Asegurando tu Zona DNS con DNSSEC: Un Paso a Paso Detallado

DNSSEC (Domain Name System Security Extensions) es una suite de extensiones al Sistema de Nombres de Dominio (DNS) que añade una capa de seguridad criptográfica. Su objetivo principal es proteger a los usuarios de ataques como la suplantación de DNS (DNS spoofing) y el envenenamiento de caché, asegurando que las respuestas DNS que reciben son auténticas y no han sido manipuladas.

Conceptos Clave en DNSSEC

Antes de sumergirnos en el procedimiento, es fundamental entender algunos conceptos clave:

- **Firmado de Zona (Zone Signing):** Este es el proceso de añadir firmas digitales a los registros DNS dentro de una zona. Estas firmas son generadas usando claves criptográficas y permiten a los resolvedores DNS verificar la autenticidad e integridad de los datos.
- **Firmado de Registros (Record Signing):** Cada registro DNS individual dentro de una zona firmada incluye una firma digital (registro RRSIG) que puede ser verificada por los resolvedores.
- **Claves DNSSEC:** DNSSEC utiliza un par de claves criptográficas:
    - **Clave de Firma de Zona (ZSK - Zone Signing Key):** Esta clave se utiliza para firmar los registros DNS individuales dentro de una zona. Se cambia con más frecuencia que la KSK.
    - **Clave de Firma de Claves (KSK - Key Signing Key):** Esta clave se utiliza para firmar la ZSK y es la clave que se publica en el dominio padre (a través de un registro DS). La KSK se cambia con menos frecuencia y es la ancla de confianza de la zona.
- **Registro DS (Delegation Signer):** Este registro se publica en la zona padre (en este caso, `aula11.local`) y contiene un hash criptográfico de la KSK de la zona hija (en este caso, tu zona delegada). Es crucial para establecer la cadena de confianza.
- **Registro DNSKEY:** Contiene las claves públicas (tanto la KSK como la ZSK) de la zona. Es utilizado por los resolvedores para verificar las firmas.

Procedimiento para Firmar la Zona "pais.aula11.local"

A continuación, se detalla el procedimiento paso a paso para firmar tu zona delegada, que denominaremos **[nombre_de_tu_zona]**.aula11.local. Recuerda **cambiar "pais" por el nombre que te haya sido asignado para tu zona**. Para este ejemplo, asumiremos el nombre ficticio "pais". La zona `aula11.local` está en el servidor 10.1.1.100 y tu zona delegada (pais.aula11.local) está en el servidor 10.1.1.120.

En el Servidor DNS de tu Zona Delegada (10.1.1.120)

Aquí es donde realizarás la mayor parte del trabajo para generar las claves y firmar la zona. Asumiremos que estás utilizando BIND como tu servidor DNS.

1. Generar las Claves DNSSEC

Necesitarás generar una ZSK y una KSK para tu zona. Es una buena práctica crear un directorio específico para tus claves DNSSEC.

```
sudo mkdir /etc/bind/keys/pais.aula11.local
sudo chown bind:bind /etc/bind/keys/pais.aula11.local
sudo chmod 700 /etc/bind/keys/pais.aula11.local
cd /etc/bind/keys/pais.aula11.local
```

Ahora, genera las claves:

- **Generar la KSK (Key Signing Key):**

  ```
  sudo dnssec-keygen -a ECDSAP256SHA256 -b 256 -n ZSK -fk pais.aula11.local
  ```

  - `-a ECDSAP256SHA256`: Algoritmo de criptografía (recomendado).
  - `-b 256`: Tamaño de la clave en bits.
  - `-n ZSK`: Tipo de clave (ZSK).
  - `-f KSK`: Marca la clave como una KSK.
  - `pais.aula11.local`: Nombre de tu zona.

  Esto creará dos archivos: `K<tu_zona>+<id_clave>+<version>.key` (clave pública) y `K<tu_zona>+<id_clave>+<version>.private` (clave privada).

- **Generar la ZSK (Zone Signing Key):**

  ```
  sudo dnssec-keygen -a ECDSAP256SHA256 -b 256 -n ZSK pais.aula11.local
  ```

  - `-n ZSK`: Tipo de clave (ZSK).

  Esto también creará dos archivos `K<tu_zona>+<id_clave>+<version>.key` y `K<tu_zona>+<id_clave>+<version>.private`.

2. Configurar la Zona en BIND para DNSSEC

Edita el archivo de configuración de tu zona (por ejemplo, `/etc/bind/db.pais.aula11.local`).

Añade las siguientes líneas a tu archivo de zona, idealmente al principio:

DNS Zone file

```
$TTL 1D
```

```
@       IN      SOA     ns1.pais.aula11.local. admin.pais.aula11.local. (
                             2025071101 ; Serial
                             3H         ; Refresh
                             1H         ; Retry
                             1W         ; Expire
                             1D )       ; Negative Cache TTL
        IN      NS      ns1.pais.aula11.local.
ns1     IN      A       10.1.1.120
```

Para activar DNSSEC, **NO AÑADAS MANUALMENTE LOS REGISTROS DNSKEY O RRSIG**. BIND los generará automáticamente cuando firmes la zona.

3. Modificar la Configuración de BIND para Cargar las Claves y Firmar la Zona

Edita tu archivo `named.conf.local` o el archivo de configuración de zona principal de BIND.

Asegúrate de que tu definición de zona se vea algo así:

Fragmento de código

```
zone "pais.aula11.local" {
    type master;
    file "/etc/bind/db.pais.aula11.local";
    allow-update { none; };
    key-directory "/etc/bind/keys/pais.aula11.local"; # Ruta donde guardaste las
claves
    auto-dnssec maintain;
    inline-signing yes; # Habilita el firmado en línea
};
```

- `key-directory`: Especifica la ubicación de tus claves DNSSEC.
- `auto-dnssec maintain`: Indica a BIND que gestione automáticamente las firmas DNSSEC.
- `inline-signing yes`: Habilita el firmado "en línea", lo que significa que BIND gestionará el proceso de firmado automáticamente sin necesidad de `dnssec-signzone`.

4. Recargar BIND

Una vez que hayas realizado los cambios en la configuración de BIND, recárgalo para que tome los nuevos ajustes y firme la zona.

```
sudo systemctl reload named
```

Si no hay errores, BIND habrá firmado la zona automáticamente. Puedes verificar la existencia de los registros `DNSKEY` y `RRSIG` utilizando `dig`.

```
dig @10.1.1.120 pais.aula11.local DNSKEY +short
dig @10.1.1.120 www.pais.aula11.local RRSIG +short
```

En el Servidor DNS Padre (aula11.local - 10.1.1.100)

El siguiente paso crucial es establecer la cadena de confianza en el dominio padre.

1. Obtener el Registro DS de la Zona Hija

Desde el servidor de tu zona delegada (10.1.1.120), necesitas obtener el registro DS generado a partir de tu KSK. BIND debería haber generado este registro automáticamente después de firmar la zona. Puedes encontrarlo en el archivo `.ds` o `.key` de tu KSK.

Para obtener el registro DS directamente:

```
cd /etc/bind/keys/pais.aula11.local
sudo dnssec-dsfromkey Kpais.aula11.local.<ID_KSK>.key
```

Reemplaza `<ID_KSK>` con el ID de la clave de tu KSK (lo encontrarás en el nombre del archivo `.key`).

La salida debería ser similar a esta:

```
pais.aula11.local. IN DS 12345 13 2 <HASH_DS_DE_TU_KSK>
```

Copia esta línea completa del registro DS. Este es el registro que debes agregar a la zona padre.

2. Agregar el Registro DS a la Zona Padre (aula11.local)

En el servidor DNS padre (10.1.1.100), edita el archivo de zona para `aula11.local` (por ejemplo, `/etc/bind/db.aula11.local`).

Busca la delegación existente para `pais.aula11.local` y añade la línea del registro DS que copiaste.

DNS Zone file

```
; Delegación de la zona pais.aula11.local
pais.aula11.local.      IN      NS      ns1.pais.aula11.local.
ns1.pais.aula11.local.  IN      A       10.1.1.120

; Registro DS para pais.aula11.local (generado de la KSK de pais.aula11.local)
pais.aula11.local. IN DS 12345 13 2 <HASH_DS_DE_TU_KSK>
```

Asegúrate de incrementar el número de serie (Serial) en el registro SOA de `aula11.local` para que los cambios sean reconocidos.

3. Recargar BIND en el Servidor Padre

Guarda el archivo de zona `db.aula11.local` y recarga BIND en el servidor padre.

```
sudo systemctl reload named
```

Verificación

Una vez completados todos los pasos, puedes verificar que DNSSEC está funcionando correctamente.

- **Desde un Resolvedor Validante (por ejemplo, utilizando `dig` con la opción `+dnssec`):**

  ```
  dig @10.1.1.100 pais.aula11.local +dnssec
  ```

  Deberías ver los registros `DNSKEY` y `RRSIG` en la respuesta. Si tu resolvedor está configurado para validar, también verás la bandera `ad` (authenticated data) en la respuesta, lo que indica que la validación DNSSEC fue exitosa.

- **Herramientas en Línea:** Puedes usar herramientas en línea como el validador DNSSEC de Verisign o el DNSSEC Analyzer de GRC para verificar la configuración de tu zona. Sin embargo, estas herramientas funcionarán solo si tu zona es accesible públicamente. Para tu entorno local, `dig` es la herramienta principal.

Al seguir estos pasos, habrás asegurado tu zona delegada `[nombre_de_tu_zona].aula11.local` con DNSSEC, añadiendo una capa vital de seguridad para tus alumnos y su comprensión de la infraestructura DNS.