AWS 白皮書

AWS 上的工作負載災難復原：雲端中的復原

AWS 上的工作負載災難復原：雲端中的復原: AWS 白皮書

Table of Contents

AWS 上的工作負載災難復原：雲端中的復原

出版日期：2021 年 2 月 12 日 (文件修訂)

摘要

災難復原是為災難做好準備並從災難中復原的過程。會防止工作負載或系統在其主要部署位置實現業務目標的事件，就被視為災難。本白皮書概述用於針對任何部署至 AWS 的工作負載規劃和測試災難復原的最佳實務，並提供不同的方法減輕風險，並滿足該工作負載的復原時間點目標 (RTO) 和復原點目標 (RPO)。

簡介

您的工作負載必須正確且一致地執行其預期功能。若想達成這個目標，您必須針對彈性進行設計。彈性是工作負載在以下方面的能力：從基礎設施或服務中斷恢復、動態取得運算資源以符合需求，以及緩解中斷狀況 (例如，設定錯誤或暫時性網路問題)。

災難復原 (DR) 是復原策略的重要組成部分，它涉及到災難發生時工作負載如何回應 (災難是指會對您的業務造成嚴重負面影響的事件)。此回應必須根據組織的業務目標，該目標指定了避免資料遺失的工作負載策略 (稱為復原點目標 (RPO))，並在工作負載無法使用的情況下減少停機時間 (稱為復原時間點目標 (RTO))。因此，您必須在設計雲端中的工作負載時實施恢復能力，以滿足特定單次災難事件的復原目標 (RPO 和 RTO)。此方法可協助您的組織根據業務持續性規劃 (BCP) 來維護業務持續性。

本白皮書重點介紹如何在 AWS 上規劃、設計和實施架構，以滿足您業務的災難復原目標。此處分享的資訊是供首席技術長 (CTO)、架構師、開發人員和營運團隊成員這類技術角色使用。

災難復原和可用性

災難復原可與可用性進行比較，可用性是復原策略的另一個重要組成部分。災難復原衡量的是單次事件的目標，而可用性目標則衡量一段時間內的值。

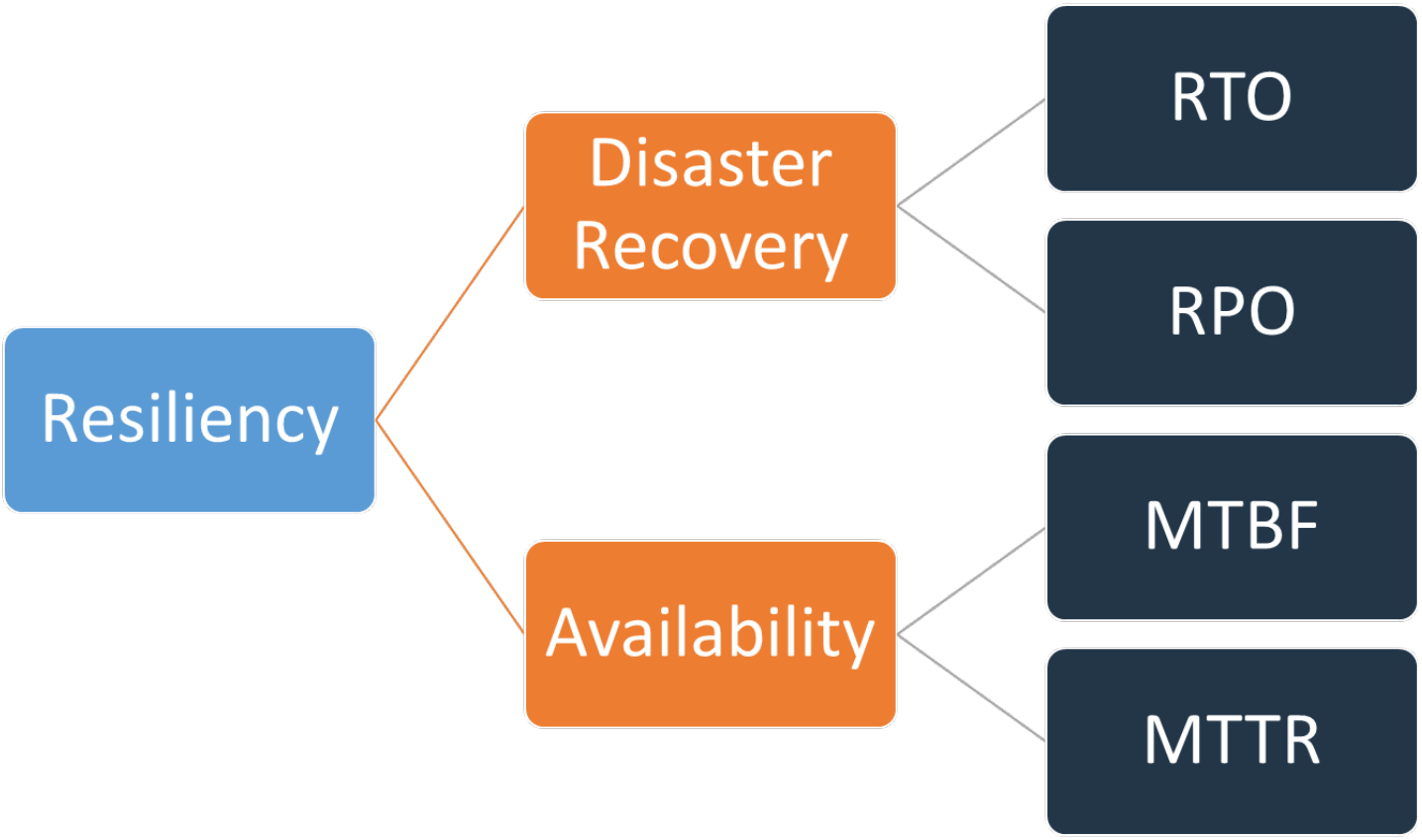

圖 1 - 彈性目標

可用性是使用平均故障間隔 (MTBF) 和平均復原時間 (MTTR) 來計算：

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

此方法通常被稱為「九」，其中 99.9% 的可用性目標稱為「三個九」。

對於您的工作負載，與其使用時間型方法，計算成功和失敗的請求可能更為容易。在這種情況下，可以使用以下計算式：

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

災難復原側重於災難事件，而可用性側重於較小規模的較常見中斷，如元件故障、網路問題和負載高峰。災難復原的目標是業務連續性，而可用性則是將工作負載可用於執行其預期業務功能的時間發揮至最大。兩者都應納入您的彈性策略。

彈性的共同責任模型

彈性是 AWS 和您 (客戶) 之間的共同責任。請務必了解災難復原和可用性作為彈性的一部分，如何在此共同責任模式下運作。

AWS 責任「雲端本身的彈性」

AWS 負責維護基礎設施的彈性，以便執行 AWS 雲端提供的所有服務。此基礎設施包含執行 AWS 雲端服務的硬體、軟體、聯網以及設施。AWS 會採取商業上合理的努力來讓這些 AWS 雲端服務可供使用，以確保服務可用性符合或超過 AWS 服務水準協議 (SLA)。

AWS 全球雲端基礎設施旨在協助客戶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，這些區域是基礎設施的實體隔離分區。可用區域會隔離可能影響工作負載彈性的故障，防止故障影響該區域的其他區域。但同時，AWS 區域中的所有可用區域都透過高頻寬、低延遲的聯網，與完全冗餘的專用都會光纖互連，在可用區域之間提供高輸送量、低延遲的聯網。區域之間的所有流量都將會加密。網路效能足以實現區域之間的同步複寫。可用區域簡化了對應用程式進行分區以實現高可用性的過程。

客戶責任「雲端中的彈性」

您的責任將由您選擇的 AWS 雲端服務決定。這決定了在履行彈性責任的過程中，您必須執行的組態工作量。例如，Amazon Elastic Compute Cloud (Amazon EC2) 等服務需要客戶執行所有必要的安全組態和管理任務。部署 Amazon EC2 執行個體的客戶需負責跨多個位置部署 EC2 執行個體 (如 AWS 可用區域)、使用 AWS Auto Scaling 等服務實施自我修復，以及針對執行個體上安裝的應用程式使用彈性的工作負載架構最佳實務。若是 Amazon S3 和 Amazon DynamoDB 等受管服務，AWS 運作基礎設施層、作業系統和平台，客戶則存取端點以儲存及擷取資料。您負責管理資料的彈性，包括備份、版本控制和複寫策略。

跨 AWS 區域的多個可用區域部署您的工作負載屬於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繼續處理請求。多可用區域架構也是 DR 策略的一部分，旨在將工作負載更好地隔離並保護其免受停電、雷擊、龍捲風、地震等問題的影響。DR 策略也可以利用多個 AWS 區域。例如，在主動/被動組態中，如果活動區域無法再為請求提供服務，則工作負載服務將從其活動區域容錯移轉到其 DR 區域。

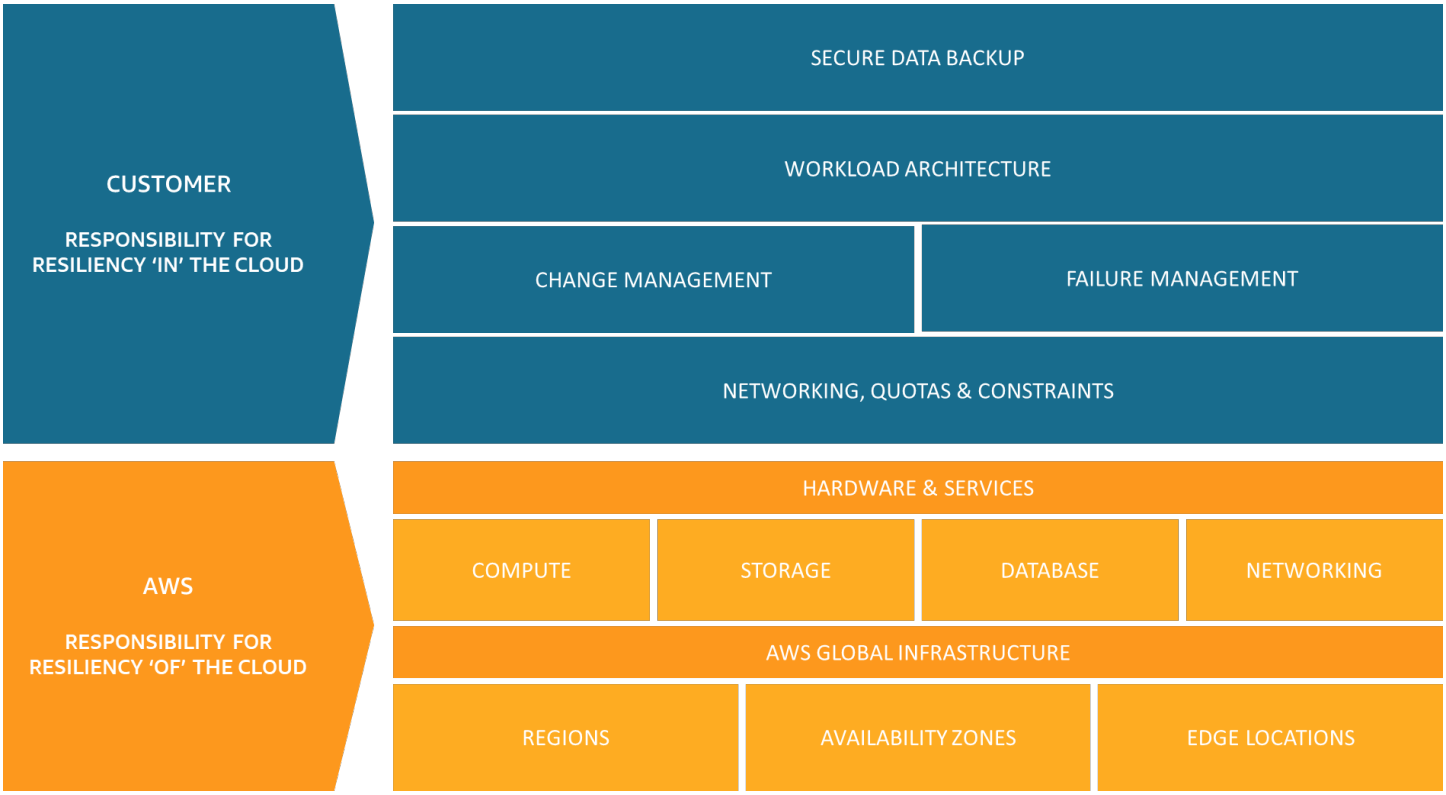

圖 2 - 彈性是 AWS 和客戶的共同責任

什麼是災難？

在規劃災難復原時，請針對以下三大類災害來評估計劃：

- 自然災害，如地震或洪水
- 技術故障，例如電源故障或網路連線問題
- 人為行動，例如無意的錯誤設定或未授權/外部方的存取或修改

這些潛在災害的每一項也會產生地理影響，可能是影響局部範圍、區域範圍、全國範圍、整個洲或全球。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，您可以採用多可用區域策略來緩解導致資料中心中斷的本地洪水問題，因為它不會影響多個可用區域。但是，攻擊生產資料的事件會需要啟用災難復原策略，以便容錯移轉到另一個 AWS 區域中的備份資料。

高可用性不是災難復原

可用性和災難復原仰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。但是，可用性側重於工作負載的元件，而災難復原則側重於整個工作負載的獨立副本。災難復原的目標與可用性不同，其目標為衡量符合災難條件之大規模事件後的恢復時間。您應先確保工作負載能符合您的可用性目標，因為高可用性架構可在發生影響可用性的事件時，讓您滿足客戶的需求。災難復原策略需要的方法與可用性不同，重點是將離散系統部署到多個位置，以便在必要時可以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，因為它會影響您採用的方法。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，不具備有高可用性。如果本地洪水問題影響該可用區域，則此方案需要容錯移轉到另一個可用區域以滿足 DR 目標。將此方案與部署多站點主動/主動的高可用性工作負載進行比較，其中工作負載跨多個活動區域部署，所有區域都為生產流量提供服務。在這種情況下，即使是發生摧毀整個區域的極罕見大規模災難，DR 策略也是透過將所有流量路由到其餘區域來完成的。

在可用性和災難復原之間，處理資料的方式也有所不同。假設有一個儲存解決方案，會持續複寫到另一個站點以實現高可用性 (例如多站點、主動/主動工作負載)。如果主要儲存裝置上的一或多個檔案遭到刪除或毀損，那麼這些破壞性變更也會複製到次要儲存裝置。在此情境下，雖然具備高可用性，但由於資料遭到刪除或毀損，進行容錯移轉的能力因此受到損害。反之，DR 策略中也需具備時間點備份。

業務連續性計劃 (BCP)

您的災難復原計劃應該屬於組織業務連續性計劃 (BCP) 的一部分，不應是獨立存在的文件。如果由於災難對工作負載以外的業務元素造成影響而無法達成工作負載的業務目標，那麼維護嚴格的災難復原目標就沒有任何意義。例如，地震可能會阻礙您運輸客戶在電子商務應用程式上購買的產品，因此即使有效的 DR 能保持工作負載正常運行，BCP 也需要滿足運輸需求。您的 DR 策略應根據業務需求、優先順序和環境而制定。

業務影響分析和風險評估

業務影響分析應量化工作負載中斷對業務的影響。它應該要識別無法使用工作負載對內部和外部客戶造成的影響，以及對您的業務的影響。分析應有助於判斷需要多快讓使工作負載可供使用，以及可容忍多少資料遺失。但是，必須指出，復原目標不應單獨制定；發生中斷的機率和復原的成本是關鍵因素，有助於了解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。您可能需要考慮將此因素納入災難復原規劃。例如，在每個人都獲得付款之前，薪資系統中斷可能會對業務產生非常大的影響，但在每個人都已經付款之後，它可能影響不大。

災難類型和地理影響的風險評估以及概述工作負載的技術實作，將決定每種災難類型發生中斷的機率。

對於極為關鍵的工作負載，您可以考慮跨多個區域的高可用性，並搭配持續備份，以將業務影響降至最低。對於沒那麼重要的工作負載，有效的策略可能是根本不需實施任何災難復原。對於某些災難場景，也可能因災難發生的機率較低，而據以做出不需災難復原策略的明智決策。請記住，AWS 區域內的可用區域在設計時即保持了它們之間的有意義距離，並仔細規劃其位置，因此大部分常見災難只會影響一個區域，而不會影響其他區域。因此，AWS 區域內的多可用區域架構，也許已能滿足您的降低風險需求。

您應評估災難復原選項的成本，以確保在考慮業務影響和風險的情況下，災難復原策略能提供正確的商業價值等級。

運用所有這些資訊，您可以記錄不同災難方案的威脅、風險、影響和成本，以及相關的復原選項。此資訊應用於確定每個工作負載的復原目標。

復原目標 (RTO 和 RPO)

在建立災難復原 (DR) 策略時，組織通常會規劃復原時間點目標 (RTO) 和復原點目標 (RPO)。

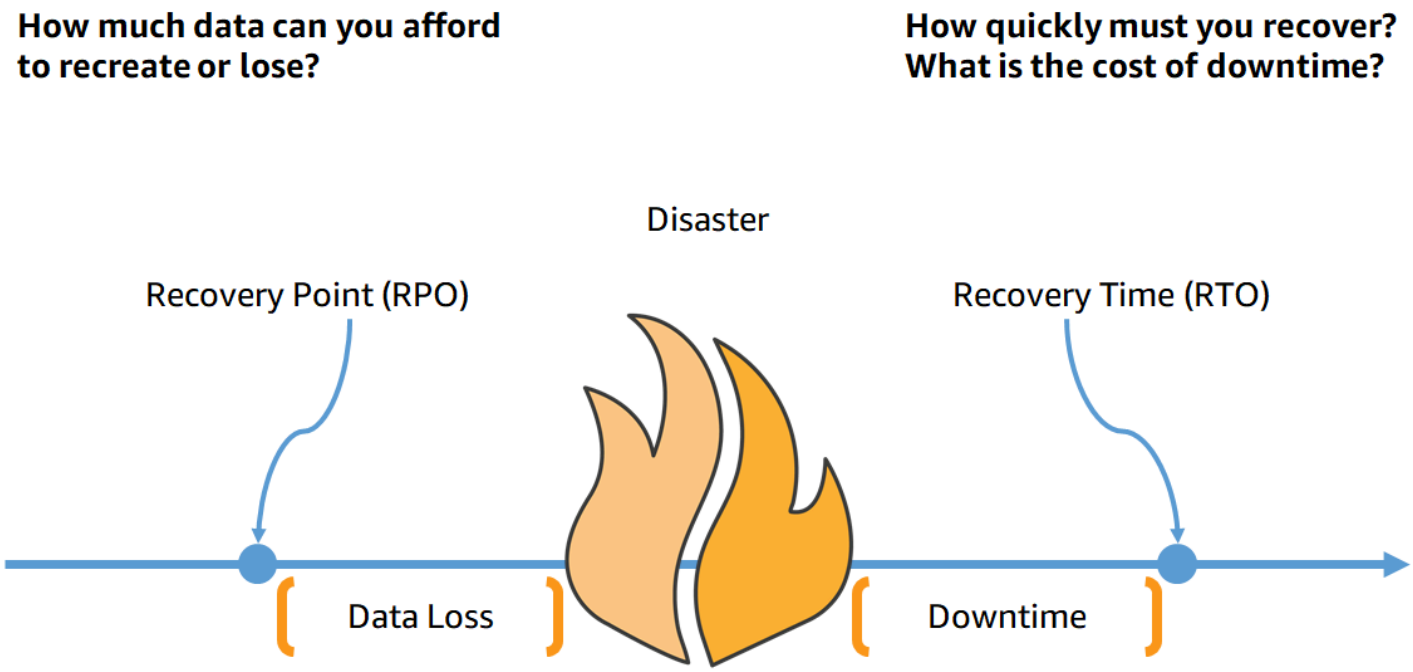

圖 3 - 復原目標

復原時間點目標 (RTO) 是服務中斷與恢復服務之間的最大可接受延遲。此目標會決定可接受的服務無法使用的時間長度，並由組織定義。

本白皮書主要討論四個 DR 策略：備份與還原、指示燈、暖待命和多站點主動/主動 (請參閱雲端中的災難復原選項)。在下圖中，該企業確定了其最大允許 RTO 以及他們可以用於服務還原策略的支出上限。鑑於企業的目標，災難復原策略指示燈或暖待命可同時滿足 RTO 和成本的標準。

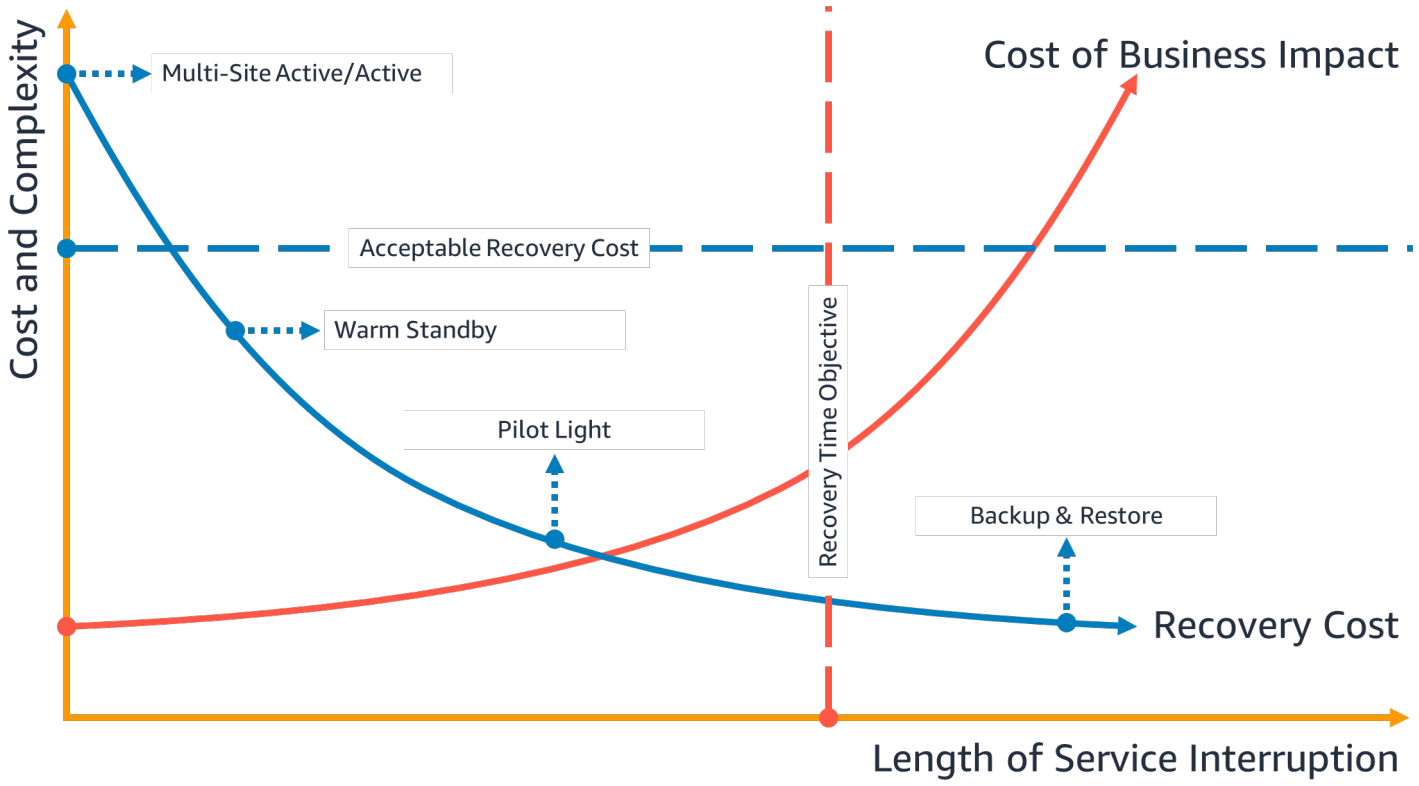

圖 4 - 復原時間點目標

復原點目標 (RPO) 是自上次資料復原點之後的最大可接受時間長度。此目標會決定最後一個復原點與服務中斷之間可接受的資料遺失，並由組織定義。

在下圖中，該企業確定了其最大允許 RPO 以及他們可以用於資料復原策略的支出上限。在四個災難復原策略中，指示燈或暖待命災難復原策略都可同時滿足 RPO 和成本的標準。

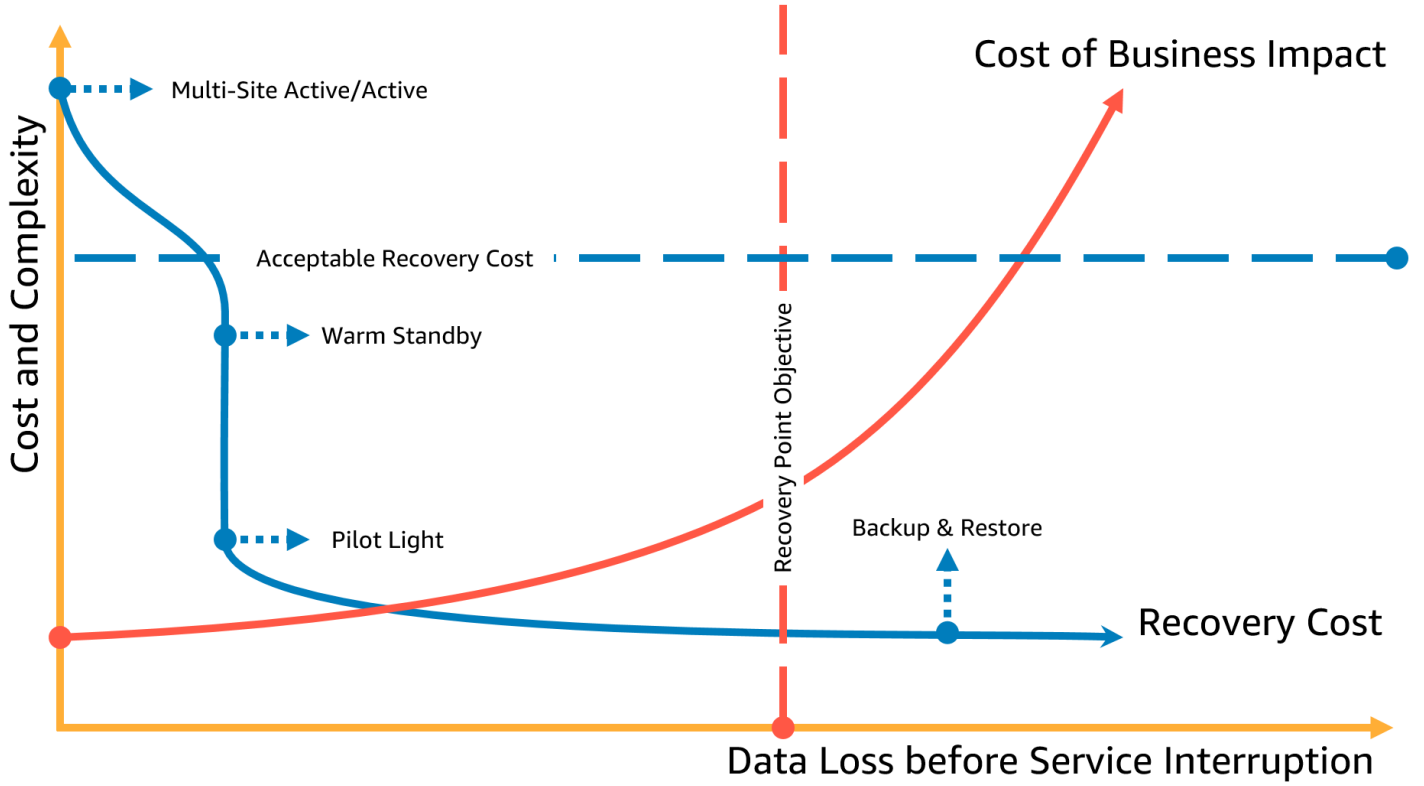

圖 5 - 復原點目標

> **Note**
>
> 如果復原的成本高於故障或遺失的成本，則除非有法規要求等次要驅動因素，否則不應設立復原選項。

雲端中的災難復原有所不同

災難復原策略隨着技術創新而演變。內部部署的災難復原計劃可能需要實際傳輸磁帶或將資料複製到另一站點。您的組織需要重新評估先前災難復原策略的業務影響、風險和成本，以便在 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括以下優勢：

- 可從災難中迅速復原，並且降低複雜性
- 簡單、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
- 有機會進行自動化，因而減少錯誤並縮短復原時間

AWS 可讓您將實體備份資料中心的固定資本費用交換為雲端中適當規模環境的可變運營費用，進而大幅降低成本。

對於許多組織來說，內部部署災難復原是根據資料中心工作負載的風險，以及將備份或複寫的資料復原到次要資料中心來制定的。當組織在 AWS 上部署工作負載時，他們可以實施架構良好的工作負載，並依靠 AWS 全球雲端基礎設施的設計來協助減輕此類中斷的影響。如需在雲端中設計和運行可靠、安全、高效且經濟高效之工作負載的架構最佳實務的詳細資訊，請參閱 AWS Well-Architected Framework - 可靠性支柱白皮書。

如果您的工作負載位於 AWS 上，則無需擔心資料中心的連線能力 (但不包括您對其的存取能力)、電源、空調、滅火設施和硬體。這一切都有人替您管理，您可以存取多個隔離故障的可用區域 (每個區域由一或多個離散資料中心組成)。

單一 AWS 區域

對於因一個實體資料中心中斷或遺失而造成的災難事件，在單一 AWS 區域的多個可用區域內實施高可用性工作負載，有助於減輕自然和技術災難，並降低人為威脅的風險，例如失誤或可能導致資料遺失的未經授權活動。每個 AWS 區域都由多個可用區域組成，每個可用區域都與其他區域的故障隔離。每個可用區域又由多個實體資料中心組成。為了更好地隔離有影響的問題並實現高可用性，您可以在同一區域的多個區域間對工作負載進行分區。可用區域專為實體冗餘設計且提供彈性，即使遇到停電、網際網路暫停服務、洪水和其他自然災害，也能實現不間斷的效能。請參閱 AWS 全球雲端基礎設施，了解 AWS 如何做到這一點。

跨單一 AWS 區域的多個可用區域進行部署，您的工作負載可以在單個 (甚至多個) 資料中心發生故障時，受到更好的保護。為了獲得單一區域部署的額外保證，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。此策略可將災難復原計劃的範圍縮小到只包括資料備份和復原。與以下章節介紹的其他多區域選項相比，透過備份到另一個 AWS 區域來利用多區域彈性簡單又便宜。例如，備份到 Amazon Simple Storage Service (Amazon S3) 可以立即擷取資料。但是，如果您針對部分資料的 DR 策略對擷取時間有更寬鬆的要求 (從幾分鐘到幾小時)，則使用 Amazon S3 Glacier 或 Amazon S3 Glacier Deep Archive 可大幅降低備份和復原策略的成本。

法規可能要求某些工作負載需有資料駐留辦法。如果這適用於位在目前只有一個 AWS 區域的工作負載，那麼除了針對上述高可用性來設計多可用區域工作負載之外，您還可以將該區域內的可用區域用作離散位置，來協助滿足適用於您在該區域內之工作負載的資料駐留要求。以下章節中介紹的 DR 策略使用多個 AWS 區域，但也可以使用可用區域 (取代區域) 來實施。

多個 AWS 區域

對於可能遺失相距很遠的多個資料中心的災難事件，您應考慮採用災難復原選項，以抵禦影響 AWS 內整個區域的自然災害和技術災難。以下各節中介紹的所有選項，都可以作為多區域架構實施來防止此類災難。

雲端中的災難復原選項

AWS 中可用的災難復原策略可以大致分為四種方法，從低成本、低複雜性的製作備份，到使用多個主動區域的較複雜策略。請務必定期測試災難復原策略，如此才能在有需要時有信心呼叫它。

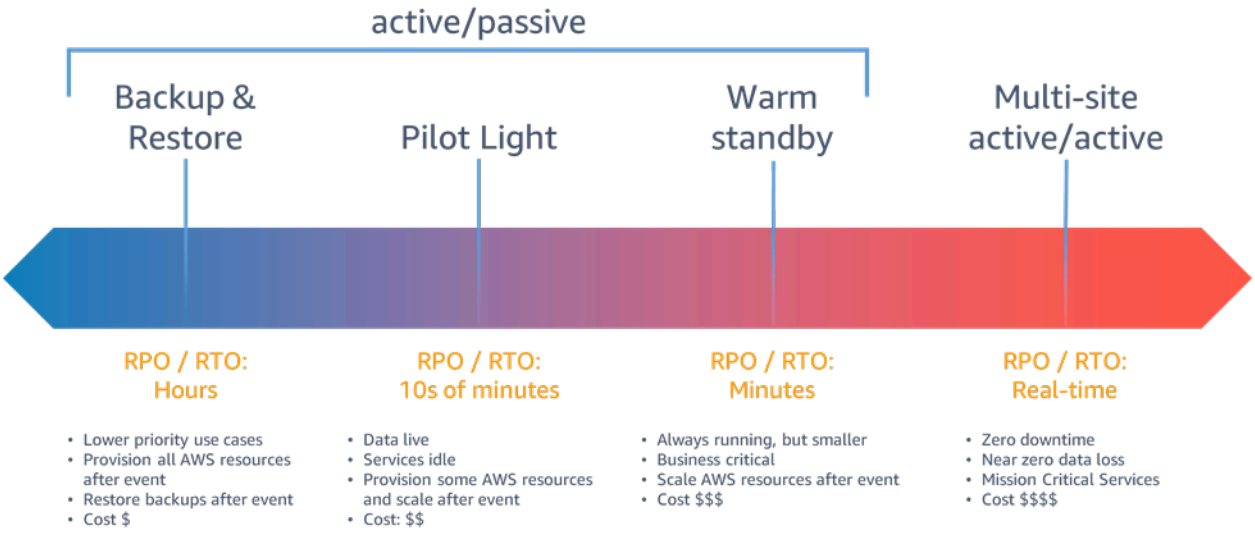

圖 6 - 災難復原策略

對於架構良好、高可用性的工作負載，因一個實體資料中心中斷或遺失而導致的災難事件，您可能只需要採用備份和還原方法即可進行災難復原。如果您對災難的定義不只是實體資料中心中斷或遺失，而是一個區域中斷或遺失，或是您受制於有所要求的法規約束，則應考慮「指示燈」、「暖待命」或「多站點主動/主動」。

備份和還原

備份和還原很適合用來緩解資料遺失或損毀造成的傷害。運用此方法，還可以搭配將資料複寫到其他 AWS 區域來緩解區域災難造成的影響，或是針對只部署到單一可用區域的工作負載，減輕其缺乏備援的缺點。除了資料以外，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。若要讓基礎設施能夠快速重新部署而不發生錯誤，您應一律使用 AWS CloudFormation 或 AWS Cloud Development Kit (AWS CDK) 等服務，以 Infrastructure as Code (IaC) 進行部署。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，並可能超過復原時間點目標 (RTO)。除了使用者資料以外，也請務必備份程式碼和組態，包括用於建立 Amazon EC2 執行個體的 Amazon Machine Images (AMI)。您可以使用 AWS CodePipeline 來自動重新部署應用程式程式碼和組態。

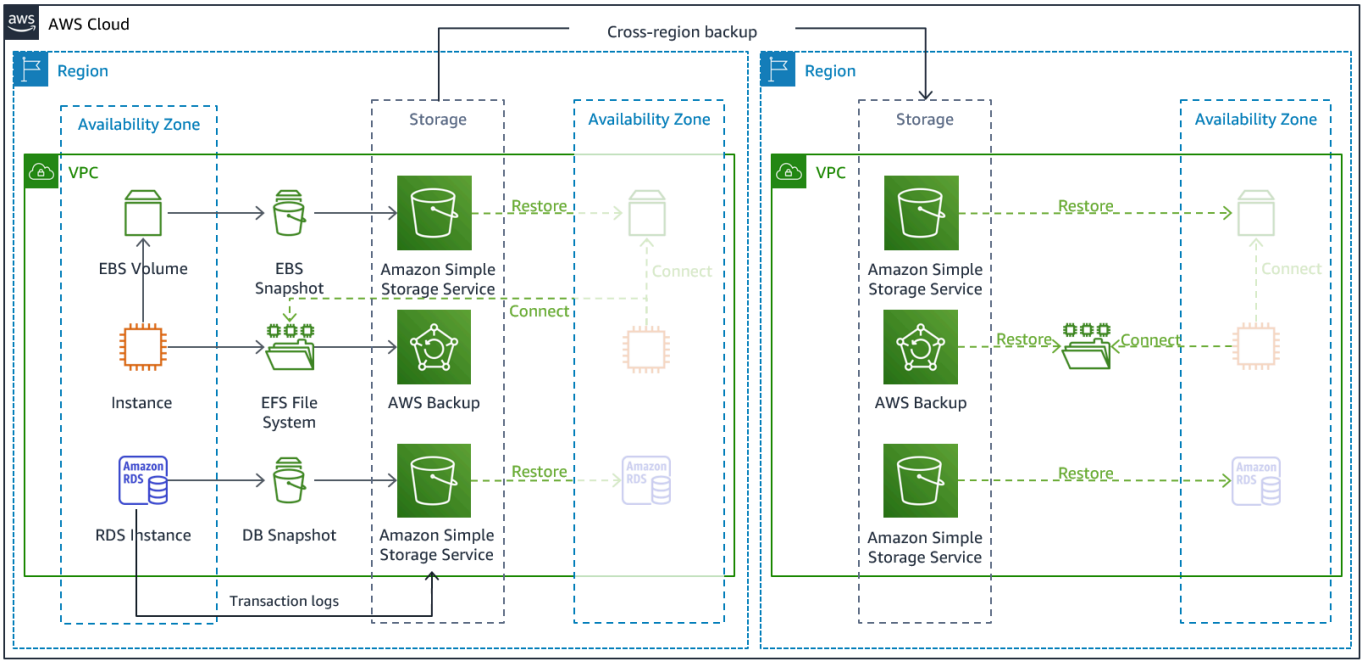

圖 7 - 備份與還原架構

AWS 服務

您的工作負載資料需要定期執行或連續不斷的備份策略。執行備份的頻率將決定可實現的復原點 (這些復原點應符合 RPO 要求)。備份也應提供將其還原到製作時間點的方法。具有時間點復原功能的備份，可透過以下服務和資源取得：

- 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 AWS Backup 時)
- Amazon Redshift 快照
- Amazon Neptune 快照

對於 Amazon Simple Storage Service (Amazon S3)，您可以使用 Amazon S3 跨區域複寫 (CRR) 將物件以非同步方式複製到 DR 區域中的 S3 儲存貯體，同時為儲存的物件提供版本控制，以便您可以選擇還原點。持續複寫資料具有備份資料的最短時間 (接近零) 的優點，但可能無法防止災難事件，例如資

料損毀或惡意攻擊 (如未經授權的資料刪除) 以及時間點備份。適用於指示燈的 AWS 服務一節會介紹持續複寫。

AWS Backup 提供一個集中位置，可用於設定、排程和監控以下服務和資源的 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 和 Amazon FSx for Lustre

AWS Backup 支援跨區域 (如災難復原區域) 複製備份。

如需 Amazon S3 資料的附加災難復原策略，您可啟用 S3 物件版本控制。物件版本控制會保留刪除或修改動作之前的原始版本，藉以避免 S3 中的資料遭受執行動作的影響。物件版本控制對於人為錯誤造成的災難，可以有效緩解。如果您使用 S3 複寫將資料備份到 DR 區域，則根據預設，在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，避免來源區域的惡意刪除。

除了資料以外，您也必須備份重新部署工作負載並滿足復原時間點目標 (RTO) 所需的組態和基礎設施。AWS CloudFormation 提供 Infrastructure as Code (IaC)，並可讓您定義工作負載中的所有 AWS 資源，因此您可以可靠地部署和重新部署到多個 AWS 帳戶和 AWS 區域。您可以將工作負載所使用的 Amazon EC2 執行個體，備份為 Amazon Machine Images (AMI)。AMI 是根據執行個體根磁碟區和連接到執行個體之任何其他 EBS 磁碟區的快照而建立的。您可以使用此 AMI 來啟動 EC2 執行個體的還原版本。AMI 可以在區域內或跨區域複製。或者，您也可以使用 AWS Backup 跨帳戶複製備份，以及將備份複製到其他 AWS 區域。跨帳戶備份功能有助於防範內部威脅或帳戶洩露等災難事件。AWS Backup 還為 EC2 備份加入額外功能 — 除了執行個體的個別 EBS 磁碟區之外，AWS Backup 也會儲存和追蹤以下中繼資料：執行個體類型、已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，此附加中繼資料僅能用於將 EC2 備份還原到同一個 AWS 區域。

儲存在災難復原區域中作為備份的任何資料，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 SDK 呼叫適用於 AWS Backup 的 API，來實作自動還原到 DR 區域。您可以將此設定為定期重複的任務，或在備份完成時觸發還原。下圖顯示使用 Amazon Simple Notification Service (Amazon SNS) 和 AWS Lambda 自動還原的範例。

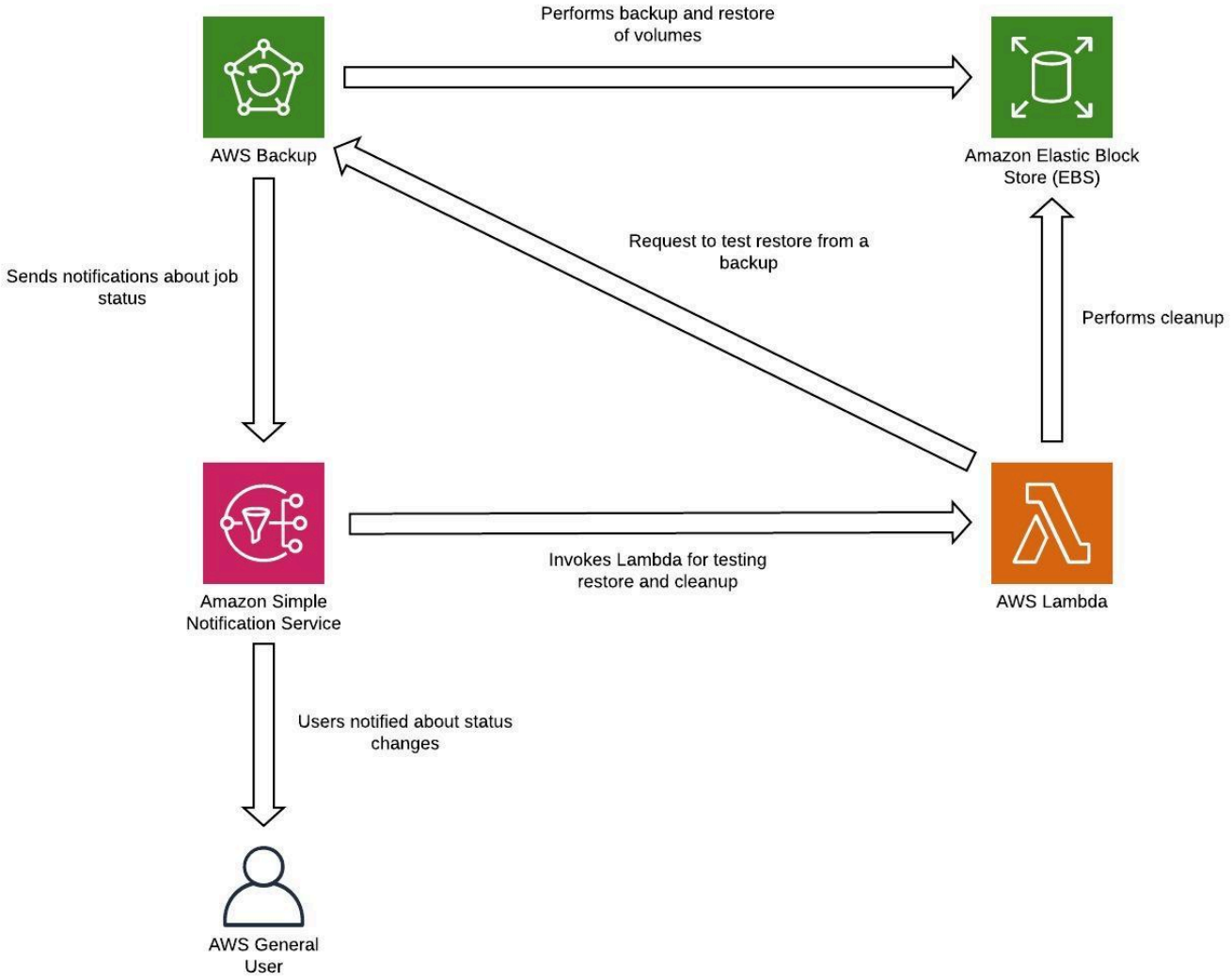

圖 8 - 還原和測試備份

> **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 實驗室：測試資料的備份與還原，了解實際操作示範。

指示燈

使用指示燈方法，您可以將資料從一個區域複寫到另一個區域，並佈建核心工作負載基礎設施的副本。支援資料複寫和備份所需的資源 (例如資料庫和物件儲存)，永遠處於開啟狀態。其他元素 (例如應用程式伺服器) 會載入應用程式程式碼和組態，但處於關閉狀態，僅在測試期間或呼叫災難復原容錯移轉時

使用。與備份和還原方法不同，您的核心基礎設施永遠可用，且您永遠可透過切換和水平擴展應用程式伺服器，來選擇快速佈建最大規模的生產環境。

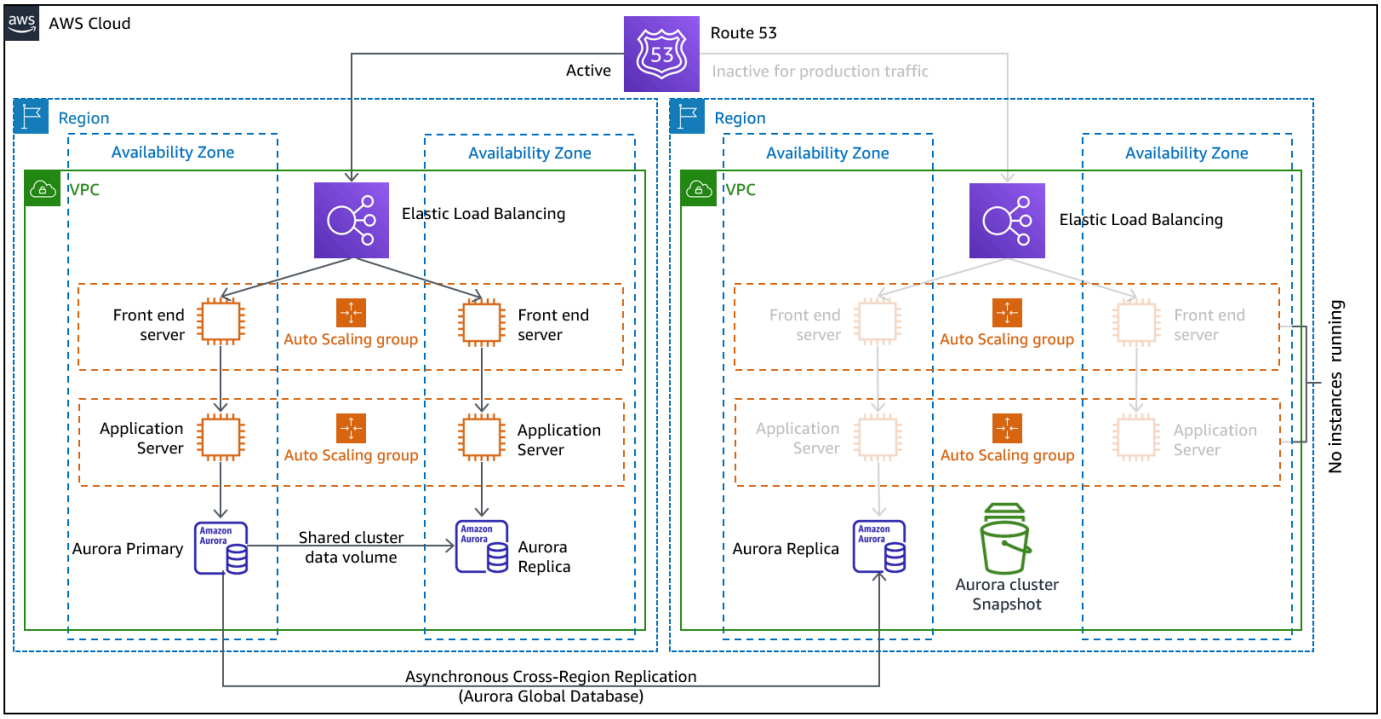

圖 9 - 指示燈架構

指示燈方法透過最大限度地減少作用中資源，來將災難復原的持續成本降至最低，並可簡化發生災難時的復原流程，因為核心基礎設施需求全部存在。此復原選項需要您變更部署方法。您需要變更每個區域的核心基礎設施，並將工作負載 (組態、程式碼) 變更同時部署到每個區域。透過自動化部署和使用 Infrastructure as Code (IaC) 跨多個帳戶和區域部署基礎設施 (將完整的基礎設施部署到主要區域，以及縮減規模/關閉部署到災難復原區域的基礎設施)，可以簡化此步驟。建議您在每個區域使用不同的帳戶，以提供最高等級的資源和安全隔離 (如果憑證洩露也是災難復原計劃的一部分)。

使用此方法，您還必須抵禦資料災難。持續複寫資料可以防止某些災難類型，但可能無法防止資料損毀或銷毀，除非您的策略還包括儲存資料的版本控制或時間點復原的選項。您可以備份災難區域中的複寫資料，以在同一個區域中建立時間點備份。

AWS 服務

除了使用備份和還原一節中介紹的 AWS 服務建立時間點備份之外，也請考慮使用以下服務建立指示燈策略。

對於指示燈，持續複寫資料到 DR 區域中的即時資料庫和資料存放區，是降低 RPO 的最佳方法 (搭配先前提及的時間點備份)。AWS 使用以下服務和資源，提供持續、跨區域的非同步資料複寫：

- Amazon Simple Storage Service (Amazon S3) 複寫
- Amazon RDS 僅供讀取複本
- Amazon Aurora Global Database
- Amazon DynamoDB 全域資料表

運用持續複寫，您的資料版本在 DR 區域中幾乎立即可用。使用適用於 S3 物件的 S3 複寫時間控制 (S3 RTC) 以及 Amazon Aurora Global Database 的管理功能等服務功能，可以監控實際複寫時間。

當發生容錯移轉以從災難復原區域執行讀/寫工作負載時，您必須將 RDS 僅供讀取複本提升為主要執行個體。對於 Aurora 以外的資料庫執行個體，此程序需要幾分鐘時間才能完成，且過程中需要重新開機。對於使用 RDS 進行跨區域複寫 (CRR) 和容錯移轉，使用 Amazon Aurora Global Database 具有幾個優勢。Global Database 使用專用基礎設施，讓您的資料庫完全可用於為您的應用程式提供服務，並且可以複寫到次要區域，典型延遲不到一秒 (在 AWS 區域內甚至可低於 100 毫秒)。使用 Amazon Aurora Global Database，如果主要區域效能下降或中斷，即使發生完全區域中斷，您也可以在 1 分鐘內，將其中一個次要區域提升為擔任讀/寫責任。提升可以自動進行，不須重新開機。

您必須在 DR 區域中，部署具有較少或較小資源之核心工作負載基礎設施的縮減規模版本。使用 AWS CloudFormation，您可以定義基礎設施，並且跨 AWS 帳戶以及跨 AWS 區域一致地部署它。AWS CloudFormation 使用預先定義的虛擬參數來識別部署它的 AWS 帳戶和 AWS 區域。因此，您可以在 CloudFormation 範本中實施條件邏輯，以便在 DR 區域中僅部署縮減版本的基礎設施。對於 EC2 執行個體部署，Amazon Machine Image (AMI) 提供硬體組態和已安裝軟體等資訊。您可以實作 Image Builder 管道來建立所需的 AMI，並將這些 AMI 複製到主要區域和備份區域。這有助於確保這些黃金 AMI 擁有在發生災難事件時，足以在新區域重新部署或水平擴展工作負載所需的一切。Amazon EC2 執行個體以縮減組態進行部署 (執行個體數少於您的主要區域)。您可以使用休眠，將 EC2 執行個體置於停止狀態，如此就不用支付 EC2 費用，只需為使用的儲存空間付費。若要啟動 EC2 執行個體，您可以使用 AWS 命令行界面 (CLI) 或 AWS SDK 建立指令碼。若要水平擴展基礎設施以支援生產流量，請參閱暖待命一節中的AWS Auto Scaling。

對於主動/待命組態 (例如指示燈)，所有流量一開始會流向主要區域，如果主要區域不再可用，則切換到災難復原區域。使用 AWS 服務時，可以考慮兩個流量管理選項。第一個選項是使用 Amazon Route 53。使用 Amazon Route 53，您可以將一個或多個 AWS 區域中的多個 IP 端點關聯至 Route 53 網域名稱。然後，您可以將流量路由到該網域名稱下的適當端點。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 DNS 備援來確保流量傳送到狀態良好的端點。

第二個選項是使用 AWS Global Accelerator。使用 AnyCast IP，您可以將一個或多個 AWS 區域中的多個端點關聯至相同的靜態 IP 地址。AWS Global Accelerator 接著會將流量路由到與該地址關聯的適當端點。Global Accelerator 運作狀態檢查會監控端點。使用這些運作狀態檢查，AWS Global

Accelerator 可以自動檢查應用程式的運作狀態，並僅將使用者流量路由到狀態良好的應用程式端點。Global Accelerator 可為應用程式端點提供較低的延遲，因為它利用廣泛的 AWS 邊緣網路，盡快將流量放到 AWS 網路骨幹網路上。Global Accelerator 還能避免 DNS 系統可能發生的快取問題 (如 Route 53)。

CloudEndure Disaster Recovery

CloudEndure Disaster Recovery (可從 AWS Marketplace 取得) 使用底層伺服器的區塊層級複寫功能，將來自任何來源的伺服器託管應用程式和伺服器託管資料庫持續複寫到 AWS 中。CloudEndure Disaster Recovery 可讓您將 AWS 雲端用作內部部署工作負載及其環境的災難復原區域。如果 AWS 託管的工作負載僅包含 EC2 上託管的應用程式和資料庫 (亦即不是 RDS)，則它也可用於這些工作負載的災難復原。CloudEndure Disaster Recovery 使用指示燈策略，在作為臨時區域的 Amazon Virtual Private Cloud (Amazon VPC) 中維護資料副本和關閉的資源。觸發容錯移轉事件時，臨時資源將用於在當作復原位置的目標 Amazon VPC 中，自動建立完整容量的部署。

圖 10 - CloudEndure Disaster Recovery 架構

暖待命

暖待命方法是為了確保在另一個區域中，有一個縮減規模但功能齊全的生產環境副本。此方法延伸指示燈概念並可縮短復原時間，因為您的工作負載在另一個區域處於永遠啟用狀態。此方法也可讓您更輕鬆地執行測試或實施連續測試，提高從災難復原的能力信心。

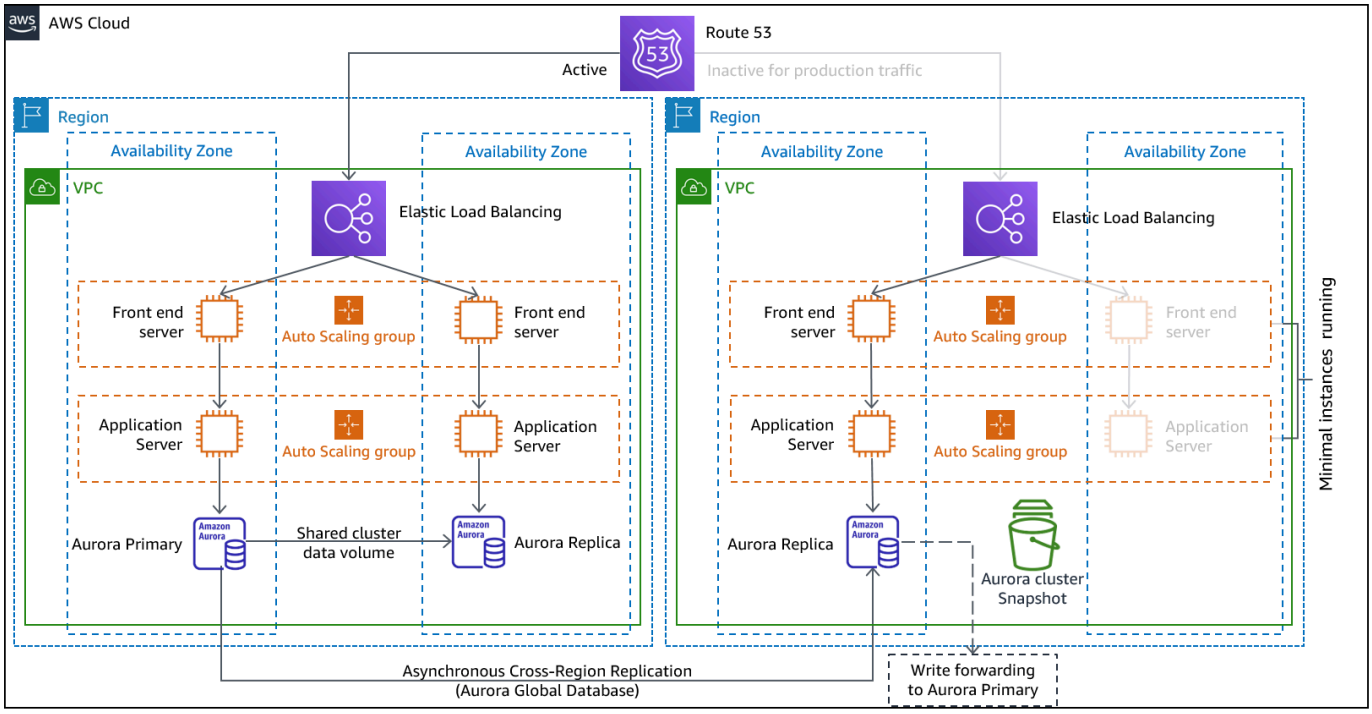

圖 11 - 暖待命架構

注意：指示燈和暖待命之間的差異有時可能很難理解。兩者都包括 DR 區域中的環境，其中包含主要區域資產的副本。差別之處在於，如果不先採取額外動作，則指示燈無法處理請求，而暖待命則可 (以降低容量的等級) 立即處理流量。指示燈方法需要您「開啟」伺服器、可能需部署額外的 (非核心) 基礎設施以及擴充規模，而暖待命只需要擴充規模 (一切項目都已部署並正在執行)。根據您的 RTO 和 RPO 需求，在這些選項之間進行選擇。

AWS 服務

備份和還原以及指示燈涵蓋的所有 AWS 服務也都用於暖待命，來進行資料備份、資料複寫、主動/待命流量路由，以及基礎設施部署 (包括 EC2 執行個體)。

AWS 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 跨 AWS 區域內的可用區域擴展部署 EC2 執行個體，進而在該區域內提供彈性。在指示燈或暖待命策略中，使用 Auto Scaling 可將 DR 區域水平擴展至完整的生產能力。例如，對於 EC2，在 Auto Scaling 群組上提高所需的容量設定。您可以透過AWS Management Console手動調整此設定、透過 AWS SDK 自動調整，也可以使用新的所需容量值重新部署 AWS CloudFormation 範本。您可以使用 AWS CloudFormation 參數來簡化重新部署 CloudFormation 範本。請確保 DR 區域中的服務配額設定夠高，以免限制您擴充規模到生產容量。

多站點主動/主動

您可以在多站點主動/主動或熱待命主動/被動策略中，於多個區域同時執行工作負載。多站點主動/主動為來自其部署之所有區域的流量提供服務，而熱待命僅為來自單個區域的流量提供服務，另一個區域則僅用於災難復原。使用多站點主動/主動方法，使用者可以存取部署工作負載之任何區域中的工作負載。這個方法是災難復原中最複雜、成本也最高的方法，但可以透過選擇正確的技術和正確實作，將復原時間縮短到接近零 (不過資料損毀仍需依賴備份，這通常會導致非零復原點)。熱待命使用主動/被動組態，使用者僅被導向至單一區域，DR 區域不接受流量。大部分客戶發現，如果想在第二個區域建立完整的環境，比較適合使用主動/主動。或者，如果您不想同時使用兩個區域來處理使用者流量，則暖待命可提供更經濟實惠且操作上較簡單的方法。

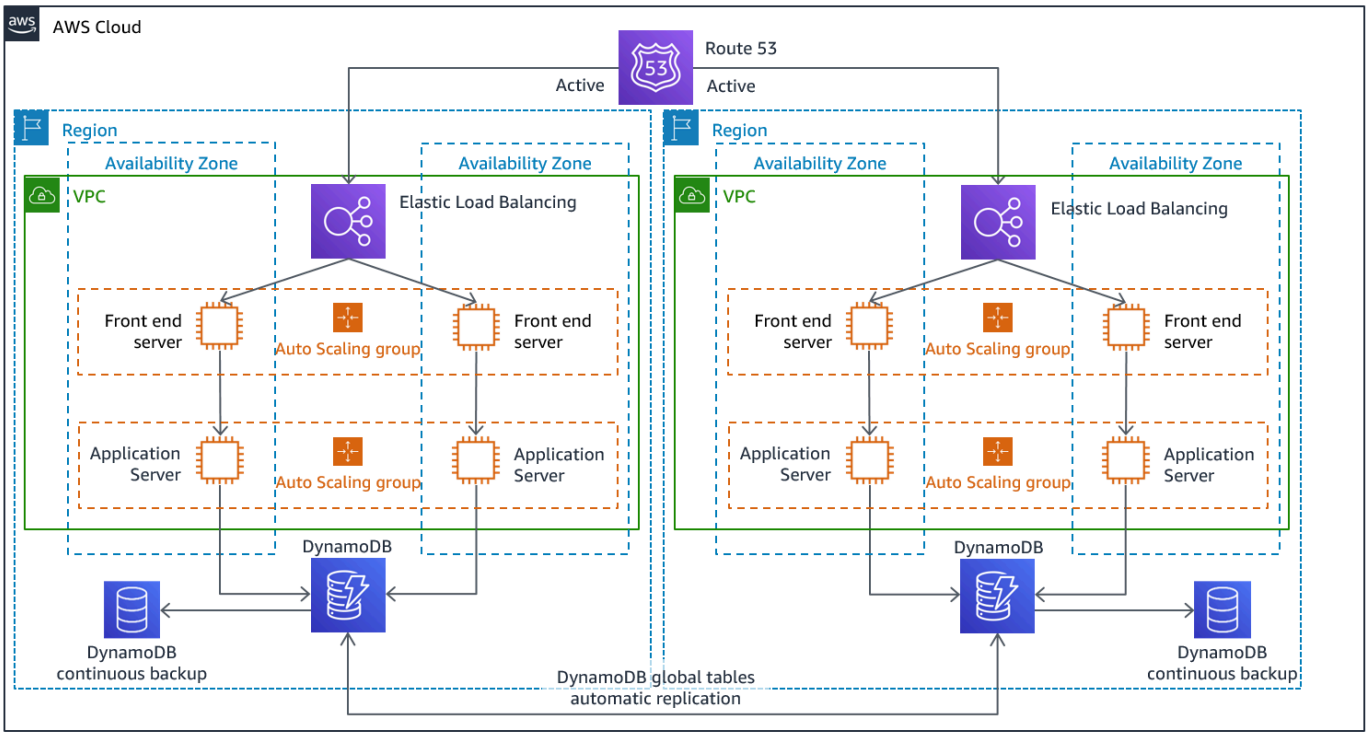

圖 12 - 多站點主動/主動架構 (將一個使用中路徑變更為非使用中，即成為熱待命)

對於多站點主動/主動，因為工作負載在多個區域中執行，因此沒有容錯移轉。在這種情況下，災難復原測試的重點是工作負載如何對遺失區域作出反應：是否將流量從故障的區域路由離開？ 其他區域可以處理所有流量嗎？ 也需要測試資料災難。備份和復原仍是必需的，也應定期測試。還應注意的是，涉及資料損毀、刪除或混淆之資料災難的復原時間永遠大於零，而且復原點永遠位於發現災難之前的某個時刻。如果保持接近零的復原時間會提高多站點主動/主動 (或熱待命) 方法的複雜性和成本，則應更努力維護安全並防止人為錯誤，以減輕人為災難。

AWS 服務

此處也將備份和還原、指示燈和暖待命涵蓋的所有 AWS 服務用於時間點資料備份、資料複寫、主動/主動流量路由，以及基礎設施部署和擴展 (包括 EC2 執行個體)。

對於前面討論的主動/被動方案 (指示燈和暖待命)，Amazon Route 53 和 AWS Global Accelerator 都可用於將網路流量路由到主動區域。對於此處的主動/主動策略，這兩種服務都允許定義政策，以決定哪些使用者移至哪個主動區域端點。使用 AWS Global Accelerator，您可以設定設定流量調撥工具來控制導向每個應用程式端點的流量百分比。Amazon Route 53 支援這個百分比方法，也支援其他多個可用政策，包括地理位置鄰近性和延遲型政策。Global Accelerator 會自動利用廣泛的 AWS 邊緣伺服器網路，盡快將流量傳輸到 AWS 骨幹網路，進而降低請求延遲。

使用此策略來複寫資料，可實現接近零的 RPO。AWS 服務 (例如 Amazon Aurora Global Database) 使用專用基礎設施，讓資料庫充分為您的應用程式提供服務，而且複寫到一個次要區域通常延遲時間不到一秒。使用主動/被動策略時，只會對主要區域進行寫入動作。與主動/主動的區別在於，設計如何處理對每個主動區域的寫入。常見的做法是設計為從離使用者最近的區域提供讀取服務，稱為讀取本機。對於寫入，您有幾個選項：

- 寫入全域策略會將所有寫入路由到單一區域。如果該區域出現故障，則會提升另一個區域來接受寫入。Aurora Global Database 非常適合寫入全域，因為它支援跨區域的僅供讀取複本同步，您也可以在 1 分鐘內，將其中一個次要區域提升為擔任讀/寫責任。
- 寫入本機策略則會將寫入路由到最近的區域 (跟讀取一樣)。Amazon DynamoDB 全域資料表支援此類策略，允許從部署全域資料表的每個區域進行讀取和寫入。Amazon DynamoDB 全域資料表會在並行更新間使用最後寫入者獲勝核對機制。
- 寫入分割區策略會根據分割區索引鍵 (類似使用者 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 複寫可用於這種情況，且目前支援在兩個區域之間進行複寫。實施此方法時，請務必在儲存貯體 A 和 B 上同時啟用複本修改同步，來複寫複寫物件上的複本中繼資料變更，例如物件存取控制清單 (ACL)、物件標籤或物件鎖定。您也可以設定是否在主動區域的儲存貯體之間複寫刪除標記。除了複寫之外，您的策略還必須包括時間點備份，以防止資料損毀或銷毀事件。

AWS CloudFormation 是一個強大的工具，可在多個 AWS 區域的 AWS 帳戶之間實施一致部署的基礎設施。AWS CloudFormation StackSets 讓您跨多個帳戶和區域使用單次操作建立、更新或刪除 CloudFormation 堆疊，藉以擴充此功能。雖然 AWS CloudFormation 使用 YAML 或 JSON 定義 Infrastructure as Code，但 AWS Cloud Development Kit (AWS CDK) 允許您使用熟悉的程式語言來定義 Infrastructure as Code (IaC)。您的程式碼將轉換為 CloudFormation，然後用於在 AWS 中部署資源。

偵測

盡快得知您的工作負載無法提供其應提供的業務成果，這點非常重要。透過這個方式，您可以快速宣布發生災難並從事件中復原。對於嚴格的復原目標，此回應時間加上適當的資訊，對於實現復原目標至關重要。如果復原點目標為 1 小時，則需要在 1 小時內偵測到事件、通知適當人員、向上呈報、評估 (不執行災難復原計劃) 的預期復原時間等相關資訊 (如果有)、宣布發生災難並進行復原。

> **Note**
>
> 如果利害關係人決定即使 RTO 會面臨風險也不援用 DR，則請重新評估 DR 計劃和目標。之所以決定不援用 DR 計劃，可能是因為計劃不充分，或者對執行缺乏信心。

在您的計劃和目標中，請務必將事件偵測、通知、呈報、發現和宣布納入考量，以提供可提供商業價值的實際、可達成目標。

AWS 會在 Service Health Dashboard (服務運作狀態儀表板) 上發佈服務可用性的最新資訊。請隨時檢查以獲取目前狀態資訊，或訂閱 RSS 摘要以獲取每個服務中斷的通知。如果您遇到服務無法顯示在 Service Health Dashboard 上的即時操作問題，則可以建立支援請求。

AWS Health Dashboard 提供會影響您帳戶的 AWS Health 事件相關資訊。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)。

對於最嚴格的 RTO 要求，您可以根據運作狀態檢查來實施自動容錯移轉。 設計能代表使用者體驗並根據關鍵績效指標的運作狀態檢查。深度運作狀態檢查會執行工作負載的關鍵功能，並超越淺層活動訊號檢查。使用以多個訊號為基礎的深度運作狀態檢查。請謹慎使用此方法，以免不慎觸發假警示，因為不必要的容錯移轉，本身就會引起可用性風險。

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到工作負載的 DR 區域，以確保滿足 RTO 和 RPO 要求。

要避免的模式是：開發鮮少執行的復原路徑。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。上次測試時可能足夠的次要存放區容量，在這種情況下可能不再能夠承受負載，或者次要區域的服務配額可能不夠。

根據我們的經驗，唯一能發揮功用的錯誤復原，是您經常測試的路徑。這就是為什麼最好擁有少量的復原路徑。

您可建立復原模式，並定期進行測試。若擁有複雜或關鍵復原路徑，您還是需要定期在生產中執行該故障，來驗證復原路徑能否發揮功用。

管理 DR 區域的組態偏移。確保根據需要在 DR 區域提供基礎設施、資料和組態。例如，檢查 AMI 和服務配額是否為最新版本。

您可以利用 AWS Config 持續監控和記錄 AWS 資源組態。AWS Config 可以偵測漂移並觸發 AWS Systems Manager Automation 來修復漂移並發出提醒。AWS CloudFormation 可以另外偵測已部署堆疊中的漂移。

結論

客户需負責維護其應用程式在雲端中的可用性。定義何謂災難，並制定一套災難復原計劃來反映這個定義及其可能對業務成果所造成影響，這是非常重要的。根據影響分析和風險評估建立復原時間點目標 (RTO) 和復原點目標 (RPO)，然後選擇適當的架構來抵禦災難。確保可以及時發現災害，更重要的是了解目標何時處於危險之中。請務必擁有計劃，並透過測試驗證計劃可行。未經驗證的災難復原計劃，可能會因缺乏信心或無法實現災難復原目標而造成無法實施。

作者群

此文件的作者包括：

- Alex Livingstone，AWS Enterprise Support 雲端操作實務主管
- 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 Well-Architected Framework 可靠性支柱
- 災難復原計劃檢查清單
- 實作運作狀態檢查
- AWS 解決方案實作：多區域應用程式架構
- AWS re:Invent 2018：適用於多區域主動-主動應用程式的架構模式 (ARC209-R2)

文件歷史記錄

變更	描述	日期
初次出版	首次出版。	2021 年 2 月 12 日

若要收到此白皮書更新的通知，請訂閱 RSS 摘要。

聲明

客戶應負責對本文件中的資訊自行進行獨立評估。本文件：(a) 僅供參考之用，(b) 代表目前的 AWS 產品供應與實務，如有變更恕不另行通知，以及 (c) 不構成 AWS 及其附屬公司、供應商或授權人的任何承諾或保證。AWS 產品或服務以「現況」提供，不提供任何明示或暗示的擔保、主張或條件。AWS 對其客戶之責任與義務，應受 AWS 協議之約束，且本文件並不屬於 AWS 與其客戶間之任何協議的一部分，亦非上述協議之修改。