Advanced DNS Operations & Security

DNS Access Lists in BIND

DNS ACLs

- ACLs and configuration options in BIND can be used to create more secure configurations
- Good operational practice suggests that ACLs and configuration options be reviewed regularly
- Make sure they are still relevant: review them regularly to ensure they are accurately reflect what you are trying to do
- It can be cumbersome and difficult to maintain

Elements in an address match list

- Individual IP addresses
- Addresses/netmask pairs
- Names of other ACLs
- In some contexts, names of keys (more on this later)

Purposes in BIND

- Restricting queries & zone xfer
- Authorizing/restricting dynamic updates
- Selecting interface to listen on
- Sorting responses
- Address match lists are always enclosed in curly braces

Notes on Address Match list

- Elements must be separated by semicolons ‘;’
- The list must be terminated with “;”
- Elements address match lists are checked squentially
- To negate elements of the address match list, prepend them with ‘!’
- Use ACL statements to name an address match list
- ACLs must be defined before they can be used elsewhere

Example: Address match lists

- For network 192.167.0.0 255.255.255.0:

  { 192.168.0.0/24; };

- For network plus loopback:

  { 192.168.0.0/24; 127.0.0.1; };

- Addresses plus key name:

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

The ACL statement

- Syntax:

  acl acl_name { address_match_list; };

- Example:

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

Notes on the ACL statement

- The acl name need not be quoted:

- There are four predefined ACLs:

any	- any IP address
none	- no IP address
localhost	- loopback, 127.0.0.1
localnets	- all the networks the name server is directly connected to

Blackhole

```
options {
    blackhole { ACL-name or itemized list; };
};
```

Allow-transfer

```
zone “myzone.example      {
        type master;
        file “myzone.example”;
        allow-transfer { ACL-name or itemized list; };

        };
```

Allow-query

```
zone “myzone.example      {
        type master;
        file “myzone.example”;
        allow-query { ACL-name or itemized list; };

        };
```

Listen-on

```
options     {
        listen-on port # { ACL-name or itemized list; };

        };
```

Questions

?