

veeam



Veeam 三步驟帶你認真檢視資料與服務保護是否確實

王國浩 (Josh Wang)
Josh.wang@veeam.com



1

我們有什麼資料

2

多久備份

3

認識與導入



資料保護解決方案的領導者



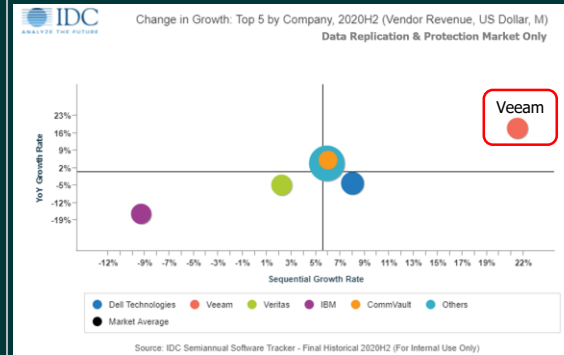
Veeam連續五年獲評為魔力象限領導者

Gartner: 2021 Magic Quadrant for Enterprise Backup and Recovery Software Solutions



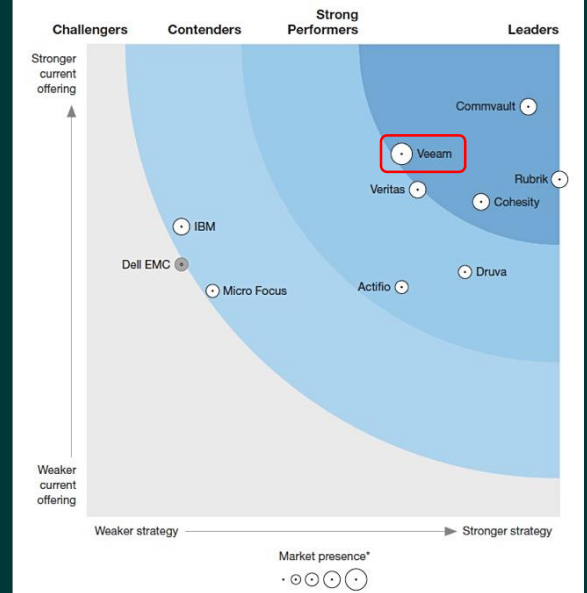
Source: Gartner (July 2021)

IDC: 2H20 Data Replication and Protection Growth Top 5 Companies by Market Share



Source: IDC, Semi-Annual Software Tracker, 2020H2
Note: Worldwide Data, circle size represents market share

Forrester Wave: Data Resiliency Solutions Q3 2019



Veeam 全方位雲端資料管理單一平台

雲端.

專為雲端供應商 AWS、Azure 和 GCP 構建的雲原生備份和恢復。

SaaS.

保護您的 Microsoft Office 365 資料，包括 OneDrive for Business 和 Teams，使企業組織可以降低資料遺失的風險。

應用程式.

加快應用程式，資料庫和容器的恢復。

虛擬.

Veeam 的虛擬化功能廣泛地保護了 VMware vSphere、Microsoft Hyper-V 和 Nutanix AHV。

實體.

保護您的非結構化 NAS 資料以及實體機和終端設備，包括 Windows、Linux、Mac、AIX 和 Solaris。

雲端



SaaS



應用程式



虛擬



實體



資料重複使用



協同作業



監控與分析



備份與備援



儲存、分析和
管理 APIs



地端資料中心



雲端公用雲



BaaS 與 DRaaS

資料再利用.

讓備份資料價值提升，可以應用在推動業務分析、決策還有系統測試/軟體開發。

協同作業.

使災難恢復計劃自動化，包括建置流程自動化、文件產出自動化和演練自動化。

監控與分析.

從資訊基礎架構中取得統一的人工智能驅動資料管理。

備份與備援.

為您的雲端、SaaS、虛擬、Kubernetes 和實體機等工作負載做集中化資料保護。

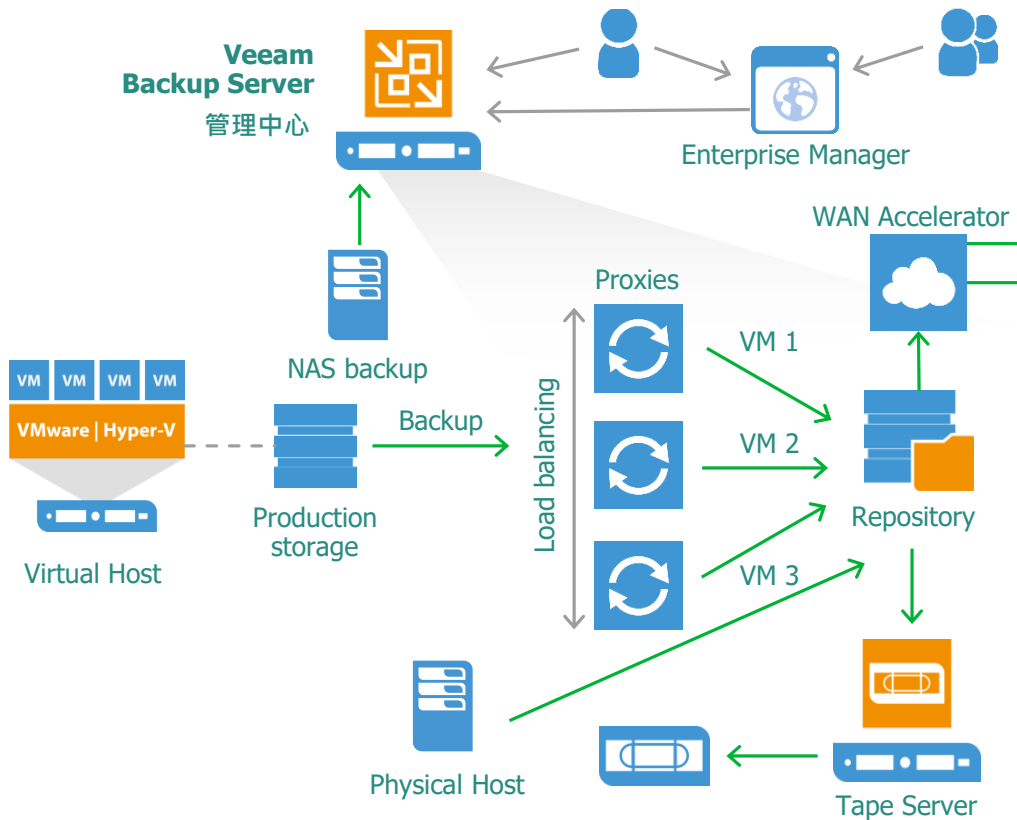
儲存、分析和 管理 APIs.

與眾多的解決方案和合作夥伴生態系統相互整合。

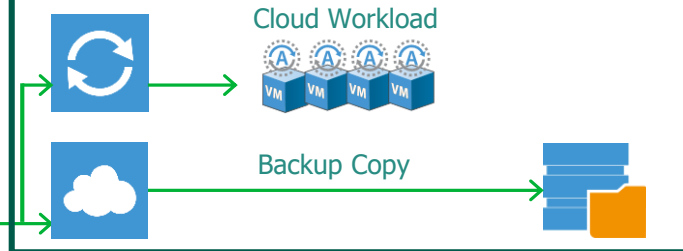
選擇最能滿足您獨特需求的服務平台。

Veeam 架構

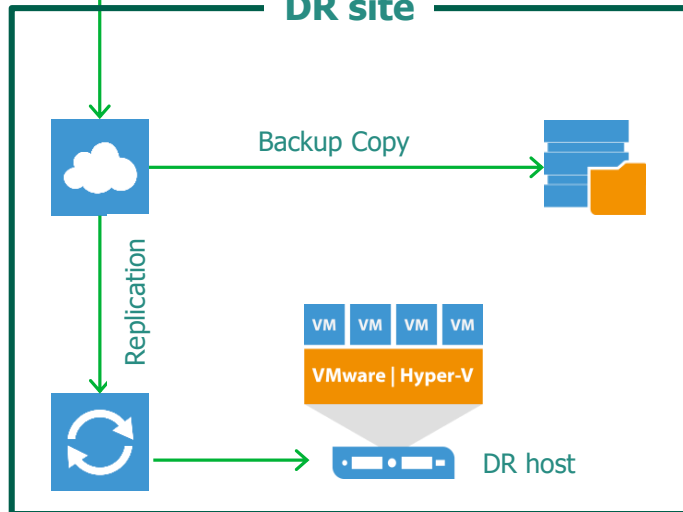
Production



Cloud



DR site



災難在很多時候真的不是天然造成的

#1 三寶員工

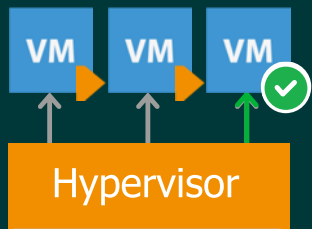


我們剛來的新人不小心誤刪老闆的電子郵件信箱, 現在還救不回來!

可以**快速**回復誤刪的系統 (即時還原)

在**3 到 5 分鐘**內從“備份檔案”或“儲存快照”啟動任何虛擬機

同時啟動多個**VM**且沒有數量上限



數分鐘內
立即上線！



實體機備份 (Veeam Agent)

- ✓ Linux
- ✓ Windows

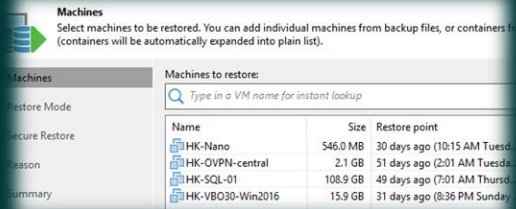
虛擬機備份 (Veeam Backup & Replication)

- ✓ Hyper-V
- ✓ Nutanix AHV
- ✓ VMware

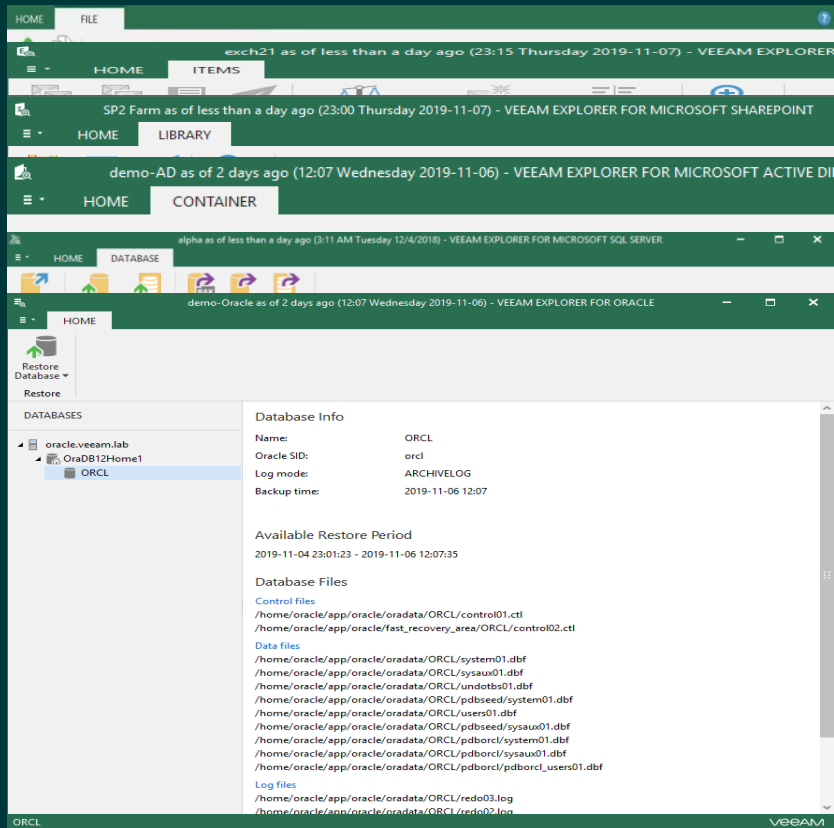
雲端工作負載備份

- ✓ 透過如 Veeam Backup for AWS 或 Veeam Agent 所保護的各式雲端虛擬機

已壓縮且已透過重複
資料刪除的備份檔案



Veeam 可以快速回復誤刪的資料



File and Folder:

回復單一檔案或資料夾到相同或不同的地方, 包含權限

Exchange:

回復任何 Exchange 物件到相同或不同的地方, 匯出, 或 Office 365

SharePoint:

瀏覽要回復的物件, 包括已刪除的檔案

Active Directory:

瀏覽, 比較並回復 Active Directory 物件到相同或不同的地方, 包括原本的密碼

SQL Server:

瀏覽並透過 transaction log 的還原, 回復 SQL 資料庫到指定的時間點

Oracle :

瀏覽並透過 transaction log 的備份及還原能力, 針對任何所支援的作業系統及 hypervisor 上的 Oracle 資料庫, 回復影像層級的備份

外部威脅常會導致服務無法存取

#2 無預警的威脅

機房內的數百台機器被駭客入侵! 而且它們都被加密完全登入不進去了!



The screenshot shows a ransomware message with a dark background and yellow and red text. At the top, there are several national flags. The main text reads: "Your personal files are encrypted by CTB-Locker. Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them. Press 'View' to view the list of files that have been encrypted. Press 'Next' for the next page." Below the text is a red warning triangle icon and a red warning message: "WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DE-CRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION." At the bottom, there are two yellow buttons: "View" and "Next >>". In the center, a digital timer displays "95:59:29".

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DE-CRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.

View 95:59:29 Next >>



如何避免勒索病毒的攻擊

1 確保軟體有定期更新

2 透過資安團隊執行資安威脅分析：
a. 經由滲透測試找出任何漏洞

3 給予員工關於資訊安全觀念的培訓：
a. 不要開啟來自於可疑或未知來源所寄來的附件檔
b. 如果病毒開始感染公司網路要立即通知相關人員

4 每天執行所有資訊的備份

5 備份所有資訊並存放到安全及異地空間

資料來源: TechRepublic - [How to avoid ransomware attacks](#)



三種不同的
資料副本



兩種不同媒體



一份異地儲存副本



副本類型：
離線氣隙
或不可修改備份

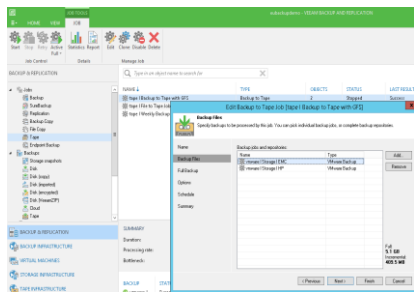


測試自動備份並驗證
復原能力後未發現任
何錯誤

veeam

以下裝置避免被勒索病毒入侵

透過 Veeam 將備份檔案寫入磁帶



透過 Veeam 將備份檔案寫入重覆資料刪除裝置
或以特殊權限連接存儲裝置



透過 Veeam 將備份檔案存放到本地物件儲存內



S3 相容物件儲存

透過 Veeam 整合 Linux 備份空間達成檔案不可更變



Linux Repository

勒索病毒攻擊 – Veeam 來防護！

為什麼？

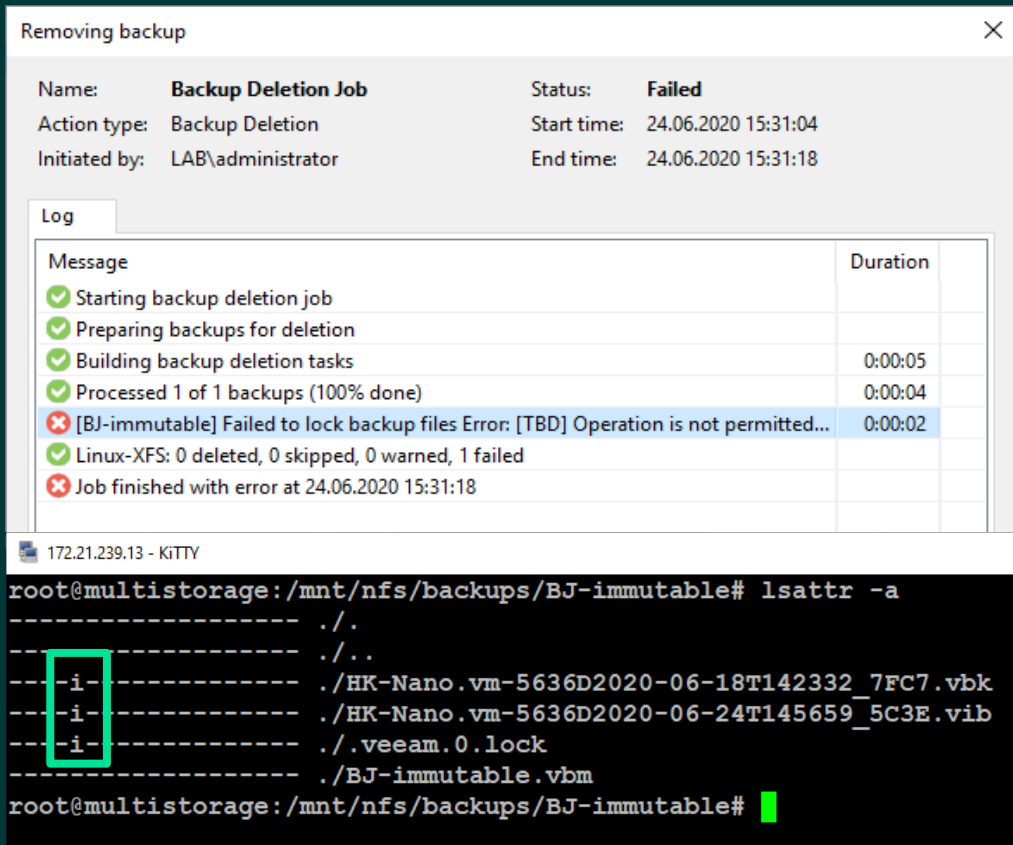
- 不受到惡意程式攻擊的儲存庫
- 如果正確設定：內部人員防護

什麼

- 拒絕備份資料的刪除

如何

- 採用 Linux 內的 “immutable flag”



Removing backup

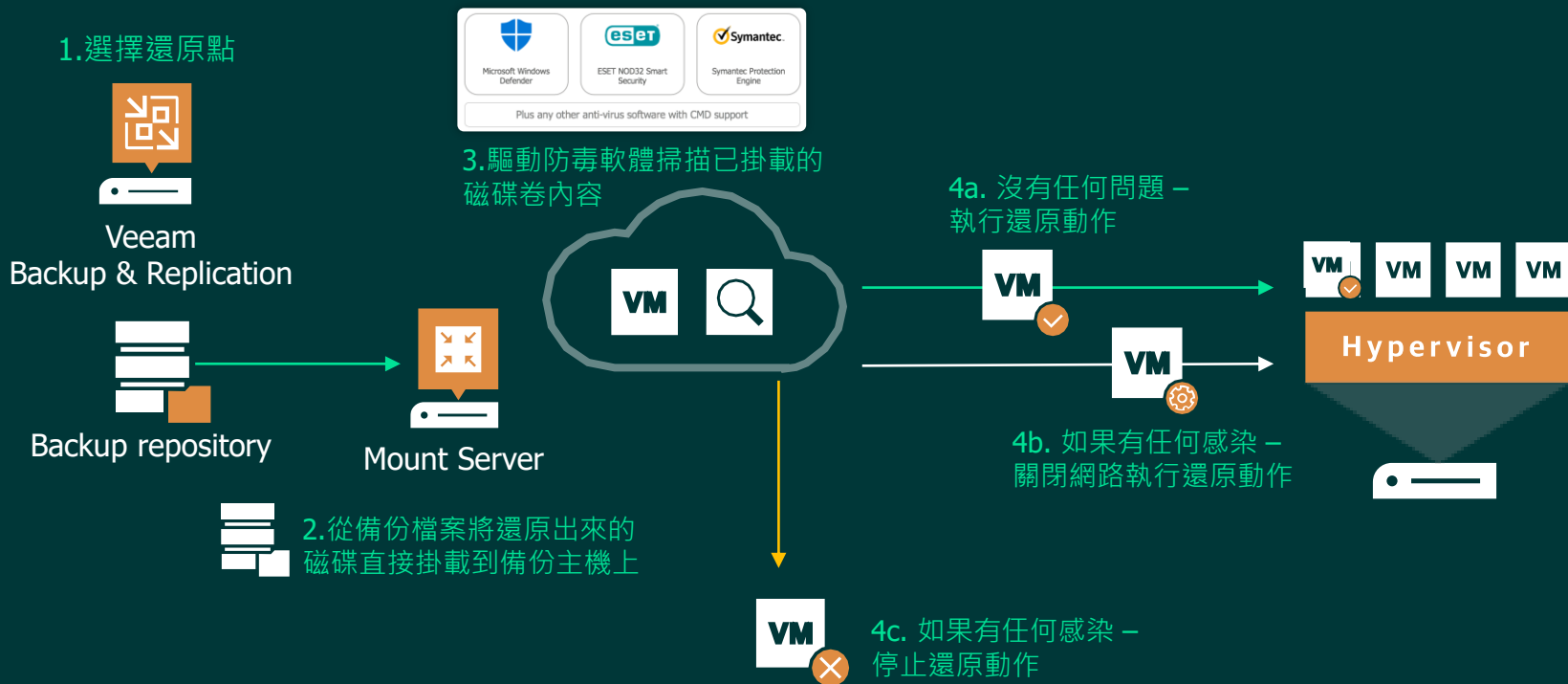
Name: **Backup Deletion Job** Status: **Failed**
Action type: Backup Deletion Start time: 24.06.2020 15:31:04
Initiated by: LAB\administrator End time: 24.06.2020 15:31:18

Log

Message	Duration
Starting backup deletion job	
Preparing backups for deletion	
Building backup deletion tasks	0:00:05
Processed 1 of 1 backups (100% done)	0:00:04
[BJ-immutable] Failed to lock backup files Error: [TBD] Operation is not permitted...	0:00:02
Linux-XFS: 0 deleted, 0 skipped, 0 warned, 1 failed	
Job finished with error at 24.06.2020 15:31:18	

```
172.21.239.13 - KITTYY
root@multistorage: /mnt/nfs/backups/BJ-immutable# lsattr -a
----- ./.
----- ./..
-i- ./HK-Nano.vm-5636D2020-06-18T142332_7FC7.vbk
-i- ./HK-Nano.vm-5636D2020-06-24T145659_5C3E.vib
-i- ./veeam.0.lock
----- ./BJ-immutable.vbm
root@multistorage: /mnt/nfs/backups/BJ-immutable#
```

潛伏期長，如何避免重複感染 (安全還原)



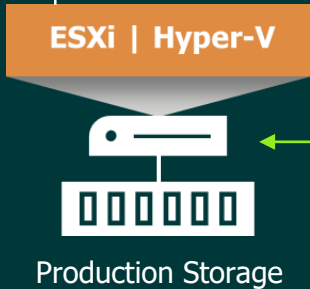
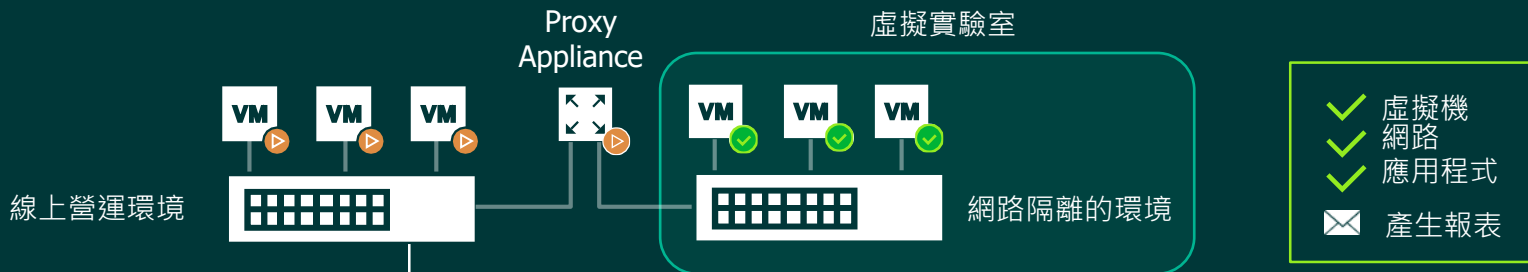
你有**驗證**過你的備份或備援資料嗎？

#3 備份檔在備份後從來
沒查看驗證過？



SureBackup/SureReplica (全自動VM備份驗證)

資料的自動驗證 & 進一步應用這份資料滿足企業所需



SureBackup: Exchange SureBackup Job							
Daily Verification Job							
Session Details							
Status	Success	Start time	1/12/2017 5:17:39 AM	Details			
Total tasks	3	End time	1/12/2017 5:35:41 AM				
Processed tasks	3	Duration	0:18:01				
Successful tasks	3	Warning tasks	0				
Failed tasks	0	Skipped tasks	0				
Progress	100 %						
Virtual machines status							
VM name	Status	Start time	End time	Heartbeat test	Ping test	Custom script test	Validation test
dns01	Success	1/12/2017 5:17:39 AM	1/12/2017 5:21:35 AM	Success	Success	Disabled	Disabled
dc01	Success	1/12/2017 5:17:39 AM	1/12/2017 5:29:04 AM	Success	Success	Success	Success
exch01	Success	1/12/2017 5:17:39 AM	1/12/2017 5:32:51 AM	Success	Success	Success	Success

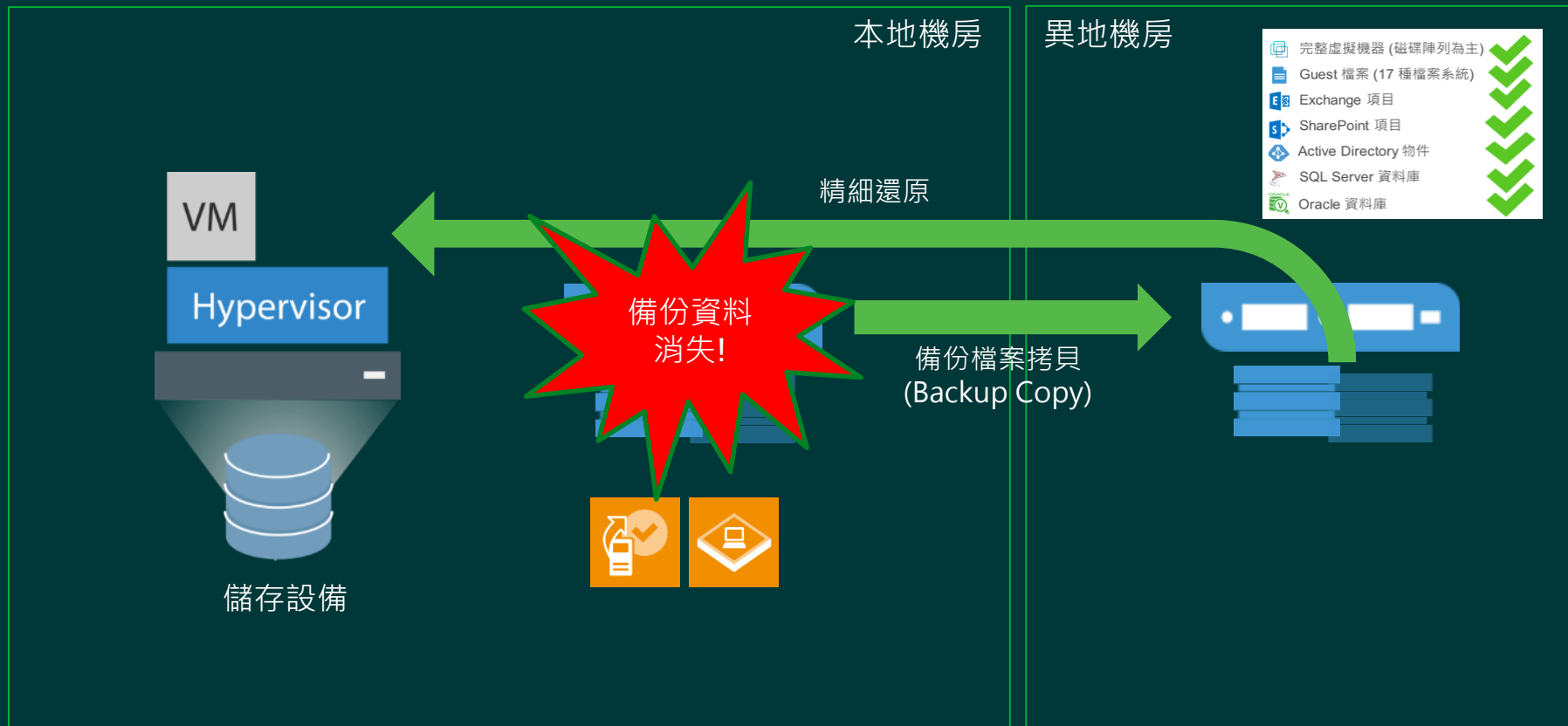
本地機房無法提供穩定的服務

#4 機房忘了擺乖乖?

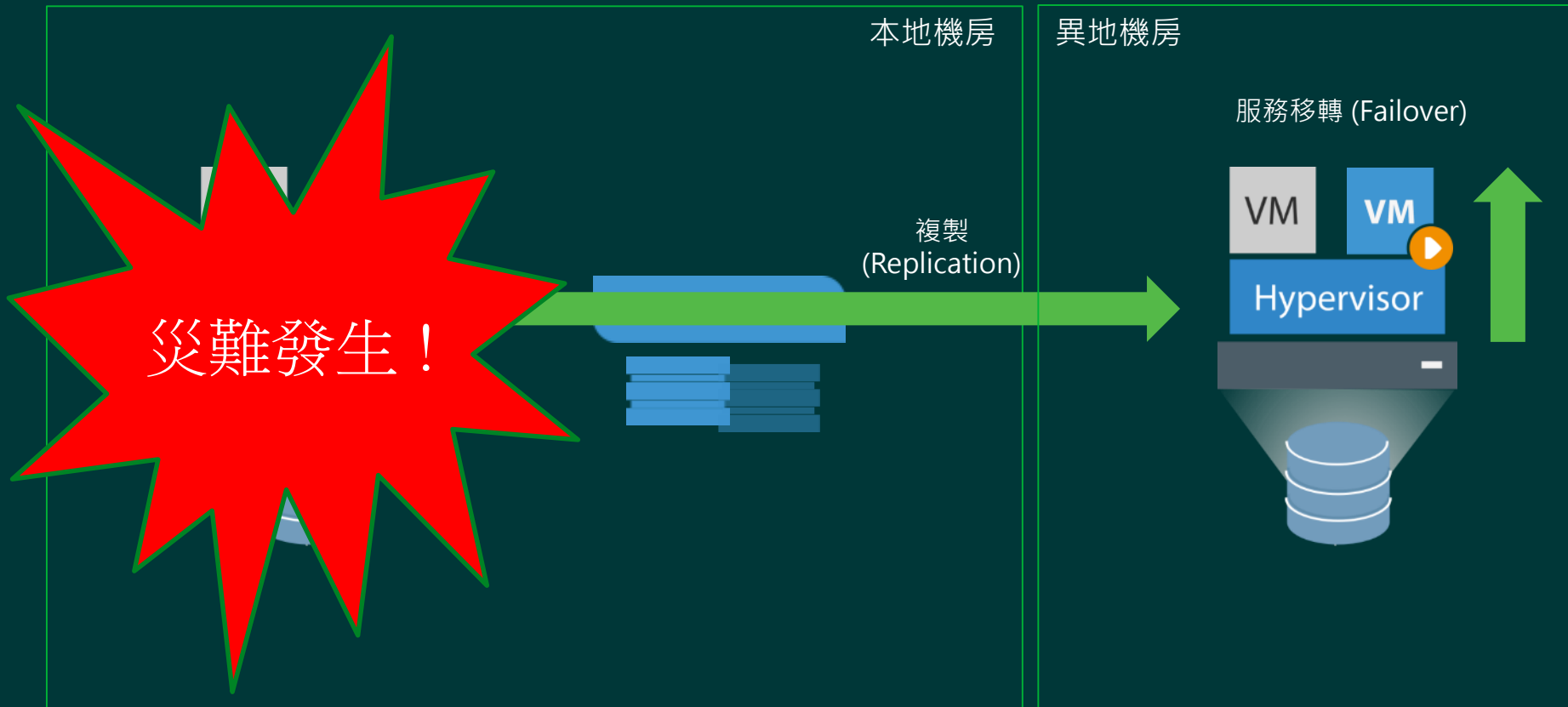
我們在過去幾年的時間內, 曾遭遇的災難



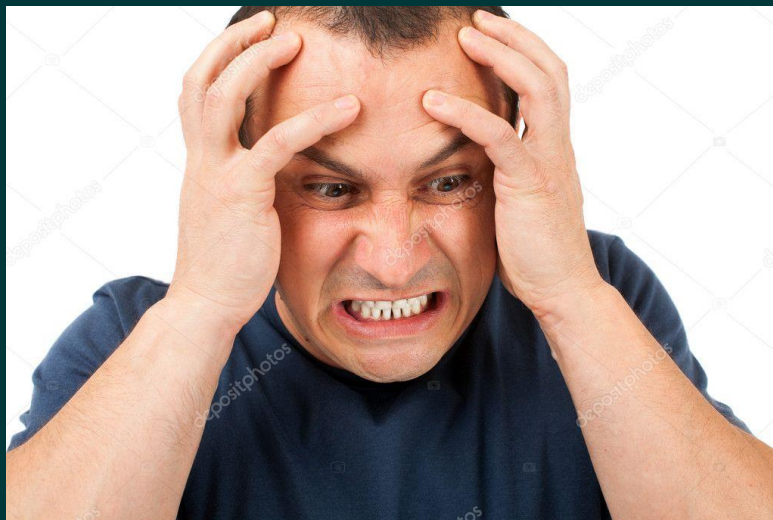
Veeam 提供異地備份降低本地資料遺失風險



Veeam 也提供異地備援提供應用程式高可用性

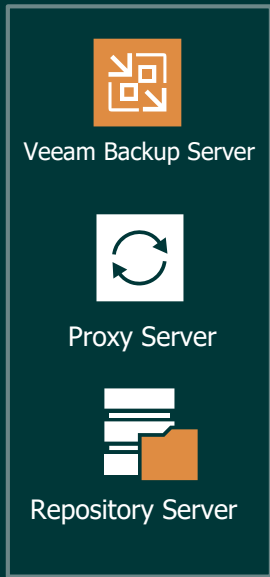
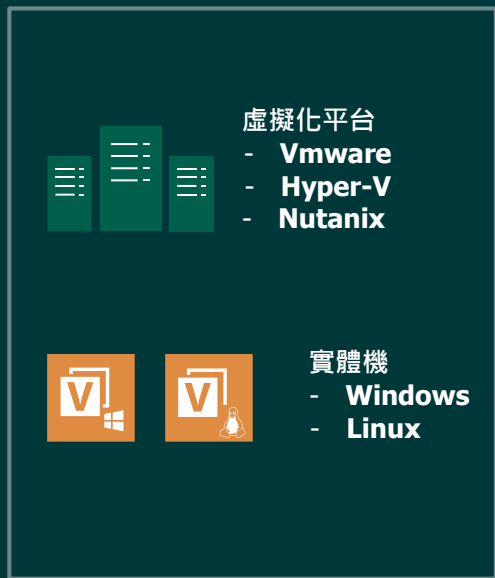


但是... 如果沒有異地機房, 該如何規劃異地備份及異地備援呢?



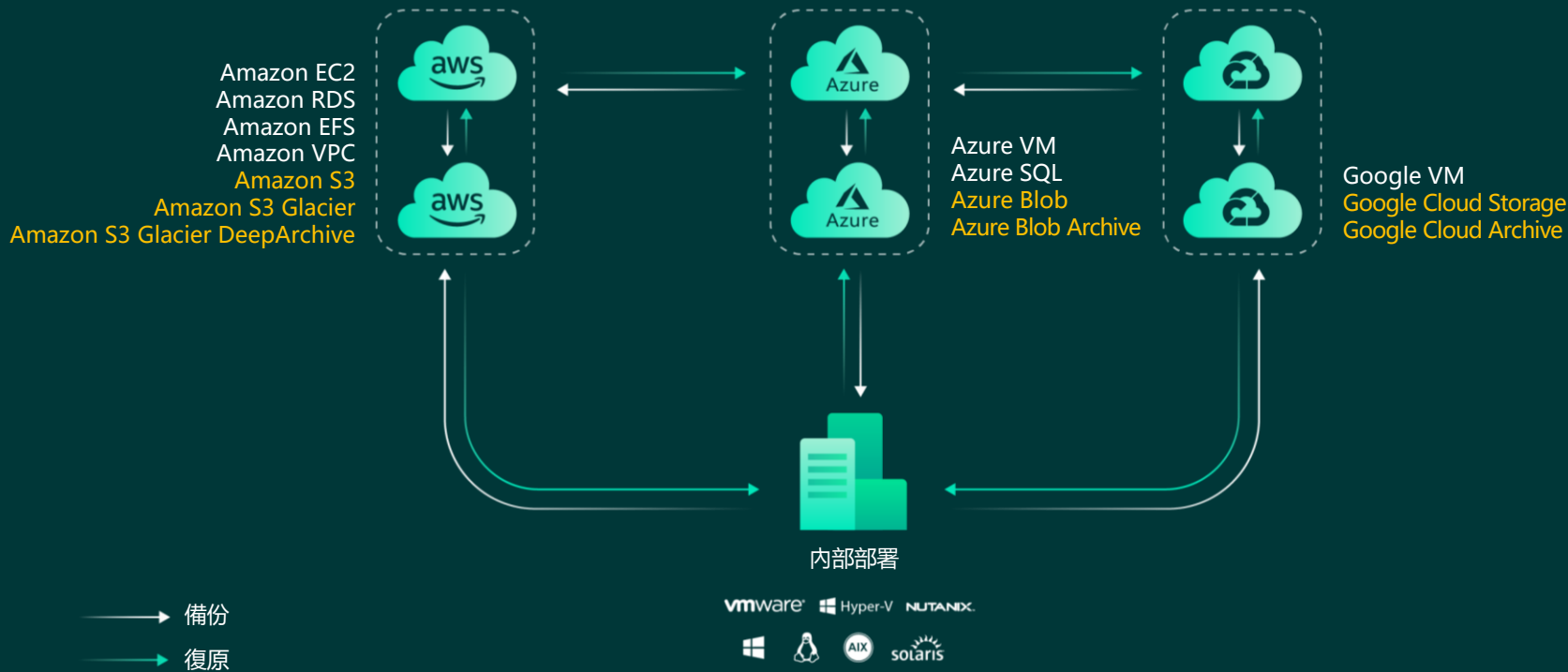
Veeam for *Cloud solution*

與Cloud彈性協同合作



擁有 資料主權，不限 任何雲端

雲端公有雲平台

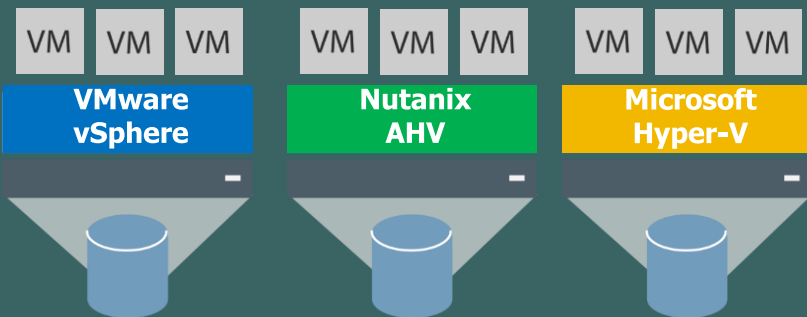


將備份檔案搬移到雲上

- 可透過政策設定將較長期的備份檔案，搬移到雲端儲存空間，
儲存成本較低
- 可選擇將已完成的備份檔，即時同步到雲端，利用雲端儲存空間達到**3-2-1備份策略**目標



即時同步 / 長久保存



On premise

Cloud資料還原至地端 (完整還原/精細還原)

- 想將上雲的服務，搬回地端



Backup Server

- 完整虛擬機器 (磁碟陣列為主)
- Guest 檔案 (17 種檔案系統)
- Exchange 項目
- SharePoint 項目
- Active Directory 物件
- SQL Server 資料庫
- Oracle 資料庫

精細還原



VM VM VM

VMware vSphere

VM VM VM

Nutanix AHV

VM VM VM

Microsoft Hyper-V



實體機
Windows
Linux



On premise

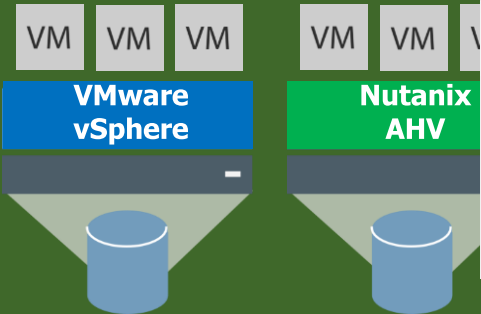
將服務搬移到雲上

- 將現有的備份檔，直接於雲端環境還原使用，將雲端作為二線DR站點
- 初期無法立即建置第二座資料中心/異地，但又短期需要擴充/移轉服務，想選擇雲端作為先行目標
- 分階段建置V2C, P2C

Direct Restore to Cloud

Backup Name	Timestamp	Source	Target
VMware - Backup from VS...	2021-10-17 22:15	SOBR	VMware
VMware - Backup of AD D...	2021-10-02 23:00	AWS S3 Reposit...	VMware
VMware - Backup of Excha...			
VMware - Backup of File S...			
VMware - Backup of Oracl...			
VMware - Backup of Share...			
VMware - Backup of SQL A...			
VMware - Backup to Data...			
VMware - Backup to Store...			
VMware - Backup to XFS R...			
Windows - Backup of AD D...			
Windows - Backup of Exch...			
exch3.demo.local			
Windows - Backup of Shar...			
Windows - Backup of Sh...			
sps3.demo.local			

- Instant recovery
- Volume restore...
- Export content as virtual disks...
- Restore guest files
- Restore application items
- Restore to Amazon EC2...
- Restore to Microsoft Azure...
- Restore to Google CE...
- Restore entire VM to Nutanix AHV...
- Create recovery media...
- Export backup...
- Remove from configuration
- Delete from disk



機房內仍有不少實體機器要保護

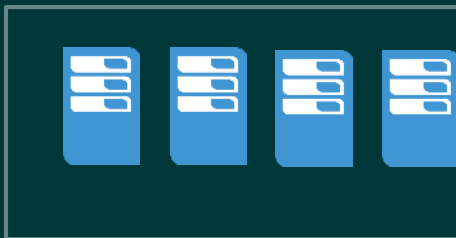
#5 實體機器的美麗與憂愁

我們機房 99% 都虛擬化了, 不過還是有一些 x86 實體主機需要保護

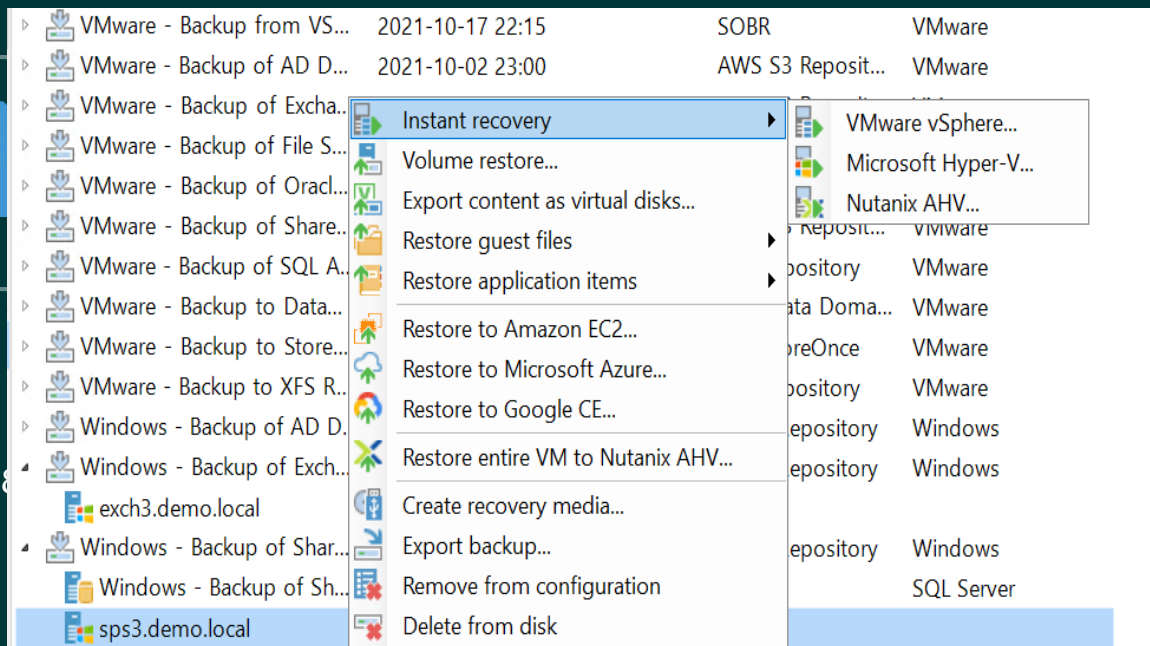


集中管理實體機統一部署Agent

實體機



- Bare metal recovery
- Export as virtual disk
- Instant Recovery to VMware &
- Application item recovery
- Restore guest files
- Restore to Amazon EC2
- Create Recovery Media



Veeam Agent for Microsoft Windows 支援

Both 64-bit and 32-bit (where applicable) versions of the following operating systems are supported¹:

- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server Semi-Annual Channel (including version 1909)
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 SP1²
- Microsoft Windows 10 (starting from version 1607 up to version 1909)³
- Microsoft Windows 8.1
- Microsoft Windows 7 SP1

Cluster

- Microsoft Windows Server Failover Clusters,
- Microsoft SQL Server Failover Cluster Instances,
- SQL Always On Availability Groups
- Microsoft Exchange Database Availability Group

參考連結:

https://helpcenter.veeam.com/docs/agentforwindows/userguide/system_requirements.html?ver=50

<https://www.veeam.com/kb2463>

Veeam Agent for Linux 支援



Linux kernel 2.6.32 or later¹ is supported.

Both 64-bit and 32-bit versions (if applicable) of the following distributions² are supported:

- Debian 8.0 – 10.3³
- Ubuntu 14.04, 16.04, 18.04, 19.10³
- RHEL 6.0 – 8.1⁴
- CentOS 6.0 – 8.1⁴
- Oracle Linux 6 – 8.1 (RHCK)³
- Oracle Linux 6 (starting from UEK R1) – Oracle Linux 7 (up to UEK R5 U2)³
- SLES 11 SP4, 12 SP1 – 15 SP1
- SLES for SAP 11 SP4, 12 SP1 – 15 SP1
- Fedora 30 – 31³
- openSUSE Leap 15.1
- openSUSE Tumbleweed³

參考連結:

https://helpcenter.veeam.com/docs/agentforlinux/userguide/system_requirements.html?ver=50

雲端 郵件 / 檔案 / 網站 備份需求 ?

#6 雲端資料保護 (Office 365 備份與還原)

雖然採用了微軟 Office 365,
但是重要資料還是需要備份
下來*... 聽說資料要自己負責!



- 微軟透過 Shared Responsibility Model 說明資料為使用者自行負責
<https://aka.ms/sharedresponsibility>

VBO for *Microsoft office 365*



保存政策：Microsoft 提供了哪些？



Office 365 備份及保存政策**僅能在你的資料遺失時提供有限的保護**，但不應該作為一個完整的備份解決方案。

保存政策總是在演進，且相對在管理及監控方面非常複雜。有些管理者認為他們都有提供足夠的保護，但到最後卻發現有些應該存在的郵件找不到了。

Sources: Exchange Online information above is based on Microsoft's [default MRM Policy](#). SharePoint Online information above is based on Microsoft's [support article](#). OneDrive for Business information is based on Microsoft's [support article](#). In some cases, these defaults can be customized by the IT Admin, but often require certain licenses and/or additional fees, and also carry the risk which allows Microsoft to automatically delete data ahead of retention policy dates if the recycle bin is full.

保存政策：Veeam 做了哪些？



Veeam Backup for Microsoft Office 365 不是簡單的填補缺失。
同時提供 Exchange Online, SharePoint Online and OneDrive for Business 等全部資料的存取與控制
並且將這些資料儲存在一個地方, 確保快速簡單且可信賴的還原。

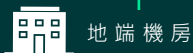
全新Veeam Backup for Microsoft Office 365

保護



備份

Veeam Backup
for Microsoft Office 365



地端 機房



Exchange



SharePoint

儲存



或
地端 機房



本地空間



S3-相容

還原

還原



Microsoft 365 - GUI 精細還原介面

The screenshot displays the Veeam Explorer for Microsoft Teams interface. The main window title is "All organizations as of less than a day ago (2:42 PM Friday 11/6/2020) - Veeam Explorer for Microsoft Teams". The interface includes a top navigation bar with "Home" and "Files" tabs, and a toolbar with "Restore File", "Save File", "Send File", "Advanced Find", and "History" options. On the left, there is a sidebar for "Organizations" showing a tree view of "AperatureLabs.onmicrosoft.com" with sub-items like "Aplabs.HR", "Aplabs.Marketing", "Aplabs.Technical", "Microsoft Teams Accounts", "Site for Documents", and "Veeam Software". The main area is titled "Restore List (5)" and contains a search bar, status indicators, and a table of restore items. A context menu is open over the "Restore Exchange Items" option in the table.

	Type	Location	Sent	Received	Restore Status
<input type="checkbox"/>	OneDrive Do...	abc_user/folder/folder2	-	-	Never started
<input checked="" type="checkbox"/>	2020_09_11_04_05_28.msg	abc_user/folder/folder2	-	-	Never started
<input checked="" type="checkbox"/>	AudioPreview.png	abc_user/ContentStyle ...	-	-	Never started
<input checked="" type="checkbox"/>	Azure AD Identity Protection ...	abc_user/inbox	February 18, 2022 4:34 AM	February 18, 2022 4:34 AM	Never started
<input checked="" type="checkbox"/>	Major update from Message ...	abc_user/inbox	February 23, 2022 8:29 AM	February 23, 2022 8:29 AM	Never started

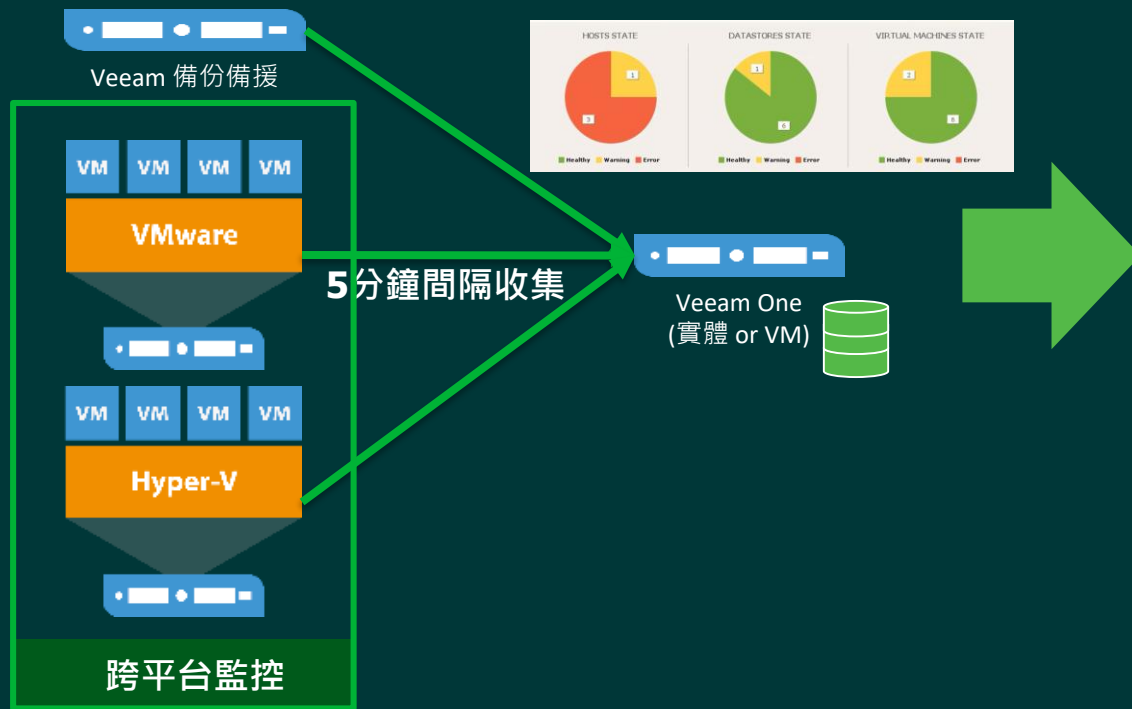
是否有預警機制可以提早通知我？

#7 最近忘了去拜拜？

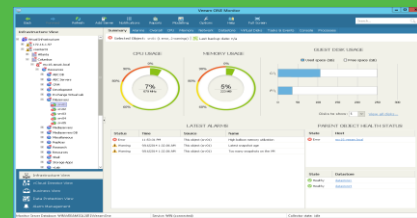
系統最近一直不穩定, 我想知道是不是資源不足還是其它原因造成?



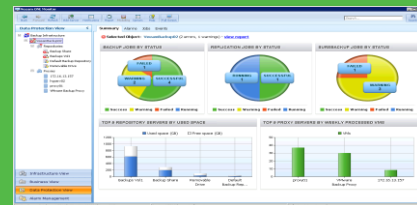
Veeam ONE 虛擬機&備份 監控維運



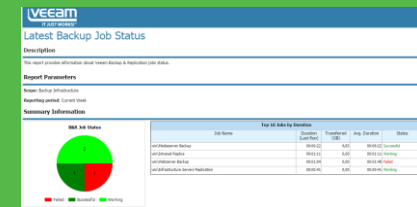
監控警示及問題排除



資源最佳化及容量預測分析



報表中心



虛擬機資源健康狀態 監控維運

The screenshot displays the Veeam ONE Client interface for Alarm Management. The top navigation bar includes options like Back, Forward, Refresh, Add Server, Notifications, Reports, Modeling, Settings, Full Screen, and Help. The main area is titled 'Alarm Management' and contains a search bar, filters, and a table of alarms.

Type	Name	Source	State	Assignment	Resolution
	DPM failed to bring host out of stand...	Predefined	Enabled	Virtual Infrastructure	Automatic
	Host failed to exit standby mode	Predefined	Enabled	Virtual Infrastructure	Automatic
	vCenter Server lost connection to host	Predefined	Enabled	Virtual Infrastructure	Automatic
	Host connection failure	Predefined	Enabled	Virtual Infrastructure	Automatic
	VM connection failure	Predefined	Enabled	Virtual Infrastructure	Automatic
	VM CPU ready	Predefined	Enabled	Virtual Infrastructure	Automatic
	VM CPU usage	Predefined	Enabled	Virtual Infrastructure	Automatic
	High balloon memory utilization	Predefined	Enabled	Virtual Infrastructure	Automatic
	VM memory swap usage	Predefined	Enabled	Virtual Infrastructure	Automatic
	VM disk SCSI connection failures	Predefined	Enabled	Virtual Infrastructure	Automatic

The 'VM CPU ready' alarm is selected, and its details are shown in the 'Alarm Settings' dialog box. The 'Rules' tab is active, showing the following configuration:

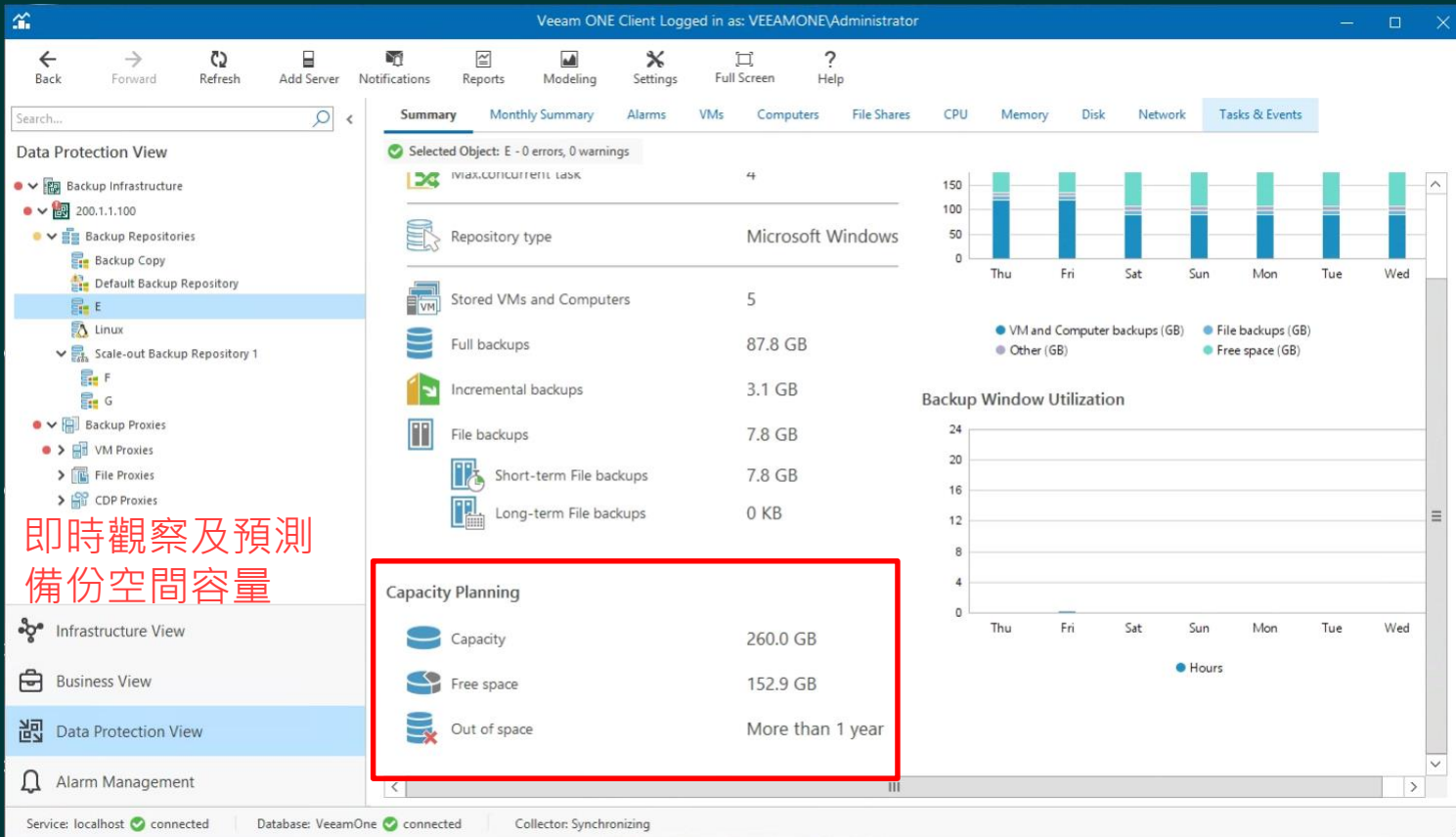
- Rule type: Usage (Enabled)
- Counter: Average CPU Ready ...
- Condition: Above
- Warning: 10.0 %
- Error: 20.0 %
- Time period: 15 min
- Aggregation: Avg

The 'Alarm Details' section on the left provides additional information:

- Knowledge:** This VM has exceeded t...
- Cause:** CPU Ready Time is the...
- Resolution:** Some CPU Ready Time slow response times an response. Consider adju...
- External:** Refer to VMware's onlin...

The bottom status bar shows 'Localhost connected' and 'Database: VeeamOne connected'.

備份主機資源 監控維運



監控可疑行為

監控“可能的勒索軟體活動”。當磁碟上有大量寫入操作並且CPU使用率很高，則將觸發此警報。

(Veeam ONE 警報機制)

The screenshot displays the Veeam ONE interface. On the left is a navigation tree with categories like Host, Virtual Machine, Cluster, CSV, Local storage, Any Object, Backup & Replication, and Internal. The main area shows a list of alarms. The 'Possible ransomware activity' alarm is selected and highlighted in blue. Below the list, the 'Alarm details' section is visible, containing 'Knowledge', 'Cause', and 'Resolution' information.

Machine remoting system failure	Predefined	Enabled	Virtual Infrastructure	Manual
Missing latest cluster configuration data	Predefined	Enabled	Virtual Infrastructure	Manual
Network communication failure	Predefined	Enabled	Virtual Infrastructure	Manual
No disk space to run this VM	Predefined	Enabled	Virtual Infrastructure	Manual
Not enough memory to start a VM	Predefined	Enabled	Virtual Infrastructure	Manual
Possible ransomware activity	Predefined	Enabled	Virtual Infrastructure	Automatic

Alarm details

Knowledge
Veeam ONE detected suspicious activity on this VM

Cause
This Virtual Machine had high write rate on datastore along with high CPU Usage which can be caused by ransomware activity

Resolution
Check if files on VM are encrypted by ransomware. Run up-to-date security software, prevent ransomware propagation, ask for qualified assistance if needed. Restore VM or encrypted files from previous backup in a case the files cannot be repaired. If VM was not affected by ransomware, raise the alarm thresholds

自動化排成報表中心

預測範圍包含: 備份空間、vSphere CPU、Memory、Datastore


• 擴充所需資源
立即掌握

The screenshot displays the Veeam ONE Web Client interface for Capacity Planning. The left sidebar shows a navigation menu with 'vSphere Capacity Planning' selected. The main content area shows the 'Capacity Planning' report page. A red box highlights the 'Report Parameters' section, which includes:

- Scope: Virtual Infrastructure
- Datstores: All Datstores
- Analyze performance data for: Past 6 Months
- Perform planning for: Next 6 months
- CPU utilization: 80.00 %
- Memory utilization threshold: 80.00 %
- Datstore space utilization threshold: 90.00 %
- Datstore read/write speed (max) threshold: 50 MBps

Below the parameters is a 'Summary' table:

Virtual Infrastructure	Days Remaining	Resources Required
Number of standalone hosts: 0	CPU: ∞	CPU: 0.00 GHz
Number of hosts: 1	Memory: 0	Memory: 2.41 GB
Number of datstores: 1	Datstore space utilization: 0	Datstore capacity: 0.04 TB




- AWS 
- Azure 
- Google Cloud 
- IBM Cloud 

Cloud



Virtual



-  VMware vSphere
-  Microsoft Hyper-V
-  Nutanix AHV

單一管理介面平台

保護與管理所有的工作負載

- Windows 
- Linux 
- MAC 
- UNIX 
- NAS 

Physical



SaaS



 Office 365

Apps



-  Databases
-  Microsoft
-  Kubernetes

Thank you

veeam