Como configurar DNSSEC em seu dominio [1]

David Robert Camargo de Campos
Rafael Dantas Justo
<tutorial-dnssec@registro.br>

Registro.br

[1] versão 1.5.0 (Revision: 7419)
A última versão deste tutorial pode ser encontrada em: ftp://ftp.registro.br/pub/doc/configuracao_dnssec_dominio.pdf

Objetivo

- O objetivo deste tutorial é implantar DNSSEC no servidor autoritativo para determinado dominio
- Todas as operações serão executadas no servidor principal (*Master*)

Requisitos

- Bind 9.7 – http://www.isc.org/downloads

Passo 1 — Criação de Chaves

registro.br
Registro de Domínios para a Internet no Brasil

Utilização do comando `dnssec-keygen` para geração de chaves:

```
$ dnssec-keygen -r /dev/urandom -f KSK -a RSASHA1 -b 1024 -n ZONE dominio.com.br
```

Onde, dominio.com.br deve ser substituído pelo seu domínio.

- O comando irá gerar dois arquivos com extensões `.key` e `.private`

Mais informações podem ser encontradas no Tutorial de DNSSEC

nic.br

Passo 2 — Assinar o domínio (arquivo de zona)

registro.br
Registro de Domínios para a Internet no Brasil

Utilização do comando `dnssec-signzone` para assinatura

```
$ dnssec-signzone -S -z -o dominio.com.br db.dominio.com.br
```

Onde, dominio.com.br deve ser substituído pelo nome do domínio e db.dominio.com.br pelo nome do arquivo de zona.

- O comando irá gerar um novo arquivo de zona com a extensão `.signed`
- O período de validade padrão da assinatura é de 30 dias

Mais informações podem ser encontradas no Tutorial de DNSSEC

nic.br

Passo 3 — Atualização do named.conf

registro.br
Registro de Domínios para a Internet no Brasil

Alteração da referência para o arquivo de zona

```
zone "dominio.com.br" {
    type master;
    file "/etc/namedb/db.dominio.com.br.signed";
    ...
};
```

Onde, dominio.com.br deve ser substituído pelo nome do domínio e db.dominio.com.br deve ser substituído pelo nome do arquivo de zona.

nic.br

Reiniciar o Bind

Passo 5 — Adicionar o DS no site do Registro.br

Copiar os dados de **KeyTag** e **Digest** do arquivo **dsset-dominio.com.br** para a interface no site do Registro.br.

Exemplo: `$ cat dsset-dominio.com.br. | head -1`

		KeyTag			Digest
dominio.com.br	IN DS	15469	5	1	5EC0184678E0B7DC3AACFFA5D0EB9DBA1F3F6C37

- Onde, dominio.com.br deve ser substituído pelo nome do domínio

Passo 6 — Aguardar nova publicação

registro.br
Registro de Domínios para a Internet no Brasil

Aguardar nova publicação no site do Registro.br

nic.br

Roteiro — Configurar um Servidor Autoritativo

registro.br
Registro de Domínios para a Internet no Brasil

1. Criar chave (dnssec-keygen) (slide ??)
2. Assinar a zona (dnssec-signzone) (slide ??)
3. Modificar o named.conf (slide ??)
4. Reiniciar o BIND (named) no servidores Master
5. Adicionar o DS no site do Registro.br (slide ??)
6. Aguardar nova publicação

nic.br

registro.br
Registro de Domínios para a Internet no Brasil

Servidor Autoritativo

Reassinar a zona antes das assinaturas expirarem

1. Incrementar o serial (record SOA) do arquivo de zona original
2. Reassinar a zona utilizando o comando dnssec-signzone

Perguntas?

http://registro.br/suporte/tutoriais/dnssec.html

Envie suas dúvidas para tutorial-dnssec@registro.br