指向冗余配置，保障 DNS 服务永续运行，支撑金融业务发展。在域名化改造过程中，华夏银行通过量身定制域名体系的顶层设计，制定标准化改造流程，统一域名生命周期管理过程中的运营模式，加速应用域名化改造进程，有效规避改造风险，构建灵活、弹性、可扩展的多数据中心域名体系架构。面向未来，华夏银行将基于域名系统的定制化、流程化改造，构建多数据中心域名体系，持续提升监测运营能力，为两地三中心的标准金融 IT 架构打造护城河，有效防控网络风险，加大力度推进产业数字金融创新实践，促进产业链、供应链、创新链的结合，为服务实体经济发展贡献金融力量。

# 北京银行：信创域名服务助力 IPv4 至 IPv6 平滑演进，支撑金融业务高速发展

北京银行加速推进金融科技底座的信息技术应用创新，采用信创域名服务方案实现关键业务由 IPv4 至 IPv6 的平滑演进，满足监管合规要求，支撑金融业务高速发展。

作为一家积极践行新时代发展使命的首都金融机构，北京银行紧紧围绕国家创新驱动发展战略，确立了“数字京行”战略体系，在金融科技层面坚持自我革命、敢为人先，多年来始终保持科技创新的高投入，积极探索信创、新技术、新场景在行内的应用落地。本文将阐述北京银行与 ZDNS 持续深度合作背景下信创域名服务的应用落地与支撑关键业务 IPv6 演进的案例情况。

## 信创 DNS 应用：首次在关键业务区域应用纯国产 DNS 软硬件设施

作为金融科技领域重要的网络基础设施之一，DNS 担负着金融行业内部业务流量交互指引的职责，是网络流量走向的核心指挥，其稳定性、安全性直接关乎金融行业业务系统运行是否平稳。经过多年的发展建设，北京银行已经实现了业务系统的深度域名化，并构建了冗余、智能、灵活的域名服务体系，基于智能解析实现精准的业务流量走向牵引，有效的提升了金融业务的高可用性。

在此基础上，2023 年北京银行更近一步，结合 IPv6 双栈改造工作的推进，在生产数据中心关键业务区域采用了基于“自研 DNS 软件红枫（Maple）”的纯国产智能 DNS 设施，作为支撑该区域业务 IPv6 双栈改造智能解析的核心组件。在信创 DNS 正式上线应用前，北京银行在功能性能、安全性、可靠性、运维管理的便捷性等多个维度对 ZDNS 信创型号进行了严苛的长稳测试，经验证 ZDNS 信创方案完全满足关键业务区域域名解析服务的相关要求，并最终成功上线运行，有效的支撑了该区域 IPv6 场景下的智能解析、冗灾调度需求。在提供全功能智能域名解析服务的同时，良好的管理兼容性也让信创设备与原有非信创设备实现统管，达到两套体系运维管理、应用配置界面的统一，让信创替换过程更加平滑。

本次信创域名服务的建设为北京银行信创工作的推进积累了宝贵的实践经验，未来北京银行将继续加速推进金融科技基础设施信创应用的广度与深度、提升国产率，进一步降低供应链不确定性带来的影响，提升金融风险的应对能力。

# 徽商银行：全面推动数字化转型，大力提升核心竞争力

徽商银行以下一代 DNS 为依托，积极推动数字化转型，通过引入先进的技术和应用，提升银行的服务效率、客户体验和风险控制能力。

徽商银行建立于 1995 年，在成立初期，徽商银行以服务地方经济发展为使命，积极支持当地企业的发展，促进了地方经济的繁荣。

自创立以来徽商银行秉持“服务地方、服务客户”的宗旨，不断提升自身的竞争力和创新能力，为客户和社会创造更大的价值。随着金融市场的不断扩大，用户对银行业务的要求的持续性、稳定性要求越来越高，徽商银行以下一代 DNS 为依托，建立了一套高效、快速、稳定的核心业务系统，积极响应国家金融改革和发展的号召，推动金融科技创新和可持续发展，为中国金融行业的发展做出更大的贡献。

## 同城中心，多节点灵活接入

随着互联网金融的蓬勃发展，徽商银行积极响应，在同城建立了“第二心脏”，以此为契机，徽商银行敏锐的捕捉到网银业务作为互联网金融的重要做成部分，其在整个核心的重要性不言而喻，为了实现应用的多点接入，动态快速感知服务状态，灵活智能的流量调度，徽商银行在网银区新建了单独的智能 DNS 系统，其独有的健康检测，多线路业务发布功能实现了多点灵活接入的同时，也保证了业务的稳定性和持续性。

## 动静分离，优化域名体系架构

作为一家现代化金融机构，徽商银行一直关注信息技术的发展和应用，积极推进数字化转型和金融科技创新。在这个过程中，优化域名体系架构是徽商银行重要的技术策略之一。

为了更好地实现业务的快速访问，徽商银行进行了域名体系架构的优化，将不同功能和服务的网站部署在不同的域名下，以实现更好的管理和资源分配。通过优化域名体系架构，徽商银行可以更好地对不同的功能和服务进行管理和维护，提高系统的可用性和稳定性。

通过优化域名体系架构，徽商银行可以更好地应对大量用户的访问和请求，提供更快速、高效、稳定的服务。同时，这种技术策略还可以降低系统的负载和风险，提高系统的安全性和可靠性。

未来，随着技术的不断进步和金融科技的发展，徽商银行将继续关注和应用新的技术手段，不断优化和升级自身的技术架构，提升服务能力和用户体验，为客户提供更好的金融服务。

## 健全架构，保证用户数据安全

为了响应国家相关信息安全相关策略，徽商银行考虑到下一代 DNS（域名系统）系统在安全性方面具备了更高的机制和保护措施。通过 DNSSEC（DNS 安全扩展）、DDoS 防护、域名过滤和黑名单、DNS 缓存污染防护、传输加密等技术能力。保护用户的 DNS 查询和互联网通信的安全。提高 DNS 系统的可靠性和安全性，为用户提供更加安全可信的网络体验。

# 郑州银行：铸造坚实网络根基，赋能业务数字化转型

郑州银行股份有限公司（以下简称“郑州银行”），坚守科技兴行宗旨，打造符合郑州银行高质量发展要求的新一代基础资源“网络根基”，推动各项业务数字化转型更高效、更智能，进一步为提升郑州银行金融服务能力和差异化核心竞争力提供坚实的科技支撑。

作为全国首家 A+H 上市城商行，郑州银行坚持“商贸物流银行、中小企业金融服务专家、精品市民银行”的特色业务定位，坚守深耕本土、支持实体经济的初心，紧扣金融业数字化转型发展的挑战和机遇，以持续创新为驱动力，在大数据、云计算、人工智能等新技术领域不断探索创新应用，并在风险管控，精准营销，降低成本，提质增效方面取得了丰硕成果。

## 完善基础资源层，铸就坚实“网络根基”

2019 年，郑州银行面向数据赋能、全面感知、可靠传输、智能分析、精准决策，开始建设安全、高效、智能的新一代 DNS 域名系统，着手筑牢数字化转型重要网络根基，并在 3 年里不断完善域名系统自身基础环境的搭建。

DNS 域名与路由组成的寻址解析体系好比内部流量导航系统，“导航系统”的组建终结了物理设施层与业务应用层长期割裂的现状，业务应用数字化转型更为高效与安全。

### ● 域名架构清晰，分区、分层提升域名解析效率

域名系统搭建初始阶段，以实现信息系统灵活、快速的切换、多中心运作、安全可靠为目标，以全面提升数据中心业务连续性及高可用性为要求，数据中心域名系统按照使用途径细分为：数据中心互联网 DNS 系统、数据中心业务区域 DNS 系统以及内网办公用户区 DNS 系统，其中：

数据中心互联网 DNS 系统，主要承载互联网类业务的域名发布，支撑信息系统多中心运营所需要的业务流量引导功能。DNS 域名系统根据 Local DNS 属性进行传统自定义域名解析，跨中心探测保证业务真实可用。针对手机银行等信息系统开发 DOH 算法，使用基于 HTTPS 隧道方式智能解析，突破传统 DNS 解析瓶颈，进一步满足业务灵活性与高可用性。

数据中心业务区域 DNS 系统按照业务分区，遵循 RFC 标准，搭建 Master-Slave 多层级 DNS 域名架构。通过标准 DNS 解析与 GSLB 功能，由前端 Slave DNS 将域名记录进行内存级缓存，对用户请求进行快速响应。数据中心双活应用域名通过 IP 地址调度、计算单元权重分配、服务优先级等多维度数据进行整体分析，从而实现业务请求精准决策，灵活分配。对于有外部域名解析需求业务系统，通过 DNS Forward 技术过滤恶意域名后转发请求至互联网，完成标准域名解析。

内网办公用户区 DNS 系统，部署两组 Local DNS 作为用户 DHCP 预分配 DNS。通过 DNS Forward 与 cache 技术将用户请求转发与缓存。与此同时，Local DNS 侧通过限制 DNS zone 进行域名请求过滤，防止权威 DNS 污染，保障域名系统纯净可用。

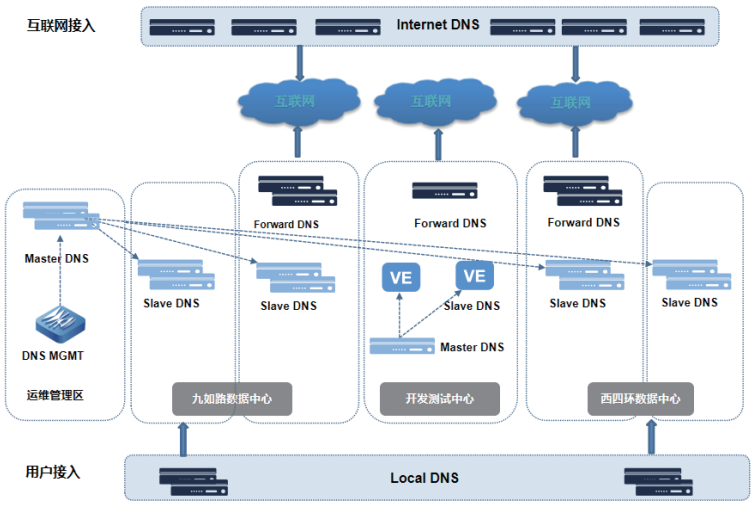



图 1 DNS 分区示意图

## 通力合作，绘制“域名地图”

DNS 域名系统与行内云平台实现集成交互，服务请求工单提交后实现自动化配置部署、域名解析集中展示、配置自动归档等多场景、多维度管理需求。“域名地图”自动接收来自 DNS 系统高速日志，通过对传输日志的格式化转换与解析，同步展示结果。实现业务系统域名“看得见、看得清、管得住、能预测”的效果。

图 2 DNS 域名地图

## 安全管控

在域名解析系统安全方面，实现了对域名解析请求进行多维度状态监控和安全防护。基于域名的细粒度访问限制，严格控制不同区域 DNS 访问需求，对访问互联网域名进行细粒度控制辅以域名威胁情报库建设，有效防护非法站点、恶意域名、钓鱼连接、勒索病毒等多种威胁。在精准感知服务状态和防范恶意攻击的同时，将安全运营由被动式响应升级为主动式防护。

## 标准化

2022 年全面开展信息系统域名化改造工作，基于标准化的域名规范，统一的域名使用基线为各类信息系统快速迁移、切换演练、容灾建设、紧急响应等场景提供一致的建设和规划方案。为业务提供多维度、多层级、多场景的适配，并基于业务的发展对标准化不断打磨，持续完善未来业务系统域名应用的场景。

## 支撑业务数字化转型双管齐下：更高效 + 更智能

依托智能、安全、可靠的下一代 DNS 域名系统架构，作为“核心入口”“导航系统”的 DNS 服务，为业务数字化转型与支撑提供了更高效、更智能的技术赋能。

- **更高效**

DNS 域名系统未来将参与业务系统全生命周期过程，在过程中以高性能、低延迟、弹性扩缩容、自动编排等特点实现“高效运维、高效应用”。全面利用 CLI 方式和 DNS 全功能 API 对接网管系统与集中运维管控平台，纳入我行统一运管体系。从性能、服务状态与可扩展性全局把控，提升运维效率、降低风险；从标准化配置方式，流程化上线、下线域名，实现域名系统高效应用。

- **更智能**

通过大数据分析、智能枢纽、全局负载、算力调度等能力提升实现应用“智能访问”。重点由应用访问的核心入口（DNS 服务），基于精准的应用级健康检查能力，丰富的负载调度策略，实现应用智能化访问，满足各类主备业务、双活应用、云环境的场景化需求，全面保障业务连续性、智能灵活的实现应用访问。

## 展望未来，持续创新

开拓创新是郑州银行的基因。郑州银行按照自己节奏一步一步完成从 Bind、DNS、智能 DNS 到下一代 DNS 基础资源层的建设，自主可控掌握网络关键基础资源，将进一步加快金融数字化转型创新步伐，打造数字化产品体系，提升数字化服务能力，更好地满足用户需求。下一代 DNS 基础资源层的顺利组建，不仅充分体现了郑州银行的金融科技创新能力，同时也将“以客户为中心”的理念落到实处，在数字化时代打造更高品质的金融服务，为赋能实体经济高质量发展奋力开创“郑银”活力。

# 深圳农商行：构建强大的 DNS 智能调度，实现银行混合云的高效运营

数字化浪潮席卷全球的当下，科技创新在现代金融体系建设中的地位和作用日渐凸显，已成为支撑金融业高质量发展的重要动能。作为坚持科技创新双轮驱动的本土银行，深圳农商银行积极贯彻落实国家重要指示精神，践行数字赋能转型发展的核心理念，推动各项金融科技成果惠及民生福祉，竭力为深圳经济社会发展提供源源不断的本土金融新动能。

目前云计算的发展前景被不断肯定，并成为金融行业数字化转型的必备能力。中国人民银行、国家发展改革委、中央网信办、银保监会等监管部门陆续出台金融行业云计算发展的指导意见，既从宏观战略层面指明云计算的发展方向，也从微观视角引导具体实践内容。同时，应用规范和标准的建立也让金融机构上云提供更加“有据可依”的良好环境。在数字化转型中，基于云计算、大数据等技术构建出的云生态必将成为银行数字化转型、开启第二发展曲线的重要力量。

在此大背景下，受服务实体经济角色定位、传统 IT 架构升级、业务模式数字化转型、顶层政策标准指引、金融信创需求驱动等因素的影响，深圳农商行上云进程不断加速，金融云架构已经步入到应用深化发展的中期阶段，其中作为互联网关键基础资源的域名系统（DNS）对银行数字化建设的支撑作用不言而喻，该行已聚焦全网业务系统进行域名化改造，在多数据中心业务连续、业务安全以及业务多活建设等方面展开积极探索。

## 打造云数据中心，业务系统上“云”

数字化转型，关键核心技术自主可控和重要信息基础设施建设是关键保障。深圳农商银行位于深圳市龙华区锦绣科学园区的同城云数据中心已投入使用，实际上，深圳农商银行一直以来大力布局底层科技力量。值得一提的是，此次新投入的数据中心引入阿里专有云平台，是继该行深圳罗湖、武汉数据中心后的第三个新型云数据中心。为支撑不断扩大的业务规模，深圳农商银行在原有的数据中心内各建设了一朵云平台，与深圳龙华云中心共同组成同城双活、异地灾备的两地三中心云架构。这也标志着深圳农商银行的 IT 基础架构完成向云原生分布式架构转型，持续支撑业务系统迁移上“云”。采用混合云架构以获得灵活性和可扩展性的同时，面临着复杂的网络管理和应用部署挑战，传统 DNS 服务在全局负载调度、架构可靠性、安全防护、自动化运维方面存在较大缺陷，已无法适应该行业务持续运行严苛的要求，所以一个强大而智能的 DNS 建设是实现高效运营和卓越用户体验的关键。

## 业务系统域名化改造：突破挑战，重塑银行业态

为更好支持多中心混合云架构体系，建立健全的 DNS 服务体系，需要业务采用域名方式运行，首先需要进行域名化改造，这种改造可以提升系统的可用性、灵活性

和安全性，但也面临诸多难点。

银行业务系统通常由多个模块和子系统组成，彼此之间存在复杂的依赖关系。域名化改造需要对系统架构进行全面分析和设计，确保改造过程中不会对系统功能和性能产生负面影响，需要充分考虑不同系统的兼容性和协同工作，确保改造过程中各系统之间的正常通信和数据交互；由于银行业务的连续性和稳定性是至关重要的，所以在域名化改造过程中，需要保证系统能够无缝切换至域名访问，避免因改造导致的业务中断或性能下降；同时也需要满足银行的安全性和合规要求，包括加强对域名系统的安全防护、防范域名劫持等

基于以上几点，该行通过对内部业务系统在设计和规划阶段进行充分的网络调研和规划后，进行详细的系统设计和改造工作：包括将 IP 地址替换为域名、调整系统配置和参数、更新系统代码和配置文件等，也要进行系统联调和测试，确保改造后的系统正常运行。最后将域名化系统与原有系统并行上线，并逐步将用户流量切换到域名化系统上。同时，要进行全面的性能测试和负载测试，确保域名化系统能够处理银行的业务需求。

## 健全 DNS 服务架构，铸就金融业务新高度

在部署上采用分布式 DNS 服务器架构，将 DNS 解析服务部署在多个地理分布的数据中心，包括在深圳同城数据中心、武汉异地数据中心以及云上环境均进行部署 DNS 解析服务集群，通过多地、多云集群协同机制，搭配业务状态的立体、快速、精准感知机制，以此作为冗灾调度决策依据，实现基于地理位置的容灾和负载均衡。

## 业务弹性扩展与混合云架构的无缝协同

同时云场景下可根据业务需求和流量变化，自动扩展解析节点，以满足高峰期和突发情况下的性能要求；也帮助该行在云地之间的资源调配和应用的灵活迁移，实现混合云架构下的业务连续性，云地协同架构也为海量的网点终端用户提供了智能、精准、高效的服务资源。

**解耦管理，集中管控**

另外从管理运维层面上，基于管理业务解耦思路，独立部署域名服务集中管理平台，监控信息与日常运维流程有效整合，实现全网服务节点的集中管控，提供实时的 DNS 解析性能监控和分析功能，帮助该行了解解析性能和业务健康状况，及时发现和解决潜在问题。

**卓越安全防护：多层次安全机制**

在安全防护上，采用业界应用高级的安全防护机制，利用多层次的安全防护手段，包括 DDoS 攻击防御、DNS 欺骗检测和防御、恶意域名过滤等，保护银行的业务免受网络威胁和安全漏洞的影响。

## 数字化转型引领市场，智能 DNS 方案助力业务腾飞

该方案帮助深圳农商行在数字化转型过程中带来了显著的效益和价值，业务平均解析时间减少 50%，提升用户访问网站的速度和响应性能；用户投诉率降低 30%，提高了用户满意度和忠诚度；在业务连续性也有好的体现，故障恢复时间缩短 70%，降低因 DNS 故障导致的业务中断风险，业务可用性提升 10%，确保金融业务的连续性和稳定性。可靠的用户体验同时也增强深圳农商行品牌形象和声誉，巩固了其在市场中的地位，并满足了业务发展的需求，吸引更多合作伙伴和客户选择该行作为合作对象。

正是因为顺应科技发展趋势，从多方面去践行”科技立行“理念，全面开启以数字化转型为方向的新征程，“零售 + 科技 + 生态”动力齐驱，深圳农商银行朝着数字化智慧型银行方向不断迈进，将继续谱写服务大湾区金融高质量发展的重彩篇章。

# 富滇银行：域名改造实现异地容灾要求，同城双活定义数据中心架构

富滇银行根据“两地三中心”异地容灾的要求对DNS服务系统规划建设，智能调度实现业务的同城双活＋异地灾备，统一管控实现多节点的智简运维，降本增效。

作为一家与云南经济发展密切相关的地方性股份制银行，富滇银行股份有限公司（简称“富滇银行”）以加快发展地方金融业、促进云南经济发展为己任，充分发挥自身品牌在云南及周边省市的影响力，持续强化对东南亚、南亚的辐射功能，拓展银行业务，加快外向型经济发展，为云南企业实施“走出去”战略提供有力的金融保障，促进云南对外经济又好又快发展。

## 两地三中心多活数据中心，重塑数字化旅程

富滇银行积极融入“数字云南”建设中，在全力支持云南加快现代化产业体系建设中实现自身健康快速发展，对银行核心系统进行重建，提升“稳态 IT”能力，加速建设“敏态 IT”能力，以数字化平台为核心，在不改变金融本质的条件下重构银行新的经营方式、商业模式，建立起以体验为核心、以数据为基础、以技术为驱动的架构体系，将客户、场景、产品、服务等转化为数字形态，优化服务与流程，提升内在价值，重塑客户的数字化旅程。

数据是数字化建设中极具价值的资产，数据的管理和应用是数字化的基础工作。基于对数据资产的高度重视，富滇银行构建同城双活异地灾备多数据中心架构，业务系统在同城数据中心实现双活或主备部署，其流量通过域名方式进行业务导向，将客户端的请求调度到就近的数据中心，当任何一个节点数据中心业务出现异常情况时，可通过域名方式实现业务数据流的服务切换，保证客户访问数据发送到可用的数据中心，从而确保业务系统的高可用服务模式，提升用户访问体验。

## 域名系统升级改造，实现多节点智简运维

域名系统 (DNS) 作为银行 IT 核心基础服务，是连接上层应用系统和底层数据资源的桥梁。采用 DNS 为网络通讯配置参数是 TCP/IP 网络应用迅速增长的必然要求，但是目前富滇银行的部分生产系统直接配置 IP 地址为网络通讯参数，应用系统的迁移、灾备都需要服务器端或客户端修改 IP 参数配置，从而造成极高的人工成本，极大地限制了应用部署的灵活性。

基于域名化改造的业务需求，富滇银行携手专业域名服务机构，根据“两地三中心”异地容灾的要求，对域名系统进行全新规划建设。在同城和异地灾备数据中心分别部署 CMS 中央管理器，对所有 DNS 服务器进行统一管理，构建全局化的 DNS 核心网络服务架构统一监管服务平台，提供数据备份、灾备切换、数据下发等服

务，确保富滇银行 DNS 核心网络服务的平台化管控。聚焦DNS服务节点，在银行主数据中心，同城数据中心、异地灾备数据中心以集群化部署，作为富滇银行终端的 DNS 服务节点，为银行办公网员工提供内网权威解析服务。在递归 / 缓存服务节点，采用与 DNS 服务节点同样的集群部署方式，为银行内部员工提供查询请求解析服务，同时开启转发功能，通过对目标地址的判断，将对内部服务器的访问直接转发到内网权威服务器，由递归 / 缓存服务器递归查询请求，实现对互联网的访问。

凭借图形化界面简化管理、高可用性机制、创新的数据同步机制、基于角色的访问控制、共享记录管理、全局搜索、集中软件更新、支持 IPv6 平滑演进以及丰富的日志和报告等优势，此次规划建设助力富滇银行完成生产环境域名化改造，并在其两地三中心建设 DNS 服务基础设施基于域名智能调度实现业务的同城双活 + 异地灾备，将 RTO 时间缩小在规定范围内，基于统一管控实现多节点的智简运维，降本增效。

富滇银行在基于 DNS 的升级改造构建安全、智能、稳定的网络核心基础架构，实现上层应用系统和底层数据资源的互通，充分发挥数据的基础性作用，加速数字化转型步伐，加速完成从高速增长向高质量增长的跑道切换，提升经营质效，为未来的可持续发展注入强大动力。

# 湖南银行：行稳致远，打造“本地设备 + 云端服务”的云地协同域名服务体系

新时代、新征程。湖南银行始终坚持金融工作的政治性、人民性，完整、准确、全面贯彻新发展理念，积极服务和融入新发展格局，以更高的政治站位、更大的责任担当，不断提升金融服务水平，全力服务“三高四新”战略定位和使命任务，努力成为一家治理完善、经营稳健，具有特色竞争力的现代化商业银行。为此湖南银行股份有限公司（以下简称“湖南银行”）制定了以“下一代 DNS”为内核的新一代域名服务体系演进路线，致力于构建一张业界领先、稳定、安全、高效的，全面支撑湖南银行数字化升级长期可持续发展的域名系统。

随着数字货币、数字银行等信息数字化趋势演变，互联网银行、远程银行、移动银行等 IT 投入逐渐扩大，湖南银行进入以数字化转型为基础，以信息技术为支撑的综合经营状态。面对银行业务开展渠道不断丰富，业务模式创新层出不穷，金融服务与各类生态场景的融合，金融行业对业务系统的灵活性、大并发、大数据量、动态应用容灾等提出了较高要求。湖南银行积极对域名系统架构创新进行实践探索，为建设分布式金融核心系统实现科技赋能。

## 云地协同的互联网域名解析系统，为湖南银行数字化转型提供稳健的新驱动

从金融 IT 的整体构架来看，分布式架构都在逐步取代“竖井开发”模式。银行 IT 新构架需要既体现高性能、高弹性、高可用性又要符合高规范性、低风险和低成本的要求。湖南银行深耕金融行业信息化建设特点和需求，域名解析系统向“数据赋能、全面感知、可靠传输、智能分析、精准决策”全面升级，为银行数字化转型提供更安全、更高效、更智能的网络根基。

自 2010 年以来，金融行业用户逐渐意识到了 DNS 云服务的优势，并开始逐步将 DNS 解析上云。对于没有自建解析服务历史包袱的客户来说，通常选择将 DNS 解析服务完全上云，以解决 DNS 安全问题。湖南银行在原有本地自建服务的用户基础上，选择本地 DNS+ 云服务混合部署的方式，本地自建和云服务同时对外提供解析服务，以提升解析服务的安全性。

湖南银行线上业务占比不断增大，业务模式由网点向电子渠道转化，数字化转型逐步走向业务常态，引入域名系统已经成为金融机构数字化转型的重要途径。湖南银行凭借自身在域名系统建设实践的积淀，实现业务系统的智能化、无感知切换，降低访问应用系统的复杂度，提高应用部署的灵活性，推动 IT 架构的技术改进，保证金融业务连续性，优化金融业务服务体验，为湖南银行科技的发展贡献基础支撑。

## 基于“5S”原则建设域名系统，打造业界领先的应用级多活数据中心解决方案

为应对当下金融行业面临的业务连续性新挑战，湖南银行从基于应用的域名化改造、如何提升用户服务体验和大数据提升网络运维能力等方面出发，基于 “5S”

域名体系建设原则， 构建应用级多活数据中心解决方案。“5S”域名体系建设的基本原则指的是：Smart（智能），通过业务状态感知及动态调度能力实现智能DNS；Scalable （可扩展），灵活的分布式部署架构支持横向扩展；Stable（高可用），在保证 DNS 系统可用性的同时为业务应用高可用提供支撑 Security（安全），提供 DNS 系统基于各种网络层及应用层 DDOS 攻击的安全防护；Standard（规范化管理），根据银行业务特点梳理并构建完善合规的域名体系。

湖南银行双活架构的“两中心，六出口，双栈协议”布局，不仅可以提升用户满意度，在容灾方面也比传统架构有更大的提升。当其中一个中心发生区域性灾难或者运营商发生重大事故，导致该中心无法对外提供服务，基于“5S”原则建设的智能 DNS 系统监测到后，会按照预先设计的优先级对用户的访问请求进行重新引流，将业务流量牵引至正常服务的数据中心，实现自动切换，减少故障对业务的影响，“5S”DNS 域名体系为湖南银行的金融科技数字化保驾护航。

## 构建域名“双轨 + 双活”体系，实现技术自主可控与业务延续高可靠

在当前经济转型和科技创新的背景下，创新型金融服务被认为是推动经济发展和提高金融业竞争力的重要手段。支持银行和金融机构开展信创业务，鼓励创新和技术应用，为银行开展业务应用创新提供了良好的政策环境和市场机遇。

湖南银行率先在域名系统建设方面实现“双轨 + 双活”，双轨是指信创和非信创两个独立业务体系运行轨道，双活是指构建两个数据中心实现业务运行高可靠。

在湖南银行的网络架构中，建立双数据中心，实现重要业务应用双活，以保证业务系统的高可用性。通过 DNS 系统的全局流量调度（GSLB），对双活业务进行容灾备份管理。通过 DNS 系统的业务健康监测机制实现业务故障的自动迁移，当一中心业务故障时，DNS 将业务解析自动切换到二中心，保证业务的连续性和可用性。双轨体系——高可用 DNS 系统在保障非信创业务平稳运行的同时，也保障了信创业务系统的安全高可用。

深耕数字化转型、发展数字经济需要 DNS 技术“向上”创新突破。湖南银行构建的“双轨 + 双活”DNS 系统，成为支撑银行数字经济成长的重要网络根基，推动数字经济底座在基础设施和基础资源等层面协同升级，促进湖南银行数字化转型迈向纵深。

# 内蒙古农信：全面投运同城双活数据中心，灾备应用水平步入全国农信先进行列

建设内蒙古农信社的高可用 DNS 域名服务系统，推进内蒙农信应用系统采用域名化形式作为通信手段。并通过合理，稳定，可靠的域名部署架构，实现同城双中心的应用系统接入，满足应用同城双活、异地应用多活需求，提升整体业务连续性。

内蒙古农信社和林、金桥双活数据中心是内蒙古农信科技发展史上规模最大、耗时最长、投入最多、影响最广的信息科技项目。同城双活数据中心成功投产，标志着内蒙古农信金融科技建设实现新的跨越，容灾体系、新技术应用步入全国农信先进行列，具备“同城双活”和“异地容灾”能力，能够满足各类业务连续性需求，对加快推进全区农信向数字化、智能化转型，全面提升业务发展、产品创新、经营转型、风险管理能力具有更大而深远的意义。基于更安全、更快捷、更高效的信息科技平台，将进一步赋能业务发展，提升内蒙古农信聚焦主业、扎根本土、服务“三农三牧”、助力小微企业的能力和水平，为内蒙古农信高质量发展插上科技翅膀，为地方经济高质量发展注入新活力。

## DNS 覆盖同城双中心，提升双活灾备能力

用户访问和业务系统之间引入域名系统，将原有的用户通过 IP 访问业务系统的紧耦合关系打破，通过域名系统，使得管理者可以根据业务的变更、冗余和切换、不同数据中心的分布等实际的情况，来进行灵活的调度和调节。将应用之间的 IP 互访形式改造成域名形式，使应用部署和迁移更加灵活，减少操作风险；也使应用系统在多中心的切换更加快捷，避免过多的系统网络调整，提高工作效率。通过合理，稳定，可靠的域名解析系统，满足应用同城双活、异地应用灾备需求，提升整体业务连续性。

采用分区架构理念，DNS 系统分别部署在双数据中心业务二区域、业务三区域、广域网区域、运维管理区域，很好的阻断终端业务跨区域、跨网段、跨路由的流量请求现象，提高网络服务安全性。同时针对不同的应用服务场景，域名解析采取动静分离方式，提高动态业务可靠性的同时，静态域名的分离，缓解了业务的压力。

内蒙古农信社建设覆盖双中心的智能 DNS 服务体系，支撑两地三中心架构建设，带动全产业支付服务升级和数字化转型，建设具有地域特色的农金业务。

# 齐鲁银行：夯实金融科技底座，助力中小银行数字化转型

齐鲁银行股份有限公司（以下简称“齐鲁银行”）随着数字化转型工作的开展，各类数字化创新和应用紧密融入业务和运营，提升金融科技能力和业务连续性水平，夯实金融科技底座，打造具有齐鲁特色的金融科技服务体系，积极助力银行数字化转型工作开展。

## 坚守初心，完成数字化转型，构建新服务型科技体系

齐鲁银行坚守“服务城乡居民、服务中小企业、服务地方经济”的初心本源，紧跟山东省新旧动能转换、济南科创金融改革试验区建设等重大战略，扎实服务实体经济。未来，齐鲁银行将以“打造行稳致远的精品银行”为目标，按照“守正奋发、转型创新、稳健合规、严管精治”的经营思路，以数字化转型推动全行高质量发展。全行信息科技发展围绕数字赋能的整体战略，以赋能引领、敏捷创新、提升科技能力、保障信息安全作为总体指导思想，达成“构建以能力提升为依托、以数字赋能业务为愿景的新服务型科技”的总体目标。

## 域名改造助力数字化转型，构建稳健、智能、安全的服务体系

齐鲁银行伴随数字化转型的开展，在完成两地三中心建设的基础上，根据同城灾备中心应用级灾备中心的定位，进行分布式业务多活、高度冗余架构的技术改造，需要一套智能化域名解析系统作为行内应用系统访问的总门户，对应用系统访问数据流量进行调度和负载分发。银行借助我国互联网域名服务头部企业的能力和产品，长远规划域名使用空间，完成应用系统的域名化设计规范，并进行应用系统域名改造，支撑行内应用系统建设和更新，为多中心、分布式、负载均衡的业务模式建设奠定基础。通过生产中心、同城灾备中心进行智能域名解析系统的分布式部署，使系统本身具有高可用性和较高的应急恢复能力，结合域名管理办法和使用命名规范，构建稳健、智能、安全、易扩展的域名服务体系。

## 智能域名解析系统保证行内业务稳健管理与灾备切换的关键利器

智能域名解析系统在支撑业务多活、敏捷冗灾的基础上，通过 API 接口与行内灾备切换管理平台对接。它能够为银行的数据中心生产和同城灾备切换提供全面的解决方案。系统具备稳健、智能、安全的特性，能够快速响应并处理网络请求，确保银行应用系统的高可用性和业务连续性。无论是在正常运营环境还是在灾难恢复的情况下，智能域名解析系统都能有效地管理和调度网络流量，保证用户能够顺利访问银行的各项服务。

通过集成 API 接口和灾备切换管理平台，系统可以实现快速切换，并及时将流量引导到备用的数据中心，以确保业务的持续运行。这样的一站式解决方案为银行提供了便利和可靠性，使其能够在面对各种网络故障和灾难事件时保持高效的运营和服务水平。

## 智能域名解析系统提升用户体验、确保可用性的关键技术

当用户访问某个域名时，域名解析系统会通过算法选择用户体验最佳的服务地址，以提高用户的使用体验。如果某个资源节点无法提供服务，DNS 服务器会将不可用的 IP 地址从域名解析结果中删除，并通知网络中的其他 DNS 服务器。这样，全网的用户都能获取到可用的解析结果，确保他们不会访问到不可用的资源节点。

在资源节点恢复正常后，域名解析系统会自动感知并重新恢复该节点的使用。这项可用性监测功能保证了用户的连续性，降低了故障对业务的影响，从而进一步提升了最终用户的使用体验。

智能的域名解析系统在提供优质服务的同时，还能减少用户与不可用资源的接触，避免无效请求，节省了用户的时间和精力。它确保了持续的服务可用性，并使用户可以畅享流畅、快速且可靠的网络体验。

# 珠海华润银行：业务应用系统域名化改造，赋能新一代银行系统智能容灾建设

华润银行作为一家扎根于粤港澳湾区核心区域的银行，正积极参与湾区建设，专注产融结合、融融结合，形成金融服务产业、产业助推金融的增长模式，坚定“打造粤港澳大湾区特色商业银行，构建金融基础设施信创平台”的战略定位，围绕产业金融、普惠金融、绿色金融、科技金融、新基建金融、跨境金融六大领域，为客户提供智慧综合金融服务，致力成为创业者、创新者、创造者的银行。

稳定、灵活、可靠的 IT 支撑系统是金融业提供智慧综合金融服务的科技基础，而作为信息化建设的核心基础设施，域名系统 (DNS) 的体系化、规范化建设将对构建稳定的信息化底座尤为重要。现网环境生产中心服务器及应用程序大多采用 IP 地址直接通信的方式，导致 IP 变更时会涉及一系列相关系统调整，产生较大变更风险。

## DNS 智能系统，实现新一代银行系统智能容灾调度

为适应新一代银行系统建设需求，以及 IT 战略未来规划两地三中心架构、实现应用多点接入、灾备快速切换、应用维护便捷等目标奠定坚实的技术基础，华润银行携手国内域名领域权威机构，搭建一套具有高可靠性、高扩展性、高处理能力的金融级智能 DNS 系统，通过域名智能调度构建珠海和汕尾双活数据中心架构，实现业务系统双活或主备部署，其流量通过域名方式进行业务导向，将客户端的请求发送到就近的数据中心，当任何一个节点数据中心业务出现异常情况时，可通过域名方式实现业务数据流的服务切换，保证客户端访问数据发送到可用的数据中心，从而确保业务系统的高可用服务模式，提升用户访问体验。

为满足基于域名调度的业务双活建设要求，行内业务系统域名化改造主要从内部 DNS 规划建议、业务域名化梳理改造、DNS 整体架构设计建议等方面展开，梳理行内若干套业务访问关系，以及每套业务系统内部访问关系，构建从前端、应用、中间件、数据库完整链条关系，为华润银行双活数据中心业务智能调度做好准备工作。

## 应用系统域名化改造，赋能全网 IT 基础架构升级

华润银行携手国内域名领域权威机构，通过对前期业务梳理、部署方案设计、应用系统 TTL 时间确定、改造进度制定、测试与开发环境改造及生产环境改造等域名化过程中各阶段的稳步推进，整体实现域名化体系规划，明确域名化命名规则，确定域名化改造实施方案，形成前端开发 / 测试 / 生产访问关系流程图，对开发 / 测试 / 生产环境进行域名化改造验证并生成相关测试报告。同时，华润银行携手域名服务机构展开域名命名规范调

研，确定域名规划与规范，根据域名命名规范，输出每套业务域名，搭建域名服务器，配置每套业务系统域名记录，对测试环境中的全部业务系统完成改造和验证，以确定域名解析改造正常运行。

华润银行通过域名化改造完成全网 IT 架构升级，为构建安全、敏捷、弹性的双活 / 多活数据中心，实现应用多点接入、灾备快速切换、应用维护便捷等奠定技术基础，为客户提供优质智慧综合金融服务。

此外，华润银行根据 DNS 整体部署策略和业务对 DNS 系统的要求，并遵循金融行业内最佳实践的原则，采用了新一代双层 DNS 架构设计的原则，部署缓存 DNS 服务器直接面向全行用户提供 DNS 解析服务，部署权威 DNS 服务器负责行内域名解析功能。同时，在双数据中心不同业务区中分别部署服务及管理节点，实现所有 DNS 服务节点的数据统一配置及管理，以 HA 或前置负载 SLB 架构组成高可用域名服务集群，面向数据中心业务系统和办公终端提供高质量的域名解析服务。借助 GSLB 智能解析调度功能，实现双中心的业务双活及灾难情况下的业务迁移，极大改善了华润银行线上业务的服务质量，提高其业务连续性保障能力。

华润银行国内域名领域权威机构协助下通过制定域名空间命名规范，内网域名从无到有，逐步实现域名体系建设；应用系统进行域名化访问后，大幅提高应用的灵活性，实现应用的数据中心级多活及快速切换，将 RTO 时间缩小至分钟级；统一的集中管理，配置下发、状态监控、日志收集，降低用户的管理难度，减少配置过程中出现的失误，基于统一管控实现多节点的智简运维，降本增效。

# 福建海峡银行：智能可靠 DNS 体系建设，多活数据中心应用域名化探索与实践

福建海峡银行自 1996 年成立以来，一代又一代的海行人坚守初心本源，在助力实体经济发展、帮扶民营小微、服务城乡居民、践行社会责任中做先锋、挑大梁，不断为地方经济发展贡献金融力量。

福建海峡银行秉承“服务地方经济、服务民企小微、服务城乡居民”的市场定位，努力探索差异化、特色化发展道路，逐渐形成契合当地经济发展的业务特色与竞争优势。2022 年获评“服务福建经济三星银行机构”“服务民营企业和中小微企业三等奖”，伴随着“产业 + 园区 + 金融”综合服务方案，品牌价值不断提升。

## 应用域名化的意义与价值

支持创新，服务发展，福建海峡银行立足地方经济，充分运用科技赋能金融服务。在数字化转型升级中，通过分布式业务多活、高可靠冗余架构技术结合应用系统域名化改造升级，进行两地三中心数据中心升级建设。

随着银行业务的发展，应用功能日益丰富。例如，手机银行应用程序就内嵌了许多功能节点。如果所有应用功能都集中部署在一台服务器上，就会存在集中式的风险，单一服务器难以承载各层面的性能、功能需求。在分布式部署的环境中，过往 IP 与业务应用紧耦合、强关联，业务互相嵌套、访问逻辑复杂，无法满足应用业务级多元化、永续服务的需求，“云化时代”必须对应用进行横向解耦和拆分。

应用域名化改造，让用户与应用、应用系统内部各组件、各业务应用系统间实现域名化交互，是破解制约金融机构多中心业务冗灾建设、构建更灵活多中心架构的重要手段。完成应用服务域名化建设，能够有效地降低应用升级和变更影响，实现敏捷开发、敏捷运维、敏捷服务。域名化的改造粒度越深，调度能力的细密程度越强，业务的连续性服务保障便越充足。

在域名化改造的推进过程中，海峡银行多部门合作联动参与，从域名命名规划、不同场景基于域名的流量调度策略制定，对域名服务器部署架构设计、业务系统、终端数据全面收集与整理，业务逻辑梳理、可行性评估等，为后续的域名化改造“打牢地基”，提供强而有力的支持。

进行域名化改造的系统将通过测试区和准生产区的测试、验证、优化，后续根据不同业务系统的重要性、优先级分批完成改造上线，通过合理的规划，让海峡银行的域名化改造建设能够高效、稳定地推进。

## 域名服务体系建设演进之路

海峡银行高度重视应用域名服务体系建设，通过体系化的 DNS 系统设计思路和采用业务成熟的层次化 DNS 服务器部署架构，建设稳定可靠、智能高效、可管可控的海峡银行 DNS 系统。

在主数据中心以 HA 双机架构部署两台管理节点，且在同城数据中心部署第三管理节点，三台管理节点数据实时同步，任意一台管理节点状态正常即可对全网 DNS 服务节点管理，进行配置下发，数据收集等操作。DNS 系统的管理平面与业务平面分离部署，确保管理节点全部故障的场景下，解析业务不受影响，降低故障风险，提升 DNS 系统的稳定性。

不同的业务区域，如网银区、业务前置区等分区单独部署 DNS 服务节点，实现终端解析区内最优访问，避免终端客户跨区域、跨网段、跨路由等流量请求信息，提高网络服务安全性。各区 DNS 解析服务节点都通过 HA 方式部署且终端（服务器）同时配置双数据中心 DNS 服务器 IP，实现双重冗余保障。

智能化的 DNS 系统，能够提供基于各种负载算法以及对应用系统的健康检测，通过智能权威域名解析手段实现对业务流量的精细化引导，确保行内各应用系统根据预设的应用场景实现业务多活或主备，支撑金融业务的永续运行。

当前海峡银行已进入深度域名化阶段，域名解析是海峡银行信息化建设的核心组成部分，为避免极端情况下全 DNS 节点都出现异常导致业务系统无法正常运行的场景，海峡银行在原有域名解析服务架构基础上，异构部署了一套 DNS 监控应急系统。该系统能够针对 DNS 的解析情况进行监控分析，针对 DNS 的配置进行自动定期备份，且在极端情况下能够快速应急接管全网解析服务，保障紧急状态下的域名访问。

海峡银行在 2021 年初开始进行域名化改造建设，2021 年 12 月完成两地三中心 DNS 系统建设并按计划开始在测试环境对业务系统域名改造进行测试验证。于 2023 年中已完成超过 20 套业务系统域名化改造正式投产上线。

未来，海峡银行将持续不断对域名化改造、对域名体系建设进行探索与实践，通过新技术赋能业务场景，满足业务发展需求，加快推进新时代数字银行、科技银行建设，为客户提供更优质的金融服务。

# 广西北部湾银行：智能 DNS 改造升级，强化根基保障数字化金融转型

广西北部湾银行通过智能 DNS 改造，强化互联网关键基础设施，保障网络安全，赋能数字化金融转型。

广西北部湾银行是顺应国家实施北部湾经济区开放开发战略，在原南宁市商业银行基础上改制设立的省级城市商业银行，于 2008 年 10 月挂牌成立。银行坚持差异化发展战略，打造核心竞争力，为北部湾经济区开放开发和广西经济发展、中国一东盟自由贸易区的建设提供强有力的金融支持。

## 数字化转型，护航北部湾银行高质量发展

近三年来，广西北部湾银行持续加大金融科技投入，年均增幅超 1 亿元。2020 年，一次性投产包括 1 个核心系统、1 个云数据中心、57 个新建系统、107 个配套系统且平稳运行，核心系统效率提升 16 倍；2021 年，在去年基础上高标准推进覆盖前、中、后台领域 28 个新系统建设，数字小微系统、供应链金融系统、新决策引擎系统、RPA 机器人等项目也相继投产，人工智能、OCR、生物识别等技术应用由点及面迅速扩大，这些数字化转型项目正成为银行金融科技以及业务创新的新基石，银行数字化转型的战略意图也正在变成现实。

同时，广西北部湾银行在组织架构中首次设置了科技职能板块，并在业务条线组建敏捷开发团队，稳步推进开放银行建设，以客户为中心，将金融科技引入业务全流程、全领域，服务体验、内部管理持续提速增效，围绕“医、食、住、行、游、娱、购、学、养、健”的多样化、组合化、智能化，“金融 + 场景”服务多点开花，越来越多金融服务从“纸上”向“指间”转变。在大数据、云计算等新技术加持下，银行构建全新数字化风险管理模式，不良贷款率大幅优于全国、全区同业平均水平。在 2021 年英国《银行家》杂志全球银行 1000 强排名中升至第 370 位，中国服务企业 500 强中升至第 334 位，在中银协 2021 年度“陀螺”评价全国 130 多家城商行中排名第 22 位。

## 智能 DNS 升级改造，强化根基保障数字化金融转型

金融创新以及数字化离不开互联网科技的应用，而伴随金融数字化、线上化发展，充分发挥互联网科技力量保障数字化转型及金融创新，成为银行业的重中之重。域名系统 (DNS) 作为与联网关键基础资源，为数字金融的高可用及安全运营提供根本性保障。

2020 年 7 月，广西北部湾银行南宁五象生产数据中心投入使用，由此形成了由五象数据中心 ( 生产中心 ) 、金融大厦数据中心 ( 同城中心 ) 以及玉林数据中心 ( 异地中心 ) 构成的两地三中心架构。在国内权威域名服务机构帮助下，银行实施了智能 DNS 改造计划，通过在行内有序推进域名化改造在五象、金融大厦和玉林三个数据中心分别部署多台智能 DNS 设备，让关键业务系统具备多数据中心业务负载均衡、业务迁移以及灾备切换能力。基于智能 DNS 对业务系统负载状态、物理分布、网络资源情况的调度业务交互，实现五象、金融大厦两个数据中心业务系统的智能调度及负载均衡，在业务系统发生故障的情况下还可将业务向玉林异地数据中心快速迁移，最大限度缩小 RTO，减少业务停顿时间，提升灾难应急处置能力。

作为“广西自己的银行”，广西北部湾银行将持续改造升级域名系统，进一步打造全国产化的信创 DNS 服务平台，稳步推进金融基础设施国产化，持续完善互联网关键基础设施，支撑省级主力金融平台、金融创新平台、地方金融人才培养平台建设，用金融力量助力区域经济高质量发展。

# 潍坊银行：坚定不移推进“域名化建设”，构建数字化发展根基

潍坊银行顺应数字化发展趋势，以数字驱动和敏捷转型激发创新动力，纵深推进数字技术与业务、管理深度融合，打造新型数字基础设施、深化关键核心技术应用，打造“数字银行”“平台银行”“生态银行”未来银行模式，建立“数字、智慧、绿色、公平”的金融服务能力，有力支撑创新驱动发展、数字经济、乡村振兴、碳达峰碳中和等战略实施，走出具有中国特色与国际接轨的金融数字化之路，助力经济社会全面奔向数字化、智能化发展新时代。

潍坊银行坚守“立足地方经济、立足小微企业、立足城乡居民”市场定位，坚持党建引领和稳中求进的总基调，聚焦公司金融、零售金融、金融市场、数字金融四大业务，深入推进数字化银行建设，努力践行社会责任，致力于打造质量好、效益好、服务好、管理好、团队好、信誉好的“六好银行”。近年来，潍坊银行“谋转型”，持续完善金融科技顶层设计，立足差异化竞争优势，制定系统的数字化转型战略，明确目标、强健肌体、释放动能，在数字金融发展中跑出“加速度”。

## 技术“壮骨”，积厚成势，未来可期

积极推进建设“敏稳双态”的 IT 架构体系，加快推进传统架构向分布式架构转型。2022 年完成数据中心基础设施架构升级，异地灾备中心基础设施扩容，稳步推进 DNS 系统建设，灵活支持“两地三中心”的多活架构体系，实现业务快速切换、应用多活、安全防护等场景，全面提升数据中心业务连续性及高可用性。

### 加速域名化改造，构建数字化发展根基

在进行域名化改造之前，应急灾备切换演练是一项极其复杂的工作，过程极其漫长，极易出现疏忽、遗漏导致切换失败的风险。当完成域名化改造后，业务系统的数据流量全部基于 DNS 指引进行交互，通过制定合适的健康探测手段，结合多级的调度策略，便捷地实现手动或自动的灾备切换操作，极大地缩短了 RTO 时间。

### 建设安全智能 DNS，完善双活灾备调度能力

依托于域名化改造的完成，对业务系统的健康状态进行检查，及时发现异常并自动完成切换，降低运维成本的同时，提供业务系统的高可用性，利用智能 DNS 的 GSLB 全局负载功能，感知应用健康状态，实现自动化的流量负载和灾备切换。

### 纯国产服务系统，实现自主可控

传统 DNS 软件存在非自主可控、断供、制裁、漏洞、后门等方面的安全风险。信创时代，潍坊银行积极推动金融创新，不断提升服务水平和用户体验，以适应现代金融业的发展趋势。

雄关漫道铸辉煌，乘风破浪续新篇。潍坊银行将站在新的历史方位，全面贯彻新发展理念，牢牢把握住数字化时代赋予的新机遇，以数字化转型为引领改革创新的总抓手，以数字化理念为企业文化强力内核，以组织机构改革为内生发展动能，以数据和技术为关键生产要素，以开放生态为重要生产方式，科学、合理、深化自身的数字化转型布局，以深入、彻底的数字化转型，引领潍坊银行高质量发展。

# 泉州银行：智能域名体系建设，铸造“业务永续”数字底座

泉州银行股份有限公司（简称：泉州银行）是成立于 1997 年的股份制商业银行，总行设于福建省泉州市，多次入选英国《银行家》权威披露的“全球银行 1000 强”榜单，荣获 2022 年度全国城商行‘十佳零售银行’奖项。

泉州银行始终坚守服务地方经济发展的使命担当，积极深化金融科技应用，赋能金融服务提质增效。近年来，泉州银行深度融入泉州数字经济发展大潮，全面推进“泉之心”重大战略工程落地，通过新核心项目群和新数据中心两大软硬件项目建设驱动升级关键基础设施，构建安全稳定、智能高效的数字底座，实现对客服务、业务发展及经营管理等全方位质的提升，为地方经济高质量发展贡献金融力量。

## 两地三中心域名系统建设之路

泉州银行为更好服务用户，借助新数据中心建设的契机，进行全面应用域名化改造，实现同城双活中心，异地灾备，智能化精准流量调度，为客户构建一张“业务永续”的数字基础底座网络。

泉州银行采用两地三中心架构，泉州东海数据中心为主数据中心，恒祥数据中心为同城数据中心，异地灾备机房部署在福州。为满足业务创新、数字化转型的需要，更好服务用户，泉州银行为保障业务的连续性，从顶层规划出发，对已有的传统两地三中心架构进行重构，全面进行应用域名化改造与域名体系建设是核心重点之一。

以 DNS 为根基，进行“新两地三中心”升级建设

第一，建设东海数据中心 IT 基础设施，东海新数据中心通过智能 DNS 解析系统，实现生产区域同城双活，分担业务、网络负载访问量，端到端实时可用，并实现自动容灾切换，将数据、业务、网络连续性落到实处，充分利用双中心资源，解决主备数据中心手动切换中断时间长、数据丢失不可挽回等问题。

第二，进行数据中心迁移工作，将恒祥数据中心整体平滑迁移至东海数据中心。

第三，进行恒祥数据中心优化改造工作，将恒祥数据中心进行设备资源整合（含现有同城灾备中心资源），并优化改造成同城双活数据中心，提升整体可靠性、容灾能力。

## 稳中向前，新时代数字化域名体系构建

在这全面 DNS 建设部署过程中，泉州银行体现出“与众不同”之处。与传统 DNS 设备替代方案不同，泉州银行从全局出发构建坚实的“两地三中心”架构，综合考量了业务、网络分区、业务应用服务、IPv4 向 IPv6 过渡等问题，不仅构建两地三中心安全、智能架构，也面向未来的数字化趋势牢筑 IT 基础设施网络根基。

**网络分区，让连接更清晰**。泉州银行意识到在数字化深化发展过程中，网络应用规模增大、线上业务增多，更规范的网络分区与物理分区相结合十分关键。因此以新建东海数据中心为契机重新规划网络分区，按照如核心

区、广域网区、运维管理区、互联网区、生产区等不同区域，构建“解析服务分区部署，管理服务统一入口”的同城双活智能化域名调度体系架构。通过物理与网络的解耦，通过 IP 地址与应用服务的解耦，大幅度提升业务连续性，实现优化调度。

**全面推进域名化改造，升级数字基础底座**。泉州银行全面进行业务系统的域名化改造，实现业务系统内部、业务系统之间、客户端访问业务系统都使用域名访问。双活业务的建设，主数据中心、同城数据中心将利用智能 DNS 的 GSLB 全局负载功能，感知应用健康状态，实现自动化的流量负载和灾备切换。域名化改造是实现基于域名进行业务流量走向精准控制的基础，DNS 服务则是具体承载域名解析和流量调度的重要基础设施，建设一套稳定可靠、智能化、高可用、易管理的域名系统，能够最大化的保障业务系统的可用性，推动全行的业务快速发展。

伴随数字化已经深入到各行业领域，金融系统更是成为数字化建设的“排头兵”。泉州银行以高性能、高可用、高安全、可管理、易扩展为原则，积极构建满足业务发展需求的对现有两地三中心架构进行重构升级。这其中，对域名系统全面统一规划、管理、升级，使其成为多数据中心、应用多点接入等 IT 战略规划建设奠定必要的基础，推动泉州银行银行核心网络建设，为泉州银行数字化转型牢筑底座。

# 泰康集团：智能 DNS 服务平台安全、高效满足混合云业务服务模式

泰康集团作为世界 500 强企业和国内头部大型保险公司，一直奉行专业化、规范化、国际化的发展战略，在泰康集团现代化、全球化、差异化的发展过程中，在信息化建设方面持续投入，目前泰康混合云数字化服务平台已成为集团信息化业务的核心支撑，在公司内部员工、客户、合作伙伴、供应商之间提供高效业务流转。

## ZDNS 为泰康集团混合云构建智能化解析平台

泰康集团在业务快速增长的同时，开始受到应用服务质量提升、系统管理模式变革等方面的挑战，由于集团原有域名解析服务体系采用微软 DNS 系统，已无法满足泰康集团复杂网络架构下的业务调度需求。

ZDNS 围绕泰康集团混合云业务服务模式和运营特点，以集团“统一管理、灵活智能、安全可靠”的要求为建设目标，为用户构建面向全网的智能 DNS 服务平台。遵循金融行业对网络安全隔离要求和原则，平台采用双管理平面和高可用架构设计，分别覆盖泰康两地三中心互联网区和生产区，实现管理层面的系统隔离，并对两大区域所有 DNS 服务节点进行统一管理；CMS 集中管控平台同时与集团原有 AD 域控结合，进行域名数据打通，实时同步用户入域时的注册记录；针对客户多地多中心场景下的业务解析调度需求，定义生产和灾备双视图，制定跨区跨网的解析请求转发策略，实现业务流量智能牵引，满足异地冗灾快速切换；DNS 平台提供了精细化且多维度的解析日志数据，帮助用户在业务运营分析、运维管理排障方面提供了信息支撑，使得信息系统管理水平上升到一个新的台阶。

# 海通证券：专业 DNS 助力为科技型投行筑牢网络根基

作为行业数字化转型的探索者和先行者，海通证券在过去五年中，紧跟国家战略，制定了十三五科技规划，以“统一管理、自主可控、融合业务、引领发展”科技方针为指引，应用架构、数据管理、基础设施、科技治理四大领域 25 项重点任务全面落地。

在全面科技赋能之下，海通证券得以重塑“数字海通”的四梁八柱，整合共享能力、系统处理能力、风险管控能力、自主可控能力、敏捷创新能力、业务融合能力提升明显。2023 年既是十三五规划的成果展示之年，更是十四五规划的谋划之年。“数字海通 2.0”也将全新启航，中国领先的科技型投行呼之欲出。

把深化证券科技运用作为第一生产力，推进证券业数字化转型和高质量创新发展，已经成为证券行业的共识。科技赋能，首先重塑的是前台各个业务条线。具体来看，海通证券在四大前台业务领域深入推进数字化转型，深入开展线上化服务。

海通证券作为国内领先的大型证券公司，随着两地三中心建设及新的办公地点的启用，现有 DNS 体系已不能满足新产生的域名解析需求。全国营业部互联网解析流量分散且安全事故频发，所内也亟需建立新的 DNS 解析体系以适应不断发展的网络要求。通过专业的 DNS 设备 DNS 安全防火墙提供丰富的安全统计报表，通过对各类安全威胁事件聚合分析，直观反映企业发生安全事件的攻击频率、严重程度、威胁事件背景等，帮助网络运维和安全团队掌握企业内的威胁现状，并提供指导响应的详细威胁背景信息，为安全防护和追溯提供有效的依据。

金融科技发展是海通证券金融科技持续领先的一个缩影。近年来，海通证券强化顶层设计，秉持“科技引领”发展战略，正式发布《海通证券股份有限公司十四五科技发展规划（2021-2025 年）》，升级金融科技创新体系，成立了金融科技创新实验室，以建设“数字海通 2.0”为目标，全面布局人工智能、区块链、云计算、大数据、移动互联网、物联网人工智能等领域，率先进入数字化转型的深水区，为行业数字化转型提供模板和样例。

凡是过往，皆为序章。海通科技将继续发扬工匠精神，坚持脚踏实地作风，传承精益求精品格，深耕金融科技应用创新，全面赋能业务，为打造中国一流的科技型投行砥砺前行。

未来公司将继续秉承“科技引领”发展理念，深入实施十四五科技发展规划，持续推进金融科技创新和数字化转型，全面提升服务实体经济、赋能普惠金融能力，彰显中国企业在全球金融数字化转型浪潮中的示范、带动、引领价值，谱写数字化转型华章。

# 中信建投：夯实网络根基，构建创新数字基础设施

加强金融行业信息基础设施自主可控能力，提升网络基础设施安全水平，中信建投证券股份有限公司（以下简称“中信建投”）高度重视新型数字基础设施建设，加强信息技术自主可控能力，筑牢网络根基。

当前，国家高度重视各行业数字化建设，强调以顶层设计为核心、以政策制定和部署落实为重点，加快数字化治理体系构建，提升数字关键技术创新水平，推进数字化转型建设步伐，共建长期、稳定、良好数字生态。

证券经营机构主动贯彻落实国家数字化发展建设的政策要求，各证券公司以数据资产为核心，以新型数字基础设施建设为抓手，以技术服务业务为导向，驱动业务创新和服务优化，推动经营质量高速发展。证券公司在实现数字化转型的过程中，通过新型“数字基建”推动数据资产转变为企业持续增值的发展动力，促进客户服务、产品运营的创新和发展。因此，实现数字化运营是证券经营机构数字化转型的重中之重。

## 构筑自主可控的网络底座

中信建投是经中国证监会批准设立的全国性大型综合证券公司。公司总部位于北京，在全国 30 个省、自治区和直辖市设有 300 余家证券分支机构，5 家全资子公司。

加强金融行业信息基础设施自主可控能力，提升网络基础设施安全水平，中信建投高度重视新型数字基础设施建设，为筑牢行业安全、可靠的信息底座探索路径，也在积极推动金融科技转型，并借助人工智能、大数据、云计算等新一代 ICT 技术的落地应用，推动各项业务与金融科技深度融合。

中信建投高度重视网络安全等级保护措施和关键信息基础设施安全保护，对网络设施进行常态化安全管理，智能化、主动防御成为了网络安全工作的核心，并积极探索创新技术、构建自主可控的、完善的网络安全组织、打造高效的安全防御体系。在金融行业数字化转型持续深入推进的今天，金融机构对应用架构和 IT 架构也提出了更高要求，包括更好的服务体验、更强的产品竞争力及更加敏捷的系统架构。为此，金融机构必须进一步优化应用架构并对其进行全方位升级和改造。

中信建投在其金融科技体系中设立信创专区，信创区的域名服务由国产领先设备承载，信创区按功能不同又划分为业务区和运维区。其中业务区由采用 HA 冗余架构部署的 DNS 解析节点承载，提供业务连续性保障、精准流量调度的解析服务；在运维区，通过同样采用 HA 架构部署的 CMS 集中管控平台实现解析节点的统一管理、统一监控、统一运维，提升运管效率。

通过整体网络架构升级以及国有产品替代，中信建投构筑了更加自主可控的金融行业网络底层基础设施。为我国证券市场在以 5G、大数据为代表的新一代信息通信技术应用过程中，网络基础设施的安全、高效，走深走实。

中信建投与 ZDNS 联合筑牢网络根基，ZDNS 信创产品自主研发 DNS 核心解析软件“红枫”，并采用国产 CPU 和操作系统等核心组件，产品性能稳定高效，在

满足自主可控的要求前提下，为客户域名系统的建设提供了有力支撑。

## 创新技术深化应用场景

在金融行业数字化转型持续深入推进的今天，依托自主技术支撑产业，金融信创体系建设，逐渐形成了良好的生态环境，金融机构可以优选采用国产芯片、操作系统、数据库等基础软硬件产品，提高信息安全和数据安全保障能力。随之对应用架构和 IT 架构也提出了更高要求，包括更好的服务体验、更强的产品竞争力及更加敏捷的系统架构。同时，金融机构也需要运用人工智能、区块链、云计算、大数据等新兴技术，将科技创新应用于金融业务场景，提高业务效率和安全性。

中信建投作为国内领先的综合类证券公司，一直致力于利用创新技术深化应用场景。在系统架构方面，中信建投注重网络与接入安全，与 ZDNS 携手打造高性能、高可靠、高安全的网络架构和设备。在业务支撑方面，中信建投打破了传统的数据库加中间件的“烟囱式”架构，实现了基础架构平台化，构建了大数据平台、人工智能平台、云平台、区块链平台等 IT 支撑平台，实现了“数字化、自动化、智能化、知识库”的落地目标。以其优秀的 IT 体系作为后盾，在业务创新方面中信建投如鱼得水，利用人工智能、区块链、云计算、大数据等新兴技术，开展了未来元宇宙、数字货币、数字人等多个领域的探索和实践。

中信建投通过夯实网络根基，构建创新数字基础设施，为金融行业数字化转型提供了有力的支撑和示范。中信建投将不断推进金融信创体系的建设和完善，为客户提供更好的服务体验和更强竞争力的产品。

# 02 政务

建设数字政府是国家战略。近年来，各级政府业务信息系统建设和应用成效显著，数据共享和开发利用取得积极进展，一体化政务服务和监管效能大幅提升，“最多跑一次”“一网通办”“一网统管”“一网协同”“接诉即办”等创新实践不断涌现，但同时，数字政府的数据开放共享、平台智能化建设等还有待加强。下一代 DNS 为数字政府建设提供了重要的底层支撑。通过域名集约化管理服务，赋能数字政府的智能集约平台支撑体系建设。

统建统管，域名体系标准化与解析管理集约化相结合。政府主管部门需从顶层规划出发，统筹设计各层级的域名服务体系，制定域名使用规范及系统构建标准，明确管理机构、域名空间及命名规则、系统建设标准、注册审批流程等要求，规范各机构的域名应用，确保域名体系的连贯性、可持续性。打造政务域名体系治理的抓手，筑牢政务信息化的底座。

业务使能，提升政务服务应急保障能力，优化“互联网 + 政务服务”体验。而基于 IP 的传统业务交互方式，在面临多中心业务多活、快速灾难迁移、业务流量精准牵引的需求时，呈现出了较强的局限性，导致政务 ICT 架构固化，缺乏灵活性，阻碍政务上云的进程。因此，开展政务数据中心、应用系统的深度域名化改造，打破 IP 与业务的紧耦合状态，实现政务业务基于域名的交互，是奠定多中心冗灾建设的重要基础，也是业内的共识。基于域名的业务交互模式，让上层业务与底层网络解耦，更有助于跨部门间业务协同、系统整合、数据共享；同时，域名化改造配合智能域名系统解析服务，基于政务业务系统的健康状态、业务请求来源的属性特征，可实现业务流量的精准牵引，常态下支撑多中心的业务负载均衡，优化政务服务体验；灾难场景下实现业务跨中心的快速迁移，保障政务服务的业务连续性。

安全加固，补齐短板，建立更加立体的政务安全防护体系。以往在政务信息安全防护体系中，DNS 的安全常常被忽略，成了立体安全防护体系中的短板。政府机构需采取措施，通过域名服务状态异常监测、威胁行为识别、过滤拦截处置、精准溯源定位、域名安全态势分析等技术手段构建具备高级安全防护能力的域名服务体系，针对政府内外网域名服务开展日常监测、定期安全评估，构筑立体的信息安全防护体系，打造第一时间识别、第一时间处置、第一时间恢复的政务安全保障能力。

# 国家信息中心：云地一体 DNS 服务架构，全面提升政务外网服务能力

国家信息中心引入云地一体 DNS 系统架构，在国家电子政务外网中央平台互联网区部署基于 BGP+ANYCAST 全球分布式云解析服务以及 4 台 DNS 本地设备，组成云地一体 DNS 集群，提供多个互联网核心业务的多活解析服务，使得 DNS 系统具备满足国家信息中心未来几年业务发展需要的能力，提升了政务外网的服务体验和用户满意度。

国家信息中心作为国家电子政务外网中央平台的建设者和运营者，对平台的数据资源体系和数据安全体系格外重视。政务外网承载多个核心政务业务系统，随着政务外网用户数量的不断增加，对解析服务质量提出了更高的要求。因此在建设 DNS 系统过程中，要充分考虑如何保证政务外网业务信息系统及相关办公信息系统的持续运营；要着力提升政务外网内部网络访问体验及访问速度；要重点增强政务外网信息系统的安全保障和攻击防护能力。

通过科学分析应用需求，专业域名服务机构 ZDNS 为国家信息中心引入云地一体 DNS 系统架构，在国家电子政务外网中央平台互联网区部署基于 BGP+ANYCAST 全球分布式云解析服务以及 4 台 DNS 本地设备，组成云地一体 DNS 集群，提供多个互联网核心业务的多活解析服务。其中本地设备服务资源独享，保障服务能力下限。ZDNS 公有云平台则基于分布式、大带宽、高冗余和独有的 6 层 DNS 攻击防护技术提供过亿 QPS 的服务承载能力，全面提升国家信息中心解析服务能力的上限。

此外，在公共区部署 4 台 DNS 设备，组成高性能 DNS 服务集群，分布在不同业务区，面向不同的对象提供差异化、高质量的域名解析服务，缓解其业务压力。同时 DNS 服务集群的建设，助力国家信息中心依靠终端的主备 DNS 实现冗余效果，当主 DNS 发生故障时，终端自行切换到备用 DNS。

为进一步提升信息系统运维能力，深入挖掘信息系统大数据潜在价值，ZDNS 配合国家信息中心共同构建 DNS 监控和大数据智能统计分析系统，实时监控国家信息中心 DNS 服务质量。深入分析 IPv4/IPv6 服务使用情况，推动 IPv6 规模部署。基于历史解析行为数据构建分析模型，提供事前攻击预警、事中攻击防护和事后攻击溯源的全过程事件分析处置能力。

在专业域名服务机构 ZDNS 的助力下，国家电子政务外网中央平台的 DNS 建设顺利完成优化升级，机构提供的方案具备良好的可扩展性，使得 DNS 系统具备满足国家信息中心未来几年业务发展需要的能力，提升了政务外网的服务体验和用户满意度。

# 最高法：域名服务体系助推智慧法院建设

最高法以促进审判体系和审判能力现代化为目标，以《人民法院信息化五年发展规划》为指导，坚持服务理念，把握“引领发展方向，驱动贯通融合，示范建设模式”基本路径，率先建成最高人民法院信息化 3.0 版，形成支持法院审判执行和其他各项工作智慧管理和运行的智慧法院。通过“互联网 +”行动，推动移动互联网、云计算、大数据、物联网健康快速发展。

## 域名服务体系规划：助力高法数字化转型，建设智慧法院

ZDNS 基于法院体系的全国组织架构、信息系统建设的长远规划，顶层设计其域名服务体系，包括域名空间、申领使用流程及制度、域名服务设施建设标准，形成了一整套的域名建设规范，为法院信息化建设的长远发展打下坚实基础。

基于 ZDNS 域名全生命周期管理平台，实现高法体系域名注册、使用、变更、退出全流程的平台化、系统化；沉淀域名资产，执行精细化的管理方式，让规划与制度有抓手、有管控手段、有落地效果；简化域名申请过程，实现业务的敏捷发布，降低域名审核人员精力投入，提质增效降本。管理业务分离的模式，集中管理、分布部署，改变了传统落后运维方式不可知、不可视、不可控的现状，助力高法信息化建设智简运维。

## 智能 DNS 解析系统：提高业务连续性、保障业务安全可靠

最高人民法院智能 DNS 系统建设实现以北京为主管理中心，广州、兰州和南京数据中心为辅数据中心的统一管理和统一配置下发的综合性、整体性和高可靠性的域名解析系统。

北京、广州、兰州和南京四地数据中心分别部署管理管理节点和服务节点。北京数据中心为主管理中心，其他三地数据中心为备管理中心，当北京数据中心的管理节点故障后可启用其他三地数据中心的任意一台管理设备接管当前故障管理节点业务保证管理中心业务的高可靠性。四地数据中心的 slave 节点（解析服务节点）通过 OSPF Anycast 架构实现个数据中心节点的负载均衡，即通过配置 Anycast，四地数据中心统一提供一个相同 VIP 给最高法院和各省高院客户端进行 DNS 解析查询。最高法院和各省高院用户端进行 DNS 解析查询时会向 VIP 发起解析查询请求，根据 OSPF 算法设备会选择最优的路径提供域名解析服务。

最高人民法院构建了一套支撑其多中心业务冗灾场景、稳健、高质量的域名服务系统，节点遍及全国四大数据中心，基于业务状态感知、请求来源精准识别、智能的调度算法实现全国不同区域的法院就近访问，实现四大中心的业务负载均衡、快速冗灾，极大的提升了高法业务系统的服务质量和稳定性。

# 全国海关信息中心：加速“本地 + 云”域名系统信创改造，提升“在线政务”服务可用性

全国海关信息中心采用 ZDNS“本地设备 + 云端服务”的云地协同服务建设方案，利用自主可控的下一代 DNS 技术，在互联网业务区实现全局负载调度，建设更为完善的“网络 + 应用”服务平台，赋能“互联网 + 政务服务”发展模式，为智慧海关的建设贡献力量。

海关总署负责全国海关组织工作，推动口岸“大通关”建设、海关监管等工作。随着互联网 + 政务服务模式的大力推进，全国海关信息中心加大了互联网政务服务领域的业务延伸，为了更好地提升“在线政务”服务可用性，需构建更为完善的“网络 + 应用”服务平台，以满足“互联网 + 政务服务”的发展需要。

## 域名系统升级改造，推进业务稳健向前

全国海关信息中心应用系统部署在两个数据中心内，每个数据中心以双线路进行接入。为了优化客户访问体验，降低用户端由于通过不同运营商线路访问在线业务时带来的跨运营商延时等因素影响，希望通过“域名”方式实现双中心、双链路的智能解析服务，从而实现数据中心容灾，提升业务系统的可用性。

针对互联网业务区建设方案，专业域名服务机构 ZDNS 提出了“本地设备 + 云端服务”的云地协同服务建设方案，实现全局负载调度。云架构与生俱来的抗 D 架构，有效确保了海关总署互联网域名解析服务的健壮性，云地二者互为备份、共同工作。

海关总署域名系统 (DNS) 整体采用双中心架构，为总署和各分署提供域名的静态和动态智能解析服务。同时，新增 CMS 中央管理器设备，实现对所有设备的配置和实时数据的收集，以及 DNS 数据和设备的配置、管理、网管、分析、应用服务器高可用等服务功能。此外在海关总署信息中心和地方分中心部署网络核心设备，开启递归、权威解析功能。

系统采用冗余架构，节点两两组成 HA 热备模式，确保解析服务高可用，同时基于该服务企业的业务状态感知和智能调度算法，支撑海关业务流量的智能牵引，实现两个异地数据中心之间的业务资源负载均衡。基于智能域名解析调度的系统交互，保证了海关业务的连续性与访问的敏捷性，而“云 + 设备”的部署，可最大程度抵御针对 DNS 的 DDOS 攻击和域名劫持等活动，让用户 IT 架构的安全防护能力得到持久保障。

海关总署聚焦域名系统的改造升级，旨在建设更为完善的“网络 + 应用”服务平台，赋能“互联网 + 政务服务”发展模式，为智慧海关的建设贡献力量。

# 上海大数据局：以新一代新技术为引擎，坚持融合创新，加快推进 IPv6 技术演进和应用创新发展

上海大数据局紧跟国家和行业脚步，致力推动 IPv6 应用深度融合，夯实网络空间安全，以新一代信息技术为引擎，发挥信息技术行业发展驱动作用，强化数字政府安全保障能力，加快建设高速泛在、安全可靠、绿色健康、可管可控的网络环境。

2023 年中央网信办、国家发展改革委、工业和信息化部联合印发《深入推进 IPv6 规模部署和应用 2023 年工作安排》通知，要求不断强化安全防护，扎实推动 IPv6 规模部署和应用向纵深发展，进一步推动政务应用 IPv6 演进升级。对于政府机构而言，IPv6+ 规模部署既是建设网络强国的重要国家战略，又是业务云化数字化转型的必经之路，充满机遇和挑战。为此上海大数据局制定了以 IPv6+ 为内核的新一代网络架构演进路线，致力于完善“IPv6+”创新生态和标准体系，不断巩固 IPv6 网络安全防护能力。全方位支撑上海大数据局数字化业务发展的统一融合、智能稳固、聚焦体验的新时代网络。

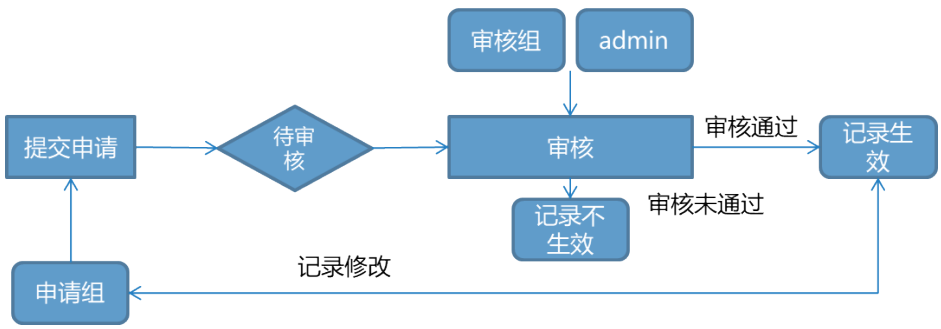
## 夯实基础，重点突破，完善“IPv6+”创新生态和标准体系建设

上海大数据局准确把握新发展阶段、新发展服务理念和新发展格局，以推动高质量发展为主题，深化供给侧结构，通过加强标准体系建设，夯实基础，重点突破，整体完善“IPv6+”创新生态。

### 统筹统建，提质增效

此次为全面加强 IPv6 应用信息资源的有序汇聚，实现统筹规划和域名体系顶层标准体系建设，按照“谁开设、谁申请、谁使用、谁负责”的原则，通过线上域名注册审批流转方式，实现域名分权分域管理。按需创建不同权限、分管不同区域的账号，所有的域名申请、注册、审批、变更、退出全部线上进行，域名审批流程线上流转，为不同部门、不同的业务的域名需要进行流程可视化审批，审批通过后可自动生效配置，快速建立域名台账管理能力，简化运维管理工作。

### 融合开放，深度挖掘



完善的日志、丰富的数据报表，实现业务系统的访问行为分析，梳理业务的访问场景，整理域名访问关系，了解业务系统的流量高峰低谷情况。同时通过多种标准协议，无缝对接第三方系统。不但提升了网络管理能力、增强了信息安全，更是提升了现有信息系统的管理范围和能力，起到了 1+1 大于 2 的效果。

## 融合创新，协同推进，强化技术智能管理和防护手段建设

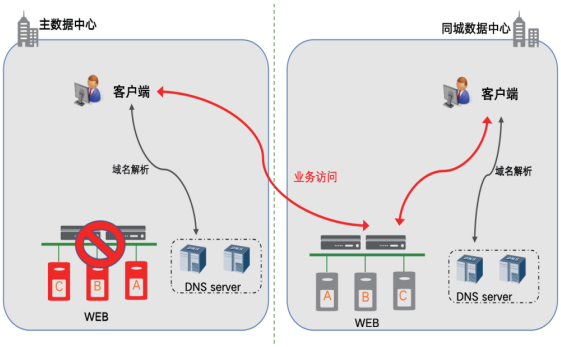
在整体建设过程中，智能 DNS 系统改造最为关键，上海大数据局与互联网域名系统国家市工程研究中心基于 IPv6 技术创新和改造项目总结积累，深入交流相关经验，探索安全可管理，防护有手段，满足多中心智能调度的可复制方式。

### 聚焦关键防护环节，加强安全防御纵深能力

每台 DNS 服务器均具备安全防护能力，能够对 DOS/DDoS 攻击、递归攻击、DNS 放大攻击等攻击类型进行有效防护，在设定防护策略后不需要手动配置即可对攻击进行自动防御。同时，针对个别域名和源 IP 地址，还可设定精细的限速防护策略，具备极高的灵活性，保障 DNS 系统的可用性和业务的永续性访问。

### 多维立体业务感知，精细化服务流程调度

DNS 按照算法将用户体验最佳的服务地址返还用户，以提高用户使用体验，当某资源无法提供服务时，DNS 服务器会将不可用的 IP 地址从域名解析结果中删除，并通知网内所有 DNS 服务服务器，全网用户均能够获得可用的解析结果，确保用户不会访问到不可用的资源节点。当资源节点恢复时，可用性监测功能会自动探测感知，恢复该资源节点使用。保证用户使用的连续性，减少故障对业务的影响，提高最终用户使用体验。



# 广西大数据中心：构建自主可控域名服务体系，保障网络根基安全助力数字政府建设

面向国家安全战略促进技术研发和创新应用，广西大数据中心电子政务信创云平台部署“中国芯”域名系统，夯实政务体系网络空间安全。

数字政府建设已经成为促进经济社会高质量发展，为推进国家治理体系和治理能力现代化提供有力支撑；在网络应用日益普及，网络安全形势日益复杂的背景下，强化数字政府的网络安全防护能力至关重要。围绕加快数字化发展、建设数字广西战略部署，数字化网络基础设施的稳定、安全十分重要。而作为网络交互的核心枢纽和链接中枢，DNS 在政务信息系统建设的复杂场景中，保障了内外网政务服务高效链接、体验优化，是政务连续性保障——构建开放共享的数据资源体系冗灾建设的重要组件和政府信息安全防护体系的重要环节。

信息安全的首要问题就是要解决信息化基础设施的安全问题，亦即解决芯片、操作系统相关供应链安全问题，作为基础软件，域名系统（DNS，Domain Name System）是所有 IP 网络（互联网和各行业内部专用信息网络）的寻址导航中心和控制中枢，也是所有网络服务和安全防护的第一跳，任何网络操作都必须依托域名系统才能完成。域名系统是网络的根基，掌握所有网络行为数据，域名基础软件是域名设备的操作系统。经探测，目前我国超过 90% 的域名服务器基于 Intel CPU+Windows/Linux 操作系统 +BIND/Windows AD 域名系统基础软件，均由国外主导，亟需加强自主创新，加快数字政府建设领域关键核心技术攻关，强化安全可靠技术和产品应用，切实提高自主可控水平；赋能政府数字化转型更安全、更高效切实筑牢数字政府建设安全防线。

通过科学分析应用需求，夯实自治区数字政务基础设施，构筑一体化多层次支撑体系，按业务功能逻辑区域在互联网接入区、公共网络区、专用网络区、政务专用区域，部署采用我国自主可控、成熟稳定的 “国产化域名基础软件”+“国产化操作系统”+“国产化 CPU”的域名系统，满足国家政策要求，安全合规，国产自主可控替代计划，规避供应链风险带来的安全事件，构建安全可控的信息化体系。

部署国产化智能 DNS 系统感知业务、网络等系统资源的运行状态，智能的调整解析结果，按需引导用户流量，支持政务多种冗灾应用场景的实现。提供一体化的域名系统管理平台，全面加强政府信息资源的有序汇聚，实现统筹规划和域名体系设计，按照“谁开设、谁申请、谁使用、谁负责”的原则完成线上域名注册审批流转分权分域管理。实时监测，落地域名管理的技术抓手，提供跨层级、跨地域、跨系统、跨部门、跨业务的协同服务。

# 江西省信息中心：政务外网域名解析系统赋能数字政府建设

近年来，江西省信息中心聚焦“作示范、勇争先”目标定位，深入贯彻实施网络强国、数字中国战略，按照江西省省委省政府决策部署，集约化推进以“一张网”“一朵云”“一个数据资源体系”“一批共性支撑系统”为核心的一体化数字基座建设，不断夯实数字基座服务支撑能力，支撑重大平台建设，创造了集约化、高标准、低成本的数字政府建设“江西模式”。

随着江西省数字政府建设的推进和深化，政务部门业务系统由自有数据中心迁移至省政务云平台部署，跨部门的业务互访、系统调用、数据交换共享愈发频繁，日趋成为常态。域名系统作为政务业务系统的“链接中枢”，需要满足集约共享、智能灵活、安全可控的新要求。因此，江西省信息中心立足全省政务外网建设实际，依托省政务云平台集约化建设了省政务外网域名解析系统，统一为各级政务部门提供域名解析、域名管理、多数据中心容灾等服务。

**集约共享：**江西省信息中心根据政务部门面向政务外网和互联网不同的需求，分别在省政务云的政务外网应用区和互联网应用区建设了域名解析系统，其中政务外网域名解析系统主要满足面向政务部门的业务系统域名需求，互联网域名解析系统主要满足面向社会公众、企业的业务系统域名解析需求，两套系统独立部署，但是统一标准规范，例如域名空间、命名规则、注册审批流程等，有效打破了“域名孤岛”，助力政务域名构架横、纵向的融汇贯通。同时，建设省政务外网统一域名服务平台，实现各业务系统、门户网站域名的集中管理、集中解析、集中防护，依托“赣政通”移动办公平台，实现注册申请审批线上办、掌上办。

**智能解析：**随着部门业务系统上云的进程不断加速，政务云平台等基础设施集约化水平不断提升，在促进业务快速发展的同时，也带来了运行风险的集中。省信息中心集约化建设了“两地三中心”容灾备份体系，为上云业务系统统一提供应用容灾、数据备份等服务。在此背景下，大多数政务部门基于 IP 的传统业务交互方式，在多数据中心的环境下呈现出了较强的局限性。因此，省信息中心对上云业务系统进行了域名化改造，让系统通过域名实现业务交互。配合智能域名系统解析服务，基于业务系统的健康状态、业务请求来源等信息，实现业务流量在多数据中心的精准牵引，并在灾难场景下实现业务跨中心的快速迁移，保障业务连续性。

**安全可靠：**域名解析系统承担着将域名翻译成 IP 地址的重要功能，是保障政务外网网络秩序安全稳定运行的导航系统，但由于 DNS 协议的特性，使其极易受到攻击，或者利用 DNS 作为攻击的媒介进行渗透。省信息中心高度重视域名解析系统安全，依托省电子政务外网安全运营中心，建设域名监测系统，通过 Ping 命令，TCP/UDP 探测和 HTTP(S) 协议等多种手段对域名解析系统和业务系统、门户网站等进行 24 小时轮询监测，发现异常情况通过邮件、短信等方式及时发起告警。部署专业 DDoS 防火墙，结合通信运营商的流量清洗服务，有效抵御 DDoS、UDP Flood 等攻击，过滤掉 DDoS 攻击流量。当遭遇相同地址攻击或数据库中出现的恶意访问地址，则由缓存系统进行应答，将用户访问或攻击分摊到不同的服务器中，从而缓解服务器压力，来达到负载均衡的效果。

# 03 教育

网络作为教育信息化建设的“神经系统”，在高校智慧校园的发展过程中扮演着重要角色。一方面，随着互联网的迅速发展，高校校园网络必须要有“质”的提升，才能让学校适应现代化教学变革；另一方面，随着高校校园网络应用规模的不断扩大，IPv4 协议下的网络地址已经不能满足更多人对新地址的需求，且所提供的协议服务水平也受到了极大的限制。如何构建一个简单、高效和智能的网络运维管理体系，提升校园网络的安全等级，同样也成了了当下智慧校园建设中所面临的严峻挑战。《关于推进 IPv6 技术演进和应用创新发展的实施意见》提出推动教育业务的云上部署，基于“IPv6+”技术支持学校开展云上教育教学、行政管理和公共服务。基于分段路由、随流检测等技术建设高质量传输的教育专网，探索产教融合的创新模式。

DNS 是高校网络服务的入口，也是高校网络流量管理的智能枢纽。下一代 DNS 致力于优化 IPv6 升级中的地址分配、地址管理和域名解析技术，助力教育领域 IPv6 发展提质升档，构建智能解析、智慧地址管理、智简运维的域名解析服务，助力高校提高管理效率、提升校园网络环境，加速推进“互联网＋智慧教育”建设进入垂直细分阶段，为高校“信息化创新一流大学”建设提供有效抓手，为智慧校园建设构筑基石。

# 中山大学：以数字化重塑未来教学空间

中山大学通过部署 DNS 专业设备，利用自主可控的下一代 DNS 技术，构建域名服务体系，通过校园内部网络，让其它校区无障碍使用 DHCP 服务，让工具驱动成为智慧学校建设的动力。

## DNS 赋能 DHCP 服务共享，工具驱动教育信息化建设

中山大学希望借助数据融通技术，通过数据驱动打造一站式校园服务平台，助力校内各项业务和服务场景实现“一网通办”、“一网通管”。此外，中山大学还提出了“Data First”的信息化建设理念，通过一切业务数据化、一切数据业务化，实现全量信息的高效融通，推进数据在高校管理中深入应用。未来，中山大学将基于各类智能化的大数据收集系统和信息整理系统，对教学过程、学习过程、校园安全、总务后勤、人财物等各类数据进行全面采集，实现管理智慧化。

在教育信息化中，“工具驱动”力量无处不在。在实现建设数字校园的过程中，利用动态地址分配 (DHCP) 的实现多校区域名地址的高效管理成了重要条件之一。为此中山大学携手专业域名服务机构 ZDNS，部署了两台域名系统 (DNS) 专用设备。通过校园内部网络，让其它校区无障碍使用 DHCP 服务，从而实现地址资源的统一管理，赋能 5 个校区基于统一平台，实现操作简单、数据可视、全网可知、运维省心。

作为行业智慧化升级的“数字助手”，DHCP 还能发挥专用高性能，确保无单点故障，永续服务，在入网高峰时，设备的高性能可轻松支撑全校 7 万终端的入网需求，师生不再感觉延迟、卡顿。当然，新技术让管理权适度集中，管理人员在责任的自我强化中，清晰风险隐患，确保系统稳定。

# 东南大学：构建安全、智能的双栈 DNS 系统

东南大学采用智能 DNS 系统，采用多校区集中管控、分离部署，实现动态、灵活的解析，结合时间、出口带宽联动等方式进行按需调度，实现多链路之间流量的智能引导，充分利用链路，保障负载均衡，为广大师生提供更良好的上网体验。

东南大学作为一所享有盛誉的国内名牌大学，是教育部直属的全国重点大学。作为国家“双一流”、“985 工程”和“211 工程”的重点建设高校，东南大学的历史可追溯到 120 年前。学校一直以服务国家为最高追求，在新的发展阶段下，秉持新发展理念，为构建新的发展格局提供服务，并提升服务国家战略科技力量的能力。

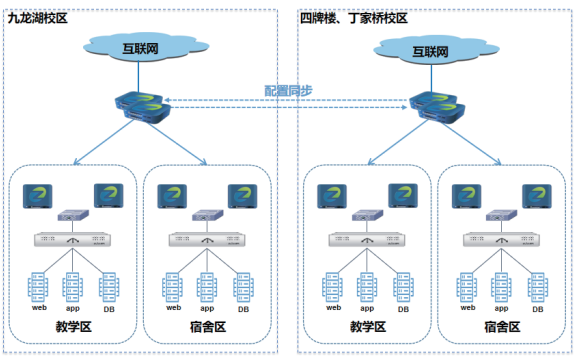
伴随网络技术的快速发展以及信息化程度的逐步深化，国内外信息安全形势日趋严峻，包括中国在内的世界各国均将国家网络安全纳入国家战略中。在我国，《网络安全法》作为网络安全领域首部基础性、综合性、框架性法律，对各组织机构提升网络安全保护能力、维护国家网络安全提出了强制性要求。《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》有关部署要求，全面深入推进 IPv6。东南大学立足新发展阶段，贯彻新发展理念，服务构建新发展格局。在提升服务国家战略科技力量的能力战略发展规划下，构建安全、智能的域名系统 (DNS) 在整个数字化转型中将显得尤为重要。

DNS 解析是选择出口链路的关键因素，其得到的目的 IP 往往直接决定了出口链路。校园网内用户多、流量大且峰值高，东南大学携手国内域名服务领域头部企业，构建智能 DNS 解析，实现动态灵活的解析策略，结合时间、出口带宽联动等方式进行按需调度，实现多链路之间流量的智能引导，充分利用链路，保障负载均衡，为广大师生提供更良好的上网体验。

智能 DNS 解析构建更健全的域名基础设施，促进信息系统访问优化，保障业务连续性，而这些功能优势具体从三大方面赋能东南大学智慧校园建设：

## 1、高可用的全新架构

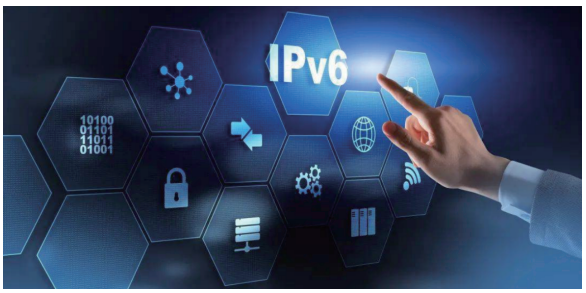
智能 DNS 相较于传统 DNS 具有全新的架构，提供了高可用机制，让网络服务互为备份。东南大学在智慧校园建设中，如果遇到突发情况导致任何一台设备下线，其它设备均可以作为补充，保障师生员工的上网体验。




## 2、现代化的双栈支持

全球基于 IPv6 的下一代互联网建设已经进入快速发展阶段，智能 DNS 能够同时满足 IPv4、IPv6 下的

域名解析功能，并且支持 IPv4 与 IPv6 共存情况下的 DNS64 功能，为学校现代化网络建设构建坚实基础。





### 3、多样的安全机制

智能 DNS 采用更加先进的设备和更加全面的安全机制的同时，采用多样性的防护策略 ( 如：域名限速、servfail 防护、本地安全策略等），可以更好地防御各种域名攻击，为在校师生的网络服务保驾护航。

东南大学聚焦互联网关键基础设施，引入智能 DNS 解析，发挥其高可用的架构、现代化的双栈支持以及多样的安全机制，为智慧校园的安全网络环境构建基础支撑，深入推进智慧校园建设，为我国智慧校园和现代化教育建设提供重要借鉴。

# 山东大学：技术驱动模式创新，数据赋能智慧建设

山东大学信息化建设旨在借助先进的信息技术和网络平台，提升教学、科研、管理和服务水平。通过引进先进设备和系统，学校实现了教学数字化、科研便捷化和管理高效化。信息化建设为学校提供了丰富的在线学习资源和交流平台，加速了科研成果的产出和传播，提高了办公效率和服务质量。山东大学将继续加大信息化建设力度，提升学校的竞争力和影响力。

山东大学是一所历史悠久、学科齐全、实力雄厚、特色鲜明的教育部直属重点综合性大学，在国内外具有重要影响，2017 年顺利迈入世界一流大学建设高校（A 类）行列。百余年间，山东大学秉承“为天下储人才”、“为国家图富强”的办学宗旨，践行“学无止境，气有浩然”的校训，蹲厉奋勉，薪火相传，形成了“崇实求新”的校风，为国家和社会培育了 40 余万各类人才，为国家和区域经济社会进展做出了重要奉献。

## 持续夯实数字化基础设施，建设智慧山大

山东大学一校三地构建了统一运维、技术先进、性能优异的新一代高速泛在校园网络，实现有线、无线、物联网和 5G“四网融合”，全校师生“一网通行”，随时随地免费使用校园网络。构建统一的公共视频服务平台，融合了硬件视频会议终端、腾讯会议、Welink、视频直播点播系统等多种资源，为一校三地行政视频会议、学术报告、各类专项会议、重大活动等提供全方位的保障和服务。

### 统筹规划，精耕细作

在教育信息化中，“工具驱动”力量无处不在，作为行业智慧化升级的“数字助手”，DNS 访问、提升用户访问体验、满足学院的个性化需求。

DNS 分布式部署集中统一管理，易于维护。权威递归分离，系统健壮性、安全性更高，提高系 统的稳定性；权威域名服务机构提供核心网络设备 (DDI) 全面支持 IPv6 解析，为将来扩大使用 IPv6 域名资源提供有力技术支撑；为校园网用户提供更快的 DNS 解析速度，多链路递归调度，优化用户体验。

### 融合创新，提档升级

面对新一代信息技术发展、互联网技术的全新要求及趋势，山东大学在夯实数字化的基础上，实现数字化向智能化的演变，通过智能信息技术，构建更 稳健的信息化基础设施，持续完善数据治理，用信息平台向学校教育和管理充分赋能，推动教育信息化行动计划的有效落实。同时注重 DNS 与“上层建筑”——新一代信息技术，衍生出的应用结合，为基于网络的物联网、云、数据互联互通，提供更多智能化的网络支撑。DDI 支持双栈服务，为后续 IPv6 的演进提供基础设施保障。

### 安全运营，精准保障

通过 DNS 部署，山东大学全面提升了网络服务质量，有效解决数据共享不畅、服务体验不佳等问题，推动管理服务提质增效。在这个过程中，安全、高效、智能的

网络系统对访问连续性、安全性的要求均有所提升，山东大学将持续完善网络安全体系，守牢网络安全底线，整体布局、统一规划，建立智能核心网络服务，实现互联网访问的智能流量调度，为校园信息化建设提供更加坚固、更安全、更高效的网络基石。

## 未来展望，持续引领，打造一流数据平台

山东大学以数据赋能学院数字化转型为契机，打造校院两级数据治理体系，完善学校全域数据库，建设符合学院特点的学院数据主题库，充分依托全域数据库落实标准化、精细化的数据管理模式，实现校院两级业务与数据的融合，推进业务创新和管理服务模式创新。同时利用信息技术创新手段，基于学校全域数据库建成学院信息化服务平台。实现学院人才培养、管理服务、教学科研等工作的数字化、智能化。山东大学以学院一体化服务平台为切入点，逐渐弱化大业务系统，促进管理和服务逐渐分离，强调一体化服务理念，逐步完成学院信息化建设的重构。通过平台的落地，有效推动了数据赋能学院数字化转型，提升山东大学各学院治理水平与治理能力的现代化。

# 中国矿业大学（北京）：提升 DNS 高可用性，智能解析助力智慧校园建设，加速教育信创落地

中国矿业大学（北京）提升 DNS 高可用性，实现智能解析，进一步夯实互联网基础，为网络空间合理资源调配提供科学支撑，助力智慧校园建设。

中国矿业大学（北京）是教育部直属的全国重点高校、国家“211 工程”、“985 优势学科创新平台项目”、“双一流”建设高校，是全国首批产业技术创新战略联盟高校，同时也是教育部与原国家安全生产监督管理总局共建高校。伴随着国家将信息化建设和网络安全的重要性提升至前所未有的高度，中国矿业大学（北京）加大网络硬件、软件投入，筑牢网络安全屏障，进一步提升学校的教学、科研、服务和管理的信息化水平，建设“智慧矿大”。

## 提升 DNS 高可用性，实现智能解析

在智慧校园建设过程中，网络的高可用性至关重要，中国矿业大学（北京）从校园网络的高可用性维度入手，增强网络根基建设。作为互联网关键基础资源，域名系统（DNS）对网络安全发挥基础支撑作用，中国矿业大学（北京）对现有 DNS 进行更新升级，以实现统一管理，即权威和递归 DNS 均通过一套管理页面进行管理，实现权威 DNS 和递归 DNS 的高可用部署以及部分应用系统的权威域名智能解析。

中国矿业大学（北京）在专业域名服务机构 ZDNS 的帮助下，采用 HA 架构对域名系统进行冗余设计，实现秒级切换。两台 DNS 网卡同时配置虚实地址，将虚地址下发给客户端作为 DNS 服务器地址，当主机出现问题切换到备机提供 DNS 解析服务时，客户端无需更换 DNS 服务器地址，使客户端能够无感知地继续进行访问；同时，浏览器使用虚地址进行登录配置，主备机自动同步配置数据，方便集中管理，进一步提升 DNS 服务的高可用性和终端的切换无感知性。

网络空间与现实空间相互映射、作用，网络空间的管理与现实空间的管理同样复杂、重要，同样需要精细化。中国矿业大学（北京）从提高核心网络服务的智能感知程度、增强精细化资源调配能力、强化互联网安全防护等角度出发，进一步提升 DNS 的高可用性，实现智能域名解析，进一步夯实互联网基础，为网络空间合理资源调配提供科学支撑，助力智慧校园建设。

# 暨南大学：整合强势资源，打造数字校园

暨南大学通过采用统一管理、分布部署的架构，在多校区分别部署专业域名服务机构提供的 DDI 服务节点和管理节点，构建起健壮的 DNS、DHCP 核心网络服务，提升校园数字化水平。

暨南大学是中央统战部、教育部、广东省人民政府共建的国家“双一流”建设高校。学校师生数目庞大，办公项目多种多样，学校内部的日常工作协调流程繁多复杂，广大师生对信息技术服务的需求也比较多元。近年来，学校相关部门积极整合各类强势资源，稳步推动智慧校园建设。

## 构建健壮网络核心服务，提升校园网络体验

暨南大学始终非常重视新技术的引进，与国内域名服务领域头部企业开展技术合作，提升校园数字化水平。作为校园网中重要的支撑基础设施——域名系统 (DNS)、动态地址分配 (DHCP) 的服务质量不但直接影响校园网的网络体验，也对学校信息工程形成一种掣肘。比如现网 DNS、DHCP 的服务，因存在多校区管理问题，三地五校区的 DNS、DHCP 服务各成一家、各自运维。不同校区负责人技术参差不齐、解析地址不清、交互故障频现等问题让管理风险常处于不可预见、不可管控的状态。其次，开源 Bind 和 BASE DHCP 的服务运维，由于配置复杂，导致误操作风险高，运行效率低。

为提高系统运行效率，本着就近服务师生用户的原则，系统运维主体通过采用统一管理、分布部署的架构，在多校区分别部署专业域名服务机构提供的 DDI 服务节点和管理节点，构建起健壮的 DNS、DHCP 核心网络服务：在暨南大学的石牌校区部署 1 套软件在虚拟机作为管理节点，对现网 DNS/DHCP 服务节点统一管控，在石牌校区部署 5 台专用智能 DNS 设备，其中 3 台 DNS 承载校内师生终端及服务器内网权威及互联网递归解析剩余 2 台承载外网权威解析；并分别在石牌校区和番禺校区各部署 2 台 DHCP 设备，各自为本校区提供 IPv4 及 IPv6 的地址下发，很好地实现了三地五校区 DDI 设备的集中统一管理，不但简化了运维操作，降低了管理人员的精力，而且权责清晰、运维便捷，确保系统图形可视、效果可观，未来可期。

# 中国劳动关系学院：提速教育信创，构建更安全、更高校、更智能的校园网络

构建更稳健的信息化基础设施，是校园管理数字化转型、校园服务智能化提升的基础。中国劳动关系学院重视网络基础设施的安全、可靠与高效，携手 ZDNS 整体规划、统一布局，通过自主可控的下一代 DNS 技术，实现异地内外网管理优化、智能调度升级。

中国劳动关系学院为提高信息互联互通效率，构建更稳健的信息化基础设施，在夯实数字化的基础上，实现数字化向智能化的演变，通过智能信息技术，构建更稳健的信息化基础设施，持续完善数据治理，用信息平台向学校教育和管理充分赋能，推动教育信息化的有效落实。

## 域名系统一体化解决方案：主辅结合，管理统一

随着院校的信息化及数字化深入，内部管理线上化、校园服务线上化……网络规模不断扩大，对网络基础设施的安全、高效、智能提出更高要求。中国劳动关系学院综合考虑内外网建设，与专业域名服务商 ZDNS 合作，采用域名系统 (DNS) 一体化解决方案，升级内网网络核心设备，确保安全稳定，同时在终端业务量增多的情况下，提升外网服务的智能调度能力。

通过北京校区网络核心设备组成 HA 作为递归 DNS 和动态地址分配 (DHCP) 的管理节点，并用 DNS 作为外网递归节点，另设 DHCP 为全校师生分配 IP 地址。通过 Master+Slave 架构作为外网权威，提供外网权威服务。北京校区作为整个 Master+slave 架构中的主区，逐州校区将 Master+Slave 架构作为北京校区的辅区域，采用主辅结合的方式，提供内网权威解析，同时单台 DHCP 为全校师生分配 IP 地址。

## 云服务：可视化管理，更自主更可控

在部署网络核心设备的同时，以设备做架构，作为权威 / 递归解析的节点，通过系统云中心的可视化管理平台可以清晰看到在本校设备运行情况、域名使用情况、CPU 利用情况等。

中国劳动关系学院外网权威节点也可实现可视化管理，对 DNS、NTP、TFTP 的服务状态进行实时监控。在权威域名服务机构打造的 Cloud 平台上实现了解析管理、地址管理、安全管理、系统管理。一方面，通过智能调度，配置多个转发明细，将不同的流量对应不用的出口和不同的调度对象，让各自出口的流量能够实现资源利用最大化，且用户解析延迟最低，另一方面，可通过管理平台创建多个视图对象，将不同视图匹配不同用户的源地址，能够将 DNS 流量匹配到对应的视图，配合转发区使用。这一整体规划与部署，让中国劳动关系学院在网络管理与应用上实现了更多自主性、可控性。

升级校园网络设施，提高自动化管理能力。中国劳动关系学院通过信息平台向学校教育和管理充分赋能，从建设更高效、更智能、更安全网络的角度出发，从网络核心单元出发，探索校园网络管理中的智能解析、智慧地址管理、智简运维的方式方法，为校园搭建安全、智能、高效的网络基石。

# 04 大型企业

随着万物互联时代的到来，互联网访问方式从最初的“人-机”寻址，发展到现在的“机-机”智能互联。这导致了接入系统规模的急剧增长和域名访问量的爆发式增加。DNS 作为互联网的第一入口，扮演着至关重要的角色，就像互联网世界的导航系统，其安全性、高效性、智能性影响着网络的互联互通。域名系统已经不仅仅是简单的“寻址解析”，而是涉及到互联网治理、网络资源和软硬件系统的全面升级。域名系统的全面升级将助力大型企业通过规范的运行管理，实现精准配置、业务系统性能稳定、软件持续升级，提升企业运营能力，保障大型企业业务系统健康运行。

每个企业，特别是大中型企业面临全球化市场，致力于通过建设新一代信息服务体系推动传统管理模式变革，实现降本增效、提升竞争力。域名等核心网络服务作为企业 IT 架构中重要的基础数字资源服务，在支撑企业数字化转型、信息化建设方面发挥着重要作用。伴随新技术、新架构在企业的大规模应用，核心网络服务需重新定义。

基于域名化建设、改造、升级大型企业的业务系统，自主可控的下一代 DNS 正在成为大型企业们“打造卓越企业集团、铸就百年民族品牌”的重要网络基础。多网统筹，提前规划设计，推进 IPv6 规模化部署，完成业务升级前置条件，全面提升关键基础设施服务能力，通过采用国产化高可靠系统架构，优化服务流程、提升故障感知能力，形成依托于多中心混合云架构的信息化服务平台，为集团复杂且多样化的应用系统提供了关键基础资源支撑。

# 中信集团：域名智能解析平台提升新一代信息服务体系

中信集团按照“践行国家战略、助力民族复兴”的使命要求，以“打造卓越企业集团、铸就百年民族品牌”为发展愿景，以“深化国企改革、加强科技创新和融入区域战略”为工作主线，深耕综合金融、先进智造、先进材料、新消费和新型城镇化五大业务板块，致力于成为践行国家战略的一面旗帜，国内领先、国际一流的科技型卓越企业集团。

在央国企数字化转型相关政策背景的推动下，中信集团经过多年规划建设，已形成依托于多中心混合云架构的信息化服务平台，为集团复杂且多样化的应用系统提供了关键基础资源支撑。随着多云混合，应用多样化两大趋势逐步形成，对 DNS 基础设施重视程度不断提高。

## 智能化解析平台助力中信集团构建新一代信息化服务体系

构建“稳运营、拓智能、提效用”的智能化解析平台，有力支撑集团混合云架构。多年来，中信集团一直在信息化领域不断加大建设投入，积极投身新型互联网信息技术的拓展应用，各类底层关键技术不断迭代，以满足集团日趋复杂的混合云架构支撑需求。在此背景下，ZDNS 与中信集团共同在域名服务体系领域进行技术探索，最终构建了满足发展要求的智能化解析平台。

更融合，更智能，更安全，下一代 DNS 多维立体建设初见成效。该平台基于中信集团混合云业务服务模式和运营特点，以域名解析系统智能调度、智简运维需求为核心目标，平台采用跨云多形态部署模式，形成异构化高可用架构，并具备高融合性、智能解析、安全防护等方案特色：

（1）与中信集团云管平台进行接口级耦合，实现域名资产生命周期的自动化管理，使域名化的系统业务“上线即可用”，全面呈现解析维度的业务运营状态；

（2）围绕混合云场景下的智能解析需求，在原有解析服务体系基础上进行层次化拆分，在递归和权威两个角色维度进行调度策略的配置落地，使解析体系架构更合理、更灵活、更具可扩展性；

（3）在安全防护方面，制定了基于 DNS 协议的安全提升方案，采用解析行为基线和威胁域名识别两种方式进行恶意行为交叉管控，将安全威胁阻断在解析环节，为中信集团安全体系补齐协议层面的防护短板。

向上支撑复杂业务应用场景，向下对接信息网络基础设施升级，下一代 DNS 助力数字经济高质量发展。随着国家面向央国企的数字化转型、自主科技创新等政策的不断推出，中信集团已实现从上层业务流到底层基础设施的全新升级，面对未来高速演进的数字化技术，下一代 DNS 还将继续协助中信集团实现“提质、降本、增效“目标，助力中信集团数字化建设和信息科技转型。

# 中远海运科技：IPv6 技术创新融合应用试点，促进互联网与企业业务深度融合，构筑下一代互联网创新发展优势

中远海运科技开展“中远海运 IPv6 升级改造和应用”项目试点有效推进 IPv6 规模部署和应用，实现互联网向 IPv6 演进升级，构建高速、移动、安全、泛在的新一代信息基础设施，促进互联网与经济社会深度融合，构筑未来发展新优势，为网络强国建设奠定坚实基础。

中远海运科技作为国内航运信息化领域的领军企业，以中国远洋海运集团为强有力的依托，致力于航运业相关应用软件和解决方案的研发工作，为用户提供高质量、多方位、深层次的航运和物流行业解决方案和集成服务。目前，公司在船公司、代理、仓储、码头、船员管理等多个航运信息化领域拥有完整的系统解决方案和成功案例；公司作为国内智能交通和交通信息化领域的开拓者之一，在智能交通领域专注深耕二十多年，拥有省级高速公路联网管理中心系统、ETC 不停车收费系统、高速公路机电系统、特大隧道和桥梁机电系统以及城市交通管理系统等一系列解决方案，技术实力处于国内同行业领先水平。公司业务遍及全国二十个省、自治区和直辖市，累计承担智能交通系统工程和软件项目近千项，市场占有率位居全国前列。

## 构建高速、移动、安全、泛在的新一代信息基础设施，促进互联网与经济社会深度融合，构筑未来发展新优势

近年来，公司积极响应国家提出的“互联网 +”行动计划，大力实施“互联网 + 交通”、“互联网 + 航运”业务模式创新，开发了“易管养”公路管理养护平台和“一海通”、“四海通”航运供应链电商平台，进一步推进公司创新转型发展。

中远海运科技股份有限公司的战略愿景是：成为一流的智慧交通和航运信息化服务商。公司坚持“战略引领、创新驱动、协同发展、产融结合、风险可控”原则，依托行业优势，充分运用移动互联网、大数据、云计算、物联网和人工智能技术，积极开展技术创新、商业模式和管理创新，致力于把公司发展成为国内领先的智慧交通、智慧航运、智慧物流解决方案提供商和运营商。

## 开展中央企业 IPv6 技术创新和融合应用试点，推进 IPv6 规模部署和应用，实现互联网向 IPv6 演进升级

IPv6 网络带来的网络安全管理成本降低和创新应用所创造的价值，有效助力企业数字化转型，为企业提供持续的降本增效能力。

中远海运集团数字化转型本部组织中远海运科技开展“中远海运 IPv6 升级改造和应用”项目试点工作，有效推进 IPv6 规模部署和应用，逐渐实现 IPv6 网络性能从趋同向优化转变，从端到端能用向好用转变，从用户数量向使用质量转变，从外部推动向内生驱动转变，整体提升了 IPv6 规模部署和应用水平。

中远海运科技结合集团网络现有情况，细化工作计划，制定“中远海运 IPv6 升级改造和应用”项目试点实施方案，分阶段制定年度工作计划，明确可量化、可检查、可评估的试点目标和阶段性成果。并根据项目试点实施方案，按计划分步骤推进网络基础设施改造，持续推进中远海运集团IPv6技术创新和融合应用试点改造工作。中远海运科技携手相关单位开展技术合作，完成 IPv6 规模部署的技术可行性验证，并在试点项目中将数据中心以互联网域名系统北京市工程研究中心支撑部署了 DDI 系统作为阶段性目标完成部署上线。

中远海科分析自身航运信息化业务高时效性、高连续性和数据传输高质量性特点和自身网络安全性的需求，以 ZDNS 作为技术支撑深入沟通交流，深度结合现网业务改造整体 DNS 架构，制定详细的域名解析规划设计和实施方案，完成域名系统的基础建设。通过 DNS 平台实现广域网业务流智能调度，实现业务流量的精准控制，提升数据传输质量，优化航运业务的服务质量；通过 DNS 平台区分 IPv4/IPv6 双栈环境下的域名记录查询，根据系统 IPv6 支持程度，过滤不完善的 AAAA 记录，实现企业在 IPv4 向 IPv6 迁移过程中，两种网络环境同时存在的环境下，针对不同网络地址的用户提供基于网络协议的调度，提升业务连续性；通过 DNS 平台与云端威胁情报联动，结合地址管理模块，有效提升了数据中心安全威胁的发现和处理能力，提升了数据中心的网络安全性。

中远海运科技与 ZDNS 基于 IPv6 技术创新和融合应用试点改造项目所总结积累，深入交流相关经验，探索形成可复制、可推广的做法，有助于推进集团下属公司 IPv6 规模部署工作，整体提升 IPv6 规模部署和应用水平，为实现互联网向 IPv6 演进升级，构建高速、移动、安全、泛在的新一代信息基础设施，促进互联网与经济社会深度融合，构筑未来发展新优势，为网络强国建设奠定坚实基础。实现集团数字化转型，助力实现集团“十四五”发展愿景，打造世界一流的全球综合物流供应链服务生态。

# 厦门航空：全面升级 DNS、DHCP 及 IPAM 核心系统，适应 IPv6 规模部署政策要求

厦门航空总部位于中国东南沿海的福建省厦门市，是中国首家按现代企业制度运行的航空公司。主营国内航空客货运输业务、福建省及其他经民航总局批准的指定地区始发至邻近国家或地区的航空客货运输业务，航空公司间的业务代理，兼营航空器维修、航空配餐、酒店、旅游、广告、进出口贸易等业务。

## 多网统筹，提前规划设计，推进 IPv6 规模化部署

厦航在追求自身发展的同时，将持续做优做强做大，不断着力转型创新，深入推进互联网协议第六版（IPv6）规模部署和应用。为了积极开展 IPv6 改造工作的要求，在公司数据中心及园区网络启用 IPv6 后，还需解决 IPv6 地址分配及 DNS 域名解析管理复杂以及缺乏自动化管理的问题。

抓住改造关键环节，全面提升域名、IP 基础设施的 IPv6 保障能力。要完成企业的 IPv6 改造，涉及改造的内容和设施非常多。通常采用逐步改造、稳步推进的方式。首先需要对基础设施改造。在 IP 管理方面，基础设施改造主要包括 IPv6 线路和地址的申请，完成对终端设备 IPv6 地址的配置，及对所有 IP 地址进行科学有效的规划和管理。其次在 DNS 方面，主要是 DNS 服务器改造。作为 IPv6 改造的主体，DNS 服务器改造主要包括增加域名所对应的 AAAA 记录，及确保其能接收来自单栈 IPv6 的 DNS 访问请求。最后才是业务系统改造。在完成对底层基础设施和 DNS 服务器的改造后，就要对上层业务进行 IPv6 改造。

## 建设下一代 DNS，完成业务升级前置条件，全面提升关键基础设施服务能力

厦门航空已完成多数据中心整体网络建设。通过建设数据中心双栈 DNS、DHCP 及 IPAM 系统，提供 IPv6 网络建设提供基础服务平台。为终端设备分发 IPv6 地址，并为所有 IP 地址进行管理和规划提供有效的手段。为了实现业务系统以“多活”或“主备”模式对外提供服务。并将业务系统逐渐从 IP 交互的方式，朝着全面域名化交互方式进行改造，实现 IP 与业务的解耦，为业务系统的 IPv6 改造提供有利条件，最终实现各个应用系统间及数据库等业务系统，均通过域名方式进行服务衔接。

（1）在主数据中心部署主用管理平台对所有服务节点进行集中管控，在灾备数据中心部署备用管理平添与主数据中心实现跨中心互备。

（2）在厦门数据中心部署 DNS、DHCP 及 IPAM 系统。关基区使用 HA 架构，为主数据中心关键基础设施区服务器及设备提供 DNS、DHCP 及 IPAM 功能；同时满足区域内的 IPv6 需求。使用 VIP 地址管理关基区的地址分发。区域配置负载均衡设备发布 VIP 提供关基区

和生产区的实际解析服务。

（3）园区使用 HA 架构。使用 VIP 替换原 DHCP 服务器。区域配置负载均衡设备发布 VIP 提供园区的实际解析服务。为园区提供 DNS、DHCP 及 IPAM 功能。使用 VIP 与原 DHCP 服务器对接，做园区地址段管理。区域配置负载均衡设备发布 VIP 提供园区的实际解析服务。

通过下一代 DNS 系统的建设，自主可控掌握网络关键基础资源，筑牢厦航重要网络根基，推动企业持续引领行业发展。建设部署的 DNS、DHCP 及 IPAM 系统通过操作系统和 DNS 协议的双重安全加固并完成统一纳管。提供横向扩容和高可靠冗余机制。提高 DNS 的运维管理效率和保障业务连续性、可靠性。持续推动安全、运行、服务、效益、管理等全方位高质量发展，打造更加卓越的绩效，成为国企高质量发展的典范。同时厦航也将坚持“复利思维”，不折腾、不动摇，着力防范化解重大风险，实现健康永续发展，打造航空“百年老店”，在“行稳”中实现“致远”。厦航始终将可持续发展作为履行社会责任的核心，在不断提高经营管理能力的同时，追求经济、社会和环境价值的最大化，对客户、社会等各个利益相关方和环境负责，推动企业可持续发展与经济发展、社会进步相得益彰。

# 海南电网：业务系统域名化改造，智能 DNS 体系建设助力打造安全可靠的智能电网

海南电网通过应用系统域名化改造，建设覆盖同城双中心的智能 DNS 服务体系，助力打造安全可靠的智能电网。

海南电网携手海南省政府实行智能电网三年行动圆满收官，全面提升了电网自动化、智能化水平，基本建成了覆盖全省范围内发、输、配、用全环节的智能电网综合示范省。与此同时，为大力支持全省 5G 网络建设，公司加强与政府部门、通信企业常态沟通，积极主动了解基站建设规划和用电需求，及时调整配电网规划，落实业扩配套项目建设，做好供电服务保障；同时推出超常规优化通信基站供电服务举措，进一步优化基站供电服务模式，打通基站供电服务“最后一公里”。智能电网，安全可靠是关键。域名系统作为网络核心基础设施，是电网智能化、信息化构建尤为重要的护城河。为此，伴随海南智能电网建设逐渐步入深水区，公司持续发力域名系统建设，为自身信息化建设构建安全保障，进而提升业务系统的可靠性和安全性，从智能电网的角度为智慧海南建设提供赋能。

## 业务系统域名化改造，保障业务服务持续稳定

基于域名化建设、改造、升级应用系统是企业信息化的发展趋势之一，至今方兴未艾。海南电网在域名化改造前，数据中心业务系统内部间的访问都还是通过 IP 进行，存在着业务系统、集群间访问灵活性不足、变更影响大等缺点。在专业域名服务机构帮助下，海南电网立足自身情况，通过“管理与业务分离”、“分区冗余部署”等方式构建了高效可靠的域名系统，通过应用系统的域名化改造，实现“应用与 IP 的解耦”、“应用与中心的解耦”，大幅提升了应用系统的可靠性和运维的便捷性，有力保障了业务服务持续稳定，助力应用系统的灵活部署。

## 智能 DNS 服务体系覆盖双中心，保障基础网络服务安全可靠

海南电网在大同及海府同城双数据中心部署智能 DNS 服务体系，在两个数据中心的 DMZ 和 IDC 区分别部署智能 DNS 服务器，两个数据中心相同区域的两台 DNS 设备通过 HA 架构实现节点的冗余，并通过虚 IP 对外提供服务，保障解析服务的可靠性与稳定性。IDC 区与 DMZ 区终端 / 服务器域名解析可直接通过区域内的 DNS 服务节点完成，无需跨区解析；当单一服务节点故障时，业务服务器 / 终端无需做任何调整，即可实现平滑切换。

此外，两个数据中心还部署有管理服务器，在确保管理节点冗余的基础上实现对全网所有 DNS 服务节点的统一管理，提供精细的数据分析，准确掌握 DNS 实时数据交互情况，提升故障定位和排查能力，实现智简运维。

海南电网通过应用系统域名化改造，建设覆盖同城双中心的智能 DNS 服务体系，提升业务系统的可靠性和安全性，助力电网智能化、信息化建设，赋能智慧海南。

# 宁夏煤业公司：构建 IPv6 演进技术体系、强化 IPv6 演进创新产业基础、加快 IPv6 基础设施演进发展

宁夏煤业公司积极响应国家能源集团的要求，以推动 IPv6 技术落地为重要目标，加快了相关工作的进行。作为国家能源集团旗下的一家重要企业，宁夏煤业公司深知信息技术的重要性和 IPv6 技术的优势，因此将其作为公司信息化发展的关键战略之一。

宁夏煤业响应国家发布的《关于推进 IPv6 技术演进和应用创新发展的实施意见》，按照指导意见，提出到 2025 年底，IPv6 技术演进和应用创新取得显著成效，网络技术创新能力明显增强，“IPv6+”等创新技术应用范围进一步扩大，“IPv6+”融合应用水平大幅提升；并在技术创新取得显著突破、产业支撑能力大幅提升、基础设施能力持续增强、重点应用成效凸显、安全保障能力显著提升。围绕构建 IPv6 演进技术体系、强化 IPv6 演进创新产业基础、加快 IPv6 基础设施演进发展、深化“IPv6+”行业融合应用、提升安全保障能力。

## 强化 IPv6 地址管理，加强基础资源管控

随着宁夏煤业信息化的的不断建设和智能设备的快速增长，IPv6 地址的管理变得至关重要。IPv6 地址的充分利用和合理分配可以提高网络的可扩展性和安全性。

为了实现强化 IPv6 地址管理，需要建立一个有效的地址分配和管理机制。这可以包括地址集中管理平台，负责分配和监控 IPv6 地址的使用情况。该软件平台可以制定和执行严格的地址分配政策，确保地址的合理分配和有效利用。此外，还可以建立地址回收机制，对未使用或滥用的地址进行回收和重新分配，以减少地址浪费。

同时，加强基础资源管控也至关重要。基础资源包括 IPv6 地址容量、网络带宽、服务器和存储资源等，是支撑互联网服务运行的重要组成部分。通过加强对这些资源的管控，可以提高服务的可靠性、稳定性和安全性。

## 构建高可用 DHCP 服务，明确 IPv6 地址管理职责

根据实际情况，宁夏煤业部署 2 台设备 DHCP 设备，采用 Failover 高可靠部署模式。同时 IPv6 地址管理实行统一管理、分配的原则。IPv6 地址管理的归口部门为宁煤集团信息化管理部，负责全集团的 IPv6 地址规划、申请及管理，并负责全集团的 IP 地址分配及管理。

集团工控网边界设备、带外管理网、语音网、办公网、视频会议网的地址由总部统一分配管理。总部负责一 / 二级单位标识的统一分配和管理，二级单位下属成员单位标识由各二级单位自行进行编码定制，其它 IPv6 地址段的分配由各单位信息管理归口单位管理。

各二级及其下属成员单位负责其内部 IPv6 地址的统一规划和管理，不得擅自使用本单位地址范围外的 IPv6 地址。当单位内地址不足时，根据业务发展情况及时向总部提出地址新增申请。

# 宁波舟山港：构筑安全防护之盾，DNS+Safeguard 守护港口网络安全的“门神”

浙江要拿“世界之最”，港口是一张重要名片。港口建设的重点，将是在宁波、舟山“一体化”之举。

千帆竞渡，万船启航。经过二十余年的不懈努力，宁波舟山港已经发展成为世界重要的集装箱远洋干线港、国内重要的铁矿石中转基地和原油转运基地、国内重要的液体化工储运基地和华东地区重要的煤炭、粮食储运基地，是国家的主枢纽港之一。2022 年，宁波舟山港货物吞吐量连续第 14 年位居全球第一。宁波舟山港航数字化改革率全国之先，以数字化改革为引领，提升营商便利化水平；以“提质提效”为主线，把握系统化、数字化、合规化“三个关键”，不断创新，不断提升网络安全能力，通过智能 DNS 及其安全防护体系建设，为港口的可持续发展贡献力量，也为宁波舟山港迈向“世界一流强港”的目标打下坚实基础。

## 智能域名解析系统，助力企业数字化改革扬帆远航

伴随着全球经济一体化进程不断加快，信息化正在成为企业参与全球竞争，提高企业核心竞争力的重要抉择。其中企业的网络性能和用户体验是成功的关键。宁波舟山港通过建设专业的智能 DNS 解析系统，有效提高了网站和应用的访问速度和响应时间，为用户提供更好的体验。

作为一项重要的 IT 基础核心服务设施，DNS 设备的高可用性、容灾等能力要求也越来越高，因此，宁波舟山港通过在双数据中心建设智能域名解析系统，提高系统的可靠性和稳定性。当某个 DNS 节点故障时，系统可以自动切换到其他可用节点，保障 DNS 解析业务的持续运行。通过监控和分析 DNS 查询数据，优化 IT 资源的配置和管理。通过减少网络延迟和带宽占用，提高整体运行效率，降低 IT 成本。通过智能 DNS 的业务解析数据进行资源管理，能够帮助宁波舟山港更好地应对业务需求和挑战，提高企业的运营效率和灵活性。在宁波舟山港数字化转型过程中，智能 DNS 解析系统能够快速响应并支持企业的业务扩展和创新。这种灵活性和创新性，能够帮助宁波舟山港在竞争激烈的市场中保持领先地位。

## 安全威胁管控系统，网络安全防护之盾

近年来，随着国家将网络安全的重要性提升至前所未有的高度，宁波舟山港是中国最重要的港口之一，处理着大量的网络流量和数据传输。为确保港口网络的安全稳定运行，由智能 DNS 解析 + 安全威胁管控系统（以下简称：Safeguard）构成的“域名 + 威胁情报库”安全联动防御体系成了不可或缺的安全防护之盾。

Safeguard 能够精确识别各种类型恶意域名，其中包括挖矿、勒索、C&C 等对企业危害极大的恶意类型。通过和智能 DNS 解析系统联动能够有效拦截恶意域名和网络攻击，防止恶意软件和病毒通过 DNS 解析进入港口网络，保护港口的敏感数据和关键系统免受攻击

和侵害。

作为港口网络安全的重要组成部分，智能 DNS 解析+Safeguard 构成的域名安全防御体系为港口提供了全面的网络安全保障。它能够监控和检测网络解析流量，识别异常行为和攻击，及时采取防御措施，保障整体网络的安全稳定运行。这不仅增强了宁波舟山港网络的抗攻击能力，还提升了整体运营效率和可靠性。为宁波舟山港的网络安全奠定了坚实基础，更为其他港口和企业提供了宝贵的经验和借鉴。宁波舟山港将继续不断创新，不断提升网络安全能力，为港口行业的可持续发展贡献力量。

## 深化域名体系建设，为港口快速发展打下了坚实基础

随着物联网、大数据等新技术的广泛应用，港口物流正面临着更多的挑战和机遇。为了满足港口的快速发展，宁波舟山港计划深化域名体系建设，再下沉部署智能 DNS 解析系统，不断提升网络性能、加强网络安全、提升业务可靠性，实现更高效的数据共享和业务协同，推动港口物流的数字化和智能化发展。提升竞争力、创新力和综合实力，实现质量更高、效益更好、规模更大的发展，为推进“双一流”建设贡献硬核力量。

# 郑州地铁集团：全面推动数字化转型，提升智能化防控能力

郑州地铁集团有限公司是 2008 年 2 月 22 日经郑州市人民政府决定成立的国有独资公司。近年来，智慧交通建设在中国加速推进。随着交通强国战略、智慧城市建设的快速推进，城市轨道交通作为其重要组成，需从传统思维向数据思维转变，以数字化驱动质量提升，更好的管控运营安全，优化交通环境，提升效能效益。

## 建设交通强国，数实融合提升智能化水平

近年来，智慧交通建设在中国加速推进。国家层面包括国务院、交通运输部、海事局等相关部门相继发布了一系列政策意见来指导和规范智慧交通行业的发展。2019 年 9 月，中共中央、国务院发布《交通强国建设纲要》，提出要推动大数据、互联网、人工智能、区块链、超级计算等新技术与交通行业深度融合，到 2035 年，基本建成交通强国。

以郑州地铁为例，2013 年郑州地铁 1 号线一期开通试运营，郑州地铁成为中国大陆第 17 个、河南省第 1 个城市轨道交通系统。截至 2022 年底，郑州地铁开通的线路共 7 条，运营里程 206.3 公里，共 152 座车站运营中，7 条线路在这个城市的地下空间穿梭。

郑州地铁以“建设成为国际领先、国内一流的轨道交通建设者和运营商”作为总体目标，随着新建设项目和开通线路不断增多，迫切需要通过数字化手段提升建设、经营和服务管理能力。

## 打造智能化 DNS 安全防控平台，提升安全态势感知能力

郑州地铁高度重视 DNS 的安全防护和服务态势感知，着力打造数字化和智能化的 DNS 安全服务体系，关注 DNS 服务安全和 DNS 数据安全，从内到外，从局部到全局，全方位保障 DNS 服务达到“看得清、防得住、管得了”的防护效果。现网使用的智能 DNS 系统与安全厂商的威胁情报库对接，针对数字货币、恶意网站、钓鱼网址等非法域名的本地拦截，实现威胁请求不出网的监管要求。

总体来看，郑州地铁希望搭建智能化 DNS 安全防控平台，以达到数据和服务的全息感知、实现数据信息与业务管理的有机融合。

未来郑州地铁的数字化将围绕公司的发展战略，在智慧服务、智慧运营、智慧建设、智慧管理等四大板块落地开花。如今郑州地铁乘着新技术的东风，不断在智慧地铁建设的道路上积极探索。郑州地铁将继续稳步推进数字化转型升级，践行“地铁让城市生活更美好”的使命，在国家中心城市建设和黄河流域高质量发展的伟大征程中贡献更多力量！

# 05 运营商 & 广电

广电行业由于其潜在数据量越大、数据隐私安全等级越低，数字化增速越高，是数字化高潜行业；5G 商用步伐加快，为广电行业带来革命性变革，其利用大数据等创新技术手段，结合云端安全能力和传统安全技术积累针对各种网络安全数据进行分析处理，贯穿威胁的整个生命周期管理。

运营商一直是数字化发展的排头兵，在国家“东数西算”等战略指引下，运营商还将成为算力网络建设的主力军。运营商行业聚焦网络体系建设，注重覆盖广度与深度，为各行业量身打造综合解决方案，为建设信息高速公路构建坚实基础。面对连接数量和流量规模的爆发式增长以及客户对网络的“按需供给”的需求变革，运营商的传统网络架构已经不能满足市场竞争、市场需求变化的要求。在此背景下，运营商将数字化转型的重点放在基于“网络智能化”的网络体系重构，从离散的专业网向虚拟化、软件化、云化的云网一体化架构转变。

面对数字时代的全新发展趋势，广电和运营商行业基于各自发展特点和需求，同时发力智慧网络建设，以顶层建设为指导，构建以下一代 DNS 为代表的的基础底座，通过核心层网络改造形成新型网络服务体系架构。聚焦关键信息基础设施，加强网络安全保障体系建设，推动网络安全创新技术能力提高、产品和服务提升，将有力保障运营商行业关键信息基础设施建设，提升重要系统、关键节点及数据的安全防护能力，支撑关键基础设施全生命周期安全管理的保障体系建设，加速数字化转型步伐。

# 四川广电：打造更安全、更高效、更智能域名解析服务平台，助力有线网络升级，夯实智能数字底座

根据四川广电业务发展实际需要，构建专业域名智能解析服务系统，采用缓存递归分离的模式和集群化的部署架构，提供更安全、更高效、更稳定的域名解析服务，满足宽带业务、固网语音等各种应用场景的需求，提升用户体验。

中国广电四川网络股份有限公司，简称“四川广电”，四川广电有线电视网络覆盖用户超 2000 万户，是传播党的声音、丰富人民生活、活跃城市文化、促进产业发展的主力军和网络强省、数字四川、智慧社会的重要建设力量。

四川广电牢记总书记关于“发展智慧广电网络”的重要指示精神，深刻领会广电集团“可管可控、安全可靠的新型融合网络建设目标”，积极参与当前全国有线电视网络整合和广电 5G 建设一体化战略。

## 升级改造基础设施，筑牢网络基石

DNS（域名解析服务）系统作为基础核心网络服务，是整个广电网络及业务访问的基石，作为四大运营商之一，DNS 服务更是广电最为核心的基础服务之一。2018 年以前，四川广电 DNS 系统基本为 BIND 自建，BIND 系统在安全性、解析能力、可靠性、可管理等方面，存在诸多不足，不能适应新的业务发展要求。

随着四川广电核心业务的不断发展和数字广电、智慧广电建设战略要求，四川广电从新一代基础设施层面，重构了 DNS 域名体系服务架构，让 DNS 系统可管可控、安全可靠。四川广电新的智能 DNS 服务架构，在安全可靠、智能解析、数据管控、数据赋能等方面，筑牢网络根基，全面适配 IPv6、固网语音、宽带有线业务、5G 等业务场景。

## 构建新一代智能域名服务架构，助力智慧广电建设

**四川广电新一代智能 DNS 系统架构优势：**

（1）管理与解析解耦：支持分布式部署与集中管理，支持分级分权管理；管理系统，支持数据配置及数据展示 WEB 可视化，DNS 服务可控可管。

（2）权威节点、缓存节点与递归节点分离：权威节点在安全性上得到提高、缓存节点提升了解析性能（缓解了省公司解析压力）、递归节点着重解决出网问题（递归出网智能策略使用、异网劫持等，优化出网体验，提升出网安全）。

（3）缓存节点下沉：采用集群化架构部署，全省用户使用统一服务 IP，并将部分缓存域名解析系统下沉于地市，整个域名解析平台负责全省宽带业务解析服务。新的智能域名解析服务平台，让全省各地市域名解析请求快速响应，用户上网更快。

（4）安全可控：新的域名系统，本身为专业系统，避免了自身诸多安全漏洞隐患；具备 DNS 安全防护功能，解决了现有安全架构在 DNS 防护方面的短板；同时满足国家在基础设施层面，自主可控战略要求。

（5）智能解析：新的域名系统，具备诸多“智能”，如智能解析调度（出 / 入网智能调度）、应用双活调度、业务健康探测 / 全网解析监测、域名画像、IPv6 支持等。

通过域名解析系统升级，四川广电构筑了更安全、更高效、更智能的网络，从而为建在网络基础之上的各类应用提供更优化的访问体验，全面支撑信息化、数字化、智慧化水平提升，为数字化转型及智慧广电建设牢筑网络基石。

# 浙江移动：构建全新域名系统承载解析服务，完善基础设施强化网络“新安全”

根据网络建设的实际需要，浙江移动构建新的域名系统承载解析服务，设备采用缓存递归分离的模式和 Anycast 集群化的部署架构，面向千万级受众人群，提供高性能、高可靠、极易扩展的域名解析服务。

近年来，我国不断加码数字化发展战略，打造数字经济新优势，协同推进数字产业化和产业数字化转型，加快数字社会建设步伐，建设数字中国。在这一背景下，中国移动通信集团浙江有限公司（简称“浙江移动”）勇于保持良好的发展态势，特别是在加快 5G 技术、大数据和人工智能融合、系统创新、流量经营、全业务及信息化拓展等方面，不断突破数字变革关键瓶颈，赋能经济社会数字化、智能化转型。

## 推动政务网络建设，为“数智化浙江”构建基础设施

面向“十四五”，浙江移动以创世界一流信息服务科技公司，做 5G 发展的领跑者、数字浙江的主力军、智慧社会的使能者、高质量发展的排头兵为使命，着手新基建、新要素、新动能、新安全四方面工作，全力推动社会数智化转型发展，推进浙江数字化改革。

截至目前，浙江移动在全省开通 5G 站点超过 4 万个，实现乡镇以上覆盖，全力打造“覆盖领先、性能优越”的 5G 精品网络。在加快建设 5G 精品网的同时，高速全光网、智能云网体系、新型云数据中心等高速泛在、天地一体、安全高效的新型信息基础也在逐步完善。

2021 年以来，政务外网、政务内网、感知网、视联网、政务云等政务网络，作为政府数字化转型的基础设施，为完善浙江省域治理体系奠定了基础。在这背后，有浙江移动近年来努力推动的“双千兆”服务，这成为浙江省政务网络体系的强力支撑系统。同时，浙江移动着力建设“两云”“网”建设，为数字化改革的数据采集、传送、存储、处理、使用，提供着全程信息服务。

浙江移动所提供的云网融合解决方案，不但助力政府提升部门协同、资源共享水平，还将打造布局合理、安全可靠、融合集约的新型云数据中心，直至建成长三角信息交汇枢纽。

## 参与建设综合应用系统，场景化应用培育“新动能”

数字化改革的推进，需要丰富的应用体系来支撑。如何通过技术创新、能力提升，创造各类丰富的应用场景，拓展面向数字生活、数字生产，数字治理的信息服务新业态、新模式，打造助力经济社会数智化转型升级的新引擎。

浙江移动的做法是，根据浙江省数字化改革的统一部署，

积极主动融入全省“1+5+2”数字化工作体系，全方位参与省数字化改革的五大综合应用系统建设。

浙江移动通过建设省级信创适配实验室，深入参与数字化改革示范工程，包括五大领域、共计 16 个政府的“8+13+11”重大标志性、示范性项目以及场景化多业务协同应用项目，打造了五大综合应用解决方案，推出了党政机关智治门户、城市大脑平台、未来社区、未来工厂、平台综合治理、公安精密智控等 90 余项创新解决方案，助力近百家企业实现智能生产，通过构建产业大脑，助力培育建设 20 家以上未来工厂和 350 家以上智能工厂。

与此同时，浙江移动发力科技与应用创新，着手建设重大创新载体，围绕 5G 产业，在全国牵头成立 14 家产业联盟，加快推进技术与经济、社会、民生融合，全力支撑数字化改革的综合应用目前，浙江移动已经推出 400 多个场景化创新应用，在全国率先发布“5G 商城”，创新推出云网、云边、云数、云智、云链、云安等 45 项“六融”产品，针对垂直行业深耕 OneCity、OnePower 等“9 ONE”平台，与横店东磁单晶电池片工厂联合，建成目前省内最大的 5G 专网应用智能工厂。

## 完善关键信息基础设施防护，强化网络“新安全”

推进数字化改革，需要强有力的网络安全防控水平，一方面要强化数据资源安全和个人信息安全保护，另一方面要做好关键信息基础设施防护。

浙江移动面向 5G、物联网、工业互联网、人工智能等新一代信息基础设施，健全了新基建安全保障体系，打造了在集团乃至业界均处于领先地位的安全管理水平。同时作为运营商，浙江移动面对数以千万计的用户提供网络接入服务时，域名系统 (DNS) 是用户访问互联网的第一环节，也是互联网业务交互的第一步骤。随着 4G、5G 业务的发展，用户数量大幅增加，现有 DNS 服务集群承载了较大的性能压力，需将部分业务分拆剥离，构建新的域名系统承载解析服务。

根据浙江移动网络建设的实际需要，权威域名服务机构 ZDNS 在浙江移动现网部署高性能软硬件的一体化设备，采用了缓存递归分离的模式和 Anycast 集群化的部署架构。在此支撑下，面向千万级的受众人群，能够提供高性能、高可靠、极易扩展的域名解析服务。

站在新起点，面向新征程，浙江移动正全面落实开创世界一流“力量大厦”战略，着力数智化转型，全面助力浙江数字化建设。

# 华数传媒：创新安全防护体系，引领数字广电“大安全”时代

华数明确安全防护策略，与时俱进持续研究引入新安全技术，利用自主创新安全防护体系，引领数字广电“大安全”时代。

华数传媒（简称“华数”）是大型国有文化传媒企业，也是国内领先的有线电视网络和新娘体运营商，拥有全媒体和宽带网络业务牌照资源，覆盖传统媒体和新媒体用户，业务遍及 30 个省、市、自治区。华数深入学习贯彻党中央关于宣传思想文化工作和广播电视工作的重要指示精神，不断推动自身变革，加快发展智慧广电和数字经济，为广电创新发展、美好生活创造、智慧城市建设赋能，走在智慧广电创新发展的第一阵营。立足新发展阶段，华数充分发挥行业龙头担当，积极融入新发展格局，争当广电网络传输的主渠道、宣传思想文化的主阵地、数字经济发展的主力军。

## 实施全新发展战略，健全“大安全”管理体系

当前，华数正在深入实施新一轮发展战略，围绕网络智能化、业务融合化、产业生态化三大方向，依托大数据、云计算、5G 网络、区块链、物联网、人工智能等新技术应用，加快向智慧运营商 & 广电和数字服务提供商转型。

近年来，华数紧紧围绕“全领域安全、全过程安全、全系统安全”，创新安全防护体系，协调推进播出安全、内容安全、网络安全，全力构建“平安华数”发展新格局、着力健全科学的“大安管理体系”。

以技术变革引领能力再造，华数创造性建成新一代省级高安直播中心，依托双中心三基地的高安高可靠架构和智能运维技术，实现了安全播出保障的重大突破。

以业务驱动引领技术创新，华数建成了业内领先的异地冗余内容中心，自主研发了业内最先进的互联网内容管控系统，构建了完备的互联网内容建设、运维、服务体系，满足自用的同时、也服务广电同行。

华数适应新技术发展变化，对标安保新标准、新要求，基于 AI、大数据等技术，研究网络行为分析、挖掘、识别、预警和追踪溯源技术，逐步建成全方位、全天候、立体化、靶向式的安全运行保障决策系统，安全管理决策能力再上新台阶。

## 明确安全防护总体策略，构建广电行业安全网络环境

华数高度重视安全防护体系建设，明确了“从单点修改向构架优化、从被动应对向主动应对从技术保障型安全向业务支撑型安全转变”的总体策略。

LDNS 系统作为宽带业务的基础设施和网络应用访问的入口，面对日益严峻的安全形势，加强自身服务安全日益迫切。华数密切跟踪信息安全前沿技术的发展趋势，与相关单位开展合作，分析宽带网络中异常

DNS 信息，通过深度 DNS 协议安全防护系统，有效降低 DNS 拒绝服务、远控连接重定向流量等威胁，保障宽带业务稳定运行，为打造安全网络环境贡献了华数智慧和华数方案。

华数针对自身异构 LDNS 系统的业务功能不完善、应急能力不足等痛点，依托专业 DNS 服务机构对 LDNS 系统和宽带流量调度机制进行深度分析，规划设计了科学的 LDNS 系统架构优化方案，并快速、高质量地完成了实施落地，显著提升了 LDNS 系统可靠性和对宽带业务流量调度的支撑能力，保障了宽带业务的服务质量，为广电行业宽带业务安全提供了成功借鉴。

华数顺应“广电总局深化拓展智慧广电建设”和“浙江全面推进数字化改革和高质量发展建设共同富裕示范区”的改革趋势，加速推进数字化转型，牢固树立底线思维，创新安全防护体系，构筑安全网络环境，发挥行业龙头担当，以自身数字化改革反哺行业数字化转型，助力实现国民经济和社会发展“十四五”规划和 2035 年远景目标。

ng-dns@zdns.cn
联系我们