# Operación y Seguridad de DNS Avanzado

## Listas de Acceso en BIND

# ACLs en BIND

- Los ACLs y las opciones de configuración pueden servir para hacer BIND mucho más seguro
- Se recomienda que se revisen los ACLs y las opciones regularmente
- Asegúrese de que aún son relevantes: revise que aún reflejan lo que usted quiere lograr
- Pueden ser difíciles de mantener

# Elementos en un ACL

- Direcciones IP individuales
- Pares de direcciones y máscaras
- Nombres de otros ACLs
- En algunos contextos, nombres de claves (más sobre esto luego)

# Finalidad

- Restringir las peticiones de récords y de transferencias de zonas
- Autorizar/restringir las actualizaciones dinámicas
- Seleccionar una interfaz donde escuchar
- Ordenar respuestas
- Las listas de concordancia siempre van envueltas en {}

# Notas sobre las listas

- Los elementos deben ir separados por punto y coma ‘;’
- La lista debe terminarse con punto y coma“;”
- Los elementos en las listas se evalúan en orden secuencial
- Para negar elementos de la lista, use el signo de exclamación como prefijo ‘!’
- Utilice los comandos para nombrar las listas
- Se deben definir los ACLs antes de que puedan aplicarse en otras secciones

# Ejemplo: ACLs

- Para la red 192.167.0.0 255.255.255.0:

  { 192.168.0.0/24; };

- Para la red, más el loopback:

  { 192.168.0.0/24; 127.0.0.1; };

- Direcciones más nombre de clave:

  {192.168.0.0/24; 127.0.0.1; noc.ws.nsrc.org; };

# El comando ACL

- Sintaxis:

  acl nombre { lista; };

- Ejemplo:

  acl internal { 127.0.0.1; 192.168.0/24; };
  acl dynamic-update { key dhcp.ws.nsrc.org; };

# Notas sobre el comando ACL

- El nombre del ACL no tiene que estar entre comillas

- Hay cuatro ACLs pre-determinados:

  any - cualquier dirección IP

  none - ninguna dirección

  localhost - loopback, 127.0.0.1, ::1

  localnets - Todas las subredes a las que está conectado el servidor

# Blackhole

```
options {
    blackhole { nombre-ACL o lista de elementos; };
};
```

# Allow-transfer

```
zone “mizona.ejemplo”      {
        type master;
        file “mizona.ejemplo”;
        allow-transfer { nombre-ACL o lista de elementos; };
        };
```

# Allow-query

```
zone “mizona.ejemplo”      {
        type master;
        file “mizona.ejemplo”;
        allow-query {nombre-ACL o lista de elementos; };

        };
```

# Listen-on

```
options    {
        listen-on port # {nombre-ACL o lista de elementos; };


        };
```

# Preguntas

?