Módulo B-DNSSEC Windows 2022 Server

VERIFICADO EN ESCENARIO

Pasos para Configurar DNSSEC en Windows Server 2022 (DC nuestro escenario)

---

1. Abrir la Consola DNS

Desde el servidor con rol DNS:

1. Abre **Server Manager → Tools → DNS**.
2. Selecciona la zona DNS que deseas firmar (skillsnet.dk).

---

2. Firmar la Zona DNS

1. Menu Action → **DNSSEC → Sign the Zone**.
2. Se abrirá el asistente **Zone Signing Wizard**.

3. Usar el Asistente para Firmar la Zona

1. **Select Signing Parameters**:
    - Puedes usar configuraciones predeterminadas o personalizar (recomendado para entornos avanzados).
    - Si es tu primera vez, selecciona **Use default settings**.
2. **Completar la Firma**:
    - Haz clic en **Finish** para completar el proceso.
    - La zona será firmada automáticamente.

---

4. Configurar Validación DNSSEC (en Clientes o Forwarders)

Para que los clientes validen respuestas DNS con DNSSEC, el servidor que les resuelve debe estar configurado para validar firmas.

1. En el servidor DNS (en DNS Manager) que actúa como **resolutor**:
    - Clic derecho en el nombre del servidor → **Properties**.
    - Ve a la pestaña **Advanced**.
    - Marca **Enable DNSSEC validation for remote responses**. (verificar que está seleccionado)

5. Verificar DNSSEC

Desde un cliente o el mismo servidor DNS, usa PowerShell o `nslookup` para probar:

```
Resolve-DnsName srv2.skillsnet.dk -DnsOnly -DnsSecOk
```

Si todo está bien, verás el campo `RRSIG` en la respuesta.
