

阿姆瑞特智能 DNS 管理系统

技术白皮书

AMARANTEN™

北京阿姆瑞特软件有限公司

目 录

序言	3
一、产品介绍	4
1.1. 产品概况	4
1.2. 安全特性	4
1.3. 稳定特性	5
1.4. 易用特性	5
1.5. 可扩展性	5
1.6. 高可用性	5
二、功能介绍	6
2.1. 智能解析功能	6
2.2. 广域负载均衡功能	6
2.3. 双机热备、负载均衡功能*.....	6
2.4. 域名管理功能	7
2.5. 三级用户管理功能	7
2.6. 域名查询统计	7
2.7. 记录迁移	7
2.8. 批量设置域名转发	7
2.9. 批量设置域名转发	8
2.10. 解析结果排序	8
2.11. 网关检测	8
2.12. 防火墙功能	8
2.13. 策略路由功能	8
2.14. 操作日志	8
2.15. 状态监控功能	9
2.16. 系统管理与维护	9
2.17. 在线升级功能	9
2.18. SSH 远程终端功能	9
2.19. 线路 IP 库同步功能	9
2.20. 二次开发接口模块*.....	10
2.21. 应急灾备解决方案*.....	10
2.22. DHCP 功能*.....	10
2.23. 链路聚合功能*.....	10
2.24. 应用服务器健康监测	10
三、移动规范 1.0	11
3.1. 基本功能要求	11
3.2. 扩展功能测试	11
3.3. 安全测试	12
3.4. 性能测试	12
四、技术架构	13
4.1. 系统架构	13
4.2. 部署结构	13

4.2.1. 主从部署结构	14
4.2.2. 多层次部署结构	14
五、公司简介	15

序言

随着互联网飞速发展，互联网信息迅速膨胀。大大小小的商业网站、个人网站，也有如雨后春笋迅速涌现。截至 2011 年底，全球活跃网站数量已经达 6.44 亿个（Pingdom 统计数据）。网站数量的增加，带来的是域名的飞速增加。加之互联网日益普及，上网用户数也在迅速增长。仅仅中国，上网用户数已经达到 5.64 亿（CNNIC 第 31 次报告，2013 年 1 月）。

如此巨大的用户量，如此繁多复杂的域名管理工作。如何去保障呢？如何去保障你的网站，你的域名能够被用户稳定、正确的访问呢？

加之国内的基础互联网的区域化问题很严重，不同的地区使用不同的 ISP，互相访问速度非常慢（电信、联通、移动、教育网之间互相访问速度）。那么又如何让你的用户访问到他能够访问的最快的服务器呢？

这个时候，您需要一套安全、稳定又易于使用的智能 DNS 系统。

一、产品介绍

1.1. 产品概况

阿姆瑞特运营商机智能 DNS 系统是一套面向网络运营商、互联网企业、大中型网站和高校的智能 DNS、域名管理及广域负载均衡解决方案。具有安全性、开放性、扩展性、模块化、标准化、可移植性等特征。

阿姆瑞特运营商机智能 DNS 系统提供有线路管理、域名管理、地址池管理、域名查询统计、监控及报警、多用户管理、操作日志等功能。全部通过中文 WEB 管理界面操作，简单易用，是为互联网企业、高校量身定做的智能 DNS 管理产品。

1.2. 安全特性

系统安全：阿姆瑞特智能 DNS 的核心操作系统是基于安全可靠的 MiniEOS™ 嵌入式系统，具备有很好的安全特性。另外，秉承只运行最少服务的原则，并且使用内核级的防火墙技术，只运行了少数几个服务，默认只开放 DNS 的 53 端口。并且可以通过 WEB 管理界面来灵活配置防火墙，进行安全防护。

应用安全：阿姆瑞特智能 DNS 会跟随应用程序的升级，而及时升级系统，修补应用安全漏洞。另外通过防火墙技术，只允许必要的服务端口对公众开放，而管理用的 WEB 端口和监控用的 SNMP 服务端口，只对内部管理 IP 开放。

抗攻击性：阿姆瑞特智能 DNS 采用的 MiniEOS™ 嵌入式系统，自身有很好的抗攻击能力。另外集成有防 DOS 攻击和 IP 欺骗的功能，可以有效抵挡恶意攻击。还集成有黑白名单功能，用户可以自行通过设定黑白名单列表，实现对系统的灵活安全防护。

1.3. 稳定特性

阿姆瑞特智能 DNS 系统运行的操作系统是基于安全可靠的 FreeBSD 操作系统自主定制研发的嵌入式操作系统 MiniEOS™ 之上，继承了 FreeBSD 作为 BSD UNIX 操作系统的坚如磐石的稳定性、可靠性和安全性，同时具备嵌入式操作系统的小巧灵活和高效性。因而产品的稳定性和安全可靠得到极高的保证。

1.4. 易用特性

阿姆瑞特智能 DNS 系统可以 100% 的通过中文 WEB 界面来完成管理和维护操作。简洁明了的图形用户界面，直观易用，极大地简化了系统配置复杂度。管理员只需要具备一定的 DNS 知识，就可以快速掌握系统的配置和维护，可以很好的使用这套系统。而且具有操作记录功能，可以跟踪管理员做了那些域名管理操作。

1.5. 可扩展性

阿姆瑞特智能 DNS 系统采取独创的灵活部署技术，可以无限分级扩展部署无限台 DNS 服务器。可以根据网站访问量和域名查询量灵活调节 DNS 服务器部署的数量，实现无限的负载扩展能力和冗余能力。独创的系统结构设计，允许用户根据业务的需要，使用不同规格的产品构成近乎线性增长的服务集群体系。

1.6. 高可用性

阿姆瑞特智能 DNS 支持 HA（双机热备）、负载均衡（双机负载均衡）、链路聚合（多块网卡绑定成一块使用）等功能。能让您的域名提供 7x24 小时不间断提供服务。

二、功能介绍

2.1. 智能解析功能

智能解析功能是根据用户来源，引导用户去访问指定的服务器。阿姆瑞特智能 DNS 系统支持最多 64 条线路的智能解析，默认已经配置有电信、网通、教育网三条线路，集成 1000 多个 IP 地址段。

您可以根据自己的需要按电信运营商划分线路，如电信、网通、教育网、联通、铁通等；或者地域划分线路，如华东、华南、华西、华北；也可以按省份划分线路，如北京、上海、广东、浙江、江苏、河南、河北、湖南、湖北、四川、山东、山西、陕西、甘肃等等。

2.2. 广域负载均衡功能

阿姆瑞特智能 DNS 系统支持全局负载均衡（GSLB）功能以及健康检测功能。这些功能，在“地址池”模块里体现。

阿姆瑞特智能 DNS 系统的监控模块会不停的监控地址池里的服务器的系统负载和健康状态，当发现负载大于指定的权值时，阿姆瑞特智能 DNS 系统会将客户的访问请求导向到负载比较轻的服务器，也可以通过置换方式，访问指定的备用服务器。从而提高客户的网络访问响应速度，同时也提高了服务质量。

2.3. 双机热备、负载均衡功能*

阿姆瑞特智能 DNS 系统支持 HA（双机热备）、负载均衡功能（双机负载均衡）、链路聚合（多块网卡绑定成一块使用）。通过这些功能，能最大化的提高服务高可用性，充分发挥硬件性能，降低 IT 成本。

2.4. 域名管理功能

阿姆瑞特智能 DNS 系统提供有专业而完备的域名管理功能。通过域名管理功能，可以让域名管理员轻松的配置和管理正解域名和反解地址。并且支持多种常用记录类型：A，A6，AAAA，CNAME，MX，NS，PTR，TXT。

2.5. 三级用户管理功能

阿姆瑞特智能 DNS 系统支持三级用户管理，分有超级管理员、域名管理员和记录管理员。超级管理员对整个系统都可以进行配置和管理，域名管理员只允许管理域名和记录，记录管理员只能管理指定域名的记录。

2.6. 域名查询统计

阿姆瑞特智能 DNS 系统支持图形查询统计，能让您直观的看到当前每秒查询统计。阿姆瑞特智能 DNS 系统支持每个域名在运行期间的查询统计。通过此功能，用户可以直观的看到每个域名、每条线路的查询统计数据，为您的运营提供参考数据。

2.7. 记录迁移

阿姆瑞特智能 DNS 系统可以将某域名下的指定类型或指定线路的记录整体迁移到另一个域名下的某种类型的某条线路中，大大减低维护负担，避免了大量记录重复删除导入的复杂操作。

2.8. 批量设置域名转发

阿姆瑞特智能 DNS 系统可以批量对域名设置转发。传统厂商的产品要么不支持域名转发，要么只能一个个设置。为了提高学校师生的上网体验，有时候学校可能会将大量的域名转发到某第三方运营商的加速设备上解析，如果一个一个单独设置，工作量非常大。阿姆瑞特智能 DNS 系统的批量转发功能完美的解

决了这一问题。

2.9. 批量设置域名转发

阿姆瑞特智能 DNS 系统可以进行根区文件的配置。将根区配置文件的内容导入到阿姆瑞特智能 DNS 系统中，就可以实现自定义根区的功能。

2.10. 解析结果排序

阿姆瑞特智能 DNS 系统可以设置 `sortlist`，使递归结果根据设定的顺序进行排序，在特定时候，可以让速度快并且稳定的结果 IP 排在前面优先访问。

2.11. 网关检测

阿姆瑞特智能 DNS 系统可以对 DNS 当前的默认网关进行检测，一旦发现网络不通或者不稳定，将默认网关切换到其他的提前配置好的网关上，确保网络始终畅通稳定。

2.12. 防火墙功能

阿姆瑞特智能 DNS 系统提供有对自身保护的防火墙功能，可以根据自己的需求设置防火墙规则，起到对系统的安全保护作用。

2.13. 策略路由功能

阿姆瑞特智能 DNS 系统提供策略路由管理功能，用户可以根据需要设定路由规则。比如支持双线接入，一台 DNS 服务器，同时接入两个 ISP 线路（如电信、网通），可以通过设置路由规则来实现双线访问。

2.14. 操作日志

阿姆瑞特智能 DNS 系统提供丰富的日志，如：DNS 日志、安全日志、系统

日志、操作日志和登录日志,通过日志全面评估当前系统的运行状态和故障定位。

2. 15. 状态监控功能

阿姆瑞特智能 DNS 系统还提供对自身运行状态进行监控。有 WEB 方式和 SNMP 方式。通过 WEB 方式可以直观的查看到当前的内存使用、系统负载和带宽流量状况。还可以通过第三方监控工具,获取 SNMP 进行监控。

2. 16. 系统管理与维护

阿姆瑞特智能 DNS 系统提供有 WEB 以及终端管理配置方式,操作简单、方便。提供配置数据的备份与恢复功能。同时提供有内置流量、负载监控功能,PING、DIG、WHOIS 常用工具。

2. 17. 在线升级功能

阿姆瑞特智能 DNS 系统提供在线升级功能,用户无需手工下载升级文件。只需要在系统里点击升级按钮,自动完成升级等操作,降低维护复杂度和风险。

2. 18. SSH 远程终端功能

阿姆瑞特智能 DNS 系统支持 SSH 远程终端管理功能,可以提供 SSH 远程终端进行基础系统的维护。还支持 System shell 功能,可以通过 System shell 进行一系列的维护和管理功能。

2. 19. 线路 IP 库同步功能

阿姆瑞特智能 DNS 系统支持线路 IP 库同步功能,可以与官方线路 IP 库保持同步更新。

2. 20. 二次开发接口模块*

阿姆瑞特智能 DNS 系统，可以为用户提供用于二次开发接口，或者标准 API 接口，以方便用户与原有的管理系统进行对接，从而保证了我们提供的智能 DNS 系统可以融入到用户原有的整个计算机网络系统，进行统一管理。

2. 21. 应急灾备解决方案*

阿姆瑞特智能 DNS 系统，可以为用户提供 DNS 系统的应急灾备解决方案，以确保万一 DNS 系统出现故障时，尽可能降低 DNS 系统的故障给用户的网络运行造成较小的影响，并在很短的时间内恢复正常工作。

2. 22. DHCP 功能*

支持动态主机设置协议（Dynamic Host Configuration Protocol, DHCP）使用 UDP 协议工作，主要有两个用途：在内部网络自动分配 IP 地址给用户，内部网络管理员作为对所有计算机作中央管理的手段。

2. 23. 链路聚合功能*

阿姆瑞特智能 DNS 支持链路聚合功能，可将两个或更多网口结合成一个单个的信道,该信道以一个单个的更高带宽的逻辑链路（网口）出现，从而大大提高网口的链路功能，提高系统对外连接的安全性和可靠性。

2. 24. 应用服务器健康监测

阿姆瑞特智能 DNS 支持应用服务器的健康检测，可以通过端口、URL 等多种方式对 web 应用服务器进行健康检测，一旦发现服务器发生异常，在解析的时候将不会解析返回给用户这台故障服务器的 IP，也可以设置替换，将解析结果替换为设定好的正常服务器的 IP。确保了对外权威域名解析结果始终是可靠的正常 IP。给外网用户访问用户自己的权威域名提供了良好的体验。

三、移动规范 1.0

在 2012 年中国移动集团组织的 DNS 设备入网测试中，阿姆瑞特智能 DNS 以比较领先的测试结果顺利达到各项指标要求。从而成为移动集团、中国电信、中国联通等运营商在 IPV6 网络升级中首选 DNS 产品。

3.1. 基本功能要求

条目	内容	测试结果
1	递归域名服务器域名查询功能	通过
2	递归域名服务器中文域名查询功能	通过
3	递归域名服务器查询过程测试	通过
4	权威域名服务器域名响应功能	通过
5	权威域名服务器中文域名响应功能	通过
6	权威服务器域名查询功能	通过
7	递归域名服务器 Cache 功能	通过
8	递归域名服务器 Sortlist 功能—排序功能	通过
9	递归域名服务器 Sortlist 功能—段内轮询	通过
10	权威域名服务器 View 功能	通过
11	递归域名服务器 IPv6\IPv4 双栈支持	通过
12	递归域名服务器对 RFC2181 的支持	通过
13	递归域名服务器使用 TCP 协议查询	通过
14	权威服务器使用 TCP 协议查询	通过
15	递归域名服务器对 EDNS0 的支持	通过
16	权威服务器对 EDNS0 的支持	通过
17	递归域名服务器 TTL 过期功能测试	通过
18	递归域名服务器 forward 功能测试	通过
19	递归域名服务器解析记录日志功能	通过
20	权威域名服务器解析记录日志功能	通过
21	递归域名服务器关键指标统计功能测试	通过

3.2. 扩展功能测试

条目	内容	测试结果
1	递归域名服务器 A 记录 IP 地址选择测试(黑名单)	通过
2	递归域名服务器 TTL 控制测试	通过
3	递归域名服务器域名不存在的重定向测试	通过
4	递归域名服务器域名查询请求快速拦截测试	通过

5	权威域名服务器错误域名泛解析功能测试	通过
---	--------------------	----

3.3. 安全测试

条目	内容	测试结果
1	权威服务器递归查询命令关闭	通过
2	递归域名服务器随机端口测试	通过
3	访问控制功能测试（黑名单）	通过
4	递归域名服务器账户保护功能测试	通过
5	权威域名服务器账户保护功能测试	通过
6	递归域名服务器系统安全日志功能	通过
7	权威域名服务器系统安全日志功能	通过
8	TSIG 功能	通过
9	DNSSEC 功能	通过
10	递归服务器递归进程的最大数量	通过
11	递归服务器对单一域的最大递归查询数量	通过

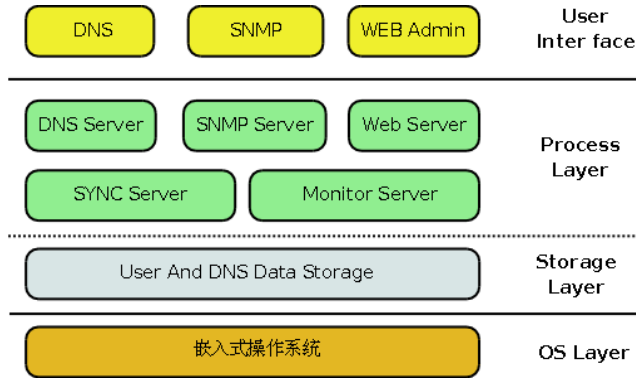
3.4. 性能测试

条目	内容	测试结果
1	递归域名服务器性能测试-完全递归	通过
2	递归域名服务器性能测试-部分递归	通过
3	递归域名服务器性能测试-有 Sortlist，部分递归	通过
4	递归服务器开启递归进程的最大数量限制的性能	通过
5	递归服务器开启单一域最大查询数量限制的性能	通过

四、技术架构

4.1. 系统架构

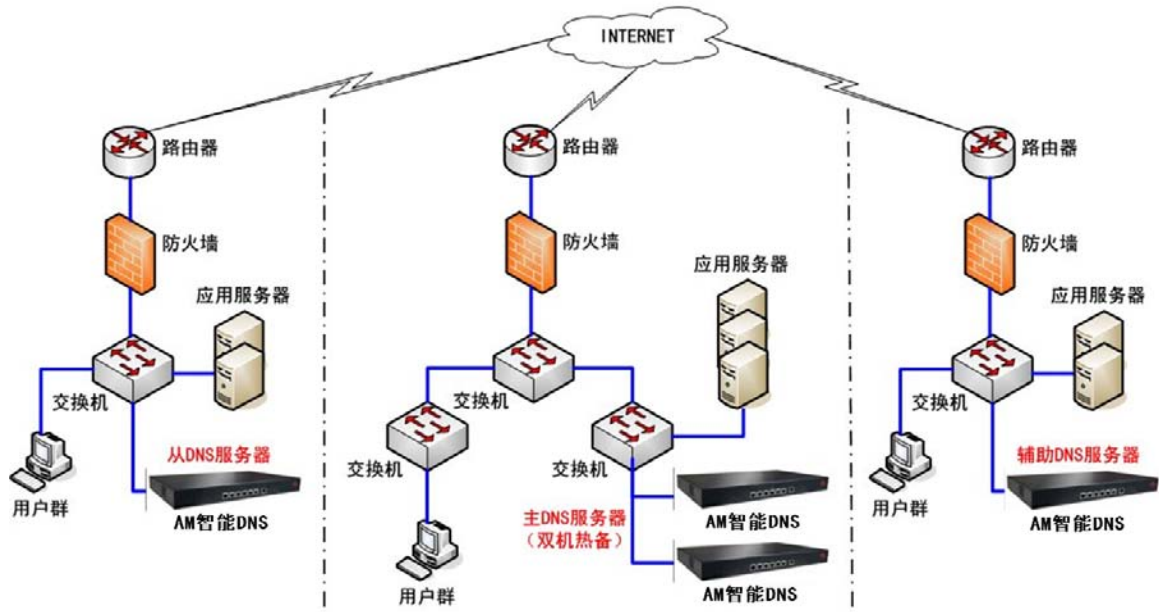
图 4.1. 系统架构图



4.2. 部署结构

阿姆瑞特智能 DNS 系统支持灵活的部署方式。可以根据需要无限级部署 DNS 服务器。实际集群部署图如下：

阿姆瑞特智能DNS群部署示意图



4.2.1. 主从部署结构

通常在一般的企业和网站，有两、三台 DNS 服务器就足够。这时候只需要部署一台主控 DNS 服务器，和两台从 DNS 服务器就可以了。部署结构如下图：

图 4.2. 主从部署结构图



4.2.2. 多层次部署结构

如果网站有大量的访问，两三台 DNS 服务器不足以支持查询请求时，可以采用多层次部署的结构。可以根据需要，分布在不同的 ISP，不同的 IDC。部署结构如下图：

图 4.3. 多层次部署结构图



提示：

1. 主控 DNS 服务器： 管理、控制服务器；
2. 辅控 DNS 服务器： 用于多级部署时，担当次级同步源；
3. 从 DNS 服务器： 最终端的查询 DNS 服务器，不能管理；