Sécurité et fiabilité du DNS

Listes d'accès (ACL) dans BIND

Listes d’accès DNS

- Les ACL (listes d’accès) et les options de configuration dans BIND peuvent être utilisées pour créer des configurations plus robustes.
- Les bonnes pratiques opérationnelles suggèrent qu’il faut revoir de manière régulière les options de configuration et les ACLs.
- Assurez-vous qu’elles soient toujours pertinentes: les passer en revue de manière régulière et s’assurer qu’elles reflètent correctement ce que vous essayez de faire.
- Ceci peut devenir fastidieux et difficile à maintenir

Éléments d’une liste ”address match” (qualification d’adresse)

- Adresses IP individuelles
- Réseaux avec masques d’adresse
- Les noms d’une autre ACLs (liste d’accès)
- Dans certains contexte, le nom d’une clé cryptographique (nous en reparlerons)

Leur utilité dans BIND

- Limiter les requêtes et l'accès au transfert de zone
- Autoriser / interdire les mises à jour dynamiques
- Indiquer sur quelle interface BIND doit écouter
- Trier les réponses
- Les listes de qualification d'adresse sont toujours entourées d'accolades '{ et }'

Notes sur les liste ”address match” (qualification d’adresse)

- Les éléments doivent être séparées par un “;”
- La liste doit se terminer par “;”
- Les éléments d’une liste address match sont traités dans l’ordre (en séquence)
- Pour donner l’inverse d’un élément dans une liste address match, le préfixer avec “!”
- Utiliser les déclaration des ACLs pour nommer les listes address match
- Les ACLs doivent être définies avant de pouvoir les utiliser ailleurs.

Exemples de liste address match

- Pour le réseau 192.168.0.0 255.255.255.0:

  { 192.168.0.0/24; };

- Pour le réseau et l'adresse locale:

  { 192.168.0.0/24; 127.0.0.1; };

- Adresses et nom de clé cryptographique:

  {192.168.0.0/24; 127.0.0.1; key-noc-nsrc; };

La déclaration d'ACL

- Syntaxe:

  acl nom_acl{ liste_qualification_adresse; };

- Exemple:

  acl interne{ 127.0.0.1; 192.168.0/24; };
  acl mise-a-jour-dynamique { key cle-nsrc-dhcp; };

Notes sur les éléments d'une ACL

- Le nom de l'ACL n'a PAS besoin d'être encadré de guillements

- Il y a 4 ACLs prédéfinies:

any	- n'importe quelle adresse IP
none	- aucune adresse IP
localhost	- loopback, 127.0.0.1, ::1
localnets	- tous les réseaux auxquels la machine faisant tourner BIND est raccordée

Trou noir

```
options {
    blackhole { nom-ACL ou liste d'éléments; };
};
```

allow-transfer

```
zone “myzone.exemple”     {
        type master;
        file “myzone.exemple”;
        allow-transfer {nom-ACL ou liste d’éléments; };

        };
```

allow-query

```
zone “myzone.exemple      {
        type master;
        file “myzone.exemple”;
        allow-query {nom-ACL ou liste d’éléments; };

        };
```

listen-on

```
options     {
        listen-on port # {nom-ACL ou liste d'éléments; };

        };
```

Questions

?