

面臨資安風險 如何確保AD的持續性和可靠性

王詩齡 Dama Wang

Quest Systems Consultant, GC



議程

- AD的重要性及管理員面臨恢復AD的挑戰
- 微軟對恢復AD的標準方式
- 如何借助Quest工具快速恢復AD正常運作？
- 雲端及混和環境應該怎麼做？

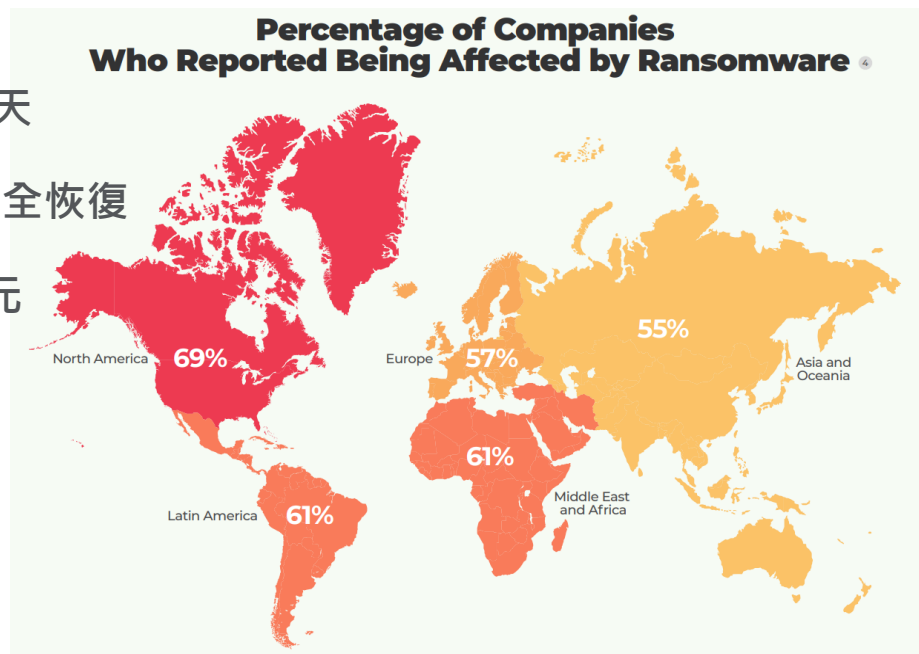


AD的重要性 管理員面臨恢復AD的挑戰



企業需要具備更安全的網路環境

- 全球超過 **50%** 的企業公開報告遭受勒索軟體攻擊
- 支付贖金的人中有 **34%** 未能取回數據
- 由於勒索軟體攻擊，平均停機時間為 **21** 天
- 企業平均需要花費**287** 天才能從攻擊中完全恢復
- **2020** 年勒索軟體的估計成本為**208** 億美元



06/07/2021

Gartner®

How to Recover From a Ransomware Attack Using Modern Backup Infrastructure

Published 4 June 2021 - ID G00738061 - 40 min read

By Analysts [Fintan Quinn](#)

“The restore process from many well-documented ransomware attacks has been hindered by not having an intact Active Directory restore process.”

Quest

Where Next Meets Now.

Active Directory是企業重要關鍵系統

組織使用 Active Directory 來管理身份並提供對業務資源的訪問

Active Directory

主要身份驗證和提供訪問權限

資料庫

用於業務分析和研究的結構化數據



檔案

用於公司內外交流非結構化數據



應用服務

提供企業業務所需的工具



端點設備

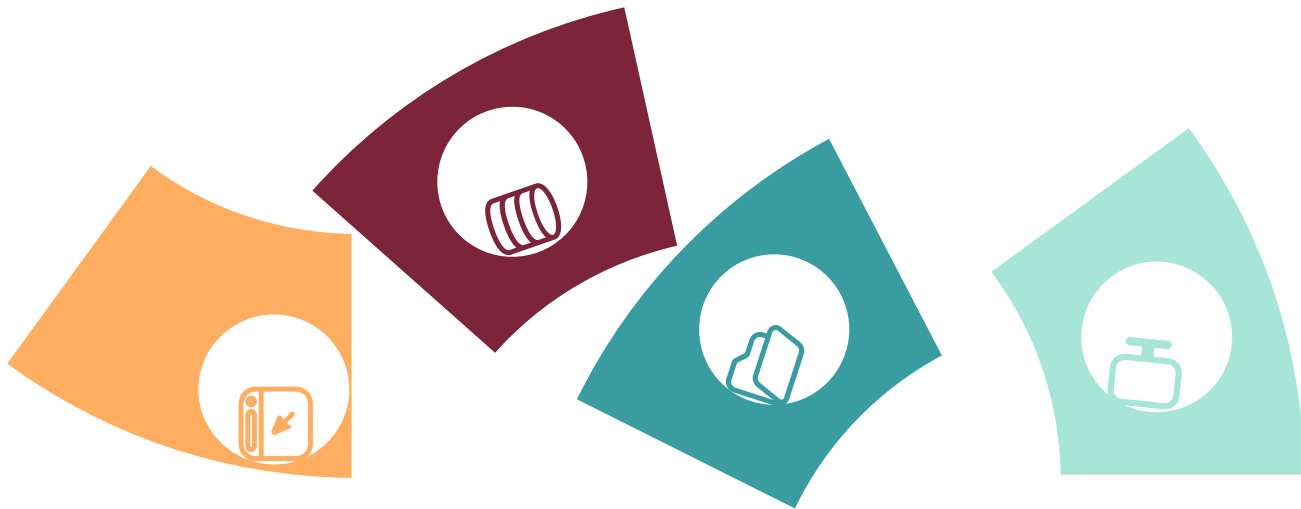
電腦、平板、手機...等業務資源設備



當沒有了 AD ...

... 服務將無法使用

“如果無法恢復網域控制器, 我們將無法恢復任何東西”



企業面臨的AD恢復挑戰

以手動還原AD/DC費時費力，且Offline方式進行影響企業運作

傳統備份不提供”精細”還原，也無法得知哪些物件或屬性已被更改或刪除

無法還原整個AD網域和樹系

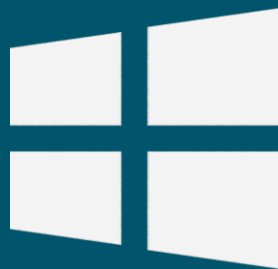
無法驗證備份檔的有效性，以確保AD/DC還原之可行性

當伺服器或作業系統損壞，無法做到裸機還原

無法備份還原Azure AD

無法將還原作業委派給其他管理員，以減輕負擔

需要提供災難還原計劃和工作流程，以符合合規性要求



微軟對恢復AD的標準方式



Sort by title

Identity and Access

Operations and Scenario Guides

Active Directory Domain Services

AD DS Operations

AD Forest Recovery Guide

AD Forest Recovery - Prerequisites

AD Forest Recovery - Steps for Recovery

AD Forest Recovery - Identify the Problem

AD Forest Recovery - Perform Initial Recovery

AD Forest Recovery - Procedures

AD Forest Recovery - FAQ

AD Forest Recovery - Recovering a single domain with multidomain forest

AD Forest Recovery - Virtualization

AD Forest Recovery - Windows Server 2003

Best Practices for Servicing Active Directory

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

AD Forest Recovery - Windows Server 2003

Active Directory Forest Recovery Guide

Article • 08/16/2021 • 2 minutes to read • +1

Is this page helpful?

In this article

Steps outlined in this guide

Applies to: Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows Server 2012 and 2012 R2, Windows Server 2008 and 2008 R2, Windows Server 2003

This guide contains best-practice recommendations for recovering an Active Directory® forest if forest-wide failure occurs on all domain controllers (DCs) in the forest incapable of functioning normally. The steps it contains serve as a template for your forest recovery plan, which you can customize for your particular environment. These steps apply to DCs that run Microsoft® Windows Server 2016, 2012 R2, 2012, 2008 R2, 2008, and 2003 operating systems.

Note

Procedures that are unique for DCs that run Windows Server 2003 are consolidated in [AD Forest Recovery Windows Server 2003](#).

Steps outlined in this guide

- [AD Forest Recovery - Prerequisites](#)
- [AD Forest Recovery - Devising a custom forest recovery plan](#)
- [AD Forest Recovery - Steps for Recovery](#)
- [AD Forest Recovery - Identify the problem](#)
- [AD Forest Recovery - Determine how to recover](#)
- [AD Forest Recovery - Perform initial recovery](#)
- [AD Forest Recovery - Procedures](#)

Microsoft's Active Directory Forest Recovery Guide

手動AD備份 和恢復



Manual Backup

需要與每一個 DC 手動備份
非常耗時



Manual Restore

手動還原備份，將WinRE映像
恢復到裸機伺服器



Custom Win Recovery Environment

為每台DC伺服器自定義WinRE，
包含安裝驅動程式



Reconfigure AD Verify AD

重新配置及驗證AD/DC同步
漫長且過程複雜容易出錯



透過Quest工具
快速恢復AD正常運作



遠端自動化 AD備份

 **Back Up Domain Controller**
Starts a wizard that helps you back up domain controllers and/or AD LDS (ADAM) hosts without putting Active Directory or AD LDS (ADAM) offline. The created backups will include the Active Directory, Group Policy, a AD LDS (ADAM) data held on the selected computers.

Quest Recovery Manager for Active Directory

File Action View Window Help

← → 📁 📄 🔄 📄 📄 📄 📄 📄 📄 📄 📄 📄

Recovery Manager for Active Directory	Collection	Last Run	Backup Type
> Replication	ACME - Full	2/17/2022 9:41:54 AM	Bare Metal
Backup Agents	ACME - Standard	1/28/2022 3:22:29 PM	Active Directory
> Storage	AUSSIE - Full	2/17/2022 9:42:38 AM	Bare Metal
> Computer Collections	AUSSIE - Standard	1/28/2022 3:22:32 PM	Active Directory
> Active Directory	POODLE - Full	2/17/2022 9:42:43 AM	Bare Metal
> Sessions	POODLE - Standard	1/28/2022 3:22:37 PM	Active Directory
> Backups			

Quest Recovery Manager for Active Directory

File Action View Window Help

← → 📁 📄 🔄 📄 📄 📄 📄 📄 📄 📄 📄 📄

Recovery Manager for Active Directory	Session	Result
> Replication	2/17/2022 9:41:54 AM - ACME - Full	Running
Backup Agents	2/17/2022 9:42:38 AM - AUSSIE - Full	Running
> Storage	2/17/2022 9:42:43 AM - POODLE - Full	Running
> Computer Collections	1/27/2022 1:31:06 PM - AUSSIE - Full	Success
> Active Directory	1/27/2022 1:31:03 PM - ACME - Full	Success
> Sessions	1/27/2022 1:31:09 PM - POODLE - Full	Success
> Backups	1/27/2022 4:02:11 PM - POODLE - Standard	Success

線上物件還原

Quest Recovery Manager for Active Directory

- Back Up System State
- Restore AD Objects Online
- Restore AD LDS (ADAM) Objects Online
- Restore Group Policy Online
- Restore System State Offline
- Ask the Experts
- On Demand Recovery for Azure AD

Detailed Report

Provides detailed information about the compare and restore operations performed on Active Directory or AD LDS (ADAM) objects with Recovery Manager.

Operation: Compare two backups

Finished on: 1/16/2020 12:20:23 AM

Source backup: C:\Users\Administrator\Documents\RMAAD.bkf (1/15/2020 2:48:29 AM)

Target backup: C:\Users\Administrator\Documents.bkf (1/16/2020 12:04:49 AM)

Backed up computer: QAD.questzot.com

Number of processed objects: 267

Operation status: Completed successfully

This report provides information about: Added, deleted, and modified objects.
Added, deleted, and modified attributes.

Number of objects by type of change

Type of change	Number of objects
Modified	3

Expand all | Collapse all

Object DN	Object class	Type of change	Modified by
[-] CN=Administrator,CN=Users,DC=questzot,DC=com	User	Modified	
[-] CN=RID Set,CN=QAD,OU=Domain Controllers,DC=questzot,DC=com	RID-Set	Modified	
[-] CN=Users,DC=questzot,DC=com	Container	Modified	

Child objects by type of change

Child object DN	Type of change	Child object class	Modified by
CN=test,CN=Users,DC=questzot,DC=com	Added	User	

Pages: 1 Date: 1/16/2020

Online Restore Wizard

Backup Selection
Depending on the wizard operation mode, the backup you select will be restored/compared to Active Directory or compared with another backup.

Registered backups:

Backup Age	Created	DC	Media
0 hour(s)	2020/1/16 上午 12:04:49	QAD.questzot.com	C:\Users\Administrator\Docum
21 hour(s)	2020/1/15 上午 02:53:44	QAD.questzot.com	C:\Users\Administrator\Docum
21 hour(s)	2020/1/15 上午 02:48:29	QAD.questzot.com	C:\Users\Administrator\Docum

To register a new backup file or Active Directory database, click Register.

Register

< 上一步(B) 下一步(N) > 取消 說明

自動化AD網 域/樹系重建

The screenshot displays the Forest Recovery Console interface. At the top, it shows the active directory forest as 'acme.test' with 8 DCs to be processed and 3 domains to be processed. A progress bar indicates an elapsed time of 00:00:50. Below this is a table listing domain controllers and their recovery status.

Domain Controller	Type	Recovery Method	Status	Domain	FSMO Role	Site	Selected Backup
dc1.acme.test	GC	Restore from backup	Perform restore from backup	acme.test	P R S D	New York	dc1.acme.test-2018-02-16 09-42-25
dc2.acme.test	DC	Reinstall Active Directory	Uninstall Active Directory Do...	acme.test	I	London	
dc3.acme.test	GC	Reinstall Active Directory	Uninstall Active Directory Do...	acme.test		Los Angeles	
dc4.child.acme.test	GC	Restore from backup	Perform restore from backup	child.acme.test		London	dc4.child.acme.test-2018-02-16 09--
dc5.child.acme.test	GC	Restore from backup	Perform restore from backup	child.acme.test	P R I	New York	dc5.child.acme.test-2018-02-16 09--
dc6.child.acme.test	GC	Restore from backup	Perform restore from backup	child.acme.test		Los Angeles	dc6.child.acme.test-2018-02-16 09--
dc7.resource.acme.test	DC	Restore from backup	Perform restore from backup	resource.acme.test	P R I	London	dc7.resource.acme.test-2018-02-16
dc8.resource.acme.test	Read-only, GC	Reinstall Active Directory	Reinstall Active Directory Do...	resource.acme.test		Los Angeles	

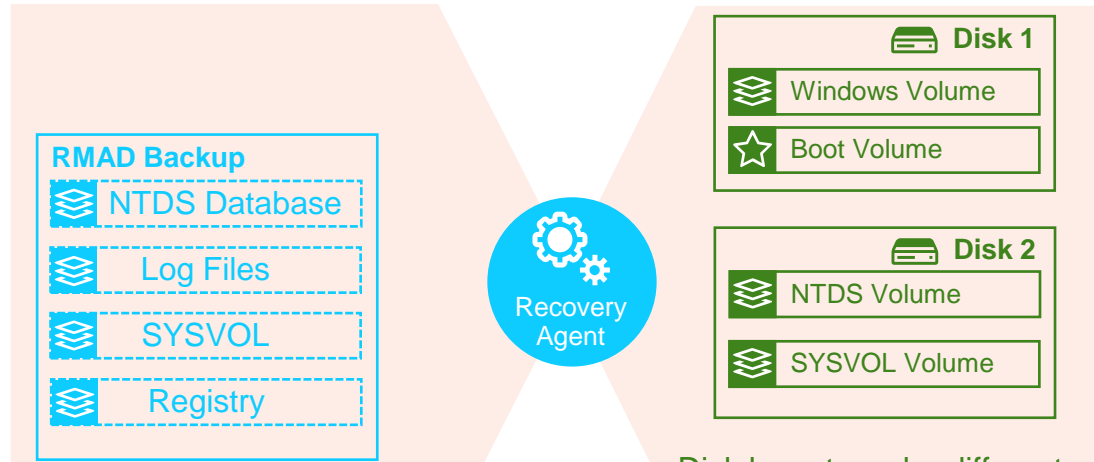
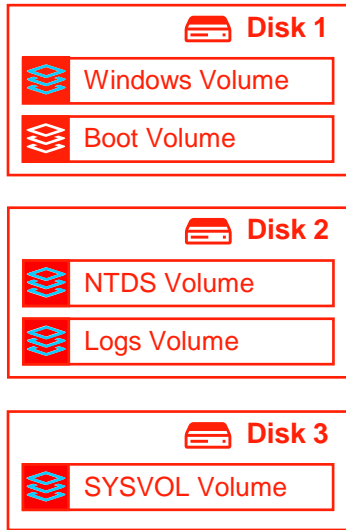
The detailed view for 'dc1.acme.test' shows the following recovery events:

- Disable windows update (2/16/2018 2:48:10 PM)
- Copy the backup file to domain controller (2/16/2018 2:48:22 PM)
- PERFORM RESTORE FROM BACKUP**
- Reset DSRM administrator password (2/16/2018 2:48:24 PM)
- Restart domain controller in DSRM (2/16/2018 2:48:35)
- Enable domain controller isolation (2/16/2018 2:48:36)
- Disable custom filters for passwords (2/16/2018 2:48:38)
- Restore data from backup (2/16/2018 2:48:38)
- Restart domain controller in normal mode
- CONFIGURE DOMAIN CONTROLLER**
- Get information about domain controller
- Select preferred DNS server
- Raise RID pool
- Invalidate RID pool

A dropdown menu is open, showing the 'Recovery method' options:

- Restore Active Directory on Clean OS (selected)
- Restore Active Directory from backup
- Restore Active Directory on Clean OS
- Bare Metal Active Directory Recovery
- Reinstall Active Directory
- Install Active Directory
- Uninstall Active Directory
- Do not recover

從乾淨的作業系統減少了惡意軟體的藏身之處



Recovery AD on Clean OS包括 AD 資料庫、AD 資料庫日誌文件、SYSVOL (群組策略、登錄腳本) 和 Windows 註冊表的必要部分。與裸機恢復備份或系統狀態備份不同，RMAD不會備份磁區 (可能會受到 root-kit 病毒的攻擊) 或整個 Windows 目錄 (包括 Windows/temp 和 Windows/winSxS，Kaseya 供應鏈/勒索軟體攻擊利用)

Clean OS + IFM 兩階段還原

Verify Settings Start Recovery Continue Recovery Cancel Backup Criteria... Configure Alerts... Configure Pauses... Schedule Verify...

Recovery mode: Forest Recovery Active Directory forest: acme.lab DCs to be processed: 3 of 6 Domains to be processed: 3 of 3
Pending DCs: 0 Succeeded DCs: 3 Failed DCs: 0
Elapsed time: 00:39:40

Computer	Type	Recovery Method	Target computer	Status	Domain
acmedc1.acme.lab	GC	Restore Active Directory on Clean OS	10.1.1.10	Completed successfully	acme.lab
acmedc2.acme.lab	GC	Do not recover (Keep in project)			acme.lab
aussiedc1.aussie.acme.lab	GC	Restore Active Directory on Clean OS	10.1.1.20	Completed successfully	aussie.acme.lab
aussiedc2.aussie.acme.lab	GC	Do not recover (Keep in project)			aussie.acme.lab
poodledc1.poodle.acme.lab	GC	Restore Active Directory on Clean OS	10.1.1.30	Completed successfully	poodle.acme.lab
poodledc2.poodle.acme.lab	GC	Do not recover (Keep in project)			poodle.acme.lab

Verify Settings Start Recovery Continue Recovery Cancel Backup Criteria... Configure Alerts... Configure Pauses... Schedule Verify...

Recovery mode: Repromotion Active Directory forest: acme.lab DCs to be processed: 3 of 6 Domains to be processed: 3 of 3
Pending DCs: 0 Succeeded DCs: 3 Failed DCs: 0
Elapsed time: 00:09:58

Computer	Type	Recovery Method	Target computer	Status	Domain
acmedc1.acme.lab	GC	Do nothing			acme.lab
acmedc2.acme.lab	GC	Install Active Directory From Media	10.1.2.10	Completed successfully	acme.lab
aussiedc1.aussie.acme.lab	GC	Do nothing			aussie.acme.lab
aussiedc2.aussie.acme.lab	GC	Install Active Directory From Media	10.1.2.20	Completed successfully	aussie.acme.lab
poodledc1.poodle.acme.lab	GC	Do nothing			poodle.acme.lab
poodledc2.poodle.acme.lab	GC	Install Active Directory From Media	10.1.2.30	Completed successfully	poodle.acme.lab



通往雲端！
混和AD環境該如何恢復呢？



混合雲使風險更加複雜



企業對Azure AD的依賴正在增加



有更多雲端物件需要保護 – O365 groups, B2B/B2C users



本地AD將影響Azure AD

MAERSK遭受NotPetya攻擊



無法檢索裝運清單



無法將貨物與貨船匹配



貨物滯留在港口



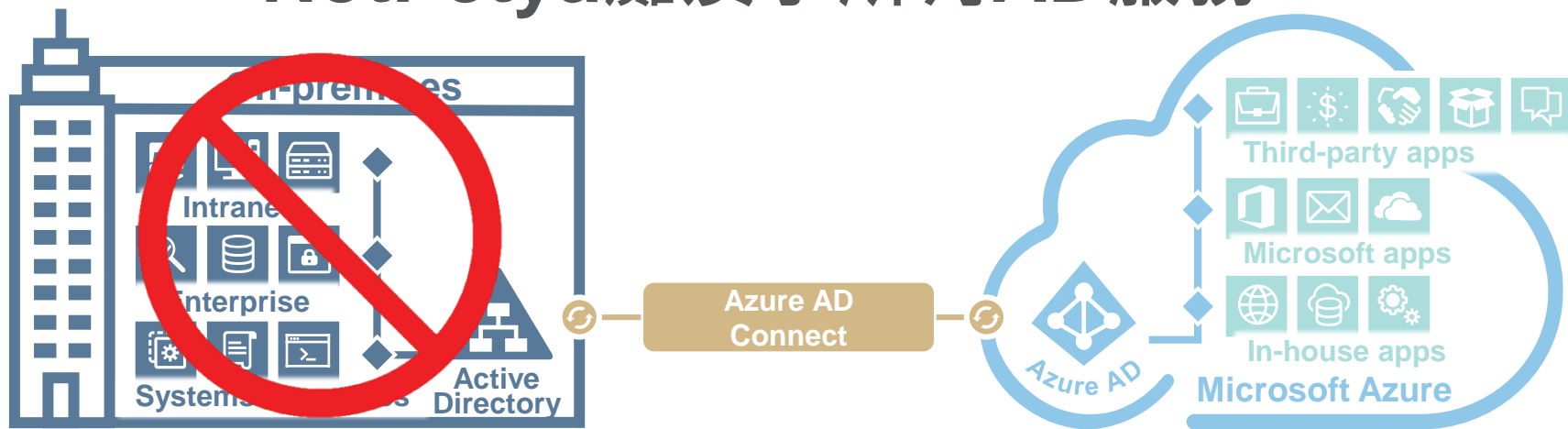
卡車停滯在
伊麗莎白海港碼頭



貨船在海上等待靠岸



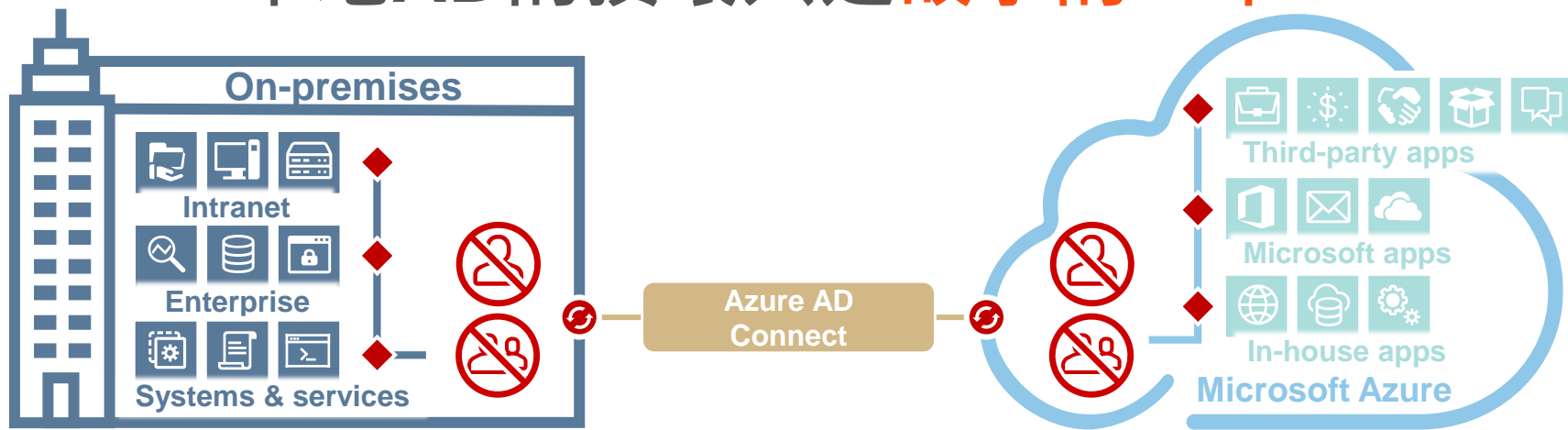
NotPetya癱瘓了所有AD服務



透過釣魚連接進入AD，然後感染至全球各地的AD

- 1. 一台普通用戶電腦因點擊**釣魚郵件**而中招，病毒感染該電腦後，獲取到本機維護過的管理員密碼。
- 2. 接下來使用該權限傳播到一台IT人員的電腦，然後在該IT人員的記憶體中**獲取到了AD網域管理權限**。
- 3. 然後開始**感染其他有權限登入的工作站、應用程式伺服器、資料庫...等**，最後直到整個公司的網路環境崩壞。

本地AD的損壞只是故事的一半



Azure AD Connect將執行其工作並刪除Azure AD中對應的物件



所有特定於雲端的帳戶屬性全部丟失。包括許可證分配、應用程式和資料存取的權限。

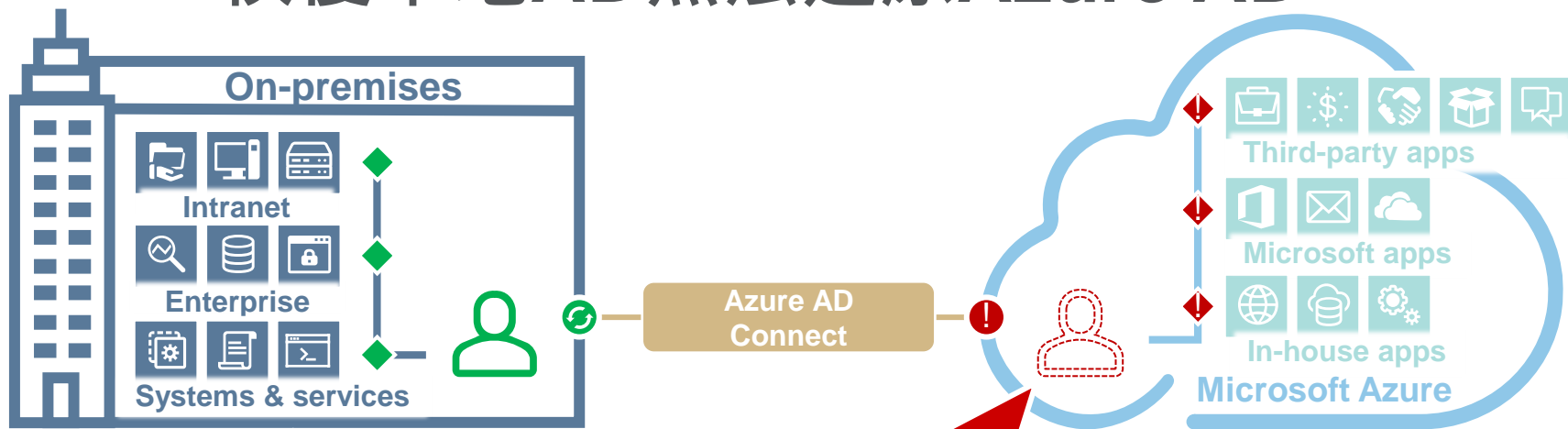


默認的情況下，每30分鐘將同步一次。在回滾變更之前，很有可能就已經完成了。



從同步中刪除帳號將會自動刪除匹配的Azure AD用戶。如果您不小心更改OU，則可能發生類似情況。

恢復本地AD無法還原Azure AD



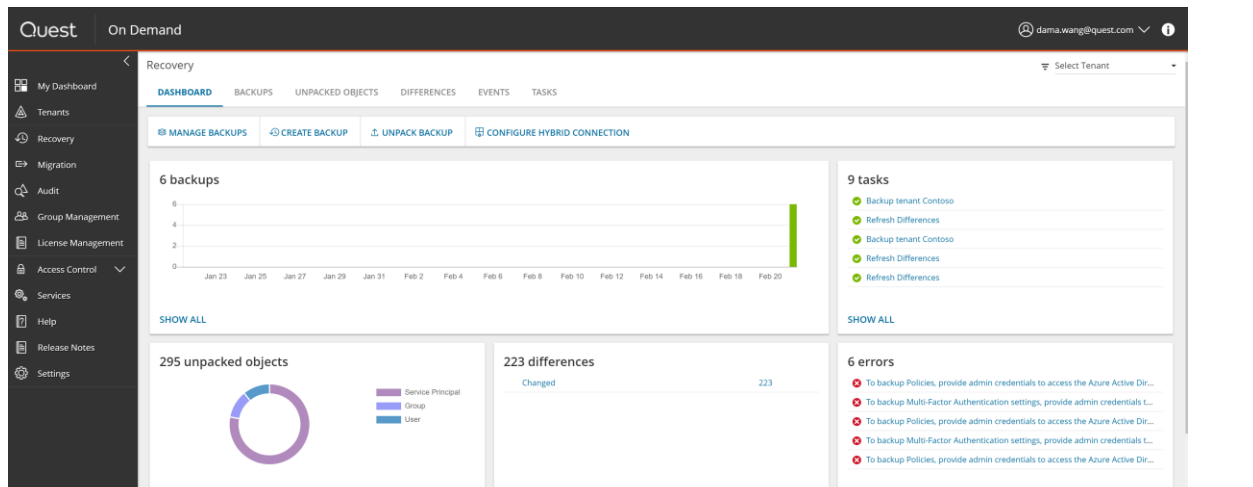
- Azure AD連接同步建立全新用戶
- 雲端相關資訊將被重置：在本地 AD上不儲存這些資訊
- 應用程式和資料存取和的存取權限中斷

[查看丟失的內容](#)

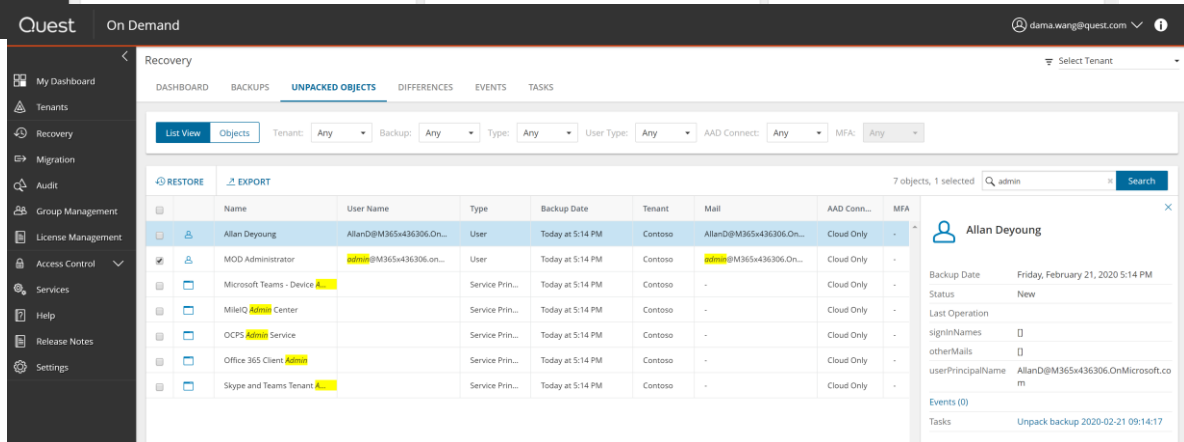


雲端備份還 還AAD物件

Quest



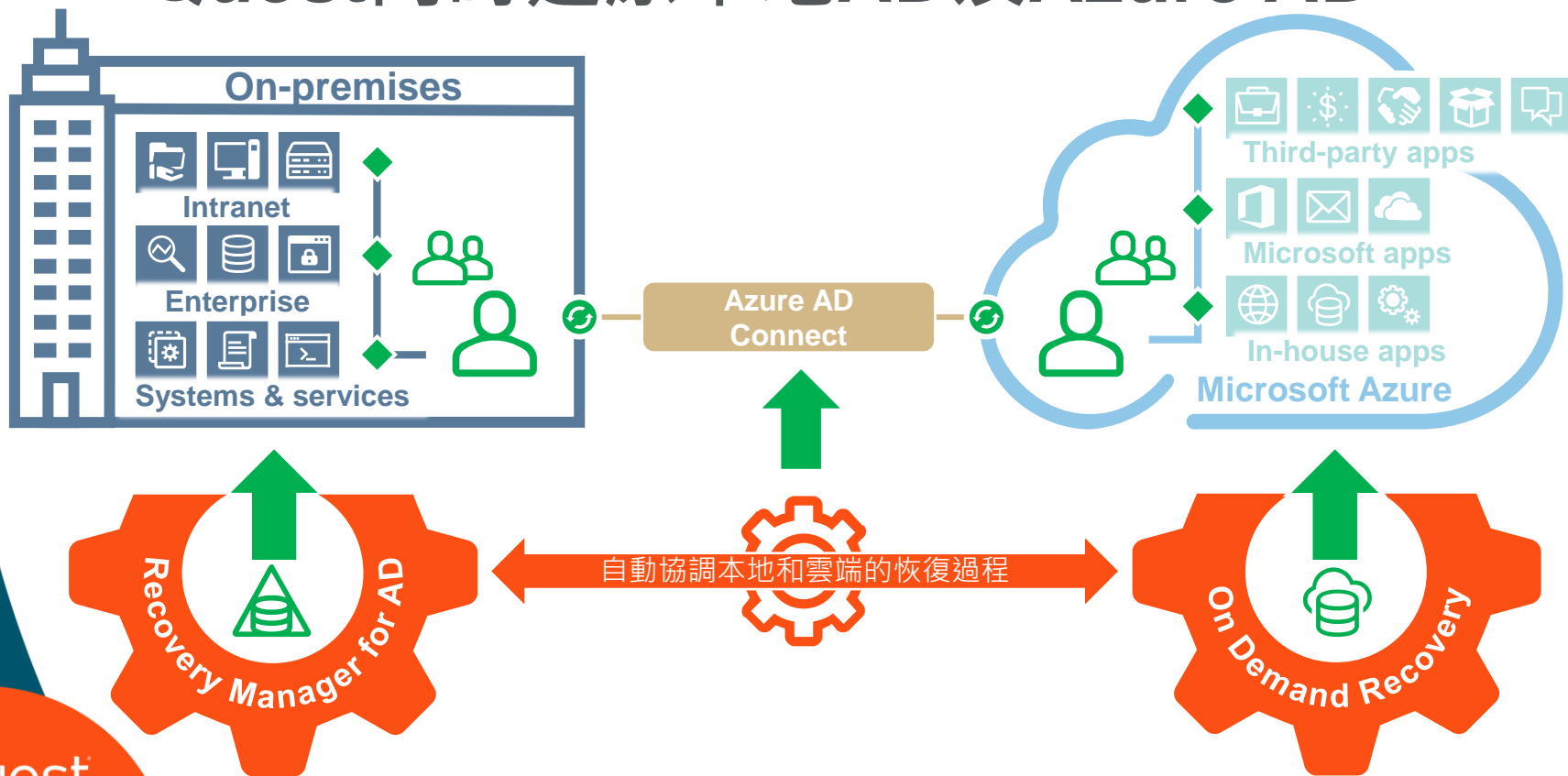
The screenshot shows the 'Recovery' dashboard in Quest On Demand. The left sidebar contains navigation options: My Dashboard, Tenants, Recovery, Migration, Audit, Group Management, License Management, Access Control, Services, Help, Release Notes, and Settings. The main content area is titled 'Recovery' and includes a 'Select Tenant' dropdown. Below the title are tabs for DASHBOARD, BACKUPS, UNPACKED OBJECTS, DIFFERENCES, EVENTS, and TASKS. The DASHBOARD tab is active, showing a 'MANAGE BACKUPS' button, a 'CREATE BACKUP' button, an 'UNPACK BACKUP' button, and a 'CONFIGURE HYBRID CONNECTION' button. A bar chart displays '6 backups' from Jan 23 to Feb 20. A list of '9 tasks' is shown on the right, including 'Backup tenant Contoso' and 'Refresh Differences'. Below the chart is a 'SHOW ALL' link. A donut chart shows '295 unpacked objects' categorized by Service Principal, Group, and User. A table shows '223 differences' with a 'Changed' status and a count of 223. A list of '6 errors' is displayed at the bottom right, all related to Azure Active Directory access issues.



The screenshot shows the 'Unpacked Objects' view in Quest On Demand. The left sidebar is the same as the previous screenshot. The main content area is titled 'Recovery' and includes a 'Select Tenant' dropdown. Below the title are tabs for DASHBOARD, BACKUPS, UNPACKED OBJECTS, DIFFERENCES, EVENTS, and TASKS. The UNPACKED OBJECTS tab is active, showing a 'List View' button, an 'Objects' button, and filters for Tenant, Backup, Type, User Type, AAD Connect, and MFA. Below the filters are 'RESTORE' and 'EXPORT' buttons. A table lists 7 objects, with 1 selected. The table columns are Name, User Name, Type, Backup Date, Tenant, Mail, AAD Conn., and MFA. The selected object is 'Allan Deyoung', a User, backed up today at 5:14 PM. A detailed view of the selected object is shown on the right, including the user's name, backup date, status, last operation, sign-in names, other mails, user principal name, and events.

Name	User Name	Type	Backup Date	Tenant	Mail	AAD Conn.	MFA
Allan Deyoung	AllanD@M365x436306.On...	User	Today at 5:14 PM	Contoso	AllanD@M365x436306.On...	Cloud Only	-
MOD Administrator	admin@M365x436306.on...	User	Today at 5:14 PM	Contoso	admin@M365x436306.On...	Cloud Only	-
Microsoft Teams - Device		Service Prin...	Today at 5:14 PM	Contoso	-	Cloud Only	-
Microsoft 365 Admin Center		Service Prin...	Today at 5:14 PM	Contoso	-	Cloud Only	-
OCPS Admin Service		Service Prin...	Today at 5:14 PM	Contoso	-	Cloud Only	-
Office 365 Client	Admin	Service Prin...	Today at 5:14 PM	Contoso	-	Cloud Only	-
Skype and Teams Tenant		Service Prin...	Today at 5:14 PM	Contoso	-	Cloud Only	-

Quest同時還原本地AD及Azure AD



Recovery Manager for AD + On Demand Recovery

混合AD環境完整備份和災難恢復解決方案



Visit www.quest.com to understand more about

- Recovery Manager for AD Disaster Recovery Edition
- On Demand Recovery

Thank You!

Quest

quest.com | confidential

Where Next Meets Now.

