2024 年 8 月|電子書

建立企業韌性

利用公有雲實現業務連續性和災難復原

NUTANIX

前言

隨著組織在日益激烈的市場中努力保持敏捷，選擇能讓客戶、利益相關者保持靈活，並即時回應需求的 IT 解決方案與基礎設施比以往任何時候都更加重要。大多數現代組織選擇將應用程式和其他工作負載遷移到公有雲——在許多情況下是多個公有雲——以實現這種敏捷性和靈活性。

管理和維護包括本地端、多個私有或公有雲以及邊緣部署的基礎設施可能會變得非常複雜，而且速度很快。如果管理這些基礎設施已經具有挑戰性，那麼當系統的一部分出現故障或在惡意攻擊中被入侵時會發生什麼呢？在混合多雲端環境中，業務連續性和災難復原是如何運作的？

在本電子書中，我們將探討為什麼企業今天與更多公有雲供應商合作，以及當最壞的情況成為現實時，他們面臨的災難復原挑戰。我們還將介紹成功的企業如何減輕停機的風險和情況，並確保更好的業務連續性，以便更成功地競爭和茁壯成長。

目錄

業務彈性復原力對於企業成功至關重要

保持營運運行——或盡快恢復營運——是當今企業的迫切需要。客戶期望靈活、便利的服務和支援，以及與大多數企業的全通路互動。在現今快速變化的數位環境中，如果你的零售網站當機，客戶很可能會幾分鐘內就在其他地方找到所需的東西。如果你的應用程式無法運作，許多客戶會迅速在社群媒體論壇上發洩他們的沮喪情緒。

停機影響的不僅僅是客戶。組織的利益相關者、供應商、合作夥伴和內部員工也依賴於對資料和系統的一致存取。如果他們無法有效地工作或與你的公司或代表進行溝通，業務將受到損害。沒有業務連續性，你將面臨品牌聲譽、盈利、客戶體驗和滿意度、品牌忠誠度等方面的風險。

一項最近的研究發現，非計畫的 IT 停機每年造成企業總損失達 4,000 億美元。這一經濟損失不僅來自於交易損失或客戶流失，還可能包括法律罰款或處罰。無法防止停機或迅速恢復將威脅到當今企業的存在。

除了業務連續性之外，企業還必須擁有強大的災難復原策略——即在未計畫的中斷後如何重新啟動系統並恢復正常營運的計畫。災難復原計畫有助於維持你的業務連續性。

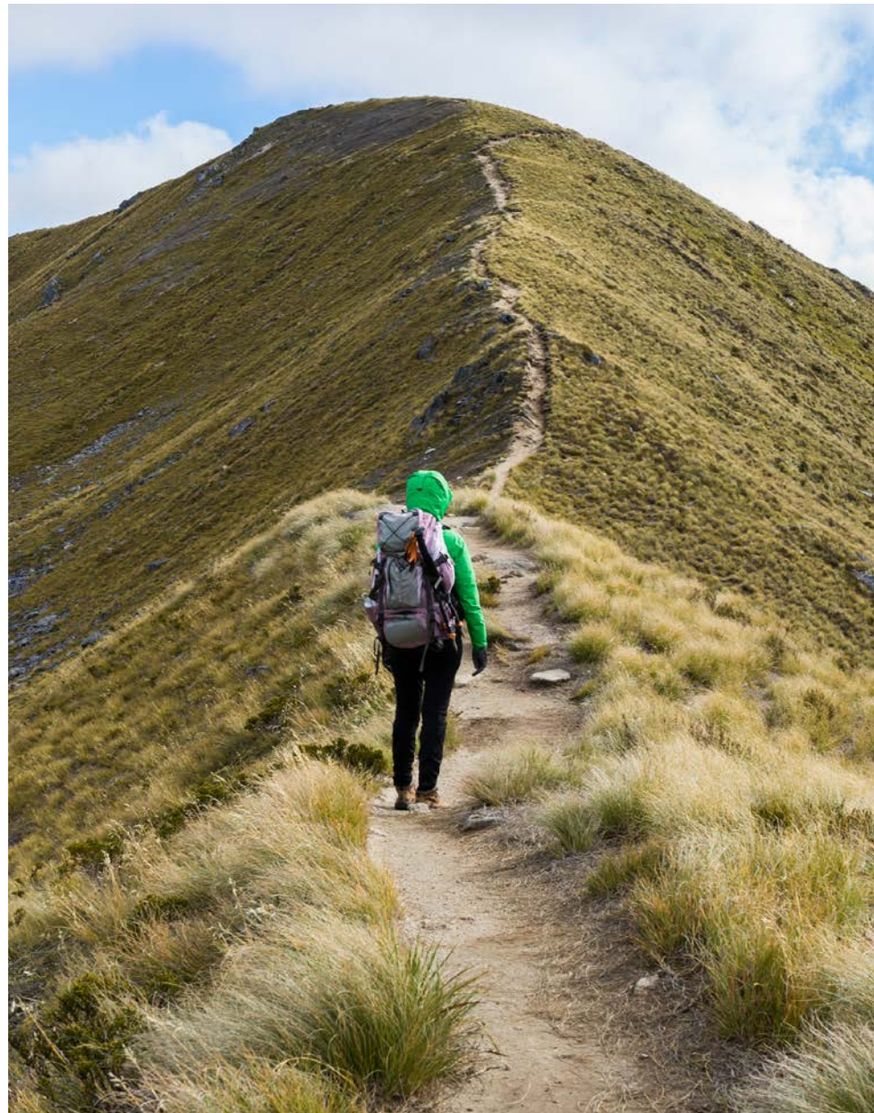
災難復原屬於業務連續性這一總體概念。業務連續性還包括資料保護，備份靜態資料並複寫生產資料，以便在惡意攻擊或其他未計畫事件發生時進行還原。資料保護和災難復原是業務彈性復原力的關鍵因素，即你能夠多快地反彈或適應對營運、員工、服務、資產或客戶構成威脅的突發、意外變化。

BCDR
代表業務連續性和災難復原，是涵蓋資料保護和災難復原所有方面的總稱。

保持營運持續性
是組織防範和從潛在威脅與漏洞中恢復的能力，並在合理的時間內以最小的損害恢復正常業務營運。

災難復原
是透過實施工具、政策和程序，以及重新建立重要業務營運，恢復關鍵 IT 功能的能力。

資料保護
處理在未計畫中斷期間遺失或損壞之資料的遷回過程。



現今的混合多雲端可能對 BCDR 構成挑戰

現代 IT 基礎架構的標準是混合多雲端。Nutanix 最近的一項研究發現，超過 80% 受調查組織認為混合 IT 環境對其管理應用程式和資料的能力最為有利。近一半的受訪者表示，混合 IT 已成為 CIO 的首要任務。

混合多雲端基礎設施為企業提供了多種部署資料和應用程式的選擇，以及各種運算成本和計費模型。這就是組織喜歡它的原因。他們可以在最佳運行環境中為每個工作負載或應用程式找到最佳位置。

然而，這些選項也有一些缺點。更多的環境意味著更多的複雜性。使用混合多雲端時，許多組織擁有來自多個供應商的解決方案，每個解決方案或環境都有其所需的工具集、技能和安全程序。對於 IT 來說，管理和監控混合多雲端基礎設施，並使每個環境互操作和連接是一項真正的挑戰。

當最壞的情況發生，資料在有意攻擊或自然災害中丟失或損壞時，這一挑戰尤為嚴重。在混合多雲端生態系統中，災難復原和維持業務連續性可能變得特別複雜。如果無法重新啟動系統並恢復資料，企業可能會遭受嚴重後果。

混合環境
IT 模型由位於各種環境中的工作負載和應用程式組成——包括本地端、託管、私有雲、公有雲和服務供應商雲端，以及邊緣位置。

多雲環境
表示組織在多個公有雲中擁有資料和應用程式。

> 隨著越來越多的環境，複雜性越來越多。對於 IT 來說，管理和監控混合多雲端基礎設施，並使每個環境互相連接操作是一項真正的挑戰。混合多雲端也使 BCDR 變得更加複雜。

不斷演變的威脅環境使 BCDR 成為必須

混合多雲端基礎設施益增的複雜性，不僅適用於管理和維護，還延伸到 BCDR。由於混合多雲端跨越本地端、邊緣和公有雲環境，你在每個環境中保護和恢復資料的方式可能有所不同。

保護你的資料和應用程式，並能夠在必要時快速恢復它們，是一項業務迫切需要，也是成功的關鍵。主要是因為當今不斷演變的威脅環境，很可能意味著你將經歷意想不到的停機，例如勒索軟體、外部入侵者、停電等等。這是「何時」，而不是「是否」的問題。

導致停機的原因可能從簡單的設備故障到內部員工的錯誤或不當行為，再到由火災、洪水或地震等自然事件引起的電力或網路中斷。

當今企業面臨的最迫切威脅之一是勒索軟體和其他網路攻擊。根據最新的 Nutanix 企業雲端指數報告，受訪企業將勒索軟體防護和資料安全列為其組織面臨的最大資料管理挑戰。71% 的受訪者在經歷勒索軟體攻擊後，回應需要數天甚至數週才能恢復全面營運。根據每個業務的情況不同，但即使只是短暫的停機也可能造成災難。

勒索軟體不會在短期內消失。事實上，攻擊的頻率正在增加。Symantec 研究在 2024 年 1 月的一項研究發現，「2023 年 10 月勒索軟體攻擊激增，2023 年 10 月受勒索軟體影響的組織數量比一年前增加了 66%。」

面對日益增長的勒索軟體攻擊和其他意外停機原因，企業擁有強大的 BCDR 計畫以提高韌性比以往任何時候都更加重要。

> 71% 曾受勒索軟體攻擊的組織表示，需要數天甚至數週才能恢復全面營運。（第六屆 Nutanix 企業雲端指數）

確保業務彈性復原力——無論你的資料位於何處

良好的 BCDR 計畫在發生停機時將會掌握企業命脈。恢復資料和維持業務連續性並不總是需要大規模操作。可以將 BCDR 視為涵蓋從簡單備份到全面災難復原的一系列流程。有時可能只是將系統還原到最近的快照，或僅保持資料盡可能最新的狀態。

當今的惡意行為者和勒索軟體不僅針對主要資料，還針對本地端的備份。這使得組織面臨更大的風險，因為如果他們無法存取備份，他們更有可能需要支付贖金。因此，創建、儲存資料和運算環境的異地副本（例如：作業系統和應用程式）是非常重要的。

長期以來，IT 行業一直依賴 3-2-1 備份規則，這一規則至今仍然有效。該規則規定，組織應至少擁有 **3** 份資料副本，儲存在 **2** 個位置，其中 **1** 個位置位於異地。

混合多雲端基礎設施的一個優點是，你已經在多個環境中擁有資料和應用程式。每個環境還可以作為系統中其他位置資料和應用程式的備份。

實現完善的 BCDR 策略並不容易。它涉及最佳實踐的謹慎組合、定期的 IT 資源備份和頻繁的災難復原計畫測試。

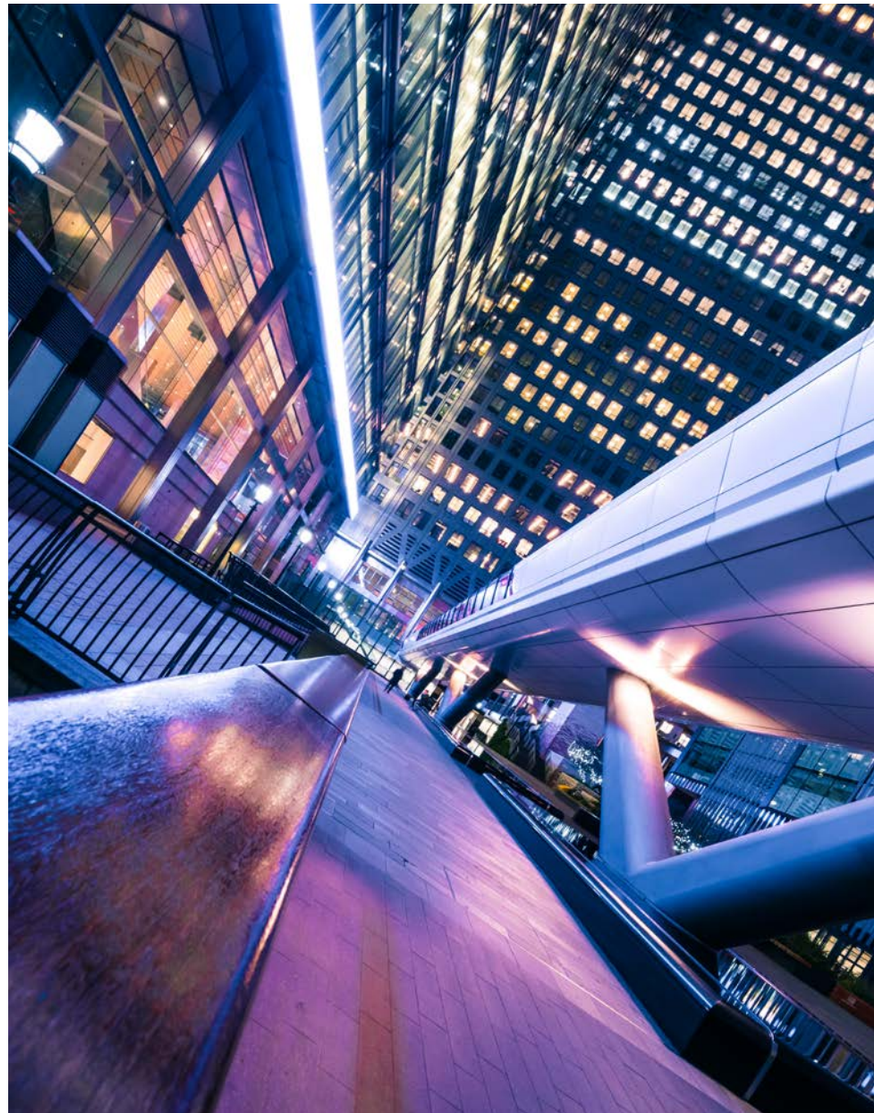
業務連續性和災難復原要求資料免受損壞、遺失或外洩。資料保護的兩個子類別是：

備份

建立資料副本的過程。大多數備份解決方案進行偶爾的完整備份，配合定期的、通常是夜間的增量備份，只複製自上次備份以來更改的資料。組織設定備份頻率和保留策略，以確保足夠的復原點並遵守法規。

複寫

在公司站點之間複製並移動資料的行為。通常以復原時間目標 (RTO) 和復原點目標 (RPO) 來衡量。它在災難發生後，提供應用程式的不間斷運行以及面向客戶的應用。複寫應配合容錯移轉和故障復原能力，以確保在災難期間最小的停機時間和資料損失。



將公有雲作為 BCDR 策略的一部分

在 3-2-1 備份規則中，許多當今的組織使用公有雲作為本地端資料的異地備份位置。事實上，IDC 2023 年的一項調查中發現，在擁有混合和/或多雲端基礎設施的企業中，67% 使用一種基於雲端的 BCDR 形式。

同一調查報告指出，關於雲端投資的兩大考量因素是 (1) 全面的安全性和 (2) 災難復原與備份。它還強調了備份和災難復原如何成為混合策略的組成部分，發現當今最常見的方法，涉及從本地端私有雲備份資料並將其儲存在公有雲中。第二常見的備份方法是將本地端資料中心的副本儲存在託管的私有雲中。

在選擇災難復原模型時，IDC 報告指出，使用混合多雲端基礎架構的企業主要是因為資料保護的優勢、資料檢索速度和管理便利性等原因。

公有雲作為災難復原策略的一部分，可以帶來極大的好處。

公有雲使快速恢復資料變得簡單，有助於減少停機時間並最小化攻擊或中斷的影響。它還提供了本地端基礎設施所不具備的各種能力和優勢，包括：

- **無資本成本**或額外購買設備的需求
- **自動化操作**減輕管理負擔
- **統一的管理平台**提升效率
- **消除**閒置資源和過時的備份
- **降低成本**並減少 IT 管理負擔
- **需要時實現快速、簡單的**擴展
- **資料不可變性**，防止資料刪除或更改

PENN NATIONAL INSURANCE

美國佩恩保險 (Penn National Insurance) 需要簡化其擴展中的本地虛擬桌面基礎設施 (VDI) 的管理方式。同時，也在尋找對基於磁帶的災難復原系統進行大幅度更新的方法。

Nutanix 透過 Nutanix Cloud Clusters (NC2) 解決了這兩個挑戰，該解決方案在本地端和 AWS 中運行，允許保險提供商完全擁抱混合多雲端模型，並輕鬆將本地端資料複寫到雲端。

美國佩恩保險資深基礎架構系統架構師 Craig Wiley 表示：「如果我們發生災難，我們可以迅速在 AWS 上啟動 NC2，並在雲端啟動複寫的資料。」「透過將我們的災難復原遷移到 AWS 雲端，我們的復原時間從幾天縮短到不到兩小時。」

在此閱讀完整案例研究

選擇基於雲端的 BCDR 解決方案應注意事項

雖然混合多雲端可能增加企業的 IT 複雜性，但你可以透過選擇具有適當功能和能力的解決方案來降低這種風險。

良好的 BCDR 解決方案的一個最重要特徵是，它允許你將混合多雲端中的所有環境，包括本地端和邊緣，作為一個單一系統來管理和監控。互操作性至關重要。事實上一些專家甚至認為，孤立的混合多雲端，每個環境彼此分離，並不是真正的混合多雲端。基礎架構的好處，只有在所有部分無縫協作時才存在。

有助於滿足各種 SLA 需求的重要特性和功能包括：

快照 — 伺服器在特定時間的快速「拍照」，包括檔案、軟體和設置。快照保留某個「時點」的狀態，不需要複製或移動伺服器的資料。

複寫 — 將資料複製到不同的站點進行儲存，通常與主要來源在地理位置上不同。

災難復原分級 — 分級可定義使用特定方法復原資料的速度。級別越高，復原速度越快（也更昂貴）。級別範圍從「無異地儲存資料」（級別 0）到「自動化災難復原，通常具有 AI 功能」（級別 7）。

AWS 彈性災難復原整合 — 彈性災難復原是一種快速、簡單的方式，將資料恢復到 AWS。如果你使用 AWS，BCDR 解決方案應與其整合。

叢集休眠 — 某些災難復原解決方案具有在關閉或進入休眠狀態時將叢集資料備份到雲端（例如 AWS 儲存桶）的能力。休眠在叢集未使用時很有益。

簡而言之，一個良好的恢復解決方案，應該允許你以最小的停機時間和資料損失恢復正常業務營運。

同步複寫
將資料在寫入主儲存時同時複寫到儲存庫的過程。

非同步複寫
資訊首先被寫入主要儲存，儲存在記憶設備中，然後在稍後的指定時間複寫到另一個儲存位置。它使用的頻寬比同步複寫少，並且設計上更適合長距離操作。

近乎同步複寫
一個持續運行的過程，只複寫已更改的資料。它是非計畫的且不需要快照。

NC2 簡化業務連續性與災難復原

使用 NC2，你的業務連續性和災難復原計畫的管理，可以變得簡單又有效率。它使組織能夠在不增加複雜性的情況下，加速其混合多雲端計畫。此外，它還提供了一鍵式災難復原功能，有助於降低維護多個災難復原站點的成本和複雜性。透過按需彈性和自動主機修復，它為所有 IT 環境提供了單一、一致的管理門戶。如果你在雲端經歷資料遺失或攻擊，你的資料和應用程式仍將可用。這在當今競爭激烈的環境中有著重大意義。

瞭解更多有關 Nutanix BCDR 解決方案 **和** NC2 **的資訊。**

你也可以免費試用**或**聯繫我們**以瞭解更多相關資訊。**

NUTANIX

info@nutanix.com | www.nutanix.com | @nutanix

eBook-Nutanix-Building-Business-Resilience-FY25Q1-V4-08292024_zh-TW-01222025