

DNSSHIM DNSSEC Automatizado

<dnsshim@registro.br>

GTER 27
19 de junho de 2009

O que é?

Ferramenta open-source que implementa o protocolo DNS e automatiza todo processo de provisionamento de zonas com suporte a DNSSEC

- Complexidade na implementação e manutenção de DNSSEC
- Gradual adoção de DNSSEC pelo mundo (.org, .gov e alguns ccTLDs)
- Possível assinatura da raiz no futuro
- Todos os TLDs sob o .br com suporte a DNSSEC
- Baixa adoção da extensão DNSSEC nos domínios .br

Adoção de DNSSEC no Mundo

Fonte: <http://www.xelerance.com/dnssec/>

World Wide DNSSEC Deployment



This map was created by Paul Wouters

Objetivo

- Promover e facilitar a utilização de DNSSEC

Objetivo

- Promover e facilitar a utilização de DNSSEC

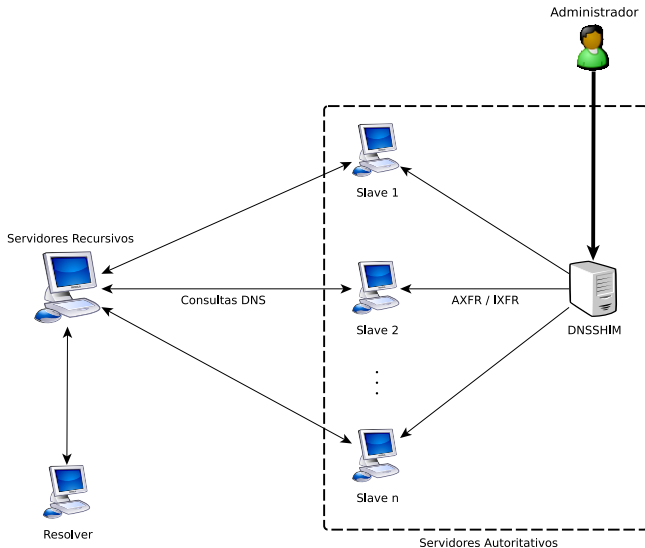
Público Alvo

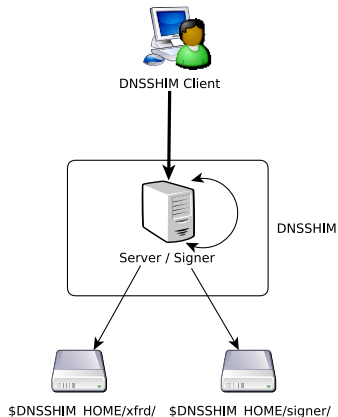
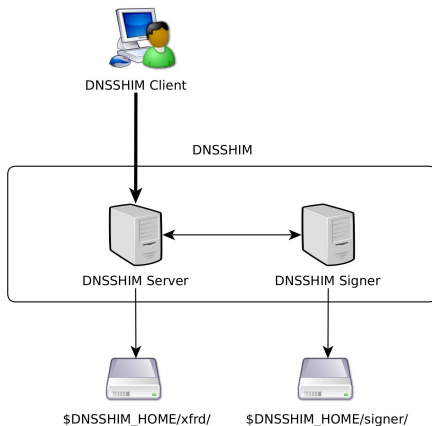
Provedores de hospedagem ou qualquer outra instituição responsável por administrar servidores DNS autoritativos para muitas zonas

- Código-fonte aberto
- Implementação em Java 1.6
- Módulo signer separado do servidor principal
- Protocolo para comunicação com cliente em XML

- DNSSEC
- Suporta AXFR e IXFR com TSIG
- Gerenciamento de chaves e assinaturas
- Importação de zonas já existentes em outros servidores via AXFR
- Importação de chaves (DNSKEY) a partir de arquivo no formato do Bind
- Gerenciamento de grupos de servidores slave
- Provisionamento automático de zonas aos servidores slave

- A
- AAAA
- CNAME
- DNSKEY
- DS
- MX
- NS
- NSEC
- RRSIG
- SOA
- TXT
- CERT
- DNAME
- HINFO
- IPSECKEY
- LOC
- MINFO
- NAPTR
- OPT
- PTR
- SRV
- SSHFP
- TSIG





- Vários usuários simultâneos
- Cada zona pode ser administrada por um ou mais usuários
- Controle de sessão por usuário
 - ▶ Login e senha

- Zonas com suporte a DNSSEC por default
 - ▶ DNSKEY gerada automaticamente na criação da zona
- Assinaturas válidas por 1 mês (default)
 - ▶ Lembrete: As chaves não expiram

Lembrete

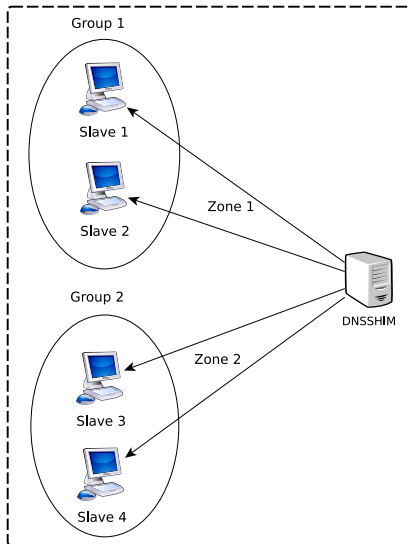
Cada record de assinatura (RRSIG) possui data de validade *inicial* e *final*

- Baseado no conceito de:
 - ▶ `scheduler_high_priority`
 - ▶ `scheduler_low_priority`
(*ambos definidos em horas*)
- Onde: `scheduler_high_priority` < `scheduler_low_priority`

Passos de Reassinatura

- 1 **Se** tempo para expiração < `scheduler_high_priority` então reassina a zona imediatamente
- 2 **Senão** reassina a zona em algum instante entre `scheduler_high_priority` e `scheduler_low_priority` antes da expiração

- Permite a criação de múltiplos grupos
- Facilita o gerenciamento de grandes quantidades de servidores
- Disponibilização de zonas por grupos
 - Exemplo: Zonas com grande demanda de requisições podem fazer parte de diversos grupos



- Utiliza XML
- TCP + TLS

Exemplo (Adição de Record)

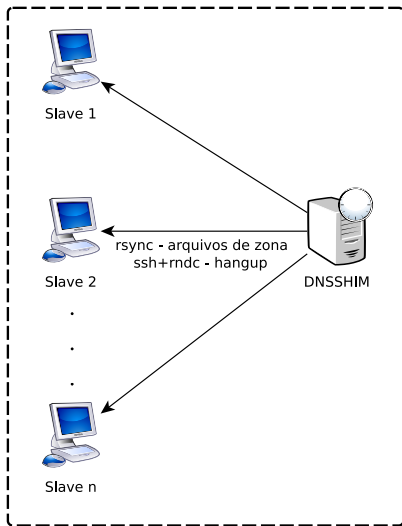
```
<?xml version="1.0" encoding="utf-8"?>
<dnsshim version="1.0">
  <request>
    <addRr>
      <sessionId>1</sessionId>
      <zone>gter.nic.br</zone>
      <rr>
        <ownername>www</ownername>
        <ttl>86400</ttl>
        <type>CNAME</type>
        <dnsClass>IN</dnsClass>
        <rdata>gter.nic.br</rdata>
      </rr>
    </addRr>
  </request>
</dnsshim>
```

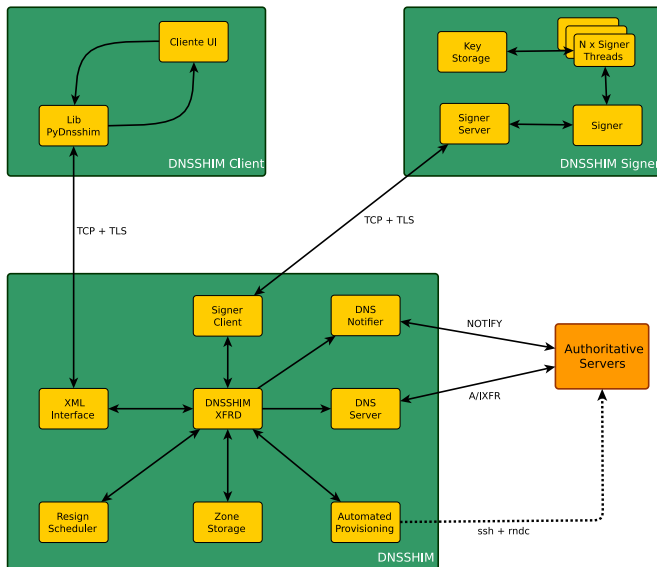
- Possibilidade de integração com outros sistemas
- Disponibilização de biblioteca em python

Provisionamento Automático de Zonas

Configuração automática dos servidores slaves para as zonas

- Compatível com Bind
- rsync
- ssh
- rndc





Dnssh – Cliente Shell-Like

- Interface em “linha de comando”
- Suporte a todos os recursos disponíveis pelo DNSSHIM
- Implementação em Python

pydnsshim – Biblioteca cliente

- Biblioteca em python para o desenvolvimento de aplicações cliente

- Cliente com interface gráfica
- Serviço Web para hospedagem DNS



Site do DNSSHIM

<http://registro.br/dnsshim/>



Tutorial de DNSSEC

<ftp://ftp.registro.br/pub/doc/tutorial-dnssec.pdf>



Manual do DNSSHIM (Inglês)

ftp://ftp.registro.br/pub/dnsshim/manual_en.pdf



DNSSHIM - Protocolo e Transporte (Inglês)

ftp://ftp.registro.br/pub/dnsshim/protocol_en.pdf

Perguntas?

Obrigado!