快速安裝DNS Server(Caching Name Server)

高雄市政府教育局 資訊教育中心網路組 張宏明 更新日期:2016/12/08

壹、DNS概念:

DNS的結構

DNS是一個分層級的分散式名稱對應系統,有點像電腦的目錄樹結構:在最頂端的是一個 "root",然後其下分為好幾個基本類別名稱,如: com、org、edu等;再下面是組織名稱, 如: sony、toshiba、intel等;繼而是主機名稱,如: www、mail、ftp等。因為當初internet是 從美國發起的,所以當時並沒有國域名稱,但隨著後來internet的蓬勃發展,DNS也加進了諸 如tw、hk、au等國域名稱。所以一個完整的dns名稱就好像是這樣的: www.xyz.com.tw,而整 個名稱對應的就是一個IP地址了。

在開始的時候,root下面只有六個組織類別: edu 教育、學術單位 org 組織、機構 net 網路、通訊單位 com 公司、企業 gov 政府機關 mil 軍事單位

不過,自從組織類別名稱開放以後,各種各樣五花八門的名稱也相繼涌現出來了,但無論如何,取名的規則最好儘量適合網站性質。除了原來的類別資料由美國本土的NIC(Network Information Center)管理之外,其它在國域以下的類別分別由該國的NIC管理。這樣的結構看起來就像這樣



快速安裝DNS Server(Caching Name Server) 第1頁

DNS的運作

在我們設定IP網路環境的時候,通常都要告訴每台主機關於DNS伺服器的地址,下面讓我們 看看DNS是怎樣運作的:

- 1. 當被詢問到有關本域名之內的主機名稱的時候, DNS伺服器會直接做出回答;
- 2. 如果所查詢的主機名稱屬於其它域名的話, 會檢查記憶體, 看看有沒有相關資料;
- 3. 如果沒有發現,則會轉向root伺服器查詢;
- 4. 然後root伺服器會將該域名之授權(authoritative)伺服器(可能會超過一台)的地址告知;
- 5. 本地伺服器然後會向其中的一台伺服器查詢,並將這些伺服器名單存到記憶體中,以備將 來之需(省卻再向root查詢的步驟);
- 6. 遠方伺服器回應查詢;
- 7. 將查詢結果回應給客戶, 並同時將結果儲存一個備份在自己的快取記憶裡面;
- 8. 如果在存放時間尚未過時之前再接到相同的查詢,則以存放於快取記憶裡面的資料來做回應。

從這個過程我們可以看出,沒有任何一台DNS主機會包含所有域名的DNS資料,資料都是分 散在全部的DNS伺服器中,而NIC只需知道各DNS伺服器地址就可以了。

分擔DNS工作

Primary(master) DNS伺服器是架設在某一個網域下被主要授權並控制所有名稱記錄的主控制 伺服器,管轄著所有該網域的記錄資料,這些記錄資料只有primary(master)可以修改。 但如果在一個比較大型的網路中,DNS伺服器就會變得很繁忙了,所以您可以設定多個DNS 來分擔master的工作,但您或許不願意到每一個DNS伺服器去更新資料吧?而且就算您願意 這樣做,也容易出現錯誤或資料不同步的情形。這樣您可以設定其它的伺服器為secondary (slave) DNS來複製master上面的記錄資料,這樣,其它的電腦可以被指定到不同的DNS做查詢, 既可以分擔master的工作,而且資料也可以自動進行同步工作。您可以設定DNS資料同步的 時間間隔,在dns檔案中的Refresh設定就是了。同時您還會看到Serial,當slave的上面的serial 數字少於它,資料就會被複製,否則會被忽略。

若您沒有被授權或指定管理某個domain的DNS,但您所管理的電腦數實在太多,您可在您管理的區域內,架一個Cache name server,以減輕對外網路的負擔。

DNS主機的安全與分工

DNS在現代網路中,擔任了極度重要的角色,再加上IPv6環境與dnssec的功能,讓DNS主機的角色日益重要;當然,若想要惡意干擾或攻擊網路,當地的DNS主機將成為最佳的選擇。因此,DNS主機的安全,就成為重要的課題。

就整個安全性的設計架構而言,單位對外正式營運的DNS主機,應當僅負責這個單位正式 domain的查詢與回覆(Interative Query);而單位內部對外查詢的部份,應另外建立一套可進行 全球正反解的遞迴查詢(Recursive Query)DNS主機,並應限制單位內部查詢,以避免其他不必 要的查詢或攻擊。

由bind架設的DNS主機,可透過view的描述,在單一台DNS主機上,實作出同時兼具Interative Query及Recursive Query的DNS主機;只要利用view描述,將單位內部與外部查詢分開來,內

部可進行Recursive Query,而外部僅限Interative Query。

但是,在windwos server架設DNS主機,則未具備類以bind的view功能,以目前最新版本的 windows DNS server,只能開啟或關閉Recursive Query功能,而不能設定校內或單位內可以 Recursive Query,校外不能Recursive Query;若要達到上述,以學校內外的網段來區分Recursive Query功能,在Microsoft的官方建議,僅能利用2台DNS主機,分別設定成Interative Query供外 部查詢貴單位之domain;而另一台設定成Recursive Query供內部查詢之用。

綜合上述,若要架設安全性較高的DNS主機,考量經濟因素(因為學校通常連買主機的經費都不足了,還要買2台主機及OS!),會以1台主機,在Linux上利用bind來建立DNS主機。但是,由於bind的view描述太過複雜,學校網管人員架設的成功率微乎其微。

因此,為了降低學校網管在經濟上或實作上的負擔,我們則建議以下DNS安全架構:

- 在市網資訊服務入口(portal.kh.edu.tw)上,申請DNS代管服務:貴單位的domain管理,就由 市網的DNS代管服務取代處理,不但可免除架設主機與安全性維護的負擔,另外可額外附 贈dnssec機制。
- 2. 學校或單位內部,則有幾項方式可供選擇來建置或架設主機:
 - (1) 校內可利用Windows或Linux架設slave DNS主機,開啟Recursive Query功能,並僅限校 內或單位內使用。
 - (2) 校內可利用市網提供的caching Name Server VM image,架設在日常工作的電腦上,提供 校內或單位內使用者作Recursive Query。
 - (3)使用市網提供的4台使用者端專用之DNS主機(uns1~uns4)進行dns查詢(Recursive Query)。 但由於DNS服務管理的單位或學校日益增多,對市網4台DNS主機而言,負載有日益增加之趨勢。

考量學校規模與經濟條件及使用負擔的各項因素,建議如下:

- 1. 若學校有能力架設bind DNS主機,則建議自行架設為宜。
- 2. 若學校僅有能力架設windows DNS主機,則建議申請DNS代管,並將原來的windows DNS 主機改設定成caching Name Server。
- 3. 若沒有上述1.2.條件的話,請直接申請DNS代管;24班以上,強烈建議增加建置一台虛擬主機caching Name Server供校內使用,以加快查詢的速度,並降低市網DNS主機的負擔。而 24班以下,考量學校人力負擔與機器規模,則建議直接使用市網的4台使用者端專用之DNS 主機即可。

貳、快速架設caching Name Server:

為了降低學校架設DNS主機的困擾與維運上的負擔,我們提供了2種簡易快速的建構的方式:

- 1. 利用單板電腦(Single-board computer),將架好的主機image檔寫到microSD卡上,開機後進 行網路環境設定,即可使用。
- 利用虛擬主機技術,將架好的主機打包成虛擬主機的image檔。學校只要下載該image檔後, 匯入虛擬主機內,再進行網路環境設定後,即可使用。

 學校可利用現有的電腦主機,安裝虛擬軟體(HyperV、VMware Player或Virtual Box)後,將 虛疑主機imgage檔匯入後使用,不用額外再準備電腦。

預裝好的DNS主機採用CentOS7平台建置,已設定好可自動更新、自動昇級與自動重開機等機制,讓學校理管人員免除不必要的維護工作,日常狀況下,只要收email確認主機目前的狀況即可。

單板電腦(Single-board computer)

目前適用的單板電腦型號如下:

- 1. Raspberry Pi 2
- 2. Raspberry Pi 3

請依型號下載相對應的image檔,再寫入microSD卡。

http://ftp.kh.edu.tw/APPL/DNS/cachingDNS/cent7-RaspberryPi2_cachingDNS_20161207.img.gz http://ftp.kh.edu.tw/APPL/DNS/cachingDNS/cent7-RaspberryPi3_cachingDNS_20161207.img.gz

虛擬主機技術:

實體機(Host)規格需求:

- 1.64位元CPU(至少雙核心)
- 2. 主記憶體至少4G
- 3. 硬碟空間至少保留20-50G給虛擬機使用
- 4. OS: Windows 7以上或Linux平台
- 5. 須安裝VMware Player或Virtual Box最新版本
- 6. 若使用Hyper-V, OS至少Windows 8/10 或 Windows Server 2008R2以上版本

虛擬機(guest)規格:

- 1.64位元CPU(單核心)
- 2. 主記憶體1G
- 3. 硬碟空間20G
- 4. OS: CentOS 7 x64版本
- 5. 利用bind架設caching Name Server

安裝虛擬主機軟體(hypervisor):

請依您的喜好,擇一套虛擬主機管理軟體(hypervisor)安裝使用。

- 1. VMware Player請至http://www.vmware.com/go/downloadplayer下載最新版本
- 2. Virtual Box請至https://www.virtualbox.org/wiki/Downloads下載最新版本
- 3. HyperV v2.0(Windwos 8內建) or HyperV v3.0(Windows 10內建),請至控制台→程式集\程式 和功能→開始或關閉Windows功能,將Hpyer安裝啟用。

下載caching Name Server VM image檔:

VMware或Virutal Box請下載: http://ftp.kh.edu.tw/APPL/DNS/cachingDNS/cent7_dns_1051205.ova HyperV請下載: http://ftp.kh.edu.tw/APPL/DNS/cachingDNS/cent7_dns_hyperv_1051205.zip

安裝期間需要的工具如下:

- 1. 解壓縮軟體 7zip: http://www.developershome.com/7-zip/
- 2. USB/SD卡/MicroSD卡Disk Image讀寫工具 Win32DiskImager: https://sourceforge.net/projects/win32diskimager/

在單板電腦(Single-board computer)上建置Caching Name Server主機:

1. 請先使用7zip工具將下載的image壓縮檔進行解壓縮

			修改日期		類型		大小
iso 🛛			2016/7/6 下午	- 01	檔案資	料夾	
Pi			2016/12/7下	午 0	檔案資	料夾	
🐼 cent7_dns_1051205.ova			2016/12/5上的	午 0	OVA 楷	案	793,459 KB
📱 cent7_dns_hyperv_1051205.zip			2016/12/8下	午 0	壓縮的	(zipped)	698,594 KB
cent7-RaspberryPi2_cachingDNS_20161207.img.	az		2016/12/8下	午 0	GZ 檔案	72	373,618 KB
cent7-RaspberryPi3_cachingDNS_20161207.img.		開啟檔案(H	H)		MA	TR.	380,730 KB
		7-Zip			>	開啟壓縮	檔
		CRC SHA			>	開啟壓縮	楅
	2	Edit with I	Notepad++			解壓縮檔	案
	(e)	使用 ESET	Endpoint Security 掃描			解壓縮至	此
		進階選項			>	解壓縮至	"cent7-Raspberry

- 2. 記得要先安裝MicroSD卡讀寫工具Win32DiskImager,並啟用這工具。
- 3. 在Win32DiskImager視窗中,左邊請填入Disk Image的檔名,右邊請選取您的MicroSD卡的 磁碟機代號,然後按下「Write」鈕,將作業系統寫入MicroSD卡中。

👒 Win32 Disk Im		×				
Image File			—Device —			
F:/CentOS7-RaspberryPi2_cacheDNS_20161207.img 📄 [J/] 🔻						
Copy 🗌 MD5 Has Progress	h:					
Version: 0.9.5	Cancel	Read	Write		Exit	
Write data in 'Image File' to 'Device'						

- 4. 完成之後,請將MicroSD卡從電腦取出,並插入Raspberry Pi 2/Pi 3的插槽,最後接上電源後 即可進行開機的程序。
- 5. 第一次開機時,進自動進行這台DNS主機主要partition擴展至全張SD上容量,完成後會自動重新開機,再進入登入的狀態。

在VMware Player上建置caching Name Server虛擬機:

- 1. 請先使用7zip工具將下載的image壓縮檔進行解壓縮。
- 2. 使用檔案總管,將滑鼠移到cent7_dns.ova檔,雙擊滑鼠左鍵,以便進行虛擬機的安裝與轉 檔工作。或按滑鼠右鍵,選「開啟檔案」也可以。

名稱		修改日期	類型		大小	
퉬 cent7_dns-pic		2014/12/1 下午 0	檔案資料夾			
퉬 old_ova		2014/12/2 上午 1	檔案資料夾			
🐏 12.DNS_Server安装.odt		2011/11/16下午	OpenDocument	t	74 KB	
💗 cent7_dns.ova		2017/12/2 上午 0	Opon Virtualizat	ji	842,596 KB	
🖳 快速安装DNS Server.docx		Open			303 KB	
		7-Zip	+			
		Edit with Notepad++				
	۲	使用 ESET Endpoint Secu	urity 掃描			
		進階選項	*			
		開啟檔案(H)	•	ij.	VirtualBox.ex	e
		永遠可以離線瀏覽(A)		ŵ	VMware Play	er
		還原酱版(\/)			選擇預設程式	(C)
		傳送到(N)	+			

3. 接下, VMware Player會詢問您虛擬機的名稱與存放的路徑, 您必須指定虛擬機存放的路徑, 以便將image檔轉換成虛擬機的檔案。

Import Virtual Machine	—
Store the new Virtual Mach	ine
Provide a name and local s virtual machine.	torage path for the new
Name for the new virtual machine:	
cent7_dns	
Storage path for the new virtual m	achine:
F:jcent7_dns	Browse
Help	Import Cancel

4. 完成後,請按下「Import」鈕,以便進行轉檔的工作。

😪 1% - VMware Player (Non-commercial use only)	😼 88% - VMware Player (Non-commercial use only)
Pløyer 👻 🕨 👻 🔚 🐻	Player 👻 🕨 👻 🛄 🍓
Importing cent7_dns	
Importing cent7_dns	Importing cent7_dns

快速安裝DNS Server(Caching Name Server) 第7頁

5. 滙入完成後, VMware Player會自動啟動這個虛擬機。您會看到開機選單。



6. 若您不動任何按鍵,5秒後,會自動帶入最新kernel版本開機。

2.325214] sd 2:0:0:0: [sda] Assuming drive cache: write through 2.325774] sd 2:0:0:0: [sda] Assuming drive cache: write through 2.327556] sd 2:0:0:0: [sda] Assuming drive cache: write through 6.999564] end_request: I/O error, dev fd0, sector 0 7.020516] end_request: I/O error, dev fd0, sector 0 7.978957] piix4_smbus 0000:00:07.3: Host SMBus controller not enabled!

7. 開機完成後,會出現系統提示號,請先輸入root的帳號與密碼,便可登入系統。

CentOS Linux 7 (Core) Kernel 3.10.0-123.9.3.el7.x86_64 on an x86_64 localhost login: _

ſ

在Virtual Box上建置caching Name Server虛擬機:

- 1. 請先使用7zip工具將下載的image壓縮檔進行解壓縮。
- 2. 使用檔案總管,將滑鼠移到cent7_dns.ova檔,雙擊滑鼠左鍵,以便進行虛擬機的安裝與轉 檔工作。或按滑鼠右鍵,選「開啟檔案」也可以。

名稱			修改日期	類型		大小
퉬 cent7_dns-pic			2014/12/1 下午 0	檔案資料本	5	
🔰 old_ova			2014/12/2 上午 1	檔案資料本	5	
🐏 12.DNS_Server安装.odt			2011/11/16 下午	OpenDoc	ument.	74 KB
💗 cent7_dns.ova		Open		<u> </u>	alizati.	842,596 KB
🗐 快速安装DNS Server.docx		7-Zip		•	Word	303 KB
	2	Edit with	Notepad++			
	۲	使用ESET	「Endpoint Security 掃	描		
		進階選項		٠.		
		開啟檔案((H)	۱.	🥡 V	irtualBox.exe
		永遠可以翻	離線瀏覽(A)		🤹 v	'Mware Player
		還原者版(M		暹	趕預設程式(C)
		傳送到(N))	×		

3. 接下來Virtual Box會提示要匯入的虛擬機的組態(config)。這裡要注意一下,您的虛擬的硬 碟機存放的路徑是否正確,若不正確,請直接點選該項目後,修改路徑。

🕞 匯入虛擬應用裝置		匯入虛擬應用裝置	[] X
應用裝置設定	擬機器和匯入 VirtualBox 機器的建議設定值。 您可以	應用裝置設定	凝機器和匯入 VirtualBox 機器的建議設定值。 您可以
在項目按兩下變更計多顯示	的內容和使用以下核取方或停用其它。 組態	在項目按照下變更計多顯示	的內容和使用以下核取力現停用其它。 組態
虚擬系統1		⊙ DVD	
😪 名稱	cent7_dns		
🗮 客體作業系統類型	🔁 Red Hat (64 bit)	🗗 網路卡	📝 Intel PRO/1000 MT Desktop (82540EM)
CPU	2	◇ 硬碟控制器 (IDE)	PIIX4
RAM	2048 MB	◇ 硬碟控制器 (IDE)	PIIX4
💿 DVD			AHCI
		▲ 🔷 硬碟控制器 (SAS)	LsiLogicSas
🗗 網路卡	📝 Intel PRO/1000 MT Desktop (82540EM) 💡	☑ 虛擬磁碟映像	C:\Users\jang\VirtualBox VMs\cent7_dns\c
🔲 重新初始化所有網路卡的) MAC 位址 (R) 還原預設値 隆入 取消	🔲 重新初始化所有網路卡的	MAC 位址 (2) [還原預設值] 匯入 取消

4. 完成後,請按「匯入」鈕後,開始轉換硬碟檔。



快速安裝DNS Server(Caching Name Server) 第9頁

5. 匯入完成後,再重新檢視一下虛擬機的組態(config)。



6. 若沒有問題,請按下「啟動(T)」圖示,以便進行開機作業。

🝓 cen	it7_dns	[執行中]	Þ] - Oracle VM VirtualBox 🔤	
機器	檢視	装置	說明	
	Cen	tOS L	Linux (3.10.0-123.9.3.el7.x86_64) 7 (Core)	
	Cen	tOS I	Linux, with Linux 3.10.0-123.el7.x86_64	
	Cen	tOS I	Linux, with Linux O-rescue-c3cb7ad7306245598af3d83b301dd68	15
	Use	the	\uparrow and \downarrow keys to change the selection.	
	Pre	ss 'e	e' to edit the selected item, or 'c' for a command prompt.	
			🛛 💿 🌽 🖶 🛄 💷 🔘	🖲 Right Ctrl 🔡

7. 若您不動任何按鍵,5秒後,會自動帶入最新kernel版本開機。

[0.000000] tsc: Fast TSC calibration failed [2.866970] sd 2:0:0:0: [sda] Incomplete mode parameter	data
[2.866970] sd 2:0:0:0: [sda] Incomplete mode parameter	• data
[2.868180] sd 2:0:0:0: [sda] Assuming drive cache: wri	ite through
I 2.870268] sd 2:0:0:0: [sda] Incomplete mode parameter	• data
[2.870282] sd 2:0:0:0: [sda] Assuming drive cache: wri	ite through
[2.873875] sd 2:0:0:0: [sda] Incomplete mode parameter	• data
[2.874005] sd 2:0:0:0: [sda] Assuming drive cache: wri	te through

CentOS Linux 7 (Core)

8. 開機完成後,會出現系統提示號,請先輸入root的帳號與密碼,便可登入系統。

CentOS Linux 7 (Core) Kernel 3.10.0-123.9.3.el7.x86_64 on an x86_64 localhost login: _

在Hyper-V上建置caching Name Server虛擬機:

1. 請先使用7zip工具將下載的image壓縮檔進行解壓縮。

名稱	^	修改日期	類型	大小
iso		2016/7/6 下午 01. 2016/12/7 下午 0.	檔案資料夾 檔案資料夾	
🙀 cent7_dns_1051205.ova		2016/12/5 上午 0.	OVA 檔案	793,459 KB
eent7_dns_hyperv_1051205.zip	PR Et / O		壓縮的 (zipped)	698,594 KB
cent7-RaspberryPi2_cachingDN:	開啟(O)	8 下午 0.	GZ 檔案	373,618 KB
cent7-RaspberryPi3_cachingDN	在新視窗開啟(E)	8 下午 0.	GZ 檔案	380,730 KB
CentOS7-RaspberryPi2_cacheDI	解壓縮全部(T)	7 下午 0.	光碟映像檔	2,929,664
	7-Zip	> 開	故壓縮檔	
	CRC SHA	> 開	欲壓縮檔	
	e 使用 ESET Endpoint Security 掃描	解	壓縮檔案	
	進階選項	> 解	壓縮至此	
	47.22.20184公共市(1)		壓縮至 "cent7_dns_hype	rv_1051205\"

2. 開啟「Hyper-V管理員」



3. 在「Hyper-V管理員」視窗中,按下右側「匯入虛擬機器...」後,在下個出現視窗中,按下 下方的「下一步(N)」鈕。

Ill Hyper-V 管理員				
檔案(F) 動作(A) 檢視(V) 說	祧明(H)			
🗢 🔿 🙍 📰 👔				
 Hyper-V 管理員				
DESKTOP-QS03PRU	虚擬機器(I)			DESKTOP-QS03PRU
	名稱	狀態	CPU 使用率 指派	新増
		此伺服器	上找不到虛擬機器。	□ 匯入虛擬機器
				📔 Hyper-V 設定
				■ 虚擬交換器管理員
				🚄 編輯磁碟
	<			🔛 檢查磁碟
☑ 匯入虛擬機器				×
└── 任恋開始則				
在您開始前	此精靈可協助您從一組調	設定檔匯入虛擬機器。	它將會引導您解決設定	問題,以準備在此電腦上
尋找資料夾	使用虛擬機器。			
選取虛擬機器				
選擇匯入類型				
摘要				
	不要再顯示此頁面(D)))		

下一步(N) >

取消

4. 在「尋找資料夾」視窗中,按下右邊的「瀏覽(B)」鈕,找到您剛剛解壓縮的VM image資料 灰所在,確定後即可看到要滙入資料來的路徑。然後按「下一步(N)」鈕。

▶ 匯入虛擬機器	×
▶ 尋找資料夾	
在您開始前 指定包含要匯入之虛擬機 尋找資料夾 資料夾(O): 選取虛擬機器 選擇匯入類型 摘要	§器的資料夾。 瀏覽(B)
 ✓ 選擇資料夾 ← → < ↑ → > 本機 > DATA-2T (F:) > 組合管理 < 新増資料夾 ▲石管理 < 新増資料夾 ◆ 下載 ● 下載 ○ centos7_dns ○ iso ● Pi ● 百樂 > ● 真面 	 ▶ 匯入虛擬機器 ▶ 尋找資料夾 在您開始前 每找資料夾 遊找資料夾 選取虛擬機器 選擇匯入類型 摘要
速取虛擬機器 在您開始前 尋找資料夾 選取要匯入的虛擬機器(S) 選取虛擬機器 名稱 選擇匯入類型 信	〕: ^ 建立日期 2015/11/9 下午 03:48:51

5. 接下來設定機器唯一識別碼,因為我們是複製資教中心製作的虛擬機器,所以我們選第三個選項,來創建一個獨立新的唯一識別碼,然後按「下一步(N)」鈕。

在您開始前	選擇要執行的匯入類型:
尋找資料夾	就地登錄虛擬機器 (使用現有的唯一識別碼)(R)
選取虛擬機器	○ 還原虛擬機器 (使用現有的唯一識別碼)(S)
選擇匯入類型	● 複製虛擬機器 (建立新的唯一識別碼)(◎)
摘要	

快速安裝DNS Server(Caching Name Server) 第14頁

6. 接下來設定新的虛擬機要存放的路徑。若您不需要變更系統預設的路徑,則請勿勾選「將 慮擬機器儲存在不同位置(S)」項目即可;若您需要變更路徑,則請勾選「將慮擬機器儲存 在不同位置(S)」項目,並將下面三項填入您所需要存儲的資料路徑。

在您開始前 尋找資料夾 選取虛擬機器 選擇匯入類型	您可以指定新資料夾或現有資料夾來儲存虛擬機器檔案。若未指定,積靈會將 腦上的預設 Hyper-V 資料夾,或是在虛擬機器設定中指定的資料夾。 ✓ 將虛擬機器儲存在不同位置(<u>S</u>) <	檔案匯入到此電
選擇目的地 選擇儲存資料夾 摘要	全流体的 C:\ProgramData\Microsoft\Windows\Hyper-V\ 检查點存放區(C):	瀏覽(<u>B</u>)
	D:\centos7_dns 智慧型分頁處理資料夾(<u>M</u>):	瀏覽(R)
	D:\centos7_dns	瀏覽(0)

在您開始前	您要將此虛擬機器的匯入虛擬硬碟儲存在何處?
尋找資料夾	位置(L): D:\ 瀏覽(B)
選取虛擬機器	
選擇匯入類型	
選擇目的地	
選擇儲存資料夾	
摘要	

7. 最後再度確認一下要匯入虛擬機器的各項摘要,確定後請按下「完成(F)」鈕,進行匯入新 機器的程序。

💌 正在完成匯入精	8 2		
在您開始前 尋找資料夾 選取虛擬機器 選擇匯入類型 選擇目的地 選擇儲存資料夾 摘要	您即將執行下列作業。 描述①: 虚擬機器: 匯入檔案: 匯入檔案: 虛擬機器設定資料夾: 虛擬機器設定資料夾: 者著型分頁處理檔案存放區: 虛擬硬碟目的資料夾:	centos7_dns F:\centos7_dns\Virtual Machines\1309E6E9-A4C4-4239-8409-0D975 複製 (產生新的識別碼) C:\ProgramData\Wicrosoft\Windows\Hyper-V\ D:\centos7_dns D:\centos7_dns D:\	5
	< 若要完成匯入並關閉此積靈,言	済按一下 [完成]。 (上一步(2) 下一步(3) 天一歩(3) 東消	

快速安裝DNS Server(Caching Name Server) 第15頁

8. 匯入完成後,回到「Hyper-V管理員」視窗,您可看到有一台虛擬機器centos7_dns存在。請 先選這台虛擬機後,再到左下方按下「連線」後,即可開啟centos7_dns虛擬機的視窗。

Hyper-V 管理員	虎擬機器(1)				動作	:		
ESKTOP-QS03PRU	2組	狀態	CPU使用率	指派的	DES	SKTOP-Q	S03PRU	
	centos7_dns	關閉		JEWAR:		新増		
					4	匯入虛撰	題機器	
					*	Hyper-\	/ 設定	
					Ĕ.	虛擬交換	國器管理員.	
					₫.	虛擬 SA	N 管理員	
	<				-	編 輯磁破	¥	
	检查點(())			_		檢查磁碼	¥	
	(2) (2)			_		停止服務	5	
		選取的虛拟	疑機器沒有檢查:	骷∘	×	移除伺服	器	
					U	重新整理	2	
						檢視		
					?	說明		
					cen	tos7_dns	;	
					-	連線		
						設定		
🖳 在 DESKTOP-QS03PRU 上	的 centos7_dns - 虛擬	機器連線				_		×
檔案(F) 動作(Δ) 媒體(M)	檢視(\/) 說明(H)							
	> № 5 ₩							
	已關閉虛擬機	器 'cento	os7_dn	s'				
;	皆要啟動虛擬機器,調	a谷 [執行] 功(能表選取 [[女動1				
狀態: 嗣閉								
						_		

快速安裝DNS Server(Caching Name Server) 第16頁

9. 如要啟動這台虛擬機,請在上方工具列按下 🕑 鈕,即可開機,開機完成後,就可看到DNS

主機登入的畫面。



項目	範例	請填寫您當地的網路環境資料
IPv4的IP/NetMask	163.32.119.177/25	
IPv4的GateWay	163.32.119.254	
IPv4的DNS主機1	163.28.136.2	
IPv4的DNS主機2	163.16.1.23	
您的網域名稱	xxx.kh.edu.tw	
IPv6的IP/NetMask	2001:288:8201:3::177/64	
IPv6的GateWay	2001:288:8201:3::1	
IPv6的DNS主機1	2001:288:8401::3	
IPv6的DNS主機2	2001:288:8201:1::10	
您的網域名稱	xxx.kh.edu.tw	
您的主機名稱(FQDN)	pc177.kiec.kh.edu.tw	

在第一次開機後,開始設定前,我們先準備本地端網路環境的相關設定參數,項目如下:

這個虛擬機的預設帳號密碼如下:

root/happy_dns@kh

dnsuser/happy_dnsuser@kh

由於這台虛擬機是中心伙伴預先安裝完成的機器,為了能讓學校快速的使用,在第一次開機 後,必須先完成機器本身的相關設定,完成後才能在學校端服務。我們將介紹一下,第一次 開機的設定,大致分成三個程序:

- 1. 網路環境設定:因為要當Server使用,最好以固定IP為主,而且必須同時設定IPv4與IPv6 的網路環境。
- 2. ssh遠端安全連線服務:因為網路環境改變,必須重新建置出新的加密金鑰。
- 3. 第一次啟動named及設定開機啟動機制,同時並設定本機防火牆開啟dns服務。

接下來,我們就來進行第一次開機後的環境設定:

1. 以root帳號登入到系統中。

2. 在/root目錄下,您可找到start_me.sh這個執行檔。

[root@localhost ~]# ls -l

總計 12

-rw-----. 1 root root 1458 11月 28 15:34 anaconda-ks.cfg

-rwxr-xr-x. 1 root root 477 11月 28 15:07 start_me.sh

-rwxr-xr-x. 1 root root 152 11月 28 15:01 sync_dns_script.sh

3. 執行start_me.sh這個執行檔,以便開始進入設定的程序。

[root@localhost ~]# ./start_me.sh

Start setup your caching name servce.....

Step1. Setup network (press any key to continue)

進入第一個步驟,要設定網路環境,若準備好相關資料的話,再按下任意鍵,以便進入網路環境設定畫面。

NetworkManager TUI
Please select an option
Edit a connection
Activate a connection
Set system hostname
Quit
<0K>

- 5. 其實是進入到一個稱為「NetworkManager TUI」的設定程式,在這個設定程式的操作方式, 先簡單地介紹如下:
 - (1) 移動要選取的欄位或選擇項目:↑↓方向鍵或tab鍵。
 - (2) 選定要選擇的選項:Enter鍵或空白鍵。

以這個主選單為例,您必須選取「Edit a connection」項目,以便進入到設定連線的畫面, 進行設定網路環境。您可將光棒移動到Edit a connection」項目後,按下Enter鍵即可。

6. 接下來在Ethernet選項內,有個「Wired connection 1」項目,也是一樣,按下Enter鍵,進入 到設定畫面。



7. 首先,我們先變更網卡代號,在「Profile name」欄內,將原來的「Wired connection 1」改為您想要的任何代號。為了避免日後忘記,我們建議沿用設備的代號為宜;所以,這個欄 位我們就改為「ens33」。(Virtual Box中,網卡代碼為「enp0s17」)

Edit connection	
Profile name <mark>Wired connection 1</mark> Device 00:0C:29:C5:CE:57 (ens33)	
= ETHERNET	<show></show>
= IPo4 CONFIGURATION <automatic> = IPo6 CONFIGURATION <automatic></automatic></automatic>	<show> <show></show></show>
[X] Automatically connect [X] Available to all users	
	<cancel> <ok></ok></cancel>

8. 接來下要設定IPv4的固定IP及其他相關參數:

請按↑↓方向鍵到「IPv4 CONFIGURATION」欄內的「<Automatic>」項目後,按下Enter鍵, 改選擇「Manual」項目後,再按下Enter鍵。

Edit connection	
Profile name <mark>ens33</mark>	
= ETHERNE	<show></show>
= IPo4 CO Automatic Automatic>	<show></show>
= IPu6 CO Link-Local Automatic>	<show></show>
[X] Autom Shared ect	
[X] Avail sers	
	<cancel> <ok></ok></cancel>

9. 再到「IPv4 CONFIGURATION」欄內的「<Show>」項目後,按下Enter鍵,讓項目變成「<Hide>」,便可將IPv4的各項欄位顯示出來。

	Edit connection	
D = 011 =		
Profile name	ens33	
Device	00:0C:29:C5:CE:57 (ens33)	
= ETHERNET		<show></show>
- IPUA CONFICURATION	(Manual)	ZHIJAN
		KIIIuez
Hadresses	<haa></haa>	
Gateway		
DNS servers	<add></add>	
Search domains	<	
Devetition	(Ne sustant sentes) (E114)	
коптид	(NO CUSTOM FOUTES) (Lait)	
[] Never use this	network for default route	
[X] Reguire IPv4 ad	dressing for this connection	
	(A-1	(01)
- IFUE CONFIGURATION	<hutomatic></hutomatic>	<2nom>
[X] Automatically con	mect	
[X] Available to all	users	
		(Cancel) (OV)

- 接下來的原則是,若該欄位沒有輸入的地方,請在該欄位的「<Add...>」項目按下Enter 鍵,以增加輸入的欄位,再輸入您當地網路環境的參數。若欄位名稱變成紅色,則表示該 欄位輸入錯誤,必須加以修正,否則無法選到右下角的「<OK>」項目。
- 11. 接下來請將剛剛您填好的網路環境各參數,填入這個介面中:



12. 接下來設定IPv6的環境,步驟如同8.~11.,但設定欄位為下半部的「IPv6 CONFIGURATION」。 請您將剛剛填好的網路環境各參數,填入這個介面中



13. 完成後,請選取畫面右下方的「<OK>」項目,按下Enter鍵後,即可回到上個選單畫面。

Ethernet 1 ens33	<add> <edit> <delete></delete></edit></add>
	(Quit)

14. 再選取畫面右下方的「<Quit>」項目,按下Enter鍵後,即可完成網路環境的設定。



15. 接下來再設定主機名稱(FQDN):請再次按任意鍵進入設定畫面。 選取「Set system hostname」項目後,按Enter鍵進入設定主機名稱。



16. 輸入畫面顯示原來預設的主機名稱,在此處,請刪除欄位中所有的文字後,重新輸入您的 主機名稱(完整名稱,FQDN),完成後選「OK」項目後,按Enter鍵完成設定。

Set Hostname	
Hostname localhost.localdomain	
	<cancel> <ok></ok></cancel>
Hostname cns xxxx kh edu tu	

17. 系統會再次跟您確認剛剛輸入的主機名稱是否正確,請選擇「OK」項目後,按下Enter鍵 即可完成設定工作。



18. 接下來,回到原來的畫面後,會看到「Press any key to restart your network....」,請按任意 鍵,以便重啟您的網卡,以便套用新的設定值。



- 19. 再來第二個步驟,重新產生sshd的加密金鑰,並重新啟用sshd服務。您只要按任意建後, 便可自動進行處理。
- 20. 最後步驟(第三步驟),啟動named服務,並設定開機啟動,最後再設定本機防火牆增加 tcp/udp的DNS服務(port 53)。這個步驟也是按任意鍵,系統會自動幫您設定好。
- 21. 好了,終於完成了所有的設定,您的caching DNS Server已經正常在運作了。

caching DNS Server網路環境與DNS功能測試:

接下來我們測試一下網路環境與DNS功能是否正常:

- 以下的所有測試,請帶入您當地虛擬主機的網路環境參數。以下的測試,是以本市某個學 校環境為例,請特別注意。
- 2. 查看網路上的狀態與設定值:

檢查IPv4/IPv6的設定值及NetMask是否跟您填的資料一致?

[root@localhost ~]# ifconfig ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 inet 163.32.119.178 netmask 255.255.255.128 broadcast 163.32.119.255 inet6 fe80::20c:29ff:fe77:7224 prefixlen 64 scopeid 0x20<link> inet6 2001:288:8201:3::178 prefixlen 64 scopeid 0x0<global> ether 00:0c:29:77:72:24 txqueuelen 1000 (Ethernet) RX packets 27038 bytes 16698156 (15.9 MiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 1199 bytes 91872 (89.7 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0 lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 inet 127.0.0.1 netmask 255.0.0.0 inet6 ::1 prefixlen 128 scopeid 0x10<host> loop txqueuelen 0 (Local Loopback) RX packets 18 bytes 1914 (1.8 KiB) RX errors 0 dropped 0 overruns 0 frame 0 TX packets 18 bytes 1914 (1.8 KiB) TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

3. 查看IPv4/IPv6的Gateway設定是否正確:

檢查IPv4/IPv6的Gateway設定值是否與您填的資料一致?

[root@localhost ~]# ip route default via 163.32.119.254 dev ens33 proto static metric 1024 163.32.119.128/25 dev ens33 proto kernel scope link src 163.32.119.178 [root@localhost ~]# ip -6 route unreachable ::/96 dev lo metric 1024 error -101 unreachable ::ffff:0.0.0.0/96 dev lo metric 1024 error -101 2001:288:8201:3::/64 dev ens33 proto kernel metric 256 unreachable 2002:a00::/24 dev lo metric 1024 error -101 unreachable 2002:7f00::/24 dev lo metric 1024 error -101 unreachable 2002:a9fe::/32 dev lo metric 1024 error -101 unreachable 2002:ac10::/28 dev lo metric 1024 error -101 unreachable 2002:c0a8::/32 dev lo metric 1024 error -101 unreachable 2002:e000::/19 dev lo metric 1024 error -101 unreachable 3ffe:ffff::/32 dev lo metric 1024 error -101 fe80::/64 dev ens33 proto kernel metric 256 default via 2001:288:8201:3::1 dev ens33 proto static metric 1024

4. 測試IPv4 Gateway是否暢通:

測試虛擬機到IPv4 Gateway之間,網路是否正常?

[root@localhost ~]# **ping -c 5 163.32.119.254** PING 163.32.119.254 (163.32.119.254) 56(84) bytes of data. 64 bytes from 163.32.119.254: icmp_seq=1 ttl=64 time=18.8 ms 64 bytes from 163.32.119.254: icmp_seq=2 ttl=64 time=45.2 ms 64 bytes from 163.32.119.254: icmp_seq=3 ttl=64 time=36.3 ms 64 bytes from 163.32.119.254: icmp_seq=4 ttl=64 time=31.9 ms 64 bytes from 163.32.119.254: icmp_seq=5 ttl=64 time=99.9 ms

--- 163.32.119.254 ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4004ms rtt min/avg/max/mdev = 18.845/46.470/99.947/28.062 ms

5. 測試IPv6 Gateway是否暢通:

測試虛擬機到IPv6 Gateway之間,網路是否正常?

[root@localhost ~]# **ping6 -c 5 2001:288:8201:3::1** PING 2001:288:8201:3::1(2001:288:8201:3::1) 56 data bytes 64 bytes from 2001:288:8201:3::1: icmp_seq=1 ttl=64 time=1.66 ms 64 bytes from 2001:288:8201:3::1: icmp_seq=2 ttl=64 time=1.87 ms 64 bytes from 2001:288:8201:3::1: icmp_seq=3 ttl=64 time=1.16 ms 64 bytes from 2001:288:8201:3::1: icmp_seq=4 ttl=64 time=1.60 ms 64 bytes from 2001:288:8201:3::1: icmp_seq=5 ttl=64 time=1.22 ms

--- 2001:288:8201:3::1 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4008ms rtt min/avg/max/mdev = 1.161/1.503/1.872/0.273 ms

6. 測試IPv4對外是否暢通:

測試虛擬機IPv4到Internet的網路是否正常?

[root@localhost ~]# **ping -c 5 8.8.8.8** PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data. 64 bytes from 8.8.8.8: icmp_seq=1 ttl=48 time=18.8 ms 64 bytes from 8.8.8.8: icmp_seq=2 ttl=48 time=19.5 ms 64 bytes from 8.8.8.8: icmp_seq=3 ttl=48 time=18.6 ms 64 bytes from 8.8.8.8: icmp_seq=4 ttl=48 time=19.2 ms 64 bytes from 8.8.8.8: icmp_seq=5 ttl=48 time=17.6 ms

--- 8.8.8.8 ping statistics ---5 packets transmitted, 5 received, 0% packet loss, time 4008ms rtt min/avg/max/mdev = 17.613/18.774/19.507/0.660 ms

7. 測試IPv6對外是否暢通:

測試虛擬機IPv6到Internet的網路是否正常?

[root@localhost ~]# ping6 -c 5 www.hinet.net
PING www.hinet.net(2001:b000:180:3::8011) 56 data bytes
64 bytes from 2001:b000:180:3::8011: icmp_seq=1 ttl=55 time=130 ms
64 bytes from 2001:b000:180:3::8011: icmp_seq=2 ttl=55 time=152 ms
64 bytes from 2001:b000:180:3::8011: icmp_seq=3 ttl=55 time=150 ms
64 bytes from 2001:b000:180:3::8011: icmp_seq=4 ttl=55 time=133 ms
64 bytes from 2001:b000:180:3::8011: icmp_seq=5 ttl=55 time=131 ms

--- www.hinet.net ping statistics ---

5 packets transmitted, 5 received, 0% packet loss, time 4005ms rtt min/avg/max/mdev = 130.772/139.742/152.624/9.672 ms

8. 測試caching DNS服務是否正常:

測試DNS功能是否正常,我們在此測試portal.kh.edu.tw的IPv4/IPv6及nodnssec/dnssec的正 解交叉測試。

[root@localhost ~]# dig	@127.0).0.1 pc	ortal.kh.ec	lu.tw a	
; <<>> DiG 9.9.4-RedHat- ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode ;; flags: qr rd ra ad; QUE	9.9.4-14. :: QUERY, RY: 1, ANS	el7 <<>> status: I SWER: 1	@127.0.0.1 NOERROR, id , AUTHORIT	portal.kh.edu.tw a d: 56378 Y: 5, ADDITIONAL: 1	
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: ;; QUESTION SECTION: ;portal.kh.edu.tw.	udp: 409	in	A		
:: ANSWER SECTION:					
portal.kh.edu.tw.	7200	IN	Α	163.16.1.40	
;; AUTHORITY SECTION: kh.edu.tw. kh.edu.tw. kh.edu.tw. kh.edu.tw. kh.edu.tw.	7200 7200 7200 7200 7200 7200	IN IN IN IN	NS NS NS NS	dns1.kh.edu.tw. ns.ks.edu.tw. dwb.ks.edu.tw. dns2.kh.edu.tw. dns.kh.edu.tw.	
;; Query time: 50 msec ;; SERVER: 127.0.0.1#53(;; WHEN: 二 12月 02 1 ;; MSG SIZE rcvd: 155 [root@localhost~]# dig	127.0.0.1 1:55:41 C @127.0) ST 2014).0.1 pc	ortal.kh.ec	lu.tw aaaa	
; <<>> DiG 9.9.4-RedHat- ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode ;; flags: qr rd ra ad; QUE	9.9.4-14. e: QUERY, RY: 1, AN	el7 <<>> status: I SWER: 1	@127.0.0.1 NOERROR, id , AUTHORIT	portal.kh.edu.tw aaaa d: 6537 Y: 5, ADDITIONAL: 1	
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: ;; QUESTION SECTION: :portal kh edu tw	udp: 409	16 INI			
;; ANSWER SECTION: portal.kh.edu.tw.	7200	IN	ΑΑΑΑ	2001:288:8401::40	
;; AUTHORITY SECTION: kh.edu.tw. kh.edu.tw. kh.edu.tw. kh.edu.tw. kh.edu.tw. kh.edu.tw.	7196 7196 7196 7196 7196 7196	IN IN IN IN	NS NS NS NS	dns.kh.edu.tw. dns2.kh.edu.tw. dwb.ks.edu.tw. dns1.kh.edu.tw. ns.ks.edu.tw.	

;; Query time: 2 msec ;; SERVER: 127.0.0.1#53(1 ;; WHEN: 二 12月 02 11	27.0.0.1) :55:45 CST	2014				
;; MSG SIZE rcvd: 167						
[root@localhost ~]# dig @127.0.0.1 portal.kh.edu.tw a +dnssec						
; <<>> DiG 9.9.4-RedHat-9 ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: ;; flags: qr rd ra ad; QUER	.9.4-14.el QUERY, st Y: 1, ANSV	7 <<>> @ atus: NC VER: 2, <i>I</i>	2127.0.0.1 DERROR, id	portal.kh.edu.tw a +dnssec : 11359 : 6, ADDITIONAL: 1		
;; OPT PSEUDOSECTION: ; EDNS: version: 0, flags: d ;; QUESTION SECTION: ;portal.kh.edu.tw.	o; udp: 40 I	96 N	A			
;; ANSWER SECTION: portal.kh.edu.tw. portal.kh.edu.tw. kh.edu.tw. htsFGiSc9Limr H1nGjFHgMt38f7PyNBVg; vLMJxOOOBmi94V1iUSM	7190 7190 ptQaRZBC Xa6j+koM sLviKOXP{	IN IN DpHQEZ! LMGJKN 3W0nim	A RRSIG 52HXBCUK /JJ2lLvfTPu kvPf68eVe	163.16.1.40 A 7 4 7200 20241124012842 20141127002842 11610 SCT1q/EPV/Tv14AnN0XWR5 VCTk1W87KkG7m v/UeTc5ShxtKUx		
JDhnJzh1QNYvIP2mZYWC TNdBOXsQOqC+tvjwVFA/ R7ftfPc0WkEG/ohihqacsn	Ja1BeJ6d rzn191jllS nu5UZVyg	Z+/68Yz iMAqX/ı jc4ovBS	UKWLYTU1 n6bwDyWy OYZECapbo	JHYjGvZzTG5xx9 J3G8VCO7OIIIj7 JEd0MFpdt+d6 SNuByA==		
;; AUTHORITY SECTION:						
kh.edu.tw.	7190	IN	NS	dns1.kh.edu.tw.		
kh.edu.tw.	7190	IN	NS	dwb.ks.edu.tw.		
kh.edu.tw.	7190	IN	NS	ns.ks.edu.tw.		
Kh.edu.tw.	7190		NS	dns.kn.edu.tw.		
kn.edu.tw	7190	IN	RRSIG	UNSZ.KN.edu.lw. NS 7 3 7200 20241124012842 20141127002842 11610		
kh.edu.tw. RBIe0WBq7Md Cw/8nxYoWOZrNLA4NVO0 SknKZNtPuoWNY1jh1/xGp TgFJ16l+7S1ECQ+2XGa75k tEJCLLDKfUy0ZHz0AVSij/X uCF/VGOFAy1Mo/39WJsV	ffEQeA8/a CU486/Dk GI/87BHc kdh+1Xja5 F9OzZHNI w+i+PdFIS	am56VlC C79NY3 E75MNy 5BlxATv/ 6Hv79ib Gryap5Qz	2nl1wJLxrrE 1l79u32mb /liU24eIJOr Bos8RAbU(xVkKzALY9 zbhp3BZMv	YRfZLksXlFoihv/Huryo Tivsbky77wwRDX ne07mDFU9fzT Cm9IHalGdA fo2+MjHvo wcNyYNwYODKi/ 16dMrw==		
;; Query time: 0 msec ;; SERVER: 127.0.0.1#53(1 ;; WHEN: 二 12月 02 11 ;; MSG SIZE rcvd: 749	27.0.0.1) :55:51 CST	2014				
[root@localhost ~]# dig (⊉127.0.().1 por	tal.kh.ed	u.tw aaaa +dnssec		
; <<>> DiG 9.9.4-RedHat-9 ; (1 server found) ;; global options: +cmd ;; Got answer: ;; ->>HEADER<<- opcode: ;; flags: qr rd ra ad; QUER	.9.4-14.el7 QUERY, st Y: 1, ANSV	7 <<>> @ atus: NC VER: 2, <i>F</i>	2127.0.0.1 DERROR, id	portal.kh.edu.tw aaaa +dnssec : 30828 : 6, ADDITIONAL: 1		

;; OPT PSEUDOSECTION:				
; EDNS: version: 0, flags:	do; udp: 4	1096		
;; QUESTION SECTION:				
;portal.kh.edu.tw.		IN	AAAA	
;; ANSWER SECTION:				
portal.kh.edu.tw.	7190	IN	ΑΑΑΑ	2001:288:8401::40
portal.kh.edu.tw.	7190	IN	RRSIG	AAAA 7 4 7200 20241124012842 20141127002842
11610 kh.edu.tw. EKu2F	nsrmpP0n	nQ7mvl	cz25j4AejzTA	FECHxRDCKQxaPXtyf/Lk3o/yvEb
XXU7T54rE3m+T9qzRY4	VVj/dc32	fcEv3BK	ktrkXZPOI7d	XI1Ica947ze
7uInsOIPImsBIXexS+J4b	93j3EP/O>	(CwUYw	/GaCNjAK2yl	.Hywas/kh+yu
oZqa3sYrkxac7qPjO/v2t	orsvDAETU	IK/OZfx	em+ixA2V55	mODzeuQ80yD
i5Wi0EQQ8KbnY7VMy4	crM4FFLX	az <mark>7idH</mark> r	jVEcGbj21Ikr	m46ObdbuBYe
FJfYuVIvtSiaikuyDK59KB	SvSm/cxBD	SIhdc7	dm2HQQLtvl	<pre>Kn1zyvRHqC0 RR2mBg==</pre>
;; AUTHORITY SECTION:				
kh.edu.tw.	7186	IN	NS	ns.ks.edu.tw.
kh.edu.tw.	7186	IN	NS	dns.kh.edu.tw.
kh.edu.tw.	7186	IN	NS	dns2.kh.edu.tw.
kh.edu.tw.	7186	IN	NS	dns1.kh.edu.tw.
kh.edu.tw.	7186	IN	NS	dwb.ks.edu.tw.
kh.edu.tw.	7186	IN	RRSIG	NS 7 3 7200 20241124012842 20141127002842 11610
kh.edu.tw. RBIe0WBq7N	1dffEQeA8	/am56V	lCnl1wJLxrrD	9YRfZLksXlFoihv/Huryo
Cw/8nxYoWOZrNLA4NV	OCU486/D	kC79NY	31l79u32mb	Tivsbky77wwRDX
SknKZNtPuoWNY1jh1/x0	GpGI/87BH	IcE75MI	NyliU24eIJOn	ne07mDFU9fzT
TgFJ16l+7S1ECQ+2XGa75	5kkdh+1Xja	a5BlxAT\	//Bos8RAbU0	Cm9IHaIGdA
tEJCLLDKfUyOZHz0AVSij,	/XF9OzZHI	NI6Hv79	ibxVkKzALY9	fo2+MjHvo
uCF/VGOFAy1Mo/39WJs	sVw+i+PdF	ISryap50	Qzbhp3BZMv	vcNyYNwYODKi/ 16dMrw==
;; Query time: 0 msec				
;; SERVER: 127.0.0.1#53	(127.0.0.1)			
;; WHEN: 二 12月 02 1	.1:55:55 C	ST 2014		
;; MSG SIZE rcvd: 761				

9. 再來,請由貴校別台電腦,測試該部虛擬主機是否正常運作中:

測試順序為:

(1)虛擬機IPv4 IP

(2)虛擬機IPv6 IP

(3)查詢虛擬機DNS正解(IPv4介面查詢)

(4)查詢虛擬機DNS正解(IPv6介面查詢)

C:\Users\jang>ping 163.32.119.178

Ping 163.32.119.178 (使用 32 位元組的資料):
回覆自 163.32.119.178: 位元組=32 time<1ms TTL=64
回覆自 163.32.119.178: 位元組=32 time<1ms TTL=64
回覆自 163.32.119.178: 位元組=32 time<1ms TTL=64
I0覆自 163.32.119.178: 位元組=32 time<1ms TTL=64
163.32.119.178 的 Ping 統計資料:
 封包: 已傳送 = 4, 已收到 = 4, 已遺失 = 0 (0% 遺失),
大約的來回時間 (毫秒):
 最小值 = 0ms, 最大值 = 0ms, 平均 = 0ms</pre>

C:\Users\jang>ping 2001:288:8201:3::178
Ping 2001:288:8201:3::178 (使用 32 位元組的資料):
回覆自 2001:288:8201:3::178: time<1ms
2001:288:8201:3::178 的 Ping 統計資料:
封包:已傳送 =4,已收到 =4,已遺失 =0(0% 遺失),
大約的來回時間 (毫秒):
最小值 = 0ms,最大值 = 0ms,平均 = 0ms
C:\Users\jang>nslookup www.google.com.tw 163.32.119.178
伺服器: office178.kiec.kh.edu.tw
Address: 163.32.119.178
未經授權的回答:
名稱: www.google.com.tw
Addresses: 2404:6800:4008:c02::5e
74.125.23.94
C:\Users\jang> nsiOokup www.googie.com.tw 2001:288:8201:3::178 伺服哭·Unknown
Address: 2001.288.8201.3178
未經授權的回答:
名稱: www.google.com.tw
Addresses: 2404:6800:4008:c02::5e
74.125.23.94

- 10. 若以上測試都成功,那恭喜您,這台虛擬機已經架設成功,並正常運作中。
- 11. 接下來,請將校內所有電腦的DNS查詢主機,優先設這台caching Name Server的IPv4/IPv6 IP,以加快校內DNS查詢的速度與效率。

因為這個虛擬機是由中心這邊先行安裝完成的,為了簡單方便設定使用,所以將一些安全性的設定先取消;若您測試安裝完成的虛擬機是正常了,接下來就要將系統調校安全一點了。

以下是一定要處理的安全設定:

更改系統預設的密碼:包含root及dnsuser這個帳號的密碼,都一定要變更;要不然看過這份文件的人,都知道預設的帳號與密碼是什麼,很容易登進去的。
 以root身份登入系統後,先改root密碼;成功後,再改dnsuser的密碼。

[root@localhost ~]# passwd 更改使用者 root 的密碼。 新 密碼: 再次輸入新的 密碼: passwd:所有驗證 token 都已成功更新。 [root@localhost ~]# passwd dnsuser 更改使用者 dnsuser 的密碼。 新 密碼: 再次輸入新的 密碼: passwd:所有驗證 token 都已成功更新。

2. 新增管理者常用的帳號與密碼。

[root@localhost~]**# adduser testuser** [root@localhost~]**# passwd testuser** 更改使用者 testuser 的密碼。 新 密碼: 再次輸入新的 密碼: passwd:所有驗證 token 都已成功更新。

- 關閉root身份登入ssh的功能: 請修改/etc/ssh/sshd_config檔,將 #PermitRootLogin yes 改為 PermitRootLogin no 完成後,再重新啟動sshd。 systemctl restart sshd.service
- 設定將系統記錄及訊息,寄發到您的email信箱。
 sed -i 's/#root:\t\tmarc/root:\t\t您的email地址/g'

new aliases

[root@localhost ~]# sed -i 's/#root:\t\tmarc/root:\t\tuser@mail.xxx.kh.edu.tw/g' /etc/aliases [root@localhost ~]# newaliases

5. 手動更新系統套件:

[root@localhost ~]# yum -y update Loaded plugins: fastestmirror, langpacks Loading mirror speeds from cached hostfile

```
* rpmforge: ftp.riken.jp
No packages marked for update
```

6. 完成以上的設定後,應可安全地讓這台虛擬機正常地運作至實體機器不能在用為止。它每 天會自動更新系統套件,並查檢kernel是否有昇版,若kernel版本昇級後,系統也會自動重 新開機。原則上,這台虛擬機並不需要太多的觀看與照顧,只要管理者定期去收取系統寄 出來的信件,及定期登入系統檢查下功能是否正常即可。

常用系統的操作命令:

- 1. 關閉主機: systemctl poweroff
- 2. 重新開機: systemctl reboot
- 重設網路環境與主機名稱: nmtui
- 4. 關閉named服務

systemctl stop named-chroot

- 5. 重新啟動named服務 systemctl restart named-chroot
- 6. 查詢named的狀態: rndc status

系統的調校:

原則上這個規格的虛擬器應足以應付24-64班左右的全校電腦查詢使用,若發現系統效能不足 或記憶體不足;您可以進行虛擬機的調校:

- 1. 記憶體部份,您可以在關機後,重新設定虛擬器的記憶體容量。先試著將記憶體調至2G 後,再觀察1-2週看看,不足的話,再往上調整。
- 2. CPU部份,若覺得1顆CPU不夠的話,可試著將CPU調成2顆。但CPU的顆數(核心數)是跟 named的執行參數有關,若您將CPU調成2顆(核心),您必須在開機後,做以下的修改:
 - 修改設定檔 /etc/sysconfig/named 在檔尾增加一行 OPTIONS="-n 2"
 - (2) 完成後存檔。
 - (3) 重新啟動named服務:

systemctl restart named-chroot.service

3. 調校後,您可利用rndc命令觀察named的狀況:

[root@localhost ~]# **rndc status** version: 9.9.4-RedHat-9.9.4-14.el7 <id:8f9657aa> CPUs found: 1 worker threads: 1 UDP listeners per interface: 1 number of zones: 6 debug level: 0 xfers running: 0 xfers deferred: 0 soa queries in progress: 0 query logging is OFF recursive clients: 0/0/1000 tcp clients: 0/100 server is up and running

以上,希望這份文件對貴校的DNS服務有幫助,若有任何問題,請逕洽中心網路管理組。