

华泰证券股份有限公司信创DNS设备采购公开招标公告
(招标编号: JSZB-2025-17398)

项目所在地区: 江苏省南京市

一、招标条件

本华泰证券股份有限公司信创DNS设备采购已由项目审批/核准/备案机关批准，项目资金来源为， 招标人为华泰证券股份有限公司。本项目已具备招标条件，现招标方式为公开招标。

二、项目概况和招标范围

规模: 为支撑华泰证券股份有限公司信息系统使用需求，对DNS设备进行必要的采购，具体技术要求详见“第四章 项目概况及需求”。本次采用公开招标方式确定中标单位，中标单位选择1家。

范围: 本招标项目划分为1个标段，本次招标为其中的：

华泰证券股份有限公司信创DNS设备采购

三、投标人资格要求

华泰证券股份有限公司信创DNS设备采购:

1. 投标人必须是在中华人民共和国境内依法注册,具有独立承担民事责任的能力, 提供营业执照有效复印件;
2. 投标人财务核算规范, 具有良好的财务状况和经济活动, 提供2023或2024年度经会计师事务所审计的“无保留意见”会计报告完整版有效复印件（至少须包括：资产负债表、利润表、现金流量表）；
3. 投标人具有依法缴纳税收和社会保障资金的良好记录, 提供2024年度全年的（1月至12月所有月份）“增值税”完税证明、近6个月内任意一个月的社保机构出具的投标人社保缴费清单材料, 社保材料必须为参保证明（加盖社保部门有效印章）或缴纳证明（加盖税务部门或社保部门有效印章）；
4. 投标人须保证, 招标人在其本国使用其提供的货物或服务时, 不存在任何已知的不合法的情形, 也不存在任何已知的与第三方专利权、著作权、商标权或工业设计权相关的任何争议。如果有任何因招标人使用投标人提供的货物或服务而提起的侵权指控, 投标人须依法承担全部责任;
5. 投标人具备履行合同所必须的经验和专业技术技能, 投标人作为投标产品的制造商或代理商, 投标人如为代理商, 须提供有效期内的代理商证明材料, 且须由投标人向招标人承诺提供原厂保修和服务, 中标后合同签订前须提供投标产品制造商的保修和服务承诺函（提供承诺书, 格式自拟）；
6. 投标人需至少提供一个自2023年1月1日至招标公告发布之日（含）（以证明文件签订日期为准）所投品牌的DNS产品服务案例, 并提供有效证明材料（注：合同金额达80万

(含)以上,且实际执行金额不得少于合同金额的30%,需提供相应的发票复印件证明材料; 合同关键词需包含“DNS”或“域名解析”或“DDI”字样, 合同复印件至少包含首页、合同标的、盖章页、金额页、采购内容说明等能够说明合同内容的信息复印件, 日期以合同签订时间为准, 复印件需清晰可见, 否则视为无效; 同一客户合同金额不累计)。

7. 投标人需参加招标人的POC测试, 并取得测试通过证明文件;
8. 投标人必须为增值税一般纳税人, 提供一般纳税人证明材料;
9. 投标人未处于被责令停业、投标资格被取消或者财产被接管、冻结和破产状态, 企业没有因骗取中标或者严重违约以及发生重大违法违纪等问题, 被有关部门暂停投标资格并在暂停期内; 本项目不接受联合体(含关联关系的企业)投标及未经招标人同意的任何形式的转包、分包(提供承诺书, 格式自拟);
10. 截至投标截止日, 投标人未被“信用中国”网站(<http://www.creditchina.gov.cn>)列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单(提供三张页面查询结果截图); 凡被列入华泰证券股份有限公司集中采购供应商不良记录名单且处于禁入期内的投标人不得参与本项目(现场核对);
11. 投标人承诺中标后, 在合同执行期内, 中标产品的市场价格下浮时, 招标人有权执行下浮后的价格, 中标人拒不执行的将被取消其中标资格(提供承诺书, 格式自拟);
12. 投标人承诺已充分理解招标需求, 可按项目的招标要求提供产品及对应的原厂维保服务(提供承诺书, 格式自拟)。

注: 以上所有资格要求条件必须在投标文件中逐条提供有效证明材料及其他相关承诺书并加盖公章, 否则投标无效。

本项目不 允许联合体投标。

四、招标文件的获取

获取时间: 2025-09-18 08:30到2025-09-25 17:30

获取方式: 1. 凡有意参加投标者, 请严格按照本公告规定时间内, 于上述时间在“中通服供应链股份有限公司电子招标系统(链捷招)”(网址:<https://jszb.chinaccs.com/>)获取招标文件; 如需领取纸质文件, 请至南京市鼓楼区镇江路13号进行纸质文件获取, 或联系招标代理发送邮寄地址后邮寄纸质文件。 2. 平台免费注册: “中通服供应链股份有限公司电子招标系统(链捷招)”企业注册信息, 提交审核单位: 江苏中博通信有限公司, 审核时间: 每日上午08时30分至11时30分, 下午13时30分至17时30分。 审核电话: 025-83303501。 3. 投标人如不按上述要求登记及获取招标文件的, 招标人将不接受该投标人所递交的投标文件。

五、投标文件的递交

递交截止时间: 2025-10-09 14:00

递交方式: 纸质递交至南京市鼓楼区镇江路13号院5号楼107会议室

六、开标时间及地点

开标时间: 2025-10-09 14:00

开标地点：南京市鼓楼区镇江路13号院5号楼107会议室

七、其他

1. 项目名称：华泰证券股份有限公司信创DNS设备采购
2. 项目编号：JSZB-2025-17398
3. 投标人承担其参加活动所产生的全部费用和成本（包括但不限于准备、编写和提交投标文件及参与投标的有关费用），无论结果如何，招标人在任何情况下均无义务和责任承担上述费用或成本。

4. POC测试时间：自招标文件停止发售日起10日内需参加POC测试，逾期不受理。

*投标人须在获得招标文件后3日内与测试负责人联系确定测试安排。

测试负责人：刘庆 联系电话：13905181321 邮箱：liu.qing@htsc.com

测试地点：南京市建邺区江东中路228号4号楼6楼

5. 平台服务费500元，不予退还。

6. 本招标公告通过江苏省招标投标公共服务平台对外公开发布。

八、监督部门

本招标项目的监督部门为。

九、联系方式

招 标 人：华泰证券股份有限公司
地 址： /
联 系 人： /
电 话： /
电 子 邮 件： /

招 标 代 理 机 构：江苏中博通信有限公司
地 址：南京市鼓楼区镇江路13号
联 系 人：王雅思、赵潇雨、宋扬
电 话：15895877258
电 子 邮 件：wangyasi.jszbt@chinaccs.cn

招标人或其招标代理机构主要负责人（项目负责人）王雅思（签名）

招标人或其招标代理机构： （盖章）

DNS 设备采购项目

测

试

文

件

华泰证券股份有限公司

二〇二五年八月

1 引言

1.1 编写目的

本文档是对华泰证券 DNS 设备采购建设项目所使用产品进行功能符合性测试、性能符合性测试等的综合测试指导性文件。本文档给出了对测试需求、测试环境、测试过程及测试结果的总体要求，是本次测试中其他文档编写及结果评价的基础。

1.2 适用范围

适用于华泰证券 DNS 设备采购建设项目 POC 测试。

1.3 测试目的

本测试是对投标人所使用产品的主要功能、性能等进行的符合确认测试，目的是为判定产品是否满足华泰证券 DNS 设备采购建设项目中所需的功能、性能等各项指标要求，并为后续的投标提供客观的依据。

1.4 测试组织工作

由华泰证券信息技术部负责牵头组织实施。

2 测试时间、地点、联系人

2.1 测试时间

自招标文件停止发售日起 10 日内需参加 POC 测试，逾期不受理。

*投标人须在获得招标文件后 3 日内与测试负责人联系确定测试安排。

2.2 测试地点

南京市建邺区江东中路 228 号。

2.3 测试负责人

姓名： 电话： 邮箱：

3 参与测试单位

3.1 参与测试的单位

4 测试具体安排

4.1 测试计划

测试总体上安排在 10 个工作日集中完成，具体计划见下表：

序号	测试时间安排	测试工作安排	备注
1	上午 9:00 开始至 18:00 结束，每天安排 一家厂商进行测试	具体安排如下： 1) 上午 9:00 参与测试单位到场签到； 2) 上午 9:00 测试评委到场签到，并 召开测试前准备会议，对测试评审规 则进行签名确认； 3) 参与测试单位进行正式测试，测试 现场只允许测试单位在场； 4) 测试结束后，由测试评委独立评审， 并汇总出具测试结果的报告。	一天时间无法完 成全部测试的，由招 标人酌情决定是否 延长测试时间；因 特殊原因无法开展 现场测试的，由招 标人另行决定测试 方式。

注：实际操作时，可根据现场情况或供应商参与数量，调整上述安排。

4.2 测试环境准备

投标人前往招标人指定的测试地点参与测试，投标人需在正式测试开始前，提
前完成组网与部署，另测试所需设备由参与厂家自行准备，包括：

- 1) 满足招标要求的智能 DNS 设备，参测的 DNS 设备需与投标品牌和型号完全
一致，否则视为投标无效；
- 2) 其他为完成测试所需的配套交换机、服务器、线缆等必要组件，以及测试
辅助仪表及仪器等。

5 测试标准和要求

按照测试功能点进行逐项测试。

6 测试评审要求

各测试评委按照评分标准，对项目测试情况进行独立评审。测试工作人员负责
汇总出具测试结果报告。测试结果报告由测试评委和参加测试单位授权人共同签字

确认。

DNS 设备采购项目测试需求

为了检验 DNS 设备采购项目潜在供应商所投 DNS 产品与采购需求匹配度，包括业务需求与技术需求的满足性及差异，特组织本次测试。通过制定测试点，逐项进行测试，逐项给出评测结果，最后给出各 DNS 产品的 POC 测试得分。根据 DNS 设备采购项目的采购需求，制定如下测试需求。

一、DNS 设备采购项目测试范围

测试范围见测试项。

二、测试要求

由参与测试的供应商自行提供 POC 测试所需的 DNS 设备及配套测试环境，配套测试环境需能满足本次 POC 测试项的要求。

供应商应细读测试点要求，并在测试期间准备好相关硬件、软件与工具，准备好测试所需相关场景案例数据，以及所需要的工具等，均包含在本次招标范围内。为公平起见，对于因准备不充分或要求理解有误等自身原因而无法正常完成的测试点，等同“不满足”处理。

三、测试指标

本次 POC 测试主要针对功能、组网能力、管理与控制平台进行测试，总计 24 项，明细如下：

1、平台整体架构功能测试

用例名称	平台整体架构功能测试
测试步骤	1、具备集中管理平台对 DNS 设备进行集中纳管、管理。 2、查看集中管理平台是否可以查看 DNS 设备的健康度及存活状态等重要信息。 4、部署主备管理平台，确认主备平台的工作状态，主平台修改相关全局参数，配置同步小于 1 分钟。 5、断开主集中管理平台的网络连接，登录备用集中管理平台确认是否可正常登陆且正常接管业务，且期间 DNS 解析服务正常，不受管理平台的故障影响。
前置条件	
预期结果	1、集中管理平台和 DNS 服务形成纳管架构。 2、DNS 设备运行状态出现变化，能够一分钟内在集中管理平台中更新体现。

	3、管理平台支持主备部署模式，且主备同步时长小于 1 分钟。 4、主管理平台发生故障时，向备平台切换过程正常，且对 DNS 服务无影响。
备注	

2、DNS 服务高可用架构测试

用例名称	DNS 服务高可用架构测试
测试步骤	1、使用两台 DNS 设备采用 HA 主备模式部署。 2、修改 HA 主备集群为非抢占模式，确认主备两台 DNS 设备的工作状态，是否有明显的提示主备分工情况，模拟主机宕机后，验证备机能正常接管业务，当主用设备恢复正常后，不会抢应回主用角色。 3、在切换过程中使用 ping 命令测试或通过自动化批量 DNS 解析探测。 4、采用负载均衡方式构建高可用架构，设置负载均衡 VIP 地址。 5、通过负载均衡 VIP 地址进行解析测试。
前置条件	
预期结果	1、HA 模式设置为非抢占模式时，当主用服务器从故障状态恢复正常后，不会抢应回主用角色。 2、HA 切换两秒内恢复域名解析，保证业务不受影响。 3、通过负载均衡 VIP 地址可以正常解析。
备注	

3、基本域名解析功能测试

用例名称	基本域名解析功能测试
测试步骤	1. 权威静态解析功能：创建静态 test.com 域名区域，自定义创建记录，验证 DNS 设备支持静态域名的 A、AAAA、CNAME、MX、NS、SRV、SOA、PTR、TXT、SPF 记录类型解析。 2. 权威动态解析功能：创建动态 test.com 域名区域，自定义创建记录，验证 DNS 设备支持动态域名的 A、AAAA、CNAME、MX 记录类型解析。 3. 转发解析功能：配置 test.com 全局转发或者 www.test.com 精细域名转发。转发支持全局/精细转发，以及支持粗细匹配方式转发，先选择精细域名转发，如果精细域名匹配不上，通过全局转发。 4、可以直接修改域名记录值、Type 类型，验证修改后符合预期。（删除再创建方式不符合本项要求）。 5、支持页面批量域名增删改操作： 1) 页面应能通过批量输入的方式，增加批量的域名。 2) 页面能对多个域名批量删除。 3) 页面可以对多个域名修改为相同值。 6、测试终端分别使用 IPv4 和 IPv6 进行验证。
前置条件	
预期结果	1、静态域名支持 A、AAAA、CNAME、MX、NS、SRV、SOA、PTR、TXT、SPF 记录类型解析。 2、动态域名支持 A、AAAA、CNAME、MX 记录类型解析。

	<p>3、转发功能支持全局/精细转发和粗细匹配方式。</p> <p>4、页面支持直接修改域名记录值、Type 类型。</p> <p>5、页面支持批量域名增删改操作。</p> <p>6、DNS 设备支持 IPv4 和 IPv6 的如上服务。</p>
备注	

4、独立部署及健康检查功能测试

用例名称	健康检查功能测试
测试步骤	<p>DNS 解析节点与服务 IP 的健康度探测节点独立分开部署，进行如下测试：</p> <p>1、配置动态域名 www.test.com，该域名在两个数据中心各有 1 个服务成员，其地址分别为 ip_1/ipv6_1 和 ip_2/ipv6_2，采用轮询调度算法。</p> <p>2、针对该域名的目标服务器地址配置 ICMP 的健康检测方式，并确定是否可以自定义探测周期、超时时间等参数。</p> <p>3、使用测试客户端持续对该域名发起解析请求确认解析结果，而后将任意一台服务器断电，查看服务成员健康检查异常/变化的日志，并再次确认解析结果。</p> <p>4、将另一个可用服务器断电，查看服务成员健康检查异常/变化的日志，使用测试客户端发起到 DNS 设备的解析请求，确认解析结果。</p> <p>5、同理完成 UDP、TCP、HTTP、HTTPS（TLS）等常用健康检测方式的验证，在使用 HTTP 或 HTTPS 模板时，可以自定义探测路径、返回字符串、协议版本、header 的 host 字段等。</p> <p>6、确认是否支持配置其他健康检测方式。</p> <p>7、调整该域名的健康检测方式为采用 TCP、HTTP 和 HTTPS 组合探测，并确认是否支持配置，查看健康检测效果。</p>
前置条件	
预期结果	<p>1、支持 DNS 解析节点与服务 IP 的健康度探测节点独立分开部署</p> <p>2、支持配置 TCP、UDP、ICMP、HTTP、HTTPS、基于 TLS 双向认证的 HTTPS 等多种协议的健康检查，且可组合为“与”“或”关系。</p> <p>3、HTTP 和 HTTPS 支持配置协议版本、header 中 host 字段、自定义探测路径、匹配指定返回字符串等。</p> <p>4、支持按照策略指定的拨测协议进行探测，并可自定义拨测间隔、超时时间、重试次数等。</p> <p>5、支持服务成员健康检查异常/变化的日志呈现。</p> <p>6、支持 IPv4 和 IPv6 的探测。</p>
备注	

5、逃生兜底功能测试

用例名称	逃生兜底功能测试
测试步骤	<p>1、在权威 DNS 设备中，配置动态域名 www.test.com 地址为 ip_1。</p> <p>2、配置探测组，采用 2 个探测设备进行轮询探测。</p> <p>3、使用 TCP 探测方式，探测周期 5 秒，超时时间 5 秒，重试 1 次，并设置延迟响应 15</p>

	<p>秒。</p> <p>4、使用客户端持续向 DNS 发起 www. test. com 域名的解析。</p> <p>5、模拟探测设备 1 探测失败，查看客户端解析结果。</p> <p>6、模拟探测设备 1 和探测设备 2 均探测失败，查看客户端解析结果。</p> <p>7、模拟恢复探测设备 2，查看客户端解析状态变化。</p>
前置条件	
预期结果	<p>1、步骤 5 当探测组中任意一台探测设备探测失败后，客户端能够一直正确获取 www. test. com 的结果。</p> <p>2、步骤 6 当探测组中两台探测设备均探测失败后，解析结果返回全量 A 或 AAAA 解析结果作为兜底或自定义失败应答的策略为“NOERROR”无具体记录值。</p> <p>4、步骤 7 当恢复探测设备 2 后，客户端最长等待 10s，获取基于调度算法的最优解析结果。</p>
备注	

6、DNS 解析会话保持功能测试

用例名称	DNS 解析会话保持功能测试
测试步骤	<p>1、在 DNS 服务器配置 www. test. com 动态域名，该域名在两个数据中心下各有 1 个服务成员，其地址分别为 ip_1/ipv6_1 和 ip_2/ipv6_2，采用 ICMP/TCP 健康检查方式对应用服务地址进行健康探测，负载算法选择轮询。</p> <p>2、对 www. test. com 域名开启“会话保持”功能，设置保持时间为 60 秒。</p> <p>3、使用客户端先发起 1 次对 www. test. com 的解析，记录解析结果。</p> <p>4、相隔 30 秒后，使用同一台客户端再次发起对 www. test. com 的解析，查看解析结果。</p> <p>5、再相隔 61 秒后，使用同一台客户端再次发起对 www. test. com 的解析，查看解析结果。</p> <p>6、访问间隔小于 10 秒时，模拟对应上一次解析地址的服务器故障，使用客户端再次进行解析测试。</p>
前置条件	
预期结果	<p>1、步骤 4 中，相隔 30 秒内解析结果不会发生变化，同步骤 3 的解析结果一致。</p> <p>2、步骤 5 中，相隔 61 秒后，解析结果可能发生变化。</p> <p>3、步骤 6 中，客户端解析出状态正常的服务成员地址。</p>
备注	

7、调度算法测试

用例名称	调度算法测试
测试步骤	<p>(一) 全局可用性+轮询：</p> <p>1、在 DNS 服务器配置 www. test. com 动态域名，该域名在两个数据中心下各有 1 个服务成员，其地址分别为 ip_1/ipv6_1 和 ip_2/ipv6_2，采用 ICMP/TCP 健康检查方式对应用服务地址进行健康探测。</p> <p>2、针对该域名的两个服务成员采用“全局可用性”+“轮询”的负载算法。</p> <p>3、使用客户端多次解析 www. test. com 域名，查看返回结果。</p>

	<p>4、模拟第一个服务成员故障，使用客户端再次解析 www.test.com 域名，查看返回解析结果。</p> <p>(二) 全局可用性+加权轮询：</p> <p>1、在 DNS 服务器配置 www.test.com 动态域名，该域名在 2 个数据中心下各有 1 个服务成员，其地址分别为 ip_1/ipv6_1 和/ip_2/ipv6_2，采用 ICMP/TCP 健康检查方式对应用服务地址进行健康探测。</p> <p>2、针对该域名的两个服务成员采用“全局可用性”+“加权轮询”的负载算法，权重比例为 1:3。</p> <p>3、使用客户端多次解析 www.test.com 域名，查看返回结果。</p> <p>4、模拟第一个服务成员故障，使用客户端再次解析 www.test.com 域名，查看返回解析结果。</p> <p>(三) 全局可用性+Topology</p> <p>1、在 DNS 服务器配置 www.test.com 动态域名，该域名在 2 个数据中心下各有 1 个服务成员，其地址分别为 ip_1/ipv6_1 和/ip_2/ipv6_2，采用 ICMP/TCP 健康检查方式对应用服务地址进行健康探测。</p> <p>2、针对该域名的两个服务成员采用“全局可用性”+“Topology”的负载算法，“Topology”规则指定源地址 A 匹配服务成员 1，源地址 B 匹配服务成员 2。</p> <p>3、使用客户端多次解析 www.test.com 域名，查看返回结果。</p> <p>4、模拟第一个服务成员故障，使用客户端再次解析 www.test.com 域名，查看返回解析结果。</p>
前置条件	
预期结果	<p>1、支持全局可用性+轮询算法解析服务成员。</p> <p>2、支持全局可用性+加权轮询算法解析服务成员。</p> <p>3、支持全局可用性+Topology 算法解析服务成员。</p>
备注	

8、自定义状态码返回功能测试

用例名称	自定义状态码返回功能测试
测试步骤	<p>1、在 DNS 设备中配置权威区 test.com，并配置域名 www.test.com，记录值为 ip_1。</p> <p>2、使用客户端向 DNS 发起 www.test.com 的域名解析查看解析结果。</p> <p>3、使用客户端向 DNS 发起一个不存在域名如 xxx.test.com 查看解析结果。</p> <p>4、在 DNS 设备上开启全局配置 NXDOMAIN 转 NOERROR 的功能。</p> <p>5、使用客户端向 DNS 发起 www.test.com 的域名解析查看解析结果。</p> <p>6、使用客户端再向 DNS 发起 xxx.test.com 查看解析结果。</p>
前置条件	
预期结果	<p>1、步骤 2 客户端向 DNS 解析 www.test.com 域名时返回 ip1。</p> <p>2、步骤 3 客户端向 DNS 解析 xxx.test.com 域名时返回 NXDOMAIN。</p> <p>3、步骤 5 客户端向 DNS 解析 www.test.com 域名时返回 ip1。</p> <p>4、步骤 6 客户端向 DNS 解析 xxx.test.com 域名时返回 NOERROR，无具体记录值。</p>
备注	

9、域名保护功能

用例名称	域名保护功能
测试步骤	1、配置权威区 test.com，开启 A/AAAA 记录唯一性保护。 2、新建 www.test.com A 记录值为 ip_1。 3、新建 www.test.com AAAA 记录值为 ipv6_1。 4、再次创建 www.test.com 的 A/AAAA 记录 ip_2/ipv6_2，弹框提示记录唯一性无法创建。
预置条件	
预期结果	开启域名记录唯一性保护，域名的 A/AAAA 记录唯一，服务创建其他记录值。
备注	

10、域名配置权限管理功能

用例名称	域名配置权限管理功能
测试步骤	1、分别设置管理员，机构 a 管理员只能管理 a.test.com 下的域名。同理机构 b 管理员只能管理 b.test.com 下的域名，总部管理员可以管理机构 a、b 和总部的域名。 2、机构 a、b 的管理员仅能查看和编辑自己管理的域名，不能看到其他机构管理的域名。 3、各个机构都应可以分配只读和读写的两类权限，分配给两类用户。
预置条件	
预期结果	1、机构 a/b 管理员只读账号，只能看到 a/b.test.com 权威区和域名记录，并且不支持新增、删除和修改对应的记录。 2、机构 a/b 管理员读写账号，只能看到 a/b.test.com 权威区和域名记录，并且支持新增、删除和修改对应的记录。 3、总部管理员只读账号，可以看到所有区和域名记录，并且不支持新增、删除和修改对应的记录。 4、总部管理员读写账号，可以看到所有区和域名记录，并且支持新增、删除和修改对应的记录。
备注	

11、动态域名解析拓扑调度功能测试

用例名称	动态域名解析拓扑调度功能测试
测试步骤	1、在 DNS 服务器配置 www.test.com 动态域名，该域名在 3 个数据中心下各有 1 个服务成员，其地址分别为 ip_1/ipv6_1、/ip_2/ipv6_2、ip_3/ipv6_3，采用 ICMP/TCP 健康检测方式对应用服务地址进行健康探测。 2、针对该域名的三个服务成员采用“Topology”的负载算法，要求客户端源匹配拓扑 1 的返回 DC1 的服务成员地址；客户端源匹配拓扑 2 的返回 DC2 的服务成员地址；客户端源匹配拓扑 3 (any 兜底) 的返回 DC3 的服务成员地址。 3、分别使用匹配拓扑 1/2/3 的客户端发起 www.test.com 的域名解析，查看返回的解析结果。 4、新增一个动态域名，关联已存在的三条拓扑规则，验证是否可以正常解析。 5、针对“Topology”的负载算法中互联网用户 IP 归属识别境内用户 IP 归属至少可实现

	基于省份及运营商两个维度组合，境外用户 IP 归属至少可基于地区或国家维度进行定义。
预置条件	
预期结果	<p>1、步骤 3 中当客户端源地址匹配拓扑 1 时返回 DC1 的服务成员地址；当客户端源地址匹配拓扑 2 时返回 DC2 的服务成员地址；当客户端源地址匹配非拓扑 1 和拓扑 2 的其他地址时返回 DC3 的服务成员地址。</p> <p>2、步骤 4 新增动态域名可直接引用当前拓扑规则返回对应的地址。</p> <p>3、用户 IP 归属满足境内用户 IP 归属至少可实现基于省份及运营商两位维度组合，境外用户 IP 归属至少可基于地区或国家维度进行定义。</p>
备注	

12、HTTPDNS 功能测试

用例名称	HTTPDNS 功能测试
测试步骤	在 HTTPDNS 正常情况下，可以正常通过 HTTPDNS 服务进行域名查询并返回智能解析结果；当 HTTPDNS 服务异常时，传统 DNS 解析服务可正常提供解析服务。
预置条件	<p>1、在智能 DNS 开启 HTTPDNS 服务，复用传统 DNS 的智能解析配置；</p> <p>2、使用不同客户端使用 HTTP 协议进行域名解析；</p> <p>3、关闭 HTTPDNS Server 模拟 HTTPDNS 服务异常，使用 DNS 标准协议进行解析。</p>
预期结果	<p>1、通过不同客户端使用 HTTP 协议进行解析查询，查询结果符合智能解析策略。</p> <p>2、关闭 HTTPDNS 服务，传统 DNS 的解析不受影响。</p>
备注	

13、批量导入导出与备份恢复功能测试

用例名称	批量导入导出与备份恢复功能测试
测试步骤	<p>1、管理中心支持页面以及命令行两种方式，导出、导入配置备份文件。</p> <p>2、将整机配置导出配置文件，支持 SCP/FTP/TFTP 的方式。</p> <p>3、对该 DNS 设备据进行增加 1 个域名、修改 1 个域名和删除 1 个域名操作，上述域名不重复。</p> <p>4、导入备份配置进行数据恢复，查看系统反馈情况。</p> <p>5、导入后，查看配置是否覆盖所有配置。（模拟配置出现问题后，快速回滚到上次全量配置）</p>
预置条件	
预期结果	<p>1、可以导出全量配置，支持 SCP/FTP/TFTP 的方式。</p> <p>2、能模拟快速回滚全量配置的方式，对全量覆盖刷入现有设备，新增配置不再存在。</p>
备注	

14、快速检索、全局搜索查询功能测试

用例名称	快速检索、全局搜索查询功能测试
------	-----------------

测试步骤	<ol style="list-style-type: none"> 1. 搜索可以针对域名、记录值、所属区域、视图、记录类型、自定义属性内容进行模糊或精细查询搜索。 2. 使用多条搜索策略进行关联搜索，单条策略可以包括等于、不等于、包含、前缀模糊、后缀模糊等条件，多条策略可以进行“与”、“或”查询。 3. 可以针对搜索的内容进行记录的修改、删除、导出操作。 4. 搜索结果可以对解析结果、TTL、属性值等进行全选编辑。
预置条件	
预期结果	<ol style="list-style-type: none"> 1、支持对全局的域名、记录值、自定义属性搜索。 2、支持使用等于、不等于、包含、前缀模糊、后缀模糊的方式查询相关域名和记录值。 3、支持组合搜索的方式“与”、“或”查询相关域名和记录值。 4、对搜索结果可以直接进行修改、删除、导出操作。 5、搜索结果可以对解析结果、TTL、属性值等进行全选编辑。
备注	

15、常规报表功能测试

用例名称	常规报表功能测试
测试步骤	<ol style="list-style-type: none"> 1、登录集中管理平台，支持查看当前配置的汇总视图信息，汇总视图应包括各 DNS 节点的状态（是否在线，响应能力等），以及查看域名解析数据（实时 QPS、时段 QPS、域名解析排行、类型、递归数、解析成功率等）、设备性能数据（CPU、内存、以及网卡流量等）曲线图。 2、测试是否能够自定义多种报表，包括 IP、域名排行，QPS，解析成功率，缓存命中率，NOERROR、NXDOMAIN 的分 IP 统计 top 等。 3、报表中应支持时间的维度应包括天、月、年。 4、查看报表是否支持导出。
预置条件	
预期结果	<ol style="list-style-type: none"> 1、具备汇总视图，可查看相关数据。 2、可以生成报表，报表可自定义。 3、自定义报表中应包括 IP、域名排行，QPS，解析成功率，缓存命中率，NOERROR、NXDOMAIN 的分 IP 统计。 4、报表的时间维度应至少能设置天/月/年三项，且按时间要求生成报表。 5、报表支持导出。
备注	

16、自定义报表功能测试

用例名称	自定义报表功能测试
测试步骤	<ol style="list-style-type: none"> 1、创建报表规则，针对关注域名进行分析，自定义报表分析类型包括：TOP 总量、TOP 百分比、百分比及次数/秒；分析项目包括：源 IP、源端口、查询区、查询记录类型、查询域名、应答状态、RD 位状态、请求签名、是否包含 EDNS、是否 TCP 请求、DO 位状态、CD 位状态、是否命中缓存、ISP、国家、省、市；匹配规则包括：所有、等于、不等于、包含、不包含；统计项目可以二层分析；数据统计分析包括：省、国家地理位置

	<p>的数据统计。</p> <ol style="list-style-type: none"> 2、关联自定义菜单。 3、查询报表结果。 4、导出报表数据格式为 CSV 或 PDF。
前置条件	
预期结果	支持以上自定义报表
备注	

17、网络管理相关功能测试

用例名称	网络管理相关功能测
测试步骤	<ol style="list-style-type: none"> 1、在 DNS 设备上完成 Syslog 相关配置。 2、验证 Syslog 服务器是否能够正确接收到事件。 3、验证设备出现端口中断、电源故障等场景，测试验证是否发出 Syslog 告警。 4、在 DNS 设备上完成 SNMPv2/3 相关配置。 5、配置 DNS 设备的网管服务器地址。 6、验证网管服务器是否能够接收到 SNMP 信息。 7、手工将 DNS 设备的系统时间设置为错误的时间。 8、配置 DNS 设备的 NTP 服务器地址。 9、约 30 秒至 1 分钟左右，验证被测设备的系统时间是否已经通过 NTP 服务器更新为正确时间。
前置条件	
预期结果	<ol style="list-style-type: none"> 1、DNS 设备支持 Syslog 功能。 2、DNS 设备能够同时支持 SNMPv2 和 SNMPv3 管理功能，支持 SNMPTrap 功能，且可以正确采集到 CPU 利用率、CPU 温度、内存利用率、磁盘利用率、整机请求数、整机应答数等信息。 3、DNS 设备的 NTP 时钟同步功能正常。
备注	

18、告警功能测试

用例名称	告警功能测试
测试步骤	<ol style="list-style-type: none"> 1、在 DNS 设备上完成域名对应 IP 的探测配置。设置应用掉线告警、域名因应用下线而无应答地址告警。 2、人为实现应用状态探测变更，验证 DNS 设备是否支持告警。 3、在 DNS 管理平台上能够很直观地看到目前 DNS 系统是否有告警，哪些节点有告警。 4、监控 DNS 设备情况，故障时产生告警，测试状态告警（DNS 设备状态、服务状态等）和阈值告警（QPS、系统资源使用率、解析成功率等），告警阈值可调整。 5、配置告警对外推送告警的方式，支持邮件告警、回调告警、SNMP 告警、syslog 告警、短信告警及声音告警方式；告警记录内容包括但不限于告警时间，节点名称及 IP、告警

	<p>事件原因。</p> <p>6、模拟设备各种故障，查看本地是否有告警信息，查看外发告警是否成功。</p>
前置条件	
预期结果	<p>1、DNS 设备在应用状态探测变更的情况下支持告警。</p> <p>2、直观看到当前系统各个 DNS 节点的告警情况。</p> <p>3、支持 DNS 设备及服务故障告警，支持状态告警（DNS 设备状态、服务状态等）和阈值告警（QPS、系统资源使用率、解析成功率等）。</p> <p>4、可调整告警阈值。</p> <p>5、可配置邮件告警、回调告警、SNMP 告警、syslog 告警、短信告警及声音告警等方式，告警记录内容包括但不限于告警时间，节点名称及 IP、告警事件原因。</p>
备注	

19、重点域名变更管理

用例名称	重点域名变更管理
测试步骤	<p>1、创建 www.test.com 域名，A 记录为 ip_1</p> <p>2、将 www.test.com 加入到重点域名中</p> <p>3、设置重点域名变更的弹窗提醒</p> <p>4、修改 www.test.com，出现相关重点域名变更弹框提醒</p>
前置条件	
预期结果	当修改重点域名时，有相应的提醒功能。
备注	

20、API 及 CLI 接口功能测试

用例名称	重点域名变更通知
测试步骤	<p>1、API 接口必须是标准的 web service，需支持主流 restful 或 soap 接口。</p> <p>2、通过 API 接口实现对数据中心的增删改查、健康检查的增删改查、服务成员的增删改查、地址池的增删改查和动态及静态域名的增删改查等。</p> <p>3、通过 CLI 命令行分别验证对数据中心的增删改、健康检查的增删改查、服务成员的增删改查、地址池的增删改查和动态及静态域名的增删改查等。</p> <p>4、下发配置成功、异常支持反馈错误日志。</p>
前置条件	
预期结果	<p>1、集中管理平台支持外部系统通过标准 restful 或 soap 接口完成配置查询、配置增删改等操作。</p> <p>2、集中管理平台支持通过 CLI 命令行完成配置查询、配置增删改等全量 API 接口支持的各类操作。</p>
备注	

21、静态域名解析压测

用例名称	重点域名变更通知
测试步骤	<p>1、配置 1 个视图，50 个区，一个区 10w 条区记录，其他区 1w 条区记录。</p> <p>2、使用压力测试工具持续高压打压 DNS，持续观察性能，打压包括三中模式全量 IPv4 业务压测、全量 IPv6 业务压测、IPv4 和 IPv6 混合压测（各 50%）。</p> <p>3、通过管理页面开启自动配置解析日志文件，到第三方服务器备份方式，包含备份传输方式包含 FTP、SCP 和 SFTP 方式。解析日志文件可以分别单独设置不同备份服务器。</p> <p>4、三次中流量模型下 QPS 达到 15w 时，使用测试终端手工连续发起 10 次解析请求，验证响应是否有明显延时、丢包。</p> <p>5、查询本次拨测的 10 条解析日志，解析日志内容包括查询时间、客户端源 IP、查询的域名、查询类型、解析状态、解析延时、日志全文等内容。</p> <p>6、日志查询检索时间是否小于 10s。</p> <p>7、日志备份信息的完整性进行校对，是否对全量日志进行备份。</p> <p>8、记录出现解析失败时的性能峰值。</p>
前置条件	
预期结果	<p>1、测试单台设备的解析性能情况，符合关键性能参数达 15W，延时不超过 1ms。</p> <p>2、连续拨测 10 次的日志记录的全面性、解析延时不超过 1ms。</p> <p>3、15W 性能下，日志查询检索时间是否小于 10s。</p> <p>4、日志备份信息完整全面。</p>
备注	

22、动态域名解析压测

用例名称	重点域名变更通知
测试步骤	<p>1、配置 5000 条动态域名，每个域名对应 2 个 IPv4 和 2 个 IPv6 地址。</p> <p>2、配置 10000 个地址配置 TCP 探测，另外 10000 个配置 HTTP 探测。3、每个域名关联 5 条静态就近性策略，总计 25000 条策略。</p> <p>4、开启解析应答日志记录和 syslog 外发功能。</p> <p>5、采用就近性解析算法，测试单台设备的解析性能情况。</p> <p>6、QPS 达到 15w 时，使用测试终端手工发起解析请求，验证响应是否有明显延时。</p> <p>7、记录出现解析失败时的性能峰值。</p>
前置条件	
预期结果	<p>1、首次出现解析失败时的峰值 QPS>15W。</p> <p>2、QPS 达到 15W 时，解析延时小于 1ms。</p>
备注	

23、设备安全管控测试

用例名称	设备安全管控测试
测试步骤	<p>1、开启双因子登陆验证功能</p> <p>2、退出管理系统，使用账号、密码、邮箱验证码登陆系统</p> <p>3、实现双因子登陆场景</p>

	4、SSH 登陆后台 root 登陆时是否支持密码时变 5、根据时变密码解密后进行设备登录
前置条件	
预期结果	支持双因子验证及密码时变
备注	

24、IP 地址库在线/本地更新

用例名称	设备安全管控测试
测试步骤	1、使用本地升级的方式更新 IP 地址库 2、使用联网的方式更新 IP 地址库
前置条件	
预期结果	支持上述两种方式更新地址库
备注	

四、硬件清单（推荐）

名称	使用对象	建议配置说明	数量	操作系统

五、测试报告

DNS 设备采购项目 POC 测试报告

参测单位：xxxx 公司

测试日期：

序号	是否标★	指标名称	不满足	满足
1	★	平台整体架构功能测试		
2	★	DNS 服务高可用架构测试		
3	★	基本域名解析功能测试		
4	★	健康检查功能测试		
5	★	逃生兜底功能测试		
6	★	DNS 解析会话保持功能测试		
7	★	调度算法测试		
8	★	自定义状态码返回功能测试		
9		域名保护功能		
10	★	域名配置权限管理功能		
11	★	动态域名解析拓扑调度功能测试		

12	★	HTTPDNS 功能测试		
13	★	批量导入导出与备份恢复功能测试		
14		快速检索、全局搜索查询功能测试		
15	★	常规报表功能测试		
16		自定义报表功能测试		
17	★	网络管理相关功能测		
18	★	告警功能测试		
19		重点域名变更管理		
20	★	API 及 CLI 接口功能测试		
21	★	静态域名解析压测		
22	★	动态域名解析压测		
23		设备安全管控测试		
24		IP 地址库在线/本地更新		

通过标准：基础指标（标★项）必须全部为“满足”，否则不通过。

测试结论：通过/不通过

华泰证券股份有限公司
信息技术部（盖章）
xxx 年 xxx 月 xx 日