DNS服務主機安裝實務

高雄市政府教育局
資訊教育中心

- 基礎安裝
- 服務型態與設定
- 安全與維運

基礎安裝

CentOS 7.x 安裝

- 最新版本
  - 7.5.1804
- 最小安裝
  - 相容性函式庫
- 基礎架構伺服器
  - DNS名稱伺服器
  - 相容性函式庫
  - 效能工具
- 安裝後更新
  - yum –y update

DNS服務初體驗→CachingDNS

- 檢查DNS服務套件是否安裝?
  - rpm -qa | grep named
- 啟動DNS服務
  - systemctl start named-chroot
- 查看DNS服務狀態
  - systemctl status named-chroot
- 查看DNS服務紀錄(log)
  - journalctl --unit=named-chroot
- 測試DNS服務
  - dig @127.0.0.1 www.google.com a
- 設定開機啟動
  - systemctl enable named-chroot

開放DNS主機對外提供服務

- 修改DNS設定檔(named.conf)
  options {
  - listen-on port 53 { ~~127.0.0.1;~~ any; };
  - listen-on-v6 port 53 { ~~::1;~~ any; };
  - allow-query   { ~~localhost;~~ any; };
- 重啟DNS服務
  - rndc reload
  - systemctl restart named-chroot
- 設定防火牆
  - firewall-cmd --add-service=dns
  - firewall-cmd --list-all
  - firewall-cmd --add-service=dns **--permanent**

測試DNS主機

- 查詢DNS主機(在PC上測試)
  - dig @192.168.173.189 www.google.com a
  - dig @192.168.173.189 www.nctu.edu.tw a

從安裝好的ova檔滙入

- 下載實作OVA檔
- 滙入virtual box，注意一下虛擬機組態
- 開機
- 預設帳號密碼
  - root/happy_dns@kh
  - user/happy_dns@kh

恭禧您! 已完成最簡單的 DNS服務主機!!

CachingDNS服務

優化您的DNS服務

- 找個好靠山→詢問上層最近的DNS服務主機
  節省每次都到dns root查詢的時間
  修改named.conf

```
options {  // 描述內最後一行增加以下設定

        max-cache-size 0;
        forward only;
        forwarders {  // 這裡放入最近的上層DNS主機IPv4/IPv6 IP
                163.28.136.14;
                2001:288:8201:1::10;
        };
};
```

- 記得向上層DNS管理單位徵詢，同意後才可實行!

讓您的DNS主機更安全

- 限制查詢網段
  - 修改named.conf
  - 在 options { 之前設定ACL

```
acl querynets {
    localhost;          localnets;
    // 放入您允許查詢這台DNS主機的網段
    192.168.4.0/24;           192.168.5.0/24;
    2001:288:8201:9::/64;  2001:288:8201:7::/64;
};
```

  - 在 options {   // 描述中修改下列參數

```
listen-on port 53 { any; };
listen-on-v6 port 53 { any;  };
allow-query     { querynets; };
recursive-clients 500;  //限制遞迴查詢數
```

還有更安全的...

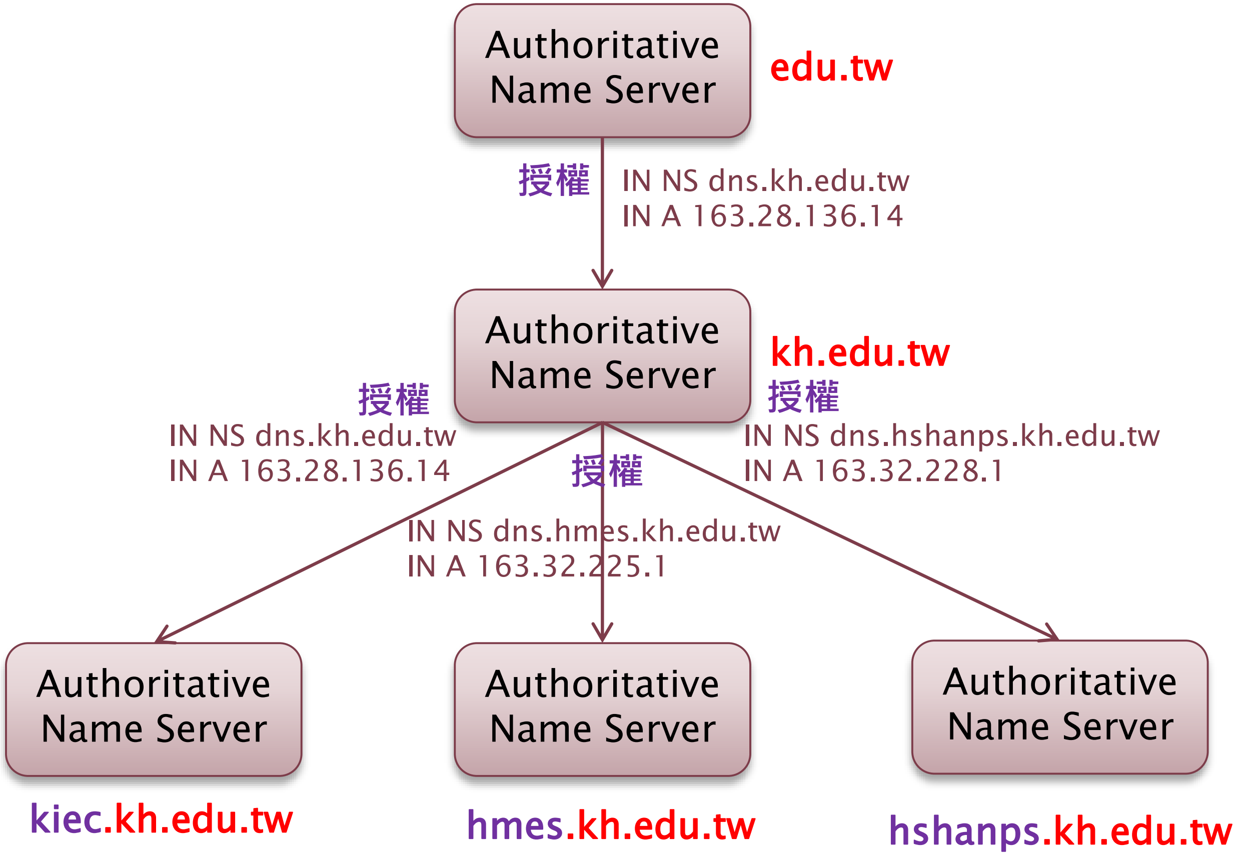
- 限制Recursive和Iterative的查詢來源
- DNSSEC
- 本機防火牆(firewalld)
  - rich-rule
- DNS各項log設定
- query log分析與設定
- CentOS 7.x自動化更新

服務型態與設定

DNS查詢服務型態

- 權威(authoritative)查詢服務
  - 被上層NS管理單位授權管轄特定領域名稱(DomainName)
  - 僅回應主機所轄之領域名稱查詢
  - Master/Slave Name Server可提供服務
- 遞迴(recursive)查詢服務
  - 代為查詢並回應完整之領域名稱查詢
  - Cache Name Server可提供服務

DomainName授權與服務型態


Authoritative Name Server
edu.tw
授權
IN NS dns.kh.edu.tw
IN A 163.28.136.14
Authoritative Name Server
kh.edu.tw
授權
IN NS dns.kh.edu.tw
IN A 163.28.136.14
授權
IN NS dns.hmes.kh.edu.tw
IN A 163.32.225.1
授權
IN NS dns.hshanps.kh.edu.tw
IN A 163.32.228.1
Authoritative Name Server
kiec.kh.edu.tw
Authoritative Name Server
hmes.kh.edu.tw
Authoritative Name Server
hshanps.kh.edu.tw

DNS主機服務型態

- 主要名稱服務:
  - Primary Name Server
  - Master Name Server
- 次要名稱服務:
  - Secondary Name Server
  - Slave Name Server
- 快取名稱服務:
  - Caching Name Server
- 協同架構
  - Primary/Secondary/Cache混用架構

主要名稱服務

- Master Name Server
- 某個領域(DomainName)下被**主要授權**並**控制**所有名稱記錄的主控制伺服器
- 管轄著所有該領域的記錄資料
- 只有Master Name Server可以修改

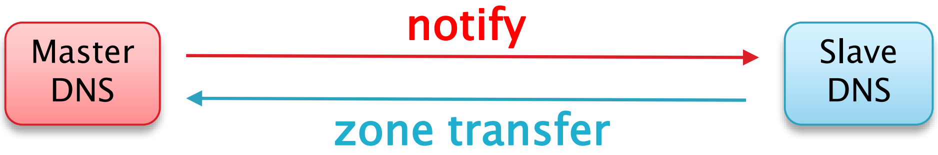
次要名稱服務

- Slave Name Server
- 同步並複製Master上管轄領域之所有名稱紀錄
- 分擔Master Name Server查詢工作

快取名稱服務

- Cache Name Server
- 未被授權或指定管理某個domain的DNS
- 管理的電腦數量太多
- 可執行遞回查詢並存儲結果，供所轄電腦下次查詢所有(cache,快取)
- 可有效降低對外DNS查詢之流量，減輕網路負擔

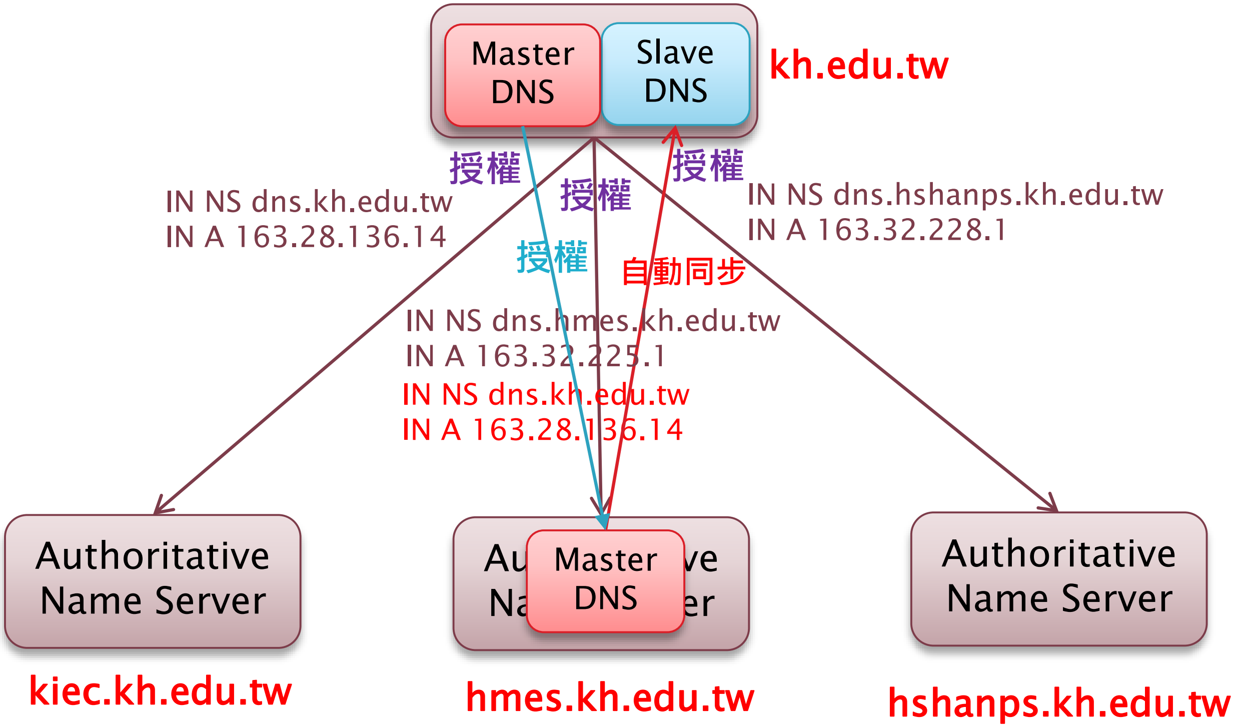
Master與Slave同步機制



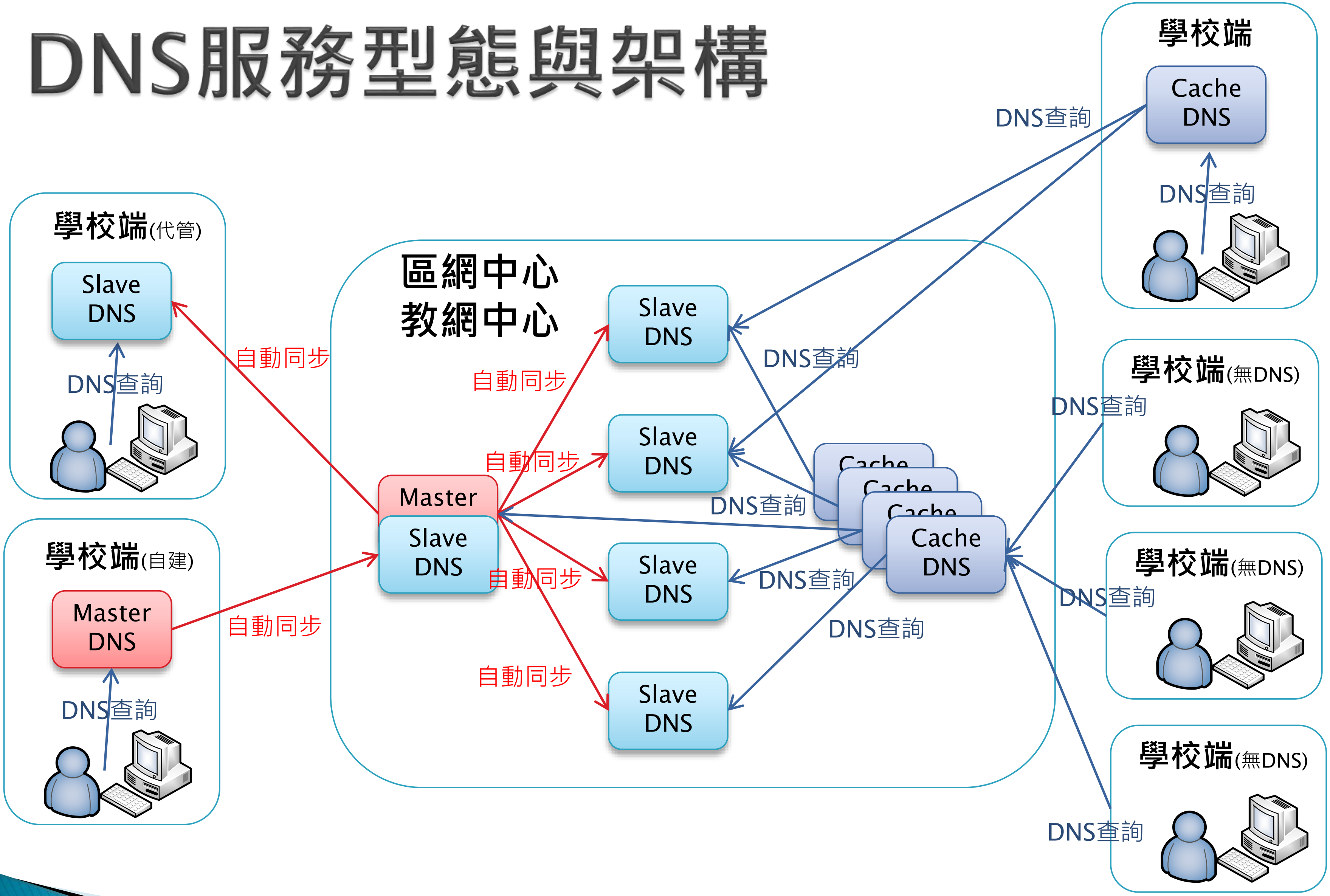
1.增刪/修改RR紀錄
2.修改serial序號
3.重啟DNS服務 or
重載DNS設定檔

1.收到notify通知
2.檢查zone的serial序號
3.序號變大→更新zone檔
4.達Retry時間,自動檢查
是否有新zone檔

DomainName授權與服務型態



DNS服務型態與架構


學校端
Cache DNS
DNS查詢
DNS查詢
學校端(代管)
Slave DNS
DNS查詢
自動同步
區網中心
教網中心
Slave DNS
自動同步
DNS查詢
Slave DNS
自動同步
Master
Slave DNS
DNS查詢
Cache
Cache
Cache
Cache DNS
學校端(無DNS)
DNS查詢
學校端(自建)
Master DNS
自動同步
DNS查詢
自動同步
Slave DNS
DNS查詢
學校端(無DNS)
DNS查詢
DNS查詢
自動同步
Slave DNS
學校端(無DNS)
DNS查詢

bind服務簡介

- DNS服務主流軟體
- OpneSource軟體
  - Unix like平台(Linux、BSD…)
  - Windows平台
- 最新版次
  - 9.12.2-P2
- CentOS 7.x 使用版次
  - 9.9.4-61.el7_5.1
- 參考文件:
  - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/networking_guide/ch-dns_servers

CentOS 7.x bind架構

- 檔案架構:

```
/etc/named.conf                    //主設定檔
/etc/named.iscdlv.key              //dnssec root金鑰
/etc/named.rfc1912.zones           //指向自己的zone設定描述
/etc/named.root.key                //dns root的dnssec金鑰
/etc/rndc.key                      //系統自動啟始的rndc金鑰
/var/named/named.ca    //dns 13個 root IPv4/IPv6位址
/var/named/named.empty             //zone設定檔
/var/named/named.localhost         //zone設定檔
/var/named/named.loopback          //zone設定檔
/run/named/session.key             //執行過程中產生的金鑰
/var/named/data/named.run          //預設log紀錄檔
/var/named/dynamic/managed-keys.bind.jnl
/var/named/dynamic/managed-keys.bind
```

CentOS 7.x bind架構

- 資料夾架構:

  /var/named/

  - 主要及master zone file放置區, named無法寫入

  /var/named/slaves/

  - Slave zone file寫入區, named可以寫入

  /var/named/dynamic

  - DDNS及DNSSEC key寫入區, named可以寫入

  /var/named/data/

  - named狀態及debug紀錄寫入區, named可以寫入

named.conf 內容架構

- acl：定義各IP或網段可視化名稱

```
acl [acl名稱] {
        localhost;                //指向loopback(127.0.0.1;::1)
        localnets;                //指向loopback網段
        10.0.2.0/24;              //IPv4網段
        2001:288:8439:2::/64      //IPv6網段
};
```

- include: 插入其他的設定檔案(通常會放在檔尾)

```
include “path/file-name”;
```

named.conf 內容架構

- options: 定義全域範圍的參數

```
options {
        listen-on port 53 { 127.0.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        allow-query     { localhost; };

        recursion yes;

        dnssec-enable yes;
        dnssec-validation yes;

        /* Path to ISC DLV key */
        bindkeys-file "/etc/named.iscdlv.key";

        managed-keys-directory "/var/named/dynamic";

        pid-file "/run/named/named.pid";
        session-keyfile "/run/named/session.key";
};
```

named.conf 內容架構

- logging: 定義log出輸的類別、型態及檔案大小...等

```
logging {
        channel default_debug {
                file "data/named.run";
                severity dynamic;
        };
};
```

named.conf 內容架構

- view: 讓DNS針對不同來源的查詢做不同的回覆

```
view "external" {
        match-clients { any; };                   //對應任何網路
        zone "test.cxm" IN {
                type master;
                file "master/test.cxm";
        };
};

view "internal" {
        match-clients { 192.168.0/24; }; //對應虛擬網段
        zone "test.cxm" IN {
                type master;
                file "master/test.cxm-internal";
        };
};
```

named.conf 內容架構

- zone: 定義正反解表

Master DNS 設定	Slave DNS 設定

zone "example.com" IN {
type master;
file “master/example.com.zone";
allow-transfer { 192.168.0.2; };
also-notify { 192.168.0.2; };
};
	zone "example.com" {
	type slave;
	masterfile-format text;
	file "slaves/example.com.zone";
	masters { 192.168.0.1; };
	};

zone "225.32.163.in-addr.arpa"{
type master;
file "master/named.hmes.arpa";
allow-transfer { 192.168.0.2; };
also-notify { 192.168.0.2; };
};
zone "f.9.2.8.8.8.2.0.1.0.0.2.ip6.arpa" {
type master;
file "master/named.hmesip6.arpa";
allow-transfer { 192.168.0.2; };
also-notify { 192.168.0.2; };
};
	zone "225.32.163.in-addr.arpa"{
	type slave;
	masterfile-format text;
	file "slaves/named.hmes.arpa";
	masters{ 163.32.225.1; };
	};
	zone "f.9.2.8.8.8.2.0.1.0.0.2.ip6.arpa" {
	type slave;
	masterfile-format text;
	file "slaves/named.hmesip6.arpa";
	masters{ 163.32.225.1; };
	};

zone file 正解表

```
$TTL        86400
@           IN          SOA         [domain].edu.tw.        root. [domain].edu.tw. (
                                    2010101201 ; serial
                                    1H ; refresh
                                    15 ; retry
                                    14D ; expire
                                    12H ; Minimum
                                    )

@           IN          MX          5           mail.[domain].edu.tw.
@           IN          NS          [domain].edu.tw.
@           IN          NS          dns.[domain].edu.tw.
@           IN          A           163.32.xxx.1
dns         IN          CNAME       [domain].edu.tw.
proxy       IN          A           163.32.xxx.2
mail        IN          A           163.32.xxx.3
            IN          AAAA        2001:288:82xx:1::3
            IN          MX          0           mail.[domain].edu.tw.
www         IN          A           163.32.xxx.4
ftp         IN          CNAME       www
vlmcs._tcp  IN          SRV         0 0 1688    kms.[domain].edu.tw.
```

zone file IPv4反解表

```
$TTL        86400
@           IN          SOA         [domain]edu.tw.      root. [domain].edu.tw. (
                                    2001101201 ; serial
                                    1H ; refresh
                                    15 ; retry
                                    14D ; expire
                                    12H ; Minimum
                                    )

@           IN          NS          [domain].edu.tw.
@           IN          NS          dns.[domain].edu.tw.
1           IN          PTR         [domain].edu.tw.
2           IN          PTR         proxy.[domain].edu.tw.
3           IN          PTR         mail.[domain].edu.tw.
4           IN          PTR         www.[domain].edu.tw.
; 使用變數作大範圍反解
$GENERATE      100-150  $      PTR     pc$.[domain].edu.tw.
```

zone file IPv6反解表

```
; IPv6 reverse lookup zone for 2001:288:82xx::/48
$TTL            86400
@               IN              SOA             dns.[domain].edu.tw.            root.dns.[domain].edu.tw. (
                                                2010102101 ; serial
                                                28800 ; refresh
                                                7200 ; retry
                                                129600 ; expire
                                                86400 ; default_ttl
                                                )
@               IN              NS              dns.[domain].edu.tw.
; for 2001:288:82xx::/48
$ORIGIN x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa.
0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0         IN              PTR             [domain].edu.tw.
; for 2001:288:82xx:1::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa.
2.0.0.0         IN              PTR             dns1.[domain].edu.tw.
5.0.0.0         IN              PTR             ftp.[domain].edu.tw.
0.1.0.0         IN              PTR             dns2.[domain].edu.tw.
4.1.0.0         IN              PTR             dns.[domain].edu.tw.
; for 2001:288:82xx:3::/64
$ORIGIN 0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.x.x.2.8.8.8.2.0.1.0.0.2.ip6.arpa.
9.0.2.0         IN              PTR             pbx.[domain].edu.tw.
```

設定檔檢查工具

- named-checkconf
- named-checkzone
    - named-checkzone [zone name] [zone file name]

zone file 增/刪/修 程序&注意事項

- 開啟zone file檔案
- 增/刪/修 RR記錄
- 修改serial序號(要比編修前大)
- 檢查編修後的zone file檔是否正確?
  - named-checkzone [zonename] [zonefile]
- 重啟dns服務 or 重新載入config
  - rndc reload
  - rndc reconfig
  - systecmtl restart named-chroot

安全與維運

- DNS對外服務
- Recursive和Iterative與安全
- 多台DNS主機維運
- DNSSEC

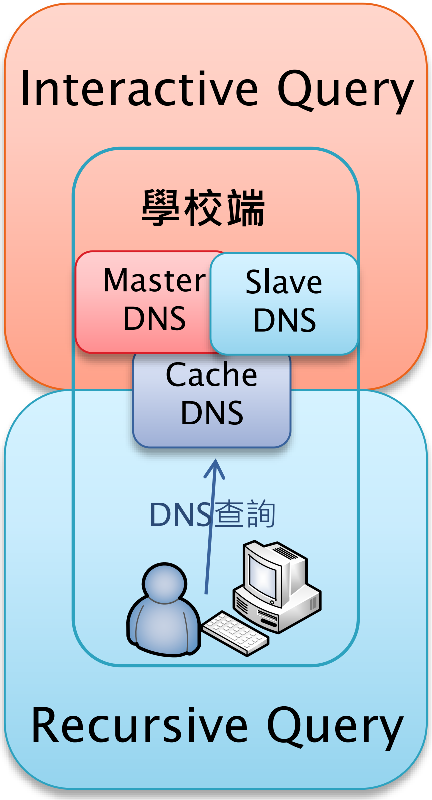
開放DNS主機對外提供服務

- 修改DNS設定檔(named.conf)
  - listen-on port 53 { any; };
  - listen-on-v6 port 53 { any; };
  - allow-query   { any; };
- 設定防火牆
  - firewall-cmd --add-service=dns
  - firewall-cmd --list-all
  - firewall-cmd --add-service=dns **--permanent**
  - firewall-cmd --reload

Recursive和Iterative與安全

```
view "external" {
    match-clients { any; };
    allow-query     { any; };
    recursion no;
    allow-query-cache { none; };
    allow-recursion { none; };
::::::
};
```

```
view "internal" {
    match-clients { trusted; };
    allow-query     { any; };
    recursion yes;
    allow-query-cache { trusted; };
    allow-recursion { trusted; };
::::::
};
```



Interactive Query

學校端

Master DNS

Slave DNS

Cache DNS

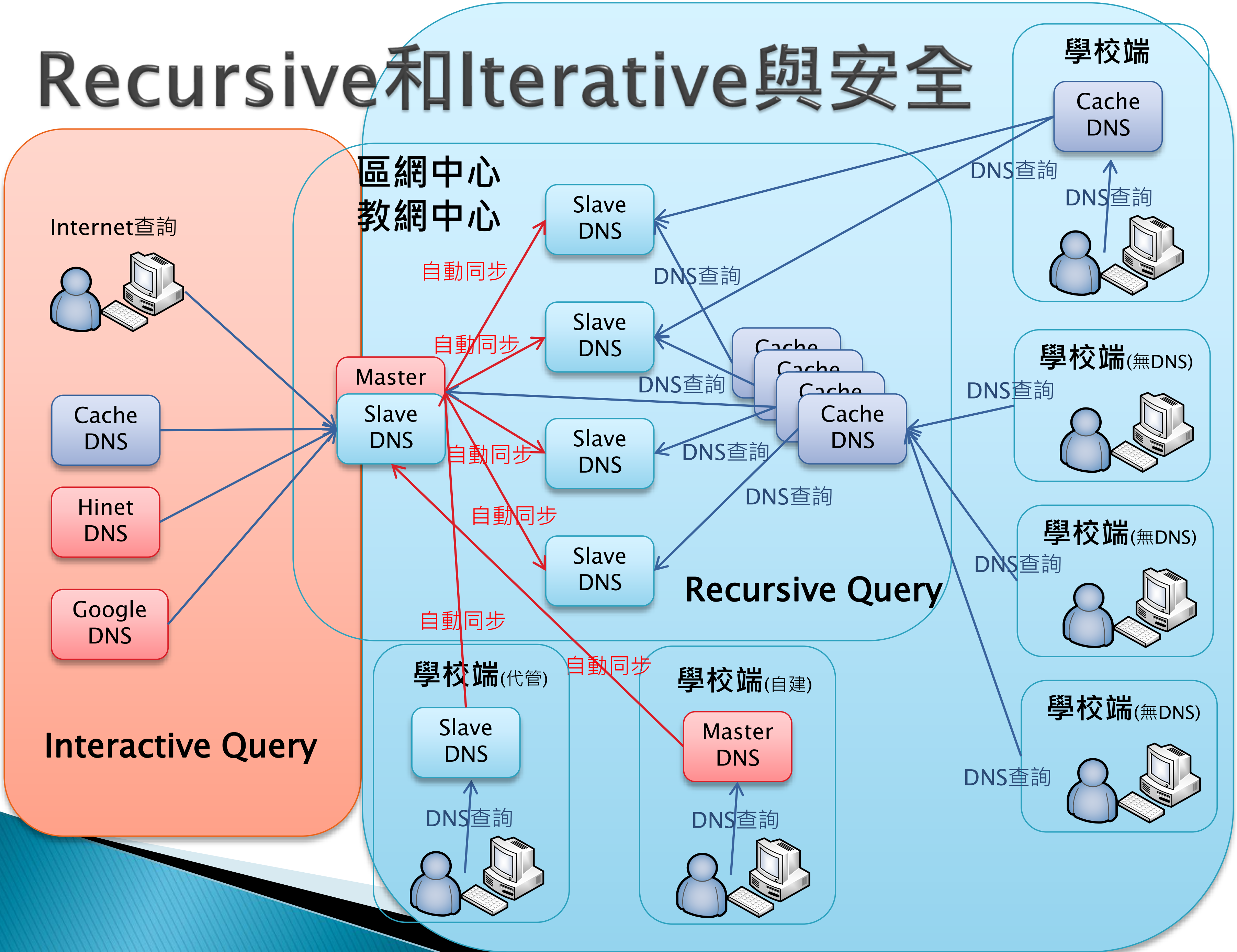
DNS查詢

Recursive Query

```
options {
    allow-query     { any; };
    recursion no;
    allow-query-cache { none; };
    allow-recursion { none; };
:::::
};
```

```
options {
    allow-query     { any; };
    recursion yes;
    allow-query-cache { trusted; };
    allow-recursion { trusted; };
::::::
};
```

Recursive和Iterative與安全



Recursive和Iterative與安全

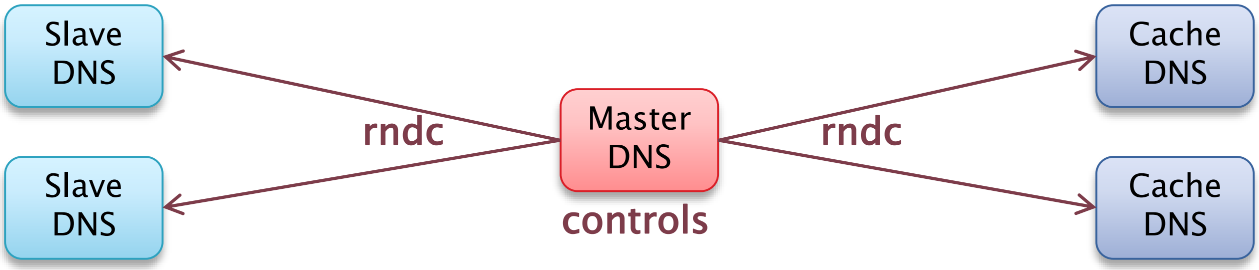
Iterative查詢服務	Recursive查詢服務
權威(Authoritative)主機必備服務	提供區域內用戶快速查詢服務

```
options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { any; };
    directory       "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
    recursion no;
    allow-query-cache { none; };
```

```
acl trusted {
    localnets;
    163.32.225.0/24;
    192.168.99.0/24;
    192.168.100.0/23;
    2001:288:829f::/48;
};

options {
    listen-on port 53 { any; };
    listen-on-v6 port 53 { any; };
    directory       "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    allow-query     { any; };
    recursion yes;
    allow-query-cache { trusted; };
    allow-recursion { trusted; };
```

多台DNS主機維運--rndc



```
key "rndc-key" {
        algorithm hmac-md5;
        secret "yarrO56F05jOnfFEleCjHl5T4yTMdKq3LgweF5wdqWQ1PsJIoQ02xxp9fNT8";
};

controls {
        inet * port 953
                allow { 127.0.0.1; } keys { "rndc-key"; };
        inet :: port 953
                allow { ::1; } keys { "rndc-key"; };
};
```

```
key "rndc-key" {
        algorithm hmac-md5;
        secret "yarrO56F05jOnfFEleCjHl5T4yTMdKq3LgweF5wdqWQ1PsJIoQ02xxp9fNT8";
};

controls {
        inet * port 953
                allow { 127.0.0.1; 163.28.136.14; } keys { "rndc-key"; };
        inet :: port 953
                allow { ::1; 2001:288:8201:1::14; } keys { "rndc-key"; };
};
```

多台DNS主機維運--rndc

- 產生rndc金鑰
- 新增 rndc.conf
- 修改 rndc.conf 檔案權限
  - chown named:named rndc.conf
  - restorecon -R /var/named/chroot/etc
- 修改named.conf
  - 檔尾新增一行:
    include "/etc/rndc.conf"
- 重啟DNS服務
  - systemctl restart named-chroot
- 受控端記得新增防火牆rule

多台DNS主機維運--rndc

- rndc-confgen –A hmac-sha256

```
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-sha256;
        secret "vlAFORsYw9CdDgyVOin9n31TuYsYRJWlGzQjzuYcuZA=";
};

options {
        default-key "rndc-key";
        default-server 127.0.0.1;
        default-port 953;
};
# End of rndc.conf

# Use with the following in named.conf, adjusting the allow list as needed:
# key "rndc-key" {
#       algorithm hmac-sha256;
#       secret "vlAFORsYw9CdDgyVOin9n31TuYsYRJWlGzQjzuYcuZA=";
# };
#
# controls {
#       inet 127.0.0.1 port 953
#               allow { 127.0.0.1; } keys { "rndc-key"; };
# };
# End of named.conf
```

多台DNS主機維運--rndc

- 受控端防火牆rule調整
  - 新增FW Service定義檔(/etc/firewalld/services/rndc.xml)

```
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>DNS</short>
  <description>rndc(remote name daemon control)可使系統管理者利用rndc command遠端
或本端(localhost)控制管理Bind，並以加密方式來傳送資料，以防止其他非授權使用者控制Bind.
Enable this option, if you plan to provide a rndc service (e.g. with bind).</description>
  <port protocol="tcp" port="953"/>
  <port protocol="udp" port="953"/>
</service>
```

  - 修改定義檔檔案權限
    - chown root:root rndc.xml
    - restorecon –R /etc/firewalld/services
  - 重啟防火牆
    - systemctl restart firewalld
  - 新增防火牆規則
    - firewall-cmd --add-service=rndc
    - firewall-cmd --add-service=rndc --permanent

多台DNS主機維運--rndc

- 查詢本機服務狀態
  - rndc status
- 查詢受控端服務狀態
  - rndc –b [fqdn/ip] status

DNSSEC介紹

- http://dnssec.tanet.edu.tw/images/DNSSEC/DNSSEC_Authoritative_ServerSOP_v2.12.pdf
- DNSSEC=DNS RR+數位簽章 (HASH雜湊+非對稱金鑰)
- 新增4種 RR Type:
  - DNSKEY: public key 公開金鑰
  - RRSIG: 數位簽章 (hash + private key)
  - DS: 上下層的DNSKEY驗證用
  - NSEC: 回應負面消息=Non-existent domain (NXDOMAIN)
    NSEC3: 先把domain Hash後再排序，回應資料上下筆domain是不存在的

DNSSEC安裝與設定

- 修改named.conf中zone描述設定

```
zone "example.com." IN {
    type master;
    auto-dnssec maintain;
    update-policy local;
    allow-transfer { slaves_list };
    also-notify     { slaves_list };
    file "master/example.com.zone";
    key-directory "/etc/pki/dnssec-keys ";
};
```

DNSSEC安裝與設定

- 修改zone file(正解表)

```
$TTL    600
@    IN   SOA example.com. admin.example.com. (
           1        ; Serial
           3600     ; Refresh
 600       ; Retry
           86400    ; Expire
 600       ; Negative Cache TTL
           )
;
@    IN   NS ns.example.com.
@    IN   NSEC3PARAM 1 0 100 61
ns   IN   A 127.0.0.1
```

DNSSEC安裝與設定

- 初始化網域金鑰

```
dnssec-keygen
-a NSEC3RSASHA1  \
-b 2048 \
-f KSK \
-r /dev/urandom \
-K /var/named/chroot/etc/pki/dnssec-keys \
-P 20181001000000 \
-A 20181001000000 \
-I 20191101000000 \
-D 20191231000000 \
example.com.tw
```

DNSSEC安裝與設定

- 建立信任鏈
  - DS
    - dnssec-dsfromkey Khmes.kh.edu.tw.+007+21174

      ```
      hmes.kh.edu.tw. IN DS 21174 7 1
      4FD41F705AE31F5DE6D168F9280C4AC10B859D80
      hmes.kh.edu.tw. IN DS 21174 7 2
      14F097735D8D2AE249BD9C01445C388A82AA926A41F331CE
      440BA2968FE491CF
      ```
    - 交給上層DNS管理單位，滙入或寫入授權domain的zone file
    - 註冊並滙入DLV服務(https://dlv.isc.org)
  - 驗證信任鏈是否建立?
    - dig +dnssec -t soa example.com @8.8.8.8
    - 回應flag中存在ad即表示建置正確

DNSSEC維護注意事項

- zone RR增刪修改
  - nsupdate
  - 修改zone file
    - 凍結 zone file: rndc freeze
    - 修改 zone file
    - 簽署 zone file:
      dnssec-signzone -3 61 -H 100 -K /var/named/chroot/etc/pki/dnssec-keys -o example.com -S -u db.example.com
    - 修改已簽署 zone file 的 owner
    - 解凍 zone file 使其生效: rndc thaw

Q & A

感謝您的聆聽