Zlope – A DNS Recursive server

2013.8

CNNIC

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

INDEX

BRIEF INTRODUCTION

A DNS recursive server with

- High query performance
- Fully control of cache
- Web interface, easy to manage
- Various statistics
- Dnssec support

BRIEF INTRODUCTION

High performance

In the same environment, the qps is about 1.5 times of bind9

Cache control

zlope has 2 levels of cache

level 1, user private data, highest priority

level 2, internet data, could be modified

Web interface

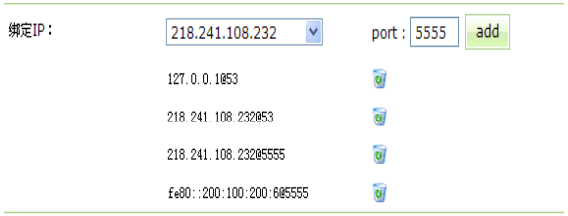
用户管理 >> 用户列表

用户管理 角色管理

帐号	角色	邮箱	电话	部门	是否在线	操作
root	root	root@163.com			是	
yhs	a	yhs@yhs.com			否	
xuht	guest	xuht@hotmail.com			否	
ffadfasdf	guest	asdfasd@123.com	1111	11111	否	
admin	root	admin@hotmail.com			是	

添加新用户

主机字符串	ttl	记录类型	记录值	管理
g2.nstld.com	164	A		
g2.nstld.com	164	A	192.42.93.32	



BRIEF INTRODUCTION

Web interface

- server management
  - 1 to n management, 1 web server, n zlope servers
- user management
  - different user with different privilege
- server configuration management
  - all config items can be modified on line
- some basic configuration can take effect immediately
  - do not need to restart the server

Statistics

thread0.num.queries=13253
thread0.num.cachehits=0
thread0.num.cachemiss=13253
thread0.num.prefetch=0
thread0.num.recursivereplies=13253
thread0.requestlist.avg=1.70769
thread0.requestlist.max=18
thread0.recursion.time.avg=0.008944
thread0.recursion.time.median=0.00238577
thread1.num.queries=531968
thread1.num.cachehits=0
thread1.num.cachemiss=531968
thread1.num.prefetch=0
thread1.num.recursivereplies=531949

DNSSEC support

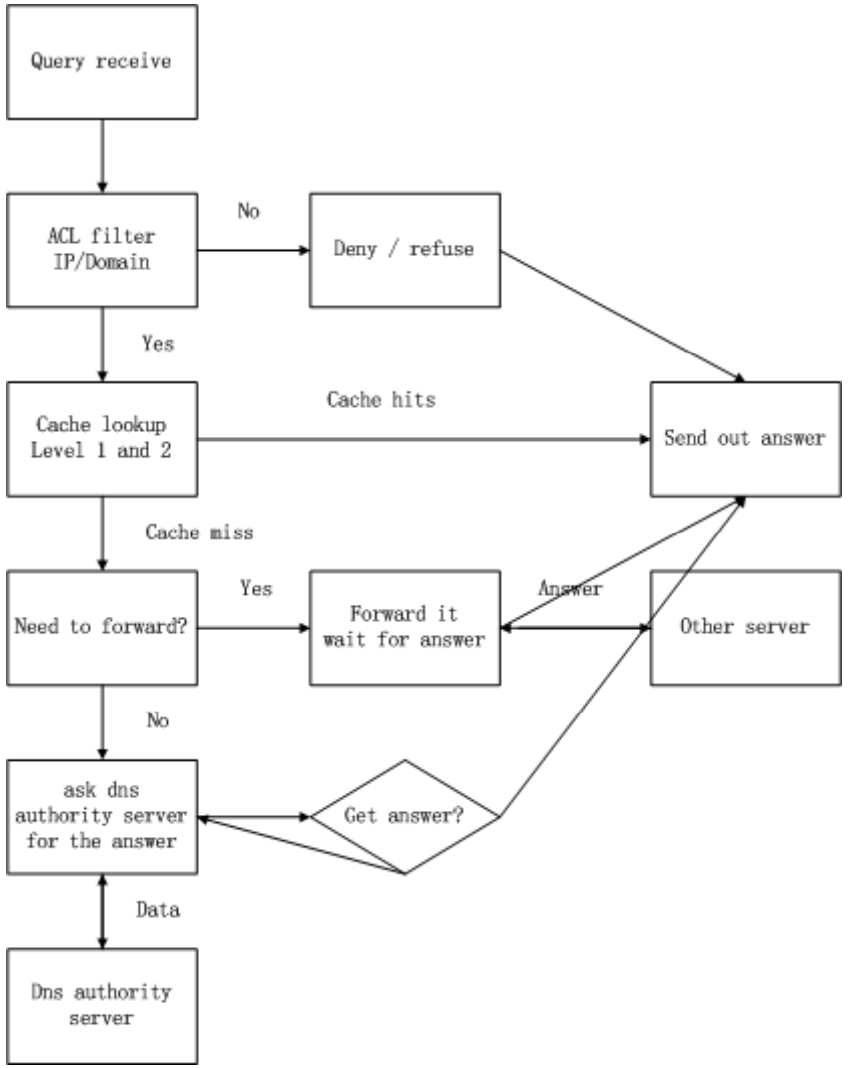
- trust key configuration
- dnssec validation
- dlv support

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

INDEX

ZLOPE QUERY PROCEDURE

Basic query process



ZLOPE QUERY PROCEDURE

Time out process

30 seconds for every query at most, return server fail when time out

If DNS authoritative server time out, try next one

no response or total time 30 seconds, return server fail

DNSSEC query

Ask authoritative server for DS, DNSKEY and RRSIG

Build up a trust chain

Do the validation

INDEX

FEATURES OF ZLOPE

Access control

Basic IP filter

deny / refuse / allow

Domain name filter

do not process queries for domain black.com

Cache control

user data

config some private domains

modify internet data

change the ip for domain www.aaa.com from 1.1.1.1 to 2.2.2.2

cache backup and restore

dump / load cache file

FEATURES OF ZLOPE

Answer control

cache round-robin(resource record)

query 1: www.example.com
answer 1: www.example.com has ip 1.1.1.1, 2.2.2.2, 3.3.3.3
query 2: www.example.com
answer 2: www.example.com has ip 2.2.2.2, 3.3.3.3, 1.1.1.1

answer intelligent sort

query 1: www.example.com source ip: 1.1.1.100
answer 1: www.example.com has ip 1.1.1.1, 2.2.2.2, 3.3.3.3
query 2: www.example.com source ip: 3.3.3.200
answer 2: www.example.com has ip 3.3.3.3, 2.2.2.2, 1.1.1.1

redirect(nxdomain answer to user specific ip)

query: www.noexist.com
normal server answer: no www.noexist.com exists(nxdomain)
server config redirect ip 1.2.3.4 answer: www.noexist.com has ip 1.2.3.4

Cache security

DNS spoofing(DNS Cache poison)

DNS server's request: what are the address records for subdomain.attacker.example?

Question: subdomain.attacker.example. IN A

Attacker's response:

Answer: (no response)

Authority section: attacker.example. 3600 IN NS ns.target.example.

Additional section: ns.target.example. IN A w.x.y.z

Or response:

Answer: (no response)

Authority section: target.example. 3600 IN NS ns.attacker.example.

Additional section: ns.attacker.example. IN A w.x.y.z

If the dns server store the authority and additional section, the target domain will be hacked.

Zlope will not fully trust the information from other DNS server, it ignores any records which are not directly relevant to the query

FEATURES OF ZLOPE

Log and statistics

System log

- Server running status
- System error

Query log

- Every incoming query

Statistics

- Specific IP statistics
- Specific domain statistics

中国信息社会重要的基础设施建设者、运行者和管理者

北京市海淀区中关村南四街四号中科院软件园　　邮编: 100190

www.cnnic.cn