

## Laboratório 4 - DNSSEC

**Objetivo:** Configurar o DNSSEC do domínio cadastrado no beta.registro.br utilizando o BIND 9.

### Configurando DNSSEC no servidor Autoritativo1

1. Acesse o servidor DNS\_Autoritativo1 e crie a pasta de chaves do DNSSEC

```
# mkdir /var/cache/bind/keys  
# chown -R bind:bind /var/cache/bind/keys  
# cd /var/cache/bind/keys
```

2. Gere as chaves do DNSSEC

```
# dnssec-keygen -aECDSAP256SHA256 -f KSK dominio.teste.br
```

**Obs:** trocar dominio.teste.br pelo domínio que você cadastrou no beta

3. Crie a assinatura do seu domínio

```
# dnssec-signzone -S -z -o dominio.teste.br /etc/bind/zones/db.dominio.teste.br
```

**Obs:** trocar dominio.teste.br pelo domínio que você cadastrou no beta

4. Configure o arquivo /etc/bind/named.conf.local

```
# nano /etc/bind/named.conf.local
```

5. No arquivo named.conf.local insira as configurações do arquivo db.dominio.teste.br

```
zone "dominio.teste.br" {
    type master;
    file "/etc/bind/zones/db.dominio.teste.br.signed";
    key-directory "/var/cache/bind/keys/";
    allow-transfer { 2001:12ff:0:b113:0:0:XX:1005; };
    also-notify { 2001:12ff:0:b113:0:0:XX:1005; };
};
```

**Obs:** trocar o XX pelo número do seu grupo

**Obs2:** trocar dominio.teste.br pelo domínio que você cadastrou no beta

**Obs3:** no trecho zone "Y.Y. o número do grupo precisa ser invertido, então se seu grupo é o 15 por exemplo, Y.Y. seria 5.1. e não 1.5.

6. Salve o arquivo (CTRL+O e CTRL+X) e execute a verificação do bind para detectar possíveis erros de digitação

```
# named-checkconf
```

7. Reinicie o serviço do bind

```
# systemctl restart bind9
```

8. Teste para verificar se o DNSSEC está funcionando

```
# dig @2001:12ff:0:b113:0:0:XX:1004 dominio.teste.br +dnssec
```

**Obs:** trocar o XX pelo número do seu grupo

**Obs2:** trocar dominio.teste.br pelo domínio que você cadastrou no beta

## Configurando DNSSEC no servidor Autoritativo2

1. Acesse o servidor DNS\_Autoritativo2 e reinicie o bind

```
# systemctl restart bind9
```

2. Teste para verificar se o DNSSEC está funcionando

```
# dig @2001:12ff:0:b113:0:0:XX:1005 dominio.teste.br +dnssec
```

**Obs:** trocar o XX pelo número do seu grupo

**Obs2:** trocar dominio.teste.br pelo domínio que você cadastrou no beta

## Configurando DNSSEC no servidor Recursivo

1. Acesse a url <https://registro.br/tecnologia/dnssec/root-anchor/> e anote a chave pública da raiz

### Chave Pública da Raiz

O .br foi um dos pioneiros na adoção de DNSSEC com as primeiras zonas sendo assinadas em junho/2007. Desde então, interessados em utilizar esta tecnologia configuravam a chave KSK do .br em seus servidores DNS recursivos.

Com a assinatura da raiz do sistema DNS em 15/07/2010, recomenda-se que apenas a chave da raiz seja utilizada como Trust Anchor na configuração de servidores DNS recursivos.

As chaves da raiz do sistema DNS no formato de arquivo de configuração do BIND (9.7.0 ou superior):

```
. initial-key 257 3 8 "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiWlvkIbzxef3
+/4RgW0q7HrxRixH1FlExOLAjr5emLvN7SWXgnLh4+B5xQ1NVz8Og8kv
ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF
0jLHwVN8efs3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
oZG+SrDK6nWeL3c6H5Apxz7LjVclutIdsIXxuOLYA4/ilBmSVIzuDWfd
RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
R1AkUTV74bU=";
```

2. Acesse o servidor DNS\_Recursivo1 e configure o arquivo /etc/bind/named.conf.options

```
# nano /etc/bind/named.conf.options
```

3. Insira a configuração trust-anchors contendo a chave da raiz

```
trust-anchors {
. initial-key 257 3 8
    "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiWlvkIbzxef3
    +/4RgW0q7HrxRixH1FlExOLAjr5emLvN7SWXgnLh4+B5xQ1NVz8Og8kv
    ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF
    0jLHwVN8efs3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
    oZG+SrDK6nWeL3c6H5Apxz7LjVclutIdsIXxuOLYA4/ilBmSVIzuDWfd
    RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
    R1AkUTV74bU=";
};
```

4. Salve o arquivo (CTRL+O e CTRL+X) e execute a verificação do bind para detectar possíveis erros de digitação

```
# named-checkconf
```

5. Reinicie o serviço do bind

```
# systemctl restart bind9
```

6. Acesse o servidor DNS\_Recursivo2 e configure o arquivo /etc/bind/named.conf.options

```
# nano /etc/bind/named.conf.options
```

7. Insira a configuração trust-anchors contendo a chave da raiz

```
trust-anchors {  
  . initial-key 257 3 8  
    "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiWlvkIbzxeF3  
    +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv  
    ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLRjyBxWezF  
    0jLHwVN8efs3rCj/EWgviWgb9tarpVUDK/b58Da+sqqls3eNbuV7pr+e  
    oZG+SrDK6nWeL3c6H5Apxz7LjVclutIdsIXxuOLYA4/ilBmSVIzuDWfd  
    RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN  
    R1AkUTV74bU=";  
};
```

8. Salve o arquivo (CTRL+O e CTRL+X) e execute a verificação do bind para detectar possíveis erros de digitação

```
# named-checkconf
```

9. Reinicie o serviço do bind

```
# systemctl restart bind9
```