

AWS Well-Architected 架構

上工作負載的災難復原 AWS：雲端中的復原



上工作負載的災難復原 AWS：雲端中的復原: AWS Well-Architected 架構

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商標或商業外觀不得用於 Amazon 產品或服務之外的任何產品或服務，不得以可能在客戶中造成混淆的任何方式使用，不得以可能貶低或損毀 Amazon 名譽的任何方式使用。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能隸屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

摘要	1
簡介	2
災難復原和可用性	2
您是 Well-Architected 嗎？	4
彈性的共同責任模型	5
AWS 責任「雲端的彈性」	5
客戶責任「雲端中的彈性」	5
什麼是災難？	7
高可用性不是災難復原	8
業務持續性計劃 (BCP)	9
業務影響分析和風險評估	9
復原目標 (RTO 和 RPO)	9
災難復原在雲端中有所不同	13
單一 AWS 區域	13
多個 AWS 區域	14
雲端中的災難復原選項	15
備份和還原	15
AWS 服務	16
指示燈	19
AWS 服務	20
AWS 彈性災難復原	22
暖待命	22
AWS 服務	23
多站點主動/主動	24
AWS 服務	25
偵測	27
測試災難復原	28
結論	29
貢獻者	30
深入閱讀	31
文件歷史紀錄	32
注意	33
AWS 詞彙表	34
.....	xxxv

上工作負載的災難復原 AWS：雲端中的復原

發佈日期：2021 年 2 月 12 日 ([文件歷史紀錄](#))

災難復原是準備災難並從災難中復原的程序。防止工作負載或系統在其主要部署位置實現其業務目標的事件會被視為災難。本文概述規劃和測試部署到任何工作負載災難復原的最佳實務 AWS，並提供不同的方法來降低風險，並滿足該工作負載的復原時間目標 (RTO) 和復原點目標 (RPO)。

本白皮書涵蓋如何實作工作負載的災難復原 AWS。如需使用 [做為現場部署工作負載災難復原網站的相關資訊](#)，請參閱 [的現場部署應用程式的災難 AWS 復原](#)。AWS

簡介

您的工作負載必須正確且一致地執行其預期功能。若要達成此目的，您必須架構彈性。彈性是工作負載從基礎設施、服務或應用程式中斷中復原的能力，動態取得運算資源以滿足需求，並減少中斷，例如組態錯誤或暫時性網路問題。

災難復原 (DR) 是彈性策略的重要部分，並擔心工作負載在災難發生時如何回應 ([災難](#)是對業務造成嚴重負面影響的事件)。此回應必須基於組織的業務目標，指定工作負載的策略，以避免遺失資料，稱為[復原點目標 \(RPO\)](#)，並減少工作負載無法使用的停機時間，稱為[復原時間目標 \(RTO\)](#)。因此，您必須在雲端工作負載的設計中實作彈性，以滿足特定一次性災難事件的復原目標 ([RPO 和 RTO](#))。此方法可協助您的組織維持業務持續性，作為[業務持續性規劃 \(BCP\)](#) 的一部分。

本文著重於如何在上規劃、設計和實作架構 AWS，以符合您業務的災難復原目標。此處共用的資訊適用於擔任技術角色的人員，例如技術長 (CTOs)、架構師、開發人員、營運團隊成員，以及負責評估和降低風險的人員。

災難復原和可用性

災難復原可以與可用性進行比較，可用性是彈性策略的另一個重要組成部分。雖然災難復原會測量一次性事件的目標，但可用性目標會測量一段時間內的平均值。

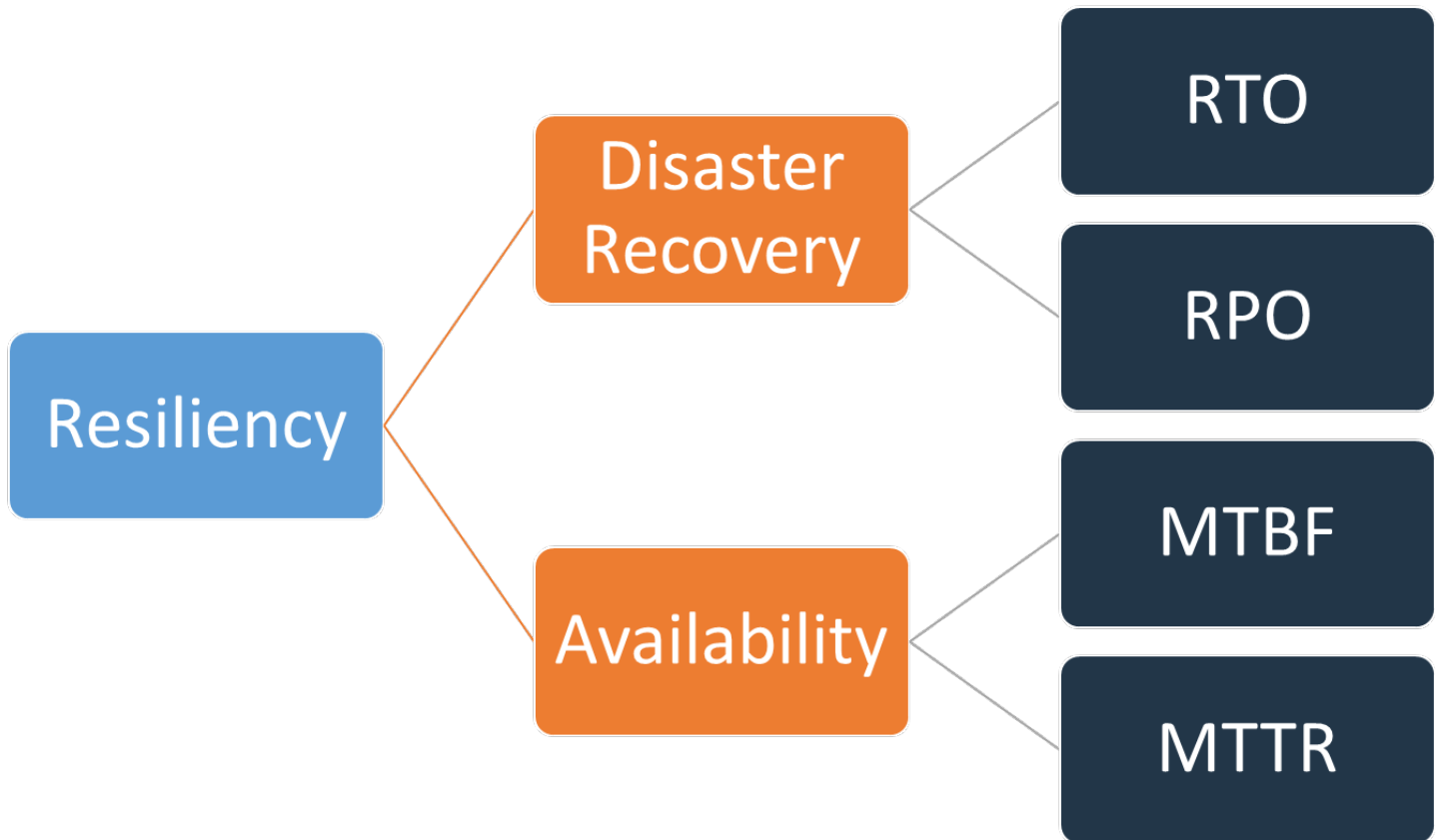


圖 1 - 彈性目標

可用性的計算方式是使用平均故障間隔時間 (MTBF) 和平均復原時間 (MTTR)：

$$Availability = \frac{Available\ for\ Use\ Time}{Total\ Time} = \frac{MTBF}{MTBF + MTTR}$$

這種方法通常稱為「nines」，其中 99.9% 的可用性目標稱為「三九」。

對於您的工作負載，計數成功和失敗的請求可能更容易，而不是使用以時間為基礎的方法。在這種情況下，可以使用下列計算：

$$Availability = \frac{Successful\ Responses}{Valid\ Requests}$$

災難復原著重於災難事件，而可用性著重於較常見的較小規模中斷，例如元件故障、網路問題、軟體錯誤和負載尖峰。災難復原的目標是業務連續性，而可用性問題是將工作負載可用於執行其預期業務功能的時間最大化。兩者都應該是彈性策略的一部分。

您是 Well-Architected 嗎？

[AWS Well-Architected Framework](#) 可協助您了解在雲端建置系統時所做決策的優缺點。架構的六大支柱可讓您學習架構最佳實務，以設計和操作可靠、安全、有效率、經濟實惠且永續的系統。您可以使用 [AWS 管理主控台中免費提供的 AWS Well-Architected 工具](#)，透過回答每個支柱的一組問題，根據這些最佳實務來檢閱工作負載。 <https://console.aws.amazon.com/wellarchitected>

本白皮書涵蓋的概念擴展了[可靠性支柱白皮書](#)中包含的最佳實務，特別是問題 [REL 13](#)：「如何規劃災難復原 (DR)？」。實作本白皮書中的實務後，請務必使用 AWS Well-Architected Tool 檢閱（或重新檢閱）工作負載。

彈性的共同責任模型

彈性是 AWS 與身為客戶的您共同的責任。請務必了解災難復原和可用性如何在此共用模型下運作，作為恢復能力的一部分。

AWS 責任「雲端的彈性」

AWS 負責執行 AWS 雲端中提供的所有服務的基礎設施彈性。此基礎設施包含執行 AWS 雲端服務的硬體、軟體、聯網和設施。AWS 會盡商業上合理的努力提供這些 AWS 雲端服務，確保服務可用性符合或超過 [AWS 服務水準協議 \(SLAs\)](#)。

[AWS Global Cloud Infrastructure](#) 旨在讓客戶能夠建置高彈性的工作負載架構。每個 AWS 區域都是完全隔離的，由多個[可用區域組成](#)，[這些可用區域](#)是基礎設施的實際隔離分割區。可用區域會隔離可能影響工作負載彈性的故障，防止這些故障影響區域中的其他區域。但同時，AWS 區域中的所有區域都會與高頻寬、低延遲聯網互連，透過全冗餘的專用都會光纖，在區域之間提供高輸送量、低延遲聯網。區域之間的所有流量都會加密。網路效能足以完成區域之間的同步複寫。應用程式跨 AZ 分割時，公司可以獲得更好的隔離和保護，讓您免於停電、雷擊、龍捲風、颶風等問題。

客戶責任「雲端中的彈性」

您的責任將由您選取的 AWS 雲端服務決定。這決定您在履行彈性責任過程中必須執行的設定工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 之類的服務需要客戶執行所有必要的彈性組態和管理任務。部署 Amazon EC2 [EC2 執行個體的客戶負責跨多個位置（例如 AWS 可用區域）部署 EC2 執行個體](#)、使用 Amazon EC2 Auto Scaling 等服務 [實作自我修復](#)，以及針對安裝在執行個體上的應用程式使用 [彈性工作負載架構最佳實務](#)。對於 Amazon S3 和 Amazon DynamoDB 等受管服務，AWS 會操作基礎設施層、作業系統和平台，以及客戶存取端點來存放和擷取資料。您負責管理您的資料的彈性，包括備份、版本控制和複寫策略。

在 AWS 區域中跨多個可用區域部署工作負載，是高可用性策略的一部分，旨在透過將問題隔離到一個可用區域來保護工作負載，並使用其他可用區域的備援來繼續處理請求。多可用區域架構也是 DR 策略的一部分，其設計目的是讓工作負載更好地隔離，並且防範例如停電、雷擊、龍捲風、地震等問題。DR 策略也可能利用多個 AWS 區域。例如，在主動/被動組態中，如果作用中區域無法再提供請求，則工作負載的服務會從其作用中區域容錯移轉至其 DR 區域。

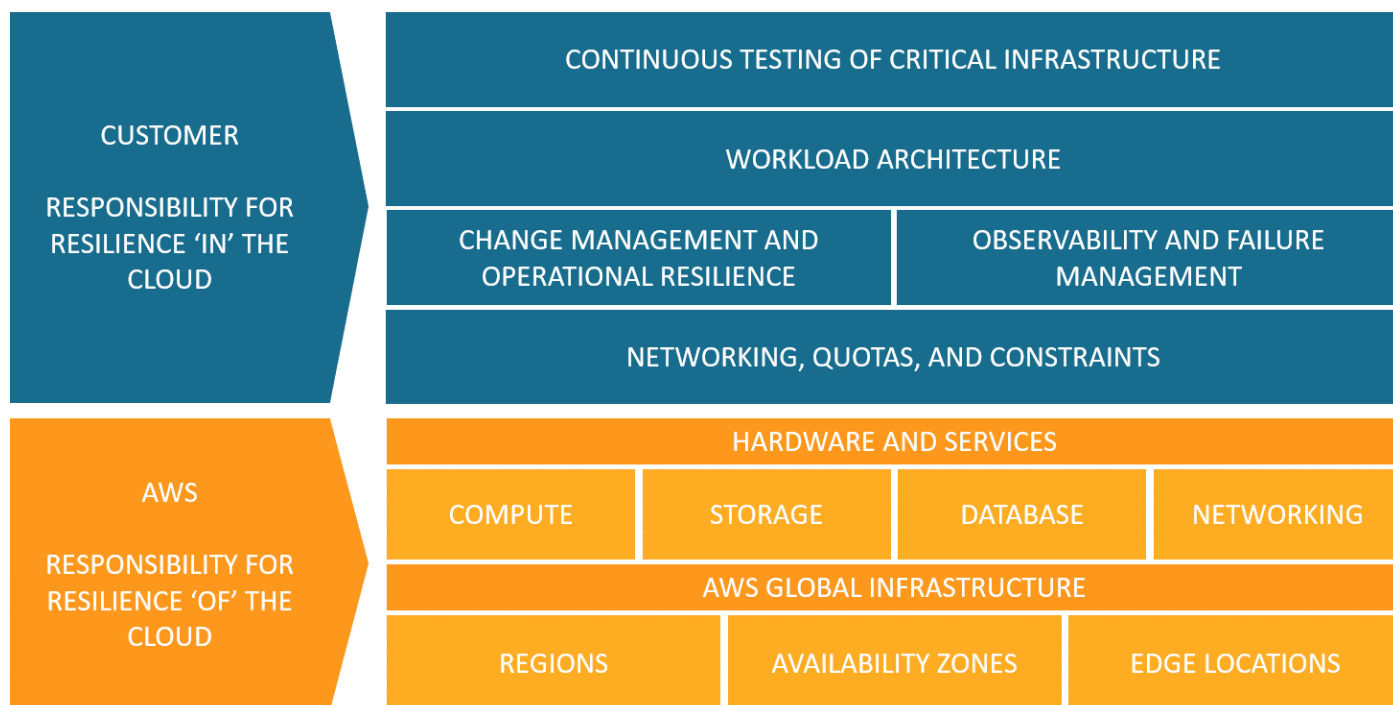


圖 2 - 彈性是 AWS 與客戶之間共同責任

什麼是災難？

規劃災難復原時，請評估您的計劃是否有這三個主要災難類別：

- 自然災難，例如地震或洪水
- 技術故障，例如電源故障或網路連線
- 人為動作，例如無意中設定錯誤或未經授權/外部存取或修改

每個潛在災難也會產生地理影響，包括當地、區域、國家/地區、洲內或全球。在考慮災難復原策略時，災難的性質和地理影響都很重要。例如，您可以透過採用異地同步備份策略來緩解造成資料中心中斷的本機洪水問題，因為它不會影響多個可用區域。不過，對生產資料的攻擊需要您調用災難復原策略，該策略會容錯移轉到另一個 AWS 區域中的備份資料。

高可用性不是災難復原

可用性和災難復原都依賴一些相同的最佳實務，例如監控故障、部署到多個位置，以及自動容錯移轉。不過，可用性著重於工作負載的元件，而災難復原著重於整個工作負載的分散複本。災難復原的目標與可用性不同，可測量符合災難資格的大規模事件之後的復原時間。您應該先確保工作負載符合可用性目標，因為高度可用的架構可讓您在發生可用性影響事件時滿足客戶的需求。您的災難復原策略需要與可用性不同的方法，專注於將離散系統部署到多個位置，以便您可以在必要時容錯移轉整個工作負載。

您必須在災難復原規劃中考慮工作負載的可用性，因為這會影響您採取的方法。在一個可用區域中的單一 Amazon EC2 執行個體上執行的工作負載沒有高可用性。如果本機洪水問題影響該可用區域，則此案例需要容錯移轉至另一個可用區域，以符合 DR 目標。將此案例與部署的[高可用性工作負載進行比較，多站台作用中/作用中](#)，其中工作負載部署在多個作用中區域，且所有區域都在提供生產流量。在這種情況下，即使不太可能發生大規模災難導致區域無法使用，DR 策略是透過將所有流量路由到其餘區域來完成。

您處理資料的方式在可用性和災難復原之間也有所不同。請考慮持續複寫到另一個網站的儲存解決方案，以實現高可用性（例如多站台、主動/主動工作負載）。如果主要儲存裝置上的檔案遭到刪除或損毀，這些破壞性變更可以複寫到次要儲存裝置。在這種情況下，即使高可用性，在資料刪除或損毀的情況下容錯移轉的能力仍會受到影響。相反地，DR 策略也需要point-in-time備份。

業務持續性計劃 (BCP)

您的災難復原計劃應該是組織業務持續性計劃 (BCP) 的子集，它不應該是獨立的文件。如果因為災難對您工作負載以外的業務元素的影響而無法達成工作負載的業務目標，則維護積極的災難復原目標並不重要。例如，地震可能會阻止您傳輸在 eCommerce 應用程式購買的產品 - 即使有效的 DR 保持工作負載正常運作，您的 BCP 仍需要滿足運輸需求。您的 DR 策略應以業務需求、優先順序和內容為基礎。

業務影響分析和風險評估

業務影響分析應量化中斷工作負載的業務影響。它應該識別無法使用工作負載對內部和外部客戶的影響，以及對業務的影響。分析應有助於判斷工作負載需要多快可用，以及可容忍多少資料遺失。但是，請務必注意，不應單獨制定復原目標；中斷的可能性和復原成本是關鍵因素，有助於告知為工作負載提供災難復原的商業價值。

業務影響可能取決於時間。建議您考慮將此納入災難復原規劃的考量。例如，在每個人獲得付款之前，薪資系統的中斷可能會對業務產生非常大的影響，但在每個人獲得付款之後，可能會對業務產生很小的影響。

災難類型和地理影響的風險評估，以及工作負載技術實作的概觀，將決定每種災難類型發生的中斷機率。

對於高度關鍵的工作負載，您可以考慮使用資料複寫和持續備份跨多個區域部署基礎設施，以將業務影響降至最低。對於較不重要的工作負載，有效的策略可能完全不會進行任何災難復原。對於某些災難案例，根據低災難發生機率，不採取任何災難復原策略作為明智決策也是有效的。請記住，AWS 區域內的可用區域在設計時已具有有意義的距離，並仔細規劃位置，因此最常見的災難應該只會影響一個區域，而不會影響其他區域。因此，AWS 區域內的多可用區域架構可能已經滿足您的大部分風險緩解需求。

應考慮業務影響和風險，評估災難復原選項的成本，以確保災難復原策略提供正確的商業價值水準。

透過這些資訊，您可以記錄不同災難案例的威脅、風險、影響和成本，以及相關的復原選項。此資訊應用於判斷每個工作負載的復原目標。

復原目標 (RTO 和 RPO)

建立災難復原 (DR) 策略時，組織最常規劃復原時間目標 (RTO) 和復原點目標 (RPO)。

How much data can you afford to recreate or lose?

How quickly must you recover? What is the cost of downtime?

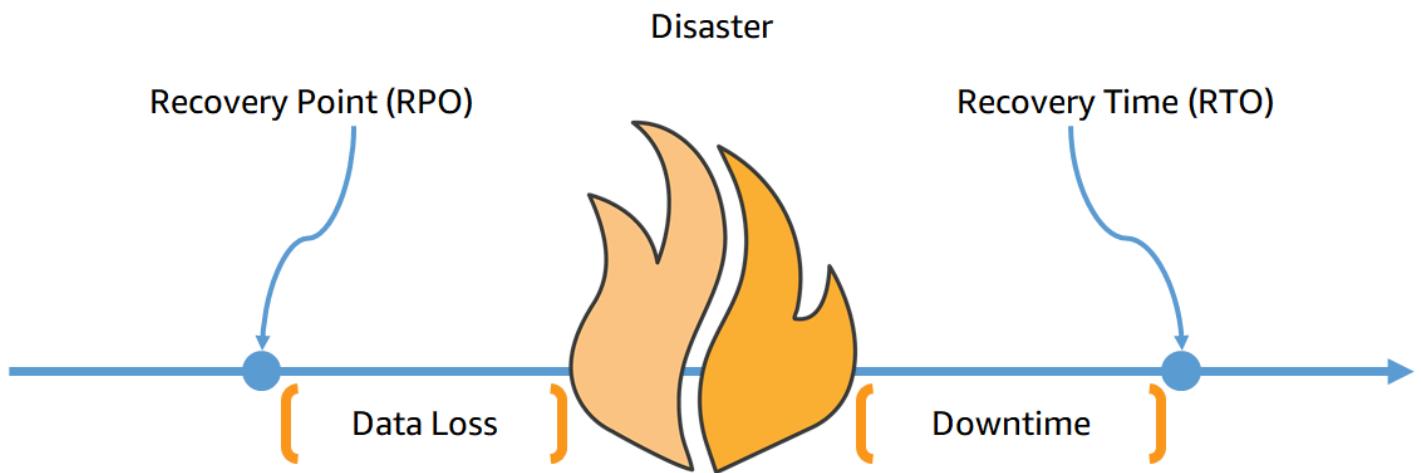


圖 3 - 復原目標

復原時間目標 (RTO) 是服務中斷和服務還原之間的最大可接受延遲。此目標決定當服務無法使用且由組織定義時，哪些是可接受的時段。

本白皮書廣泛討論四種 DR 策略：備份和還原、指示燈、暖待命和多站台作用中/作用中（請參閱 [雲端中的災難復原選項](#)）。在下圖中，企業已決定其允許的 RTO 上限，以及他們可以在服務還原策略上花費的限制。基於業務目標，DR 策略指示燈或暖待命將同時滿足 RTO 和成本標準。

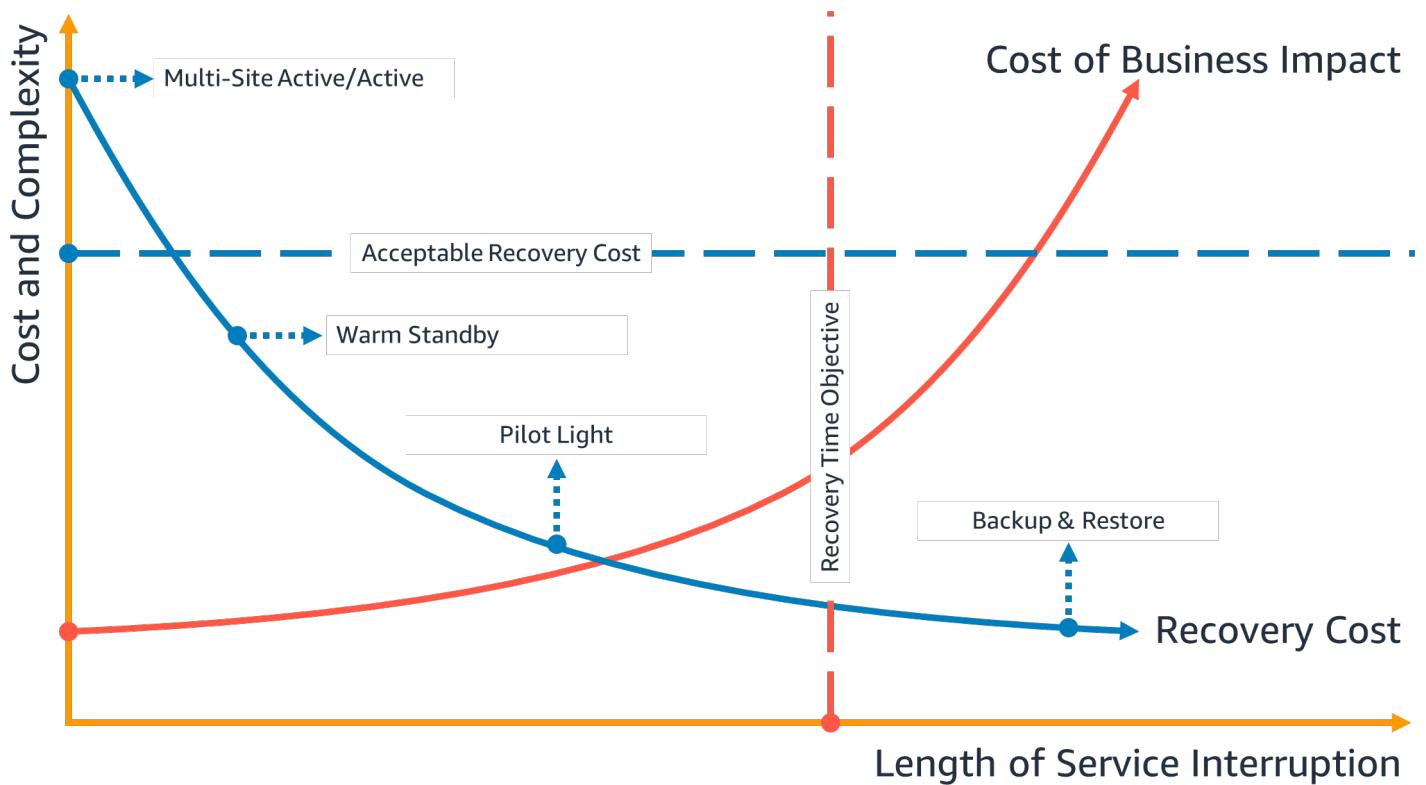


圖 4 - 復原時間目標

復原點目標 (RPO) 是自上次資料復原點以來可接受的時間上限。此目標會決定在最後一個復原點與服務中斷之間可接受的資料遺失情況，並由組織定義。

在下圖中，企業已決定其允許的 RPO 上限，以及他們可以在資料復原策略上花費的限制。在四個 DR 策略中，指示燈或暖待命 DR 策略都符合 RPO 和成本的條件。

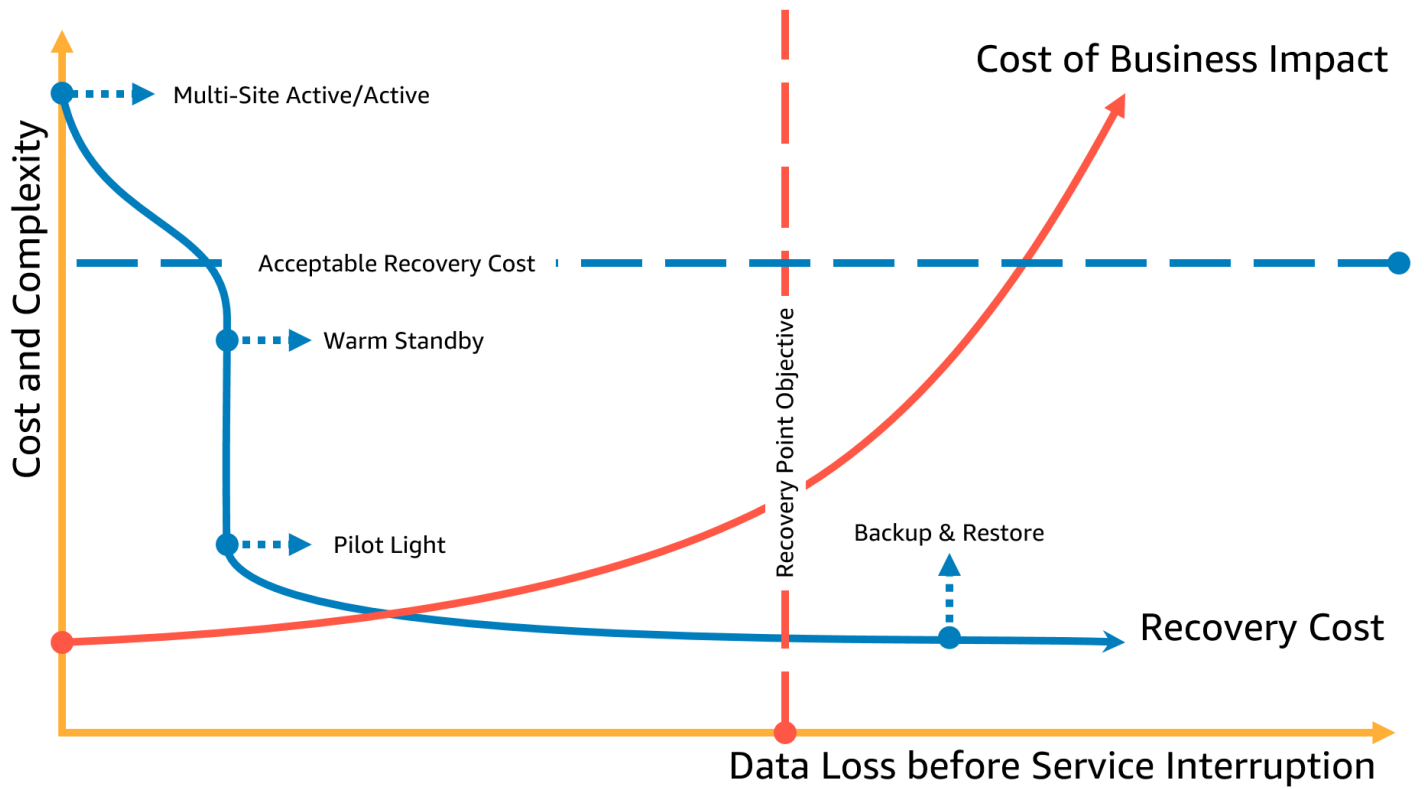


圖 5 - 復原點目標

Note

如果復原策略的成本高於故障或遺失的成本，則不應設置復原選項，除非有法規要求等次要驅動程式。進行此評估時，請考慮各種成本的復原策略。

災難復原在雲端中有所不同

災難復原策略隨著技術創新而演進。現場部署的災難復原計劃可能涉及實際傳輸磁帶或將資料複寫到另一個網站。您的組織需要重新評估其先前災難復原策略的業務影響、風險和成本，才能在 AWS 上實現其 DR 目標。與傳統環境相比，AWS 雲端中的災難復原包含下列優點：

- 從降低複雜性的災難中快速復原
- 簡單且可重複的測試可讓您更輕鬆、更頻繁地進行測試
- 降低管理開銷可減少營運負擔
- 自動化的機會可降低錯誤機率並縮短復原時間

AWS 可讓您將實體備份資料中心的固定資本費用，轉換為雲端中已授權環境的可變操作費用，進而大幅降低成本。

對於許多組織而言，內部部署災難復原是以資料中心工作負載或工作負載中斷的風險，以及備份或複寫資料至次要資料中心的復原為依據。當組織在 AWS 上部署工作負載時，他們可以實作架構良好的工作負載，並依賴 AWS 全球雲端基礎設施的設計，以協助減輕此類中斷的影響。請參閱 [AWS Well-Architected Framework - 可靠性支柱白皮書](#)，以取得在雲端設計和操作可靠、安全、高效且經濟實惠工作負載之架構最佳實務的詳細資訊。使用 [AWS Well-Architected Tool](#) 定期檢閱您的工作負載，以確保它們遵循 Well-Architected Framework 的最佳實務和指導。該工具可在 [中免費使用 AWS 管理主控台](#)。

如果您的工作負載在 AWS 上，您不需要擔心資料中心連線能力（存取的能力除外）、電源、冷氣、防火和硬體。所有這些都是為您管理的，您可以存取多個錯誤隔離的可用區域（每個區域都由一或多個離散的資料中心組成）。

單一 AWS 區域

對於基於中斷或遺失一個實體資料中心的災難事件，在單一 AWS 區域內的多個可用區域中實作高可用性工作負載有助於緩解自然和技術災難。持續備份此單一區域中的資料可以降低人為威脅的風險，例如可能導致資料遺失的錯誤或未經授權的活動。每個 AWS 區域由多個可用區域組成，每個可用區域與其他區域中的故障隔離。每個可用區域輪流由一或多個離散的實體資料中心組成。為了更好地隔離有影響力的問題並實現高可用性，您可以將工作負載分割到相同區域中的多個區域。可用區域專為實體備援而設計，並提供彈性，即使在停電、網際網路停機時間、洪水和其他自然災難的情況下，也能提供不間斷的效能。請參閱 [AWS 全球雲端基礎設施](#)，了解 AWS 如何做到這一點。

透過在單一 AWS 區域中跨多個可用區域部署，您的工作負載可更好地防止單一（甚至多個）資料中心故障。為了對您的單一區域部署提供額外保證，您可以將資料和組態（包括基礎設施定義）備份到另一個區域。此策略可減少災難復原計劃的範圍，只包含資料備份和還原。相對於下節所述的其他多區域選項，透過備份到另一個 AWS 區域來利用多區域彈性是簡單且便宜的。例如，備份到 [Amazon Simple Storage Service \(Amazon S3\)](#) 可讓您立即擷取資料。不過，如果您部分資料的 DR 策略對擷取時間的需求更為寬鬆（從幾分鐘到幾小時），則使用 [Amazon Glacier](#) 或 [Amazon Glacier Deep Archive](#) 將大幅降低備份和復原策略的成本。

有些工作負載可能有法規資料駐留需求。如果這適用於目前只有一個 AWS 區域的工作負載，則除了如上所述設計多可用區域工作負載以獲得高可用性之外，您還可以使用該區域內 AZs 作為分散的位置，這有助於解決適用於該區域內工作負載的資料駐留要求。以下各節所述的 DR 策略使用多個 AWS 區域，但也可以使用可用區域而非區域來實作。

多個 AWS 區域

對於災難事件，包括將多個資料中心彼此失去遠距離的風險，您應該考慮災難復原選項，以緩解影響 AWS 內整個區域的自然和技術災難。以下章節中所述的所有選項都可以實作為多區域架構，以防止此類災難。

雲端中的災難復原選項

您在 AWS 中可用的災難復原策略可以廣泛分為四種方法，從低成本和低複雜性的備份，到使用多個作用中區域更複雜的策略。主動/被動策略使用主動網站（例如 AWS 區域）來託管工作負載並提供流量。被動網站（例如不同的 AWS 區域）用於復原。在觸發容錯移轉事件之前，被動網站不會主動提供流量。

定期評估和測試災難復原策略至關重要，以便您可以放心地在必要時叫用災難復原策略。使用 [AWS Resilience Hub](#) 持續驗證和追蹤 AWS 工作負載的彈性，包括您是否可能符合 RTO 和 RPO 目標。

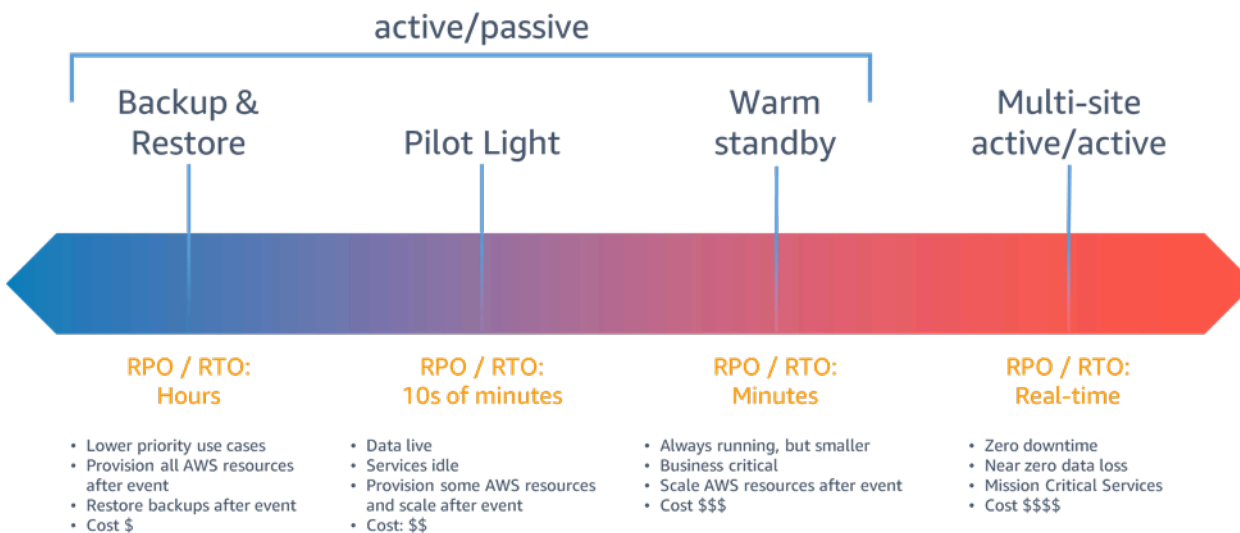


圖 6 - 災難復原策略

對於在**架構良好**、高可用性工作負載中中斷或遺失一個實體資料中心的災難事件，您可能只需要備份和還原方法來進行災難復原。如果您的災難定義超出了區域實體資料中心的中斷或遺失，或者如果您受到法規要求，則應考慮指示燈、暖待命或多站台主動/主動。

選擇您的策略以及實作策略的 AWS 資源時，請記住，在 AWS 中，我們通常會將服務劃分為資料平面和控制平面。資料平面負責提供即時服務，而控制平面則用於設定環境。為了達到最大的彈性，您應該僅使用資料平面操作做為容錯移轉操作的一部分。這是因為資料平面通常比控制平面具有更高的可用性設計目標。

備份和還原

備份和還原是緩解資料遺失或損毀的適當方法。此方法也可以透過將資料複寫到其他 AWS 區域來緩解區域災難，或減輕部署到單一可用區域的工作負載缺乏備援。除了資料之外，您還必須在復原區域中重

新部署基礎設施、組態和應用程式程式碼。若要快速重新部署基礎設施而不發生錯誤，您應該一律使用基礎設施做為程式碼 (IaC) 來部署，例如 [AWS CloudFormation](#) 或 [AWS Cloud Development Kit \(AWS CDK\)](#)。如果沒有 IaC，在復原區域中還原工作負載可能會很複雜，這將導致復原時間增加，並可能超過您的 RTO。除了使用者資料之外，也請務必備份程式碼和組態，包括您用來建立 [Amazon EC2 執行個體的 Amazon Machine Image \(AMIs\)](#)。Amazon EC2 您可以使用 [AWS CodePipeline](#) 自動重新部署應用程式程式碼和組態。

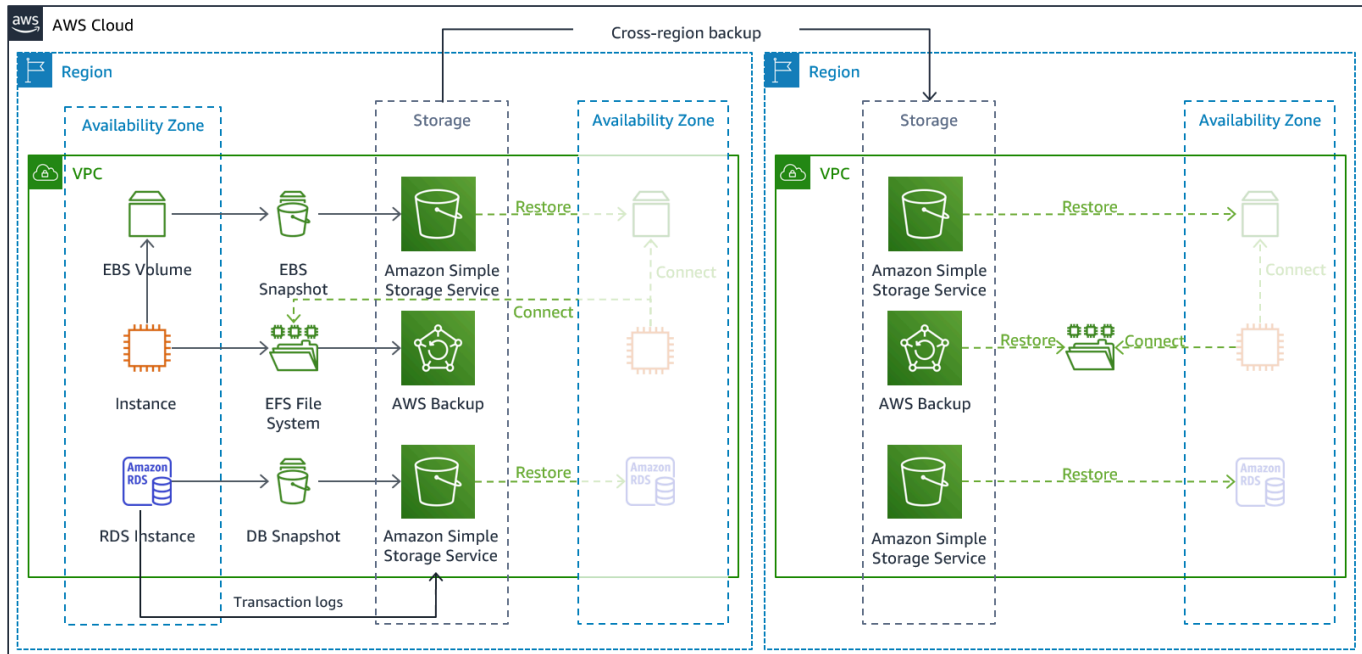


圖 7 - 備份和還原架構

AWS 服務

您的工作負載資料需要定期執行或持續執行的備份策略。執行備份的頻率將決定可實現的復原點（應符合您的 RPO）。備份也應該提供將其還原至擷取時間點的方法。具有 point-in-time 復原的備份可透過下列服務和資源取得：

- [Amazon Elastic Block Store \(Amazon EBS\) 快照](#)
- [Amazon DynamoDB 備份](#)
- [Amazon RDS 快照](#)
- [Amazon Aurora 資料庫快照](#)
- [Amazon EFS 備份](#)（使用時 AWS Backup）
- [Amazon Redshift 快照](#)

- [Amazon Neptune 快照](#)
- [Amazon DocumentDB](#)
- [Amazon FSx for Windows File Server](#)、[Amazon FSx for Lustre](#)、[Amazon FSx for NetApp ONTAP](#) 和 [Amazon FSx for OpenZFS](#)

對於 Amazon Simple Storage Service (Amazon S3)，您可以使用 [Amazon S3 跨區域複寫 \(CRR\)](#) 以非同步方式持續將物件複製到 DR 區域中的 S3 儲存貯體，同時為存放的物件提供版本控制，以便選擇還原點。持續複寫資料的優點是備份資料的最短時間（接近零），但可能無法防範災難事件，例如資料損毀或惡意攻擊（例如未經授權的資料刪除）以及 point-in-time 備份。持續複寫涵蓋在 [AWS Services for Pilot Light](#) 區段中。

[AWS Backup](#) 提供集中位置來設定、排程和監控下列服務和資源的 AWS 備份功能：

- [Amazon Elastic Block Store \(Amazon EBS\)](#) 磁碟區
- [Amazon EC2 執行個體](#)
- [Amazon Relational Database Service \(Amazon RDS\)](#) 資料庫（包括 [Amazon Aurora](#) 資料庫）
- [Amazon DynamoDB](#) 資料表
- [Amazon Elastic File System \(Amazon EFS\)](#) 檔案系統
- [AWS Storage Gateway](#) 磁碟區
- [Amazon FSx for Windows File Server](#)、[Amazon FSx for Lustre](#)、[Amazon FSx for NetApp ONTAP](#) 和 [Amazon FSx for OpenZFS](#)

AWS Backup 支援跨區域複製備份，例如至災難復原區域。

作為 Amazon S3 資料的額外災難復原策略，請啟用 [S3 物件版本控制](#)。物件版本控制可在動作之前保留原始版本，以保護 S3 中的資料免於刪除或修改動作的後果。物件版本控制可有效緩解人為錯誤類型的災難。如果您使用 S3 複寫將資料備份到 DR 區域，則根據預設，當來源儲存貯體中刪除物件時，[Amazon S3 只會在來源儲存貯體中新增刪除標記](#)。此方法可保護 DR 區域中的資料，避免來源區域中的惡意刪除。

除了資料之外，您還必須備份必要的組態和基礎設施，以重新部署工作負載並滿足復原時間目標 (RTO)。[AWS CloudFormation](#) 提供基礎設施即程式碼 (IaC)，並可讓您定義工作負載中的所有 AWS 資源，以便可靠地部署和重新部署到多個 AWS 帳戶和 AWS 區域。您可以將工作負載使用的 Amazon EC2 執行個體備份為 Amazon Machine Image (AMIs)。AMI 是從執行個體根磁碟區的快照，以及連接至執行個體的任何其他 EBS 磁碟區建立。您可以使用此 AMI 啟動 EC2 執行個體的還原版本。您可以

在區域內或跨區域複製 AMI。或者，您可以使用 [AWS Backup](#) 將備份跨帳戶複製到其他 AWS 區域。跨帳戶備份功能有助於防止災難事件，包括內部威脅或帳戶入侵。除了執行個體的個別 EBS 磁碟區之外，AWS Backup 還新增額外的 EC2 備份功能，AWS Backup 也會存放和追蹤下列中繼資料：執行個體類型、設定的虛擬私有雲端 (VPC)、安全群組、IAM 角色、監控組態和標籤。不過，只有在將 EC2 備份還原至相同的 AWS 區域時，才會使用此額外的中繼資料。

存放在災難復原區域中做為備份的任何資料都必須在容錯移轉時還原。AWS Backup 提供還原功能，但目前未啟用排程或自動還原。您可以使用 AWS 開發套件來呼叫 APIs，實作自動還原至 DR 區域 AWS Backup。您可以將此設定為定期重複任務，或在每次備份完成時觸發還原。下圖顯示使用 [Amazon Simple Notification Service \(Amazon SNS\)](#) 和自動還原的範例 [AWS Lambda](#)。實作排定的定期資料還原是個好主意，因為從備份還原的資料是控制平面操作。如果此操作在災難期間無法使用，您仍然可以從最近的備份建立可操作的資料存放區。

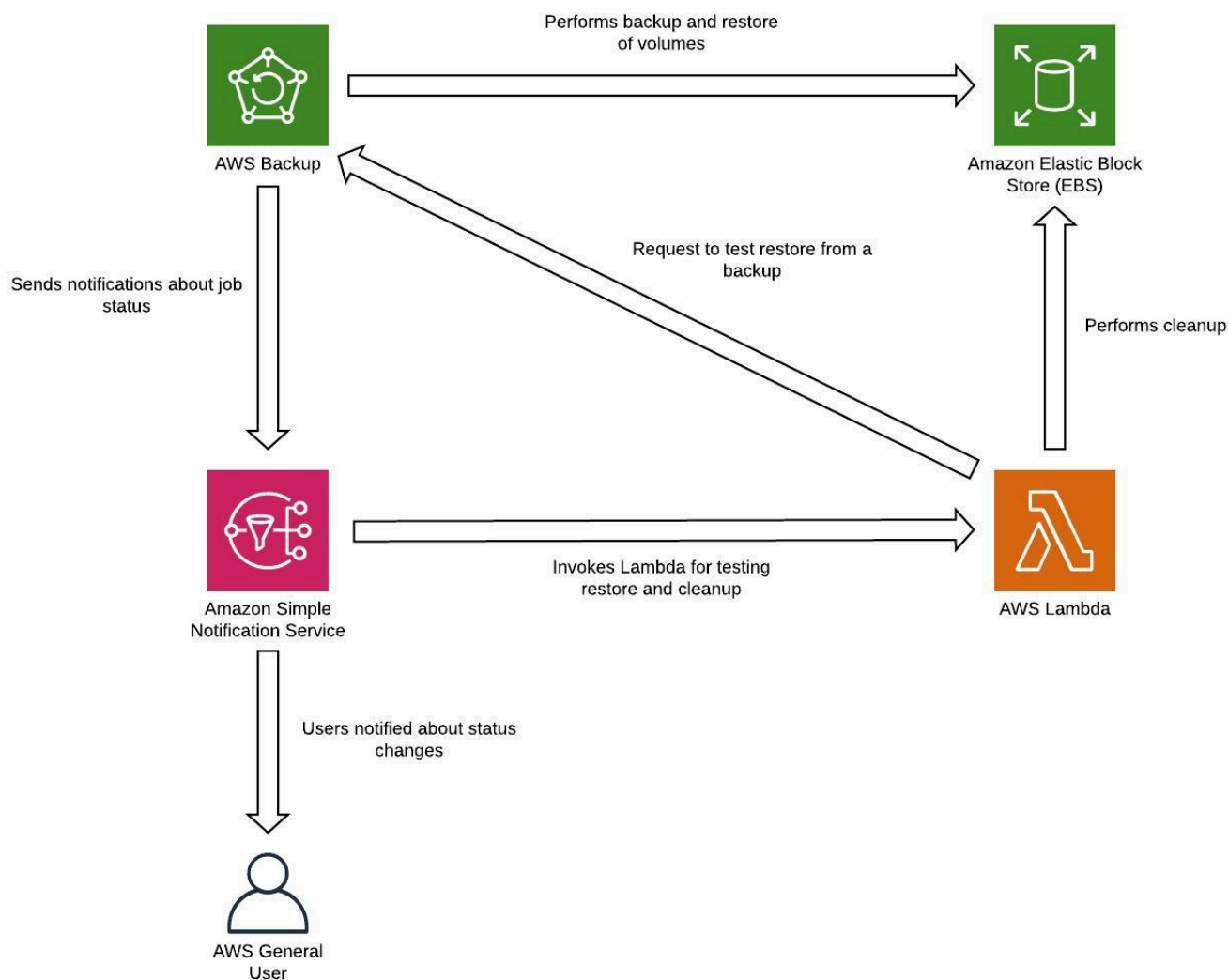


圖 8 - 還原和測試備份

Note

備份策略必須包括測試備份。如需詳細資訊，請參閱[測試災難復原](#)一節。請參閱 [AWS Well-Architected Lab：測試資料的備份和還原](#)，以實際示範實作。

指示燈

使用指示燈方法，您可以將資料從一個區域複製到另一個區域，並佈建核心工作負載基礎設施的副本。支援資料複製和備份所需的資源 (例如資料庫和物件儲存) 始終處於開啟狀態。其他元素，例如應用程式伺服器，會載入應用程式碼和組態，但「關閉」並只在測試期間或調用災難復原容錯移轉時使用。在雲端中，您可以在不需要資源時彈性取消佈建資源，並在執行時佈建資源。「關閉」的最佳實務是不部署資源，然後視需要建立組態和功能來部署資源 (「開啟」)。與備份和還原方法不同，您的核心基礎設施一律可用，而且您隨時可以選擇透過開啟和擴展應用程式伺服器來快速佈建完整規模的生產環境。

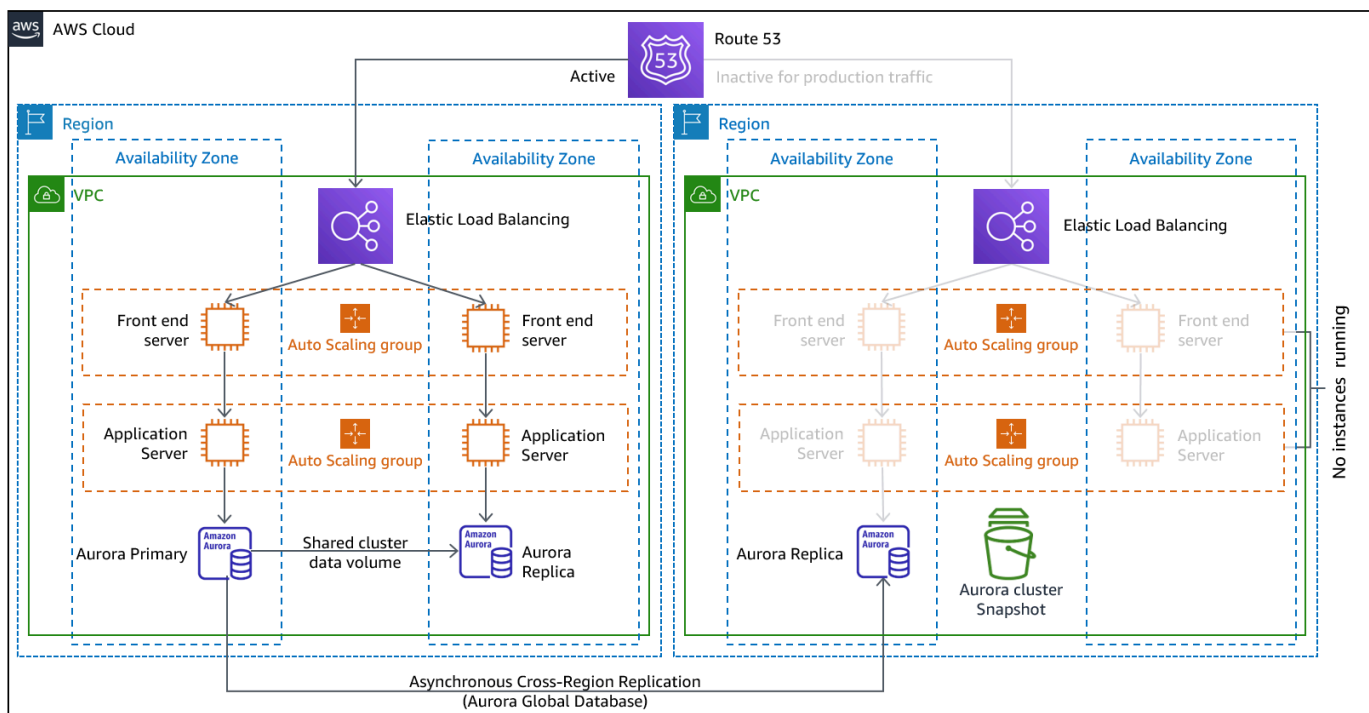


圖 9 - 指示燈架構

指示燈方法透過將作用中資源降至最低，將災難復原的持續成本降至最低，並在災難發生時簡化復原，因為核心基礎設施要求都已就緒。此復原選項會要求您變更部署方法。您需要對每個區域進行核心基礎設施變更，並將工作負載 (組態、程式碼) 變更同時部署到每個區域。您可以透過自動化部署並使用基礎設施做為程式碼 (IaC) 跨多個帳戶和區域部署基礎設施 (完整基礎設施部署至主要區域，以及縮

減/關閉基礎設施部署至 DR 區域)，來簡化此步驟。建議您在每個區域使用不同的帳戶，以提供最高層級的資源和安全隔離（如果遭入侵的登入資料也是您災難復原計畫的一部分）。

使用此方法，您還必須緩解資料災難。持續資料複寫可以保護您防範某些類型的災難，但它不能保護您防範資料損毀或破壞，除非您的策略也包括所存放資料的版本控制，或時間點復原的選項。您可以在災難區域中備份複寫的資料，以在相同區域中建立point-in-time備份。

AWS 服務

除了使用[備份和還原](#)區段中涵蓋的 AWS 服務來建立point-in-time備份之外，也請為您的指示燈策略考慮下列服務。

對於指示燈，持續資料複寫到 DR 區域中的即時資料庫和資料存放區是低 RPO 的最佳方法（除了先前討論point-in-time備份之外使用時）。AWS 使用下列服務和資源，為資料提供持續、跨區域、非同步的資料複寫：

- [Amazon Simple Storage Service \(Amazon S3\) 複寫](#)
- [Amazon RDS 僅供讀取複本](#)
- [Amazon Aurora 全域資料庫](#)
- [Amazon DynamoDB 全域資料表](#)
- [Amazon DocumentDB 全域叢集](#)
- [Amazon ElastiCache \(Redis OSS\) 的全域資料存放區](#)

透過持續複寫，資料版本幾乎可在您的 DR 區域中立即使用。您可以使用 [S3 物件的 S3 複寫時間控制 \(S3 RTC\)](#) S3和 [Amazon Aurora 全域資料庫的管理功能](#)等服務功能來監控實際的複寫時間。

當容錯移轉從災難復原區域執行讀取/寫入工作負載時，您必須提升 RDS 僅供讀取複本，才能成為主要執行個體。對於 [Aurora 以外的資料庫執行個體](#)，[程序](#)需要幾分鐘才能完成，重新啟動是程序的一部分。對於使用 RDS 的跨區域複寫 (CRR) 和容錯移轉，使用 [Amazon Aurora 全域資料庫](#)提供數種優點。全球資料庫使用專用基礎設施，讓您的資料庫完全可供您的應用程式使用，並且可以複寫到一般延遲低於一秒的次要區域 (AWS 區域內的延遲遠低於 100 毫秒)。使用 Amazon Aurora 全域資料庫，如果您的主要區域發生效能降低或中斷，即使發生完整的區域中斷，您也可以提升其中一個次要區域在不到一分鐘內承擔讀取/寫入責任。您也可以設定 Aurora 來監控所有次要叢集的 RPO 延遲時間，以確保至少一個次要叢集保持在目標 RPO 時段內。

具有較少或較小資源的核心工作負載基礎設施的縮減版本，必須部署在您的 DR 區域中。使用 AWS CloudFormation，您可以定義基礎設施，並在 AWS 帳戶和 AWS 區域之間一致地部署。AWS

CloudFormation 使用預先定義的[虛擬參數](#)來識別部署的 AWS 帳戶和 AWS 區域。因此，您可以在 [CloudFormation 範本中實作條件邏輯](#)，以在 DR 區域中僅部署基礎設施的縮減規模版本。對於 EC2 執行個體部署，Amazon Machine Image (AMI) 會提供硬體組態和安裝的軟體等資訊。您可以實作[映像建置器](#)管道，建立您需要 AMIs，並將其複製到主要和備份區域。這有助於確保這些黃金 AMIs 擁有在發生災難事件時，在新區域中重新部署或擴展工作負載所需的一切。Amazon EC2 執行個體會部署在縮減規模的組態中（相較於主要區域，執行個體較少）。若要橫向擴展基礎設施以支援生產流量，請參閱「[暖待命](#)」一節中的 [Amazon EC2 Auto Scaling](#)。

對於主動/被動組態，例如指示燈，所有流量最初都會進入主要區域，並在主要區域不再可用時切換到災難復原區域。此容錯移轉作業可以自動或手動啟動。根據運作狀態檢查或警示自動啟動容錯移轉時，應謹慎使用。即使使用此處討論的最佳實務，復原時間和復原點也會大於零，並導致可用性和資料的某些損失。如果您在不需要（錯誤警示）時容錯移轉，則會發生這些損失。因此通常使用手動啟動的容錯移轉。在此情況下，您仍應將容錯移轉的步驟自動化，讓手動啟動就像按下按鈕一樣簡易。

使用 AWS 服務時，有幾個流量管理選項需要考慮。

一種選擇是使用 [Amazon Route 53](#)。使用 Amazon Route 53，您可以將一或多個 AWS 區域中的多個 IP 端點與 Route 53 網域名稱建立關聯。然後，您可以將流量路由到該網域名稱下的適當端點。在容錯移轉時，您需要將流量切換到復原端點，並遠離主要端點。Amazon Route 53 運作狀態檢查會監控這些端點。使用這些運作狀態檢查，您可以設定自動啟動的 DNS 容錯移轉，以確保流量只會傳送到運作狀態良好的端點，這是在資料平面上進行的高度可靠操作。若要使用手動啟動的容錯移轉實作此項目，您可以使用 [Amazon Application Recovery Controller \(ARC\)](#)。使用 ARC，您可以建立 Route 53 運作狀態檢查，不實際檢查運作狀態，而是做為您可以完全控制的開啟/關閉開關。您可以使用 AWS CLI 或 AWS 開發套件，使用此高可用性的資料平面 API 來編寫容錯移轉指令碼。您的指令碼會切換這些切換 (Route 53 運作狀態檢查)，告知 Route 53 將流量傳送至復原區域，而非主要區域。手動啟動容錯移轉的另一個選項是使用加權路由政策，並變更主要和復原區域的權重，以便所有流量流向復原區域。不過請注意，這是控制平面操作，因此不像使用 Amazon Application Recovery Controller (ARC) 的資料平面方法那樣有彈性。

另一個選項是使用 [AWS Global Accelerator](#)。使用 AnyCast IP，您可以將一或多個 AWS 區域中的多個端點與相同的靜態公有 IP 地址建立關聯。AWS Global Accelerator 然後，會將流量路由到與該地址相關聯的適當端點。[Global Accelerator 運作狀態檢查](#)會監控端點。使用這些運作狀態檢查，會 AWS Global Accelerator 檢查應用程式的運作狀態，並將使用者流量自動路由至運作狀態良好的應用程式端點。對於手動啟動的容錯移轉，您可以調整哪個端點使用流量撥號接收流量，但請注意這是控制平面操作。Global Accelerator 可降低應用程式端點的延遲，因為它利用廣泛的 AWS 邊緣網路，盡快將流量放置在 AWS 網路骨幹上。Global Accelerator 也可避免 DNS 系統（例如 Route 53）可能發生的快取問題。

[Amazon CloudFront](#) 提供原始伺服器容錯移轉，如果對主要端點的指定請求失敗，CloudFront 會將請求路由至次要端點。與之前描述的容錯移轉操作不同，所有後續請求仍然會移至主要端點，而且每個請求都會進行容錯移轉。

AWS 彈性災難復原

[AWS Elastic Disaster Recovery \(DRS\)](#) AWS 會使用基礎伺服器的區塊層級複寫，持續將伺服器託管的應用程式和伺服器託管資料庫從任何來源複寫至。Elastic Disaster Recovery 可讓您使用中的區域 AWS 雲端作為內部部署或另一個雲端提供者及其環境上託管的工作負載的災難復原目標。如果 AWS 託管工作負載僅包含 EC2 上託管的應用程式和資料庫（即不是 RDS），則它也可以用於託管工作負載的災難復原。Elastic Disaster Recovery 使用指示燈策略，在用作預備區域的 [Amazon Virtual Private Cloud \(Amazon VPC\)](#) 中維護資料副本和「關閉」資源。觸發容錯移轉事件時，暫存資源會用來自動在做為復原位置的目標 Amazon VPC 中建立完整容量部署。

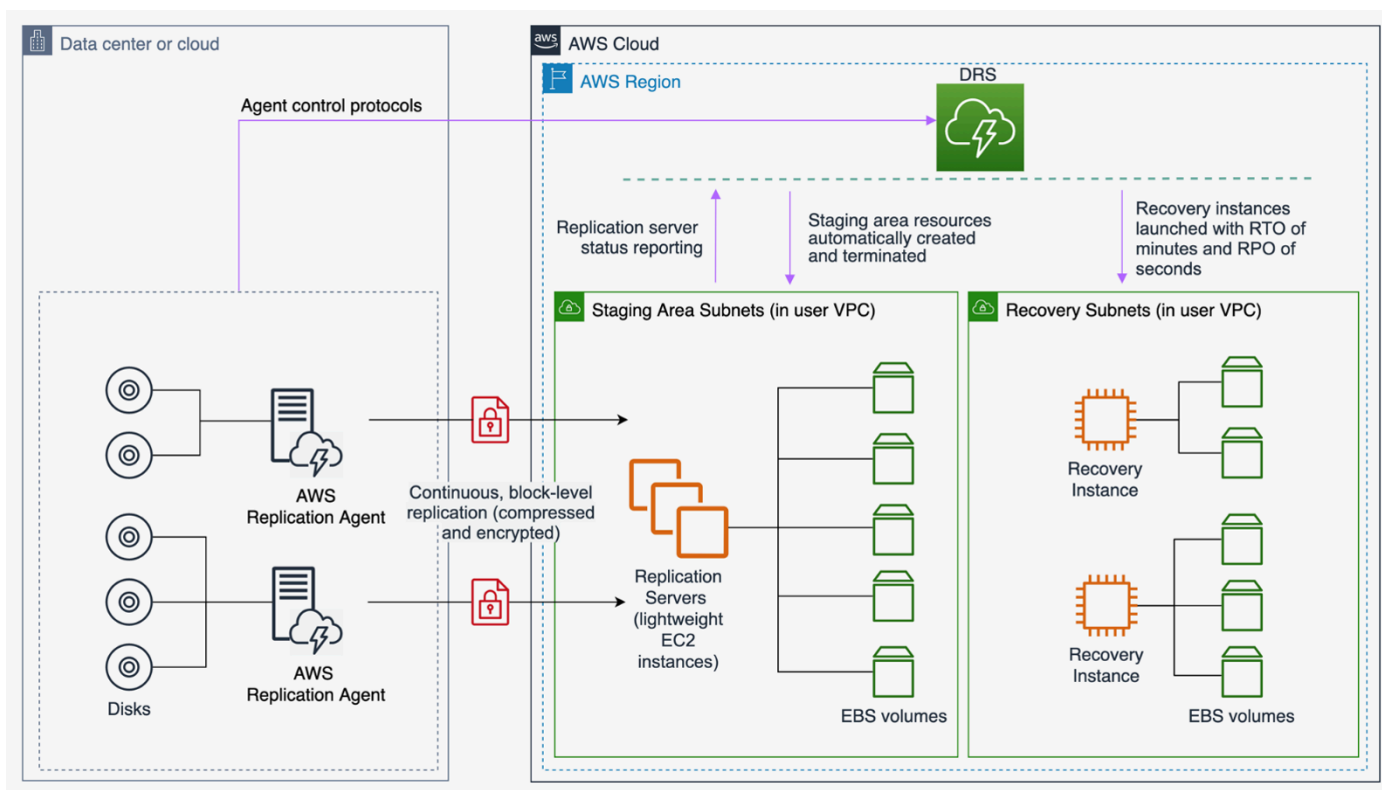


圖 10 - AWS 彈性災難復原架構

暖待命

暖待命方法包括確保在另一個區域中有規模縮減但功能完整的生產環境副本。這種方法擴充了指示燈概念並減少了復原時間，因為您的工作負載始終在另一個區域中開啟。此方法也可讓您更輕鬆地執行測試或實作持續測試，以提高您對從災難復原能力的信心。

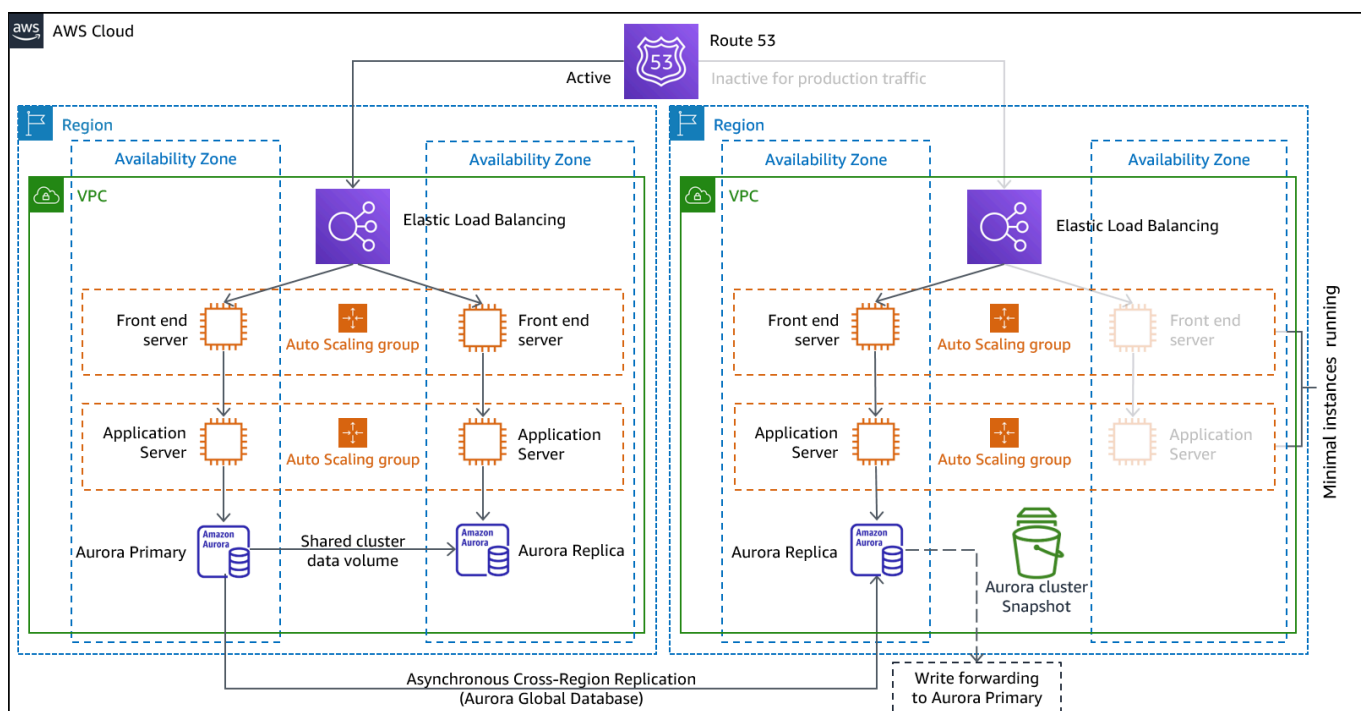


圖 11 - 暖待命架構

注意：[指示燈](#)和[暖待命](#)之間的差異有時很難理解。兩者都包含 DR 區域中的環境，其中包含主要區域資產的副本。差別在於，指示燈無法在未先採取其他動作的情況下處理請求，而暖待命可以立即處理流量（容量降低）。指示燈方法需要您「開啟」伺服器，可能部署其他（非核心）基礎設施並向上擴展，而暖待命只需要您向上擴展（所有項目都已部署並執行）。使用您的 RTO 和 RPO 需求，協助您選擇這些方法。

AWS 服務

[備份和還原](#)和[指示燈](#)涵蓋的所有 AWS 服務也會在暖待命中用於資料備份、資料複寫、主動/被動流量路由，以及部署基礎設施，包括 EC2 執行個體。

[Amazon EC2 Auto Scaling](#) 用於擴展 AWS 區域內的資源，包括 Amazon EC2 執行個體、Amazon ECS 任務、Amazon DynamoDB 輸送量和 Amazon Aurora 複本。[Amazon EC2 Auto Scaling](#) 會在 AWS 區域內跨可用區域擴展 EC2 執行個體的部署，在該區域內提供彈性。使用 Auto Scaling 將 DR 區域擴展為完整的生產功能，作為指示燈或暖待命策略的一部分。例如，對於 EC2，增加 Auto Scaling 群組上所需的容量設定。您可以透過 手動調整此設定 AWS 管理主控台、透過 AWS 開發套件自動調整，或使用新的所需容量值重新部署 AWS CloudFormation 範本。您可以使用 AWS CloudFormation 參數，讓重新部署 CloudFormation 範本變得更容易。請確定 DR [區域中的服務配額](#)設定夠高，以免限制您擴展到生產容量。

由於 Auto Scaling 是一種控制平面活動，因此對它採取相依性將降低整體復原策略的彈性。這是權衡。您可以選擇佈建足夠的容量，讓復原區域可以處理部署的完整生產負載。此靜態穩定組態稱為熱待命（請參閱下一節）。或者，您可以選擇佈建較少的資源，其成本較低，但依賴 Auto Scaling。有些 DR 實作會部署足夠的資源來處理初始流量、確保低 RTO，然後依賴 Auto Scaling 來提升後續流量。

多站點主動/主動

您可以在多個區域中同時執行工作負載，做為多站台主動/主動或熱待命主動/被動策略的一部分。多站台作用中/作用中（多站台作用中/作用中）會為部署區域的所有流量提供服務，而熱待命只會為來自單一區域的流量提供服務，而其他區域則只會用於災難復原。透過多站台主動/主動方法，使用者可以在部署工作負載的任何區域中存取工作負載。這種方法是最複雜且成本最高的災難復原方法，但對於具有正確技術選擇和實作的大多數災難，它可以將復原時間縮短到接近零（但是資料損毀可能需要依賴備份，這通常會導致非零的復原點）。熱待命使用主動/被動組態，其中只會將使用者導向單一區域，且 DR 區域不會接收流量。大多數客戶發現，如果他們要在第二個區域中站立一個完整的環境，則使用它是有意義的/有作用的。或者，如果您不想使用這兩個區域來處理使用者流量，則熱待命會提供更經濟且操作較不複雜的方法。

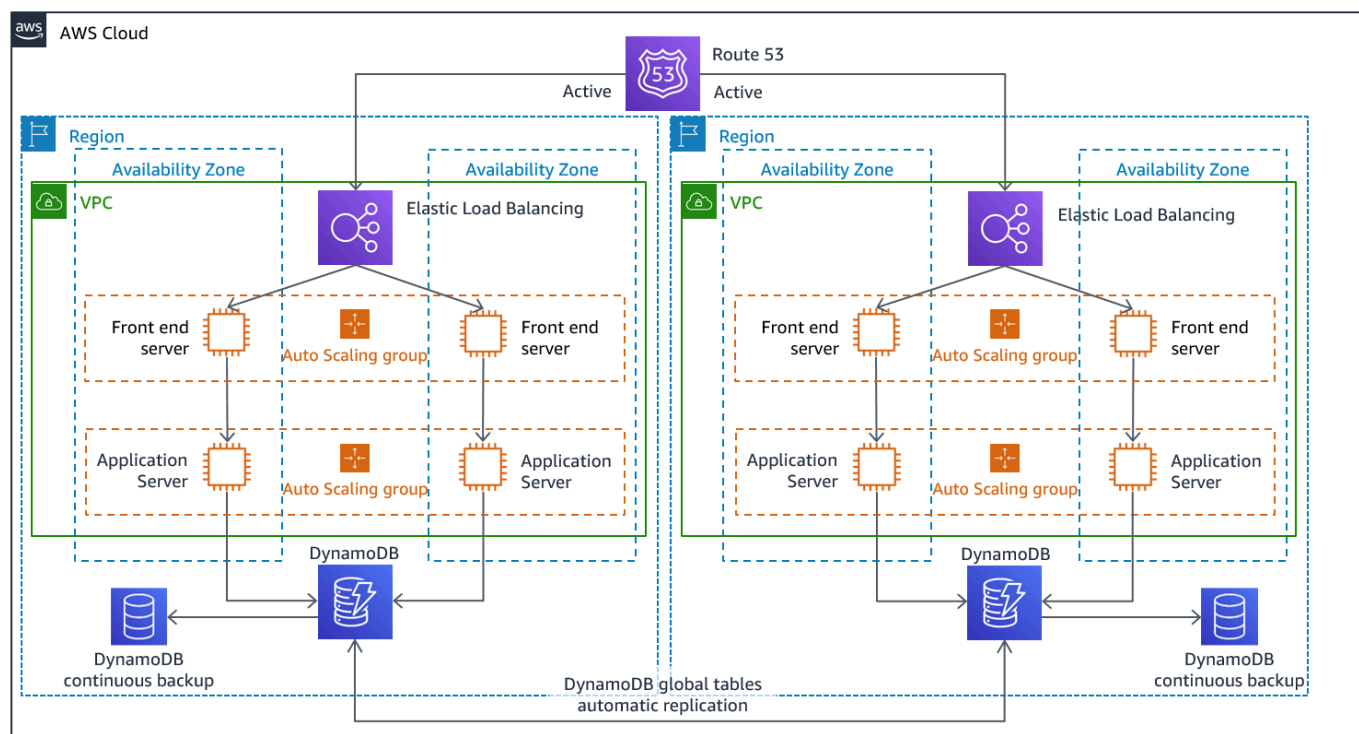


圖 12 - 多站台主動/主動架構（將一個作用中路徑變更為非作用中以進行熱待命）

使用多站台作用中/作用中時，由於工作負載正在多個區域中執行，因此在此案例中沒有容錯移轉等情況。在此情況下，災難復原測試會著重於工作負載對區域遺失的反應：流量是否從故障的區域路由出？

其他（區域）是否可以處理所有流量？也需要測試資料災難。備份和復原仍然是必要的，應該定期測試。也應注意，涉及資料損毀、刪除或混淆的資料災難復原時間一律大於零，且復原點一律會在發現災難之前的某個時間點。如果需要多站台主動/主動（或熱待命）方法的額外複雜性和成本，以維持接近零的復原時間，則應採取額外的努力來維護安全性並防止人為錯誤，以減輕人為災難。

AWS 服務

此處也使用[備份和還原](#)、[指示燈](#)和[暖待命](#)涵蓋的所有 AWS 服務，進行point-in-time資料備份、資料複寫、主動/主動流量路由，以及部署和擴展基礎設施，包括 EC2 執行個體。

對於先前討論的主動/被動案例（指示燈和暖待命），Amazon Route 53 和 AWS Global Accelerator 都可以用於將網路流量路由到作用中區域。對於此處的主動/主動策略，這兩個服務也啟用政策的定義，以決定哪些使用者前往哪個作用中區域端點。AWS Global Accelerator 使用 [設定流量撥號以控制導向每個應用程式端點的流量百分比](#)。Amazon Route 53 支援此百分比方法，以及[多個其他可用的政策](#)，包括地理位置鄰近性和以延遲為基礎的政策。[Global Accelerator 會自動利用 AWS 邊緣伺服器的廣泛網路](#)，盡快將流量加入 AWS 網路骨幹，進而降低請求延遲。

使用此策略的非同步資料複寫可啟用近乎零的 RPO。[Amazon Aurora 全域資料庫](#)等 AWS 服務使用專用基礎設施，讓您的資料庫完全可供您的應用程式使用，並可複寫至最多五個次要區域，一般延遲不到一秒。使用主動/被動策略時，寫入只會發生在主要區域。主動/主動的差異在於設計如何處理與寫入每個主動區域的資料一致性。通常會設計要從最接近使用者的區域提供的使用者讀取，稱為本機讀取。透過寫入，您有幾個選項：

- 寫入全域策略會將所有寫入路由至單一區域。如果該區域發生故障，則會提升另一個區域以接受寫入。[Aurora 全域資料庫](#)非常適合全域寫入，因為它支援跨區域與僅供讀取複本同步處理，而且您可以在一分鐘內提升其中一個次要區域承擔讀取/寫入責任。Aurora 也支援寫入轉送，可讓 Aurora 全域資料庫中的次要叢集將執行寫入操作的 SQL 陳述式轉送至主要叢集。
- 寫入本機策略路由寫入最接近的區域（如同讀取）。[Amazon DynamoDB 全域資料表](#)可啟用此類策略，允許從部署全域資料表的每個區域進行讀取和寫入。Amazon DynamoDB 全域資料表使用最後一個寫入器，可在並行更新之間取得對帳。
- 寫入分割策略會根據分割區索引鍵（例如使用者 ID）將寫入指派給特定區域，以避免寫入衝突。雙向[設定的](#) Amazon S3 複寫可用於此案例，目前支援兩個區域之間的複寫。實作此方法時，請務必在儲存貯體 A 和 B 上啟用[複本修改同步](#)，以在複寫物件上複寫複本中繼資料變更，例如物件存取控制清單 (ACLs)、物件標籤或物件鎖定。您也可以設定是否要在作用中區域中的儲存貯體之間[複寫刪除標記](#)。除了複寫之外，您的策略還必須包含point-in-time備份，以防止資料損毀或損毀事件。

AWS CloudFormation 是一種強大的工具，可在多個 AWS 區域中的 AWS 帳戶之間強制執行持續部署的基礎設施。[AWS CloudFormation StackSets](#) 可讓您透過單一操作，跨多個帳戶和區域建立、更新或

刪除 CloudFormation 堆疊，藉此擴充此功能。雖然 AWS CloudFormation 使用 YAML 或 JSON 將基礎設施定義為程式碼，但 [AWS Cloud Development Kit \(AWS CDK\)](#) 可讓您使用熟悉的程式設計語言將基礎設施定義為程式碼。您的程式碼會轉換為 CloudFormation，然後用於在 AWS 中部署資源。

偵測

請務必盡快知道您的工作負載未提供應交付的業務成果。透過這種方式，您可以快速宣告災難並從事件中復原。對於積極的復原目標，此回應時間結合適當的資訊對於實現復原目標至關重要。如果您的復原時間目標是一小時，則您需要偵測事件、通知適當的人員、參與呈報程序、評估預期的復原時間資訊（如果有的話）（不執行 DR 計畫）、宣告災難並在一小時內復原。

Note

如果利益相關者決定不叫用 DR，即使 RTO 存在風險，則重新評估 DR 計劃和目標。不調用 DR 計劃的決定可能是因為計劃不足或對執行缺乏信心。

將事件偵測、通知、呈報、探索和宣告納入您的規劃和目標中至關重要，以提供提供商業價值的實際、可實現的目標。

AWS 會在服務[運作狀態儀表板](#)上發佈有關服務可用性 up-to-the-minute。隨時檢查以取得目前的狀態資訊，或訂閱 RSS 摘要，以便在每個個別服務中斷時收到通知。如果您遇到我們其中一個服務未顯示在服務運作狀態儀表板上的即時操作問題，您可以建立[支援請求](#)。

[AWS Health 儀表板](#) 提供有關可能影響您的帳戶 AWS Health 之事件的資訊。資訊以兩種方式呈現：儀表板（依類別顯示最近和近期事件）和完整的事件日誌（顯示過去 90 天內的所有事件）。

如需最嚴格的 RTO 需求，您可以根據[運作狀態檢查實作自動容錯移轉](#)。根據關鍵效能指標，設計代表使用者體驗的運作狀態檢查。深度運作狀態檢查會執行工作負載的關鍵功能，並超越淺活動訊號檢查。根據多個訊號使用深層運作狀態檢查。使用此方法時請小心，以免觸發錯誤警示，因為在本身不需要時容錯移轉會帶來可用性風險。

測試災難復原

測試災難復原實作以驗證實作，並定期測試容錯移轉至工作負載的 DR 區域，以確保符合 RTO 和 RPO。

要避免的模式是開發很少執行的復原路徑。例如，您可能有一個次要資料存放區，只供唯讀查詢之用。當您寫入資料存放區而主資料存放區發生故障時，您可能需要容錯移轉到次要資料存放區。如果您不經常測試此容錯移轉，則可能會發現您對次要資料存放區的功能的假設不正確。您上次測試時可能已經足夠之次要的容量，在此案例中可能不再能容忍負載，或次要區域中的服務配額可能不夠。

我們的經驗顯示，唯一能發揮功用的錯誤復原，是您經常測試的路徑。這就是為什麼擁有少量復原路徑是最好的原因。

您可建立復原模式，並定期進行測試。如果您有複雜或關鍵的復原路徑，您仍然需要在生產環境中定期執行該失敗，以驗證復原路徑是否正常運作。

在 DR 區域管理組態偏離。請確定您的基礎設施、資料和組態是 DR 區域中需要的。例如，檢查 AMIs 和服務配額是否為 up-to-date。

您可以使用 [AWS Config](#) 持續監控和記錄您的 AWS 資源組態。AWS Config 可以偵測偏離，並觸發 [AWS Systems Manager Automation](#) 修正偏離和引發警示。[AWS CloudFormation](#) 還可以偵測已部署堆疊中的偏離。

結論

客戶負責確保其應用程式在雲端中的可用性。務必定義什麼是災難，並制定災難復原計劃來反映此定義及其可能對業務成果造成的影響。根據影響分析和風險評估建立復原時間目標 (RTO) 和復原點目標 (RPO)，然後選擇適當的架構來緩解災難。確保偵測災難是可行且及時的，了解目標何時處於風險中至關重要。確保您擁有計劃，並透過測試驗證計劃。尚未驗證的災難復原計劃，因為缺乏信心或無法滿足災難復原目標而未實作的風險。

貢獻者

本文件的貢獻者包括：

- Alex Livingstone , AWS Enterprise Support 雲端營運實務主管
- Seth Eliot , Amazon Web Services 首席可靠性解決方案架構師

深入閱讀

如需其他資訊，請參閱：

- [AWS 架構中心](#)
- [可靠性支柱，AWS Well-Architected Framework](#)
- [災難復原計畫檢查清單](#)
- [實作運作狀態檢查](#)
- [AWS 上的災難復原 \(DR\) 架構，第 I 部分：雲端中的復原策略](#)
- [AWS 上的災難復原 \(DR\) 架構，第 II 部分：使用快速復原進行備份和還原](#)
- [AWS 上的災難復原 \(DR\) 架構，第 III 部分：指示燈和暖待命](#)
- [AWS 上的災難復原 \(DR\) 架構，第 IV 部分：多站台主動/主動](#)
- [使用 Amazon Route 53 建立災難復原機制](#)
- [在災難復原計畫中盡可能減少相依關係](#)
- [AWS Well-Architected 災難復原實驗室的手](#)
- [AWS 解決方案實作：多區域應用程式架構](#)
- [AWS re：Invent 2018：多區域主動-主動應用程式的架構模式 \(ARC209-R2\)](#)

文件歷史記錄

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
次要更新	錯誤修正和許多小變更。	2022 年 4 月 1 日
白皮書已更新	次要編輯更新。	2022 年 3 月 21 日
白皮書已更新	新增資料平面和控制平面的相關資訊。新增如何實作主動/被動容錯移轉的詳細資訊。將 CloudEndure 災難復原取代為 AWS 彈性災難復原。	2022 年 2 月 17 日
次要更新	AWS Well-Architected Tool 已新增 資訊。	2022 年 2 月 11 日
初次出版	白皮書首次發佈。	2021 年 2 月 12 日

注意

客戶有責任對本文件中的資訊進行自己的獨立評定。本文件：(a) 僅供參考，(b) 代表目前的 AWS 產品和實務，如有變更，恕不另行通知，且 (c) 不會從 AWS 及其附屬公司、供應商或授權方建立任何承諾或保證。AWS 產品或服務以「原樣」提供，不做任何明示或暗示的保證、表示或條件。AWS 對其客戶的責任與義務應由 AWS 協議管轄，本文並非 AWS 與其客戶之間的任何協議的一部分，也並非上述協議的修改。

© 2022 Amazon Web Services, Inc. 或其附屬公司。保留所有權利。

AWS 詞彙表

如需最新的 AWS 術語，請參閱 AWS 詞彙表 參考中的[AWS 詞彙表](#)。

本文為英文版的機器翻譯版本，如內容有任何歧義或不一致之處，概以英文版為準。