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

Neste teste, é esperado localizarmos alguns registros do DNSSEC presentes na resposta, como **RRSIG** que contém uma assinatura criptográfica e o **NSEC**, que é utilizado para provar com segurança que determinado domínio existe, ou não.

Configurando DNSSEC no servidor Recursivo

A Chave Pública está disponível no site https://registro.br/tecnologia/dnssec/root-anchor/ e pode ser anotada para a configuração do DNSSEC, mas também podemos utilizar o script abaixo:

1. Acesse o servidor **DNS_Recursivo1** e faça o download do script do Registro.br para obter a Chave Pública da Raiz:

```
# wget https://ftp.registro.br/pub/doc/fetch_root_anchor.sh
```

2. Execute o script baixado. Copie o **initial-key** exibido após a execução.

```
# chmod +x fetch_root_anchor.sh
# ./fetch_root_anchor.sh
```

Após a execução do script, deverá aparecer no terminal duas chaves públicas da raiz, como visto abaixo. Utilizaremos a chave destacada em negrito.

```
. initial-key 257 3 8
"AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJN
nOAlFNKF2jBosZBU5eeHspaQWOmOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6i
rwCzVBApESjbUdpWWmEnhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUK
EpUge71M3ej2/7CPqpdVwuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XB
uzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxPvYLw4z9mR7K2vaF18UYH9Z9GNUUeayffKC73
PYc=";
. initial-key 257 3 8
"AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRi
xHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n
9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqql
s3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUf
hHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=";
```

3. Copie a chave pública da raiz demarcada e configure o arquivo /etc/bind/named.conf.options

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

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

```
trust-anchors {
. initial-key 257 3 8
         "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
          +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
          ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
          0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
          oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
          RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
          R1AkUTV74bU=";
};
```

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

```
# named-checkconf
```

6. Reinicie o serviço do bind

```
# systemctl restart bind9
```

7. Acesse o servidor **DNS_Recursivo2**, realize o download do script novamente e anote a chave pública.

```
# wget https://ftp.registro.br/pub/doc/fetch_root_anchor.sh
# chmod +x fetch_root_anchor.sh
# ./fetch_root_anchor.sh
```

```
. initial-key 257 3 8
"AwEAAa96jeuknZlaeSrvyAJj6ZHv28hhOKkx3rLGXVaC6rXTsDc449/cidltpkyGwCJN
nOAlFNKF2jBosZBU5eeHspaQWOmOElZsjICMQMC3aeHbGiShvZsx4wMYSjH8e7Vrhbu6i
rwCzVBApESjbUdpWWmEnhathWu1jo+siFUiRAAxm9qyJNg/wOZqqzL/dL/q8PkcRU5oUK
EpUge71M3ej2/7CPqpdVwuMoTvoB+ZOT4YeGyxMvHmbrxlFzGOHOijtzN+u1TQNatX2XB
uzZNQ1K+s2CXkPIZo7s6JgZyvaBevYtxPvYLw4z9mR7K2vaF18UYH9Z9GNUUeayffKC73
PYc=";
. initial-key 257 3 8
"AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3+/4RgWOq7HrxRi
xHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kvArMtNROxVQuCaSnIDdD5LKyWbRd2n
9WGe2R8PzgCmr3EgVLrjyBxWezF0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqql
s3eNbuv7pr+eoZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfdRUf
hHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwNR1AkUTV74bU=";
```

8. Configure o arquivo /etc/bind/named.conf.options

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

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

```
trust-anchors {
. initial-key 257 3 8
         "AwEAAaz/tAm8yTn4Mfeh5eyI96WSVexTBAvkMgJzkKTOiW1vkIbzxeF3
          +/4RgWOq7HrxRixHlFlExOLAJr5emLvN7SWXgnLh4+B5xQlNVz8Og8kv
          ArMtNROxVQuCaSnIDdD5LKyWbRd2n9WGe2R8PzgCmr3EgVLrjyBxWezF
          0jLHwVN8efS3rCj/EWgvIWgb9tarpVUDK/b58Da+sqqls3eNbuv7pr+e
          oZG+SrDK6nWeL3c6H5Apxz7LjVc1uTIdsIXxuOLYA4/ilBmSVIzuDWfd
          RUfhHdY6+cn8HFRm+2hM8AnXGXws9555KrUB5qihylGa8subX2Nn6UwN
          R1AkUTV74bU=";
};
```

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

```
# named-checkconf
```

11. Reinicie o serviço do bind

```
# systemctl restart bind9
```

12. Acesse o **Cliente** e teste o DNSSEC.

```
# dig @2001:12ff:0:b113::XX:1001 dominio.teste.br +dnssec
# dig @2001:12ff:0:b113::XX:1002 dominio.teste.br +dnssec
```

Neste teste, esperamos localizar, além dos registros do DNSSEC presentes na resposta, como **RRSIG** que contém uma assinatura criptográfica e o **NSEC**, que é utilizado para provar com segurança que determinado domínio existe, ou não, outras flags como **ad** (**Authenticated Data**) no header e **do** (**DNSSEC OK**), indicando que o servidor recursivo possui DNSSEC habilitado. A flag **ad** mostra que a resposta recebida passou pelo processo de validação do DNSSEC.