AWS 白皮书

AWS 故障隔离界限

AWS 故障隔離界限: AWS 白皮书

Table of Contents

AWS Well-Architected

出版日期：二 ○ 二二年十一月十六日（文件修訂）

摘要

Amazon Web Services (AWS) 提供不同的隔離界限，例如可用區域 (AZ)、區域、控制平面和資料平面。本白 paper 詳細說明如何AWS使用這些邊界來建立區域、區域和全球服務。其中也包含有關如何考慮這些不同服務的相依性，以及如何改善使用這些服務建置之工作負載彈性的規範性指引。

你 Well-Architected?

AWSWell-Architected 的架構可協助您瞭解在雲端中建置系統時所做決策的優缺點。Framework 的六大支柱可讓您學習如何設計和操作可靠、安全、高效、符合成本效益且可持續發展的系統的架構最佳實務。使用中免費提供的 AWS Well-Architected ToolAWS Management Console，您可以針對每個支柱回答一組問題，根據這些最佳實務來檢閱工作負載。

如需雲端架構的更多專家指導和最佳實務 (參考架構部署、圖表和白皮書)，請參閱架構中心。AWS

簡介

AWS營運全球基礎架構，以提供雲端服務，協助客戶以彈性、安全、可擴充且高度可用的方式部署工作負載。此AWS基礎架構使用多重故障隔離架構，協助客戶達成彈性目標。這些故障隔離界限可讓客戶設計工作負載，以利用他們所提供的可預測影響限制範圍。了解如何使用這些界限設計AWS服務也很重要，這樣您就可以有意地選擇為工作負載選取的相依性。

本 paper 將首先概述AWS全球基礎架構及其提供的故障隔離界限，以及用於設計我們服務的一些模式。本 paper 接下來將利用這項理解基準，概述不同AWS服務範圍：區域、區域和全球。它也會提供建置架構的最佳實務，這些架構使用這些隔離界限和不同的服務範圍來改善執行工作負載的彈性AWS。特別是，它提供了有關如何在全球服務上採取依賴關係，同時最大限度地減少單點故障的規定性指導。這可協助您針對AWS相依性，以及如何針對高可用性 (HA) 和災難復原 (DR) 設計工作負載，做出明智的選擇。

AWS 基礎設施

本節提供AWS全域基礎結構及其提供的錯誤隔離界限的摘要。此外，本節將提供控制平面和數據平面的概念，這是如何AWS設計其服務的關鍵區別的概述。此資訊提供了一項基準，以瞭解故障隔離界限和服務的控制平面和資料平面如何套用至我們在下一節中討論的AWS服務類型。

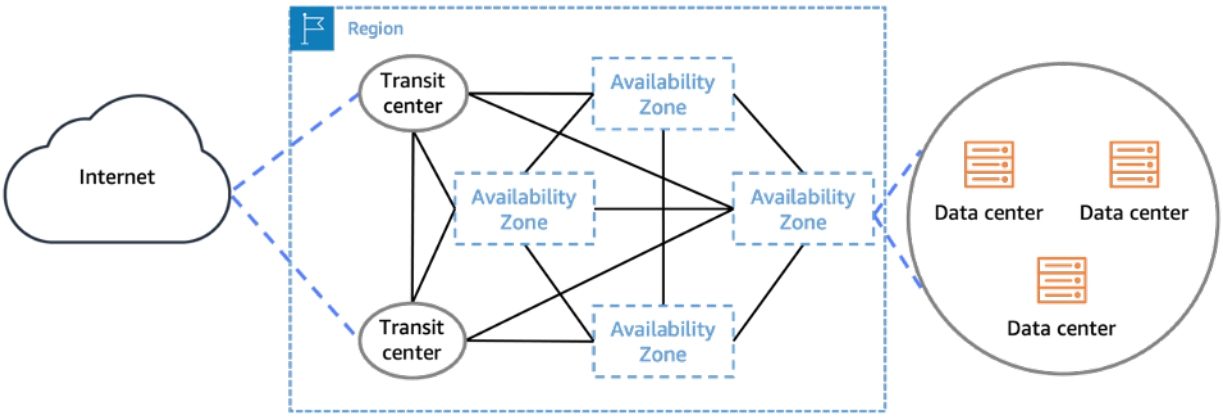
主題

可用區域

AWS在全球數個區域內運作超過 100 個可用區域 (目前的數字可在這裡找到：AWS全球基礎架構)。可用區域是一或多個獨立的資料中心，其中包含獨立的備援電源基礎架構、網路和連線能力AWS 區域。區域中的可用區域彼此之間有意義的距離，最多可達 60 英里（約 100 公里）以防止相關故障，但距離足以使用低於 10 毫秒延遲的同步複寫。它們的設計不會同時受到共同命運情境的影響，例如公用事業電源，水中斷，纖維隔離，地震，火災，龍捲風或洪水。常見的故障點 (如發電機和冷卻設備) 不會跨可用區域共用，而是由獨立的變電站供應。AWS將更新部署到其服務時，相同區域中可用區域的部署會及時分開，以防止相關故障。

區域中的所有可用區域都透過完全備援的專用都會光纖，與高頻寬、低延遲的網路互連。區域中的每個可用區域透過兩個傳輸中心連接到網際網路，在這些交通中心與多個第一層網際網路供應商的對AWS等 (如需詳細資訊，請參閱 Amazon Web Services 概觀)。

這些功能可提供可用區域彼此之間的強大隔離，我們稱之為可用區域獨立性 (AZI)。可用區域的邏輯結構及其與網際網路的連線如下圖所示。



可用區域由一或多個實體資料中心組成，這些中心彼此冗餘連線以及網際網路

區域

每個區域AWS 區域由地理區域內的多個獨立且實際上獨立的可用區域組成。所有區域目前都有三個以上的可用區域。區域本身會與其他區域隔離並獨立於其他區域，但本文件稍後提及的一些例外情況 (請參閱全域單一區域作業)。這種區域之間的區隔會將服務失敗 (發生時) 限制在單一區域。在這種情況下，其他地區的正常操作不會受到影響。此外，除非您明確使用AWS服務提供的複寫或複製功能，或自行複製資源，否則您在一個區域中建立的資源和資料不存在於任何其他區域中。

截至 2022 年 12 月的目前和計劃中的 AWS 區域

AWSLocal Zones

AWSL@@ ocal Zones 是一種基礎架構部署，可將運算、儲存、資料庫和其他特定AWS服務放在靠近大型人口和產業中心的地方。您可以使用AWS本機區域中的運算和儲存服務等服務，在邊緣執行低延遲應用程式，或簡化混合雲移轉作業。Local Zones 具有本機網際網路輸入和輸出以減少延遲，但也可透過 Amazon 的備援和高頻寬私有網路連接至其父區域，讓在 L AWS ocal Zones 執行的應用程式能夠快速、安全且順暢地存取全方位服務。

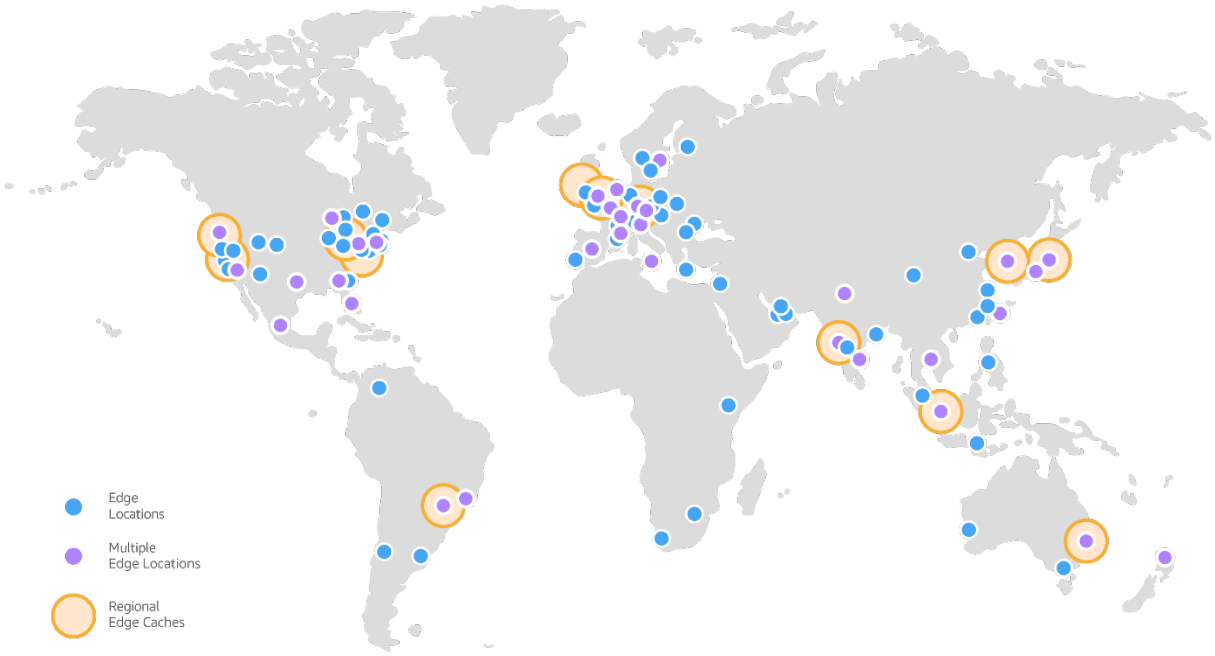
AWS Outposts

AWS Outposts是一系列全受管解決方案，可將AWS基礎架構和服務提供到幾乎任何內部部署或邊緣位置，以獲得真正一致的混合體驗。 Outposts 解決方案可讓您在內部部署擴充和執行原生AWS服務，並提供多種外形規格，從 1U 和 2U Outposts 伺服器到 42U Outposts 機架，以及多機架部署。

使用時AWS Outposts，您可以在本機執行特定AWS服務，並連線到父項中可用的各種服務AWS 區域。 AWS Outposts是完全受管且可設定的運算與儲存機架，採用AWS設計硬體所建置，可讓客戶在內部部署執行運算與儲存，同時順暢地連接AWS雲端中的各種服務。

存在點

除了AWS 區域和可用區域之外，AWS還營運全球分佈式存在點 (PoP) 網路。這些 PoPs 託管 Amazon CloudFront，一個內容交付網絡（CDN）; Amazon 路線 53，公共域名系統（DNS）解析服務; 和AWS全球加速器（AGA），邊緣聯網優化服務。全球邊緣網路目前由 410 多個組成 PoPs，包括 400 多個節點，以及遍及 48 個國家/地區 90 多個城市的 13 個區域中層快取 (目前狀態可在此處找到：Amazon CloudFront 主要功能)。



Amazon CloudFront 全球邊緣網路

每個 PoP 都與其他 PoP 隔離，這意味著影響單個 PoP 或大都市區的故障不會影響全球網絡的其餘部分。與全球數千個 Tier 1/2/3 電信運營商的AWS網絡同行，與所有主要接入網絡緊密連接，以實現最佳性能，並具有數百 TB 的部署容量。邊緣位置AWS 區域透過AWS網路骨幹連接到，這是一種完全備援的多重 100GbE parallel 光纖，可環繞全球，並與數萬個網路連結，以改善原點擷取和動態內容加速。

資料分割

AWS將區域群組為分割區。每個區域都只在一個分割區中，而且每個分割區都有一個或多個區域。分區具有獨立的AWS Identity and Access Management（IAM）實例，並在不同分區中的區域之間提供硬式界限。 AWS商業區域在aws隔斷中，中國區域在aws-cn隔斷中，AWS GovCloud 區域在aws-us-gov隔斷中。某些AWS服務旨在提供跨區域功能，例如 Amazon S3 跨區域複寫或 AWS Transit Gateway 區域間對等。這些類型的功能僅在相同分割區中的區域之間支援。您無法使用來自某個分割區的 IAM 登入資料與不同分割區中的資源互動。

控制平面和資料平面

AWS將大多數服務分成控制平面和數據平面的概念。這些術語來自網絡世界，特別是路由器。路由器的數據平面是它的主要功能，是根據規則移動數據包。但是必須從某個地方創建和分發路由策略，這就是控制平面進入的地方。

控制平面提供用於建立、讀取/描述、更新、刪除和列出 (CRUDL) 資源的管理 API。例如，以下是所有控制平面動作：啟動新的 Amazon 彈性運算雲端 (Amazon EC2) 執行個體、建立 Amazon 簡單儲存服務 (Amazon S3) 儲存貯體，以及描述 Amazon 簡單佇列服務 (Amazon SQS) 佇列。啟動 EC2 執行個體時，控制平面必須執行多項任務，例如尋找具有容量的實體主機、配置網路界面、準備 Amazon 彈性區塊存放區 (Amazon EBS) 磁碟區、產生 IAM 登入資料、新增安全群組規則等。控制平面往往是複雜的協調和聚合系統。

數據平面是提供服務的主要功能。例如，以下是每個涉及服務的資料平面的所有部分：執行中的 EC2 執行個體本身、讀取和寫入 EBS 磁碟區、取得和放入 S3 儲存貯體中的物件，以及 Route 53 回應 DNS 查詢和執行運作狀態檢查。

與控制面相比，資料平面刻意不那麼複雜，移動零件較少，這些平面通常會實作複雜的工作流程、商務邏輯和資料庫系統。這使得失敗事件在統計學上降低資料平面與控制平面中發生的可能性。雖然資料和控制平面都有助於整體運作和服務的成功，但將它們AWS視為獨特的元件。這種分離具有效能和可用性的優點。

靜態穩定性

AWS服務最重要的彈性特徵之一就是所AWS謂的靜態穩定性。這個術語意味著系統在靜態狀態下運行，並繼續正常運行，而不需要在故障或依賴關係不可用期間進行更改。我們這樣做的一種方法是防止我們服務中的循環依賴，從而阻止其中一個服務成功恢復。我們執行此操作的另一種方法是保持現有狀態。我們認為控制平面在統計學上比數據平面更容易失敗的事實。雖然資料平面通常依賴於從控制平面到達的資料，但資料平面會維持其現有狀態，即使面對控制平面損壞也能繼續工作。資源的資料平面存取權一旦佈建，就不會依賴於控制平面，因此不會受到任何控制平面損害的影響。換句話說，即使建立、修改或刪除資源的能力受損，現有資源仍然可用。這使得AWS數據平面靜態穩定，以防止控制平面中的損害。您可以實現不同的模式，以針對不同類型的依賴失敗靜態穩定。

您可以在 Amazon EC2 中找到靜態穩定性的範例。一旦 EC2 執行個體啟動，就和資料中心中的實體伺服器一樣可用。它不依賴於任何控制平面 API 來保持運行狀態，或在重新啟動後再次開始運行。其他AWS資源 (例如 VPC、Amazon S3 儲存貯體和物件以及 Amazon EBS 磁碟區) 擁有相同的屬性。

靜態穩定性是一種深深根植於服務AWS設計方式的概念，但它也是一種可供客戶使用的模式。事實上，以彈性方式使用不同類型服務的最佳實AWS務指南，大多數是實作生產環境的靜態穩定性。最可

靠的恢復和緩解機制是需要最少更改才能實現恢復的機制。預先佈建額外的容量有助於實現靜態穩定性，而不是依賴 EC2 控制平面啟動新的 EC2 執行個體以從故障的可用區域復原。因此，消除復原路徑中控制平面 (實作資源變更的 API) 的相依性，有助於產生更具彈性的工作負載。如需靜態穩定性、控制平面和資料平面的詳細資訊，請參閱 Amazon 建置者的程式庫文章使用可用區域的靜態穩定性。

Summary

AWS在我們的基礎架構中利用不同的容器來建立故障隔離。核心基礎結構故障容器包括分割區、區域、可用區域、控制平面和資料平面。接下來，我們將研究不同類型的AWS服務、如何在設計中使用這些容器，以及如何使用這些容器架構工作負載以提供彈性。

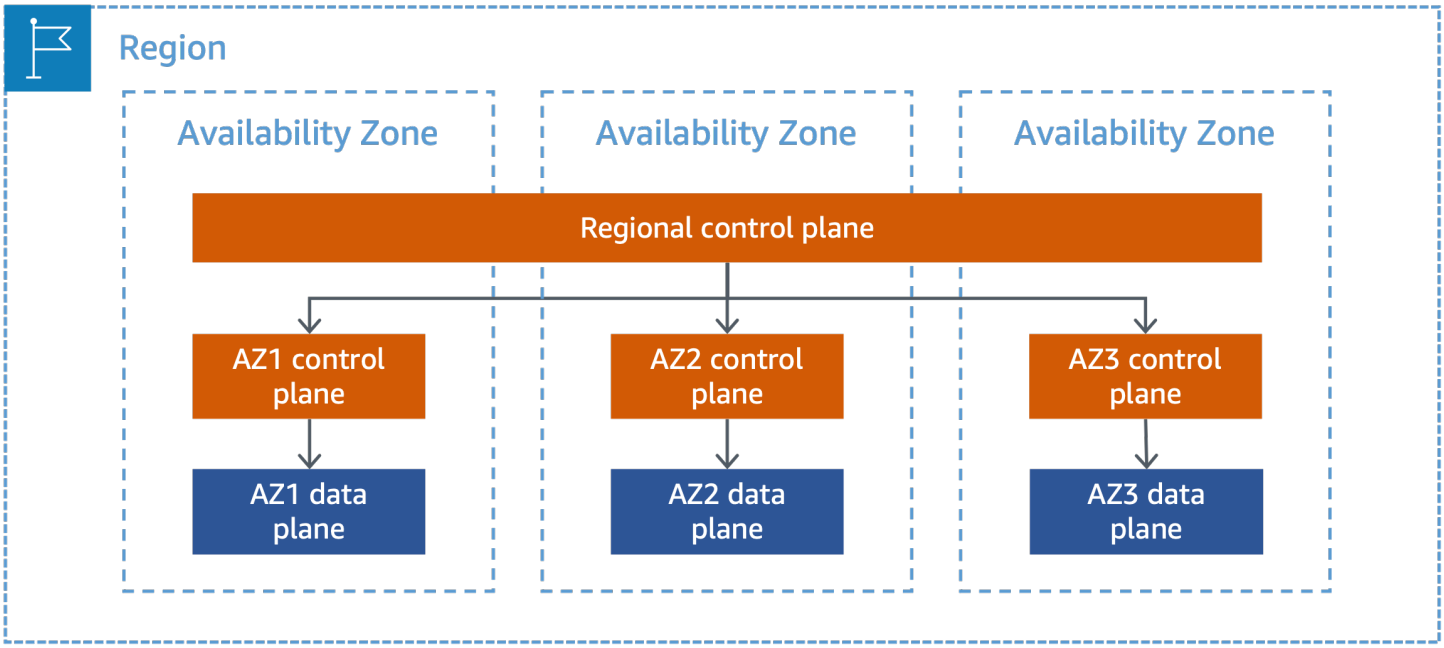
AWS 服務類型

AWS 根據故障隔離邊界來運作三種不同類別的服務：區域、區域和全球。本節將更詳細地說明這些不同類型的服務的設計方式，以便您可以判斷特定服務類型的服務中的故障將如何影響執行的工作負載 AWS。它還提供了如何架構工作負載以彈性方式使用這些服務的高層級指導。對於全球服務，本文件也在中附錄 A-部分服務指引提供規範性指引，附錄 B-邊緣網路全球服務指南可協助您避免服務中的控制平面損傷對工作負載造成影響，協助您安全地採取全域 AWS 服務的相依性，同時將單點故障引入降到最低。

主題

區域服務

可用區域獨立性 (AZI) 能 AWS 夠提供區域服務，例如 Amazon EC2 和 Amazon EBS。區域服務是提供指定資源部署到哪個可用區域的能力的服務。這些服務在區域內的每個可用區域中獨立運作，更重要的是，在每個可用區域也會獨立失敗。這表示一個可用區域中的服務元件不會取得其他可用區域中元件的相依性。我們可以這樣做是因為區域服務具有區域資料平面。在某些情況下，例如 EC2，該服務還包括用於區域對齊操作的區域控制平面，例如啟動 EC2 執行個體。對於這些服務， AWS 還提供區域控制平面端點，以便於與服務互動。區域控制平面還提供區域範圍的功能，以及作為區域控制平面頂部的聚合和路由層。這顯示在下圖中。



區域隔離控制平面和資料平面的區域服務

可用區域讓客戶能夠操作比單一資料中心更具高可用性、容錯能力和可擴充性的生產工作負載。當工作負載使用多個可用區域時，客戶可以更好地隔離並避免影響單一可用區域實體基礎架構的問題。這有助於客戶建置跨可用區域備援的服務，如果架構正確，即使一個可用區域發生故障，仍可保持運作。客戶可以利用 AZI 建立高可用性和彈性的工作負載。在您的架構中實作 AZI 可協助您從隔離的可用區域故障中快速復原，因為您在一個可用區域中的資源可最小化或消除與其他可用區域中的資源互動。這有助於移除跨可用區域相依性，進而簡化可用區域疏散。如需建立可用區域撤離機制的詳細資訊，請參閱進階異地同步備份復原模式。此外，您可以遵循其自身服務 AWS 使用的一些相同的最佳作法，例如一次只將變更部署到單一可用區域，或者在可用區域中發生嚴重變更時，從服務中移除可用區域，以進一步利用可用區域。

靜態穩定性也是多可用區域架構的重要概念。您應該規劃使用多可用區域架構的故障模式之一是可用區域的遺失，這可能會導致可用區域的容量損失。如果您沒有預先佈建足夠的容量來處理可用區域的損失，這可能會導致剩餘的容量因目前的負載而不堪重負。此外，您將需要依賴用於替換損失容量的區域服務的控制平面，與靜態穩定的設計相比，可靠性較低。在這種情況下，預先佈建足夠的額外容量可協助您在不需要動態變更的情況下繼續正常作業，以防遺失容錯網域 (例如可用區域)，從而保持靜態穩定。

您可以選擇使用跨多個可用區域部署的 EC2 執行個體 auto 動調整規模群組，根據工作負載的需求動態擴展和擴展。自動縮放功能適用於在數分鐘到數十分鐘內逐漸變化的使用情況。但是，啟動新的 EC2 執行個體需要時間，尤其是在執行個體需要啟動載入時 (例如安裝代理程式、應用程式二進位檔案或組態檔)。在此期間，您剩餘的容量可能會因目前的負載而不堪重負。此外，透過 auto 擴展部署新執行

個體也依賴 EC2 控制平面。這提供了一個權衡：為了在單一可用區域遺失時保持靜態穩定，您需要在其他可用區域預先佈建足夠的 EC2 執行個體，以處理已從受損可用區域轉移出來的負載，而不是依賴 auto 擴展佈建新執行個體。不過，預先佈建額外容量可能會產生額外費用。

例如，在正常操作期間，假設您的工作負載需要六個執行個體來服務跨三個可用區域的客戶流量。為了在單一可用區域故障時保持靜態穩定，您需要在每個可用區域部署三個執行個體，總共九個執行個體。如果單一可用區域值的執行個體失敗，您仍然可以剩下六個，並且能夠繼續為客戶流量提供服務，而無需在故障期間佈建和設定新的執行個體。實現 EC2 容量的靜態穩定性需要額外的費用，因為在這種情況下，您會額外執行 50% 的執行個體。並非所有可預先佈建資源的服務都會產生額外費用，例如預先佈建 S3 儲存貯體或使用者。您將需要權衡實施靜態穩定性的任何權衡，以免超過工作負載所需的復原時間的風險。

AWS Local Zones 和 Outposts 使特定 AWS 服務的數據平面更接近最終用戶。這些服務的控制平面位於父區域中。在您建立本機區域或 Outposts 子網路的可用區域上，您的本機區域或 Outposts 執行個體將具有區域服務 (例如 EC2 和 EBS) 的控制平面相依性。他們也會依賴區域服務的區域控制平面，例如 Elastic Load Balancing (ELB)、安全群組和 Amazon Elastic Kubernetes Service (Amazon EKS) 受管 Kubernetes 控制平面 (如果您使用 EKS)。有關 Outposts 的其他特定信息，請參閱文檔以及支持和維護常見問題解答。使用 Local Zones 或 Outposts 時實現靜態穩定性，以幫助提高控制平面損傷或與父區域的網絡連接中斷的彈性。

區域服務

區域服務是 AWS 建立在多個可用區域之上的服務，因此客戶不必弄清楚如何充分利用區域服務。我們以邏輯方式將跨多個可用區域部署的服務組合在一起，向客戶呈現單一區域端點。Amazon SQS 和 Amazon DynamoDB 支援是區域服務的範例。他們使用可用區域的獨立性和備援，將基礎設施故障降到最低，因為可用性和耐久性風險。例如，Amazon S3 將請求和資料分散到多個可用區域，其設計目的是從可用區域的故障中自動復原。不過，您只能與服務的區域端點互動。

AWS 相信大多數客戶可以使用依賴區域服務的區域服務或異地同步備份架構，在單一區域實現其彈性目標。不過，某些工作負載可能需要額外的備援，而且您可以使用的隔離 AWS 區域 來建立多區域架構以達到 HA 或業務持續性目的。物理和邏輯之間的分離 AWS 區域 避免了它們之間的相關故障。換句話說，類似於您是 EC2 客戶，並且可以通過跨可用區域部署從可用區域的隔離中受益，您可以跨多個區域部署來獲得相同的區域服務優勢。這需要您為應用程式實作多區域架構，以協助您抵禦區域服務的損害。

不過，實現多區域架構的優點可能很困難；要利用區域隔離，而不是在應用程式層級撤銷任何事情，需要仔細的工作。例如，如果您要在區域之間容錯移轉應用程式，則需要在每個區域中保持應用程式堆疊之間的嚴格分隔、注意所有應用程式相依性，並將應用程式的所有部分一起容錯移轉。透過複雜的微服

務架構實現這一目標，該架構在應用程式之間具有許多相依性，需要在許多工程和業務團隊之間進行規劃和協調。允許個別工作負載做出自己的容錯移轉決策，使協調不那麼複雜，但是透過與單一區域內部相比，跨區域發生的延遲顯著差異來引入模態行為。

AWS 目前不提供同步跨區域複寫功能。跨區域使用非同步複寫的資料存放區 (由提供 AWS) 時，當您在區域之間容錯移轉應用程式時，可能會遺失資料或不一致。為了減少可能出現的不一致情況，您需要一個可靠的資料對帳程序，讓您有信心且可能需要在整個工作負載產品組合的多個資料存放區上進行操作，否則您必須願意接受資料遺失。最後，您需要練習容錯移轉，以便知道它可以在您需要時運作。在區域之間定期輪換您的應用程式以實踐容錯移轉是一項大量的時間和資源投資 如果您決定跨區域使用同步複寫的資料存放區來支援從多個區域同時執行的應用程式，則此類跨越 100 或 1000 英哩的資料庫的效能特性和延遲與在單一區域中運作的資料庫有很大的不同。這需要您從頭開始計劃應用程序堆棧以解釋此行為。這也會讓兩個區域的可用性成為硬性相依性，因此可能會降低工作負載的彈性。

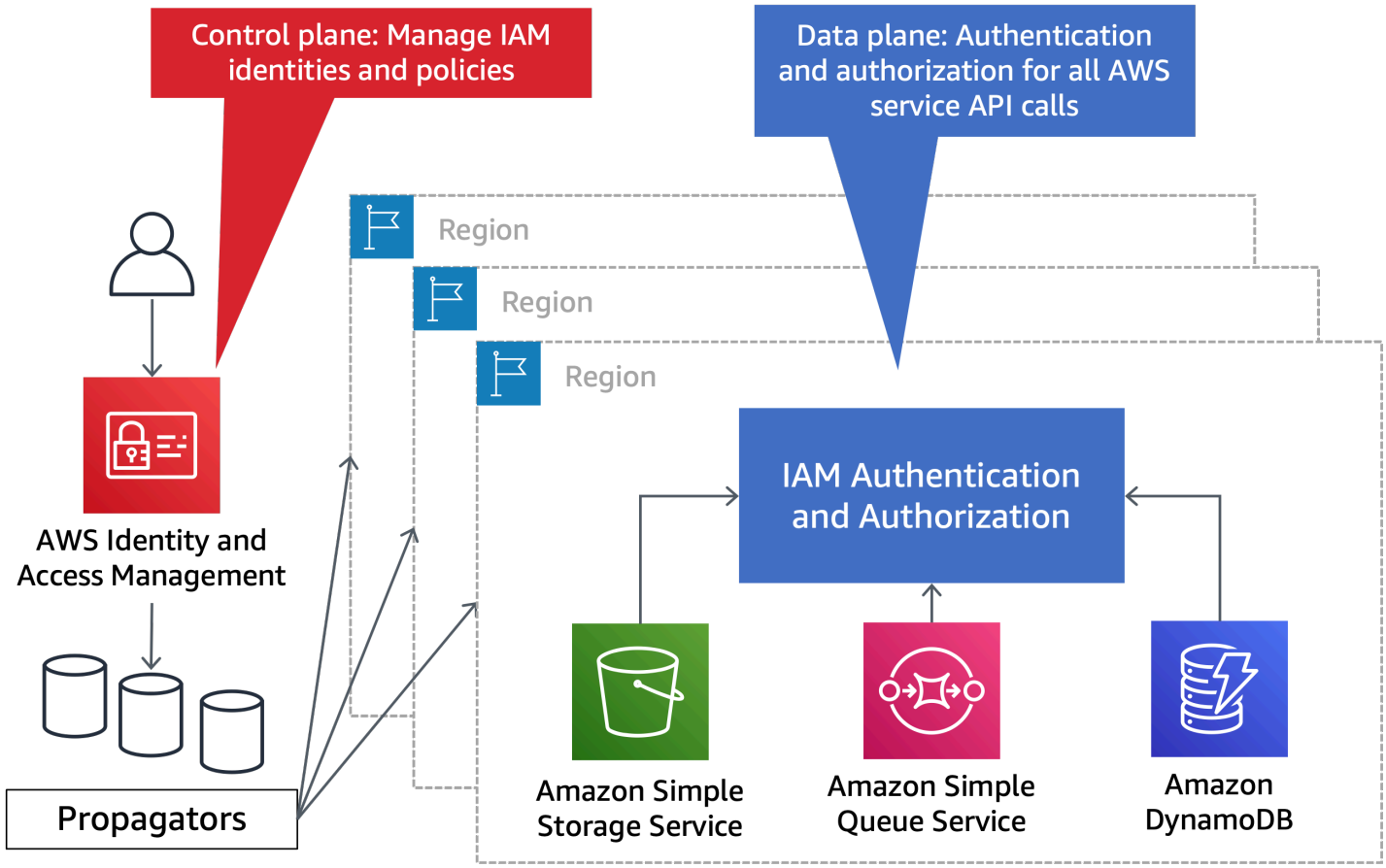
全球服務

除了區域和區域 AWS 服務外，還有一小組服 AWS 務，其控制平面和資料平面在每個區域中並不獨立存在。由於它們的資源不是特定於區域的，因此通常稱為全域資源。為了實現靜態穩定性，全球 AWS 服務仍然遵循分離控制平面和數據平面的傳統 AWS 設計模式。大多數全球服務的顯著差異在於它們的控制平面託管在一個單一的 AWS 區域，而資料平面則是全球分佈的。根據您選取的組態，有三種不同類型的全域服務和一組服務可能會顯示為全域。

以下各節將識別每種類型的全域服務，以及它們的控制平面和資料平面是如何分離的。您可以使用此資訊來指導如何建置可靠的高可用性 (HA) 和災難復原 (DR) 機制，而無需依賴全域服務控制平面。這種方法有助於移除架構中的單一故障點，並避免潛在的跨區域影響，即使您所在的區域與託管全域服務控制平面的地方不同。它也可協助您安全地實作不依賴全域服務控制平面的容錯移轉機制。

依分割區獨一無二的全域服務

某些全域 AWS 服務存在於每個分割區中 (在本 paper 中稱為部分服務)。分區服務在一個單 AWS 區域一的提供他們的控制平面。某些部分服務 (例如 AWS 網路管理員) 僅限控制平面，並協調其他服務的資料平面。其他部分服務 (例如 IAM) 都有自己的資料平面，這些資料平面會隔離並分散到分區 AWS 區域 中的所有資料平面。分區服務中的故障不會影響其他磁碟分割。在aws分割區中，IAM 服務的控制平面位於us-east-1區域中，分割區的每個區域都有隔離的資料平面。分割服務在和aws-cn分割區中也有獨立的控制平面aws-us-gov和資料平面。控制平面和 IAM 數據平面的分離示於下圖中。



IAM 具有單一控制平面和區域化資料平面

以下是分割服務及其控制平面在aws分割區中的位置：

- AWS IAM (us-east-1)
- AWS Organizations (us-east-1)
- AWS 帳戶管理 (us-east-1)
- Route 53 應用程序恢復控制器（ARCus-west-2）（ ）-此服務僅存在於aws分區中
- AWS 網路管理員 (us-west-2)
- 53 號路線私人域名 (us-east-1)

如果任何這些服務控制平面有可用性影響的事件，您可能無法使用這些服務提供的 CRUD 類型操作。因此，如果您的復原策略依賴於這些作業，則對控制平面或託管控制平面的區域產生可用性影響，將減少您成功復原的機會。 附錄 A-部分服務指引提供在復原期間移除全域服務控制平面相依性的策略。

建議

請勿在復原路徑中依賴部分服務的控制平面。而是仰賴這些服務的資料平面作業。如需有附錄 A-部分服務指引關如何設計分區服務的其他詳細資訊，請參閱。

邊緣網路中的全球服務

下一組全域 AWS 服務在aws分割區中有一個控制平面，並將其資料平面託管在全域存在點 (PoP) 基礎結構 (也可能也是 AWS 區域 如此)。託管在的數據平面 PoPs 可以從任何分區以及互聯網的資源訪問。例如，Route 53 在us-east-1區域中運作其控制平面，但其資料平面分佈在 PoPs 全球數百個以及每個區域 AWS 區域 (以支援區域內的 Route 53 公用和私有 DNS)。Route 53 健康狀態檢查也是資料平面的一部分，並從aws分割區 AWS 區域 中的八個執行。客戶可以使用 Route 53 公共託管區域從互聯網上的任何地方解析 DNS，包括其他分區 GovCloud，例如，以及從 V AWS irtual Private Cloud (VPC)（ VPC ）。以下是全域邊緣網路服務及其在aws分割區中的控制平面位置：

- 53 號路線公共網域名稱 (us-east-1)
- Amazon CloudFront （ us-east-1 ）
- AWS WAF 經典的 CloudFront （ us-east-1 ）
- AWS WAF 為 CloudFront （ us-east-1 ）
- Amazon Certificate Manager（ ACM ） CloudFront （ us-east-1 ）
- AWS Global Accelerator (AGA) (us-west-2)
- AWS Shield Advanced (us-east-1)

如果您對 EC2 執行個體或彈性 IP 地址使用 AGA 運作狀態檢查，這些檢查會使用 Route 53 運作狀態檢查 建立或更新 AGA 健康狀態檢查將取決於中的 Route 53 控制平面us-east-1。AGA 健康檢查的執行使用 Route 53 健康檢查資料平面。

在影響託管這些服務的控制平面的區域的故障，或影響控制平面本身的故障期間，您可能無法使用這些服務提供的 CRUD 類型操作。如果您已在復原策略中對這些作業採取相依性，則該策略成功的可能性可能會比僅依賴這些服務的資料平面來得低。

建議

請勿依賴復原路徑中邊緣網路服務的控制平面。而是仰賴這些服務的資料平面作業。如需有附錄 B-邊緣網路全球服務指南關如何在邊緣網路中設計全球服務的其他詳細資訊，請參閱。

全球單一區域營運

最終類別是由具有全域影響範圍的服務內的特定控制平面作業組成，而不是像先前類別那樣的整個服務。當您與所指定區域中的區域和區域服務互動時，某些作業會對單一區域具有與資源所在位置不同的基礎相依性。這些與僅在單一區域中提供的服務不同；如需這些服務附錄 C-單一區域服務的清單，請參閱。

在影響基礎全域相依性的失敗期間，您可能無法使用相依作業的 CRUD 類型動作。如果您已在復原策略中對這些作業採取相依性，則該策略成功的可能性可能會比僅依賴這些服務的資料平面來得低。針對復原策略，您應該避免與這些作業相依性。

以下是其他服務可能依賴的服務列表，這些服務具有全局範圍：

- 53 號幹線

  有數個 AWS 服務會建立提供資源特定 DNS 名稱的資源。例如，當您佈建 Elastic Load Balancer (ELB) 時，服務會針對 ELB 在 Route 53 中建立公用 DNS 記錄和健全狀況檢查。這取決於中的 Route 53 控制平面`us-east-1`。您使用的其他服務也可能需要佈建 ELB、建立公用 Route 53 DNS 記錄，或建立 Route 53 運作狀態檢查，做為其控制平面工作流程的一部分。例如，佈建 Amazon API 閘道 REST API 資源、Amazon Relational Database Service 服務 (Amazon RDS) 資料庫或亞馬遜 OpenSearch 服務網域，都會在路線 53 中建立 DNS 記錄。以下是其控制平面取決於中的 Route 53 控制平面`us-east-1`來建立、更新或刪除 DNS 記錄、託管區域和/或建立 Route 53 運作狀態檢查的服務清單。此清單並非詳盡無遺；它的目的是強調一些最常用的服務，其建立、更新或刪除資源的控制平面動作取決於 Route 53 控制平面：
  - 亞馬遜網關休息和 HTTP API
  - Amazon RDS 執行個體
  - Amazon Aurora 資料
  - Amazon ELB 負載平衡器
  - AWS PrivateLink VPC 端端
  - AWS Lambda 网址
  - Amazon ElastiCache
  - Amazon OpenSearch 服務
  - Amazon CloudFront
  - Amazon MemoryDB for Redis
  - Amazon Neptune
  - Amazon DynamoDB Accelerator (DAX)

- AGA
- Amazon Elastic Container Service (Amazon ECS) 與基於 DNS 的服務發現 (它使用 AWS Cloud Map API 來管理路由 53 DNS)
- Amazon EKS 庫伯爾尼特控制平面

  請務必注意，EC2 執行個體主機名稱的 VPC DNS 服務獨立存在於每個執行個體主機名稱中， AWS 區域 且不依賴於 Route 53 控制平面。在 VPC DNS 服務中為 EC2 執行個體 AWS 建立的記錄 (例如`ip-10-0-10.ec2.internal`、`ip-10-0-1-5.compute.us-west-2.compute.internal`、`i-0123456789abcdef.ec2.internal`、`i-0123456789abcdef.us-west-2.compute.internal`、和) 不依賴中的 Route 53 控制平面`us-east-1`。

  > **建議**
  >
  > 請勿依賴建立、更新或刪除需要在復原路徑中建立、更新或刪除 Route 53 資源記錄、託管區域或健康狀態檢查的資源。預先佈建這些資源 (例如 ELB)，以防止依賴復原路徑中的 Route 53 控制平面。

- Amazon Simple Storage Service (Amazon S3)

  下列 Amazon S3 控制平面操作在`aws`分割區`us-east-1`中具有基礎相依性。影響 Amazon S3 或其他服務的故障`us-east-1`可能會導致其他區域的這些控制平面動作受損：

```
PutBucketCors
DeleteBucketCors
PutAccelerateConfiguration
PutBucketRequestPayment
PutBucketObjectLockConfiguration
PutBucketTagging
DeleteBucketTagging
PutBucketReplication
DeleteBucketReplication
PutBucketEncryption
DeleteBucketEncryption
PutBucketLifecycle
DeleteBucketLifecycle
PutBucketNotification
PutBucketLogging
DeleteBucketLogging
```

```
PutBucketVersioning
PutBucketPolicy
DeleteBucketPolicy
PutBucketOwnershipControls
DeleteBucketOwnershipControls
PutBucketAcl
PutBucketPublicAccessBlock
DeleteBucketPublicAccessBlock
```

Amazon S3 多區域存取點 (MRAP) 的控制平面僅託管於該區域中，us-west-2並請求直接建立、更新或刪除 MRAP 以該區域為目標。MRAP 的控制平面在 MRAP 設定為提供內us-west-2容的每個區域中us-east-1，也有 AGA、路線 53 英寸和 ACM 的基本相依性。您不應該依賴 MRAP 控制平面在復原路徑或您自己系統資料層的可用性。這與 MRAP 容錯移轉控制不同，這些控制項用於為 MRAP 中的每個值區指定主動或被動路由狀態。這些 API 託管在五個中 AWS 區域，可用於使用服務的數據層有效轉移流量。

此外，Amazon S3 儲存貯體名稱是全域唯一的us-east-1，而且對CreateBucket和 DeleteBucket API 的所有呼叫都依賴於aws分割區中的名稱，以確保名稱的唯一性，即使 API 呼叫是針對您要建立儲存貯體的特定區域。最後，如果您有重要的值區建立工作流程，則不應依賴值區名稱的任何特定拼字的可用性，尤其是遵循可辨別模式的拼字。

> **建議**
>
> 請勿依賴刪除或建立新的 S3 儲存貯體或更新 S3 儲存貯體組態作為復原路徑的一部分。使用必要的組態預先佈建所有必要的 S3 儲存貯體，這樣您就不需要進行變更即可從故障中復原。這種方法也適用於 MRAP。

- CloudFront

  Amazon API Gateway 提供邊緣最佳化的 API 端點。建立這些端點取決於中的 CloudFront控制平面，us-east-1以便在閘道端點前面建立發佈。

  > **建議**
  >
  > 請勿依賴建立新的邊緣最佳化 API Gateway 端點做為復原路徑的一部分。預先佈建所有必要的 API Gateway 端點。

本節中討論的所有相依性都是控制平面動作，而不是資料平面動作。如果您的工作負載設定為靜態穩定，則這些相依性不會影響您的復原路徑，請記住，靜態穩定性需要額外的工作或服務才能實作。

使用預設全域端點的服務

在少數情況下， AWS 服務會提供預設的全域端點，例如 AWS 安全性權杖服務 (AWS STS)。其他服務可能會在其預設組態中使用此預設全域端點。這意味著您正在使用的區域服務可能對單個服務具有全局依賴性 AWS 區域。下列詳細資訊說明如何移除預設全域端點上的意外相依性，以協助您以地區方式使用服務。

AWS STS：STS 是一種 Web 服務，可讓您為 IAM 使用者或您驗證的使用者 (聯合身分使用者) 請求臨時、有限權限的登入資料。 AWS 軟體開發套件 (SDK) 和命令列介面 (CLI) 的 STS 使用預設為`us-east-1`. STS 服務也提供區域端點。依預設，這些端點會在預設啟用的區域中啟用。您可以依照下列指示設定 SDK 或 CLI，隨時利用這些功能：AWS STS 區域化端點。使用 SigV4a 也需要從地區 STS 端點要求的臨時登入資料。您無法使用全域 STS 端點進行此作業。

> **建議**
>
> 更新您的 SDK 和 CLI 組態以使用地區 STS 端點。

安全斷言標記語言（SAML）登錄：SAML 服務全部存在。 AWS 區域若要使用此服務，請選擇適當的地區 SAML 端點，例如 https://us-west-2.signin.aws.amazon.com/saml。您必須更新信任策略和身分識別提供者 (IdP) 中的組態，才能使用地區端點。如需特定詳細資訊，請參閱 AWS SAML 文件。

如果您使用的是也託管於的 IdP AWS，則在 AWS 失敗事件期間也可能會受到影響。這可能會導致您無法更新 IdP 組態，或者您可能無法完全同盟。如果您的 IdP 受損或無法使用，您應該預先佈建「防碎玻璃」用戶。如需如何以附錄 A-部分服務指引靜態穩定的方式建立防碎玻璃使用者的詳細資訊，請參閱。

> **建議**
>
> 更新您的 IAM 角色信任政策以接受來自多個區域的 SAML 登入。在失敗期間，如果偏好的端點受損，請更新您的 IdP 組態以使用不同的區域 SAML 端點。創建一個破碎玻璃用戶（s）的情況下，您的 IdP 受損或不可用。

AWS IAM 身分中心：身分識別中心是一種雲端服務，可讓您輕鬆集中管理客戶 AWS 帳戶 和雲端應用程式的單一登入存取。身分識別中心必須部署在您選擇的單一區域中。不過，服務的預設行為是使用託管於中us-east-1的全域 SAML 端點 (https://signin.aws.amazon.com/saml)。如果您已將身分識別中心部署到其他部署 AWS 區域，則應更新每個權限集的 relaystate URL，以將相同的地區主控台端點作為身分識別中心部署的目標。例如，如果您將身分識別中心部署到us-west-2，則應將權限集的轉送狀態更新為使用 https://us-west-2.console.aws.amazon.com。這會移除身分識別中心部署us-east-1中的任何相依性。

此外，由於 IAM 身分中心只能部署到單一區域，因此您應該預先佈建「防破」使用者，以防部署受損。如需如何以附錄 A-部分服務指引靜態穩定的方式建立防碎玻璃使用者的詳細資訊，請參閱。

> **建議**
>
> 在 IAM 身分中心中設定權限集的轉送狀態 URL，以符合部署服務的區域。如果您的 IAM 身分中心部署無法使用，請建立防漏使用者。

Amazon S3 儲存鏡頭：儲存鏡頭提供名為的預設儀表板 default-account-dashboard。儀表板組態及其關聯的指標會儲存在中us-east-1。您可以指定儀表板組態和指標資料的主區域，在其他區域建立其他控制面板。

> **建議**
>
> 如果在影響服務的故障期間需要來自預設 S3 Storage Lens 儀表板的資料us-east-1，請在備用本地區域建立其他儀表板。您也可以複製在其他區域中建立的任何其他自訂儀表板。

全球服務摘要

全球服務的資料平面採用與區域 AWS 服務類似的隔離和獨立原則。影響某個區域中 IAM 資料平面的故障不會影響另一個 AWS 區域區域中 IAM 資料平面的運作。同樣地，影響 PoP 中 Route 53 資料平面的失敗不會影響路由 53 資料平面在其餘部分的 PoPs操作。因此，我們必須考慮的是服務可用性事件，這些事件會影響控制平面運作或影響控制平面本身的區域。因為每個全域服務只有一個控制平面，因此影響該控制平面的失敗可能會對 CRUD 類型作業產生跨區域的影響 (這些作業通常用來設定或設定服務，而不是直接使用服務)。

建構工作負載以彈性方式使用全域服務的最有效方法是使用靜態穩定性。在故障情況下，將您的工作負載設計為不需要使用控制平面進行變更，以減輕影響或容錯移轉至不同位置。如需如何利用這些類型的全域服務，以移除控制平面相依性並消除單一故障點的規範性指引，請參閱和。附錄 A-部分服務

指引 附錄 B-邊緣網路全球服務指南如果您需要控制平面作業中的資料進行復原，請在可透過其資料平面存取的資料存放區中快取此資料，例如 AWS Systems Manager 參數存放區 (SSM 參數存放區) 參數、DynamoDB 表或 S3 儲存貯體。對於冗餘，您也可以選擇將該數據存儲在其他區域中。例如，遵循 Route 53 應用程式復原控制器 (ARC) 的最佳做法，您應該對五個區域叢集端點進行硬式編碼或書籤。在失敗事件期間，您可能無法存取某些 API 作業，包括未託管在極可靠資料平面叢集上的 Route 53 ARC API 作業。您可以使用 `DescribeCluster` API 作業列出路由 53 ARC 叢集的端點。

以下是一些最常見的錯誤配置或反模式的摘要，這些錯誤配置或反模式引入了對全局服務的控制平面的依賴關係：

- 變更 Route 53 記錄，例如更新 A 記錄的值或變更加權記錄集的權重，以執行容錯移轉。
- 在容錯移轉期間建立或更新 IAM 資源，包括 IAM 角色和政策。這通常不是故意的，但可能是未經測試的容錯移轉計劃的結果。
- 運營商依靠 IAM 身份中心在故障事件期間獲得生產環境的訪問權限。
- 當您將身分識別中心部署到不同區域`us-east-1`時，依賴預設的 IAM 身分中心組態來利用主控台。
- 變更 AGA 流量撥號權重以手動執行區域容錯移轉。
- 更新 CloudFront 發行版的來源組態，使其無法遠離受損的來源。
- 在故障事件期間佈建災難復原 (DR) 資源，例如 ELB 和 RDS 執行個體，這取決於在 Route 53 中建立 DNS 記錄。

以下是本節所提供有助於防止先前常見反模式的彈性方式使用全域服務的建議摘要。

推薦摘要

請勿在復原路徑中依賴部分服務的控制平面。而是仰賴這些服務的資料平面作業。如需有附錄 A-部分服務指引關如何設計分區服務的其他詳細資訊，請參閱。
請勿依賴復原路徑中邊緣網路服務的控制平面。而是仰賴這些服務的資料平面作業。如需有附錄 B-邊緣網路全球服務指南關如何在邊緣網路中設計全球服務的其他詳細資訊，請參閱。
請勿依賴建立、更新或刪除需要在復原路徑中建立、更新或刪除 Route 53 資源記錄、託管區域或健康狀態檢查的資源。預先佈建這些資源 (例如 ELB)，以防止依賴復原路徑中的 Route 53 控制平面。
請勿依賴刪除或建立新的 S3 儲存貯體或更新 S3 儲存貯體組態作為復原路徑的一部分。使用必要的組態預先佈建所有必要的 S3 儲存貯體，這樣您就不需要進行變更即可從故障中復原。這種方法也適用於 MRAP。
請勿依賴建立新的邊緣最佳化 API Gateway 端點做為復原路徑的一部分。預先佈建所有必要的 API Gateway 端點。

更新您的 SDK 和 CLI 組態以使用地區 STS 端點。
更新您的 IAM 角色信任政策以接受來自多個區域的 SAML 登入。在失敗期間，如果偏好的端點受損，請更新您的 IdP 組態以使用不同的區域 SAML 端點。創建破碎玻璃用戶的情況下，您的 IdP 受損或不可用。
在 IAM 身分中心中設定權限集的轉送狀態 URL，以符合部署服務的區域。如果您的身分識別中心部署無法使用，請建立防漏使用者。
如果在影響服務的故障期間需要來自預設 S3 Storage Lens 儀表板的資料`us-east-1`，請在備用本地區域建立其他儀表板。您也可以複製在其他區域中建立的任何其他自訂儀表板。

結論

AWS為錯誤隔離邊界提供了數種不同的結構。您應該考慮如何設計區域、區域和全球服務，以及對工作負載的潛在影響，以及工作負載在控制層損傷期間恢復的能力。靜態穩定性是您在使用AWS服務時避免控制平面相依性並建立可靠且有彈性的 HA 和 DR 機制的主要方法之一。

附錄 A-部分服務指引

對於部分服務，您應該實作靜態穩定性，以便在AWS服務控制平面損壞期間維持工作負載的彈性。以下提供了有關如何考慮部分服務的依賴性以及在控制平面障礙期間哪些將和可能不起作用的規定指導。

AWS Identity and Access Management (IAM)

AWS Identity and Access Management(IAM) 控制平面包含所有公用 IAM API (包括存取顧問，但不包括隨處存取分析器或 IAM 角色)。這包括`CreateRole`、、`AttachRolePolicy`和`ChangePassword`、`UpdateSAMLProvider`之類的動作`UpdateLoginProfile`。IAM 資料層為每AWS 區域個資料層中的 IAM 主體提供身份驗證和授權。在控制平面損害期間，IAM 的 CRUDL 類型操作可能無法運作，但現有主體的身份驗證和授權將繼續工作。STS 是一種僅限資料平面的服務，與 IAM 分開，不依賴於 IAM 控制平面。

這意味著，當您規劃 IAM 的依賴關係時，不應依賴恢復路徑中的 IAM 控制平面。例如，「break-glass」管理員使用者的靜態穩定設計是建立附加適當權限的使用者、設定密碼並佈建存取金鑰和秘密存取金鑰，然後將這些認證鎖定在實體或虛擬保存庫中。在緊急情況下需要時，請從 Vault 擷取使用者身分證明，並視需要使用它們。non-statically-stable設計是在失敗期間佈建使用者，或預先佈建使用者，但僅在需要時附加管理原則。這些方法取決於 IAM 控制平面。

AWS Organizations

AWS Organizations控制平面包含所有公用組 Organizations API `AcceptHandshake`、`AttachPolicy`，例如`CreateAccount`、`CreatePolicy`、和`ListAccounts`。沒有用於的資料平面AWS Organizations。它協調其他服務（例如 IAM）的數據平面。在控制平面減損期間，Organizations 的 CRUDL 類型作業可能無法運作，但服務控制政策 (SCP) 和標籤政策等政策將繼續運作，並作為 IAM 授權程序的一部分進行評估。Organizations 織支援的其他AWS服務中委派的管理員功能和多帳戶功能也會繼續運作。

這意味著，當您計劃依賴關係時AWS Organizations，您不應該依賴復原路徑中的「Organizations」控制平面。而是在恢復計劃中實現靜態穩定性。例如，一non-statically-stable種方法可能是更新 SCP 以移除AWS 區域透過`aws:RequestedRegion`條件允許的限制，或為特定 IAM 角色啟用管理員許可。這會依賴「Organizations」控制平面來進行這些更新。更好的方法是使用會話標籤來授予管理員權限的使用。您的身分識別提供者 (IdP) 可以包含可根據`aws:PrincipalTag`條件評估的工作階段標籤，這可協助您動態設定特定主體的權限，同時協助您的 SCP 保持靜態。這會移除控制平面的相依性，並僅使用資料平面動作。

AWS Account Management

AWS帳戶管理控制平面託管於 us-east-1 中，由所有用於管理的公用 API 組成AWS 帳戶，例如和。GetContactInformation PutContactInformation它還包括AWS 帳戶通過管理控制台創建或關閉新的。的 APICloseAccount，CreateAccountCreateGovCloudAccount，和DescribeAccount是AWS Organizations控制平面的一部分，這也託管在 us-東 1。此外，在以外的地方建立GovCloud帳戶AWS Organizations依賴 us-east-1 中的AWS 帳戶管理控制平面。此外，GovCloud帳戶必須是 1：1 鏈接到aws分區AWS 帳戶中的。在aws-cn分區中創建帳戶並不依賴 us-east-1。的資料平面AWS 帳戶就是帳戶本身。在控制面障礙期間，CRUD 類型的操作（例如創建新帳戶或獲取和更新聯繫信息）AWS 帳戶可能無法正常工作。IAM 政策中的帳戶參考仍會繼續運作。

這意味著，當您計劃對AWS帳戶管理的依賴關係時，您不應該依賴復原路徑中的帳戶管理控制平面。雖然帳戶管理控制平面不提供您通常會在復原情況下使用的直接功能，但有時候您可能會這麼做。例如，靜態穩定的設計是預先佈建容錯移轉所需的所有內AWS 帳戶容。設non-statically-stable計是在失敗事件AWS 帳戶期間建立新的，以託管 DR 資源。

Route 53 Application Recovery Controller

Route 53 ARC 的控制平面由用於復原控制和復原準備的 API 組成，如下所示：Amazon Route 53 應用程式復原控制器端點和配額。您可以使用控制平面來管理整備檢查、路由控制和叢集作業。ARC 的資料平面是您的復原叢集，它會管理 Route 53 健康狀態檢查所查詢的路由控制值，並實作安全規則。Route 53 ARC 的資料平面功能可透過復原叢集 API 來存取https://aaaaaaaa.route53-recovery-cluster.eu-west-1.amazonaws.com。

這意味著您不應該依賴於恢復路徑中的 Route 53 ARC 控制平面。有兩種最佳作法可協助實作此指引：

- 首先，將五個區域叢集端點加入書籤或硬式編碼。這樣就不需要在容錯移轉案例期間使用DescribeCluster控制平面作業來探索端點值。
- 其次，使用路由 53 ARC 叢集 API，方法是使用 CLI 或 SDK 來執行路由控制項的更新，而不是AWS Management Console. 這會移除管理主控台做為容錯移轉計畫的相依性，並確保它只依賴於資料平面動作。

AWS Network Manager

AWS網路管理員服務主要是控制平面唯一的系統，主控在美國西部 -2。其目的是跨區域和內部部署位置AWS 帳戶，集中管理您的AWS 雲端廣域網路 (WAN) 核心網路和 AWS Transit Gateway 網路的組態。它也會在 us-west-2 中彙總您的 Cloud WAN 指標，也可透過資料平面存取。CloudWatch如果網

路管理員受損，其所協調之服務的資料平面將不會受到影響。雲端 WAN 的CloudWatch指標也可在美國西部 -2 中使用。如果您想要歷史指標資料 (例如每個區域輸入和傳出的位元組)，以了解在影響 us-west-2 的故障期間或出於其他操作目的時可能轉移到其他區域的流量量，可以直接從CloudWatch主控台匯出這些指標為 CSV 資料，或使用以下方法：將 Amazon CloudWatch 指標發佈到 CSV 檔案。資料可以在`AWS/Network Manager`命名空間下找到，您可以根據您選擇的排程執行此操作，並將其存放在 S3 或您選取的其他資料存放區中。若要實作靜態穩定的復原計畫，請勿使用 AWS Network Manager 對網路進行更新，或依賴其控制平面作業中的資料進行容錯移轉輸入。

53 號路線私人域名

每個分割區都支援 Route 53 私人託管區域；但是，Route 53 中私有託管區域和公共託管區域的考量是相同的。請參閱附錄 B-邊緣網路全球服務指南中的 Amazon Route 53。

附錄 B-邊緣網路全球服務指南

對於邊緣網路全球服務，您應該實作靜態穩定性，以便在AWS服務控制平面損壞期間維持工作負載的彈性。

Route 53

Route 53 控制平面包含所有公用 Route 53 API，涵蓋託管區域、記錄、健康狀態檢查、DNS 查詢記錄、可重複使用的委派集、流量原則和成本分配標記的功能。它託管在 us-east-1。資料平面是權威 DNS 服務，橫跨 200 多個 POP 位置執行AWS 區域，根據託管區域和運作狀態檢查資料回答 DNS 查詢。此外，Route 53 具有用於運行狀態檢查的數據平面，該數據平面也是跨多個全球分佈的服務。AWS 區域此資料平面執行運作狀態檢查、彙整結果，並將其傳遞到 Route 53 公有和私有 DNS 和 AGA 的資料平面。在控制平面障礙期間，Route 53 的 CRUD 類型作業可能無法運作，但 DNS 解析和健康狀態檢查，以及因健康狀態檢查變更而導致的路由更新將繼續運作。

這表示，當您規劃 Route 53 上的相依性時，您不應該依賴復原路徑中的 Route 53 控制平面。例如，靜態穩定的設計是使用健康狀態檢查的狀態在區域之間執行容錯移轉，或撤除可用區域。您可以使用 Route 53 應用程式復原控制器 (ARC) 路由控制項，手動變更健全狀況檢查的狀態，並變更 DNS 查詢的回應。有類似於 ARC 提供的模式，您可以根據您的要求實現。其中一些模式概述在使用 Route 53 建立災難復原機制和進階異地同步備份復原模式健康狀態檢查斷路器部分。如果您選擇使用多區域 DR 計劃，請預先佈建需要建立 DNS 記錄的資源，例如 ELB 和 RDS 執行個體。non-statically-stable設計是透過 `ChangeResourceRecordSets` API 更新 Route 53 資源記錄的值、變更加權記錄的權重，或建立新記錄以執行容錯移轉。這些方法取決於 Route 53 控制平面。

Amazon CloudFront

Amazon CloudFront 控制平面包含CloudFront用於管理分發的所有公用 API，並在 us-east-1 中託管。資料平面是從邊緣網路中提供的PoPs散佈本身。它會執行來源內容的要求處理、路由和快取。在控制平面受損期間，CloudFront(包括無效驗證要求) 的 CRUD 類型作業可能無法運作，但是您的內容將會繼續快取並提供服務，並且原始容錯移轉將會繼續運作。

這意味著，當您計劃依賴關係時CloudFront，您不應該依賴恢復路徑中的CloudFront控制平面。例如，靜態穩定的設計是使用自動來源容錯移轉來減輕從損害到您其中一個來源的影響。您也可以選擇使用 Lamda @Edge 建立原始負載平衡或容錯移轉，請參閱使用 Amazon 的高可用性應用程式的三種進階設計模式和使用 Amazon CloudFront CloudFront 和 Amazon S3 建置多區域主動-主動式地理鄰近應用程式，以取得有關該模式的詳細資訊。一種non-statically-stable設計是手動更新發行版的配置以響應原始故障。這種方法將取決於CloudFront控制平面。

Amazon Certificate Manager

如果您在CloudFront散發中使用自訂憑證，您也會對 ACM 具有相依性。將自訂憑證與 us-east-1 區域CloudFront中的 ACM 控制平面使用 us-east-1 區域中的 ACM 控制平面。在控制平面受損期間，您在發行版中設定的現有憑證將繼續運作，以及自動憑證續約。請勿依賴變更散發的組態或建立新憑證做為復原路徑的一部分。

AWS網頁應用程式防火牆 (WAF) 和 WAF 典型

如果您AWS WAF與CloudFront發行版一起使用，則會依賴 WAF 控制平面，WAF 控制平面也託管在 us-east-1 區域中。在控制平面受損期間，設定的 Web 存取控制清單 (ACL) 及其相關規則會繼續運作。請勿依賴將 WAF Web ACL 更新為復原路徑的一部分。

AWS Global Accelerator

AGA 控制平面由所有公開的 AGA API 組成，並託管在美國西部 -2 中。資料平面是 AGA 提供給您註冊端點的任意傳播 IP 位址的網路路由。AGA 還使用 Route 53 運行狀態檢查來確定 AGA 端點的健康狀態，這是 Route 53 數據平面的一部分。在控制平面減損期間，AGA 的 CRUD 型操作可能無法正常工作。路由傳送至您現有的端點，以及用於將流量路由或轉移到其他端點和端點群組的現有運作狀態檢查、流量撥號和端點加權組態，將會繼續運作。

這意味著，當您計劃依賴 AGA 時，您不應該依賴恢復路徑中的 AGA 控制平面。例如，靜態穩定的設計是使用已設定的健全狀況檢查的狀態，以便遠離健康狀態不良的端點。如需此組態的範例，請參閱AWS使用AWS全域加速器中的〈部署多區域應用程式〉。non-statically-stable設計是在損害期間修改 AGA 流量撥號百分比、編輯端點群組或從端點群組移除端點。這些方法將取決於 AGA 控制平面。

Amazon Shield

亞馬遜 Shield 進階控制平面由所有公開 Shield 牌進階 API 組成，並託管於美國東部 -1。這包括功能 `CreateProtectionCreateProtectionGroup`，例如`AssociateHealthCheck`，`DesribeDRTAccess`，和`ListProtections`。數據層是由 Shield 高級提供的 DDoS 保護以及 Shield 高級指標的創建。Shield 進階也會使用 Route 53 健康狀態檢查 (這是 Route 53 資料平面的一部分)，如果您已設定這些檢查。在控制面障礙期間，Shield Advanced 的 CRUD 類型作業可能無法運作，但為您的資源設定的 DDoS 保護以及對運作狀態檢查變更的回應仍將繼續運作。

這意味著您不應該依賴恢復路徑中的 Shield 牌高級控制平面。雖然 Shield 進階控制平面無法提供您通常會在復原情況下使用的直接功能，但有時候您可能會這麼做。例如，靜態穩定的設計是將您的 DR 資

源設定為保護群組的一部分，並進行與其相關聯的健康狀態檢查，而不是在故障發生後設定該保護。這樣可以防止根據 Shield 牌進階控制平面進行恢復。

附錄 C-單一區域服務

以下是服務或該服務中的特定功能（列在服務名稱後面的括號中）的列表，這些功能僅在單一區域中可用。當您需要規劃其控制平面和資料平面上的相依性時，這些服務針對其他全域服務提供的實作靜態穩定性的相同指引也適用於這些服務。

- 企業版 Alexa
- AWS Marketplace(AWS Marketplace目錄 API、AWS Marketplace商務分析、AWS Marketplace權益服務)
- B@@ illing and Cost Management (AWS Cost Explorer、AWS成本與用量報表、AWS預算、Savings Plans)
- AWS BugBust
- Amazon Mechanical Turk
- Amazon Chime
- Amazon Chime 語音開發套件 (PSTN 音訊、簡訊、身分識別)
- AWSChatbot
- AWS DeepRacer
- AWSDevice Farm
- Amazon GameSparks
- Amazon Honeycode

貢獻者

本文件的貢獻者包括：

- 邁克爾·哈肯，首席解決方案架構師，Amazon Web Services

文件修訂

如要接收此白皮書更新的通知，請訂閱 RSS 摘要。

變更	描述	日期
次要修訂	更新了指南以符合 IAM 最佳實務。如需詳細資訊，請參閱 IAM 中的安全最佳實務。	2023 年 2 月 9 日
初始出版	白皮書已發佈。	2022 年 11 月 16 日

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。

注意

客戶有責任自行對本文件中的資訊進行獨立評估。本文件：(a) 僅供參考，(b) 代表目前的AWS產品供應項目和做法，如有變更，恕不另行通知，且 (c) 不會向其關聯公司、供應商或授權人建立任何承諾或保證。AWS AWS產品或服務係依「原狀」提供，不含任何明示或暗示之擔保、陳述或條件。客戶的責任和責任由AWS協議控制，本文件不屬於與客戶之間AWS的任何協議的一部分，也不會修改。AWS

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。