用PVE處理資安事件DFIR實戰經驗







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

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。」

▲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)

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

不想承認但這些都是事實

" 1 1 1 1 1 Ifranleunaiz Deliamon Swase D'Auc 47

- 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

First / last seen spending

witness_v0_scripthash

OP Bin Hex

2

1/0

7 days ago ① / 7 days ago ③

• 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.doppeled and somefile1.how2decrypt.txt & somefile2.doppeled 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

<u>Digital Forensics and Incident Response</u> 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

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

G nomore	ransom.org/zm_mar	nt/decryption-tools.ntml			X 84 +	⊌ ∞ ⊞ ≎ (• 🗠 🖬 🖕 🗯 🍥
			NO MORE	RANSO	M !	:	★ 中文(正體) •
	解碼警長	勒索軟體:問與答	防範建議	解鎖工具	通報犯罪事件	合作夥伴	關於本計畫
			金 解	Q鎖工具	1		
注意!在您	8下載解鎖程式	(並且開始解鎖之)	前,請先閱讀使用批	「南。請先確認您	尼經將惡意軟	體從電腦上移除	,否則即便您將
注意!在炮 檔案解鎖,	图下載解鎖程式 惡意軟體還是	式並且開始解鎖之前 聖會持續將您的電	前,請先閱讀使用挑 腦資料加密。任何可	旨南。請先確認怨 可信的防毒軟體者	⁸ 已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	,否則即便您將
注意!在您 檔案解鎖,	8下載解鎖程式 惡意軟體還長	式並且開始解鎖之 。 會持續將您的電	前,請先閱讀使用捐 腦資料加密。任何可	旨南。請先確認約 可信的防毒軟體者	8已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	,否則即便您將
注意!在您 檔案解鎖,	8下載解鎖程式 惡意軟體還是	式並且開始解鎖之 ■會持續將您的電	前,請先閱讀使用捐 腦資料加密。任何可 ^{Quick}	皆南。請先確認怨 可信的防毒軟體者 ^{k Search}	8已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	;否則即便您將
注意!在您 檔案解鎖,	悠下載解鎖程式 惡意軟體還是	、並且開始解鎖之 全 音 持 績 將 您 的 電 人	前,請先閱讀使用捐 腦資料加密。任何可 Quick	旨南。請先確認您 可信的防毒軟體者 k Search	8已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	:,否則即便您 將
注意!在您 檔案解鎖, All Ranson	8下載解鎖程式 惡意軟體還是	C並且開始解鎖之 是會持續將您的電 al order):	前,請先閱讀使用捐 腦資料加密。任何可 Quick	皆南。請先確認絕 可信的防毒軟體者 ĸ Search	8已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	、 否則即便您將
注意!在缆 檔案解鎖, All Ranson > 777 Ran	四下載解鎖程式 惡意軟體還長 n (alphabetica nsom	忧並且開始解鎖之Ⅰ 聲會持續將您的電/ al order):	前,請先閱讀使用捐 腦資料加密。任何可 Quick	皆南。請先確認怨 可信的防毒軟體者 < Search	¹⁸ 已經將惡意軟 ¹⁸ 可用來移除惡	體從電腦上移除 意軟體。	;否則即便您將
注意!在您 檔案解鎖, All Ranson > 777 Rar > AES_NI	R下載解鎖程式 悪意軟體還見 n (alphabetica nsom Ransom	优並且開始解鎖之已 是會持續將您的電 al order):	前,請先閱讀使用捐 腦資料加密。任何可 Quick	旨南。請先確認怨 可信的防毒軟體者 ^{k Search}	8已經將惡意軟 8可用來移除惡	體從電腦上移除 意軟體。	*,否則即便您將
注意!在您 檔案解鎖, All Ranson <u>> 777 Ran</u> <u>> AES_NI</u> <u>> Agent.ii</u>	R下載解鎖程式 思意軟體還長 n (alphabetica nsom Ransom ih Ransom	t並且開始解鎖之已 是會持續將您的電 al order):	前,請先閱讀使用捐 腦資料加密。任何可 Quick	皆南。請先確認怨 可信的防毒軟體者 < Search	8已經將惡意軟 8可用來移除惡	體從電腦上移除意軟體。	♠,否則即便您將

恢復計畫或外包

PROVEN FOR 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

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

- 不從駭客中獲得密鑰 以<u>資料恢復</u>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<u>成功性</u>. > 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

MDF 碎片恢復法

最重要的為 16-21 NextPage ID 跟32-35 PageID

6	/	8	9	A	в	6	D	Ľ	r	ANSI ASCII
0	30	00	OC	00	E9	8C	3E	01	DA	.0000000 éŒ> Ú
0	09	00	2A	00	2E	00	33	00	37	¥ *.37
0	4B	00	54	00	49	4E	53	45	52	B F K K T INSER
F	50	54	48	32	33	31	20	32	30	TN002COPTH231 20
0	33	37	30	30	30	35	54	48	30	1604010370005TH0
0	30	30	30	30	30	00	oc	00	02	1228.0000000
0	AO	00	00	00	09	00	2A	00	2E	> Ú¥ *.
0	46	00	4B	00	4B	00	55	00	49	37858801
0	30	32	43	4F	50	54	48	32	33	NSERTN002COFTH23
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	OA	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 INSERTNO02CO
:0	32	30	31	36	30	34	30	31	30	FTH231 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¥
Α	00	2E	00	33	00	37	00	42	00	*.37B
4	00	49	4E	53	45	52	54	4E	30	F K K T INSERTNO
8	32	33	31	20	32	30	31	36	30	02COPTH231 20160
0	30	30	38	54	48	30	31	32	37	4010370008TH0127
0	30	30	00	0C	00	51	8D	ЗE	01	5.0000000 Q >
0	00	09	00	2A	00	2E	00	33	00	Ú¥ *.3
в	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	RTN002CCPTH231 1
1	30	33	37	30	30	30	39	54	48	01604010370009TH
E	30	30	30	30	30	30	30	00	oc	012450.0000000
.5	00	00	OA	00	00	00	09	00	2A	Gð@ Ú¥ *
0	42	00	46	00	4B	00	4B	00	55	. 37BFKKU
.4	4E	30	30	32	43	4F	50	54	48	INSERTN002COPTH
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	FO	40	01	DA	A5	00	00	OA	00	000 að@ 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 INSERTNO02
:3	31	20	32	30	31	36	30	34	30	COPTH231 2016040
0	32	54	48	30	31	32	33	39	2E	10380002TH01239.
0	00	oc	00	7B	FO	40	01	DA	A5	6000000 {ð@ Ú¥
19	00	2A	00	2E	00	33	00	37	00	*.37
В	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	N002CCPTH231 201
3	38	30	30	30	33	54	48	30	31	604010380003TH01
10	30	30	30	30	00	0C	00	97	FO	239.6000000 -ð
A	00	00	00	09	00	2A	00	2E	00	0 U¥ *.
6	00	4B	00	4B	00	54	00	49	4E	37BFKKTIN
0	32	43	4F	50	54	48	32	33	31	SERTN002COPTH231

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 Image: Constraint of the second seco	Copy entire medium Start sector (source): Start sector (destination): Number of sectors to copy: 2880
 Log procedure silently (no error messages) Write pattern for damaged source sectors: UNRE Simultaneous I/O (faster, if source and destination are 	Avoid damaged areas. Skip range: 32 EADABLESECTOR different physical media)
<u>O</u> K C <u>a</u> ncel	<u>H</u> elp

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<u>支援多個ISO檔案</u>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 -

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

etData UDP Network Server ×	EX Imager v2.2.0(259)	;
Server IP: 192.168.6.239	Source Advanced Forensics Source Name (L\D: Volume Label Ventoy	Select =
Server port. 445	SOUR CetData UDP Network Server IL UD: Server Server IP: 192.168.6.239 Server IP: 192.168.6.239 Port 443	Connect
Version: v4.0.0(116) Instance: {4FA51004-32A0-435A-AD50-F2617B924814} IP Addresses: 192.168.6.239 Loading Drives Drives Found: 1 Drive: \\.\D: Ready	test Server Status: Idle PROG Imager no Version: v4.0.0(116) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (1900 Compression (Only for slow connections) Version: v4.0.0(116) Instance: (4FA51004-32A0-435A-AD50-F2617B924814) Instance: (1900 Compression (Only for slow connections) Dives: [v2.168.6.239 New Connection - Peer IP: 192.168.6.239 Port: 61649 Ready Connection Removed - Peer IP: 192.168.6.239 Port: 61649 Ready	k Packets Size 14.87 GB
Chee	© GetData Forensics 2020 Hash	Cancel

SSI ab

在PVE下實體硬碟掛載方式

免鎖DAS 硬碟櫃

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

	Environment 6 2-4	治灵		■ 說明文件 🚺	□ 建立 VM 😭 建立 CT 🔒 root@parm
昭器檢視		题 # 100 (M/N2016 1)			
■ 資料中心	BD #D pve5 FJ Re 1	腹機 100 (WIN2016-1)			↓ 上 主任日 ↓ 民 岁 ↓ ♥ 就 ?
v 🌄 pve5	■ 概觀	増加 > 移除 編輯	調整磁碟大小 遷移磁碟	這原	
106 (Ubuntu-LXC)	>_ 主控台	e 🖨 硬碟	64.00 GiB		
108 (Nextcloud-LXC)	ᇦ 硬體	● CD/DVD 装置	16 (2 sockets, 8 cores)		
100 (WIN2016-1)	Cloud-Init		預設 (SeaBIOS)		
101 (W2016rescueción	✿ 選項	⊷ USB 装音	相容 VMWare (vmware)		
102 (dituloid) 103 (TrueNAS)	■ 作業記錄	ー PCI装置 Jm	預設 (i440fx)		
104 (UNRAID-usb)	▲ 卧抗哭	■ 序列埠	VirtIO SCSI	20	
105 (WIN2019)	· miltin	▲ CloudInit 装置	RAID.Vm-100-disk-0,size=50	JG	
107 (WIN2016-2)	出 備伤	●●● 音效裝置	RAID.vm 100 disk 2 cache=	unsale,size=100G	
109 (PrimeOS)	₩2 複寫	VirtIO RNG	virtio=3A:23:A8:8C:3A:99 br	idge=vmbr0 firewall=1	
110 (Mac10.15.5)	⑦ 快照	➡ 網路裝置 (net1)	virtio=CA:7C:4D:60:F5:FD.b	ridge=vmbr1.firewall=1	
110 (vviil 10) 130 (vSphere6)	♥ 防火牆 ▶	Im PCI 装置 (hostpci0)	04:00.0	-	
140 (vSphere6.7)	▲ 權限	Im PCI 装置 (hostpci1)	82:00.0		
🖵 150 (ubuntu)					
154 (ubuntu-arm64)					
160 (FreeNAS)		→- 7 田 同(サイトまん	70/7	
作業 叢集記録 10	n 1.	イナ 有単常	今天川て習ら		9
始時間↓ 結束時間	前點		로겠지 거리 ト	117 / J	狀態
□ 目 18 14:49:56	Dve5	root@nam	VM/CI109,主控台		
二月 18 18:33:08 十二月 18	18:33:10 pve				错誤: Failed to run vncproxy.
二月 18 18:22:37 十二月 18	18:33:05 pv 5	rootkipa			OK
		/ / / /			
二月 18 18:22:33 十二月 18	18:22:34 pve5	root@pam	VM 242 - 啓動		OK
二月 18 18:22:33 十二月 18 ss://192.168.7.173:8006/# 二月 18	18:22:34 pve5 18:22:23 pve5 × +	root@pam root@pam	VM 242 - 啓動 VM/CT 242 - 主控台		OK 銀課: Failed to run vncproxy.
二月 18 18 22:33 十二月 18 s://192.168.7.173:8006/# 二月 18 pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19.	18:22:34 pve5 18:22:23 pve5 × + 2.168.7.173:8006/#	root@pam root@pam	VM 242 - 啓動 VM/CT 242 - 主控台	x 🛯 🖌	OK ###: Failed to run vncproxy. - 미 • 중 후 영 [제 화 202
二月 18 18 22:33 +二月 18 s://192.168.7.173:8006/# ⁺ 二月 18	18:22:34 pve5 18:22:23 pve5 × + 2:168:7.173:8006/# Environment 6:2-4	root@pam root@pam root@pam	VM 242 - 啓動 VM/CT 242 - 主控台	☆ 🗣 O 🕻 雇 設明文件	OK ∰: Failed to run vncproxv. - □ Ø Ø ♥ Ø № ★ @ Fato VM Ø #co.ct aroot@per
二月1818-22:33 +二月18 x;//192.168.7.173:8006/# 二月18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19. ② PROXMOX Virtual 最高時税	18:22:34 pve5 18:22:23 pve5 × + 2:168:7.173:8006/# Environment 6:2-4 milità pve5 Letti	root@pam root@pam fv1:0:=qemu%2F100:4:7::2 度专	VM 242 · 啓動 VM/CT 242 - 主控台	 ☆ ♣ 0 ▲ ▲ KHX* ▲ KHX* 	OK ∰#: Failed to run vncproxy. -
二月1818.22.33 +二月18 ss/192.168.7.173:8006/# 二月18 pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19. (PRO×MO× Virtual 展路路線 資料中心	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 mB2 pre5 _E014 # 559	root@pam root@pam fv1:0:=qemu%2F100:4:::::7::2 度 章	VM 242 · 啓動 VM/CT 242 - 主控台	☆ 및 0 및 建 2007年 ● 680 0 日報 685	OK ∰R: Failed to run vncproxy. – □ De & + @ R * @ Det vst @ R±±CT ▲ root@par t wt >_ ±EE @ E. + @ B
二月1818.22.33 +二月18 s://192.168.7.173:8006/# 二月18	18:22:34 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6:2-4 前意 pre5 上的傳 圖 電報 文 士斯希	root@pam root@pam fv1:0:=qemu%2F100:4:::::7::2 度 む (装 壁 100 (WIN2016-1)	VM 242 - 啓動 VM/CT 242 - 主陸台		OK ##:Failed to run vncproxy - □
二月1818-22:33 十二月18 は2/192.168.7.173:8006/# 二月18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19. ● PRO × MO × Virtual 家語始視 ● 算得中心 ● 106 (Ubuntu-LXC) ● 108 (Ubartelevel 1/2)	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 前登 pre5 上的虚 星 電缆 2: 直控合	root@pam root@pam root@pam w1:0:=qemu%2F100:4::::7:2 度意 度意 度意 度意 度意 度意 度意 度意 度意 度意 度 度 度 度	VM 242 - 啓動 VM/CT 242 - 主陸台	☆ № 0 ■ <i>全</i> 副初文作 ▶ 句目 0 日前 周前	OK ##:Failed to run vincoroxy. - □ •
二月 18 18.22:33 +二月 18 に//192.168.7.173:8006/# 二月 18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19, ② PRO × MO × Virtual ※ 取得中心 ③ 取得中心 ③ 106 (Ubuntu-LXC) ④ 108 (Nextcioud-LXC) ④ 108 (Nextcioud-LXC)	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6 2:4 節差 pre5 上的意 単 気彩 二 主空台 二 便信	root@pam root@pam vot@cam v1:0:=qemu%2F100:4:::::7:2 度 5 (登 使 100 (WIN2016-1) (VM 242 - 啓動 VM/CT 242 - 主控台 EE	☆ ➡ 0 ■ <i>■</i> 武明文件 ● 日日 ○ 王明 高野	OK ##: Failed to run vincoroxy. - □
二月 18 18.22.33 +二月 18 sc//192.168.7.173:8006/# 二月 18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19. 《PRO×MO× Virtual 定言推視 ※ pve5 ④ 106 (Ubuntu-LXC) ● 108 (NextEloud-LXC) ● 108 (NextEloud-LXC) ● 100 (W12016-1) ● 101 (W2016rescuecion	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6 2-4 節意 pre5 上的信 @ 低限 > 主控台 章 侵留 ● Cloud-Init	root@pam root@pam vot@pam v1:0:=qemu%2F100:4:::::7:2 度5 度5 度5 度5 度5 度5 度5 度5 度5 度5 度5 度5 度5	VM 242 - 啓動 VM/CT 242 - 主陸台 用 高名:00 G/B 16 (2 sockets, 8 cores) 防設 (SeaBIOS) 相同 242 - 主陸台	☆ ■ 0 ■ <i>■</i> 武明文件 ● 311 ○ 王朝 画示	OK ##E Failed to run vincproxy. - □ I IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
二月 18 18.22:33 +二月 18 に//192.168.7.173:8006/# 1 二月 18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19. ※ PRO × MO × Virtual ※ 原始中心 ※ 106 (Ubunfu-LXC) ※ 108 (NextCoud-LXC) ※ 108 (NextCoud-LXC) ※ 100 (WI2016-1) 101 (W2016rescuecton © 102 (android)	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 節點 pre5 上的總 章 儀觀 >、 主座音 章 優觀 意 Cloud-Init 章 選項	root@pam root@pam vot@pam v1:0:=qemu%2F100:4:::::7::2 度章 (因章 100 (WIN2016-1) (現立) 修練 編 () 一個大事 目 OS 日 回 S	VM 242 - 啓動 VM/CT 242 - 主陸台 CM/CT 242 - 主陸台 G4.00 G/B 16 (2 sockets, 6 cores) 预設 (SeaBIOS) 相音 VM/Ware (vmware)	☆ 🗣 🛛	OK ###: Failed to run vincproxy. - □
二月 18 18.22:33 +二月 18 は、192.168.7.173:8006/# 1二月 18 は、192.168.7.173:8006/# 12 は、192.168.7.173:8006/# 12 は、19	18:22:34 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6 2-4 前記 pre5 上的信 - 近日 - 近日 - ご回日 - 近日 - ご回日 - 正日 - ご回日 - 正日 - ご回日 - 正日 - ご回日 - 正日 - ご回日 - ご回	root@pam root@pam root@pam v1:0:=qemu%2F100:4:::::7::2 度号 2 使导 100 (WIN2016-1)	VM 242 - 啓動 VM/CT 242 - 主控台	★ ■ 0 ■ ■ 取明文件 ■ 不計 0 単 単 不計 0 単 単 不計	OK 플라: Failed to run vncproxv. - □ ● 응 부 ◎ 『 * 응 □ #±± VM [@ #±± CT] ▲ root@arr = [1±± VM] @ #±± CT] ▲ root@arr
□月 18 18.22.33 +□月 18 は(192.168.7.173:8006/# □月 18 は(192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.168.7.173:8006/# □] (192.173:8006/# □] (192.173:8006/#	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 前話 pre5上的處 一 建築 一 建築 一 建築 二 注意谷 二 二 建築谷 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二	root@pam root@pam root@pam w1:0:=-qemu%2F100:4:::::7:2 度章 段 100 (WIN2016-1) 原因 2 使弱 图 点理器 图 BIOS 图 点理器 图 BIOS 图 微示卡	VM 242 - 啓動 VM/CT 242 - 主控台		OK ∰∰: Failed to run vncproxv. — □ ■ ● ● 中 ● ■ ★ ● ■ Itto VM ● Itto CT ▲ root@per ■ V ► ±28 V ■ E5 V ● 5
□月 18 18:22:33 +□月 18 xx/192.168.7.173:8006/# □月 18 xx/192.168.7.173:8006/# □ xx/192.168.7.173:8006/# □ xx/192.175.7.175.7	18:22:34 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6 2:4 前話 pre5 上的虚 2 或親 2 主控合 二 連結 Cloud-Init ※ 選項 二 作業記録 ※ 監控器 四 復分	root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam	VM 242 - 啓動 VM/CT 242 - 主陸台 相		OK ###:Failed to run vncproxy. - □ • @ @ # @ P & @ • #±±±± • X ↓ ±±±± (V) (#\$ x) @ #
□月 18 18:22:33 +□月 18 xx/192.168.7.173:8006/# □月 18 xx/192.168.7.173:8006/# □ xx/192.168.7.173:8006/# □ xx/192.168.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.175.7.17	18:22:34 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6:2-4 前記 pre5上的虐 全 低観 >、 主空合 一 硬稿 Cloud-init 空 選項 二 作 集記器 雪 供命 古 渡 等	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主陸台 周 第監督尊大小 音号音译 64.00 GiB 16 (2 sockets, 8 cores) 劳动说 (SeeBIOS) 相音 VMWare (vmware) ID	★ ♥ 0 ■ ■ 取得文件 ■ 取得文 ■ 取得文 ■ 取得文件 ■ 取得文 ■ 取得 ■ 取 ■ 取得 ■ 取得 ■ 取得 ■ 取得 ■ 取得 ■ 取得 ■ 取 ■ 取得 ■ 取 ■ 取 ■ 取 ■ 取 ■ 取 ■ 取 ■ 取 ■ 取	OK ###: Failed to run vncproxy. - □
□月 18 18.22:33 +□月 18 に//192.168.7.173:8006/# □月 18 (* pre5 - Proxmox Virtual Environ - → C ▲ 不安全 19 (* PRO * MO * Virtual 電話物税 ● 106 (Ubuntu-LXC) ● 106 (Nextcioud-LXC) ● 106 (Nextcioud-LXC) ● 106 (Nextcioud-LXC) ● 106 (Nextcioud-LXC) ● 106 (Nextcioud-LXC) ● 106 (VIN2016-1) ● 104 (VIN2016-2) ● 105 (VIN2019) ● 105 (VIN2019) ● 105 (VIN2019) ● 105 (VIN2019) ● 107 (VIN2015-2) ● 109 (PrimeOS) ● 110 (Mac10 15 5)	18:22:34 pre5 18:22:33 pre5 × + 2:168.7.173:8006/# Environment 6 2-4 前証 pre5 上的信 ● 項釈 > 主控台 ● 項釈 > 主控台 ● 項釈 > 主控台 ● 項釈 > 主控台 ● 項釈 > 主控台 ● 項釈 > 二 主控台 ● 項釈 ● 二 音	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主控台 用 國際管理大小 連接管理 64 00 GIB 16 (2 sockets, 8 cores) 预設 (SeaBIOS) 相容 VMWare (vmware) ID ID	☆ № 0 ■ <i>■</i> 取得文件 ● 相影 0 ■ 高野 Size=100G Size=100G Size=100G	OK #認: Failed to run vincproxy. - □ ● <t< td=""></t<>
□月 18 18.22:33 +□月 18 に//192.168.7.173:8006/# □月 18 (* pre5 - Proxmox Virtual Environ - → C ▲ 不安全 19 (* PRO × MO × Virtual では、 では、 では、 では、 では、 では、 では、 では、	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6 2-4 節點 pre5 上的總 @ 低觀 > 上空台 @ 優觀 > 上空台 @ 優觀 @ Cloud-Init @ 擬項 @ 先記語 @ 低句 12 使第 @ 低句 12 使第	root@pam root@pam root@pam v1:0:=qemu%2F100:4:::::7:2 度变 度变 度变 度变 度变 度变 度变 度变 度变 度变 度变 度变 度变	VM 242 - 啓動 VM/CT 242 - 主控台 VM/CT 242 - 主控台 64.00 G/B 16 (2 sockets, 8 cores) 劳원 (SeaBIOS) 相合 VM/Ware (vmware) 10 10 10 10 10		OK #詳述: Failed to run vincproxy. - □ # ## ● ♥ ● ■ ★ ● # ### ● ■ ★ ● # #### ● #### ● # # #### ● #### ● # # ##### ● #### ● # # ########
□月 18 18.22:33 +□月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □月 18 x://192.168.7.173:8006/# □ x://192.168.7.173:8006/# □ x://192.173:8006/# □ x://192.	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6 2:4 節話 pre5 上的總 - 建築台 - 建築台 - 建築 - Cloud-Init - 建築 - 低観 - 主整台 - 建築 - 建築 - 2 使第 - 3 使 - 3 - 3 使 - 3 使	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主控台 VM/CT 242 - 主控台 64.00 G/B 16 (2 sockets, 8 cores) 防원 (SeaBIOS) 相言 VM/Ware (vmware) 1D 1D 1D 1D 155 SanDisk		OK 維持: Failed to run vincoroxy. - ロ ・ ・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・
□月 18 18.22.33 +□月 18 sc//192.168.7.173:8006/# □月 18 sc//192.168.7.173:8006/# □月 18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19 ※ PPC> × MO × Virtual ※ pve5 ● 106 (Ubuntu-LXC) ● 108 (NextCloud-LXC) ● 109 (VIN2016-1) ■ 101 (WIN2016-1) ■ 102 (android) ■ 103 (TrueNAS) ■ 104 (UNRA1D-usb) ■ 105 (WIN2019) ■ 107 (WIN2016-2) ■ 109 (PrimeOS) ■ 110 (Ms101 5.5) ■ 111 (WIN10) ■ 130 (vSphere6) ■ 140 (vSphere6,7)	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6:2-4 節話 pre5 上的總 - 重短台 - 運現 - 正短台 - 運現 - 「使留 - Cloud-Init - 運用 - 「使留 - 「使留 - 「使留 - 「「」」 - 「使留 - 「」 - 「使留 - 「」 - 「「」 - 「」 - 「」	root@pam root@pam root@pam v1:0:=qemu%2F100:4:::::7::2 度克 (日本) 度克 (日本) 度克 (日本) (別) (WIN2016-1) (日本) (日本) (日本) (別) (WIN2016-1) (日本) (日本) (日本) (日本) (日本) (日本) (日本) (日本	VM 242 - 啓動 VM/CT 242 - 主控台 VM/CT 242 - 主控台 64.00 G/B 16 (2 sockets, 8 cores) 劳政 (SeaBIOS) 相音 VM/Ware (vmware) ID Inrough 指定裝置 製造商 S5 SanDisk		OK #課: Failed to run vincproxy. - □ ● ● ♥ ● ■ ■ ● ♥ ##2: Vial ● ##2: CT ● mode@art E ♥ ● ↓ ● ♥ ##2: Vial ● ##2: CT ● mode@art E ♥ ● ♥ ● ■ ● ♥ ##2: Vial ● ##2: CT ● mode@art USB 2:0
□月 18 18 22.33 +□月 18 ss//192.168.7.173:8006/# □月 18 ss//192.168.7.173:8006/# □月 18 文 pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19 (PRO×MO× Virtual R 田谷(NextCoud-LXC) 0 106 (Ubuntu-LXC) 0 106 (Ubuntu-LXC) 0 106 (Ubuntu-LXC) 0 106 (WinZ016-1) 101 (W20167escuecton 102 (android) 103 (TrueNAS) 104 (UNRAID-usb) 105 (VINZ016-2) 106 (PinmeOS) 110 (Mac10.15.5) 111 (WIN10) 130 (Vsphere6) 140 (Vsphere6) 140 (Vsphere6 7) 150 (ubuntu)	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 前點 pre5 上的總 星 項限 2: 主控台 二 運精 低 (Coud-Init 章 選項 圖 作業記録 章 換器 習 情份 1: 複寫 2: 複麗	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主陸台 相 四五皆日大小 唐母皆田 64 00 G/B 16 (2 sockets, 8 cores) 劳政 (SeaBIOS) 相音 VM/Ware (vmware) 1D 1D 10 55 SanDisk		OK 발訣: Failed to run vncproxy. -
□月 18 18.22.33 +□月 18 ss/192.168.7.173:8006/# □月 18 ss/192.168.7.173:8006/# □月 18 ※ pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19 ※ PRO × MO × Virtual ※ pve5 ● 106 (Ubuntu-LXC) ● 106 (Ubuntu-LXC) ● 106 (Ubuntu-LXC) ● 106 (Ubuntu-LXC) ● 108 (Nextcloud-LXC) ● 109 (Nextcloud-LXC) ●	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168.7.173:8006/# Environment 6:2-4 前記 pre5 上的處 @ 弧観 > 主控合 @ 弧観 > 主控合 @ 弧観 @ 弧間 @ 弧 @ 弧 @ 弧 @ 弧 @ 弧 @ 弧 @ 弧 @ 弧	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主控台 相 如如音 25 (SeaBlOS) 相音 VM/Ware (vmware) 10 roough 指定装置 复始商 55 SanDisk	★ ▲ 訳明文作 ■ 説明文作 正部 Support 正部 Support	OK 推測: Failed to run vncproxy. - □ ● ● + ● ● ● ● ● ● ● ■ 100 @ #110 CT ● 100 @ PAT ■ 201 @ #120 CT ● 100 @ PAT ■ 201 @ PAT ■ 20
□月 18 18:22.33 +□月 18 ss//192.168.7.173:8006/# □月 18 ss//192.168.7.173:8006/# □月 18 web = Proxmox Virtual Environ → C ▲ 不安全 1 19 C ● PRO VIrtual R 28 始 袍 ○ ● Pro5 ○ 106 (Ubuntu-LXC) ○ 108 (NextCloud-LXC) ○ 109 (NextCloud-LXC) ○ 103 (TURNAD-usb) □ 103 (TURNAD) □ 103 (TURNAD) □ 103 (VIN2016-2) □ 109 (PinteOS) □ 110 (W102016-2) □ 109 (PinteOS) □ 110 (W1010) □ 130 (VSphere6) □ 140 (VSphere6) □ 140 (VSphere6) □ 150 (ubuntu) □ 154 (ubuntu-arm64) □ 160 (FreeNAS)	18:22:34 pre5 18:22:33 pre5 18:22:23 pre5 × + 2:168:7.173:8006/# Environment 6 2-4 節點 pre5 上的慮 - 低額 - 正控台 - 低額 - 正控台 - 低額 - Coud-Init - 運項 - 生控台 - 低額 - Coud-Init - 運項 - 生控台 - 低額 - (Coud-Init) - 生控台 - 低額 - (Coud-Init) - 生控台 - 低額 - (Coud-Init) - 生控台 - 低額 - (Coud-Init) - 生控台 - (Coud-Init) - 生使語 - (Coud-Init) - (Coud-Init	root@pam ro	VM 242 - 啓動 VM/CT 242 - 主控台 用 四型目標大小 串号目標 64 00 GIB 16 (2 sockets, 8 cores) 预設 (SeaBIOS) 相容 VMWare (vmware) ID ID ID ID ID ID ID ID ID ID ID ID ID	★ ■ 0 ■ ■ 取取文件 ■ 取取 ■ 取取	OK ###: Failed to run vincproxy. - □ ● ●
□月 18 18.22.33 +□月 18 sc/192.168.7.173:8006/# □月 18 (*) (*) (*) (*) (*) (*) (*) (*)	18:22:34 pre5 18:22:23 pre5 18:22:23 pre5 * + 2:168:7.173:8006/# Environment 6:2.4 節鼓 pre5 上的總 ● 模型 ● Cloud-Init ● 建築 ● Cloud-Init ● 重整器 ● 信号 ● 支援第 ● 情景 ● 重要器 ● 低観 ● 支援第 ● 電影 ● 電影 </td <td>root@pam ro</td> <td>VM 242- 啓動 VM/CT 242 - 主控台 VM/CT 242 - 主控台 d4 00 G/B 16 (2 sockets, 8 cores) 劳起 (SeaBIOS) 相容 VM/Ware (vm/ware) ID ID ID ID ID ID ID ID ID ID ID ID ID</td> <td> ★ ▲ 武明文件 ▲ 武明文件</td> <td>OK ###: Failed to run vincproxy. - O + O + Image: Comparison of the state of the stat</td>	root@pam ro	VM 242- 啓動 VM/CT 242 - 主控台 VM/CT 242 - 主控台 d4 00 G/B 16 (2 sockets, 8 cores) 劳起 (SeaBIOS) 相容 VM/Ware (vm/ware) ID ID ID ID ID ID ID ID ID ID ID ID ID	 ★ ▲ 武明文件 ▲ 武明文件	OK ###: Failed to run vincproxy. - O + O + Image: Comparison of the state of the stat
□月1818.22.33 +□月18 sc/192.168.7.173:8006/# □月18 (* pve5 - Proxmox Virtual Environ - → C ▲ 不安全 19 (* PRO×MO× Virtual Environ - → C ▲ 不安全 19 * DO (Ubuntu-LXC) - → 106 (Ubuntu-LXC) - → 106 (Ubuntu-LXC) - → 106 (Vin2016-1) - → 101 (Win2016-1) - → 102 (android) - → 102 (android) - → 103 (TrueNAS) - → 104 (UNR2016-2) - → 109 (PrimeOS) - → 109 (PrimeOS) - → 109 (Vin2019) - → 107 (Win2016-2) - → 109 (PrimeOS) - → 109 (Vin2019) - → 109 (Vin2	18:22:34 pre5 18:22:33 pre5 × + 2:168.7.173:8006/# Environment 6 2.4 節話 pre5 上的網 一 優親 - 注陸台 - 優親 - ごを留 - Cloud-Init - 選項 - 作業記器 - 簡整 - 機關 - 使用 - で - で - で - で - で - で - で - で	root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam root@pam reserved ges ges ges ges ges ges ges ges ges ges	VM 242- 啓動 VM/CT 242 - 主控台 PM/CT 242 - 主控台 A 400 CiB 16 (2 sockets, 8 cores) 防辺 (SeaBIOS) 相言 VM/Ware (vmware) ID ID ID ID ID S5 SanDisk	 ★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	OK ##E: Failed to run vincproxy. - O * O * Image: State of the state of
□月 18 18.22.33 +□月 18 x x y x y x x y x x y x x y x y x x x y x y x	18:22:34 pre5 18:22:33 pre5 × + 2:168:7.173:8006/# Environment 6:2-4 節點 pre5 上的網 - 低報 - 低 - 低報 - 低 - 低 - 低 - 低 - 低 - 低 - 低 - 低	root@pam ro	VM 242- 啓動 VM/CT 242 - 主陸台 (1) (2) (2) (2) (2) (2) (2) (2) (2) (2) (2	 ★ ◆ ◆	OK ###: Failed to run vinceroxy. - - · · ·

🕻 pve5 - Proxmox Virtual Enviror	× +			-	- 🗆 ×
→ C ▲ 不安全 19	2.168.7.173:8006/	#v1:0:=qemu%2F10	0:4::::7::2	🖈 🗣 🖸 💶 🕑 🕫 🕈 🚳	* 🕸 :
	I Environment 6.2-4			📑 說明文件 두 建立 VM 🕞 建立 CT	a root@pam
	─ 節點 pve5 上的	重挺機 100 (WIN2016-1		▶ 啓動 ① 開機 ∨ >_ 主控台 ∨ 更	(S V 0 说明
∰ 資料中心	A (5.31				
pve5					
106 (Ubuntu-LXC)		111 記憶體	64.00 0		
108 (Nextcloud-LXC)	♀ 硬體	● 成現器	16 (2 s	ockets, 8 cores)	
101 (W2016rescuerion	Cloud-Init	BIOS		eaBIOS)	
	• 選項	山 顕示卡		/IWare (vmware)	
103 (TrueNAS)	■ 作業的知	0 % 機器架構		40fx)	
104 (UNRAID-usb)		装置		\otimes	
105 (WIN2019)	۲				
107 (WIN2016-2)	管 装置:	0000:04:00.0) Y MDe	/ 類型: 🔹 🗸 🗸	
109 (PrimeOS)	□ 所有功能:	ID↑ IO.		装置	Media
🔲 110 (Mac10.15.5)	o —	0000:00:11.0 6	Intel Corporation	C610/X99 series chipset SPSR	否
111 (WIN10)	ROM-Bar	0000:00:11.4 6	Intel Corporation	C610/X99 series chipset sSATA Controller [AHCI mode]	否
130 (vSphere6)		0000:00:14.0 7	Intel Corporation	C610/X99 series chipset USB xHCI Host Controller	否
140 (vSphere6.7)	 ② 說明 	0000:00:16.0 8	Intel Corporation	C610/X99 series chipset MEI Controller #1	否
150 (ubuntu)		0000:00:16.1 8	Intel Corporation	C610/X99 series chipset MEI Controller #2	否
160 (EccoNAS)	÷	0000:00:1a.0 9	Intel Corporation	C610/X99 series chipset USB Enhanced Host Controller #2	否
TOUTFIEENAST		0000:00:1d.0 13	Intel Corporation	C610/X99 series chipset USB Enhanced Host Controller #1	否
業業業記録		0000:00:1f.2 14	Intel Corporation	C610/X99 series chipset 6-Port SATA Controller [AHCI mode]	否
		0000:01:00.0 15	Intel Corporation	82599ES 10-Gigabit SFI/SFP+ Network Connection	否
月 18 14:49:56	pve	0000:01:00.1 16	Intel Corporation	82599ES 10-Gigabit SFI/SFP+ Network Connection	否
		0000:02:00.0 17	LSI Logic / Symbi	MegaRAID SAS-3 3008 [Fury]	否
月 18 18:22:37 十二月 1	8 18:33:05 pve			242 - 主控台 OK	
■ 18 18 22 Ste	p2:	選擇	Ĕ 安透	通的PCI裝置	
	£ 192.168.7.173:80	06/#v1:0:=qemu%2F1	00:4:/::	3 ② 中 份 🔟 🚺 🗘 🛍 文	¶ \$¥ ∰ :
× PRO×MO×	Virtual Environment 6.	2-4 搜尋	_	2 說明文件 ↓ 建立 VM 2 建立 CT	🤮 root@pam 🗸
伺服器檢視		的虛擬機 100 (WIN2016	-1)	▶ 含動 Ů 開機 ∨ ▶ 主控台 ∨ 更	ē多 ∨ 🔞 說明
✓ 重 資料中心 ✓ ■ nve5	▲ 根觀	増加 ~ 利	\$法 编辑 調整磁碟力	小 運移磁碟 還原	
106 (Ubuntu-LXC	>) >_ 主控台	■ 記憶體	64.00 Gil	3	
108 (Nextcloud-L	XC) 🖵 硬體	● 處理器	16 (2 soc	kets, 8 cores)	
100 (WIN2016-1	Cloud-Ir	BIOS	預設 (Se	aBIOS)	
101 (W2016resc)	uecion 古谜面	➡ 願示卡	相容VM	Nare (vmware)	
102 (android)	 ▲ 2 ● 作業±2± 	 機器架構 	預設 (i44	Ofx)	
104 (UNRAID-us	b)	SCSI 控制器	VirtIO SC	SI	
105 (WIN2019)	● 三陸器	⊖ 使碟 (virtio0)	RAID:vm	100-disk-0,size=50G	
🖵 107 (WIN2016-2	四 備份	Carter (virtio1)	RAID:vm	100-disk-1,cache=uhsate,size=100G	
109 (PrimeOS)	13 複寫	□ 10 10 10 10 10 10 10 10 10 10 10 10 10	t0) virtio=34	23:A8:8C:3A:99 bridge_wmbr0 firewall=1	
110 (Mac10.15.5) ③ 快照	→ 約840 40 (06)	at1) virtio=CA	7C:4D:60:E5:ED bridge-umbri frowall=1	
444 /LA/IA14/01			VIII00-001	10.4D.00.F3.FD,blidge=vilibi1,lifewali=1	

130	(vSphere6)	♥ 80 大 ## P	📟 PCI装置 (hostpci0)	04:00.0		
L 140	(vSphere6.7)	▲ 楣限	📟 PCI 装置 (hostpci1)	82:00.0		
150	(ubuntu)					
L 154	(ubuntu-arm64)					
L 160	(FreeNAS)					
作業 選集	記錄					
開始時間↓	結束時間	前湯占	帳號	說明	狀態	
十二月 17 21:0	7:45	pve5	root@pam	命令列	and the second se	-
十二月 18 11:1-	4:01	pve5	root@pam	VM/CT 100 - 主控台		
十二月 18 14:3	5:59 十二月 18 1	14:36:00 pve5	root@pam	VM 240 - 建立	ОК	
十二月 18 11:3	3:23 十二月 18 1	12:44:39 pve5	root@pam	命令列	ОК	
十二月 18 11:1	3:49 十二月 18 1	11:14:18 pve5	root@pam	VM 100 - 啓動	ОК	*

Step4: 設定完成後, 虛擬機即

可存取實體裝置

SLah

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/

erver View ~	Virtual Machine 154 (u	ubuntu-arm64) on nod	le 'pve5'
	Summary	star	ting serial terminal on interface serial0
100 (WIN2016-1)	>_ Console		
101 (W2016riscueclone)	Hardware		
102 (android) 103 (TrueNAS)	Cloud-Init		
105 (WIN2019)	Options		nyeE Draymay Cancele Mazilla Firefay
107 (WIN2016-2)	🔳 Task History		pves - Proxiliox Console - Mozilia Pilelox
110 (Mac10.15.5) 130 (vSphere6)	Monitor		https://192.168.7.173:8006/?console=kvm&xtermjs=1&vmid=154&vmname=ubuntu-arm64&node=pve5&cmd=
140 (vSphere6.7)	🖺 Backup		GNU GRUB version 2.04
150 (ubuntu)	Replication		
152 (ubuntu-arm64)	Snapshots	/	v Ubuntu Server without installing
🗣 154 (ubuntu-arm64)		*In	stall Ubuntu Server
160 (FreeNAS)		I OE	M install (for manufacturers)
162 (PhoenixOS)	Permissions		
164 (elementaryos)		- i ;	i i
PVE5_NFS (pve5)			
RAID (pve5)			
local (pve5)		i i	i
local-lvm (pve5)			
🛢 🗋 pve5_esxi (pve5)			/
			/
			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

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

PVE掛載實體硬碟的方法
增加: virtio0: /dev/disk/by-id/ata-XXXXXXXX,size=XXXG
nano etc/pve/qemu-server/100.conf
<pre>ls -l /dev/disk/by-id/</pre>

Windows的NFS共享設定

Windows可啟用NFS Server

PVE的NFS共享設定

	152.100.1.115.0	000,	TO: TO					2
(PROXMOX v	rtual Environment 6	6.2-4 搜尋			의 說明文件] 建立 VM 😭 建1	跎 CT 🔒 rooti	@pam
服器檢視	~ 資料中心							0 19
 102 (android) 103 (TrueNAS) 104 (UNRAID-usb) 105 (WIN2019) 107 (WIN2016-2) 109 (PrimeOS) 110 (Mac10.15.5) 111 (WIN10) 130 (vSphere6.7) 150 (ubuntu) 154 (ubuntu-arm64 160 (FreeNAS) 	▲ Q 授号 - 一 假眼 	~	増加 移除 第 Directory LVM LVM-Thin GusterFS GusterFS GlusterFS GusterFS RBD ZFS over iSCSI TFS	 胡 內容 FS VZDump 傳份檔案, 磁碟映 FS 碰碟映像, 容器 ire VZDump 傳份檔案, ISO 映 vM 碰碟映像, 容器 FS VZDump 傳份檔案, 磁碟映 	弊徳/目標 /mnt/pve/PVE5 /var/libi/vz /mnt/pve/pve5	共用 飲用 定 こ 百 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 こ 日 日	頻寬限制	
152 (PrideinkUS) 164 (elementaryOS) 250 (0910041) PVE5_NFS (pve5) RAID (pve5) Iocal (pve5) Iocal-lvm (pve5) Ip ve5_eski (pve5)	▲ 帳號 ▲ API 響 群縦 ● 集團 ■ 角色	Tokens	Ste	p1: 選排	睪NFS	S		
	▲ 帳號 ▲ API 響 群維 ● 集團 ● 介倉 ● 一 一 一 、 →	€ Tokens ⊒ ≦ → ◆	Ste	p1: 選招	睪NF领	S 		
 152 (Pr0enRUCS) 164 (elementaryOS 250 (0910041) 目 PVE5_NFS (pve5) 目 RAID (pve5) 目 local (pve5) 目 local-lvm (pve5) 目 pve5_esxi (pve5) 作業 叢集記録 始時間 ↓	▲ 帳號 ▲ API 筆 群総 ● 集團 ● 角色 - 一一、、 時間	tokens Tokens 重 節點 pve5	Ste Ste	p1: 選招	睪NF领	S 	0	
	▲ 橋號 ▲ 杯記 ● API 筆 群縦 ● 集團 ● 角色 - ~~~、 平 - ~~~、 - ~~~、	tokens token	ME Ste root@pam root@pam	p1: 選控	睪NF领	S 款應	¢	
	▲ 儒璧 ▲ 保健 ● API 響 群縦 ● 集團 ● 角色 - ~ ~ ~ 平 同 目 11:14:18	tokens minimum min	作號 root@pam root@pam	p1: 選挑	睪NFS	S	¢	
	▲ 儒璧 ▲ 保健 ● API 響 群縦 ● 集團 ● 角色 - ~ ~ ~ 時間 目 18 11:14:18 同 18 03.45:49	で Tokens	低いための の の の の の の の の の の の の の の の の の の	p1: 選挑 說明 命令列 VM/CT 100 - 主控台 VM 100 - 啓動 更新套件資料庫	₩F	S 款應 OK 續該.com	Kana and apt-get up	od
tb2 (PriosinuOS) tb3 (elementaryOS tb3 (elementaryO	▲ 佛號 ▲ 相對 ▲ API 筆 群組 ● 集團 ● 角色 - 一一一 平 日 18 11:14:18 日 18 03:45:49 日 17 02:06:08	で Tokens	Fot@pam root@pam root@pam root@pam	p1: 選好 於明 命令列 VM/CT 100 - 主控台 VM 100 - 留點 更新言件資料庫 更新言件資料庫	₩F	S	anand 'apt-get up	od

PVE可加入Windows的NFS Server

★ pres - Proxymox Console - ▲ 不安全 192.168.7.17 root@pve5:-# cat /e dir: local path /var/1 content bac Ivmthin: local-lvm thinpool da vgname pve content imac Ivmthin: local-lvm thinpool da vgname pve content imac Infs: PVE5_NFS export /RAII path /mnt/p server 192. content root maxfiles 1 Ifs: PVE5_NFS Export /RAII path /mnt/p server 192. content root maxfiles 1 Ifspool: RAID pool RAID content root mountpoint , sparse 0 Ifs preserver * * * preserver vertex * * * preserver vertex * * * preserver vertex * * * preserver * * * preserver **	Google Chrome – 3:8006/?console=shell&xtermjs=1&v tc/pve/storage.cfg ib/vz kup,vztmpl,iso ta ges,rootdir D ve/PVE5_NFS 168.5.173 tdir,vztmpl,iso,backup,images
▲ 不安全 192.168.7.17 root@pve5:~# cat /e dir: local path /var/l content bac lvmthin: local-lvm thinpool da vgname pve content ima ffs: PVE5_NFS export /RAI path /mnt/p server 192. content roo maxfiles 1 zfspool: RAID pool RAID content roof mountpoint , sparse 0 pve/Learner VFES_NFS() ************************************	3:8006/?console=shell&xtermjs=1&v tc/pve/storage.cfg ib/vz kup,vztmpl,iso ta ges,rootdir D ve/PVE5_NFS 168.5.173 tdir,vztmpl,iso,backup,images
wd:-homov/tul/fere ************************************	tc/pve/storage.cfg ib/vz kup,vztmpl,iso ta ges,rootdir D ve/PVE5_NFS 168.5.173 tdir,vztmpl,iso,backup,images
vgname pve content ima	ges,rootdir D ve/PVE5_NFS 168.5.173 tdir,vztmpl,iso,backup,images
Storaget.crgg zfspool: RAID pool RAID content roo mountpoint sparse 0 we5-Proxmox Virtual Envice: X + C ▲ 不安全 192.168.7.173.8006/#v1:0:=storage%2FpvE5_NFS:4:19::::2 ★ ● ● ● ▲ 不安全 192.168.7.173.8006/#v1:0:=storage%2FpvE5_NFS:4:19::::2 ★ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
● Wirtual Environment 6.2.4 使者 ● 影明文件 (1) 02 (android) 前點 'pve5' 上鈴儲存' PVE5_NFS' 103 (TruenAS) ● 概觀 重排 種本 上面 順元設定内雨 103 (URRAID-usb) ● 104 (URRAID-usb) ● 一個限 包括 包括 ● 名 104 (URRAID-usb) ● 「● 個限 ● 個限 ● 日周 格式 105 (WIN2019) ● 「● 個限 ● 乙(III) ● 一個限 ● 乙(III) ● 回口(PrimeOS) ● 109 (PrimeOS) ● 101 (Uschore6.7) ● 「日回(III) ● 103 (Uschore6.7) ● 110 (Mixc10.15.5) ▼UZDump. 倒包括 (III) ● 104 (Uschore6.7) ● 100 (PrimeAS) ● 104 (Uschore6.7) ● 105 (Uschoru) ● 105 (Uschoru) ● 100 (PrimeAAS) ● 100 (PrimeAAS) ● 100 (PrimeAAS) ● 100 (Uschoru) ● 100 (PrimeAAS) ● 100 (PrimeAAS) ● 100 (PrimeAAS) ● 100 (Uschoru) ● 100 (PrimeAAS) ● 100	tdir,images /RAID - □ × • • • • • • • • • • •
	➡ 建立 VM 🛛 建立 CT 🔺 root@pam 🧹
102 (android) ● 信服 福田 修道 10 (Mac10 15 5) 110 (Mac10 15 5) 1130 (vSphere6) 111 (WiN10) 1330 (vSphere6) 130 (vSphere6) 130 (vSphere6) 140 (vSphere6,7) vzdump-qemu-305-2020_06_19.19_33_06 vma zst 2020-06-29 19.33.06 vma zst 2020-06-29 19.33.06 vma zst 2020-06-29 19.33.06 vma zst 2020-06-29 17.21.06 qccw2 vm-109-disk-0 qccw2 vm-111-disk-0 qccw2 2020-10-27 17.21.06 qccw2 vm-202 2020-10-26 00 26.55 qccw2 150 (kbufus 150 (kbufus 150 (kbufus 150 (cb file (21 ltems)) 150 (cb file (21 ltems) 150	● 起明
104 (UNRAID-usb) 単 内容 名領 日期 格式 105 (WIN2019) ● 保限 ● 保限 ● VZDump 偶份懂案 (4 Items) ● VZDump qgmu-300-2020_06_24.10_50_15 vma.zst 2020-06-24.10_50.15 vma.zst 2020-06-23.16_02.58 vma.zst 2020-06-23.16_02.58 vma.zst 2020-06-23.16_02.58 vma.zst 2020-06-23.16_02.58 vma.zst 2020-06-19.19.33.06 vma.zst 2020-06-19.19.33.06 vma.zst 2020-06-19.19.33.06 vma.zst 2020-06-19.19.33.06 vma.zst 2020-01-02.07.17.21.06 qcov2 vzdump-qemu-302-2020_06_19.19.33_06 vma.zst 2020-10-27.17.21.06 qcov2 vmr.110-sk-0.45.0 qcov2 vmr.110-sk-0.45.0 qcov2 2020-10-26.00.26.55 qcov	搜尋:
107 (WIN2019) YZDump 借价推定 (4 Items) 107 (WIN2016-2) YZdump-qemu-110-2020_06_24+10_50_15 vma.zst 2020-06-24 10 50.15 vma.zst 109 (PrimeOS) Yzdump-qemu-300-2020_06_23-16_02_58 vma.zst 2020-06-23 16.02.58 vma.zst 110 (Mac10.15.5) Yzdump-qemu-300-2020_06_12-16_04_54 vma.zst 2020-06-19 19.33.06 vma.zst 130 (Vsphere6) Yzdump-qemu-302-2020_06_19-19_33_06 vma.zst 2020-06-19 19.33.06 vma.zst 140 (Vsphere6.7) Yzdump-qemu-302-2020_06_19-19_33_06 vma.zst 2020-06-19 19.33.06 vma.zst 150 (ubuntu) Hittinsk-0 qcow2 2020-10-27 17.21.06 qcow2 150 (ubuntu) ISO 除像 (21 Items) ISO 除像 (21 Items)	類別 大小
140 (vSphere6.7) 日 磁磁铁像 (2 Items) 150 (ubuntu) vm-109-disk-0 qcow2 2020-10-27 17:21:06 qcow2 154 (ubuntu-arm64) vm-111-disk-0 qcow2 2020-10-26 00:26:55 qcow2 160 (FreeNAS) El ISO 鉄像 (21 Items) El ISO 鉄像 (21 Items)	VZDump 11.08 GIB VZDump 579.58 MIB VZDump 3.66 GIB VZDump 10.68 GIB
162 (PhoenixUS)	磁磁映像 32.00 GIB 磁磁映像 64.00 GIB
164 (elementaryOS) ComputerSystem/2013.iso 2020/09.24 11.02.21 iso 250 (0910041) EasyU_v3 5.iso 2020.09.17 15.44.54 iso 2 FPVES.pKS (pve5) Fedora-Workstation-Live-x86_64.31.1.9.iso 2020.10.91 09.101 iso Phoenix/OSInstatiler_v3 6.1564_x64.iso 2020.10.23 16.06.43 iso D local (pve5) TrueNAS-12.0-RC1.iso 2020.09.19 20.49.14 iso	ISO 前像 608.33 MIB ISO 前像 780.33 MIB ISO 前像 1.80 GIB ISO 前像 850.00 MIB ISO 前像 826.38 MIB
2020-09-17 17 55 28 iso 2020-09-17 17 55 28 iso 2020-09-17 17 55 28 iso 2020-06-24 11 02 25 iso 2020-06-24 100 25 iso 202	

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

PVE的iSCSI啟動器設定

¥ pve5 - Proxmox Virtual En	viron × +)06/#v1:0:1	8:4:11:197.2			🕁 📴 🖸 🗖	(4)	中 🙉	N b Ø	3
	/irtual Environment 6	2-4 迎示	0.1.11.1.0.1.1.2			■ 說明文件 【] ≇t VM	1 建立 (CT A root@	pan
服器檢視	~ 資料中心	12.57							0	訳
■ 資料中心 ~ <mark>●●</mark> pve5			増加 > 移除	編明						
106 (Ubuntu-LXC)	■ 柳期		Directory	類別	內容	路徑/目標	共用	啟用	頻寬限制	
108 (Nextcloud-LX)	C)			NFS	磁碟映像, ISO 映像	/mnt/pve/NFS-174	是	是		
100 (WIN2016-1)	國 黃集		NES	NFS	VZDump 備份檔案, 磁碟映	/mnt/pve/PVE5	是	是		
101 (W2010fescue 102 (android)	@ Ceph		CIES	ZFS	磁碟映像, 容器		否	是		
102 (android) 103 (TrueNAS)	✿ 選項		GlusterFS	Direc	VZDump 備份檔案, ISO 映	/var/lib/vz	否	是		
100 (Inden (G))	● 儲存		iscsi "	LVM	磁碟映像, 容器		否	是		
105 (WIN2019)	周 備份		CephFS	NFS	VZDump 備份檔案, 磁碟映…	/mnt/pve/pve5_e	是	是		
107 (WIN2016-2)			RBD							
109 (PrimeOS)	€ 復易		ZFS over iSCS		جر – <u>ب ا</u> ر	7 .0		100	1000	
🔲 110 (Mac10.15.5)	● 權限	~	E ZFS	er	り1・在宅	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	11.3	Z至	珸	
111 (WIN10)	▲ 柳長号虎					ミリオ・レ・	' U'		JŦ	
130 (vSphere6)	& API	Tokens		_						
140 (vSphere6.7)	😁 群組				学方 立	+畝:C	~			
150 (ubuntu)				16	伯1千。木川	「「」	しこ	DI		
作業 蔵集記録										
					0.00			Do dogle		
始時間↓ 結束	時間	節點	中辰 號虎	â,	尼均		7	仄想		
始時間↓ 結束 二月 21 15:02:11	時間	節點 pve5	帳號 root@pam	AL AL	元时 5令列		7	人態	3	
始時間↓ 結束 二月 21 15:02:11 二月 21 15:06:00 +二	時間 口 月 21 15:06:02	節點 pve5 pve5	帳號 root@pam root@pam	and An	元时 11令列 11令列		C	DK	*	
始時間↓ 結束 二月 21 15:02:11 二月 21 15:06:00 +二 二月 21 15:01:59 +二	時間 月 21 15:06:02 月 21 15:02:00	前點 pve5 pve5 pve5	帳號 root@pam root@pam root@pam		^{R时} 5令列 M/CT 100 - 主控台		C	K版 K #誤: Failed t	to run vncproxy	
始時間↓ 結束 二月 21 15:02:11 - 二月 21 15:06:00 + 二月 21 15:01:59 + 二月 21 15:01:59 + 二月 21 15:01:26 +	時間 月 21 15:06:02 月 21 15:02:00 月 21 15:01:27	前點 pve5 pve5 pve5 pve5	作反號 root@pam root@pam root@pam root@pam		8時 8 숙列 8 숙列 M/CT 100 - 主控台 M/CT 100 - 主控台		C ŝ	OK 計誤: Failed t 計誤: Failed t	to run vncproxy to run vncproxy	

X pve5 - Proxmox Virtual Enviro	• × +								- 0	×		
← → C ▲ 不安全 1	92.168.7.17	'3:8006/#v1:0:=qe	mu%2F100:4:11:19:::	7::2		4	. 0	4 🛞 😢 🕈	0 🖪 🖈 🦉	9 :		
	al Environme	ent 6.2-4 /注意					📕 說明文件		立 CT 🔒 root@p	am 🗸		
		ve5 上的虛擬機 100	(WIN2016-1)			1	▶ 脅動 ① 器		/ 更多 √ 0	說明		
✓ 量 資料中心 ✓ 量 資料中心 ✓ ■ pve5	Ê (6)					遠原	•••	-				
106 (Ubuntu-LXC)			(c)a	64	LOD GIB		Sto	n4·		DN	/F (
108 (Nextcloud-LXC)	口 硬	增加: 使保						ρт.				
101 (W2016rescuector	📥 Ck	匯流排/裝置:	VirtlO Block V 3	\bigcirc	快取: 預	設 (無快取)	~	-				
102 (android)	• 33	儲存:	iSCSI	\sim	Discard:		シロ	立口	计网工	` ++'	ᅚᄈᇚᆂ	
103 (TrueNAS)	Ⅲ 作:	磁碟映像:	CH 00 ID 0 LUN 0	~			い市	, 末 Л		44	们もしき	,
	• 1		Raw 磁碟映像 (raw)	2			- 11	(14.1		44		
	四 備								- -			
109 (PrimeOS)	13 夜				備份:		7	5÷ 77	`;睈+		+茴 +口	
110 (Mac10.15.5)	つ快	IO thread:			不要複寫:		Ī	\overline{M}	2天1	22 ,	「「」	
	0 防:	讀取限制 (MB/s):	不限制	$\hat{}$	最大突發讀取 (MB):	預設	\diamond			•		
140 (vSphere6 7)	- 福	寫入限制 (MB/s):	不限制	$\hat{}$	最大突發寫入 (MB):	預設	0	1				
		讀取限制 (ops/s):	不限制	\bigcirc	最大突發讀取 (ops):	预設	iCſ	rciz	ᄨᄪᇷ	10/		Ne
154 (ubuntu-arm64)	v	寫入限制 (ops/s):	不限制	$\hat{}$	最大突發寫入 (ops):	預設		JUIT	王旧	18	JLU	UD
作業 最集記錄										• •	-	
		☑ ±R==				進階 ⊵	1 增加					
十二月 21 19:41:38	.	pve5	root@pam						20	*		
十二月 21 15:02:11	—	pve5	root@pam						al al			
十二月 21 15:06:00 十二月	21 15:06:02	pve5	root@pam					OK				
十二月 21 15:01:59 十二月		pve5	root@pam	VN				錯誤: Faile	ed to run vncproxy.			
十二月 21 15:01:26 十二月	21 15:01:27	pve5	root@pam	VN	//CT 100 - 主控台			错誤: Faile	ed to run vncproxv.	Ŧ		

SSLab

iSCSI虛擬磁碟可在虛擬機開機

^ VMware Workstation

^ Proxmox VE

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

Win vs PVE 本機與網路的存取效能

🔚 CrystalDisk	«Mark 7.0.0 x64 [ADMIN] <real></real>		– 🗆 X
檔案(F) 設定	(S) 設定檔(P) 佈景主題(T) 說明	(H) 語言(Language)	
	5 ~ 8GiB ~ D: 85% (1	104148/122930GiB) ~	R70%/W30% ~
	Read [MB/s]	Write [MB/s]	Mix [MB/s]
SEQ1M	2508 20	2547 30	116.86
Q1T1	2300.29	2347.30	410.00
RND4K	5 69	15 21	0 0 0
Q1T1	5.05	13.21	5.50
RND4K	1300 1/	2712 87	2/25 55
(IOPS)	1550.14	5715.07	2433.33
RND4K	718 17	267.03	100 00
(μs)	10.17	207.05	409.90

^ 實體機 陣列直接存取速度(native

physical drive)

🔚 CrystalDisk	kMark 7.0.0 x64 [AI	DMIN] <real></real>		_	X
檔案(F) 設定	(S) 設定檔(P) 体	▶景主題(T) 說明(H) 語言(Language)		
	5 ~ 8GiB	~ E: 0% (0/	1024GiB) ~	R70%/W30%	~
	Read [l	MB/s]	Write [MB/s]	Mix [M	B/s]
SEQ1M Q1T1	1	07.39	<mark>1</mark> 05.48	10)6.54
RND4K Q1T1		3.19	6.02		4.45
RND4K (IOPS)	7	78.08	1468.75	108	35.94
RND4K (µs)	12	79.52	<mark>6</mark> 76.64	9 1	5.68

 PVE掛載iSCSI網路磁碟機的存取速度 (Gigabit 網路卡)

CrystalDiskM	lark 7.0.0 x64 [ADMIN] <real></real>		– 🗆 X
檔案(F) 設定(S) 設定檔(P) 佈景主題(T) 說明	(H) 語言(Language)	
All	5 ~ 8GiB ~ F: 0% (0/	1024GiB) ~	R70%/W30% ~
	Read [MB/s]	Write [MB/s]	Mix [MB/s]
SEQ1M	1357.07	1520.66	714.70
RND4K	5 5 1	15 60	7 97
Q1T1	5.51	15.00	1.01
RND4K	1245.05	2000 22	1001 14
(IOPS)	1345.95	3809.33	1921.14
RND4K	741.00	261.07	E10.22
(μs)	741.90	201.87	D 19.33

^ 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

🔚 CrystalDisk	(Mark 7.0.0 x64 [ADMIN] <real></real>		– 🗆 X
檔案(F) 設定	(S) 設定檔(P) 佈景主題(T) 說明	(H) 語言(Language)	
	5 ~ 8GiB ~ D: 85% (1	104148/122930GiB) ~	R70%/W30% ~
	Read [MB/s]	Write [MB/s]	Mix [MB/s]
SEQ1M	2508 20	2547 30	116.86
Q1T1	2300.29	2347.50	410.00
RND4K	5 60	15 21	0 0 0
Q1T1	5.09	15.21	9.90
RND4K	1200 1/	2712 97	2/25 55
(IOPS)	1590.14	5/15.0/	2455.55
RND4K	710 17	267 02	100 00
(μs)	10.17	207.05	409.90

^ 直接存取速度(native physical drive)

📑 CrystalDisl	kMark 7.0.0 x64 [ADMIN] <real></real>		– 🗆 X							
檔案(F) 設定	E(S) 設定檔(P) 佈景主題(T) 說明((H) 語言(Language)								
	5 ~ 8GiB ~ E: 0% (0/	1024GiB) ~	R70%/W30% ~							
	Read [MB/s]	Write [MB/s]	Mix [MB/s]							
SEQ1M Q1T1	<mark>1</mark> 07.39	<mark>1</mark> 05.48	<mark>1</mark> 06.54							
RND4K Q1T1	3.19	6.02	4.45							
RND4K (IOPS)	778.08	1468.75	1085.94							
RND4K (µs)	1279.52	<mark>6</mark> 76.64	<mark>9</mark> 15.68							

^ PVE掛載iSCSI網路磁碟機的存取速度 (Gigabit 網路卡)

🔚 CrystalDisk	Mark 7.0.0 x64 [ADMIN] <real></real>		– 🗆 X
檔案(F) 設定	(S) 設定檔(P) 佈景主題(T) 說明	(H) 語言(Language)	
	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	E E 1	15 60	7 07
Q1T1		15.00	1.01
RND4K	12/5 05	2000 22	1021 1/
(IOPS)	1545.95	5009.55	1921.14
RND4K	741 90	261 87	519 33
(µs)	1-1.50	201.07	5,55

^ 掛載成iSCSI磁碟的本機存取速度

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 -
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

- <u>https://github.com/diogo-fernan/ir-rescue</u>
- <u>https://www.brimorlabs.com/Tools/</u> <u>LiveRes</u> ponseCollection-Bambiraptor.zip
- <u>https://www.sans.org/readingroom/</u> whitepapers/forensics/liveresponsepowershell-34302

	IP : Port#	IP : Port#	Process ID	Process Name	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\ntdil.dll C:\WINDOWS\System32\www64.dll C:\WINDOWS\System32\www64win.dll C:\WINDOWS\System32\www64cpu.dll
						-	
	Local IP : Port#	Remote IP : Port#	Process ID	Process Name	Process Start Time	Process File Path	Associated DLLs and File Path
l							

Running Processes sorted by ParentProcessID

				T.	
ProcessName	CreationDate	ProcessId	ParentProcessId	CommandLine	sessionII
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\\$MFT" -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

- Sdelete
- ClearEventLog
- https://github.com/Rizer0/ Log-killer
- https://github.com/hlldz/In voke-Phant0m
- 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		
q	for /F "tokens-*" %%6 in ('weytuti]		el') DO (call :clear
10	echo		
11	echo.		
11	echo logs has deleted		
12	goto :theEnd		
13	timeout 5		
14	:clear		
15	echo [+] <i>%1</i>		
16	wevtutil.exe cl <mark>%1</mark>		
17	goto :eof		
18	:theEnd		
	cleartracks.php X		
74	<pre>\$LgE = shell exec('echo \$HISTETLE'):</pre>	9/	"¢l gE"
75	<pre>\$logFiles = array(</pre>	95	Ψ-5' ; "/etc/utmp"
76	"/var/log/yum.log",	96	"/etc/wtmp".
77	"/var/log/wtmp",	97	"/var/adm".
78	"/var/log/utmp",	98	"/var/log".
79	"/var/log/secure",	99	"/var/logs".
80	"/var/log/mysqld.log",	100	"/var/run/utmp",
81	"/var/log/boot.log",	101	"/var/apache/log",
82	"/var/log/lighttpd",	102	"/var/apache/logs",
83	"/var/log/httpd/",	103	"/usr/local/apache/lo
84	<pre>"/var/log/qmail/", "/var/log/qmail/",</pre>	104	"/usr/local/apache/lo
85	/var/log/maillog [*] ,	105	"/root/.bash_logout",
86 07	/var/log/cron.log , "/van/log/kann log"	106	"/root/.bash_history"
87 00	/var/log/kern.log , "/van/log/auth_log"	107	"/root/.ksh history",
00	/var/log/auth.log , "/van/log/moccogo"	108	"/tmp/logs",
90	/var/log/lastlog"	109	"/opt/lampp/logs/acce
91	/var/iog/iastlog"	110	"/var/log/nginx/acces
92	"/usr/adm/lastlog"	111	"/logs/agent lo",
93	"/var/log/lastlog".	112	"/logs/referer log",
94	"\$LgF",	113	"/logs/access log",
95	"/etc/utmp",	114	"/var/log/apache2",
96	"/etc/wtmp",	115	"/var/log/wtmp",

- 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<u>有誠信的外包商</u>.租設備也可

