# DNSSEC – Provisionamento e Reassinatura Automática com Bind

GTER 30

Wilson Rogério Lopes <wilson@registro.br>

Nov / 2010

# Motivação

- Zonas com DNSSEC **precisam** ser reassinadas periodicamente

  RRSIG's tem um período de validade

- Falta de mecanismo padronizado para provisionamento de zonas nos servidores master/slaves.
- Bind a partir da versão 9.7.x fornece opções para provisionamento e reassinatura automática de zonas.

## DNSSEC

- Extensão do protocolo DNS
- Garante origem (autenticidade) e integridade
- Tutorial DNSSEC - ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf

## Bind

- Software do ISC que implementa o protocolo DNS
- Versão 9.7.2 - http://www.isc.org/software/bind/972-p2

# Agenda

- Cenário comum

  Provisionamento de zonas *master/slaves*

  Procedimento para assinatura de zonas com DNSSEC

  Administração das zonas – adição/remoção *resource records* (RR's)

- Cenário automatizado

  Provisionamento de zonas via rndc

  *Smart Signing*

  Administração de zonas via *dynamic updates*

- **Provisionamento de zonas no master e slaves**
- Servidor Master

  - Criar arquivo de zona

  - Incluir configuração da zona no named.conf (ou uso de *include*)

  - *Restart* ou *Hangup* no processo *named*

- Servidor Slave

  - Incluir configuração da zona no named.conf (forma “manual” ou scp,rsync...)

  - *Restart* ou *Hangup* no processo *named*

  * RR's da zonas recebidos via axfr/ixfr

- **Assinatura de zonas com DNSSEC**

  - Gerar chaves – *dnssec-keygen*

  - Include da chave no arquivo de zona

  - Assinar a zona – *dnssec-signzone*

  - Periodicamente reassinar as zonas

    . Update do Serial – Notify/XFR para os slaves

    . Assinar a zonas

- **Administração das zonas assinadas**
- Adição/Remoção de um ou mais RR's

  Necessário:

  - Update do *Serial*

  - Reassinar zona

  - *Restart/Hangup* do *named*

- **Provisionamento de zonas via rndc**

rndc – *remote name daemon control*

- TCP porta 953

- Usado para start/stop/reload do *named*

- Usa TSIG para assinar transação

- A partir da versão 9.7.0 – rndc sign

- A partir da versão 9.7.2 – rndc add zone / del zone

- **Provisionamento de zonas via rndc**
- Servidor master e slaves

- Habilitar configuração de zonas via rndc

named.conf

```
Options {
        …
        allow-new-zones yes;
        }
```

- **Provisionamento de zonas via rndc**
- Habilitar rndc e aplicar restrição de acesso

- Master

```
controls { inet 127.0.0.1 port 953
        allow { 127.0.0.1; } keys { "rndc-key"; };
        };
```

- Slave

```
controls { inet <ip_ext> port 953
        allow { <ip_servidor_master>; } keys { "rndc-key"; };
        };
```

- **Provisionamento de zonas via rndc**
- Gerar TSIG e incluir no rndc.conf

shell# dnssec-keygen -a HMAC-MD5 -b 512 -n HOST rndc-key

**rndc.conf**

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "AeXbgTDog1zh87trVIQFJHw==";
        };
options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
        };
```

- **Provisionamento de zonas via rndc e *Smart Signing***
- **Configurar zona – Servidor Master**

- Criar arquivo de zona - db.dominio.com.br

Deve conter pelo menos o SOA e os NS's

- Adicionar zona via rndc

shell# rndc addzone dominio.com.br '{type master; file "/etc/db.dominio.com.br"; **auto-dnssec maintain**; update-policy local; key-directory "etc/keys"; };'

. Gera um arquivo .nzf na raiz de configuração do Bind

. Não é necessário restart/hangup do *named*

**auto-dnssec maintain;**

- Permite o uso do *rndc sign* e a reassinatura automática das zonas quando necessário

**update-policy local;**

- Habilita o *dynamic update* na zona

- Permite somente updates vindos de localhost

- Gera automaticamente uma chave TSIG para assinar os dynamic updates

<bind-rootdir>/var/run/named/session.key

**key-directory "etc/keys";**

- Diretório que armazenará as chaves dnssec.

## Gerar chaves que assinarão a zona

shell# dnssec-keygen -r /dev/urandom -K <bind-rootdir>/etc/keys -f KSK -a RSASHA1 -b 1024 dominio.com.br

## Assinar zona – somente na inclusão da zona

shell# rndc sign dominio.com.br

*A zona será assinada com a chave privada respectiva e por default as assinaturas terão validade de 30 dias.

*A zona será reassinada e o serial será incrementado automaticamente pelo Bind quando necessário.

*Se já existir uma chave no diretório *keys* no ato da adição da zona via *rndc*, esta já será assinada, sem a necessidade de executar o *rndc sign*.

- **Provisionamento de zonas via rndc**
- **Configurar zona – Servidor Slave**

shell# rndc -s <ip-servidor-slave> addzone dominio.com.br '{type slave; file "/etc/db.dominio.com.br"; masters { ip-servidor-master; }; };'

. Gera um arquivo .nzf na raiz de configuração do Bind

. Não é necessário restart/hangup do *named*

Log:

24-Nov-2010 16:46:49.285 general: info: received control channel command 'addzone dominio.com.br {type master; file "/etc/db.dominio.com.br"; auto-dnssec maintain; update-policy local; key-directory "etc/keys"; };'

24-Nov-2010 16:46:49.285 general: info: zone dominio.com.br/IN: loaded serial 2010112401

24-Nov-2010 16:46:49.285 general: info: zone dominio.com.br/IN: reconfiguring zone keys

- **Provisionamento de zonas via rndc**
- **Remoção zona**

shell# rndc delzone dominio.com.br

Log:

20-Nov-2010 16:59:24.113 general: info: received control channel command 'delzone dominio.com.br'

20-Nov-2010 16:59:24.113 general: info: zone dominio.com.br removed via delzone

- **Administração de zonas via *dynamic updates***

*Dynamic update* – UDP porta 53

Operação necessária somente no servidor master

***nsupdate*** – cliente para administração de RR's via *dynamic updates*

**nsupdate -l**

- Conectará em localhost e usará chave “session.key”gerada pelo Bind.

Adicionar RR - update add <RR> <RDATA>

Remover RR – update delete <RR> <RDATA>

- **Administração de zonas via *dynamic updates***
  - Inclusão de um RR

```
shell# nsupdate -l
> update add www.dominio.com.br. 300 IN A 10.0.0.1
> show
Outgoing update query:
;; ->>HEADER<<- opcode: UPDATE, status: NOERROR, id:      0
;; flags:; ZONE: 0, PREREQ: 0, UPDATE: 0, ADDITIONAL: 0
;; UPDATE SECTION:
www.dominio.com.br.    300     IN      A       10.0.0.1

> send
```

- **Administração de zonas via *dynamic updates***

Log:

24-Nov-2010 16:55:52.849 update: info: client 127.0.0.1#11577: updating zone 'dominio.com.br/IN': adding an RR at 'www.dominio.com.br' A

* RR será automaticamente assinado

* Serial será incrementado automaticamente

* SOA e NSEC's afetados serão reassinados automaticamente

- **Administração de zonas via *dynamic updates***
  - Remoção de um RR

shell# nsupdate -l

> update delete www.dominio.com.br. A

> send

Log:

24-Nov-2010 16:58:37.376 update: info: client 127.0.0.1#62460: updating zone 'dominio.com.br/IN': deleting rrset at 'www.dominio.com.br' A

- **Administração de zonas via *dynamic updates***
  - Remoção de um RR

shell# nsupdate -l

> update delete www.dominio.com.br. A

> send

Log:

24-Nov-2010 16:58:37.376 update: info: client 127.0.0.1#62460: updating zone 'dominio.com.br/IN': deleting rrset at 'www.dominio.com.br' A

# Referências

- Tutorial DNSSEC Registro.br - ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf

- Alan Clegg, ISC – NANOG 50 - Deploying DNSSEC Using BIND 9.7 http://www.nanog.org/meetings/nanog50/presentations/Sunday/NANOG50.Talk6.NANOG-50-Clegg.pdf