DNS進階管理與除錯

鄭翔耀

jeffery@stepwise.com.tw

自我介紹

- 經歷: SI界8年
- 專長: 虛擬化、異地備援、網路系統整合與資安服務
- 服務客戶: 大專院校網路/系統維護、公家機關、私人企業

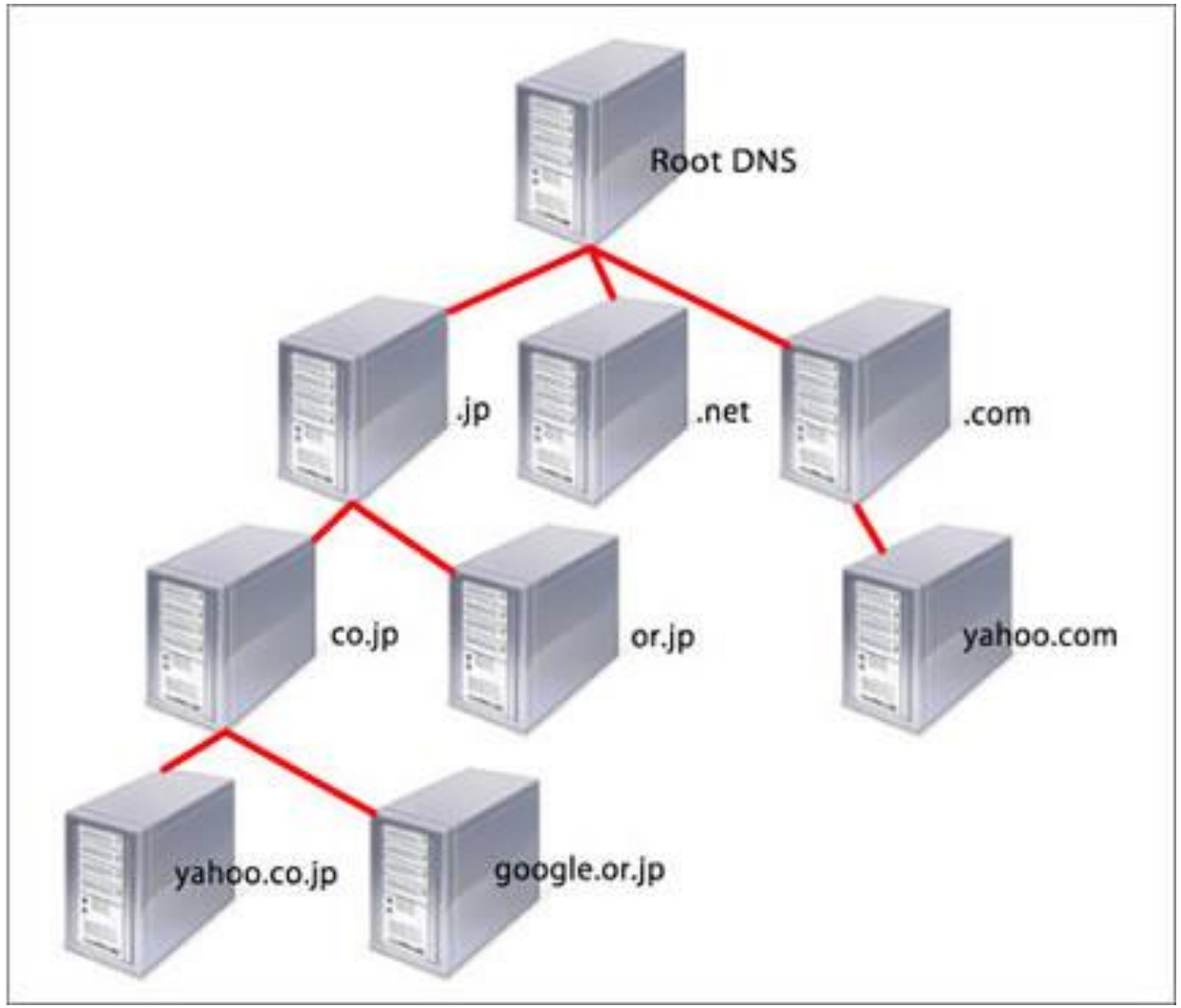
大綱

- DNS 安全性設定
- DNS 紀錄檔設定
- DNS 進階限制
- DNS 服務監控
- DNS 常見問題
- DNS 檢測步驟

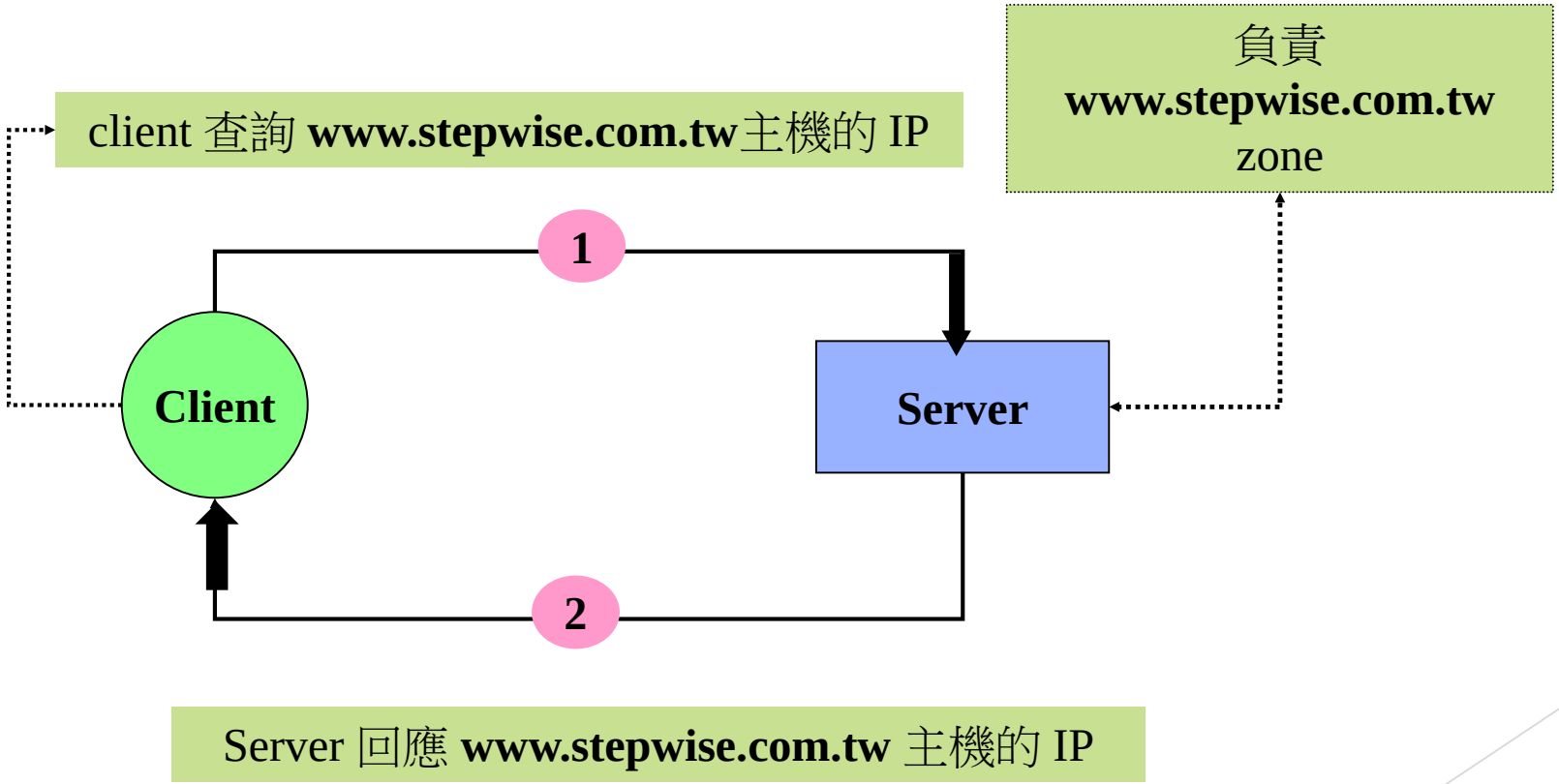
DNS樹狀階層結構

- **DNS** 特點
  - DNS 為分散式系統，每個區段由其所屬的組織機自行管理
  - DNS 資料庫結構為階層式，類似於樹狀結構
- 階層式架構
  - 依照組織與國家區分
    - 早期只有使用 “組織” 區分，後來才加上 “國家”
  - 組織與國家
    - 組織：**gov、edu、com、net、org、mil、int**
    - 國家：**tw 、jp、cn、it、uk、hk …..**

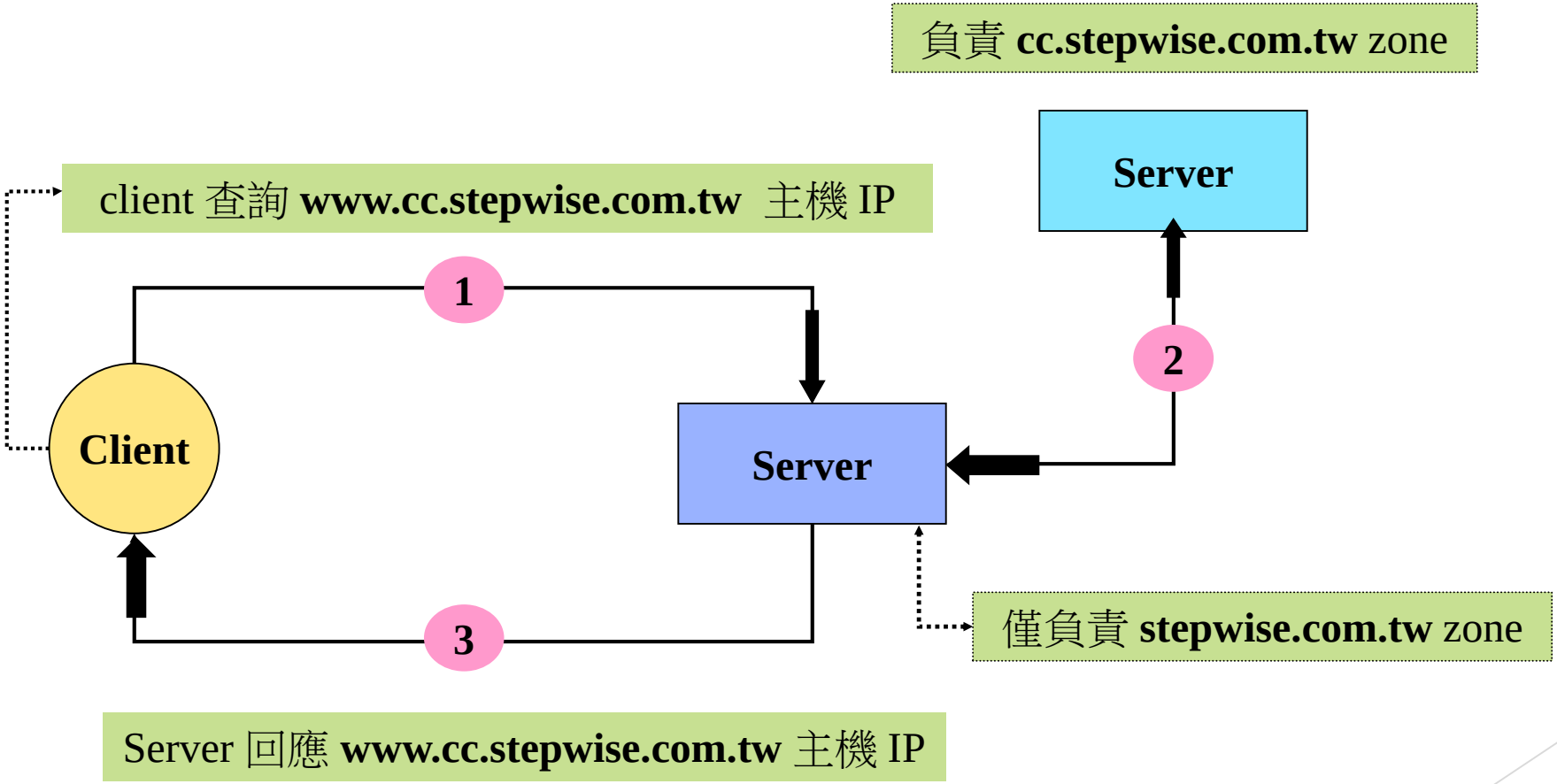
DNS樹狀階層結構


Root DNS
.jp
.net
.com
co.jp
or.jp
yahoo.com
yahoo.co.jp
google.or.jp

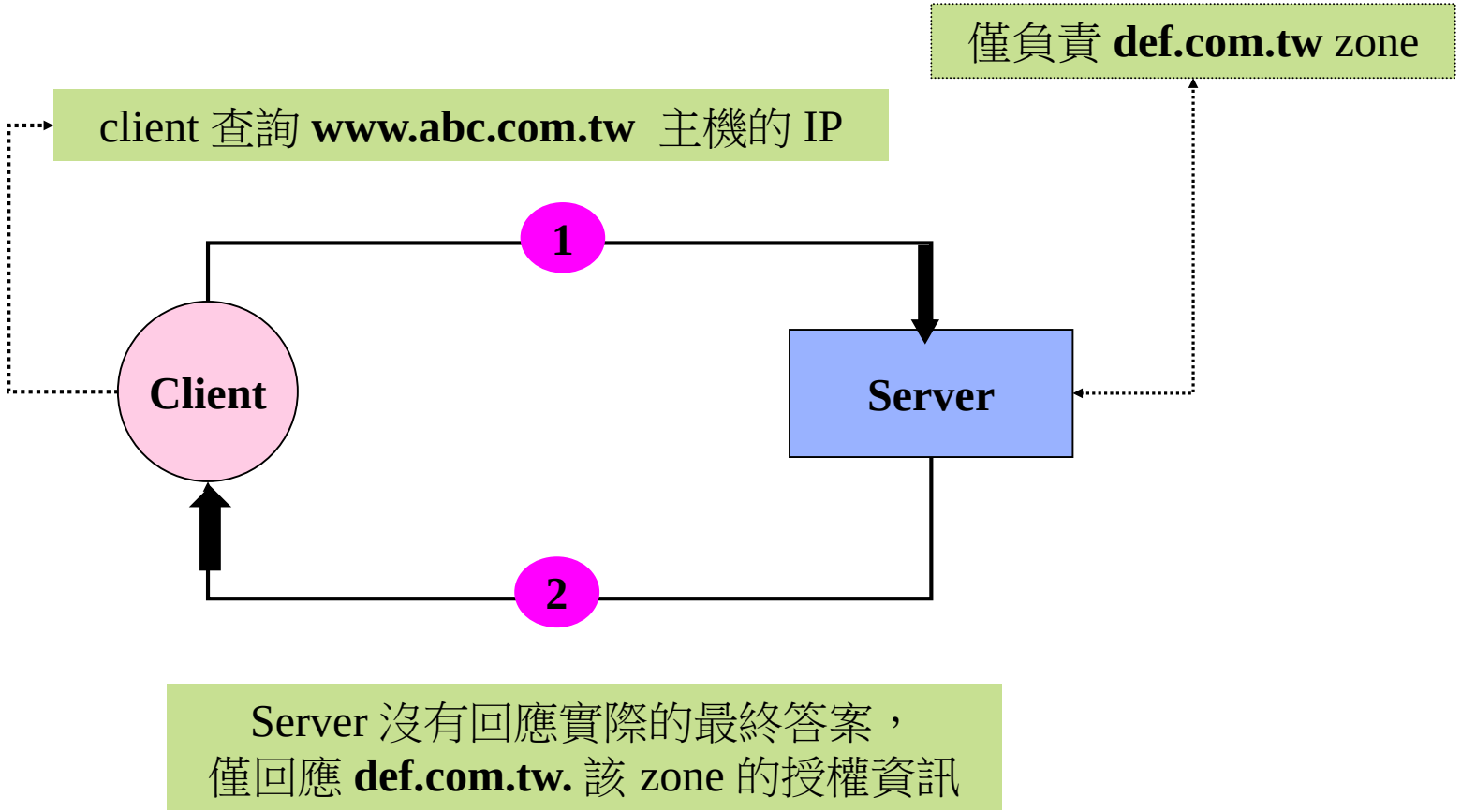
DNS查詢模式


負責
www.stepwise.com.tw
zone
client 查詢 www.stepwise.com.tw主機的 IP
1
Client
Server
2
Server 回應 www.stepwise.com.tw 主機的 IP

DNS查詢模式


負責 cc.stepwise.com.tw zone
Server
client 查詢 www.cc.stepwise.com.tw 主機 IP
1
2
Client
Server
3
僅負責 stepwise.com.tw zone
Server 回應 www.cc.stepwise.com.tw 主機 IP

DNS查詢模式



Server 沒有回應實際的最終答案，
僅回應 **def.com.tw.** 該 zone 的授權資訊

DNS Server種類

- **Matser DNS Server**
  - 提供完整的資訊服務，記錄保存著設定資料
- **Slave DNS Server**
  - 資料由 Master DNS 主機傳輸而來，不需要額外編輯相關資料
- **Cache Only DNS Server**
  - 向 root server 詢問，遞迴的方式逐漸查詢並紀錄相關資訊
- **Forwarding DNS Server**
  - 自己轄區無相關資訊時，指定將該查詢動作丟給某個主機，請對方代為查詢

DNS 安全性設定

- DNS 紀錄檔設定
- DNS 進階限制
- DNS 服務監控
- DNS 常見問題
- DNS 檢測步驟

DNS軟體

- 主要套件 rpm 套件
  - **bind-utils**
    - dns 相關用戶端程式工具 (nslookup, host, dig ..)
  - **bind**
    - 主要的 dns server 服務程式
  - **bind-chroot**
    - 提供 bind 於 chroot 環境所需的必要檔案
  - **caching-nameserver**
    - caching only dns 服務必要檔案

Chroot環境配置

- 說明
  - 提供讓 named 程式在 chroot 運作執行，提供更安全運作環境
- 檔案
  - **/etc/sysconfig/named**
    - 提供給 /etc/init.d/named script 執行讀入的配置檔案
    - **CHROOT_DIR** 設定決定是否使用 chroot
      - **CHROOT_DIR=/var/named/chroot**
    - 實際式執行
      - **/usr/sbin/named -t /var/named/chroot**

Chroot環境配置

- 依據 **/etc/init.d/named** 寫法，先偵測是否有配置使用 **chroot** 環境
- 情況
  - 一般環境 (無使用 chroot 環境)
    - **/etc** - 主要組態檔案放置目錄
    - **/var/named/** - 正反解資料檔案放置目錄
  - 有使用 chroot 環境
    - **/var/named/chroot/etc/**
    - **/var/named/chroot/var/named**

    (原本的位置多加上 **/var/named/chroot/** 路徑)

DNS設定檔

- **named.conf** 設定檔內容
  - **options { ..... ; ..... ; };**
    - 主要參數設定
  - **logging { ..... ; ..... ; };**
    - 紀錄檔參數設定
  - **view name { ..... ; ..... ; };**
    - 指定符合指定特定來源時使用組態設定
  - **zone name { ..... ; ..... ; };**
    - 宣告管理該 zone 區段，包含正反解配置等項目

DNS設定檔

- **options {}** 內容
  - **listen-on port 53 { ip-address ; .....};**
    - 聆聽的 ipv4 位址與 port
  - **listen-on-v6 port 53 { ip-address ; .....};**
    - 聆聽的 ipv6 位址與 port
  - **directory** “/var/named”;
    - 正反解資料檔案放置目錄

DNS設定檔

- **options {}** 內容
  - **query-source port 53;**
    - 指定查詢 ipv4 資訊時，指定 source port
  - **query-source-v6 port 53;**
    - 指定查詢 ipv6 資訊時，指定 source port
  - **allow-query { ip-address ; ...; };**
    - 允許可以查詢的 ip 位址清單

Zone轄區宣告

- **zone**
  - 說明為轄區指定資訊，表示所管轄的網域區段
  - 格式組成
    - **zone** “*ZONENAME*" in {
      - **type** *TYPE*;
      - **file** “*FILENAME*";
    - };
  - 格式說明
    - 整個敘述使用 { } 包起來，用；分號結束
    - zone 區段內的每個的敘述，最後也使用；分號結束

Zone轄區宣告

- **zone**
  - 組成項目
    - **ZONENAME**
      - 正解項目，使用　“網域名稱”
      - 反解項目，使用　“ip + **.in-addr.arpa**“ 為結尾
    - **type**
      - 指定 name server 的類型
      - 可以使用項目：**hint**、**master**、**slave** 與 **forward**
    - **file**
      - 指定該 zone 區段內管轄的資料檔案名稱

DNS正解設定

- 正解 **zone** 宣告
  - 宣告管轄指定的轄區
  - 設定項目
    - **zone “team01.com.tw“ {**
      - **type master;**
      - **file “master/team01.com.tw.zone";**
      - **allow-query { any; };**
    - **};**
  - 設定注意項目
    - **zone** 的名稱後面不帶有 **“.”** 符號

DNS正解檔設定

```
$TTL    1D
@    IN    SOA dns.teamXX.com.tw.    root.dns.teamXX.com.tw.    (
                    2015071200 ; serial
                    10H        ; refresh
                    2H         ; retry
                    4W         ; expire
                    1D    )    ; TTL
     IN    NS    dns.teamXX.com.tw.
dns  IN    A     10.8.1.1XX
xp   IN    A     10.8.1.XX
```

SOA 區段資料

NS 紀錄

A 正解紀錄

DNS正解檔設定

- 其他正解 **zone** 宣告
  - **CNAME** (別名) 設定
    - **test1 IN CNAME www**
    - **test2 IN CNAME www.seed.net.tw.**
  - 多重 A 紀錄設定 (**Round-Robin**)
    - **test3 IN A 192.168.1.1**
    - **IN A 192.168.1.2**
    - **IN A 192.168.1.3**

DNS正解檔設定

- 其他正解 **zone** 宣告
  - **IPv6 A** 紀錄
    - **test4 IN　AAAA　::1**

DNS反解設定

- 反解 **zone** 宣告
  - 宣告管轄指定的轄區
  - 設定項目
    - **zone “1.8.10.in-addr.arpa" {**
      - **type master;**
      - **file “master/10.8.1.zone";**
      - **allow-query { any; };**
    - **};**
  - 設定注意項目
    - **IP** 網段寫法相反，**zone** 的名稱後面固定帶有 **“in-addr.arpa”**

DNS正解檔設定

```
$TTL    1D
@    IN    SOA dns.teamXX.com.tw.    root.dns.teamXX.com.tw.    (
                2015071200 ; serial
                10H        ; refresh
                2H         ; retry
                4W         ; expire
                1D    )    ; TTL
     IN    NS    dns.teamXX.com.tw.
1    IN    PTR xp.teamXX.com.tw.
1XX IN    PTR dns.teamXX.com.tw.
```

SOA 區段資料

NS 紀錄

PTR 反解紀錄

DNS Zone資料項目

- **@ IN SOA dns.teamXX.com.tw. root.dns.teamXX.com.tw. (…)**
  - **(…)** 放置項目
    - **serial** - slave 用來判斷 master 主機是否異動的依據
    - **refresh** - slave 每隔 refresh 時間連到 master 主機問 serial
    - **retry** - slave 當 refresh 時間失敗則每隔 retry 再次訊問
    - **expire** - slave 在 master 於 expire 連線失敗就作廢資料
    - **ttl** - 提供給外面 dns 查詢資料後快取時間

DNS SOA 資料項目

- **SOA** 內 5 組數值項目

Serial ; Refresh ; Retry ; Expire ; TTL

  - **Serial**
    - 為 32bit 組成的 10 進位數值
    - 一般習慣使用 **西元+月份+日+2位數字** 組成的序號
    - 提供給 Slave 主機判斷 Master 主機資料是否有異動過的依據
      - slave 主機是否更新的判斷
        - **master dns zone serial > slave dns zone serial**
    - 若有異動過 master 主機資料，master 主機序號要增加

DNS SOA 資料項目

- **SOA** 內 5 組數值項目

Serial ; **Refresh** ; Retry ; Expire ; TTL

  - **Refresh**
    - 時間欄位，預設為秒數，可以搭配 D/W/H/M 等單位
    - Slave 主機每隔 Refresh 時間連線到 Master 主機詢問序號
    - 若是 Master 主機的序號大於 Slave 主機的序號，Slave 主機會連線到 Master 主機將 zone 資料抓回進行更新

DNS SOA 資料項目

- **SOA** 內 5 組數值項目

Serial ; Refresh ; **Retry** ; Expire ; TTL

  - **Retry**
    - 時間欄位，預設為秒數，可以搭配 D/W/H/M 等單位
    - 若是 Slave 主機每隔 Refresh 時間連線詢問失敗，後續會每隔 Retry 時間重新詢問
    - 若已經於 retry 時間後可以正常詢問到資料，後續會再依據 refresh 時間進行下次查詢比對 serial 資料是否異動

DNS SOA 資料項目

- **SOA** 內 5 組數值項目

  Serial ; Refresh ; Retry ; **Expire** ; TTL

  - **Expire**
    - 時間欄位，預設為秒數，可以搭配 D/W/H/M 等單位
    - 若是 Slave 主機已經在過了 Expire 時間後還是無法聯繫上 Master 主機進行序號詢問，後續就把該管轄的資訊作廢，不再提供該 zone 區段資料查詢

DNS SOA 資料項目

- **SOA** 內 5 組數值項目

  Serial ; Refresh ; Retry ; Expire ; **TTL**

  - **TTL (Time to Live)**
    - 時間欄位，預設為秒數，可以搭配 D/W/H/M 等單位
    - 資料存活時間，當外面 DNS 主機查詢該 zone 區掉資料時，回應該資料快取的有效期限
    - SOA 欄位差異
      - SOA 內的 **TTL** 欄位，回應查詢不存在資料有效期限
      - **$TTL** 項目設定，回應查詢存在網路資料的有效期限

DNS 允許遞迴查詢

root@ns01:/root

```
acl localsubnets { 127.0.0.1; 192.168.0.0/16; };

options {
        directory "/var/named";
        dump-file "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        listen-on port 53 { any; };
        allow-recursion { localsubnets; };
};
```

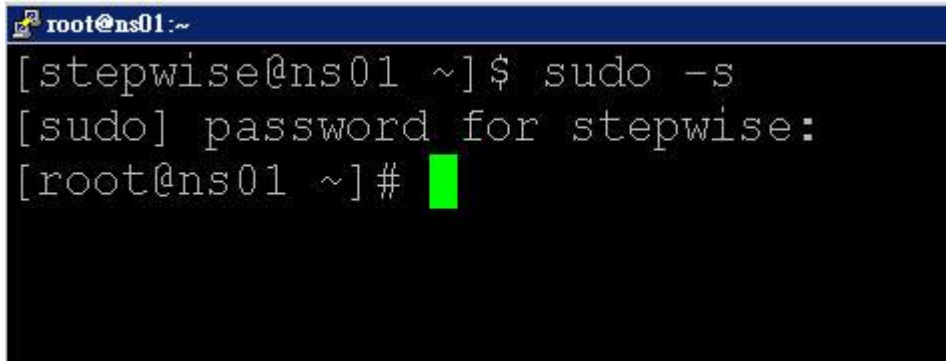
DNS Server存取安全設定

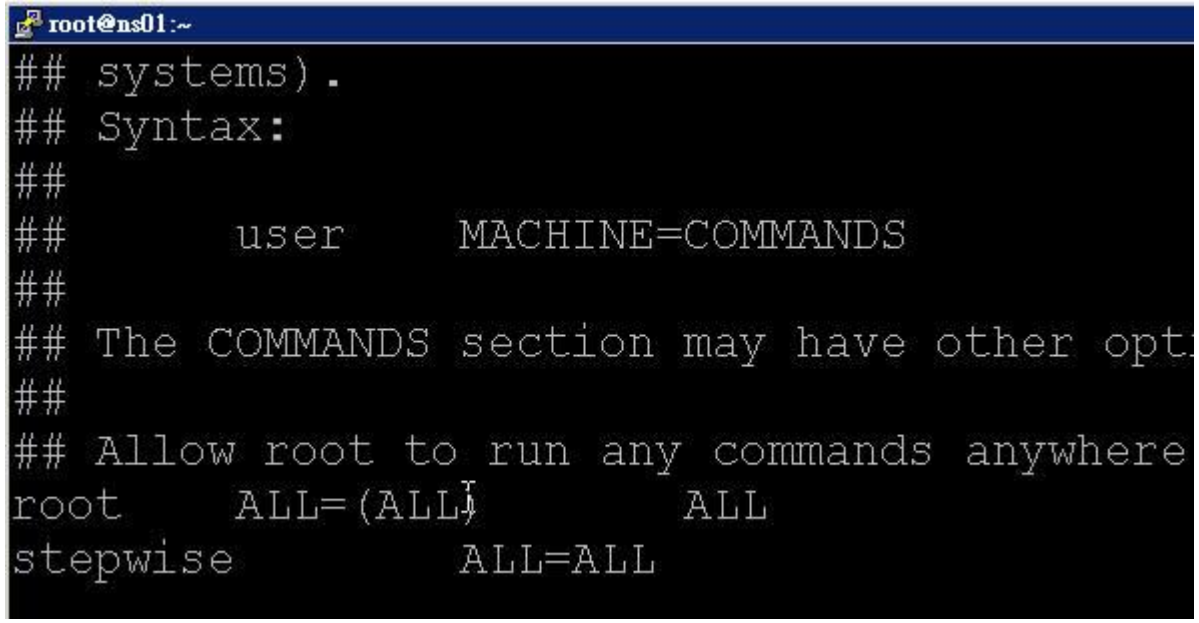
- ssh login 限制
  - 禁止root login

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
```

DNS Server存取安全設定

- 使用sudo轉換身分





DNS Server存取安全設定

- ssh login 限制
  - tcp wrapper

```
[root@ns01 root]# more /etc/hosts.allow
#
# hosts.allow   This file describes the names of the hosts which are
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
sshd : [redacted].0/255.255.255.0 : allow
sshd : [redacted].0/255.255.255.0 : allow
sshd : ALL : deny
```

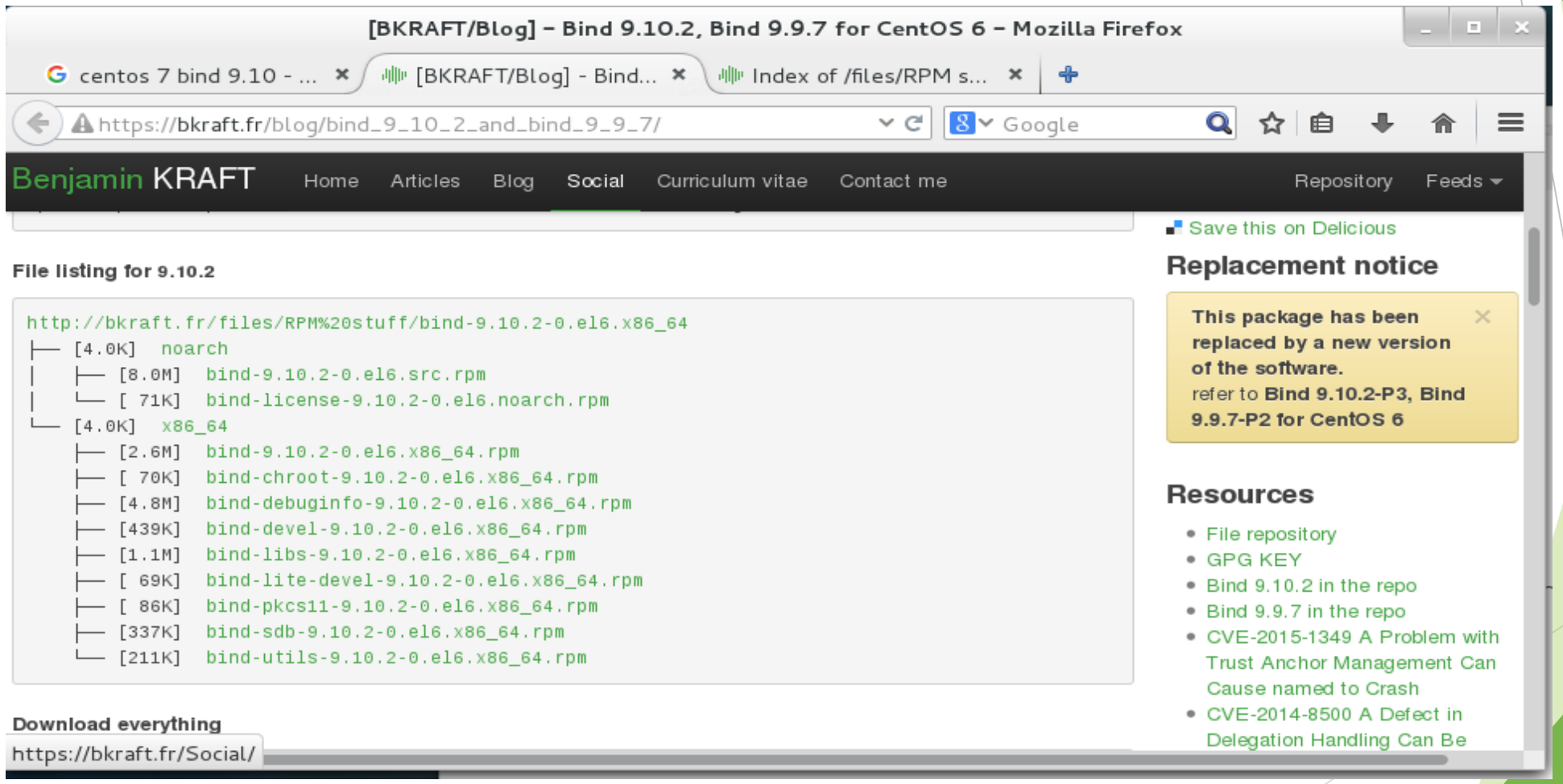
DNS Server防火牆設定

- Iptables –L –n
- Iptables –A OUTPUT –o eth0 –p udp –s $FW_IP –sport 1024:65535 –d any/0 –dport 53 –j ACCEPT
- Iptables –A INPUT –I eth0 –p udp –s any/0 –sport 53 –d $FW_IP –dport 1024:65535 –j ACCEPT
- Firewall-cmd --list-all
- Firewall-cmd –add-service=dns –permanent
- Firewall-cmd --reload
- 或是disable iptables，使用一般防火牆阻擋

BIND版本更新

- 建議升級至bind 9.10以上版本
  - http://tacert.tanet.edu.tw/prog/showrpt.php?id=3151

Wget下載rpm


[BKRAFT/Blog] – Bind 9.10.2, Bind 9.9.7 for CentOS 6 – Mozilla Firefox
centos 7 bind 9.10 - ...
[BKRAFT/Blog] - Bind...
Index of /files/RPM s...
https://bkraft.fr/blog/bind_9_10_2_and_bind_9_9_7/
Google
Benjamin KRAFT
Home
Articles
Blog
Social
Curriculum vitae
Contact me
Repository
Feeds
Save this on Delicious
File listing for 9.10.2
http://bkraft.fr/files/RPM%20stuff/bind-9.10.2-0.el6.x86_64
├── [4.0K] noarch
│ ├── [8.0M] bind-9.10.2-0.el6.src.rpm
│ └── [71K] bind-license-9.10.2-0.el6.noarch.rpm
└── [4.0K] x86_64
├── [2.6M] bind-9.10.2-0.el6.x86_64.rpm
├── [70K] bind-chroot-9.10.2-0.el6.x86_64.rpm
├── [4.8M] bind-debuginfo-9.10.2-0.el6.x86_64.rpm
├── [439K] bind-devel-9.10.2-0.el6.x86_64.rpm
├── [1.1M] bind-libs-9.10.2-0.el6.x86_64.rpm
├── [69K] bind-lite-devel-9.10.2-0.el6.x86_64.rpm
├── [86K] bind-pkcs11-9.10.2-0.el6.x86_64.rpm
├── [337K] bind-sdb-9.10.2-0.el6.x86_64.rpm
└── [211K] bind-utils-9.10.2-0.el6.x86_64.rpm
Download everything
https://bkraft.fr/Social/
Replacement notice
This package has been replaced by a new version of the software.
refer to Bind 9.10.2-P3, Bind 9.9.7-P2 for CentOS 6
Resources
File repository
GPG KEY
Bind 9.10.2 in the repo
Bind 9.9.7 in the repo
CVE-2015-1349 A Problem with Trust Anchor Management Can Cause named to Crash
CVE-2014-8500 A Defect in Delegation Handling Can Be

Slave dns記錄

```
[root@ns01 dns]# more dummy-block
$TTL    600
@       IN      SOA     ns01.[redacted]. root.rs2.[redacted]. (
                        2013103116
                        10800
                        3600
                        604800
                        86400 )
@               IN      NS      ns01.[redacted].
@               IN      NS      ns02.[redacted].
@               IN      A       127.0.0.1
*               IN      A       127.0.0.1
[root@ns01 dns]#
```

```
[root@ns02 dns]# more dummy-block
edutw憭? -(74%)
[root@ns02 dns]#
```

- DNS 安全性設定

DNS 紀錄檔設定

- DNS 進階限制
- DNS 服務監控
- DNS 常見問題
- DNS 檢測步驟

DNS Log設定說明

- queies.log　　紀錄client查詢此DNS Server的所有紀錄
- default.log　　紀錄BIND啟動及ZONE Transfer狀態
- security.log　　紀錄拒絕存取
- lamer　　紀錄在此DNS查不到的紀錄

DNS Log設定屬性

- size　　檔案大小
- severity　　截取log等級
  - Critical、Error、Warning、Notice、Info、Debug、Dynamic
- print-severity　　是否顯示log等級
- print-category　　是否顯示log等級
- print-time　　是否顯示log時間

```
channel security.log {
        file"/var/log/security.log" versions 3 size 100m;
        severity info;
        print-severity yes;
        print-time yes;
        print-category yes;
    };
```

DNS Log設定

```
logging {
    channel queries.log {
        file "/var/log/queries.log";
        severity dynamic;
        print-time yes;
    };
    category queries { queries.log; };

    channel security.log {
        file "/var/log/security.log";
        severity dynamic;
        print-time yes;
    };
    category security { security.log; };
```

DNS Log設定

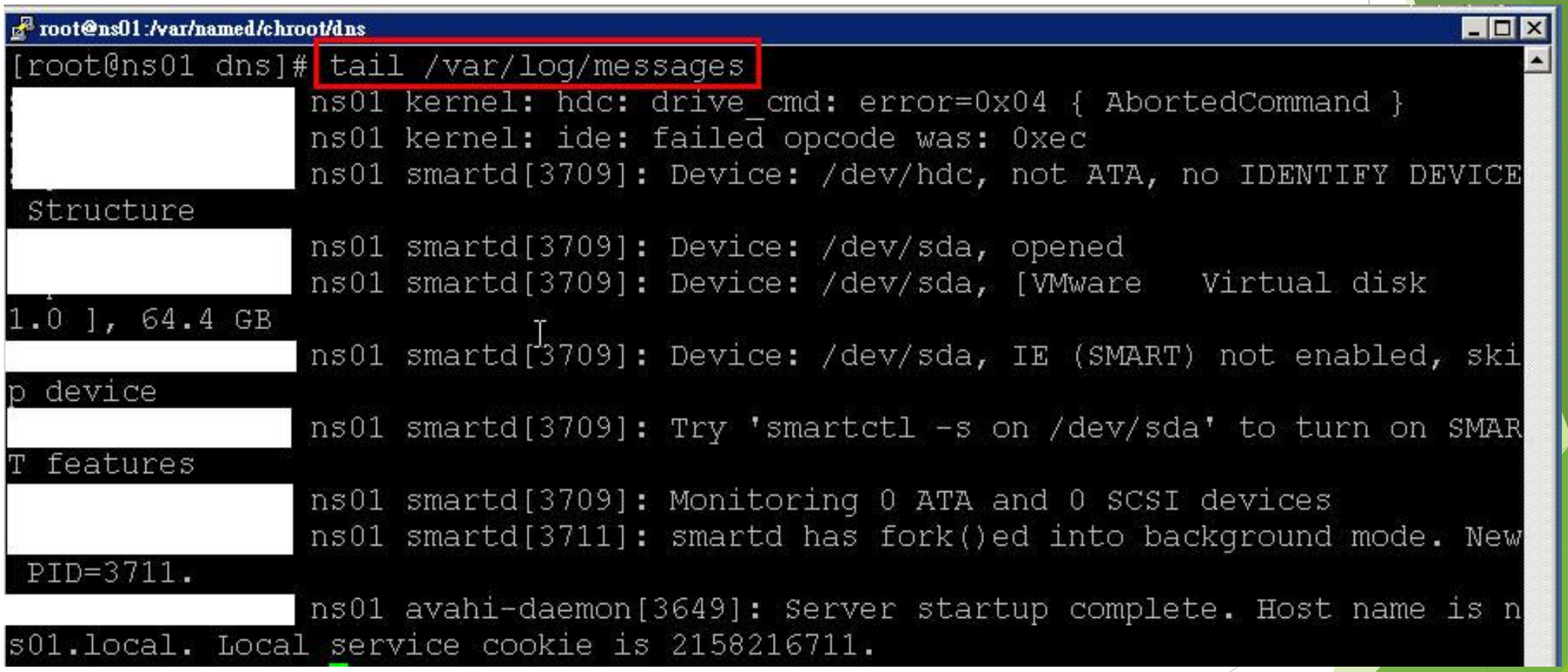
```
channel xfer-in.log {
    file "/var/log/xfer-in.log";
    severity dynamic;
    print-time yes;
};
category xfer-in { xfer-in.log; };

channel xfer-out.log {
    file "/var/log/xfer-out.log";
    severity dynamic;
    print-time yes;
};
category xfer-out { xfer-out.log; };

channel notify.log {
    file "/var/log/notify.log";
    severity dynamic;
    print-time yes;
};
category notify { notify.log; };
```

DNS Log

```
/var/named/chroot/var/log
[root@ns01 log]# ls -alh
total 6.7G
drwxrwx--- 2 named named 4.0K Sep 20 04:02 .
drwxr-x--- 6 root  named 4.0K Jul 29 07:08 ..
-rw-r--r-- 1 named named 6.9M Aug 20 10:10 client.log
-rw-r--r-- 1 named named    0 Mar 12  2013 config.log
-rw-r--r-- 1 named named  75M Sep 22 06:18 default.log
-rw-r--r-- 1 named named 4.0G Sep 22 06:19 lame-servers.log
-rw-r--r-- 1 named named 6.2K Sep  3 15:18 network.log
-rw-r--r-- 1 named named 425K Sep 22 06:08 notify.log
-rw-r--r-- 1 named named 446M Sep 22 06:21 queries.log
-rw-r--r-- 1 named named 665M Sep 20 04:02 queries.log.1
-rw-r--r-- 1 named named 401M Sep 13 04:02 queries.log.2
-rw-r--r-- 1 named named 533M Sep  6 04:02 queries.log.3
-rw-r--r-- 1 named named 595M Aug 30 04:02 queries.log.4
-rw-r--r-- 1 named named    0 Mar 12  2013 resolver.log
-rw-r--r-- 1 named named  14M Sep 22 06:21 security.log
-rw-r--r-- 1 named named  16M Sep 20 03:53 security.log.1
-rw-r--r-- 1 named named  19M Sep 13 03:49 security.log.2
-rw-r--r-- 1 named named  23M Sep  6 04:00 security.log.3
-rw-r--r-- 1 named named  21M Aug 30 03:59 security.log.4
-rw-r--r-- 1 named named    0 Mar 12  2013 xfer-in.log
-rw-r--r-- 1 named named 344K Sep 22 06:10 xfer-out.log
```

系統Log

- 可從/var/log/messages看系統log是否有異常



- DNS 安全性設定
- DNS 紀錄檔設定

DNS 進階限制

- DNS 服務監控
- DNS 常見問題
- DNS 檢測步驟

DNS 進階限制功能

- **DNS allow-query**
  - 說明
    - 提供限制查詢來源
  - 預設設定
    - 預設為任何來源皆可以連線查詢
  - 使用語法
    - **allow-query { address_match_list; };**
  - 使用範圍
    - 於 **options** 與 **zone** 區段內

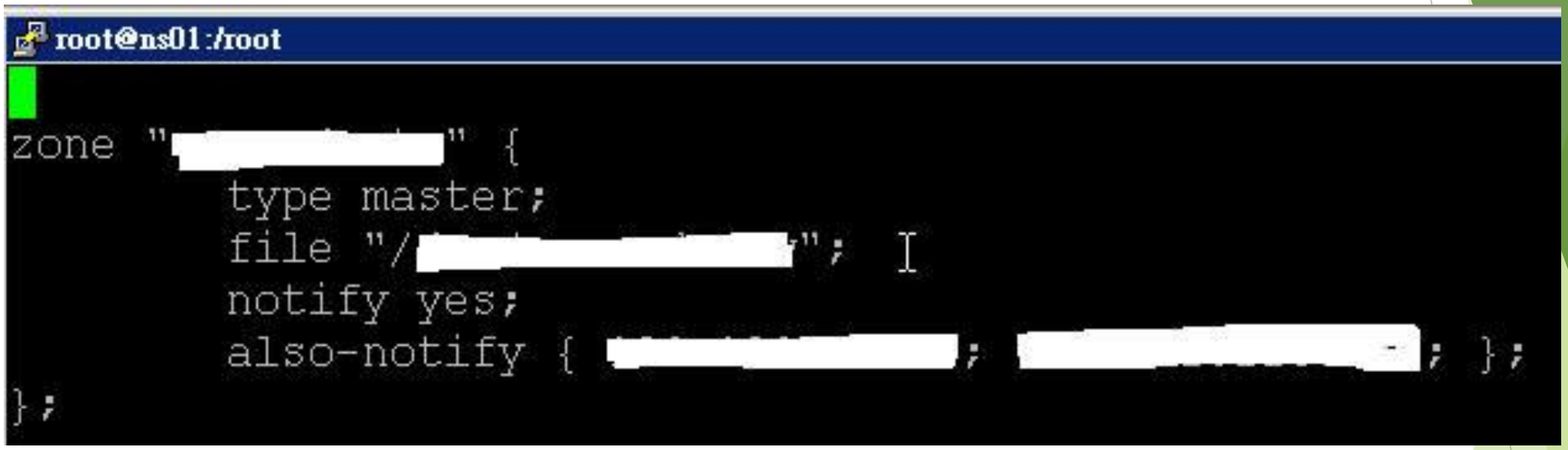
DNS 進階限制功能

- **DNS Notify**
  - 說明
    - 轄區變更通知 (Master DNS Server 資料變更後通知 Slave Server)
  - 使用語法
    - **notify yes | no;** - 是否開啟該功能
    - ***also-notify { addresslist; };*** - 一併對指定主機進行通知
  - 使用範圍
    - 於 **options** 與 **zone** 區段內

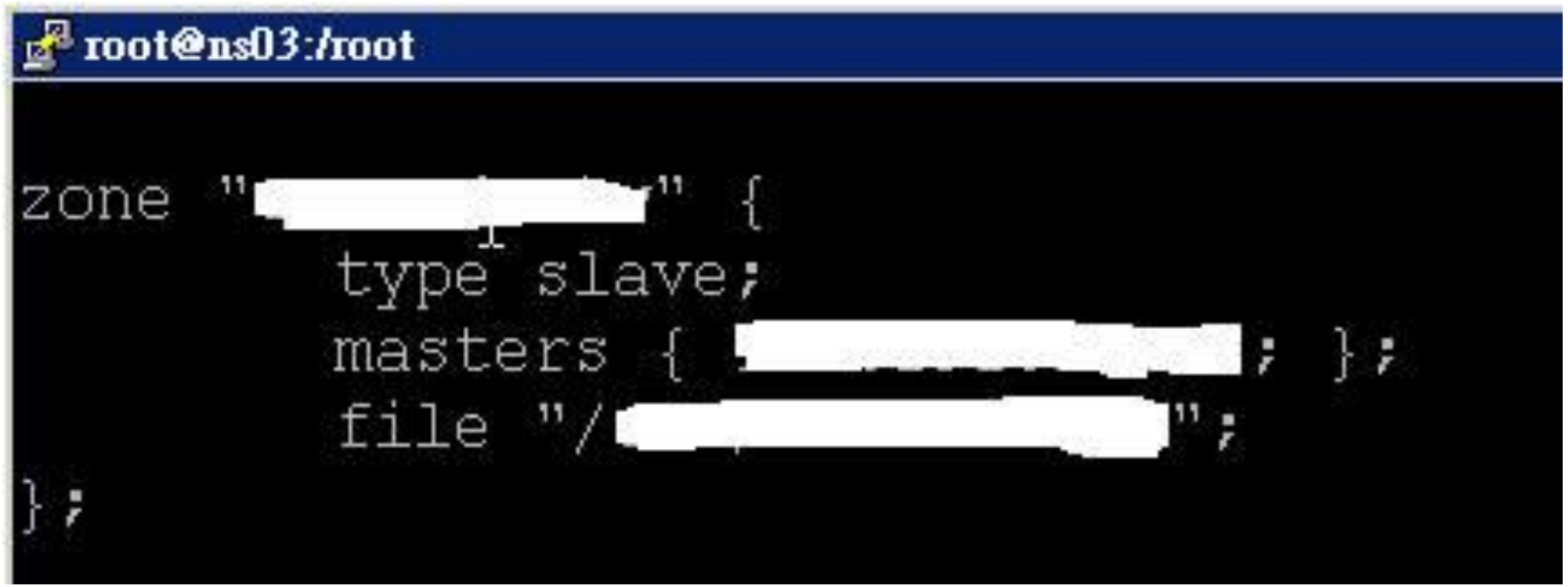
DNS 進階限制功能

- **DNS allow-notify**
  - 說明
    - 提供限制轄區變更通知來源 (zone 為 slave 才可以使用)
  - 預設設定
    - 預設只有 *masters { ...}* 區段來源可以進行
  - 使用語法
    - **allow-notify { address_match_list; };**
  - 使用範圍
    - 於 **options** 與 **zone** 區段內

Master DNS Notify



Slave DNS Notify



DNS 進階限制功能

- **DNS allow-recursion / recursion**
  - 說明
    - 提供限制允許指定來源才可以使用遞迴查詢功能
  - 預設設定
    - 預設為允許任何來源皆可以遞迴查詢資料
      - **allow-recursion { any; };**
      - **recursion yes ;**
  - 使用語法
    - **allow-recursion { address_match_list; };**
    - **recursion yes | no;**

DNS 進階限制功能

- **ACL (Access Control List)**
  - 說明
    - 定義 acl 清單
    - 提供給 **allow-*** 系列參數使用
  - 格式
    - **acl “name” { address_match_list; };**
  - 預先定義好的存取清單名稱
    - **none、any、localhost、localnets**

- **DNS** 安全性設定
- **DNS** 紀錄檔設定
- **DNS** 進階限制

DNS 服務監控

- DNS 常見問題
- **DNS 檢測步驟**

DNS查詢工具

- **dns** 相關工具
  - 程式項目
    - **nslookup**、**host**、**dig**
  - 程式項目說明
    - **nslookup** (query Internet name servers interactively)
    - **host** (DNS lookup utility)
    - **dig** (DNS lookup utility)

DNS查詢工具

- **nslookup**
  - 使用方式
    - nslookup [option] [host-to-find] [dns-server]
  - 交談模式常用的命令
    - **exit**
      - 結束程式
    - **lserver / server**：切換 name server
      - **lserver**，使用本機 /etc/resolv.conf 的 nameserver 敘述查詢切換到新的 name server
      - **server**，使用目前指定的 default name server 查詢

DNS查詢工具

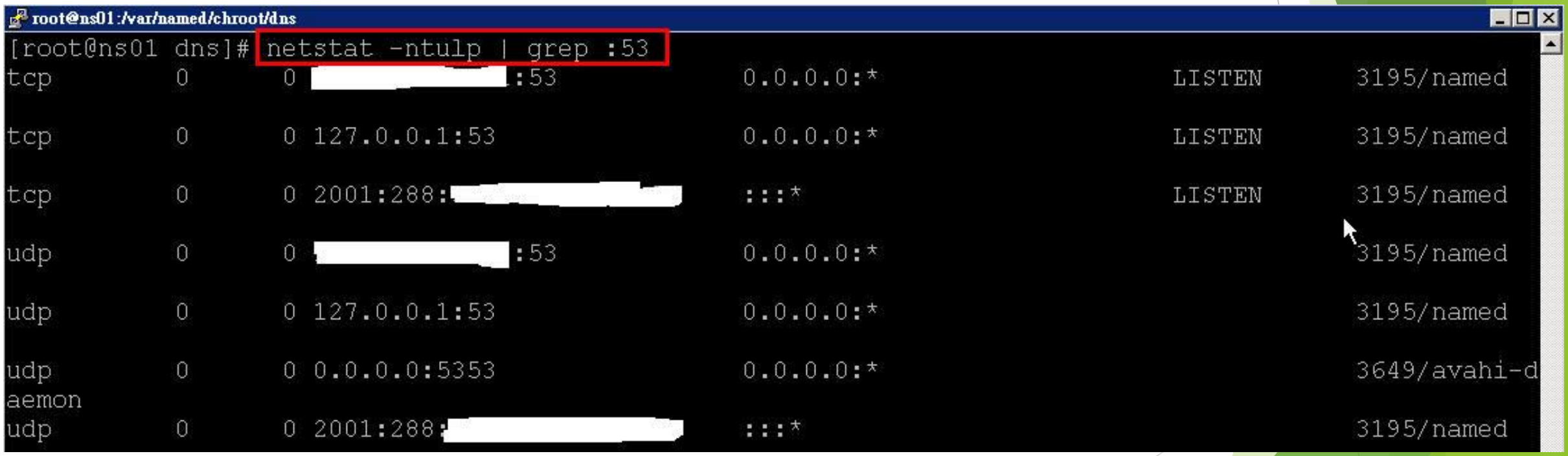
- **nslookup**
  - 交談模式常用的命令
    - **set [no]recurse**：設定使用 [非] 遞回類型尋找
    - **set type=N**：設定查詢類型 (any,cname,a,soa,ns,mx,txt)
  - 範例
    - **nslookup www.seed.net.tw**
    - **nslookup www.yahoo.com dns.hinet.net**
    - **nslookup -type=ns yahoo.com**

DNS查詢工具

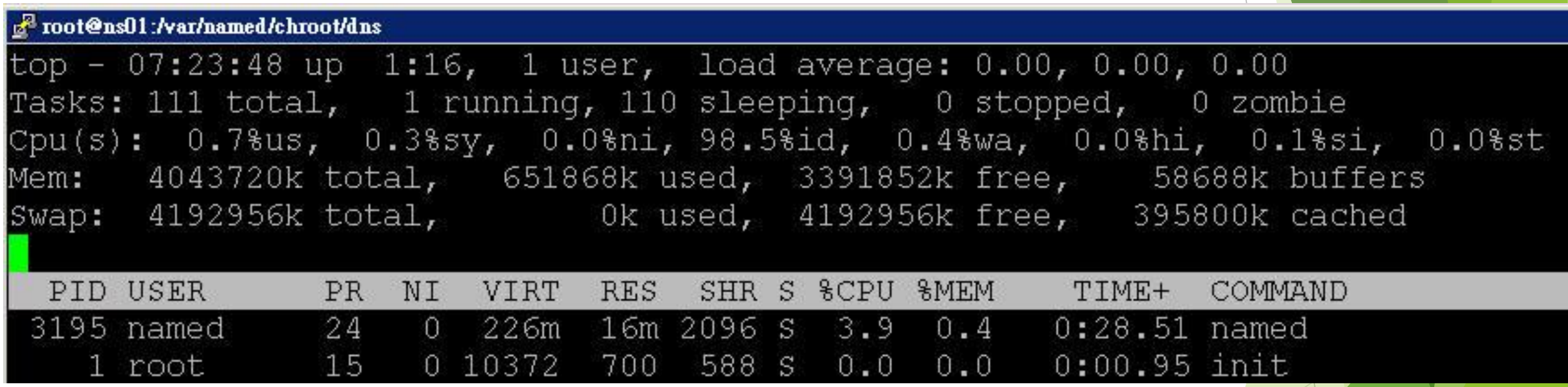
- **dig**
  - 說明：Domain Information Gopher
  - 使用方式
    - dig @server domain quert-type query-class
  - 範例
    - **dig　hinet.net**
    - **dig　hinet.net　soa**
    - **dig　@dns.seed.net.tw　seed.net.tw　ns**
    - **dig　-x　168.95.1.1**

DNS 服務Port

- ifconfig 確認IP
- netstat -ntulp | grep :53



Top指令確認系統資源

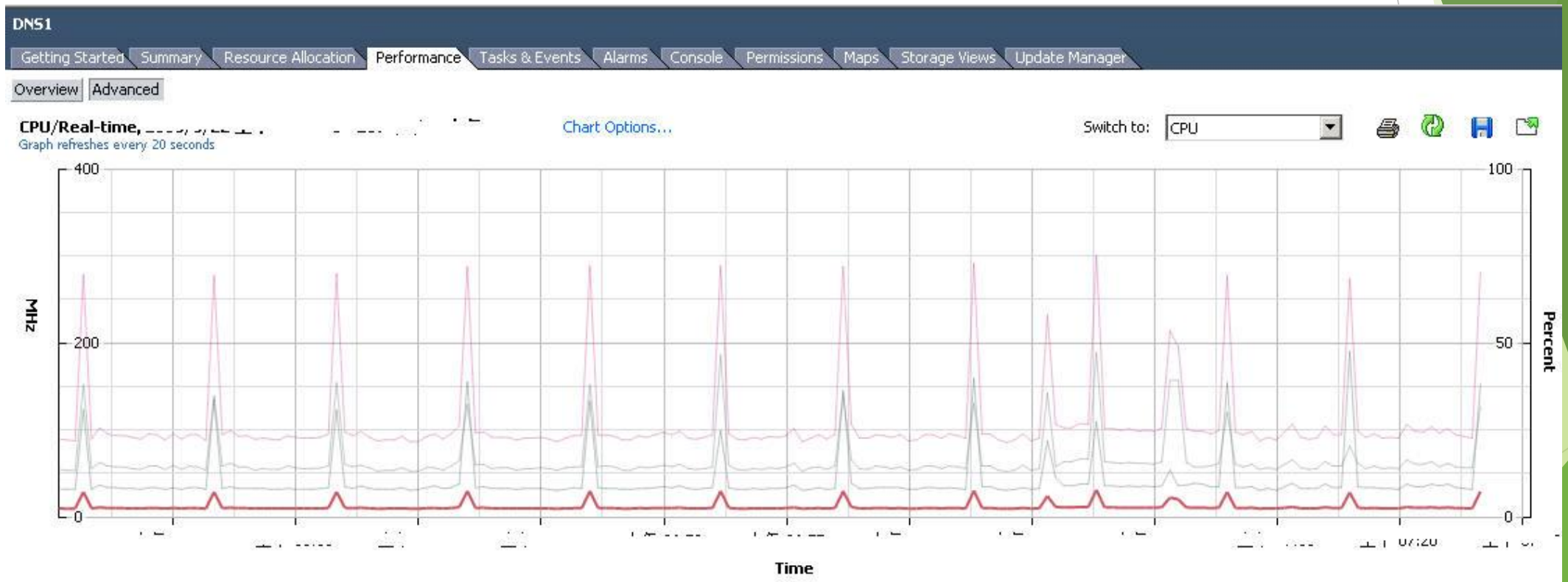


MRTG、nagios監控服務

- https://www.eriklundblad.com/log/post/monitor-bind-with-mrtg/
- https://exchange.nagios.org/directory/Plugins/Network-Protocols/DNS/check_dns-2Epl-(Advanced-Nagios-Plugins-Collection)/details

Hypervisor上的DNS VM

- 可由VM看Performance

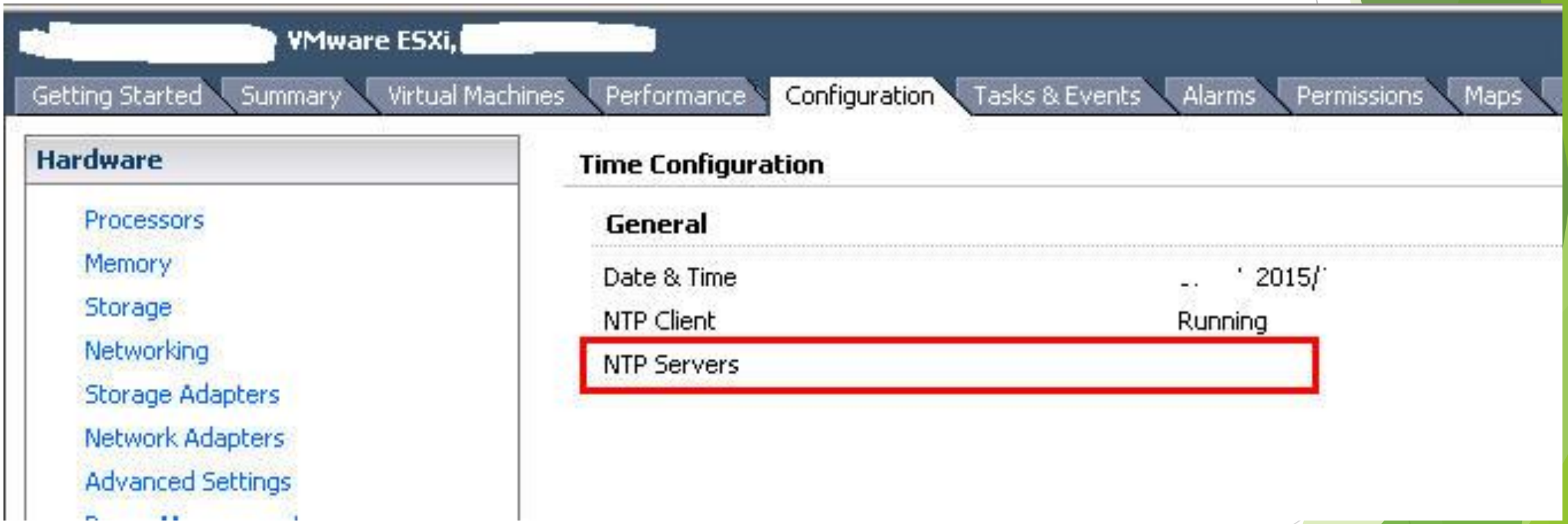


Performance Chart Legend

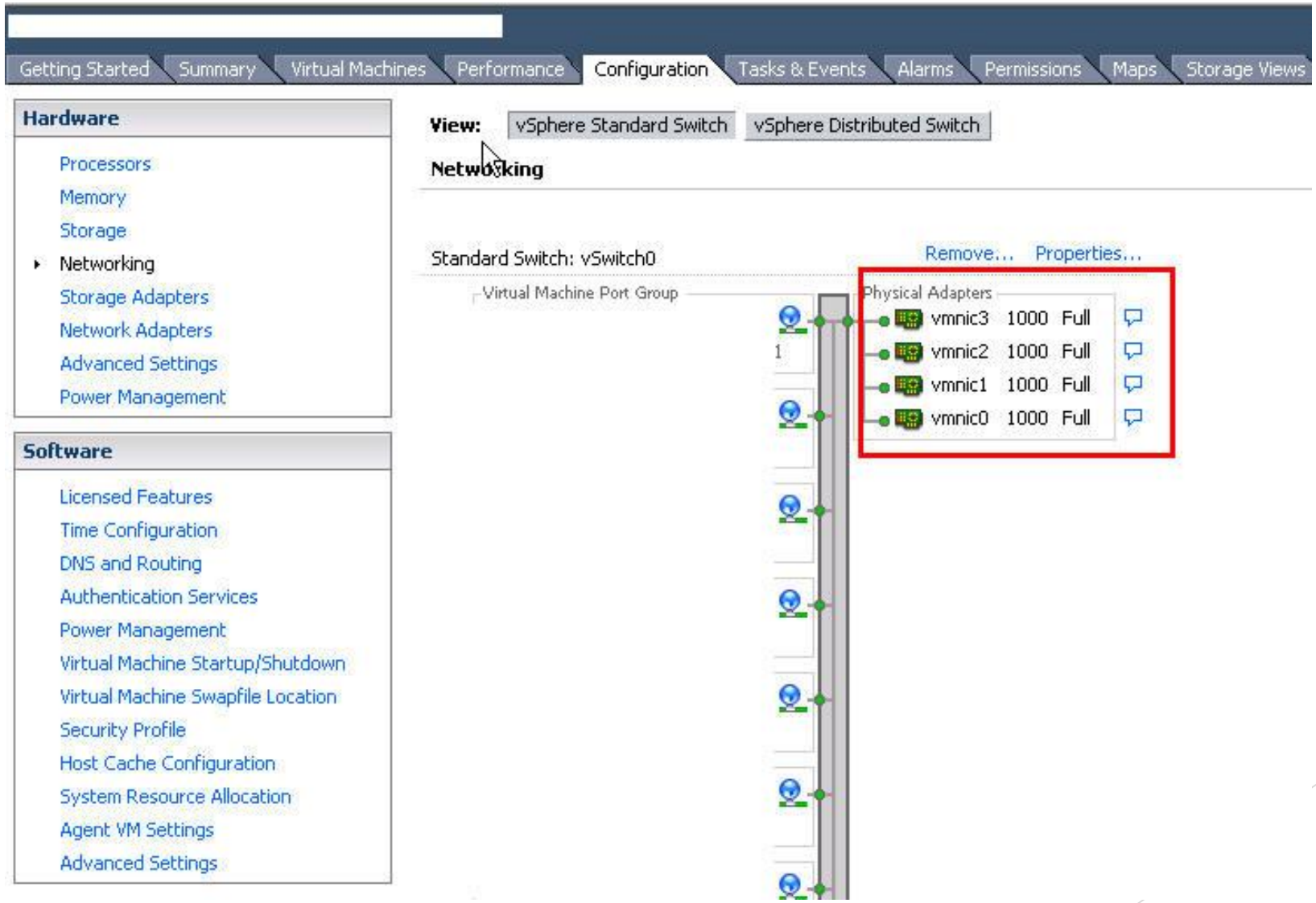
Key	Object	Measurement	Rollup	Units	Latest	Maximum	Minimum	Average
	1	Usage in MHz	Average	MHz	153	190	30	40.617
	DNS1	Usage	Average	Percent	7.08	7.56	2.15	2.728
	DNS1	Usage in MHz	Average	MHz	282	301	85	108.56
	0	Usage in MHz	Average	MHz	126	189	52	64.423

Hypervisor上的DNS VM

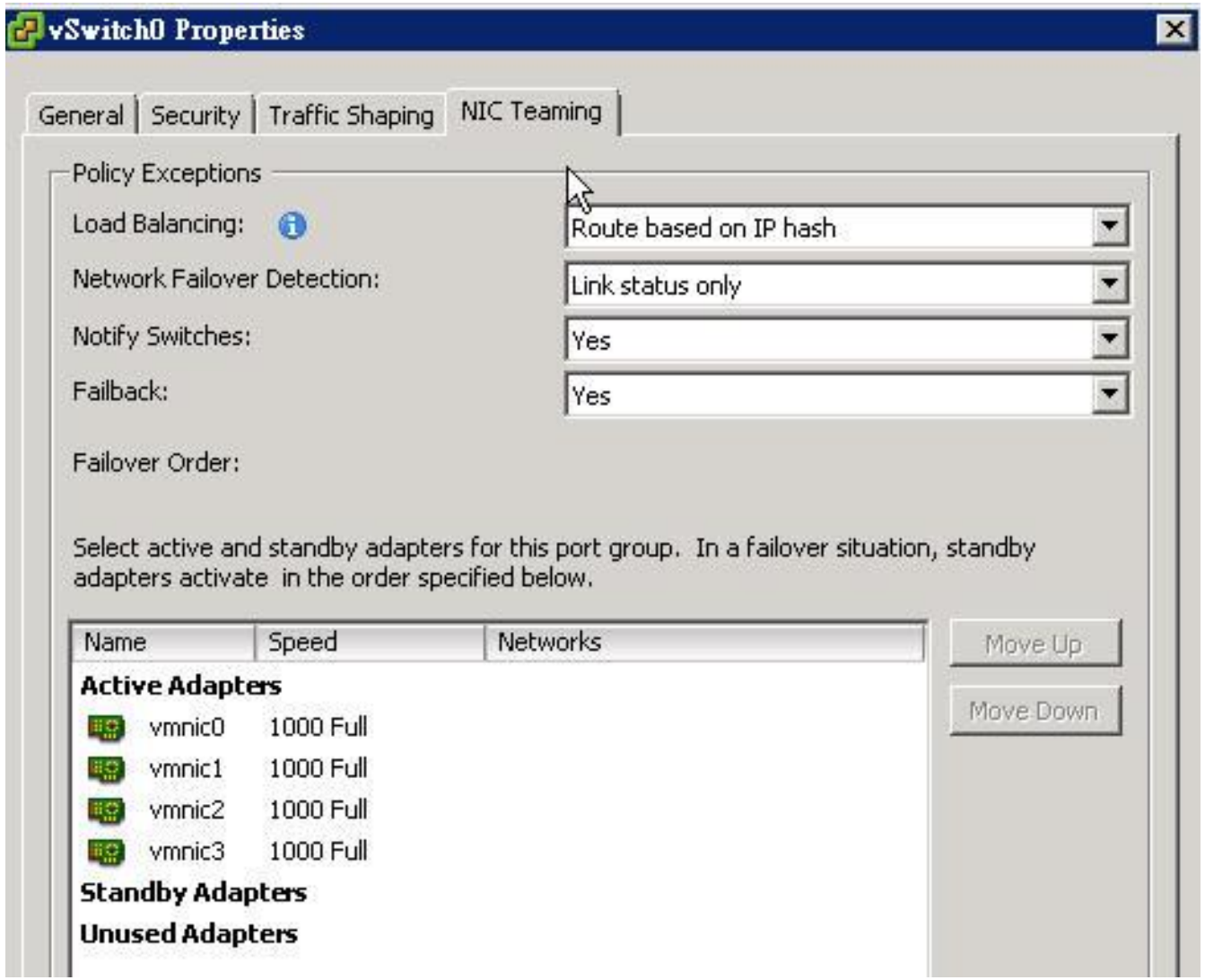
Hypervisor校時



Hypervisor網路redundant

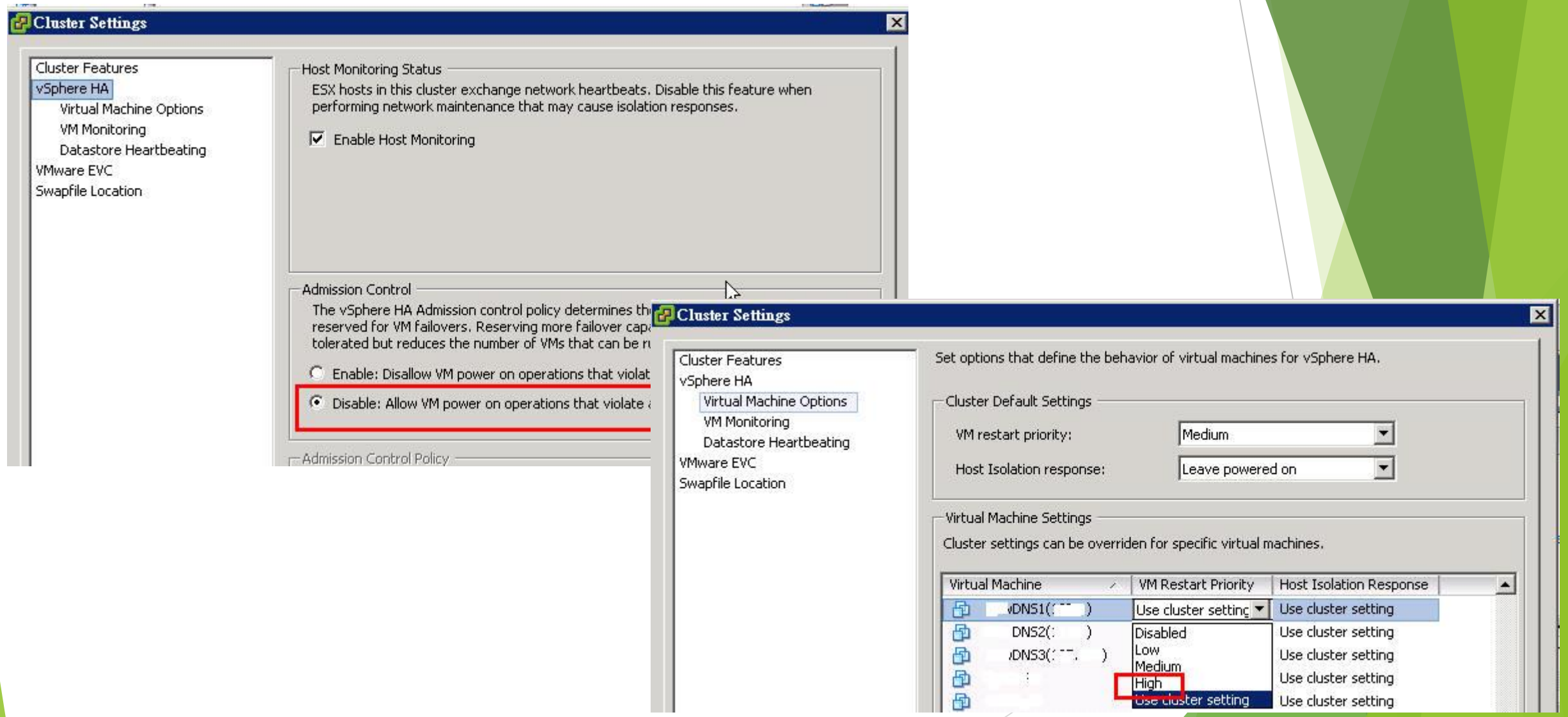


Hypervisor網路redundant




```
interface GigabitEthernet1/0/1
 description "Connect to [redacted]"
 switchport trunk allowed vlan [redacted]
 switchport mode trunk
 channel-group 1 mode on
!
interface GigabitEthernet1/0/2
 description "Connect to [redacted]"
 switchport trunk allowed vlan [redacted]
 switchport mode trunk
 channel-group 1 mode on
!
```

VMware HA細部微調



DNS設定備份、主機/VM備份

- 1. 將named.conf等相關設定tar備份
- 2. 定期將主機備份

- DNS 安全性設定
- DNS 紀錄檔設定
- DNS 進階限制
- DNS 服務監控

DNS 常見問題

- DNS 檢測步驟

一、設定錯誤、啟動失敗

- 1. 更改以下檔案若有missing config會造成啟動失敗
  - named.conf
  - 相關include設定檔
- 2. 建議更改前cp設定檔備份
  - 若重啟服務失敗則趕快先將設定檔cp回來
- 3. “;”容易忘記

二、slave DNS沒有更新記錄

- 1. 檢查slave dns notify log

```
[root@ns02 log]# tail notify.log
[redacted] client [redacted]#10420: received notify for zone
0.in-addr.arpa'
[redacted] client [redacted]#30512: received notify for zone
0.in-addr.arpa'
[redacted] client [redacted]#30114: received notify for zone
0.in-addr.arpa'
```

- 2. 檢查slave dns

```
[root@ns02 log]# tail xfer-in.log
[redacted] transfer of '[redacted]/IN' from [redacted]#53:
sing [redacted]#43857
[redacted] transfer of '[redacted]/IN' from [redacted]#53:
mpleted: 1 messages, 6 records, 203 bytes, 0.001 secs (203000 bytes/sec)
[redacted] transfer of '[redacted]/IN' from [redacted]#53: conn
```

二、slave DNS沒有更新記錄

- 3. telnet檢查兩台dns server port 53是否開通
- 4. 檢查設定master dns是否有將該zone設定notify yes與also-notify
- 5. 檢查設定slave dns是否有將該zone設定masters ip

三、更新master dns記錄，slave沒有同步

- 1. 檢查slave dns notify log

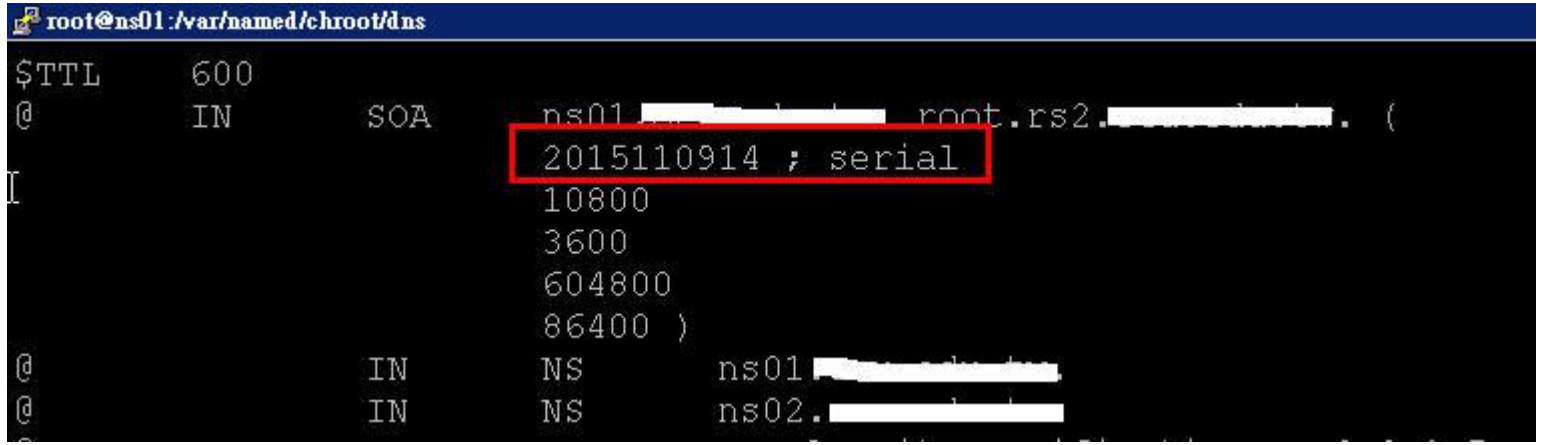
```
[root@ns02 log]# tail notify.log
[redacted] client [redacted]#10420: received notify for zone
0.in-addr.arpa'
[redacted] client [redacted]#30512: received notify for zone
0.in-addr.arpa'
[redacted] client [redacted]#30114: received notify for zone
0.in-addr.arpa'
```

- 2. 檢查slave dns

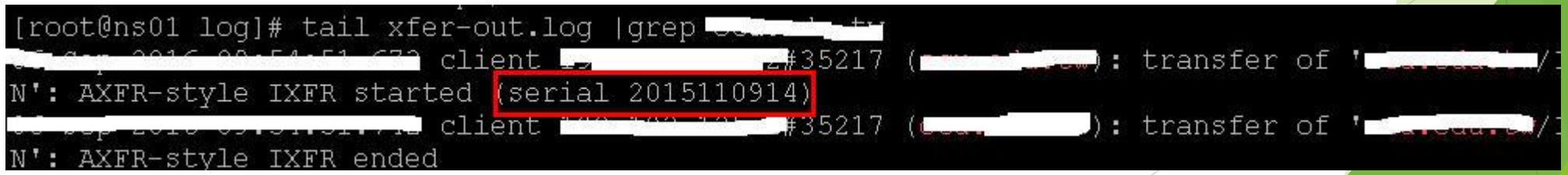
```
[root@ns02 log]# tail xfer-in.log
[redacted] transfer of '[redacted]/IN' from [redacted]#53:
sing [redacted]#43857
[redacted] transfer of '[redacted]/IN' from [redacted]#53:
mpleted: 1 messages, 6 records, 203 bytes, 0.001 secs (203000 bytes/sec)
[redacted] transfer of '[redacted]/IN' from [redacted]#53: conn
```

三、更新master dns記錄，slave沒有同步

- 3. master dns設定是否有更新serial number



- 4. master dns檢查xfer-out log



四、dns query外網速度慢

- 1. 確認是否有設定forwarders
- 2. 確認dns server使用該forwarder ip查詢是否會被阻擋
- 3. 可設定多組forwarders ip

五、dns無法query至網外

- 1. 確認是否有被教育部通報IP被阻擋
  - http://rs.edu.tw/tanet/spam.html
  - http://block.mlc.edu.tw/
  - https://www.tc.edu.tw/net/netflow
- 2. DNS NAT IP最好跟user網段對外NAT分開

六、DNS反應速度很慢

- 1. 由DNS top或MRTG檢查dns cpu loading
- 2. 檢查dns security log是否有大量錯誤
- 3. 有可能被DDoS
- 4. 確認區域是否allow外部query

七、一定要設定反解嗎?

- 反解IP只是一連串的符號
  - Dns.stepwise.com.tw → 125.227.68.246
  - 125.227.68.246 → 125-227-68-246.HINET-IP.hinet.net
- 哪種狀況要使用反解
  - Mail server
  - vmware
- 反解的好處
  - 增加連線速度
  - Mail Spam

八、避免LAME Server

- 建置兩台DNS Server作同步，進階再作負載平衡
- Server第二組DNS IP不要設定外部DNS IP
- 與上層組織設定第二組DNS
- Master、slave DNS最好在不同的sub-net

九、mail server寄信都被退，是否跟DNS有關

- https://www.senderbase.org/
  - 檢查有無在黑名單
- DNS不需修改A record
- Mail server可修改NAT對外IP

十、DNS Server無法寫入資料

- 確認系統碟使用量
- 刪除不必要檔案
- Rotate log
- LVM增加空間

十一、開網頁速度慢

- 確認內、外部開啟網頁速度
- 檢查IPV6 DNS設定
- 檢查web IPV6 IP

十二、DNS負載平衡須知

- DNS server負載需注意
  - 去回不同路
- 線路負載需注意
  - 外部Dns query路徑

- DNS 安全性設定
- DNS 紀錄檔設定
- DNS 進階限制
- DNS 服務監控
- DNS 常見問題

DNS 檢測步驟

檢測查詢一-確認第二層ns ip

- Dig @8.8.8.8 com.tw ns
- Nslookup
  - Server 8.8.8.8
  - Set type=ns
  - Com.tw

檢測查詢二-確認第三層ns ip

- Dig @a.twnic.net.tw stepwise.com.tw ns
- Nslookup
  - Server a.twnic.net.tw
  - Set type=ns
  - Stepwise.com.tw

檢測查詢三-確認dns servers ns record

- Dig @dns.stepwise.com.tw stepwise.com.tw ns
- Dig @dns2.stepwise.com.tw stepwise.com.tw ns
- Nslookup
  - Server dns.stepwise.com.tw
  - Set type=ns
  - Stepwise.com.tw
  - Server dns2.stepwise.com.tw
  - Set type=ns
  - Stepwise.com.tw

檢測查詢四-確認SOA序號

- Dig @dns.stepwise.com.tw stepwise.com.tw SOA
- Dig @dns2.stepwise.com.tw stepwise.com.tw SOA

- Nslookup
  - Server dns.stepwise.com.tw
  - Set type=soa
  - Stepwise.com.tw
  - Server dns2.stepwise.com.tw
  - Set type=soa
  - Stepwise.com.tw

檢測查詢五-確認MX record

- Dig @dns.stepwise.com.tw stepwise.com.tw mx
- Dig @dns2.stepwise.com.tw stepwise.com.tw mx

- Nslookup
  - Server dns.stepwise.com.tw
  - Set type=mx
  - Stepwise.com.tw
  - Server dns2.stepwise.com.tw
  - Set type=mx
  - Stepwise.com.tw

檢測查詢六-確認a record(www網站)

- Dig @dns.stepwise.com.tw www.stepwise.com.tw a
- Dig @dns2.stepwise.com.tw www.stepwise.com.tw a

- Nslookup
  - Server dns.stepwise.com.tw
  - Set type=a
  - www.stepwise.com.tw
  - Server dns2.stepwise.com.tw
  - Set type=a
  - www.stepwise.com.tw

檢測查詢七-其它網站工具

- https://www.whatsmydns.net
- https://dnschecker.org/
- http://dnscheck.pingdom.com/