**一、现状与目标**

## 1.1 现状

目前广东南方新媒体股份有限公司的办公域名解析系统（DNS）为美国微软公司的Windows AD域控制器提供的DNS服务，共部署了2台x86服务器，为广东南方新媒体股份有限公司办公终端和办公系统各服务器提供主机名解析、内网域名解析、互联网递归解析等功能，但Windows DNS存在以下风险：

**1.1.1、不符合政策要求：**不满足国家信创相关法律法规要求和关于信息技术安全的相关标准和规范，存在合规性风险。

**1.1.2、安全风险大：**Windows操作系统及DNS软件安全漏洞众多，经常需要更新，存在较大的安全风险。

**1.1.3、解析服务能力差、运维管理成本高：**不具备智能解析能力，无力支撑广域网流量调度、上网行为管理和安全审计，且DNS运行状态完全不可视，无法直接查看解析日志记录，人工投入精力大。

## 1.2 目标

本项目旨在实现对广东南方新媒体股份有限公司现有办公DNS系统的国产化改造替代，提升办公DNS的安全性和自主可控性，同时确保改造替换过程中的业务连续性和数据安全性。具体如下：

**1.2.1、建设国产化DNS**：采用国产化的服务器（国产CPU）、操作系统以及DNS应用软件，满足实际使用过程中对功能、性能、安全性和稳定性的要求，将现有Windows DNS的主机记录、递归解析等平稳、完整地迁移到国产化DNS系统。

**1.2.2、提升管理效率，满足安全审计要求：**通过集中式的管理平台，实现对DNS域名解析系统的统一管理和监控。提供详细的解析日志查询和统计分析报表，帮助管理人员了解系统的运行状况和用户访问情况，为办公系统上网安全审计提供数据支持。

**1.2.3、实现技术自主可控**：积极推进智能DNS域名解析系统的国产化，采用国内自主研发的技术和产品，减少对国外技术的依赖。

**二、项目需求**

本项目建设的国产化DNS需求主要包括：合规性需求和技术需求。

## 2.1 合规性需求

确保DNS系统的建设和运行符合国家信创相关法律法规要求，遵循国家关于信息技术安全的相关标准和规范。

## 2.2 技术需求

2.2.1、权威域名解析：在DNS上配置权威域名解析，提供给内网办公区用户使用。支持常用SOA记录、NS记录、A记录、AAAA记录、CNAME记录、PTR记录、MX记录、SRV记录、TXT记录、SPF记录、NAPTR等记录配置及解析，同时支持删除A、AAAA记录时相关的MX、SRV、PTR记录联动删除，保持记录维护一致性。

2.2.2、递归域名解析：对于本地DNS服务器自身不具备解析能力或没有缓存相应的解析结果的请求，向其他DNS服务器发起请求进行逐级查询，直到找到能够提供解析结果的DNS服务器，并将该结果返回给请求方。支持多链路负载解析调度，合理调度和使用多链路带宽；支持基于视图的多种转发策略（顺序转发、RTT转发、白名单）；支持基于视图的存根区、重定向、本地控制策略；支持视图、转发区、存根区等资源记录的禁用/启用；支持DNS64，平滑IPv6演进，支持双栈DNS；支持IDN、根配置；支持缓存预取和缓存管理；支持AAAA过滤；支持视图指定ACL不进行递归查询；支持失败转发；支持请求源地址健康检测和智能切换等。

2.2.3、分析监控：系统支持分析监控展示包括但不限于QPS、解析成功率、缓存命中率、并发递归数、CPU利用率、CPU温度、内存利用率、磁盘利用率、网卡流量等，数据实时更新，提供分钟级更新粒度，同时可实时统计近期解析域名排行、解析IP排行、解析状态及解析类型等。

2.2.4、审核管理：支持审核工作流，关键配置需要高权限管理员审核后才能生效，支持账户分权，可设定基于视图、区、权威记录的不可见/只读/修改权限；支持账户分权，可设定基于视图、区、权威记录类型、单独权威记录的隐藏/只读/读写权限。

2.2.5、解析日志：DNS的解析日志能够根据客户端IP、解析状态、记录类型、请求域名、解析延迟（精确到微秒）、日志全文进行分列展示；并可对指定时间段内的所有日志进行包含、等于、不等于的关键字段匹配，多个匹配条件支持“与”“或”方式的高级搜索。日志保存期限不少于180天，满足对安全审计、历史解析状态查询、网络流量分析和故障排除的要求。

2.2.6、智能访问调度：支持DNS多种负载均衡包括轮询、加权轮询、静态就近性、全局可用性、CPU/内存、动态就近性、多维度可用性算法、丢包率算法、静态保持算法、备选IP等算法；支持两级访问调度，即优先按照某策略调度到某应用服务器池，然后再根据某策略调度到该池内具体服务器；支持对应用服务器池的活跃地址数进行检测，支持图形化展现域名的调度逻辑和资源状态，对应用健康度、解析情况，应用状态情况可视化展示。

2.2.8、智能权威查询：支持对A、AAAA、CNAME、NAPTA、MX、SRV类型的域名配置静态就近性、轮询、加权轮询等调度策略。

2.2.9、智能递归查询：支持多种智能算法，可配置First、only等转发方式，关联RTT动态转发、ORDER按序转发、转发例外等转发策略，同时支持转发失败后通过递归迭代继续查询；支持转发服务器分组，支持转发服务器健康探测和异常告警，对异常服务器支持复检，保证异常服务器恢复后快速可用。

2.2.10、网络安全与访问控制：支持对所有资源类型进行强解析，包括：A记录、AAAA记录、SOA记录、MX记录、CNAME记录、NAPTR记录、TXT记录、SRV记录、PTR记录，DNAME记录、SPF记录、CAA记录、All记录、NS记录、Type（0-65535）类型，可配置强制解析结果：NXDOMAIN、NOERROR无记录或者直接丢弃。支持在DNS服务器中设置域名解析、屏蔽或重定向规则，将某些域名解析的结果指向另外的IP地址或拒绝解析某些域名，限制内网用户对某些危险或不安全的域名的访问；支持对用户的访问行为进行分析，及时发现和阻止非法访问或恶意攻击。

2.2.11、高可用性（HA）：支持HA双机互为实时备份或多主架构，任何一台故障其它节点不受影响，故障发生后会自动切换到另一台设备上。其中，一台设备设置为活跃设备对内提供服务，另一台设备机器作为备份设备，两台设备之间进行实时数据备份，以保证两台设备上的数据一致，同时，两台机器对外提供相同的业务IP。

2.2.12、跨平台兼容性：需兼容原有Windows AD提供的DNS服务，提供全面的AD集成，包括支持SRV和动态更新协议,平滑地将DNS服务从Windows DC迁移到DNS设备。

## 2.3 安全需求

**2.3.1、网络安全**

本项目需按等保二级要求进行建设，满足广东南方新媒体股份有限公司网络安全要求后方可上线。

**2.3.2、数据安全**

本项目支持国家商用密码算法，支持通过 SM3 国密算法进行DNS 数据更新与存储，保障DNS数据在传输和存储过程中的安全性、真实性、合法性和完整性。

**三、采购清单**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **数量** | **单位** | **单价(万元)** | **合计(万元)** |
| 1 | 国产化DNS应用软件（含相关实施服务） | 2 | 套 |  |  |
| **备注：**本项目由采购方提供硬件设备及操作系统。 | | | | | |