Софийски Университет
"Св. Климент Охридски"

Изграждане и поддържане на DNSBL – колаборативно решение за участниците в БИОМ

Веселин Колев, Георги Найденов,
Стефан Димитров, Николай Николов

DNSBL – кратко описание

Технически формализъм на DNSBL:

- **базата с IP адреси или адресни мрежи на източници, се съхранява в DNS зона на домейн (напр. `dnsbl.uni-sofia.bg`) като за всеки IP адрес или мрежа от IP адреси, се изгражда A ресурсен запис към IP адрес от 127.0.0.0/8;**

- **изграждането на ресурсния A запис следва синтаксиса на in-addr.arpa представянето, например за IP адрес на източник на SPAM 192.168.12.25, ще има ресурсен запис:**

```
25.12.168.192.zonename.tld.  A 127.0.0.1
```

Технически формализъм на DNSBL:

- **когато в зоната се описва мрежа от източници на SPAM, това става на базата на цял октет (“wildcard”), без възможност за задаване на мрежова маска, например за мрежата 192.168.12.0/24:**

```
*.12.168.192.zonename.tld.   A   127.0.0.1
```

- **зоната на DNSBL домейна се актуализира най-често в динамичен режим, за да не се налага честата ръчна редакция на съдържанието - времеемка задача, повишаваща вероятността за допускане на грешки.**

Трансфер на съдържанието на зони на DNSBL зони:

- **трансферът от първичния сървър за имена към вторичните следва да бъде инкрементален (IXFR), а не пълен (AXFR) – зоните на такива домейни са големи по обем;**
- **трансферът на зоните трябва да е на база електронно подписани заявки за трансфер и отговори (TSIG);**
- **зоните на DNSBL домейните следва да бъдат забранени за свободен трансфер – те са списък на потенциално използваеми "зомби" хостове, проблемни SMTP сървъри, отворени SOCKS сървъри и др.**

Използване на DNSBL от SMTP сървър (пример за Sendmail):

```
edit -> /etc/mail/sendmail.mc:


FEATURE(`blacklist_recipients')dnl
FEATURE(`dnsbl',`dnsbl.uni-sofia.bg',`"550 Your IP
  address "$&{client_addr}" are listed in dnsbl.uni-
  sofia.bg"')dnl


# m4 /etc/mail/sendmail.mc > /etc/mail/sendmail.cf
# service sendmail restart
```

Използване на DNSBL от SPAM филтър на съдържание (пример за SpamAssassin):

- **списък с най-често използвани DNSBL зони на домейни:**

```
/usr/share/spamassassin/20_dnsbl_tests.cf
```

- **възможност за прибавяне на нови DNSBL зони чрез шаблон в**

```
/etc/mail/spamassassin/local.cf
```

Разлики в използването на DNSBL от SMTP сървър и SPAM филтър на съдържание:

- **използването на DNSBL от SMTP сървър води до автоматично прекратяване на инициираната от източника на SPAM SMTP сесия (*отхвърляне на сесията по протокола на услугата*);**

- **използването на DNSBL от SPAM филтър на съдържание следва политиката на филтъра – най-често маркира съдържанието като нежелано (напр. [SPAM] маркер с Subject на електронното писмо (*приемане на съдържанието по протоколната сесия и третирането му като нежелано от софтуера за филтрация*).**

Софийски Университет
"Св. Климент Охридски"

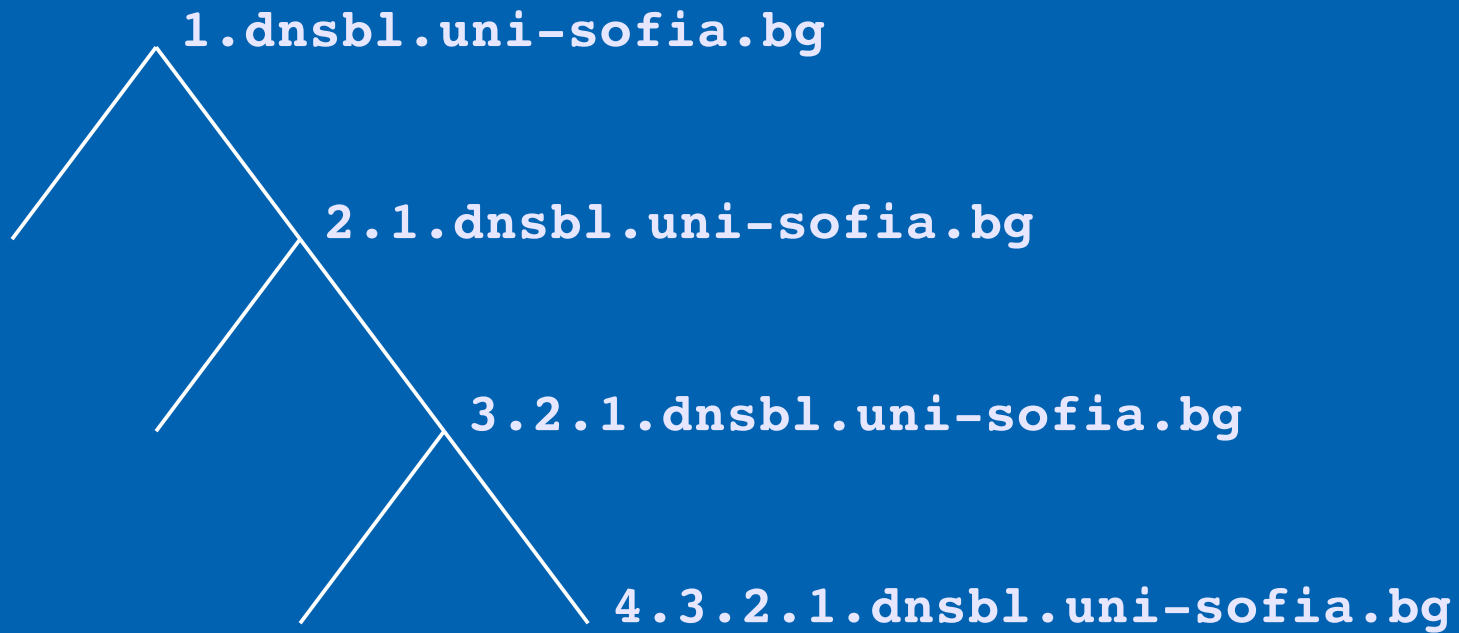
DNSBL – използване на йерархична база данни за съхранение на съдържанието

(примери за BIND9 и Red Hat Directory Server)

Предимства на йерархичната база данни при обслужването на DNSBL:

- позволява създаване на дървовидна структура за търсене (свойствена за DNS) в база от данни, чрез която се ускорява търсенето посредством намаляване на броя претърсвани елементи на база поддърво;
- по-икономична откъм потребление на памет, в сравнение със стандартния модел на съхранение и обслужване на зони в BIND9 – чувствителна икономия на ресурси при големи като обем зони на DNSBL домейни;
- лека за инсталиране, настройка и обслужване.

Примерна схема за извличане на ресурсен запис за 4.3.2.1.dnsbl.uni-sofia.bg



Използване на LDAP директориен сървър за обслужване на DNSBL:

- реализира йерархична база от данни;
- лек като софтуерна реализация;
- икономичен откъм потребление на системни ресурси;
- високопроизводителен;
- лесен за инсталиране;
- лесен за конфигуриране и административно обслужване;
- лесна и бърза актуализация на базата от данни;
- добра интеграция с BIND9;
- висока скорост на търсене и извличане на заявки;
- вътрешни механизми за повишаване на сигурността (ACI);
- ясен и прост механизъм за репликация на базата.

Red Hat Directory Server:

- наследник на Netscape Directory Server;
- отворен и изчистен изходен код с висока честота на одит;
- поддръжка на стабилните версии в рамките на дълъг жизнен цикъл;
- разработван от отворено общество на разработчици в рамките на Fedora Project;
- бърза реализация на актуализации по сигурността;
- голяма мрежа от потребители обменящи опит;
- обширна и удобна за четене документация;
- HTTP/HTTPS базирано API за управление и комуникация;
- с пъти по-бърз от OpenLDAP и по-функционален от него;
- лицензно чист и ясен.

BIND SDB (Simplified Database Backend):

- предлага поддръжка на BIND9 за съхранение на съдържанието на зони на домейни във външна за сървъра база данни – dirdb, SQL, LDAP;
- част от официалния пакет BIND9 на ISC;
- поддържа се от по-големите и значими UNIX и Linux дистрибуции;
- реализира услугата чрез нов демон – `named_sdb`, различен от `named`;
- прилага ясна и лесна за описание в директорийния сървър LDAP схема;
- предлага инструментариум за конвертиране на зона от файл към LDAP ldif съдържание и обратно (`zone2ldap`, `ldap2zone`).

Пригодена за Red Hat Directory Server LDAP схема за поддръжка на зона на домейн:

- **свободно достъпна на адрес:**

  http://www.vesselin.org/papers/files/dnszone.ldif

- **добавяема в реално време към контейнера със схеми на директорйния сървър (без рестартиране на услугата):**

```
$ ldapmodify -D “cn=Directory Manager” -w - -f dnszone.ldif
```

Деклариране на зона с LDAP поддръжка в BIND9 (`named.conf`):

```
zone "dnsbl.uni-sofia.bg" {
        type master;
        database "ldap ldap://127.0.0.1/dc=dnsbl.uni-
  sofia.bg,o=dns 3600";
};
```

Шаблон на dn за въвеждане на източник на SPAM в DNSBL:

- ldif файл (`new.ldif`):

```
dn: relativeDomainName=12,dc=100,dc=168,dc=192,dc=dnsbl.uni-
  sofia.bg,o=dns
objectClass: top
objectClass: dNSZone
relativeDomainName: 12
ARecord: 127.0.0.1
dNSTTL: 60
zoneName: dnsbl.uni-sofia.bg
```

- въвеждане в LDAP директорията:

```
$ ldapmodify -D “uid=manager,o=dns” -w - -f -a new.ldif
```

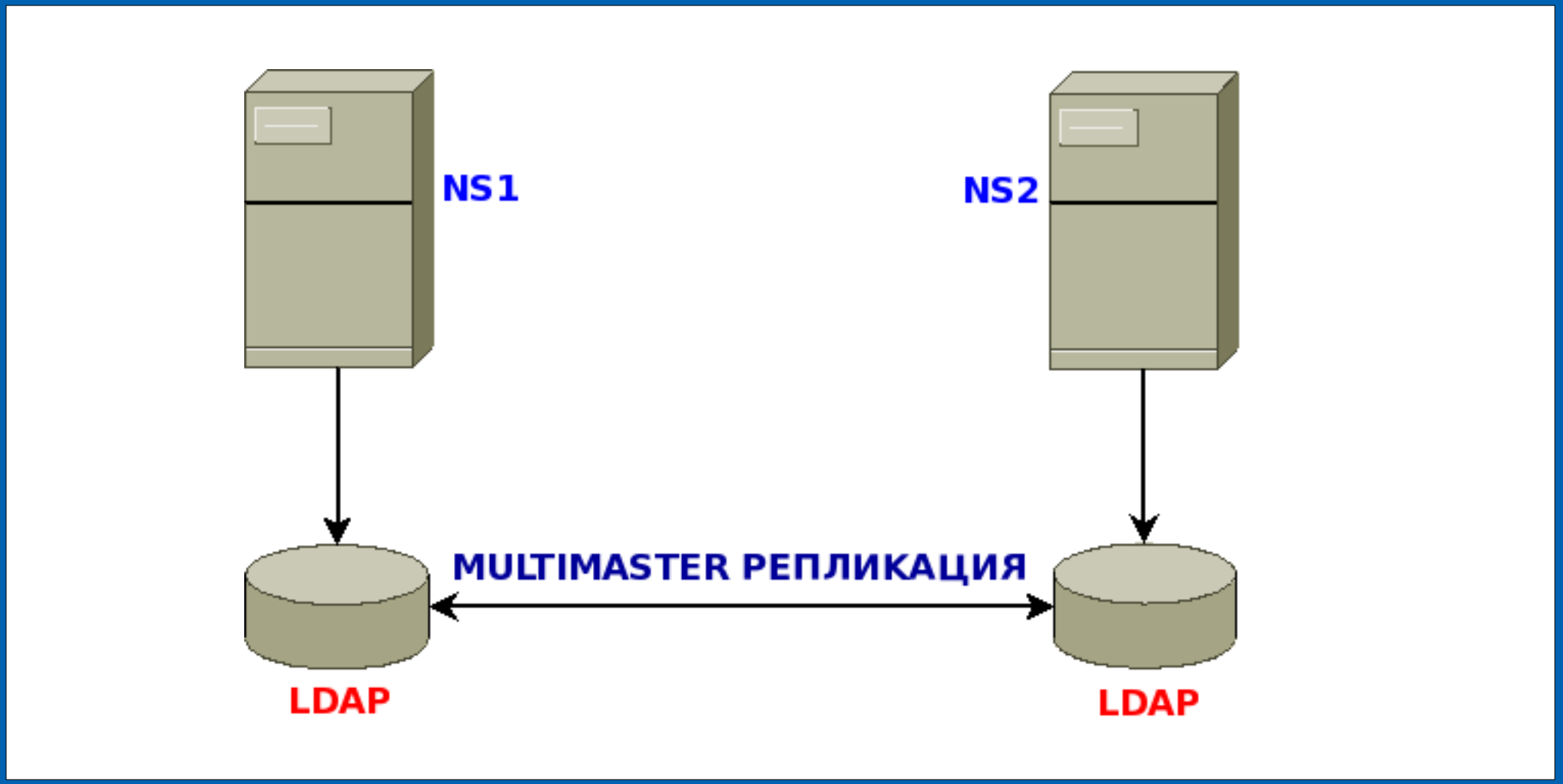
Софийски Университет
"Св. Климент Охридски"

DNSBL – колаборация с БИОМ

Проект за създаване на DNSBL с ресурси на БИОМ:

- да се създаде DNSBL зона на домейн (предложение dnsbl.acad.bg);
- да се изработи сървър за имена за домейна, свързани с йерархична база от данни в режим “multimaster” (споделяне на практически опит - СУ);
- да се изработи документ с ясни критерии как и кога един източник на SPAM се обявява в зоната и кога се премахва от нея;
- да се организира редовното актуализиране на съдържанието на зоната от одобрен за целта екип администратори, показали отговорно и безпристрастно поведение в Мрежата;
- да се обяви проекта публично в българското и световното интернет пространство.

Принципна схема на “multimaster” сървър за имена



Пример за недопустима и нарочна злоупотреба с DNSBL:

Описание:

Администраторът на DNSBL зоната на ISOC.BG Димитър Ганчев, в разрез с всякаква етика относно администрирането на подобен обществено обявен ресурс, прибавя като излъчвател на SPAM сървъра на NOVE Холдинг единствено и само заради възникнал личен конфликт между администратора на NOVE Атанас Бъчваров и председателя на ISOC.BG Вени Марковски.

- **Следствие:**

Загуба на доверие в ресурса и ISOC.BG

? ВЪПРОСИ ?

⇦ МНЕНИЯ ⇨

☜ ДИСКУСИЯ ☞