

# 用PVE處理資安事件DFIR實戰經驗



# 講師介紹

專長: 硬體資安 資料恢復 數位鑑識  
儲存嵌入式系統開發與恢復  
Maker&Hacker

OSSLab 開放軟體實驗室創辦人

演講經歷:

HITCON 2012, 2015

HITCON Pacific 2017

2018 台灣資安高峰會

2019 IT home 資安大會



# 近期有不少台灣大型上市櫃公司遭駭

駭客入侵台灣10大企業！研華慘遭勒索10億  
仁寶認栽付千萬贖金

ETtoday新聞雲



▲研華董事長劉克振近年持續推動物聯網，但公司伺服器在11月19日也證實被駭客針對性地入侵。（圖 / CTWANT提供）

仁寶遭到駭客攻擊，「事發後，仁寶以備份系統還原後，就查不出DoppelPaymer最初的入侵手法及潛伏時間。」「聽說DoppelPaymer提供的錢包已入帳28枚比特幣（約新台幣1,400萬元），就在仁寶被駭後1周。」

新聞來源: <https://finance.ettoday.net/news/1872347>

# 不想承認但這些都是事實

Bitcoin Address: bc1q2se6clfqgnlcvnajz8aljsmp

### General info

Address

Balance

Last seen receiving

**Total received**  
28.37069317 BTC / 500,448.84 USD

**First / last seen receiving**  
14 days ago / 14 days ago

Address type: witness\_v0\_scripthash

Script: 0 5433ac7d320227fc327d908fdca1b0cceec67a7 [OP] [Bin] [Hex]

Transaction count: 2

Output count / Unspent output count: 1 / 0

- Amount to pay (in Bitcoin): **1100 BTC or 1055.6759 BTC** if you decide to pay in 01 days 07h:54m:48s .
- Contact email: F...@protonmail.com
- Use chat in the right bottom of this page to contact us. You have 48 hours to get discount opportunity.

It may take us a few hours to reply. You may also need to refresh this page in tor browser.

To show you that our decryptor works we will unlock a couple of your files as an example.

For this to happen you need to pack a ZIP with 2 pairs of your unique files: *somefile1.dopeled* and *somefile1.how2decrypt.txt* & *somefile2.dopeled* and *somefile2.how2decrypt.txt* which have no sensitive information but only you own them, and send them to us.

Huge amount of data exfiltrated from you will be published in 2-3 weeks if no co **Online cha** made.

當初被勒索 **1100 BTC**, 約台幣5億

仁寶後來支付 **28 BTC**, 約 50萬美元(台幣1400多萬元)

# 當遇到時該做的應對 DFIR

Digital Forensics and Incident Response  
要數位鑑識，也要應變反應

DF = 數位鑑識

IR = 即時回應

降低損失、回復正常



DFIR目的是找出受害的根源與原因  
並且快速應對這狀況 將服務恢復上線

進程分析

工具排查

網路排查

文件排查

後門排查

應急溯源

Windows應急

Web伺服器日誌分析

中間件伺服器日誌分析

資料庫伺服器日誌分析

作業系統日誌分析

安全產品日誌分析

日誌分析

進程分析

工具排查

網路排查

文件排查

後門排查

應急溯源

Linux應急

# 資料無價

一般資安公司不太想面對這問題  
但還是很重要

因為還是會有這樣況：

    備份的不夠完整

    備份還原時間太長

還是會有可能遇到

    需要資料救援手段

    或跟駭客談判付費狀況



# 沒備份恢復計畫或外包

## 重建資料成本

- > 評估資料是否重要
- > 自行重建需要多少時間和人力

## 要找外包商嗎？

- > 建構資料恢復環境需要多少時間
- > 勒索病毒中招後的時間壓力

## 恢復資料手段

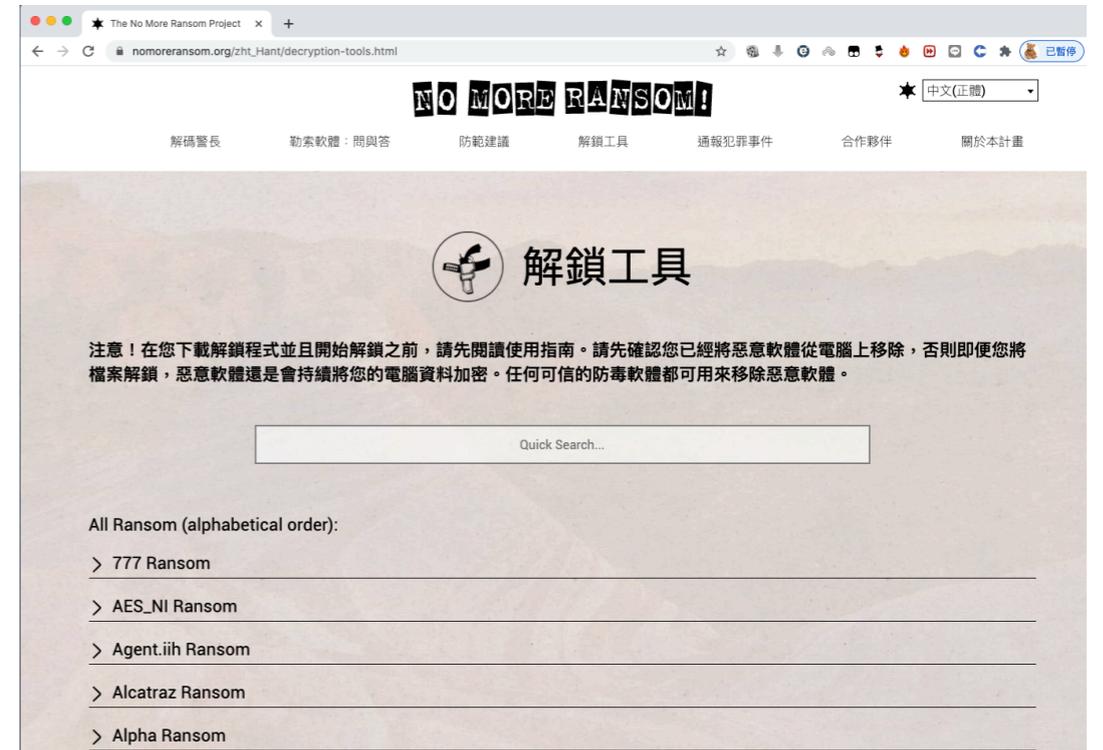
- > 以資料救援手段恢復
- > 付款駭客解密做的資料回復

# 遇到勒索病毒的第一時間狀況

1. 拔掉網路線
2. 盡量取得記憶體 DUMP, 或快照
3. 關不關機風險
4. 網路隔離
5. 如果要只能選擇走駭客解密路線.  
建議外包商可能報價.

判定勒索病毒類型 已有現成工具

[https://www.nomoreransom.org/zht\\_Hant/partners.html](https://www.nomoreransom.org/zht_Hant/partners.html)



# 恢復計畫或外包

PROVEN  
DATA

Proven Data 這間公司聲稱透過他們「最新研發的技術」，承諾他們可以幫助客戶恢復被勒贖的資料，幫他們解鎖。

Contact

REAS



## Data Recovery

We've recovered data from all major hard drive & server manufacturers and all data loss scenarios. We pride ourselves on industry leading success rates of 98%!



## Cyber Security

We know how to prevent cyber attacks because we've provided support for thousands of cyber incidents. Let us help you protect your business with industry leading tools and



## Digital Forensics

Certified digital forensic examiners experienced in investigations for ransomware, data breaches, and employee misconduct.



## Ransomware Recovery

As one of the first companies that helped with ransomware recovery, rest assured that we have the experience to get you up and running fast!

# 應變勒索攻擊資安事件的能力

- 病毒分析
- 安全日誌分析
- 安全工具與腳本開發
- 網路安全分析
- 關聯分析
- 記憶體分析
- 加密類型與檔案系統評估資料恢成功性
- 評估與駭客團隊談判成功性與價位

# 外包商的職責

1. 不從駭客中獲得密鑰 以資料恢復手段  
> 拯救資料成功性 完整性 時效性
2. 萬一要付款給勒索方 判定此案成功性.  
> 駭客組織是否有誠信 解密程式是否有漏洞可以用

萬一撕票後？

誠信的外包若遇到撕票 還有啥方法？

# 資料恢復手段 Raw Recovery

Hex搜索Magic Number,再擷取box size存取檔案

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	00	00	00	20	66	74	79	70	71	74	20	20	20	05	03	00	ftypqt
00000010	71	74	20	20	00	00	00	00	00	00	00	00	00	00	00	00	qt
00000020	00	00	00	08	77	69	64	65	00	31	CA	34	6D	64	61	74	wide 1É4mdat
00000030	00	00	01	B0	01	00	00	01	B5	89	13	00	00	01	00	00	° μI

Diagram labels with arrows pointing to specific hex values:

- Box Size: points to 00 at offset 0
- Compatible Brand: points to 08 at offset 2
- Type: points to 66 at offset 4
- Major Brand: points to 71 at offset 8
- Minor Version: points to 05 at offset C

# MDF 碎片恢復法

最重要的為 16-21 NextPage ID 跟32-35 PageID

```
0 / 8 9 A B C D E F ANSI ASCII
:0 30 00 0C 00 E9 8C 3E 01 DA 00000000 éG> Ú
:0 09 00 2A 00 2E 00 33 00 37 ¥ * . 3 7
:0 4B 00 54 00 49 4E 53 45 52 B F K K T INSE
:F 50 54 48 32 33 31 20 32 30 TN002COPHTH231 20
:0 33 37 30 30 30 35 54 48 30 1604010370005TH0
:0 30 30 30 30 30 00 0C 00 02 1228.0000000
:0 0A 00 00 00 09 00 2A 00 2E > Ú¥ * .
:0 46 00 4B 00 4B 00 55 00 49 3 7 B F K K U I
:0 30 32 43 4F 50 54 48 32 33 NSERTN002COPHTH23
:0 34 30 31 30 33 37 30 30 30 1 20160401037000
:1 30 30 2E 30 30 30 30 30 30 6TH012100.000000
:E 01 DA A5 00 00 0A 00 00 00 0 > Ú¥
:3 00 37 00 42 00 46 00 4B 00 * . 3 7 B F K
:3 45 52 54 4E 30 30 32 43 4F K T INSERTN002CO
:0 32 30 31 36 30 34 30 31 30 PTH231 201604010
:4 48 30 31 32 33 35 2E 30 30 370007TH01235.00
:C 00 38 8D 3E 01 DA A5 00 00 00000 8 > Ú¥
:A 00 2E 00 33 00 37 00 42 00 * . 3 7 B
:4 00 49 4E 53 45 52 54 4E 30 F K K T INSERTN0
:8 32 33 31 20 32 30 31 36 30 02COPHTH231 20160
:0 30 30 38 54 48 30 31 32 37 4010370008TH0127
:0 30 30 00 0C 00 51 8D 3E 01 5.0000000 Q >
:0 00 09 00 2A 00 2E 00 33 00 Ú¥ * . 3
:B 00 4B 00 55 00 49 4E 53 45 7 B F K K U INSE
:3 4F 50 54 48 32 33 31 20 31 RTN002COPHTH231 1
:1 30 33 37 30 30 30 39 54 48 01604010370009TH
:E 30 30 30 30 30 30 00 0C 012450.0000000
:5 00 00 0A 00 00 00 09 00 2A G&@ Ú¥ *
:0 42 00 46 00 4B 00 4B 00 55 . 3 7 B F K K U
:4 4E 30 30 32 43 4F 50 54 48 INSERTN002COPHTH
:1 36 30 34 30 31 30 33 38 30 231 201604010380
:1 32 31 31 37 2E 30 30 30 30 001TH012117.0000
:1 F0 40 01 DA A5 00 00 0A 00 000 a&@ Ú¥
:E 00 33 00 37 00 42 00 46 00 * . 3 7 B F
:9 4E 53 45 52 54 4E 30 30 32 K K T INSERTN002
:3 31 20 32 30 31 36 30 34 30 COPHTH231 2016040
:0 32 54 48 30 31 32 33 39 2E 10380002TH01239.
:0 00 0C 00 7B F0 40 01 DA A5 6000000 {&@ Ú¥
:9 00 2A 00 2E 00 33 00 37 00 * . 3 7
:B 00 54 00 49 4E 53 45 52 54 B F K K T INSERT
:0 54 48 32 33 31 20 32 30 31 N002COPHTH231 201
:3 38 30 30 30 33 54 48 30 31 604010380003TH01
:0 30 30 30 00 0C 00 97 F0 239.6000000 -&
:A 00 00 00 09 00 2A 00 2E 00 @ Ú¥ * .
:6 00 4B 00 4B 00 54 00 49 4E 3 7 B F K K T IN
:0 32 43 4F 50 54 48 32 33 31 SERTN002COPHTH231
```

Bytes	Content
00	HeaderVersion (tinyint)
01	Type (tinyint)
02	TypeFlagBits (tinyint)
03	Level (tinyint)
04-05	FlagBits (smallint)
06-07	IndexID (smallint)
08-11	PreviousPageID (int)
12-13	PreviousFileID (smallint)
14-15	Pminlen (smallint)
16-19	NextPageID (int)
20-21	NextPageFileID (smallint)
22-23	SlotCnt (smallint)
24-27	ObjectID (int)
28-29	FreeCnt (smallint)
30-31	FreeData (smallint)
32-35	PageID (int)
36-37	FileID (smallint)
38-39	ReservedCnt (smallint)
40-43	Lsn1 (int)
44-47	Lsn2 (int)
48-49	Lsn3 (smallint)
50-51	XactReserved (smallint)
52-55	XdesIDPart2 (int)
56-57	XdesIDPart1 (smallint)
58-59	GhostRecCnt (smallint)
60-63	Checksum/Tornbits (int)



# 最重要的是全硬碟備份

Clone Disk (Copy Sectors) ✕

Source: medium    
[mod1-1.dd] (1.4 MB)

Destination: medium    
Removable medium 1, USB v2.0Flash Disk (1

Copy entire medium

Start sector (source):

Start sector (destination):

Number of sectors to copy:

Log procedure silently (no error messages)  Avoid damaged areas. Skip range:

Write pattern for damaged source sectors:

Simultaneous I/O (faster, if source and destination are different physical media)

# 全硬碟備份

- 實體主機備份
  - 獨立硬碟 (dd/raw, image)
  - 針對RAID 硬體Pool (dd/raw, d01, e01)
  - LVM後的分區
- VM格式檔案備份
  - PVE (dd/raw, qcow2)
  - Windows (vhd, vhdx)
  - VMware (vmdk)

# 全硬碟備份必備工具

- 必需準備**全硬碟備份必備工具**
- 用其他媒體來開機, 以免動到原先硬碟資料

## 1. BOSS Card (OS開機碟)

- 安裝兩支SATA SSD, Windows OS預先安裝好
- 個別設定成Legacy BIOS與UEFI模式開機



## 2. Ventoy (高速多OS開機隨身碟)

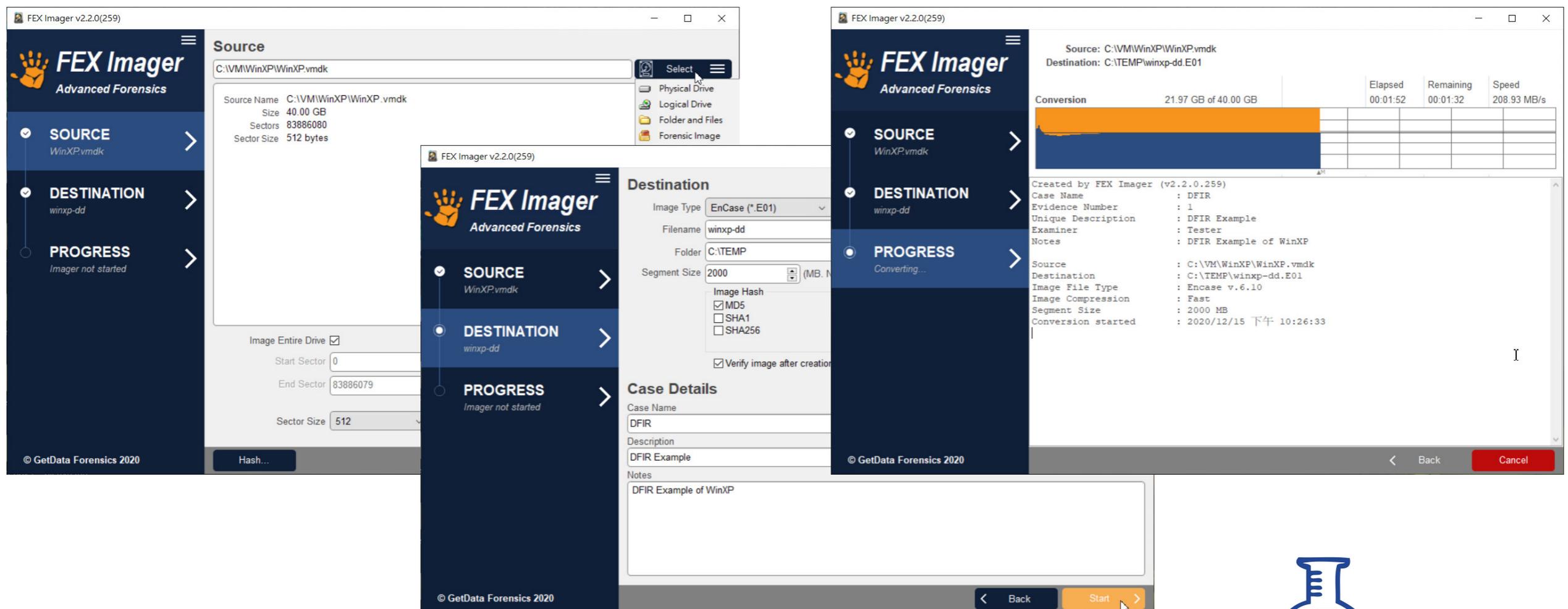
- 可直接支援多個ISO檔案開機, 圖形選單好用
- 要有WinPE 開機系統 (處理Windows 相關 OS)
- 建議有Parted Magic 維護系統 (處理Linux 相關 OS)



# 必備的磁碟影像製作/轉換工具

FEX Imager: 一套免費影像檔製作/轉換工具 (推薦)

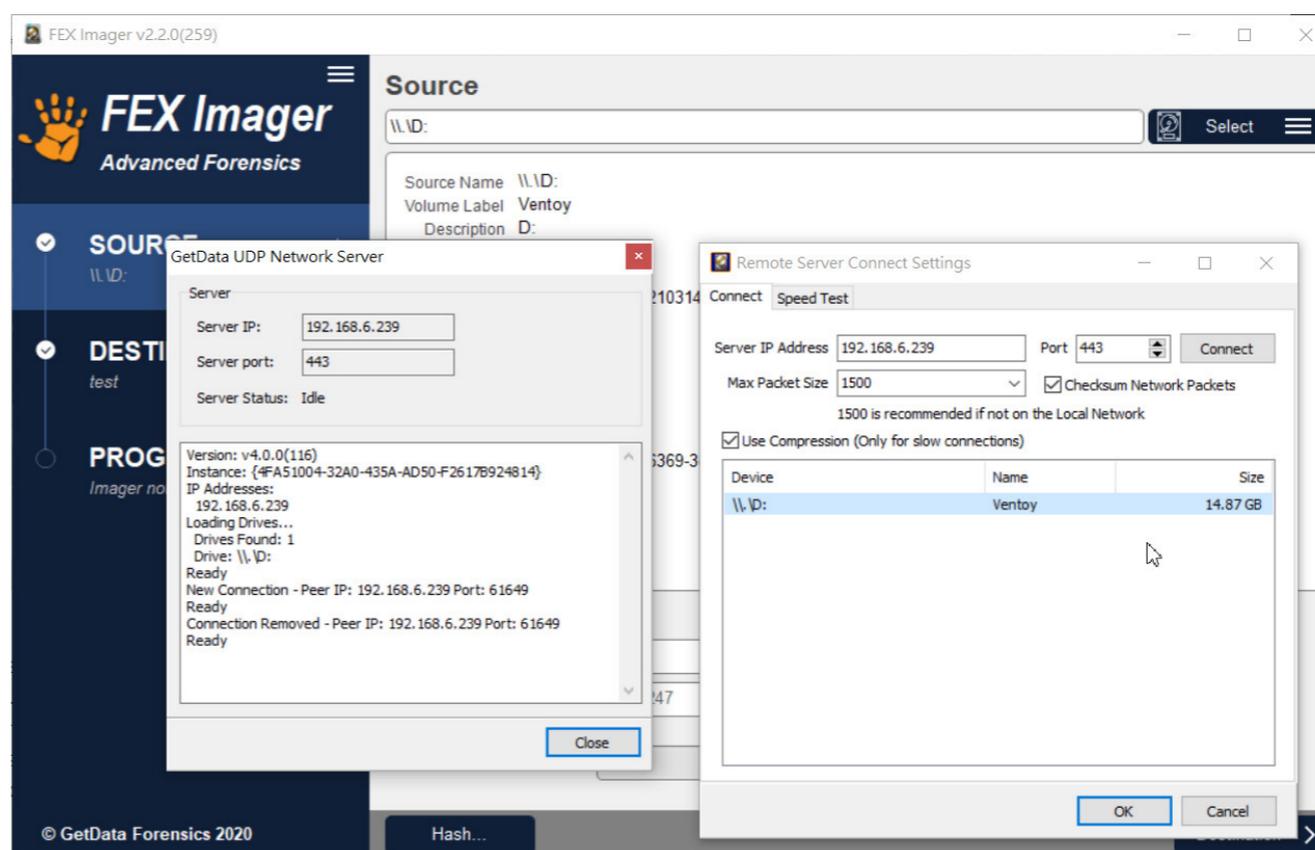
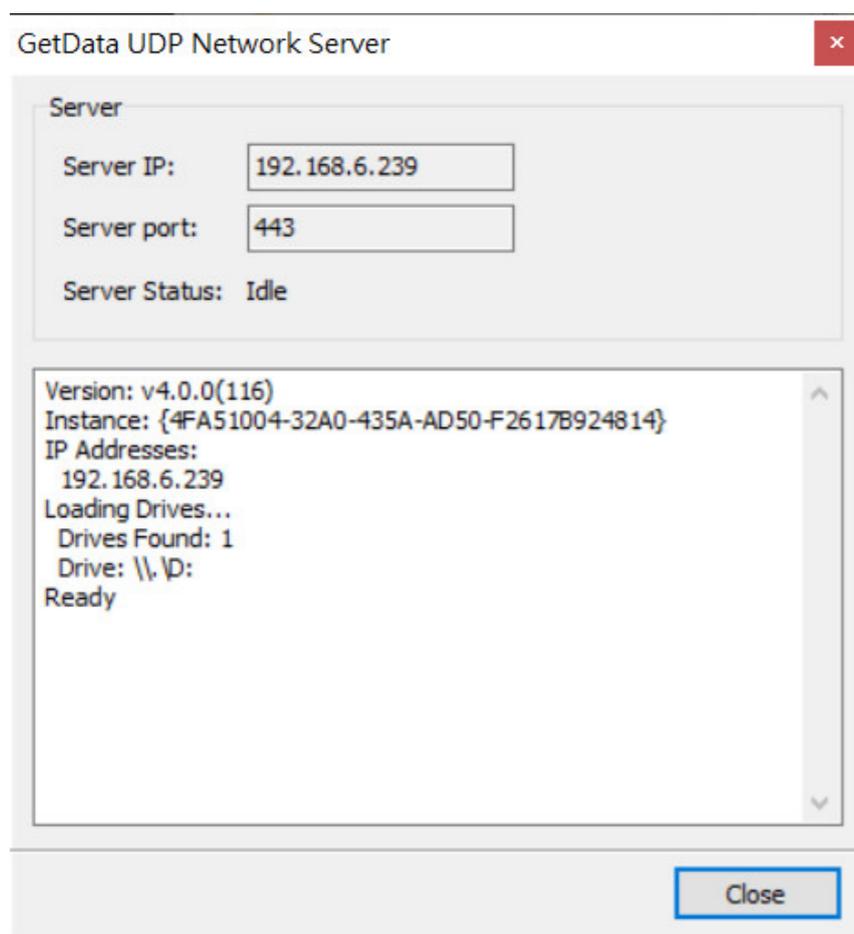
- 支援 實體/邏輯磁碟機/檔案目錄/鑑定影像檔/網路磁碟
- 支援完整md5/sha1/sha256 hash認證
- 可以轉換成 dd/raw 檔案 -



Local模式: 建立Disk Image

# 支援遠端鏡像軟體

- FEX Imager:** 一套免費影像檔製作/轉換工具 (推薦)
- 遠端模式建Image，被dump者可先執行Servlet
  - Client端可以透過連接該IP，來dump 遠端的磁碟機



Remote模式: 建立Disk Image

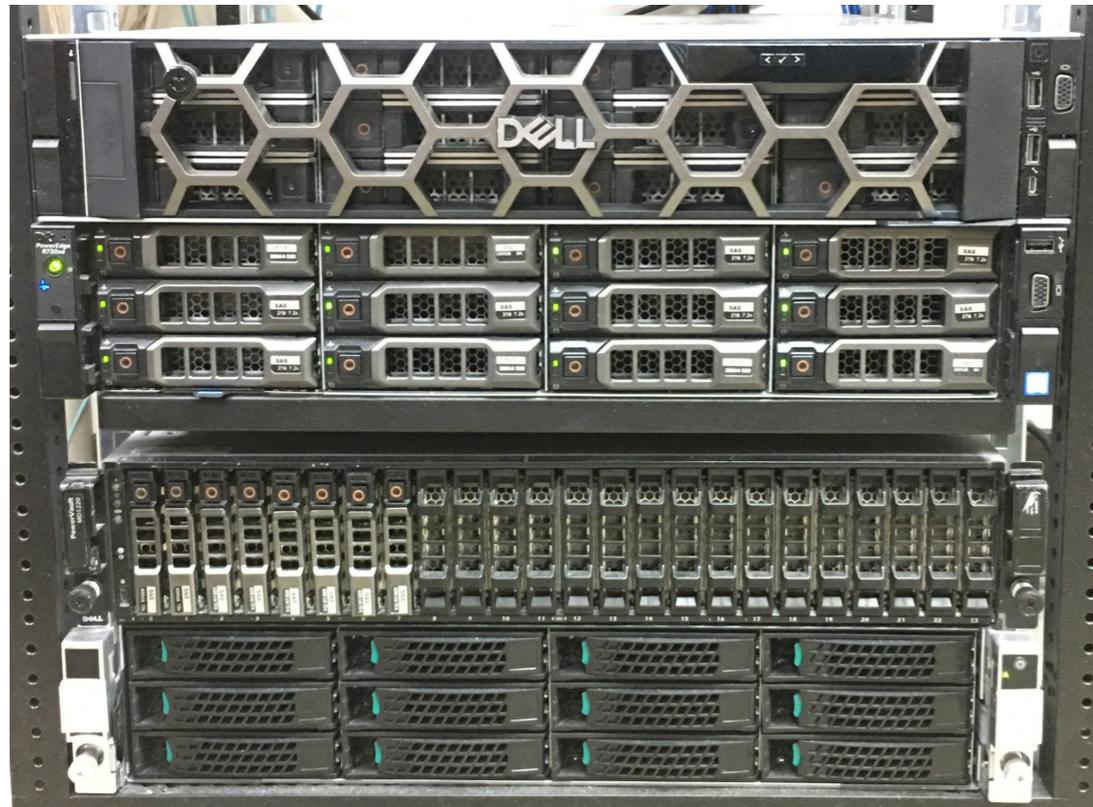
# 在PVE下實體硬碟掛載方式

## 免鎖DAS 硬碟櫃



```
1 | ls -l /dev/disk/by-id/  
2 |  
3 | nano etc/pve/qemu-server/100.conf  
4 |  
5 | 增加:  
6 | virtio0: /dev/disk/by-id/ata-XXXXXXXX,size=XXXG
```

# OSSLab的DFIR Server硬體配置



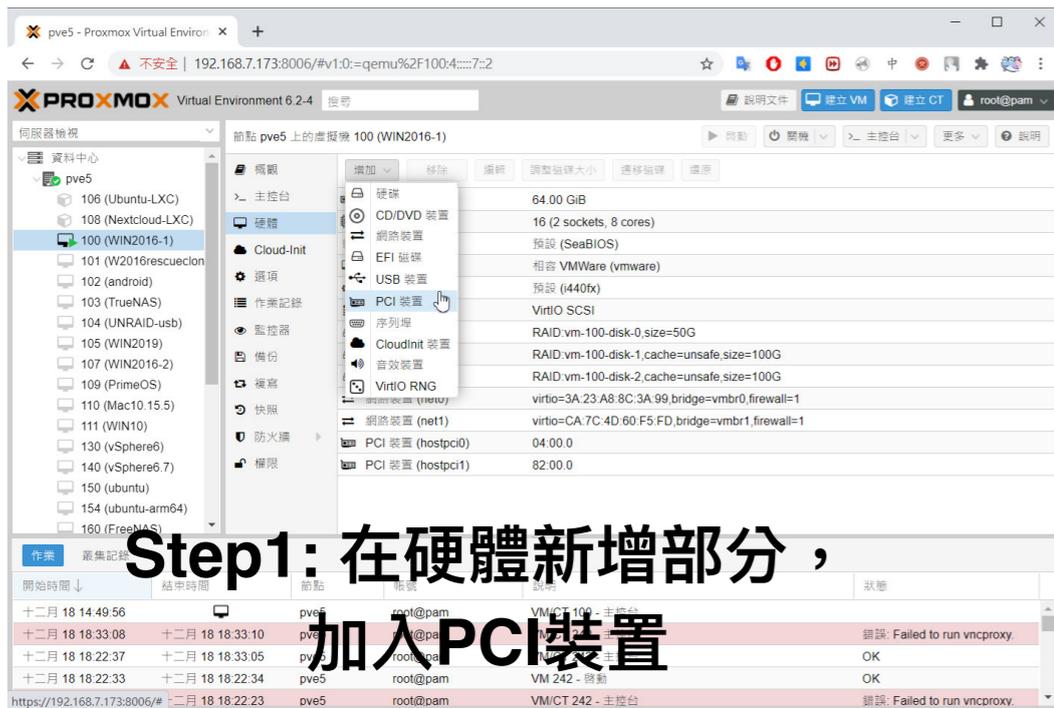
**R740xd 伺服器主機: 12x12TB3.5”  
HDD  
(Windows主機:)**

**R730 伺服器主機: 12x10TB 3.5” HDD  
(Proxmox VE主機)**

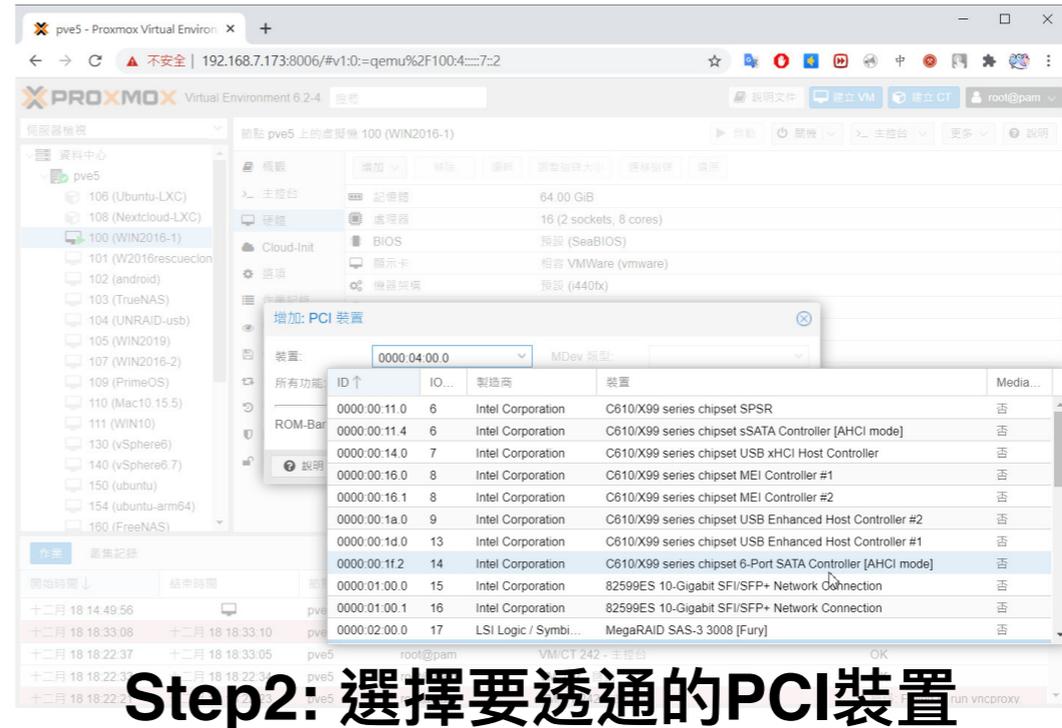
**Dell MD1200 2.5” 24-bay Drive Bays  
(連接實體硬碟, 框架要上螺絲)**

**Intel 3.5” 12-bay Drive Bays  
(連接實體硬碟, 框架要上螺絲)**

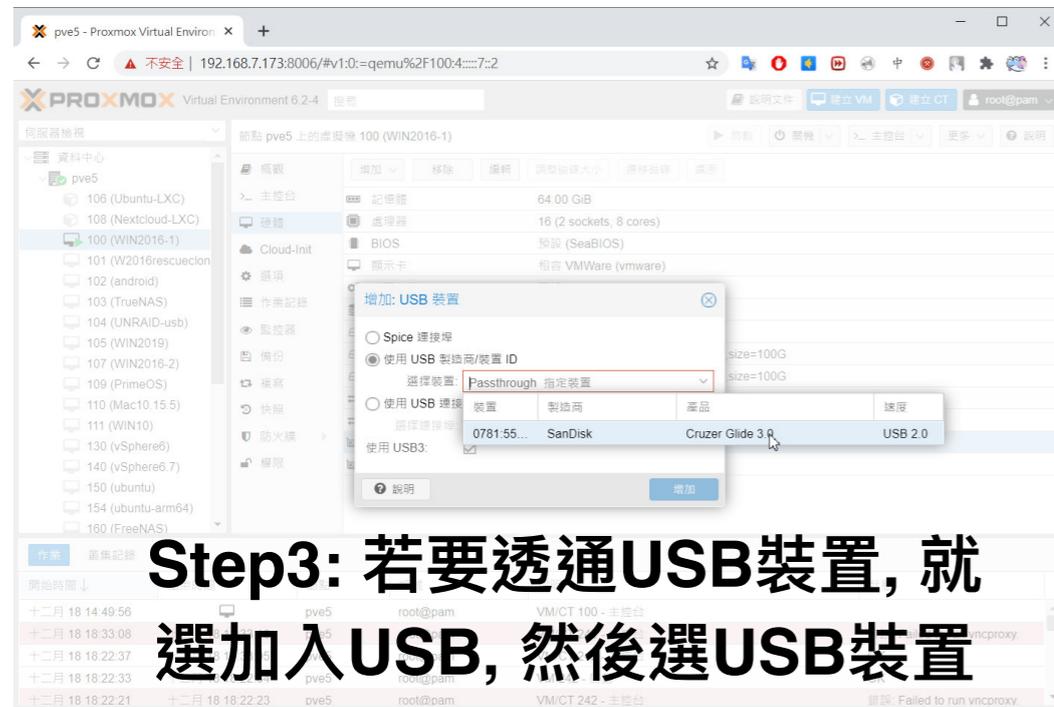
# PVE的硬體透通設定



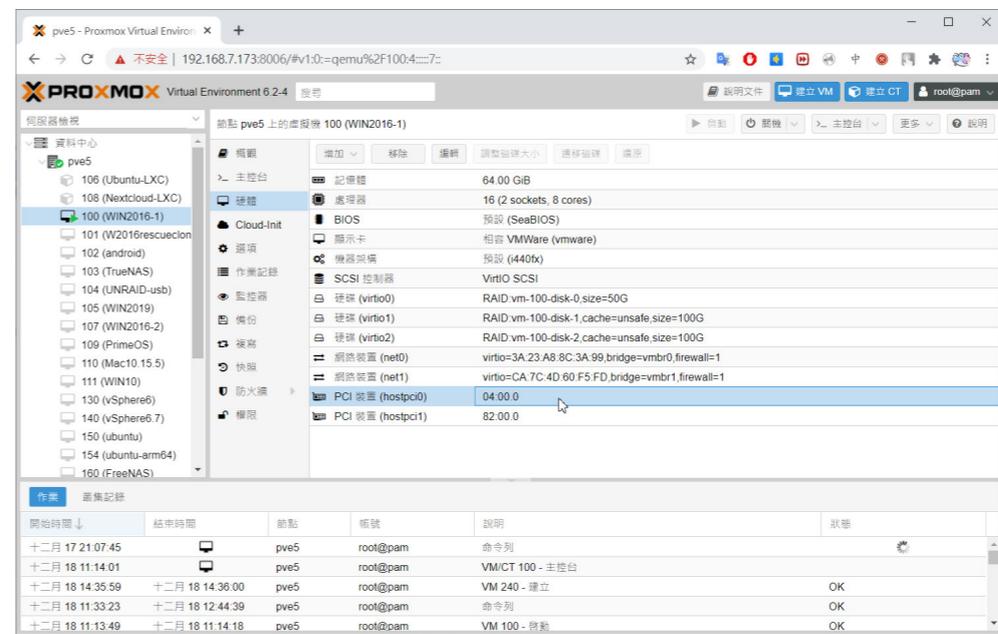
**Step1: 在硬體新增部分，加入PCI裝置**



**Step2: 選擇要透通的PCI裝置**



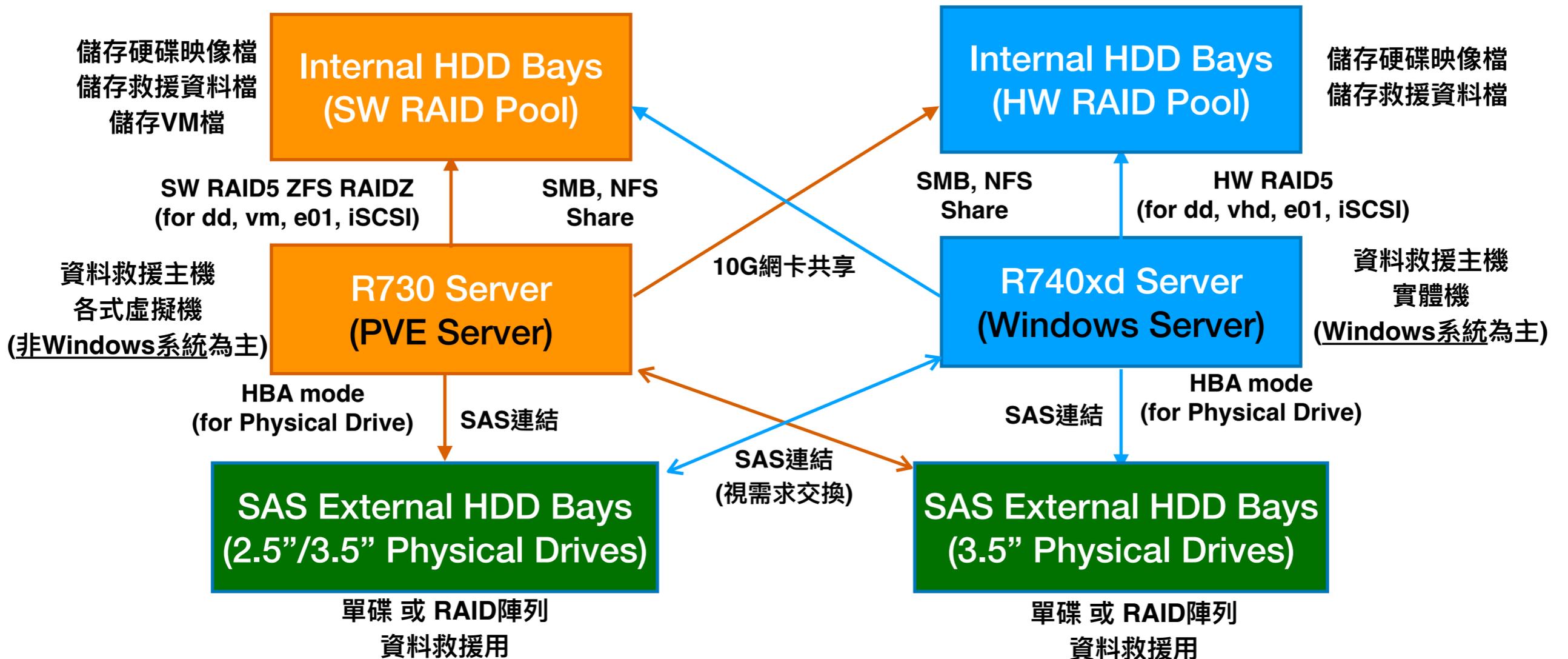
**Step3: 若要透通USB裝置，就選加入USB，然後選USB裝置**



**Step4: 設定完成後，虛擬機即可存取實體裝置**

PVE可加入實體USB與PCIe Storage裝置

# OSSLab的Server應用配置



2台超大容量伺服器主機

(皆384GB RAM, 100+ TB RAID5, Xeon Gold 5119T x2 CPU)

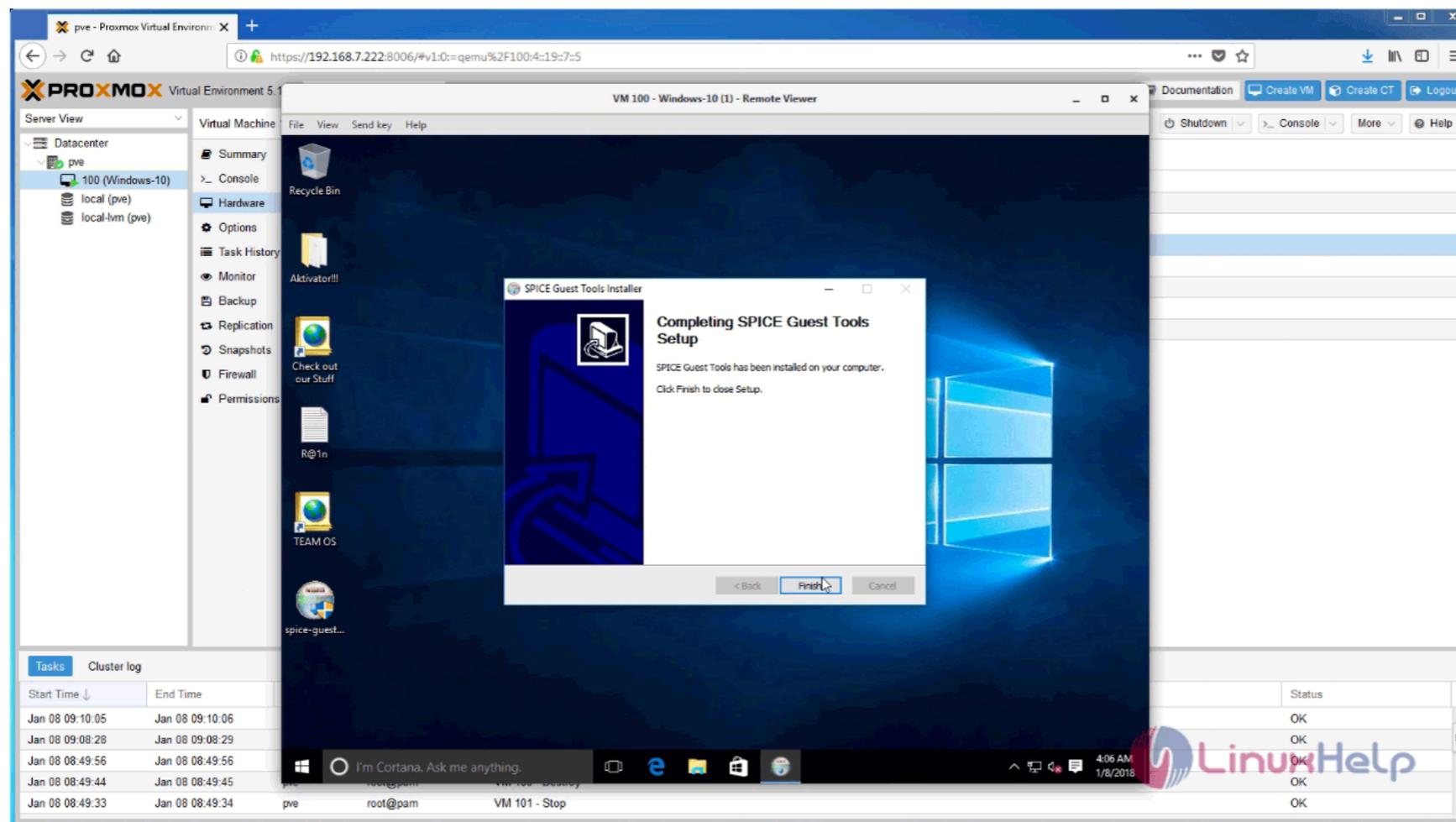
# 超大的儲存Pool WD Ultrastar Data60

一次可以插上60顆 raid pool



# 打仗需要搶時間

- VMware不支援DD格式，也無法用掛載磁碟直接boot  
等轉檔時間 會等到天荒到老
- 若採用PVE的QEMU虛擬化，可以直接掛載DD格式



# QEMU可跨CPU架構

- 其他虛擬機管理系統，僅支援x86虛擬機
- PVE的QEMU除可支援x86, 亦可支援ARM
- PVE模擬Ubuntu ARM: 建構ARM版NAS救援環境

<https://www.osslab.com.tw/proxmox-arm-virtualization/>

Server View

Virtual Machine 154 (ubuntu-arm64) on node 'pve5'

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

Backup

Replication

Snapshots

Firewall

Permissions

starting serial terminal on interface serial0

pve5 - Proxmox Console - Mozilla Firefox

https://192.168.7.173:8006/?console=kvm&xtermjs=1&vmid=154&vmname=ubuntu-arm64&node=pve5&cmd:

```
GNU GRUB version 2.04

-----
Try Ubuntu Server without installing
*Install Ubuntu Server
OEM install (for manufacturers)
-----

Use the ^ and v keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the commands
before booting or 'c' for a command-line. ESC to return previous
menu.
```

# 虛擬機掛載實體硬碟

- PVE 用 VirtIO 掛載實體硬碟, 幾近原生速度
- PVE 可掛載DD/RAW格式, 並可直接boot
- Windows要掛載必須先轉成VHDX檔案
- DD速度比較:
  - Physical HDD to Win 實體機 約2000MB/s
  - Physical HDD to PVE 虛擬機 約1200MB/s

```
ls -l /dev/disk/by-id/  
  
nano etc/pve/qemu-server/100.conf  
  
增加:  
virtio0: /dev/disk/by-id/ata-XXXXXXXX,size=XXXG
```

PVE掛載實體硬碟的方法

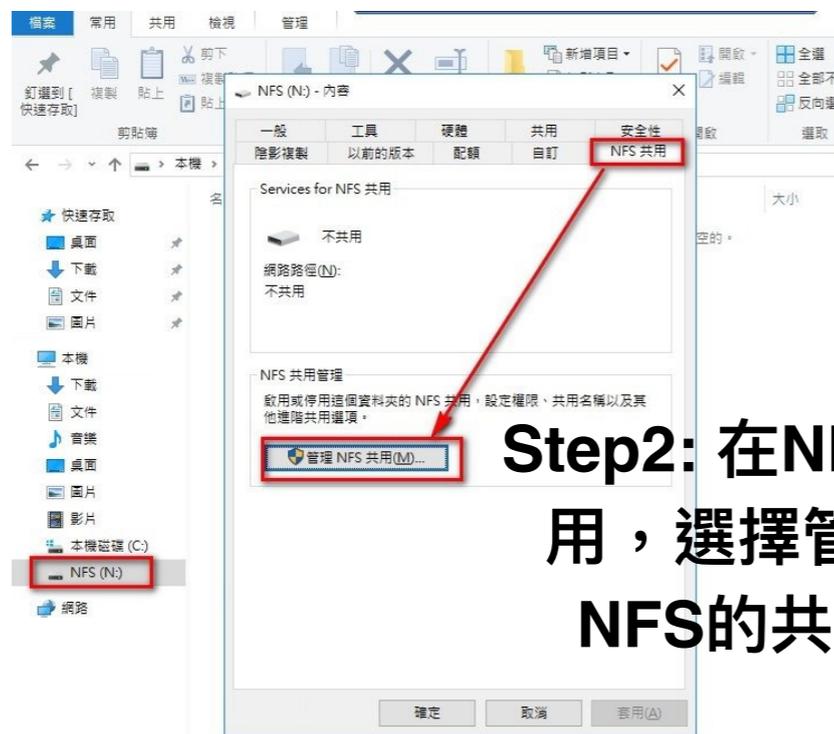
# Windows的NFS共享設定



**Step1: 伺服器管理員:角色裡加入 Server for NFS**



**Step3: 將此NFS 設定成共用夾**



**Step2: 在NFS共用, 選擇管理 NFS的共用**



**Step4: 進入NFS 目錄權限, 讓把 root讀寫加進來**

**Windows可啟用NFS Server**



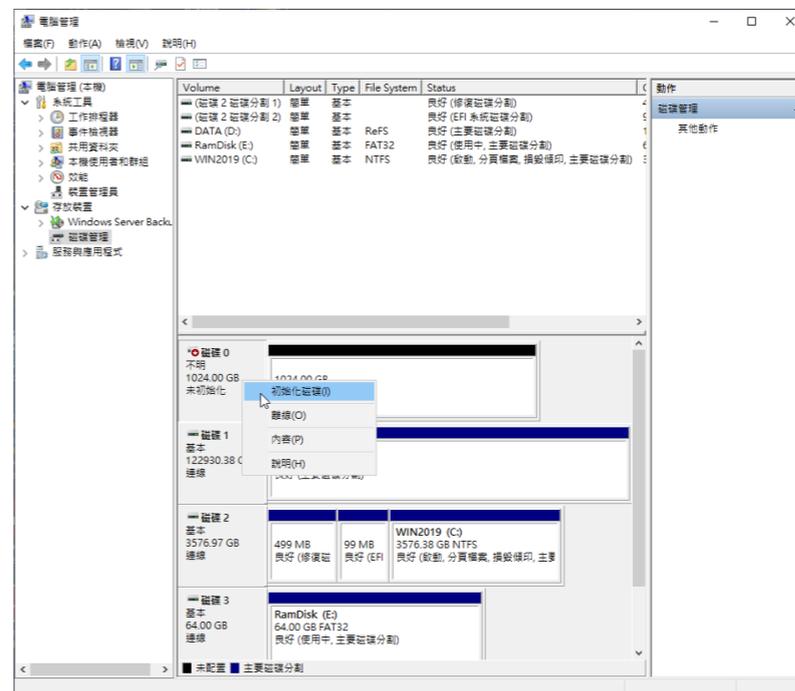
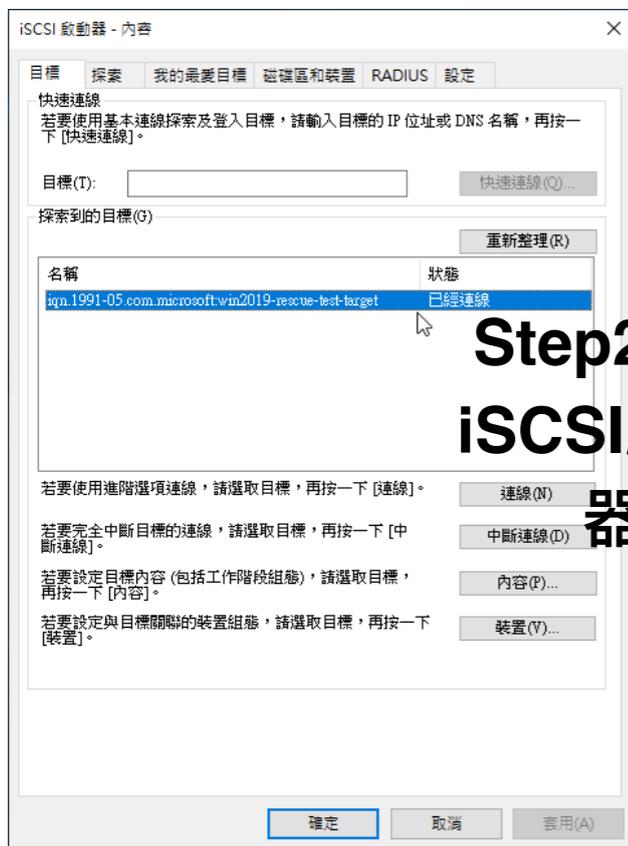
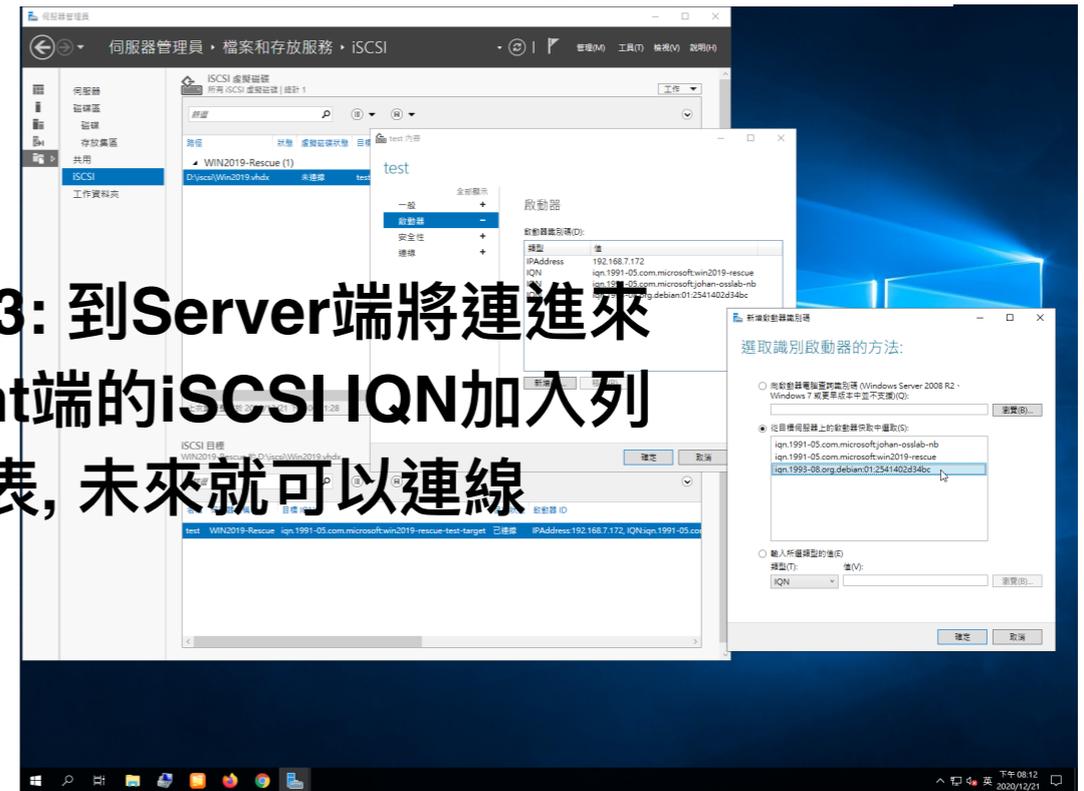
# iSCSI 虛擬磁碟機建立與掛載

1. 先在Windows Server建立iSCSI虛擬磁碟
  - 安裝 iSCSI Target Server功能
  - 建立一個超大 **vhdx** 檔案, 並分享成一個LUN
  - 開放給其他電腦掛載使用 (Windows / PVE)
  - 掛載後, 即可視為**實體硬碟**來進行資料救援
2. Windows掛載方式
  - 透過iSCSI啟動器來加入iSCSI目標
  - 在Windows Server端加入該啟動器, 掛載後即可存取LUNs
  - 各種救援工具, 皆可直接讀寫該iSCSI虛擬磁碟
3. PVE的掛載方式
  - 透過GUI於資料中心的儲存選項, 新增iSCSI
  - 在Windows Server端加入該啟動器, 掛載後即可存取LUNs
  - 輸入ID/Portal IP與Target
  - 儲存區就會多出iSCSI LUNs

# Windows的iSCSI設定

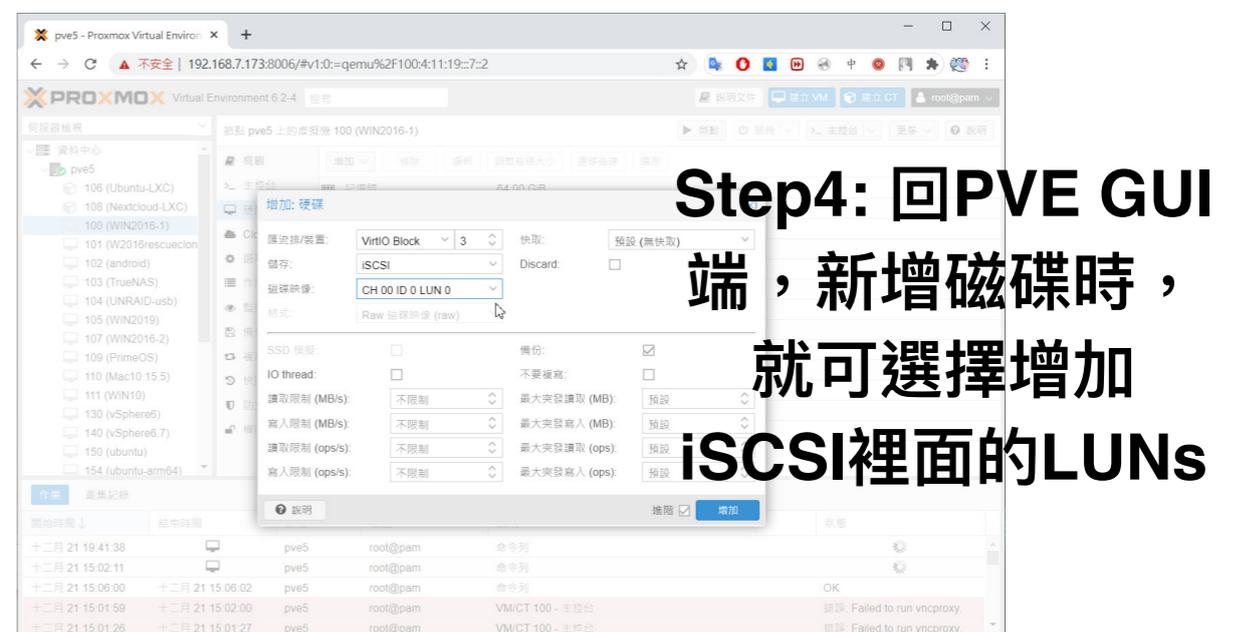
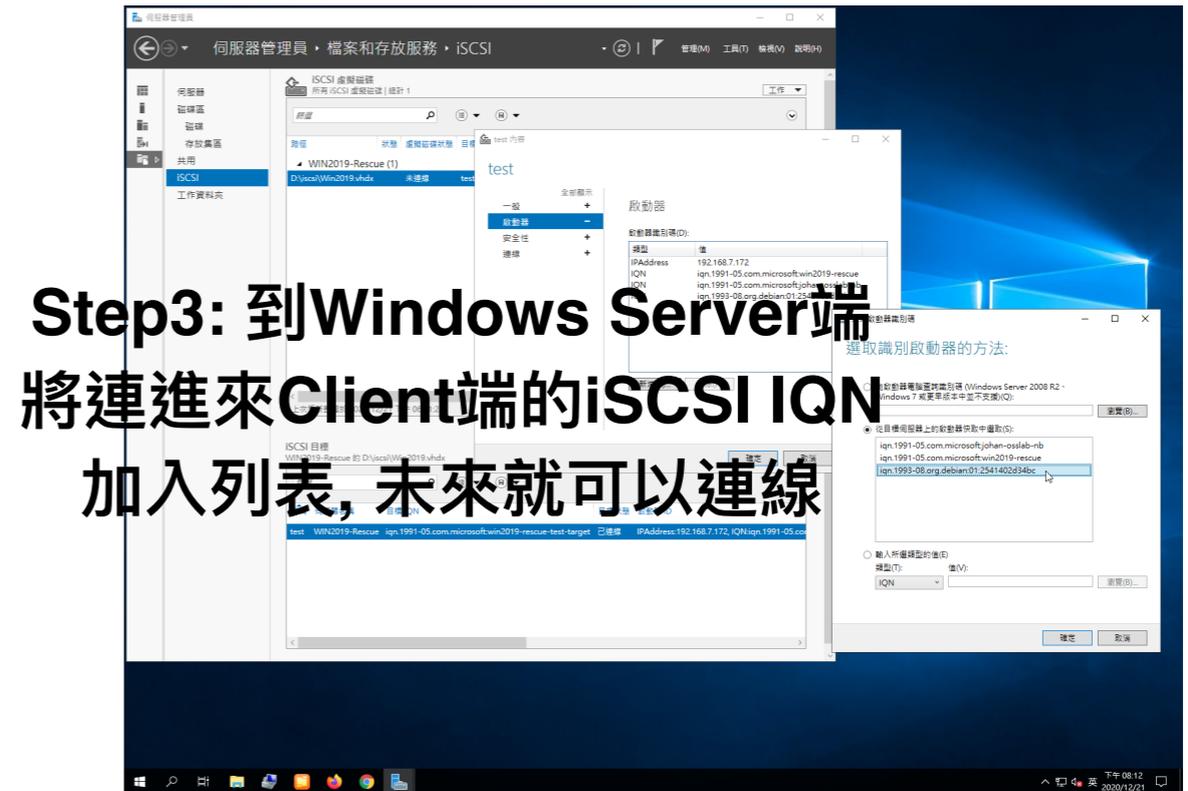
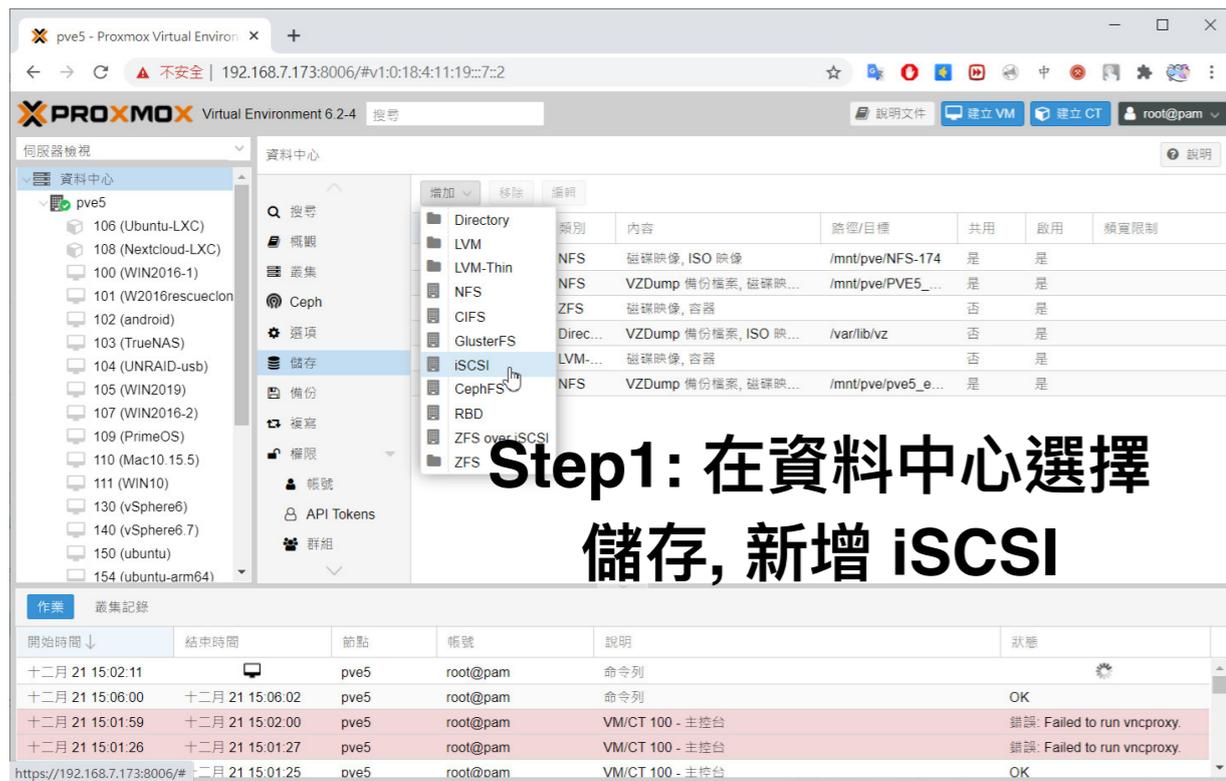


Step3: 到Server端將連進來Client端的iSCSI IQN加入列表, 未來就可以連線

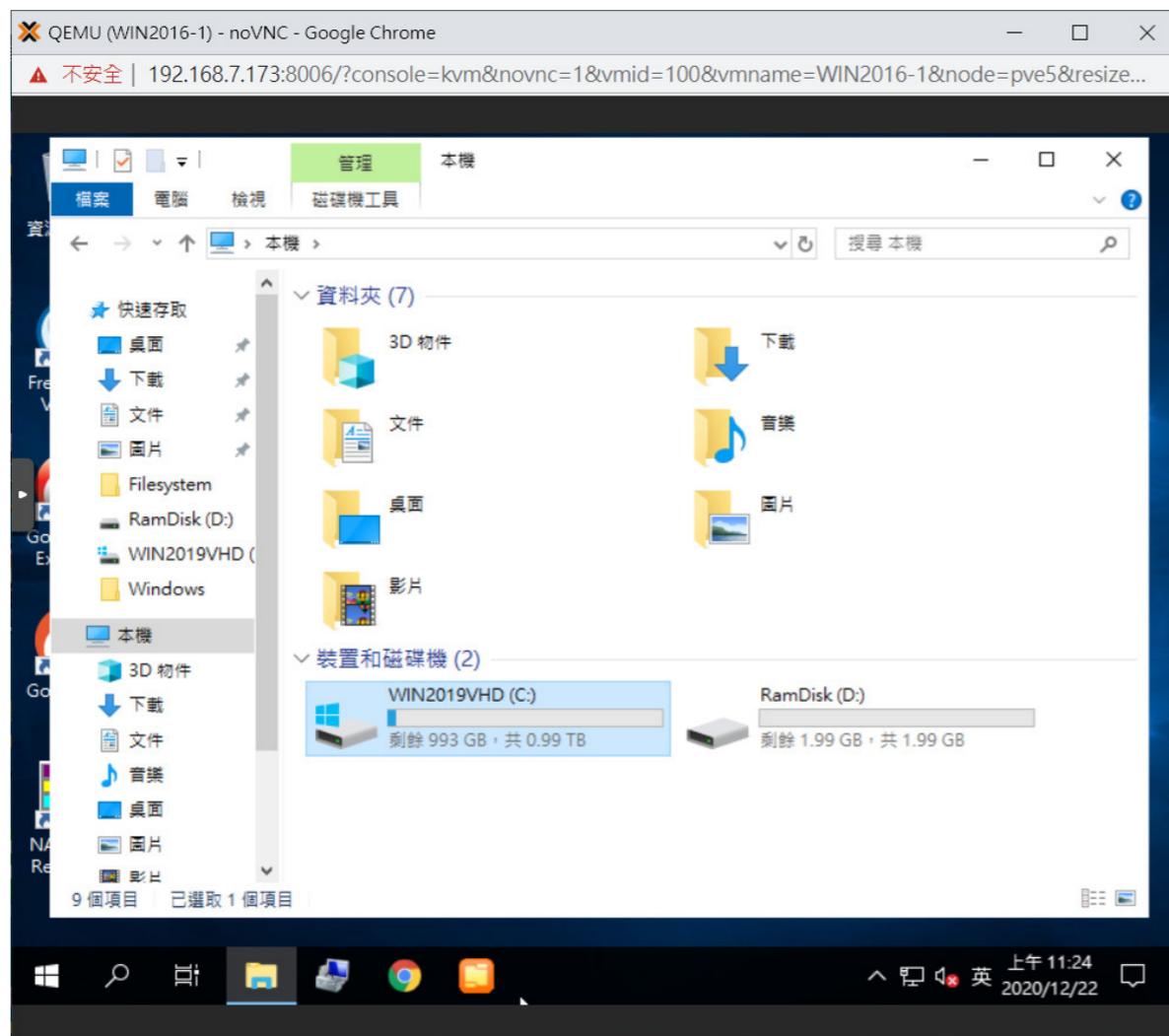


Windows可輕鬆設定iSCSI Target與Initiator

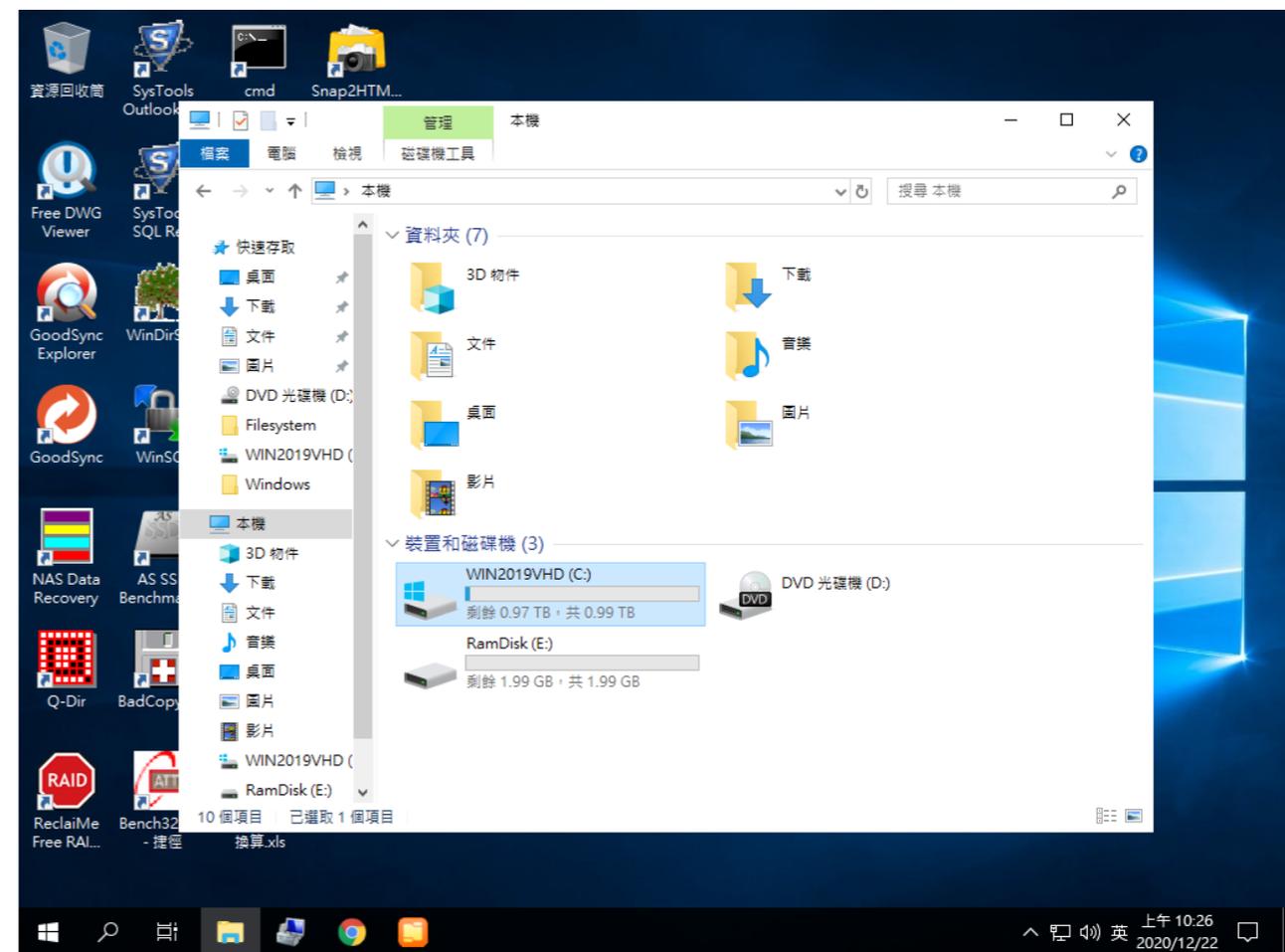
# PVE的iSCSI啟動器設定



# iSCSI 虛擬磁碟可在虛擬機開機



^ Proxmox VE



^ VMware Workstation

# 10G iSCSI存取效能

- Server R740效能 Client T430測試:

275GB檔案dd約10.5分鐘 (442MB/s) (單一機器存取時)

- R740 Hyper-V 本地Raid 上VHD直接掛載 效能讀寫: CrystalDisk 循序讀寫 617 / 728 MB/s

```
系統管理員: C:\Windows\SYSTEM32\cmd.exe
新目錄      8      D:\110share\Image\1017685\PC3000\
100% 新檔案      8.0 m      Attr.map
100% 新檔案      8.0 m      Head.map
100% 新檔案      209        Stat_0.txt
100% 新檔案      1077       task.bak
100% 新檔案      22.3 m     Task.fdb
100% 新檔案      140        task.info
100% 新檔案      6340      task.log
100% 新檔案      1077       task.prm
新目錄      2      D:\110share\Image\1017685\PC3000\!BackUp\
100% 新檔案      140        task.info
100% 新檔案      816        task.prm
新目錄      0      D:\110share\Image\1017685\PC3000\temp\
-----
          總計      已複製      略過      不符      失敗      額外
目錄 :          4          0          0          0          0
檔案 :          12         1          0          0          0
位元組 : 278,075 g 278,075 g          0          0          0
時間 : 0:10:29 0:10:29          0:00:00 0:00:00

速度 :          474409483 位元組/秒。
速度 :          27145.928 MB/分。
已結束 : 2020年10月30日 下午 12:08:35

D:\110share\Image\1017685>
微軟注音 半 :
```

# Win vs PVE 本機與網路的存取效能

All	5	8GiB	D: 85% (104148/122930GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	2508.29	2547.30	416.86	
RND4K Q1T1	5.69	15.21	9.98	
RND4K (IOPS)	1390.14	3713.87	2435.55	
RND4K (µs)	718.17	267.03	409.90	

^ 實體機 陣列直接存取速度(native physical drive)

All	5	8GiB	E: 0% (0/1024GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	107.39	105.48	106.54	
RND4K Q1T1	3.19	6.02	4.45	
RND4K (IOPS)	778.08	1468.75	1085.94	
RND4K (µs)	1279.52	676.64	915.68	

^ PVE掛載iSCSI網路磁碟機的存取速度 (Gigabit 網路卡)

All	5	8GiB	F: 0% (0/1024GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	1357.07	1520.66	714.70	
RND4K Q1T1	5.51	15.60	7.87	
RND4K (IOPS)	1345.95	3809.33	1921.14	
RND4K (µs)	741.90	261.87	519.33	

^ 實體機 掛載成iSCSI磁碟的本機存取速度

# iSCSI在本機與網路的存取效能

All	5	8GiB	D: 85% (104148/122930GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	2508.29	2547.30	416.86	
RND4K Q1T1	5.69	15.21	9.98	
RND4K (IOPS)	1390.14	3713.87	2435.55	
RND4K (μs)	718.17	267.03	409.90	

^ 直接存取速度(native physical drive)

All	5	8GiB	F: 0% (0/1024GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	1357.07	1520.66	714.70	
RND4K Q1T1	5.51	15.60	7.87	
RND4K (IOPS)	1345.95	3809.33	1921.14	
RND4K (μs)	741.90	261.87	519.33	

^ 掛載成iSCSI磁碟的本機存取速度

All	5	8GiB	E: 0% (0/1024GiB)	R70%/W30%
	Read [MB/s]	Write [MB/s]	Mix [MB/s]	
SEQ1M Q1T1	107.39	105.48	106.54	
RND4K Q1T1	3.19	6.02	4.45	
RND4K (IOPS)	778.08	1468.75	1085.94	
RND4K (μs)	1279.52	676.64	915.68	

^ PVE掛載iSCSI網路磁碟機的存取速度  
(Gigabit 網路卡)

# 開機狀況下記憶體中的密鑰

<https://www.passware.com/kit-business/filetypes/>

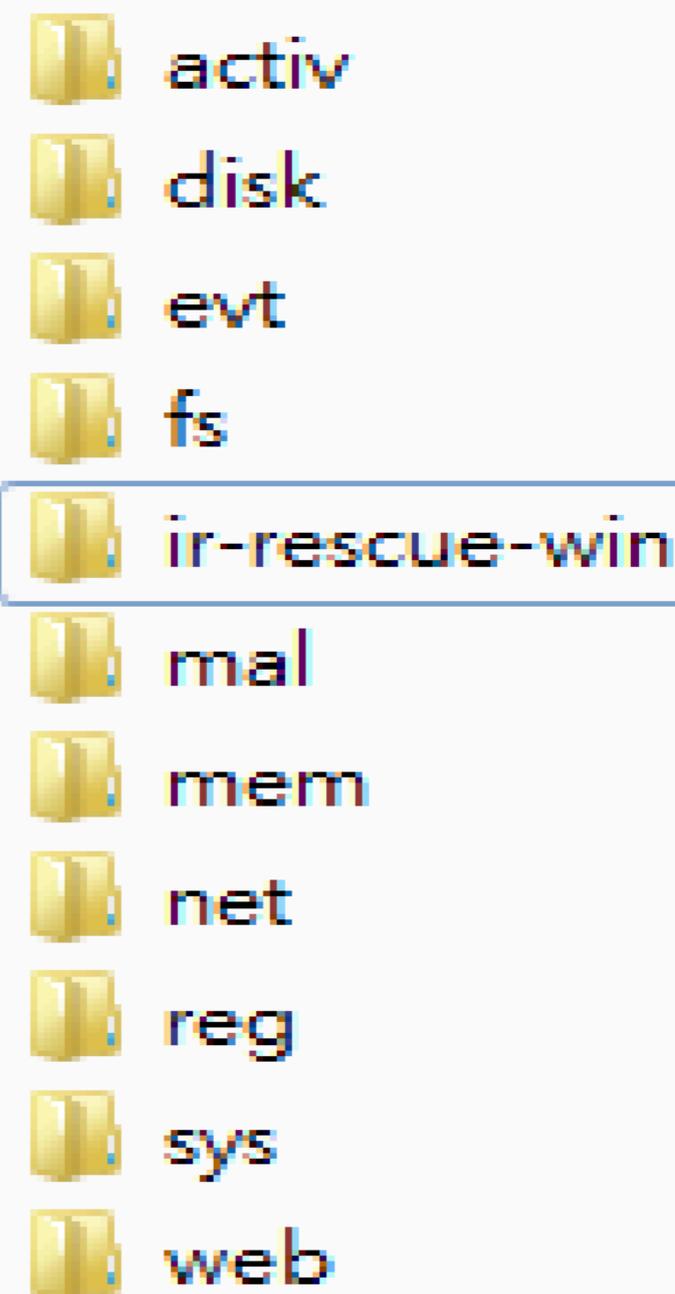
只要取得開機記憶體，就有機會得到

Bitlocker, PGP, TrueCrypt, VeraCrypt等密鑰

Apple File System (APFS)	DMG, DD, IMG, BIN, E01, EX01	Instant Removal (Memory Analysis) / Brute-force - Slow GPU
Symantec Endpoint Encryption	DD, IMG, BIN, E01, EX01	Instant Removal (Memory Analysis) / Brute-force - Slow GPU
LUKS Disk Image	DD, IMG, BIN, E01, EX01	Instant Removal (Memory Analysis) / Brute-force - Slow GPU
Mac OS / FileVault2	DMG, DD, IMG, BIN, E01, EX01	Instant Removal (Memory Analysis) / Brute-force - Slow GPU
MS Excel 2007	XLSX, XLSM	Instant Recovery or Removal (Memory Analysis) / Brute-force - Slow GPU
MS Excel 2010	XLSX, XLSM	Instant Recovery or Removal (Memory Analysis) / Brute-force - Slow GPU
MS Excel 2013	XLSX, XLSM	Instant Recovery or Removal (Memory Analysis) / Brute-force - Slow GPU
MS Excel 2016	XLSX, XLSM	Instant Recovery or Removal (Memory Analysis) / Brute-force - Slow GPU
MS Excel 2019	XLSX, XLSM	Instant Recovery or Removal (Memory Analysis) / Brute-force - Slow GPU
MS Windows NT User / Secure Boot Option		Instant Recovery (Memory Analysis) or Removal
MS Windows 2000 User / Secure Boot Option		Instant Recovery (Memory Analysis) or Removal
MS Windows 2000 Server User / Secure Boot Option		Instant Recovery (Memory Analysis) or Removal
MS Windows 2000 Server Active Directory Administrator		Instant Recovery (Memory Analysis) or Removal

# Windows IR toolkit

- <https://github.com/diogo-fernan/ir-rescue>
- <https://www.brimorlabs.com/Tools/LiveResponseCollection-Bambiraptor.zip>
- <https://www.sans.org/readingroom/whitepapers/forensics/liveresponse-powershell-34302>



Local IP : Port#	Remote IP : Port#	Process ID	Process Name	Process Start Time	Process File Path	Associated DLLs and File Path
[::1]:1731	[::1]:1733	7840	LMS	2017/8/14 上午 07:48:23	C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe	Module ----- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe C:\WINDOWS\SYSTEM32\ntdll.dll C:\WINDOWS\System32\wow64.dll C:\WINDOWS\System32\wow64win.dll C:\WINDOWS\System32\wow64cpu.dll

Local IP : Port#	Remote IP : Port#	Process ID	Process Name	Process Start Time	Process File Path	Associated DLLs and File Path
[::1]:1733	[::1]:1731	7840	LMS	2017/8/14 上午 07:48:23	C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe	Module ----- C:\Program Files (x86)\Intel\Intel(R) Management Engine Components\LMS\LMS.exe C:\WINDOWS\SYSTEM32\ntdll.dll C:\WINDOWS\System32\wow64.dll C:\WINDOWS\System32\wow64win.dll C:\WINDOWS\System32\wow64cpu.dll

## Running Processes sorted by ParentProcessID

ProcessName	CreationDate	ProcessId	ParentProcessId	CommandLine	sessionID
OneDriveSetup.exe	2017/8/14 上午 07:47:21	13912	13716	C:\Users\天俊\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\OneDriveSetup.exe /update /peruser /childprocess	1
analyzeMFT.exe	2017/8/14 上午 09:46:27	9740	12552	C:\ACER\RLTSCAN\analyzeMFT -f "C:\ACER\RLTSCAN\2017.08.14_ALPHA-I7_ALPHA-I7\MFT\SMFT" -o C:\ACER\RLTSCAN\2017.08.14_ALPHA-I7_ALPHA-I7\MFT\C_MFT.csv	1
conhost.exe	2017/8/14 上午 09:46:17	13952	12552	??C:\WINDOWS\system32\conhost.exe 0x4	1
conhost.exe	2017/8/14 上午 09:46:53	13232	12484	??C:\WINDOWS\system32\conhost.exe 0x4	1
powershell.exe	2017/8/14 上午 09:47:13	9444	12484	"C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe" -ExecutionPolicy Bypass -File LRUP.PS1	1

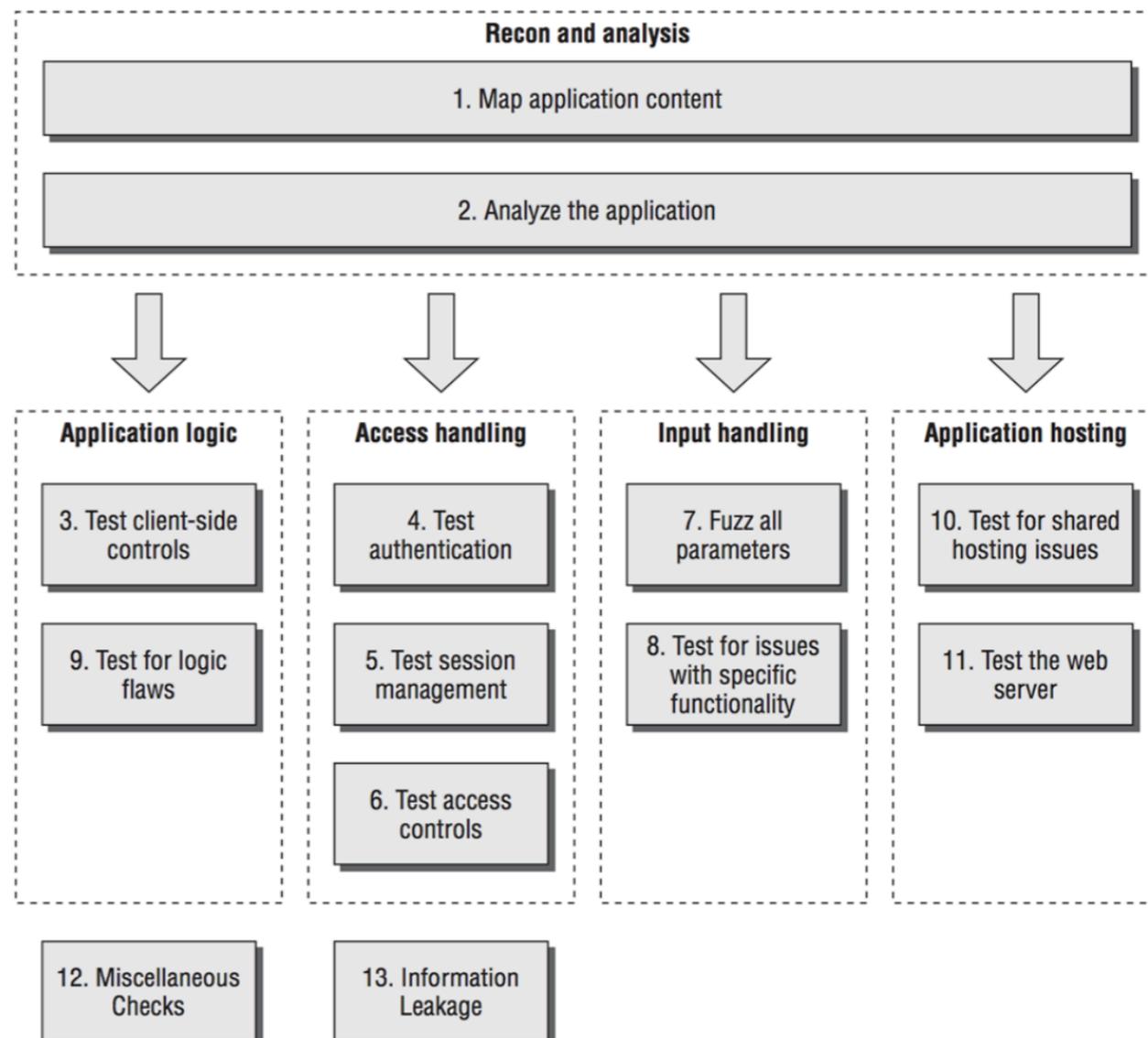
# 網站駭侵調查思路

有LOG:

- 一網頁平台記錄檔
- 一網頁主機其餘服務存取記錄檔
- 一檔案時間軸分析

沒LOG:

- 一用入侵網站的思維作研判
- 一請參考右圖黑站思路



# 滅證

- Sdelete
- ClearEventLog
- <https://github.com/Rizer0/Log-killer>
- <https://github.com/hlldz/Invoke-Phantom>
- History 全清除
- /var/log/\* 全清除
- /home/wwwroot/\* 全清除 (只殘留資料夾)
- /etc/ 相關config 全清除

```
3 title Log Killer
4 echo -----
5 echo ==                Log killer                ==
6 echo ==  This tool going to delete all logs !  ==
7 echo -----
8 timeout 5
9 for /F "tokens=*" %%G in ('wevtutil.exe el') DO (call :clear
10 echo.
11 echo logs has deleted
12 goto :theEnd
13 timeout 5
14 :clear
15 echo [+] %1
16 wevtutil.exe cl %1
17 goto :eof
18 :theEnd
19 timeout 5
```

```
cleartracks.php x
74 $LgF = shell_exec('echo $HISTFILE');
75 $logFiles = array(
76 "/var/log/yum.log",
77 "/var/log/wtmp",
78 "/var/log/utmp",
79 "/var/log/secure",
80 "/var/log/mysqld.log",
81 "/var/log/boot.log",
82 "/var/log/lighttpd",
83 "/var/log/httpd/",
84 "/var/log/qmail/",
85 "/var/log/maillog",
86 "/var/log/cron.log",
87 "/var/log/kern.log",
88 "/var/log/auth.log",
89 "/var/log/message",
90 "/var/log/lastlog",
91 "/var/adm/lastlog",
92 "/usr/adm/lastlog",
93 "/var/log/lastlog",
94 "$LgF",
95 "/etc/utmp",
96 "/etc/wtmp",
```

```
cleartracks.php x
94 "$LgF",
95 "/etc/utmp",
96 "/etc/wtmp",
97 "/var/adm",
98 "/var/log",
99 "/var/logs",
100 "/var/run/utmp",
101 "/var/apache/log",
102 "/var/apache/logs",
103 "/usr/local/apache/lo
104 "/usr/local/apache/lo
105 "/root/.bash_logout",
106 "/root/.bash_history",
107 "/root/.ksh_history",
108 "/tmp/logs",
109 "/opt/lampp/logs/acce
110 "/var/log/nginx/acces
111 "/logs/agent_lo",
112 "/logs/referer_log",
113 "/logs/access_log",
114 "/var/log/apache2",
115 "/var/log/wtmp",
```

# 總結

- 在資安事件發生時 數位鑑識與即時回應處理  
資料恢復與上線
- 遇到資安事件時，請務必將事故硬碟dd存證
- 備份用意主要是取得被駭證據，以便日後DFIR分析，追蹤系統漏洞，並有利於資料救援需求。
- 若遇到棘手的勒索病毒或資料救援事件，若無法自行搞定，建議還是尋求有誠信的外包商。

# 應對勒索病毒最好方法

- 攻擊手法太多樣  
基本資安保護
  - 1.強密碼 定期更換 定期弱掃
  - 2.設備清點 關非必要port 與服務
  - 3.定期更新 資安情報取得.
- 備份 不管多沒錢  
機器永遠比軟體 人工便宜
- 若遇到棘手的勒索病毒或資料救援事件, 若無法自行搞定, 建議還是尋求有誠信的外包商.租設備也可