aws

開發人員指南

Amazon Route 53 Application Recovery Controller

Amazon Route 53 Application Recovery Controller: 開發人員指南

Table of Contents

什麼是 Route 53 弧？ 1
比較異地同步備份和多區域功能 3
異地同步備份復 5
區域轉移 5
區域轉移如何工作 6
AWS 區域 7
區域移位元件 10
資料與控制平面 12
定價 12
最佳實務 12
API 操作 14
使用 CLI 作業的範例 15
支援的資源 18
開始、更新或取消區域偏移 19
日誌記錄和監控 21
適用於區域轉移的 IAM 28
區域自動換檔 37
區域自動換檔的工作原理 38
關於區域自動換檔 43
AWS 區域 43
區域自動換檔組件 43
資料與控制平面 46
定價 46
最佳實務 47
API 操作 50
使用 CLI 作業的範例 51
啟用和使用區域自動換檔 56
日誌記錄和監控 59
身分和存取權管理 66
多區域復原 80
路由控制 80
關於路由控制 81
AWS 地區 82
元件 83

資料與控制平面 85
標記 86
定價 87
開始使用多區域復原 87
最佳實務 89
API 操作 91
使用 CLI 作業的範例 94
使用路由控制元件 110
日誌記錄和監控 126
身分和存取權管理 130
配額 143
準備檢查 143
什麼是準備檢查？ 144
AWS 地區 149
元件 150
資料與控制平面 152
標記 152
定價 153
設定彈性應用程式 153
最佳實務 154
API 操作 154
使用 CLI 作業的範例 156
使用復原群組和整備程度檢查 166
監控就緒狀態 170
取得架構建議 172
建立跨帳戶授權 173
整備規則、資源類型和 ARNS 175
日誌記錄和監控 192
身分和存取權管理 205
配額 218
程式碼範例 220
動作 220
GetRoutingControlState 220
UpdateRoutingControlState 223
安全 227
資料保護 227

靜態加密 228
傳輸中加密 228
身分和存取權管理 228
物件 229
使用身分驗證 229
使用政策管理存取權 232
Route 53 ARC 功能如何與 IAM 搭配使用 233
身分型政策範例 234
AWS 受管政策 234
故障診斷 239
日誌記錄和監控 241
法規遵循驗證 241
恢復能力 242
基礎架構安全 243
文件歷史紀錄 244
..... ccliv

什麼是 Amazon 路由 53 應用程序恢復控制器？

Amazon Route 53 應用程式復原控制器 (Route 53 ARC) 可協助您為上執行的應用程式做好準備並完成更快的復原作業 AWS。Route 53 ARC 提供兩組功能：多重可用區域 (AZ) 復原，包括區域移位和區域自動換檔，以及多區域復原，其中包括路由控制和整備檢查。使用 Route 53 ARC，您可以利用高可用性的復原工具，快速減輕影響多地區或異地同步備份應用程式的損傷。您也可以使用整備檢查，深入瞭解應用程式和資源是否已準備好進行復原。

AWS 全球雲端基礎架構提供容錯能力和復原能力，每個都 AWS 區域 由多個完全隔離的可用區域組成。Route 53 ARC 可在此 AWS 結構內運作，以協助您的應用程式具有彈性。

異地同步備份復

如果您有專為利用可用區域而建置的應用程式 AWS，您可以使用區域偏移快速隔離並從 AZ 損傷中復原。區域轉移可讓您暫時將受支援資源的流量從 AZ 移至運作良好的 AZ，從可用區域 (AZ) 減損中復原。 AWS 區域啟動區域轉移可協助您的應用程式快速復原，例如，從開發人員的錯誤程式碼部署或單一可用區域中的 AWS 損壞中復原。透過將流量移開，您可以在一個 AZ 中發生問題時，減少使用您應用程式的用戶端所造成的影響。

您可以針對「區域」中帳戶中任何支援的資源開始區域轉移。 AWS 服務會在 Route 53 ARC 中使用區域偏移自動註冊支援的 AWS 資源，以便您可以隨時開始區域偏移。

區域自動換檔是 Route 53 ARC 中的一項功能，您可以啟用授權 AWS 將流量從 AZ 轉移為代表您支援的資源，轉移到. AWS 區域 AWS 當內部遙測表明某個區域中的一個 AZ 有可能影響客戶的損害時，會啟動自動切換。內部遙測結合了來自多個來源 (包括 AWS 網路) 以及 Amazon EC2 和 Elastic Load Balancing 服務的指標。

區域移位和自動換檔是暫時的。當您開始手動區域班次時，您必須指定最多三天的 (可延伸) 到期日。如果您想繼續使流量遠離 AZ，可以更新區域轉移並設定新的到期日。使用區域自動切換，當指標顯示不再存在問題或潛在問題時 AWS 結束自動換檔。

若要深入瞭解這些功能，請參閱下列章節：

- Amazon Route 53 應用程序恢復控制器的區域轉移
- Amazon 路線 53 應用程序恢復控制器中的區域自動換檔

多區域復原

如果您有一個應用程式，您已經設計來運作另一個以 AWS 區域 繼續作業，您可以使用路由控制進行容錯移轉。路由控制可讓您在發生問題時容錯移轉流量，以確保應用程式保持可用狀態。 AWS 區域 路由控制包括安全規則，透過施加您定義的護欄，協助保護您免受意外結果的影響。使用這些規則，您可以確定一次只啟用並使用中的其中一個應用程式複本，例如作用中或待命複本。

對於多區域復原，Route 53 ARC 可以協助您容錯移轉 DNS 流 AWS 區域量。Route 53 ARC 中極為可靠的路由控制功能，可讓您將流量從受損區域重新路由至健康的區域，藉此復原應用程式。

透過整備檢查，Route 53 ARC 會持續監控 AWS 資源配額、容量和網路路由原則，並可以通知您有關會影響容錯移轉至複本和復原能力的變更。持續的整備程度檢查有助於確保您可以持續將多區域應用程式維護在調整和設定為處理容錯移轉流量的狀態。當您第一次設定 Route 53 ARC，以及在正常的應用程式作業期間，就緒檢查很有用。準備程度檢查不適用於事件期間容錯移轉的關鍵路徑中。

若要深入瞭解這些功能，請參閱下列章節：

- Amazon 路由 53 應用程式復原控制器中的路由
- Amazon 路線 53 應用程序恢復控制器中的準備

比較 Amazon Route 53 應用程式復原控制器的異地同步備份和多區域復原功能

Amazon Route 53 應用程式復原控制器中的區域移位、區域自動換檔和路由控制都可以實現快速復原，並協助您確保應用程式的彈性。 AWS 這些選項具有高可用性，可在應用程式延遲增加或可用性降低的情況下支援復原。這些選項可將流量從孤立的損傷中轉移出來，從而限制因受損而損失的影響和時間，從而協助快速復原應用程式。

路由控制主要集中在多個區 AWS 域 (多區域) 中的 AWS 應用程式，而區域移位和區域自動換檔僅支援使用異地同步備份應用程式為負載平衡器轉移流量。如本節所述，還有其他差異。

下表中的資訊包括區域偏移、區域自動換檔和路由控制的一些主要功能，以及選項之間的比較方式。這些說明可協助您進一步瞭解特定選項如何成為組織災難復原需求的最佳選擇。

路由控制	區域轉移	區域自動換檔
區域性 將流量從一個 AWS 區域重新路由到另一個區域（主要） 也可用於跨可用區域重新路由	區域 將流量從可用區域移開 流量會進入區域中的其他可用區域，而非特定目標	區域 將流量從可用區域移開 流量會進入區域中的其他可用區域，而非特定目標
需要設定 需要配置和設置	無需安裝即可 由支援的服務自動啟用 (目前 Network Load Balancer 和 Application Load Balancer)	需要練習運行設置 適用於支援的服務 (目前 Network Load Balancer 和 Application Load Balancer)
客戶啟動 客戶決定何時重新路由流量	客戶啟動 客戶決定何時開始區域偏移	AWS-啟動 AWS 代表您將應用程式流量從 AZ 轉移
基於收費 路由控制需要個別費用	包含在服務中 支援的負載平衡器包含建立區域轉移以將流量從 AZ 移開	包含在服務中

路由控制	區域轉移	區域自動換檔
		支援的負載平衡器包含啟動自動換檔以代表您將流量從 AZ 移開
不過期 流量可以無限期地重新路由至複本	臨時 所有區域班次必須設定為到期	臨時 AWS 開始和結束自動換檔

若要深入瞭解這些功能，請參閱下列章節：

- Amazon Route 53 應用程序恢復控制器的區域轉移
- Amazon 路線 53 應用程序恢復控制器中的區域自動換檔
- Amazon 路由 53 應用程式復原控制器中的路由

使用區域移位和區域自動切換來復原 Amazon Route 53 應用程式復原控制器中的應用程式

本節說明如何使用 Amazon Route 53 應用程式復原控制器中的功能，從可用區域 (AZ) 中的問題可靠地復原 AWS 應用程式。這些功能包括區域移位和區域自動切換，可暫時將流量從 AZ 移開，以取得 Elastic Load Balancing 資源，以縮短應用程式的復原時間。

區域轉移和區域自動換檔之間的主要區別在於，其中一個是您控制的手動交通轉移，另一個代表您自動將流量從減值中移開。

- 使用區域轉移時，您可以手動將受管理的 Elastic Load Balancing 資源的流量移至 AWS 區域 遠離可用區域。
- 使用區域自動切換，在活動期間，Elastic Load Balancing 流量會代表您自動從受損的 AZ 轉移到區域中健康的 AZ。

下列主題說明區域偏移和區域自動切換功能，以及如何使用這些功能。

主題

- Amazon Route 53 應用程序恢復控制器的區域轉移
- Amazon 路線 53 應用程序恢復控制器中的區域自動換檔

Amazon Route 53 應用程序恢復控制器的區域轉移

透過 Amazon Route 53 應用程式復原控制器中的區域轉移，您可以將 Elastic Load Balancing 資源的流量從中的可用區域移開 AWS 區域，以快速緩解問題並快速復原應用程式。請注意，Elastic Load Balancing 資源必須關閉跨區域負載平衡，才能使用此功能。

當您在一個區域中的多個 (通常是三個) AZ 中的負載平衡器上部署和執行 AWS 應用程式時，您可以透過啟動區域轉移，快速復原受損可用區域中的應用程式。將您的應用程式流量轉移到運作良好的 AZ，可減少因停電或硬體或軟體問題所造成的影響持續時間和嚴重程度。

您可能會選擇轉移流量，例如，因為錯誤的部署會造成延遲問題，或是因為可用區域受損。區域轉移不需要進階設定步驟，但您的 AWS 組態必須支援在沒有可用區域的情況下處理用戶端負載。支援的負載平衡器資源會自動向 Amazon Route 53 應用程式復原控制器註冊，因此您可以在需要時為負載平衡器啟動區域轉移。

啟動區域偏移不需要設置或配置。確保您有足夠的容量將流量從可用區域轉移出來之後，請選擇要移開的可用區域和要將流量轉移出去的資源，然後開始區域轉移。您可以隨時取消班次，讓流量開始返回可用區域。

所有區域轉移都是暫時緩解措施。您可以在開始區域輪班時設定初始到期時間，從一小時到三天 (72 小時)，如果您需要繼續流量轉移，則可以延長該到期時間。

請注意，在某些特定情況下，區域轉移不會轉移來自 AZ 的流量。如需區域偏移支援的更多資訊，請參閱支援區域移位和區域自動換檔的資源。

區域轉移如何工作

當您啟動負載平衡器資源的區域轉移時，資源的流量會從您指定的可用區域移開。若要開始轉換，Amazon Route 53 應用程式復原控制器請求負載平衡器運作狀態檢查，將可用區域設定為狀態不良，以使其運作狀態檢查失敗。運作狀態不良的運作狀態檢查會導致 Amazon Route 53 自動從 DNS 撤回資源的對應 IP 位址，以便從可用區域重新導向流量。新連線現在會路由到中的 AWS 區域 其他可用區域。

請務必注意，區域轉移不會以一般方式使用健康狀態檢查，其中健康狀態檢查會監控負載平衡器或應用程式的基礎健康狀態。相反地，Route 53 ARC 會使用健康狀態檢查做為將流量從可用區域移開的機制。此機制要求將健全狀況檢查明確設定為狀況不良，然後再次設定為狀況良好，以變更流量流量的方式。

流量開始轉移-當您在 Route 53 ARC 中開始區域轉移時，由於交通流量涉及的步驟，您可能看不到流量立即移出可用區域。視用戶端行為和連線重複使用情況而定，可用區域中的現有進行中連線也可能需要很短的時間才能完成。視您的 DNS 設定和其他因素而定，現有的連線可能會在幾分鐘內完成，或可能需要更長的時間。如需詳細資訊，請參閱確保流量轉移快速完成。

交通轉移結束-當區域轉移到期或您取消時，Route 53 ARC 採取措施停止轉移交通。它會反轉開始流量轉移的程序，並要求將 Route 53 健康狀態檢查再次設定為狀況良好。健康狀態檢查會導致還原原始區域 IP 位址。現在，復原的可用區域會再次包含在負載平衡器的路由中，流量會開始繼續流向 AZ。

您必須將所有區域班次設定為在開始班次時到期。您最初可以將區域轉移設定為最多三天 (72 小時) 到期。不過，您可以隨時更新區域偏移量，以設定新的到期日。如果您準備好將流量還原到可用區域，也可以在區域轉移到期之前取消該區域轉移。

當交通不轉移時

在一些特定的情況下，區域轉移不會轉移來自 AZ 的流量。例如，如果 AZ 中的負載平衡器目標群組沒有任何執行個體，或者所有執行個體運作狀態不良，則負載平衡器處於失敗開啟狀態。如果您在此案例中啟動負載平衡器的區域偏移，區域偏移不會變更負載平衡器使用的 AZ，因為負載平衡器已處於失敗

開啟狀態。這是預期的行為。如果所有 AZ 都無法打開（狀態不良），則區域轉移不能強制一個 AZ 不健康，並將流量轉移到區域中的其他 AZ。第二種情況是，如果您為中 AWS Global Accelerator的加速器端點的 Application Load Balancer 器啟動區域轉移。作為全域加速器中加速器端點的應用程式負載平衡器不支援區域轉移。

如需區域偏移支援的更多資訊，請參閱支援區域移位和區域自動換檔的資源。

AWS 區域 區域移位的可用性

如需 Amazon Route 53 應用程式復原控制器的區域支援和服務端點的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器端點和 Amazon Web Services 一般參考中的配額。

區域移位目前可在此處 AWS 區域 列出。中國地區（即中國（北京）地區和中國（寧夏）地區也可以使用區域轉移。

區域名稱	區域	端點	通訊協定
美國東部 (俄亥俄)	us-east-2	arc-zonal-shift.us-east-2.amazonaws.com	HTTPS
美國東部 (維吉尼亞北部)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
美國西部 (奧勒岡)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
非洲 (開普敦)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
亞太區域 (香港)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
亞太區域 (海德拉巴)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS

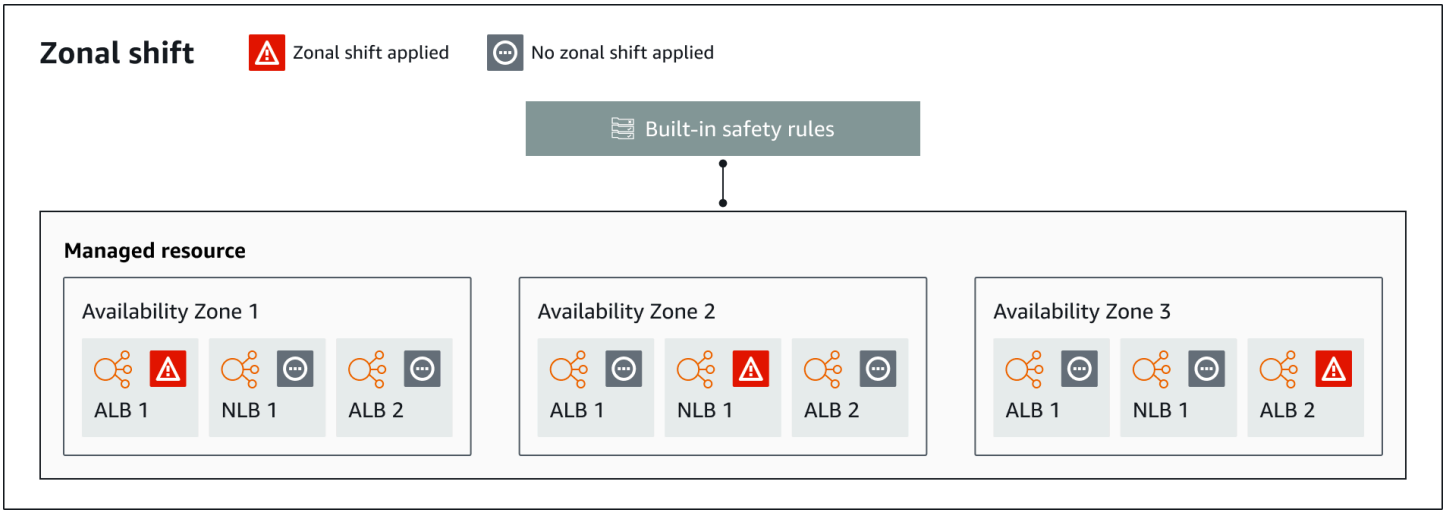
區域名稱	區域	端點	通訊協定	
亞太區域 (雅加達)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS	
亞太區域 (墨爾本)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com	HTTPS	
亞太區域 (孟買)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com	HTTPS	
亞太區域 (大阪)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com	HTTPS	
亞太區域 (首爾)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com	HTTPS	
亞太區域 (新加坡)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com	HTTPS	
亞太區域 (雪梨)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS	
亞太區域 (東京)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS	
加拿大 (中部)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS	
加拿大西部 (卡加利)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS	
歐洲 (法蘭克福)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS	

區域名稱	區域	端點	通訊協定	
歐洲 (愛爾蘭)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS	
歐洲 (倫敦)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS	
歐洲 (米蘭)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS	
歐洲 (巴黎)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS	
歐洲 (西班牙)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS	
歐洲 (斯德哥爾摩)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS	
歐洲 (蘇黎世)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS	
以色列 (特拉維夫)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS	
中東 (巴林)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS	
中東 (阿拉伯聯合大公國)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS	
南美洲 (聖保羅)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	HTTPS	

區域名稱	區域	端點	通訊協定	
AWS GovCloud (美國東部)	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS	
AWS GovCloud (美國西部)	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS	

區域移位元件

下圖說明區域轉移將流量從可用區域轉移的範例 AWS 區域。區域移位中內建的檢查可防止您在資源已有作用中的班次時啟動另一個區域偏移。



以下是 Route 53 ARC 中區域偏移能力的組成部分。

區域轉移

您可以針對 AWS 帳戶中的受管理資源開始區域轉移 AWS 區域，以暫時將流量從區域中的可用區域移至區域中運作良好的 AZ，以便快速從一個 AZ 中的問題中復原。目前，您只能針對未設定跨區域負載平衡的網路負載平衡器和應用程式負載平衡器啟動區域偏移。支援的負載平衡器會在 Route 53 ARC 中為您自動註冊。

內建安全檢查

Route 53 ARC 中內建的檢查可防止資源的多個流量轉移一次生效。也就是說，只有一個客戶啟動的區域轉移、練習執行區域轉移或資源自動換檔，才能主動將流量從可用區域轉移出來。例如，如果您在資源目前使用自動切換移位時啟動該資源的區域偏移，則您的區域偏移優先。如需詳細資訊，請參閱練習執行的結果Amazon 路線 53 應用程序恢復控制器中的區域自動換檔和結果。

資源識別符

要包含在區域移位中的資源識別碼。識別碼是資源的 Amazon 資源名稱 (ARN)。

對於區域轉移，您只能為 Route 53 ARC 支援的 AWS 服務選擇帳戶中的資源。這些 AWS 服務中支援的資源會由服 AWS 務自動向 Route 53 ARC 註冊。

> **Note**
>
> 目前，您只能在關閉跨區域負載平衡的情況下啟動網路負載平衡器和應用程式負載平衡器的區域轉移。

受管資源

AWS 服務使用 Route 53 ARC 自動註冊資源以進行區域移位。已註冊的資源是 Route 53 ARC 中的受管理資源。

資源名稱

您可以為區域偏移指定的 Route 53 ARC 中的資源名稱。

狀態（區域偏移狀態）

區域偏移的狀態。對`Status`於區域偏移，可以具有下列其中一個值：

- 活動：區域偏移已開始並處於活動狀態。
- 已過期：區域偏移已過期（超過到期時間）。
- 已取消：區域移位已取消。

已套用狀態

套用狀態會指出資源的工作班次是否有效。具有狀態的轉移`APPLIED`決定了可用區域，其中應用程式流量已移走資源，以及該班次何時結束。

到期時間（到期時間）

區域偏移的到期時間（到期時間）。區域轉移是暫時的。對於客戶啟動的區域班次，您可以一開始將區域班次設定為使用中最多三天 (72 小時)。

當您開始區域偏移時，您可以指定要使其處於活動狀態的時間長度，Route 53 ARC 將其轉換為到期時間（到期時間）。您可以取消客戶啟動的區域轉移，例如，如果您已準備好將流量還原到可用區域。或者，您也可以透過更新以指定其他到期時間長度來延長客戶啟動的區域偏移量。

您可以取消客戶啟動的區域班次和區域班次，以區域自動班次為練習執行 AWS 開始。

區域偏移的資料和控制平面

當您規劃容錯移轉和災難復原時，請考慮容錯移轉機制的彈性。我們建議您確保在容錯移轉期間所依賴的機制具有高可用性，以便在災難情況下需要時可以使用它們。一般而言，您應該隨時為您的機制使用資料平面函數，以獲得最大的可靠性和容錯能力。考慮到這一點，重要的是要了解服務的功能如何在控制平面和數據平面之間劃分，以及何時可以依賴服務數據層面對極高可靠性的期望。

與大多數 AWS 服務一樣，控制平面和數據平面支持區域移位功能的功能。雖然這兩者都是為了可靠而建置，但控制平面已針對資料一致性進行了最佳化，而資料平面則針對可用性進行最佳化。資料平面是專為復原而設計的，因此即使在中斷性事件期間，控制平面可能無法使用時，也能維持可用性。

一般而言，控制平面可讓您執行基本的管理功能，例如建立、更新和刪除服務中的資源。資料平面提供服務的核心功能。

如需有關資料平面、控制平面以及如何 AWS 建置服務以符合高可用性目標的詳細資訊，請參閱 Amazon Builders' Library 中的使用可用區域的靜態穩定性 paper。

Amazon Route 53 應用程式復原控制器中區域轉移的定價

對於區域轉移，您可以針對支援的資源啟動區域轉移，以從可用區域中的問題中復原應用程式。使用區域移位不收取額外費用。

您只需為您在 Amazon Route 53 應用程式復原控制器中使用的部分付費。如需 Route 53 ARC 的詳細定價資訊和定價範例，請參閱 Amazon Route 53 定價，然後向下捲動至 Amazon Route 53 應用程式復原控制器。

Route 53 ARC 中區域變化的最佳實踐

我們建議在 Route 53 ARC 中使用區域轉移進行異地同步備份復原的最佳實務。區域轉移通常會從即時應用程式中移除容量，因此在生產環境中使用時請務必小心。

主題

- 容量規劃和預先擴充
- 限制用戶端保持連線至端點的時間
- 事先測試開始區域偏移
- 確保所有可用區域的健康狀況良好並吸收流量
- 使用資料平面 API 作業進行災難復原
- 僅暫時以區域轉移移動流量

容量規劃和預先擴充

確定您已規劃且已預先調整規模或可以自動調整規模的足夠容量，以容納啟動區域轉移時強加在可用區域上的額外負載。使用復原導向架構，典型的建議是預先調整運算容量，以包含足夠的成長空間，以便在三個複本中的其中一個 (通常) 離線時為尖峰流量提供服務。

例如，當您針對單一負載平衡器資源啟動區域轉移時，會暫時從負載平衡器後方移除一個可用區域的容量。根據您啟動的區域轉移以及負載平衡器的設定方式而定，您必須確定已仔細規劃管理剩餘可用區域上增加的負載。

限制用戶端保持連線至端點的時間

當 Amazon Route 53 應用程式復原控制器將流量從損害轉移出來時 (例如，使用區域移位或區域自動切換)，Route 53 ARC 用來移動應用程式流量的機制就是 DNS 更新。DNS 更新會導致所有新連線導向遠離受損位置。

但是，具有預先存在開啟連線的用戶端可能會繼續對受損位置發出要求，直到用戶端重新連線為止。為確保快速復原，我們建議您限制用戶端保持連線至端點的時間長度。

如果您使用應用程式負載平衡器，則可以使用`keepalive`此選項來設定連線持續的時間長度。如需詳細資訊，請參閱應用 Application Load Balancer 使用指南中的 HTTP 用戶端保持活動持續時間

根據預設，應用程式負載平衡器會將 HTTP 用戶端保持作用持續時間值設定為 3600 秒或 1 小時。我們建議您降低與應用程式復原時間目標內嵌的值，例如 300 秒。當您選擇 HTTP 用戶端 keepalive 持續時間時間時，請考慮這個值是一般而言，更頻繁地重新連線之間的權衡，這可能會影響延遲，並且更快速地將所有用戶端從受損的 AZ 或區域移開。

事先測試開始區域偏移

透過啟動區域變更，定期測試從應用程式可用區域移出的流量。規劃並執行起始區域轉移 (最好在測試和生產環境中)，作為定期容錯移轉測試的一部分，以便在發生災難時復原應用程式。定期測試是確保您已做好準備，並有信心在操作事件發生時緩解問題的關鍵部分。

確保所有可用區域的健康狀況良好並吸收流量

區域輪班的工作方式是將資源 (即應用程式複本) 標記為可用區域中的狀況不良。這表示，確保應用程式之負載平衡器中的目標通常狀況良好且主動在某個區域中的可用區域中接收流量至關重要。我們建議您使用儀表板來追蹤此情況，包括例如，狀態不良目標的「Elastic Load Balancing」測量結果，以及「每個可用區域處理的 BytesExduction」。

考慮從第二個相鄰區域監控資源的健康狀態。這種方法的優點在於它可以更能代表您的最終用戶體驗，並且還可以降低應用程序和監視同時受到相同災難影響的風險 (「共同命運」)。

使用資料平面 API 作業進行災難復原

若要在需要快速復原應用程式時啟動區域轉移，但相依性很少，我們建議您在可能的情況下使用具有區域移位動作的 AWS Command Line Interface 或 API，並使用預先儲存的認證。您也可以在中啟動區域偏移 AWS Management Console，以便於使用。但是，當快速、可靠的復原至關重要時，資料平面作業是更好的選擇。如需詳細資訊，請參閱區域偏移 API 參考指南。

僅暫時以區域轉移移動流量

區域轉移會暫時將流量從可用區域移開，以減輕損害。您應該在採取動作修正問題後，立即將應用程式的資源還原為服務。如此可確保您的整體應用程式會還原至原始的完全備援、彈性狀態。

區域移位 API 作業

下表列出您可以使用區域轉移使用的 Route 53 ARC API 作業，這些作業會將流量從異地同步備份應用程式的可用區域移開。此表格也包含相關文件的連結。

如需如何搭配使用常用區域移位 API 作業的範例 AWS Command Line Interface，請參閱使用 AWS CLI 帶區域偏移的範例。

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
啟動區域轉移	請參閱開始區域移位	請參閱StartZonal班次
更新區域轉移	請參閱更新或取消區域偏移	請參閱UpdateZonal班次

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
列出區域位移	請參閱Amazon Route 53 應用程序恢復控制器的區域轉移	請參閱ListZonal班次
列出受管資源	請參閱支援區域移位和區域自動換檔的資源	查看ListManaged資源
取得受管理資源	請參閱支援區域移位和區域自動換檔的資源	請參閱GetManaged資源
取消區域轉移	請參閱更新或取消區域偏移	請參閱CancelZonal班次

使用 AWS CLI 帶區域偏移的範例

本節 AWS Command Line Interface 將逐步介紹使用區域移位的簡單應用程式範例，並使用使用 API 操作的 Amazon Route 53 應用程式復原控制器中的區域轉移功能。這些範例旨在協助您深入了解如何使用 CLI 處理區域偏移。

Route 53 ARC 中的區域轉移可讓您暫時將支援資源的流量從可用區域移開，以便您的應用程式可以繼續與. AWS 區域區域移位目前支援網路負載平衡器和應用程式負載平衡器，且跨區域負載平衡已關閉。

讓我們來看看使用 AWS Command Line Interface. 您也可以使用 AWS CLI 更新區域偏移量，例如，設定新的到期時間。所有區域輪班都是臨時的，最初必須設置為在三天內到期。不過，您可以稍後更新區域偏移量，以設定新的到期日。

若要取得有關使用的更多資訊 AWS CLI，請參閱《AWS CLI 指令參考》。如需區域轉移 API 動作的清單以及詳細資訊的連結，請參閱區域移位 API 作業。

開始區域偏移

您可以使用`start-zonal-shift`指令使用 CLI 啟動區域偏移。

```
aws arc-zonal-shift start-zonal-shift \
      --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890" \
      --away-from="usw2-az1" \
      --expires-in="5m" \
      --comment="Shifting traffic away from USW2-AZ1"
```

```
{
   "zonalShiftId": "2222222-3333-444-1111",
   "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
   "awayFrom": "usw2-az1",
   "expiryTime": 2022-11-14T01:40:42+00:00,
   "startTime": 2022-11-14T01:35:42+00:00,
   "status": "ACTIVE",
   "comment": "Shifting traffic away from USW2-AZ1"
}
```

取得受管理資源

您可以使用get-managed-resource命令，透過 CLI 取得有關受管理資源的資訊。

```
aws arc-zonal-shift get-managed-resource \
   --resource-identifier="arn:aws:testservice::111122223333:ExampleALB123456890
```

```
{
    "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "name": "TestResource",
    "appliedWeights": {
        "usw2-az1": 1.0,
        "usw2-az2": 1.0,
        "usw2-az3": 1.0
    },
    "zonalShifts": []
}
```

列出受管資源

您可以使用list-managed-resources命令使用 CLI 列出帳戶中的受管資源。

```
aws arc-zonal-shift list-managed-resources
```

```
{
    "items": [
        {
            "arn": "arn:aws:testservice::111122223333:ExampleALB123456890",
            "name": "TestResource",
            "availabilityZones": [
                "usw2-az1",
```

```
                "usw2-az2",
                "usw2-az3"
            ]
        }
    ]
}
```

列出區域位移

您可以使用`list-zonal-shifts`命令使用 CLI 列出帳戶中的區域變化。

```
aws arc-zonal-shift list-zonal-shifts
```

```
{
    "items": [
        {
            "zonalShiftId": "2222222-3333-444-1111",
            "resourceIdentifier":
 "arn:aws:testservice::111122223333:ExampleALB123456890",
            "awayFrom": "usw2-az1",
            "expiryTime": 2022-11-15T09:10:42+00:00,
            "startTime": 2022-11-13T01:35:42+00:00,
            "status": "ACTIVE",
            "comment": "Shifting traffic away from USW2-AZ1"
        }
    ]
}
```

更新區域偏移

您可以使用`update-zonal-shift`指令使用 CLI 更新區域偏移。

```
aws arc-zonal-shift update-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890" \
   --expires-in="1h" \
   --comment="Still shifting traffic away from USW2-AZ1"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
```

```
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "ACTIVE",
    "comment": "Still shifting traffic away from USW2-AZ1"
}
```

取消區域位移

您可以使用cancel-zonal-shift指令使用 CLI 取消區域偏移。

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2022-11-15T10:35:42+00:00,
    "startTime": 2022-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Shifting traffic away from USW2-AZ1"
}
```

支援區域移位和區域自動換檔的資源

Amazon Route 53 應用程式復原控制器目前支援區域移位和區域自動換檔的下列資源：

- Network Load Balancer
- Application Load Balancer

支援的負載平衡資源會自動註冊 Route 53 ARC，因此您可以將它們與區域偏移 (和區域自動切換) 搭配使用。您可以在 Elastic Load Balancing 控制台（大多數情況下 AWS 區域）或 Route 53 ARC 中為負載平衡器啟動區域偏移。

檢閱下列條件，以便在 Route 53 ARC 中使用區域轉移和資源：

- 跨區域負載平衡不支援區域偏移。對於要向 Route 53 ARC 註冊的負載平衡器，請確定您已在 Elastic Load Balancing 中關閉負載平衡器的跨區域負載平衡。
- 在一些特定的情況下，區域轉移不會轉移來自 AZ 的流量。例如，如果 AZ 中的負載平衡器目標群組沒有任何執行個體，或者所有執行個體運作狀態不良，則負載平衡器處於失敗開啟狀態，而且您無法移開其中一個 AZ。

- 同時支援公用和內部 (私人) 網路負載平衡器和應用程式負載平衡器。
- 資源必須處於作用中狀態且完全佈建，才能轉移其流量。在開始資源的區域轉移之前，請檢查以確保它是 Route 53 ARC 中的受管理資源。例如，您可以檢視中受管理資源的清單 AWS Management Console，或者您可以將`get-managed-resource`作業與資源的識別碼搭配使用。
- 作為中加速器端點的應用程式負載平衡器不支援區域移位。 AWS Global Accelerator
- 當應用程式負載平衡器是 Network Load Balancer 的目標時，請從 Network Load Balancer 啟動區域轉移。如果您從 Application Load Balancer 啟動區域轉移，Network Load Balancer 不會停止向 Application Load Balancer 及其目標傳送流量。
- 區域轉移的資源必須是已由 AWS 服務向 Route 53 ARC 註冊的受管資源。在關閉跨區域負載平衡的情況下，Elastic Load Balancing 會自動註冊 Route 53 ARC 網路負載平衡器和應用程式負載平衡器。
- 若要使用資源開始區域轉移，它必須部署在可用區域中，以及您開始工作班次的位 AWS 區域 置。確保您在轉移的 AZ 所在的相同區域中開始區域轉移，並且您要轉移流量的資源也位於相同的 AZ 和區域。
- 確保您擁有正確的 IAM 許可，以便將區域轉移與資源搭配使用。如需詳細資訊，請參閱 區域轉移的 IAM 和許可。

開始、更新或取消區域偏移

本節提供了使用區域偏移的程序，包括開始區域偏移和取消區域偏移。

開始區域移位

本節中的步驟說明如何在 Amazon Route 53 應用程式復原控制器主控台上啟動客戶啟動的區域轉移。若要以程式設計方式使用區域偏移，請參閱區域移位 API 參考指南。

除了在 Route 53 ARC 中開始區域轉移之外，您還可以在 Elastic Load Balancing 控制台（在支持的區域中）中為負載平衡器啟動區域偏移。如需詳細資訊，請參閱 Elastic Load Balancing 使用指南中的區域偏移。

開始區域偏移的步驟

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域偏移。
3. 在「區域偏移量」頁面上，選擇「開始區域偏移量」。

4. 選取要將流量移出的可用區域。
5. 從「資源」表格中選取要將流量移開的負載平衡器。
6. 在「設定區域工作班次到期時間」中，選擇或輸入區域工作班次的到期日。區域偏移最初可以設定為使用 1 分鐘或最多三天 (72 小時)。

   所有區域轉移都是暫時的。您必須設定到期日，但您可以稍後更新作用中的班次，以設定最多三天的新到期期限。
7. 輸入註解。如果您想要的話，您可以稍後更新區域轉移以編輯註釋。
8. 選取此核取方塊以確認啟動區域轉移會將流量從可用區域移開，以減少應用程式的可用容量。
9. 選擇 開始使用。

更新或取消區域偏移

本節中的步驟說明如何在 Amazon Route 53 應用程式復原控制器主控台上更新啟動的區域轉移或取消區域轉移。若要以程式設計方式使用區域偏移，請參閱區域移位 API 參考指南。

您可以更新區域偏移量以設定新的到期日，或編輯或取代區域偏移量的註解。您可以在區域偏移到期前隨時取消。

您可以取消您啟動的區域班次，或針對區域自動班次的練習執行，取消為資源 AWS 開始的區域工作班次。若要進一步瞭解區域自動切換中的練習班次，請參閱。區域自動換檔和練習運行如何工作

更新區域偏移

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域偏移。
3. 選取您要更新的區域偏移量，然後選擇 [更新區域偏移量]。
4. 針對設定區域轉移到期日，選擇性選取或輸入到期日。
5. 針對註解，選擇性編輯現有註解或輸入新註解。
6. 選擇更新。

取消區域偏移

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。

2. 在異地同步備份下，選擇區域偏移。
3. 選取您要取消的區域偏移量，然後選擇「取消區域偏移量」。
4. 在確認強制回應對話方塊中，選擇確認。

記錄和監控 Amazon Route 53 應用程式復原控制器中的區域轉移

您可以使用 AWS CloudTrail 和 Amazon 監控 Amazon EventBridge Route 53 應用程式復原控制器中的區域變化，以分析模式並協助疑難排解問題。

主題

- 使用記錄區域移位 API 調用 AWS CloudTrail
- 與 Amazon 一起使用區域移位 EventBridge

使用記錄區域移位 API 調用 AWS CloudTrail

Amazon Route 53 應用程式復原控制器的區域轉移與整合 AWS CloudTrail，該服務可提供 Route 53 ARC 中使用者、角色或 AWS 服務所採取動作的記錄。 CloudTrail 將區域移位的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Route 53 ARC 主控台的呼叫，以及針對區域移位的 Route 53 ARC API 作業的程式碼呼叫。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括區域轉移的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 Route 53 ARC 進行區域轉移的要求、提出請求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

區域偏移信息 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當在 Route 53 ARC 中針對區域移位發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄。

對於正在進行的事件記錄 AWS 帳戶，包括 Route 53 ARC 中區域轉移的事件，請創建一條路線。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的

Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 Route 53 ARC 動作都由記錄下來， CloudTrail 並記錄在 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南中。例如，呼叫`StartZonalShift`和動`ListManagedResources`作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

在事件歷史記錄中查看 Route 53 ARC 事件

CloudTrail 可讓您在事件歷史記錄中檢視最近的事件。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。

瞭解區域移位記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範區域位移`ListManagedResources`動動作的 CloudTrail 記錄項目。

```
{
      "eventVersion": "1.08",
      "userIdentity": {
```

```
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

下列範例顯示的 CloudTrail 記錄項目會示範區域偏移發生衝突例外狀況的`StartZonalShift`動作。

```
{
      "eventVersion": "1.08",
```

```
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:10:38Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "StartZonalShift",
     "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "errorCode": "ConflictException",
      "errorMessage": "There's already an active zonal shift for that resource
 identifier: 'arn:aws:testservice:us-west-2:077059137270:testResource/456apples'.
 Active zonal shift: 'bac23b74-176e-c073-de8f-484ca508910f'",
      "requestParameters": {
        "resourceIdentifier": "arn:aws:testservice:us-
west-2:077059137270:testResource/456apples",
        "awayFrom": "usw2-az1",
        "expiresIn": "2m",
        "comment": "HIDDEN_FOR_SECURITY_REASONS"
      },
      "responseElements": null,
      "requestID": "OP4OYXZ54HUPMIPGWH_EXAMPLE",
      "eventID": "0bca6660-e999-43a5-9008-EXAMPLE",
      "readOnly": false,
      "eventType": "AwsApiCall",
```

```
    "managementEvent": true,
    "recipientAccountId": "111122223333"
    "eventCategory": "Management"
    }
  }
```

與 Amazon 一起使用區域移位 EventBridge

使用 Amazon EventBridge，您可以設定事件驅動的規則，以監控區域轉移資源並啟動使用其他服務的目標動作。 AWS 例如，您可以設定傳送電子郵件通知的規則，方法是在區域轉換開始時發出 Amazon SNS 主題。

您可以在 Amazon 創建規則以 EventBridge 應對區域轉移採取行動。區域偏移的事件指定有關區域移位的狀態資訊。例如，當您開始區域偏移時，便會建立事件。

要捕獲您感興趣的特定區域移位事件，請定義 EventBridge 可用於檢測事件的特定事件模式。事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

盡可能發出事件。 EventBridge 在正常操作情況下，它們是從 53 ARC 公路交付到近乎實時的。但是，可能會出現可能會延遲或阻止事件傳遞的情況。

如需 EventBridge 規則如何處理事件模式的詳細資訊，請參閱 EventBridge.

使用以下方式監控區域偏移資源 EventBridge

使用 EventBridge，您可以建立規則，以定義 Route 53 ARC 為其資源發出事件時要採取的動作。例如，您可以建立規則，在您開始區域轉移時傳送電子郵件訊息。

若要在主控台中輸入或複製事件模式並貼上，請選取要在 EventBridge 主控台中使用 [輸入我自己的] 選項的選項。為了協助您判斷可能對您有用的事件模式，本主題包含區域偏移事件比對模式的範例。

建立資源事件的規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇您 AWS 區域 要在其中建立規則的地區，也就是您有興趣觀看賽事的地區。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的Name (名稱)，或者輸入描述。
5. 對於事件匯流排，保留預設值 (預設值)。
6. 選擇下一步。
7. 對於「建置」事件模式步驟，對於事件來源，保留預設值「AWS 事件」。

8. 在 [範例事件] 下，選擇 [輸入我自己]。
9. 對於範例事件，請輸入或複製並貼上事件模式。

示例 Route 53 ARC 事件模式

事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

- 從 53 號公路弧區域移位中選擇所有事件。

```
{
    "source": [
        "aws.arc-zonal-shift"
    ]
}
```

指定要用作目標的 CloudWatch 記錄群組

建立 EventBridge 規則時，您必須指定傳送符合規則之事件的目標。如需的可用目標清單 EventBridge，請參閱 EventBridge 主控台中可用的目標。您可以新增至 EventBridge 規則的其中一個目標是 Amazon CloudWatch 日誌群組。本節說明將 CloudWatch 記錄群組新增為目標的需求，並提供在建立規則時新增記錄群組的程序。

若要將 CloudWatch 記錄群組新增為目標，您可以執行下列其中一項作業：

- 建立新的記錄群組
- 選擇現有的記錄群組

如果您在建立規則時使用主控台指定新的記錄群組， EventBridge 會自動為您建立記錄群組。請確定您用作 EventBridge 規則目標的記錄群組開頭為`/aws/events`。如果您想要選擇現有的記錄群組，請注意，只有開頭為的記錄群組`/aws/events`會顯示為下拉式功能表中的選項。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立新日誌群組。

如果您使用主控台外部的 CloudWatch 作業來建立或使用 CloudWatch 記錄群組做為目標，請確定您已正確設定權限。如果您使用主控台將記錄群組新增至 EventBridge 規則，則記錄群組的資源型政策會自動更新。但是，如果您使用 AWS Command Line Interface 或 AWS SDK 來指定記錄群組，則必須更新記錄群組的以資源為基礎的原則。下列範例原則說明您必須在記錄群組的以資源為基礎的原則中定義的權限：

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

您無法使用主控台為記錄群組設定以資源為基礎的政策。若要將必要的權限新增至以資源為基礎的政策，請使用 CloudWatch PutResourcePolicyAPI 作業。然後，您可以使用 describe-resource-policiesCLI 命令來檢查您的原則是否已正確套用。

為資源事件建立規則並指定 CloudWatch 記錄群組目標

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇您 AWS 區域 要在其中建立規則的規則。
3. 選擇 [建立規則]，然後輸入有關該規則的任何資訊，例如事件模式或排程詳細資訊。

   若要取得有關為 Route 53 ARC 建立 EventBridge 規則的詳細資訊，請參閱本主題稍早的章節。
4. 在 「選擇目標」 頁面上，選擇CloudWatch作為您的目標。
5. 從下拉式功能表中選擇 CloudWatch 記錄群組。

Amazon Route 53 應用程式復原控制器中區域轉移的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Route 53 ARC 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

目錄

- 區域轉移如何與 IAM 搭配使用
- 區域轉移的 IAM 和許可
- Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例

區域轉移如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon Route 53 應用程式復原控制器中區域轉移的存取權限之前，請先了解哪些 IAM 功能可用於區域轉移。

您可以在區域轉移中使用的 IAM 功能

IAM 功能	區域移位支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否

IAM 功能	區域移位支持
服務連結角色	是

若要取得 AWS 服務如何搭配大多數 IAM 功能運作的高階整體檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Route 53 ARC 的基於身份的政策

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

若要檢視 Route 53 ARC 身分識別型原則的範例，請參閱。Amazon Route 53 應用程式復原控制器中的身分識別型政策範例

Route 53 內的資源為基礎的政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。

區域轉移的政策動作

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看區域轉移的 Route 53 ARC 動作清單，請參閱服務授權參考資料中的 Amazon Route 53 區域轉移所定義的動作。

Route 53 ARC 中針對區域移位的政策動作在動作之前使用以下前綴：

```
arc-zonal-shift
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，以下內容：

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "arc-zonal-shift:Describe*"
```

若要檢視 Route 53 ARC 以身分識別為基礎的區域轉移政策範例，請參閱。Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例

區域轉移的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看資源類型及其 ARN 的清單，以及您可以使用每個資源的 ARN 指定的動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 定義的行動-區域移位

若要查看可搭配條件索引鍵使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 定義的條件鍵-區域移位

若要檢視 Route 53 ARC 以身分識別為基礎的區域轉移政策範例，請參閱。Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例

區域偏移的政策條件索引鍵

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看區域移位條件索引鍵的清單，請參閱服務授權參考資料中的下列主題：

- Amazon 路線 53 定義的條件鍵-區域移位

若要查看可搭配條件索引鍵使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 定義的行動-區域移位
- Amazon 路線 53 定義的資源類型-區域轉移

若要檢視 Route 53 ARC 以身分識別為基礎的區域轉移政策範例，請參閱。Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例

Route 53 中的訪問控制列表（ACL）

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

基於屬性的訪問控制（ABAC）與 Route 53 ARC

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

Route 53 弧包括對 ABAC 的以下部分支持：

- 區域移位支持 ABAC，用於在 Route 53 ARC 中註冊用於區域移位的託管資源。如需適用於 Network Load Balancer 和應用程式負載平衡器管理資源的 ABAC 詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的 Elastic Load Balancing ABAC。

使用臨時登入資料與 Route 53 ARC

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Route 53 ARC 的跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 實體 (使用者或角色) 在中執行動作時 AWS，系統會將您視為主體。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。

若要查看動作是否需要原則中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 區域轉移

Route 53 ARC 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

Route 53 ARC 的服務連結角色

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

區域轉移不使用服務連結角色。

區域轉移的 IAM 和許可

本節提供有關 Amazon Route 53 應用程式復原控制器中區域轉移功能的許可如何運作的其他資訊，特別是當您使用其他 AWS 服務 (例如 Elastic Load Balancing) 的功能時。若要了解 Route 53 ARC 功能一般如何與 IAM 和許可搭配使用，請檢閱概觀主題中的資訊Amazon Route 53 應用程式復原控制器中區域轉移的 Identity and Access Management。

除了 IAM 概觀主題中概述的許可外，以下內容適用於 IAM 和許可的區域轉移：

- 確保您具有在 Route 53 ARC 中使用區域偏移所需的權限。有關更多信息，請參閱區域班次控制台訪問和區域移位操作訪問。
- 您不需要透過 IAM 新增其他 Elastic Load Balancing 許可，即可在 Route 53 ARC 中的帳戶中處理受管負載平衡器資源的區域轉移。
- 提供 Elastic Load Balancing 完整存取權的 AWS 受管理原則包含使用區域轉移的權限。如果您對 Elastic Load Balancing 存取使用 AWS 受管政策，則不需要 IAM 中的其他許可即可啟動負載平衡器的區域轉移，或在 Elastic Load Balancing 主控台中使用。如需詳細資訊，請參閱 E lastic Load Balancing 的AWS 受管原則。

Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例

根據預設，使用者和角色沒有建立或修改 Route 53 ARC 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Route 53 ARC 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon Route 53 應用程式復原控制器的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 範例：區域移位控制台存取
- 範例：區域移位 API 動作

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 Route 53 ARC 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您的使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

範例：區域移位控制台存取

若要存取 Amazon Route 53 應用程式復原控制器主控台，您必須擁有最少的一組許可。這些權限必須允許您列出和查看有關 Route 53 ARC 資源的詳細信息 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要讓使用者擁有在中使用區域移位的完整存取權 AWS Management Console，請將如下所示的原則附加至使用者：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        }
    ]
}
```

範例：區域移位 API 動作

區域轉移 API 會暫時將流量從可用區域移開，以復原應用程式。

若要確保使用者可以使用區域移位 API 動作，請附加與使用者需要使用的 API 作業對應的政策，如下所示：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift"
             ],
            "Resource": "*"
        }
    ]
}
```

Amazon 路線 53 應用程序恢復控制器中的區域自動換檔

使用區域自動切換，您可 AWS 以授權在事件期間代表您將應用程式的資源流量從可用區域轉移，以協助縮短復原時間。 AWS 當內部遙測指出存在可用區域損害可能會影響客戶時，啟動自動切換。當 AWS 啟動自動切換時，應用程式流量到您已設定為區域自動切換的資源會開始從可用區域移開。

請注意，Route 53 ARC 不會檢查個別資源的健康狀況。 AWS 當 AWS 遙測偵測到可用區域的損害可能會對客戶造成影響時，啟動自動切換。在某些情況下，流量可能會因未受到影響的資源而移開。

使用區域自動切換，您也可 AWS 以授權代表您將應用程式的資源流量從可用區域轉移出來，以進行定期練習執行。區域自動換檔需要練習運行。Route 53 ARC 開始進行練習的區域轉移可幫助您確保在自動換檔期間將流量從可用區域轉移對於您的應用是安全的。通過啟動區域轉移，將資源的流量從可用區域轉移，從而定期運行實踐會定期測試您的應用程序可以在沒有一個可用區域的情況下正常運行。練習執行會每週進行一次，並提供結果 (例如SUCCEEDED或)，FAILED以協助您瞭解應用程式是否如預期般運作。

> **Important**
>
> 在您設定實務執行或啟用區域自動切換之前，我們強烈建議您在部署應用程式資源的區域中，預先調整應用程式資源容量。當自動換檔或練習執行開始時，您不應該依賴隨需調整。區域自動換檔 (包括練習執行) 可獨立運作，且不會等待 auto 動縮放動作完成。依賴 auto 擴展而不是預先調整規模，可能會導致應用程式復原的時間更長。

如果您使用 auto 擴展來處理常規流量週期，強烈建議您將 auto 擴展的最小容量設定為在可用區域遺失的情況下繼續正常運作。

如果您計劃啟用區域自動換檔或設定練習執行，請在預先調整應用程式資源容量之後，測試您的應用程式是否可以在沒有一個可用區域的情況下正常運作。若要測試此問題，請啟動區域轉移，將資源的流量從可用區域移開。

為了確保使用區域轉移進行的測試是有效的，請務必驗證流量是否如預期從您轉離的 AZ 排出。應用程式負載平衡器和網路負載平衡器都會在 Amazon 中提供每個 AZ 指標，供您用來監控 CloudWatch此指標。視服務和用戶端重複使用連線的時間長度而定，流量可能會持續到您轉移離開的可用區域的時間超過您預期的時間。若要深入了解，請參閱限制用戶端保持連線到端點的時間。

透過啟動和評估區域轉移，確認應用程式可以在流量從可用區域轉移到可用區域的情況下繼續正常運作之後，Route 53 ARC 執行的一般做法可協助您持續確認您有足夠的容量進行自動切換。

除了在 Route 53 ARC 主控台中為負載平衡器資源啟用區域自動切換之外，您還可以選擇在 Amazon EC2 主控台中為特定負載平衡器啟用區域自動切換。若要進一步瞭解如何使用 Elastic Load Balancing 啟用區域自動換檔，請參閱 Elastic Load Balancing 使用者指南中的區域偏移。

自動移位和練習執行區域偏移是暫時的。使用自動切換功能，當受影響的可用區域復原時， AWS 會停止將資源的流量從可用區域轉移出去。客戶的應用程式流量會返回區域中的所有可用區域。執行練習時，流量會從可用區域移出單一資源約 30 分鐘，然後轉移回區域中的所有可用區域。

您可以設定 Amazon EventBridge 通知，以提醒您有關自動換班和練習執行的資訊。如需詳細資訊，請參閱 使用區域自動換檔與 Amazon EventBridge。

區域自動換檔和練習運行如何工作

Amazon Route 53 應用程式復原控制器中的區域自動切換功能可讓您代表您 AWS 將資源的流量從 AWS 可用區域轉移出可用區域中的客戶時。區域自動切換是專為在中的所有可用區域中預先調整資源所設計 AWS 區域，因此應用程式可以在遺失一個可用區域的情況下正常運作。

使用區域自動換檔時，您必須設定練習執行，Route 53 ARC 會定期將資源的流量從一個可用區域轉移。Route 53 ARC 排程練習會針對每個具有與其關聯的練習執行組態的資源執行大約每週執行一次。每個資源的練習執行會獨立排程。

對於每次練習執行，Route 53 ARC 都會記錄一個結果。如果練習執行被封鎖條件中斷，練習執行結果不會標示為成功。如需練習執行結果的詳細資訊，請參閱練習執行的成果。

您可以設定 Amazon EventBridge 通知，將自動換班和練習執行的相關資訊傳送給您。如需詳細資訊，請參閱 使用區域自動換檔與 Amazon EventBridge。

主題

- AWS 啟動和停止自動換檔時
- 當 Route 53 ARC 建立明細表時，開始和結束練習管路
- 區域班次、練習執行和自動切換的優先順序
- 停止資源的使用中自動換檔或練習執行
- 流量如何轉移
- 練習運行的警報
- 封鎖的日期和封鎖的視窗 (UTC)

AWS 啟動和停止自動換檔時

當您為資源啟用區域自動切換時，您授權代表您在事件期間 AWS 將應用程式的資源流量從可用區域轉移，以協助減少復原的時間。

為了達到這個目標，區域自動換檔會使用 AWS 遙測功能，儘早偵測出可用區域的損害可能會對客戶造成影響。當 AWS 啟動自動切換時，對已設定資源的流量會立即開始從受損的可用區域轉移，這可能會對客戶造成影響。

區域自動換檔是專為已針對所有可用區域中所有可用區域預先調整應用程式資源的客戶所設計的功能。 AWS 區域當自動換檔或練習執行開始時，您不應該依賴隨需調整。

AWS 當它確定可用區域已恢復時結束自動換檔。

當 Route 53 ARC 建立明細表時，開始和結束練習管路

Route 53 ARC 每週為資源安排練習運行，持續約 30 分鐘。Route 53 ARC 獨立排程、開始和管理每個資源的練習執行。Route 53 ARC 不會針對同一帳戶中的資源進行批次處理練習執行。

當練習執行持續達到預期的持續時間 (不中斷) 時，會標示為的結果SUCCESSFUL。還有其他幾種可能的結果：FAILEDINTERRUPTED、和PENDING。結果值和說明包含在「練習執行的成果」一節中。

有一些情況下，當 Route 53 ARC 中斷練習運行並結束它。例如，如果在練習執行期間啟動了自動切換，Route 53 ARC 會中斷練習執行並結束它。作為另一個範例，假設資源對練習執行有不良反

應，並導致您指定監視練習執行進入ALARM狀態的警示。在這個案例中，Route 53 ARC 也會中斷練習執行並結束它。

此外，Route 53 ARC 無法為資源開始排程練習執行時，也有數種情況。

為了回應資源的中斷和封鎖實務執行，Route 53 ARC 會執行下列動作：

- 如果資源的練習執行在進行中時中斷，Route 53 ARC 會將每週的練習執行結束，並排定下週的資源執行新練習。每週的練習結果是INTERRUPTED在這種情況下，而不是FAILED。FAILED只有當監視練習執行的結果警示進入練習執行期間的ALARM狀態時，練習執行結果才會設定為。
- 如果在排定資源的練習執行開始時存在封鎖限制，Route 53 ARC 不會啟動練習執行。Route 53 ARC 會繼續定期監視，以確定是否仍有一個或多個阻塞約束。當沒有任何阻塞約束時，Route 53 ARC 會啟動資源的練習運行。

以下是阻止 Route 53 ARC 啟動或繼續資源執行練習的封鎖條件約束的範例：

- 當 AWS Fault Injection Service 實驗正在進行時，Route 53 ARC 不會開始或繼續練習執行。如果在 Route 53 ARC 已排定練習執行開始時 AWS FIS 事件處於作用中狀態，則 Route 53 ARC 不會開始練習執行。Route 53 ARC 在整個練習運行過程中監視阻塞約束，包括 AWS FIS 事件。如果 AWS FIS 事件在練習執行處於作用中狀態時開始，Route 53 ARC 會結束練習執行，並且不會嘗試啟動另一個事件，直到資源的下一個定期排程練習執行為止。
- 如果區域中有目前 AWS 事件，Route 53 ARC 不會開始資源的練習執行，並結束區域中的作用中練習執行。

當練習執行完成而不被中斷時，Route 53 ARC 會照常在一週內安排下一個練習執行。如果因為封鎖限制而未啟動練習執行，例如 AWS FIS 實驗或您指定的封鎖時間範圍，Route 53 ARC 會繼續嘗試開始練習執行，直到可以開始練習執行為止。

區域班次、練習執行和自動切換的優先順序

一次生效的資源不能有一個以上的流量轉移，也就是說，只有一種做法會執行區域轉移、客戶啟動的區域轉移或資源的自動換檔。當有多個交通變化正在進行中時，Route 53 ARC 會遵循優先順序，以確定資源的流量變化有效。

優先順序的整體原則是，您作為客戶開始的區域班次的優先順序高於自動換檔，這優先於實務執行。也就是說，客戶啟動的區域班次 > 自動換檔 > 練習執行區域班次。

為了說明這一點，以下是一些示例情況的優先級如何工作：

- 如果有作用中的自動工作班次，而您對已啟用自動切換作業的資源啟動區域工作班次，則您開始的區域工作班次為。APPLIED資源現在會偏離適用區域轉移的可用區域。如果區域移位在結束

自動換檔之前 AWS 結束，則自動換檔將成為移位。APPLIED因此，資源會從正在進行自動切換 AWS 的可用區域移開。

- 如果您針對已啟用自動切換工作班次的資源啟動了作用中的區域移位，並 AWS 啟動自動切換作業，則該資源存在自動切換作業。但是，區域偏移設定為，APPLIED且自動切換設定為，NOT APPLIED直到區域偏移結束為止。然後，自動換檔的狀態會更新為，APPLIED而自動換檔會將資源的流量移開，直到 AWS 結束自動換檔為止。
- 如果資源正在執行作用中的實務，而您啟動了資源的區域轉移，將相同可用區域的流量轉移，則練習執行會中斷。如果您啟動了將流量從不同可用區域轉移的區域轉移，則執行作業會照常繼續執行。
- 如果資源有使用中的區域轉移，且 Route 53 ARC 已排程開始練習執行，則練習執行會延遲一個小時。然後，Route 53 ARC 再次嘗試開始練習執行。Route 53 ARC 會繼續每小時檢查一次，直到可以開始練習執行為止。

資源目前有效的流量偏移已將套用的區域偏移狀態設定為APPLIED。任何時候都只能設定APPLIED一個班次。正在進行的其他班次設定為ACTIVE。

停止資源的使用中自動換檔或練習執行

若要停止資源的進行中自動工作班次，請停用資源的區域自動切換作業。

當您停用區域自動切換時，資源的練習執行組態不會受到影響。依照相同的排程，資源仍會進行定期練習執行。如果您想要停止練習執行，除了停用自動換檔，您必須刪除與資源相關聯的練習執行組態。

當您刪除練習執行組態時， AWS 會停止執行練習執行，以便每週將資源的流量從可用區域轉移。此外，由於區域自動切換需要執行練習，因此當您使用 Route 53 ARC 主控台刪除練習執行組態時，此動作也會停用資源的區域自動切換。不過，請注意，如果您使用區域自動換檔 API 刪除練習執行，您必須先停用資源的區域自動切換。

若要停止使用中的練習執行，請取消練習執行區域偏移。如需詳細資訊，請參閱 取消練習運行區域移位。

流量如何轉移

對於自動換檔和實踐執行區域班次，流量將使用 Route 53 ARC 用於客戶啟動的區域班次相同的機制將流量從可用區域轉移。若要將跨區域負載平衡關閉的負載平衡器的流量從可用區域轉移出來，Route 53 ARC 會將可用區域的負載平衡器健康狀態檢查設定為狀態不良，使其健康狀態檢查失敗。不健康的運作狀態檢查會導致 Amazon Route 53 從 DNS 撤回資源的對應 IP 位址，以便從可用區域重新導向流量。新連線現在會路由到中的 AWS 區域 其他可用區域。

使用自動換檔時，當可用區域復原並 AWS 決定結束自動換檔時，Route 53 ARC 會反轉健康狀態檢查程序，要求還原 Route 53 健康狀態檢查。然後，會還原原始區域 IP 位址，如果健全狀況檢查持續狀態良好，則可用區域會再次包含在負載平衡器的路由中。

重要的是要注意，自動換檔不是基於監視負載平衡器或應用程式基礎健康狀態的健康狀態檢查。Route 53 ARC 使用健康狀態檢查將流量從可用區域移開，方法是要求運作狀態檢查設定為不健康狀態，然後在結束自動換檔或區域轉移時再次將健康狀態檢查還原為正常狀態。

練習運行的警報

您可以在區域自動換檔中為練習運行指定兩個 CloudWatch 警報。第一個警報，即結果警報，是必需的。您應該設定結果警示，以在每 30 分鐘的練習執行期間，當流量從可用區域移出可用區域時，監控應用程式的健全狀況。

若要讓練習執行生效，請指定監控資源或應用程式度量的 CloudWatch 警示作為結果警示，該警示會在您的應用程式受到一個可用區域遺失的不利影響時回應ALARM狀態。如需詳細資訊，請參閱中為練習執行指定的警示一節設定區域自動換檔時的最佳作法。

結果警示也提供 Route 53 ARC 針對每個練習執行報告的練習執行結果的資訊。如果警示進入ALARM狀態，練習執行會結束，並將練習執行結果傳回為FAILED。如果練習執行完成 30 分鐘排定的測試期間，且結果警示未進入ALARM狀態，則結果會傳回為SUCCEEDED。所有結果值的清單以及說明會在「練習執行結果」一節中提供。

或者，您可以指定第二個警報，即阻塞警報。阻塞警報阻止練習從開始或繼續運行，當它處於一個ALARM狀態。當警報處於狀態時，此警報會阻止練習運行流量轉移而不被啟動，並停止任何進行中的練習運行。ALARM

例如，在具有多個微服務的大型架構中，當一個微服務遇到問題時，您通常會想要停止應用程式環境中的所有其他變更，包括封鎖實務執行。

封鎖的日期和封鎖的視窗 (UTC)

您可以選擇封鎖特定行事曆日期或特定時間範圍的練習執行，也就是 UTC 的日期和時間。

例如，如果您已排定在 2024 年 5 月 1 日啟動應用程式更新，而且您不想練習執行在當時將流量轉移掉，您可以設定封鎖的2024-05-01日期。

或者，假設您每週執行三天的業務報告摘要。在這個案例中，您可能會將下列週期性的天數和時間設定為封鎖的視窗，例如，在 UTC 中：MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30。

關於區域自動換檔

區域自動切換是一項功能，可代表您 AWS 將應用程式資源流量從可用區域移開。 AWS 當內部遙測指出存在可用區域損害可能會影響客戶時，啟動自動切換。內部遙測結合了來自多個來源 (包括 AWS 網路) 以及 Amazon EC2 和 Elastic Load Balancing 服務的指標。

您可以在關閉跨區域負載平衡的情況下為網路負載平衡器和應用程式負載平衡器啟用區域自動切換功能。

當您在一個區域中多個 (通常是三個) AZ 中的負載平衡器上部署和執行 AWS 應用程式，並預先調整以支援靜態穩定性時， AWS 可透過使用自動換檔將流量轉移出來，快速復原 AZ 中的客戶應用程式。藉由將資源流量轉移至該地區的其他 AZ， AWS 可以減少因停電、硬體或軟體問題或其他損傷所造成的潛在影響的持續時間和嚴重程度。

當 AWS 開始負載平衡資源的自動切換時，Route 53 ARC 會將負載平衡器資源的對應 IP 地址的 Amazon Route 53 運作狀態檢查設定為狀態不良，以便資源的流量不再導向至可用區域。當 AWS 確定 AZ 已準備好讓應用程式流量傳回時，Route 53 ARC 會還原 Route 53 健康狀態檢查，並還原原始區域 IP 位址。

當您為資源啟用區域自動切換時，您還必須配置資源的練習執行。 AWS 執行練習大約每週執行 30 分鐘，以協助您確保您有足夠的容量來執行應用程式，而不需要區域中的任何一個可用區域。

與區域轉移一樣，在某些特定情況下，區域自動換檔不會將流量從 AZ 轉移出來。例如，如果 AZ 中的負載平衡器目標群組沒有任何執行個體，或者所有執行個體運作狀態不良，則負載平衡器處於失敗開啟狀態，而且您無法移開其中一個 AZ。

若要進一步瞭解區域自動切換，請參閱。Amazon 路線 53 應用程序恢復控制器中的區域自動換檔

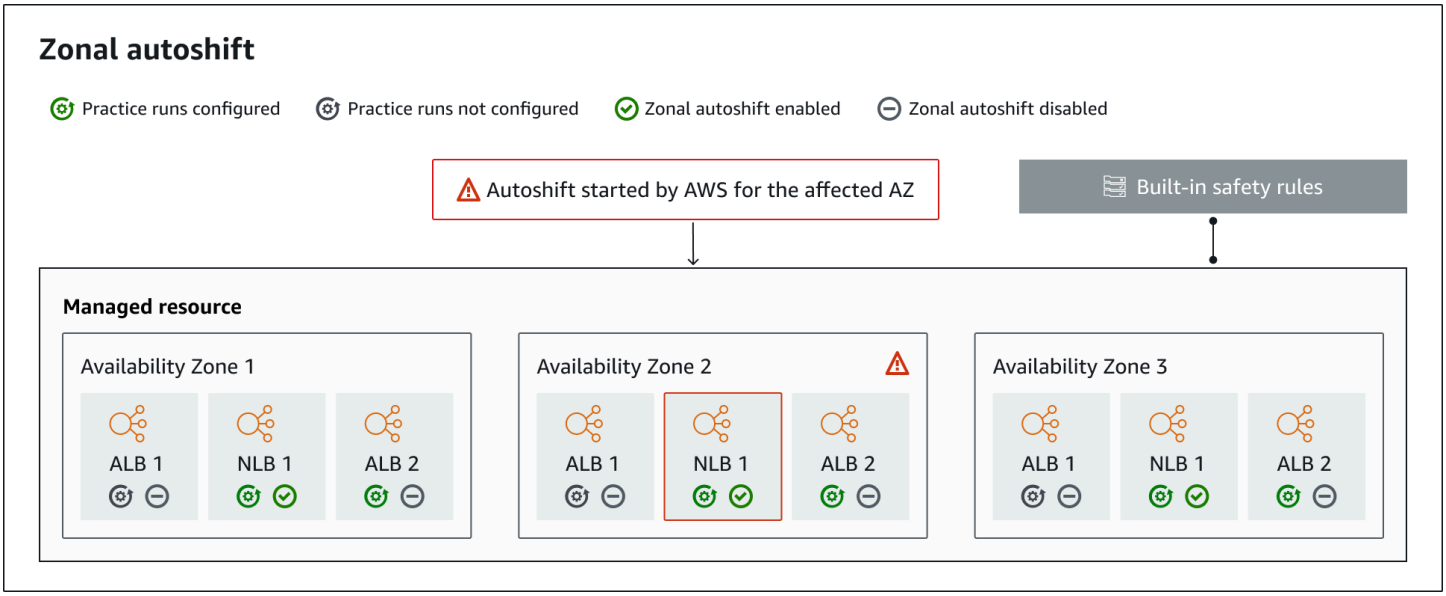
AWS 區域 區域自動換檔的可用性

區域自動換檔目前在商業上可用。 AWS 區域

如需 Amazon Route 53 應用程式復原控制器的區域支援和服務端點的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器端點和 Amazon Web Services 一般參考中的配額。

區域自動換檔組件

下圖說明自動換檔將流量從可用區域移出的範例。 AWS 當內部遙測指出存在可用區域損害可能會影響客戶時，啟動自動切換。



以下是 Route 53 ARC 中區域自動換檔功能的組成部分。

區域自動換檔

區域自動換檔會將資源的流量移開，而不需要您採取任何動作。區域自動換檔是 Route 53 ARC 中的一項功能，當內部遙測指出存在可能影響客戶的可用區域損害時，會 AWS 啟動自動換檔。請注意，在某些情況下，資源可能會移走未受到影響的情況。

練習運行

當您啟用資源的區域自動切換時，您也必須設定資源的區域自動切換作業執行。 AWS 執行區域轉移練習大約每週運行一次，持續約 30 分鐘。實務執行可確保您的應用程式在遺失一個可用區域的情況下正常執行。在練習執行中，透過區域轉移， AWS 將資源的流量從一個可用區域轉移，然後在練習執行結束時將流量轉移回去。

練習運行配置

練習執行組態會定義封鎖的日期和視窗 (如果有的話)，以及您針對區域自動切換中的資源執行指定的 CloudWatch警示。您可以隨時編輯練習執行、新增或變更封鎖的日期或時段，或更新練習執行的警示。

若要啟用區域自動切換，您必須有資源的練習執行組態您也可以刪除練習執行。若要刪除資源的練習執行組態，必須停用區域自動切換。

練習運行警報

配置練習執行時，您可以根據資源和應用程式需求指定在中 CloudWatch建立的 CloudWatch 警示。如果您的應用程式受到練習執行的不利影響，您指定的警示可能會封鎖練習執行開始，或停止進行中的練習執行。

如果您指定的警示進入ALARM狀態，Route 53 ARC 會結束練習執行的區域偏移，因此資源的流量不會再從可用區域移開。

您可以為練習執行指定兩種類型的警示：結果警示、在練習執行期間監視資源和應用程式的健全狀況，以及封鎖警示 (您可以設定以防止執行練習執行開始或停止進行中的練習執行)。需要結果警報；阻塞警報是可選的。

練習跑步成果

Route 53 ARC 會報告每次練習執行的結果。以下是可能的練習運行結果：

- 待處理：練習執行的區域偏移為作用中 (進行中)。還沒有結果可以返回。
- 成功：在練習執行期間，結果警示未進入ALARM狀態，且練習執行已完成整個 30 分鐘的測試期間。
- 中斷：練習執行結束的原因不是進入ALARM狀態的結果警示。練習運行可以由於各種原因而中斷。例如，由於為練習執行指定的封鎖警示進入ALARM狀態而結束的練習執行結果為INTERRUPTED。如需有關INTERRUPTED結果原因的詳細資訊，請參閱練習執行的成果。
- 失敗：結果警示在練習執行期間進入ALARM狀態。

內建安全規則

Route 53 ARC 中內置的安全規則可防止資源的多個交通轉移一次生效。也就是說，只有一個客戶啟動的區域轉移、練習執行區域轉移或資源的自動換檔，才能主動將流量從可用區域轉移出去。例如，如果您在資源目前使用自動切換檔移開時啟動該資源的區域偏移，則區域偏移優先。如需詳細資訊，請參閱練習執行的成果。

資源識別符

用於啟用區域自動換檔的資源識別碼，也就是資源的 Amazon 資源名稱 (ARN)。

您只能為 Route 53 ARC 支援的 AWS 服務中的帳戶中的資源啟用區域自動切換功能。這些 AWS 服務中支援的資源會由服 AWS 務自動向 Route 53 ARC 註冊。

> **Note**
>
> 在關閉跨區域負載平衡的情況下，您只能為網路負載平衡器和應用程式負載平衡器設定區域自動換檔。

受管資源

AWS 服務使用 Route 53 ARC 自動註冊資源，以進行區域自動換檔。已註冊的資源是 Route 53 ARC 中的受管理資源。

資源名稱

Route 53 ARC 中受管理資源的名稱。

已套用狀態

套用狀態會指出資源的流量偏移是否有效。當您設定區域自動換檔時，資源可能會有多個作用中的流量移位，也就是執行區域轉移、客戶啟動的區域偏移或自動切換。但是，只會套用一個，也就是一次對資源有效。具有狀態的轉移`APPLIED`決定了可用區域，其中應用程式流量已移走資源，以及該流量轉移何時結束。

用於區域自動換檔的資料和控制平面

當您規劃容錯移轉和災難復原時，請考慮容錯移轉機制的彈性。我們建議您確保在容錯移轉期間所依賴的機制具有高可用性，以便在災難情況下需要時可以使用它們。一般而言，您應該隨時為您的機制使用資料平面函數，以獲得最大的可靠性和容錯能力。考慮到這一點，重要的是要了解服務的功能如何在控制平面和數據平面之間劃分，以及何時可以依賴服務數據層面對極高可靠性的期望。

一般而言，控制平面可讓您執行基本的管理功能，例如建立、更新和刪除服務中的資源。資料平面提供服務的核心功能。

如需有關資料平面、控制平面以及如何 AWS 建置服務以符合高可用性目標的詳細資訊，請參閱 Amazon Builders' Library 中的使用可用區域的靜態穩定性 paper。

Amazon Route 53 應用程式復原控制器中的區域自動換檔定價

對於區域自動換檔，當 AWS 判斷存在可能對客戶應用程式造成不利影響的潛在問題時，代表您 AWS 將流量從可用區域移開，以取得支援的資源。啟用區域自動換檔不收取額外費用。

您只需為您在 Amazon Route 53 應用程式復原控制器中使用的部分付費。如需 Route 53 ARC 的詳細定價資訊和定價範例，請參閱 Amazon Route 53 定價，然後向下捲動至 Amazon Route 53 應用程式復原控制器。

設定區域自動換檔時的最佳作法

在 Amazon Route 53 應用程式復原控制器中啟用區域自動切換時，請注意下列最佳實務和考量事項。

區域自動換檔包括兩種類型的流量移位：自動換檔和練習執行區域變速。

- 使用自動切換功能， AWS 可代表您在事件期間將應用程式資源流量從可用區域移除，藉此縮短復原時間。
- 使用練習執行時，Route 53 ARC 會代表您啟動區域偏移。區域轉移會將流量從可用區域轉移出資源，然後按每週節奏再次轉移。實務執行可協助您確定已針對區域中的可用區域擴充足夠容量，讓應用程式容忍一個可用區域的遺失。

有幾個最佳做法和考量要牢記自動換檔和練習執行。在啟用區域自動切換或設定資源的練習執行之前，請檢閱下列主題。

主題

- 限制用戶端保持連線至端點的時間
- 預先調整資源容量並測試轉移流量
- 注意資源類型和限制
- 指定練習執行的警示
- 評估練習執行的成果

限制用戶端保持連線至端點的時間

當 Amazon Route 53 應用程式復原控制器將流量從損害轉移出來時 (例如，使用區域移位或區域自動切換)，Route 53 ARC 用來移動應用程式流量的機制就是 DNS 更新。DNS 更新會導致所有新連線導向遠離受損位置。但是，具有預先存在開啟連線的用戶端可能會繼續對受損位置發出要求，直到用戶端重新連線為止。為確保快速復原，我們建議您限制用戶端保持連線至端點的時間長度。

如果您使用應用程式負載平衡器，則可以使用`keepalive`此選項來設定連線持續的時間長度。我們建議您降低與應用程式復原時間目標內嵌的`keepalive`值，例如 300 秒。當您選擇`keepalive`時間時，請考慮這個值通常是更頻繁地重新連接之間的折衷，這可能會影響延遲，並且更快地將所有用戶端從受損的可用區域或區域移開。

如需有關設定應用程式負載平衡器keepalive選項的詳細資訊，請參閱《應用程式負載平衡器使用指南》中的 HTTP 用戶端 keepalive 持續時間。

預先調整資源容量並測試轉移流量

AWS 將流量從一個可用區域轉移到區域轉移或自動換檔時，重要的是，剩餘的可用區域可以為您的資源提高的請求率提供服務，這一點很重要。這種模式被稱為靜態穩定性。如需詳細資訊，請參閱 Amazon Builder 程式庫中的使用可用區域的靜態穩定性白皮書。

例如，如果您的應用程式需要 30 個執行個體來為其用戶端提供服務，您應該在三個可用區域佈建 15 個執行個體，總共 45 個執行個體。如此一來，當 AWS 流量從一個可用區域轉移 (使用自動切換或執行練習期間) 仍然AWS 可以跨兩個可用區域，為應用程式的用戶端提供剩餘總共 30 個執行個體的服務。

Route 53 ARC 中的區域自動切換功能可協助您快速從可用區域中的 AWS 事件復原，當您的應用程式具有預先調整資源以正常運作且遺失一個可用區域的情況下。在您啟用資源的區域自動工作班次之前，請在中的所有已設定可用區域中調整資源產能。 AWS 區域然後，啟動資源的區域偏移，以測試當流量從可用區域移開時，您的應用程式是否仍可正常執行。

使用區域偏移進行測試之後，請啟用區域自動切換，並設定應用程式資源的練習執行。使用區域自動換檔執行的定期練習可協助您確保 (在持續的基礎上)，確保您的容量仍可適當調整。透過跨可用區域的足夠容量，您的應用程式可以在自動換檔期間繼續為用戶端提供服務，而不會中斷。

如需有關開始資源區域偏移的詳細資訊，請參閱Amazon Route 53 應用程序恢復控制器的區域轉移。

注意資源類型和限制

區域自動換檔支援將流量從可用區域移出，以支援區域轉移所支援的所有資源。一般而言，支援跨區域負載平衡關閉的網路負載平衡器和應用程式負載平衡器。在一些特定的資源案例中，區域自動切換不會從可用區域轉移流量以進行自動換檔。

例如，如果可用區域中的負載平衡器目標群組沒有任何執行個體，或者所有執行個體運作狀態不良，則負載平衡器處於失敗開啟狀態。如果在此案例中 AWS 啟動負載平衡器的自動切換，則自動切換不會變更負載平衡器使用的可用區域，因為負載平衡器已處於失敗開啟狀態。這是預期的行為。 AWS 區域 如果所有可用區域都無法開啟 (運作狀況不良)，則 Autoshift 不會導致一個可用區域運作狀況不良，並將流量轉移到其他可用區域。

第二個案例是，如果 AWS 啟動應用程式負載平衡器的自動換檔，該 Application Load Balancer 器是中 AWS Global Accelerator的加速器端點。與區域移位一樣，作為全域加速器中加速器端點的應用程式負載平衡器不支援自動切換。

若要查看有關支援資源的詳細資訊，包括要注意的所有需求和例外狀況，請參閱支援區域移位和區域自動換檔的資源。

指定練習執行的警示

您至少設定一個警報 (結果警示)，以便使用區域自動換檔練習執行。或者，您也可以配置第二個警報-阻塞警報-。

當您考慮針對資源的練習執行設定的 CloudWatch 警示時，請記住下列事項：

- 對於必要的結果警示，我們建議您將 CloudWatch 警示設定為在資源或應用程式的度量指出將流量從可用區域轉離可用區域會對效能造成不利影響時進入ALARM狀態。例如，您可以決定資源要求率的臨界值，然後將警示設定為在超過閾值時進入ALARM狀態。您必須負責設定適當的警示，AWS 以便結束練習執行並傳回FAILED結果。
- 我們建議您遵循架構AWS 良好的框架，該框架建議您實施關鍵績效指標（KPI）作為警報。CloudWatch如果您這麼做，您可以使用這些警示來建立複合警示作為安全觸發程序，以防止練習執行在可能導致您的應用程式遺漏重要績效指標時開始執行。當警示不再處於某個ALARM狀態時，Route 53 ARC 會在下次為資源排定練習執行時開始練習執行。
- 對於練習執行封鎖警示，如果您選擇進行設定，您可能會選擇追蹤特定度量，以指出您不希望練習執行開始。
- 對於練習執行警示，您必須先在 Amazon 中設定每個警示指定 Amazon CloudWatch 資源名稱 (ARN)。您指定的 CloudWatch 警示可以是複合警示，可讓您包含數個度量，以及可觸發警示進入ALARM狀態的應用程式和資源的檢查。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的合併警示。
- 請確定您為練習執行指定的 CloudWatch 警示與設定練習執行的資源位於相同的區域。

評估練習執行的成果

Route 53 ARC 會報告每次練習執行的結果。練習執行後，評估結果，並判斷您是否需要採取行動。例如，您可能需要擴展容量或調整警報的配置。

以下是可能的練習運行結果：

- 成功：在練習執行期間，結果警示未進入ALARM狀態，且練習執行已完成整個 30 分鐘的測試期間。
- 失敗：結果警示在練習執行期間進入ALARM狀態。
- 中斷：練習執行結束的原因不是進入ALARM狀態的結果警示。練習運行可能由於各種原因而中斷，包括：
  - 練習運行已結束，因為在區域中 AWS 啟動了自動換檔 AWS 區域 或有警報條件。

  - 實踐運行已結束，因為已刪除資源的練習運行配置。
  - 實務執行已結束，因為在可用區域中的資源啟動了客戶啟動的區域轉移，而實務執行區域轉移正在將流量從中移開。
  - 實踐運行已結束，因為無法再訪問為練習運行配置指定的 CloudWatch 警報。
  - 練習執行已結束，因為為練習執行指定的封鎖警示進入ALARM狀態。
  - 練習運行由於未知原因而結束。
- 擱置中：練習執行處於作用中 (進行中)。還沒有結果可以返回。

區域自動切換 API 操作

下表列出您可以與區域自動切換搭配使用的 Route 53 ARC API 作業。如需搭配使用區域自動切換 API 作業的範例 AWS CLI，請參閱。

如需如何搭配使用常用區域自動切換 API 作業的範例 AWS Command Line Interface，請參閱。使用帶區域自動 AWS CLI 換檔的範例

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
創建練習運行配置	請參閱啟用或停用區域自動切換	請參閱 CreatePracticeRunConfiguration
刪除練習執行組態	請參閱設定、編輯或刪除練習執行組態	請參閱 DeletePracticeRunConfiguration
列出自動切換	請參閱Amazon 路線 53 應用程序恢復控制器中的區域自動換檔	請參閱 ListAutoshifts
列出區域自動換檔的資源	請參閱支援區域移位和區域自動換檔的資源	查看ListManaged資源
取得區域自動換檔的資源	請參閱支援區域移位和區域自動換檔的資源	請參閱GetManaged資源
編輯練習執行組態	請參閱設定、編輯或刪除練習執行組態	請參閱 UpdatePracticeRunConfiguration

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
啟用或停用區域自動切換	請參閱啟用或停用區域自動切換	請參閱 UpdateZonalAutoshiftConfiguration

使用帶區域自動 AWS CLI 換檔的範例

本節 AWS Command Line Interface 將介紹使用區域自動換檔的簡單應用程式範例，以及使用 API 操作在 Amazon Route 53 應用程式復原控制器中使用區域自動切換功能。這些範例旨在協助您深入了解如何使用 CLI 使用區域自動換檔。

區域自動換檔是 Route 53 ARC 中的一種功能。使用區域自動切換，您可 AWS 以授權在事件期間代表您將支援的應用程式資源流量從可用區域轉移，以協助縮短復原時間。區域自動換檔包括練習執行，這也會將流量從可用區域移開，以協助持續驗證自動換檔對您的應用程式是否安全。

區域自動換檔目前支援網路負載平衡器和應用程式負載平衡器，且跨區域負載平衡已關閉。

如需詳細資訊，請參閱 支援區域移位和區域自動換檔的資源。

本節提供下列範例，說明如何開始使用和使用區域自動切換：

- 建立資源的練習執行組態。
- 啟用和停用資源的自動換檔。
- 通過取消練習運行開始的區域轉移來結束進行中的練習運行。
- 停用資源的區域自動切換功能，以結束進行中的自動換檔。
- 編輯資源的練習執行組態，以變更指定的警示或封鎖的日期或視窗。
- 刪除資源的練習執行組態。

若要取得有關使用的更多資訊 AWS CLI，請參閱《AWS CLI 指令參考》。如需區域自動切換 API 動作的清單以及詳細資訊的連結，請參閱。區域自動切換 API 操作

創建練習運行配置

您必須先為資源建立練習執行組態，以選擇所需練習執行的選項，才能為資源啟用區域自動切換作業。您可以使用`create-practice-run-configuration`命令使用 CLI 為資源建立練習執行組態。

建立資源的練習執行組態時，請注意下列事項：

- 目前唯一支援的警報類型是CLOUDWATCH。
- 您必須使用與部署資源 AWS 區域 相同的警示。
- 需要指定結果警示。指定阻塞警報是可選的。
- 指定封鎖的日期或封鎖的視窗是選擇性的。

您可以使用create-practice-run-configuration命令使用 CLI 建立練習執行組態。

例如，要為資源創建練習運行配置，請使用如下命令：

```
aws arc-zonal-shift create-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --outcome-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
MyAppHealthAlarm \
      --blocking-alarms
 type=CLOUDWATCH,alarmIdentifier=arn:aws:cloudwatch:Region:111122223333:alarm:Region-
BlockWhenALARM \
      --blocked-dates 2023-12-01 --blocked-windows Mon:10:00-Mon:10:30
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                  {
              "type": "CLOUDWATCH",
              "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
```

```
        ],
        "blockedDates": [
            "2023-12-01"
        ]
}
```

啟用或停用自動換檔

透過使用 CLI 更新區域自動換檔狀態，可以啟用或停用資源的自動換檔。若要變更區域自動切換狀態，請使用指update-zonal-autoshift-configuration令。

例如，若要為資源啟用自動換檔，請使用如下命令：

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="ENABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "ENABLED"
}
```

取消進行中的自動工作班次

若要取消資源的進行中自動工作班次，請停用區域自動切換功能。這與您一般用來停用區域自動切換的指令相同，因此當您停用區域自動切換來取消進行中的自動切換時，資源也不會受到 future 自動換檔的影響。您可以更新區域自動切換，以便隨時再次啟用它。

請注意，您可以停用資源的區域自動切換，而不刪除資源的練習執行組態。

若要使用 CLI 取消自動切換，請使用指令停用區域轉換。update-zonal-autoshift-configuration例如，若要結束資源的自動換檔，請使用如下命令：

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

取消進行中的練習執行

您可以取消實務執行為資源開始的區域轉移，以取消使用 CLI 執行的進行中實務。若要取消練習執行，請使用cancel-zonal-shift指令。

例如，若要取消資源的練習執行，請使用類似下列的命令：

```
aws arc-zonal-shift cancel-zonal-shift \
   --zonal-shift-id="="arn:aws:testservice::111122223333:ExampleALB123456890"
```

```
{
    "zonalShiftId": "2222222-3333-444-1111",
    "resourceIdentifier": "arn:aws:testservice::111122223333:ExampleALB123456890",
    "awayFrom": "usw2-az1",
    "expiryTime": 2024-11-15T10:35:42+00:00,
    "startTime": 2024-11-15T09:35:42+00:00,
    "status": "CANCELED",
    "comment": "Practice Run Started"
}
```

編輯練習執行組態

您可以使用 CLI 編輯資源的練習執行組態，以更新不同的組態選項，例如變更練習執行的警示，或在 Route 53 ARC 無法啟動練習執行時更新封鎖的日期或封鎖的視窗。若要編輯練習執行組態，請使用update-practice-run-configuration指令。

編輯資源的練習執行組態時，請注意下列事項：

- 目前唯一支援的警報類型是CLOUDWATCH。
- 您必須使用與部署資源 AWS 區域 相同的警示。
- 需要指定結果警示。指定阻塞警報是可選的。
- 指定封鎖的日期或封鎖的視窗是選擇性的。

- 您指定的封鎖日期或封鎖的時段會取代任何現有值。

例如，若要編輯資源的練習執行組態以指定新的封鎖日期，請使用如下所示的命令：

```
aws arc-zonal-shift update-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --blocked-dates 2024-03-01
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "zonal-shift-elb"
   "zonalAutoshiftStatus": "DISABLED",
   "practiceRunConfiguration": {
       "blockingAlarms": [
                   {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-BlockWhenALARM"
           }
       ]
       "outcomeAlarms": [
           {
               "type": "CLOUDWATCH",
               "alarmIdentifier": "arn:aws:cloudwatch:us-west-2:111122223333:alarm:us-
west-2-MyAppHealthAlarm"
           }
       ],
       "blockedWindows": [
           "Mon:10:00-Mon:10:30"
       ],
       "blockedDates": [
           "2024-03-01"
       ]
}
```

刪除練習執行組態

您可以刪除資源的練習執行組態，但必須先停用資源的區域自動切換作業。要啟用區域自動切換，資源必須具有練習執行組態。定期執行作業可協助您確保您的應用程式可以在沒有可用區域的情況下正常執行。

若要使用 CLI 刪除練習執行組態，請先使用指令停用區域自動切換 (如果需要)。update-zonal-autoshift然後，刪除練習運行配置，使用delete-practice-run-configuration命令。

首先，使用如下命令禁用資源的區域自動切換：

```
aws arc-zonal-shift update-zonal-autoshift-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
      --zonal-autoshift-status="DISABLED"
```

```
{
   "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
west-2:111122223333:ExampleALB123456890",
   "zonalAutoshiftStatus": "DISABLED"
}
```

然後，刪除練習運行配置，使用如下命令：

```
aws arc-zonal-shift delete-practice-run-configuration \
      --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890"
```

```
{
   "arn": "arn:aws:elasticloadbalancing:us-west-2:111122223333:ExampleALB123456890",
   "name": "TestResource",
   "zonalAutoshiftStatus": "DISABLED"
}
```

啟用和使用區域自動換檔

本節提供在 Amazon Route 53 應用程式復原控制器中使用區域自動換檔的程序，包括啟用和停用區域自動換檔、設定練習執行，以及取消進行中的實務執行。

啟用或停用區域自動切換

本節中的步驟說明如何在 Amazon Route 53 應用程式復原控制器主控台上啟用或停用區域自動切換。若要以程式設計方式使用區域自動切換，請參閱區域偏移和區域自動切換 API 參考指南。

啟用區域自動切換時，您授權代表您在事件期間 AWS 將應用程式資源流量從可用區域轉移，以協助縮短復原時間。

啟用或停用區域自動切換

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域自動切換。
3. 在資源區域自動工作班次組態下，選擇資源。
4. 在「動作」功能表中，選擇「啟用區域自動切換」或「停用區域自動切換」，然後依照步驟完成更新。

如果資源沒有練習執行組態，則無法使用 [啟用區域自動切換]。若要設定練習執行組態並啟用區域自動切換，請選擇 [設定區域自動切換]。

設定、編輯或刪除練習執行組態

本節中的步驟說明如何在 Amazon Route 53 應用程式復原控制器主控台上編輯或刪除練習執行組態。若要以程式設計方式使用區域自動切換 (包括練習執行組態的變更)，請參閱區域移位和區域自動切換 API 參考指南。

如果您在控制台中刪除練習運行配置，則會禁用區域自動切換。您必須先停用區域自動切換，才能使用 API 作業刪除練習執行組態。您可以在不啟用區域自動切換的情況下設定練習執行。但是，若要為資源啟用區域自動切換，您必須為資源配置練習執行。

若要設定練習執行

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域自動切換。
3. 選擇「設定區域自動切換」。
4. 選擇要設定區域自動切換的資源。
5. 如果您不想 AWS 在發生事件時啟動資源的自動切換，請選擇停用區域自動切換。 AWS 如果您選擇，您可以繼續使用精靈來設定練習執行組態，而不啟用自動換檔。
6. 選擇資源練習執行的選項。對於鬧鐘，您可以執行以下操作：

   - (必要) 指定結果警示，以監視此資源的練習執行。
   - (選擇性) 為此資源的練習執行指定封鎖警示。

   如需詳細資訊，請參閱中的〈為練習執行指定的警示〉一節設定區域自動換檔時的最佳作法。

7. 選擇性地指定封鎖日期和封鎖的時段。選擇日期或時段 (天數與時間)，以阻止 Route 53 ARC 開始執行此資源的實務執行。所有日期和時間均為 UTC。
8. 選取核取方塊以確認您已閱讀確認備註。
9. 選擇建立。

若要編輯練習執行組態

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域自動切換。
3. 在資源區域自動工作班次組態下，選擇資源。
4. 在 [動作] 功能表中，選擇 [編輯練習執行組態]。
5. 變更練習執行組態，以執行下列一或多項作業：
   - 對於鬧鐘，您可以執行以下操作：
     - 對於阻塞警報，您可以添加警報，刪除警報或指定不同的阻塞警報。
     - 對於監控練習運行的結果警報，您可以指定要使用的不同 CloudWatch 警報。需要結果警示，因此您無法刪除結果警示。
   - 對於封鎖的日期和封鎖的視窗，您可以新增日期或日期和時間，或移除或更新現有的日期或日期和時間。所有日期和時間均為 UTC。
6. 選擇儲存。

若要刪除練習執行組態

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域自動切換。
3. 在資源區域自動工作班次組態下，選擇資源。
4. 在 [動作] 功能表中，選擇 [刪除練習執行組態]。
5. 在確認強制回應對話方塊中，輸入`Delete`，然後選擇 [刪除]。

   請注意，刪除控制台中的練習運行配置也會禁用資源的區域自動切換。區域自動換檔需要為資源配置練習運行。

取消練習運行區域移位

本節中的步驟說明如何在 Amazon Route 53 應用程式復原控制器主控台上取消區域轉移。若要以程式設計方式使用區域移位和區域自動切換，請參閱區域偏移和區域自動切換 API 參考指南。

您可以取消您自己啟動的區域班次。您也可以取消針對區域自 AWS 動班次執行練習執行的資源開始的區域班次。

取消練習執行區域偏移的步驟

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域偏移。
3. 選取您要取消的區域偏移量，然後選擇「取消區域偏移量」。
4. 在確認強制回應對話方塊中，選擇確認。

記錄和監控 Amazon Route 53 應用程式復原控制器中的區域自動換檔

您可以使用 AWS CloudTrail 和 Amazon 監控 Amazon EventBridge Route 53 應用程式復原控制器中的區域自動換檔，以分析模式並協助疑難排解問題。

主題

- 使用記錄區域自動切換 API 呼叫 AWS CloudTrail
- 使用區域自動換檔與 Amazon EventBridge

使用記錄區域自動切換 API 呼叫 AWS CloudTrail

Amazon Route 53 應用程式復原控制器的區域自動切換功能與整合 AWS CloudTrail，這項服務可提供 Route 53 ARC 中使用者、角色或 AWS 服務所採取動作的記錄。 CloudTrail 將區域移位的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Route 53 ARC 主控台的呼叫，以及針對區域移位的 Route 53 ARC API 作業的程式碼呼叫。

如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括區域轉移的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 Route 53 ARC 進行區域轉移的要求、提出請求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

區域自動換檔資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當 Route 53 ARC 中針對區域自動換檔發生活動時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄。

如需正在進行的事件記錄 AWS 帳戶，包括 Route 53 ARC 中區域自動切換的事件，請建立軌跡。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

所有 Route 53 ARC 動作都由記錄下來， CloudTrail 並記錄在 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南中。例如，呼叫`StartZonalShift`和動`ListManagedResources`作會在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

在事件歷史記錄中查看 Route 53 ARC 事件

CloudTrail 可讓您在事件歷史記錄中檢視最近的事件。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。

瞭解區域自動切換記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範區域自動切換`ListManagedResources`動作之動作的 CloudTrail 記錄項目。


```
{
      "eventVersion": "1.08",
      "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
          "sessionIssuer": {
            "type": "Role",
            "principalId": "AROA33L3W36EXAMPLE",
            "arn": "arn:aws:iam::111122223333:role/admin",
            "accountId": "111122223333",
            "userName": "EXAMPLENAME"
          },
          "webIdFederationData": {},
          "attributes": {
            "creationDate": "2022-11-14T16:01:51Z",
            "mfaAuthenticated": "false"
          }
        }
      },
      "eventTime": "2022-11-14T16:14:41Z",
      "eventSource": "arc-zonal-shift.amazonaws.com",
      "eventName": "ListManagedResources",
      "awsRegion": "us-west-2",
      "sourceIPAddress": "192.0.2.50",
      "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
      "requestParameters": null,
      "responseElements": null,
      "requestID": "VGXG4ZUE7UZTVCMTJGIAF_EXAMPLE",
      "eventID": "4b5c42df-1174-46c8-be99-d67_EXAMPLE",
```

```
      "readOnly": true,
      "eventType": "AwsApiCall",
      "managementEvent": true,
      "recipientAccountId": "111122223333"
      "eventCategory": "Management"
      }
    }
```

使用區域自動換檔與 Amazon EventBridge

使用 Amazon EventBridge，您可以設定事件驅動的規則，以監控區域自動換檔資源，並啟動使用其他服務的目標動作。 AWS 例如，您可以設定傳送電子郵件通知的規則，方法是在區域自動切換的練習執行開始時，傳送 Amazon SNS 主題。

您可以在 Amazon 中創建規則以對區域自動 EventBridge 換檔採取行動。區域自動換檔事件的事件會指定有關練習執行自動換檔的狀態資訊，例如，當練習執行正在進行中。

若要擷取您感興趣的特定區域自動切換事件，請定義 EventBridge 可用來偵測事件的特定事件模式。事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

盡可能發出事件。 EventBridge 在正常操作情況下，它們是從 53 ARC 公路交付到近乎實時的。但是，可能會出現可能會延遲或阻止事件傳遞的情況。

如需 EventBridge 規則如何處理事件模式的詳細資訊，請參閱 EventBridge.

使用以下方式監控區域自動換檔資源 EventBridge

使用 EventBridge，您可以建立規則，以定義 Route 53 ARC 為其資源發出事件時要採取的動作。例如，您可以建立規則，在區域自動切換的練習執行開始時傳送電子郵件訊息。

若要在主控台中輸入或複製事件模式並貼上，請選取要在 EventBridge 主控台中使用 [輸入我自己的] 選項的選項。為了協助您判斷可能對您有用的事件模式，本主題包含您可以使用的區域自動切換事件比對模式和區域自動切換事件的範例。

建立資源事件的規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇您 AWS 區域 要在其中建立規則的地區，也就是您有興趣觀看賽事的地區。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的Name (名稱)，或者輸入描述。
5. 對於事件匯流排，保留預設值 (預設值)。

6. 選擇下一步。
7. 對於「建置」事件模式步驟，對於事件來源，保留預設值「AWS 事件」。
8. 在 [範例事件] 下，選擇 [輸入我自己]。
9. 對於範例事件，請輸入或複製並貼上事件模式。

範例區域自動換檔事件模式

事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

您可以將此區段中的事件模式複製並貼 EventBridge 到中，以建立可用來監視區域自動切換動作和資源的規則。

當您為區域自動切換事件建立事件模式時，您可以為下列項目指定下列任一項目：`detail-type`

- `Autoshift In Progress`
- `Autoshift Completed`
- `Practice Run Started`
- `Practice Run Succeeded`
- `Practice Run Interrupted`
- `Practice Run Failed`

當練習執行中斷時，有關造成中斷的原因的詳細資訊，請參閱`additionalFailureInfo`欄位。

- 從已開始練習執行的區域自動換檔中選取所有事件。 。

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Started"
    ]
}
```

- 從練習運行失敗的區域自動換檔中選擇所有事件。 。

```
{
    "source": [
```

```
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Practice Run Failed"
    ]
}
```

範例區域自動換檔事件

以下是區域自動切換動作的範例事件：

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Practice Run Interrupted",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [
        "TEST-EXAMPLE-2023-11-16-23-28-11-5"
    ],
    "detail": {
        "version": "0.0.1",
        "data": {
            "additionalFailureInfo": "Practice run interrupted. The blocking alarm
 entered ALARM state."
        },
        "metadata": {
            "awayFrom": "use1-az2"
        }
    }
}
```

指定要用作目標的 CloudWatch 記錄群組

建立 EventBridge 規則時，您必須指定傳送符合規則之事件的目標。如需的可用目標清單 EventBridge，請參閱 EventBridge 主控台中可用的目標。您可以新增至 EventBridge 規則的其中一個目標是 Amazon CloudWatch 日誌群組。本節說明將 CloudWatch 記錄群組新增為目標的需求，並提供在建立規則時新增記錄群組的程序。

若要將 CloudWatch 記錄群組新增為目標，您可以執行下列其中一項作業：

- 建立新的記錄群組
- 選擇現有的記錄群組

如果您在建立規則時使用主控台指定新的記錄群組，EventBridge 會自動為您建立記錄群組。請確定您用作 EventBridge 規則目標的記錄群組開頭為/aws/events。如果您想要選擇現有的記錄群組，請注意，只有開頭為的記錄群組/aws/events會顯示為下拉式功能表中的選項。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立新日誌群組。

如果您使用主控台外部的 CloudWatch 作業來建立或使用 CloudWatch 記錄群組做為目標，請確定您已正確設定權限。如果您使用主控台將記錄群組新增至 EventBridge 規則，則記錄群組的資源型政策會自動更新。但是，如果您使用 AWS Command Line Interface 或 AWS SDK 來指定記錄群組，則必須更新記錄群組的以資源為基礎的原則。下列範例原則說明您必須在記錄群組的資源型原則中定義的權限：

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

您無法使用主控台為記錄群組設定以資源為基礎的政策。若要將必要的權限新增至以資源為基礎的政策，請使用 CloudWatch PutResourcePolicyAPI 作業。然後，您可以使用 describe-resource-policiesCLI 命令來檢查您的原則是否已正確套用。

為資源事件建立規則並指定 CloudWatch 記錄群組目標

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇您 AWS 區域 要在其中建立規則的規則。
3. 選擇 [建立規則]，然後輸入有關該規則的任何資訊，例如事件模式或排程詳細資訊。

   若要取得有關為 Route 53 ARC 建立 EventBridge 規則的詳細資訊，請參閱本主題稍早的章節。
4. 在 「選擇目標」 頁面上，選擇CloudWatch作為您的目標。
5. 從下拉式功能表中選擇 CloudWatch 記錄群組。

區域自動換檔的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Route 53 ARC 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

目錄

- Amazon Route 53 應用程式復原控制器中的區域自動切換如何搭配 IAM 搭配
- 區域自動切換的身分識別原則範例
- 在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔
- AWS Amazon Route 53 應用程式復原控制器中區域自動切換的受管政策

Amazon Route 53 應用程式復原控制器中的區域自動切換如何搭配 IAM 搭配

在您使用 IAM 管理 Amazon Route 53 應用程式復原控制器中區域自動換檔的存取權限之前，請先了解哪些 IAM 功能可搭配區域自動換檔使用。

您可以在 Amazon Route 53 應用程式復原控制器中搭配區域自動換檔使用的 IAM 功能

IAM 功能	支援區域自動換檔
身分型政策	是
資源型政策	否
政策動作	是

IAM 功能	支援區域自動換檔
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要取得 AWS 服務如何搭配大多數 IAM 功能運作的高階整體檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Route 53 ARC 的基於身份的政策

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

若要檢視 Route 53 ARC 身分識別型原則的範例，請參閱。Amazon Route 53 應用程式復原控制器中的身分識別型政策範例

Route 53 內的資源型政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。

Route 53 的政策行動

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看區域自動切換的 Route 53 ARC 動作清單，請參閱服務授權參考資料中的 Amazon Route 53 區域轉移所定義的動作。

Route 53 ARC 中針對區域自動切換的原則動作會在動作之前使用下列前置詞：

```
arc-zonal-shift
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，以下內容：

```
"Action": [
      "arc-zonal-shift:action1",
      "arc-zonal-shift:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 `Describe` 文字的所有動作，請包含以下動作：

```
"Action": "arc-zonal-shift:Describe*"
```

若要檢視 Route 53 ARC 以身分識別為基礎的區域自動切換原則範例，請參閱。區域自動切換的身分識別原則範例

Route 53 ARC 中區域自動換檔的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

`Resource` JSON 政策元素可指定要套用動作的物件。陳述式必須包含 `Resource` 或 `NotResource` 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看資源類型及其 ARN 的清單，以及您可以使用每個資源的 ARN 指定的動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 定義的行動-區域移位

若要查看可搭配條件索引鍵使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 定義的條件鍵-區域移位

若要檢視 Route 53 ARC 以身分識別為基礎的區域自動切換原則範例，請參閱。區域自動切換的身分識別原則範例

Route 53 ARC 中區域自動切換的政策條件鍵

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看區域自動切換的 Route 53 ARC 條件金鑰清單，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 區域移位的條件鍵

若要查看可搭配條件索引鍵使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 區域移位定義的操作

若要檢視 Route 53 ARC 以身分識別為基礎的區域自動切換原則範例，請參閱。區域自動切換的身分識別原則範例

Route 53 中的訪問控制列表（ACL）

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

基於屬性的訪問控制（ABAC）與 Route 53 ARC

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

Route 53 弧中的區域自動換檔包括對 ABAC 的以下部分支持：

- 區域自動換檔支援 ABAC，用於在 Route 53 ARC 中註冊用於區域移位的受管資源。如需適用於 Network Load Balancer 和應用程式負載平衡器管理資源的 ABAC 詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的 Elastic Load Balancing ABAC。

使用臨時登入資料與 Route 53 ARC

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而非使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Route 53 ARC 的跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 實體 (使用者或角色) 在中執行動作時 AWS，您會被視為主體。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。

若要查看動作是否需要原則中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 區域轉移

Route 53 ARC 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

Route 53 ARC 的服務連結角色

支援服務連結角色	是

服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 Route 53 ARC 服務連結角色的詳細資訊，請參閱在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

區域自動切換的身分識別原則範例

根據預設，使用者和角色沒有建立或修改 Route 53 ARC 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授

予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Route 53 ARC 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon Route 53 應用程式復原控制器的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 範例：區域自動換檔主控台存取
- 範例：Route 53 ARC API 動作

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 Route 53 ARC 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定 AWS 服務) 使用 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

範例：區域自動換檔主控台存取

若要存取 Amazon Route 53 應用程式復原控制器主控台，您必須擁有至少一組許可。這些權限必須允許您列出和查看有關 Route 53 ARC 資源的詳細信息 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要執行某些工作，使用者必須擁有建立與 Route 53 ARC 中區域自動切換相關聯的服務連結角色的權限。如需進一步了解，請參閱在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔。

若要讓使用者擁有在中使用區域自動切換的完整存取權 AWS Management Console，請將如下原則附加至使用者：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
                   "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
```

```
        {
            "Effect": "Allow",
            "Action": "ec2:DescribeAvailabilityZones",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "cloudwatch:DescribeAlarms",
            "Resource": "*"
        }
    ]
}
```

範例：Route 53 ARC API 動作

您可以使用原則來確保使用者可以針對區域自動切換使用 Route 53 ARC API 動作來設定區域自動切換，以便代表您將應用程式資源流量從可用區域轉 AWS 移到中運作良好的 AZ，以協助縮短事件期間復原的時間。 AWS 區域若要提供這些權限，請附加與使用者需要使用的 API 作業對應的原則，如下所述。

若要執行某些工作，使用者必須擁有與 Route 53 ARC 相關聯之服務連結角色的權限。下列範例原則包含建立服務連結角色所需的權限。如需進一步了解，請參閱在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔。

若要使用區域自動切換的 API 作業，請將下列原則附加至使用者：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "arc-zonal-shift:ListManagedResources",
                   "arc-zonal-shift:GetManagedResource",
                   "arc-zonal-shift:ListZonalShifts",
                   "arc-zonal-shift:StartZonalShift",
                   "arc-zonal-shift:UpdateZonalShift",
                   "arc-zonal-shift:CancelZonalShift",
                   "arc-zonal-shift:CreatePracticeRunConfiguration",
                   "arc-zonal-shift:DeletePracticeRunConfiguration",
                   "arc-zonal-shift:ListAutoshifts",
                   "arc-zonal-shift:UpdatePracticeRunConfiguration",
```

```
                    "arc-zonal-shift:UpdateZonalAutoshiftConfiguration"
             ],
            "Resource": "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                    "cloudwatch:DescribeAlarms",
                    "health:DescribeEvents"
            ],
            "Resource" : "*"
        },
        {
            "Effect" : "Allow",
            "Action" : [
                    "arc-zonal-shift:CancelZonalShift",
                    "arc-zonal-shift:GetManagedResource",
                    "arc-zonal-shift:StartZonalShift",
                    "arc-zonal-shift:UpdateZonalShift"
            ],
            "Resource" : "*"
        }
    ]
}
```

在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔

Amazon Route 53 應用程式復原控制器中的區域自動切換使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至服務的唯一 IAM 角色類型，在本例中為 Route 53 ARC。服務連結角色由 Route 53 ARC 預先定義，包含服務為特定目的代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓您更輕鬆地設定 Route 53 ARC，因為您不需要手動新增必要的權限。Route 53 ARC 會定義服務連結角色的權限，除非另有定義，否則只有 Route 53 ARC 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可以保護您的 Route 53 ARC 區域自動換檔資源，因為您無法不小心移除存取資源的權限。

如需其他支援服務連結角色之服AWS 務的相關資訊，請參閱搭配 IAM 使用的服務，並在服務連結角色欄中尋找具有 Yes 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

服務連結角色權限 AWSServiceRoleForZonalAutoshiftPracticeRun

Route 53 ARC 會使用名為的服務連結角色AWSServiceRoleForZonalAutoshiftPracticeRun來執行下列作業：

- 監控客戶提供的 Amazon CloudWatch 警示和客戶 AWS Health Dashboard 事件以進行實務執行
- 管理練習運行（練習區域轉移）

本節說明服務連結角色的權限，以及建立、編輯和刪除角色的相關資訊。

服務連結角色權限 AWSServiceRoleForZonalAutoshiftPracticeRun

此服務連結角色使用受管理策略`AWSZonalAutoshiftPracticeRunSLRPolicy`。

服AWSServiceRoleForZonalAutoshiftPracticeRun務連結角色會信任下列服務擔任該角色：

- `practice-run.arc-zonal-shift.amazonaws.com`

若要檢視此原則的權限，請參閱AWS 受管理AWSZonalAutoshiftPracticeRunSLRPolicy的策略參考中的。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

建立路 Route 53 ARC 的AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色

您不需要手動建立AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色。當您在 AWS Management Console、或 AWS SDK 中建立第一個練習執行設定時 AWS CLI，Route 53 ARC 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立第一個練習執行組態時，Route 53 ARC 會再次為您建立服務連結角色。

編輯路 Route 53 ARC 的AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色

Route 53 ARC 不允許您編輯AWSServiceRoleForZonalAutoshiftPracticeRun服務連結的角色。建立服務連結角色之後，您無法變更角色的名稱，因為其他實體可能會參照該角色。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除 Route 53 ARC 的AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。不過，您必須先清除服務連結角色的資源，才能手動刪除該角色。

停用自動切換後，您可以刪除AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色。如需自動切換功能的詳細資訊，請參閱Amazon Route 53 應用程序恢復控制器的區域轉移。

> **Note**
>
> 如果 Route 53 ARC 服務在您嘗試刪除資源時使用該角色，則服務角色刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試刪除角色。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色。AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

更新 Route 53 ARC 服務連結角色，適用於區域自動換檔

如需 Route 53 ARC 服務連結角色之 AWS 受管理原則的更新，請參閱 Route 53 ARC 的AWS 受管理原則更新表格。您也可以在 Route 53 ARC 文件歷史記錄頁面上訂閱自動 RSS 警示。

AWS Amazon Route 53 應用程式復原控制器中區域自動切換的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略： AWSZonalAutoshiftPracticeRunSLRPolicy

您不得將 `AWSZonalAutoshiftPracticeRunSLRPolicy` 連接到 IAM 實體。此政策附加至服務連結角色，該角色允許 Amazon Route 53 應用程式復原控制器針對區域自動切換執行下列動作：

- 監控客戶提供的 Amazon CloudWatch 警示和客戶 AWS Health Dashboard 事件以進行實務執行
- 管理練習運行（練習區域轉移）

如需詳細資訊，請參閱 在 Route 53 ARC 中使用服務鏈接角色進行區域自動換檔。

區域自動 AWS 切換的受管原則更新

如需有關 Route 53 ARC 自此服務開始追蹤這些變更以來區域自動切換 AWS 受管政策的更新詳細資訊，請參閱。Amazon Route 53 應用程式復原控制器的 AWS 受管政策更新如需有關此頁面變更的自動警示，請訂閱 Route 53 ARC 文件歷史記錄頁面上的 RSS 摘要。

使用路由控制復原 Amazon Route 53 應用程式復原控制器中的多區域應用程式

本節說明如何使用 Amazon Route 53 應用程式復原控制器中的路由控制功能，將干擾降到最低，並在您將 AWS 應用程式部署為多個使用者提供連續性 AWS 區域。

您還可以了解準備程度檢查，這是 Route 53 ARC 中的一項功能，可用於深入瞭解應用程式和資源是否已準備好進行復原。

本節中的主題說明路由控制和整備程度檢查功能、如何設定它們以及如何使用它們。

主題

- Amazon 路由 53 應用程式復原控制器中的路由
- Amazon 路線 53 應用程序恢復控制器中的準備

Amazon 路由 53 應用程式復原控制器中的路由

若要容錯移轉到多個應用程式複本的流量 AWS 區域，您可以使用 Amazon Route 53 應用程式復原控制器中的路由控制，該控制器與 Amazon Route 53 中的特定運作狀態檢查整合。路由控制是簡單的開關開關，可讓您將用戶端流量從一個區域複本切換到另一個區域複本。流量重新路由是透過使用 Amazon Route 53 DNS 記錄設定的路由控制運作狀態檢查來完成。例如，DNS 容錯移轉記錄，與每個區域中應用程式複本前面的網域名稱相關聯。

本節說明路由控制的運作方式、如何設定路由控制元件，以及如何使用它們重新路由傳送流量以進行容錯移轉。

Route 53 ARC 中的路由控制元件包括：叢集、控制面板、路由控制和路由控制健康狀態檢查。所有路由控制項都分組在控制面板上。您可以在 Route 53 ARC 為叢集建立的預設控制台上將它們分組，或建立您自己的自訂控制面板。您必須先建立叢集，才能建立控制台或路由控制項。Route 53 ARC 中的每個集群都是五個端點的數據平面 AWS 區域。

建立路由控制項和路由控制健全狀況檢查之後，您可以建立路由控制的安全規則，以協助避免意外復原自動化副作用。您可以使用或 API 動作 (建議) 或使用.，更新路由控制狀態，以個別 AWS CLI 或批次重新路由流量的路由。 AWS Management Console

本節說明路由控制項的運作方式，以及如何建立和使用這些控制項來重新路由傳送應用程式的流量。

> **Important**
>
> 若要瞭解如何準備使用 Route 53 ARC 重新路由傳送流量，做為應用程式在災難情況下的容錯移轉計畫的一部分，請參閱路 Route 53 ARC 中路由控制的最佳實踐。

關於路由控制

路由控制會使用 Amazon Route 53 中的運作狀態檢查重新導向流量，這些檢查設定為與復原群組中儲存格頂層資源 (例如 Elastic Load Balancing 器) 相關聯的 DNS 記錄。您可以將流量從一個儲存格重新導向至另一個儲存格，例如，將路由控制狀態更新為 0ff (以停止流量到一個儲存格)，然後將另一個路由控制狀態更新為 0n (以啟動流量到另一個儲存格)。變更流量流程的程序是與路由控制項相關聯的 Route 53 健康狀態檢查，在 Route 53 ARC 根據對應的路由控制狀態更新後，將其設定為狀況良好或不良狀態。

路由控制支援具有 DNS 端點的任何 AWS 服務之間的容錯移轉。您可以將路由控制狀態更新為容錯移轉流量以進行災難復原，或是偵測到應用程式的延遲下降或其他問題時。

您也可以設定路由控制的安全規則，以確保使用路由控制項重新路由傳送流量不會影響可用性。如需詳細資訊，請參閱 建立路由控制的安全規則 。

請務必注意，路由控制項本身並不是監控端點基礎健康狀態的健康狀態檢查。例如，與 Route 53 健康狀態檢查不同，路由控制項不會監視回應時間或 TCP 連線時間。路由控制是一種簡單的開關，可控制健康狀態檢查。一般而言，您可以將狀態變更為重新導向流量，而且該狀態變更會將流量移至整個應用程式堆疊的特定端點，或防止路由傳送至整個應用程式堆疊。例如，在簡單的案例中，當您將路由控制狀態從變更0n為時0ff，它會更新 Route 53 健全狀況檢查，您已與 DNS 容錯移轉記錄相關聯，以便將流量移出端點。

如何使用路由控制

若要更新路由控制狀態，以便重新路由傳送流量，您必須連線到 Route 53 ARC 中的其中一個叢集端點。如果您嘗試連線的端點無法使用，請嘗試使用另一個叢集端點變更狀態。您變更路由控制狀態的程序應準備好輪替嘗試每個端點，因為叢集端點會在可用和無法使用的狀態中循環，以進行定期維護和更新。

當您建立路由控制項時，您可以設定 DNS 記錄，將路由控制健全狀況檢查與每個應用程式複本前面的 Route 53 DNS 名稱產生關聯。例如，若要控制跨兩個負載平衡器 (兩個區域中各一個) 的流量容錯移轉，您可以建立兩個路由控制健全狀況檢查，並將它們與兩個 DNS 記錄產生關聯，例如，具有容錯移轉路由原則的別名記錄，以及各自負載平衡器的網域名稱。

您也可以使用 Route 53 ARC 路由控制搭配 Route 53 ARC 路由控制以及 Route 53 健全狀況檢查和 DNS 記錄集，使用 DNS 記錄搭配加權路由原則，設定更複雜的流量容錯移轉案例。若要查看詳細範例，請參閱下列部落格文章中有關容錯移轉使用者流量的 AWS 章節：使用 Amazon Route 53 應用程式復原控制器建置高彈性應用程式，第 2 部分：多區域堆疊

當您啟動 AWS 區域 使用路由控制項的容錯移轉時，由於流量流程涉及的步驟，您可能看不到流量立即移出區域。根據用戶端行為和連線重複使用，區域中的現有進行中連線也可能需要很短的時間才能完成。視您的 DNS 設定和其他因素而定，現有的連線可能會在幾分鐘內完成，或可能需要更長的時間。如需詳細資訊，請參閱確保流量轉移快速完成。

如何使用路由控制

Route 53 ARC 中的路由控制比使用傳統健康狀態檢查重新路由流量有許多好處。例如：

- 路由控制項可讓您容錯移轉整個應用程式堆疊。這與基於資源級運作狀態檢查的 Amazon EC2 執行個體一樣，容錯處理堆疊的個別元件有所不同。
- 路由控制提供您安全、簡單的手動覆寫功能，可用來轉移流量以進行維護，或在內部監視器未偵測到問題時從故障中復原。
- 您可以將路由控制與安全規則搭配使用，以防止全自動運作狀態檢查型自動化可能發生的常見副作用，例如容錯移轉至尚未準備好進行容錯移轉的待命基礎結構。

以下是將路由控制納入容錯移轉策略的範例，以改善應用程式中應用程式的彈性和可用性 AWS。

您可以跨區域執行多個 (通常為三個) 備援複本，以支援高可用性 AWS 應用程式。 AWS 然後，您可以使用 Amazon Route 53 路由控制將流量路由到適當的複本。

例如，您可以將一個應用程式複本設定為作用中並提供應用程式流量，而另一個則是待命複本。當使用中複本發生故障時，您可以在該處重新路由使用者流量，以還原應用程式的可用性。您應該根據監視和健全狀況檢查系統的資訊，決定是否要離開或離開複本。

如果您想要啟用更快的復原速度，您可以為架構選擇另一個選項是主動-主動式實作。使用這種方法，您的複本會同時處於作用中狀態。這表示您只需將流量重新路由傳送至另一個作用中複本，即可將使用者從受損的應用程式複本移開，從失敗中復原。

AWS 路由控制的可用區域

如需 Amazon Route 53 應用程式復原控制器的區域支援和服務端點的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器端點和 Amazon Web Services 一般參考中的配額。

> **Note**
>
> Amazon Route 53 應用程式復原控制器中的路由控制是一項全域功能。但是，您必須在區域 Route 53 ARC 指 AWS CLI 令中指定美國西部 (奧勒岡`--region us-west-2`) 區域 (指定參數)。也就是說，當您建立叢集、控制台或路由控制項等資源時。

Route 53 ARC 路由控制是一種開/關切換開關，可變更 Route 53 ARC 健全狀況檢查的狀態，然後該記錄可與重新導向流量的 DNS 記錄相關聯，例如，從主要部署複本到待命部署複本。

如果發生應用程式失敗或延遲問題，您可以更新路由控制狀態，將流量從主要複本轉移到 (例如待命複本)。透過使用高度可靠的 Route 53 ARC 資料平面 API 作業來進行路由控制查詢和路由控制狀態更新，您可以仰賴 Route 53 ARC 在災難復原案例期間進行容錯移轉。如需詳細資訊，請參閱 使用路由 Route 53 ARC API 取得和更新路由控制狀態 (建議使用)。

Route 53 ARC 會在叢集中維護路由控制狀態，這是一組五個備援區域端點。Route 53 ARC 會將路由控制狀態變更傳播到位於 Amazon EC2 叢集中的叢集，以取得跨五個 AWS 區域的仲裁。傳播後，當您查詢 Route 53 ARC 的路由控制狀態，使用 API 和高度可靠的數據平面，它返回一致視圖。

您可以與五個叢集端點中的任何一個互動，以將路由控制的狀態從 (例如，更新`Off`為) `On`。然後，Route 53 ARC 會將更新傳播到叢集的五個區域。

所有五個叢集端點之間的資料一致性平均在 5 秒內達成，且最長不超過 15 秒。

Route 53 ARC 透過其資料平面提供極高的可靠性，可讓您跨儲存格手動容錯移轉應用程式。Route 53 ARC 可確保您始終可以存取五個叢集端點中的至少三個，以執行路由控制狀態變更。請注意，每個 Route 53 ARC 叢集都是單一租用戶，以確保您不會受到可能拖慢存取模式的「雜訊鄰居」的影響。

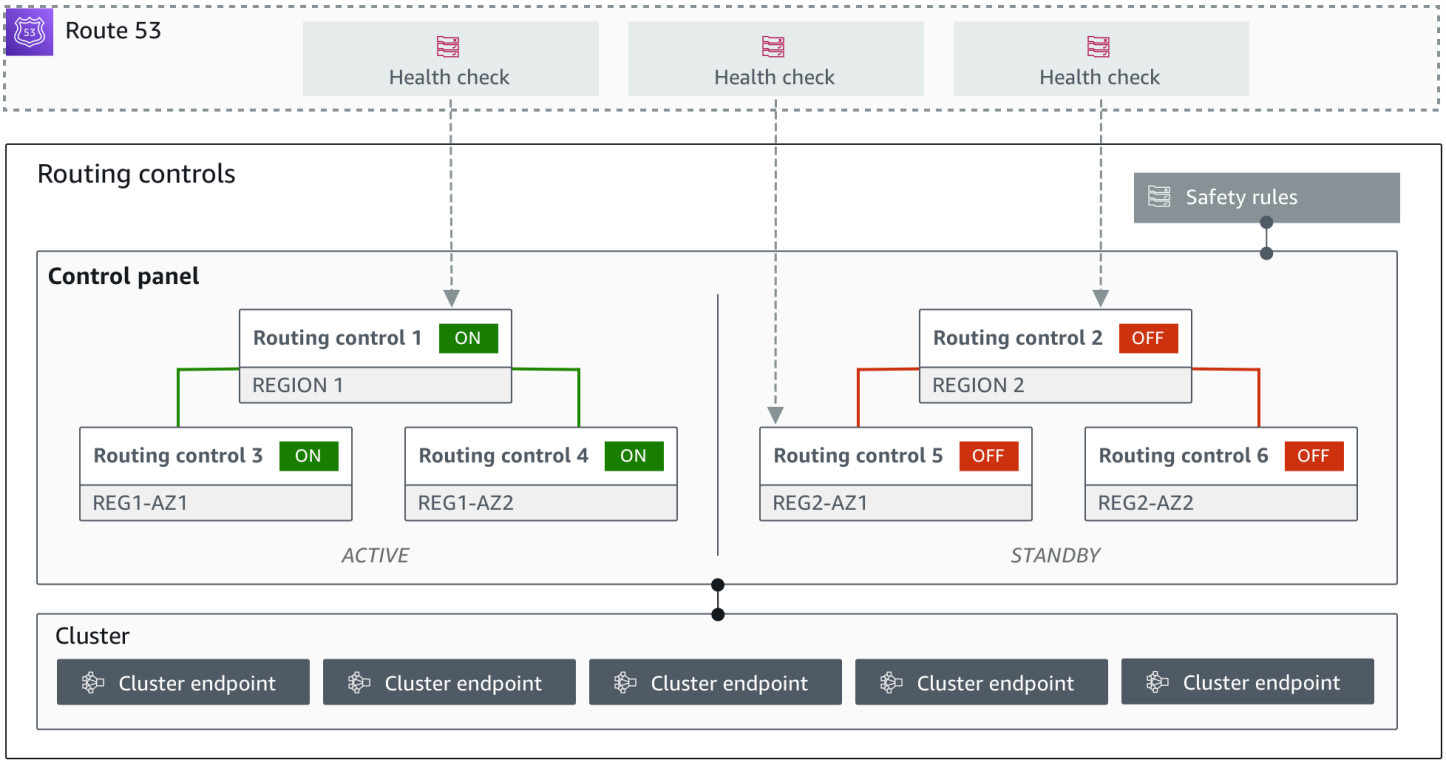
當您變更路由控制狀態時，您必須仰賴下列三個條件，這三個條件極不可能失敗：

- 您的五個端點中至少有三個可用，並參與仲裁。
- 您擁有有效的 IAM 登入資料，並且可以對有效的區域叢集端點進行驗證。
- Route 53 資料平面狀態良好 (此資料平面設計為符合 100% 可用性 SLA)。

路由控制元件

下圖說明在 Route 53 ARC 中支援繞線控制特徵的零組件的範例。此處顯示的路由控制項 (分組為一個控制台) 可讓您管理兩個區域中每個區域中兩個可用區域的流量。當您更新路由控制狀態時，Route 53

ARC 會變更 Amazon Route 53 中的運作狀態檢查，以便將 DNS 流量重新導向至不同的儲存格。您為路由控制項設定的安全規則有助於避免失敗開啟案例和其他意外後果。



以下是 Route 53 ARC 中線路設計控制特徵的零組件。

叢集

叢集是一組五個備援的區域端點，您可以根據這些端點起始 API 呼叫以更新或取得路由控制狀態。叢集包含預設控制台，您可以在一個叢集上裝載多個控制台和路由控制項。

路由控制

路由控制是一種簡單的開/關切換開關，裝載於叢集上，可用來控制用戶端流量進出儲存格的路由。當您產生線路設計控制時，您可以在路線 53 中加入 Route 53 ARC 健康檢查。當您更新 Route 53 ARC 中的路由控制狀態時，這可讓您重新路由傳送流量 (使用針對應用程式的 DNS 記錄設定的健全狀況檢查)。

路由控制健康檢查

路由控制項與 Route 53 中的健康檢查相整合。健全狀況檢查與每個應用程式複本前面的 DNS 記錄相關聯，例如容錯移轉記錄。當您變更路由控制狀態時，Route 53 ARC 會更新對應的健康狀態檢查，以便將流量重新導向 (例如，容錯移轉至待命複本)。

控制面板

控制面板將一組相關的路由控制項群組在一起。您可以將多個路由控制項與一個控制台相關聯，然後建立控制台的安全規則，以確保您所建立的流量重新導向更新是安全的。例如，您可以為每個可用區域中的每個負載平衡器設定路由控制項，然後將它們分組在相同的控制台中。然後，您可以新增安全規則 (「宣告規則」)，以確保至少有一個區域 (由路由控制項表示) 在任何時間處於作用中狀態，以避免意外的「失敗開啟」案例。

預設控制面板

當您建立叢集時，Route 53 ARC 會建立預設的控制面板。根據預設，您在叢集上建立的所有路由控制項都會新增至預設控制台。或者，您可以建立自己的控制台，將相關的路由控制項分組。

安全規則

安全規則是您新增至路由控制項的規則，以確保復原動作不會意外損害應用程式的可用性。例如，您可以建立安全規則來建立路由控制，做為整體「開啟/關閉」開關，以便您可以啟用或停用一組其他路由控制項。

端點 (叢集端點)

Route 53 ARC 中的每個叢集都有五個區域端點，可用於設定和擷取路由控制狀態。您存取端點的程序應假設 Route 53 ARC 會定期啟動和關閉端點以進行維護，因此您應該連續嘗試每個端點，直到連線到端點為止。您可以存取端點以取得路由控制的目前狀態 (開啟或關閉)，並透過變更路由控制狀態來觸發應用程式的容錯移轉。

用於路由控制的資料和控制平面

當您規劃容錯移轉和災難復原時，請考慮容錯移轉機制的彈性。我們建議您確保在容錯移轉期間所依賴的機制具有高可用性，以便在災難情況下需要時可以使用它們。一般而言，您應該隨時為您的機制使用資料平面函數，以獲得最大的可靠性和容錯能力。考慮到這一點，重要的是要了解服務的功能如何在控制平面和數據平面之間劃分，以及何時可以依賴服務數據層面對極高可靠性的期望。

與大多數 AWS 服務一樣，路由控制平面和資料平面支援路由控制功能的功能。雖然這兩者都是為了可靠而建置，但控制平面已針對資料一致性進行了最佳化，而資料平面則針對可用性進行最佳化。資料平面是專為復原而設計的，因此即使在中斷性事件期間，控制平面可能無法使用時，也能維持可用性。

一般而言，控制平面可讓您執行基本的管理功能，例如建立、更新和刪除服務中的資源。資料平面提供服務的核心功能。因此，建議您在可用性很重要時使用資料平面作業，例如當您需要在中斷期間將流量重新路由傳送至待命複本時。

對於佈線控制，控制平面和資料平面分割如下：

- 路由控制的控制平面 API 是復原控制組態 API，支援美國西部 (奧勒岡) 區域 (us-west-2)。您可以使用這些 API 作業或建立或刪除叢集、控制台和路由控制項，以協助您準備災難復原事件，當您可能需要為應用程式重新路由傳送流量時。 AWS Management Console 路由控制組態控制平面不具高可用性。
- 路由控制資料平面是跨越五個地理位置 AWS 隔離區域的專用叢集。每位客戶都使用路由控制平面建立一或多個叢集。叢集主控控制台和路由控制項。然後，當您想要重新路由傳送應用程式的流量時，您可以使用路由控制 (復原叢集) API 來取得、列出和更新路由控制狀態。路由控制資料平面具有高可用性。

由於路由控制資料平面具有高可用性，因此當您想要容錯移轉以從事件復原時，建議您計劃使用來進行 API 呼叫，以便處理路由控制狀態。 AWS Command Line Interface 如需使用製程控制來準備並完成復原作業時的主要考量事項的詳細資訊，請參閱路 Route 53 ARC 中路由控制的最佳實踐。

如需有關資料平面、控制平面以及如何 AWS 建置服務以符合高可用性目標的詳細資訊，請參閱 Amazon Builders' Library 中的使用可用區域的靜態穩定性 paper。

Amazon Route 53 應用程式復原控制器中的路由控制標

標記是您用來識別和組織資源的單字或片語 (中繼 AWS 資料)。可以新增多個標籤到每個資源，且每個標籤皆包含您所定義的金鑰和值。例如，關鍵字可能是環境，而值可能是生產環境。可以根據新增的標籤來搜尋與篩選資源。

您可以在 Route 53 ARC 的路由控制中標記下列資源：

- 叢集
- 控制面板
- 安全規則

路由 53 ARC 中的標記只能透過 API 使用，例如，使用 AWS CLI.

以下是使用在繞線控制中加標籤的範例 AWS CLI。

```
aws route53-recovery-control-config --region us-west-2 create-cluster --
cluster-name example1-cluster --tags Region=PDX,Stage=Prod
```

```
aws route53-recovery-control-config --region us-west-2 create-control-panel
--control-panel-name example1-control-panel --cluster-arn arn:aws:route53-
```

```
recovery-control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
--tags Region=PDX,Stage=Prod
```

如需詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的復原控制組態 API 參考指南TagResource中的。

路 Route 53 ARC 中路由控制的定價

使用 Amazon Route 53 應用程式復原控制器，您只需為設定在服務中使用的項目付費。對於 Route 53 ARC 中的路由控制，您需要支付您建立的每個叢集的小時費用。每個叢集都可以裝載多個路由控制項，用來觸發應用程式容錯移轉。

為了協助管理成本並提高效率，您可以為叢集設定跨帳戶共用，以便與多個 AWS 帳戶共用一個叢集。如需詳細資訊，請參閱 Support Route 53 ARC 中叢集的跨帳戶。

如需 Route 53 ARC 的詳細定價資訊和定價範例，請參閱 Amazon Route 53 應用程式復原控制器定價，然後向下捲動至 Amazon Route 53 應用程式復原控制器。

開始使用 Amazon Route 53 應用程式復原控制器中的多區域復原

若要使用 Amazon Route 53 應用程式復原控制器中的路由控制容錯移轉應用程式，您必須擁有多個 AWS 應用程式 AWS 區域。若要開始使用，首先，請確定您的應用程式是在每個區域的獨立複本中設定，以便您可以在事件期間從一個容錯移轉到另一個。然後，您可以建立路由控制項，將應用程式流量從主要應用程式容錯移轉至次要應用程式，以維持使用者的連續性。

> **Note**
>
> 如果您的應用程式被可用區域隔離，請考慮使用區域移位或區域自動換檔來進行容錯移轉復原。無需設定即可使用區域移位或區域自動換檔，從可用區域損壞中可靠地復原應用程式。如需詳細資訊，請參閱 使用區域移位和區域自動切換來復原 Amazon Route 53 應用程式復原控制器中的應用程式。

為了讓您可以在事件期間使用 Route 53 ARC 路由控制來復原應用程式，建議您至少設定兩個作為彼此複本的應用程式。每個複本或儲存格都代表一個 AWS 區域. 將應用程式資源設定為與 Region 保持一致之後，請執行下列步驟，確定您的應用程式已設定成功復原。

提示：為了協助簡化設定，我們提供 AWS CloudFormation 和 HashiCorp Terraform 範本，這些範本會建立具有彼此獨立失敗的備援複本的應用程式。若要深入瞭解並下載範本，請參閱設定範例應用程式。

若要準備使用路由控制，請執行下列動作，確定應用程式已設定為具備復原能力：

1. 建立獨立的應用程式堆疊副本 (網路和運算層)，這些複本是每個區域中彼此的複本，以便在發生事件時可以容錯移轉流量。請確定您的應用程式程式碼中沒有任何跨區域相依性，這會導致一個複本失敗影響另一個複本。若要成功容錯移轉 AWS 區域，您的堆疊邊界應位於區域內。
2. 跨複本複製應用程式的所有必要可設定狀態資料。您可以使用資料 AWS 庫服務來協助複製資料。

開始使用流量容錯移轉的路由控制

Amazon Route 53 應用程式復原控制器中的路由控制可讓您觸發容錯移轉，讓流量在單獨 AWS 區域執行的冗餘應用程式副本或複本之間容錯移轉。容錯移轉是使用 Amazon 路由 53 資料平面，透過 DNS 執行。

在每個區域中設定複本之後 (如下一節所述)，您可以將每個複本與路由控制項產生關聯。首先，您要將路由控制項與每個區域中複本的頂層網域名稱建立關聯。然後，您可以將路由控制健全狀況檢查新增至路由控制項，以便它可以開啟和關閉流量流量。這可讓您控制應用程式複本之間的流量路由。

您可以更新中的路由控制狀態 AWS Management Console 以容錯移轉流量，但我們建議您改用 Route 53 ARC 動作 (使用 API) 或 AWS CLI變更它們。API 操作不依賴於控制台，因此它們更具彈性。

例如，若要在區域之間進行容錯移轉 (從 us-west-1 到 us-east-1)，您可以使用 `update-routing-control-state` API 動作將狀態設定為和為。`us-west-1` `Off` `us-east-1` `On`

在您建立路由控制元件以設定應用程式的容錯移轉之前，請確定您的應用程式已孤立到區域複本中，以便您可以從一個複本容錯移轉到另一個複本。若要深入瞭解並開始分隔新應用程式或建立範例堆疊，請參閱下一節。

設定範例應用程式

為了幫助您了解路由控制的工作原理，我們提供了一個名為`TicTacToe`. 該示例使用 AWS CloudFormation 模板來簡化流程，以及帶有示例應用程序的可下載 AWS CloudFormation 和 HashiCorp Terraform 模板，以便您可以自己快速探索 Route 53 ARC 的設置和使用。

部署範例應用程式之後，您可以使用範本建立 Route 53 ARC 元件，然後探索使用路由控制項來管理應用程式的流量。您可以針對自己的案例和應用程式調整範本和程序。

- AWS CloudFormation：若要開始使用範例應用程式和 AWS CloudFormation 範本，請參閱此 Amazon S3 儲存貯體上的 README 指示。您可以閱讀《使用 AWS CloudFormation 者指南》中的AWS CloudFormation 概念，進一步瞭解如何使用 AWS CloudFormation 範本。

- HashiCorp Terraform：若要開始使用範例應用程式和 Terraform 範本，請參閱此 Amazon S3 儲存貯體上的讀我檔案指示。您可以閱讀文件，進一步了解如何使用 Terraform 範本。 HashiCorp

路 Route 53 ARC 中路由控制的最佳實踐

針對 Amazon Route 53 應用程式復原控制器中路由控制的復原和容錯移轉準備，我們建議採用下列最佳實務。

主題

- 確保專門建置、長期使用的 AWS 憑證安全，並隨時可存取
- 針對容錯移轉所涉及的 DNS 記錄選擇較低的 TTL 值
- 限制用戶端保持連線至端點的時間
- 將五個區域叢集端點和路由控制 ARN 加入書籤或硬式編碼
- 隨機選擇其中一個端點以更新路由控制狀態
- 使用極其可靠的資料平面 API 來列出和更新路由控制項狀態，而不是主控台

確保專門建置、長期使用的 AWS 憑證安全，並隨時可存取

在災難復原 (DR) 案例中，使用簡單的方法來存取 AWS 和執行復原工作，將系統相依性降至最低。建立專門用於 DR 工作的 IAM 長期登入資料，並將登入資料安全地保存在內部部署實體安全或虛擬保管庫中，以便在需要時進行存取。使用 IAM，您可以集中管理安全登入資料，例如存取金鑰和 AWS 資源存取權限。對於非 DR 工作，建議您繼續使用AWS 單一登入等 AWS 服務來使用同盟存取。

若要使用復原叢集資料平面 API 在 Route 53 ARC 中執行容錯移轉工作，您可以將 Route 53 ARC IAM 政策附加至您的使用者。如需進一步了解，請參閱Amazon Route 53 應用程式復原控制器中的身分識別型政策範例。

針對容錯移轉所涉及的 DNS 記錄選擇較低的 TTL 值

對於您可能需要在容錯移轉機制中變更的 DNS 記錄，尤其是健全狀況檢查的記錄，使用較低的 TTL 值是適當的。在這種情況下，將 TTL 設為 60 秒或 120 秒是常見的選擇。

DNS TTL (存留時間) 設定會告訴 DNS 解析程式在要求新記錄之前快取記錄的時間長度。當您選擇 TTL 時，您可以在延遲和可靠性以及對變更的回應能力之間進行平衡。DNS 解析器在記錄上的 TTL 較短，因為 TTL 指定它們必須更頻繁地查詢，因此 DNS 解析器會更快地注意到記錄的更新。

如需詳細資訊，請參閱 Amazon 路線 53 DNS 的最佳實務中為 DNS 記錄選擇 TTL 值。

限制用戶端保持連線至端點的時間

當您使用路由控制從一個轉移 AWS 區域 到另一個路由控制時，Amazon Route 53 應用程式復原控制器用來移動應用程式流量的機制是 DNS 更新。此更新會導致所有新的連線導向遠離受損的位置。

但是，具有預先存在開啟連線的用戶端可能會繼續對受損位置發出要求，直到用戶端重新連線為止。為確保快速復原，我們建議您限制用戶端保持連線至端點的時間長度。

如果您使用應用程式負載平衡器，則可以使用`keepalive`此選項來設定連線持續的時間長度。如需詳細資訊，請參閱應用 Application Load Balancer 使用指南中的 HTTP 用戶端保持活動持續時間

根據預設，應用程式負載平衡器會將 HTTP 用戶端保持作用持續時間值設定為 3600 秒或 1 小時。我們建議您降低與應用程式復原時間目標內嵌的值，例如 300 秒。當您選擇 HTTP 用戶端 keepalive 持續時間時間時，請考慮這個值是一般而言，更頻繁地重新連線之間的權衡，這可能會影響延遲，並且更快速地將所有用戶端移開受損的可用區域或區域。

將五個區域叢集端點和路由控制 ARN 加入書籤或硬式編碼

我們建議您將 Route 53 ARC 地區叢集端點的本機複本保留在書籤中，或儲存在用於重試端點的自動化程式碼中。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 DescribeClusterAPI 作業列出路由 53 ARC 叢集的端點。

隨機選擇其中一個端點以更新路由控制狀態

我們建議您在需要容錯移轉時，使用五個區域叢集端點的隨機端點更新 (和擷取) 路由控制狀態。如果該端點失敗，請重試其他每個區域端點。如需將程式碼範例與 AWS SDK 搭配使用的相關資訊，包括嘗試叢集端點的範例，請參閱使用 AWS SDK 的應用程序恢復控制器的代碼示例。

使用極其可靠的資料平面 API 來列出和更新路由控制項狀態，而不是主控台

使用 Route 53 ARC 資料平面 API，透過控制項作業檢視路由控制項和狀態，並更新路由控制狀態，以重新導向流量以便隨UpdateRoutingControlState作業進行容錯移轉。ListRouting您可以使用 AWS CLI (如下列範例所示) 或使用其中一個 AWS SDK 撰寫的程式碼。Route 53 ARC 透過資料層中的 API 提供了極高的可靠性，以便容錯移轉流量。我們建議您使用 API，而不是變更 AWS Management Console.

Connect 到您的其中一個區域叢集端點，讓 Route 53 ARC 使用資料平面 API。如果端點無法使用，請嘗試連線到另一個叢集端點。

如果安全規則封鎖路由控制狀態更新，您可以略過它以進行更新和容錯移轉流量。如需詳細資訊，請參閱 覆蓋安全規則以重新路由交通。

使用 Route 53 ARC 測試容錯移轉

使用 Route 53 ARC 路由控制定期測試容錯移轉，以便從主要應用程式堆疊容錯移轉至次要應用程式堆疊。確保您添加的 Route 53 ARC 結構與堆棧中的正確資源對齊非常重要，並且所有內容都按照您的期望運行。您應該在為您的環境設定 Route 53 ARC 之後進行測試，並繼續定期測試，以便準備好容錯移轉環境，然後才能發生故障情況，而您需要快速啟動並執行次要系統，以避免使用者停機。

製程控制 API 作業

本節包含的表格列出了可用於在 Amazon Route 53 應用程式復原控制器中設定和使用路由控制的 API 操作，以及相關文件的連結。

如需如何搭配使用通用路由控制組態 API 作業的範例 AWS Command Line Interface，請參閱 將路由 Route 53 ARC 路由控制 API 作業搭配使用的範例 AWS CLI。

下表列出可用於路由控制組態的 Route 53 ARC API 作業，並附有相關文件的連結。

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
建立叢集	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱 CreateCluster
描述叢集	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱 DescribeCluster
刪除叢集	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱 DeleteCluster
列出帳戶的叢集	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱 ListClusters
建立路由控制	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱CreateRouting控制
描述路由控制	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱DescribeRouting控制

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
更新製程控制	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱UpdateRouting控制
刪除路由控制	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱DeleteRouting控制
列出路由控制項	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱ListRouting控制
創建一個控制面板	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱CreateControl面板
描述控制面板	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱DescribeControl面板
更新控制面板	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱UpdateControl面板
刪除控制面板	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱DeleteControl面板
列出控制面板	請參閱在路 Route 53 ARC 中產生線路設計控制零組件	請參閱ListControl面板
建立安全規則	請參閱建立路由控制的安全規則	請參閱CreateSafety規則
描述安全規則	請參閱建立路由控制的安全規則	請參閱DescribeSafety規則
更新安全規則	請參閱建立路由控制的安全規則	請參閱UpdateSafety規則
刪除安全規則	請參閱建立路由控制的安全規則	請參閱DeleteSafety規則
列出安全規則	請參閱建立路由控制的安全規則	查看ListSafety規則

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
列出相關的 Route 53 健康檢查	請參閱在 Route 53 ARC 中建立路由控制健康檢查	見ListAssociated路線 53 HealthChecks
列出叢集共用的 AWS RAM 資源策略	請參閱 Support Route 53 ARC 中叢集的跨帳戶	查看GetResource政策

下表列出可用於透過路由控制資料平面管理流量容錯移轉的一般 Route 53 ARC API 作業，並附有相關文件的連結。

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
取得路由控制狀態	請參閱 取得和更新中的路由控制狀態 AWS Management Console	請參閱 GetRoutingControlState
列出路由控制項	N/A	請參閱ListRouting控制
更新路由控制狀態	請參閱 取得和更新中的路由控制狀態 AWS Management Console	請參閱 UpdateRoutingControlState
更新多重製程控制狀態	請參閱 取得和更新中的路由控制狀態 AWS Management Console	請參閱 UpdateRoutingControlStates

搭配 AWS SDK 使用此服務

AWS 軟件開發套件（SDK）可用於許多流行的編程語言。每個 SDK 都提供 API、程式碼範例和說明文件，讓開發人員能夠更輕鬆地以偏好的語言建置應用程式。

SDK 文件	代碼範例
AWS SDK for C++	AWS SDK for C++ 程式碼範例
AWS CLI	AWS CLI 程式碼範例

SDK 文件	代碼範例
AWS SDK for Go	AWS SDK for Go 程式碼範例
AWS SDK for Java	AWS SDK for Java 程式碼範例
AWS SDK for JavaScript	AWS SDK for JavaScript 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
AWS SDK for .NET	AWS SDK for .NET 程式碼範例
AWS SDK for PHP	AWS SDK for PHP 程式碼範例
AWS Tools for PowerShell	PowerShell 程式碼範例的工具
AWS SDK for Python (Boto3)	AWS SDK for Python (Boto3) 程式碼範例
AWS SDK for Ruby	AWS SDK for Ruby 程式碼範例
適用於 Rust 的 AWS SDK	適用於 Rust 的 AWS SDK 程式碼範例
適用於 SAP ABAP 的 AWS SDK	適用於 SAP ABAP 的 AWS SDK 程式碼範例
適用於 Swift 的 AWS SDK	適用於 Swift 的 AWS SDK 程式碼範例

如需此服務的特定範例，請參閱 使用 AWS SDK 的應用程序恢復控制器的代碼示例。

> **可用性範例**
>
> 找不到所需的內容嗎？ 請使用本頁面底部的提供意見回饋連結申請程式碼範例。

將路由 Route 53 ARC 路由控制 API 作業搭配使用的範例 AWS CLI

本節 AWS Command Line Interface 將逐步介紹使用路由控制的簡單應用程式範例，並使用使用 API 操作的 Amazon Route 53 應用程式復原控制器中的路由控制功能。這些範例旨在協助您開發如何使用 CLI 使用路由控制的基本瞭解。

透過 Amazon Route 53 應用程式復原控制器中的路由控制，您可以在不同 AWS 區域 或可用區域中執行的備援應用程式副本或複本之間觸發流量容錯移轉。

您可以將路由控制組織成群組 (稱為控制台)，這些群組已佈建在叢集上。Route 53 ARC 叢集是全域部署的一組地區端點。叢集端點提供高可用性 API，可用於設定和擷取路由控制狀態。如需繞線控制特徵元件的詳細資訊，請參閱路由控制元件 。

> **Note**
>
> Route 53 ARC 是支援多個端點的全域服務 AWS 區域。但是，您必須在大多數 Route 53 ARC CLI 命令中指定美國西部 (奧勒岡) 區域 `--region us-west-2` — 也就是指定參數。例如，當您建立復原群組、控制台和叢集時，請使用`region`參數。
> 建立叢集時，Route 53 ARC 會為您提供一組地區端點。若要取得或更新路由控制狀態，您必須在 CLI 命令中指定區域端點 (AWS 區域 和端點 URL)。

若要取得有關使用的更多資訊 AWS CLI，請參閱《 AWS CLI 指令參考》。如需路由控制 API 動作的清單，請參閱 製程控制 API 作業和 製程控制 API 作業。

我們會先建立您需要使用路由控制來管理容錯移轉的元件，從建立叢集開始。

設定製程控制元件

我們的第一步是建立叢集。Route 53 ARC 叢集是由五個端點組成的一組，五個端點各有一個 AWS 區域。Route 53 ARC 基礎結構支援這些端點協調工作，以確保容錯移轉作業的高可用性和順序一致性。

1. 建立叢集

1. 建立叢集。

```
aws route53-recovery-control-config --region us-west-2 create-cluster --cluster-name
 NewCluster
```

```
{
    "Cluster": {
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "Name": "NewCluster",
        "Status": "PENDING"
    }
```

```
}
```

當您第一次建立 Route 53 ARC 資源時，它的狀態為叢集建立PENDING時。您可以通過調用來檢查其進度describe-cluster。

1b。描述叢集。

```
aws route53-recovery-control-config --region us-west-2 \
    describe-cluster --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh
```

```
{
    "Cluster":{
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "ClusterEndpoints":[
            {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
            {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
            {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
            {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
            {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
        ]
        "Name": "NewCluster",
        "Status": "DEPLOYED"
    }
}
```

狀態為「已部署」時，Route 53 ARC 已成功建立具有一組端點的叢集，供您與之互動。您可以透過呼叫列出所有叢集list-clusters。

1C。列出您的叢集。

```
aws route53-recovery-control-config --region us-west-2 list-clusters
```

```
{
    "Clusters": [
```

```
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/1234abcd-abcd-1234-abcd-1234abcdefgh",
            "ClusterEndpoints":[
                {"Endpoint": "https://host-aaaaaa.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-bbbbbb.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-cccccc.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-dddddd.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-eeeeee.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "AnotherCluster",
            "Status": "DEPLOYED"
        },
        {
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "ClusterEndpoints": [
                {"Endpoint": "https://host-ffffff.us-east-1.example.com", "Region":"us-
east-1"},
                {"Endpoint": "https://host-gggggg.ap-southeast-2.example.com",
 "Region":"ap-southeast-2"},
                {"Endpoint": "https://host-hhhhhh.eu-west-1.example.com", "Region":"eu-
west-1"},
                {"Endpoint": "https://host-iiiiii.us-west-2.example.com", "Region":"us-
west-2"},
                {"Endpoint": "https://host-jjjjjj.ap-northeast-1.example.com",
 "Region":"ap-northeast-1"}
            ],
            "Name": "NewCluster",
            "Status": "DEPLOYED"
        }
    ]
}
```

2. 創建一個控制面板

控制面板是用於組織 Route 53 ARC 路由控制項的邏輯群組。當您建立叢集時，Route 53 ARC 會自動為您提供呼叫的控制面板`DefaultControlPanel`。您可以立即使用此控制面板。

一個控制面板只能存在於一個叢集中。如果您想要將控制台移至另一個叢集，您必須刪除它，然後在第二個叢集中建立它。您可以通過調用查看帳戶中的所有控制面板`list-control-panels`。若只要查看特定叢集中的控制面板，請新增`--cluster-arn`欄位。

2a. 列出控制面板。

```
aws route53-recovery-control-config --region us-west-2 \
    list-control-panels --cluster-arn arn:aws:route53-recovery-
control::111122223333:cluster/eba23304-1a51-4674-ae32-b4cf06070bdd
```

```
{
    "ControlPanels": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/1234567dddddd1234567dddddd1234567",
            "ClusterArn": "arn:aws:route53-recovery-
control::111122223333:cluster/5678abcd-abcd-5678-abcd-5678abcdefgh",
            "DefaultControlPanel": true,
            "Name": "DefaultControlPanel",
            "RoutingControlCount": 0,
            "Status": "DEPLOYED"
        }
    ]
}
```

（可選）通過調用創建自己的控制面板`create-control-panel`。

2b. 創建一個控制面板。

```
aws route53-recovery-control-config --region us-west-2 create-control-panel \
        --control-panel-name NewControlPanel2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": false,
```

```
        "Name": "NewControlPanel2",
        "RoutingControlCount": 0,
        "Status": "PENDING"
    }
}
```

當您第一次建立 Route 53 ARC 資源時，它的狀態為正在建立PENDING時。您可以通過電話檢查進度describe-control-panel。

2C。描述控制面板。

```
aws route53-recovery-control-config --region us-west-2 describe-control-panel \
    --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "ControlPanel": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ClusterArn": "arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh",
        "DefaultControlPanel": true,
        "Name": "DefaultControlPanel",
        "RoutingControlCount": 0,
        "Status": "DEPLOYED"
    }
}
```

3. 建立路由控制

現在您已設定叢集並查看控制台，就可以開始建立路由控制項。建立路由控制項時，至少必須指定路由控制項所在叢集的 Amazon 資源名稱 (ARN)。您也可以為路由控制項指定控制台的 ARN。您還需要指定控制面板所在的叢集。

如果您未指定控制台，則會將您的路由控制項新增至自動建立的控制台DefaultControlPanel。

通過調用創建路由控件create-routing-control。

3. 建立路由控制項。

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
    --routing-control-name NewRc1 \
```

```
    --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
{
    "RoutingControl": {
        "ControlPanelArn": " arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "PENDING"
    }
}
```

路由控制項遵循與其他 Route 53 ARC 資源相同的建立模式，因此您可以透過呼叫描述作業來追蹤它們的進度。

3B. 描述路由控制。

```
aws route53-recovery-control-config --region us-west-2 describe-routing-control \
       --routing-control-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "RoutingControl": {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "Name": "NewRc1",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "Status": "DEPLOYED"
    }
}
```

您可以通過調用列出控制面板中的路由控制項`list-routing-controls`。控制面板 ARN 是必需的。

3C。列出路由控制項。

```
aws route53-recovery-control-config --region us-west-2 list-routing-controls \
        --control-panel-arn arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456
```

```
{
    "RoutingControls": [
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc1",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
            "Status": "DEPLOYED"
        },
        {
            "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
            "Name": "Rc2",
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
            "Status": "DEPLOYED"
        }
    ]
}
```

在下面的例子中，我們與路由控制狀態的工作，我們假設你有這一節中列出的兩個路由控件（Rc1 和 Rc2）。在此範例中，每個路由控制項代表應用程式部署在其中的可用區域。

4. 建立安全規則

當您同時使用多個路由控制項時，您可能會決定要在啟用和停用它們時採取一些保護措施，以避免意外後果，例如關閉兩個路由控制和停止所有流量流量。若要建立這些保護措施，請建立路由控制安全規則。

有兩種類型的安全規則：斷言規則和門控規則。若要進一步瞭解安全規則，請參閱建立路由控制的安全規則。

下列呼叫提供建立宣告規則的範例，以確保在任何指定時間將On兩個路由控制項中的至少一個設定為。若要建立規則，請create-safety-rule使用assertion-rule參數執行。

如需宣告規則 API 作業的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南AssertionRule中的。

4a. 建立宣告規則。

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --assertion-rule '{"Name": "TestAssertionRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "AssertedControls":
        ["arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
        "RuleConfig": {"Threshold": 1, "Type": "ATLEAST", "Inverted": false}}'
```

```
{
    "Rule": {
        "ASSERTION": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/333333444444",
            "AssertedControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestAssertionRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 1,
                "Type": "ATLEAST"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

下列呼叫提供建立閘控規則的範例，該規則為控制台中的一組目標路由控制項提供整體的「開/關」或「閘控」開關。這可讓您不允許更新目標路由控制項，例如，自動化功能無法進行未經授權的更新。在此範例中，閘控開關是由參數指定的路由控制，並且由GatingControls參數指定了控制或「門控」的兩個路由控制項。TargetControls

> **Note**
>
> 在建立閘控規則之前，您必須建立閘控路由控制 (不包括 DNS 容錯移轉記錄) 以及目標路由控制 (您使用 DNS 容錯移轉記錄設定)。

若要建立規則，請create-safety-rule使用gating-rule參數執行。

如需宣告規則 API 作業的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南GatingRule中的。

4b. 建立閘控規則。

```
aws route53-recovery-control-config --region us-west-2 create-safety-rule \
        --gating-rule '{"Name": "TestGatingRule",
        "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
        "WaitPeriodMs": 5000,
        "GatingControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
def123def123def"]
        "TargetControls": ["arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/
ghi456ghi456ghi",
        "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"],
        "RuleConfig": {"Threshold": 0, "Type": "OR", "Inverted": false}}'
```

```
{
    "Rule": {
        "GATING": {
            "Arn": "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/safetyrule/444444444444",
            "GatingControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/def123def123def"
```

```
            ],
            "TargetControls": [
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/ghi456ghi456ghi"
                "arn:aws:route53-recovery-control::888888888888:controlpanel/
zzz123yyy456xxx789zzz123yyy456xxx/routingcontrol/lmn789lmn789lmn"
            ],
            "ControlPanelArn": "arn:aws:route53-recovery-
control::888888888888:controlpanel/zzz123yyy456xxx789zzz123yyy456xxx",
            "Name": "TestGatingRule",
            "RuleConfig": {
                "Inverted": false,
                "Threshold": 0,
                "Type": "OR"
            },
            "Status": "PENDING",
            "WaitPeriodMs": 5000
        }
    }
}
```

與其他路由控制資源一樣，您可以在安全規則傳播到資料平面後描述、列出或刪除這些規則。

設定一或多個安全規則之後，您可以繼續與叢集互動、設定或擷取路由控制項的狀態。如果`set-routing-control-state`作業中斷了您所建立的規則，您會收到類似下列內容的例外狀況：

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb01234563333333444444
```

第一個標識符是與路由控制 ARN 連接的控制面板 ARN。第二個標識符是與安全規則 ARN 連接的控制面板 ARN。

5. 建立健康狀態檢

若要使用路由控制來容錯移轉流量，請在 Amazon Route 53 中建立運作狀態檢查，然後將運作狀態檢查與 DNS 記錄建立關聯。若要容錯移轉流量，Route 53 ARC 路由控制項會將健康狀態檢查設定為失敗，以便 Route 53 會重新路由流量。(健康狀態檢查無效您的應用程式的健康狀態；它只是用來重新路由流量的方法。)

舉例來說，假設您有兩個儲存格 (區域或可用區域)。您可以將一個設定為應用程式的主要儲存格，另一個設定為次要儲存格，以容錯移轉至。

若要設定容錯移轉的健全狀況檢查，您可以執行下列動作，例如：

1. 使用 Route 53 ARC CLI 為每個儲存格建立路由控制項。
2. 使用 Route 53 CLI 在路由 53 中為每個路由控制項建立路由 53 ARC 健康狀態檢查。
3. 使用 Route 53 CLI 在 Route 53 中建立兩個容錯移轉 DNS 記錄，並將健全狀況檢查與每個記錄建立關聯。

5a. 為每個儲存格建立路由控制項。

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell1 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

```
aws route53-recovery-control-config --region us-west-2 create-routing-control \
        --routing-control-name RoutingControlCell2 \
        --cluster-arn arn:aws:route53-recovery-control::111122223333:cluster/5678abcd-
abcd-5678-abcd-5678abcdefgh
```

5b. 為每個路由控制項建立健康狀態檢查。

> **Note**
>
> 您可以使用 Amazon Route 53 CLI 創建路由 53 ARC 運行狀態檢查。

```
aws route53 create-health-check --caller-reference RoutingControlCell1 \
        --health-check-config \
        Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell1",
        "HealthCheckConfig": {
```

```
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

```
aws route53 create-health-check --caller-reference RoutingControlCell2 \
    --health-check-config \
    Type=RECOVERY_CONTROL,RoutingControlArn=arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567
```

```
{
    "Location": "https://route53.amazonaws.com/2015-01-01/healthcheck/11111aaaa-bbbb-
cccc-dddd-ffffff22222",
    "HealthCheck": {
        "Id": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx",
        "CallerReference": "RoutingControlCell2",
        "HealthCheckConfig": {
            "Type": "RECOVERY_CONTROL",
            "Inverted": false,
            "Disabled": false,
            "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
        },
        "HealthCheckVersion": 1
    }
}
```

5c. 建立兩個容錯移轉 DNS 記錄，並將健全狀況檢查與每個記錄建立關聯。

您可以使用路由 53 CLI 在路由 53 中建立容錯移轉 DNS 記錄。若要建立記錄，請遵循 Amazon Route 53 AWS CLI 指令參考中的指示，以取得變更資源- 記錄集命令。在記錄中，指定每個儲存格的 DNS 值，以及 Route 53 為健康狀態檢查建立的對應`HealthCheckID`值 (請參閱 6b)。

對於主要儲存格：

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "primary",
    "Failover": "PRIMARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell1.yourdomain.com"
        }
    ],
    "HealthCheckId": "xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
}
```

對於次要儲存格：

```
{
    "Name": "myapp.yourdomain.com",
    "Type": "CNAME",
    "SetIdentifier": "secondary",
    "Failover": "SECONDARY",
    "TTL": 0,
    "ResourceRecords": [
        {
            "Value": "cell2.yourdomain.com"
        }
    ],
    "HealthCheckId": "yyyyyy-yyyy-yyyy-yyyy-yyyyyyyyyyyy"
}
```

現在，若要從主要儲存格容錯移轉到次要儲存格，您可以依照步驟 4b 中的 CLI 範例來更新`RoutingControlCell1`到`OFF`和`RoutingControlCell2`到`ON`的狀態。

列出並更新路由控制項與狀態 AWS CLI

建立 Amazon Route 53 應用程式復原控制器資源 (例如叢集、路由控制和控制面板) 之後，您可以與叢集互動，列出和更新容錯移轉的路由控制狀態。

Route 53 ARC 會為您建立的每個叢集提供一組叢集端點，五個端點各有一個 AWS 區域。當您呼叫叢集以擷取或將路由控制狀態設定為或時，必須指定這些區域端點之一 (AWS 區域 和端點 URL) `Off`。`On`當您使用 AWS CLI、取得或更新路由控制狀態時，除了區域端點之外，您還必須指定地區端點`--region`的，如本節中的範例所示。

您可以使用任何區域叢集端點。我們建議您的系統在區域端點之間輪換，並準備好重試每個可用的端點。如需依序說明嘗試叢集端點的程式碼範例，請參閱使用 AWS SDK 的應用程序恢復控制器的操作。

若要取得有關使用的更多資訊 AWS CLI，請參閱《 AWS CLI 指令參考》。如需路由控制 API 動作的清單和詳細資訊的連結，請參閱 製程控制 API 作業。

> **Important**
>
> 雖然您可以在 Amazon Route 53 主控台上更新路由控制狀態，但我們建議您使用 AWS CLI 或 AWS SDK 更新路由控制狀態。Route 53 ARC 透過 Route 53 ARC 路由控制資料平面提供極高的可靠性，用於重新路由流量和跨單元的故障轉移。如需有關使用 Route 53 ARC 進行容錯移轉的更多建議，請參閱路 Route 53 ARC 中路由控制的最佳實踐。

當您建立路由控制時，狀態會設定為`Off`。這表示流量不會路由至該路由控制的目標儲存格。您可以透過執行指令來驗證路由控制項的狀態`get-routing-control-state`。

若要確定要指定的區域和端點，請執行指`describe-clusters`令以檢視`ClusterEndpoints`。每個都`ClusterEndpoint`包括一個區域和對應的端點，您可以用來取得或更新路由控制狀態。DescribeCluster是一個恢復控制配置 API 操作。我們建議您將 Route 53 ARC 地區叢集端點的本機複本保留在書籤中，或以硬式編碼保留您用來重試端點的自動化程式碼。

1. 列出路由控制項

您可以使用高度可靠的 Route 53 ARC 資料平面端點來檢視路由控制和路由控制狀態。

1. 列出特定控制台的路由控制項。如果不指定控制面板，則`list-routing-controls`返回叢集中的所有路由控制項。

```
aws route53-recovery-cluster list-routing-controls --control-panel-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{
    "RoutingControls": [{
        "ControlPanelArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
```

```
        "RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlName": "RCOne",
        "RoutingControlState": "On"
    },
    {
        "ControlPanelArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
        "ControlPanelName": "ExampleControlPanel",
        "RoutingControlArn": "arn:aws:route53-recovery-
control::023759465626:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
zzzzxxxxyyyy123456",
        "RoutingControlName": "RCTwo",
        "RoutingControlState": "Off"
    }
]
```

2. 取得路由控制項

2. 取得路由控制狀態。

```
aws route53-recovery-cluster get-routing-control-state --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
    "RoutingControlName": "RCOne",
    "RoutingControlState": "On"
}
```

2. 更新製程控制

若要將流量路由傳送至路由控制項控制的目標端點，請將路由控制狀態更新為On。執行指令來更新路由控制狀態update-routing-control-state。（請求成功時，響應為空。）

2a. 更新路由控制狀態。

```
aws route53-recovery-cluster update-routing-control-state \
        --routing-control-arn \
        arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567 \
        --routing-control-state On \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

您可以透過一個 API 呼叫，同時更新多個路由控制項：update-routing-control-states。（請求成功時，響應為空。）

2b. 一次更新數個製程控制狀態 (批次更新)。

```
aws route53-recovery-cluster update-routing-control-states \
        --update-routing-control-state-entries \
        '[{"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567",
        "RoutingControlState": "Off"}, \
        {"RoutingControlArn": "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
hijklmnop987654321",
        "RoutingControlState": "On"}]' \
        --region us-west-2 \
        --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

```
{}
```

在路 Route 53 ARC 中使用線路設計控制零組件

主題

- 在路 Route 53 ARC 中產生線路設計控制零組件
- 在 Route 53 ARC 中檢視和更新路由控制狀態
- 建立路由控制的安全規則
- Support Route 53 ARC 中叢集的跨帳戶

在路 Route 53 ARC 中產生線路設計控制零組件

本節說明如何建立叢集、路由控制、運作狀態檢查和控制面板，以便在 Amazon Route 53 應用程式復原控制器中使用路由控制。

首先建立叢集，主控您的路由控制項，以及您用來將它們分組的控制台。然後建立路由控制和健康狀態檢查，以便您可以將流量重新路由到另一個儲存格容錯移轉，以便流量進入備份複本，例如。

請注意，您需要針對您建立的每個叢集按小時計費。您通常只需要一個叢集即可裝載路由控制項和控制台，以便管理應用程式的復原控制。此外，您可以使用來設定資源共用 AWS Resource Access Manager，以便一個叢集可以主控多個擁有的路由控制項和其他 Route 53 ARC 資源 AWS 帳戶。要了解 Route 53 ARC 中的資源共享， Support Route 53 ARC 中叢集的跨帳戶. 如需定價資訊，請參閱 Amazon Route 53 應用程式復原控制器定價，然後向下捲動至 Amazon 路線 53。

若要使用路由控制來容錯移轉流量，請建立路由控制運作狀態檢查，並與應用程式中資源的 Amazon Route 53 DNS 記錄相關聯。舉例來說，假設您有兩個儲存格，其中一個是您已設定為應用程式的主要儲存格，另一個是您設定為次要儲存格以容錯移轉至的儲存格。

若要設定容錯移轉的健全狀況檢查，請執行下列動作：

1. 為每個儲存格建立路由控制項。
2. 為每個路由控制項建立健康狀態檢查。
3. 建立兩個 DNS 記錄，例如兩個 DNS 容錯移轉記錄，並將健全狀況檢查與每個記錄建立關聯。

您可能會建立路由控制項的另一個案例是，當您建立閘控規則的安全規則時。在這種情況下，您不會將健康狀態檢查和 DNS 記錄與路由控制項產生關聯，因為您將使用它作為閘控路由控制項。如需詳細資訊，請參閱 建立路由控制的安全規則 。

這些小節包括在 Route 53 ARC 控制台上建立用於繞線控制之元件的步驟。若要瞭解如何搭配 Route 53 ARC 使用復原控制設定 API 作業，請參閱 製程控制 API 作業.

在 Route 53 ARC 中創建集群

您必須建立叢集來裝載 Route 53 ARC 中的路由控制和控制台。

叢集是一組備援的區域端點，您可以針對其執行 API 呼叫，以更新或取得一或多個路由控制項的狀態。單一叢集可以裝載多個路由控制項。

> **Important**
>
> 請注意，您需要針對您建立的每個叢集按小時計費。一個叢集可以裝載許多路由控制和控制面板，以進行復原控制管理，通常足以應用程式使用。

建立叢集

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇 Clusters (叢集)。
3. 選擇 [建立]，然後輸入叢集的名稱。
4. 選擇建立叢集。

在路 Route 53 ARC 中產生線路設計控制

為您要將流量路由傳送至的每個儲存格建立路由控制項。例如，當您有一個應用程式的資源為可復原性設定為孤立時，每個儲存格可能會有一個儲存格 AWS 區域，以及每個區域中每個可用區域的巢狀儲存格。在這個案例中，您會建立每個儲存格和每個巢狀儲存格的路由控制項。

當您建立路由控制時，請記住，路由控制名稱在每個控制台中都必須是唯一的。

建立用於重新路由傳送流量的路由控制項之後，您可以將每個控制項與健全狀況檢查產生關聯，這可讓您根據與每個儲存格相關聯的 DNS 記錄，將流量路由到儲存格。如果您要將閘控規則設定為安全規則，並建立閘控路由控制項，則不會將健康狀態檢查新增至路由控制項。

若要建立路由控制

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。
3. 在「路由控制」頁面上，選擇「建立」，然後選擇「路由」控制項。
4. 輸入路由控制項的名稱、選擇要新增控制項的叢集，然後選擇將其新增至現有的控制台，包括使用預設控制台。或者，建立新的控制台。
5. 如果您選擇建立新的控制台，請選擇要在其上建立控制台的叢集，然後輸入面板的名稱。
6. 選擇「建立製程控制」。

7. 請遵循下列步驟來命名並建立路由控制項。

在 Route 53 ARC 中建立路由控制健康檢查

您可以將路由控制健全狀況檢查與要用於重新路由傳送流量的每個路由控制項產生關聯。然後，您可以使用 Amazon Route 53 DNS 記錄來設定每個運作狀態檢查，例如容錯移轉 DNS 記錄。然後，您只需更新相關路由控制的狀態，將其設定為On或Off，就可以在 Amazon Route 53 應用程式復原控制器中重新路由流量。

> **Note**
>
> 您無法編輯現有的路由控制健康狀態檢查，將其與不同的路由控制項產生關聯。

若要建立路由控制健全狀況檢查

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。
3. 在 [路由控制] 頁面上，選擇路由控制項。
4. 在 [路由控制項詳細資料] 頁面上，選擇 [建立健全狀況檢查
5. 輸入健全狀況檢查的名稱，然後選擇 [建立]。

接下來，您會建立 Route 53 DNS 記錄，並將路由控制健康狀態檢查與每個記錄建立關聯。例如，假設您想要使用兩個 DNS 容錯移轉記錄，將路由控制健全狀況檢查與產生關聯。若要讓 Route 53 ARC 使用路由控制項正確容錯移轉流量，請先在 Route 53 中建立兩個容錯移轉記錄：主要和次要記錄。如需設定 DNS 容錯移轉記錄的相關資訊，請參閱 Health 檢查概念。

當您建立主要容錯移轉記錄時，值應如下所示：

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Primary
Failover: Primary
TTL: 0
Resource Records:
Value: cell1.yourdomain.com
```

```
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

次要容錯移轉記錄值應如下所示：

```
Name: myapp.yourdomain.com
Type: CNAME
Set Identifier: Secondary
Failover: Secondary
TTL: 0
Resource Records:
Value: cell2.yourdomain.com
Health Check ID: xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
```

現在，假設您想要重新路由流量，因為發生故障。若要這麼做，您可以更新相關聯的製程控制狀態，將主要製程控制狀態變更為，OFF而將次要製程控制狀態變更為ON。執行此操作時，相關聯的健全狀況檢查會停止流量進入主要複本，並將其路由傳送至次要複本。如需有關使用路由控制容錯移轉流量的詳細資訊，請參閱 使用路由 Route 53 ARC API 取得和更新路由控制狀態 (建議使用)。

若要查看使用 Route 53 ARC API 作業建立路由控制項和相關聯健全狀態檢查的 AWS CLI 指令範例，請參閱 將路由 Route 53 ARC 路由控制 API 作業搭配使用的範例 AWS CLI。

在 Route 53 ARC 中創建一個控制面板

Amazon Route 53 應用程式復原控制器中的控制面板可讓您將相關的路由控制群組在一起。根據容錯移轉的範圍，控制台可以具有代表應用程式內的微服務、整個應用程式本身或應用程式群組的路由控制項。將路由控制項群組到控制台的好處是，您可以搭配控制台使用安全規則，以協助保護流量路由變更。

當您建立叢集時，Route 53 ARC 會建立預設的控制面板。您可以使用路由控制項的預設控制台，也可以建立一或多個控制台來分組路由控制項。請注意，控制台名稱僅支援 ASCII 字元。

本節包括在 Route 53 ARC 控制台上創建控制面板的步驟。如需搭配 Route 53 ARC 使用復原控制設定 API 作業的相關資訊，請參閱 製程控制 API 作業.

建立控制台

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。

3. 在「路由」控制項頁面上，選擇「建立」，然後選擇 「控制」面板。
4. 選擇要在其上建立控制台的叢集，然後輸入面板的名稱。
5. 選擇「建立控制台」。

在 Route 53 ARC 中檢視和更新路由控制狀態

本節說明如何在 Amazon Route 53 應用程式復原控制器中檢視和更新路由控制狀態。路由控制是簡單的開關開關，可管理復原群組中儲存格的流量流量。儲存格通常 AWS 區域是包含您資源的可用區域，或有時是可用區域。當路由控制狀態為時0n，流量會流至由該路由控制項控制所控制的儲存格。

您可以將路由控制項群組到控制台，這些控制台是邏輯容錯移轉群組。例如，當您在主控台上開啟控制台時，您可以一次檢視群組的所有路由控制項，以查看流量流動的位置。

您可以在 Route 53 ARC 主控台上更新路由控制狀態，或使用路由 53 ARC API 來更新路由控制狀態。建議您使用 API 更新路由控制狀態。首先，Route 53 ARC 透過資料平面中的 API 提供極高的可靠性，以便執行這些動作。當您變更這些狀態時，這很重要，因為路由狀態變更會透過重新路由傳送應用程式流量跨儲存格容錯移轉。此外，如果您嘗試連線到的叢集端點無法使用，您可以視需要嘗試循環連線到不同的叢集端點，使用 API 來嘗試連線到不同的叢集端點。

您可以更新一個製程控制狀態，也可以一次更新數個製程控制狀態。例如，您可能想要將一個路由控制狀態設定0ff為阻止流量流向一個儲存格，例如應用程式遇到延遲增加的可用區域。同時，您可能想要將另一個路由控制狀態設定為啟動流0n向其他儲存格或可用區域的流量。在這個案例中，您可以同時更新這兩個路由控制狀態，因此流量會繼續流動。

主題

- 使用路由 Route 53 ARC API 取得和更新路由控制狀態 (建議使用)
- 取得和更新中的路由控制狀態 AWS Management Console

使用路由 Route 53 ARC API 取得和更新路由控制狀態 (建議使用)

我們建議您使用 Amazon Route 53 應用程式復原控制器 API 操作來取得或更新路由控制狀態，方法是使用 AWS CLI 命令或使用您開發的程式碼來搭配其中一個 AWS SDK 使用 Route 53 ARC API 操作。建議您搭配 CLI 或程式碼使用 API 作業來處理路由控制狀態，而不是使用 AWS Management Console.

Route 53 ARC 通過使用 API 更新路由控制狀態，因為路由控制存儲在高可用性集群中，因此為跨單元（AWS 區域）進行故障轉移提供了極高的可靠性。Route 53 ARC 可確保您始終可以存取五個區域叢

集端點中的至少三個，以進行路由控制狀態變更。若要使用 API 取得或變更路由控制狀態，請連線至其中一個地區叢集端點。如果端點無法使用，您可以嘗試連線到另一個叢集端點。

您可以在 Route 53 主控台中檢視叢集的區域叢集端點清單，或使用 API 動作、DescribeCluster。您取得和變更路由控制狀態的程序應該視需要嘗試輪替每個端點，因為叢集端點會在可用和無法使用的狀態中循環，以進行定期維護和更新。

我們提供詳細的資訊和程式碼範例，說明如何使用 Route 53 ARC API 作業取得和更新路由控制狀態，以及使用區域叢集端點。如需詳細資訊，請參閱下列內容：

- 如需說明如何輪換區域叢集端點以取得和設定路由控制狀態的程式碼範例，請參閱使用 AWS SDK 的應用程序恢復控制器的操作。
- 如需使用取得和更新路由控制狀態的相關資訊，請參閱 列出並更新路由控制項與狀態 AWS CLI。AWS CLI

取得和更新中的路由控制狀態 AWS Management Console

您可以在中取得和更新路由控制狀態 AWS Management Console。不過請注意，您無法在主控台中選擇不同的區域叢集端點。也就是說，沒有像使用 Amazon Route 53 應用程式復原控制器 API 一樣，在主控台中選擇和輪換叢集端點的程序。此外，控制台不具有高可用性，而 Route 53 ARC 數據平面提供了極高的可靠性。基於這些原因，我們建議您使用 Route 53 ARC API 來取得及更新生產作業的製程控制狀態。

如需有關使用 Route 53 ARC 進行容錯移轉的更多建議，請參閱路 Route 53 ARC 中路由控制的最佳實踐。

若要在主控台中檢視和更新路由控制項，請遵循下列程序中的步驟。

若要取得路由控制狀態

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。
3. 從清單中選擇控制台並檢視路由控制項。

若要更新一或多個製程控制狀態

1. 在以下位置打開 Amazon 路線 53 控制台 https://console.aws.amazon.com/route53/home。

2. 在 [應用程式復原控制器] 下，選擇 [路由
3. 選擇 [動作]，然後選擇 [變更流量路由]。
4. 根據您希望流量為應用程式流動Off或停止流動的位置On，將一或多個路由控制項的狀態更新為或。
5. 在文字方塊中輸入 confirm。
6. 選擇 [更新流量路由]。

建立路由控制的安全規則

當您同時使用多個路由控制項時，您可能會決定要採取適當的保護措施，以避免意外後果。例如，您可能想要避免意外關閉應用程式的所有路由控制項，這會導致失敗開啟的案例。或者，您可能想要實作主開關以停用一組路由控制項，也許是為了防止自動化重新路由流量。為了在 Route 53 ARC 中為路由控制建立類似的保護措施，您需要建立安全規則。

您可以使用路由控制項、規則和您指定的其他選項組合來設定路由控制的安全規則。每個安全規則都與單個控制面板相關聯，但控制面板可以有多個安全規則。建立安全規則時，請記住，每個控制台中的安全規則名稱必須是唯一的。

主題

- 安全規則的類型
- 在主控台上建立安全規則
- 在主控台上編輯或刪除安全規則
- 覆蓋安全規則以重新路由交通

安全規則的類型

安全規則有兩種類型：宣告規則和閘控規則，您可以使用這些規則以不同的方式保護容錯移轉。

判斷提示規則

使用宣告規則時，當您變更一或一組路由控制狀態時，Route 53 ARC 會強制符合您設定規則時所設定的條件，否則路由控制狀態不會變更。

其中一個有用的範例是防止失敗開啟案例，例如停止流量進入一個儲存格但不開始流向另一個儲存格的流量的案例。為了避免這種情況，斷言規則確保在任何給定時間，控制面板中的路由控制項集中至少有一個On路由控制項。如此可確保流量至少流向應用程式的一個區域或可用區域。

若要查看建立宣告規則以強制執行此條件的範例 AWS CLI 命令，請參閱中 將路由 Route 53 ARC 路由控制 API 作業搭配使用的範例 AWS CLI的建立安全規則。

如需宣告規則 API 作業屬性的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南AssertionRule中的。

閘控規則

使用閘控規則時，您可以在一組路由控制項上強制執行整體開關，以便根據您在規則中指定的一組條件來強制執行這些路由控制狀態是否可以變更。最簡單的準則是您指定為切換器的單一路由控制是否設為ON或OFF。

若要實作此功能，您可以建立閘控路由控制項，用作整體交換器和目標路由控制項，以控制到不同區域或可用區域的流量。然後，若要防止手動或自動更新您為閘控規則設定的目標路由控制項，請將閘控路由控制狀態設定為Off。若要允許更新，請將其設定為On。

若要查看建立實作這種整體切換的閘控規則的範例 AWS CLI 命令，請參閱中的建立安全規則 將路由 Route 53 ARC 路由控制 API 作業搭配使用的範例 AWS CLI。

如需閘控規則 API 作業屬性的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南GatingRule中的。

在主控台上建立安全規則

本節中的步驟說明如何在 Route 53 ARC 主控台上建立安全規則。無論您是建立宣告規則還是閘控規則，這些步驟都是類似的。差異在程序中註明。

若要了解如何搭配 Amazon Route 53 應用程式復原控制器使用復原和路由控制 API 操作，請參閱 製程控制 API 作業。

若要建立安全規則

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。
3. 在「路由」控制項頁面上，選擇控制台。
4. 在 [控制台詳細資料] 頁面上，選擇 [動作]，然後選擇 [新增安全規則]。
5. 選擇要新增的規則型態：宣告規則或閘控規則。
6. 選擇名稱，並選擇性地變更等待期間。
7. 指定安全規則的組態選項。

- 對於宣告規則，請指定宣告的路由控制項。
- 針對閘控規則，指定閘控路由控制項和目標路由控制項。

對於這兩個規則，請選擇類型和臨界值，以及規則是否反轉來指定規則組態。

> **Note**
>
> 若要進一步了解如何指定宣告規則，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南中提供的AssertionRule操作資訊。若要進一步了解如何指定閘控規則，請參閱 Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南中提供的GatingRule作業資訊。

8. 選擇建立。

在主控台上編輯或刪除安全規則

本節中的步驟說明如何在 Route 53 ARC 主控台上編輯或刪除安全規則。您只能對安全規則進行有限的編輯，以變更名稱或更新等待期間。若要進行其他變更，請刪除並重新建立安全規則。

若要進一步了解如何搭配 Amazon Route 53 應用程式復原控制器使用 API 操作，請參閱 製程控制 API 作業.

若要刪除安全規則

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇「製程控制」。
3. 在「路由」控制項頁面上，選擇控制台。
4. 在控制台詳細資料頁面上，選擇安全規則，然後選擇 [刪除] 或 [編輯]。

覆蓋安全規則以重新路由交通

在某些情況下，您可能想要略過使用您已設定的安全規則強制執行的路由控制保護措施。例如，您可能希望快速容錯移轉以進行災難復原，而一或多個安全規則可能會意外阻止您更新路由控制狀態以重新路由傳送流量。在這樣的「中斷」案例中，您可以覆寫一或多個安全規則，以變更路由控制狀態並容錯移轉應用程式。

當您使用或update-routing-control-states AWS CLI 指令搭配safety-rules-to-override參數來更新路由控制狀態 (或多個路由控制狀態) 時，可以略過安全規則。update-routing-control-state使用您要覆寫的安全規則的 Amazon 資源名稱 (ARN) 指定參數，或指定以逗號分隔的 ARN 清單來覆寫兩個或更多安全規則。

當安全規則封鎖路由控制狀態更新時，錯誤訊息會包含封鎖更新之規則的 ARN。因此，您可以記下 ARN，然後使用安全規則覆寫參數在路由控制狀態 CLI 命令中指定它。

> **Note**
>
> 由於您要更新的路由控制項可能有多個安全規則，因此您可以執行 CLI 命令，以一個安全規則覆寫來更新路由控制狀態，但會出現另一個安全規則封鎖更新的錯誤訊息。繼續將安全規則 ARN 加入至 update 指令中要覆寫的規則清單 (以逗號分隔)，直到更新指令順利完成為止。

若要進一步瞭解如何搭配 API 和 SDK 使用SafetyRulesToOverride屬性，請參閱UpdateRoutingControlState。

以下是兩個用來覆寫安全規則以更新路由控制狀態的 CLI 命令範例。

覆寫一個安全規則

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
    --safety-rules-to-override arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888 \
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

覆寫兩個安全規則

```
aws route53-recovery-cluster --region us-west-2 update-routing-control-state \
    --routing-control-arn \
    arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/
routingcontrol/abcdefg1234567 \
    --routing-control-state On \
```

```
    --safety-rules-to-override "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
yyyyyyy8888888" \
    "arn:aws:route53-recovery-
control::111122223333:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/safetyrule/
qqqqqqq7777777"
    --endpoint-url https://host-dddddd.us-west-2.example.com/v1
```

Support Route 53 ARC 中叢集的跨帳戶

Amazon Route 53 應用程式復原控制器與整合 AWS Resource Access Manager 以啟用資源共用功能。 AWS RAM 是一項可讓您與其他人 AWS 帳戶 或透過共用資源的服務 AWS Organizations。對於 Route 53 ARC，您可以共用叢集資源。

使用 AWS RAM，您可以透過建立資源共用來共用您擁有的資源。資源共用指定要共用的資源，以及要與其共用的參與者。參加者可包括：

- 所有者組織 AWS 帳戶 內部或外部的特定內部或外部 AWS Organizations
- 其組織內部的組織單位 AWS Organizations
- 它的整個組織 AWS Organizations

若要取得有關的更多資訊 AWS RAM，請參閱AWS RAM 使用者指南。

透過在 Route 53 ARC 中使 AWS Resource Access Manager 用跨帳戶共用叢集資源，您可以使用一個叢集來裝載多個不同的控制面板和路由控制項 AWS 帳戶。當您選擇共用叢集時，您指定 AWS 帳戶的其他叢集可以使用叢集來裝載自己的控制面板和路由控制項，讓不同團隊之間的路由功能有更多的控制和彈性。

AWS RAM 是一項可協助 AWS 客戶安全地共用資源的服務 AWS 帳戶。透過 AWS RAM，您可以使用 IAM 角色和使用者在中 AWS Organizations共用組織或組織單位 (OU) 內的資源。 AWS RAM 是共用叢集的集中且受控管的方式。

共用叢集時，您可以減少組織所需的叢集總數。使用共用叢集，您可以分配跨不同團隊執行叢集的總成本，以較低的成本將 Route 53 ARC 的優點發揮到最大。建立在叢集中託管的資源不會對擁有者或參與者產生額外費用。) 跨帳戶共用叢集也可以簡化將多個應用程式上線至 Route 53 ARC 的程序，特別是如果您在多個帳戶和營運團隊中分散了大量應用程式時。

若要在 Route 53 ARC 中開始使用跨帳戶共用，請在中建立資源共 AWS RAM用。資源共用指定有權共用您帳戶擁有之叢集的參與者。然後，參與者可以使用或使用 AWS Management Console 或 AWS

SDK 執行 Route 53 ARC API 作業，在叢集中建立資源，例如控制台和路由控制項。 AWS Command Line Interface

本主題說明如何共用您擁有的資源，以及如何使用與您共用的資源。

目錄

- 共用叢集的先決條件
- 共用叢集
- 取消共用共用叢集
- 識別共用叢集
- 共用叢集的責任和權限
- 帳單成本
- 配額

共用叢集的先決條件

- 若要共用叢集，您必須在 AWS 帳戶. 這表示必須在您的帳戶中配置或佈建資源。您無法共用已與您共用的叢集。
- 若要與中的組織或組織單位共用叢集 AWS Organizations，您必須啟用與共用 AWS Organizations。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的透過 AWS Organizations啟用共用。

共用叢集

當您共用您擁有的叢集時，您指定要共用叢集的參與者可以在叢集中建立並裝載他們自己的 Route 53 ARC 資源。

若要共用叢集，您必須將其新增至資源共用。資源共用是一 AWS RAM 種可讓您共用資源的資源 AWS 帳戶。資源共用指定要共用的資源，以及與其共用的參與者。若要共用叢集，您可以建立新的資源共用或將資源新增至現有的資源共用。若要建立新的資源共用，您可以使用AWS RAM 主控台，或搭配 AWS Command Line Interface 或 AWS SDK 使用 AWS RAM API 作業。

如果您是組織的一員， AWS Organizations 且已啟用組織內的共用功能，則組織中的參與者會自動獲得共用叢集的存取權。否則，參與者會收到加入資源共用的邀請，並在接受邀請後授與共用叢集的存取權。

您可以使用 AWS RAM 主控台或搭配或 SDK 使用 AWS RAM API 作業來共用您擁有的 AWS CLI 叢集。

使用主控台共用您擁有的 AWS RAM 叢集

請參閱《使用指南》中的〈建立資源共AWS RAM用〉。

若要共用您擁有的叢集 AWS CLI

使用 create-resource-share 命令。

取消共用共用叢集

取消共用叢集時，以下內容適用於參與者和擁有者：

- 目前的參與者資源會繼續存在於非共用叢集中。
- 參與者可以繼續更新非共用叢集中的路由控制狀態，以管理應用程式容錯移轉的路由。
- 參與者無法再在非共用叢集中建立新資源。
- 如果參與者在非共用叢集中仍有資源，則擁有者無法刪除共用叢集。

若要取消共用您擁有的共用叢集，請將其從資源共用中移除。您可以使用 AWS RAM 主控台或搭配 AWS CLI 或 SDK 使用 AWS RAM API 作業來執行此操作。

若要取消共用您使用主控台擁有的 AWS RAM 共用叢集

請參閱《AWS RAM 使用者指南》中的更新資源共享。

若要取消共用您所擁有的共用叢集 AWS CLI

使用 disassociate-resource-share 命令。

識別共用叢集

擁有者和參與者可以透過檢視中的資訊來識別共用叢集 AWS RAM。他們也可以使用 Route 53 ARC 主控台和 AWS CLI.

一般而言，若要進一步瞭解您已共用或已與您共用的資源，請參閱 AWS Resource Access Manager 使用者指南中的資訊：

- 身為擁有者，您可以使用來檢視與他人共用的所有資源 AWS RAM。如需詳細資訊，請參閱在中檢視您的共用資源 AWS RAM。
- 身為參與者，您可以使用來檢視與您共用的所有資源 AWS RAM。如需詳細資訊，請參閱在中檢視您的共用資源 AWS RAM。

身為擁有者，您可以透過檢視 AWS Management Console 或使用 AWS Command Line Interface 與 Route 53 ARC API 作業中的資訊來判斷您是否共用叢集。

使用主控台識別您擁有的叢集是否共用

在叢集的 AWS Management Console詳細資料頁面上，查看叢集共用狀態。

若要識別您擁有的叢集是否共用，請使用 AWS CLI

使用取得資源原則命令。如果叢集有資源策略，命令會傳回有關策略的資訊。

身為參與者，當叢集與您共用時，您通常必須接受共用。此外，叢集的 [擁有者] 欄位包含叢集擁有者的帳戶。

共用叢集的責任和權限

擁有者的許可

當您與其他叢集共用您擁有的叢集時 AWS 帳戶，允許使用該叢集的參與者可以在叢集中建立控制台、路由控制和其他資源。

身為叢集擁有者，您必須負責建立、管理和刪除叢集。您無法修改或刪除參與者建立的資源，例如路由控制和安全規則。例如，您無法更新參與者建立的路由控制來變更路由控制狀態。

不過，您可以檢視由您擁有之叢集中的參與者所建立的路由控制項的詳細資料。例如，您可以使用 AWS Command Line Interface 或 AWS SDK 呼叫 Route 53 ARC 路由控制 API 作業，來檢視路由控制狀態。

如果您需要修改參與者建立的資源，他們可以在 IAM 中設定具有資源存取權限的角色，並將您的帳戶新增至該角色。

參與者的權限

一般而言，參與者可以建立和使用控制台、路由控制項、安全規則和健康狀態檢查，這些都是在與他們共用的叢集中建立的。他們只能在擁有資源的情況下檢視、修改或刪除共用叢集中的叢集資源。例如，參與者可以針對已建立的控制台建立和刪除安全規則。

以下限制適用於參與者：

- 參與者無法檢視、修改或刪除其他帳戶使用共用叢集建立的控制面板。
- 參與者無法檢視、建立或修改由其他帳號在共用叢集中建立的資源的路由控制 (包括路由控制狀態)。

- 參與者無法建立、修改或檢視共用叢集中其他帳戶所建立的安全規則。
- 參與者無法在共用叢集的預設控制台中新增資源，因為它屬於叢集擁有者。

如前所述，參與者無法在共用叢集的預設控制台中建立路由控制項，因為叢集擁有者擁有預設控制台。不過，叢集擁有者可以建立跨帳戶 IAM 角色，以提供存取叢集預設控制面板的權限。然後，擁有者可以授與參與者擔任角色的權限，以便參與者可以存取預設控制面板以使用它，但是擁有者已透過角色的權限指定。

帳單成本

Route 53 ARC 中叢集的擁有者需支付與叢集相關聯的費用。對於叢集擁有者或參與者而言，建立叢集中託管的資源不會產生額外費用。

如需詳細的定價資訊和範例，請參閱 Amazon Route 53 應用程式復原控制器定價並向下捲動至 Amazon Route 53 應用程式復原控制器。

配額

在共用叢集中建立的所有資源 (包括所有可存取共用叢集的參與者所建立的資源) 會計入叢集和其他資源 (例如路由控制) 的有效配額。如果共用叢集資源的帳號的配額高於叢集擁有者的配額，則叢集擁有者的配額優先順序高於共用帳號的配額。

若要更好地瞭解其運作方式，請參閱下列範例。為了說明配額如何使用資源共用，在這些範例中，假設叢集擁有者是 Owner，而叢集已與之共用的帳戶是「參與者」。

控制面板配額

系統會針對擁有者每個叢集的總控制面板強制執行配額。

例如，假設 Owner 的每個集群控制面板數量配額為 50，並且在集群中有 13 個控制面板。現在，假設參與者的配額設置為 150。在這個案例中，參與者最多只能在共用叢集中建立 37 個控制台 (也就是 50-13)。

此外，如果共用叢集的其他帳戶也建立控制面板，則這些也會計入 50 個控制面板的叢集整體配額中。

路由控制配額

路由控制有多個配額：每個控制面板的配額、每個叢集的配額，以及每個安全規則的配額。所有這些配額的擁有者配額優先。

例如，假設每個叢集的路由控制項數目擁有 300 個配額，而且叢集中已有 300 個路由控制項。現在，假設參加者將此配額設置為 500。在這個案例中，參與者無法在共用叢集中建立任何新的路由控制項。

安全規則配額

針對每個控制面板配額的擁有者安全規則強制執行配額。

例如，每個控制面板的安全規則數量擁有 20 個配額，而參與者將此配額設置為 80。在此案例中，由於擁有者的下限優先順序，因此參與者最多只能在共用叢集的控制台中建立 20 個安全規則。

如需路由控制配額的清單，請參閱路由控制配額。

記錄和監控 Amazon Route 53 應用程式復原控制器中的路由控制

您可以 AWS CloudTrail 用來監控 Amazon Route 53 應用程式復原控制器中的路由控制，以分析模式並協助疑難排解問題。

主題

- 使用記錄 Route 53 ARC API 呼叫 AWS CloudTrail

使用記錄 Route 53 ARC API 呼叫 AWS CloudTrail

Amazon Route 53 應用程式復原控制器整合在一起 AWS CloudTrail，這項服務可提供 Route 53 ARC 中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 將 Route 53 ARC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Route 53 ARC 主控台的呼叫，以及對 Route 53 ARC API 作業的程式碼呼叫。

如果您建立追蹤，您可以啟用連續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Route 53 ARC 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 Route 53 ARC 發出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Route 53 弧資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 Route 53 ARC 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以查看，搜索和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄。

對於正在進行的事件記錄 AWS 帳戶，包括 Route 53 ARC 的事件，請創建一條線索。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

Amazon Route 53 應用程式復原控制器的復原準備 API 參考指南、Amazon Route 53 應用程式復原控制器的復原控制組態 API 參考指南、Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南都會記錄下來，並記錄在 Amazon Route 53 應用程式復原控制器的路由控制 API 參考 CloudTrail 例如，呼叫`UpdateRoutingControlState`和`CreateRecoveryGroup`動作會`CreateCluster`在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

在活動歷史記錄中查看 Route 53 ARC 事件

CloudTrail 可讓您在事件歷史記錄中檢視最近的事件。若要檢視 Route 53 ARC API 要求的事件，您必須在主控台頂端的「區域」選取器中選擇美國西部 (奧勒岡)。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。

瞭解 Route 53 ARC 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範設定路由控制之CreateCluster動作的 CloudTrail 記錄項目。


```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "IAMUser",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:iam::111122223333:user/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/smithj",
              "accountId": "111122223333",
              "userName": "smithj"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "CreateCluster",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "ClientToken": "12345abcdef-1234-5678-abcd-12345abcdef",
      "ClusterName": "XYZCluster"
  },
  "responseElements": {
      "Cluster": {
          "Arn": "arn:aws:route53-recovery-control::012345678901:cluster/abc123456-
aa11-bb22-cc33-abc123456",
          "ClusterArn": "arn:aws:route53-recovery-control::012345678901:cluster/
abc123456-aa11-bb22-cc33-abc123456",
          "Name": "XYZCluster",
          "Status": "PENDING"
      }
```

```
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

下列範例顯示示範路由控制UpdateRoutingControlState動作的 CloudTrail 記錄項目。

```
{
  "eventVersion": "1.08",
   "userIdentity": {
     "type": "AssumedRole",
     "principalId": "A1B2C3D4E5F6G7EXAMPLE",
     "arn": "arn:aws:sts::111122223333:assumed-role/admin/smithj",
     "accountId": "111122223333",
     "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
     "sessionContext": {
          "sessionIssuer": {
              "type": "Role",
              "principalId": "A1B2C3D4E5F6G7EXAMPLE",
              "arn": "arn:aws:iam::111122223333:role/admin",
              "accountId": "111122223333",
              "userName": "admin"
          },
          "webIdFederationData": {},
          "attributes": {
              "mfaAuthenticated": "false",
              "creationDate": "2021-06-30T04:44:41Z"
          }
      }
  },
  "eventTime": "2021-06-30T04:45:46Z",
  "eventSource": "route53-recovery-control-config.amazonaws.com",
  "eventName": "UpdateRoutingControl",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "192.0.2.50",
  "userAgent": "aws-cli/2.0.0 Python/3.8.2 Darwin/19.6.0 botocore/2.0.0dev7",
  "requestParameters": {
      "RoutingControlName": "XYZRoutingControl3",
```

```
      "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
  },
  "responseElements": {
      "RoutingControl": {
          "ControlPanelArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456",
          "Name": "XYZRoutingControl3",
          "Status": "DEPLOYED",
          "RoutingControlArn": "arn:aws:route53-recovery-
control::012345678:controlpanel/0123456bbbbbbb0123456bbbbbb0123456/routingcontrol/
abcdefg1234567"
      }
  },
  "requestID": "6090509a-5a97-4be6-8e6a-7d73example",
  "eventID": "9cab44ef-0777-41e6-838f-f249example",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```


路由控制的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Route 53 ARC 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

目錄

- Amazon Route 53 應用程式復原控制器中的路由控制如何搭配 IAM 運作
- Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例
- AWS Amazon Route 53 應用程式復原控制器中路由控制的受管政策

Amazon Route 53 應用程式復原控制器中的路由控制如何搭配 IAM 運作

在您使用 IAM 管理 Amazon Route 53 應用程式復原控制器中路由控制的存取權限之前，請先了解哪些 IAM 功能可與路由控制搭配使用。

您可以在 Amazon Route 53 應用程式復原控制器中搭配路由控制使用的 IAM 功能

IAM 功能	路由控制支援
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC(政策中的標籤)	部分
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	否

若要取得 AWS 服務如何搭配大多數 IAM 功能運作的高階整體檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

Route 53 ARC 的基於身份的政策

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

若要檢視 Route 53 ARC 以身分識別為基礎的原則以進行路由控制的範例，請參閱。Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例

路由控制內的資源型政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。

路由控制的原則動作

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看路由控制的 Route 53 ARC 動作清單，請參閱服務授權參考中由 Amazon Route 53 復原控制定義的動作和 Amazon Route 53 復原叢集定義的動作。

Route 53 ARC 中用於路由控制的策略操作在操作之前使用以下前綴，具體取決於您正在使用的 API：

```
route53-recovery-control-config
route53-recovery-cluster
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，您可以執行下列操作：

```
"Action": [
      "route53-recovery-control-config:action1",
      "route53-recovery-control-config:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "route53-recovery-control-config:Describe*"
```

若要檢視 Route 53 ARC 以身分識別為基礎的原則以進行路由控制的範例，請參閱。Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例

Route 53 的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

在服務授權參考中，您可以看到下列與 Route 53 ARC 相關的資訊：

若要查看資源類型及其 ARN 的清單，以及您可以使用每個資源的 ARN 指定的動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 恢復控制定義的操作
- Amazon 路由 53 恢復集群定義的操作。

若要檢視 Route 53 ARC 以身分識別為基礎的原則以進行路由控制的範例，請參閱。Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例

Route 53 ARC 的政策條件索引鍵

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看路由控制的 Route 53 ARC 條件金鑰清單，請參閱服務授權參考資料中的下列主題：

- Amazon Route 53 恢復控制的條件鍵
- Amazon 路由 53 恢復集群的條件密鑰

若要查看可搭配條件索引鍵使用的動作和資源，請參閱服務授權參考中的下列主題：

- 若要查看資源類型及其 ARN 的清單，請參閱 Amazon Route 53 復原控制和 Amazon Route 53 復原叢集定義的動作定義的動作。
- 若要查看可以使用每個資源的 ARN 指定的動作清單，請參閱 Amazon Route 53 復原控制項定義的資源和 Amazon Route 53 復原叢集定義的資源。

若要檢視 Route 53 ARC 以身分識別為基礎的原則，以進行路由控制，請參閱 Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例

Route 53 中的訪問控制列表（ACL）

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

基於屬性的訪問控制（ABAC）與 Route 53 ARC

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

Route 53 弧線路控制包括對 ABAC 的下列支援：

- 恢復控制 Config 支持 ABAC。
- 復原叢集不支援 ABAC。

使用臨時登入資料與 Route 53 ARC

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

Route 53 ARC 的跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 實體 (使用者或角色) 在中執行動作時 AWS，系統會將您視為主體。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。

若要查看動作是否需要原則中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon 路線 53 恢復集群
- Amazon 路線 53 恢復控制

Route 53 ARC 的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

Route 53 ARC 的服務連結角色

支援服務連結角色	是

服務連結角色是連結至服務的一種服務角色類型。 AWS 服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的 AWS 帳戶中，且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

路由控制不使用服務連結角色。

Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例

根據預設，使用者和角色沒有建立或修改 Route 53 ARC 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Route 53 ARC 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon Route 53 應用程式復原控制器的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 範例：用於路由控制的 Route 53 ARC 主控台存取
- 範例：用於路由控制組態的路由 Route 53 ARC API 動作

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 Route 53 ARC 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始授與使用者和工作負載的權限，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access

Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。

- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

範例：用於路由控制的 Route 53 ARC 主控台存取

若要存取 Amazon Route 53 應用程式復原控制器主控台，您必須擁有至少一組許可。這些權限必須允許您列出和查看有關 Route 53 ARC 資源的詳細信息 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色在您僅允許存取特定 API 作業時仍可使用 Route 53 ARC 主控台，請同時將 Route 53 ARC 的`ReadOnly` AWS 受管理原則附加至實體。如需詳細資訊，請參閱《Route 53 ARC Route 53 ARC 管理政策》頁面或《IAM 使用者指南》中的向使用者新增許可。

若要讓使用者能夠透過主控台使用 Route 53 ARC 路由控制功能的完整存取權，請將類似下列的原則附加給使用者，讓使用者擁有設定 Route 53 ARC 路由控制資源和作業的完整權限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-cluster:GetRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlState",
                   "route53-recovery-cluster:UpdateRoutingControlStates",
                   "route53-recovery-control-config:CreateCluster",
                   "route53-recovery-control-config:CreateControlPanel",
                   "route53-recovery-control-config:CreateRoutingControl",
                   "route53-recovery-control-config:CreateSafetyRule",
                   "route53-recovery-control-config:DeleteCluster",
                   "route53-recovery-control-config:DeleteControlPanel",
                   "route53-recovery-control-config:DeleteRoutingControl",
                   "route53-recovery-control-config:DeleteSafetyRule",
```

```
                    "route53-recovery-control-config:DescribeCluster",
                    "route53-recovery-control-config:DescribeControlPanel",
                    "route53-recovery-control-config:DescribeSafetyRule",
                    "route53-recovery-control-config:DescribeRoutingControl",
                    "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                    "route53-recovery-control-config:ListClusters",
                    "route53-recovery-control-config:ListControlPanels",
                    "route53-recovery-control-config:ListRoutingControls",
                    "route53-recovery-control-config:ListSafetyRules",
                    "route53-recovery-control-config:UpdateControlPanel",
                    "route53-recovery-control-config:UpdateRoutingControl",
                    "route53-recovery-control-config:UpdateSafetyRule"
             ],
            "Resource": "*"
        },
                {
            "Effect": "Allow",
            "Action": [
                    "route53:GetHealthCheck",
                    "route53:CreateHealthCheck",
                    "route53:DeleteHealthCheck",
                    "route53:ChangeTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

範例：用於路由控制組態的路由 Route 53 ARC API 動作

若要確保使用者可以使用 Route 53 ARC API 動作來搭配 Route 53 ARC 路由控制設定，請附加與使用者需要使用的 API 作業相對應的原則，如下所述。

要使用 API 操作進行恢復控制配置，請將類似以下的策略附加到用戶：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "route53-recovery-control-config:CreateCluster",
                    "route53-recovery-control-config:CreateControlPanel",
                    "route53-recovery-control-config:CreateRoutingControl",
```

```
                "route53-recovery-control-config:CreateSafetyRule",
                "route53-recovery-control-config:DeleteCluster",
                "route53-recovery-control-config:DeleteControlPanel",
                "route53-recovery-control-config:DeleteRoutingControl",
                "route53-recovery-control-config:DeleteSafetyRule",
                "route53-recovery-control-config:DescribeCluster",
                "route53-recovery-control-config:DescribeControlPanel",
                "route53-recovery-control-config:DescribeSafetyRule",
                "route53-recovery-control-config:DescribeRoutingControl",
                "route53-recovery-control-config:GetResourcePolicy",
                "route53-recovery-control-config:ListAssociatedRoute53HealthChecks",
                "route53-recovery-control-config:ListClusters",
                "route53-recovery-control-config:ListControlPanels",
                "route53-recovery-control-config:ListRoutingControls",
                "route53-recovery-control-config:ListSafetyRules",
                "route53-recovery-control-config:ListTagsForResource",
                "route53-recovery-control-config:UpdateControlPanel",
                "route53-recovery-control-config:UpdateRoutingControl",
                "route53-recovery-control-config:UpdateSafetyRule",
                "route53-recovery-control-config:TagResource",
                "route53-recovery-control-config:UntagResource"
            ],
            "Resource": "*"
        }
    ]
}
```

若要使用復原叢集資料平面 API 執行 Route 53 ARC 路由控制中的工作，例如，將路由控制狀態更新為在災難事件期間容錯移轉，您可以將 Route 53 ARC IAM 政策附加到 IAM 使用者。

`AllowSafetyRuleOverride`布林值允許覆寫您已設定為路由控制項的保護措施的安全規則。在「破壞」案例中，可能需要此權限，才能略過災難或其他緊急容錯移轉案例中的保護措施。例如，操作員可能需要快速容錯移轉以進行災難復原，而一個或多個安全規則可能會意外地阻止重新路由傳送流量所需的路由控制狀態更新。此權限允許操作員在進行 API 呼叫以更新路由控制狀態時指定要覆寫的安全規則。如需詳細資訊，請參閱 覆蓋安全規則以重新路由交通。

如果您想要允許運算子使用復原叢集資料平面 API，但要防止覆寫安全規則，您可以將原則 (如下所示) 附加至`AllowSafetyRuleOverridesfalse`布林值。若要允許運算子覆寫安全規則，請將`AllowSafetyRuleOverrides`布林值設定為`true`。

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:GetRoutingControlState",
                "route53-recovery-cluster:ListRoutingControls"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "route53-recovery-cluster:UpdateRoutingControlStates",
                "route53-recovery-cluster:UpdateRoutingControlState"
            ],
            "Resource": "*",
            "Condition": {
                "Bool": {
                    "route53-recovery-cluster:AllowSafetyRulesOverrides": "false"
                }
            }
        }
    ]
}
```

AWS Amazon Route 53 應用程式復原控制器中路由控制的受管政策

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 受管理的策略： AmazonRoute53 RecoveryControlConfigFullAccess

您可以將 AmazonRoute53RecoveryControlConfigFullAccess 連接到 IAM 實體。此原則授與在 Route 53 ARC 中使用復原控制組態的動作的完整存取權。將其附加至需要完整存取復原控制設定動作的 IAM 使用者和其他主體。

您可以自行決定新增其他 Amazon Route 53 動作的存取權，讓使用者能夠針對路由控制建立運作狀態檢查。例如，您可以允許下列一或多個動作的權限：route53:GetHealthCheckroute53:CreateHealthCheck、route53:DeleteHealthCheck、和route53:ChangeTagsForResource。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryControlConfigFullAccess的策略參考中的AmazonRoute53。

AWS 受管理的策略： AmazonRoute53 RecoveryControlConfigReadOnlyAccess

您可以將 AmazonRoute53RecoveryControlConfigReadOnlyAccess 連接到 IAM 實體。對於需要查看路由控制和安全規則配置的用戶而言，這很有用。此原則會授與在 Route 53 ARC 中使用復原控制組態之動作的唯讀存取權。這些使用者無法建立、更新或刪除修復控制資源。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryControlConfigReadOnlyAccess的策略參考中的AmazonRoute53。

AWS 受管理的策略： AmazonRoute53 RecoveryClusterFullAccess

您可以將 AmazonRoute53RecoveryClusterFullAccess 連接到 IAM 實體。此原則授與在 Route 53 ARC 中處理叢集資料平面的動作的完整存取權。將其附加到 IAM 使用者和其他需要更新和擷取路由控制狀態的完整存取權限的主體。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryClusterFullAccess的策略參考中的AmazonRoute53。

AWS 受管理的策略： AmazonRoute53 RecoveryClusterReadOnlyAccess

您可以將 AmazonRoute53RecoveryClusterReadOnlyAccess 連接到 IAM 實體。此原則會授與 Route 53 ARC 中叢集資料平面的唯讀存取權。這些使用者可以擷取路由控制狀態，但無法更新它們。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryClusterReadOnlyAccess的策略參考中的AmazonRoute53。

路由控制的 AWS 受管理策略更新

如需有關 Route 53 ARC 中路由控制的 AWS 受管原則更新，自此服務開始追蹤這些變更後的詳細資訊，請參閱Amazon Route 53 應用程式復原控制器的 AWS 受管政策更新。如需有關此頁面變更的自動警示，請訂閱 Route 53 ARC 文件歷史記錄頁面上的 RSS 摘要。

路由控制配額

Amazon Route 53 應用程式復原控制器中的路由控制必須遵守下列配額 (先前稱為限制)。

實體	配額
每個帳戶的叢集數目	2
每個集群的控制面板數量	50
每個控制面板的路由控制數	100
每個叢集的路由控制總數 (在所有控制面板中)	300
每個控制面板的安全規則數	20
每個UpdateRoutingControlStates作業呼叫的路由控制項數	10
對叢集端點的變更 API 呼叫次數 (每秒)	3

Amazon 路線 53 應用程序恢復控制器中的準備

透過 Amazon Route 53 應用程式復原控制器中的準備就緒檢查，您可以深入瞭解應用程式和資源是否已準備好進行復原。在 Route 53 ARC 中建立 AWS 應用程式模型並建立整備檢查之後，檢查會持續監控應用程式的相關資訊，例如 AWS 資源配額、容量和網路路由原則。然後，您可以選擇收到有關會影響您容錯移轉到應用程式複本以從事件復原之能力的變更的通知。整備程度檢查有助於確保您可以持續將多區域應用程式維持在調整和設定為處理容錯移轉流量的狀態。

本章說明如何在 Route 53 ARC 中建立應用程式的模型，藉由建立描述應用程式的復原群組和儲存格，以設定可讓整備檢查運作的結構。然後，您可以按照步驟添加整備檢查和整備範圍，以便 Route 53 ARC 可以審核應用程序的準備情況。

建立整備檢查之後，您可以監視資源的整備狀態。整備程度檢查可協助您確保待命應用程式複本及其資源持續符合您的生產複本，反映生產應用程式的容量、路由原則及其他組態詳細資料。如果複本不相符，您可以新增容量或變更組態，以便再次對齊應用程式複本。

> **Important**
>
> 整備檢查對於持續驗證應用程式複本組態和執行階段狀態是否符合最有用。整備檢查不應該用來指出生產複本是否健康，也不應該依賴整備檢查作為災難事件期間容錯移轉的主要觸發器。

什麼是 Amazon Route 53 應用程序恢復控制器的準備檢查？

Route 53 ARC 中的準備程度檢查會持續 (以一分鐘的間隔) 稽核 AWS 已佈建容量、服務配額、節流限制，以及檢查中所包含資源的組態和版本差異不相符。整備檢查可以通知您這些差異，以便您可以確保每個複本具有相同的配置設置和相同的運行時狀態。雖然整備檢查可確保跨複本設定的容量是一致的，但您不應該期望它們代表您決定複本的容量。例如，您應該瞭解應用程式需求，以便在每個複本中以足夠的緩衝區容量調整 Auto Scaling 群組的大小，以便管理其他儲存格是否無法使用。

對於配額，當 Route 53 ARC 偵測到與整備檢查不相符時，它可以採取措施，藉由增加較低的配額以符合較高的配額來調整複本的配額。當配額相符時，就會顯示整備檢查狀態`READY`。(請注意，這不是立即更新程序，而且總時間取決於特定的資源類型和其他因素。)

第一個步驟是設定整備檢查，以建立代表您應用程式的復原群組。每個復原群組都包含每個個別容錯裝置或應用程式複本的儲存格。接下來，您會為應用程式中的每個資源類型建立資源集，並將整備檢查與資源集產生關聯。最後，您將資源與整備範圍產生關聯，因此您可以取得復原群組 (您的應用程式) 或個別儲存格 (複本，即區域或可用區域 (AZ)) 中資源的整備狀態。

整備程度 (也就是`READY`或`NOT READY`) 是以整備程度檢查範圍內的資源和資源類型的規則集為基礎。每個資源類型都有一組準備規則，Route 53 ARC 會檢查用來稽核資源是否準備就緒。資源是`READY`否為基於每個整備規則的定義方式。所有整備規則都會評估資源，但有些人會彼此比較資源，有些則會查看資源集中每個資源的特定資訊。

透過新增整備檢查，您可以透過下列其中一種方式監視整備狀態：使用 EventBridge AWS Management Console、在中或使用 Route 53 ARC API 動作。您也可以監控不同內容中資源的準備狀態，包括儲存格的準備程度和應用程式的準備情況。使用 Route 53 ARC 中的跨帳戶授權功能，可以更輕鬆地從單一 AWS 帳戶設定和監視分散式資源。

使用整備檢查監控應用程式複本

Route 53 ARC 會使用整備檢查來稽核您的應用程式複本，以確保每個複本具有相同的組態設定和相同的執行階段狀態。整備檢查會持續稽核應用程式的 AWS 資源容量、組態、 AWS 配額和路由原則，這些資訊可用來協助確保複本已準備好進行容錯移轉。整備程度檢查可協助您確保您的復原環境已調整規模，並設定為在需要時容錯移轉至。

以下各節提供有關整備檢查如何運作的詳細資訊。

整備程度檢查和應用程式複本

若要準備復原，您必須始終在複本中保持足夠的備用容量，以吸收來自其他可用區域或區域的容錯移轉流量。Route 53 ARC 會持續 (每分鐘一次) 檢查您的應用程式，以確保佈建的容量在所有可用區域或區域之間相符。

Route 53 ARC 檢查的容量包括 Amazon EC2 執行個體計數、Aurora 讀取和寫入容量單位，以及亞馬遜 EBS 磁碟區大小。如果您擴充主要複本中資源值的容量，但忘記也增加待命複本中的對應值，Route 53 ARC 會偵測不相符，以便您可以增加待命中的值。

> **Important**
>
> 整備檢查對於持續驗證應用程式複本組態和執行階段狀態是否符合最有用。整備檢查不應該用來指出生產複本是否健康，也不應該依賴整備檢查作為災難事件期間容錯移轉的主要觸發器。

在作用中-待命組態中，您應該根據您的監視和健康狀態檢查系統，決定是否要離開或離開小區，並將整備檢查視為這些系統的補充服務。Route 53 ARC 準備程度檢查不具備高可用性，因此您不應該依賴停電期間可存取的檢查。此外，在災難事件期間，已檢查的資源可能也無法使用。

您可以監視特定儲存格 (AWS 區域或可用區域) 或整體應用程式中應用程式資源的整備狀態。當整備檢查狀態變更時，您可以收到通知，例如`Not ready`，透過在中建立規則 EventBridge。如需詳細資訊，請參閱 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge。您也可以在中檢視整備狀態 AWS Management Console，或使用 API 作業，例如`get-recovery-readiness`。如需詳細資訊，請參閱 準備程度檢查 API 作業。

準備檢查的工作原理

Route 53 ARC 會使用整備檢查來稽核您的應用程式複本，以確保每個複本具有相同的組態設定和相同的執行階段狀態。

例如，若要準備復原，您必須始終保持足夠的備用容量，以吸收來自其他可用區域或區域的容錯移轉流量。Route 53 ARC 會持續 (每分鐘一次) 檢查您的應用程式，以確保佈建的容量在所有可用區域或區域之間相符。Route 53 ARC 檢查的容量包括 Amazon EC2 執行個體計數、Aurora 讀取和寫入容量單位，以及亞馬遜 EBS 磁碟區大小。如果您擴充主要複本中資源值的容量，但忘記也增加待命複本中的對應值，Route 53 ARC 會偵測不相符，以便您可以增加待命中的值。

> **Important**
>
> 整備檢查對於持續驗證應用程式複本組態和執行階段狀態是否符合最有用。整備檢查不應該用來指出生產複本是否健康，也不應該依賴整備檢查作為災難事件期間容錯移轉的主要觸發器。

在作用中-待命組態中，您應該根據您的監視和健康狀態檢查系統，決定是否要離開或離開小區，並將整備檢查視為這些系統的補充服務。Route 53 ARC 準備程度檢查不具備高可用性，因此您不應該依賴停電期間可存取的檢查。此外，在災難事件期間，已檢查的資源可能也無法使用。

您可以監視特定儲存格 (AWS 區域或可用區域) 或整體應用程式中應用程式資源的整備狀態。當整備檢查狀態變更時，您可以收到通知，例如`Not ready`，透過在中建立規則 EventBridge。如需詳細資訊，請參閱 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge。您也可以在中檢視整備狀態 AWS Management Console，或使用 API 作業，例如`get-recovery-readiness`。如需詳細資訊，請參閱 準備程度檢查 API 作業。

準備規則如何決定準備狀態

Route 53 ARC 準備程度檢查會根據每個資源類型的預先定義規則及這些規則的定義方式來決定整備狀態。Route 53 ARC 針對其支援的每種資源類型包含一組規則。例如，Route 53 ARC 具有適用於 Amazon Aurora 叢集、Auto Scaling 群組等的整備規則群組。有些整備規則會將集合中的資源互相比較，有些則會查看資源集中每個資源的特定資訊。

您無法新增、編輯或移除整備規則或規則群組。不過，您可以建立 Amazon CloudWatch 警示並建立整備檢查，以監控警示的狀態。例如，您可以建立自訂 CloudWatch 警示來監控 Amazon EKS 容器服務，並建立整備檢查以稽核警示的整備狀態。

您可以在建立資源集 AWS Management Console 時檢視中每個資源類型的所有整備規則，也可以稍後瀏覽至資源集的詳細資訊頁面來檢視整備規則。您也可以在下一節中檢視整備規則：Route 53 中的準備規則。

當整備檢查使用一組規則稽核一組資源時，每個規則的定義方式會決定結果是否為`READY`或`NOT READY`針對所有資源，或是不同資源的結果是否不同。此外，您還可以透過多種方式檢視整備狀態。例

如，您可以檢視資源集中資源群組的整備狀態，或檢視復原群組或儲存格 (也就是區 AWS 域或可用區域，視您設定復原群組的方式而定) 的整備狀態摘要。

每個規則說明中的措辭都會說明它如何評估資源，以判斷套用該規則時的整備狀態。規則被定義為檢查每個資源或檢查資源集中的所有資源以確定準備程度。具體而言，規則的運作方式如下：

- 規則會檢查資源集中的每個資源以確保條件。
  - 如果所有資源都成功，則會將所有資源設定為READY。
  - 如果其中一個資源失敗，則該資源會設定為NOT READY，而其他儲存格會保留READY。

  例如：MskClusterState:檢查每個 Amazon MSK 叢集以確保其處於某ACTIVE個狀態。
- 規則會檢查資源集中的所有資源以確保條件。
  - 如果確保條件，則所有資源都設置為READY。
  - 如果有任何不符合條件，則會將所有資源設定為NOT READY。

  例如：VpcSubnetCount:檢查所有VPC子網路，以確保它們具有相同數目的子網路。
- 非嚴重規則：規則會檢查資源集中的所有資源，以確保條件。
  - 如果有任何失敗，就緒狀態會維持不變。具有此行為的規則在其描述中有附註。

  例如：ElbV2CheckAzCount:檢查每個 Network Load Balancer，以確保其僅附加到一個可用區域。附註：此規則不會影響整備狀態。

此外，Route 53 ARC 需要額外的配額步驟。如果整備檢查偵測到任何支援資源的服務配額 (資源建立和作業的最大值) 之間的儲存格不相符，Route 53 ARC 會自動提高配額較低的資源配額。這僅適用於配額（限制）。對於容量，您應該根據應用程式需求增加額外容量。

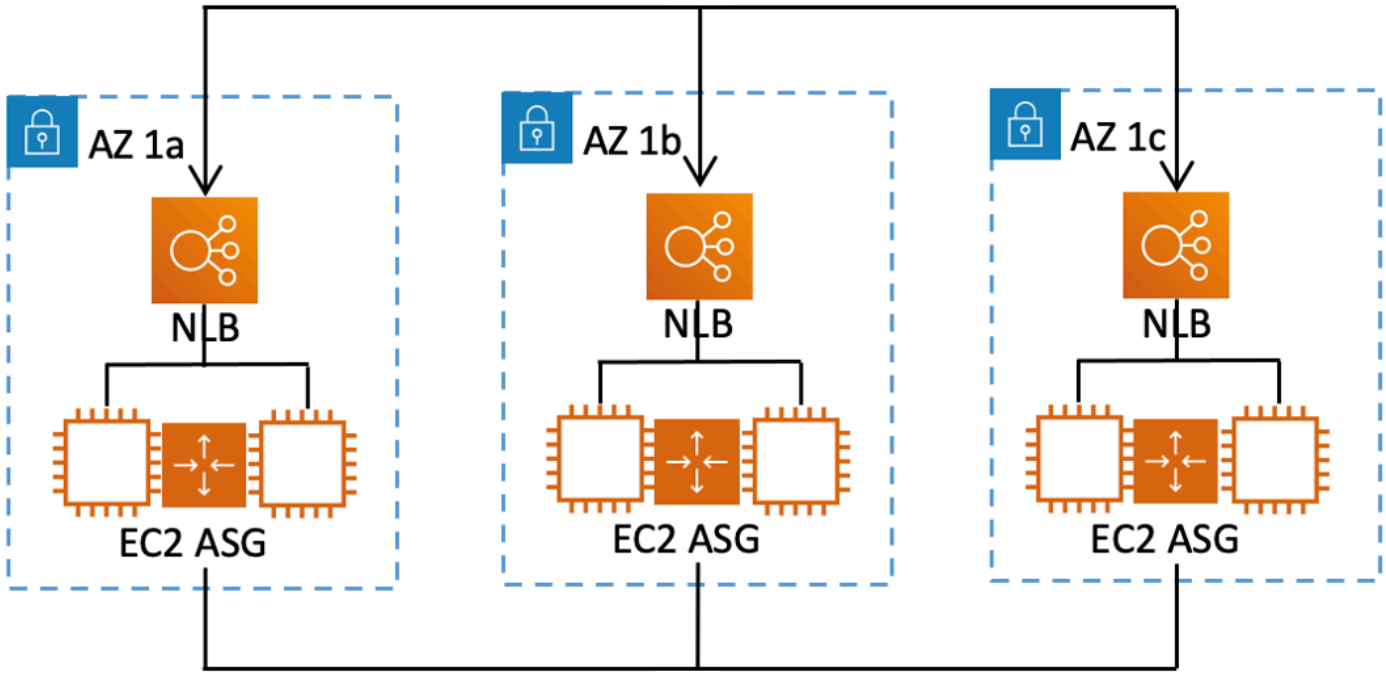
您也可以設定 Amazon EventBridge 通知以進行整備檢查，例如當任何準備檢查狀態變更為時NOT READY。然後，當偵測到組態不相符時， EventBridge 會傳送通知給您，您可以採取更正動作，確定應用程式複本已對齊並準備好進行復原。如需詳細資訊，請參閱 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge。

整備程度檢查、資源集和整備範圍如何協同運作

整備檢查一律會稽核資源集中的資源群組。您可以建立資源集 (個別或在建立整備檢查時)，將 Route 53 ARC 復原群組中儲存格 (可用區 AWS 域或區域) 中的資源分組，以便您可以定義整備檢查。資源集通常是相同類型資源的群組 (例如網路負載平衡器)，但也可以是 DNS 目標資源，用於架構整備程度檢查。

您通常會為應用程式中的每種資源類型建立一個資源集和整備檢查。若要進行架構整備檢查，請為其建立頂層 DNS 目標資源和全域 (復原群組層級) 資源集，然後針對個別的資源集建立儲存格層級 DNS 目標資源。

下圖顯示具有三個儲存格 (可用區域) 的復原群組範例，每個儲存格都具有 Network Load Balancer (NLB) 和 Auto Scaling 群組 (ASG)。



在這個案例中，您會建立三個網路負載平衡器的資源集和整備程度檢查，以及三個 Auto Scaling 群組的資源集和整備程度檢查。現在，您可以依資源類型，針對復原群組的每一組資源進行整備檢查。

藉由為資源建立整備範圍，您可以新增儲存格或復原群組的整備檢查摘要。若要指定資源的整備範圍，請將儲存格或復原群組的 ARN 與資源集中的每個資源產生關聯。您可以在為資源集建立整備檢查時執行此動作。

例如，當您針對此復原群組的網路負載平衡器新增資源集的整備檢查時，您可以同時將整備範圍新增至每個 NLB。在這種情況下，您會將 AZ 1a 的 ARN 與 AZ 1a 中的 NLB、的 ARN 與 NLB 中的 ARN 相關聯AZ 1b，AZ 1b以及中的 NLB 的 ARN 相關聯。AZ 1c AZ 1c當您為 Auto Scaling 群組建立整備情況檢查時，您也可以執行相同的動作，在針對 Auto Scaling 群組資源集建立整備程度檢查時，將整備範圍指派給每個群組。

您可以選擇在建立整備檢查時關聯整備範圍，不過，我們強烈建議您進行設定。準備範圍可讓 Route 53 ARC 顯示復原群組摘要NOT READY準備程度檢查和儲存格層級摘要準備程度檢查的正確READY或整備狀態。除非您設置了準備範圍，否則 Route 53 ARC 無法提供這些摘要。

請注意，當您新增應用程式層級或全域資源 (例如 DNS 路由原則) 時，不會為整備範圍選擇復原群組或儲存格。相反，您可以選擇全局資源（無單元格）。

DNS 目標資源整備度檢查：稽核備援準備程度

透過 Route 53 ARC 中的 DNS 目標資源整備程度檢查，您可以稽核應用程式的架構和備援準備程度。這種類型的整備程度檢查會持續掃描應用程式的架構和 Amazon Route 53 路由政策，以稽核跨區域和跨區域的相依性。

復原導向的應用程式具有多個獨立複本，這些複本被隔離到可用區域或 AWS 區域中，因此複本可以彼此獨立失敗。如果您的應用程式需要調整為正確孤立，Route 53 ARC 會建議您視需要進行的變更，以更新架構，以協助確保其具備彈性並準備好容錯移轉。

Route 53 ARC 會自動偵測應用程式中儲存格的數量和範圍 (代表複本或容錯單元)，以及儲存格是由可用區域或區域隔離。然後，Route 53 ARC 會識別並向您提供有關儲存格中應用程式資源的資訊，以判斷這些資源是否正確地分隔至區域或區域。例如，如果您的儲存格範圍為特定區域，整備檢查可以監視負載平衡器及其後面的目標是否也孤立於這些區域。

使用此資訊，您可以判斷是否需要進行變更，以將儲存格中的資源與正確的區域或區域對齊。

若要開始使用，您可以為應用程式建立 DNS 目標資源，以及它們的資源集和整備程度檢查。如需詳細資訊，請參閱 在 Route 53 ARC 中獲取架構建議。

整備程度檢查和災難復原案例

Route 53 ARC 準備程度檢查可協助您確保應用程式擴充以處理容錯移轉流量，讓您深入瞭解應用程式和資源是否已準備好進行復原。準備檢查狀態不應當作表示生產複本狀況良好的信號。但是，您可以使用整備檢查作為應用程式和基礎結構監視或健康檢查程式系統的補充，以判斷是否要離開或移除複本。

在緊急情況或中斷時，請使用運作狀態檢查和其他資訊的組合來判斷您的待命是否已擴充、狀態良好，並準備好容錯移轉生產流量。例如，除了驗證待命的準備檢查狀態之外，請檢查針對待命單元執行的 Canaries 是否符合您的成功準備條件READY。

請注意，Route 53 ARC 準備程度檢查託管在單一 AWS 區域、美國西部 (奧勒岡州)，而且在中斷或災難期間，整備檢查資訊可能會過時，或者檢查可能無法使用。如需詳細資訊，請參閱 用於路由控制的資料和控制平面。

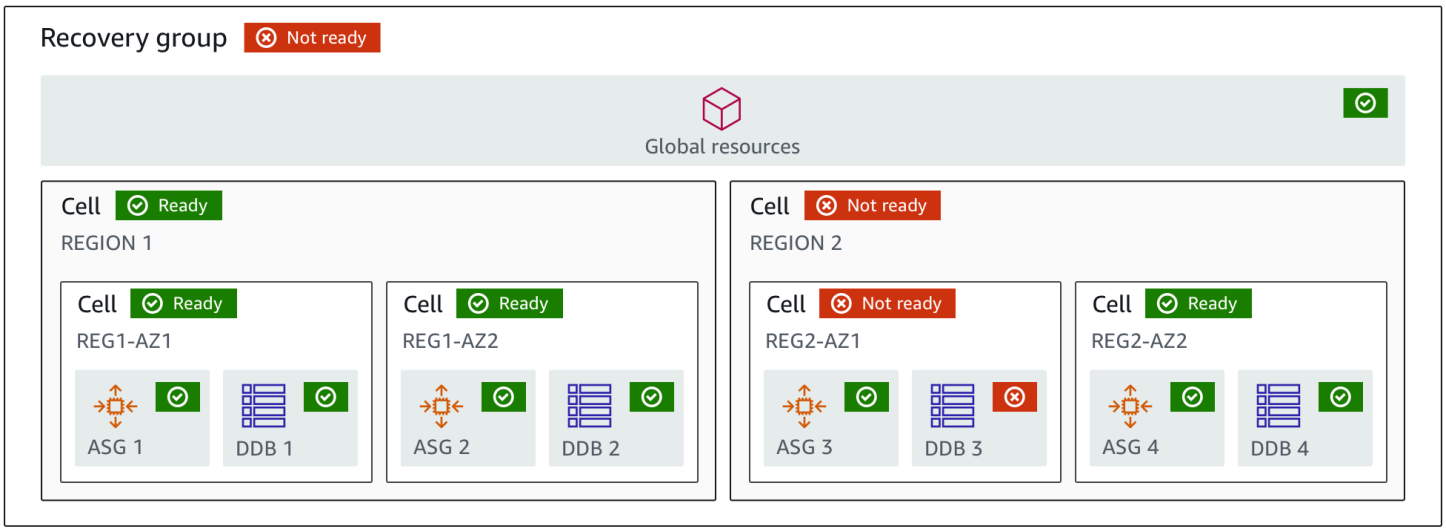
AWS 準備度檢查的區域可用性

如需 Amazon Route 53 應用程式復原控制器的區域支援和服務端點的詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器端點和 Amazon Web Services 一般參考中的配額。

> **Note**
>
> Amazon Route 53 應用程式復原控制器中的準備程度檢查是全球功能。不過，整備檢查資源位於美國西部 (奧勒岡) 區域，因此您必須在區域 Route 53 ARC AWS CLI 命令中指定美國西部 (奧勒岡`--region us-west-2`) 區域 (指定參數)，例如，當您建立資源集和整備檢查等資源時。

準備檢查元件

下圖說明設定為支援整備檢查功能的範例復原群組。此範例中的資源會分為復原群組中的儲存格 (依據 AWS 區域) 和巢狀儲存格 (依可用區域)。復原群組 (應用程式) 的整體就緒狀態，以及每個儲存格 (區域) 和巢狀儲存格 (可用區域) 的個別整備狀態。



以下是 Route 53 ARC 中準備檢查功能的組成部分。

細胞

儲存格會定義應用程式的複本或獨立的容錯移轉單位。它會將應用程式在複本中獨立執行所需的所有 AWS 資源分組。例如，主要儲存格中可能有一組資源，在待命儲存格中可能有另一組資源。您可以決定儲存格所包含內容的界限，但儲存格通常代表可用區域或區域。儲存格內可以有多個儲存格 (巢狀儲存格)，例如區域內的 AZ。每個巢狀儲存格代表一個隔離的容錯移轉單元。

復原群組

儲存格會收集到復原群組中。復原群組代表您要檢查容錯移轉準備就緒的應用程式或應用程式群組。它由兩個或多個單元組成，或複製品，在功能方面彼此匹配。例如，如果您有一個 Web 應用程式跨 us-east-1a 和 us-east-1b 複寫，其中 us-east-1b 是您的容錯移轉環境，您可以在 Route 53

ARC 中將此應用程式表示為具有兩個儲存格的復原群組：一個在 us-東 1a 和一個在 us-東 1b。復原群組也可以包含全域資源，例如 Route 53 健康狀態檢查。

資源和資源識別碼

在 Route 53 ARC 中建立用於整備檢查的元件時，您可以使用資源識別碼指定資源，例如 Amazon DynamoDB 表、Network Load Balancer 或 DNS 目標資源。資源識別碼可以是資源的 Amazon 資源名稱 (ARN)，或者 (對於 DNS 目標資源)，Route 53 ARC 在建立資源時產生的識別碼。

DNS 目標資源

DNS 目標資源是指應用程式的網域名稱和其他 DNS 資訊 (例如網域指向的 AWS 資源) 的組合。包含 AWS 資源是可選的，但如果您提供資源，它必須是 Route 53 資源記錄或 Network Load Balancer。當您提供 AWS 資源時，您可以取得更詳細的架構建議，協助您改善應用程式的復原彈性。您可以在 Route 53 ARC 中針對 DNS 目標資源建立資源集，然後針對資源集建立整備檢查，以便取得應用程式的架構建議。整備檢查也會根據 DNS 目標資源的整備規則，監控應用程式的 DNS 路由原則。

資源集

資源集是跨越多個儲存格的一組 AWS 資源，包括資源或 DNS 目標資源。例如，您可能在 us-east-1a 中有一個負載平衡器，而在 us-東 1b 中有另一個負載平衡器。若要監視負載平衡器的復原準備程度，您可以建立包含兩個負載平衡器的資源集，然後針對資源集建立整備程度檢查。Route 53 ARC 將不斷檢查集合中資源的準備情況。您也可以新增整備範圍，將資源集中的資源與您為應用程式建立的復原群組產生關聯。

準備規則

準備規則是 Route 53 ARC 對資源集中的一組資源執行的稽核。Route 53 ARC 針對其支援整備檢查的每種資源類型都有一組準備規則。每個規則都包含一個 ID 和說明，說明 Route 53 ARC 檢查資源的內容。

準備檢查

整備情況檢查會監控應用程式中的資源集 (例如一組 Amazon Aurora 執行個體)，Route 53 ARC 正在稽核復原準備情況。整備檢查可以包括稽核，例如容量組態、 AWS 配額或路由原則。例如，如果您想要稽核跨兩個可用區域之 Amazon EC2 Auto Scaling 群組的準備情況，您可以使用兩個資源 ARN (每個 Auto Scaling 群組各一個) 建立資源集的整備程度檢查。然後，為了確保每個群組都相等縮放，Route 53 ARC 會持續監控兩個群組中的執行個體類型和計數。

準備範圍

整備範圍可識別特定整備檢查所包含的資源分組。整備檢查的範圍可以是復原群組 (也就是整個應用程式的全域) 或儲存格 (也就是區域或可用區域)。對於做為 Route 53 ARC 全域資源的資源，請

將整備範圍設定為復原群組或全域資源層級。例如，Route 53 健康狀態檢查是 Route 53 ARC 中的全域資源，因為它不是特定於區域或可用區域。

準備程度檢查的資料和控制平面

當您規劃容錯移轉和災難復原時，請考慮容錯移轉機制的彈性。我們建議您確保在容錯移轉期間所依賴的機制具有高可用性，以便在災難情況下需要時可以使用它們。一般而言，您應該隨時為您的機制使用資料平面函數，以獲得最大的可靠性和容錯能力。考慮到這一點，重要的是要了解服務的功能如何在控制平面和數據平面之間劃分，以及何時可以依賴服務數據層面對極高可靠性的期望。

與大多數 AWS 服務一樣，控制平面和資料平面支援整備檢查功能的功能。雖然這兩者都是為了可靠而建置，但控制平面已針對資料一致性進行了最佳化，而資料平面則針對可用性進行最佳化。資料平面是專為復原而設計的，因此即使在中斷性事件期間，控制平面可能無法使用時，也能維持可用性。

一般而言，控制平面可讓您執行基本的管理功能，例如建立、更新和刪除服務中的資源。資料平面提供服務的核心功能。

對於整備檢查，有一個單一的 API，即恢復準備 API，用於控制面和數據平面。整備程度檢查和整備資源僅適用於美國西部 (奧勒岡) 區域 (us-west-2)。整備檢查控制平面和資料平面是可靠的，但不是高可用性。

如需有關資料平面、控制平面以及如何 AWS 建置服務以符合高可用性目標的詳細資訊，請參閱 Amazon Builders' Library 中的使用可用區域的靜態穩定性 paper。

在 Amazon Route 53 應用程序恢復控制器中標記整備檢

標記是您用來識別和組織資源的單字或片語 (中繼 AWS 資料)。可以新增多個標籤到每個資源，且每個標籤皆包含您所定義的金鑰和值。例如，關鍵字可能是環境，而值可能是生產環境。可以根據新增的標籤來搜尋與篩選資源。

您可以在 Route 53 ARC 中的準備檢查中標記下列資源：

- 資源集
- 準備檢查

路由 53 ARC 中的標記只能透過 API 使用，例如，使用 AWS CLI.

以下是使用在整備檢查中標記的範例 AWS CLI。

```
aws route53-recovery-readiness --region us-west-2 create-resource-
set --resource-set-name dynamodb_resource_set --resource-set-type
AWS::DynamoDB::Table --resources ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/PDXCell,ResourceArn=arn:aws:dynamodb:us-
west-2:111122223333:table/PDX_Table ReadinessScopes=arn:aws:aws-recovery-
readiness::111122223333:cell/IADCell,ResourceArn=arn:aws:dynamodb:us-
east-1:111122223333:table/IAD_Table --tags Stage=Prod

aws route53-recovery-readiness --region us-west-2 create-readiness-
check --readiness-check-name dynamodb_readiness_check --resource-set-name
dynamodb_resource_set --tags Stage=Prod
```

如需詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的復原準備程度 API 參考指南TagResource中的。

在 Route 53 ARC 中進行準備檢查的定價

使用 Amazon Route 53 應用程式復原控制器，您只需為設定在服務中使用的項目付費。對於整備檢查，您需要支付每個配置的整備檢查小時費用。

如需 Route 53 ARC 的詳細定價資訊和定價範例，請參閱 Amazon Route 53 應用程式復原控制器定價，然後向下捲動至 Amazon Route 53 應用程式復原控制器。

為您的應用程式設定彈性復原程序

若要將 Amazon Route 53 應用程式復原控制器與位於多個 AWS 區域的 AWS 應用程式搭配使用，請遵循以下指導方針來設定應用程式的彈性，以便有效地支援復原整備程度。然後，您可以為應用程式建立整備程度檢查，並設定路由控制，以重新路由傳送流量以進行容錯移轉。您還可以查看 Route 53 ARC 提供的有關可提高恢復能力的應用程序架構的建議。

> **Note**
>
> 如果您的應用程式被可用區域隔離，請考慮使用區域移位或區域自動換檔來進行容錯移轉復原。無需設定即可使用區域移位或區域自動換檔，從可用區域損壞中可靠地復原應用程式。若要將流量從可用區域移開負載平衡器資源，請在 Route 53 ARC 主控台或 Elastic Load Balancing 主控台中啟動區域轉移。或者，您可以將 AWS Command Line Interface 或 AWS SDK 與區域移位 API 動作搭配使用。如需詳細資訊，請參閱 Amazon Route 53 應用程序恢復控制器的區域轉移。

若要深入了解如何開始使用彈性容錯移轉組態，請參閱開始使用 Amazon Route 53 應用程式復原控制器中的多區域復原。

在 Route 53 ARC 中進行準備檢查的最佳實踐

對於 Amazon Route 53 應用程式復原控制器中的準備程度檢查，我們建議採用下列最佳

新增就緒狀態變更的通知

在 Amazon 中設定規則， EventBridge 以便在整備狀態變更時傳送通知，例如從READY到NOT READY。當您收到通知時，您可以調查並解決問題，以確保您的應用程式和資源在預期時已準備好進行容錯移轉。

您可以設定 EventBridge 規則來傳送數個整備檢查狀態變更的通知，包括復原群組 (針對您的應用程式)、儲存格 (例如 AWS 區域) 或資源集的整備狀態檢查。

如需詳細資訊，請參閱 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge。

準備程度檢查 API 作業

下表列出可用於復原準備程度 (整備檢查) 的 Route 53 ARC 作業，並附有相關文件的連結。

如需如何搭配使用常見復原整備 API 作業的範例 AWS Command Line Interface，請參閱 使用 Route 53 ARC 準備就緒檢查 API 作業的範例 AWS CLI。

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
建立儲存格	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱 CreateCell
獲取一個單元格	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱 GetCell
刪除儲存格	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱 DeleteCell
更新儲存格	N/A	請參閱UpdateCell
列出帳戶的儲存格	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱 ListCells

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
建立復原群組	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱CreateRecovery群組
取得復原群組	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱GetRecovery群組
更新復原群組	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱UpdateRecovery群組
刪除復原群組	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱DeleteRecovery群組
列出復原群組	請參閱 在 Route 53 ARC 中建立、更新和刪除復原群組	請參閱ListRecovery群組
建立資源集	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱CreateResource設定
取得資源集	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱GetResource設定
更新資源集	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱UpdateResource設定
刪除資源集	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱DeleteResource設定
列出資源集	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱ListResource集
建立整備檢查	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱CreateReadiness檢查
取得準備程度檢查	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱GetReadiness檢查
更新整備檢查	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱UpdateReadiness檢查

動作	使用路 Route 53 ARC 控制台	使用 Route 53 的應用程式介面
刪除整備檢查	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱DeleteReadiness檢查
列出準備檢查	請參閱在 Route 53 ARC 中創建和更新準備檢查	請參閱ListReadiness支票
列出整備規則	請參閱Route 53 中的準備規則描述	請參閱 ListRules
檢查整個準備檢查的狀態	請參閱監測 Route 53 弧的準備狀態	請參閱 GetReadinessCheckStatus
檢查資源的狀態	請參閱監測 Route 53 弧的準備狀態	請參閱GetReadinessCheckResource狀態
檢查儲存格的狀態	請參閱監測 Route 53 弧的準備狀態	請參閱 GetCellReadinessSummary
檢查復原群組的狀態	請參閱監測 Route 53 弧的準備狀態	查看GetRecoveryGroupReadiness摘要

使用 Route 53 ARC 準備就緒檢查 API 作業的範例 AWS CLI

本節 AWS Command Line Interface 將逐步介紹簡單的應用程式範例，並使用 API 操作在 Amazon Route 53 應用程式復原控制器中使用整備檢查功能。這些範例旨在協助您深入瞭解如何使用 CLI 使用整備檢查功能。

Route 53 ARC 稽核中的準備就緒檢查是否有應用程式複本中的資源不相符。若要為您的應用程式設定整備檢查，您必須在 Route 53 ARC 儲存格中設定應用程式資源或模型，以符合您為應用程式建立的複本。然後，您可以設定稽核這些複本的準備程度檢查，以協助您確保待命應用程式複本及其資源與您的生產複本一致，持續不斷

讓我們來看一個簡單的案例，其中您有一個名為的應用程序，Simple-Service該應用程序當前在美國東部（維吉尼亞北部）區域（us-east-1）運行。您也可以在美國西部 (奧勒岡) 區域 (US-西部 -2) 擁有應用程式的待命副本。在此範例中，我們將設定整備檢查，以比較這兩個版本的應用程式。這可讓我們確保待命區域 (美國西部 (奧勒岡) 區域已準備好接收流量 (如果需要在容錯移轉案例中)。

若要取得有關使用的更多資訊 AWS CLI，請參閱《AWS CLI 指令參考》。如需整備 API 動作的清單和詳細資訊的連結，請參閱 準備程度檢查 API 作業。

Route 53 ARC 中的儲存格代表故障界限 (例如可用區域或區域)，並會收集到復原群組中。復原群組代表您要檢查容錯移轉準備就緒的應用程式。如需整備檢查元件的詳細資訊，請參閱準備檢查元件 。

> **Note**
>
> Route 53 ARC 是支援多個端點的全域服務， AWS 區域 但您必須在大多數 Route 53 ARC CLI 命令中指定美國西部 (奧勒岡`--region us-west-2`) 區域 (也就是指定參數)。例如，建立復原群組或整備檢查等資源。

對於我們的應用程序示例，我們將首先為每個擁有資源的區域創建一個單元格。然後我們會建立復原群組，然後完成設定以進行整備檢查。

1. 建立儲存格

1. 建立一個 us-east-1 儲存格。

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name east-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
    "CellName": "east-cell",
    "Cells": [],
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1b。建立一個 us-west-1 儲存格。

```
aws route53-recovery-readiness --region us-west-2 create-cell \
    --cell-name west-cell
```

```
{
    "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell",
    "CellName": "west-cell",
    "Cells": [],
```

```
    "ParentReadinessScopes": [],
    "Tags": {}
}
```

1C。現在我們有兩個儲存格。您可以通過調用 `list-cells` API 來驗證它們是否存在。

```
aws route53-recovery-readiness --region us-west-2 list-cells
```

```
{
    "Cells": [
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell",
            "CellName": "east-cell",
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        },
        {
            "CellArn": "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell",
            "CellName": "west-cell"
            "Cells": [],
            "ParentReadinessScopes": [],
            "Tags": {}
        }
    ]
}
```

2. 建立復原群組

復原群組是 Route 53 ARC 中復原準備程度的最上層資源。復原群組代表整個應用程式。在此步驟中，我們將建立復原群組以建立整體應用程式的模型，然後新增我們建立的兩個儲存格。

2a. 建立復原群組。

```
aws route53-recovery-readiness --region us-west-2 create-recovery-group \
    --recovery-group-name simple-service-recovery-group \
       --cells "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"\
       "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
```

```
{
```

```
    "Cells": [],
    "RecoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/simple-service-recovery-group",
    "RecoveryGroupName": "simple-service-recovery-group",
    "Tags": {}
}
```

2b. (選擇性) 您可以透過呼叫 `list-recovery-groups` API 確認復原群組是否已正確建立。

```
aws route53-recovery-readiness --region us-west-2 list-recovery-groups
```

```
{
    "RecoveryGroups": [
        {
            "Cells": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell",
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "RecoveryGroupArn": "arn:aws:route53-recovery-
readiness::111122223333:recovery-group/simple-service-recovery-group",
            "RecoveryGroupName": "simple-service-recovery-group",
            "Tags": {}
        }
    ]
}
```

現在我們有了應用程序的模型，讓我們添加要監視的資源。在 Route 53 ARC 中，您要監視的一組資源稱為資源集。資源集包含全部相同類型的資源。我們會將資源集中的資源彼此進行比較，以協助判斷單元是否準備好進行容錯移轉。

3. 建立資源集

假設我們的應用Simple-Service程式確實非常簡單，而且只使用 DynamoDB 表。它在 us-east-1 中有一個 DynamoDB 表，在 us-west-2 中有另一個表。資源集也包含整備範圍，可識別每個資源所包含的儲存格。

三 建立反映Simple-Service應用程式資源的資源集。

```
aws route53-recovery-readiness --region us-west-2 create-resource-set \
    --resource-set-name ImportantInformationTables \
    --resource-set-type AWS::DynamoDB::Table \
    --resources
```

```
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
west-cell"
    ResourceArn="arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1",ReadinessScopes="arn:aws:route53-recovery-readiness::111122223333:cell/
east-cell"
```

```
{
    "ResourceSetArn": "arn:aws:route53-recovery-readiness::111122223333:resource-set/
sample-resource-set",
    "ResourceSetName": "ImportantInformationTables",
    "Resources": [
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/west-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "ReadinessScopes": [
                "arn:aws:route53-recovery-readiness::111122223333:cell/east-cell"
            ],
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
        }
    ],
    "Tags": {}
}
```

3B. (選擇性) 您可以呼叫 `list-resource-sets` API 來驗證資源集中包含的內容。這會列出 AWS 帳號的所有資源集。在這裡，你可以看到，我們只是我們上面創建的一個資源集。

```
aws route53-recovery-readiness --region us-west-2 list-resource-sets
```

```
{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
```

```
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/east-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
            ],
            "Tags": {}
        }
    ]
}{
    "ResourceSets": [
        {
            "ResourceSetArn": "arn:aws:route53-recovery-
readiness::111122223333:resource-set/ImportantInformationTables",
            "ResourceSetName": "ImportantInformationTables",
            "Resources": [
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-readiness::111122223333:cell/west-
cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
                },
                {
                    "ReadinessScopes": [
                        "arn:aws:route53-recovery-
readiness::&ExampleAWSAccountNo1;:cell/east-cell"
                    ],
                    "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast1"
                }
```

```
            ],
            "Tags": {}
        }
    ]
}
```

現在，我們已經創建了單元格，恢復組和資源集，以在 Route 53 ARC 中為Simple-Service應用程序建模。接下來，我們將設定整備程度檢查，以監控資源是否準備容錯移轉。

4. 建立整備檢查

整備檢查會將一組規則套用至附加至檢查的資源集中的每個資源。每種資源類型都有特定的規則。也就是說，有不同的規則 `AWS::DynamoDB::TableAWS::EC2::Instance`，等等。規則會檢查資源的各種維度，包括組態、容量 (在可用且適用的情況下)、限制 (在適用的情況下) 及製程組態。

> **Note**
>
> 若要在整備檢查中查看套用至資源的規則，您可以使用 `get-readiness-check-resource-status` API，如步驟 5 所述。若要查看 Route 53 ARC 中所有準備規則的清單，請使用`list-rules`或參閱Route 53 中的準備規則描述。Route 53 ARC 具有針對每種資源類型執行的特定規則集；目前無法自訂這些規則。

4a. 建立資源集的整備程度檢查ImportantInformationTables。

```
aws route53-recovery-readiness --region us-west-2 create-readiness-check \
    --readiness-check-name ImportantInformationTableCheck --resource-set-name
 ImportantInformationTables
```

```
{
    "ReadinessCheckArn": "arn:aws:route53-recovery-readiness::111122223333:readiness-
check/ImportantInformationTableCheck",
    "ReadinessCheckName": "ImportantInformationTableCheck",
    "ResourceSet": "ImportantInformationTables",
    "Tags": {}
}
```

4b. (選擇性) 若要確認已成功建立整備檢查，請執行 `list-readiness-checks` API。此 API 顯示帳戶中的所有整備檢查。

```
aws route53-recovery-readiness --region us-west-2 list-readiness-checks
```

```
{
    "ReadinessChecks": [
        {
            "ReadinessCheckArn": "arn:aws:route53-recovery-
readiness::111122223333:readiness-check/ImportantInformationTableCheck",
            "ReadinessCheckName": "ImportantInformationTableCheck",
            "ResourceSet": "ImportantInformationTables",
            "Tags": {}
        }
    ]
}
```

5. 監控整備檢查

現在，我們已經建立應用程式的模型並新增整備檢查，我們已準備好監控資源。您可以在四個層級建立應用程式整備程度的模型：整備程度檢查層次 (一組資源)、個別資源層次、儲存格層次 (可用區域或區域中的所有資源)，以及復原群組層次 (整體應用程式)。下面提供了用於獲取每種類型的準備狀態的命令。

5a. 查看整備檢查的狀態。

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status\
    --readiness-check-name ImportantInformationTableCheck
```

```
{
    "Readiness": "READY",
    "Resources": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:53:39Z",
            "Readiness": "READY",
            "ResourceArn": "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsEast2"
    ]
```

```
}
```

5b. 在整備檢查中查看單一資源的詳細整備狀態，包括每個已檢查規則的狀態。

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-resource-status \
    --readiness-check-name ImportantInformationTableCheck \
    --resource-identifier "arn:aws:dynamodb:us-west-2:111122223333:table/
TableInUsWest2"
```

```
{"Readiness": "READY",
    "Rules": [
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoTableStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsPeakRcuWcu"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsConfig"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
```

```
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsStatus"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoGSIsCapacity"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoReplicationLatency"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoAutoScalingConfiguration"
        },
        {
            "LastCheckedTimestamp": "2021-01-07T00:55:41Z",
            "Messages": [],
            "Readiness": "READY",
            "RuleId": "DynamoLimits"
        }
    ]
}
```

5c. 查看細胞的整體準備情況。

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary \
    --cell-name west-cell
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
```

```
    ]
}
```

5d. 最後，請參閱復原群組層級應用程式的最上層準備程度。

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary
 \
    --recovery-group-name simple-service-recovery-group
```

```
{
    "Readiness": "READY",
    "ReadinessChecks": [
        {
            "Readiness": "READY",
            "ReadinessCheckName": "ImportantTableCheck"
        }
    ]
}
```

使用復原群組和整備程度檢查

本節說明並提供復原群組和整備檢查的程序，包括建立、更新和刪除這些資源。

在 Route 53 ARC 中建立、更新和刪除復原群組

復原群組代表您在 Amazon Route 53 應用程式復原控制器中的應用程式。它通常由兩個或多個單元組成，這些單元在資源和功能方面是彼此的複本，因此您可以從一個單元容錯移轉到另一個單元。每個儲存格都包含一個區域或可用 AWS 區域的作用中資源的 Amazon 資源名稱 (ARN)。資源可能是 Elastic Load Balancing 負載平衡器、Auto Scaling 群組或其他資源。代表另一個區域或區域的對應儲存格具有與使用中儲存格中相同類型的待命資源 — 負載平衡器、Auto Scaling 群組等。

儲存格代表應用程式的複本。Route 53 ARC 中的準備檢查可協助您判斷應用程式是否已準備好從一個複本容錯移轉到另一個複本。不過，您應該根據您的監控和健康狀態檢查系統，決定是否要離開或失敗複本，並將整備檢查視為這些系統的補充服務。

整備程度會檢查稽核資源，以根據該類型資源的一組預先定義規則來確定其準備程度。使用複本建立復原群組之後，您可以針對應用程式中的資源新增 Route 53 ARC 準備檢查，因此 Route 53 ARC 可協助確保複本在一段時間內具有相同的安裝和組態。

主題

- 建立復原群組
- 更新和刪除復原群組和儲存格

建立復原群組

本節中的步驟說明如何在 Route 53 ARC 主控台上建立復原群組。若要了解如何搭配 Amazon Route 53 應用程式復原控制器使用復原準備程式 API 操作，請參閱 準備程度檢查 API 作業

若要建立復原群組

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [復原整備] 頁面上，選擇 [建立]，然後選擇 [復原] 群組。
4. 輸入復原群組的名稱，然後選擇 [下一步]。
5. 選擇建立儲存格，然後選擇 [新增儲存格]。
6. 輸入儲存格的名稱。例如，如果您在美國西部 (加利佛尼亞北部) 有應用程式複本，您可以新增名為的儲存格`MyApp-us-west-1`。
7. 選擇「新增儲存格」，然後為第二個儲存格新增名稱。例如，如果您在美國東部 (俄亥俄州) 有複本，您可以新增名為的儲存格 `MyApp-us-east-2`。
8. 如果您要新增巢狀儲存格 (區域內可用區域中的複本)，請選擇「動作」，選擇「新增巢狀儲存格」，然後輸入名稱。
9. 新增應用程式複本的所有儲存格和巢狀儲存格後，請選擇下一步。
10. 檢閱您的復原群組，然後選擇 [建立復原群組]。

更新和刪除復原群組和儲存格

本節中的步驟說明如何更新和刪除復原群組，以及如何刪除 Route 53 ARC 主控台上的儲存格。若要了解如何搭配 Amazon Route 53 應用程式復原控制器使用復原準備程式 API 操作，請參閱 準備程度檢查 API 作業

更新或刪除復原群組，或刪除儲存格

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。

3. 在 [復原整備] 頁面上，選擇復原群組。
4. 若要使用復原群組，請選擇 [動作]，然後選擇 [編輯復原群組] 或 [刪除復原群組]。
5. 編輯復原群組時，您可以新增或移除儲存格或巢狀儲存格。

   - 若要新增儲存格，請選擇「新增儲存格」。
   - 若要移除儲存格，請在儲存格旁的「動作」標籤下，選擇「刪除儲存格」。

在 Route 53 ARC 中創建和更新準備檢查

本節提供整備檢查和資源集的程序，包括建立、更新及刪除這些資源。

建立和更新整備檢查

本節中的步驟說明如何在 Route 53 ARC 主控台上建立整備檢查。若要了解如何搭配 Amazon Route 53 應用程式復原控制器使用復原準備程式 API 操作，請參閱 準備程度檢查 API 作業

若要更新整備檢查，您可以編輯整備檢查的資源集、新增或移除資源，或變更資源的整備範圍。

若要建立整備檢查

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [整備] 頁面上，選擇 [建立]，然後選擇 [整備] 檢查。
4. 輸入整備檢查的名稱，選擇要檢查的資源類型，然後選擇 [下一步]。
5. 新增資源集以進行整備檢查。資源集是不同複本中相同類型的資源群組。選擇下列其中一項：

   - 使用您已建立的資源集中的資源建立整備程度檢查。
   - 建立新的資源集。

   如果您選擇建立新的資源集，請輸入該資源集的名稱，然後選擇「新增」。
6. 針對要包含在集合中的每個資源逐個複製並貼上 Amazon 資源名稱 (ARN)，然後選擇 [下一步]。

> **Tip**
>
> 如需 Route 53 ARC 對每種資源類型所預期之 ARN 格式的範例和更多資訊，請參閱Route 53 ARC 中的資源類型和 ARN 格式。

7. 如果您願意，請檢視 Route 53 ARC 檢查您包含在此整備檢查中的資源類型時將使用的整備規則。然後選擇下一步。
8. (選擇性) 在 [復原群組名稱] 底下，選擇要與整備檢查產生關聯的復原群組，然後針對每個資源 ARN，從資源所在的下拉式功能表中選擇儲存格 (區域或可用區域)。如果它是應用程式層級資源 (例如 DNS 路由原則)，請選擇全域資源 (無儲存格)。

   這會指定整備程度檢查中資源的整備範圍。

   > **Important**
   >
   > 雖然此步驟是選用的，但必須新增整備範圍，才能取得復原群組和儲存格的摘要整備資訊。如果您略過此步驟，但未在此處選擇整備範圍，將整備檢查與復原群組的資源產生關聯，Route 53 ARC 無法傳回復群組或儲存格的摘要整備資訊。

9. 選擇下一步。
10. 檢閱確認頁面上的資訊，然後選擇 [建立整備檢查]。

若要刪除整備檢查

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 選擇整備檢查，然後在 [動作] 底下選擇 [刪除]。

建立和編輯資源集

一般而言，您會建立資源集做為建立整備檢查的一部分，但也可以個別建立資源集。您也可以編輯資源集以新增或移除資源。本節中的步驟說明如何在 Route 53 ARC 主控台上建立或編輯資源集。若要了解如何搭配 Amazon Route 53 應用程式復原控制器使用復原準備程式 API 操作，請參閱 準備程度檢查 API 作業

若要建立資源集

1. 在以下位置打開路線 53 控制台。 https://console.aws.amazon.com/route53/home
2. 在應用程式復原控制器下，選擇資源集。
3. 選擇建立。
4. 輸入資源集的名稱，然後選擇要包含在資源集中的資源類型。

5. 選擇 [新增]，然後輸入要新增至資源集的 Amazon 資源名稱 (ARN)。
6. 完成新增資源之後，請選擇 [建立資源集]。

若要編輯資源集

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [資源集] 底下，選擇 [動作]，然後選擇 [編輯]。
4. 執行以下任意一項：
   - 若要從資源集中移除資源，請選擇 [移除]。
   - 若要將資源新增至資源集，請選擇 [新增]，然後輸入資源的 Amazon 資源名稱 (ARN)。
5. 您也可以編輯資源的整備範圍，將資源與整備檢查的不同儲存格產生關聯。
6. 選擇儲存。

監測 Route 53 弧的準備狀態

您可以在 Amazon Route 53 應用程式復原控制器中查看應用程式的準備情況如下：

- 資源集中資源的整備程度檢查層級
- 個別資源層次
- 可用區 AWS 域或區域中所有資源的儲存格 (應用程式複本) 層次
- 整個應用程式的復原群組層次

您可以收到有關準備狀態變更的通知，或者您可以在 Route 53 主控台或使用 Route 53 ARC CLI 命令監視整備狀態變更。

準備狀態通知

您可以使用 Amazon 設 EventBridge 定事件驅動的規則來監控 Route 53 ARC 資源，並通知您整備狀態的變更。如需詳細資訊，請參閱 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge。

在 Route 53 ARC 主控台中監控準備狀態

下列程序說明如何監視中的復原準備程度 AWS Management Console。

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [整備] 頁面的 [復原群組] 底下，檢視每個復原群組 (應用程式) 的復原群組整備狀態。

   您也可以檢視特定儲存格或個別資源的準備情況。

使用 CLI 命令監控整備狀態

本節提供 AWS CLI 指令範例，可用來查看應用程式的整備狀態和不同層級的資源。

為資源集做好準備

您為資源集 (一組資源) 建立的整備檢查狀態。

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName
```

為單一資源做好準備

若要在整備檢查中取得單一資源的狀態，包括已檢查的每個整備規則的狀態，請指定整備檢查名稱和資源 ARN。例如：

```
aws route53-recovery-readiness --region us-west-2 get-readiness-check-status --readiness-check-name ReadinessCheckName --resource-arn "arn:aws:dynamodb:us-west-2:111122223333:table/TableName"
```

為細胞做好準備

單一儲存格的狀態，也就是「區域」或「可用區域」。

```
aws route53-recovery-readiness --region us-west-2 get-cell-readiness-summary --cell-name CellName
```

應用程式的準備

整體應用程式在復原群組層級的狀態。

```
aws route53-recovery-readiness --region us-west-2 get-recovery-group-readiness-summary --recovery-group-name RecoveryGroupName
```

在 Route 53 ARC 中獲取架構建議

如果您有現有的應用程式，Amazon Route 53 應用程式復原控制器可以評估應用程式的架構和路由政策，以提供修改設計的建議，以改善應用程式的復原彈性。在 Route 53 ARC 中建立代表應用程式的復原群組之後，請依照本節中的步驟取得應用程式架構的建議。

建議您為復原群組的 DNS 目標資源指定目標資源 (如果尚未指定)，以便提供更詳細的建議。當您提供其他信息時，Route 53 ARC 可以為您提供更好的建議。例如，如果您輸入 Amazon Route 53 資源記錄或 Network Load Balancer 做為目標資源，Route 53 ARC 可提供有關您是否已為復原群組建立最佳儲存格數目的相關資訊。

請注意下列 DNS 目標資源的事項：

- 僅為目標資源指定 Route 53 資源記錄或 Network Load Balancer。
- 只為每個復原群組建立一個 DNS 目標資源。
- 建議：為每個儲存格建立一個 DNS 目標資源。
- 使用整備檢查將 DNS 目標資源分組到一個資源集中。

下列程序說明如何建立 DNS 目標資源，並取得應用程式的架構建議。

取得更新架構的建議

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [復原群組名稱] 底下，選擇代表您應用程式的復原群組。
4. 在 [復原群組詳細資料] 頁面的 [動作] 功能表上，選擇 [取得此復原群組的架構建議]。
5. 如果您尚未建立 DNS 目標資源整備程度檢查，請建立一個，讓 Route 53 ARC 可以提供架構建議。選擇建立 DNS 目標資源。

   如需 DNS 目標資源的詳細資訊，請參閱準備檢查元件 。
6. 若要建立 DNS 目標資源的資源集，請建立整備檢查。輸入整備檢查的名稱，然後針對整備檢查的類型選擇 DNS 目標資源。
7. 輸入資源集的名稱。
8. 輸入應用程式的屬性，包括 DNS 名稱、託管區域 ARN 和記錄集識別碼。

> **Tip**
>
> 若要查看託管區域 ARN 的格式，請參閱中的託管區域的 ARN 格式。Route 53 ARC 中的資源類型和 ARN 格式

選擇性地，但強烈建議您選擇 [新增選用屬性]，並提供 Network Load Balancer ARN 或網域的 Route 53 資源記錄。

9. (選擇性) 在復原群組組態中，選擇 DNS 目標資源的儲存格，以設定整備範圍。
10. 選擇「建立資源集」。
11. 在 [復原群組詳細資料] 頁面上選擇 [取得架構建議]。Route 53 ARC 會在頁面上顯示一組建議。

檢閱建議清單。然後，您可以決定是否以及如何進行更改以提高應用程序的恢復彈性。

在 Route 53 ARC 中創建跨帳戶授權

您可能會將資源分散到多個 AWS 帳戶中，這可能會讓您全面了解應用程式的健康狀況變得具有挑戰性。這也可能使得很難獲得快速決策所需的信息。為了協助簡化 Amazon Route 53 應用程式復原控制器中的準備就緒檢查，您可以使用跨帳戶授權。

Route 53 ARC 中的跨帳戶授權可與準備檢查功能搭配使用。透過跨帳戶授權，您可以使用一個中央 AWS 帳戶來監控位於多個 AWS 帳戶的資源。在每個具有您要監視之資源的帳戶中，您都會授權中央帳戶存取這些資源。然後，中央帳戶可以針對所有帳戶中的資源建立整備檢查，並從中央帳戶，您可以監視容錯移轉的準備情況。

> **Note**
>
> 主控台無法使用跨帳戶授權設定。而是使用 Route 53 ARC API 操作來設置和使用跨帳戶授權。為了協助您開始使用，本節提供 AWS CLI 指令範例。

假設應用程式在美國西部 (奧勒岡) 區域 (us-west-2) 具有資源的帳戶，而且在美國東部 (維吉尼亞北部) 區域 (us-east-1) 中也有一個帳戶具有您想要監視的資源。Route 53 ARC 可以允許您通過使用跨帳戶授權來監視來自一個帳戶的兩組資源，us-west-2。

例如，假設您有以下 AWS 帳戶：

- 美國西部帳戶：
- 美國東部帳戶：

在 us-east-1 帳戶 (111111111111) 中，我們可以啟用跨帳戶授權，以允許 us-west-2 帳戶 (999999999999) 帳戶中的 (根) 使用者指定 Amazon 資源名稱 (ARN)，方法是在 us-west-2 IAM 帳戶中指定 (根) 使用者的 Amazon 資源名稱 (ARN)。`arn:aws:iam::999999999999:root`建立授權之後，us-west-2 帳戶可以將 us-east-1 擁有的資源新增至資源集，並建立整備檢查，以便在資源集上執行。

下列範例說明設定一個帳戶的跨帳戶授權。您必須在每個具有要在 Route 53 ARC 中新增和監視的 AWS 資源的其他帳戶中啟用跨帳戶授權。

> **Note**
>
> Route 53 ARC 是一項全域服務，支援多個區 AWS 域中的端點，但您必須在大多數 Route 53 ARC CLI 命令中指定美國西部 (奧勒岡`--region us-west-2`) 區域 (也就是指定參數)。

下列 AWS CLI 指令顯示如何針對此範例設定跨帳戶授權：

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    create-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

若要停用此授權，請執行下列動作：

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
    delete-cross-account-authorization --cross-account-authorization
 arn:aws:iam::999999999999:root
```

若要為您提供跨帳戶授權的所有帳戶簽入特定帳戶，請使用指`list-cross-account-authorizations`令。請注意，此時您無法檢查其他方向。也就是說，您無法搭配帳戶設定檔使用的 API 作業，以列出已獲得跨帳戶授權以新增和監控資源的所有帳戶。

```
aws route53-recovery-readiness --region us-west-2 --profile profile-in-us-east-1-
account \
```

```
    list-cross-account-authorizations
```

```
{
    "CrossAccountAuthorizations": [
        "arn:aws:iam::999999999999:root"
    ]
}
```

整備規則、資源類型和 ARNS

本節包括整備規則說明、支援的資源類型以及用於資源集之 Amazon 資源名稱 (ARN) 格式的參考資訊。

Route 53 中的準備規則描述

本節列出 Amazon Route 53 應用程式復原控制器支援的所有資源類型的整備程序規則說明。若要查看 Route 53 ARC 支援的資源類型清單，請參閱Route 53 ARC 中的資源類型和 ARN 格式。

您也可以透過執行下列動作，在 Route 53 ARC 主控台上檢視整備規則說明，或使用 API 作業：

- 若要在主控台中檢視整備規則，請遵循下列程序中的步驟：在主控台上檢視整備規則
- 若要使用 API 檢視整備規則，請參閱ListRules作業。

主題

- Route 53 中的準備規則
- 在主控台上檢視整備規則

Route 53 中的準備規則

本節列出 Route 53 ARC 支援之每個資源類型的整備規則集。

當您查看規則描述時，您可以看到其中大多數都包含「檢查全部」或「檢查每個」字詞。若要瞭解這些術語如何解釋規則在整備檢查環境中的運作方式，以及 Route 53 ARC 如何設定準備狀態的其他詳細資料，請參閱準備規則如何判斷準備狀態。

準備規則

Route 53 ARC 通過使用以下準備規則審核資源。

Amazon API Gateway 版本 1 階段

- ApiGwV1ApiKeyCount：檢查所有 API Gateway 階段，以確保它們具有相同數量的 API 密鑰鏈接到它們。
- ApiGwV1ApiKeySource：檢查所有 API Gateway 階段，以確保它們具有相同的`API Key Source`值。
- ApiGwV1BasePath：檢查所有 API Gateway 階段，以確保它們連結至相同的基本路徑。
- ApiGwV1BinaryMediaTypes：檢查所有 API Gateway 階段，以確保它們支援相同的二進位媒體類型。
- ApiGwV1CacheClusterEnabled：檢查所有 API Gateway 階段，以確保所有階段都已`Cache Cluster`啟用，或者沒有啟用。
- ApiGwV1CacheClusterSize：檢查所有 API Gateway 階段，以確保它們具有相同`Cache Cluster Size`的。如果其中一個值較大，則其他人將標記為「未就緒」。
- ApiGwV1CacheClusterStatus：檢查所有 API Gateway 階段，以確保處`Cache Cluster`於「可用」狀態。
- ApiGwV1DisableExecuteApiEndpoint：檢查所有 API Gateway 階段，以確保所有階段都已`Execute API Endpoint`禁用，或者沒有禁用。
- ApiGwV1DomainName：檢查所有 API Gateway 階段，以確保它們鏈接到相同的域名。
- ApiGwV1EndpointConfiguration：檢查所有 API Gateway 階段，以確保它們連結到具有相同端點組態的網域。
- ApiGwV1EndpointDomainNameStatus：檢查所有 API Gateway 階段，以確保它們所連結的網域名稱處於「可用」狀態。
- ApiGwV1MethodSettings：檢查所有 API Gateway 階段，以確保它們具有相同的`Method Settings`值。
- ApiGwV1MutualTlsAuthentication：檢查所有 API Gateway 階段，以確保它們具有相同的`Mutual TLS Authentication`值。
- ApiGwV1Policy：檢查所有 API Gateway 階段，以確保所有使用 API 層級政策，或者沒有使用。
- ApiGwV1RegionalDomainName：檢查所有 API Gateway 階段，以確保它們連結到相同的區域網域名稱。附註：此規則不會影響整備狀態。
- ApiGwV1ResourceMethodConfigs：檢查所有 API Gateway 階段，以確保它們具有類似的資源階層，包括相關組態。
- ApiGwV1SecurityPolicy：檢查所有 API Gateway 階段，以確保它們具有相同的`Security Policy`值。

- ApiGwV1Quotas：檢查所有 API Gateway 群組，以確保它們符合「Service Quotas」管理的配額 (限制)。
- ApiGwV1UsagePlans：檢查所有 API Gateway 階段，以確保它們以相同`Usage Plans`的組態連結到。

Amazon API Gateway 版本 2 階段

- ApiGwV2ApiKeySelectionExpression：檢查所有 API Gateway 階段，確保它們具有相同的`API Key Selection Expression`值。
- ApiGwV2ApiMappingSelectionExpression：檢查所有 API Gateway 階段，以確保它們具有相同的`API Mapping Selection Expression`值。
- ApiGwV2CorsConfiguration：檢查所有 API Gateway 階段，以確保它們具有相同的 CORS 相關組態。
- ApiGwV2DomainName：檢查所有 API Gateway 階段，以確保它們鏈接到相同的域名。
- ApiGwV2DomainNameStatus：檢查所有 API Gateway 階段，以確保網域名稱處於「可用」狀態。
- ApiGwV2EndpointType：檢查所有 API Gateway 階段，以確保它們具有相同的`Endpoint Type`值。
- ApiGwV2Quotas：檢查所有 API Gateway 群組，以確保它們符合「Service Quotas」管理的配額 (限制)。
- ApiGwV2MutualTlsAuthentication：檢查所有 API Gateway 階段，以確保它們具有相同的`Mutual TLS Authentication`值。
- ApiGwV2ProtocolType：檢查所有 API Gateway 階段，以確保它們具有相同的`Protocol Type`值。
- ApiGwV2RouteConfigs：檢查所有 API Gateway 階段，以確保它們具有相同組態的相同路由階層。
- ApiGwV2RouteSelectionExpression：檢查所有 API Gateway 階段，以確保它們具有相同的`Route Selection Expression`值。
- ApiGwV2RouteSettings：檢查所有 API Gateway 階段，以確保它們具有相同的`Default Route Settings`值。
- ApiGwV2SecurityPolicy：檢查所有 API Gateway 階段，以確保它們具有相同的`Security Policy`值。
- ApiGwV2StageVariables：檢查所有 API Gateway 階段，以確保它們都與其他階段`Stage Variables`相同。

- ApiGwV2ThrottlingBurstLimit：檢查所有 API Gateway 階段，以確保它們具有相同的`Throttling Burst Limit`值。
- ApiGwV2ThrottlingRateLimit：檢查所有 API Gateway 階段，以確保它們具有相同的`Throttling Rate Limit`值。

Amazon Aurora 集群

- RdsClusterStatus：檢查每個 Aurora 叢集，以確保其狀態為`AVAILABLE`或`BACKING-UP`。
- RdsEngineMode：檢查所有 Aurora 叢集，以確保它們具有相同的`Engine Mode`值。
- RdsEngineVersion：檢查所有 Aurora 叢集，以確保它們具有相同的`Major Version`值。
- RdsGlobalReplicaLag：檢查每個 Aurora 叢集，以確保其擁有少於 30 秒`Global Replica Lag`的時間。
- RdsNormalizedCapacity：檢查所有 Aurora 叢集，以確保它們的標準化容量在資源集中最大值的 15% 以內。
- RdsInstanceType：檢查所有 Aurora 叢集，以確保它們具有相同的執行個體類型。
- RdsQuotas：檢查所有 Aurora 叢集，以確保它們符合 Service Quotas 管理的配額 (限制)。

Auto Scaling 群組

- AsgMinSizeAndMaxSize：檢查所有「Auto Scaling」群組，以確保它們具有相同的最小和最大群組大小。
- AsgAZCount：檢查所有 Auto Scaling 群組，以確保它們具有相同數量的可用區域。
- AsgInstanceTypes：檢查所有 Auto Scaling 群組，以確保它們具有相同的執行個體類型。附註：此規則不會影響整備狀態。
- AsgInstanceSizes：檢查所有 Auto Scaling 群組，以確保它們具有相同的執行個體大小。
- AsgNormalizedCapacity：檢查所有 Auto Scaling 群組，以確保它們的標準化容量在資源集中最大值的 15% 以內。
- AsgQuotas：檢查所有 Auto Scaling 群組，以確保它們符合「Service Quotas」管理的配額 (限制)。

CloudWatch 警報

- CloudWatchAlarmState：檢查 CloudWatch 警報以確保每個警報都不處於`ALARM`或狀`INSUFFICIENT_DATA`態。

客戶閘道

- CustomerGatewayIpAddress：檢查所有客戶閘道，以確保它們具有相同的 IP 位址。
- CustomerGatewayState：檢查客戶閘道，以確保每個閘道都處於狀`AVAILABLE`態。

- CustomerGatewayVPNType：檢查所有客戶閘道，以確保它們具有相同的 VPN 類型。

DNS target resources

- DnsTargetResourceHostedZoneConfigurationRule：檢查所有 DNS 目標資源，以確保它們具有相同的 Amazon Route 53 託管區域 ID，並且每個託管區域都不是私有的。附註：此規則不會影響整備狀態。
- DnsTargetResourceRecordSetConfigurationRule：檢查所有 DNS 目標資源，以確保它們具有相同的資源記錄快取存留時間 (TTL)，並且 TTL 小於或等於 300。
- DnsTargetResourceRoutingRule：檢查與別名資源記錄集關聯的每個 DNS 目標資源，以確保它會將流量路由到目標資源上設定的 DNS 名稱。附註：此規則不會影響整備狀態。
- DnsTargetResourceHealthCheckRule：檢查所有 DNS 目標資源，以確保健全狀況檢查與其資源記錄集相關聯 (否則不適用)。附註：此規則不會影響整備狀態。

Amazon DynamoDB 資料表

- DynamoConfiguration：檢查所有 DynamoDB 表，以確保它們具有相同的金鑰、屬性、伺服器端加密和串流組態。
- DynamoTableStatus：檢查每個 DynamoDB 表格，以確保其狀態為「作用中」。
- DynamoCapacity：檢查所有 DynamoDB 表格，以確保其佈建的讀取容量和寫入容量在資源集中最大容量的 20% 以內。
- DynamoPeakRcuWcu：檢查每個 DynamoDB 表格，以確保其具有與其他表格相似的尖峰流量，以確保佈建的容量。
- DynamoGsiPeakRcuWcu：檢查每個 DynamoDB 表格，以確保其具有與其他表格相似的最大讀取和寫入容量，以確保佈建的容量。
- DynamoGsiConfig：檢查具有全域次要索引的所有 DynamoDB 表格，以確保表格使用相同的索引、金鑰結構描述和投影。
- DynamoGsiStatus：檢查具有全域次要索引的所有 DynamoDB 表格，以確保全域次要索引具有作用中狀態。
- DynamoGsiCapacity：檢查具有全域次要索引的所有 DynamoDB 表格，以確保表格已在資源集中最大容量的 20% 內佈建 GSI 讀取容量和 GSI 寫入容量。
- DynamoReplicationLatency：檢查屬於全域表的所有 DynamoDB 表，以確保它們具有相同的複寫延遲。
- DynamoAutoScalingConfiguration：檢查啟用「Auto Scaling」的所有 DynamoDB 表格，以確保它們具有相同的最小、最大值和目標讀取和寫入容量。
- DynamoQuotas：檢查所有 DynamoDB 表格，以確保其符合「Service Quotas」管理的配額 (限制)。

Elastic Load Balancing (傳統負載平衡器)

- ElbV1CheckAzCount：檢查每個 Classic Load Balancer，以確保其僅附加到一個可用區域。附註：此規則不會影響整備狀態。
- ElbV1AnyInstances：檢查所有傳統負載平衡器，以確保它們至少有一個 EC2 實例。
- ElbV1AnyInstancesHealthy：檢查所有傳統負載平衡器，以確保它們具有至少一個運作良好的 EC2 執行個體。
- ElbV1Scheme：檢查所有傳統負載平衡器，以確保它們具有相同的負載平衡器方案。
- ElbV1HealthCheckThreshold：檢查所有傳統負載平衡器，以確保它們具有相同的健康狀態檢查閾值。
- ElbV1HealthCheckInterval：檢查所有傳統負載平衡器，以確保它們具有相同的健康狀態檢查間隔值。
- ElbV1CrossZoneRoutingEnabled：檢查所有傳統負載平衡器，以確保它們具有相同的跨區域負載平衡值 (已啟用或停用)。
- ElbV1AccessLogsEnabledAttribute：檢查所有傳統負載平衡器，以確保它們對存取記錄具有相同的值 (已啟用或停用)。
- ElbV1ConnectionDrainingEnabledAttribute：檢查所有傳統負載平衡器，以確保它們具有相同的連線排空值 (已啟用或停用)。
- ElbV1ConnectionDrainingTimeoutAttribute：檢查所有傳統負載平衡器，以確保它們具有相同的連線排除逾時值。
- ElbV1IdleTimeoutAttribute：檢查所有傳統負載平衡器，以確保它們具有相同的閒置逾時值。
- ElbV1ProvisionedCapacityLcuCount：檢查佈建 LCU 大於 10 的所有傳統負載平衡器，以確保它們在資源集中佈建最高 LCU 的 20% 內。
- ElbV1ProvisionedCapacityStatus：檢查每個 Classic Load Balancer 上佈建的容量狀態，以確保其值不為 [已停用] 或 [擱置中]。

Amazon EBS 磁碟區

- EbsVolumeEncryption：檢查所有EBS磁碟區，以確保它們具有相同的加密值 (已啟用或停用)。
- EbsVolumeEncryptionDefault：檢查所有EBS磁碟區，以確保它們在預設情況下具有相同的加密值 (已啟用或停用)。
- EbsVolumeIops: 檢查所有EBS磁碟區，以確保它們具有相同的每秒輸入/輸出操作 (IOPS)。
- EbsVolumeKmsKeyId：檢查所有EBS卷以確保它們具有相同的默認 AWS KMS 密鑰 ID。
- EbsVolumeMultiAttach：檢查所有EBS磁碟區，以確保它們對多重連接 (ENABLED 或 DISABLED) 具有相同的值。

- EbsVolumeQuotas: 檢查所有EBS磁碟區，以確保它們符合「Service Quotas」設定的配額 (限制)。
- EbsVolumeSize：檢查所有EBS卷以確保它們具有相同的可讀大小。
- EbsVolumeState：檢查所有EBS磁碟區，以確保它們具有相同的磁碟區狀態。
- EbsVolumeType：檢查所有EBS磁碟區，以確保它們具有相同的磁碟區類型。

AWS Lambda 函數

- LambdaMemorySize：檢查所有 Lambda 函數，以確保它們具有相同的記憶體大小。如果一個人有更多的內存，其他人被標記NOT READY。
- LambdaFunctionTimeout：檢查所有 Lambda 函數，以確保它們具有相同的逾時值。如果其中一個值較大，則會標記其他值NOT READY。
- LambdaFunctionRuntime：檢查所有 Lambda 函數，以確保它們都具有相同的執行階段。
- LambdaFunctionReservedConcurrentExecutions：檢查所有 Lambda 函數，以確保它們都具有相同的Reserved Concurrent Executions值。如果其中一個值較大，則會標記其他值NOT READY。
- LambdaFunctionDeadLetterConfig：檢查所有 Lambda 函數，以確保它們都具有Dead Letter Config定義，或者沒有一個。
- LambdaFunctionProvisionedConcurrencyConfig：檢查所有 Lambda 函數，以確保它們具有相同的Provisioned Concurrency值。
- LambdaFunctionSecurityGroupCount：檢查所有 Lambda 函數，以確保它們具有相同的Security Groups值。
- LambdaFunctionSubnetIdCount：檢查所有 Lambda 函數，以確保它們具有相同的Subnet Ids值。
- LambdaFunctionEventSourceMappingMatch：檢查所有 Lambda 函數，以確保所有選擇的Event Source Mapping 屬性在它們之間相符。
- LambdaFunctionLimitsRule：檢查所有 Lambda 函數，以確保它們符合 Service Quotas 管理的配額 (限制)。

網路負載平衡器和應用程式負載平衡器

- ElbV2CheckAzCount：檢查每個 Network Load Balancer，以確保其僅連接到一個可用區域。附註：此規則不會影響整備狀態。
- ElbV2TargetGroupsCanServeTraffic：檢查每個 Network Load Balancer 和 Application Load Balancer，以確保其具有至少一個運作良好的 Amazon EC2 執行個體。
- ElbV2State：檢查每個 Network Load Balancer 和 Application Load Balancer，以確保其處於狀ACTIVE態。

- ElbV2IpAddressType：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們具有相同的 IP 位址類型。
- ElbV2Scheme：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們具有相同的配置。
- ElbV2Type：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們具有相同的類型。
- ElbV2S3LogsEnabled：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們對於 Amazon S3 伺服器存取日誌具有相同的值 (已啟用或停用)。
- ElbV2DeletionProtection：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們具有相同的刪除保護值 (已啟用或停用)。
- ElbV2IdleTimeoutSeconds：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們在閒置時間秒內具有相同的值。
- ElbV2HttpDropInvalidHeaders：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們對於 HTTP 卸除無效標頭具有相同的值。
- ElbV2Http2Enabled：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們對 HTTP2 具有相同的值 (已啟用或停用)。
- ElbV2CrossZoneEnabled：檢查所有網路負載平衡器和應用程式負載平衡器，以確保它們具有相同的跨區域負載平衡值 (已啟用或停用)。
- ElbV2ProvisionedCapacityLcuCount：檢查佈建 LCU 大於 10 的所有網路負載平衡器和應用程式負載平衡器，以確保它們在資源集中佈建最高 LCU 的 20% 以內。
- ElbV2ProvisionedCapacityEnabled：檢查所有網路負載平衡器和應用程式負載平衡器佈建的容量狀態，以確保其值不為 [已停用] 或 [擱置]。

Amazon MSK 叢集

- MskClusterClientSubnet：檢查每個 MSK 叢集，以確保它只有兩個或只有三個用戶端子網路。
- MskClusterInstanceType：檢查所有 MSK 叢集，以確保它們具有相同的 Amazon EC2 執行個體類型。
- MskClusterSecurityGroups：檢查所有 MSK 叢集，以確保它們具有相同的安全群組。
- MskClusterStorageInfo：檢查所有 MSK 叢集，以確保它們具有相同的 EBS 儲存磁碟區大小。如果其中一個值較大，則其他人將標記為「未就緒」。
- MskClusterACMCertificate：檢查所有 MSK 叢集，以確保它們具有相同的用戶端授權憑證 ARN 清單。
- MskClusterServerProperties：檢查所有 MSK 叢集，以確保它們具有相同的值。`Current Broker Software Info`
- MskClusterKafkaVersion：檢查所有 MSK 叢集，以確保它們具有相同的 Kafka 版本。

- MskClusterEncryptionInTransitInCluster：檢查所有 MSK 叢集，以確保它們具有相同的值。`Encryption In Transit In Cluster`
- MskClusterEncryptionInClientBroker：檢查所有 MSK 叢集，以確保它們具有相同的值。`Encryption In Transit Client Broker`
- MskClusterEnhancedMonitoring：檢查所有 MSK 叢集，以確保它們具有相同的值。`Enhanced Monitoring`
- MskClusterOpenMonitoringInJmx：檢查所有 MSK 叢集，以確保它們具有相同的值。`Open Monitoring JMX Exporter`
- MskClusterOpenMonitoringInNode：檢查所有 MSK 叢集，以確保它們具有相同的值 `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3：檢查所有 MSK 叢集，以確保它們具有相同的值。`Is Logging in S3`
- MskClusterLoggingInFirehose：檢查所有 MSK 叢集，以確保它們具有相同的值。`Is Logging In Firehose`
- MskClusterLoggingInCloudWatch：檢查所有 MSK 叢集，以確保它們具有相同的值。`Is Logging Available In CloudWatch Logs`
- MskClusterNumberOfBrokerNodes：檢查所有 MSK 叢集，以確保它們具有相同的值。`Number of Broker Nodes`如果其中一個值較大，則其他人將標記為「未就緒」。
- MskClusterState：檢查每個 MSK 叢集，以確保其處於作用中狀態。
- MskClusterLimitsRule：檢查所有 Lambda 函數，以確保它們符合 Service Quotas 管理的配額 (限制)。

Amazon 路線 53 健康檢查

- R53HealthCheckType：檢查每個 Route 53 健康狀態檢查，以確保它不是「計算的」類型，並且所有檢查都是相同類型的。
- R53HealthCheckDisabled：檢查每個 Route 53 健康狀態檢查，以確保其沒有停用狀態。
- R53HealthCheckStatus：檢查每個 Route 53 健康狀態檢查，以確保其處於「成功」狀態。
- R53HealthCheckRequestInterval：檢查所有 Route 53 健康檢查，以確保它們都具有相同的`Request Interval`值。
- R53HealthCheckFailureThreshold：檢查所有 Route 53 健康檢查，以確保它們都具有相同的值 `Failure Threshold.`
- R53HealthCheckEnableSNI：檢查所有 Route 53 健康檢查，以確保它們都具有相同的值 `Enable SNI.`

- R53HealthCheckSearchString：檢查所有 Route 53 健康檢查，以確保它們都具有相同的值 `Search String`.
- R53HealthCheckRegions：檢查所有 Route 53 健康檢查，以確保它們都具有相同的 AWS 區域列表。
- R53HealthCheckMeasureLatency：檢查所有 Route 53 健康檢查，以確保它們都具有相同的`Measure Latency`值。
- R53HealthCheckInsufficientDataHealthStatus：檢查所有 Route 53 健康檢查，以確保它們都具有相同的`Insufficient Data Health Status`值。
- R53HealthCheckInverted：檢查所有 Route 53 的健康檢查，以確保它們全部倒置或全部未倒置。
- R53HealthCheckResourcePath：檢查所有 Route 53 健康檢查，以確保它們都具有相同的`Resource Path`值。
- R53HealthCheckCloudWatchAlarm：檢查所有 Route 53 健康狀態檢查，以確保與它們相關聯的 CloudWatch 警報具有相同的設置和配置。

Amazon SNS 訂閱

- SnsSubscriptionProtocol：檢查所有 SNS 訂閱，以確保它們具有相同的通訊協定。
- SnsSubscriptionSqsLambdaEndpoint：檢查具有 Lambda 或 SQS 端點的所有 SNS 訂閱，以確保它們具有不同的端點。
- SnsSubscriptionNonAwsEndpoint：檢查具有非AWS 服務端點類型 (例如電子郵件) 的所有 SNS 訂閱，以確保訂閱具有相同的端點。
- SnsSubscriptionPendingConfirmation：檢查所有 SNS 訂閱，以確保它們對於「待確認」具有相同的值。
- SnsSubscriptionDeliveryPolicy：檢查使用 HTTP/S 的所有 SNS 訂閱，以確保它們對於「有效傳遞期間」具有相同的值。
- SnsSubscriptionRawMessageDelivery：檢查所有 SNS 訂閱，以確保它們對「原始訊息傳送」具有相同的值。
- SnsSubscriptionFilter：檢查所有 SNS 訂閱，以確保它們對「篩選原則」具有相同的值。
- SnsSubscriptionRedrivePolicy：檢查所有 SNS 訂閱，以確保它們具有相同的「重新驅動策略」值。
- SnsSubscriptionEndpointEnabled：檢查所有 SNS 訂閱，以確保它們對於「已啟用端點」具有相同的值。
- SnsSubscriptionLambdaEndpointValid：檢查具有 Lambda 端點的所有 SNS 訂閱，以確保它們具有有效的 Lambda 端點。

- SnsSubscriptionSqsEndpointValidRule：檢查使用 SQS 端點的所有 SNS 訂閱，以確保它們具有有效的 SQS 端點。
- SnsSubscriptionQuotas：檢查所有 SNS 訂閱，以確保其符合「Service Quotas」管理的配額 (限制)。

Amazon SNS 主題

- SnsTopicDisplayName：檢查所有 SNS 主題，以確保它們具有相同的`Display Name`值。
- SnsTopicDeliveryPolicy：檢查具有 HTTPS 訂閱者的所有 SNS 主題，以確保它們具有相同`EffectiveDeliveryPolicy`的主題。
- SnsTopicSubscription：檢查所有 SNS 主題，以確保每個通訊協定的訂閱者數量相同。
- SnsTopicAwsKmsKey：檢查所有 SNS 主題，以確保所有主題或沒有任何主題具有 AWS KMS 金鑰。
- SnsTopicQuotas：檢查所有 SNS 主題，以確保其符合「Service Quotas」管理的配額 (限制)。

Amazon SQS 佇列

- SqsQueueType：檢查所有 SQS 佇列，以確保它們的值都相同。`Type`
- SqsQueueDelaySeconds：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Delay Seconds`
- SqsQueueMaximumMessageSize：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Maximum Message Size`
- SqsQueueMessageRetentionPeriod：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Message Retention Period`
- SqsQueueReceiveMessageWaitTimeSeconds：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Receive Message Wait Time Seconds`
- SqsQueueRedrivePolicyMaxReceiveCount：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Redrive Policy Max Receive Count`
- SqsQueueVisibilityTimeout：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Visibility Timeout`
- SqsQueueContentBasedDeduplication：檢查所有 SQS 佇列，以確保它們都具有相同的值。`Content-Based Deduplication`
- SqsQueueQuotas：檢查所有 SQS 佇列，以確保它們符合「Service Quotas」管理的配額 (限制)。

Amazon VPC

- VpcCidrBlock：檢查所有 VPC，以確保它們對 CIDR 區塊網路大小具有相同的值。

- VpcCidrBlocksSameProtocolVersion：檢查具有相同 CIDR 區塊的所有 VPC，以確保它們對於網際網路串流通訊協定版本號碼具有相同的值。
- VpcCidrBlocksStateInAssociationSets：檢查所有 VPC 的所有 CIDR 區塊關聯集，以確保它們都具有處於某個狀態的 CIDR 區塊。ASSOCIATED
- VpcIpv6CidrBlocksStateInAssociationSets：檢查所有 VPC 的所有 CIDR 區塊關聯集，以確保它們都具有相同位址數目的 CIDR 區塊。
- VpcCidrBlocksInAssociationSets：檢查所有 VPC 的所有 CIDR 區塊關聯集，以確保它們都具有相同的大小。
- VpcIpv6CidrBlocksInAssociationSets：檢查所有 VPC 的所有 IPv6 CIDR 區塊關聯集，以確保它們具有相同的大小。
- VpcState：檢查每個 VPC 以確保其處於一AVAILABLE個狀態。
- VpcInstanceTenancy：檢查所有 VPC，以確保它們都具有相同的值。Instance Tenancy
- VpcIsDefault：檢查所有 VPC，以確保它們具有相同的值 Is Default.
- VpcSubnetState：檢查每個 VPC 子網路，以確保其處於「可用」狀態。
- VpcSubnetAvailableIpAddressCount：檢查每個 VPC 子網路，以確保其可用 IP 位址計數大於零。
- VpcSubnetCount：檢查所有 VPC 子網路，以確保它們具有相同數量的子網路。
- VpcQuotas：檢查所有 VPC 子網路，以確保其符合「Service Quotas」管理的配額 (限制)。

AWS VPN 連接

- VpnConnectionsRouteCount：檢查所有 VPN 連接，以確保它們至少具有一個路由，以及相同數量的路由。
- VpnConnectionsEnableAcceleration：檢查所有 VPN 連接，以確保它們具有相同的Enable Accelerations值。
- VpnConnectionsStaticRoutesOnly：檢查所有 VPN 連接，以確保它們具有相同的值 Static Routes Only.
- VpnConnectionsCategory：檢查所有 VPN 連接，以確保它們具有的VPN類別。
- VpnConnectionsCustomerConfiguration：檢查所有 VPN 連接，以確保它們具有相同的Customer Gateway Configuration值。
- VpnConnectionsCustomerGatewayId：檢查每個 VPN 連接，以確保其連接了客戶閘道。
- VpnConnectionsRoutesState：檢查所有 VPN 連接以確保它們處於一個AVAILABLE狀態。
- VpnConnectionsVgwTelemetryStatus：檢查每個 VPN 連接，以確保其具有 VGW 狀態。UP

- VpnConnectionsVgwTelemetryIpAddress：檢查每個 VPN 連線，以確保每個 VGW 遙測具有不同的外部 IP 位址。
- VpnConnectionsTunnelOptions：檢查所有 VPN 連接，以確保它們具有相同的通道選項。
- VpnConnectionsRoutesCidr：檢查所有 VPN 連接，以確保它們具有相同的目標 CIDR 塊。
- VpnConnectionsInstanceType：檢查所有 VPN 連接以確保它們具有相同`Instance Type`的連接。

AWS VPN 閘道

- VpnGatewayState：檢查所有 VPN 閘道，以確保它們處於「可用」狀態。
- VpnGatewayAsn：檢查所有 VPN 閘道，以確保它們具有相同的 ASN。
- VpnGatewayType：檢查所有 VPN 閘道，以確保它們具有相同的類型。
- VpnGatewayAttachment：檢查所有 VPN 閘道，以確保它們具有相同的附件配置。

在主控台上檢視整備規則

您可以在 (依每個資源類型列出) 上檢視整備規則。 AWS Management Console

在主控台上檢視整備規則

1. 在開啟 Route 53 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備檢查。
3. 在 [資源類型] 下，選擇您要檢視其規則的資源類型。

Route 53 ARC 中的資源類型和 ARN 格式

在 Amazon Route 53 應用程式復原控制器中建立資源集時，請指定要包含在集合中的資源類型，並為要包含的每個資源指定 Amazon 資源名稱 (ARN)。Route 53 ARC 需要為每種資源類型提供特定的 ARN 格式。本節列出了 Route 53 ARC 支援的資源類型，以及每一種類型的相關 ARN 格式。

具體格式取決於資源。當您提供 ARN 時，請以您的資源特定資訊取代##文字。

> **Note**
>
> 請注意，Route 53 ARC 資源所需的 ARN 格式可能與服務本身對其資源所需的 ARN 格式不同。例如，服務授權參考中每個服務的 [資源類型] 區段中描述的 ARN 格式可能不包含 Route 53 ARC 支援 Route 53 ARC 服務中功能所需的 AWS 帳戶 ID 或其他資訊。

AWS::ApiGateway::Stage

亞 Amazon API Gateway 版本 1 階段。

- ARN 格式:`arn:partition:apigateway:region:account:/restapis/api-id/stages/stage-name`

  範例：`arn:aws:apigateway:us-east-1:111122223333:/restapis/123456789/stages/ExampleStage`

  如需詳細資訊，請參閱 API Gateway Amazon 資源名稱 (ARN) 參考資料。

AWS::ApiGatewayV2::Stage

亞 Amazon API Gateway 版本 2 階段。

- ARN 格式:`arn:partition:apigateway:region:account:/apis/api-id/stages/stage-name`

  範例：`arn:aws:apigateway:us-east-1:111122223333:/apis/123456789/stages/ExampleStage`

  如需詳細資訊，請參閱 API Gateway Amazon 資源名稱 (ARN) 參考資料。

AWS::CloudWatch::Alarm

一個 Amazon CloudWatch 警報。

- ARN 格式:`arn:partition:cloudwatch:region:account:alarm:alarm-name`

  範例：`arn:aws:cloudwatch:us-west-2:111122223333:alarm:test-alarm-1`

  如需詳細資訊，請參閱 Amazon 定義的資源類型 CloudWatch。

AWS::DynamoDB::Table

一個 Amazon DynamoDB 表。

- ARN 格式:arn:*partition*:dynamodb:*region*:*account*:table/*table-name*

  範例：arn:aws:dynamodb:us-west-2:111122223333:table/BigTable

  如需詳細資訊，請參閱 DynamoDB 資源和作業。

AWS::EC2::CustomerGateway

客戶閘道裝置。

- ARN 格式:arn:*partition*:ec2:*region*:*account*:customer-gateway/*CustomerGatewayId*

  範例：arn:aws:ec2:us-west-2:111122223333:customer-gateway/vcg-123456789

  如需詳細資訊，請參閱 Amazon EC2 定義的資源類型。

AWS::EC2::Volume

Amazon EBS 卷。

- ARN 格式:arn:*partition*:ec2:*region*:*account*:volume/*VolumeId*

  範例：arn:aws:ec2:us-west-2:111122223333:volume/volume-of-cylinder-is-pi

  如需詳細資訊，請參閱 API Gateway Amazon 資源名稱 (ARN) 參考資料。

AWS::ElasticLoadBalancing::LoadBalancer

Classic Load Balancer。

- ARN 格式:arn:*partition*:elasticloadbalancing:*region*:*account*:loadbalancer/*LoadBalance*

  範例：arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB

  如需詳細資訊，請參閱 E lastic Load Balancing 資源。

AWS::ElasticLoadBalancingV2::LoadBalancer

Network Load Balancer 或 Application Load Balancer。

- Network Load Balancer 的 ARN 格式：arn:*partition*:elasticloadbalancing:*region*:*account*:loadbalancer/net/*LoadBalancerName*

Network Load Balancer 範例：arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB

- 應用程式負載平衡器的 ARN 格式：arn:*partition*:elasticloadbalancing:*region*:*account*:loadbalancer/app/*LoadBalancerName*

  Application Load Balancer 的範例：arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/app/sandbox-alb/123456789acbdeALB

  如需詳細資訊，請參閱 E lastic Load Balancing 資源。

AWS::Lambda::Function

一個 AWS Lambda 函數。

- ARN 格式:arn:*partition*:lambda:*region*:*account*:function:*FunctionName*

  範例：arn:aws:lambda:us-west-2:111122223333:function:my-function

  如需詳細資訊，請參閱 Lambda 動作的資源和條件。

AWS::MSK::Cluster

一個 Amazon MSK 叢集。

- ARN 格式:arn:*partition*:kafka:*region*:*account*:cluster/*ClusterName*/*UUID*

  範例：arn:aws:kafka:us-east-1:111122223333:cluster/demo-cluster-1/123456-1111-2222-3333

  如需詳細資訊，請參閱 Amazon Managed Streaming for Apache Kafka 定義的資源類型。

AWS::RDS::DBCluster

Aurora 資料庫叢集。

- ARN 格式:arn:*partition*:rds:*region*:*account*:cluster:*DbClusterInstanceName*

  範例：arn:aws:rds:us-west-2:111122223333:cluster:database-1

  如需詳細資訊，請參閱使用 Amazon RDS 中的 Amazon 資源名稱 (ARN)。

AWS::Route53::HealthCheck

Amazon 路線 53 健康檢查。

- ARN 格式:arn:*partition*:route53:::healthcheck/*Id*

  範例：arn:aws:route53:::healthcheck/123456-1111-2222-3333

AWS::SQS::Queue

一個 Amazon SQS 隊列。

- ARN 格式:arn:*partition*:sqs:*region*:*account*:*QueueName*

  範例：arn:aws:sqs:us-west-2:111122223333:StandardQueue

  如需詳細資訊，請參閱 Amazon 簡單佇列服務資源和操作。

AWS::SNS::Topic

Amazon SNS 主題。

- ARN 格式:arn:*partition*:sns:*region*:*account*:*TopicName*

  範例：arn:aws:sns:us-west-2:111122223333:TopicName

  如需詳細資訊，請參閱 Amazon SNS 資源 ARN 格式。

AWS::SNS::Subscription

Amazon SNS 訂閱。

- ARN 格式:arn:*partition*:sns:*region*:*account*:*TopicName*:*SubscriptionId*

  範例：arn:aws:sns:us-west-2:111122223333:TopicName:12345678901234567890

AWS::EC2::VPC

Virtual Private Cloud (VPC)。

- ARN 格式:arn:*partition*:ec2:*region*:*account*:vpc/*VpcId*

  範例：arn:aws:ec2:us-west-2:111122223333:vpc/vpc-123456789

  如需詳細資訊，請參閱 VPC 資源。

AWS::EC2::VPNConnection

虛擬私人網路 (VPN) 連線。

- ARN 格式:arn:*partition*:ec2:*region*:*account*:vpn-connection/*VpnConnectionId*

範例：arn:aws:ec2:us-west-2:111122223333:vpn-connection/vpn-123456789

如需詳細資訊，請參閱 Amazon EC2 定義的資源類型。

AWS::EC2::VPNGateway

虛擬私人網路 (VPN) 閘道。

- ARN 格式:arn:*partition*:ec2:*region*:*account*:vpn-gateway/*VpnGatewayId*

  範例：arn:aws:ec2:us-west-2:111122223333:vpn-gateway/vgw-123456789acbdefgh

  如需詳細資訊，請參閱 Amazon EC2 定義的資源類型。

AWS::Route53RecoveryReadiness::DNSTargetResource

用於整備檢查的 DNS 目標資源包括 DNS 記錄類型、網域名稱、路由 53 託管區域 ARN，以及 Network Load Balancer ARN 或路由 53 記錄集識別碼。

- 託管區域的 ARN 格式：arn:*partition*:route53::*account*:hostedzone/*Id*

  託管區域的範例：arn:aws:route53::111122223333:hostedzone/abcHostedZone

  注意：您必須在託管區域 ARN 中包含帳戶 ID，如此處所指定。需要帳號 ID，以便 Route 53 ARC 可以輪詢資源。該格式與 Amazon Route 53 所需的 ARN 格式有意不同，請參閱服務授權參考中的 Route 53 服務資源類型中所述。

- Network Load Balancer 的 ARN 格式：arn:*partition*:elasticloadbalancing:*region*:*account*:loadbalancer/net/*LoadBalancerName*

  Network Load Balancer 範例：arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh

  如需詳細資訊，請參閱 E lastic Load Balancing 資源。

記錄和監控 Amazon Route 53 應用程式復原控制器中的準備程度檢查

您可以使用 Amazon CloudWatch 和 Amazon 監控 Amazon Route 53 應 EventBridge 用程式復原控制器中的準備就緒檢查，以分析模式並協助疑難排解問題。 AWS CloudTrail

> **Note**
>
> 您必須在主控台和使用時 CloudWatch 檢視美國西部 (奧勒岡) 區域中 Route 53 ARC 的指標和記錄 AWS CLI。使用時 AWS CLI，請包含下列參數，為您的命令指定美國西部 (奧勒岡) 區域：`--region us-west-2`。

主題

- 在 Route 53 ARC 中使用 Amazon CloudWatch 進行準備檢查
- 使用記錄準備檢查 API 呼叫 AWS CloudTrail
- 在 Amazon Route 53 ARC 中使用準備檢查 EventBridge

在 Route 53 ARC 中使用 Amazon CloudWatch 進行準備檢查

Amazon Route 53 應用程式復原控制器會將資料點發佈到 Amazon CloudWatch ，以便您檢查整備 CloudWatch 可讓您擷取有關這些資料點的統計資料，做為一組排序的時間序列資料 (稱為指標)。您可以將指標視為要監控的變數，且資料點是該變數在不同時間點的值。例如，您可以監控指定時間段內通過「 AWS 區域」的流量。每個資料點都有關聯的時間戳記和可選的測量單位。

您可以使用指標來確認系統的運作符合預期。例如，如果指標超出您認為可接受的範圍，您可以建立 CloudWatch 警示來監控指定的指標並啟動動作 (例如傳送通知至電子郵件地址)。

如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南。

主題

- Route 53 弧度量
- Route 53 ARC 指標的統計資料
- 在 Route 53 中檢視 CloudWatch 度量

Route 53 弧度量

`AWS/Route53RecoveryReadiness` 命名空間包含下列指標。

指標	描述
`ReadinessChecks`	表示 Route 53 ARC 處理的就緒檢查數目。量度可以按照其狀態進行標註，如下所示。

指標	描述
	單位:Count. 報告條件：有非零值。 統計：唯一有用的統計數據是Sum。 維度 • READY • NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	表示 Route 53 ARC 所處理的資源數量，這些資源可依據 API 所定義的資源識別碼進行維度設定。 單位:Count. 報告條件：有非零值。 統計：唯一有用的統計數據是Sum。 維度 • ResourceSetType ：這些是資源類型，按 Route 53 ARC 評估的每個給定類型的資源數進行過濾 例如：AWS::CloudWatch::Alarm

Route 53 ARC 指標的統計資料

CloudWatch 根據 Route 53 ARC 發佈的度量資料點提供統計資料。統計資料是指定期間內測量結果資料的彙總。當您請求統計資料時，傳回的資料流是藉由指標名稱和維度做識別。維度是用來單獨辨識指標的名稱/值組。

以下是您可能會覺得有用的公制/維度組合的範例：

- 檢視 Route 53 ARC 評估是否準備就緒程度的準備程度檢查次數。

- 檢視由 Route 53 ARC 評估之指定資源集型態的資源總數。

在 Route 53 中檢視 CloudWatch 度量

您可以使用 CloudWatch 主控台或檢視 Route 53 ARC 的 CloudWatch 度量 AWS CLI。在主控台中，測量結果會顯示為監視圖表。

您必須在主控台或使用時 CloudWatch 檢視美國西部 (奧勒岡) 區域中 Route 53 ARC 的度量 AWS CLI。使用時 AWS CLI，請包含下列參數，為您的命令指定美國西部 (奧勒岡) 區域：`--region us-west-2`。

使用 CloudWatch 主控台檢視指標

1. 請在以下位置開啟 CloudWatch 主控台。 https://console.aws.amazon.com/cloudwatch/
2. 在導覽窗格中，選擇 指標。
3. 選取路由 53 RecoveryReadiness 命名空間。
4. (選用) 若要檢視所有維度的指標，請在搜尋欄位中鍵入其名稱。

若要使用 AWS CLI

使用下列 list-metrics 命令來列出可用指標：

```
aws cloudwatch list-metrics --namespace AWS/Route53RecoveryReadiness --region us-west-2
```

若要取得測量結果的統計資料，請使用 AWS CLI

使用下列get-metric-statistics命令取得指定測量結果和維度的統計資料。請注意， CloudWatch 將每個唯一維度組合視為單獨的量度。您無法使用未特別發佈的維度組合來擷取統計資料。您必須指定建立指標時所使用的相同維度。

下列範例會列出 Route 53 ARC 中帳戶每分鐘評估的整備檢查總計。

```
aws cloudwatch get-metric-statistics --namespace AWS/Route53RecoveryReadiness \
--metric-name ReadinessChecks \
--region us-west-2 \
--statistics Sum --period 60 \
--dimensions Name=State,Value=READY \
--start-time 2021-07-03T01:00:00Z --end-time 2021-07-03T01:20:00Z
```

以下是來自命令的範例輸出：

```
{
    "Label": "ReadinessChecks",
    "Datapoints": [
        {
            "Timestamp": "2021-07-08T18:00:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:04:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:01:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:02:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        },
        {
            "Timestamp": "2021-07-08T18:03:00Z",
            "Sum": 1.0,
            "Unit": "Count"
        }
    ]
}
```

使用記錄準備檢查 API 呼叫 AWS CloudTrail

Amazon Route 53 應用程式復原控制器整合在一起 AWS CloudTrail，這項服務可提供 Route 53 ARC 中使用者、角色或 AWS 服務所採取的動作記錄。 CloudTrail 將 Route 53 ARC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 Route 53 ARC 主控台的呼叫，以及對 Route 53 ARC API 作業的程式碼呼叫。

如果您建立追蹤，您可以啟用連續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 Route 53 ARC 的事件。如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。

使用收集的資訊 CloudTrail，您可以判斷向 Route 53 ARC 發出的要求、提出要求的 IP 位址、提出要求的人員、提出要求的時間以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

Route 53 弧資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動在 Route 53 ARC 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷程記錄。

對於正在進行的事件記錄 AWS 帳戶，包括 Route 53 ARC 的事件，請創建一條線索。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。依預設，當您在主控台中建立追蹤時，該追蹤會套用至所有的 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定 Amazon SNS 通知 CloudTrail
- 從多個區域接收 CloudTrail 日誌文件並從多個帳戶接收 CloudTrail 日誌文件

Amazon Route 53 應用程式復原控制器的復原準備 API 參考指南、Amazon Route 53 應用程式復原控制器的復原控制組態 API 參考指南、Amazon Route 53 應用程式復原控制器的路由控制 API 參考指南都會記錄下來，並記錄在 Amazon Route 53 應用程式復原控制器的路由控制 API 參考 CloudTrail 例如，呼叫`UpdateRoutingControlState`和`CreateRecoveryGroup`動作會`CreateCluster`在 CloudTrail 記錄檔中產生項目。

每一筆事件或日誌專案都會包含產生請求者的資訊。身分資訊可協助您判斷下列事項：

- 要求是使用根使用者登入資料還是 AWS Identity and Access Management (IAM) 使用者登入資料提出。
- 提出該請求時，是否使用了特定角色或聯合身分使用者的暫時安全憑證。
- 請求是否由其他 AWS 服務提出。

如需詳細資訊，請參閱CloudTrail 使 userIdentity 元素。

在事件歷史記錄中查看 Route 53 ARC 事件

CloudTrail 可讓您在事件歷史記錄中檢視最近的事件。若要檢視 Route 53 ARC API 要求的事件，您必須在主控台頂端的區域選取器中選擇美國西部 (奧勒岡)。若要取得更多資訊，請參閱《使用指南》中的〈AWS CloudTrail 使用 CloudTrail 事件歷程〉。

瞭解 Route 53 ARC 記錄檔項目

追蹤是一種組態，可讓事件以日誌檔的形式傳遞到您指定的 Amazon S3 儲存貯體。 CloudTrail 記錄檔包含一或多個記錄項目。事件代表來自任何來源的單一請求，包括有關請求的操作，動作的日期和時間，請求參數等信息。 CloudTrail 日誌文件不是公共 API 調用的有序堆棧跟踪，因此它們不會以任何特定順序顯示。

下列範例顯示示範整備檢查`CreateRecoveryGroup`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "A1B2C3D4E5F6G7EXAMPLE",
        "arn": "arn:aws:iam::111122223333:role/admin",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA33L3W36EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/admin",
                "accountId": "111122223333",
                "userName": "EXAMPLENAME"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2021-07-06T18:08:03Z",
    "eventSource": "route53-recovery-readiness.amazonaws.com",
    "eventName": "CreateRecoveryGroup",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.50",
```

```
    "userAgent": "Boto3/1.17.101 Python/3.8.10 Linux/4.14.231-180.360.amzn2.x86_64
 exec-env/AWS_Lambda_python3.8 Botocore/1.20.102",
    "requestParameters": {
        "recoveryGroupName": "MyRecoveryGroup"
    },
    "responseElements": {
        "Access-Control-Expose-Headers": "x-amzn-errortype,x-amzn-requestid,x-amzn-
errormessage,x-amzn-trace-id,x-amzn-requestid,x-amz-apigw-id,date",
        "cells": [],
        "recoveryGroupName": "MyRecoveryGroup",
        "recoveryGroupArn": "arn:aws:route53-recovery-readiness::111122223333:recovery-
group/MyRecoveryGroup",
        "tags": "***"
    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


在 Amazon Route 53 ARC 中使用準備檢查 EventBridge

您可以使用 Amazon 設定事件驅動規則 EventBridge，以監控 Amazon Route 53 應用程式復原控制器中的整備程度檢查資源，然後啟動使用其他 AWS 服務的目標動作。例如，您可以設定傳送電子郵件通知的規則，方法是在就緒檢查狀態從「就緒」變更為「準備就緒」時，傳送 Amazon SNS 主題。

> **Note**
>
> Route 53 ARC 僅在美國西部 (奧勒岡) (美國西部 -2) 區域發佈準備檢查 EventBridge 事件。AWS 若要接收整備檢查的 EventBridge 事件，請在美國西部 (奧勒岡) 區域建立 EventBridge 規則。

您可以在 Amazon 中創建規則 EventBridge 來處理以下 Route 53 ARC 準備檢查事件：

- 準備檢查準備。事件會指定準備檢查狀態是否變更，例如，從「就緒」變更為「未就緒」。

要捕獲您感興趣的特定 Route 53 ARC 事件，請定義 EventBridge 可用於檢測事件的特定事件模式。事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

盡可能發出事件。 EventBridge 在正常操作情況下，它們是從 53 ARC 公路交付到近乎實時的。但是，可能會出現可能會延遲或阻止事件傳遞的情況。

如需 EventBridge 規則如何處理事件模式的詳細資訊，請參閱 EventBridge.

監控整備程度檢查資源 EventBridge

使用 EventBridge，您可以建立規則，以定義 Route 53 ARC 針對整備檢查資源發出事件時要採取的動作。

要鍵入或複製事件模式並將其粘貼到 EventBridge 控制台中，請在控制台中選擇「輸入我自己的選項」選項。為了協助您判斷可能對您有用的事件模式，本主題包含範例整備事件模式。

建立資源事件的規則

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. AWS 區域 若要在中建立規則，請選擇美國西部 (奧勒岡)。這是整備事件所需的區域。
3. 選擇 Create rule (建立規則)。
4. 輸入規則的Name (名稱)，或者輸入描述。
5. 對於事件匯流排，保留預設值 (預設值)。
6. 選擇下一步。
7. 對於「建置」事件模式步驟，對於事件來源，保留預設值「AWS 事件」。
8. 在 [範例事件] 下，選擇 [輸入我自己]。
9. 對於範例事件，請輸入或複製並貼上事件模式。如需範例，請參閱下一節。

範例整備事件模式

事件模式與它們相符的事件具有相同的結構。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

您可以將此區段中的事件模式複製並貼 EventBridge 到中，以建立可用來監視 Route 53 ARC 動作和資源的規則。

下列事件模式提供範例，您可以在中用 EventBridge 於 Route 53 ARC 中的整備檢查功能。

- 從 Route 53 ARC 準備檢查中選擇所有事件。

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ]
}
```

- 僅選取與儲存格相關的事件。

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ]
}
```

- 僅選取與名為的特定儲存格相關的事件*MyExampleCell*。

```
{
    "source": [
        "aws.route53-recovery-readiness"
    ],
    "detail-type": [
        "Route 53 Application Recovery Controller cell readiness status change"
    ],
    "resources": [
        "arn:aws:route53-recovery-readiness::111122223333:cell/MyExampleCell"
    ]
}
```

- 只選取任何復原群組、儲存格或整備檢查狀態變成時的事件*NOT READY*。

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
```

```
      }
   }
}
```

- 只選取任何復原群組、儲存格或整備檢查變成任何項目時的事件，但除外 *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

以下是復原群組準備狀態變更的 Route 53 ARC 事件範例：

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller recovery group readiness
 status change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:recovery-group/BillingApp"
    ],
    "detail": {
        "recovery-group-name": "BillingApp",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
```

```
        }
    }
}
```

以下是儲存格就緒狀態變更的 Route 53 ARC 事件範例：

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller cell readiness status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:cell/PDXCell"
    ],
    "detail": {
        "cell-name": "PDXCell",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

以下是準備檢查狀態變更的 Route 53 ARC 事件範例：

```
{
    "version": "0",
    "account":"111122223333",
    "detail-type":"Route 53 Application Recovery Controller readiness check status
 change",
    "source":"route53-recovery-readiness.amazonaws.com",
    "time":"2020-11-03T00:31:54Z",
    "id": "1234a678-1b23-c123-12fd3f456e78",
    "region": "us-west-2",
    "resources":[
        "arn:aws:route53-recovery-readiness::111122223333:readiness-check/
UserTableReadinessCheck"
```

```
    ],
    "detail": {
    "readiness-check-name": "UserTableReadinessCheck",
        "previous-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        },
        "new-state": {
            "readiness-status": "READY|NOT_READY|UNKNOWN|NOT_AUTHORIZED"
        }
    }
}
```

指定要用作目標的 CloudWatch 記錄群組

建立 EventBridge 規則時，您必須指定傳送符合規則之事件的目標。如需的可用目標清單 EventBridge，請參閱 EventBridge 主控台中可用的目標。您可以新增至 EventBridge 規則的其中一個目標是 Amazon CloudWatch 日誌群組。本節說明將 CloudWatch 記錄群組新增為目標的需求，並提供在建立規則時新增記錄群組的程序。

若要將 CloudWatch 記錄群組新增為目標，您可以執行下列其中一項作業：

- 建立新的記錄群組
- 選擇現有的記錄群組

如果您在建立規則時使用主控台指定新的記錄群組， EventBridge 會自動為您建立記錄群組。請確定您用作 EventBridge 規則目標的記錄群組開頭為/aws/events。如果您想要選擇現有的記錄群組，請注意，只有開頭為的記錄群組/aws/events會顯示為下拉式功能表中的選項。如需詳細資訊，請參閱 Amazon CloudWatch 使用者指南中的建立新日誌群組。

如果您使用主控台外部的 CloudWatch 作業來建立或使用 CloudWatch 記錄群組做為目標，請確定您已正確設定權限。如果您使用主控台將記錄群組新增至 EventBridge 規則，則記錄群組的以資源為基礎的政策會自動更新。但是，如果您使用 AWS Command Line Interface 或 AWS SDK 來指定記錄群組，則必須更新記錄群組的以資源為基礎的原則。下列範例原則說明您必須在記錄群組的以資源為基礎的原則中定義的權限：

```
{
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
```

```
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:region:account:log-group:/aws/events/*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ],
  "Version": "2012-10-17"
}
```

您無法使用主控台為記錄群組設定以資源為基礎的政策。若要將必要的權限新增至以資源為基礎的策略，請使用 CloudWatch PutResource策略 API 作業。然後，您可以使用描述資源政策 CLI 命令來檢查您的策略是否已正確套用。

為資源事件建立規則並指定 CloudWatch 記錄群組目標

1. 在以下位置打開 Amazon EventBridge 控制台 https://console.aws.amazon.com/events/。
2. 選擇您 AWS 區域 要在其中建立規則的規則。
3. 選擇 [建立規則]，然後輸入有關該規則的任何資訊，例如事件模式或排程詳細資訊。

   如需建立整備程度 EventBridge 規則的詳細資訊，請參閱使用監視整備檢查資源 EventBridge。
4. 在 「選擇目標」 頁面上，選擇CloudWatch作為您的目標。
5. 從下拉式功能表中選擇 CloudWatch 記錄群組。

Identity and Access Management 以檢查整備程

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Route 53 ARC 資源。IAM 是您可以使用的 AWS 服務 ，無需額外付費。

目錄

- 服務龍中的準備程度如何檢查；與 IAM 合作
- Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

- 在 Route 53 ARC 中使用服務連結角色進行準備檢查
- AWS 在 Amazon Route 53 應用程式復原控制器中進行整備檢查的受管

服務龍中的準備程度如何檢查；與 IAM 合作

在您使用 IAM 管理 Route 53 ARC 的存取權限之前，請先了解哪些 IAM 功能可與 Route 53 ARC 搭配使用。

在 Amazon Route 53 應用程式復原控制器中使用 IAM 管理整備檢查的存取權限之前，請先了解哪些 IAM 功能可搭配整備檢查使用。

您可以在 Amazon Route 53 應用程式復原控制器中搭配整備檢查使用的 IAM 功能

IAM 功能	準備檢查支持
身分型政策	是
資源型政策	否
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	否
ABAC (政策中的標籤)	是
臨時憑證	是
主體許可	是
服務角色	否
服務連結角色	是

若要取得 AWS 服務如何搭配大多數 IAM 功能運作的高階整體檢視，請參閱 IAM 使用者指南中的搭配 IAM 使用的AWS 服務。

以身分識別為基礎的準備程度檢查

支援身分型政策	是

身分型政策是可以連接到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

使用 IAM 身分型政策，您可以指定允許或拒絕的動作和資源，以及在何種條件下允許或拒絕動作。您無法在身分型政策中指定主體，因為這會套用至連接的使用者或角色。如要了解您在 JSON 政策中使用的所有元素，請參閱《IAM 使用者指南》中的 IAM JSON 政策元素參考。

若要檢視 Route 53 ARC 身分識別型原則的範例，請參閱。Amazon Route 53 應用程式復原控制器中的身分識別型政策範例

整備檢查內的資源型政策

支援以資源基礎的政策	否

資源型政策是附加到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。

準備程度檢查的政策動作

支援政策動作	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼条件下可以對什麼資源執行哪些動作。

JSON 政策的 `Action` 元素描述您可以用來允許或拒絕政策中存取的動作。原則動作通常與關聯的 AWS API 作業具有相同的名稱。有一些例外狀況，例如沒有相符的 API 操作的僅限許可動作。也有一些作業需要政策中的多個動作。這些額外的動作稱為相依動作。

政策會使用動作來授予執行相關聯動作的許可。

若要查看 Route 53 ARC 動作以進行整備檢查的清單，請參閱服務授權參考中由 Amazon Route 53 復原準備程度定義的動作。

Route 53 ARC 中針對準備檢查的原則動作，請在動作之前使用下列前置詞：

```
route53-recovery-readiness
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，以下內容：

```
"Action": [
      "route53-recovery-readiness:action1",
      "route53-recovery-readiness:action2"
         ]
```

您也可以使用萬用字元 (*) 來指定多個動作。例如，若要指定開頭是 Describe 文字的所有動作，請包含以下動作：

```
"Action": "route53-recovery-readiness:Describe*"
```

若要檢視 Route 53 ARC 身分識別型原則以進行整備檢查的範例，請參閱。Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

準備程度檢查的政策資源

支援政策資源	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Resource JSON 政策元素可指定要套用動作的物件。陳述式必須包含 Resource 或 NotResource 元素。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。您可以針對支援特定資源類型的動作 (稱為資源層級許可) 來這麼做。

對於不支援資源層級許可的動作 (例如列出操作)，請使用萬用字元 (*) 來表示陳述式適用於所有資源。

```
"Resource": "*"
```

若要查看區域轉移的 Route 53 ARC 動作清單，請參閱 Amazon Route 53 復原準備程式定義的動作。

若要檢視 Route 53 ARC 身分識別型原則以進行整備檢查的範例，請參閱。Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

準備程度檢查的政策條件金鑰

支援服務特定政策條件金鑰	是

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

Condition 元素 (或 Condition 區塊) 可讓您指定使陳述式生效的條件。Condition 元素是選用項目。您可以建立使用條件運算子的條件運算式 (例如等於或小於)，來比對政策中的條件和請求中的值。

若您在陳述式中指定多個 Condition 元素，或是在單一 Condition 元素中指定多個索引鍵， AWS 會使用邏輯 AND 操作評估他們。如果您為單一條件索引鍵指定多個值，請使用邏輯OR運算來 AWS 評估條件。必須符合所有條件，才會授與陳述式的許可。

您也可以在指定條件時使用預留位置變數。例如，您可以只在使用者使用其 IAM 使用者名稱標記時，將存取資源的許可授予該 IAM 使用者。如需更多資訊，請參閱 IAM 使用者指南中的 IAM 政策元素：變數和標籤。

AWS 支援全域條件金鑰和服務特定條件金鑰。若要查看所有 AWS 全域條件金鑰，請參閱《IAM 使用者指南》中的AWS 全域條件內容金鑰。

若要查看 Route 53 ARC 動作以進行就緒檢查的清單，請參閱 Amazon Route 53 復原準備的條件金鑰

若要查看可與條件金鑰搭配整備檢查使用的動作和資源，請參閱 Amazon Route 53 復原準備程度定義的動作

若要檢視 Route 53 ARC 身分識別型原則以進行整備檢查的範例，請參閱。Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

整備檢查中的存取控制清單 (ACL)

支援 ACL	否

存取控制清單 (ACL) 可控制哪些主體 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

以屬性為基礎的存取控制 (ABAC)，含整備檢查

支援 ABAC (政策中的標籤)	部分

屬性型存取控制 (ABAC) 是一種授權策略，可根據屬性來定義許可。在中 AWS，這些屬性稱為標籤。您可以將標籤附加到 IAM 實體 (使用者或角色) 和許多 AWS 資源。為實體和資源加上標籤是 ABAC 的第一步。您接著要設計 ABAC 政策，允許在主體的標籤與其嘗試存取的資源標籤相符時操作。

ABAC 在成長快速的環境中相當有幫助，並能在政策管理變得繁瑣時提供協助。

若要根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件金鑰，在政策的條件元素中，提供標籤資訊。

如果服務支援每個資源類型的全部三個條件金鑰，則對該服務而言，值為 Yes。如果服務僅支援某些資源類型的全部三個條件金鑰，則值為 Partial。

如需 ABAC 的詳細資訊，請參閱《IAM 使用者指南》中的什麼是 ABAC?。如要查看含有設定 ABAC 步驟的教學課程，請參閱《IAM 使用者指南》中的使用屬性型存取控制 (ABAC)。

恢復準備（準備檢查）支持 ABAC。

使用臨時登入資料與整備檢查

支援臨時憑證	是

當您使用臨時憑據登錄時，某些 AWS 服務 不起作用。如需其他資訊，包括哪些 AWS 服務 與臨時登入資料搭配AWS 服務 使用，請參閱 IAM 使用者指南中的 IAM。

如果您使用除了使用者名稱和密碼以外的任何方法登入，則您正在 AWS Management Console 使用臨時認證。例如，當您 AWS 使用公司的單一登入 (SSO) 連結存取時，該程序會自動建立暫時認證。當您以使用者身分登入主控台，然後切換角色時，也會自動建立臨時憑證。如需切換角色的詳細資訊，請參閱《IAM 使用者指南》中的切換至角色 (主控台)。

您可以使用 AWS CLI 或 AWS API 手動建立臨時登入資料。然後，您可以使用這些臨時登入資料來存取 AWS。 AWS 建議您動態產生臨時登入資料，而不是使用長期存取金鑰。如需詳細資訊，請參閱 IAM 中的暫時性安全憑證。

整備程度檢查的跨服務主體權限

支援轉寄存取工作階段 (FAS)	是

當您使用 IAM 實體 (使用者或角色) 在中執行動作時 AWS，系統會將您視為主體。政策能將許可授予主體。當您使用某些服務時，您可能會執行一個動作，然後在不同的服務中觸發另一個動作。在此情況下，您必須具有執行這兩個動作的許可。

若要查看整備檢查中的動作是否需要政策中的其他相依動作，請參閱 Amazon Route 53 復原準備

整備程度檢查的服務角色

支援服務角色	否

服務角色是服務擔任的 IAM 角色，可代您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。

用於整備程度檢查的服務連結

支援服務連結角色	是

服務連結角色是一種連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需有關建立或管理 Route 53 ARC 服務連結角色的詳細資訊，請參閱在 Route 53 ARC 中使用服務連結角色進行準備檢查。

如需建立或管理服務連結角色的詳細資訊，請參閱可搭配 IAM 運作的AWS 服務。在表格中尋找服務，其中包含服務連結角色欄中的 Yes。選擇是連結，以檢視該服務的服務連結角色文件。

Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

根據預設，使用者和角色沒有建立或修改 Route 53 ARC 資源的權限。他們也無法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 來執行工作。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

若要了解如何使用這些範例 JSON 政策文件建立 IAM 身分型政策，請參閱《IAM 使用者指南》中的建立 IAM 政策。

如需 Route 53 ARC 定義的動作和資源類型的詳細資訊，包括每種資源類型的 ARN 格式，請參閱服務授權參考中的 Amazon Route 53 應用程式復原控制器的動作、資源和條件金鑰。

主題

- 政策最佳實務
- 範例：準備檢查主控台存取
- 範例：準備就緒檢查 API 動作以進行準備檢查

政策最佳實務

以身分識別為基礎的原則會決定某人是否可以在您的帳戶中建立、存取或刪除 Route 53 ARC 資源。這些動作可能會讓您的 AWS 帳戶產生費用。當您建立或編輯身分型政策時，請遵循下列準則及建議事項：

- 開始使用 AWS 受管原則並邁向最低權限權限 — 若要開始將權限授與使用者和工作負載，請使用可授與許多常見使用案例權限的AWS 受管理原則。它們可用在您的 AWS 帳戶. 建議您透過定義特定於您使用案例的 AWS 客戶管理政策，進一步降低使用權限。如需更多資訊，請參閱 IAM 使用者指南中的 AWS 受管政策或任務職能的AWS 受管政策。
- 套用最低許可許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的權限。為實現此目的，您可以定義在特定條件下可以對特定資源採取的動作，這也稱為最低權限許可。如需使用 IAM 套用許可的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 中的政策和許可。
- 使用 IAM 政策中的條件進一步限制存取權 – 您可以將條件新增至政策，以限制動作和資源的存取。例如，您可以撰寫政策條件，指定必須使用 SSL 傳送所有請求。您也可以使用條件來授與對服務動作的存取權 (如透過特定) 使用這些動作 AWS 服務，例如 AWS CloudFormation。如需更多資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策元素：條件。
- 使用 IAM Access Analyzer 驗證 IAM 政策，確保許可安全且可正常運作 – IAM Access Analyzer 驗證新政策和現有政策，確保這些政策遵從 IAM 政策語言 (JSON) 和 IAM 最佳實務。IAM Access Analyzer 提供 100 多項政策檢查及切實可行的建議，可協助您編寫安全且實用的政策。如需更多資訊，請參閱 IAM 使用者指南中的 IAM Access Analyzer 政策驗證。
- 需要多因素身份驗證 (MFA) — 如果您的案例需要 IAM 使用者或根使用者 AWS 帳戶，請開啟 MFA 以獲得額外的安全性。若要在呼叫 API 作業時請求 MFA，請將 MFA 條件新增至您的政策。如需更多資訊，請參閱 IAM 使用者指南中的設定 MFA 保護的 API 存取。

如需 IAM 中最佳實務的相關資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。

範例：準備檢查主控台存取

若要存取 Amazon Route 53 應用程式復原控制器主控台，您必須擁有最少的一組許可。這些權限必須允許您列出和查看有關 Route 53 ARC 資源的詳細信息 AWS 帳戶。如果您建立比最基本必要許可更嚴格的身分型政策，則對於具有該政策的實體 (使用者或角色) 而言，主控台就無法如預期運作。

您不需要為僅對 AWS CLI 或 AWS API 進行呼叫的使用者允許最低主控台權限。反之，只需允許存取符合他們嘗試執行之 API 操作的動作就可以了。

若要確保使用者和角色在您僅允許存取特定 API 作業時仍可使用整備檢查主控台，請同時將`ReadOnly` AWS 受管理的原則以進行整備檢查附加至實體。如需詳細資訊，請參閱 IAM 使用者指南中的整備檢查整備檢查受管政策頁面或向使用者新增許可。

若要執行某些工作，使用者必須擁有建立與 Route 53 ARC 中整備檢查相關聯的服務連結角色的權限。如需進一步了解，請參閱在 Route 53 ARC 中使用服務連結角色進行準備檢查。

若要讓使用者透過主控台完整存取使用整備檢查功能，請將下列原則附加至使用者：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                   "route53-recovery-readiness:CreateCell",
                   "route53-recovery-readiness:CreateCrossAccountAuthorization",
                   "route53-recovery-readiness:CreateReadinessCheck",
                   "route53-recovery-readiness:CreateRecoveryGroup",
                   "route53-recovery-readiness:CreateResourceSet",
                   "route53-recovery-readiness:DeleteCell",
                   "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                   "route53-recovery-readiness:DeleteReadinessCheck",
                   "route53-recovery-readiness:DeleteRecoveryGroup",
                   "route53-recovery-readiness:DeleteResourceSet",
                   "route53-recovery-readiness:GetArchitectureRecommendations",
                   "route53-recovery-readiness:GetCell",
                   "route53-recovery-readiness:GetCellReadinessSummary",
                   "route53-recovery-readiness:GetReadinessCheck",
                   "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                   "route53-recovery-readiness:GetReadinessCheckStatus",
```

```
                    "route53-recovery-readiness:GetRecoveryGroup",
                    "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                    "route53-recovery-readiness:GetResourceSet",
                    "route53-recovery-readiness:ListCells",
                    "route53-recovery-readiness:ListCrossAccountAuthorizations",
                    "route53-recovery-readiness:ListReadinessChecks",
                    "route53-recovery-readiness:ListRecoveryGroups",
                    "route53-recovery-readiness:ListResourceSets",
                    "route53-recovery-readiness:ListRules",
                    "route53-recovery-readiness:UpdateCell",
                    "route53-recovery-readiness:UpdateReadinessCheck",
                    "route53-recovery-readiness:UpdateRecoveryGroup",
                    "route53-recovery-readiness:UpdateResourceSet"
                ],
                "Resource": "*"
            }
        ]
}
```

範例：準備就緒檢查 API 動作以進行準備檢查

若要確保使用者可以使用 Route 53 ARC API 動作來處理 Route 53 ARC 準備檢查控制平面 (例如，建立復原群組、資源集和整備檢查)，請附加與使用者需要使用的 API 作業對應的原則，如下所述。

若要執行某些工作，使用者必須擁有建立與 Route 53 ARC 中整備檢查相關聯的服務連結角色的權限。如需進一步了解，請參閱在 Route 53 ARC 中使用服務連結角色進行準備檢查。

要使用 API 操作進行準備檢查，請將類似以下的策略附加給用戶：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                    "route53-recovery-readiness:CreateCell",
                    "route53-recovery-readiness:CreateCrossAccountAuthorization",
                    "route53-recovery-readiness:CreateReadinessCheck",
                    "route53-recovery-readiness:CreateRecoveryGroup",
                    "route53-recovery-readiness:CreateResourceSet",
                    "route53-recovery-readiness:DeleteCell",
                    "route53-recovery-readiness:DeleteCrossAccountAuthorization",
                    "route53-recovery-readiness:DeleteReadinessCheck",
```

```
                    "route53-recovery-readiness:DeleteRecoveryGroup",
                    "route53-recovery-readiness:DeleteResourceSet",
                    "route53-recovery-readiness:GetArchitectureRecommendations",
                    "route53-recovery-readiness:GetCell",
                    "route53-recovery-readiness:GetCellReadinessSummary",
                    "route53-recovery-readiness:GetReadinessCheck",
                    "route53-recovery-readiness:GetReadinessCheckResourceStatus",
                    "route53-recovery-readiness:GetReadinessCheckStatus",
                    "route53-recovery-readiness:GetRecoveryGroup",
                    "route53-recovery-readiness:GetRecoveryGroupReadinessSummary",
                    "route53-recovery-readiness:GetResourceSet",
                    "route53-recovery-readiness:ListCells",
                    "route53-recovery-readiness:ListCrossAccountAuthorizations",
                    "route53-recovery-readiness:ListReadinessChecks",
                    "route53-recovery-readiness:ListRecoveryGroups",
                    "route53-recovery-readiness:ListResourceSets",
                    "route53-recovery-readiness:ListRules",
                    "route53-recovery-readiness:ListTagsForResources",
                    "route53-recovery-readiness:UpdateCell",
                    "route53-recovery-readiness:UpdateReadinessCheck",
                    "route53-recovery-readiness:UpdateRecoveryGroup",
                    "route53-recovery-readiness:UpdateResourceSet",
                    "route53-recovery-readiness:TagResource",
                    "route53-recovery-readiness:UntagResource"
                ],
                "Resource": "*"
            }
        ]
}
```

在 Route 53 ARC 中使用服務連結角色進行準備檢查

Amazon Route 53 應用程式復原控制器使用 AWS Identity and Access Management (IAM) 服務連結角色。服務連結角色是直接連結至服務的唯一 IAM 角色類型，在本例中為 Route 53 ARC。服務連結角色由 Route 53 ARC 預先定義，並包含服務為特定目的代表您呼叫其他 AWS 服務所需的所有權限。

服務連結角色可讓您更輕鬆地設定 Route 53 ARC，因為您不需要手動新增必要的權限。Route 53 ARC 定義了其服務鏈接角色的權限，除非另有定義，否則只有 Route 53 ARC 可以擔任其角色。定義的許可包括信任政策和許可政策，且該許可政策無法附加至其他 IAM 實體。

您必須先刪除角色的相關資源，才能刪除服務連結角色。這可以保護您的 Route 53 ARC 資源，因為您無法不小心移除存取資源的權限。

如需其他支援服務連結角色之服AWS 務的相關資訊，請參閱搭配 IAM 使用的服務，並在服務連結角色欄中尋找具有 Yes 的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

Route 53 ARC 具有下列服務連結角色，本章將說明這些角色：

- Route 53 ARC 使用名為 Route53 的服務連結角色RecoveryReadinessServiceRolePolicy來存取資源和組態以檢查準備情況。
- Route 53 ARC 使用名為自動班次實務執行的服務連結角色，監控客戶提供的 Amazon CloudWatch 警示和客戶 AWS Health Dashboard 事件，並開始執行實務。

Route53 的服務連結角色權限 RecoveryReadinessServiceRolePolicy

Route 53 ARC 使用名為 Route53 的服務連結角色RecoveryReadinessServiceRolePolicy來存取資源和組態以檢查準備情況。本節說明服務連結角色的權限，以及建立、編輯和刪除角色的相關資訊。

Route53 的服務連結角色權限 RecoveryReadinessServiceRolePolicy

此服務連結角色使用受管理策略`Route53RecoveryReadinessServiceRolePolicy`。

Route53 服RecoveryReadinessServiceRolePolicy務連結角色會信任下列服務來擔任此角色：

- `route53-recovery-readiness.amazonaws.com`

若要檢視此原則的權限，請參閱AWS 受管理的原則參考RecoveryReadinessServiceRolePolicy中的Route53。

您必須設定許可，IAM 實體 (如使用者、群組或角色) 才可建立、編輯或刪除服務連結角色。如需詳細資訊，請參閱 IAM 使用者指南中的服務連結角色許可。

為路線 53 ARC 建立 Route 53 由 53 RecoveryReadinessServiceRolePolicy 服務連結角色

您不需要手動建立 Route53 RecoveryReadinessServiceRolePolicy 服務連結角色。當您在 AWS Management Console、或 AWS API 中建立第一個整備檢查或跨帳戶授權時 AWS CLI，Route 53 ARC 會為您建立服務連結角色。

若您刪除此服務連結角色，之後需要再次建立，您可以在帳戶中使用相同程序重新建立角色。當您建立第一個整備檢查或跨帳戶授權時，Route 53 ARC 會再次為您建立服務連結角色。

編輯路線 53 ARC 的 Route 53 由 53 RecoveryReadinessServiceRolePolicy 服務連結角色

路由 53 ARC 不允許您編輯路由 53 RecoveryReadinessServiceRolePolicy 服務連結的角色。建立服務連結角色之後，您無法變更角色的名稱，因為其他實體可能會參照該角色。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱 IAM 使用者指南中的編輯服務連結角色。

刪除路由 53 ARC 的 Route 53 由 53 RecoveryReadinessServiceRolePolicy 服務連結角色

若您不再使用需要服務連結角色的功能或服務，我們建議您刪除該角色。如此一來，您就沒有未主動監控或維護的未使用實體。然而，在手動刪除服務連結角色之前，您必須先清除資源。

移除整備檢查和跨帳戶授權後，您可以刪除 Route RecoveryReadinessServiceRolePolicy 53 服務連結角色。如需整備檢查的詳細資訊，請參閱Amazon 路線 53 應用程序恢復控制器中的準備。如需跨帳戶授權的詳細資訊，請參閱。在 Route 53 ARC 中創建跨帳戶授權

> **Note**
>
> 如果 Route 53 ARC 服務在您嘗試刪除資源時使用該角色，則服務角色刪除可能會失敗。如果發生這種情況，請等待幾分鐘，然後再次嘗試刪除角色。

使用 IAM 手動刪除服務連結角色

使用 IAM 主控台或 AWS API 刪除 Route53 RecoveryReadinessServiceRolePolicy 服務連結角色。AWS CLI如需詳細資訊，請參閱《IAM 使用者指南》中的刪除服務連結角色。

Route 53 ARC 服務連結角色的更新，以進行整備檢查

如需 Route 53 ARC 服務連結角色之 AWS 受管理原則的更新，請參閱 Route 53 ARC 的AWS 受管理原則更新表格。您也可以在 Route 53 ARC 文件歷史記錄頁面上訂閱自動 RSS 警示。

AWS 在 Amazon Route 53 應用程式復原控制器中進行整備檢查的受管

受 AWS 管理的策略是由建立和管理的獨立策略 AWS。 AWS 受管理的策略旨在為許多常見使用案例提供權限，以便您可以開始將權限指派給使用者、群組和角色。

請記住， AWS 受管理的政策可能不會為您的特定使用案例授與最低權限權限，因為這些權限可供所有 AWS 客戶使用。我們建議您定義使用案例專屬的客戶管理政策，以便進一步減少許可。

您無法變更受 AWS 管理策略中定義的權限。如果 AWS 更新 AWS 受管理原則中定義的權限，則此更新會影響附加原則的所有主體識別 (使用者、群組和角色)。 AWS 當新的啟動或新 AWS 服務 的 API 操作可用於現有服務時，最有可能更新 AWS 受管理策略。

如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS 受管政策。

AWS 管理策略：路由 53 RecoveryReadinessServiceRolePolicy

您不得將 Route53RecoveryReadinessServiceRolePolicy 連接到 IAM 實體。此政策附加至服務連結角色，可讓 Amazon Route 53 應用程式復原控制器存取 Route 53 ARC 使用或管理的 AWS 服務和資源。如需詳細資訊，請參閱 在 Route 53 ARC 中使用服務連結角色進行準備檢查。

AWS 受管理的策略： AmazonRoute53 RecoveryReadinessFullAccess

您可以將 AmazonRoute53RecoveryReadinessFullAccess 連接到 IAM 實體。此政策授予完整存取 Route 53 ARC 中使用復原準備程度 (整備檢查) 的動作。將其附加至需要完整存取復原整備動作的 IAM 使用者和其他主體。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryReadinessFullAccess的策略參考中的AmazonRoute53。

AWS 受管理的策略： AmazonRoute53 RecoveryReadinessReadOnlyAccess

您可以將 AmazonRoute53RecoveryReadinessReadOnlyAccess 連接到 IAM 實體。此原則授與在 Route 53 ARC 中使用復原準備程度的動作的唯讀存取權。對於需要檢視整備狀態和復原群組組態的使用者而言，此功能非常有用。這些使用者無法建立、更新或刪除復原整備資源。

若要檢視此原則的權限，請參閱AWS 受管理RecoveryReadinessReadOnlyAccess的策略參考中的AmazonRoute53。

準備就緒的 AWS 受管政策更新

如需 Route 53 ARC 自此服務開始追蹤這些變更以來，針對準備就緒檢查的 AWS 受管政策更新的詳細資訊，請參閱Amazon Route 53 應用程式復原控制器的 AWS 受管政策更新。如需有關此頁面變更的自動警示，請訂閱 Route 53 ARC 文件歷史記錄頁面上的 RSS 摘要。

準備檢查配額

Amazon Route 53 應用程式復原控制器中的準備程度檢查必須遵守下列配額 (先前稱為限制)。

實體	配額
每個帳戶的復原群組數目	5
每個帳戶的儲存格數	15

實體	配額
每個儲存格的巢狀儲存格數	3
每個復原群組的儲存格數	3
每個儲存格的資源數	10
每個復原群組的資源數目	10
每個資源集的資源數	6
每個帳號的資源集數	200
每個帳戶的整備檢查次數	200
跨帳戶授權數	100

使用 AWS SDK 的應用程序恢復控制器的代碼示例

下列程式碼範例說明如何搭配 AWS 軟體開發套件 (SDK) 使用應用程式復原控制器。

Actions 是大型程式的程式碼摘錄，必須在內容中執行。雖然動作會告訴您如何呼叫個別服務函數，但您可以在其相關情境和跨服務範例中查看內容中的動作。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用此服務。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

程式碼範例

- 使用 AWS SDK 的應用程序恢復控制器的操作
  - 搭GetRoutingControlState配 AWS 開發套件或 CLI 使用
  - 搭UpdateRoutingControlState配 AWS 開發套件或 CLI 使用

使用 AWS SDK 的應用程序恢復控制器的操作

下列程式碼範例示範如何使用 AWS SDK 執行個別應用程式復原控制器動作。這些摘錄會呼叫應用程式復原控制器 API，而且是來自必須在內容中執行的大型程式碼摘錄。每個範例都包含一個連結 GitHub，您可以在其中找到設定和執行程式碼的指示。

下列範例僅包含最常使用的動作。如需完整清單，請參閱 Amazon Route 53 應用程式復原控制器 API 參考資料。

範例

- 搭GetRoutingControlState配 AWS 開發套件或 CLI 使用
- 搭UpdateRoutingControlState配 AWS 開發套件或 CLI 使用

搭`GetRoutingControlState`配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用`GetRoutingControlState`。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static GetRoutingControlStateResponse
 getRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn) {
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region())).build();
                return client.getRoutingControlState(
                        GetRoutingControlStateRequest.builder()
                                .routingControlArn(routingControlArn).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考GetRoutingControlState中的。

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
import boto3


def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def get_routing_control_state(routing_control_arn, cluster_endpoints):
    """
    Gets the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to look up.
    :param cluster_endpoints: The list of cluster endpoints to query.
    :return: The routing control state response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
```

```
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.get_routing_control_state(
                RoutingControlArn=routing_control_arn
            )
            return response
        except Exception as error:
            print(error)
            raise error
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件GetRoutingControlState中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用此服務。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

搭UpdateRoutingControlState配 AWS 開發套件或 CLI 使用

下列程式碼範例會示範如何使用UpdateRoutingControlState。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在AWS 設定和執行程式碼範例儲存庫。

```
    public static UpdateRoutingControlStateResponse
updateRoutingControlState(List<ClusterEndpoint> clusterEndpoints,
            String routingControlArn,
            String routingControlState) {
```

```
        // As a best practice, we recommend choosing a random cluster endpoint to
 get or
        // set routing control states.
        // For more information, see
        // https://docs.aws.amazon.com/r53recovery/latest/dg/route53-arc-best-
practices.html#route53-arc-best-practices.regional
        Collections.shuffle(clusterEndpoints);
        for (ClusterEndpoint clusterEndpoint : clusterEndpoints) {
            try {
                System.out.println(clusterEndpoint);
                Route53RecoveryClusterClient client =
 Route53RecoveryClusterClient.builder()
                        .endpointOverride(URI.create(clusterEndpoint.endpoint()))
                        .region(Region.of(clusterEndpoint.region()))
                        .build();
                return client.updateRoutingControlState(
                        UpdateRoutingControlStateRequest.builder()

 .routingControlArn(routingControlArn).routingControlState(routingControlState).build());
            } catch (Exception exception) {
                System.out.println(exception);
            }
        }
        return null;
    }
```

- 如需 API 詳細資訊，請參閱 AWS SDK for Java 2.x API 參考[UpdateRoutingControlState](中的。)

Python

適用於 Python (Boto3) 的 SDK

> **Note**
>
> 還有更多關於 GitHub。尋找完整範例，並了解如何在[AWS 設定和執行程式碼範例儲存庫](。)

```
import boto3
```

```
def create_recovery_client(cluster_endpoint):
    """
    Creates a Boto3 Route 53 Application Recovery Controller client for the
 specified
    cluster endpoint URL and AWS Region.

    :param cluster_endpoint: The cluster endpoint URL and Region.
    :return: The Boto3 client.
    """
    return boto3.client(
        "route53-recovery-cluster",
        endpoint_url=cluster_endpoint["Endpoint"],
        region_name=cluster_endpoint["Region"],
    )



def update_routing_control_state(
    routing_control_arn, cluster_endpoints, routing_control_state
):
    """
    Updates the state of a routing control. Cluster endpoints are tried in
    sequence until the first successful response is received.

    :param routing_control_arn: The ARN of the routing control to update the
 state for.
    :param cluster_endpoints: The list of cluster endpoints to try.
    :param routing_control_state: The new routing control state.
    :return: The routing control update response.
    """

    # As a best practice, we recommend choosing a random cluster endpoint to get
 or set routing control states.
    # For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    random.shuffle(cluster_endpoints)
    for cluster_endpoint in cluster_endpoints:
        try:
            recovery_client = create_recovery_client(cluster_endpoint)
            response = recovery_client.update_routing_control_state(
                RoutingControlArn=routing_control_arn,
                RoutingControlState=routing_control_state,
```

```
            )
            return response
        except Exception as error:
            print(error)
```

- 如需 API 的詳細資訊，請參閱AWS 開發套件UpdateRoutingControlState中的 Python (博托 3) API 參考。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱搭配 AWS SDK 使用此服務。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

Amazon Route 53 應用程序恢復控制器中

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，這些架構是為了滿足對安全性最敏感的組織的需求而建置的。

安全是 AWS 與您之間共同的責任。共同責任模型將其描述為雲端的安全性和雲端中的安全性：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。若要了解適用於 Amazon Route 53 應用程式復原控制器的合規計劃，請參閱AWS 合規計劃的合規計劃AWS 服務範的服務。
- 雲端中的安全性 — 您的責任取決於您使用的 AWS 服務。您也必須對其他因素負責，包括資料的機密性、您公司的要求和適用法律和法規。

本文件可協助您瞭解如何在使用 Route 53 ARC 時套用共同的責任模型。下列主題說明如何設定 Route 53 ARC 以符合您的安全性和合規性目標。您還將學習如何使用其他 AWS 服務來幫助您監控和保護 Route 53 ARC 資源。

主題

- Amazon Route 53 應用程式復原控制器中的資料
- Amazon Route 53 應用程式復原控制器的 Identity and Access Management
- Amazon Route 53 應用程式復原控制器中的記錄和
- Amazon Route 53 應用程式復原控制器的合規驗證
- Amazon Route 53 應用程序恢復控制器中
- Amazon Route 53 應用程式復原控制器的基礎

Amazon Route 53 應用程式復原控制器中的資料

AWS 共同責任模型適用於 Amazon Route 53 應用程式復原控制器中的資料保護。如此模型所述，AWS 負責保護執行所有 AWS 雲端. 您負責維護在此基礎設施上託管內容的控制權。您也同時負責所使用 AWS 服務 的安全組態和管理任務。如需資料隱私權的詳細資訊，請參閱資料隱私權常見問答集。如需有關歐洲資料保護的相關資訊，請參閱 AWS 安全性部落格上的 AWS 共同的責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者。如此一來，每個使用者都只會獲得授與完成其任務所必須的許可。我們也建議您採用下列方式保護資料：

- 每個帳戶均要使用多重要素驗證 (MFA)。
- 使用 SSL/TLS 與 AWS 資源進行通訊。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 使用設定 API 和使用者活動記錄 AWS CloudTrail。
- 使用 AWS 加密解決方案，以及其中的所有默認安全控制 AWS 服務。
- 使用進階的受管安全服務 (例如 Amazon Macie)，協助探索和保護儲存在 Amazon S3 的敏感資料。
- 如果透過命令列介面或 API 存取時需要經 AWS 過 FIPS 140-2 驗證的加密模組，請使用 FIPS 端點。如需有關 FIPS 和 FIPS 端點的更多相關資訊，請參閱聯邦資訊處理標準 (FIPS) 140-2 概觀。

我們強烈建議您絕對不要將客戶的電子郵件地址等機密或敏感資訊，放在標籤或自由格式的文字欄位中，例如名稱欄位。這包括當您使用控制台，API 或 AWS SDK AWS 服務 使用 Route 53 ARC 或其他方式時。 AWS CLI您在標籤或自由格式文字欄位中輸入的任何資料都可能用於計費或診斷日誌。如果您提供外部伺服器的 URL，我們強烈建議請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

靜態加密

客戶組態資訊會儲存在服務擁有的 Amazon DynamoDB 全域表中，並在靜態時加密。

包含 Route 53 ARC 叢集中儲存格狀態的資料集會寫入 Amazon EBS 磁碟區進行備份。Route 53 ARC 會在資料靜態時使用預設的 Amazon EBS 加密。

傳輸中加密

客戶要求與回應 (Route 53 ARC 組態、就緒狀態查詢、儲存格狀態更新等) 會在整個服務的傳輸期間使用 TLS 加密。

Amazon Route 53 應用程式復原控制器的 Identity and Access Management

AWS Identity and Access Management (IAM) 可協助系統管理員安全地控制 AWS 資源存取權。 AWS 服務 IAM 管理員控制哪些人可以驗證 (登入) 和授權 (具有權限) 以使用 Route 53 ARC 資源。您可以使用 IAM AWS 服務 ，無需額外付費。

物件

根據您在 Route 53 ARC 中所做的工作，使用方式 AWS Identity and Access Management (IAM) 會有所不同。

服務使用者 — 如果您使用 Route 53 ARC 服務來執行工作，則管理員會為您提供所需的認證和權限。當您使用更多 Route 53 ARC 功能來完成工作時，您可能需要額外的權限。了解存取許可的管理方式可協助您向管理員請求正確的許可。如果您無法在 Route 53 ARC 中存取特徵，請參閱疑難排解 Amazon Route 53 應用程式復原控制器的身分。

服務管理員 — 如果您負責公司的 Route 53 ARC 資源，您可能擁有對 Route 53 ARC 的完整存取權。決定您的服務使用者應該存取哪些 Route 53 ARC 功能和資源是您的工作。接著，您必須將請求提交給您的 IAM 管理員，來變更您服務使用者的許可。檢閱此頁面上的資訊，了解 IAM 的基本概念。若要進一步了解貴公司如何將 IAM 與 Route 53 ARC 搭配使用，請參閱亞馬遜路線 53 應用程式復原控制器功能如何與 IAM 搭配。

IAM 管理員 — 如果您是 IAM 管理員，您可能想要瞭解如何撰寫政策來管理 Route 53 ARC 存取權的詳細資訊。若要檢視可在 IAM 中使用的 Route 53 ARC 身分型政策範例，請參閱。Amazon Route 53 應用程式復原控制器中的身分識別型政策範例

使用身分驗證

驗證是您 AWS 使用身分認證登入的方式。您必須以 IAM 使用者身分或假設 IAM 角色進行驗證 (登入 AWS)。 AWS 帳戶根使用者

您可以使用透過 AWS 身分識別來源提供的認證，以聯合身分識別身分登入。 AWS IAM Identity Center (IAM 身分中心) 使用者、貴公司的單一登入身分驗證，以及您的 Google 或 Facebook 登入資料都是聯合身分識別的範例。您以聯合身分登入時，您的管理員先前已設定使用 IAM 角色的聯合身分。當您使 AWS 用同盟存取時，您會間接擔任角色。

根據您的使用者類型，您可以登入 AWS Management Console 或 AWS 存取入口網站。如需登入的詳細資訊 AWS，請參閱AWS 登入 使用者指南中的如何登入您 AWS 帳戶的。

如果您 AWS 以程式設計方式存取，請 AWS 提供軟體開發套件 (SDK) 和命令列介面 (CLI)，以使用您的認證以加密方式簽署要求。如果您不使用 AWS 工具，則必須自行簽署要求。如需使用建議的方法自行簽署請求的詳細資訊，請參閱 IAM 使用者指南中的簽署 AWS API 請求。

無論您使用何種身分驗證方法，您可能都需要提供額外的安全性資訊。例如， AWS 建議您使用多重要素驗證 (MFA) 來增加帳戶的安全性。如需更多資訊，請參閱 AWS IAM Identity Center 使用者指南中的多重要素驗證和 IAM 使用者指南中的在 AWS中使用多重要素驗證 (MFA)。

AWS 帳戶 根使用者

建立時 AWS 帳戶，您會從一個登入身分開始，該身分可完整存取該帳戶中的所有資源 AWS 服務 和資源。此身分稱為 AWS 帳戶 root 使用者，可透過使用您用來建立帳戶的電子郵件地址和密碼登入來存取。強烈建議您不要以根使用者處理日常任務。保護您的根使用者憑證，並將其用來執行只能由根使用者執行的任務。如需這些任務的完整清單，了解需以根使用者登入的任務，請參閱 IAM 使用者指南中的需要根使用者憑證的任務。

聯合身分

最佳作法是要求人類使用者 (包括需要系統管理員存取權的使用者) 使用與身分識別提供者的同盟，才能使用臨時認證 AWS 服務 來存取。

聯合身分識別是來自企業使用者目錄的使用者、Web 身分識別提供者、Identi ty Center 目錄，或使用透過身分識別來源提供的認證進行存取 AWS 服務 的任何使用者。 AWS Directory Service同盟身分存取時 AWS 帳戶，他們會假設角色，而角色則提供臨時認證。

對於集中式存取權管理，我們建議您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中建立使用者和群組，也可以連線並同步到自己身分識別來源中的一組使用者和群組，以便在所有應用程式 AWS 帳戶 和應用程式中使用。如需 IAM Identity Center 的相關資訊，請參閱 AWS IAM Identity Center 使用者指南中的什麼是 IAM Identity Center？。

IAM 使用者和群組

IAM 使用者是您內部的身分，具 AWS 帳戶 有單一人員或應用程式的特定許可。建議您盡可能依賴暫時憑證，而不是擁有建立長期憑證 (例如密碼和存取金鑰) 的 IAM 使用者。但是如果特定使用案例需要擁有長期憑證的 IAM 使用者，建議您輪換存取金鑰。如需更多資訊，請參閱 IAM 使用者指南中的為需要長期憑證的使用案例定期輪換存取金鑰。

IAM 群組是一種指定 IAM 使用者集合的身分。您無法以群組身分簽署。您可以使用群組來一次為多名使用者指定許可。群組可讓管理大量使用者許可的程序變得更為容易。例如，您可以擁有一個名為 IAMAdmins 的群組，並給予該群組管理 IAM 資源的許可。

使用者與角色不同。使用者只會與單一人員或應用程式建立關聯，但角色的目的是在由任何需要它的人員取得。使用者擁有永久的長期憑證，但角色僅提供暫時憑證。如需進一步了解，請參閱 IAM 使用者指南中的建立 IAM 使用者 (而非角色) 的時機。

IAM 角色

IAM 角色是您 AWS 帳戶 內部具有特定許可的身分。它類似 IAM 使用者，但不與特定的人員相關聯。您可以切換角色，在中暫時擔任 IAM 角色。 AWS Management Console 您可以透過呼叫 AWS CLI 或

AWS API 作業或使用自訂 URL 來擔任角色。如需使用角色的方法更多相關資訊，請參閱 IAM 使用者指南中的使用 IAM 角色。

使用暫時憑證的 IAM 角色在下列情況中非常有用：

- 聯合身分使用者存取 – 若要向聯合身分指派許可，請建立角色，並為角色定義許可。當聯合身分進行身分驗證時，該身分會與角色建立關聯，並獲授予由角色定義的許可。如需有關聯合角色的相關資訊，請參閱 IAM 使用者指南中的為第三方身分提供者建立角色。如果您使用 IAM Identity Center，則需要設定許可集。為控制身分驗證後可以存取的內容，IAM Identity Center 將許可集與 IAM 中的角色相關聯。如需有關許可集的資訊，請參閱 AWS IAM Identity Center 使用者指南中的許可集。
- 暫時 IAM 使用者許可 – IAM 使用者或角色可以擔任 IAM 角色來暫時針對特定任務採用不同的許可。
- 跨帳戶存取權 – 您可以使用 IAM 角色，允許不同帳戶中的某人 (信任的委託人) 存取您帳戶中的資源。角色是授予跨帳戶存取權的主要方式。但是，對於某些策略 AWS 服務，您可以將策略直接附加到資源（而不是使用角色作為代理）。若要了解跨帳戶存取權角色和資源型政策間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源類型政策的差異。
- 跨服務訪問 — 有些 AWS 服務 使用其他 AWS 服務功能。例如，當您在服務中進行呼叫時，該服務通常會在 Amazon EC2 中執行應用程式或將物件儲存在 Amazon Simple Storage Service (Amazon S3) 中。服務可能會使用呼叫主體的許可、使用服務角色或使用服務連結角色來執行此作業。
  - 轉寄存取工作階段 (FAS) — 當您使用 IAM 使用者或角色在中執行動作時 AWS，您會被視為主體。使用某些服務時，您可能會執行某個動作，進而在不同服務中啟動另一個動作。FAS 會使用主體呼叫的權限 AWS 服務，並結合要求 AWS 服務 向下游服務發出要求。只有當服務收到需要與其 AWS 服務 他資源互動才能完成的請求時，才會發出 FAS 請求。在此情況下，您必須具有執行這兩個動作的許可。如需提出 FAS 請求時的政策詳細資訊，請參閱《轉發存取工作階段》。
  - 服務角色 – 服務角色是服務擔任的 IAM 角色，可代表您執行動作。IAM 管理員可以從 IAM 內建立、修改和刪除服務角色。如需更多資訊，請參閱 IAM 使用者指南中的建立角色以委派許可給 AWS 服務。
  - 服務連結角色 — 服務連結角色是連結至. AWS 服務服務可以擔任代表您執行動作的角色。服務連結角色會顯示在您的中， AWS 帳戶 且屬於服務所有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。
- 在 Amazon EC2 上執行的應用程式 — 您可以使用 IAM 角色來管理在 EC2 執行個體上執行的應用程式以及發出 AWS CLI 或 AWS API 請求的臨時登入資料。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體設定檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得暫時憑證。如需更多資訊，請參閱 IAM 使用者指南中的利用 IAM 角色來授予許可給 Amazon EC2 執行個體上執行的應用程式。

若要了解是否要使用 IAM 角色或 IAM 使用者，請參閱 IAM 使用者指南中的建立 IAM 角色 (而非使用者) 的時機。

使用政策管理存取權

您可以透 AWS 過建立原則並將其附加至 AWS 身分識別或資源來控制中的存取。原則是一個物件 AWS ，當與身分識別或資源相關聯時，會定義其權限。 AWS 當主參與者 (使用者、root 使用者或角色工作階段) 提出要求時，評估這些原則。政策中的許可決定是否允許或拒絕請求。大多數原則會 AWS 以 JSON 文件的形式儲存在中。如需 JSON 政策文件結構和內容的更多相關資訊，請參閱 IAM 使用者指南中的 JSON 政策概觀。

管理員可以使用 AWS JSON 政策來指定誰可以存取哪些內容。也就是說，哪個主體在什麼條件下可以對什麼資源執行哪些動作。

預設情況下，使用者和角色沒有許可。若要授予使用者對其所需資源執行動作的許可，IAM 管理員可以建立 IAM 政策。然後，管理員可以將 IAM 政策新增至角色，使用者便能擔任這些角色。

IAM 政策定義該動作的許可，無論您使用何種方法來執行操作。例如，假設您有一個允許 `iam:GetRole` 動作的政策。具有該原則的使用者可以從 AWS Management Console AWS CLI、或 AWS API 取得角色資訊。

身分型政策

身分型政策是可以附加到身分 (例如 IAM 使用者、使用者群組或角色) 的 JSON 許可政策文件。這些政策可控制身分在何種條件下能對哪些資源執行哪些動作。若要了解如何建立身分類型政策，請參閱 IAM 使用者指南中的建立 IAM 政策。

身分型政策可進一步分類成內嵌政策或受管政策。內嵌政策會直接內嵌到單一使用者、群組或角色。受管理的策略是獨立策略，您可以將其附加到您的 AWS 帳戶. 受管政策包括 AWS 受管政策和客戶管理的策略。若要了解如何在受管政策及內嵌政策間選擇，請參閱 IAM 使用者指南中的在受管政策和內嵌政策間選擇。

資源型政策

資源型政策是連接到資源的 JSON 政策文件。資源型政策的最常見範例是 IAM 角色信任政策和 Amazon S3 儲存貯體政策。在支援資源型政策的服務中，服務管理員可以使用它們來控制對特定資源的存取權限。對於附加政策的資源，政策會定義指定的主體可以對該資源執行的動作以及在何種條件下執行的動作。您必須在資源型政策中指定主體。主參與者可以包括帳戶、使用者、角色、同盟使用者或。 AWS 服務

資源型政策是位於該服務中的內嵌政策。您無法在以資源為基礎的政策中使用 IAM 的 AWS 受管政策。

存取控制清單 (ACL)

存取控制清單 (ACL) 可控制哪些委託人 (帳戶成員、使用者或角色) 擁有存取某資源的許可。ACL 類似於資源型政策，但它們不使用 JSON 政策文件格式。

Amazon S3 和 Amazon VPC 是支援 ACL 的服務範例。 AWS WAF若要進一步了解 ACL，請參閱 Amazon Simple Storage Service 開發人員指南中的存取控制清單 (ACL) 概觀。

其他政策類型

AWS 支援其他較不常見的原則類型。這些政策類型可設定較常見政策類型授予您的最大許可。

- 許可界限 – 許可範圍是一種進階功能，可供您設定身分型政策能授予 IAM 實體 (IAM 使用者或角色) 的最大許可。您可以為實體設定許可界限。所產生的許可會是實體的身分型政策和其許可界限的交集。會在 `Principal` 欄位中指定使用者或角色的資源型政策則不會受到許可界限限制。所有這類政策中的明確拒絕都會覆寫該允許。如需許可範圍的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 實體許可範圍。
- 服務控制策略（SCP）— SCP 是 JSON 策略，用於指定中組織或組織單位（OU）的最大權限。AWS Organizations AWS Organizations 是一種用於分組和集中管理您企業擁 AWS 帳戶 有的多個服務。若您啟用組織中的所有功能，您可以將服務控制政策 (SCP) 套用到任何或所有帳戶。SCP 限制成員帳戶中實體的權限，包括每個 AWS 帳戶根使用者帳戶。如需組織和 SCP 的更多相關資訊，請參閱 AWS Organizations 使用者指南中的 SCP 運作方式。
- 工作階段政策 – 工作階段政策是一種進階政策，您可以在透過編寫程式的方式建立角色或聯合使用者的暫時工作階段時，作為參數傳遞。所產生工作階段的許可會是使用者或角色的身分型政策和工作階段政策的交集。許可也可以來自資源型政策。所有這類政策中的明確拒絕都會覆寫該允許。如需更多資訊，請參閱 IAM 使用者指南中的工作階段政策。

多種政策類型

將多種政策類型套用到請求時，其結果形成的許可會更為複雜、更加難以理解。要了解如何在涉及多個政策類型時 AWS 確定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

亞馬遜路線 53 應用程式復原控制器功能如何與 IAM 搭配

如需每項 Amazon Route 53 應用程式復原控制器功能如何與 IAM 搭配使用的相關資訊，請參閱下列主題：

- 適用於區域轉移的 IAM
- 適用於區域自動換檔的 IAM
- 適用於路由控制的 IAM
- IAM 的準備就緒檢查

Amazon Route 53 應用程式復原控制器中的身分識別型政策範例

若要查看 Amazon Route 53 應用程式復原控制器中每個功能的身分型政策範例，請參閱各 AWS Identity and Access Management 章節中每個功能的下列主題：

- 區域自動切換的身分識別原則範例
- Amazon Route 53 應用程式復原控制器中區域轉移的身分識別型政策範例
- Amazon Route 53 應用程式復原控制器中路由控制的身分識別型政策範例
- Amazon Route 53 應用程式復原控制器中適用於整備檢查的身分識別原則範例

AWS 適用於 Amazon Route 53 應用程式復原控制器

如需具有 AWS 受管政策之 Amazon Route 53 應用程式復原控制器功能的受管政策 (包括服務連結角色的受管政策) 的相關資訊，請參閱下列主題：

- 區域自動換檔的管理策略
- 路由控制的管理策略
- 管理準備檢查政策

Amazon Route 53 應用程式復原控制器的 AWS 受管政策更新

檢視有關 Route 53 ARC 中功能的 AWS 受管政策更新的詳細資料，因為此服務開始追蹤這些變更。如需有關此頁面變更的自動警示，請訂閱 Route 53 ARC 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	日期
AWSServiceRoleForPercPracticePolicy— 新政策	Route 53 ARC 為自動換檔和練習運行添加了一個新的服務鏈接角色。	2023 年 11 月 30 日

變更	描述	日期
	Route 53 ARC 使用服務連結角色啟用的許可來監控客戶提供的 Amazon CloudWatch 警示和客戶 AWS Health Dashboard 事件以進行實務執行，並開始執行實務。 若要深入瞭解新的服務連結角色，請參閱服務連結角色權限 AWSServiceRoleForZonalAutoshiftPracticeRun。	
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — 更新的政策	新增的權限`GetResourcePolicy` ，以支援傳回共用資源之資 AWS Resource Access Manager 源原則的詳細資料。	2023 年 10 月 18 日

路線 53 RecoveryReadiness ServiceRole 政策 — 更新的政策	Route 53 ARC 新增了新的許可，以查詢有關 Amazon EC2 執行個體的資訊。
	
	Route 53 ARC 使用下列許可來支援輪詢 Amazon EC2 執行個體、執行整備程度檢查並判斷執行個體的整備狀態。
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		2023 年 2 月 17 日

變更	描述	日期
路線 53 RecoveryReadiness ServiceRole 政策 — 更新的政策	Route 53 ARC 添加了一個新的權限來查詢有關 Lambda 函數的信息。 Route 53 ARC 使用下列權限來查詢 Lambda 函數的相關資訊，以執行整備程度檢查並判斷函數的整備狀態。 `lambda:ListProvisionedConcurrencyConfigs`	2022 年 8 月 31 日
AmazonRoute53 RecoveryControl ConfigFull 訪問-更新的策略	從政策中移除 Amazon Route 53 許可，並新增列出可選許可的附註。	2022 年 5 月 26 日
AmazonRoute53 RecoveryControl ConfigFull 訪問-更新的策略	添加缺少所需的 Amazon 路線 53 許可的政策。	2022 年 4 月 15 日
AmazonRoute53 RecoveryCluster ReadOnly 訪問-更新的策略	Route 53 ARC 添加了一個新的權限`route53-recovery-cluster:ListRoutingControls` ，允許列出路由控制 ARN 具有高可用性。	2022 年 3 月 15 日
AmazonRoute53 RecoveryControl ConfigRead OnlyAccess — 更新的政策	Route 53 ARC 添加了一個新的權限`route53-recovery-control-config:ListTagsForResources` ，允許列出資源的標籤。	2021 年 12 月 20 日

變更	描述	日期
路線 53 RecoveryReadiness ServiceRole 政策 — 更新的政策	Route 53 ARC 添加了一個新的權限來查詢有關 Amazon API Gateway 的信息。 Route 53 ARC 會使用權限來查詢 API Gateway 的相關資訊`apigateway:GET` ，以執行整備檢查並判斷整備狀態。	2021 年 10 月 28 日
AmazonRoute53 RecoveryReadiness ReadOnly 訪問權限-添加了新的權限	Route 53 ARC 為 AmazonRoute53 RecoveryReadiness ReadOnly 訪問添加了兩個新的權限： Route 53 ARC 會使用`route53-recovery-readiness:GetArchitectureRecommendations` 和`route53-recovery-readiness:GetCellReadinessSummary` 允許這些動作的唯讀存取權，以便使用復原準備工作。	2021 年 10 月 15 日

變更	描述	日期

路線 53 RecoveryReadiness ServiceRole 政策 — 更新的政策	Route 53 ARC 新增了新的權限來查詢 Lambda 函數的相關資訊。
	
	Route 53 ARC 使用下列權限查詢 Lambda 函數的相關資訊，以執行整備程度檢查並判斷這些函數的整備狀態。
	
	`lambda:GetFunctionConcurrency`
	
	`lambda:GetFunctionConfiguration`
	
	`lambda:GetProvisionedConcurrencyConfig`
	
	`lambda:ListAliases`
	
	`lambda:ListVersionsByFunction`
	
	`lambda:ListEventSourceMappings`
	
	`lambda:ListFunctions`
		2021 年 10 月 8 日

變更	描述	日期
Route53 RecoveryReadiness ServiceRole 策略 — 新增了新的受管理策略	Route 53 ARC 新增了下列新的受管理政策： AmazonRoute53 RecoveryReadiness FullAccess AmazonRoute53 RecoveryReadiness ReadOnly 訪問權限 AmazonRoute53 RecoveryCluster FullAccess AmazonRoute53 RecoveryCluster ReadOnly 訪問權限 AmazonRoute53 RecoveryControl ConfigFull 訪問權限 AmazonRoute53 RecoveryControl ConfigRead OnlyAccess	2021 年 8 月 18 日
Route 53 ARC 開始跟踪更改	Route 53 ARC 開始追蹤其 AWS 管理政策的變更。	2021 年 7 月 27 日

疑難排解 Amazon Route 53 應用程式復原控制器的身分

使用下列資訊可協助您診斷和修正使用 Amazon Route 53 應用程式復原控制器和 IAM 時可能遇到的常見問題。

主題

- 我沒有被授權在 Route 53 ARC 中執行動作
- 我沒有授權執行 iam：PassRole
- 我想允許我以外的人訪問我 AWS 帳戶 的 Route 53 ARC 資源

我沒有被授權在 Route 53 ARC 中執行動作

如果 AWS Management Console 告訴您您沒有執行動作的授權，則您必須聯絡管理員以尋求協助。您的管理員是提供您認證的人員。

下列範例錯誤會在mateojackson IAM 使用者嘗試使用主控台檢視一個虛構 *my-example-widget* 資源的詳細資訊，但卻無虛構 route53-recovery-readiness:*GetWidget* 許可時發生。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 route53-recovery-readiness:GetWidget on resource: my-example-widget
```

在此情況下，Mateo 會請求管理員更新他的政策，允許他使用 *my-example-widget* 動作存取 route53-recovery-readiness:*GetWidget* 資源。

我沒有授權執行 iam：PassRole

如果您收到未授權執行iam:PassRole動作的錯誤訊息，則必須更新您的原則，以允許您將角色傳遞給 Route 53 ARC。

有些 AWS 服務 允許您將現有角色傳遞給該服務，而不是建立新的服務角色或服務連結角色。如需執行此作業，您必須擁有將角色傳遞至該服務的許可。

當名為的 IAM 使用者marymajor嘗試使用主控台在 Route 53 ARC 中執行動作時，就會發生下列範例錯誤。但是，動作請求服務具備服務角色授予的許可。Mary 沒有將角色傳遞至該服務的許可。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在這種情況下，Mary 的政策必須更新，允許她執行 iam:PassRole 動作。

如果您需要協助，請聯絡您的 AWS 管理員。您的管理員提供您的簽署憑證。

我想允許我以外的人訪問我 AWS 帳戶 的 Route 53 ARC 資源

您可以建立一個角色，讓其他帳戶中的使用者或您組織外部的人員存取您的資源。您可以指定要允許哪些信任物件取得該角色。針對支援基於資源的政策或存取控制清單 (ACL) 的服務，您可以使用那些政策來授予人員存取您的資源的許可。

如需進一步了解，請參閱以下內容：

- 若要瞭解 Route 53 ARC 是否支援這些功能，請參閱亞馬遜路線 53 應用程式復原控制器功能如何與 IAM 搭配。

- 若要了解如何提供對您所擁有資源 AWS 帳戶 的存取權，請參閱《IAM 使用者指南》中您擁有的另一 AWS 帳戶 個 IAM 使用者提供存取權限。
- 若要了解如何將資源存取權提供給第三方 AWS 帳戶，請參閱 IAM 使用者指南中的提供第三方 AWS 帳戶 擁有的存取權。
- 若要了解如何透過聯合身分提供存取權，請參閱 IAM 使用者指南中的將存取權提供給在外部進行身分驗證的使用者 (聯合身分)。
- 若要了解使用角色和資源型政策進行跨帳戶存取之間的差異，請參閱 IAM 使用者指南中的 IAM 角色與資源型政策的差異。

Amazon Route 53 應用程式復原控制器中的記錄和

監控是維護 Amazon Route 53 應用程式復原控制器和 AWS 解決方案的可用性和效能的重要組成部分。您應該從 AWS 解決方案的所有部分收集監視資料，以便在發生多點失敗時更輕鬆地偵錯。AWS 提供數種工具來監控 Route 53 ARC 資源和活動，以及回應潛在事件，例如 AWS CloudTrail 和 Amazon CloudWatch。

如需在 Route 53 ARC 中監視每個功能的相關資訊，請參閱下列主題：

- 區域移位的記錄和監控
- 記錄和監控區域自動換檔
- 路由控制的記錄和監控
- 記錄和監控準備程度檢查

Amazon Route 53 應用程式復原控制器的合規驗證

第三方稽核員會評估 Amazon Route 53 應用程式復原控制器的安全性和合規性，做為多個 AWS 合規計劃的一部分。這些包括 SOC、PCI、HIPAA 等。

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 在 Amazon Web Services 上架構 HIPAA 安全性與合規性 — 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- Amazon GuardDuty — 透過監控環境中的 AWS 帳戶可疑和惡意活動，藉此 AWS 服務 偵測您的工作負載、容器和資料的潛在威脅。 GuardDuty 可協助您滿足特定合規性架構所要求的入侵偵測需求，如 PCI DSS 等各種合規性需求。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

Amazon Route 53 應用程序恢復控制器中

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域與低延遲、高輸送量和高冗餘網路相連。透過可用區域，您可以設計與操作的應用程式和資料庫，在可用區域之間自動容錯移轉而不會發生中斷。可用區域的可用性、容錯能力和擴展能力，均較單一或多個資料中心的傳統基礎設施還高。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

除了 AWS 全球基礎架構之外，Route 53 ARC 還提供多種功能，以協助支援您的資料恢復能力和備份需求。

Amazon Route 53 應用程式復原控制器的基礎

作為受管服務，Amazon Route 53 應用程式復原控制器受到 AWS 全球網路安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全 若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好的架構中的基礎結構保護。

您可以使用 AWS 已發佈的 API 呼叫，透過網路存取路由 53 ARC。使用者端必須支援下列專案：

- Transport Layer Security (TLS)。我們需要 TLS 1.2 並建議使用 TLS 1.3。
- 具備完美轉送私密(PFS)的密碼套件，例如 DHE (Ephemeral Diffie-Hellman)或 ECDHE (Elliptic Curve Ephemeral Diffie-Hellman)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以使用 AWS Security Token Service (AWS STS) 以產生暫時安全憑證以簽署請求。

Amazon Route 53 應用程式復原控制器開發人員指南的記錄

下列項目說明對 Amazon Route 53 應用程式復原控制器文件所做的重要變更。

- 版本：最新
- 最新文件更新：2024 年 4 月 30 日

變更	描述	日期
按每個功能進行文件重組	將要孤立的開發人員指南內容重組為子開發指南。也就是說，現在有單獨的部分包含 Route 53 ARC 中每個功能的完整資訊：用於異地同步備份復原的區域移位和區域自動換檔，以及多區域復原的路由控制和整備檢查。 如需詳細資訊，請參閱什麼是 Amazon Route 53 應用程式復原控制器。	2024 年 4 月 30 日
添加區域自動換檔功能	在 Route 53 ARC 中新增新功能，您可 AWS 以授權代表您將應用程式的資源流量從可用區域轉移，以協助縮短事件期間的復原時間。 如需詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器中的區域自動切換。	2023 年 11 月 30 日
新增服務連結角色	為區域自動換檔練習執行新增服務連結角色。AWSServiceRoleForZonalAutoshiftPracticeRun	2023 年 11 月 30 日

變更	描述	日期
	如需詳細資訊，請參閱的 AWSServiceRoleForZonalAutoshiftPracticeRun服務連結角色權限。	
新增叢集的跨帳戶支援	在 Route 53 ARC 中添加對叢集的跨帳戶支援 AWS Resource Access Manager，以便您可以輕鬆安全地使用一個叢集來裝載多個不同 AWS 帳戶擁有的控制面板和路由控制項。 如需詳細資訊，請參閱 Route 53 ARC 中的叢集 Support 跨帳戶。	2023 年 10 月 18 日
更新受管理的策略	更新受`AmazonRoute53RecoveryControlConfigReadOnly` 管理的策略以新增權限`GetResourcePolicy` ，以支援傳回共用資源之資 AWS Resource Access Manager 源策略的詳細資料。 如需詳細資訊，請參閱AWS 受管理的策略。	2023 年 9 月 19 日

變更	描述	日期
更新的服務連結角色	為 Route 53 ARC `ec2:DescribeVpnGateways` 的`ec2:DescribeCustomerGateways` 服務連結角色增加了新許可，以支援輪詢 Amazon EC2 執行個體。 如需詳細資訊，請參閱針對 Route 53 ARC 使用服務連結角色。	2023 年 2 月 17 日
用於區域移位的 GA 版本	支援 Route 53 ARC 的區域移位 GA 版本，其中包括針對在路線 53 ARC 中註冊用於區域移位的受管資源的基於屬性的存取控制 (ABAC)。 如需詳細資訊，請參閱使用 Route 53 ARC 的以屬性為基礎的存取控制 (ABAC)。	2023 年 1 月 10 日
添加了新的異地同步備份區域轉移	已新增內容，說明 Route 53 ARC (異地同步備份應用程式的區域轉移) 中的新服務。您可以啟動區域轉移，以暫時將負載平衡器資源的流量從可用區域移開。 有關更多信息，請參閱 Route 53 ARC 中的區域偏移。	2022 年 11 月 28 日

變更	描述	日期
更新的服務連結角色	為 Route 53 ARC 的服務連結角色新增了新權限`lambda:ListProvisionedConcurrencyConfigs` ，以查詢 Lambda 函數的相關資訊。 如需詳細資訊，請參閱針對 Route 53 ARC 使用服務連結角色。	2022 年 8 月 31 日
已更新受管政策	更新受`AmazonRoute53RecoveryControlConfigFullAccess` 管政策以移除 Amazon Route 53 許可，並將其列為選用權限。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策。	2022 年 5 月 26 日
已更新受管政策	已更新受`AmazonRoute53RecoveryControlConfigFullAccess` 管政策，以納入必要的 Amazon Route 53 許可。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策。	2022 年 4 月 15 日

變更	描述	日期
為新列表路由控件 API 添加了 CLI 示例	針對極度可靠的 Route 53 ARC 資料平面 API 中包含的新清單路由控制項 API 作業新增了 CLI 命令範例和最佳實務建議。 如需詳細資訊，請參閱列出和更新路由控制項與狀態。	2022 年 3 月 31 日
新增對覆寫安全規則的支援	已新增覆寫安全規則的支援，可讓您略過使用您已設定之安全規則強制執行的路由控制保護措施。例如，在容錯移轉期間進行災難復原時，可能需要安全規則覆寫。 如需詳細資訊，請參閱覆寫安全規則以重新路由流量。	2022 年 3 月 2 日
新增額外的標記支援	新增對 Route 53 ARC 中標記其他資源的支援，包括叢集、控制面板、路由控制項和安全規則。 如需詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器中的標記。	2021 年 12 月 20 日

變更	描述	日期
已更新受管政策	更新受AmazonRoute53RecoveryControlConfigReadOnly 管理的策略，以新增列出資源標籤的權限。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策	2021 年 12 月 20 日
增加了對實時警報的支持 EventBridge	已新增支援 EventBridge，這表示現在您可以新增規則以取得警示，並針對 Route 53 ARC 準備檢查狀態變更執行動作，例如，當狀態從「就緒」變更為「不就緒」時。 有關更多信息，請參閱在 Amazon 上使用 Route 53 ARC EventBridge。	2021 年 12 月 20 日
添加了路由控制狀態代碼示例	已新增程式碼範例，說明當您使用 API 作業取得或更新路由控制狀態時，依序嘗試叢集端點。 如需詳細資訊，請參閱 Amazon Route 53 應用程式復原控制器的 API 範例。	2021 年 11 月 16 日

變更	描述	日期
新增權限至唯讀原則	為策略添加了兩個新權限`AmazonRoute53RecoveryReadinessReadOnlyAccess` ：`route53-recovery-readiness:GetArchitectureRecommendations` 和`route53-recovery-readiness:GetCellReadinessSummary` 。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策。	2021 年 11 月 9 日
增加了對 Amazon API Gateway 資源類型的支持	新增了新的資源類型 Amazon API Gateway，並更新了 Route 53 ARC 服務連結角色許可，讓 Route 53 ARC 可以透過整備檢查來稽核 API Gateway。 如需詳細資訊，請參閱整備規則和支援的資源類型和針對 Route 53 ARC 使用服務連結角色。	2021 年 10 月 28 日

變更	描述	日期
新增對 Lambda 函數資源類型的支援	新增了新的資源類型 Lambda 函數，並更新了 Route 53 ARC 服務連結角色權限，讓 Route 53 ARC 可以使用整備檢查來稽核 Lambda 函數。 如需詳細資訊，請參閱整備規則和支援的資源類型和針對 Route 53 ARC 使用服務連結角色。	2021 年 10 月 8 日
添加鏈接 CloudFormation 和地形模板	已新增可下載 AWS CloudFormation 和 Hashicorp Terraform 範本的連結，以協助您快速開始使用 Route 53 Arc。如需詳細資訊，請參閱新應用程式的復原準備程度。	2021 年 9 月 13 日

變更	描述	日期
新增受管理的政策	為 Route 53 ARC 新增下列 AWS 受管理的政策：AmazonRoute53RecoveryReadinessFullAccess AmazonRoute53RecoveryReadinessReadOnlyAccess AmazonRoute53RecoveryClusterFullAccess 、AmazonRoute53RecoveryClusterReadOnlyAccess 、AmazonRoute53RecoveryControlConfigFullAccess 、、和AmazonRoute53RecoveryControlConfigReadOnlyAccess 。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策。	2021 年 8 月 18 日
開始追蹤 AWS Amazon Route 53 應用程式復原控制器的受管政策	受管理策略的更新將從最初發行日期開始追蹤。 如需詳細資訊，請參閱 AWS Amazon Route 53 應用程式復原控制器的受管政策。	2021 年 7 月 27 日

變更	描述	日期
Amazon 路由 53 應用程序恢復控制器的初始版	Route 53 ARC 透過集中協調區域內或跨多個 AWS 區域的容錯移轉，提升應用程式的可用性。Route 53 ARC 提供整備程度檢查，以確保您的應用程式可擴充以處理容錯移轉流量，並設定為繞過故障的路由。它還提供極其可靠的路由控制，因此您可以透過重新路由傳送流量 (例如跨可用區域或區域) 來復原應用程式。如需詳細資訊，請參閱何謂 Route 53 ARC？。	2021 年 7 月 27 日

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。