aws

開發人員指南

Amazon Application Recovery Controller (ARC)

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

Amazon Application Recovery Controller (ARC): 開發人員指南

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

Amazon 的商標和商業外觀不得用於任何非 Amazon 的產品或服務，也不能以任何可能造成客戶混淆、任何貶低或使 Amazon 名譽受損的方式使用 Amazon 的商標和商業外觀。所有其他非 Amazon 擁有的商標均為其各自擁有者的財產，這些擁有者可能附屬於 Amazon，或與 Amazon 有合作關係，亦或受到 Amazon 贊助。

Table of Contents

什麼是 ARC？ 1
多可用區域復原 1
多區域復原 2
Amazon Application Recovery Controller (ARC) 整備檢查可用性變更 3
遷移選項 3
比較多可用區域和多區域功能 4
異地同步備份復原 6
區域轉移 6
區域轉移的運作方式 7
AWS 區域 7
區域轉移元件 12
資料和控制平面 13
定價 14
最佳實務 14
API 操作 15
使用 CLI 操作的範例 16
支援的資源 20
啟動、更新或取消區域轉移 30
日誌記錄和監控 32
區域轉移的 IAM 36
區域自動轉移 45
區域自動轉移的運作方式 46
AWS 區域 53
區域自動轉移元件 54
資料和控制平面 56
定價 56
最佳實務 57
API 操作 60
使用 CLI 操作的範例 61
啟用和使用區域自動轉移 67
使用 測試區域自動轉移 AWS FIS 71
日誌記錄和監控 72
身分和存取權管理 82
配額 93

多區域復原 94
路由控制 94
關於路由控制 95
AWS 區域 96
元件 97
資料和控制平面 99
標記 100
定價 101
多區域復原入門 101
最佳實務 102
API 操作 105
使用 CLI 操作的範例 108
使用路由控制元件 123
日誌記錄和監控 139
身分和存取權管理 143
配額 155
準備度檢查 156
什麼是準備度檢查？ 156
AWS 區域 163
元件 164
資料和控制平面 166
標記 166
定價 167
設定彈性應用程式 168
最佳實務 168
API 操作 169
使用 CLI 操作的範例 171
使用復原群組和準備度檢查 181
監控整備狀態 186
取得架構建議 187
建立跨帳戶授權 189
就緒規則、資源類型和 ARNS 191
日誌記錄和監控 209
身分和存取權管理 223
配額 235
區域切換 236

關於區域切換 236
最佳實務 247
教學課程：主動/被動計劃 249
教學課程：報告自動產生 255
教學課程：執行 RDS 復原後工作流程 257
API 操作 259
使用區域切換 261
儀表板 290
跨帳戶支援 291
身分和存取權管理 296
日誌記錄和監控 316
配額 324
程式碼範例 325
基本概念 325
動作 325
安全 336
資料保護 336
靜態加密 337
傳輸中加密 337
身分和存取權管理 337
目標對象 337
使用身分驗證 338
使用政策管理存取權 339
Amazon Application Recovery Controller (ARC) 功能如何與 IAM 搭配使用 340
身分型政策範例 340
AWS 受管政策 341
疑難排解 346
AWS PrivateLink 348
日誌記錄和監控 350
法規遵循驗證 350
恢復能力 350
基礎設施安全性 351
文件歷史紀錄 352
..... ccclxv

什麼是 ARC？

Amazon Application Recovery Controller (ARC) 可協助您為 AWS 在全球雲端基礎設施上執行的應用程式準備並完成更快的復原。

ARC 提供下列功能：

- 多可用區域 (AZ) 復原，包括區域轉移和區域自動轉移，可讓您暫時將流量從受損的 AZ 轉移到運作狀態良好的 AZ，從單一 AZ 受損復原。
- 多區域復原，包括用於區域應用程式復原的路由控制和區域切換，以及應用程式監控的準備度檢查。

多可用區域復原

區域轉移

您可以使用 ARC 區域轉移，快速隔離和復原單一可用區域 (AZ) 受損。區域轉移會暫時將受支援資源的流量從受損的 AZ 轉移到相同 AWS 區域中運作狀態良好的 AZs。啟動區域轉移有助於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從單一可用區域中的 AWS 損害復原。將流量移離受損的可用區域，可降低在受損的可用區域中使用您的應用程式之用戶端的影響。

您可以為 區域中您帳戶中任何支援的資源啟動區域轉移 AWS 。區域轉移是手動和暫時的。開始區域轉移時，您必須指定最長三天的 （ 可延伸 ） 過期。若要為支援的資源啟用區域轉移，請參閱 支援的資源。

區域自動轉移

ARC 區域自動轉移授權 代表您 AWS 將流量從受支援資源的受損 AZ 轉移到相同 AWS 區域中運作狀態良好的 AZs。當內部遙測顯示 AWS 區域中的一個 AZ 存在可能影響客戶的受損時， 會 AWS 啟動區域自動轉移。內部遙測包含來自多個來源的指標，包括 AWS 網路，以及 Amazon EC2 和 Elastic Load Balancing 服務。

區域自動轉移是暫時的。當內部遙測指標顯示不再存在問題或潛在問題時， 會 AWS 結束區域自動轉移。

若要進一步了解這些功能，請參閱下列章節：

- ARC 中的區域轉移
- ARC 中的區域自動轉移

多區域復原

區域切換

ARC 中的區域切換提供集中式、自動化且可觀察的解決方案，以進行多區域應用程式復原。區域切換可協助您規劃和協調整個應用程式的復原 AWS 區域，以協助確保業務持續性並降低營運開銷。

您可以使用區域切換，跨多個 AWS 帳戶協調應用程式資源的大規模、複雜復原任務。如果 AWS 區域受損，您使用區域切換建立的計劃可能會容錯移轉或將資源切換到另一個區域，讓您的應用程式可以在運作狀態良好的情況下繼續運作 AWS 區域。

路由控制

ARC 非常可靠的路由控制可啟用多區域復原，讓您的應用程式可以容錯移轉跨 AWS 區域的網域名稱系統 DNS 流量。

如果您的應用程式設計為在多個 AWS 區域之外操作，您可以使用 ARC 路由控制在區域之間進行容錯移轉。路由控制可讓您將流量從受損 AWS 區域容錯移轉至運作狀態良好的 AWS 區域，以確保您的應用程式維持可用性。路由控制包含安全規則，可透過強加您定義的護欄，協助保護您免於意外結果。例如，您可以強加安全規則，只啟用和使用其中一個作用中或待命的應用程式複本。

準備度檢查

ARC 整備檢查會持續監控 AWS 資源配額、容量和網路路由政策，並通知您可能影響您容錯移轉至複本應用程式並從區域損害中復原的變更。持續整備檢查可確保您可以將多區域應用程式維持在已擴展和設定為處理容錯移轉流量的狀態。當您第一次設定 ARC 時，以及在正常應用程式操作期間，準備度檢查非常有用。準備度檢查不適用於事件期間容錯移轉的關鍵路徑。

若要進一步了解這些功能，請參閱下列章節：

- ARC 中的區域切換
- ARC 中的路由控制
- ARC 中的準備度檢查

Amazon Application Recovery Controller (ARC) 整備檢查可用性變更

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。

在仔細考慮之後，我們決定從 2026 年 4 月 30 日起，將 Amazon Application Recovery Controller (ARC) 中的整備檢查功能關閉給新客戶。現有客戶可以繼續正常使用該服務。

ARC 整備檢查是一項功能，可讓您監控資源的整備情況以進行災難復原。ARC 將繼續提供，但準備度檢查功能自 2026 年 4 月 30 日起將不再開放給新客戶使用。

> **Note**
>
> 繼續完全支援 ARC 和 ARC 區域切換。只有整備檢查功能會受到此變更的影響。區域切換、路由控制、區域轉移和區域自動轉移沒有變更。

遷移選項

對於與整備檢查類似的功能，我們建議您將多區域應用程式加入 ARC 區域切換。

ARC 區域切換是全受管服務，可提供完整的多區域復原協同運作。它包含稱為計劃評估的功能，它會定期監控區域切換計劃的狀態，以確保準備執行。

若要開始使用 ARC 區域切換，請參閱 ARC 中的區域切換。

比較 ARC 中的多可用區域和多區域復原功能

Amazon Application Recovery Controller (ARC) 中的區域轉移、區域自動轉移、路由控制和區域切換都可以實現快速復原，並協助您確保 AWS 應用程式的彈性。這些功能是高度可用的，有助於在應用程式遇到延遲增加或可用性降低的情況下支援復原。這些功能也有助於快速復原應用程式，方法是將流量移離隔離的損害，以限制損害所造成的影響和時間。

路由控制和區域切換專注於多個 AWS 區域（多區域）中的 AWS 應用程式，而區域轉移和區域自動轉移僅支援使用多可用區域應用程式轉移受支援資源的流量。

下表中的資訊包含 ARC 彈性功能的一些主要功能。這些描述可協助您更加了解特定選項如何成為您應用程式需求的最佳選擇。

路由控制	區域切換	區域轉移	區域自動轉移
區域性 將流量從一個區域路由到另一個 AWS 區域（主要）	區域性 將流量從一個區域路由到另一個 AWS 區域（主要）	區域 將流量移離可用區域 流量會前往 區域中的其他可用區域，而不是特定目標	區域 將流量移離可用區域 流量會前往 區域中的其他可用區域，而不是特定目標
需要設定 需要組態和設定	需要設定 需要組態和設定	可能需要設定 需要選擇加入一些支援的資源 如需詳細資訊，請參閱 支援的資源	需要設定 必須針對支援的資源啟用 如需詳細資訊，請參閱 支援的資源
客戶起始 客戶決定何時重新路由流量	客戶起始 客戶決定何時重新路由流量	客戶起始 客戶決定何時開始區域轉移	AWS- 啟動 AWS 代表您將應用程式流量移離 AZ
費用型 需要個別的路由控制費用	費用型 區域切換計劃需要個別費用	包含在 服務中（不收取額外費用）	包含在 服務中（不收取額外費用）

路由控制	區域切換	區域轉移	區域自動轉移
		支援的資源包含建立區域轉移，以將流量移離AZs	支援的 資源包含開始自動轉移以代表您將流量移離 AZs
不會過期 流量可以無限期重新路由到複本	不會過期 應用程式可以無限期地轉移到複本	暫時 所有區域轉移都必須設定為過期	暫時 AWS 開始和結束自動轉移

若要進一步了解這些功能，請參閱下列章節：

- ARC 中的區域轉移
- ARC 中的區域自動轉移
- ARC 中的路由控制
- ARC 中的區域切換

使用區域轉移和區域自動轉移來復原 ARC 中的應用程式

本節說明如何使用 Amazon Application Recovery Controller (ARC) 中的功能，可靠地從受損可用區域 (AZ) 的問題復原資源 AWS 。區域轉移和區域自動轉移會暫時將支援資源的流量從受損的可用區域轉移，從而縮短應用程式的復原時間。

區域轉移和區域自動轉移之間的主要區別在於，其中一個是您控制的手動流量轉移，另一個則代表您自動轉移流量遠離受損。

- 使用區域轉移時，您可以手動將 中支援資源的流量移 AWS 區域 離可用區域。
- 使用區域自動轉移時，支援資源的流量會自動從受損的可用區域轉移，並重新路由至相同區域中運作狀態良好的AZs AWS 區域。

下列主題說明區域轉移和區域自動轉移功能，以及如何使用這些功能。

主題

- ARC 中的區域轉移
- ARC 中的區域自動轉移

ARC 中的區域轉移

Amazon Application Recovery Controller (ARC) 區域轉移可讓您將支援資源的流量從 中受損的可用區域 (AZ) 轉移到相同區域中 AWS 區域 運作狀態良好的 AZs。將資源的流量移離受損的可用區，可縮短停電或可用區中的硬體或軟體問題所造成的影響持續時間和嚴重性，並有助於減輕問題並快速復原應用程式。舉例來說，由於部署不良導致延遲問題或可用區域受損，您可選擇轉移流量。

您必須選擇加入資源，才能使用區域轉移。如需詳細資訊，請參閱 支援的資源。

在開始區域轉移之前，您必須預先調整應用程式的比例，並確保您有足夠的容量將流量移離可用區域。在預先擴展之後，您可以選擇要轉移的可用區域，以及要轉移流量的資源，然後啟動區域轉移。您可以隨時取消轉移，讓流量開始返回原始可用區域。如需詳細資訊，請參閱ARC 中的區域轉移最佳實務

所有區域轉移均為臨時緩解措施。開始進行區域轉移時，您可以設定初始到期時間，從一分鐘到三天 (72 小時)，如果需要繼續轉移流量，則可以延長時間。

在特定情況下，區域轉移不會將流量移離 AZ。如需詳細資訊，請參閱支援的資源。

區域轉移的運作方式

當您為支援的資源啟動區域轉移時，資源的流量會移離您指定的可用區域 (AZ)。ARC 支援的資源提供將指定 AZ 標記為運作狀態不佳的整合，這會導致流量從受損的 AZ 轉移。

流量開始轉移 - 當您在 ARC 中開始區域轉移時，可能不會看到流量立即移出可用區域。根據用戶端行為和連線重複使用，在可用區域中現有的進行中連線可能需要一小段時間才能完成。DNS 設定和包括現有連線的其他因素只需幾分鐘即可完成，但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。

流量轉移結束 - 當區域轉移過期或取消時，ARC 會採取步驟來停止轉移流量，並反轉啟動流量轉移的程序。現在，復原的 AZ 會辨識為可供資源使用，而流量會繼續流入 AZ。

您必須在開始輪班時將所有區域輪班設定為過期。您最初可以將區域轉移設定為在最多三天 (72 小時) 內過期。不過，您可以隨時更新區域轉移以設定新的過期時間。如果您準備好將流量還原到可用區域，也可以在區域轉移過期之前取消。

當流量不會轉移時 - 在特定情況下，區域轉移不會將流量從可用區域轉移。例如，假設您在 AZs 中的負載平衡器目標群組沒有任何執行個體，或所有執行個體運作狀態不佳時，啟動負載平衡器的區域轉移。在此案例中，負載平衡器處於故障開啟狀態，啟動區域轉移不會轉移流量。

在您開始資源的區域轉移之前，請確定符合成功區域轉移的所有條件。 AWS 資源會以不同的方式處理區域轉移。如需區域轉移支援的詳細資訊，請參閱 支援的資源。

AWS 區域 區域轉移的可用性

如需 Amazon Application Recovery Controller (ARC) 的區域支援和服務端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Application Recovery Controller (ARC) 端點和配額。

此處 AWS 區域 列出的 目前提供區域轉移和區域自動轉移。中國區域也提供區域轉移和區域自動轉移，也就是中國 （北京） 區域和中國 （寧夏） 區域。使用 Amazon Application Recovery Controller (ARC) 的資源可能會有其他考量。如需詳細資訊，請參閱 支援的資源。

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	
		arc-zonal-shift-fips.us-east-2.api.aws	HTTPS	

區域名稱	區域	端點	通訊協定
		arc-zonal-shift.us-east-2.api.aws	HTTPS
美國東部 (維吉尼亞北部)	us-east-1	arc-zonal-shift.us-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-east-1.api.aws	HTTPS
		arc-zonal-shift.us-east-1.api.aws	HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	arc-zonal-shift.us-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-1.api.aws	HTTPS
		arc-zonal-shift.us-west-1.api.aws	HTTPS
美國西部 (奧勒岡)	us-west-2	arc-zonal-shift.us-west-2.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-west-2.api.aws	HTTPS
		arc-zonal-shift.us-west-2.api.aws	HTTPS
Africa (Cape Town)	af-south-1	arc-zonal-shift.af-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.af-south-1.api.aws	HTTPS
亞太區域 (香港)	ap-east-1	arc-zonal-shift.ap-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-1.api.aws	HTTPS
亞太區域 (海德拉巴)	ap-south-2	arc-zonal-shift.ap-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-2.api.aws	HTTPS
亞太區域 (雅加達)	ap-southeast-3	arc-zonal-shift.ap-southeast-3.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-3.api.aws	HTTPS
亞太地區 (馬來西亞)	ap-southeast-5	arc-zonal-shift.ap-southeast-5.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-5.api.aws	HTTPS

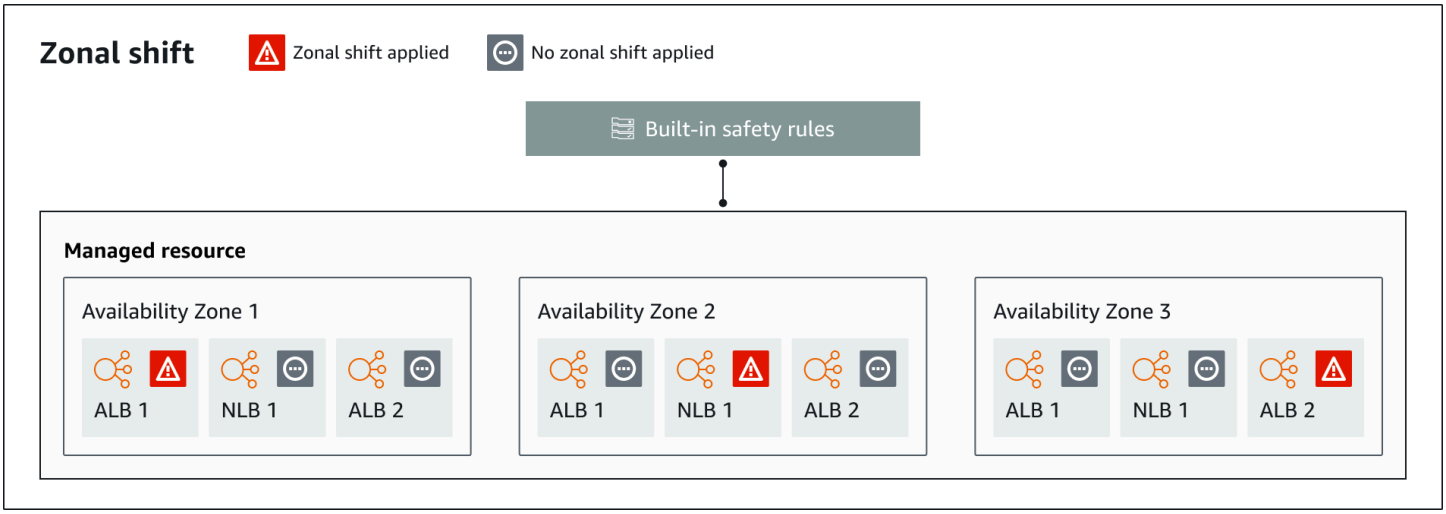
區域名稱	區域	端點	通訊協定
亞太區域 (墨爾本)	ap-southeast-4	arc-zonal-shift.ap-southeast-4.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-4.api.aws	HTTPS
亞太區域 (孟買)	ap-south-1	arc-zonal-shift.ap-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-south-1.api.aws	HTTPS
亞太區域 (紐西蘭)	ap-southeast-6	arc-zonal-shift.ap-southeast-6.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-6.api.aws	HTTPS
亞太區域 (大阪)	ap-northeast-3	arc-zonal-shift.ap-northeast-3.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-3.api.aws	HTTPS
亞太區域 (首爾)	ap-northeast-2	arc-zonal-shift.ap-northeast-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-2.api.aws	HTTPS
亞太區域 (新加坡)	ap-southeast-1	arc-zonal-shift.ap-southeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-1.api.aws	HTTPS
亞太區域 (雪梨)	ap-southeast-2	arc-zonal-shift.ap-southeast-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-2.api.aws	HTTPS
亞太區域 (台北)	ap-east-2	arc-zonal-shift.ap-east-2.amazonaws.com	HTTPS
		arc-zonal-shift.ap-east-2.api.aws	HTTPS
亞太區域 (泰國)	ap-southeast-7	arc-zonal-shift.ap-southeast-7.amazonaws.com	HTTPS
		arc-zonal-shift.ap-southeast-7.api.aws	HTTPS

區域名稱	區域	端點	通訊協定
亞太區域 (東京)	ap-northeast-1	arc-zonal-shift.ap-northeast-1.amazonaws.com	HTTPS
		arc-zonal-shift.ap-northeast-1.api.aws	HTTPS
加拿大 (中部)	ca-central-1	arc-zonal-shift.ca-central-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-central-1.api.aws	HTTPS
		arc-zonal-shift.ca-central-1.api.aws	HTTPS
加拿大西部 (卡加利)	ca-west-1	arc-zonal-shift.ca-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.ca-west-1.api.aws	HTTPS
		arc-zonal-shift.ca-west-1.api.aws	HTTPS
歐洲 (法蘭克福)	eu-central-1	arc-zonal-shift.eu-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-1.api.aws	HTTPS
歐洲 (愛爾蘭)	eu-west-1	arc-zonal-shift.eu-west-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-1.api.aws	HTTPS
歐洲 (倫敦)	eu-west-2	arc-zonal-shift.eu-west-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-2.api.aws	HTTPS
歐洲 (米蘭)	eu-south-1	arc-zonal-shift.eu-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-1.api.aws	HTTPS
歐洲 (巴黎)	eu-west-3	arc-zonal-shift.eu-west-3.amazonaws.com	HTTPS
		arc-zonal-shift.eu-west-3.api.aws	HTTPS
歐洲 (西班牙)	eu-south-2	arc-zonal-shift.eu-south-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-south-2.api.aws	HTTPS

區域名稱	區域	端點	通訊協定
歐洲 (斯德哥爾摩)	eu-north-1	arc-zonal-shift.eu-north-1.amazonaws.com	HTTPS
		arc-zonal-shift.eu-north-1.api.aws	HTTPS
歐洲 (蘇黎世)	eu-central-2	arc-zonal-shift.eu-central-2.amazonaws.com	HTTPS
		arc-zonal-shift.eu-central-2.api.aws	HTTPS
以色列 (特拉維夫)	il-central-1	arc-zonal-shift.il-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.il-central-1.api.aws	HTTPS
墨西哥 (中部)	mx-central-1	arc-zonal-shift.mx-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.mx-central-1.api.aws	HTTPS
中東 (巴林)	me-south-1	arc-zonal-shift.me-south-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-south-1.api.aws	HTTPS
中東 (阿拉伯聯合大公國)	me-central-1	arc-zonal-shift.me-central-1.amazonaws.com	HTTPS
		arc-zonal-shift.me-central-1.api.aws	HTTPS
南美洲 (聖保羅)	sa-east-1	arc-zonal-shift.sa-east-1.amazonaws.com	HTTPS
		arc-zonal-shift.sa-east-1.api.aws	HTTPS
AWS GovCloud（美國東部）	us-gov-east-1	arc-zonal-shift.us-gov-east-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-east-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-east-1.api.aws	HTTPS
AWS GovCloud（美國西部）	us-gov-west-1	arc-zonal-shift.us-gov-west-1.amazonaws.com	HTTPS
		arc-zonal-shift-fips.us-gov-west-1.api.aws	HTTPS
		arc-zonal-shift.us-gov-west-1.api.aws	HTTPS

區域轉移元件

下圖說明區域轉移轉移流量從 中的可用區域轉移的範例 AWS 區域。當資源已有作用中的輪班時，在區域輪班中內建的檢查會阻止您啟動資源的另一個區域輪班。



以下是 ARC 中區域轉移功能的元件。

區域轉移

您為 AWS 帳戶中的受管資源開始區域轉移，以暫時將流量從 中的可用區域移出 AWS 區域，轉移到區域中運作狀態良好的AZs，以從一個可用區域中的問題快速復原。如需區域轉移支援資源的詳細資訊，請參閱 支援的資源。

內建安全檢查

內建於 ARC 的檢查可防止資源一次發生多個流量轉移。也就是說，只有一個客戶起始的區域轉移、實務執行或資源的自動轉移可以主動將流量移離可用區域。例如，如果您在資源目前以自動轉移轉移時啟動該資源的區域轉移，則您的區域轉移優先。如需詳細資訊，請參閱 ARC 中的區域自動轉移和 練習執行的結果。

資源識別符

要在區域轉移中包含的資源識別符。識別符是資源的 Amazon Resource Name (ARN)。

對於區域轉移，您只能為 ARC 支援 AWS 的服務選擇帳戶中的資源。如需區域轉移支援資源的詳細資訊，請參閱 支援的資源。

受管資源

有些 AWS 資源必須手動選擇加入區域轉移，其他資源會自動啟用。如需區域轉移支援資源的詳細資訊，請參閱 支援的資源。

資源名稱

您可以在 ARC 中為區域轉移指定的資源名稱。

狀態 （區域轉移狀態）

區域轉移的狀態。區域轉移Status的 可以有下列其中一個值：

- ACTIVE：區域轉移已啟動並處於作用中狀態。
- 過期：區域轉移已過期 （超過到期時間）。
- 已取消：區域轉移已取消。

套用狀態

套用的狀態指出資源的輪班是否有效。狀態為 的轉移會APPLIED決定資源的應用程式流量已轉移的可用區域，以及該轉移何時結束。

輪班類型

定義區域轉移類型。shiftType 可以有下列值：

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- PRACTICE_RUN
- FIS_EXPERIMENT

到期時間 （到期時間）

區域輪班的到期時間 （到期時間）。區域轉移是暫時性的。對於區域轉移，您可以最初將區域轉移設定為作用中長達三天 (72 小時）。

當您開始區域轉移時，您可以指定要它處於作用中狀態的時間長度，ARC 會轉換為到期時間 （到期時間）。例如，如果您準備好將流量還原到可用區域，您可以取消區域轉移。或者，您可以更新客戶起始的區域轉移，以指定另一個過期時間長度，以延長該區域轉移。

您可以取消屬於區域自動轉移一部分的區域轉移實務執行。

區域轉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依賴的機制具有高度可用性，以便在災難情況下需要它們時使用。一般而言，您應該盡可能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，了解服務的功能如何在控制平面和資料平面之間分割，以及何時可以使用服務的資料平面依賴極端可靠性。

與大多數 AWS 服務一樣，控制平面和資料平面支援區域轉移功能的功能。雖然這兩者都建置為可靠，但控制平面會針對資料一致性進行最佳化，而資料平面則會針對可用性進行最佳化。資料平面專為彈性而設計，因此即使在破壞性事件期間，當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。

如需資料平面、控制平面以及 如何 AWS 建置服務以滿足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白皮書。

ARC 中區域轉移的定價

對於區域轉移，您可以為支援的資源啟動區域轉移，從可用區域中的問題中復原應用程式。使用區域轉移不收取額外費用。

如需 ARC 和定價範例的詳細定價資訊，請參閱 ARC 定價。

ARC 中的區域轉移最佳實務

我們建議在 ARC 中使用區域轉移進行多可用區域復原的下列最佳實務。

主題

- 容量規劃和預先擴展
- 限制用戶端保持連線至端點的時間
- 事先測試開始區域轉移
- 確保所有可用區域都正常運作並取得流量
- 使用資料平面 API 操作進行災難復原
- 僅暫時移動具有區域轉移的流量

容量規劃和預先擴展

確定您已規劃 ，且已預先擴展或 可以自動擴展足夠的容量，以因應啟動區域轉移時對可用區域施加的額外負載。使用復原導向架構時，典型的建議是預先擴展運算容量，以在其中一個 （通常） 三個複本離線時，包含足夠的總空間來為您的尖峰流量提供服務。

當您為支援的資源啟動區域轉移，且流量從可用區域轉移時，您的應用程式用來服務請求的容量會移除。您必須確定已規劃從可用區域轉移流量，並且可以繼續在其餘AZs服務請求。

限制用戶端保持連線至端點的時間

當 Amazon Application Recovery Controller (ARC) 將流量移離損害時，例如使用區域轉移或區域自動轉移，ARC 用來移動應用程式流量的機制是 DNS 更新。DNS 更新會導致所有新連線被導向至受損的位置。

不過，具有預先存在開放連線的用戶端可能會繼續對受損位置提出請求，直到用戶端重新連線為止。為了確保快速復原，建議您限制用戶端保持連線至端點的時間。

事先測試開始區域轉移

透過啟動區域轉移，定期測試從應用程式的可用區域移出的流量。規劃並執行啟動區域轉移，最好是在測試和生產環境中，作為在發生災難時復原應用程式之定期容錯移轉測試的一部分。定期測試是確保您已準備好並有信心在發生操作事件時緩解問題的關鍵部分。

確保所有可用區域都正常運作並取得流量

區域轉移的運作方式是將資源標記為在可用區域中運作狀態不佳的應用程式複本。這表示請務必確保應用程式中的資源整體狀況良好，並主動在區域中的可用區域中接收流量。我們建議您使用儀表板來追蹤此狀況，例如，針對運作狀態不佳的目標和位元組的 Elastic Load Balancing 指標每個可用區域處理。 bytesProcessed

請考慮從第二個相鄰區域監控資源的運作狀態。這種方法的優點是它可以更代表您的最終使用者體驗，也可以降低應用程式和監控同時受到相同災難影響的風險。

使用資料平面 API 操作進行災難復原

若要在需要快速復原應用程式時啟動區域轉移，只要相依性極少，我們建議您使用 AWS Command Line Interface 或 API 搭配區域轉移動作，並盡可能使用預先存放的登入資料。您也可以在 中開始區域轉移 AWS 管理主控台，以方便使用。但是，當快速、可靠的復原至關重要時，資料平面操作是更好的選擇。如需詳細資訊，請參閱區域轉移 API 參考指南。

僅暫時移動具有區域轉移的流量

區域轉移會暫時將流量移離可用區域，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至服務。這可確保您的整體應用程式還原至其原始完全備援、彈性狀態。

區域轉移 API 操作

下表列出您可以使用區域轉移的 ARC API 操作，這會將流量移離多可用區域應用程式的可用區域。資料表中還包含相關文件的連結。

如需如何搭配 使用常用區域轉移 API 操作的範例 AWS Command Line Interface，請參閱 AWS CLI 搭配區域轉移使用 的範例。

Action	使用 ARC 主控台	使用 ARC API
開始區域轉移	請參閱 啟動區域轉移	請參閱 StartZonalShift
更新區域轉移	請參閱 更新或取消區域轉移	請參閱 UpdateZonalShift
列出區域轉移	請參閱 ARC 中的區域轉移	請參閱 ListZonalShifts
列出受管資源	請參閱 支援的資源	請參閱 ListManagedResources
取得受管資源	請參閱 支援的資源	請參閱 GetManagedResource
取消區域轉移	請參閱 更新或取消區域轉移	請參閱 CancelZonalShift

AWS CLI 搭配區域轉移使用 的範例

本節提供使用區域轉移的應用程式範例，使用 AWS Command Line Interface 使用 API 操作在 Amazon Application Recovery Controller (ARC) 中使用區域轉移功能。這些範例旨在協助您了解如何使用 CLI 處理區域轉移。

ARC 中的區域轉移可讓您暫時將支援資源的流量移離可用區域，讓您的應用程式可以繼續與 中的其他可用區域正常運作 AWS 區域。

所有區域轉移都是暫時的，且最初必須設定為在三天內過期。不過，您可以稍後更新區域轉移來設定新的過期時間。

如需使用 的詳細資訊 AWS CLI，請參閱 AWS CLI 命令參考。如需區域轉移 API 動作和詳細資訊連結的清單，請參閱 區域轉移 API 操作。

開始區域轉移

您可以使用 `start-zonal-shift`命令，透過 CLI 啟動區域轉移。

```
aws arc-zonal-shift start-zonal-shift \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05 \
       --away-from use1-az1 \
```

```
       --expires-in 10m \
       --comment "Shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T21:37:26-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

取得受管資源

您可以使用 get-managed-resource命令，透過 CLI 取得受管資源的相關資訊。

```
aws arc-zonal-shift get-managed-resource \
       --resource-identifier arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05
```

```
{
    "appliedWeights": {
        "use1-az1": 0.0,
        "use1-az2": 1.0,
        "use1-az6": 1.0
    },
    "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/
Testing/5a19403ecd42dc05",
    "autoshifts": [],
    "name": "Testing",
    "zonalAutoshiftStatus": "DISABLED",
    "zonalShifts": [
        {
            "appliedStatus": "APPLIED",
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
```

```
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
            "shiftType": "MANUAL"
        }
    ]
}
```

列出受管資源

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

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

```
{
    "items": [
        {
            "appliedWeights": {
                "use1-az1": 0.0,
                "use1-az2": 1.0,
                "use1-az6": 1.0
            },
            "arn": "arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/
app/Testing/5a19403ecd42dc05",
            "autoshifts": [],
            "availabilityZones": [
                "use1-az1",
                "use1-az2",
                "use1-az6"
            ],
            "name": "Testing",
            "practiceRunStatus": "DISABLED",
            "zonalAutoshiftStatus": "DISABLED",
            "zonalShifts": [
                {
                    "appliedStatus": "APPLIED",
                    "awayFrom": "use1-az1",
                    "comment": "Shifting traffic away from use1-az1",
                    "expiryTime": "2024-12-17T21:37:26-08:00",
                    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
                    "startTime": "2024-12-17T21:27:26-08:00",
                    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
                }
            ]
```

```
        }
    ]
}
```

列出區域轉移

您可以使用 list-zonal-shifts命令，透過 CLI 列出帳戶中的區域轉移。

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

```
{
    "items": [
        {
            "awayFrom": "use1-az1",
            "comment": "Shifting traffic away from use1-az1",
            "expiryTime": "2024-12-17T21:37:26-08:00",
            "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
            "startTime": "2024-12-17T21:27:26-08:00",
            "status": "ACTIVE",
            "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
        }
    ]
}
```

更新區域轉移

您可以使用 update-zonal-shift命令，透過 CLI 更新區域轉移。

```
aws arc-zonal-shift update-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38 \
       --expires-in 1h \
       --comment "Still shifting traffic away from use1-az1"
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "ACTIVE",
```

```
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

取消區域轉移

您可以使用 `cancel-zonal-shift`命令，透過 CLI 取消區域轉移。

```
aws arc-zonal-shift cancel-zonal-shift \
       --zonal-shift-id 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "use1-az1",
    "comment": "Still shifting traffic away from use1-az1",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

支援的資源

Amazon Application Recovery Controller (ARC) 目前支援為區域轉移和區域自動轉移啟用下列資源：

- Amazon EC2 Auto Scaling 群組
- Amazon Elastic Kubernetes Service
- Application Load Balancer 啟用或停用跨區域負載平衡
- Network Load Balancer 啟用或停用跨區域負載平衡

如需 Network Load Balancer 和 Application Load Balancer 的特定需求，請參閱本節中的其他主題。

檢閱下列在 ARC 中使用區域轉移、區域自動轉移和資源的條件：

- 資源必須處於作用中狀態並完全佈建，才能轉移其流量。在您開始資源的區域轉移之前，請檢查以確定它是 ARC 中的受管資源。例如，在 中檢視受管資源的清單 AWS 管理主控台，或使用`get-managed-resource`具有資源識別符的操作。
- 若要使用資源啟動區域轉移，必須部署在可用區域以及您 AWS 區域 開始轉移的位置。請確定您在要轉移的 AZ 所在的相同區域中啟動區域轉移，而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，以搭配 資源使用區域轉移。如需詳細資訊，請參閱區域轉移的 IAM 和許可。
- 當 Network Load Balancer 或 Application Load Balancer 處於故障開啟狀態時，區域轉移將不會生效。這是預期的行為，因為區域轉移無法強制 AZ 運作狀態不良，然後在負載平衡器故障開啟時，將流量轉移到區域中的其他 AZs。如需詳細資訊，請參閱 Network Load Balancer 使用者指南中的針對負載平衡器使用 Route 53 DNS 容錯移轉，以及 Application Load Balancer 使用者指南中的針對負載平衡器使用 Route 53 DNS 容錯移轉。
- 如果多個負載平衡器將流量轉送到相同的目標，則啟用跨區域負載平衡器的區域轉移會降低所有負載平衡器的目標容量，即使其流量不是因區域轉移而轉移。

Amazon EC2 Auto Scaling 群組

Amazon EC2 Auto Scaling 群組包含一組 Amazon EC2 執行個體，這些執行個體被視為邏輯分組，用於自動擴展和管理。Auto Scaling 群組也讓您可以使用 Amazon EC2 Auto Scaling 功能，例如運作狀態檢查替換和擴展政策。維持 Auto Scaling 群組中的執行個體數量和自動擴展都是 Amazon EC2 Auto Scaling 服務的核心功能。

對 Auto Scaling 群組使用區域轉移

若要啟用區域轉移，請使用下列其中一種方法。

Console

在新群組上啟用區域轉移 （主控台）

1. 遵循使用啟動範本建立 Auto Scaling 群組中的指示，並完成程序中的每個步驟，直到步驟 10。
2. 在與其他 服務整合頁面上，針對 ARC 區域轉移，選取核取方塊以啟用區域轉移。
3. 針對運作狀態檢查行為，選擇忽略運作狀態不佳或取代運作狀態不佳。如果設定為 `replace-unhealthy`，運作狀態不佳的執行個體將在可用區域中以作用中區域轉移取代。如果設為 `ignore-unhealthy`，則運作狀態不佳的執行個體不會在可用區域中以作用中區域轉移取代。
4. 繼續執行使用啟動範本建立 Auto Scaling 群組中的步驟。

AWS CLI

在新群組上啟用區域轉移 (AWS CLI)

將 `--availability-zone-impairment-policy` 參數新增至 create-auto-scaling-group 命令。

`--availability-zone-impairment-policy` 參數有兩個選項：

- ZonalShiftEnabled – 如果設定為 `true`，Auto Scaling 會使用 ARC 區域轉移註冊 Auto Scaling 群組，您可以在 ARC 主控台上啟動、更新或取消區域轉移。如果設定為 `false`，Auto Scaling 會從 ARC 區域轉移取消註冊 Auto Scaling 群組。您必須已啟用區域轉移，才能將 設定為 `false`。
- ImpairedZoneHealthCheckBehavior – 如果設定為 `replace-unhealthy`，運作狀態不佳的執行個體將在可用區域中取代為作用中區域轉移。如果設為 `ignore-unhealthy`，則運作狀態不佳的執行個體不會在可用區域中以作用中區域轉移取代。

下列範例會在名為 的新 Auto Scaling 群組上啟用區域轉移*my-asg*。

```
aws autoscaling create-auto-scaling-group \
  --launch-template LaunchTemplateName=my-launch-template,Version='1' \
  --auto-scaling-group-name my-asg \
  --min-size 1 \
  --max-size 10 \
  --desired-capacity 5 \
  --availability-zones us-east-1a us-east-1b us-east-1c \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

Console

在現有群組上啟用區域轉移 （主控台）

1. 前往網址 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台，然後從導覽窗格中選擇 Auto Scaling 群組。
2. 在畫面頂端的導覽列上，選擇您在其中建立 Auto Scaling 群組 AWS 區域 的 。
3. 選取 Auto Scaling 群組旁的核取方塊。

   頁面底部會開啟一個分割窗格。

4. 在整合索引標籤的 ARC 區域轉移下，選擇編輯。
5. 選取核取方塊以啟用區域轉移。
6. 針對運作狀態檢查行為，選擇忽略運作狀態不佳或取代運作狀態不佳。
   - 如果運作狀態檢查行為設定為忽略運作狀態不佳，則運作狀態不佳的執行個體不會在可用區域中以作用中區域轉移取代。
   - 如果運作狀態檢查行為設定為取代運作狀態不佳，則運作狀態不佳的執行個體會在可用區域中以作用中區域轉移取代。
7. 選擇更新。

AWS CLI

在現有群組上啟用區域轉移 (AWS CLI)

將 `--availability-zone-impairment-policy` 參數新增至 update-auto-scaling-group 命令。

`--availability-zone-impairment-policy` 參數有兩個選項：

- ZonalShiftEnabled – 如果設定為 TRUE，Auto Scaling 會使用 ARC 區域轉移註冊 Auto Scaling 群組，您可以在 ARC 主控台上啟動、更新或取消區域轉移。如果設定為 FALSE，Auto Scaling 會從 ARC 區域轉移取消註冊 Auto Scaling 群組。您必須已啟用區域轉移，才能將其設定為 FALSE。
- ImpairedZoneHealthCheckBehavior – 如果設定為 `replace-unhealthy`，運作狀態不佳的執行個體將在可用區域中取代為作用中區域轉移。如果設為 `ignore-unhealthy`，則運作狀態不佳的執行個體將不會在可用區域中以作用中區域轉移取代。

下列範例會在指定的 Auto Scaling 群組上啟用區域轉移。

```
aws autoscaling update-auto-scaling-group --auto-scaling-group-name my-asg \
  --availability-zone-impairment-policy '{
      "ZonalShiftEnabled": true,
      "ImpairedZoneHealthCheckBehavior": IgnoreUnhealthy
    }'
```

若要啟動區域轉移，請參閱 啟動、更新或取消區域轉移。

Auto Scaling 群組的區域轉移運作方式

假設您有具有下列可用區域的 Auto Scaling 群組：

- us-east-1a
- us-east-1b
- us-east-1c

您注意到 中的失敗us-east-1a並開始區域轉移。在 中啟動區域轉移時，會發生下列行為us-east-1a。

- 向外擴展 – Auto Scaling 會在運作狀態良好的可用區域 (us-east-1b 和) 中啟動所有新的容量請求us-east-1c。
- 動態擴展 – Auto Scaling 可防止擴展政策減少所需的容量。Auto Scaling 不會阻止擴展政策增加所需的容量。
- 執行個體重新整理 – Auto Scaling 會對作用中區域轉移期間延遲的任何執行個體重新整理程序延長逾時。

可用區域運作狀態檢查行為選擇受損	運作狀態檢查行為
Replace unhealthy	Instances that appear unhealthy will be replaced in all Availability Zones (us-east-1a , us-east-1b , and us-east-1c).
Ignore unhealthy	Instances that appear unhealthy will be replaced in us-east-1b and us-east-1c . Instances are not replaced in the Availability Zone with the active zonal shift (us-east-1a).

使用區域轉移的最佳實務

若要在使用區域轉移時維持應用程式的高可用性，我們建議採用下列最佳實務。

- 監控 EventBridge 通知，以判斷何時持續發生可用區域受損事件。如需詳細資訊，請參閱使用 EventBridge 自動化 Amazon EC2 Auto Scaling。

- 使用具有適當閾值的擴展政策，以確保您有足夠的容量來容忍遺失可用區域。
- 設定運作狀態最低百分比為 100 的執行個體維護政策。使用此設定，Auto Scaling 會等待新執行個體準備就緒，再終止運作狀態不佳的執行個體。

對於預先擴展的客戶，我們也建議使用下列項目：

- 選取忽略運作狀態不佳做為受損可用區域的運作狀態檢查行為，因為您在受損事件期間不需要取代運作狀態不佳的執行個體。
- 在 Auto Scaling 群組的 ARC 中使用區域自動轉移。中的區域自動轉移功能 Amazon 應用程式復原控制器 (ARC) 可讓 在 AWS 偵測到可用區域中的受損時， AWS 將資源的流量移離可用區域。如需詳細資訊，請參閱ARC 中的區域自動轉移。

對於具有跨區域停用負載平衡器的客戶，我們也建議：

- 僅針對您的可用區域分佈使用平衡。
- 如果您在 Auto Scaling 群組和負載平衡器上使用區域轉移，請務必先取消 Auto Scaling 群組上的區域轉移。然後，請等到容量在所有可用區域之間達到平衡。 再取消負載平衡器上的區域轉移。
- 由於啟用區域轉移並使用跨區域停用的負載平衡器時，容量可能會不平衡，因此 Auto Scaling 具有額外的驗證。如果您遵循最佳實務，您可以透過選取 中的核取方塊 AWS 管理主控台或使用 `CreateAutoScalingGroup`、 或 中的 `skip-zonal-shift-validation`旗標`UpdateAutoScalingGroup`來確認此可能性`AttachTrafficSources`。

Amazon Elastic Kubernetes Service

Amazon EKS 提供的功能可讓您讓應用程式對運作狀態降低或可用區域受損等事件更具彈性。當您在 Amazon EKS 叢集中執行工作負載時，您可以使用區域轉移或區域自動轉移，進一步改善應用程式環境的容錯能力和應用程式復原能力。

搭配 Amazon Elastic Kubernetes Service 使用區域轉移

若要啟用區域轉移，請使用下列其中一種方法。如需詳細資訊，請參閱《Amazon Elastic Kubernetes Service 使用者指南》中的了解 ARC 區域轉移。

Console

在新的 Amazon EKS 叢集上啟用區域轉移 （主控台）

1. 尋找您要向 ARC 註冊的 Amazon EKS 叢集名稱和區域。

2. 在 https://console.aws.amazon.com/eks/home#/clusters 開啟 Amazon EKS 主控台。
3. 選取您的叢集。
4. 在叢集資訊頁面上，選取概觀索引標籤。
5. 在區域轉移下，選擇管理。
6. 針對 EKS 區域轉移，選擇啟用或停用。

AWS CLI

在新的 Amazon EKS 叢集上啟用區域轉移 (AWS CLI)

- 輸入以下命令：

```
aws eks create-cluster --name my-eks-cluster --role-
arn my-role-arn-to-create-cluster --resources-vpc-config
 subnetIds=string,string,securityGroupIds=string,string,endpointPublicAccess=boolean,end
 --zonal-shift-config enabled=true
```

在現有的 Amazon EKS 叢集上啟用區域轉移 (AWS CLI)

- 輸入以下命令：

```
aws eks update-cluster-config --name my-eks-cluster --zonal-shift-config
 enabled=true
```

您可以為 Amazon EKS 叢集啟動區域轉移，也可以透過啟用區域自動轉移 AWS 來允許 為您執行。使用 ARC 啟用 Amazon EKS 叢集區域轉移後，您可以使用 ARC AWS 主控台、CLI 或區域轉移和區域自動轉移 APIs 啟動區域轉移或啟用區域自動轉移。

如需啟動區域轉移的詳細資訊，請參閱 啟動、更新或取消區域轉移。

如需使用區域轉移啟用 Amazon EKS 的詳細資訊，請參閱《Amazon Elastic Kubernetes Service 使用者指南》中的了解 Amazon EKS 中的 ARC 區域轉移。

Amazon Elastic Kubernetes Service 的區域轉移如何運作

在 Amazon EKS 區域轉移期間，會自動執行下列動作：

- 封鎖受影響可用區域中的所有節點。這可防止 Kubernetes 排程器將新的 Pod 排程到運作狀態不佳 AZ 中的節點。
- 如果您使用的是受管節點群組，可用區域重新平衡會暫停，而且 Auto Scaling 群組會更新，以確保新的 Amazon EKS 資料平面節點只會在運作狀態良好的AZs啟動。
- 運作狀態不佳的 AZ 中的節點不會終止，也不會從這些節點移出 Pod。這是為了確保區域轉移過期或取消時，您的流量可以安全地返回仍有完整容量的 AZ。
- EndpointSlice 控制器會在受損的 AZ 中找到所有 Pod 端點，並從相關的 EndpointSlices 中移除它們。此操作可確保僅鎖定運作狀態良好可用區域中的 Pod 端點，來接收網路流量。若區域轉移取消或到期，EndpointSlice 控制器將更新 EndpointSlices，以便在還原的可用區域中納入這些端點。

如需詳細資訊，請參閱AWS 容器部落格。

Application Load Balancer

使用 Application Load Balancer 的區域轉移

若要搭配區域轉移使用 Application Load Balancer，您必須在 Application Load Balancer 屬性中啟用 ARC 區域轉移整合。Application Load Balancer 支援跨區域啟用或跨區域停用組態的區域轉移。

啟用 ARC 整合並開始使用區域轉移之前，請檢閱下列資訊：

- 您只能針對單一可用區域，啟動特定負載平衡器的區域轉移。您無法為多個可用區域啟動區域轉移。
- AWS 當多個基礎設施問題影響 服務時， 會主動從 DNS 移除區域負載平衡器 IP 地址。在啟動區域轉移之前，請務必檢查目前的可用區域容量。
- 區域轉移不適用於單一可用區域目標群組。
- 當 Application Load Balancer 是 Network Load Balancer 的目標時，請務必從 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 將無法辨識轉移，並繼續將流量傳送至 Application Load Balancer。

您可以在 Elastic Load Balancing 主控台 （大部分為 AWS 區域) 或 ARC 主控台中啟動負載平衡器的區域轉移。

Console

在負載平衡器上啟用區域轉移 （主控台）

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。

2. 在導覽頁面的負載平衡下，選擇負載平衡器。
3. 選取 Application Load Balancer 名稱。
4. 在屬性索引標籤上，編輯。
5. 在可用區域路由組態下，針對 >ARC 區域轉移整合，選擇啟用。
6. 選擇儲存。

AWS CLI

在負載平衡器上啟用區域轉移 (AWS CLI)

- 輸入以下命令：

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-alb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

如需啟動區域轉移的詳細資訊，請參閱 啟動、更新或取消區域轉移。

您可以使用 keepalive選項來設定連線持續的時間長度。如需詳細資訊，請參閱《Application Load Balancer 使用者指南》中的 HTTP 用戶端保持連線持續時間。根據預設，Application Load Balancer 會將 HTTP 用戶端持續作用持續時間值設定為 3600 秒或 1 小時。我們建議您降低值，使其與應用程式的復原時間目標保持一致，例如 300 秒。當您選擇 HTTP 用戶端保持連線持續時間時，請考慮此值是在一般情況下更頻繁重新連線、可能影響延遲，以及更快速地將所有用戶端移離受損的 AZ 或區域之間的取捨。

Application Load Balancer 的區域轉移如何運作

在啟用跨區域負載平衡的 Application Load Balancer 上啟動區域轉移時，所有目標的流量都會在受影響的可用區域中遭到封鎖，而區域轉移會從 DNS 中移除區域 IP 地址。

如需詳細資訊，請參閱《Application Load Balancer 使用者指南》中的 Application Load Balancer 整合。

Network Load Balancer

使用 Network Load Balancer 的區域轉移

若要搭配區域轉移使用 Network Load Balancer，您必須在 Network Load Balancer 屬性中啟用 ARC 區域轉移整合。Network Load Balancer 支援跨區域啟用或跨區域停用組態的區域轉移。

您可以選擇加入哪些資源來使用區域轉移和區域自動轉移，以及何時想要從受損的可用區域失敗。支援面向網際網路和內部 Network Load Balancer。

若要為啟用跨區域 Network Load Balancer 啟用區域轉移，連接至負載平衡器的所有目標群組必須符合下列要求。

- 必須啟用跨區域負載平衡，或將 設定為 `use_load_balancer_configuration`。
  - 如需目標群組跨區域負載平衡的詳細資訊，請參閱目標群組的跨區域負載平衡。
- 目標群組通訊協定必須是 TCP 或 TLS。
  - 如需 Network Load Balancer 目標群組通訊協定的詳細資訊，請參閱路由組態。
- 必須停用運作狀態不佳目標的連線終止。
  - 如需目標群組連線終止的詳細資訊，請參閱運作狀態不佳目標的連線終止。
- 目標群組不得有任何 Application Load Balancer 做為目標。
  - 如需 Application Load Balancer 做為目標的詳細資訊，請參閱使用 Application Load Balancer 做為 Network Load Balancer 的目標。

您可以使用 AWS CLI AWS 管理主控台、 或 Elastic Load Balancing 小工具，啟動 Network Load Balancer 的區域轉移。當 Application Load Balancer 是 Network Load Balancer 的目標時，您必須從 Network Load Balancer 開始區域轉移。如果您從 Application Load Balancer 開始區域轉移，Network Load Balancer 不會停止將流量傳送至 Application Load Balancer 及其目標。

Console

在負載平衡器上啟用區域轉移 （主控台）

1. 前往 https://console.aws.amazon.com/ec2/ 開啟 Amazon EC2 主控台。
2. 在導覽頁面的負載平衡下，選擇負載平衡器。
3. 選取 Network Load Balancer 名稱。
4. 在屬性索引標籤中，選擇編輯。
5. 在可用區域路由組態下，針對 ARC 區域轉移整合，選擇啟用。
6. 選擇儲存。

AWS CLI

在負載平衡器上啟用區域轉移 (AWS CLI)

- 輸入以下命令：

```
aws elbv2 modify-load-balancer-attributes --load-balancer-arn my-nlb-arn --
attributes Key=zonal_shift.config.enabled,Value=true
```

如需啟動區域轉移的詳細資訊，請參閱 啟動、更新或取消區域轉移。

Network Load Balancer 的區域轉移運作方式

ARC 會為已註冊的 Network Load Balancer 建立運作狀態檢查失敗，以便在啟動區域轉移時，從 DNS 中移除受損 AZ 中的 Network Load Balancer 節點。Network Load Balancer 會停用受影響區域中的目標，使其停止接收流量，而 Elastic Load Balancing 會將這些目標視為區域轉移的已停用目標。處於停用狀態的目標會繼續接收運作狀態檢查。當目標運作狀態良好且區域轉移過期（或取消）時，路由至先前受損區域中的目標會繼續。

在啟用跨區域負載平衡的 Network Load Balancer 區域轉移期間，會從 DNS 中移除區域負載平衡器 IP 地址。與受損可用區域中目標的現有連線會持續存在，直到它們有機關閉，而新的連線不會再路由到受損可用區域中的目標。

如需詳細資訊，請參閱《Network Load Balancer 使用者指南》中的 Network Load Balancer 的區域轉移。 Load Balancer

啟動、更新或取消區域轉移

本節提供區域轉移的使用程序，包括啟動區域轉移和取消區域轉移。

啟動區域轉移

本節中的步驟說明如何在 Amazon Application Recovery Controller (ARC) 主控台上啟動客戶起始的區域轉移。若要以程式設計方式使用區域轉移，請參閱區域轉移 API 參考指南。

除了在 ARC 中啟動區域轉移之外，您也可以在 Elastic Load Balancing 主控台（在支援的區域中）中啟動負載平衡器的區域轉移。如需詳細資訊，請參閱 Elastic Load Balancing 使用者指南中的區域轉移。

啟動區域轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域轉移。
3. 在區域轉移頁面上，選擇開始區域轉移。
4. 選取您要從中轉移流量的可用區域。
5. 從資源資料表中選取支援的資源，以轉移流量。
6. 針對設定區域轉移過期，選擇或輸入區域轉移的過期。區域轉移最初可以設定為作用中 1 分鐘或最多三天 (72 小時）。

   所有區域轉移都是暫時的。您必須設定過期，但稍後可以更新作用中的輪班，將新的過期期間設定為最多三天。
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. 選取核取方塊，確認開始區域轉移會減少應用程式的可用容量，方法是將流量移離可用區域。
9. 選擇 開始使用。

更新或取消區域轉移

本節中的步驟說明如何更新您在 Amazon Application Recovery Controller (ARC) 主控台上啟動的區域轉移，或取消區域轉移。若要以程式設計方式使用區域轉移，請參閱區域轉移 API 參考指南。

您可以更新區域轉移以設定新的過期，或編輯或取代區域轉移的註解。您可以在區域轉移過期之前隨時取消區域轉移。

您可以取消您啟動的區域轉移，或為區域自動轉移實務執行的資源 AWS 啟動的區域轉移。若要進一步了解區域自動轉移中的練習轉移，請參閱 區域自動轉移和實務執行的運作方式。

更新區域轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域轉移。
3. 選取您要更新的區域轉移，然後選擇更新區域轉移。
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。

取消區域轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在異地同步備份下，選擇區域轉移。
3. 選取您要取消的區域轉移，然後選擇取消區域轉移。
4. 在確認模式對話方塊中，選擇確認。

在 Amazon Application Recovery Controller (ARC) 中記錄和監控區域轉移

您可以使用 在 Amazon Application Recovery Controller (ARC) 中 AWS CloudTrail 監控區域轉移，以分析模式並協助疑難排解問題。

主題

- 使用 記錄區域轉移 API 呼叫 AWS CloudTrail

使用 記錄區域轉移 API 呼叫 AWS CloudTrail

ARC 的區域轉移已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 ARC 中 AWS 服務所採取動作的記錄。CloudTrail 會將區域轉移的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 ARC 主控台的呼叫，以及對區域轉移的 ARC API 操作的程式碼呼叫。

如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括區域轉移的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 所收集的資訊，判斷針對區域轉移向 ARC 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的區域轉移資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當區域轉移在 ARC 中發生活動時，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他 AWS 服務事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

若要持續記錄 中的事件 AWS 帳戶，包括 ARC 中區域轉移的事件，請建立線索。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon

S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 ARC 動作，並記錄在 Amazon Application Recovery Controller 的路由控制 API 參考指南中。例如，對 `StartZonalShift` 以及 `ListManagedResources` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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：

- 請求是使用根或 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 userIdentity 元素。

在事件歷史記錄中檢視 ARC 事件

CloudTrail 可讓您使用 Event history (事件歷史記錄) 檢視最近的事件。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。

了解區域轉移日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範區域轉移`ListManagedResources`的動作。

```
{
      "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": "2022-11-14T16:14:41Z",
      "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 CloudTrail 日誌項目，示範具有區域轉移衝突例外StartZonalShift狀況的動作。


```
{
      "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"
      }
    }
```

ARC 中區域轉移的 Identity and Access Management

AWS Identity and Access Management (IAM) 是一種 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目錄

- 區域轉移如何與 IAM 搭配使用
- 區域轉移的 IAM 和許可
- ARC 中區域轉移的身分型政策範例

區域轉移如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon Application Recovery Controller (ARC) 中區域轉移的存取權之前，請先了解哪些 IAM 功能可與區域轉移搭配使用。

您可以搭配區域轉移使用的 IAM 功能

IAM 功能	區域轉移支援
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

IAM 功能	區域轉移支援
主體許可	是
服務角色	否
服務連結角色	是

若要取得 AWS 服務如何與大多數 IAM 功能搭配使用的高階整體檢視，請參閱《IAM 使用者指南》中的與 IAM AWS 搭配使用的 服務。

ARC 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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 ARC 身分型政策的範例，請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例。

ARC 內的資源型政策

支援資源型政策：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。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 ARC 動作清單，請參閱《服務授權參考》中的 Amazon Route 53 區域轉移定義的動作。

ARC 中區域轉移的政策動作在動作之前使用下列字首：

```
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，下列項目：

```
"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*"
```

若要檢視區域轉移的 ARC 身分型政策範例，請參閱 ARC 中區域轉移的身分型政策範例。

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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看資源類型及其 ARNs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 Route 53 定義的動作 - 區域轉移

若要查看可與條件索引鍵搭配使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon Route 53 - 區域轉移定義的條件索引鍵

若要檢視區域轉移的 ARC 身分型政策範例，請參閱 ARC 中區域轉移的身分型政策範例。

區域轉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` 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看區域轉移條件索引鍵的清單，請參閱服務授權參考中的下列主題：

- Amazon Route 53 - 區域轉移定義的條件索引鍵

若要查看可與條件金鑰搭配使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon Route 53 定義的動作 - 區域轉移
- Amazon Route 53 定義的資源類型 - 區域轉移

若要檢視區域轉移的 ARC 身分型政策範例，請參閱 ARC 中區域轉移的身分型政策範例。

ARC 中的存取控制清單 (ACLs)

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。

使用 ARC 的屬性型存取控制 (ABAC)

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，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

ARC 包含下列對 ABAC 的部分支援：

- 區域轉移支援在 ARC 中為區域轉移註冊的受管資源 ABAC。如需有關 ABAC for Network Load Balancer 和 Application Load Balancer 受管資源的詳細資訊，請參閱Elastic Load Balancing 使用者指南》中的 ABAC with Elastic Load Balancing。

搭配 ARC 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

ARC 的跨服務主體許可

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，您會被視為委託人。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政策中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon Route 53 區域轉移

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

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 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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 Amazon Application Recovery Controller (ARC) 中區域轉移功能許可運作方式的額外資訊，特別是當您使用來自 Elastic Load Balancing 等 AWS 其他服務的功能時。若要了解 ARC 功能如何使用 IAM 和一般許可，請檢閱概觀主題 中的資訊ARC 中區域轉移的 Identity and Access Management。

區域轉移支援 Application Load Balancer、Network Load Balancer、Amazon EC2 Auto Scaling 群組和 Amazon EKS。您可以使用 IAM 條件金鑰，將 IAM 許可政策範圍限定為這些資源。以下是使用具有多種不同類型資源之條件索引鍵的範例政策：

```
{
    "Condition": {
        "StringLike": {
            "arc-zonal-shift:ResourceIdentifier": [
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/net/
*",
                "arn:aws:elasticloadbalancing:us-east-1:123456789012:loadbalancer/app/
*",
                "arn:aws:eks:us-east-1:123456789012:cluster/*"
            ]
        }
    },
    "Action": [
        "arc-zonal-shift:StartZonalShift"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
```

如需詳細資訊，請參閱支援的資源。

除了 IAM 概觀主題中概述的許可之外，下列適用於 IAM 和許可的區域轉移：

- 請確定您擁有在 ARC 中使用區域轉移所需的許可。如需詳細資訊，請參閱區域轉移主控台存取和區域轉移操作存取。
- 您不需要使用 IAM 新增額外的 Elastic Load Balancing 許可，即可在 ARC 中使用帳戶中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 受管政策包含使用區域轉移的許可。如果您將 AWS 受管政策用於 Elastic Load Balancing 存取，則不需要 IAM 中的其他許可，即可進行區域轉移，以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 AWS Elastic Load Balancing 的 受管政策。

ARC 中區域轉移的身分型政策範例

根據預設，使用者和角色沒有建立或修改 ARC 資源的許可。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。

如需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 (主控台)。

如需 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 ARNs 格式，請參閱《服務授權參考》中的 Amazon Application Recovery Controller (ARC) 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 範例：區域輪班主控台存取
- 範例：區域轉移 API 動作

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 等使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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：區域輪班主控台存取

若要存取 Amazon Application Recovery Controller (ARC) 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 ARC 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。

若要授予使用者在 中使用區域轉移的完整存取權 AWS 管理主控台，請將如下所示的政策連接到使用者：

JSON

```
{
    "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：區域轉移 API 動作

區域轉移 API 會暫時將流量移離可用區域，以復原應用程式。

為了確保使用者可以使用區域轉移 API 動作，請連接對應至使用者需要使用的 API 操作的政策，例如下列項目：

JSON

```
{
    "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": "*"
        }
    ]
}
```

ARC 中的區域自動轉移

使用區域自動轉移時，您授權 AWS 代表您在事件期間從可用區域 (AZ) 轉移應用程式的資源流量，以協助縮短復原時間。當內部遙測顯示有可能影響客戶的可用區域受損時， 會 AWS 啟動自動轉移。當 AWS 啟動自動轉移時，您為區域自動轉移設定之資源的應用程式流量會開始從可用區域轉移。

請注意，ARC 不會檢查個別資源的運作狀態。 AWS 當遙測偵測到有可能影響客戶的可用區域受損時， 會 AWS 啟動自動轉移。在某些情況下，對於沒有影響的資源，流量可能會轉移。

使用區域自動轉移，您也可以授權 代表您從可用區域 AWS 轉移應用程式的資源流量，以進行定期實務執行。區域自動轉移需要練習執行。ARC 針對實務執行啟動的區域轉移，可協助您確保在自動轉移期間從可用區域轉移流量對您的應用程式是安全的。實務會定期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，方法是啟動區域轉移，將資源的流量移離可用區域。練習每週執行一次，並提供 SUCCEEDED或 等結果FAILED，以協助您了解應用程式是否如預期運作。

> **Important**
>
> 在您設定實務執行或啟用區域自動轉移之前，強烈建議您在部署應用程式資源的區域中，預先擴展所有可用區域中的應用程式資源容量。當自動轉移或實務執行開始時，您不應依賴擴展需求。區域自動轉移，包括練習執行、獨立運作，而且不會等待自動擴展動作完成。依賴自動擴展而不是預先擴展，可能會導致應用程式需要更長的時間才能復原。
> 如果您使用自動擴展來處理定期的流量週期，強烈建議您設定自動擴展的最低容量，以便在失去可用區域的情況下繼續正常運作。

如果您打算啟用區域自動轉移或設定實務執行，請在預先擴展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。若要測試這一點，請啟動區域轉移，將資源的流量移離可用區域。

啟用區域自動轉移後，建議您啟動並評估隨需實務執行區域轉移，以驗證您的應用程式是否可在流量移離可用區域的情況下繼續正常運作。然後，ARC 執行的常規實務會協助您持續確認您是否有足夠的容量進行自動轉移。

為了確保具有區域轉移的測試有效，請務必驗證流量是否如預期從您轉移的 AZ 耗盡。例如，Application Load Balancer 和 Network Load Balancer 都會在 Amazon CloudWatch 中提供每個可

用區域指標，供您用來監控。根據服務和用戶端重複使用連線的時間長度，流量可能會繼續轉移到您移離的 AZ 的時間超過預期。若要進一步了解，請參閱限制用戶端與您的端點保持連線的時間。

您可以在 ARC 主控台中為支援的資源啟用區域自動轉移。或者，在 Amazon EC2 主控台中，您可以選擇為特定負載平衡器資源啟用區域自動轉移。若要進一步了解如何使用 Elastic Load Balancing 啟用區域自動轉移，請參閱Elastic Load Balancing 使用者指南》中的區域轉移。

自動轉移和練習執行區域轉移是暫時的。透過自動轉移，當受影響的可用區域復原時， 會 AWS 停止將資源流量從可用區域轉移。客戶的應用程式流量會返回 區域中的所有可用區域。透過練習執行，流量會從單一資源的可用區域轉移約 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，以提醒您自動轉移和練習執行。如需詳細資訊，請參閱搭配 Amazon EventBridge 使用區域自動轉移。

區域自動轉移和實務執行的運作方式

Amazon Application Recovery Controller (ARC) 中的區域自動轉移功能允許 代表您將資源的流量 AWS 移離可用區域，當 AWS 判斷存在可能影響可用區域中客戶的損害時。區域自動轉移是專為在 中所有可用區域中預先擴展的資源所設計 AWS 區域，因此應用程式可以在失去一個可用區域的情況下正常運作。

使用區域自動轉移時，您需要設定實務執行，其中 ARC 會定期將資源的流量從一個可用區域轉移。對於具有與其相關聯之實務執行組態的每個資源，ARC 排程實務大約每週執行一次。每個資源的練習執行會獨立排程。

對於每個練習執行，ARC 會記錄結果。如果實務執行因封鎖條件而中斷，實務執行結果不會標示為成功。如需練習執行結果的詳細資訊，請參閱練習執行的結果。

您可以設定 Amazon EventBridge 通知，以傳送自動轉移和練習執行的相關資訊給您。如需詳細資訊，請參閱搭配 Amazon EventBridge 使用區域自動轉移。

目錄

- 關於區域自動轉移
- 當 AWS 啟動和停止自動轉移
- 當 ARC 排程、開始和結束練習執行時
- 練習執行的容量檢查
- 實務執行和自動轉移的通知
- 區域輪班的優先順序

- 停止資源的作用中自動轉移或實務執行
- 如何轉移流量
- 練習執行的警示
- 封鎖的視窗和允許的視窗 (UTC)

關於區域自動轉移

區域自動轉移是一項功能，其中 會代表您將應用程式資源流量 AWS 移離可用區域。當內部遙測顯示存在可能影響客戶的可用區域受損時， 會 AWS 啟動自動轉移。內部遙測包含來自多個來源的指標，包括 AWS 網路，以及 Amazon EC2 和 Elastic Load Balancing 服務。

您必須為支援 AWS 的資源手動啟用區域自動轉移。

當您在區域多個 （通常為三個） AZs 的負載平衡器上部署和執行 AWS 應用程式，並且預先擴展以支援靜態穩定性時， AWS 可以透過自動轉移轉移流量來快速復原 AZ 中的客戶應用程式。透過將資源流量轉移到 區域中的其他 AZs， AWS 可以減少因停電、AZ 中的硬體或軟體問題或其他損害所造成的潛在影響的持續時間和嚴重性。

ARC 支援的資源提供將指定 AZ 標記為運作狀態不佳的整合，這會導致流量移離受損的 AZ。

當您為資源啟用區域自動轉移時，您還必須為資源設定練習執行。 AWS 會執行大約每週一次的練習執行 30 分鐘，以協助您確保您有足夠的容量執行應用程式，而沒有 區域中的其中一個可用區域。

如同區域轉移，在少數特定情況下，區域自動轉移不會將流量移離可用區域。例如，如果 AZs 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佳，則負載平衡器會處於故障開啟狀態，您無法轉移其中一個 AZs。

若要進一步了解區域自動轉移，請參閱ARC 中的區域自動轉移。

當 AWS 啟動和停止自動轉移

當您為資源啟用區域自動轉移時，您授權 AWS 代表您在事件期間從可用區域轉移應用程式的資源流量，以協助縮短復原時間。

為了達成此目的，區域自動轉移會使用 AWS 遙測功能，盡早偵測是否存在可能影響客戶的可用區域受損。當 AWS 啟動自動轉移時，對已設定資源的流量會立即開始從可能影響客戶的受損可用區域轉移。

區域自動轉移是一項功能，專為已針對 中的所有可用區域預先擴展其應用程式資源的客戶而設計 AWS 區域。當自動轉移或實務執行開始時，您不應依賴擴展需求。

AWS 會在判斷可用區域已復原時結束自動轉移。

當 ARC 排程、開始和結束練習執行時

ARC 會每週排程資源的實務執行約 30 分鐘。ARC 會個別排程、啟動和管理每個資源的實務執行。ARC 不會同時批次處理相同帳戶中資源的實務執行。您也可以自行開始隨需練習執行，以協助確認您的設定對區域自動轉移事件是否安全。

當實務執行在預期持續時間內繼續進行，而不會中斷時，它會以 的結果來標記SUCCESSFUL。還有幾個其他可能的結果：FAILED、 INTERRUPTEDCAPACITY_CHECK_FAILED和 PENDING。結果值和描述包含在練習執行的結果區段中。

在某些情況下，ARC 會中斷實務執行並結束。例如，如果自動轉移在實務執行期間啟動，ARC 會中斷實務執行並結束。另一個範例是，假設資源對實務執行有不利的回應，並導致您指定用來監控實務執行的警示進入 ALARM 狀態。在此案例中，ARC 也會中斷實務執行並結束。

此外，在幾種情況下，ARC 不會開始資源的排程實務執行。

為了回應資源的中斷和封鎖實務執行，ARC 會執行下列動作：

- 如果資源的實務執行在進行中時中斷，ARC 會將每週實務執行視為結束，並為資源排程下週的新實務執行。每週實務成果INTERRUPTED在此案例中，而不是 FAILED。FAILED 只有在監控練習執行的結果警示在練習執行期間進入 ALARM 狀態時，練習執行結果才會設為 。
- 如果資源的實務執行排定啟動時有封鎖限制，ARC 不會啟動實務執行。ARC 會繼續定期監控，以判斷是否仍有一或多個封鎖限制條件。當沒有任何封鎖限制時，ARC 會開始資源的實務執行。

以下是阻止 ARC 啟動或繼續資源實務執行的封鎖限制範例：

- 進行 AWS Fault Injection Service 實驗時，ARC 不會啟動或繼續練習執行。如果 AWS FIS 事件在 ARC 已排定實務執行啟動時處於作用中狀態，ARC 不會啟動實務執行。ARC 會在整個實務執行期間監控封鎖限制，包括 AWS FIS 事件。如果 AWS FIS 事件在實務執行作用中時啟動，ARC 會結束實務執行，並且不會嘗試啟動另一個練習，直到資源的下一個定期排程實務執行為止。
- 如果區域中目前有 AWS 事件，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，ARC 會照常排程一週內的下一個練習執行。如果實務執行因為封鎖限制而未啟動，例如您指定的 AWS FIS 實驗或封鎖時段，ARC 會繼續嘗試啟動實務執行，直到可啟動實務執行為止。

練習執行的容量檢查

當實務執行開始時，為了暫時將流量移離可用區域，ARC 會執行檢查，以確認您在其他可用區域中有足夠的容量，以安全地將流量移離可用區域。如果沒有足夠的可用容量，則練習執行的流量轉移不會啟動，練習執行也會結束。

此外，在 ARC 結束自動轉移啟動的流量轉移之前，ARC 會在區域自動轉移完成時執行負載平衡器資源的容量檢查。如果容量檢查在自動轉移結束時失敗，流量不會移回移出的可用區域。

只有負載平衡器和 Auto Scaling 群組才能完成平衡容量檢查。

對於負載平衡器資源，容量檢查會驗證與負載平衡器相關聯的運作狀態良好的主機是否分散在可用區域。具體而言，容量檢查可確保註冊資源的所有可用區域中運作狀態良好的主機數量都已平衡。對於容量檢查，平衡表示每個可用區域的運作狀態良好容量與其他區域相同，在小變異數內。

請注意，容量檢查不會套用到具有 Lambda 類型之目標群組的負載平衡器，也不會套用到 Application Load Balancer，因為這些目標不會按區域設定。

Auto Scaling 群組也會完成容量檢查。對於 Auto Scaling 群組，容量檢查會驗證 Auto Scaling 群組的運作狀態良好的區域總容量，也就是所有可用區域中運作狀態良好的主機總數，符合該 Auto Scaling 群組所需的容量集。

當容量檢查失敗時

當容量檢查發現資源的可用容量未平衡時，練習執行的結果為 CAPACITY_CHECK_FAILED。若要進一步了解為什麼容量檢查失敗，請參閱 的註解欄位ZonalShiftSummary。若要尋找練習執行區域轉移的註解欄位，請執行下列動作：

1. 使用 AWS CLI，列出您在使用 ListZonalShifts API 操作之實務執行中指定的資源的區域轉移。

   FOr 範例，若要傳回區域轉移，您可以執行類似下列的命令：

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

2. 檢閱傳回的ZonalShiftSummary物件陣列，尋找因容量檢查而失敗之實務執行的區域轉移。
3. 對於適用的區域轉移，請檢閱 Comment 欄位中的資訊。

實務執行和自動轉移的通知

您可以透過設定 Amazon EventBridge 通知，選擇收到資源練習執行和自動轉移的通知。即使您尚未為任何資源啟用區域自動轉移，也稱為自動轉移觀察器通知，也可以設定 EventBridge 通知。 透過自動轉移觀察器通知，您會收到 ARC 在可用區域可能受損時啟動的所有自動轉移通知。請注意，您必須在 AWS 區域 要接收通知的每個 中設定此選項。

若要查看啟用自動轉移觀察器通知的步驟，請參閱 啟用或停用自動轉移觀察器通知。若要進一步了解通知選項以及如何在 EventBridge 中設定這些選項，請參閱 搭配 Amazon EventBridge 使用區域自動轉移。

區域輪班的優先順序

在特定時間不能有多個套用的區域轉移。也就是說，只有一個實務會執行資源的區域轉移、客戶起始的區域轉移、自動轉移或 AWS FIS 實驗。啟動第二個區域轉移時，ARC 會遵循優先順序來判斷資源的有效區域轉移類型。

優先順序的一般原則是您以客戶身分開始的分區輪班優先於其他輪班類型。不過，請注意，目前執行AWS的練習執行會阻止您啟動隨需練習執行。

若要說明 ARC 中的優先順序，下列是優先順序在範例案例中的運作方式：

已套用區域轉移類型	區域轉移類型已啟動	結果
AWS FIS 實驗	練習執行	實務執行將無法開始，因為 AWS FIS 實驗優先。
AWS FIS 實驗	手動區域轉移	AWS FIS 實驗將被取消，並將套用手動區域轉移。
AWS FIS 實驗	區域自動轉移	AWS FIS 實驗將被取消，並將套用區域自動轉移。
AWS FIS 實驗	AWS FIS 實驗	啟動的 AWS FIS 實驗將無法啟動，因為有執行中的現有實驗觸發了 AWS FIS 自動轉移動作。

已套用區域轉移類型	區域轉移類型已啟動	結果
練習執行	手動區域轉移	練習執行將取消，並將結果設定為 INTERRUPTED ，並將套用區域轉移。
練習執行	AWS FIS 實驗	練習執行將取消，並將結果設定為 INTERRUPTED ，並將 AWS FIS 套用實驗。
練習執行	區域自動轉移	練習執行將取消，並將結果設定為 INTERRUPTED ，並將套用區域自動轉移。
手動區域轉移	練習執行	練習執行將無法啟動。
手動區域轉移	AWS FIS 實驗	AWS FIS 實驗將無法啟動，或者如果已經在進行中，則無法啟動。
手動區域轉移	區域自動轉移	區域自動轉移將ACTIVE不在資源APPLIED上。手動區域轉移優先。
區域自動轉移	AWS FIS 實驗	AWS FIS 實驗將無法啟動，或者如果正在進行，將會失敗。
區域自動轉移	手動區域轉移	區域自動轉移將ACTIVE不在資源APPLIED上。手動區域轉移優先。
區域自動轉移	練習執行	實務執行將無法啟動，因為區域自動轉移優先。

目前對資源生效的流量轉移，其套用的區域轉移狀態會設定為 APPLIED。任何時候都只會有一種轉移設定為 APPLIED。其他進行中的輪班會設定為 NOT_APPLIED，但仍保持 ACTIVE 狀態。

停止資源的作用中自動轉移或實務執行

若要停止資源正在進行的自動轉移，您必須取消區域轉移。

依相同的排程，資源仍會定期執行實務。如果您想要在停用自動轉移之外停止練習執行，您必須刪除與資源相關聯的練習執行組態。

當您刪除實務執行組態時， 會 AWS 停止執行實務執行，每週將資源的流量從可用區域轉移。此外，由於區域自動轉移需要練習執行，當您使用 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轉移。不過，請注意，如果您使用區域自動轉移 API 刪除實務執行，您必須先停用資源的區域自動轉移。

如需詳細資訊，請參閱取消區域自動轉移及啟用和使用區域自動轉移。

如何轉移流量

對於自動轉移和練習執行區域轉移，流量會使用 ARC 用於客戶起始區域轉移的相同機制，從可用區域轉移。運作狀態檢查不佳會導致 Amazon Route 53 從 DNS 撤銷資源的對應 IP 地址，以便從可用區域重新導向流量。新的連線現在改為路由至 中的其他可用區域 AWS 區域 。

使用自動轉移時，當可用區域復原並 AWS 決定結束自動轉移時，ARC 會反轉運作狀態檢查程序，請求還原 Route 53 運作狀態檢查。然後，會還原原始區域 IP 地址，如果運作狀態檢查持續正常，則可用區域會再次包含在應用程式的路由中。

請務必注意，自動轉移並非以監控負載平衡器或應用程式基礎運作狀態的運作狀態檢查為基礎。ARC 使用運作狀態檢查將流量從可用區域移開，方法是請求運作狀態檢查設定為運作狀態不佳，然後在結束自動轉移或區域轉移時，再次將運作狀態檢查還原為正常。

練習執行的警示

您可以為區域自動轉移中的實務執行指定兩種類型的 CloudWatch 警示：結果警示和封鎖警示。

結果警示 （必要）

對於第一個類型的警示，結果警示，至少需要指定一個警示。當流量在每個 30 分鐘練習執行期間移離可用區域時，您應該設定結果警示來監控應用程式的運作狀態。

若要讓實務執行有效，請至少指定一個符合下列兩個條件的 CloudWatch 警示做為結果警示：

警示會監控資源或應用程式的指標

AND

當您的應用程式因失去一個可用區域而受到負面影響時，警示會以 ALARM 狀態回應。

如需詳細資訊，請參閱 中您為練習執行指定的警示一節設定區域自動轉移時的最佳實務。

結果警示也提供 ARC 針對每個練習執行所回報的練習執行結果資訊。如果結果警示進入 ALARM 狀態，ARC 會結束練習執行，並傳回 的練習執行結果FAILED。如果練習執行完成 30 分鐘的測試期間，而且您指定的任何結果警示都未進入 ALARM 狀態，則傳回的結果為 SUCCEEDED。所有結果值的清單以及說明，都會在練習執行的結果區段中提供。

封鎖警示 （選用）

或者，您可以指定第二類警示，即封鎖警示。當一或多個警示處於 ALARM 狀態時，封鎖警示區塊實務會從開始或繼續執行。當至少一個警示處於 ALARM 狀態時，封鎖警示區塊練習執行流量轉移，使其無法啟動，並停止任何進行中的練習執行。

例如，在具有多個微服務的大型架構中，當一個微服務發生問題時，您通常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。您可以在 ARC 中新增封鎖警示來完成此操作。

封鎖的視窗和允許的視窗 (UTC)

您可以選擇封鎖或允許特定行事曆日期或特定時段的練習執行，也就是 UTC 中指定的日期和時間。

例如，如果您有排定在 2024 年 5 月 1 日啟動的應用程式更新，而且您不希望此時練習執行將流量移出，您可以設定 的封鎖日期2024-05-01。

或者，假設您每週執行三天的業務報告摘要。在此案例中，您可以將下列週期性日期和時間設定為封鎖時段，例如，在 UTC 中：MON-20:30-21:30 WED-20:30-21:30 FRI-20:30-21:30。

或者，您也可以決定星期三和星期五從中午到 5：00 是 ARC 開始練習執行的最佳時間，以測試您的設定。在此案例中，您可以將下列週期性日期和時間設定為允許的時段，例如，在 UTC 中：WED-12:00-17:00 FRI-12:00-17:00。

AWS 區域 區域自動轉移的可用性

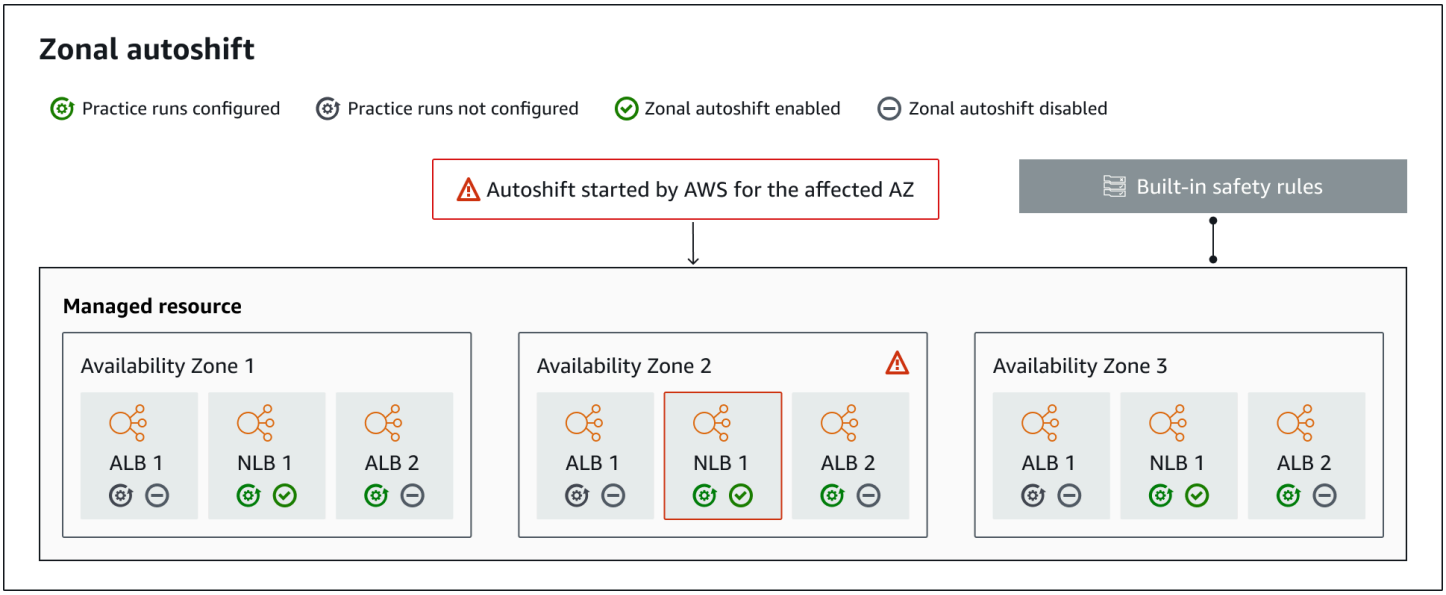
區域轉移和區域自動轉移目前可在商業 AWS 區域以及中國區域使用，也就是中國 （北京） 區域和中國 （寧夏） 區域。

使用 Amazon Application Recovery Controller (ARC) 的資源可能包含其他考量事項。如需詳細資訊，請參閱支援的資源。

如需 ARC 區域支援和服務端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Application Recovery Controller (ARC) 端點和配額。

區域自動轉移元件

下圖說明自動轉移流量移離可用區域的範例。當內部遙測顯示存在可能影響客戶的可用區域受損時，會 AWS 啟動自動轉移。



以下是 ARC 中區域自動轉移功能的元件。

區域自動轉移

區域自動轉移會轉移資源的流量，而不需要您採取任何動作。區域自動轉移是 ARC 的一項功能，當內部遙測顯示存在可能影響客戶的可用區域受損時， 會 AWS 啟動自動轉移。請注意，在某些情況下，資源可能會轉移，而不會產生影響。

練習執行

當您為資源啟用區域自動轉移時，您還必須為資源設定區域自動轉移實務執行。 會為實務 AWS 執行區域轉移大約每週執行約 30 分鐘。您也可以排程隨需執行的練習。

實務執行可確保您的應用程式可以正常執行，並遺失一個可用區域。在實務執行中， 會使用區域轉移將資源的流量 AWS 移離一個可用區域，然後在實務執行結束時將流量移返。

練習執行組態

使用練習執行組態，您可以定義 ARC 何時可以為具有區域自動轉移的資源開始練習執行的時間範圍（封鎖或允許的時段）。您也可以定義 AWS 實務執行的 CloudWatch 警示。您可以隨時編輯練習執行組態、新增或變更封鎖或允許的時段，或更新練習執行的警示。

若要啟用區域自動轉移，您必須為資源設定實務執行組態。

您可以刪除實務執行，但首先必須停用區域自動轉移。

練習執行警示

當您設定實務執行時，您可以根據您的資源和應用程式需求，指定 CloudWatch 警示（您第一次在 CloudWatch 中建立的警示）。如果您的應用程式受到練習執行的負面影響，您指定的警示可能會封鎖練習執行的開始，或可以停止進行中的練習執行。

如果您指定的警示進入 ALARM 狀態，ARC 會結束實務執行的區域轉移，讓資源的流量不會再從可用區域轉移。

您為練習執行指定的警示有兩種類型：結果警示、在練習執行期間監控資源和應用程式的運作狀態，以及封鎖警示，您可以設定這些警示來防止練習執行開始，或停止進行中練習執行。至少需要一個結果警示；封鎖警示是選用的。

練習執行結果

ARC 會報告每個實務執行的結果。以下是可能的演練結果：

- 待定：實務執行的區域轉移為作用中（進行中）。尚無結果可傳回。
- SUCCEEDED：結果警示未在練習執行期間進入 ALARM 狀態，且練習執行已完成完整的 30 分鐘測試期間。
- INTERRUPTED：由於不是結果警示進入 ALARM 狀態的原因，實務執行結束。演練可能因各種不同的原因而中斷。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 INTERRUPTED 結果的原因詳細資訊，請參閱演練的結果。
- 失敗：在演練期間結果警示進入 ALARM 狀態。
- CAPACITY_CHECK_FAILED：對負載平衡和 Auto Scaling 群組資源在可用區域之間平衡容量檢查失敗。

內建安全規則

ARC 內建的安全規則可防止資源一次發生多個流量轉移。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（由 AWS 客戶啟動或由客戶啟動），或資源的自動轉移可以主動將流量移離可用區域。例如，如果您在資源目前以自動轉移轉移時啟動該資源的區域轉移，則您的區域轉移優先。如需詳細資訊，請參閱區域輪班的優先順序。

資源識別符

要啟用區域自動轉移之資源的識別符，即資源的 Amazon Resource Name (ARN)。您只能為 ARC 支援之服務中的 帳戶中 AWS 的資源啟用區域自動轉移。

受管資源

Application Load Balancer 會自動向 ARC 註冊資源以進行區域自動轉移。您必須手動選擇加入其他資源以進行區域自動轉移。

資源名稱

ARC 中受管資源的名稱。

套用狀態

套用的狀態指出資源的流量轉移是否有效。當您設定區域自動轉移時，資源可以有多個作用中流量轉移，也就是練習執行區域轉移、客戶起始的區域轉移或自動轉移。不過，一次只會套用一個資源生效的 ，也就是 。狀態為 的轉移會APPLIED決定資源的應用程式流量已轉移的可用區域，以及該流量轉移何時結束。

輪班類型

定義區域轉移類型。區域輪班可以有下列其中一種類型：

- ZONAL_SHIFT
- ZONAL_AUTOSHIFT
- 練習_RUN
- FIS_EXPERIMENT

區域自動轉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依賴的機制具有高度可用性，以便在災難情況下需要它們時使用。一般而言，您應該盡可能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，了解服務的功能如何在控制平面和資料平面之間分割，以及何時可以使用服務的資料平面依賴極端可靠性。

一般而言，控制平面可讓您執行基本管理功能，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。

如需資料平面、控制平面以及 如何 AWS 建置服務以滿足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白皮書。

ARC 中區域自動轉移的定價

對於區域自動轉移， 會在 AWS 判斷存在可能對客戶應用程式造成負面影響的潛在問題時，代表您 AWS 轉移來自可用區域的流量以取得支援的資源。啟用區域自動轉移無需額外費用。

如需 ARC 和定價範例的詳細定價資訊，請參閱 ARC 定價。

設定區域自動轉移時的最佳實務

當您在 Amazon Application Recovery Controller (ARC) 中啟用區域自動轉移時，請注意下列最佳實務和考量事項。

區域自動轉移包含兩種類型的流量轉移：自動轉移和練習執行區域轉移。

- 透過自動轉移， 可在事件期間代表您從可用區域轉移應用程式資源流量， AWS 協助縮短復原時間。
- 透過練習執行，ARC 會代表您啟動區域轉移，或您啟動區域轉移練習執行。 AWS 練習執行區域轉移會將流量從資源的可用區域轉移，然後每週再次返回。實務執行可協助您確保已為區域中的可用區域擴展足夠的容量，讓您的應用程式可容忍遺失一個可用區域。

在自動轉移和實務執行中，有幾個最佳實務和考量事項需要記住。在啟用區域自動轉移或設定資源的實務執行之前，請檢閱下列主題。

主題

- 限制用戶端與您的端點保持連線的時間
- 預先擴展您的資源容量並測試轉移流量
- 請注意資源類型和限制
- 指定練習執行的警示
- 評估練習執行的結果

限制用戶端保持連線至端點的時間

當 Amazon Application Recovery Controller (ARC) 將流量移離損害時，例如使用區域轉移或區域自動轉移，ARC 用來移動應用程式流量的機制是 DNS 更新。DNS 更新會導致所有新連線被導向至受損的位置。不過，具有預先存在開啟連線的用戶端可能會繼續對受損位置提出請求，直到用戶端重新連線為止。為了確保快速復原，建議您限制用戶端保持連線至端點的時間。

如果您使用 Application Load Balancer，您可以使用 `keepalive`選項來設定連線持續的時間。我們建議您降低`keepalive`值，使其與應用程式的復原時間目標保持一致，例如 300 秒。當您選擇`keepalive`時間時，請考慮此值是在更頻繁重新連線之間交換，這會影響延遲，並更快速地將所有用戶端移離受損的可用區域或區域。

如需設定 Application Load Balancer `keepalive`選項的詳細資訊，請參閱Application Load Balancer 使用者指南》中的 HTTP 用戶端持續作用持續時間。

預先擴展您的資源容量並測試轉移流量

當 AWS 將流量移離區域轉移或自動轉移的可用區域時，請務必讓剩餘的可用區域為您的資源提供更高的請求率。此模式稱為靜態穩定性。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，您應該跨三個可用區域佈建 15 個執行個體，總共 45 個執行個體。透過這樣做，當 使用自動轉移或在實務執行期間從一個可用區域 AWS 轉移流量時，仍然AWS 可以為應用程式的用戶端提供兩個可用區域剩餘的 30 個執行個體。

ARC 中的區域自動轉移功能可協助您在具有預先調整規模之資源的應用程式無法正常運作時，快速從可用區域中 AWS 的事件復原。為資源啟用區域自動轉移之前，請在 中所有設定的可用區域中擴展資源容量 AWS 區域。然後，開始資源的區域轉移，以測試您的應用程式在流量移離可用區域時是否仍然正常執行。

使用區域轉移進行測試後，請啟用區域自動轉移，並設定應用程式資源的實務執行。執行您自己的隨需實務執行，以協助確保正確擴展您的組態。使用區域自動轉移執行的定期實務可協助您持續確保容量仍能適當擴展。透過跨可用區域的足夠容量，您的應用程式可以在自動轉移期間繼續為用戶端提供服務，而不會中斷。

如需為資源啟動區域轉移的詳細資訊，請參閱 ARC 中的區域轉移。

請注意資源類型和限制

對於區域轉移支援的所有資源，區域自動轉移支援將流量移出可用區域。在少數特定資源案例中，區域自動轉移不會將流量從可用區域轉移。

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佳，則負載平衡器會處於故障開啟狀態。如果 在此情況下 AWS 啟動負載平衡器的自動轉移，則自動轉移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故障開啟狀態。這是預期的行為。 AWS 區域 如果所有可用區域都無法開啟 （運作狀態不佳），則 Autoshift 無法導致一個可用區域運作狀態不佳，也無法將流量轉移到 中的其他可用區域。

若要查看支援資源的詳細資訊，包括所有需要注意的要求和例外狀況，請參閱 支援的資源。

指定練習執行的警示

您必須為使用區域自動轉移的實務執行設定至少一種警示類型 （結果警示）。您也可以選擇性地設定第二類警示 （封鎖警示）。

當您考慮為資源練習執行的 CloudWatch 警示時，請記住下列事項：

- 您必須為實務執行組態設定至少一個結果警示。對於結果警示，我們建議您將 CloudWatch 警示設定為在資源或應用程式的指標指出從可用區域轉移流量對效能造成負面影響時進入 ALARM 狀態。例如，您可以判斷資源請求率的閾值，然後將警示設定為在超過閾值時進入 ALARM 狀態。您有責任設定適當的警示，以結束 AWS 實務執行並傳回FAILED結果。
- 我們建議您遵循 AWS Well Architected Framework，建議您實作關鍵效能指標 (KPIs做為 CloudWatch 警示。如果您這樣做，您可以使用這些警示來建立複合警示，以用作安全觸發，以防止實務執行在可能導致應用程式遺漏 KPI 時啟動。當警示不再處於 ALARM 狀態時，ARC 會在下次排程資源的練習執行時開始練習執行。
- 對於練習執行封鎖警示，如果您選擇設定一個 （或多個），您可以選擇追蹤用來指示您不希望 AWS 練習執行開始的特定指標，例如，當警示指出有持續的事件時。
- 對於練習執行警示，您可以為每個警示指定 Amazon Resource Name (ARN)，因此您必須先在 Amazon CloudWatch 中設定警示。您指定的 CloudWatch 警示可以是複合警示，可讓您包含應用程式和資源的數個指標和檢查，以觸發警示進入 ALARM 狀態。或者，您可以設定個別警示，然後為您的練習執行組態指定每種類型的多個警示。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 警示與您設定練習執行的資源位於相同的區域。

評估實務執行的結果

ARC 會報告每個實務執行的結果。練習執行後，評估結果，並判斷是否需要採取動作。例如，您可能需要擴展容量或調整警示的組態。

以下是可能的演練結果：

- SUCCEEDED：在練習執行期間，沒有結果警示進入 ALARM 狀態，且練習執行已完成完整的 30 分鐘測試期間。
- 失敗：至少一個結果警示在練習執行期間進入 ALARM 狀態。
- INTERRUPTED：由於不是結果警示進入 ALARM 狀態的原因，實務執行結束。實務執行可能會因為各種原因而中斷，包括下列項目：
  - 練習執行已結束，因為 在 中 AWS 啟動自動轉移， AWS 區域 或在 區域中有警示條件。
  - 練習執行已結束，因為已刪除資源的練習執行組態。
  - 練習執行已結束，因為在練習執行區域轉移正在轉移流量的可用區域中，資源已啟動客戶起始的區域轉移。
  - 練習執行已結束，因為無法再存取針對練習執行組態指定的 CloudWatch 警示。
  - 練習執行已結束，因為針對練習執行指定的封鎖警示進入 ALARM 狀態。

  - 練習執行因不明原因結束。
  - 練習執行已結束，因為已啟動優先順序為 的區域自動轉移。請參閱區域轉移的優先順序。
- CAPACITY_CHECK_FAILED：對負載平衡和 Auto Scaling 群組資源在可用區域之間平衡容量檢查失敗。
- PENDING：實務執行為作用中 （進行中）。尚無結果可傳回。

區域自動轉移 API 操作

下表列出您可以搭配區域自動轉移使用的 ARC API 操作。如需搭配 使用區域自動轉移 API 操作的範例 AWS CLI，請參閱 。

如需如何搭配 使用常用區域自動轉移 API 操作的範例 AWS Command Line Interface，請參閱 AWS CLI 搭配區域自動轉移使用 的範例。

Action	使用 ARC 主控台	使用 ARC API
建立練習執行組態	請參閱 啟用或停用區域自動轉移	請參閱 CreatePracticeRunConfiguration
刪除實務執行組態	請參閱 設定、編輯或刪除實務執行組態	請參閱 DeletePracticeRunConfiguration
列出自動轉移	請參閱 ARC 中的區域自動轉移	請參閱 ListAutoshifts
列出區域自動轉移的資源	請參閱 支援的資源	請參閱 ListManagedResources
取得區域自動轉移的資源	請參閱 支援的資源	請參閱 GetManagedResource
編輯實務執行組態	請參閱 設定、編輯或刪除實務執行組態	請參閱 UpdatePracticeRunConfiguration
啟用或停用區域自動轉移	請參閱 啟用或停用區域自動轉移	請參閱 UpdateZonalAutoshiftConfiguration
啟用或停用自動轉移觀察器通知	請參閱 啟用和使用區域自動轉移	請參閱 UpdateAutoshiftObserverNotificationStatus

Action	使用 ARC 主控台	使用 ARC API
開始練習執行	請參閱 啟動練習執行區域轉移	請參閱 StartPracticeRun
取消練習執行	請參閱 取消練習執行區域轉移	請參閱 CancelPracticeRun

AWS CLI 搭配區域自動轉移使用 的範例

本節將逐步介紹使用區域自動轉移的簡單應用程式範例，使用 AWS Command Line Interface 使用 API 操作在 Amazon Application Recovery Controller (ARC) 中使用區域自動轉移功能。這些範例旨在協助您了解如何使用 CLI 使用區域自動轉移。

區域自動轉移是 ARC 中的功能。使用區域自動轉移，您可以授權 AWS 在事件期間代表您從可用區域轉移支援的應用程式資源流量，以協助縮短復原時間。如需可與區域自動轉移搭配使用之資源的詳細資訊，請參閱 支援的資源。

區域自動轉移包括實務執行，也會將流量移離可用區域，以協助驗證自動轉移對您的應用程式是否安全。

如需區域自動轉移 API 動作的清單和詳細資訊的連結，請參閱 區域自動轉移 API 操作。如需使用 的詳細資訊 AWS CLI，請參閱 AWS CLI 命令參考。

目錄

- 建立練習執行組態
- 啟用或停用自動轉移
- 開始隨需練習執行
- 取消進行中的實務執行
- 取消進行中自動轉移
- 編輯實務執行組態
- 刪除實務執行組態

建立練習執行組態

在為資源啟用區域自動轉移之前，您必須為資源建立實務執行組態，以選擇所需實務執行的選項。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。

當您為資源建立練習執行組態時，請注意下列事項：

- 目前唯一支援的警示類型是 CLOUDWATCH。
- 您必須使用 AWS 區域 資源部署所在的相同 警示。
- 需要指定結果警示。指定封鎖警示是選用的。
- 指定封鎖或允許的日期或時段是選用的。

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

例如，若要為資源建立練習執行組態，請使用如下所示的命令：

```
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"
        ]
}
```

啟用或停用自動轉移

您可以使用 CLI 更新區域自動轉移狀態，以啟用或停用資源的自動轉移。若要變更區域自動轉移狀態，請使用 update-zonal-autoshift-configuration命令。

例如，若要啟用資源的自動轉移，請使用如下所示的命令：

```
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"
}
```

開始隨需練習執行

您可以使用 start-practice-run命令，透過 CLI 啟動隨需練習執行區域轉移。

例如，若要開始資源的練習執行，請使用如下所示的命令：

```
aws arc-zonal-shift start-practice-run
    --resource-
identifier="arn:aws:elasticloadbalancing:Region:111122223333:ExampleALB123456890" \
    "awayFrom": "usw2-az1",
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Practice run started. Shifting traffic away from Availability Zone
 usw2-az1.",
```

```
}
```

取消進行中的實務執行

您可以使用 cancel-practice-run命令，透過 CLI 取消進行中的做法執行。

例如，若要取消資源的練習執行，請使用如下所示的命令：

```
aws arc-zonal-shift cancel-practice-run \
   --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 canceled"
}
```

取消進行中自動轉移

您可以使用 CLI 取消進行中的自動轉移，方法是取消資源的區域自動轉移。若要取消區域自動轉移，請使用 cancel-zonal-shift command。

```
aws arc-zonal-shift cancel-zonal-shift --zonal-shift-id
 9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38
```

```
{
    "awayFrom": "usw2-az1",
    "comment": "Zonal autoshift started. Shifting traffic away from Availability Zone
 usw2-az1.",
    "expiryTime": "2024-12-17T22:29:38-08:00",
    "resourceIdentifier": "arn:aws:elasticloadbalancing:us-
east-1:111122223333:loadbalancer/app/Testing/5a19403ecd42dc05",
    "startTime": "2024-12-17T21:27:26-08:00",
    "status": "CANCELED",
    "zonalShiftId": "9ac9ec1e-1df1-0755-3dc5-8cf573cd9c38"
}
```

編輯實務執行組態

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，或更新 ARC 不會開始練習執行的封鎖日期或封鎖時段。若要編輯練習執行組態，請使用 update-practice-run-configuration命令。

當您編輯資源的練習執行組態時，請注意下列事項：

- 目前唯一支援的警示類型是 CLOUDWATCH。
- 您必須使用 AWS 區域 資源部署所在的相同 警示。
- 需要指定結果警示。指定封鎖警示是選用的。
- 指定封鎖日期或封鎖時段是選用的。
- 您指定的封鎖日期或封鎖時段會取代任何現有的值。

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"
        ]
}
```

刪除實務執行組態

您可以刪除資源的實務執行組態，但您必須先停用資源的區域自動轉移。需要資源才能讓實務執行組態啟用區域自動轉移。定期執行實務可協助您確保您的應用程式能夠在沒有一個可用區域的情況下正常執行。

若要使用 CLI 刪除實務執行組態，請先使用 `update-zonal-autoshift`命令視需要停用區域自動轉移。然後，若要刪除練習執行組態，請使用 `delete-practice-run-configuration`命令。

首先，使用如下所示的命令來停用資源的區域自動轉移：

```
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，使用如下所示的命令刪除練習執行組態：

```
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轉移

本節提供在 Amazon Application Recovery Controller (ARC) 中使用區域自動轉移的程序。啟用區域自動轉移後，您可以變更練習執行組態、啟動隨需練習執行、取消進行中輪班，包括練習執行，或啟用自動轉移觀察器通知。

啟用或停用區域自動轉移

此處的步驟說明如何在 Amazon Application Recovery Controller (ARC) 主控台上啟用或停用區域自動轉移。若要以程式設計方式使用區域自動轉移，請參閱區域轉移和區域自動轉移 API 參考指南。

啟用區域自動轉移時，您授權 AWS 代表您在事件期間從可用區域轉移應用程式資源流量，以協助縮短復原時間。

啟用或停用區域自動轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift。
2. 在資源區域自動轉移組態下，選擇資源。
3. 在動作功能表中，選擇啟用區域自動轉移，然後依照步驟完成更新。

如果資源沒有實務執行組態，則無法使用啟用區域自動轉移。若要設定練習執行組態並啟用區域自動轉移，請選擇設定區域自動轉移。

目錄

- 設定、編輯或刪除實務執行組態
- 取消區域自動轉移
- 啟動練習執行區域轉移
- 取消練習執行區域轉移
- 啟用或停用自動轉移觀察器通知

設定、編輯或刪除實務執行組態

本節中的步驟說明如何在 Amazon Application Recovery Controller (ARC) 主控台上編輯或刪除實務執行組態。若要以程式設計方式使用區域自動轉移，包括實務執行組態的變更，請參閱區域轉移和區域自動轉移 API 參考指南。

如果您在主控台中刪除練習執行組態，則區域自動轉移會停用。您必須先停用區域自動轉移，才能使用 API 操作刪除實務執行組態。您可以設定實務執行，而無需啟用區域自動轉移。不過，若要為資源啟用區域自動轉移，您必須為資源設定實務執行。

設定練習執行

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift。
2. 選擇設定區域自動轉移。
3. 選擇要設定區域自動轉移的資源。
4. 如果您不想 AWS 在發生 AWS 事件時啟動資源的自動轉移，請選擇停用區域自動轉移。您可以選擇繼續精靈來設定練習執行組態，而無需啟用自動轉移。
5. 選擇資源練習執行的選項。您可以針對警示執行下列操作：

   - （必要）指定至少一個結果警示來監控此資源的實務執行。
   - （選用）為此資源的實務執行指定一或多個封鎖警示。

   如需詳細資訊，請參閱 中您為練習執行指定的警示一節設定區域自動轉移時的最佳實務。
6. 或者，指定封鎖的時段或允許的時段，以封鎖 ARC 開始練習執行，或允許 ARC 開始此資源的練習執行。所有日期和時間均以 UTC 表示。
7. 選取核取方塊以確認您已閱讀確認備註。
8. 選擇建立。

編輯練習執行組態

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift。
2. 在資源區域自動轉移組態下，選擇資源。
3. 在動作功能表中，選擇編輯實務執行組態。
4. 變更實務執行組態，以執行下列一或多個動作：

   - 您可以針對警示執行下列操作：
     - 對於封鎖警示，您可以新增一或多個警示或刪除警示。
     - 對於結果警示，您可以新增一或多個警示或刪除警示。至少需要一個結果警示，因此您無法刪除組態中的所有結果警示。

- 對於封鎖的時段和允許的時段，您可以新增日期和時間，也可以移除或更新現有的日期和時間。所有日期和時間均以 UTC 表示。

5. 選擇儲存。

刪除實務執行組態

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/autoshift。
2. 在資源區域自動轉移組態下，選擇資源。
3. 在動作功能表中，選擇刪除實務執行組態。
4. 在確認模式對話方塊中，輸入 `Delete`，然後選擇刪除。

   請注意，在主控台中刪除練習執行組態也會停用資源的區域自動轉移。區域自動轉移需要為資源設定實務執行。

取消區域自動轉移

若要停止資源的進行中區域自動轉移，您必須取消區域自動轉移。

停止進行中的區域自動轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/。
2. 選取您要取消的區域自動轉移，然後選擇取消區域轉移。
3. 在確認模態對話方塊中，選擇確認。

啟動練習執行區域轉移

本節中的步驟說明如何在 ARC 主控台上啟動隨需練習執行區域轉移。若要以程式設計方式使用區域轉移和區域自動轉移，請參閱區域轉移和區域自動轉移 API 參考指南。

您可以在設定區域自動轉移並建立練習執行組態之後，啟動練習執行區域轉移。

啟動練習執行區域轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/。
2. 在區域自動轉移資源下，瀏覽至已設定區域自動轉移的個別資源。

3. 在資源概觀頁面上，選擇開始練習執行。
4. 選取可用區域，然後輸入練習執行的註解。實務執行會將流量從您選取的可用區域轉移。
5. 選擇 開始使用。

取消練習執行區域轉移

本節中的步驟說明如何在 ARC 主控台上取消區域轉移。若要以程式設計方式使用區域轉移和區域自動轉移，請參閱區域轉移和區域自動轉移 API 參考指南。

您可以取消自己啟動的區域輪班或練習執行。您也可以取消為區域自動轉移實務執行的資源 AWS 啟動的區域轉移。

若要取消練習執行區域轉移

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/。
2. 選取您要取消的練習執行區域轉移，然後選擇取消區域轉移或取消練習執行。
3. 在確認模態對話方塊中，選擇確認。

啟用或停用自動轉移觀察器通知

您可以將區域自動轉移設定為每當 AWS 開始自動轉移時，透過 Amazon EventBridge 通知您，以將流量移離可能受損的可用區域。您必須在 AWS 區域 要接收通知的每個 中設定此選項。您不需要使用區域自動轉移設定任何特定資源，即可啟用這些個別的通知。如需詳細資訊，請參閱搭配 Amazon EventBridge 使用區域自動轉移。

本節中的步驟說明如何使用 Amazon Application Recovery Controller (ARC) 主控台啟用自動轉移觀察器通知。若要以程式設計方式使用區域自動轉移，請參閱區域轉移和區域自動轉移 API 參考指南。

啟用或停用自動轉移觀察器通知

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/zonalshift/home#/。
2. 在入門下，選擇啟用自動轉移觀察器通知。
3. 在確認對話方塊中，選擇啟用觀察者通知。

使用 測試區域自動轉移 AWS FIS

您可以使用 AWS Fault Injection Service 來設定和執行實驗，以協助您模擬真實世界條件，例如可用區域可用性：電力中斷案例，示範在潛在廣泛的可用區域受損期間，在已啟用自動轉移的 資源上啟動區域自動轉移時 AWS 會發生什麼情況。

啟動`aws:arc:start-zonal-autoshift`復原動作可讓您示範 AWS 如何在啟用區域自動轉移的資源中自動轉移流量，使其遠離潛在受損的 AZ，並在執行 AZs 可用性案例 AWS 區域 期間，將它們重新路由至相同 中運作狀態良好的 AZ。

例如，您可以使用 AWS FIS 案例程式庫來模擬因電源中斷所造成的 AZ 受損。在此實驗中，AZ 電源中斷開始的五分鐘後，復原動作`aws:arc:start-zonal-autoshift`會自動將資源流量移離指定的 AZ。流量會在電力中斷的剩餘 25 分鐘內轉移，以示範當有潛在的廣泛 AZ 受損時，如何觸發自動轉移。當實驗完成時，流量轉移會結束，且流量會再次開始流向所有可用AZs。此程序示範從影響 AZ 的電源事件中完全復原。

實驗與區域自動轉移實務執行的差異

AWS FIS 實驗與區域自動轉移實務執行的不同之處在於，在實務執行期間，ARC 會將資源的流量從一個 AZ 轉移為正常程序的一部分，以確保您的應用程式可以容忍 AZ 的遺失。不過，在 AWS FIS 實驗期間， AWS FIS 會示範如何代表您觸發已啟用自動轉移之資源的 AZ 損害和自動轉移，然後在損害解決後取消自動轉移。

您無法在執行時更新 AWS FIS 起始的區域轉移。此外，如果您在 外部取消區域轉移 AWS FIS， AWS FIS 實驗會結束。

AWS FIS 過期型安全機制

AWS FIS 使用 StartZonalShift、UpdateZonalShift 和 CancelZonalShift API 操作來管理區域轉移，這些請求的 `expiresIn` 欄位設定為 1 分鐘做為安全機制。如果發生意外事件，例如網路中斷或系統問題，這 AWS FIS 可讓 快速復原區域轉移。在 ARC AWS FIS主控台中，過期時間欄位會顯示受管，而實際的預期過期取決於區域轉移動作中指定的持續時間。如需練習執行的詳細資訊，請參閱區域自動轉移和練習執行的運作方式

在特定時間不能有多個套用的區域轉移。也就是說，只有一個實務會執行資源的區域轉移、客戶起始的區域轉移、自動轉移或 AWS FIS 實驗。啟動第二個區域轉移時，ARC 會遵循優先順序來判斷資源的有效區域轉移類型。如需區域輪班優先順序的詳細資訊，請參閱 區域輪班的優先順序。

如需 AWS FIS 復原動作的詳細資訊，請參閱AWS Fault Injection Service 《 使用者指南》中的AWS FIS 復原動作。

在 Amazon Application Recovery Controller (ARC) 中記錄和監控區域自動轉移

您可以使用 AWS CloudTrail 和 Amazon EventBridge 在 Amazon Application Recovery Controller (ARC) 中監控區域自動轉移，以分析模式並協助疑難排解問題。

主題

- 使用 記錄區域自動轉移 API 呼叫 AWS CloudTrail
- 搭配 Amazon EventBridge 使用區域自動轉移

使用 記錄區域自動轉移 API 呼叫 AWS CloudTrail

ARC 的區域自動轉移已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 ARC 中 AWS 服務所採取動作的記錄。CloudTrail 會將區域轉移的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 ARC 主控台的呼叫，以及對區域轉移的 ARC API 操作的程式碼呼叫。

如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括區域轉移的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 所收集的資訊，判斷針對區域轉移向 ARC 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的區域自動轉移資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當區域自動轉移的 ARC 中發生活動時，該活動會記錄在 CloudTrail 事件中，以及事件歷史記錄中的其他 AWS 服務事件。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

若要持續記錄 中的事件 AWS 帳戶，包括 ARC 中區域自動轉移的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析 CloudTrail 日誌中收集的事件資料並對其採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合

- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 ARC 動作，並記錄在 Amazon Application Recovery Controller 的路由控制 API 參考指南中。例如，對 `StartZonalShift` 以及 `ListManagedResources` 動作發出的呼叫會在 CloudTrail 日誌檔案中產生項目。

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：

- 請求是使用根或 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 userIdentity 元素。

在事件歷史記錄中檢視 ARC 事件

CloudTrail 可讓您使用 Event history (事件歷史記錄) 檢視最近的事件。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。

了解區域自動轉移日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範區域自動轉移`ListManagedResources`的動作。

```
{
      "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": "2022-11-14T16:14:41Z",
      "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"
      }
    }
```


搭配 Amazon EventBridge 使用區域自動轉移

使用 Amazon EventBridge，您可以設定事件驅動規則來監控區域自動轉移資源，並啟動使用其他 AWS 服務的目標動作。例如，您可以在區域自動轉移實務執行開始時發出 Amazon SNS 主題訊號，以設定傳送電子郵件通知的規則。

您可以在 Amazon EventBridge 中建立規則，以對區域自動轉移採取行動。區域自動轉移的事件會指定實務執行或自動轉移的狀態資訊，例如，當實務執行開始時。您可以設定區域自動轉移，以針對您為服務啟用的資源通知您區域自動轉移事件。

除了或其他通知之外，您也可以選擇啟用自動轉移觀察器通知，這會在每當 AWS 啟動潛在受損可用區域的自動轉移時提供通知事件。當您已啟用區域自動轉移之資源的流量從可用區域轉移時，自動轉移觀

察器通知與您收到的通知不同。您不需要使用區域自動轉移設定任何資源，即可啟用自動轉移觀察器通知。如需詳細資訊，請參閱啟用和使用區域自動轉移。

若要擷取您感興趣的特定區域自動轉移事件，請定義 EventBridge 可用來偵測事件的事件特定模式。事件模式的結構與其相符的事件相同。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。在正常操作情況下，它們會以近乎即時的方式從 ARC 交付至 EventBridge。不過，可能會發生可能延遲或阻止交付事件的情況。

如需 EventBridge 規則如何使用事件模式的詳細資訊，請參閱 EventBridge 中的事件和事件模式。

使用 EventBridge 監控區域自動轉移資源

使用 EventBridge，您可以建立規則，定義 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，在區域自動轉移實務執行開始時傳送電子郵件訊息。

若要在 EventBridge 主控台中輸入或複製事件模式並貼上，請選取 選項以在主控台中使用輸入我自己的選項。為了協助您判斷可能對您有用的事件模式，本主題包含區域自動轉移事件比對模式和區域自動轉移事件的範例，供您使用。

建立資源事件的規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 選擇 AWS 區域 您要在其中建立規則的 ，這是您有興趣觀看事件的區域。
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，請保留預設值 。
6. 選擇下一步。
7. 對於建置事件模式步驟，對於事件來源，請保留預設值 AWS 事件。
8. 在範例事件下，選擇輸入我自己的事件。
9. 對於範例事件，輸入或複製並貼上事件模式。

區域自動轉移事件模式範例

事件模式的結構與其相符的事件相同。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

您可以將此區段的事件模式複製並貼到 EventBridge 中，以建立可用來監控區域自動轉移動作和資源的規則。

當您為區域自動轉移事件建立事件模式時，您可以為 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
- FIS Experiment Autoshift In Progress
- FIS Experiment Autoshift Completed
- FIS Experiment Autoshift Canceled
- Manual Shift Started
- Manual Shift Updated
- Manual Shift Canceled

當實務執行中斷時，如需造成中斷之原因的詳細資訊，請參閱 additionalFailureInfo 欄位。

您可以選擇啟用 AWS 自動轉移觀察器通知來監控所有自動轉移。啟用自動轉移觀察器通知後，若要接收通知，請選擇收到區域自動轉移詳細資訊類型的通知Autoshift In Progress。若要查看啟用自動轉移觀察器通知的步驟，請參閱 啟用和使用區域自動轉移。

如需範例，請參閱範例區域自動轉移事件一節。

- 從已啟動自動轉移的區域自動轉移中選取所有事件。

  注意下列事項：

  - 如果您已啟用自動轉移觀察器通知，ARC 會傳回所有自動轉移事件。
  - 如果您沒有啟用自動轉移觀察器通知，ARC 只會在您為區域自動轉移設定的資源包含在自動轉移中時傳回自動轉移事件。

```
{
    "source": [
        "aws.arc-zonal-shift"
    ],
    "detail-type": [
        "Autoshift In Progress"
```

```
    ]
}
```

- 從練習執行已開始的區域自動轉移中選取所有事件。

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

- 從練習執行失敗的區域自動轉移中選取所有事件。

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

區域自動轉移事件範例

本節包含區域自動轉移動作的範例事件。

以下是 Autoshift In Progress動作的範例事件，當 1) 啟用自動轉移觀察器通知，以及 2) 您尚未設定包含於自動轉移的區域自動轉移資源時：

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "source": "aws.arc-zonal-shift",
    "account": "111122223333",
    "time": "2023-11-16T23:38:14Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
```

```
        "version": "0.0.1",
        "data": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":"AWS has started an autoshift for an impaired Availability Zone.
 This notification
            is separate from autoshift notifications for resources, if any, that you
 have configured for
            zonal autoshift. For details, see the Developer Guide."
        }
    }
}
```

以下是 Autoshift In Progress動作的範例事件，當 1) 自動轉移觀察器通知已停用，且 2) 您已使用包含在自動轉移中的區域自動轉移設定資源時：

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

以下是 Practice Run Interrupted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"
        }
    }
}
```

以下是 FIS Experiment Autoshift In Progress動作的範例事件：

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "FIS Experiment Autoshift In Progress",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

以下是 Manual Shift Started動作的範例事件。在資源上呼叫 StartZonalShift API 時發出：

```
{
    "version": "0",
    "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4",
    "detail-type": "Manual Shift Started",
    "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": "",
        "metadata": {
            "awayFrom": "use1-az2",
            "notes":""
        }
    }
}
```

指定要用作目標的 CloudWatch 日誌群組

建立 EventBridge 規則時，您必須指定要傳送符合規則之事件的目標。如需 EventBridge 可用目標的清單，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 日誌群組新增為目標的需求，並提供在建立規則時新增日誌群組的程序。

若要將 CloudWatch 日誌群組新增為目標，您可以執行下列其中一項操作：

- 建立新的日誌群組
- 選擇現有的日誌群組

如果您在建立規則時使用主控台指定新的日誌群組，EventBridge 會自動為您建立日誌群組。請確定您用作 EventBridge 規則目標的日誌群組以 開頭/aws/events。如果您想要選擇現有的日誌群組，請注意，只有開頭為 的日誌群組才會在下拉式功能表中/aws/events顯示為選項。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的建立新的日誌群組。

如果您使用主控台外部的 CloudWatch 操作建立或使用 CloudWatch 日誌群組做為目標，請確定您正確設定許可。如果您使用主控台將日誌群組新增至 EventBridge 規則，則日誌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 開發套件來指定日誌群組，則必須更新日誌群組的資源型政策。下列範例政策說明您必須在日誌群組的資源型政策中定義的許可：

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

您無法使用 主控台為日誌群組設定資源型政策。若要將必要的許可新增至以資源為基礎的政策，請使用 CloudWatch PutResourcePolicy API 操作。然後，您可以使用 describe-resource-policies CLI 命令來檢查政策是否正確套用。

為資源事件建立規則並指定 CloudWatch 日誌群組目標

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 選擇您要 AWS 區域 在其中建立規則的 。
3. 選擇建立規則，然後輸入該規則的任何相關資訊，例如事件模式或排程詳細資訊。

   如需為 ARC 建立 EventBridge 規則的詳細資訊，請參閱本主題前面的章節。
4. 在選取目標頁面上，選擇 CloudWatch 做為您的目標。

5. 從下拉式選單中選擇 CloudWatch 日誌群組。

ARC 中區域自動轉移的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目錄

- ARC 中的區域自動轉移如何與 IAM 搭配使用
- ARC 中區域自動轉移的身分型政策範例
- 在 ARC 中使用服務連結角色進行區域自動轉移
- AWS ARC 中區域自動轉移的 受管政策

ARC 中的區域自動轉移如何與 IAM 搭配使用

在您使用 IAM 在 Amazon Application Recovery Controller (ARC) 中管理區域自動轉移的存取權之前，請先了解哪些 IAM 功能可與區域自動轉移搭配使用。

您可以在 ARC 中搭配區域自動轉移使用的 IAM 功能

IAM 功能	區域自動轉移支援
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

IAM 功能	區域自動轉移支援
主體許可	是
服務角色	否
服務連結角色	是

若要取得 AWS 服務如何與大多數 IAM 功能搭配使用的高階整體檢視，請參閱《IAM 使用者指南》中的與 IAM AWS 搭配使用的 服務。

ARC 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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 ARC 身分型政策的範例，請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例。

ARC 內的資源型政策

支援資源型政策：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。

ARC 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。政策會使用動作來授予執行相關聯動作的許可。

若要查看區域自動轉移的 ARC 動作清單，請參閱《服務授權參考》中的 Amazon Route 53 區域轉移定義的動作。

ARC 中的區域自動轉移政策動作在動作之前使用下列字首：

```
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，下列項目：

```
"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*"
```

若要檢視區域自動轉移的 ARC 身分型政策範例，請參閱 ARC 中區域自動轉移的身分型政策範例。

ARC 中區域自動轉移的政策資源

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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看資源類型及其 ARNs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 Route 53 定義的動作 - 區域轉移

若要查看可與條件索引鍵搭配使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon Route 53 - 區域轉移定義的條件索引鍵

若要檢視區域自動轉移的 ARC 身分型政策範例，請參閱 ARC 中區域自動轉移的身分型政策範例。

ARC 中區域自動轉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` 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看區域自動轉移的 ARC 條件索引鍵清單，請參閱服務授權參考中的下列主題：

- Amazon Route 53 區域轉移的條件索引鍵

若要查看可與條件金鑰搭配使用的動作和資源，請參閱服務授權參考中的下列主題：

- Amazon Route 53 區域轉移定義的動作

若要檢視區域自動轉移的 ARC 身分型政策範例，請參閱 ARC 中區域自動轉移的身分型政策範例。

ARC 中的存取控制清單 (ACLs)

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。

使用 ARC 的屬性型存取控制 (ABAC)

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，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

ARC 中的區域自動轉移包括下列對 ABAC 的部分支援：

- 區域自動轉移支援在 ARC 中為區域轉移註冊的受管資源 ABAC。如需有關 ABAC for Network Load Balancer 和 Application Load Balancer 受管資源的詳細資訊，請參閱Elastic Load Balancing 使用者指南》中的 ABAC with Elastic Load Balancing。

搭配 ARC 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

ARC 的跨服務主體許可

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，您會被視為委託人。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政策中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon Route 53 區域轉移

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

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 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 ARC 服務連結角色的詳細資訊，請參閱 在 ARC 中使用服務連結角色進行區域自動轉移。

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。在資料表中尋找服務，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。

ARC 中區域自動轉移的身分型政策範例

根據預設，使用者和角色沒有建立或修改 ARC 資源的許可。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。

如需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 (主控台)。

如需 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 ARNs 格式，請參閱《服務授權參考》中的 Amazon Application Recovery Controller (ARC) 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 範例：區域自動轉移主控台存取
- 範例：ARC API 動作

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義

特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。

- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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：區域自動轉移主控台存取

若要存取 Amazon Application Recovery Controller (ARC) 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 ARC 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。

若要執行某些任務，使用者必須具有在 ARC 中建立與區域自動轉移相關聯之服務連結角色的許可。如需詳細資訊，請參閱 在 ARC 中使用服務連結角色進行區域自動轉移。

若要授予使用者在 中使用區域自動轉移的完整存取權 AWS 管理主控台，請將如下所示的政策連接到使用者：

JSON

```
{
```

```
    "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：ARC API 動作

您可以使用政策來確保使用者可以使用區域自動轉移的 ARC API 動作來設定區域自動轉移，以便 代表您將應用程式資源流量從可用區域 AWS 轉移到 中運作狀態良好的AZs AWS 區域，以協助縮短事件期間的復原時間。若要提供這些許可，請連接對應至使用者需要使用的 API 操作的政策，如下所述。

若要執行某些任務，使用者必須具有與 ARC 相關聯的服務連結角色的許可。建立服務連結角色所需的許可包含在下列範例政策中。如需詳細資訊，請參閱 在 ARC 中使用服務連結角色進行區域自動轉移。

若要使用區域自動轉移的 API 操作，請將下列政策連接至使用者：

JSON

```
{
    "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 ARC 中使用服務連結角色進行區域自動轉移

Amazon Application Recovery Controller 中的區域自動轉移使用 a 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，在此情況下為 ARC。服務連結角色是由 ARC 預先定義，並包含服務為了特定目的代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 ARC，因為您不必手動新增必要的許可。ARC 定義服務連結角色的許可，除非另有定義，否則只有 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。這可保護您的 ARC 區域自動轉移資源，因為您不會不小心移除存取資源的許可。

如需其他支援服務連結角色的相關資訊，請參閱服務連結角色欄中與 AWS IAM 搭配使用的服務，並尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

AWSServiceRoleForZonalAutoshiftPracticeRun 的服務連結角色許可

ARC 使用名為 AWSServiceRoleForZonalAutoshiftPracticeRun 的服務連結角色來執行下列動作：

- 監控客戶提供的 Amazon CloudWatch 警示和客戶 Health 儀板表 事件，以進行實務執行
- 管理實務執行 （實務區域轉移）

本節說明服務連結角色的許可，以及建立、編輯和刪除角色的相關資訊。

AWSServiceRoleForZonalAutoshiftPracticeRun 的服務連結角色許可

此服務連結角色使用 受管政策 `AWSZonalAutoshiftPracticeRunSLRPolicy`。

AWSServiceRoleForZonalAutoshiftPracticeRun 服務連結角色信任下列服務擔任該角色：

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

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AWSZonalAutoshiftPracticeRunSLRPolicy。

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 ARC 建立 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 管理主控台 AWS CLI、 或 AWS SDK 中建立第一個練習執行組態時，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，ARC 會再次為您建立服務連結角色。

編輯 ARC 的 AWSServiceRoleForZonalAutoshiftPracticeRun 服務連結角色

ARC 不允許您編輯 AWSServiceRoleForZonalAutoshiftPracticeRun 服務連結角色。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考該角色。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」的編輯服務連結角色。

刪除 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，才能手動將其刪除。

停用自動轉移後，您可以刪除 AWSServiceRoleForZonalAutoshiftPracticeRun 服務連結角色。如需自動轉移功能的詳細資訊，請參閱 ARC 中的區域轉移。

> **Note**
>
> 如果 ARC 服務在您嘗試刪除資源時使用角色，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 AWS CLI、 或 AWS API 來刪除 AWSServiceRoleForZonalAutoshiftPracticeRun 服務連結角色。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。

區域自動轉移的 ARC 服務連結角色更新

如需 ARC 服務連結角色的 AWS 受管政策更新，請參閱 ARC 的AWS 受管政策更新資料表。您也可以在 ARC 文件歷史記錄頁面上訂閱自動 RSS 提醒。

AWS ARC 中區域自動轉移的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：AWSZonalAutoshiftPracticeRunSLRPolicy

您不得將 AWSZonalAutoshiftPracticeRunSLRPolicy 連接到 IAM 實體。此政策會連接到服務連結角色，允許 Amazon Application Recovery Controller (ARC) 對區域自動轉移執行下列動作：

- 監控客戶提供的 Amazon CloudWatch 警示和客戶 Health 儀板表 事件，以進行實務執行
- 管理實務執行（實務區域轉移）
- 管理練習執行和自動轉移的平衡容量檢查

如需詳細資訊，請參閱在 ARC 中使用服務連結角色進行區域自動轉移。

區域自動轉移的 AWS 受管政策更新

如需自此服務開始追蹤 ARC 中區域自動轉移的 AWS 受管政策更新詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 的 AWS 受管政策更新。如需此頁面變更的自動提醒，請訂閱 ARC 文件歷史記錄頁面上的 RSS 摘要。

區域自動轉移的配額

Amazon Application Recovery Controller (ARC) 中的區域自動轉移受下列配額約束。

實體	配額
每個實務執行組態的結果警示數量	10 您可以請求提高配額。
每個實務執行組態的封鎖警示數量	10 您可以請求提高配額。

使用路由控制來復原 ARC 中的多區域應用程式

本節說明如何使用 Amazon Application Recovery Controller (ARC) 中的路由控制功能，將中斷降至最低，並在您將 AWS 應用程式部署到多個應用程式時，協助為使用者提供持續性 AWS 區域。

您也可以了解準備度檢查，這是 ARC 中的一項功能，可用來深入了解您的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檢查功能、設定方式，以及使用方式。

主題

- ARC 中的路由控制
- ARC 中的準備度檢查
- ARC 中的區域切換

ARC 中的路由控制

若要容錯移轉多個應用程式複本的流量 AWS 區域，您可以使用 Amazon Application Recovery Controller (ARC) 中的路由控制，這些控制與 Amazon Route 53 中的特定運作狀態檢查類型整合。路由控制是簡單的開關，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，與每個區域中應用程式複本前面的網域名稱相關聯的 DNS 容錯移轉記錄。

本節說明路由控制的運作方式、如何設定路由控制元件，以及如何使用這些元件來重新路由流量以進行容錯移轉。

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運作狀態檢查。所有路由控制都會在控制面板上分組。您可以在 ARC 為叢集建立的預設控制面板上將其分組，或建立您自己的自訂控制面板。您必須先建立叢集，才能建立控制面板或路由控制。ARC 中的每個叢集都是五個端點的資料平面 AWS 區域。

建立路由控制和路由控制運作狀態檢查之後，您可以建立路由控制的安全規則，以協助防止意外的復原自動化副作用。您可以使用 或 AWS CLI API 動作 （建議），或使用 來更新路由控制狀態，以個別或批次重新路由流量 AWS 管理主控台。

本節說明路由控制的運作方式，以及如何建立和使用它們來為您的應用程式重新路由流量。

> **Important**
>
> 若要了解如何在災難案例中準備使用 ARC 來重新路由流量，做為應用程式容錯移轉計劃的一部分，請參閱 ARC 中路由控制的最佳實務。

關於路由控制

路由控制會使用 Amazon Route 53 中的運作狀態檢查來重新導向流量，這些運作狀態檢查是以與復原群組中儲存格的最上層資源相關聯的 DNS 記錄所設定，例如 Elastic Load Balancing 負載平衡器。您可以將流量從一個儲存格重新導向到另一個儲存格，例如，將路由控制狀態更新為 `Off`（停止流量流到一個儲存格），並將另一個路由控制狀態更新為 On（啟動流量流到另一個）。變更流量流程的程序是與路由控制相關聯的 Route 53 運作狀態檢查，在 ARC 更新之後，根據對應的路由控制狀態將其設定為運作狀態或運作狀態不佳。

路由控制支援容錯移轉具有 DNS 端點的任何 AWS 服務。您可以更新路由控制狀態，以容錯移轉流量進行災難復原，或偵測應用程式的延遲下降或其他問題。

您也可以設定路由控制的安全規則，以確保使用路由控制重新路由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，路由控制本身並非監控端點基礎運作狀態的運作狀態檢查。例如，與 Route 53 運作狀態檢查不同，路由控制不會監控回應時間或 TCP 連線時間。路由控制是一種簡單的開關，可控制運作狀態檢查。一般而言，您會變更狀態以重新導向流量，而該狀態變更會將流量移至整個應用程式堆疊的特定端點，或防止路由至整個應用程式堆疊。例如，在簡單案例中，當您將路由控制狀態從 變更為 On 時`Off`，它會更新與 DNS 容錯移轉記錄相關聯的 Route 53 運作狀態檢查，以將流量從端點移出。

如何使用路由控制

若要更新路由控制狀態，以便重新路由流量，您必須連線到 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。您應該準備好變更路由控制狀態的程序，以輪換方式嘗試每個端點，因為叢集端點會循環顯示可用和無法使用的狀態，以進行定期維護和更新。

當您建立路由控制時，您可以設定 DNS 記錄，將路由控制運作狀態檢查與每個應用程式複本前面的 Route 53 DNS 名稱建立關聯。例如，若要控制兩個負載平衡器之間的流量容錯移轉，請在兩個區域中各建立一個路由控制運作狀態檢查，並將其與兩個 DNS 記錄建立關聯，例如具有容錯移轉路由政策的別名記錄，以及個別負載平衡器的網域名稱。

您也可以使用 ARC 路由控制搭配 Route 53 運作狀態檢查和 DNS 記錄集，並使用具有加權路由政策的 DNS 記錄，來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 AWS 部落格文章中

有關容錯移轉使用者流量的章節：使用 Amazon Application Recovery Controller (ARC) 建置高彈性的應用程式，第 2 部分：多區域堆疊

當您 AWS 區域 使用路由控制啟動 的容錯移轉時，由於流量流程涉及的步驟，您可能不會立即看到流量移出 區域。視用戶端行為和連線重複使用而定，區域中現有的進行中連線也可能需要一小段時間才能完成。根據您的 DNS 設定和其他因素，現有的連線可能會在幾分鐘內完成，或者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。

路由控制的優點

相較於使用傳統運作狀態檢查重新路由流量，ARC 中的路由控制有一些好處。例如：

- 路由控制可讓您容錯移轉整個應用程式堆疊。這與 Amazon EC2 執行個體根據資源層級運作狀態檢查而容錯移轉堆疊的個別元件相反。
- 路由控制為您提供安全、簡單的手動覆寫，您可以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，以防止全自動化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設施。

以下是將路由控制整合到您的容錯移轉策略中的範例，以改善應用程式的彈性和可用性 AWS。

您可以透過跨區域執行多個（通常是三個）備援複本 AWS ，在 上支援高可用性 AWS 的應用程式。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，並為應用程式流量提供服務，而另一個則是待命複本。當您的作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。您應該根據監控和運作狀態檢查系統的資訊，決定要從複本失敗還是失敗。

如果您想要啟用更快的復原，您可以為架構選擇的另一個選項是主動-主動實作。使用此方法時，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到另一個作用中複本，即可將使用者移離受損的應用程式複本，從失敗中復原。

AWS 路由控制的區域可用性

如需 Amazon Application Recovery Controller (ARC) 的區域支援和服務端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Application Recovery Controller (ARC) 端點和配額。

> **Note**
>
> Amazon Application Recovery Controller (ARC) 中的路由控制是一項全域功能。不過，您必須在區域 ARC AWS CLI 命令中指定美國西部（奧勒岡）區域（指定 參數 `--region us-west-2`)。也就是說，當您建立叢集、控制面板或路由控制等資源時。

ARC 路由控制是一種開/關開關，可變更 ARC 運作狀態檢查的狀態，然後可以與將流量重新導向的 DNS 記錄建立關聯，例如，從主要部署複本重新導向至待命部署複本。

如果發生應用程式故障或延遲問題，您可以更新路由控制狀態，將流量從主要複本轉移到待命複本。透過使用高度可靠的 ARC 資料平面 API 操作進行路由控制查詢和路由控制狀態更新，您可以在災難復原案例期間依賴 ARC 進行容錯移轉。如需詳細資訊，請參閱使用 ARC API 取得和更新路由控制狀態（建議）。

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。ARC 會將路由控制狀態變更傳播到位於 Amazon EC2 機群的叢集，以取得五個 AWS 區域的仲裁。傳播之後，當您使用 API 和高度可靠的資料平面來查詢路由控制狀態的 ARC 時，它會傳回共識檢視。

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

所有五個叢集端點的資料一致性平均在 5 秒內達到，最多不超過 15 秒。

ARC 提供極高的可靠性及其資料平面，可讓您手動容錯移轉跨儲存格的應用程式。ARC 可確保您永遠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 ARC 叢集都是單一租用戶，以確保您不會受到可能減慢存取模式的「雜訊鄰近」影響。

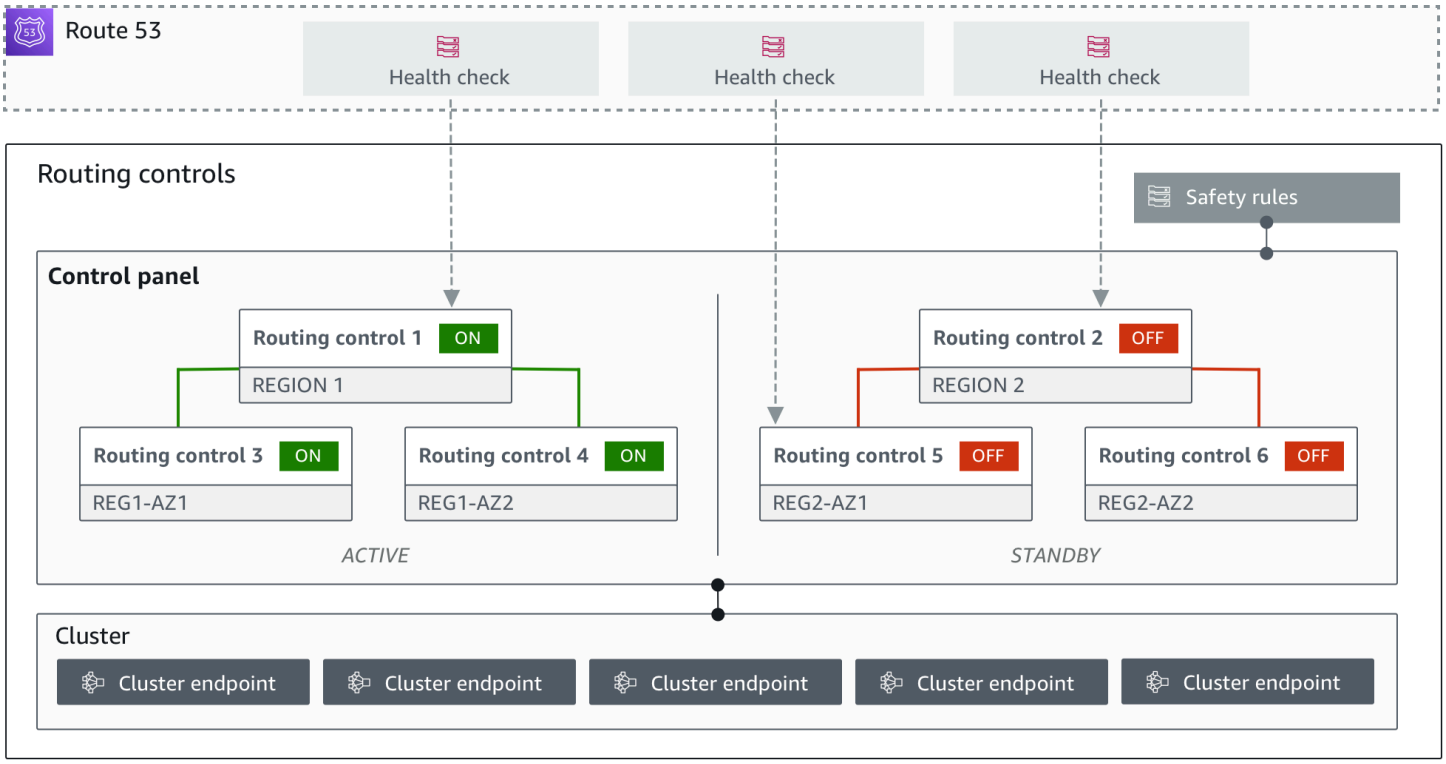
當您變更路由控制狀態時，您會依賴下列三個條件，這些條件極不可能失敗：

- 您五個端點中至少有三個可用並參與規定人數。
- 您有運作中的 IAM 登入資料，可以對運作中的區域叢集端點進行身分驗證。
- Route 53 資料平面運作狀態良好（此資料平面的設計符合 100% 的可用性 SLA)。

路由控制元件

下圖說明支援 ARC 中路由控制功能的元件範例。此處顯示的路由控制（分組為一個控制面板）可讓您管理兩個區域中兩個可用區域的流量。當您更新路由控制狀態時，ARC 會變更 Amazon Route 53 中

的運作狀態檢查，將 DNS 流量重新導向至不同的儲存格。您為路由控制設定的安全規則有助於避免故障開啟案例和其他意外後果。



以下是 ARC 中路由控制功能的元件。

叢集

叢集是一組五個備援的區域端點，您可以對其啟動 API 呼叫以更新或取得路由控制狀態。叢集包含預設控制面板，您可以在一個叢集上託管多個控制面板和路由控制。

路由控制

路由控制是一種簡單的開/關開關，託管在叢集上，用於控制傳入和傳出儲存格的用戶端流量路由。當您建立路由控制時，您可以在 Route 53 中新增 ARC 運作狀態檢查。這可讓您在 ARC 中更新路由控制狀態時，重新路由流量（使用運作狀態檢查，以應用程式的 DNS 記錄設定）。

路由控制運作狀態檢查

路由控制與 Route 53 中的運作狀態檢查整合。運作狀態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，ARC 會更新對應的運作狀態檢查，將流量重新導向，例如容錯移轉至待命複本。

控制面板

控制面板會將一組相關的路由控制分組在一起。您可以將多個路由控制與一個控制面板建立關聯，然後為控制面板建立安全規則，以確保您所做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，然後將它們分組在相同的控制面板中。然後，您可以新增安全規則 (「聲明規則」)，確保至少有一個區域 （由路由控制表示） 隨時處於作用中狀態，以避免意外的「故障開啟」案例。

預設控制面板

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

安全規則

安全規則是您新增至路由控制的規則，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，做為整體的「開啟/關閉」切換，以便啟用或停用一組其他路由控制。

端點 （叢集端點）

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該假設 ARC 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，直到您連線到端點為止。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依賴的機制具有高度可用性，以便在災難情況下需要它們時使用。一般而言，您應該盡可能將資料平面函數用於您的機制，以獲得最大的可靠性和容錯能力。考慮到這一點，了解服務的功能如何在控制平面和資料平面之間分割，以及何時可以使用服務的資料平面依賴極端可靠性。

與大多數 AWS 服務一樣，控制平面和資料平面支援路由控制功能的功能。雖然這兩者都建置為可靠，但控制平面會針對資料一致性進行最佳化，而資料平面則會針對可用性進行最佳化。資料平面專為彈性而設計，因此即使在破壞性事件期間，當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，我們建議您在可用性很重要時使用資料平面操作，例如，當您需要在中斷期間將流量重新路由到待命複本時。

對於路由控制，控制平面和資料平面的分割方式如下：

- 用於路由控制的控制平面 API 是美國西部（奧勒岡）區域 (us-west-2) 支援的復原控制組態 API。您可以使用這些 API 操作或 AWS 管理主控台 來建立或刪除叢集、控制面板和路由控制，以便在您可能需要為應用程式重新路由流量時，協助準備災難復原事件。路由控制組態控制平面不是高度可用的。
- 路由控制資料平面是橫跨五個地理隔離 AWS 區域的專用叢集。每個客戶都會使用路由控制控制平面建立一或多個叢集。叢集託管控制面板和路由控制。然後，當您想要為應用程式重新路由流量時，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。路由控制資料平面為高可用性。

由於路由控制資料平面高度可用，因此建議您計劃在想要容錯移轉以從事件復原時 AWS Command Line Interface ，使用 進行 API 呼叫來使用路由控制狀態。如需有關使用路由控制準備和完成復原操作時的關鍵考量的詳細資訊，請參閱 ARC 中路由控制的最佳實務。

如需資料平面、控制平面以及 如何 AWS 建置服務以滿足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白皮書。

在 Amazon Application Recovery Controller (ARC) 中標記路由控制

標籤是您用來識別和組織 AWS 資源的單字或片語（中繼資料）。您可以為每個資源新增多個標籤，每個標籤都包含您定義的索引鍵和值。例如，金鑰可能是環境，而值可能是生產。您可以根據新增的標籤來搜尋和篩選資源。

您可以在 ARC 中的路由控制中標記下列資源：

- 叢集
- 控制面板
- 安全規則

ARC 中的標記只能透過 API 使用，例如使用 AWS CLI。

以下是使用 在路由控制中標記的範例 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 Application Recovery Controller (ARC) 的復原控制組態 API 參考指南》中的 TagResource。

ARC 中路由控制的定價

對於 ARC 中的路由控制，您需要為建立的每個叢集支付每小時成本。每個叢集都可以託管多個路由控制，您可用來觸發應用程式容錯移轉。

為了協助管理成本和提高效率，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，請參閱支援 ARC 中叢集的跨帳戶。

如需 ARC 和定價範例的詳細定價資訊，請參閱 ARC 定價。

Amazon Application Recovery Controller (ARC) 中的多區域復原入門

若要在 Amazon Application Recovery Controller (ARC) 中使用路由控制來容錯移轉應用程式，您必須有多個 AWS 應用程式 AWS 區域。若要開始使用，請先確定您的應用程式已在每個區域中的孤立複本中設定，以便在事件期間從一個 容錯移轉到另一個 。然後，您可以建立路由控制，將應用程式流量從主要應用程式重新路由到次要應用程式，以維持使用者的連續性。

> **Note**
>
> 如果您有由可用區域隔離的應用程式，請考慮使用區域轉移或區域自動轉移進行容錯移轉復原。不需要設定即可使用區域轉移或區域自動轉移，以可靠地從可用區域受損復原應用程式。如需詳細資訊，請參閱使用區域轉移和區域自動轉移來復原 ARC 中的應用程式。

為了讓您在事件期間使用 ARC 路由控制來復原應用程式，我們建議您至少設定兩個應用程式，這些應用程式是彼此的複本。每個複本或儲存格都代表 AWS 區域。設定應用程式資源以符合區域後，請執行下列步驟，確保您的應用程式設定成功復原。

秘訣：為了協助簡化設定，我們提供 CloudFormation 和 HashiCorp Terraform 範本，以建立具有獨立於彼此失敗之備援複本的應用程式。若要進一步了解並下載範本，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，確保您的應用程式已設定為具有彈性：

1. 建立應用程式堆疊（網路和運算層）的獨立複本，這些複本是每個區域中彼此的複本，以便在發生事件時，您可以將流量從一個區域容錯移轉到另一個區域。請確定您的應用程式程式碼中沒有任何

會導致一個複本故障影響另一個複本的跨區域相依性。若要成功容錯移轉 AWS 區域，您的堆疊邊界應該位於 區域內。

2. 跨複本複製應用程式的所有必要狀態資料。您可以使用 AWS 資料庫服務來協助複寫資料。

流量容錯移轉的路由控制入門

Amazon Application Recovery Controller (ARC) 中的路由控制可讓您觸發容錯移轉，讓流量在單獨執行的備援應用程式複本或複本之間容錯移轉 AWS 區域。容錯移轉是使用 Amazon Route 53 資料平面搭配 DNS 執行。

在每個區域中設定複本後，如下一節所述，您可以將每個複本與路由控制建立關聯。首先，您將路由控制與每個區域中複本的最上層網域名稱建立關聯。然後，您將路由控制運作狀態檢查新增至路由控制，使其可以開啟和關閉流量。這可讓您控制應用程式複本之間的流量路由。

您可以在 中更新路由控制狀態 AWS 管理主控台 以容錯移轉流量，但我們建議您改用 ARC 動作、使用 API AWS CLI或 來變更它們。API 動作不依賴主控台，因此更具彈性。

例如，若要在區域之間容錯移轉，從 us-west-1 到 us-east-1，您可以使用 `update-routing-control-state` API 動作將 的狀態設定為 `us-west-1Off`，並將 `us-east-1`設定為 `On`。

在您建立路由控制元件來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成區域複本，以便您可以從一個複本容錯移轉到另一個複本。若要進一步了解並開始孤立新的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

為了協助您了解路由控制的運作方式，我們提供名為 的範例應用程式`TicTacToe`。此範例使用 CloudFormation 範本來簡化程序，以及可下載的 CloudFormation 範本，讓您可以快速探索自行設定和使用 ARC。

部署範例應用程式後，您可以使用範本建立 ARC 元件，然後使用路由控制來管理通往應用程式的流量流程。您可以針對自己的案例和應用程式調整範本和程序。

若要開始使用範例應用程式和 CloudFormation 範本，請參閱 ARC GitHub 儲存庫中的 README 說明。您可以閱讀 AWS CloudFormation 《 使用者指南》中的CloudFormation 概念，進一步了解如何使用 CloudFormation 範本。

ARC 中路由控制的最佳實務

對於 ARC 中的路由控制，我們建議採用下列復原和容錯移轉準備的最佳實務。

主題

- 確保專用、長期的 AWS 登入資料安全且隨時可存取
- 為涉及容錯移轉的 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 ARNs 加入書籤或硬式程式碼
- 隨機選擇其中一個端點以更新您的路由控制狀態
- 使用非常可靠的資料平面 API 來列出和更新路由控制狀態，而不是主控台

確保專用、長期的 AWS 登入資料安全且隨時可存取

在災難復原 (DR) 案例中，使用存取 AWS 和執行復原任務的簡單方法，將系統相依性降至最低。建立專門針對 DR 任務的 IAM 長期憑證，並將憑證安全地保存在內部部署實體安全或虛擬保存庫中，以便在需要時存取。透過 IAM，您可以集中管理安全登入資料，例如存取金鑰，以及存取 AWS 資源的許可。對於非 DR 任務，我們建議您繼續使用聯合存取，並使用 AWS AWS 單一登入等服務。

若要使用復原叢集資料平面 API 在 ARC 中執行容錯移轉任務，您可以將 ARC IAM 政策連接至使用者。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例。

為涉及容錯移轉的 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，尤其是使用較低的 TTL 值檢查運作狀態的記錄是適當的。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）設定會告知 DNS 解析程式在請求新的記錄之前快取記錄的時間。當您選擇 TTL 時，您可以權衡延遲和可靠性，以及對變更的回應能力。當記錄的 TTL 較短時，DNS 解析程式會更快地通知記錄更新，因為 TTL 指定他們必須更頻繁地查詢。

如需詳細資訊，請參閱 Amazon Route 53 DNS 最佳實務中的選擇 DNS 記錄的 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路由到 AWS 區域 另一個路由時，Amazon Application Recovery Controller (ARC) 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連線被導向至受損的位置。

不過，具有預先存在開放連線的用戶端可能會繼續對受損位置提出請求，直到用戶端重新連線為止。為了確保快速復原，建議您限制用戶端保持連線至端點的時間。

如果您使用 Application Load Balancer，您可以使用 `keepalive`選項來設定連線持續的時間。如需詳細資訊，請參閱《Application Load Balancer 使用者指南》中的 HTTP 用戶端保持連線持續時間。

根據預設，Application Load Balancer 會將 HTTP 用戶端持續作用持續時間值設定為 3600 秒或 1 小時。我們建議您降低值，使其與應用程式的復原時間目標保持一致，例如 300 秒。當您選擇 HTTP 用戶端保持連線持續時間時，請考慮此值是在一般更頻繁重新連線、可能影響延遲，以及更快速地將所有用戶端移離受損的可用區域或區域之間交換。

將五個區域叢集端點和路由控制 ARNs 加入書籤或硬式程式碼

我們建議您將 ARC 區域叢集端點的本機副本保留在書籤中，或儲存在用來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 操作，包括未託管在極可靠資料平面叢集上的 ARC API 操作。您可以使用 DescribeCluster API 操作列出 ARC 叢集的端點。

隨機選擇其中一個端點以更新您的路由控制狀態

路由控制提供五個區域端點，以確保高可用性，即使在處理故障時也是如此。為了實現完整的彈性，請務必具有可視需要使用所有五個端點的重試邏輯。如需搭配 AWS SDK 使用程式碼範例的資訊，包括嘗試叢集端點的範例，請參閱 使用 AWS SDKs的應用程式復原控制器程式碼範例。

使用非常可靠的資料平面 API 來列出和更新路由控制狀態，而不是主控台

使用 ARC 資料平面 API，透過 ListRoutingControls 操作檢視您的路由控制和狀態，並使用 UpdateRoutingControlState 操作更新路由控制狀態以重新導向容錯移轉的流量。您可以使用 AWS CLI（如這些範例所示）或使用其中一個 AWS SDKs 撰寫的程式碼。ARC 透過資料平面中的 API 提供極高的可靠性，以容錯移轉流量。建議您使用 API，而不是變更 中的路由控制狀態 AWS 管理主控台。

連線至其中一個區域叢集端點，讓 ARC 使用資料平面 API。如果端點無法使用，請嘗試連線至另一個叢集端點。

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並容錯移轉流量。如需詳細資訊，請參閱覆寫安全規則以重新路由流量。

使用 ARC 測試容錯移轉

使用 ARC 路由控制定期測試容錯移轉，從主要應用程式堆疊容錯移轉至次要應用程式堆疊。請務必確保您新增的 ARC 結構與堆疊中的正確資源一致，而且一切都如您預期般運作。您應該在為您的環境設定 ARC 之後進行測試，並繼續定期測試，以便在遇到需要次要系統快速啟動和執行以避免使用者停機的故障情況之前，準備好您的容錯移轉環境。

路由控制 API 操作

本節包含具有列出 API 操作的資料表，可用於在 Amazon Application Recovery Controller (ARC) 中設定和使用路由控制，以及相關文件的連結。

如需如何搭配 使用常見路由控制組態 API 操作的範例 AWS Command Line Interface，請參閱 搭配 使用 ARC 路由控制 API 操作的範例 AWS CLI。

下表列出可用於路由控制組態的 ARC API 操作，以及相關文件的連結。

Action	使用 ARC 主控台	使用 ARC API
建立 叢集	請參閱 在 ARC 中建立路由控制元件	請參閱 CreateCluster
描述叢集	請參閱 在 ARC 中建立路由控制元件	請參閱 DescribeCluster
刪除叢集	請參閱 在 ARC 中建立路由控制元件	請參閱 DeleteCluster
列出 帳戶的叢集	請參閱 在 ARC 中建立路由控制元件	請參閱 ListClusters
建立路由控制	請參閱 在 ARC 中建立路由控制元件	請參閱 CreateRoutingControl
描述路由控制	請參閱 在 ARC 中建立路由控制元件	請參閱 DescribeRoutingControl
更新路由控制	請參閱 在 ARC 中建立路由控制元件	請參閱 UpdateRoutingControl
刪除路由控制	請參閱 在 ARC 中建立路由控制元件	請參閱 DeleteRoutingControl
列出路由控制	請參閱 在 ARC 中建立路由控制元件	請參閱 ListRoutingControls

Action	使用 ARC 主控台	使用 ARC API
建立控制面板	請參閱 在 ARC 中建立路由控制元件	請參閱 CreateControlPanel
描述控制面板	請參閱 在 ARC 中建立路由控制元件	請參閱 DescribeControlPanel
更新控制面板	請參閱 在 ARC 中建立路由控制元件	請參閱 UpdateControlPanel
刪除控制面板	請參閱 在 ARC 中建立路由控制元件	請參閱 DeleteControlPanel
列出控制面板	請參閱 在 ARC 中建立路由控制元件	請參閱 ListControlPanels
建立安全規則	請參閱 建立路由控制的安全規則	請參閱 CreateSafetyRule
描述安全規則	請參閱 建立路由控制的安全規則	請參閱 DescribeSafetyRule
更新安全規則	請參閱 建立路由控制的安全規則	請參閱 UpdateSafetyRule
刪除安全規則	請參閱 建立路由控制的安全規則	請參閱 DeleteSafetyRule
列出安全規則	請參閱 建立路由控制的安全規則	請參閱 ListSafetyRules
列出相關聯的 Route 53 運作狀態檢查	請參閱 在 ARC 中建立路由控制運作狀態檢查	請參閱 ListAssociatedRoute53HealthChecks
列出叢集共用 AWS RAM 的資源政策	請參閱 支援 ARC 中叢集的跨帳戶	請參閱 GetResourcePolicy

下表列出常見的 ARC API 操作，您可以使用路由控制資料平面來管理流量容錯移轉，以及相關文件的連結。

Action	使用 ARC 主控台	使用 ARC API
取得路由控制狀態	請參閱 在 中取得和更新路由控制狀態 AWS 管理主控台	請參閱 GetRoutingControlState
列出路由控制	N/A	請參閱 ListRoutingControls
更新路由控制狀態	請參閱 在 中取得和更新路由控制狀態 AWS 管理主控台	請參閱 UpdateRoutingControlState
更新多個路由控制狀態	請參閱 在 中取得和更新路由控制狀態 AWS 管理主控台	請參閱 UpdateRoutingControlStates

將此服務與 AWS SDK 搭配使用

AWS 軟體開發套件 (SDKs) 適用於許多熱門的程式設計語言。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
適用於 C++ 的 AWS SDK	適用於 C++ 的 AWS SDK 程式碼範例
AWS CLI	AWS CLI 程式碼範例
適用於 Go 的 AWS SDK	適用於 Go 的 AWS SDK 程式碼範例
適用於 Java 的 AWS SDK	適用於 Java 的 AWS SDK 程式碼範例
適用於 JavaScript 的 AWS SDK	適用於 JavaScript 的 AWS SDK 程式碼範例
適用於 Kotlin 的 AWS SDK	適用於 Kotlin 的 AWS SDK 程式碼範例
適用於 .NET 的 AWS SDK	適用於 .NET 的 AWS SDK 程式碼範例
適用於 PHP 的 AWS SDK	適用於 PHP 的 AWS SDK 程式碼範例

SDK 文件	代碼範例
AWS Tools for PowerShell	AWS Tools for PowerShell 程式碼範例
適用於 Python (Boto3) 的 AWS SDK	適用於 Python (Boto3) 的 AWS SDK 程式碼範例
適用於 Ruby 的 AWS SDK	適用於 Ruby 的 AWS SDK 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 SDKs的應用程式復原控制器程式碼範例。

> **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。

搭配 使用 ARC 路由控制 API 操作的範例 AWS CLI

本節將逐步介紹使用路由控制的簡單應用程式範例，使用 AWS Command Line Interface 在 Amazon Application Recovery Controller (ARC) 中使用 API 操作的路由控制功能。這些範例旨在協助您了解如何使用 CLI 進行路由控制。

透過 Amazon Application Recovery Controller (ARC) 中的路由控制，您可以在單獨或可用區域中執行的備援應用程式複本 AWS 區域 或複本之間觸發流量容錯移轉。

您可以將路由控制組織到叢集上佈建的稱為控制面板的群組。ARC 叢集是全域部署的一組區域性端點。叢集端點提供高可用性 API，您可以用來設定和擷取路由控制狀態。如需路由控制功能元件的詳細資訊，請參閱 路由控制元件。

> **Note**
>
> ARC 是支援多個端點的全域服務 AWS 區域。不過，您必須在大多數 ARC CLI 命令`--region us-west-2`中指定美國西部（奧勒岡）區域，也就是指定 參數。例如，當您建立復原群組、控制面板和叢集時，請使用 `region` 參數。
> 當您建立叢集時，ARC 會為您提供一組區域端點。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)。

如需使用 的詳細資訊 AWS CLI，請參閱 AWS CLI 命令參考。如需路由控制 API 動作的清單，請參閱路由控制 API 操作和 路由控制 API 操作。

首先，我們將使用路由控制來建立管理容錯移轉所需的元件，從建立叢集開始。

設定路由控制元件

我們的第一步是建立叢集。ARC 叢集是一組五個端點，每五個端點各一個 AWS 區域。ARC 基礎設施支援這些端點協同運作，以確保容錯移轉操作的高可用性和循序一致性。

1. 建立 叢集

1a. 建立叢集。`network-type` 是選用的，可以是 `IPV4`或 `DUALSTACK`。預設值為 `IPV4`。

```
aws route53-recovery-control-config create-cluster --cluster-name test --network-type
 DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

當您第一次建立 ARC 資源時，它在建立叢集`PENDING`時的狀態為 。您可以呼叫 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::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

當狀態為 DEPLOYED 時，ARC 已成功建立具有一組端點的叢集，供您互動。您可以呼叫 來列出所有叢集`list-clusters`。

1c. 列出您的叢集。

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

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "DEPLOYED",
    "Owner": "123456789123",
    "NetworkType": "DUALSTACK"
}
```

1d. 更新叢集的網路類型。選項為 IPV4 或 DUALSTACK。

```
aws route53-recovery-control-config update-cluster \
--cluster-arn arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234 \
--network-type DUALSTACK
```

```
"Cluster": {
    "ClusterArn": "arn:aws:route53-recovery-
control::123456789123:cluster/12341234-1234-1234-1234-123412341234",
    "Name": "test",
    "Status": "PENDING",
    "Owner": "123456789123",
```

```
   "NetworkType": "DUALSTACK"
}
```

2. 建立控制面板

控制面板是用於組織 ARC 路由控制的邏輯分組。當您建立叢集時，ARC 會自動為您提供一個控制面板，稱為 DefaultControlPanel。您可以立即使用此控制面板。

控制面板只能存在於一個叢集中。如果您想要將控制面板移至另一個叢集，您必須將其刪除，然後在第二個叢集中建立它。您可以呼叫 來查看帳戶中的所有控制面板list-control-panels。若要只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"
        }
    ]
}
```

或者，您也可以呼叫 來建立自己的控制面板create-control-panel。

2b. 建立控制面板。

```
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"
    }
}
```

當您首次建立 ARC 資源時，其在建立PENDING時的狀態為 。您可以呼叫 來檢查進度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面板，您可以開始建立路由控制。建立路由控制時，您必須至少指定要路由控制所在的叢集的 Amazon Resource Name (ARN)。您也可以指定路由控制的控制面板 ARN。您還需要指定控制面板所在的叢集。

如果您未指定控制面板，您的路由控制會新增至自動建立的控制面板 DefaultControlPanel。

呼叫 來建立路由控制create-routing-control。

3a. 建立路由控制。

```
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"
    }
}
```

路由控制遵循與其他 ARC 資源相同的建立模式，因此您可以透過呼叫描述操作來追蹤其進度。

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"
    }
}
```

您可以呼叫 ，列出控制面板中的路由控制`list-routing-controls`。控制面板 ARN 是必要的。

3c. 列出路由控制。

```
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"
        }
    ]
}
```

在下列範例中，我們處理路由控制狀態時，假設您有兩個路由控制列於本節 (Rc1 和 Rc2)。在此範例中，每個路由控制代表應用程式部署所在的可用區域。

4. 建立安全規則

當您同時使用多個路由控制時，您可以決定在啟用和停用它們時要採取一些保護措施，以避免意外的後果，例如關閉兩個路由控制並停止所有流量流程。若要建立這些保護措施，您可以建立路由控制安全規則。

安全規則有兩種類型：聲明規則和閘道規則。若要進一步了解安全規則，請參閱 建立路由控制的安全規則。

以下呼叫提供建立宣告規則的範例，以確保On在任何指定時間，兩個路由控制中至少有一個設定為 。若要建立規則，您可以使用 `assertion-rule` 參數執行 `create-safety-rule` 。

如需聲明規則 API 操作的詳細資訊，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 AssertionRule。

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道規則的範例，為控制面板中的一組目標路由控制項提供整體的「開啟/關閉」或「閘道」切換。這可讓您不允許更新目標路由控制，例如，自動化無法進行未經授權的更新。在此範例中，門控開關是由 GatingControls 參數指定的路由控制，而由 TargetControls 參數指定的兩個路由控制或 "gated"。

> **Note**
>
> 建立閘道規則之前，您必須建立閘道路由控制，其中不包含 DNS 容錯移轉記錄，以及使用 DNS 容錯移轉記錄設定的目標路由控制。

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

如需聲明規則 API 操作的詳細資訊，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 GatingRule。

4b. 建立閘道規則。

```
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
        }
    }
}
```

如同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之後加以描述、列出或刪除。

設定一或多個安全規則後，您可以繼續與叢集互動、設定或擷取路由控制的狀態。如果`set-routing-control-state`操作中斷您建立的規則，您會收到類似以下的例外狀況：

```
Cannot modify control state for [0123456bbbbbbb0123456bbbbbb01234560123
abcdefg1234567] due to failed rule evaluation
0123456bbbbbbb0123456bbbbbb0123456333333444444
```

第一個識別符是與路由控制 ARN 串連的控制面板 ARN。第二個識別符是與安全規則 ARN 串連的控制面板 ARN。

5. 建立運作狀態檢查

若要使用路由控制容錯移轉流量，您可以在 Amazon Route 53 中建立運作狀態檢查，然後將運作狀態檢查與您的 DNS 記錄建立關聯。若要容錯移轉流量，ARC 路由控制會將運作狀態檢查設定為失敗，以便 Route 53 重新路由流量。（運作狀態檢查對您的應用程式的運作狀態無效；它只是用作重新路由流量的方法。）

例如，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運作狀態檢查，您可以執行下列動作，例如：

1. 使用 ARC CLI 為每個儲存格建立路由控制。
2. 使用 Route 53 CLI 為每個路由控制在 Route 53 中建立 ARC 運作狀態檢查。
3. 使用 Route 53 CLI 在 Route 53 中建立兩個容錯移轉 DNS 記錄，並將運作狀態檢查與每個記錄建立關聯。

5a. 為每個儲存格建立路由控制。

```
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. 為每個路由控制建立運作狀態檢查。

> **Note**
>
> 您可以使用 Amazon Route 53 CLI 建立 ARC 運作狀態檢查。

```
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-fffff22222",
    "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，並將運作狀態檢查與每個記錄建立關聯。

您可以使用 Route 53 CLI 在 Route 53 中建立容錯移轉 DNS 記錄。若要建立記錄，請遵循 change-resource-record-sets 命令的 Amazon Route 53 AWS CLI Command Reference 中的指示。在記錄

中，指定每個儲存格的 DNS 值，以及 Route 53 為運作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至次要儲存格，您可以遵循步驟 4b 中的 CLI 範例，將 的狀態更新RoutingControlCell1為 OFF，並將 更新RoutingControlCell2為 ON。

使用 列出和更新路由控制和狀態 AWS CLI

建立叢集、路由控制和控制面板等 Amazon Application Recovery Controller (ARC) 資源之後，您可以與叢集互動，以列出和更新容錯移轉的路由控制狀態。

對於您建立的每個叢集，ARC 會為您提供一組叢集端點，每五個端點中各一個 AWS 區域。當您呼叫叢集以擷取或將路由控制狀態設定為 On或 時，您必須指定其中一個區域端點 (AWS 區域 和端點 URL)Off。當您使用 AWS CLI來取得或更新路由控制狀態時，除了區域端點之外，您還必須指定區域端點--region的 ，如本節範例所示。

您可以使用任何區域叢集端點。建議您的系統輪換區域端點，並準備好使用每個可用的端點重試。如需循序說明嘗試叢集端點的程式碼範例，請參閱 使用 AWS SDKs的應用程式復原控制器的動作。

如需使用 的詳細資訊 AWS CLI，請參閱 AWS CLI 命令參考。如需路由控制 API 動作和詳細資訊連結的清單，請參閱 路由控制 API 操作。

> **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。ARC 提供極高的可靠性與 ARC 路由控制資料平面，用於重新路由流量和跨儲存格容錯移轉。如需使用 ARC 進行容錯移轉的更多建議，請參閱 ARC 中路由控制的最佳實務。

當您建立路由控制時，狀態會設為 Off。這表示流量不會路由到該路由控制的目標儲存格。您可以執行命令 來驗證路由控制的狀態get-routing-control-state。

若要判斷要指定的區域和端點，請執行 describe-clusters命令以檢視 ClusterEndpoints。每個 都ClusterEndpoint包含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 是一種復原控制組態 API 操作。我們建議您將 ARC 區域叢集端點的本機副本保留在書籤中，或以自動化程式碼進行硬式編碼，以用於重試端點。

1. 列出路由控制

您可以使用高度可靠的 ARC 資料平面端點來檢視路由控制和路由控制狀態。

1. 列出特定控制面板的路由控制。如果您未指定控制面板， 會list-routing-controls傳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

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. 更新路由控制

若要將流量路由至由路由控制控制控制的目標端點，請將路由控制狀態更新為 On。執行命令 來更新路由控制狀態update-routing-control-state。（請求成功時，回應為空白。）

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
```

```
{}
```

您可以使用一個 API 呼叫同時更新數個路由控制：update-routing-control-states。（請求成功時，回應為空白。）

2b. 一次更新數個路由控制狀態（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 ARC 中使用路由控制元件

主題

- 在 ARC 中建立路由控制元件
- 在 ARC 中檢視和更新路由控制狀態
- 建立路由控制的安全規則
- 支援 ARC 中叢集的跨帳戶

在 ARC 中建立路由控制元件

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 Application Recovery Controller (ARC) 中使用路由控制。

首先建立叢集，以託管您的路由控制和用於分組的控制面板。然後建立路由控制和運作狀態檢查，以便您可以將流量從一個儲存格重新路由到另一個儲存格，以便流量進入備份複本。

請注意，系統會針對您建立的每個叢集按小時收費。您通常只需要一個叢集來託管路由控制和控制面板，以管理應用程式的復原控制。此外，您可以使用 設定資源共用 AWS Resource Access Manager，讓一個叢集可以託管路由控制和多個 擁有的其他 ARC 資源 AWS 帳戶。若要了解 ARC 中的資源共用，請支援 ARC 中叢集的跨帳戶。如需定價資訊，請參閱 Amazon Application Recovery Controller (ARC) 定價。

若要使用路由控制容錯移轉流量，您可以建立路由控制運作狀態檢查，以便與應用程式中資源的 Amazon Route 53 DNS 記錄建立關聯。例如，假設您有兩個儲存格，其中一個已設定為應用程式的主要儲存格，另一個已設定為次要儲存格則會容錯移轉。

若要設定容錯移轉的運作狀態檢查，請執行下列動作：

1. 為每個儲存格建立路由控制。
2. 為每個路由控制建立運作狀態檢查。
3. 建立兩個 DNS 記錄，例如兩個 DNS 容錯移轉記錄，並將運作狀態檢查與每個記錄建立關聯。

另一個您可能建立路由控制的情況是，當您建立屬於閘道規則的安全規則時。在此情況下，您不會將運作狀態檢查和 DNS 記錄與路由控制建立關聯，因為您會將其用作閘道路由控制。如需詳細資訊，請參閱建立路由控制的安全規則。

這些區段包含在 ARC 主控台上建立路由控制的元件步驟。若要了解如何搭配 ARC 使用復原控制組態 API 操作，請參閱 路由控制 API 操作。

在 ARC 中建立叢集

您必須建立叢集，以在 ARC 中託管路由控制和控制面板。

叢集是一組備援的區域端點，您可以對其執行 API 呼叫來更新或取得一或多個路由控制的狀態。單一叢集可以託管許多路由控制。

> **Important**
>
> 請注意，系統會針對您建立的每個叢集按小時收費。一個叢集可以託管許多路由控制和控制面板以進行復原控制管理，通常足以進行應用程式。

建立叢集

1. 在 開啟 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 Create Cluster (建立叢集)。

在 ARC 中建立路由控制

為您要路由流量的每個儲存格建立路由控制。例如，當您的應用程式具有為可復原性而孤立的資源時，每個區域可能都有一個儲存格 AWS 區域，每個區域內每個可用區域的巢狀儲存格。在此案例中，您會為每個儲存格和每個巢狀儲存格建立路由控制。

當您建立路由控制時，請記住路由控制名稱在每個控制面板中必須是唯一的。

建立路由控制以用於重新路由流量之後，您可以將每個流量與運作狀態檢查建立關聯，這可讓您根據與每個流量相關聯的 DNS 記錄，將流量路由到儲存格。如果您要將閘道規則設定為安全規則並建立閘道路由控制，則不會將運作狀態檢查新增至路由控制。

建立路由控制

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 在路由控制頁面上，選擇建立，然後選擇路由控制。
4. 輸入路由控制的名稱，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面板，包括使用預設控制面板。或者，建立新的控制面板。
5. 如果您選擇建立新的控制面板，請選擇要建立控制面板的叢集，然後輸入面板的名稱。
6. 選擇建立路由控制。

7. 依照步驟來命名和建立路由控制。

在 ARC 中建立路由控制運作狀態檢查

您可以將路由控制運作狀態檢查與要用於重新路由流量的每個路由控制建立關聯。然後，您可以使用 Amazon Route 53 DNS 記錄設定每個運作狀態檢查，例如容錯移轉 DNS 記錄。然後，您只需更新相關聯路由控制的狀態，即可在 Amazon Application Recovery Controller (ARC) 中重新路由流量，將其設定為 `On`或 `Off`。

> **Note**
>
> 您無法編輯現有的路由控制運作狀態檢查，將其與不同的路由控制建立關聯。

建立路由控制運作狀態檢查

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 在路由控制頁面上，選擇路由控制。
4. 在路由控制詳細資訊頁面上，選擇建立運作狀態檢查。
5. 輸入運作狀態檢查的名稱，然後選擇建立。

接著，您可以建立 Route 53 DNS 記錄，並將路由控制運作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 容錯移轉記錄來與路由控制運作狀態檢查建立關聯。若要讓 ARC 使用路由控制正確容錯移轉流量，請先在 Route 53 中建立兩個容錯移轉記錄：主要和次要。如需設定 DNS 容錯移轉記錄的詳細資訊，請參閱運作狀態檢查概念。

當您建立主要容錯移轉記錄時，這些值應該如下：

```
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該如下：

```
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。若要這樣做，請更新相關聯的路由控制狀態，將主要路由控制狀態變更為 ，OFF並將次要路由控制狀態變更為 ON。當您執行此操作時，相關聯的運作狀態檢查會停止流量前往主要複本，並改為將其路由至次要複本。如需使用路由控制容錯移轉流量的詳細資訊，請參閱 使用 ARC API 取得和更新路由控制狀態（建議）。

若要查看使用 ARC API 操作建立路由控制和相關聯運作狀態檢查的 AWS CLI 命令範例，請參閱 搭配使用 ARC 路由控制 API 操作的範例 AWS CLI。

在 ARC 中建立控制面板

Amazon Application Recovery Controller (ARC) 中的控制面板可讓您將相關路由控制分組在一起。視容錯移轉的範圍而定，控制面板可以具有代表應用程式內微服務的路由控制、整個應用程式本身或一組應用程式。將路由控制分組到控制面板的好處是，您可以搭配控制面板使用安全規則，以協助保護流量路由變更。

當您建立叢集時，ARC 會建立預設控制面板。您可以使用預設控制面板進行路由控制，也可以建立一或多個控制面板來將路由控制分組。請注意，控制面板名稱僅支援 ASCII 字元。

本節包含在 ARC 主控台上建立控制面板的步驟。如需搭配 ARC 使用復原控制組態 API 操作的詳細資訊，請參閱 路由控制 API 操作。

建立控制面板

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 在路由控制頁面上，選擇建立，然後選擇控制面板。
4. 選擇要建立控制面板的叢集，然後輸入面板的名稱。
5. 選擇建立控制面板。

在 ARC 中檢視和更新路由控制狀態

本節說明如何在 Amazon Application Recovery Controller (ARC) 中檢視和更新路由控制狀態。路由控制是簡單的開關，可管理流向復原群組中儲存格的流量。儲存格通常 AWS 區域或有時是包含 資源的可用區域。當路由控制狀態為 時On，流量會流向由該路由控制控制的儲存格。

您可以將路由控制分組到控制面板，也就是邏輯容錯移轉分組。例如，當您在主控台上開啟控制面板時，您可以一次檢視分組的所有路由控制，以查看流量的流動位置。

您可以在 ARC 主控台或使用 ARC API 更新路由控制狀態。建議您使用 API 更新路由控制狀態。首先，ARC 在資料平面中使用 API 提供極高的可靠性，以執行這些動作。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應用程式流量，跨儲存格容錯移轉。此外，如果您嘗試連線的叢集端點無法使用，您可以使用 API 視需要嘗試輪換連線到不同的叢集端點。

您可以更新一個路由控制狀態，也可以一次更新數個路由控制狀態。例如，您可能想要將一個路由控制狀態設定為 Off，以停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 On，以啟動流向另一個儲存格或可用區域的流量。在此案例中，您可以同時更新兩個路由控制狀態，讓流量繼續流動。

主題

- 使用 ARC API 取得和更新路由控制狀態 （ 建議 ）
- 在 中取得和更新路由控制狀態 AWS 管理主控台

使用 ARC API 取得和更新路由控制狀態 （ 建議 ）

我們建議您使用 Amazon Application Recovery Controller (ARC) 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 SDKs 使用 ARC API 操作。建議使用 API 操作搭配 CLI 或程式碼，以使用路由控制狀態，而不是使用 AWS 管理主控台。

ARC 透過使用 API 更新路由控制狀態來提供跨儲存格容錯移轉的極高可靠性 (AWS 區域)，因為路由控制存放在高可用性的叢集中。ARC 可確保您隨時都能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，請連線至其中一個區域叢集端點。如果端點無法使用，您可以嘗試連線至另一個叢集端點。

您可以在 Route 53 主控台中，或使用 API 動作 DescribeCluster 來檢視叢集的區域叢集端點清單。取得和變更路由控制狀態的程序應視需要輪換嘗試每個端點，因為叢集端點會循環顯示可用和無法使用的狀態，以進行定期維護和更新。

我們提供詳細資訊和程式碼範例，以使用 ARC API 操作來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 SDKs 的應用程式復原控制器的動作。
- 如需使用 AWS CLI 取得和更新路由控制狀態的詳細資訊，請參閱 使用 列出和更新路由控制和狀態 AWS CLI。

在 中取得和更新路由控制狀態 AWS 管理主控台

您可以在 中取得和更新路由控制狀態 AWS 管理主控台。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，您不需要像使用 Amazon Application Recovery Controller (ARC) API 一樣，在主控台中選擇和輪換叢集端點的程序。此外，當 ARC 資料平面提供極高的可靠性時，主控台無法高度使用。基於這些原因，我們建議您使用 ARC API 來取得和更新生產操作的路由控制狀態。

如需使用 ARC 進行容錯移轉的更多建議，請參閱 ARC 中路由控制的最佳實務。

若要在 主控台中檢視和更新路由控制，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 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 從清單中，選擇控制面板並檢視路由控制項。

更新一或多個路由控制狀態

1. 開啟位於 https：// 的 Amazon Route 53 主控台。 https://console.aws.amazon.com/route53/home
2. 在應用程式復原控制器下，選擇路由控制。
3. 選擇動作，然後選擇變更流量路由。
4. 將一或多個路由控制的狀態更新為 `Off`或 `On`，取決於您希望流量流向或停止為應用程式流向的位置。
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時，您可以決定要採取保護措施，以避免意外的後果。例如，您可能想要防止不小心關閉應用程式的所有路由控制，這會導致故障開啟案例。或者，您可能想要實作主開關來停用

一組路由控制，可能是為了防止自動化重新路由流量。若要在 ARC 中建立路由控制的防護，請建立安全規則。

您可以使用路由控制、規則和您指定之其他選項的組合來設定路由控制的安全規則。每個安全規則都與單一控制面板相關聯，但控制面板可以有多個安全規則。當您建立安全規則時，請記住，安全規則名稱在每個控制面板中必須是唯一的。

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
- 覆寫安全規則以重新路由流量

安全規則的類型

有兩種類型的安全規則：聲明規則和閘道規則，您可以用不同的方式保護容錯移轉。

聲明規則

使用宣告規則時，當您變更一個或一組路由控制狀態時，ARC 會強制執行您在設定規則時設定的條件，否則路由控制狀態不會變更。

其中一個有用的範例是防止故障開啟案例，例如您停止流量流向一個儲存格，但不啟動流向另一個儲存格的流量的情況。為了避免這種情況，宣告規則可確保控制面板中一組路由控制項中至少有一個路由控制項On在任何指定時間。這可確保流量流向應用程式至少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，請參閱在 中建立安全規則搭配 使用 ARC 路由控制 API 操作的範例 AWS CLI。

如需聲明規則 API 操作屬性的詳細資訊，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 AssertionRule。

閘道規則

使用閘道規則，您可以對一組路由控制強制執行整體開啟/關閉切換，以便根據您在規則中指定的一組條件強制執行是否可以變更這些路由控制狀態。最簡單的條件是您指定為切換的單一路由控制是設定為 ON或 OFF。

若要實作此功能，您可以建立門控路由控制，以使用 做為整體交換器，以及目標路由控制，以控制流向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道規則設定的目標路由控制狀態，請將閘道路由控制狀態設定為 Off。若要允許更新，您可以將其設定為 On。

若要查看建立實作此類整體切換的閘道規則的範例 AWS CLI 命令，請參閱在 中建立安全規則搭配使用 ARC 路由控制 API 操作的範例 AWS CLI。

如需閘道規則 API 操作屬性的詳細資訊，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 GatingRule。

在主控台上建立安全規則

本節中的步驟說明如何在 ARC 主控台上建立安全規則。無論您建立宣告規則或閘道規則，這些步驟都很類似。差異會記錄在程序中。

若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用復原和路由控制 API 操作，請參閱 路由控制 API 操作。

建立安全規則

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 在路由控制頁面上，選擇控制面板。
4. 在控制面板詳細資訊頁面上，選擇動作，然後選擇新增安全規則。
5. 選擇要新增的規則類型：宣告規則或閘道規則。
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。

   - 針對宣告規則，指定宣告的路由控制。
   - 對於閘道規則，指定閘道路由控制和目標路由控制。

   針對這兩個規則，選擇類型和閾值，以及是否反轉規則，以指定規則組態。

   > **Note**
   >
   > 若要進一步了解如何指定宣告規則，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 AssertionRule 操作提供的資訊。若要進一步了解如何指定閘道規則，請參閱《Amazon Application Recovery Controller 的路由控制 API 參考指南》中的 GatingRule 操作提供的資訊。

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 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。

若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用 API 操作，請參閱 路由控制 API 操作。

刪除安全規則

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇路由控制。
3. 在路由控制頁面上，選擇控制面板。
4. 在控制面板詳細資訊頁面上，選擇安全規則，然後選擇刪除或編輯。

覆寫安全規則以重新路由流量

在某些情況下，您可能想要略過已設定安全規則強制執行的路由控制保護措施。例如，您可能想要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流量。在這樣的「中斷玻璃」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您的應用程式。

您可以使用 `update-routing-control-state`或 `update-routing-control-states` AWS CLI 命令搭配 `safety-rules-to-override` 參數，在更新路由控制狀態（或多個路由控制狀態）時略過安全規則。使用您要覆寫之安全規則的 Amazon Resource Name (ARN) 指定 參數，或指定以逗號分隔的 ARNs 清單來覆寫兩個或多個安全規則。

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**
>
> 由於您更新之路由控制項可能有多個安全規則，因此您可以執行 CLI 命令，使用一個安全規則覆寫來更新路由控制狀態，但收到另一個安全規則封鎖更新的錯誤。繼續將安全規則 ARNs 新增至更新命令中要覆寫的規則清單，並以逗號分隔，直到更新命令成功完成。

若要進一步了解如何搭配 API 和 SDKs 使用 `SafetyRulesToOverride` 屬性，請參閱 UpdateRoutingControlState。

以下是覆寫安全規則以更新路由控制狀態的兩個 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
```

支援 ARC 中叢集的跨帳戶

Amazon Application Recovery Controller (ARC) 與 整合 AWS Resource Access Manager 以啟用資源共用。 AWS RAM 是一種服務，可讓您與其他 AWS 帳戶 或透過 共用資源 AWS Organizations。對於 ARC 路由控制，您可以共用叢集資源。

您可以透過建立資源共享 AWS RAM，與 共用您擁有的資源。資源共用會指定要共用的資源，以及要共用的資源參與者。參與者可以包括：

- 中的擁有者組織 AWS 帳戶 內部或外部特定 AWS Organizations

- 中的組織單位 AWS Organizations
- 其在 中的整個組織 AWS Organizations

如需 的詳細資訊 AWS RAM，請參閱AWS RAM 《 使用者指南》 。

透過使用 AWS Resource Access Manager 在 ARC 中跨帳戶共用叢集資源，您可以使用一個叢集來託管數個不同 擁有的控制面板和路由控制 AWS 帳戶。當您選擇共用叢集時， AWS 帳戶 您指定的其他可以使用叢集來託管自己的控制面板和路由控制，從而對跨不同團隊的路由功能提供更多控制和彈性。

AWS RAM 是一項服務，可 AWS 協助客戶安全地跨 共用資源 AWS 帳戶。透過 AWS RAM，您可以使用 IAM 角色和使用者 AWS Organizations在 中的組織或組織單位 (OUs) 內共用資源。 AWS RAM 是一種集中且受控制的方式，可共用叢集。

當您共用叢集時，您可以減少組織所需的叢集總數。透過共用叢集，您可以分配在不同團隊之間執行叢集的總成本，以降低成本最大化 ARC 的優勢。（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加入 ARC 的程序，特別是如果您有大量應用程式分散在多個帳戶和營運團隊。

若要開始使用 ARC 中的跨帳戶共用，您可以在其中建立資源共用 AWS RAM。資源共享會指定有權共享您帳戶所擁有叢集的參與者。然後，參與者可以使用 或使用 AWS Command Line Interface AWS SDKs AWS 管理主控台 執行 ARC API 操作，在叢集中建立資源，例如控制面板和路由控制。

本主題說明如何共用您擁有的參數，以及如何使用與您共用的參數。

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
- 共用叢集的責任和許可
- 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 中擁有叢集 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。

- 若要與組織或 中的組織單位共用叢集 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。
- AWS RAM 全域資源的資源共用，例如叢集，必須在美國東部 （維吉尼亞北部） 區域 (us-east-1) 建立。

共用叢集

當您共享您擁有的叢集時，您指定共享叢集的參與者可以在叢集中建立和託管自己的 ARC 資源。

若要共用叢集，您必須將其新增至資源共用。資源共用是可讓您在 AWS 帳戶之間共用資源的一種 AWS RAM 資源。資源共用會指定要共用的資源，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享，您可以使用 AWS RAM 主控台，或搭配 AWS Command Line Interface AWS SDKs使用 AWS RAM API 操作。

如果您是 中的組織的一部分， AWS Organizations 且已啟用組織內的共用，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享的邀請，並在接受邀請後獲得共用叢集的存取權。

您可以使用 AWS RAM 主控台，或搭配 AWS CLI 或 SDK 使用 AWS RAM API 操作，來共用您擁有的叢集。 SDKs

使用 AWS RAM 主控台共用您擁有的叢集

請參閱AWS RAM 《 使用者指南》中的建立資源共享。

使用 共享您擁有的叢集 AWS CLI

使用 create-resource-share 命令。

授予共用叢集的許可

在帳戶之間共用叢集需要 IAM 主體透過 共用叢集的許可 AWS RAM。

我們建議您使用 AmazonRoute53RecoveryControlConfigFullAccess受管 IAM 政策，以確保您的 IAM 主體具有共用和使用共用叢集所需的許可。

使用自訂 IAM 政策共用叢集需要該叢集的 route53-recovery-control-config:PutResourcePolicy、 route53-recovery-control-

config:GetResourcePolicy和 route53-recovery-control-config:DeleteResourcePolicy許可。 PutResourcePolicy和 DeleteResourcePolicy是僅限許可的 IAM 動作。在沒有這些許可 AWS RAM 的情況下嘗試透過 共用叢集將導致錯誤。

如需 IAM AWS Resource Access Manager 使用方式的詳細資訊，請參閱AWS RAM 《 使用者指南》中的如何使用 AWS Resource Access Manager IAM。

取消共用共用叢集

當您取消共用叢集時，下列項目適用於參與者和擁有者：

- 目前參與者資源會繼續存在於未共用的叢集中。
- 參與者可以繼續更新未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。
- 參與者無法再於未共用叢集中建立新的資源。
- 如果參與者在未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，請從資源共用中移除它。您可以使用 AWS RAM 主控台或搭配 或 AWS CLI SDKs 使用 AWS RAM API 操作來執行此操作。

使用 AWS RAM 主控台取消共用您擁有的共用叢集

請參閱《AWS RAM 使用者指南》中的更新資源共享。

使用 取消共用您擁有的共用叢集 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在 中檢視資訊來識別共用叢集 AWS RAM。他們也可以使用 ARC 主控台和取得共用資源的相關資訊 AWS CLI。

一般而言，若要進一步了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 檢視您與他人共用的所有資源 AWS RAM。如需詳細資訊，請參閱在 中檢視共用資源 AWS RAM。
- 身為參與者，您可以使用 檢視與您共用的所有資源 AWS RAM。如需詳細資訊，請參閱在 中檢視共用資源 AWS RAM。

身為擁有者，您可以透過在 中檢視資訊 AWS 管理主控台 或使用 AWS Command Line Interface 搭配 ARC API 操作來判斷是否要共用叢集。

使用主控台識別是否共用您擁有的叢集

在叢集 AWS 管理主控台的詳細資訊頁面上，請參閱叢集共用狀態。

使用 識別是否共用您擁有的叢集 AWS CLI

使用 get-resource-policy 命令。如果叢集有資源政策，命令會傳回政策的相關資訊。

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。

共用叢集的責任和許可

擁有者的許可

當您與其他人共用您擁有的叢集時 AWS 帳戶，允許使用叢集的參與者可以在叢集中建立控制面板、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，以變更路由控制狀態。

不過，您可以檢視您擁有之叢集中參與者所建立路由控制的詳細資訊。例如，您可以使用 AWS Command Line Interface AWS SDKs 呼叫 ARC 路由控制 API 操作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 中設定具有存取資源許可的角色，並將您的帳戶新增至角色。

參與者的許可

一般而言，參與者可以在與其共用的叢集中建立並使用控制面板、路由控制、安全規則和運作狀態檢查。他們只有在擁有資源時，才能檢視、修改或刪除共用叢集中的叢集資源。例如，參與者可以為他們已建立的控制面板建立和刪除安全規則。

下列限制適用於參與者：

- 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、建立或修改其他帳戶在共用叢集中建立之資源的路由控制，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建立的安全規則。
- 參與者無法在共用叢集的預設控制面板中新增資源，因為它屬於叢集擁有者。

如上所述，參與者無法在共用叢集的預設控制面板中建立路由控制，因為叢集擁有者擁有預設控制面板。不過，叢集擁有者可以建立跨帳戶 IAM 角色，提供存取叢集預設控制面板的許可。然後，擁有者可以授予參與者擔任角色的許可，以便參與者可以存取預設控制面板來使用它，但擁有者已透過角色的許可指定。

帳單成本

ARC 中叢集的擁有者需支付叢集的相關費用。對於叢集擁有者或參與者，建立叢集中託管的資源無需額外費用。

如需詳細的定價資訊和範例，請參閱 Amazon Application Recovery Controller (ARC) 定價。

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，都會計入叢集和其他資源的有效配額，例如路由控制。如果共用叢集資源的帳戶配額高於叢集擁有者的配額，則叢集擁有者的配額優先於共用帳戶配額。

若要進一步了解其運作方式，請參閱下列範例。為了說明配額如何使用資源共用，針對這些範例，假設叢集擁有者是擁有者，而已共用叢集的帳戶是參與者。

控制面板配額

每個叢集的擁有者控制面板總數會強制執行配額。

例如，假設擁有者對每個叢集的控制面板數量有 50 個配額，而且叢集中有 13 個控制面板。現在，假設參與者的配額設定為 150。在此案例中，參與者最多只能在共用叢集中建立 37 個控制面板（即 50-13)。

此外，如果共用叢集的其他帳戶也建立控制面板，這些帳戶也會計入 50 個控制面板的叢集整體配額。

路由控制配額

路由控制具有多個配額：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。擁有者的配額優先於所有這些配額。

例如，假設擁有者對每個叢集的路由控制數量有 300 個配額，而且叢集中已有 300 個路由控制。現在，假設參與者將此配額設定為 500。在此案例中，參與者無法在共用叢集中建立新的路由控制。

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，假設每個控制面板的安全規則數量的擁有者配額為 20，且參與者將此配額設為 80。在此案例中，由於擁有者的下限優先，參與者在共用叢集的控制面板中最多只能建立 20 個安全規則。

如需路由控制配額的清單，請參閱 路由控制的配額。

在 Amazon Application Recovery Controller (ARC) 中記錄和監控路由控制

您可以使用 AWS CloudTrail 在 Amazon Application Recovery Controller (ARC) 中監控路由控制，以分析模式並協助疑難排解問題。

主題

- 使用 記錄 ARC API 呼叫 AWS CloudTrail

使用 記錄 ARC API 呼叫 AWS CloudTrail

Amazon Application Recovery Controller (ARC) 已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 ARC 中 AWS 服務所採取動作的記錄。CloudTrail 會將 ARC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 ARC 主控台的呼叫，以及對 ARC API 操作的程式碼呼叫。

如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 ARC 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 所收集的資訊，判斷向 ARC 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 ARC 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 ARC 中發生時，該活動會與事件歷史記錄中的其他 AWS 服務事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

若要持續記錄 中的事件 AWS 帳戶，包括 ARC 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀

- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 ARC 動作，並記錄在 Amazon Application Recovery Controller 的 Recovery Readiness API 參考指南、Amazon Application Recovery Controller 的 Recovery Control Configuration API 參考指南，以及 Amazon Application Recovery Controller 的 Routing Control API 參考指南中。例如，對 `CreateCluster`、`UpdateRoutingControlState` 和 `CreateRecoveryGroup` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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 userIdentity 元素。

檢視事件歷史記錄中的 ARC 事件

CloudTrail 可讓您使用 Event history (事件歷史記錄) 檢視最近的事件。若要檢視 ARC API 請求的事件，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）。如需詳細資訊，請參閱「AWS CloudTrail 使用者指南」中的使用 CloudTrail 事件歷史記錄。

了解 ARC 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範設定路由控制`CreateCluster`的動作。

```
{
  "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 CloudTrail 日誌項目，示範路由控制UpdateRoutingControlState的動作。

```
{
  "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"
}
```


中路由控制的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目錄

- Amazon Application Recovery Controller (ARC) 中的路由控制如何與 IAM 搭配使用
- ARC 中路由控制的身分型政策範例
- AWS Amazon Application Recovery Controller (ARC) 中路由控制的受管政策

Amazon Application Recovery Controller (ARC) 中的路由控制如何與 IAM 搭配使用

在您使用 IAM 管理 Amazon Application Recovery Controller (ARC) 中路由控制的存取權之前，請先了解哪些 IAM 功能可與路由控制搭配使用。

您可以在 Amazon Application Recovery Controller (ARC) 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

IAM 功能	路由控制支援
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 服務如何與大多數 IAM 功能搭配使用的高階整體檢視，請參閱《IAM 使用者指南》中的與 IAM AWS 搭配使用的 服務。

ARC 的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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。

若要檢視路由控制的 ARC 身分型政策範例，請參閱 ARC 中路由控制的身分型政策範例。

路由控制內的資源型政策

支援資源型政策：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。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 ARC 動作清單，請參閱服務授權參考中的 Amazon Route 53 復原控制項定義的動作和 Amazon Route 53 復原叢集定義的動作。

ARC 中的路由控制政策動作會在動作之前使用下列字首，視您使用的 API 而定：

```
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*"
```

若要檢視路由控制的 ARC 身分型政策範例，請參閱 ARC 中路由控制的身分型政策範例。

ARC 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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該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 ARC 相關的資訊：

若要查看資源類型及其 ARNs 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 Route 53 復原控制項定義的動作
- Amazon Route 53 Recovery Cluster 定義的動作。

若要檢視路由控制的 ARC 身分型政策範例，請參閱 ARC 中路由控制的身分型政策範例。

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` 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看路由控制的 ARC 條件索引鍵清單，請參閱服務授權參考中的下列主題：

- Amazon Route 53 復原控制項的條件索引鍵
- Amazon Route 53 Recovery Cluster 的條件索引鍵

若要查看可與條件金鑰搭配使用的動作和資源，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 ARNs 的清單，請參閱 Amazon Route 53 復原控制項定義的動作和 Amazon Route 53 復原叢集定義的動作。
- 若要查看您可以使用每個資源的 ARN 指定的動作清單，請參閱 Amazon Route 53 Recovery Controls 定義的資源和 Amazon Route 53 Recovery Cluster 定義的資源。

若要檢視路由控制的 ARC 身分型政策範例，請參閱 ARC 中路由控制的身分型政策範例

ARC 中的存取控制清單 (ACLs)

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。

使用 ARC 的屬性型存取控制 (ABAC)

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，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

ARC 路由控制包括下列對 ABAC 的支援：

- 復原控制組態支援 ABAC。
- 復原叢集不支援 ABAC。

搭配 ARC 使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時，會自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

ARC 的跨服務主體許可

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，您會被視為委託人。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政策中的其他相依動作，請參閱服務授權參考中的下列主題：

- Amazon Route 53 復原叢集
- Amazon Route 53 復原控制

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

ARC 的服務連結角色

支援服務連結角色：

服務連結角色是連結至 服務的一種 AWS 服務角色。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帳戶中 AWS ，並由服務擁有。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。

ARC 中路由控制的身分型政策範例

根據預設，使用者和角色沒有建立或修改 ARC 資源的許可。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。

如需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 (主控台)。

如需 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 ARNs 格式，請參閱《服務授權參考》中的 Amazon Application Recovery Controller (ARC) 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 範例：用於路由控制的 ARC 主控台存取
- 範例：用於路由控制組態的 ARC API 動作

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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 ARC 主控台存取

若要存取 Amazon Application Recovery Controller (ARC) 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 ARC 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。

為了確保使用者和角色在僅允許存取特定 API 操作時仍可使用 ARC 主控台，請將 ARC 的`ReadOnly` AWS 受管政策連接至實體。如需詳細資訊，請參閱《IAM 使用者指南》中的 ARC 受管政策頁面或新增許可給使用者。

若要授予使用者透過主控台使用 ARC 路由控制功能的完整存取權，請將如下所示的政策連接至使用者，以授予使用者設定 ARC 路由控制資源和操作的完整許可：

JSON

```
{
    "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 ARC API 動作

為了確保使用者可以使用 ARC API 動作來使用 ARC 路由控制組態，請連接對應至使用者需要使用的 API 操作的政策，如下所述。

若要使用復原控制組態的 API 操作，請將如下所示的政策連接至使用者：

JSON

```
{
    "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 在 ARC 路由控制中執行任務，例如，將路由控制狀態更新為在災難事件期間容錯移轉，您可以將如下的 ARC IAM 政策連接至您的 IAM 使用者。

AllowSafetyRuleOverride 布林值提供許可，以覆寫您已設定為路由控制防護的安全規則。在「中斷玻璃」案例中，可能需要此許可，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，而一或多個安全規則可能會意外阻止重新路由流量所需的路由控制狀態更新。此許可允許操作員在進行 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，請參閱覆寫安全規則以重新路由流量。

如果您想要允許 運算子使用復原叢集資料平面 API，但防止覆寫安全規則，您可以使用AllowSafetyRuleOverrides布林值將如下所示的政策連接至 false。若要允許運算子覆寫安全規則，請將AllowSafetyRuleOverrides布林值設定為 true。

JSON

```
{
    "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 Application Recovery Controller (ARC) 中路由控制的受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。當新的 AWS 服務 啟動或新的 API 操作可供現有服務使用時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：AmazonRoute53RecoveryControlConfigFullAccess

您可以將 AmazonRoute53RecoveryControlConfigFullAccess 連接到 IAM 實體。此政策授予在 ARC 中使用復原控制組態之動作的完整存取權。將其連接到需要完全存取復原控制組態動作的 IAM 使用者和其他主體。

您可以自行決定新增對其他 Amazon Route 53 動作的存取權，讓使用者能夠建立路由控制的運作狀態檢查。例如，您可以允許下列一或多個動作的許可：route53:GetHealthCheck、route53:DeleteHealthCheck、route53:CreateHealthCheck和 route53:ChangeTagsForResource。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryControlConfigFullAccess。

AWS 受管政策：AmazonRoute53RecoveryControlConfigReadOnlyAccess

您可以將 AmazonRoute53RecoveryControlConfigReadOnlyAccess 連接到 IAM 實體。它適用於需要檢視路由控制和安全規則組態的使用者。此政策授予在 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、更新或刪除復原控制資源。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryControlConfigReadOnlyAccess。

AWS 受管政策：AmazonRoute53RecoveryClusterFullAccess

您可以將 AmazonRoute53RecoveryClusterFullAccess 連接到 IAM 實體。此政策授予在 ARC 中使用叢集資料平面之動作的完整存取權。將其連接到需要完整存取權才能更新和擷取路由控制狀態的 IAM 使用者和其他主體。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryClusterFullAccess。

AWS 受管政策：AmazonRoute53RecoveryClusterReadOnlyAccess

您可以將 AmazonRoute53RecoveryClusterReadOnlyAccess 連接到 IAM 實體。此政策授予 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。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryClusterReadOnlyAccess。

AWS 受管政策：AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy

您可以將 AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy 連接到 IAM 實體。此政策會授予 ARC 區域切換計畫執行和評估的許可。將其連接到用於區域切換計畫執行的 IAM 角色。

許可詳細資訊

此政策包含以下許可：

- arc-region-switch:GetPlan – 允許主體擷取區域切換計劃的組態詳細資訊。
- arc-region-switch:GetPlanExecution – 允許主體擷取特定區域切換計畫執行的相關資訊。
- arc-region-switch:ListPlanExecutions – 允許主體列出區域切換計劃的所有執行。
- iam:SimulatePrincipalPolicy – 允許主體模擬和評估 IAM 角色可執行的動作。此許可範圍僅限於 IAM 角色，並在計劃評估期間使用，以在執行區域切換計劃之前驗證是否具備必要的許可。
- cloudwatch:DescribeAlarms：允許主體擷取 Amazon CloudWatch 警示的相關資訊。

- `cloudwatch:DescribeAlarmHistory` – 允許主體擷取 Amazon CloudWatch 警示的歷史狀態變更。
- `cloudwatch:GetMetricStatistics` – 允許主體擷取 Amazon CloudWatch 指標的統計資料。

若要檢視政策的詳細資訊，包括最新版本的 JSON 政策文件，請參閱《 AWS 受管政策參考指南》中的 AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy。

路由控制的 AWS 受管政策更新

如需自此服務開始追蹤 ARC 中路由控制的 AWS 受管政策更新詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 的 AWS 受管政策更新。如需此頁面變更的自動提醒，請訂閱 ARC 文件歷史記錄頁面上的 RSS 摘要。

路由控制的配額

Amazon Application Recovery Controller (ARC) 中的路由控制受限於下列配額 （ 先前稱為限制 ）。

實體	配額
每個帳戶的叢集數目	2
每個叢集的控制面板數量	50
每個控制面板的路由控制數目	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量	20
每個 UpdateRoutingControlStates 操作呼叫的路由控制數目	10
每秒對叢集端點的變動 API 呼叫數	3

ARC 中的準備度檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

透過 Amazon Application Recovery Controller (ARC) 中的準備程度檢查，您可以深入了解您的應用程式和資源是否已準備好進行復原。在 ARC 中建立 AWS 應用程式模型並建立準備度檢查後，檢查會持續監控應用程式的相關資訊，例如 AWS 資源配額、容量和網路路由政策。然後，您可以選擇收到變更的通知，這些變更會影響您容錯移轉至應用程式複本從事件復原的能力。準備度檢查有助於確保您可以持續將多區域應用程式維持在擴展和設定以處理容錯移轉流量的狀態。

本章說明如何透過建立描述您應用程式的復原群組和儲存格，在 ARC 中建立應用程式模型，以設定讓準備度檢查能夠運作的結構。然後，您可以依照步驟新增準備程度檢查和準備程度範圍，讓 ARC 可以稽核應用程式的準備程度。

建立整備檢查之後，您可以監控資源的整備狀態。準備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，以反映生產應用程式的容量、路由政策和其他組態詳細資訊。如果複本不相符，您可以新增容量或變更組態，讓您的應用程式複本再次對齊。

> **Important**
>
> 準備度檢查對於持續驗證應用程式複本組態和執行時間狀態是否一致最有用。準備度檢查不應用於指示您的生產複本是否正常運作，您也不應依賴準備度檢查作為災難事件期間容錯移轉的主要觸發條件。

什麼是 Amazon Application Recovery Controller (ARC) 中的準備程度檢查？

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

ARC 中的整備檢查會持續（每隔一分鐘）稽核 AWS 佈建容量、服務配額、限流限制，以及檢查中所包含資源的組態和版本差異。準備度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組態設定和相同的執行時間狀態。雖然整備檢查可確保跨複本設定的容量一致，但您不應期望他們代表您決定複本的容量。例如，您應該了解您的應用程式需求，以便在每個複本中使用足夠的緩衝容量來調整 Auto Scaling 群組大小，以便在另一個儲存格無法使用時管理。

對於配額，當 ARC 偵測到與整備檢查不相符時，可以透過增加較低的配額來調整複本的配額，以符合較高的配額。當配額相符時，整備檢查狀態會顯示 READY。（請注意，這不是立即更新程序，而且總時間取決於特定資源類型和其他因素。）

第一步是設定整備檢查，以建立代表您應用程式的復原群組。每個復原群組都會包含應用程式的每個個別故障遏制單位或複本的儲存格。接著，您可以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建立關聯。最後，您可以將資源與整備範圍建立關聯，以便取得復原群組（您的應用程式）或個別儲存格（複本，即區域或可用區域 (AZs)) 中資源的整備狀態。

準備程度（即 READY或 NOT READY) 是以準備程度檢查範圍內的資源，以及資源類型的一組規則為基礎。每種資源類型都有一組整備規則，ARC 檢查會使用這些規則來稽核資源的整備。資源是否READY根據每個整備規則的定義。所有整備規則都會評估資源，但有些則彼此比較資源，有些則查看資源集中每個資源的特定資訊。

透過新增整備檢查，您可以透過以下幾種方式之一來監控整備狀態：使用 EventBridge AWS 管理主控台、在 中或使用 ARC API 動作。您也可以監控不同內容中資源的整備狀態，包括儲存格的整備程度和應用程式的整備程度。使用 ARC 中的跨帳戶授權功能，讓您更輕鬆地設定和監控單一 AWS 帳戶的分散式資源。

使用整備檢查監控應用程式複本

ARC 會使用整備檢查來稽核您的應用程式複本，以確保每個複本都有相同的組態設定和相同的執行時間狀態。整備檢查會持續稽核應用程式 AWS 的資源容量、組態、 AWS 配額和路由政策、可用來協助確保複本已準備好進行容錯移轉的資訊。準備度檢查可協助您確保復原環境已擴展，並設定為在需要時容錯移轉至 。

下列各節提供有關整備檢查如何運作的詳細資訊。

準備度檢查和您的應用程式複本

若要準備進行復原，您必須隨時在複本中維持足夠的備用容量，以吸收來自其他可用區域或區域的容錯移轉流量。ARC 會持續（一分鐘一次）檢查您的應用程式，以確保您佈建的容量符合所有可用區域。

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 Amazon EBS 磁碟區大小。如果您擴展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，ARC 會偵測到不相符，以便您可以增加待命中的值。

> **Important**
>
> 準備度檢查對於持續驗證應用程式複本組態和執行時間狀態是否一致最有用。準備度檢查不應用於指示您的生產複本是否正常運作，您也不應依賴準備度檢查作為災難事件期間容錯移轉的主要觸發條件。

在主動待命組態中，您應該根據您的監控和運作狀態檢查系統，決定是否要離開或進入儲存格，並將整備檢查視為這些系統的補充服務。ARC 整備檢查並非高度可用，因此您不應依賴中斷期間可存取的檢查。此外，在災難事件期間，也可能無法使用已檢查的資源。

您可以監控特定儲存格 (AWS 區域或可用區域） 中應用程式資源或整體應用程式的整備狀態。您可以在 EventBridge 中建立規則，`Not ready`以在整備檢查狀態變更為 時收到通知。如需詳細資訊，請參閱在 ARC 中使用整備檢查搭配 Amazon EventBridge。您也可以在 中 AWS 管理主控台或使用 API 操作來檢視整備狀態，例如 `get-recovery-readiness`。如需詳細資訊，請參閱準備檢查 API 操作。

整備檢查的運作方式

ARC 會使用整備檢查來稽核您的應用程式複本，以確保每個複本都有相同的組態設定和相同的執行時間狀態。

例如，若要準備進行復原，您必須隨時維持足夠的備用容量，以吸收來自其他可用區域或區域的容錯移轉流量。ARC 會持續 （一分鐘一次） 檢查您的應用程式，以確保您佈建的容量符合所有可用區域。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 Amazon EBS 磁碟區大小。如果您擴展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，ARC 會偵測到不相符，以便您可以增加待命中的值。

> **Important**
>
> 準備度檢查對於持續驗證應用程式複本組態和執行時間狀態是否一致最有用。準備度檢查不應用於指示您的生產複本是否正常運作，您也不應依賴準備度檢查作為災難事件期間容錯移轉的主要觸發條件。

在主動待命組態中，您應該根據您的監控和運作狀態檢查系統，決定是否要離開或進入儲存格，並將整備檢查視為這些系統的補充服務。ARC 整備檢查並非高度可用，因此您不應依賴中斷期間可存取的檢查。此外，在災難事件期間，也可能無法使用已檢查的資源。

您可以監控特定儲存格 (AWS 區域或可用區域） 中應用程式資源或整體應用程式的整備狀態。您可以在 EventBridge 中建立規則，`Not ready`以在整備檢查狀態變更為 時收到通知。如需詳細資訊，請參閱在 ARC 中使用整備檢查搭配 Amazon EventBridge。您也可以在 中 AWS 管理主控台或使用 API 操作來檢視整備狀態，例如 `get-recovery-readiness`。如需詳細資訊，請參閱準備檢查 API 操作。

整備規則如何判斷整備狀態

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

ARC 整備檢查會根據每個資源類型的預先定義規則以及這些規則的定義方式來決定整備狀態。ARC 會針對其支援的每種資源類型包含一組規則。例如，ARC 具有 Amazon Aurora 叢集、Auto Scaling 群組等的整備規則群組。有些準備規則會將集合中的資源相互比較，有些則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，並建立整備檢查來監控警示的狀態。例如，您可以建立自訂 CloudWatch 警示來監控 Amazon EKS 容器服務，並建立整備檢查來稽核警示的整備狀態。

您可以在建立資源集 AWS 管理主控台 時檢視 中每個資源類型的所有整備規則，也可以稍後導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：ARC 中的準備度規則。

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 `READY`還是`NOT READY`所有資源，還是不同資源的結果會不同。此外，您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 （即 AWS 區域或可用區域，取決於您設定復原群組的方式） 的整備狀態摘要。

每個規則描述中的措辭都會說明如何評估資源，以判斷套用該規則時的整備狀態。定義規則以檢查每個資源，或檢查資源集中的所有資源，以判斷準備程度。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，所有資源都會設定為 READY。
  - 如果某個資源失敗，該資源會設定為 NOT READY，而其他儲存格仍為 READY。

  例如：MskClusterState:檢查每個 Amazon MSK 叢集，以確保其處於 ACTIVE 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，所有資源都會設定為 READY。
  - 如果有任何 不符合條件，所有資源都會設定為 NOT READY。

  例如：VpcSubnetCount:檢查所有VPC子網路，以確保它們具有相同數量的子網路。
- 非關鍵規則：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，整備狀態保持不變。具有此行為的規則在其描述中有備註。

  例如：ElbV2CheckAzCount:檢查每個 Network Load Balancer，以確保它只連接到一個可用區域。
  注意：此規則不會影響整備狀態。

此外，ARC 會針對配額採取額外的步驟。如果整備檢查偵測到任何支援資源之服務配額（資源建立和操作的最大值）的儲存格不相符，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新增額外的容量。

您也可以為整備檢查設定 Amazon EventBridge 通知，例如，當任何整備檢查狀態變更為 時NOT READY。然後，當偵測到組態不相符時，EventBridge 會傳送通知給您，而且您可以採取修正動作，以確保您的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 ARC 中使用整備檢查搭配 Amazon EventBridge]。

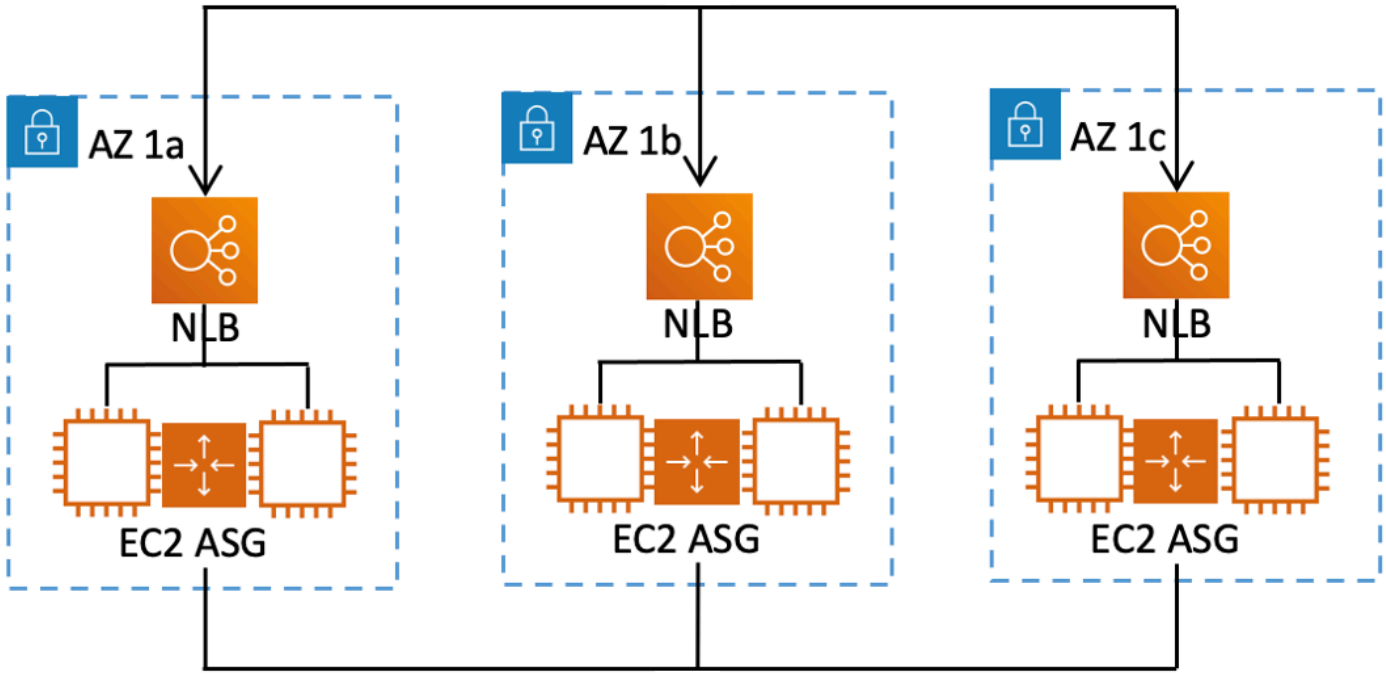
整備檢查、資源集和整備範圍如何一起運作

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 [Amazon Application Recovery Controller (ARC) 整備檢查可用性變更]。

準備度檢查一律會稽核資源集中的資源群組。您可以建立資源集（分開建立整備檢查時或建立整備檢查時），將 ARC 復原群組中儲存格（可用區域或 AWS 區域）中的資源分組，以便定義整備檢查。資源集通常是相同類型資源的群組（例如 Network Load Balancer)，但也可以是 DNS 目標資源，用於架構準備度檢查。

您通常會為應用程式中每種類型的資源建立一個資源集和整備檢查。對於架構準備度檢查，您可以為其建立頂層 DNS 目標資源和全域（復原群組層級）資源集，然後為個別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，每個都具有 Network Load Balancer (NLB) 和 Auto Scaling 群組 (ASG)。



在此案例中，您會為三個 Network Load Balancer 建立資源集和整備檢查，並為三個 Auto Scaling 群組建立資源集和整備檢查。現在，您可以依資源類型，針對復原群組的每組資源進行整備檢查。

透過建立資源的整備範圍，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建立關聯。您可以在建立資源集的整備檢查時執行此操作。

例如，當您為此復原群組的 Network Load Balancer 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。在此情況下，您會將 AZ 1a 的 ARN 與 AZ 1a 中的 NLB 建立關聯、將 的 ARN AZ 1b與 NLB 建立關聯AZ 1b，並將 的 ARN AZ 1c 與 中的 NLB 建立關聯AZ 1c。當您為 Auto Scaling 群組建立整備檢查時，您會執行相同的動作，當您為 Auto Scaling 群組資源集建立整備檢查時，將整備範圍指派給每個群組。

建立整備檢查時，您可以選擇是否關聯整備範圍，但強烈建議您設定它們。整備範圍可讓 ARC 顯示復原群組摘要整NOT READY備檢查和儲存格層級摘要整備檢查的正確READY或整備狀態。除非您設定整備範圍，否則 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 路由政策時，不會為整備範圍選擇復原群組或儲存格。反之，您可以選擇全域資源（無儲存格）。

DNS 目標資源整備檢查：稽核彈性整備

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

透過 ARC 中的 DNS 目標資源準備程度檢查，您可以稽核應用程式的架構和彈性準備程度。這種類型的整備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相依性。

復原導向應用程式具有多個複本，這些複本會孤立到可用區域或 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以正確孤立，ARC 會視需要建議您可以進行的變更，以更新架構，以協助確保其彈性並準備好進行容錯移轉。

ARC 會自動偵測應用程式中儲存格的數量和範圍（代表複本或故障控制單位），以及儲存格是否依可用區域或區域隔離。然後，ARC 會識別並為您提供儲存格中應用程式資源的相關資訊，以判斷它們是否正確孤立至區域或區域。例如，如果您的儲存格範圍限定在特定區域，準備度檢查可以監控負載平衡器及其背後的目標是否也會孤立到這些區域。

透過此資訊，您可以判斷是否需要進行變更，才能將儲存格中的資源對齊正確的區域或區域。

若要開始使用，請為您的應用程式建立 DNS 目標資源，以及資源集和準備度檢查。如需詳細資訊，請參閱在 ARC 中取得架構建議。

準備度檢查和災難復原案例

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

ARC 整備檢查可協助您確保應用程式已擴展以處理容錯移轉流量，藉此深入了解您的應用程式和資源是否已準備好進行復原。準備度檢查狀態不應用作訊號，以指示生產複本運作狀態良好。不過，您可以使用整備檢查作為應用程式和基礎設施監控或運作狀態檢查系統的補充，以判斷要從複本失敗還是失敗。

在緊急情況下或中斷時，使用運作狀態檢查和其他資訊的組合來判斷您的待命已擴展、運作狀態良好，並準備好讓您容錯移轉生產流量。例如，檢查針對待命儲存格執行的 Canary 是否符合您的成功條件，以及驗證待命的準備度檢查狀態是否為 READY。

請注意，ARC 整備檢查託管於單一 AWS 區域、美國西部（奧勒岡），以及在中斷或災難期間，整備檢查資訊可能會過時或檢查可能會無法使用。如需詳細資訊，請參閱用於路由控制的資料和控制平面。

AWS 整備檢查的區域可用性

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

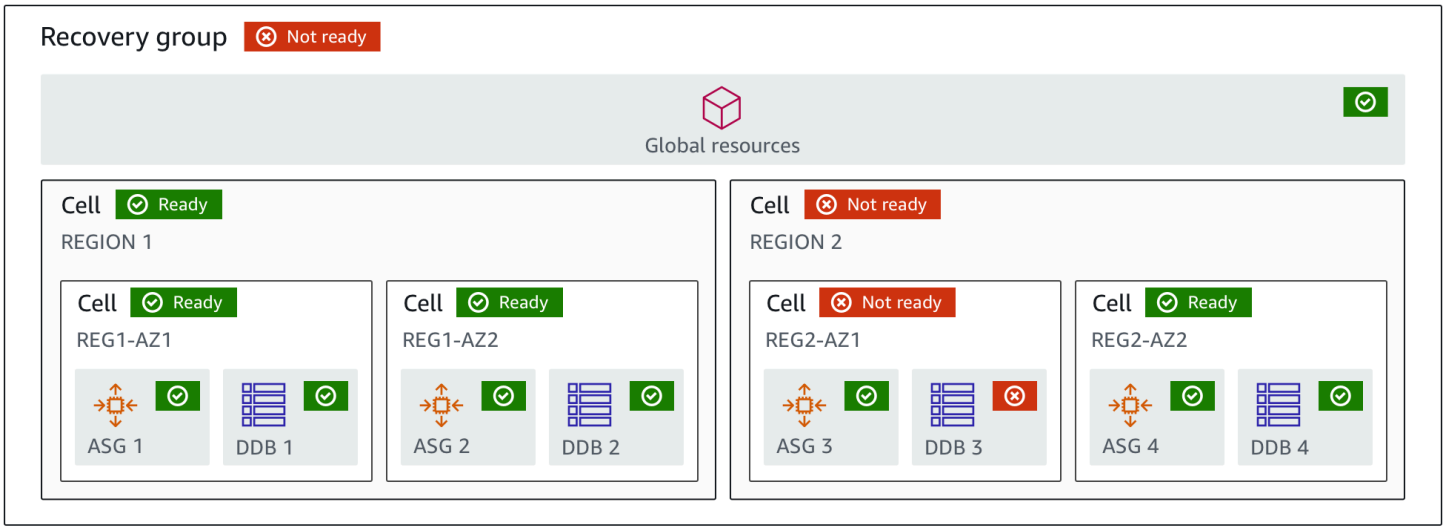
如需 Amazon Application Recovery Controller (ARC) 的區域支援和服務端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Application Recovery Controller (ARC) 端點和配額。

> **Note**
>
> Amazon Application Recovery Controller (ARC) 中的就緒狀態檢查是一項全域功能。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 ARC AWS CLI 命令中指定美國西部（奧勒岡）區域（指定 參數 `--region us-west-2`），例如，當您建立資源集和整備檢查等資源時。

準備度檢查元件

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

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組為復原群組中的儲存格（依 AWS 區域) 和巢狀儲存格（依可用區域）。復原群組（應用程式）的整體整備狀態，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 ARC 中整備檢查功能的元件。

儲存格

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，您可能在主要儲存格中有一組資源，在待命儲存格中有另一組資源。您可以判斷儲存格包含的內容邊界，但儲存格通常代表可用區域或區域。您可以在儲存格內擁有多個儲存格（巢狀儲存格），例如區域內AZs。每個巢狀儲存格代表一個隔離的容錯移轉單位。

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狀態的應用程式或應用程式群組。它由兩個或多個儲存格或複本組成，在功能上彼此相符。例如，如果您有一個 Web 應用程式複寫到 us-east-1a 和 us-east-1b，其中 us-east-1b 是您的容錯移轉環境，您可以在 ARC 中表示此

應用程式為有兩個儲存格的復原群組：一個在 us-east-1a 中，另一個在 us-east-1b 中。復原群組也可以包含全域資源，例如 Route 53 運作狀態檢查。

資源和資源識別符

當您在 ARC 中建立準備度檢查的元件時，您可以使用資源識別符指定資源，例如 Amazon DynamoDB 資料表、Network Load Balancer 或 DNS 目標資源。資源識別符是資源的 Amazon Resource Name (ARN)，或者，對於 DNS 目標資源，ARC 建立資源時產生的識別符。

DNS 目標資源

DNS 目標資源是應用程式網域名稱和其他 DNS 資訊的組合，例如網域指向 AWS 的資源。包含資源是選用的 AWS ，但如果您提供，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 ARC 中為 DNS 目標資源建立資源集，然後為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 路由政策。

資源集

資源集是一組橫跨多個儲存格的資源，包括 AWS 資源或 DNS 目標資源。例如，您可能在 us-east-1a 中有負載平衡器，並在 us-east-1b 中有另一個負載平衡器。若要監控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，然後建立資源集的準備程度檢查。ARC 會持續檢查集合中資源的準備狀態。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建立關聯。

準備度規則

整備規則是 ARC 針對資源集中一組資源執行的稽核。ARC 針對其支援整備檢查的每種資源類型都有一組整備規則。每個規則都包含 ID 和說明 ARC 檢查資源的描述。

準備度檢查

整備檢查會監控應用程式中的資源集，例如一組 Amazon Aurora 執行個體，ARC 正在稽核其復原整備。準備度檢查可能包括稽核，例如容量組態、 AWS 配額或路由政策。例如，如果您想要跨兩個可用區域稽核 Amazon EC2 Auto Scaling 群組的準備程度，您可以為具有兩個資源 ARNs 的資源集建立準備程度檢查，每個 Auto Scaling 群組各一個。然後，為了確保每個群組均等擴展，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涵蓋的資源群組。整備檢查的範圍可以是復原群組 （即全域至整個應用程式） 或儲存格 （即區域或可用區域）。對於做為 ARC 全域資源的資源，請將整備範圍設定為至復原群組或全域資源層級。例如，Route 53 運作狀態檢查是 ARC 中的全域資源，因為它不是特定於區域或可用區域。

準備度檢查的資料和控制平面

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

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依賴的機制具有高度可用性，以便在災難情況下需要它們時使用。一般而言，您應該盡可能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，了解服務的功能如何在控制平面和資料平面之間分割，以及何時可以使用服務的資料平面依賴極端可靠性。

如同大多數 AWS 服務，控制平面和資料平面支援整備檢查功能。雖然這兩者都建置為可靠，但控制平面會針對資料一致性進行最佳化，而資料平面則會針對可用性進行最佳化。資料平面專為彈性而設計，因此即使在破壞性事件期間，當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，控制平面和資料平面都有一個 API，即復原整備 API。整備檢查和整備資源僅位於美國西部（奧勒岡）區域 (us-west-2)。整備檢查控制平面和資料平面可靠，但並非高度可用。

如需有關資料平面、控制平面以及 如何 AWS 建置服務以滿足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白皮書。

在 Amazon Application Recovery Controller (ARC) 中標記準備度檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

標籤是您用來識別和組織 AWS 資源的單字或片語（中繼資料）。您可以為每個資源新增多個標籤，每個標籤都包含您定義的索引鍵和值。例如，金鑰可能是環境，而值可能是生產。您可以根據新增的標籤來搜尋和篩選資源。

您可以在 ARC 中的整備檢查中標記下列資源：

- 資源集
- 準備度檢查

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 Application Recovery Controller (ARC) 的 Recovery Readiness API 參考指南》中的 TagResource。

ARC 中整備檢查的定價

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

您為每個設定的整備檢查支付每小時費用。

如需 ARC 和定價範例的詳細定價資訊，請參閱 ARC 定價。

為您的應用程式設定彈性復原程序

若要將 Amazon Application Recovery Controller (ARC) 與位於多個 AWS 區域中 AWS 的應用程式搭配使用，請遵循準則來設定應用程式以實現彈性，以便您可以有效地支援復原準備。然後，您可以為應用程式建立整備檢查，並設定路由控制來重新路由流量以進行容錯移轉。您也可以檢閱 ARC 提供給 的建議，了解可改善彈性的應用程式架構。

> **Note**
>
> 如果您有由可用區域隔離的應用程式，請考慮使用區域轉移或區域自動轉移進行容錯移轉復原。不需要設定即可使用區域轉移或區域自動轉移，以可靠地從可用區域受損復原應用程式。若要將流量移離負載平衡器資源的可用區域，請在 ARC 主控台或 Elastic Load Balancing 主控台中啟動區域轉移。或者，您可以使用 AWS Command Line Interface 或 AWS SDK 搭配區域轉移 API 動作。如需詳細資訊，請參閱ARC 中的區域轉移。

若要進一步了解彈性容錯移轉組態的入門，請參閱 Amazon Application Recovery Controller (ARC) 中的多區域復原入門。

ARC 中整備檢查的最佳實務

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

我們建議在 Amazon Application Recovery Controller (ARC) 中執行下列整備檢查最佳實務。

新增整備狀態變更的通知

在 Amazon EventBridge 中設定規則，以便在整備檢查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 （適用於您的應用程式）、儲存格 （例如 AWS 區域） 或資源集的整備檢查。

如需詳細資訊，請參閱在 ARC 中使用整備檢查搭配 Amazon EventBridge。

準備檢查 API 操作

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

下表列出可用於復原準備 （準備度檢查） 的 ARC 操作，以及相關文件的連結。

如需如何搭配 使用常見復原準備 API 操作的範例 AWS Command Line Interface，請參閱 搭配 使用 ARC 整備檢查 API 操作的範例 AWS CLI。

Action	使用 ARC 主控台	使用 ARC API
建立儲存格	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 CreateCell
取得儲存格	請參閱 在 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 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 ARC 中建立、更新和刪除復原群組	請參閱 ListCells
建立復原群組	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 CreateRecoveryGroup
取得復原群組	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 GetRecoveryGroup
更新復原群組	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 UpdateRecoveryGroup

Action	使用 ARC 主控台	使用 ARC API
刪除復原群組	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 DeleteRecoveryGroup
列出復原群組	請參閱 在 ARC 中建立、更新和刪除復原群組	請參閱 ListRecoveryGroups
建立資源集	請參閱 在 ARC 中建立和更新整備檢查	請參閱 CreateResourceSet
取得資源集	請參閱 在 ARC 中建立和更新整備檢查	請參閱 GetResourceSet
更新資源集	請參閱 在 ARC 中建立和更新整備檢查	請參閱 UpdateResourceSet
刪除資源集	請參閱 在 ARC 中建立和更新整備檢查	請參閱 DeleteResourceSet
列出資源集	請參閱 在 ARC 中建立和更新整備檢查	請參閱 ListResourceSets
建立整備檢查	請參閱 在 ARC 中建立和更新整備檢查	請參閱 CreateReadinessCheck
取得整備檢查	請參閱 在 ARC 中建立和更新整備檢查	請參閱 GetReadinessCheck
更新整備檢查	請參閱 在 ARC 中建立和更新整備檢查	請參閱 UpdateReadinessCheck
刪除整備檢查	請參閱 在 ARC 中建立和更新整備檢查	請參閱 DeleteReadinessCheck
列出整備檢查	請參閱 在 ARC 中建立和更新整備檢查	請參閱 ListReadinessChecks
列出整備規則	請參閱 ARC 中的就緒規則描述	請參閱 ListRules

Action	使用 ARC 主控台	使用 ARC API
檢查整個整備檢查的狀態	請參閱 在 ARC 中監控整備狀態	請參閱 GetReadinessCheckStatus
檢查資源的狀態	請參閱 在 ARC 中監控整備狀態	請參閱 GetReadinessCheckResourceStatus
檢查儲存格的狀態	請參閱 在 ARC 中監控整備狀態	請參閱 GetCellReadinessSummary
檢查復原群組的狀態	請參閱 在 ARC 中監控整備狀態	請參閱 GetRecoveryGroupReadinessSummary

搭配 使用 ARC 整備檢查 API 操作的範例 AWS CLI

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

本節會逐步解說簡單的應用程式範例，使用 AWS Command Line Interface 來使用 API 操作在 Amazon Application Recovery Controller (ARC) 中使用整備檢查功能。這些範例旨在協助您了解如何使用 CLI 使用整備檢查功能。

對應用程式複本中資源的不相符進行 ARC 稽核中的準備度檢查。若要設定應用程式的整備檢查，您必須在 ARC 儲存格中設定或建模您的應用程式資源，以符合您為應用程式建立的複本。然後，您可以設定準備度檢查來稽核這些複本，以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

讓我們來看一個簡單的案例，其中您有一個名為 的應用程式目前在美國東部 （維吉尼亞北部） 區域 Simple-Service (us-east-1) 執行。您也可以在美國西部 （奧勒岡） 區域 (us-west-2) 取得應用程式的待命副本。在此範例中，我們將設定準備度檢查來比較這兩個版本的應用程式。這可讓我們確保待命美國西部 （奧勒岡） 區域準備好在容錯移轉案例中需要 時接收流量。

如需使用 的詳細資訊 AWS CLI，請參閱 AWS CLI 命令參考。如需整備 API 動作和詳細資訊連結的清單，請參閱 準備檢查 API 操作。

ARC 中的儲存格代表故障界限（例如可用區域或區域），並收集到復原群組中。復原群組代表您要檢查容錯移轉準備狀態的應用程式。如需整備檢查元件的詳細資訊，請參閱 準備度檢查元件。

> **Note**
>
> ARC 是一種全域服務，支援多個端點， AWS 區域 但您必須在大多數 ARC CLI 命令中指定美國西部（奧勒岡）區域（即指定 參數 `--region us-west-2`)。例如，建立資源，例如復原群組或整備檢查。

在我們的應用程式範例中，我們將從為每個擁有資源的區域建立一個儲存格開始。然後，我們將建立復原群組，然後完成準備度檢查的設定。

1. 建立儲存格

1a. 建立 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 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。您可以呼叫 `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 ARC 中復原準備的最上層資源。復原群組代表應用程式整體。在此步驟中，我們將建立復原群組來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. （選用）您可以呼叫 `list-recovery-groups` API 來驗證您的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": {}
        }
    ]
}
```

現在我們的應用程式已有模型，讓我們新增要監控的資源。在 ARC 中，您要監控的一組資源稱為資源集。資源集包含所有相同類型的資源。我們將資源集中的資源相互比較，以協助判斷儲存格的容錯移轉準備程度。

3. 建立資源集

假設我們的Simple-Service應用程式確實非常簡單，且僅使用 DynamoDB 資料表。它在 us-east-1 中有 DynamoDB 資料表，在 us-west-2 中有另一個資料表。資源集也包含整備範圍，可識別每個資源包含在其中的儲存格。

3a. 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.（選用）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 帳戶的所有資源集。在這裡，您可以看到我們只有上面建立的一個資源集。

```
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，我們已建立儲存格、復原群組和資源集，以在 ARC 中建立Simple-Service應用程式模型。接下來，我們將設定準備程度檢查，以監控資源是否準備好容錯移轉。

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。規則專屬於每個資源類型。也就是說，AWS::DynamoDB::Table、 AWS::EC2::Instance等有不同的規則。規則會檢查資源的各種維度，包括組態、容量 （如果可用且適用）、限制 （如果可用且適用） 和路由組態。

> **Note**
>
> 若要查看套用至整備檢查中資源的規則，您可以使用 get-readiness-check-resource-status API，如步驟 5 所述。若要查看 ARC 中所有整備規則的清單，請使用 list-rules或參閱 ARC 中的就緒規則描述。ARC 有一組特定的規則，其會針對每個資源類型執行；目前這些規則無法自訂。

4a. 建立資源集的整備檢查 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. （選用） 若要驗證是否已成功建立整備檢查，請執行 list-readiness-checks API。此 API 會顯示 帳戶中的所有準備度檢查。

```
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. 監控準備度檢查

現在我們已將應用程式建模並新增準備度檢查，我們已準備好監控資源。您可以在四個層級建立應用程式的準備度模型：準備度檢查層級（一組資源）、個別資源層級、儲存格層級（可用區域或區域中的所有資源），以及復原群組層級（應用程式整體）。以下提供取得每種準備狀態的命令。

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. 請參閱儲存格的整體準備程度。

```
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，在復原群組層級查看應用程式的頂層整備。

```
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"
        }
    ]
}
```

使用復原群組和準備度檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

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 ARC 中建立、更新和刪除復原群組

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

復原群組代表您在 Amazon Application Recovery Controller (ARC) 中的應用程式。它通常由兩個或多個儲存格組成，這些儲存格在資源和功能方面是彼此的複本，因此您可以從一個儲存格容錯移轉到另一個儲存格。每個儲存格都包含一個 AWS 區域或可用區域的作用中資源的 Amazon Resource Name

ARNs)。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作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。ARC 中的準備度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運作狀態檢查系統，決定是否要離開或離開複本，並將整備檢查視為這些系統的補充服務。

準備度會檢查稽核資源，以根據該資源類型的一組預先定義規則來判斷其準備程度。使用複本建立復原群組後，您可以為應用程式中的資源新增 ARC 整備檢查，以便 ARC 協助確保複本在一段時間內具有相同的設定和組態。

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 ARC 主控台上建立復原群組。若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用復原準備 API 操作，請參閱 準備檢查 API 操作。

建立復原群組

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。
3. 在復原準備頁面上，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，然後新增第二個儲存格的名稱。例如，如果您在美國東部 （俄亥俄） 有複本，您可以新增名為 的儲存格 `MyApp-us-east-2`。
8. 如果您想要新增巢狀儲存格 （區域中可用區域中的複本），請選擇動作，選擇新增巢狀儲存格，然後輸入名稱。
9. 當您為應用程式複本新增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，以及刪除 ARC 主控台上的儲存格。若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用復原準備 API 操作，請參閱 準備檢查 API 操作。

若要更新或刪除復原群組，或刪除儲存格

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。
3. 在復原準備頁面上，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 ARC 中建立和更新整備檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

本節提供整備檢查和資源集的程序，包括建立、更新和刪除這些資源。

建立和更新整備檢查

本節中的步驟說明如何在 ARC 主控台上建立整備檢查。若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用復原準備 API 操作，請參閱 準備檢查 API 操作。

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。

建立整備檢查

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。

3. 在就緒頁面上，選擇建立，然後選擇就緒檢查。
4. 輸入整備檢查的名稱，選擇您要檢查的資源類型，然後選擇下一步。
5. 為您的整備檢查新增資源集。資源集是不同複本中相同類型的一組資源。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檢查。
   - 建立新的資源集。

   如果您選擇建立新的資源集，請輸入其名稱，然後選擇新增。
6. 針對您要包含在集合中的每個資源逐一複製並貼上 Amazon Resource Name (ARNs)，然後選擇下一步。

   > **Tip**
   >
   > 如需 ARC 預期每個資源類型的 ARN 格式範例和詳細資訊，請參閱 ARC 中的資源類型和 ARN 格式。
7. 如果您願意，請檢視 ARC 檢查您在此整備檢查中包含的資源類型時將使用的整備規則。然後選擇下一步。
8. （選用）在復原群組名稱下，選擇要與整備檢查建立關聯的復原群組，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）。如果是應用程式層級資源，例如 DNS 路由政策，請選擇全域資源（無儲存格）。

   這會指定整備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，以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，且未在此處選擇整備範圍，將整備檢查與復原群組的資源建立關聯，ARC 就無法傳回復原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。

刪除整備檢查

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

2. 選擇準備度檢查。
3. 選擇整備檢查，然後在動作下，選擇刪除。

建立和編輯資源集

一般而言，您會建立資源集作為建立整備檢查的一部分，但您也可以另外建立資源集。您也可以編輯資源集來新增或移除資源。本節中的步驟說明如何在 ARC 主控台上建立或編輯資源集。若要了解如何搭配 Amazon Application Recovery Controller (ARC) 使用復原準備 API 操作，請參閱 準備檢查 API 操作。

建立資源集

1. 在 https：// 開啟 Route 53 主控台。 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，然後選擇要包含在集合中的資源類型。
5. 選擇新增，然後輸入要新增至集之資源的 Amazon Resource Name (ARN)。
6. 新增資源完成後，請選擇建立資源集。

編輯資源集

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。
3. 在資源集下，選擇動作，然後選擇編輯。
4. 執行以下任意一項：
   - 若要從集合中移除資源，請選擇移除。
   - 若要將資源新增至集，請選擇新增，然後輸入資源的 Amazon Resource Name (ARN)。
5. 您也可以編輯資源的整備範圍，將資源與不同的儲存格建立關聯，以進行整備檢查。
6. 選擇儲存。

在 ARC 中監控整備狀態

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

您可以在下列層級的 Amazon Application Recovery Controller (ARC) 中查看應用程式的準備程度：

- 資源集中資源的準備程度檢查
- 個別資源層級
- 可用區域或 AWS 區域中所有資源的儲存格 （ 應用程式複本 ） 層級
- 應用程式整體的復原群組層級

您可以收到整備狀態變更的通知，也可以在 Route 53 主控台中或使用 ARC CLI 命令來監控整備狀態變更。

就緒狀態通知

您可以使用 Amazon EventBridge 設定事件驅動規則來監控 ARC 資源，並通知您整備狀態的變更。如需詳細資訊，請參閱在 ARC 中使用整備檢查搭配 Amazon EventBridge。

在 ARC 主控台中監控整備狀態

下列程序說明如何在 中監控復原準備程度 AWS 管理主控台。

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。
3. 在就緒頁面的復原群組下，檢視每個復原群組 （ 應用程式 ） 的復原群組就緒狀態。

   您也可以檢視特定儲存格或個別資源的準備程度。

使用 CLI 命令監控整備狀態

本節提供 AWS CLI 命令範例，可用來查看不同層級的應用程式和資源的準備狀態。

資源集的準備度

您已為資源集（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
```

單一資源的準備度

若要取得整備檢查中單一資源的狀態，包括每個已檢查整備規則的狀態，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"
```

儲存格的準備度

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
```

應用程式準備度

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 ARC 中取得架構建議

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

如果您有現有的應用程式，Amazon Application Recovery Controller (ARC) 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 ARC 中建立代表您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。

如果您尚未指定 DNS 目標資源，建議您為復原群組指定目標資源，以便我們提供更詳細的建議。當您提供其他資訊時，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，ARC 可以提供有關您是否已建立復原群組最佳數量儲存格的資訊。

對於 DNS 目標資源，請注意下列事項：

- 僅指定目標資源的 Route 53 資源記錄或 Network Load Balancer。
- 每個復原群組只能建立一個 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 目標資源分組為一個資源集。

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 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。
3. 在復原群組名稱下，選擇代表您應用程式的復原群組。
4. 在復原群組詳細資訊頁面上的動作功能表上，選擇取得此復原群組的架構建議。
5. 如果您尚未建立 DNS 目標資源整備檢查，請建立一個，讓 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 準備度檢查元件。
6. 若要建立 DNS 目標資源的資源集，您可以建立整備檢查。輸入整備檢查的名稱，然後在整備檢查類型中選擇 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 ID。

> **Tip**
>
> 若要查看託管區域 ARN 的格式，請參閱 中託管區域的 ARN 格式ARC 中的資源類型和 ARN 格式。

或者，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. （選用）在復原群組組態中，為您的 DNS 目標資源選擇儲存格，以設定整備範圍。
10. 選擇建立資源集。
11. 在復原群組詳細資訊頁面上，選擇取得架構建議。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變更，以改善應用程式的復原彈性。

在 ARC 中建立跨帳戶授權

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

您可能將資源分散到多個 AWS 帳戶，這可能會讓您難以全面檢視應用程式的運作狀態。也可能導致難以取得快速決策所需的資訊。為了協助簡化 Amazon Application Recovery Controller (ARC) 中的準備度檢查，您可以使用跨帳戶授權。

ARC 中的跨帳戶授權可與整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 帳戶中的資源。在具有您要監控之資源的每個帳戶中，您授權中央帳戶存取這些資源。然後，中央帳戶可以為所有帳戶中的資源建立整備檢查，並從中央帳戶監控容錯移轉的整備情況。

> **Note**
>
> 主控台中無法使用跨帳戶授權設定。反之，請使用 ARC API 操作來設定和使用跨帳戶授權。為了協助您開始使用，本節提供 AWS CLI 命令範例。

假設應用程式有一個帳戶，其在美國西部（奧勒岡）區域 (us-west-2) 擁有資源，還有一個帳戶，其具有您要在美國東部（維吉尼亞北部）區域 (us-east-1) 中監控的資源。ARC 可讓您使用跨帳戶授權，從一個帳戶 us-west-2 監控兩組資源。

例如，假設您有下列 AWS 帳戶：

- 美國西部帳戶：999999999999
- 美國東部帳戶：111111111111

在 us-east-1 帳戶 (111111111111) 中，我們可以透過在 us-west-2 IAM 帳戶中指定 （ 根 ） 使用者的 Amazon Resource Name (ARN)，啟用跨帳戶授權以允許 us-west-2 帳戶 (999999999999) 存取：`arn:aws:iam::999999999999:root`。建立授權後，us-west-2 帳戶可以將 us-east-1 擁有的資源新增至資源集，並建立準備度檢查以在資源集上執行。

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 ARC 中新增和監控之 AWS 資源的其他帳戶中啟用跨帳戶授權。

> **Note**
>
> ARC 是一種全域服務，支援多個區域中 AWS 的端點，但您必須在大多數 ARC CLI 命令中指定美國西部 （ 奧勒岡 ） 區域 （ 即指定 參數 `--region us-west-2`)。

下列 AWS CLI 命令顯示如何設定此範例的跨帳戶授權：

```
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
```

若要為您已提供跨帳戶授權的所有帳戶檢查特定帳戶，請使用 `list-cross-account-authorizations`命令。請注意，目前您無法檢查其他方向。也就是說，沒有 API 操作可與帳戶設定檔搭配使用，以列出已授予其跨帳戶新增和監控資源授權的所有帳戶。

```
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"
    ]
}
```

就緒規則、資源類型和 ARNS

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

本節包含整備規則描述的參考資訊，以及支援的資源類型，以及您用於資源集的 Amazon Resource Name (ARNs) 格式。

ARC 中的就緒規則描述

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

本節列出 Amazon Application Recovery Controller (ARC) 支援的所有資源類型的整備規則描述。若要查看 ARC 支援的資源類型清單，請參閱 ARC 中的資源類型和 ARN 格式。

您也可以在 ARC 主控台或使用 API 操作檢視整備規則描述，方法如下：

- 若要在主控台中檢視整備規則，請遵循下列步驟：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 操作。

主題

- ARC 中的準備度規則
- 在主控台上檢視整備規則

ARC 中的準備度規則

本節列出 ARC 支援的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所有或檢查每個項目的術語。若要了解這些術語如何解釋規則在整備檢查中的運作方式，以及 ARC 如何設定整備狀態的其他詳細資訊，請參閱整備規則如何決定整備狀態。

準備度規則

ARC 使用以下整備規則來稽核資源。

Amazon API Gateway 第 1 版階段

- ApiGwV1ApiKeyCount：檢查所有 API Gateway 階段，以確保它們具有與其連結的相同數量 API 金鑰。
- ApiGwV1ApiKeySource：檢查所有 API Gateway 階段，以確保它們具有相同的 值`API Key Source`。
- ApiGwV1BasePath：檢查所有 API Gateway 階段，以確保它們連結到相同的基本路徑。
- 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 都已啟用或沒有`Cache Cluster`啟用。
- ApiGwV1CacheClusterSize：檢查所有 API Gateway 階段，以確保它們具有相同的 `Cache Cluster Size`。如果某個值較大，則其他值會標記為「未就緒」。
- ApiGwV1CacheClusterStatus：檢查所有 API Gateway 階段，以確保 `Cache Cluster` 處於可用狀態。
- ApiGwV1DisableExecuteApiEndpoint：檢查所有 API Gateway 階段，以確保所有 都`Execute API Endpoint`已停用，或沒有。
- ApiGwV1DomainName：檢查所有 API Gateway 階段，以確保它們連結到相同的網域名稱。
- 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，以確保其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 值`Method Settings`。
- ApiGwV1MutualTlsAuthentication：檢查所有 API Gateway 階段，以確保它們具有相同的值`Mutual TLS Authentication`。
- ApiGwV1Policy：檢查所有 API Gateway 階段，以確保所有階段都使用 API 層級政策，或無。
- 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。注意：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，包括相關的組態。
- ApiGwV1SecurityPolicy：檢查所有 API Gateway 階段，以確保它們具有相同的 值`Security Policy`。
- ApiGwV1Quotas：檢查所有 API Gateway 群組，以確保符合 Service Quotas 管理的配額 （限制）。
- ApiGwV1UsagePlans：檢查所有 API Gateway 階段，以確保它們`Usage Plans`以相同的組態連結到 。

Amazon API Gateway 第 2 版階段

- ApiGwV2ApiKeySelectionExpression：檢查所有 API Gateway 階段，確保它們具有相同的值`API Key Selection Expression`。
- ApiGwV2ApiMappingSelectionExpression：檢查所有 API Gateway 階段，以確保它們具有相同的 值`API Mapping Selection Expression`。
- 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，以確保它們連結到相同的網域名稱。
- 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 值`Endpoint Type`。
- ApiGwV2Quotas：檢查所有 API Gateway 群組，以確保符合 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值`Mutual TLS Authentication`。
- ApiGwV2ProtocolType：檢查所有 API Gateway 階段，以確保它們具有相同的 值`Protocol Type`。

- ApiGwV2RouteConfigs：檢查所有 API Gateway 階段，以確保它們具有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值`Route Selection Expression`。
- ApiGwV2RouteSettings：檢查所有 API Gateway 階段，以確保它們具有相同的 值`Default Route Settings`。
- ApiGwV2SecurityPolicy：檢查所有 API Gateway 階段，以確保它們具有相同的 值`Security Policy`。
- 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值`Throttling Burst Limit`。
- ApiGwV2ThrottlingRateLimit：檢查所有 API Gateway 階段，以確保它們具有相同的值`Throttling Rate Limit`。

Amazon Aurora 叢集

- 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，以確保其具有相同的 值`Engine Mode`。
- RdsEngineVersion：檢查所有 Aurora 叢集，以確保其具有相同的 值`Major Version`。
- RdsGlobalReplicaLag：檢查每個 Aurora 叢集，以確保其具有少於 30 秒`Global Replica Lag`的 。
- RdsNormalizedCapacity：檢查所有 Aurora 叢集，以確保其具有資源集中最大值 15% 內的標準化容量。
- 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，以確保其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，以確保其具有相同的執行個體類型。注意：此規則不會影響整備狀態。
- AsgInstanceSizes：檢查所有 Auto Scaling 群組，以確保其具有相同的執行個體大小。

- AsgNormalizedCapacity：檢查所有 Auto Scaling 群組，以確保其具有資源集中最大值 15% 內的標準化容量。
- AsgQuotas：檢查所有 Auto Scaling 群組，以確保符合 Service Quotas 管理的配額 （限制）。

CloudWatch 警示

- CloudWatchAlarmState：檢查 CloudWatch 警示，以確保每個警示都未處於 ALARM或 INSUFFICIENT_DATA 狀態。

客戶閘道

- CustomerGatewayIpAddress：檢查所有客戶閘道，以確保它們具有相同的 IP 地址。
- CustomerGatewayState：檢查客戶閘道，以確保每個閘道都處於 AVAILABLE 狀態。
- 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，並且每個託管區域不是私有的。注意：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)，且 TTLs小於或等於 300。
- DnsTargetResourceRoutingRule：檢查與別名資源記錄集相關聯的每個 DNS 目標資源，以確保其將流量路由到目標資源上設定的 DNS 名稱。注意：此規則不會影響整備狀態。
- DnsTargetResourceHealthCheckRule：檢查所有 DNS 目標資源，以確保運作狀態檢查在適當時與其資源紀錄集相關聯，否則不會關聯。注意：此規則不會影響整備狀態。

Amazon DynamoDB 資料表

- DynamoConfiguration：檢查所有 DynamoDB 資料表，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 資料表，以確保其狀態為 ACTIVE。
- DynamoCapacity：檢查所有 DynamoDB 資料表，以確保其佈建的讀取容量和寫入容量在資源集中容量上限的 20% 內。
- DynamoPeakRcuWcu：檢查每個 DynamoDB 資料表，確保其具有與其他資料表類似的尖峰流量，以確保佈建的容量。
- DynamoGsiPeakRcuWcu：檢查每個 DynamoDB 資料表，確保其具有與其他資料表類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 資料表，以確保資料表使用相同的索引、索引鍵結構描述和投影。

- DynamoGsiStatus：檢查具有全域次要索引的所有 DynamoDB 資料表，以確保全域次要索引具有 ACTIVE 狀態。
- DynamoGsiCapacity：檢查具有全域次要索引的所有 DynamoDB 資料表，以確保資料表已佈建資源集中最大容量的 20% 內的 GSI 讀取容量和 GSI 寫入容量。
- DynamoReplicationLatency：檢查所有屬於全域資料表的 DynamoDB 資料表，以確保它們具有相同的複寫延遲。
- DynamoAutoScalingConfiguration：檢查已啟用 Auto Scaling 的所有 DynamoDB 資料表，以確保它們具有相同的最小、最大和目標讀取和寫入容量。
- DynamoQuotas：檢查所有 DynamoDB 資料表，以確保它們符合 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，以確保它只連接到一個可用區域。注意：此規則不會影響整備狀態。
- ElbV1AnyInstances：檢查所有 Classic Load Balancer，以確保它們至少有一個 EC2 執行個體。
- ElbV1AnyInstancesHealthy：檢查所有 Classic Load Balancer，以確保它們至少有一個運作狀態良好的 EC2 執行個體。
- ElbV1Scheme：檢查所有 Classic Load Balancer，以確保它們具有相同的負載平衡器方案。
- ElbV1HealthCheckThreshold：檢查所有 Classic Load Balancer，以確保它們具有相同的運作狀態檢查閾值。
- ElbV1HealthCheckInterval：檢查所有 Classic Load Balancer，以確保它們具有相同的運作狀態檢查間隔值。
- ElbV1CrossZoneRoutingEnabled：檢查所有 Classic Load Balancer，以確保它們具有相同的跨區域負載平衡值 (ENABLED 或 DISABLED)。
- ElbV1AccessLogsEnabledAttribute：檢查所有 Classic Load Balancer，以確保它們具有相同的存取日誌值 (ENABLED 或 DISABLED)。
- ElbV1ConnectionDrainingEnabledAttribute：檢查所有 Classic Load Balancer，以確保它們具有相同的連接耗盡值 (ENABLED 或 DISABLED)。
- ElbV1ConnectionDrainingTimeoutAttribute：檢查所有 Classic Load Balancer，以確保它們具有相同的連線耗盡逾時值。
- ElbV1IdleTimeoutAttribute：檢查所有 Classic Load Balancer，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 Classic Load Balancer，以確保它們位於資源集中佈建最高 LCU 的 20% 內。

- ElbV1ProvisionedCapacityStatus：檢查每個 Classic Load Balancer 上的佈建容量狀態，以確保其沒有 DISABLED 或 PENDING 的值。

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 (ENABLED 或 DISABLED)。
- EbsVolumeEncryptionDefault：檢查所有EBS磁碟區，以確保其預設具有相同的加密值 (ENABLED 或 DISABLED)。
- 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磁碟區，以確保它們具有相同的預設 AWS KMS 金鑰 ID。
- EbsVolumeMultiAttach：檢查所有EBS磁碟區，以確保多連接 (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磁碟區，以確保它們具有相同的可讀取大小。
- 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。如果其中一個記憶體較多，則其他記憶體會標示為 `NOT READY`。
- LambdaFunctionTimeout：檢查所有 Lambda 函數，以確保它們具有相同的逾時值。如果某個值較大，則其他值會標記為 `NOT READY`。
- LambdaFunctionRuntime：檢查所有 Lambda 函數，以確保它們都有相同的執行時間。
- LambdaFunctionReservedConcurrentExecutions：檢查所有 Lambda 函數，以確保它們都具有相同的 值`Reserved Concurrent Executions`。如果某個值較大，則其他值會標記為 `NOT READY`。
- LambdaFunctionDeadLetterConfig：檢查所有 Lambda 函數，以確保它們都具有已`Dead Letter Config`定義的函數，或沒有任何函數。
- LambdaFunctionProvisionedConcurrencyConfig：檢查所有 Lambda 函數，以確保它們具有相同的 值`Provisioned Concurrency`。
- LambdaFunctionSecurityGroupCount：檢查所有 Lambda 函數，以確保它們具有相同的值`Security Groups`。

- LambdaFunctionSubnetIdCount：檢查所有 Lambda 函數，以確保它們具有相同的 值`Subnet Ids`。
- 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）。

Network Load Balancer 和 Application Load Balancer

- ElbV2CheckAzCount：檢查每個 Network Load Balancer，以確保它只連接到一個可用區域。注意：此規則不會影響整備狀態。
- ElbV2TargetGroupsCanServeTraffic：檢查每個 Network Load Balancer 和 Application Load Balancer，以確保其至少有一個運作狀態良好的 Amazon EC2 執行個體。
- ElbV2State：檢查每個 Network Load Balancer 和 Application Load Balancer，以確保其處於 `ACTIVE` 狀態。
- ElbV2IpAddressType：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的 IP 地址類型。
- ElbV2Scheme：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的結構描述。
- ElbV2Type：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的類型。
- ElbV2S3LogsEnabled：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的 Amazon S3 伺服器存取日誌值 (ENABLED 或 DISABLED)。
- ElbV2DeletionProtection：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的刪除保護值 (ENABLED 或 DISABLED)。
- ElbV2IdleTimeoutSeconds：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們在閒置時間秒內具有相同的值。
- ElbV2HttpDropInvalidHeaders：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保其具有相同的 HTTP 捨棄無效標頭值。
- ElbV2Http2Enabled：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保其具有相同的 HTTP2 值 (ENABLED 或 DISABLED)。
- ElbV2CrossZoneEnabled：檢查所有 Network Load Balancer 和 Application Load Balancer，以確保它們具有相同的跨區域負載平衡值 (ENABLED 或 DISABLED)。
- ElbV2ProvisionedCapacityLcuCount：檢查佈建 LCU 大於 10 的所有 Network Load Balancer 和 Application Load Balancer，以確保它們位於資源集中佈建最高 LCU 的 20% 內。

- ElbV2ProvisionedCapacityEnabled：檢查所有 Network Load Balancer 和 Application Load Balancer 佈建的容量狀態，以確保其沒有 DISABLED 或 PENDING 的值。

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。如果某個值較大，則其他值會標記為「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 ARNs 清單。
- MskClusterServerProperties：檢查所有 MSK 叢集，以確保其具有相同的 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，以確保其具有相同的值`Encryption In Transit In Cluster`。
- MskClusterEncryptionInClientBroker：檢查所有 MSK 叢集，以確保其具有相同的值`Encryption In Transit Client Broker`。
- MskClusterEnhancedMonitoring：檢查所有 MSK 叢集，以確保其具有相同的 值`Enhanced Monitoring`。
- MskClusterOpenMonitoringInJmx：檢查所有 MSK 叢集，以確保其具有相同的 值`Open Monitoring JMX Exporter`。
- MskClusterOpenMonitoringInNode：檢查所有 MSK 叢集，以確保其具有相同的 值 `Open Monitoring Not Exporter.`
- MskClusterLoggingInS3：檢查所有 MSK 叢集，以確保其具有相同的 值`Is Logging in S3`。
- MskClusterLoggingInFirehose：檢查所有 MSK 叢集，以確保其具有相同的 值`Is Logging In Firehose`。
- MskClusterLoggingInCloudWatch：檢查所有 MSK 叢集，以確保其具有相同的 值`Is Logging Available In CloudWatch Logs`。
- MskClusterNumberOfBrokerNodes：檢查所有 MSK 叢集，以確保其具有相同的 值`Number of Broker Nodes`。如果某個值較大，則其他值會標記為「未就緒」。
- MskClusterState：檢查每個 MSK 叢集，以確保其處於 ACTIVE 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 Route 53 運作狀態檢查

- R53HealthCheckType：檢查每個 Route 53 運作狀態檢查，以確保其不屬於 CALCULATED 類型，且所有檢查都屬於相同類型。
- R53HealthCheckDisabled：檢查每個 Route 53 運作狀態檢查，以確保它沒有 DISABLED 狀態。
- R53HealthCheckStatus：檢查每個 Route 53 運作狀態檢查，以確保其具有成功狀態。
- R53HealthCheckRequestInterval：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的值`Request Interval`。
- R53HealthCheckFailureThreshold：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的 值 `Failure Threshold.`
- R53HealthCheckEnableSNI：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的 值 `Enable SNI.`
- R53HealthCheckSearchString：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的 值 `Search String.`
- R53HealthCheckRegions：檢查所有 Route 53 運作狀態檢查，以確保它們都有相同的 AWS 區域清單。
- R53HealthCheckMeasureLatency：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的 值`Measure Latency`。
- R53HealthCheckInsufficientDataHealthStatus：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的 值`Insufficient Data Health Status`。
- R53HealthCheckInverted：檢查所有 Route 53 運作狀態檢查，以確保它們全部反轉，或全部未反轉。
- R53HealthCheckResourcePath：檢查所有 Route 53 運作狀態檢查，以確保它們都具有相同的值`Resource Path`。
- R53HealthCheckCloudWatchAlarm：檢查所有 Route 53 運作狀態檢查，以確保與其相關聯的 CloudWatch 警示具有相同的設定和組態。

Amazon SNS 訂閱

- SnsSubscriptionProtocol：檢查所有 SNS 訂閱，以確保其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：檢查所有具有非AWS 服務端點類型的 SNS 訂閱，例如電子郵件，以確保訂閱具有相同的端點。
- SnsSubscriptionPendingConfirmation：檢查所有 SNS 訂閱，以確保它們具有相同的 '待定確認' 值。
- SnsSubscriptionDeliveryPolicy：檢查所有使用 HTTP/S 的 SNS 訂閱，以確保它們具有相同的 'Effective Delivery Period' 值。
- SnsSubscriptionRawMessageDelivery：檢查所有 SNS 訂閱，以確保它們具有相同的 'Raw Message Delivery' 值。
- SnsSubscriptionFilter：檢查所有 SNS 訂閱，以確保它們具有相同的 'Filter Policy' 值。
- SnsSubscriptionRedrivePolicy：檢查所有 SNS 訂閱，以確保它們具有相同的 'Redrive Policy' 值。
- SnsSubscriptionEndpointEnabled：檢查所有 SNS 訂閱，以確保它們具有相同的 'Endpoint Enabled' 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：檢查所有使用 SQS 端點的 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，以確保其具有相同的 值`Display Name`。
- SnsTopicDeliveryPolicy：檢查具有 HTTPS 訂閱者的所有 SNS 主題，以確保它們具有相同的 `EffectiveDeliveryPolicy`。
- SnsTopicSubscription：檢查所有 SNS 主題，以確保其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都有 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，以確保它們都是 的相同值`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 VPCs

- VpcCidrBlock：檢查所有 VPCs，以確保它們都具有相同的 CIDR 區塊網路大小值。
- VpcCidrBlocksSameProtocolVersion：檢查具有相同 CIDR 區塊的所有 VPCs，以確保其具有相同的網際網路串流通訊協定版本編號值。
- VpcCidrBlocksStateInAssociationSets：檢查所有 VPCs 的所有 CIDR 區塊關聯集，以確保它們都有處於 `ASSOCIATED` 狀態的 CIDR 區塊。
- VpcIpv6CidrBlocksStateInAssociationSets：檢查所有 VPCs 的所有 CIDR 區塊關聯集，以確保它們都有具有相同數量地址的 CIDR 區塊。
- VpcCidrBlocksInAssociationSets：檢查所有 VPCs 的所有 CIDR 區塊關聯集，以確保它們的大小相同。
- VpcIpv6CidrBlocksInAssociationSets：檢查所有 VPCs 的所有 IPv6 CIDR 區塊關聯集，以確保它們的大小相同。
- VpcState：檢查每個 VPC 以確保其處於 `AVAILABLE` 狀態。
- VpcInstanceTenancy：檢查所有 VPCs，以確保它們都具有相同的 值`Instance Tenancy`。
- VpcIsDefault：檢查所有 VPCs，以確保其具有相同的 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，以確保其可用的 IP 地址計數大於零。
- 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，以確保它們符合 Service Quotas 管理的配額（限制）。

Site-to-Site VPN 連線

- VpnConnectionsRouteCount：檢查所有 VPN 連線，以確保它們至少有一個路由，以及相同的路由數量。
- VpnConnectionsEnableAcceleration：檢查所有 VPN 連線，以確保其具有相同的 值`Enable Accelerations`。
- VpnConnectionsStaticRoutesOnly：檢查所有 VPN 連線，以確保其具有相同的 值 `Static Routes Only.`
- VpnConnectionsCategory：檢查所有 VPN 連線，以確保它們的類別為 VPN。
- VpnConnectionsCustomerConfiguration：檢查所有 VPN 連線，以確保其具有相同的值`Customer Gateway Configuration`。
- VpnConnectionsCustomerGatewayId：檢查每個 VPN 連線，以確保其已連接客戶閘道。
- VpnConnectionsRoutesState：檢查所有 VPN 連線，以確保它們處於 `AVAILABLE` 狀態。
- VpnConnectionsVgwTelemetryStatus：檢查每個 VPN 連線，以確保其 VGW 狀態為 UP。
- VpnConnectionsVgwTelemetryIpAddress：檢查每個 VPN 連接，以確保每個 VGW 遙測都有不同的外部 IP 地址。
- VpnConnectionsTunnelOptions：檢查所有 VPN 連線，以確保它們具有相同的通道選項。
- VpnConnectionsRoutesCidr：檢查所有 VPN 連線，以確保它們具有相同的目的地 CIDR 區塊。
- VpnConnectionsInstanceType：檢查所有 VPN 連線，以確保它們具有相同的 `Instance Type`。

Site-to-Site VPN 閘道

- VpnGatewayState：檢查所有 VPN 閘道，以確保其處於可用狀態。
- 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，以確保其具有相同的連接組態。

在主控台上檢視整備規則

您可以在 上檢視整備規則 AWS 管理主控台，依每個資源類型列出。

在主控台上檢視整備規則

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 選擇準備度檢查。

3. 在資源類型下，選擇您要檢視規則的資源類型。

ARC 中的資源類型和 ARN 格式

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

當您在 Amazon Application Recovery Controller (ARC) 中建立資源集時，您可以為要包含的每個資源指定要包含在集合中的資源類型，以及 Amazon Resource Name (ARNs)。ARC 預期每個資源類型都有特定的 ARN 格式。本節列出 ARC 支援的資源類型，以及每個類型相關的 ARN 格式。

特定格式取決於 資源。當您提供 ARN 時，請將*##*文字取代為您的資源特定資訊。

> **Note**
>
> 請注意，ARC 對資源所需的 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所述的 ARN 格式，可能不會包含 ARC 支援 ARC 服務中的功能所需的 AWS 帳戶 ID 或其他資訊。

AWS::ApiGateway::Stage

Amazon API Gateway 第 1 版階段。

- 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 Resource Name (ARN) 參考。

AWS::ApiGatewayV2::Stage

Amazon API Gateway 第 2 版階段。

- 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 Resource Name (ARN) 參考。

AWS::CloudWatch::Alarm

Amazon CloudWatch 警示。

- 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 CloudWatch 定義的資源類型。

AWS::DynamoDB::Table

Amazon DynamoDB 資料表。

- 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 資源和操作。

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 磁碟區。

- 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 Resource Name (ARN) 參考。

AWS::ElasticLoadBalancing::LoadBalancer

Classic Load Balancer。

- ARN 格式：
  `arn:partition:elasticloadbalancing:region:account:loadbalancer/LoadBalancerN`

  範例：`arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/123456789abcbdeCLB`

  如需詳細資訊，請參閱 Elastic 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 的範例： `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdeNLB`
- Application Load Balancer 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 Elastic Load Balancing 資源。

AWS::Lambda::Function

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

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，請參閱在 Amazon RDS 中使用 Amazon Resource Name (ARNs)。

AWS::Route53::HealthCheck

Amazon Route 53 運作狀態檢查。

- ARN 格式： arn:*partition*:route53:::healthcheck/*Id*

範例：arn:aws:route53:::healthcheck/123456-1111-2222-3333

AWS::SQS::Queue

Amazon SQS 佇列。

- 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 Simple Queue Service 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

虛擬私有網路 (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

虛擬私有網路 (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

準備度檢查的 DNS 目標資源包括 DNS 記錄類型、網域名稱、Route 53 託管區域 ARN，以及 Network Load Balancer ARN 或 Route 53 記錄集 ID。

- 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 ARNs 中包含帳戶 ID，如此處所述。帳戶 ID 是必要的，讓 ARC 可以輪詢資源。格式刻意與 Amazon Route 53 所需的 ARN 格式不同，如服務授權參考中的 Route 53 服務資源類型所述。

- Network Load Balancer 的 ARN 格式：`arn:partition:elasticloadbalancing:region:account:loadbalancer/net/LoadBalancerName`

  Network Load Balancer 的範例： `arn:aws:elasticloadbalancing:us-west-2:111122223333:loadbalancer/net/sandbox-net/123456789acbdefgh`

  如需詳細資訊，請參閱 Elastic Load Balancing 資源。

在 Amazon Application Recovery Controller (ARC) 中記錄和監控準備度檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

您可以使用 Amazon CloudWatch AWS CloudTrail和 Amazon EventBridge 在 Amazon Application Recovery Controller (ARC) 中監控整備檢查，以分析模式並協助疑難排解問題。

> **Note**
>
> 您必須檢視美國西部 （奧勒岡） 區域中 ARC 的 CloudWatch 指標和日誌，包括主控台和使用時 AWS CLI。當您使用 時 AWS CLI，請包含下列參數來指定命令的美國西部 （奧勒岡） 區域：`--region us-west-2`。

主題

- 在 ARC 中使用 Amazon CloudWatch 搭配整備檢查
- 使用 記錄整備檢查 API 呼叫 AWS CloudTrail
- 在 ARC 中使用整備檢查搭配 Amazon EventBridge

在 ARC 中使用 Amazon CloudWatch 搭配整備檢查

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

Amazon Application Recovery Controller (ARC) 會將資料點發佈至 Amazon CloudWatch，以進行準備度檢查。CloudWatch 可讓使用一組時間序列資料的形式來擷取這些資料點的相關統計資料，也就是指標。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，您可以監控指定期間內透過 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，若指標超過您認為能夠接受的範圍，您可以建立 CloudWatch 警示來監控指定的指標並執行動作 (例如傳送通知到電子郵件地址)。

如需更多資訊，請參閱 Amazon CloudWatch 使用者指南。

主題

- ARC 指標
- ARC 指標的統計資料
- 在 ARC 中檢視 CloudWatch 指標

ARC 指標

`AWS/Route53RecoveryReadiness` 命名空間包含下列指標。

指標	Description
`ReadinessChecks`	代表 ARC 處理的整備檢查數量。指標可以依其狀態進行維度，如下所示。 單位：`Count`。 報告條件：有非零值。 統計資料：唯一有用的統計資料是 `Sum`。

指標	Description
	維度 • READY • NOT_READY • NOT_AUTHORIZED • UNKNOWN
Resources	代表 ARC 處理的資源數量，可由其資源識別符加以維度，如 API 所定義。 單位：Count。 報告條件：有非零值。 統計資料：唯一有用的統計資料是 Sum。 維度 • ResourceSetType ：這些是資源類型，依 ARC 評估的每個指定類型的資源數量進行篩選 例如：AWS::CloudWatch::Alarm

ARC 指標的統計資料

CloudWatch 會根據 ARC 發佈的指標資料點提供統計資料。統計資料是指定期間內指標資料的彙總。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。

以下是您可能會發現有用的指標/維度組合範例：

- 檢視 ARC 評估的整備程度檢查數量。
- 檢視 ARC 評估之指定資源集類型的資源總數。

在 ARC 中檢視 CloudWatch 指標

您可以使用 CloudWatch 主控台或 檢視 ARC 的 CloudWatch 指標 AWS CLI。在 主控台中，指標會顯示為監控圖表。

您必須檢視美國西部 （奧勒岡） 區域中 ARC 的 CloudWatch 指標，無論是在主控台或使用 時 AWS CLI。當您使用 時 AWS CLI，請包含下列參數來指定命令的美國西部 （奧勒岡） 區域：`--region us-west-2`。

使用 CloudWatch 主控台檢視指標

1. 在 https://console.aws.amazon.com/cloudwatch/ 開啟 CloudWatch 主控台。
2. 在導覽窗格中，選擇指標。
3. 選取 Route53RecoveryReadiness 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。

使用 檢視指標 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
```

使用 取得指標的統計資料 AWS CLI

使用下列 get-metric-statistics 命令來取得指定指標和維度的統計資料。請注意，CloudWatch 將把維度的各獨特組合視為個別指標。您無法使用未特別發佈的維度組合擷取統計資料。您必須指定建立指標時所使用的相同維度。

下列範例列出 ARC 中帳戶每分鐘評估的總整備度檢查。

```
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 記錄整備檢查 API 呼叫 AWS CloudTrail

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

已與 服務整合 AWS CloudTrail，此服務提供使用者、角色或 ARC 中 AWS 服務所採取動作的記錄。CloudTrail 會將 ARC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 ARC 主控台的呼叫，以及對 ARC API 操作的程式碼呼叫。

如果您建立線索，則可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 ARC 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 所收集的資訊，判斷向 ARC 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 ARC 資訊

當您建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。在 ARC 中發生活動時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

若要持續記錄 中的事件 AWS 帳戶，包括 ARC 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案傳送到您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案和接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 ARC 動作，並記錄在 Amazon Application Recovery Controller 的 Recovery Readiness API 參考指南、Amazon Application Recovery Controller 的 Recovery Control Configuration API 參考指南，以及 Amazon Application Recovery Controller 的 Routing Control API 參考指南中。例如，對 `CreateCluster`、`UpdateRoutingControlState` 和 `CreateRecoveryGroup` 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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 userIdentity 元素。

在事件歷史記錄中檢視 ARC 事件

CloudTrail 可讓您使用 Event history (事件歷史記錄) 檢視最近的事件。若要檢視 ARC API 請求的事件，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）。如需詳細資訊，請參閱 AWS CloudTrail 使用者指南中的使用 CloudTrail 事件歷史記錄。

了解 ARC 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範準備度檢查`CreateRecoveryGroup`的動作。

```
{
    "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": {
                "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 ARC 中使用整備檢查搭配 Amazon EventBridge

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

使用 Amazon EventBridge，您可以設定事件驅動規則，監控 Amazon Application Recovery Controller (ARC) 中的整備檢查資源，然後啟動使用其他服務的目標動作 AWS 。例如，您可以在整備檢查狀態從 READY 變更為 NOT READY 時發出 Amazon SNS 主題訊號，以設定傳送電子郵件通知的規則。

> **Note**
>
> ARC 只會在美國西部 （ 奧勒岡 ） (us-west-2) AWS 區域中發佈 EventBridge 事件以進行整備檢查。若要接收 EventBridge 事件以進行整備檢查，請在美國西部 （ 奧勒岡 ） 區域中建立 EventBridge 規則。

您可以在 Amazon EventBridge 中建立規則，以處理下列 ARC 整備檢查事件：

- 就緒狀態檢查準備。事件會指定整備檢查狀態是否從 READY 變更為 NOT READY。

若要擷取您感興趣的特定 ARC 事件，請定義 EventBridge 可用來偵測事件的事件特定模式。事件模式的結構與其相符的事件相同。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。在正常操作情況下，它們會以近乎即時的方式從 ARC 交付至 EventBridge。不過，可能會發生可能延遲或阻止交付事件的情況。

如需 EventBridge 規則如何使用事件模式的詳細資訊，請參閱 EventBridge 中的事件和事件模式。

使用 EventBridge 監控整備檢查資源

透過 EventBridge，您可以建立規則，定義 ARC 針對整備檢查資源發出事件時要採取的動作。

若要在 EventBridge 主控台中輸入或複製事件模式並貼上，請在主控台中選取 以輸入我自己的選項。為了協助您判斷可能對您有用的事件模式，本主題包含準備程度事件模式範例。

建立資源事件的規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 若要 AWS 區域 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，請保留預設值 。
6. 選擇下一步。
7. 對於建置事件模式步驟，對於事件來源，請保留預設值 AWS 事件。
8. 在範例事件下，選擇輸入我自己的事件。
9. 針對範例事件，輸入或複製並貼上事件模式。如需範例，請參閱下一節。

準備事件模式範例

事件模式的結構與其相符的事件相同。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

您可以將此區段的事件模式複製並貼到 EventBridge 中，以建立可用來監控 ARC 動作和資源的規則。

下列事件模式提供您可以在 EventBridge 中用於 ARC 中整備檢查功能的範例。

- 從 ARC 整備檢查中選取所有事件。

```
{
    "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"
    ]
}
```

- 僅選取與稱為 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"
    ]
}
```

- 只有在任何復原群組、儲存格或整備檢查狀態變成 時，才選取事件*NOT READY*。

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail-type":{
      "new-state":{
         "readiness-status":[
            "NOT_READY"
         ]
      }
   }
}
```

- 只有在任何復原群組、儲存格或整備檢查變成除了 以外的任何項目時，才選取事件 *READY*

```
{
   "source":[
      "aws.route53-recovery-readiness"
   ],
   "detail":{
      "new-state":{
         "readiness-status":[
            {
               "anything-but":"READY"
            }
         ]
      }
   }
}
```

以下是復原群組整備狀態變更的 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 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"
        }
    }
}
```

以下是整備檢查狀態變更的 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 日誌群組

建立 EventBridge 規則時，您必須指定要傳送符合規則之事件的目標。如需 EventBridge 可用目標的清單，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 日誌群組新增為目標的需求，並提供在建立規則時新增日誌群組的程序。

若要將 CloudWatch 日誌群組新增為目標，您可以執行下列其中一項操作：

- 建立新的日誌群組
- 選擇現有的日誌群組

如果您在建立規則時使用主控台指定新的日誌群組，EventBridge 會自動為您建立日誌群組。請確定您用作 EventBridge 規則目標的日誌群組以 開頭/aws/events。如果您想要選擇現有的日誌群組，請注意，只有開頭為 的日誌群組才會在下拉式功能表中/aws/events顯示為選項。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 操作建立或使用 CloudWatch 日誌群組做為目標，請確定您正確設定許可。如果您使用主控台將日誌群組新增至 EventBridge 規則，則日誌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 來指定日誌群組，則必須更新日誌群組的資源型政策。下列範例政策說明您必須在日誌群組的資源型政策中定義的許可：

JSON

```
{
    "Version":"2012-10-17",

    "Statement": [
        {
            "Action": [
                "logs:CreateLogStream",
                "logs:PutLogEvents"
            ],
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "events.amazonaws.com",
                    "delivery.logs.amazonaws.com"
                ]
            },
            "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/
events/*:*",
            "Sid": "TrustEventsToStoreLogEvent"
        }
    ]
}
```

您無法使用 主控台為日誌群組設定資源型政策。若要將必要的許可新增至以資源為基礎的政策，請使用 CloudWatch PutResourcePolicy API 操作。然後，您可以使用 describe-resource-policies CLI 命令來檢查政策是否正確套用。

為資源事件建立規則並指定 CloudWatch 日誌群組目標

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 選擇您要 AWS 區域 在其中建立規則的 。
3. 選擇建立規則，然後輸入該規則的任何相關資訊，例如事件模式或排程詳細資訊。

   如需建立 EventBridge 規則以進行整備的詳細資訊，請參閱使用 EventBridge 監控整備檢查資源。
4. 在選取目標頁面上，選擇 CloudWatch 做為您的目標。

5. 從下拉式選單中選擇 CloudWatch 日誌群組。

ARC 中準備度檢查的 Identity and Access Management

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （登入） 和授權 （具有許可） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目錄

- Amazon Application Recovery Controller (ARC) 中的整備檢查如何與 IAM 搭配使用
- ARC 中整備檢查的身分型政策範例
- 在 ARC 中使用服務連結角色進行整備檢查
- AWS ARC 中準備檢查的 受管政策

Amazon Application Recovery Controller (ARC) 中的整備檢查如何與 IAM 搭配使用

在您使用 IAM 管理對 ARC 的存取之前，請先了解哪些 IAM 功能可與 ARC 搭配使用。

在您使用 IAM 管理 Amazon Application Recovery Controller (ARC) 中整備檢查的存取權之前，請先了解哪些 IAM 功能可用於整備檢查。

您可以在 Amazon Application Recovery Controller (ARC) 中搭配整備檢查使用的 IAM 功能

IAM 功能	準備度檢查支援
身分型政策	是
資源型政策	否
政策動作	是

IAM 功能	準備度檢查支援
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 服務如何與大多數 IAM 功能搭配使用的高階整體檢視，請參閱《IAM 使用者指南》中的與 IAM AWS 搭配使用的 服務。

整備檢查的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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 ARC 身分型政策的範例，請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例。

整備檢查中的資源型政策

支援資源型政策：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。

整備檢查的政策動作

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。政策會使用動作來授予執行相關聯動作的許可。

若要查看整備檢查的 ARC 動作清單，請參閱《服務授權參考》中的 Amazon Route 53 Recovery Readiness 定義的動作。

ARC 中用於整備檢查的政策動作在動作之前使用下列字首：

```
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，下列項目：

```
"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*"
```

若要檢視整備檢查的 ARC 身分型政策範例，請參閱 ARC 中整備檢查的身分型政策範例。

準備度檢查的政策資源

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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要查看區域轉移的 ARC 動作清單，請參閱 Amazon Route 53 Recovery Readiness 定義的動作。

若要檢視整備檢查的 ARC 身分型政策範例，請參閱 ARC 中整備檢查的身分型政策範例。

整備檢查的政策條件索引鍵

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 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要查看整備檢查的 ARC 動作清單，請參閱 Amazon Route 53 Recovery Readiness 的條件索引鍵

若要查看您可以搭配具有整備檢查的條件金鑰使用的動作和資源，請參閱 Amazon Route 53 Recovery Readiness 定義的動作

若要檢視整備檢查的 ARC 身分型政策範例，請參閱 ARC 中整備檢查的身分型政策範例。

準備度檢查中的存取控制清單 ACLs)

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。

具有整備檢查的屬性型存取控制 (ABAC)

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，根據稱為標籤的屬性定義許可權。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

復原準備 （準備度檢查） 支援 ABAC。

使用臨時登入資料進行整備檢查

支援臨時憑證：是

臨時登入資料提供對 AWS 資源的短期存取，並在您使用聯合或切換角色時自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

準備度檢查的跨服務主體許可

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，您會被視為委託人。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 Recovery Readiness

準備度檢查的服務角色

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

準備度檢查的服務連結角色

支援服務連結角色：是

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。IAM 管理員可以檢視，但不能編輯服務連結角色的許可。

如需建立或管理 ARC 服務連結角色的詳細資訊，請參閱 在 ARC 中使用服務連結角色進行整備檢查。

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。在資料表中尋找服務，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。

ARC 中整備檢查的身分型政策範例

根據預設，使用者和角色沒有建立或修改 ARC 資源的許可。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。

如需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 (主控台)。

如需 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 ARNs 格式，請參閱《服務授權參考》中的 Amazon Application Recovery Controller (ARC) 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 範例：準備度檢查主控台存取
- 範例：準備度檢查 API 動作的準備度檢查

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作

AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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：準備度檢查主控台存取

若要存取 Amazon Application Recovery Controller (ARC) 主控台，您必須擁有一組最低許可。這些許可必須允許您列出和檢視 中 ARC 資源的詳細資訊 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。

對於僅呼叫 AWS CLI 或 AWS API 的使用者，您不需要允許最低主控台許可。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。

為了確保使用者和角色在僅允許存取特定 API 操作時仍可使用整備檢查主控台，請將整備檢查的`ReadOnly` AWS 受管政策附加至實體。如需詳細資訊，請參閱準備檢查就緒狀態檢查受管政策頁面，或《IAM 使用者指南》中的新增許可給使用者。

若要執行某些任務，使用者必須具有在 ARC 中建立與整備檢查相關聯之服務連結角色的許可。如需詳細資訊，請參閱 在 ARC 中使用服務連結角色進行整備檢查。

若要授予使用者透過主控台使用整備檢查功能的完整存取權，請將如下所示的政策連接到使用者：

JSON

```
{
    "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：準備度檢查 API 動作的準備度檢查

為了確保使用者可以使用 ARC API 動作來使用 ARC 整備檢查控制平面，例如建立復原群組、資源集和整備檢查，請連接對應至使用者需要使用的 API 操作的政策，如下所述。

若要執行某些任務，使用者必須具有在 ARC 中建立與整備檢查相關聯之服務連結角色的許可。如需詳細資訊，請參閱 在 ARC 中使用服務連結角色進行整備檢查。

若要使用 API 操作進行整備檢查，請將如下所示的政策連接到使用者：

JSON

```
{
    "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 ARC 中使用服務連結角色進行整備檢查

Amazon Application Recovery Controller 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，在此情況下為 ARC。服務連結角色是由 ARC 預先定義，並包含服務為了特定目的代表您呼叫其他 AWS 服務所需的所有許可。

服務連結角色可讓您更輕鬆地設定 ARC，因為您不必手動新增必要的許可。ARC 定義其服務連結角色的許可，除非另有定義，否則只有 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。這可保護您的 ARC 資源，因為您不會不小心移除存取資源的許可。

如需其他支援服務連結角色的相關資訊，請參閱服務連結角色欄中與 AWS IAM 搭配使用的服務，並尋找具有是的服務。選擇具有連結的是，以檢視該服務的服務連結角色文件。

ARC 具有下列服務連結角色，如本章所述：

- ARC 使用名為 Route53RecoveryReadinessServiceRolePolicy 的服務連結角色來存取資源和組態，以檢查準備狀態。
- ARC 使用名為 的服務連結角色進行自動轉移練習執行、監控客戶提供的 Amazon CloudWatch 警示和客戶 Health 儀板表 事件，以及開始練習執行。

Route53RecoveryReadinessServiceRolePolicy 的服務連結角色許可

ARC 使用名為 Route53RecoveryReadinessServiceRolePolicy 的服務連結角色來存取資源和組態，以檢查準備狀態。本節說明服務連結角色的許可，以及建立、編輯和刪除角色的相關資訊。

Route53RecoveryReadinessServiceRolePolicy 的服務連結角色許可

此服務連結角色使用 受管政策 `Route53RecoveryReadinessServiceRolePolicy`。

Route53RecoveryReadinessServiceRolePolicy 服務連結角色信任下列服務擔任該角色：

- `route53-recovery-readiness.amazonaws.com`

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 Route53RecoveryReadinessServiceRolePolicy。

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 ARC 建立 Route53RecoveryReadinessServiceRolePolicy 服務連結角色

您不需要手動建立 Route53RecoveryReadinessServiceRolePolicy 服務連結角色。當您在 AWS CLI、或 AWS API AWS 管理主控台中建立第一個整備檢查或跨帳戶授權時，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，ARC 會再次為您建立服務連結角色。

編輯 ARC 的 Route53RecoveryReadinessServiceRolePolicy 服務連結角色

ARC 不允許您編輯 Route53RecoveryReadinessServiceRolePolicy 服務連結角色。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考角色。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」的編輯服務連結角色。

刪除 ARC 的 Route53RecoveryReadinessServiceRolePolicy 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之後，您就可以刪除 Route53RecoveryReadinessServiceRolePolicy 服務連結角色。如需整備檢查的詳細資訊，請參閱 ARC 中的準備度檢查。如需跨帳戶授權的詳細資訊，請參閱 在 ARC 中建立跨帳戶授權。

> **Note**
>
> 如果 ARC 服務在您嘗試刪除資源時使用角色，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 AWS CLI、 或 AWS API 來刪除 Route53RecoveryReadinessServiceRolePolicy 服務連結角色。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 ARC 服務連結角色以進行整備檢查

如需 ARC 服務連結角色的 AWS 受管政策更新，請參閱 ARC 的AWS 受管政策更新表。您也可以在 ARC 文件歷史記錄頁面上訂閱自動 RSS 提醒。

AWS ARC 中準備檢查的 受管政策

AWS 受管政策是由 AWS AWS 受管政策建立和管理的獨立政策旨在為許多常用案例提供許可，以便您可以開始將許可指派給使用者、群組和角色。

請記住， AWS 受管政策可能不會授予特定使用案例的最低權限許可，因為這些許可可供所有 AWS 客戶使用。我們建議您定義特定於使用案例的客戶管理政策，以便進一步減少許可。

您無法變更 AWS 受管政策中定義的許可。如果 AWS 更新受 AWS 管政策中定義的許可，則更新會影響政策連接的所有委託人身分（使用者、群組和角色）。 AWS 服務 當新的 啟動或新的 API 操作可用於現有服務時， AWS 最有可能更新 AWS 受管政策。

如需詳細資訊，請參閱 IAM 使用者指南中的 AWS 受管政策。

AWS 受管政策：Route53RecoveryReadinessServiceRolePolicy

您不得將 Route53RecoveryReadinessServiceRolePolicy 連接到 IAM 實體。此政策會連接到服務連結角色，允許 Amazon Application Recovery Controller (ARC) 存取 AWS 由 ARC 使用或管理的服務和資源。如需詳細資訊，請參閱在 ARC 中使用服務連結角色進行整備檢查。

AWS 受管政策：AmazonRoute53RecoveryReadinessFullAccess

您可以將 AmazonRoute53RecoveryReadinessFullAccess 連接到 IAM 實體。此政策授予在 ARC 中使用復原準備（準備度檢查）之動作的完整存取權。將其連接到需要完整存取復原準備動作的 IAM 使用者和其他主體。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryReadinessFullAccess。

AWS 受管政策：AmazonRoute53RecoveryReadinessReadOnlyAccess

您可以將 AmazonRoute53RecoveryReadinessReadOnlyAccess 連接到 IAM 實體。此政策授予在 ARC 中處理復原準備之動作的唯讀存取權。它適用於需要檢視整備狀態和復原群組組態的使用者。這些使用者無法建立、更新或刪除復原準備度資源。

若要檢視此政策的許可，請參閱《 AWS 受管政策參考》中的 AmazonRoute53RecoveryReadinessReadOnlyAccess。

適用於整備的 AWS 受管政策更新

如需自此服務開始追蹤這些變更以來，ARC 中針對整備檢查的 AWS 受管政策更新詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 的 AWS 受管政策更新。如需此頁面變更的自動提醒，請訂閱 ARC 文件歷史記錄頁面上的 RSS 摘要。

整備檢查的配額

> **Note**
>
> 自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。

Amazon Application Recovery Controller (ARC) 中的準備度檢查受下列配額 （ 先前稱為限制 ） 約束。

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量	15
每個儲存格的巢狀儲存格數量	3
每個復原群組的儲存格數量	3
每個儲存格的資源數量	10
每個復原群組的資源數量	10
每個資源集的資源數量	6
每個帳戶的資源集數目	200
每個帳戶的整備檢查數量	200
跨帳戶授權的數量	100

ARC 中的區域切換

您可以使用 ARC 中的區域切換，為跨 AWS 帳戶的應用程式資源協調大規模、複雜的復原任務，以協助確保業務持續性並降低營運開銷。區域切換提供集中且可觀察的解決方案，您可以手動執行，或使用 Amazon CloudWatch 警示觸發來自動化。如果 AWS 區域 受損，您可以使用區域切換容錯移轉或將資源切換到另一個區域，來執行您建立的計劃。這可確保您的應用程式可以繼續運作，並在運作狀態良好的 中執行 AWS 區域。

區域切換是以您為特定復原需求設計和設定的計劃概念為基礎建置。每個計劃都包含由步驟組成的工作流程。每個步驟都會執行一或多個執行區塊，該區域切換會平行或依序執行，以完成應用程式復原。每個執行區塊都會處理不同的任務，例如切換資源或管理應用程式的流量重新導向。如需更多彈性，您可以透過將子計劃新增至整體父計劃來建立父計劃。

區域切換包含下列項目：

- 支援主動/被動和主動/主動組態。如果您有作用中/被動的多區域組態，則可以容錯移轉和容錯回復；如果您的應用程式在多個區域中設定為作用中/作用中，則可以轉移並傳回 。
- 跨帳戶支援您在應用程式復原中包含的應用程式資源。您也可以跨帳戶共用區域切換計劃。
- 自動容錯移轉或切換，方法是根據 Amazon CloudWatch 警示觸發計畫執行。或者，您可以選擇手動執行區域切換計畫。
- 功能完整的儀表板，可讓您即時了解復原程序。
- 每個 中的資料平面 AWS 區域，因此您可以執行區域切換計畫，而無需依賴您要停用的區域。

區域切換完全由 管理 AWS。使用區域切換可讓您受益於復原平台的彈性，該平台著重於應用程式的特定需求，而不是建置和維護指令碼，以及手動收集復原資料。

關於區域切換

使用區域切換，您可以協調特定步驟來切換 AWS 區域 多區域應用程式執行所在的 。

區域切換是以您為特定復原需求設計和設定的計劃概念為基礎建置。每個計劃都包含由步驟組成的工作流程。每個步驟都會執行一或多個執行區塊，該區域切換會平行或依序執行，以完成應用程式復原。每個執行區塊都會處理不同的任務，例如切換資源或管理應用程式的流量重新導向。如需更多彈性，您可以透過新增子計畫來建立父系計畫。

每當您建立或更新計劃時，區域切換會執行計劃評估，以確保 IAM 許可、資源組態或執行容量沒有問題。區域切換會定期執行這些評估，並針對發現的任何問題產生警告。

區域切換也會計算每個計劃執行的實際復原時間值，以協助您評估計劃是否符合您的目標。您可以在的區域切換儀表板中檢視復原時間和計畫執行的其他詳細資訊 AWS 管理主控台。如需詳細資訊，請參閱區域切換儀表板。

若要進一步了解區域切換中的每個區域，請參閱下列各節。

區域切換計劃

區域切換計畫是區域切換中最上層的資源。您應該將您的計劃範圍限定在特定多區域應用程式。計劃可讓您在指定的 中執行一系列區域切換執行區塊，啟用或停用您的應用程式及其資源，包括跨帳戶資源，以建置工作流程來復原 AWS 區域 應用程式。

計劃是由一或多個工作流程組成，可讓您啟用或停用特定工作流程 AWS 區域。您可以在工作流程中設定執行區塊以循序執行，也可以指定某些區塊平行執行。

對於您為主動/被動多區域方法設定的計劃，您可以建立一個可用於啟用其中一個區域的工作流程，或兩個單獨的啟用工作流程，每個區域一個。對於您為主動/主動方法設定的計劃，您可以建立一個工作流程來啟用您的區域，以及一個工作流程來停用您的區域。

AWS 區域 是全球 AWS 叢集資料中心所在的地理位置。每個區域的設計都完全與其他區域隔離，提供容錯能力和穩定性。使用區域切換時，您需要考慮應用程式部署在哪些區域，以及您要用於復原的區域。

區域切換支援 AWS 區域 在提供服務的任何兩個之間進行復原。當您設定區域切換計劃時，您可以指定應用程式部署所在的區域，以及您想要使用的復原方法：主動/被動或主動/主動。

例如，您可能有主動/被動的多區域方法，其中 us-east-1 作為主要區域，us-west-2 作為待命區域。若要從影響 us-east-1 中應用程式的操作問題中復原應用程式，您可以執行區域切換計畫來啟用 us-west-2。這會導致應用程式從 us-east-1 中的資源切換到 us-west-2 中的資源。

區域切換計畫使用與您在建立計畫時指定的 IAM 角色相關聯的許可來執行。

您可以建立多個計劃，每個多區域應用程式各一個計劃，然後透過建立父計劃，以所需的順序協調這些計劃的復原。父計畫是使用區域切換計畫執行區塊做為步驟的計畫。計劃階層僅限於兩個層級（父系和子系），但您可以在相同的父系計劃下包含多個子系計劃。

工作流程和執行區塊

建立區域切換計畫後，您必須將一或多個工作流程新增至計畫，以定義您希望計畫為應用程式復原執行的步驟。對於每個工作流程，您可以新增包含執行區塊的步驟。每個執行區塊都會執行特定的復原動

作，例如擴展資源或更新路由控制以重新路由流量。步驟會組織這些執行區塊，並控制它們是平行還是循序執行。透過建立父系計劃，您也可以協調多個應用程式復原到您正在啟用之區域的順序。

您可以將執行區塊組織成工作流程中的步驟。每個步驟都可以包含一或多個平行執行的執行區塊，而且您可以安排在工作流程中循序執行的步驟。此外，視資源而定，您可以選擇執行具有正常（計劃）或不良（計劃）執行的執行區塊。

- 穩定執行：規劃的執行工作流程。當您的環境運作狀態良好時，您可以使用優雅工作流程來執行所有步驟，以有序地執行計劃。
- 不穩健的執行：意外的執行。不良工作流程模式只會使用必要的步驟和動作。此模式會變更工作流程中執行區塊的行為，或略過特定的執行區塊。
- 復原後執行：在成功復原後執行以準備未來區域事件的工作流程。復原後執行可以建立僅供讀取複本、透過 Lambda 函數執行自訂邏輯、新增手動核准閘道，以及嵌入用於複雜協同運作的子計畫。這些執行需要兩個區域都正常運作，並在先前受損的區域中執行。

最後，您也可以設定執行區塊的跨帳戶資源。首先，您必須遵循 中的指引來設定許可區域切換中的跨帳戶支援。設定必要的 IAM 角色之後，您可以在計劃工作流程的執行區塊中新增跨帳戶資源。若要新增跨帳戶資源，當您新增步驟時，您可以指定具有其他資源許可的目標 IAM 角色 AWS 帳戶。您也必須為跨帳戶角色指定您在信任政策中提供的外部 ID。如需建立所需 IAM 角色的詳細資訊，請參閱 跨帳戶資源許可。

若要進一步了解工作流程，請參閱 建立區域切換計畫工作流程。如需每種執行區塊類型的詳細資訊，包括組態步驟、運作方式，以及做為計畫評估一部分評估的內容，請參閱 新增執行區塊。

計畫評估

計劃評估是一種自動化程序，區域切換會在建立或更新計劃時執行，之後在穩定狀態期間每 30 分鐘執行一次。評估程序會驗證計劃組態和資源組態的數個關鍵層面。評估包括驗證 IAM 許可、資源組態和執行容量。

如果區域切換發現可能無法成功執行計劃的問題，會產生計劃評估警告，這會在主控台的計劃詳細資訊頁面上反白顯示。您也可以使用 Amazon EventBridge 使用計劃評估警告，也可以使用區域切換 API 檢視警告。如需計劃評估 API 的詳細資訊，請參閱《Amazon Application Recovery Controller (ARC) 的區域交換器 API 參考指南》中的 GetPlanEvaluationStatus。

您可以在計劃詳細資訊頁面上的計劃評估索引標籤中，查看計劃評估表面問題的詳細資訊和建議補救措施。我們建議您也透過執行區域切換計畫來測試應用程式復原，而且不要僅倚賴區域切換計畫評估來測試復原計畫是否如預期般運作。

自動計劃執行報告

區域切換可以自動為計劃執行產生全面的 PDF 報告，以協助您滿足法規合規要求。這些報告提供災難復原測試和實際復原事件的證據，包括詳細的執行時間表、計劃組態和資源狀態。

當您為計劃設定自動產生報告時，區域切換會在每個計劃執行完成後建立 PDF 報告，並將其交付至您指定的 Amazon S3 儲存貯體。報告通常會在執行完成後 30 分鐘內提供。需支付 S3 儲存成本。

每個報告都包含：

- 具有服務概觀和報告建立日期的執行摘要
- 規劃執行時存在的組態詳細資訊
- 包含步驟、受影響資源和狀態的詳細執行時間表
- 規劃執行開始時出現的警告
- Amazon CloudWatch 警示狀態和相關警示的警示歷史記錄
- 對於父計畫、子計畫的組態和執行詳細資訊
- 術語和概念詞彙表

若要啟用自動產生報告，請在建立或更新計劃時設定報告輸出目的地。您還必須確保計劃的執行 IAM 角色具有將報告寫入 Amazon S3 儲存貯體的必要許可，並存取產生報告內容所需的資源。如需所需許可的相關資訊，請參閱自動計劃執行報告許可。

您可以檢視報告產生的狀態，並從 主控台的計劃執行詳細資訊頁面下載完成的報告。如果報告產生發生錯誤，例如許可不足或 Amazon S3 儲存貯體設定錯誤，區域切換會提供錯誤詳細資訊，協助您對問題進行疑難排解。

計劃評估會持續驗證您的報告組態，包括驗證執行角色是否具有所需的 IAM 許可。如果區域切換偵測到會阻止成功產生報告的組態問題，則會產生警告，您可以在計劃詳細資訊頁面上檢視這些警告。

區域警示和實際復原時間

區域切換會計算每個計劃執行的實際復原時間值，您可以在計劃執行後檢視該值。實際復原時間會顯示在計劃執行詳細資訊頁面上，讓您可以將實際時間與您建立計劃時指定的復原時間目標進行比較。

實際復原時間的計算方式為計劃執行完成所需的總時間，以及您設定的特定 Amazon CloudWatch 警示之前經過的任何額外時間都會返回綠色狀態。

若要支援計算計劃執行的準確實際復原時間，您必須為區域切換計劃設定區域 Amazon CloudWatch 警示，以提供每個區域中應用程式運作狀態的訊號。執行計劃時，區域切換會使用這些應用程式運作狀態

警示來判斷您的應用程式何時再次運作良好。然後，區域切換會根據您設定的應用程式運作狀態警示，根據您的計劃執行新增至應用程式恢復運作狀態所需時間的實際復原時間，來計算實際復原時間。

將 CloudWatch 警示新增至區域切換計劃之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱應用程式運作狀態許可的 CloudWatch 警示。

AWS 區域

區域切換適用於所有商業 AWS 區域區域，以及 AWS GovCloud (US) 區域。

如需 Amazon Application Recovery Controller (ARC) 的區域支援和服務端點的詳細資訊，請參閱《Amazon Web Services 一般參考》中的 Amazon Application Recovery Controller (ARC) 端點和配額。

區域名稱	區域	端點	通訊協定
美國東部 (俄亥俄)	us-east-2	arc-region-switch.us-east-2.api.aws arc-region-switch-fips.us-east-2.api.aws	HTTPS HTTPS
美國東部 (維吉尼亞北部)	us-east-1	arc-region-switch.us-east-1.api.aws arc-region-switch-control-plane-fips.us-east-1.api.aws arc-region-switch-fips.us-east-1.api.aws arc-region-switch-control-plane.us-east-1.api.aws	HTTPS HTTPS HTTPS HTTPS
美國西部 (加利佛尼亞北部)	us-west-1	arc-region-switch.us-west-1.api.aws arc-region-switch-fips.us-west-1.api.aws	HTTPS HTTPS
美國西部 (奧勒岡)	us-west-2	arc-region-switch.us-west-2.api.aws arc-region-switch-fips.us-west-2.api.aws	HTTPS HTTPS
Africa (Cape Town)	af-south-1	arc-region-switch.af-south-1.api.aws	HTTPS

區域名稱	區域	端點	通訊協定	
亞太區域 (香港)	ap-east-1	arc-region-switch.ap-east-1.api.aws	HTTPS	
亞太區域 (海德拉巴)	ap-south-2	arc-region-switch.ap-south-2.api.aws	HTTPS	
亞太區域 (雅加達)	ap-southeast-3	arc-region-switch.ap-southeast-3.api.aws	HTTPS	
亞太地區 (馬來西亞)	ap-southeast-5	arc-region-switch.ap-southeast-5.api.aws	HTTPS	
亞太區域 (墨爾本)	ap-southeast-4	arc-region-switch.ap-southeast-4.api.aws	HTTPS	
亞太區域 (孟買)	ap-south-1	arc-region-switch.ap-south-1.api.aws	HTTPS	
亞太區域 (紐西蘭)	ap-southeast-6	arc-region-switch.ap-southeast-6.api.aws	HTTPS	
亞太區域 (大阪)	ap-northeast-3	arc-region-switch.ap-northeast-3.api.aws	HTTPS	
亞太區域 (首爾)	ap-northeast-2	arc-region-switch.ap-northeast-2.api.aws	HTTPS	
亞太區域 (新加坡)	ap-southeast-1	arc-region-switch.ap-southeast-1.api.aws	HTTPS	

區域名稱	區域	端點	通訊協定	
亞太地區 (悉尼)	ap-southeast-2	arc-region-switch.ap-southeast-2.api.aws	HTTPS	
亞太區域 (台北)	ap-east-2	arc-region-switch.ap-east-2.api.aws	HTTPS	
亞太區域 (泰國)	ap-southeast-7	arc-region-switch.ap-southeast-7.api.aws	HTTPS	
亞太區域 (東京)	ap-northeast-1	arc-region-switch.ap-northeast-1.api.aws	HTTPS	
加拿大 (中部)	ca-central-1	arc-region-switch.ca-central-1.api.aws	HTTPS	
加拿大西部 (卡加利)	ca-west-1	arc-region-switch.ca-west-1.api.aws	HTTPS	
歐洲 (法蘭克福)	eu-central-1	arc-region-switch.eu-central-1.api.aws	HTTPS	
歐洲 (愛爾蘭)	eu-west-1	arc-region-switch.eu-west-1.api.aws	HTTPS	
歐洲 (倫敦)	eu-west-2	arc-region-switch.eu-west-2.api.aws	HTTPS	
歐洲 (米蘭)	eu-south-1	arc-region-switch.eu-south-1.api.aws	HTTPS	
歐洲 (巴黎)	eu-west-3	arc-region-switch.eu-west-3.api.aws	HTTPS	

區域名稱	區域	端點	通訊協定
歐洲 (西班牙)	eu-south-2	arc-region-switch.eu-south-2.api.aws	HTTPS
歐洲 (斯德哥爾摩)	eu-north-1	arc-region-switch.eu-north-1.api.aws	HTTPS
歐洲 (蘇黎世)	eu-central-2	arc-region-switch.eu-central-2.api.aws	HTTPS
以色列 (特拉維夫)	il-central-1	arc-region-switch.il-central-1.api.aws	HTTPS
墨西哥 (中部)	mx-central-1	arc-region-switch.mx-central-1.api.aws	HTTPS
中東 (巴林)	me-south-1	arc-region-switch.me-south-1.api.aws	HTTPS
中東 (阿拉伯聯合大公國)	me-central-1	arc-region-switch.me-central-1.api.aws	HTTPS
南美洲 (聖保羅)	sa-east-1	arc-region-switch.sa-east-1.api.aws	HTTPS
AWS GovCloud （美國東部）	us-gov-east-1	arc-region-switch.us-gov-east-1.api.aws	HTTPS
		arc-region-switch-fips.us-gov-east-1.api.aws	HTTPS

區域名稱	區域	端點	通訊協定	
AWS GovCloud（美國西部）	us-gov-west-1	arc-region-switch.us-gov-west-1.api.aws arc-region-switch-control-plane-fips.us-gov-west-1.api.aws arc-region-switch-fips.us-gov-west-1.api.aws arc-region-switch-control-plane.us-gov-west-1.api.aws	HTTPS HTTPS HTTPS HTTPS	

區域切換元件

以下是 Amazon Application Recovery Controller (ARC) 中區域切換功能的元件和相關概念。

計畫

計劃是應用程式的基本復原程序。您可以使用要依序或平行執行的執行區塊來建置一或多個工作流程，以建立計畫。然後，當區域性受損時，您可以執行計劃，透過轉移應用程式以在運作狀態良好的區域中執行，來完成應用程式的復原。

子計畫

子計畫是一種獨立的計畫，可以從父計畫中執行，以協調更複雜的應用程式復原案例。您可以巢狀化區域切換計劃一個層級。

工作流程

區域切換計劃包含一或多個工作流程。工作流程是由包含執行區塊的步驟組成，您指定平行或依序執行，以完成區域作為復原計畫的一部分的啟用或停用。對於您設定為具有主動/被動方法的計劃，您可以建立一個工作流程，可用於啟用其中一個區域，或為每個區域建立一個單獨的啟用工作流程。對於您為主動/主動方法設定的計劃，您可以建立一個工作流程來啟用您的區域，以及一個工作流程來停用您的區域。

執行區塊

您可以將步驟新增至包含執行區塊的區域切換計畫工作流程。執行區塊可讓您在啟用區域中指定多個應用程式或資源的復原。當您將步驟新增至工作流程時，您可以與其他步驟依序新增，或與一或多個其他步驟平行新增。

優雅和不羈的組態

您可以選擇執行具有優雅（計劃）或不良（計劃外）執行的特定執行區塊。當您的環境運作狀態良好時，您可以使用優雅工作流程來執行所有步驟，以有序地執行計劃。不良工作流程模式只會使用必要的步驟和動作。當您以不良模式執行計劃時，它會變更工作流程中執行區塊的行為，或略過特定執行區塊，視執行區塊的類型而定。

特定類型的執行區塊在執行時會有不同的行為。有關這些差異的詳細資訊，請參閱 一節，其中包含每種執行區塊的詳細資訊。如需詳細資訊，請參閱新增執行區塊。

主動/主動和主動/被動組態

為跨多個區域的應用程式建立彈性組態有兩種主要方法：主動/被動和主動/主動。區域切換支援這兩種方法的應用程式復原。

使用主動/被動組態，您可以在兩個不同的區域中部署應用程式的兩個複本，而客戶流量只會前往一個區域。

使用主動/主動組態，您可以將兩個複本部署到兩個不同的區域，但兩個複本都在處理工作或接收流量。

計劃執行

當區域切換計劃執行時，它會透過為應用程式及其接收的流量啟用運作狀態良好的區域，在區域受損時實作應用程式的復原。使用主動/主動組態時，您也可以執行計劃執行來停用受損的區域。

應用程式運作狀態警示

應用程式運作狀態警示是您為計劃指定的 CloudWatch 警示，用於指示每個區域中應用程式的運作狀態。區域切換使用應用程式運作狀態警示，協助判斷切換區域以實作復原後的實際復原時間。

觸發

您可以使用區域切換中的觸發程序來自動化應用程式復原。當您建立觸發時，您可以指定一或多個 Amazon CloudWatch 警示，並定義應啟動計畫執行的警示條件（例如 "red" 或 "green")。當符合指定的條件時，區域切換會自動執行計畫。觸發條件與應用程式運作狀態警示不同：觸發啟動計劃執行，而應用程式運作狀態警示可協助區域切換在計劃完成後計算實際的復原時間。

復原後工作流程

復原後工作流程是選用的工作流程，會在成功復原後執行，為未來的區域事件做好準備。這些工作流程需要兩個區域都正常運作，並在先前受損的區域中執行。復原後執行會參考最近復原執行的復原執行 ID。

復原後工作流程支援下列執行區塊：

- RDS 建立跨區域複本
- 自訂動作 Lambda
- 手動核准
- 區域切換計畫

儀表板

區域切換包含儀表板，您可以在其中即時追蹤計劃執行的詳細資訊。

區域切換的資料和控制平面

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依賴的機制具有高度可用性，以便在災難情況下需要它們時使用。一般而言，您應該盡可能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，了解服務的功能如何在控制平面和資料平面之間分割，以及何時可以使用服務的資料平面依賴極端可靠性。

如同許多 AWS 服務，控制平面和資料平面支援區域切換功能的功能。雖然這兩種類型都建置為可靠，但控制平面會針對資料一致性進行最佳化，而資料平面則會針對可用性進行最佳化。資料平面專為彈性而設計，因此即使在破壞性事件期間，當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，我們建議您在可用性很重要時使用資料平面操作，例如，當您需要在中斷期間取得區域切換計畫的相關資訊時。

對於區域切換，控制平面和資料平面分割如下：

- 區域切換的控制平面位於美國東部（維吉尼亞北部）區域 (us-east-1)、 AWS GovCloud (US-West) 區域 (us-gov-west-1)，僅用於服務管理，也就是建立和更新計劃，而不是用於復原，也就是執行計劃。區域切換組態控制平面 API 操作不高度可用。
- 區域切換在每個區域都有獨立的資料平面 AWS 區域。您應該使用資料平面進行復原動作，也就是執行區域切換計畫。如需資料平面操作的清單，請參閱 區域切換 API 操作。這些區域切換資料平面操作具有高可用性。

區域切換在每個 中提供獨立的主控台 AWS 區域，可呼叫復原任務的資料平面 API 操作，因此您可以在要啟動的區域中使用主控台來執行應用程式復原計劃。如需有關使用區域切換準備和完成復原操作時的重要考量的詳細資訊，請參閱 ARC 中區域切換的最佳實務。

如需資料平面、控制平面以及 如何 AWS 建置服務以滿足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白皮書。

ARC 區域切換的標記；

標籤是您用來識別和組織 AWS 資源的單字或片語 （中繼資料）。您可以為每個資源新增多個標籤，每個標籤都包含您定義的索引鍵和值。例如，金鑰可能是環境，而值可能是生產。您可以根據新增的標籤來搜尋和篩選資源。

您可以在 ARC 的區域切換中標記下列資源：

- 計劃

ARC 中的標記只能透過 API 使用，例如使用 AWS CLI。

以下是使用 在區域切換中標記的範例 AWS CLI。

```
aws arc-region-switch --region us-east-1 create-plan --plan-name example-plan --tags Region=IAD,Stage=Prod
```

如需詳細資訊，請參閱《Amazon Application Recovery Controller (ARC) 的區域交換器 API 參考指南》中的 TagResource。

ARC 中區域切換的定價

您為每個設定的區域切換計劃支付固定的每月成本。

如需 ARC 和定價範例的詳細定價資訊，請參閱 ARC 定價。

ARC 中區域切換的最佳實務

建議您在 Amazon Application Recovery Controller (ARC) 中使用區域切換進行復原和容錯移轉準備的下列最佳實務。

主題

- 確保專用、長期的 AWS 登入資料安全且隨時可存取
- 為涉及容錯移轉的 DNS 記錄選擇較低的 TTL 值
- 保留關鍵應用程式所需的容量
- 使用極為可靠的資料平面 API 操作來列出和取得區域切換計畫的相關資訊

- 使用 ARC 測試容錯移轉

確保專用、長期的 AWS 登入資料安全且隨時可存取

在災難復原 (DR) 案例中，使用存取 AWS 和執行復原任務的簡單方法，將系統相依性降至最低。建立專門用於 DR 任務的 IAM 長期憑證，並將憑證安全地保存在現場部署實體安全或虛擬保存庫中，以在需要時存取 。透過 IAM，您可以集中管理安全登入資料，例如存取金鑰，以及存取 AWS 資源的許可。對於非 DR 任務，我們建議您繼續使用聯合存取，並使用 AWS AWS Single Sign-On 等服務。

為涉及容錯移轉的 DNS 記錄選擇較低的 TTL 值

對於可能需要在容錯移轉機制中變更的 DNS 記錄，尤其是使用較低的 TTL 值檢查運作狀態的記錄是適當的。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）設定會告知 DNS 解析程式在請求新的記錄之前快取記錄的時間。當您選擇 TTL 時，您可以權衡延遲和可靠性，以及對變更的回應能力。當記錄的 TTL 較短時，DNS 解析程式會更快地通知記錄更新，因為 TTL 指定他們必須更頻繁地查詢。

如需詳細資訊，請參閱 Amazon Route 53 DNS 最佳實務中的選擇 DNS 記錄的 TTL 值。

保留關鍵應用程式所需的容量

區域切換包含執行區塊類型，有助於在復原過程中擴展運算資源。如果您在計劃中使用這些執行區塊，區域切換不保證達到所需的運算容量。如果您有重要的應用程式且需要保證存取容量，建議您預留容量。

您可以遵循一些策略，在次要區域中保留運算容量，同時限制成本。若要進一步了解，請參閱具有預留容量的指示燈：如何使用隨需容量預留最佳化 DR 成本。

使用極為可靠的資料平面 API 操作來列出和取得區域切換計畫的相關資訊

使用資料平面 API 操作，在事件期間使用和執行您的區域切換計畫。如需區域切換資料平面操作的清單，請參閱 區域切換 API 操作。

每個區域中的區域切換主控台會使用資料平面操作來執行區域切換計劃。您也可以使用 AWS CLI 或執行您使用其中一個 SDKs 撰寫的程式碼，來呼叫資料平面 API AWS 操作。ARC 在資料平面中使用 API 提供極高的可靠性。

使用 ARC 測試應用程式復原

使用 ARC 區域切換定期測試應用程式復原、在另一個區域中啟用次要應用程式堆疊 AWS 區域，或執行區域切換計畫來停用其中一個區域，以切換主動-主動組態。

請務必確保您建立的區域切換計畫與堆疊中的正確資源一致，而且一切都如您預期般運作。您應該在為您的環境設定區域切換後進行測試，並繼續定期測試，以便驗證復原程序是否正常運作。在遇到故障情況之前，請定期執行此測試，以協助避免使用者停機。

ARC 區域切換 DNS 容錯移轉與 Route 53 加速復原

加速復原為用於更新已啟用此功能之公有託管區域記錄的 APIs 提供 60 分鐘的目標 RTO。如果您需要維持對 RTO 的控制，而不是等待 AWS 完成復原所需的 APIs，您應該使用 ARC Routing 控制項或 ARC Region switch Route 53 運作狀態檢查執行區塊。

教學課程：建立主動/被動區域切換計畫

本教學課程會引導您為在 us-east-1 中執行的應用程式建立主動/被動區域切換計畫，並復原至 us-west-2。此範例包括用於運算的 Amazon EC2 執行個體、用於儲存的 Amazon Aurora 全域資料庫，以及用於 DNS 的 Amazon Route 53。

在本教學課程中，您將完成下列步驟：

- 建立區域切換計畫
- 建置計劃的工作流程和執行區塊
- 建置 EC2 Auto Scaling 群組執行區塊
- 建置兩個手動核准執行區塊
- 建置兩個自訂動作 Lambda 執行區塊
- 建置 Amazon Aurora Global Database 執行區塊
- 建置 ARC 路由控制區塊
- 執行區域切換計畫

先決條件

開始本教學課程之前，請確認您在這兩個區域中都具備下列先決條件：

- 具有適當許可的 IAM 角色
- EC2 Auto Scaling 群組
- 用於維護頁面和圍欄的 Lambda 函數
- Aurora 全域資料庫
- ARC 路由控制

步驟 1：建立區域切換計畫

1. 從區域切換主控台中，選擇建立區域切換計劃。
2. 提供下列詳細資訊：
   - 主要區域：選擇 us-east-1
   - 待命區域：選擇 us-west-2
   - 所需的復原時間目標 (RTO)（選用）
   - IAM 角色：輸入計劃執行 IAM 角色。此 IAM 角色允許區域切換在執行期間呼叫 AWS 服務。
3. 選擇建立。

（選用）將來自不同 AWS 帳戶的資源新增至您的區域切換計畫：

1. 建立跨帳戶角色：
   - 在託管資源的帳戶中，建立 IAM 角色。
   - 新增計劃將存取之特定資源的許可。
   - 新增允許執行角色擔任新角色的信任政策。
   - 輸入並記下您將用作共用秘密的外部 ID。
2. 在您的計劃中設定 資源：
   - 當您將資源新增至計劃時，請指定兩個額外的欄位：
     - crossAccountRole：您在步驟 1 中建立之角色的 ARN
     - externalId：您在步驟 1 中輸入的外部 ID

EC2 Auto Scaling 執行區塊存取帳戶 987654321 中資源的範例組態：

```
{
  "executionBlock": "EC2AutoScaling",
  "name": "ASG",
  "crossAccountRole": "arn:aws:iam::987654321:role/RegionSwitchCrossAccountRole",
  "externalId": "unique-external-id-123",
  "autoScalingGroupArn": "arn:aws:autoscaling:us-
west-2:987654321:autoScalingGroup:*:autoScalingGroupName/CrossAccountASG"
}
```

必要許可：

- 執行角色必須具有跨帳戶角色的 sts：AssumeRole 許可。
- 跨帳戶角色必須僅具有所存取特定資源的許可。
- 跨帳戶角色的信任政策必須包含：
  - 執行角色的帳戶做為信任的實體。
  - 外部 ID 條件。
- 如需設定跨帳戶角色的詳細資訊，請參閱 跨帳戶資源許可。

在執行計畫之前，區域切換會驗證下列項目：

- 執行角色可以擔任跨帳戶角色。
- 跨帳戶角色具有必要的許可。
- 外部 ID 符合信任政策。

步驟 2：建置計劃的工作流程和執行區塊

1. 在區域切換計畫詳細資訊頁面中，選擇建置工作流程。
2. 選取為所有區域建立相同的啟用工作流程。
3. 輸入區域啟用工作流程描述（選用）。這將用於在執行計劃時輕鬆識別工作流程。
4. 選擇儲存並繼續。

新增 EC2 Auto Scaling 執行區塊

如需此執行區塊的詳細資訊，請參閱 Amazon EC2 Auto Scaling 群組執行區塊。

1. 選擇新增步驟，然後選擇依序執行。
2. 選取 EC2 Auto Scaling 執行區塊，然後選擇新增和編輯。此區塊可讓您開始增加被動區域中的容量。
3. 在右側面板中，設定 區塊：
   - 步驟名稱：輸入「擴展」
   - 步驟描述（選用）
   - us-east-1 的 Auto Scaling 群組 ARN：us-east-1 中 ASG 的 ARN
   - us-west-2 的 Auto Scaling 群組 ARN：us-west-2 中 ASG 的 ARN
   - 符合來源區域的容量的百分比：輸入 100

- 容量監控方法：保留為「最近」
- 逾時 （選用）

如需此執行區塊所需 IAM 許可的資訊，請參閱 EC2 Auto Scaling 執行區塊範例政策。

4. 選擇儲存步驟。

新增手動核准執行區塊

如需此執行區塊的詳細資訊，請參閱 手動核准執行區塊。

1. 選擇新增步驟。
2. 選取手動核准執行區塊，並將其新增至設計視窗。此區塊允許在繼續之前進行人工驗證。
3. 在右側面板中，設定 區塊：
   - 步驟名稱：輸入「設定前手動核准」
   - 步驟描述 （選用）
   - IAM 核准角色：使用者必須擔任的角色，才能核准執行
   - 逾時 （選用）。逾時後，執行會暫停，您可以選擇重試、略過或取消。

   如需此執行區塊所需 IAM 許可的資訊，請參閱 手動核准執行區塊範例政策。
4. 選擇儲存步驟。

新增維護頁面的自訂動作 Lambda 執行區塊

如需此執行區塊的詳細資訊，請參閱 自訂動作 Lambda 執行區塊。

1. 選擇新增步驟。
2. 選取自訂動作 Lambda 執行區塊，然後選擇新增和編輯。此區塊會在啟用的區域中發佈維護頁面。
3. 在右側面板中，設定 區塊：
   - 步驟名稱：輸入「顯示維護頁面」
   - 步驟描述 （選用）
   - 用於啟用 us-east-1 的 Lambda ARN：部署在 us-east-1 中的維護頁面 Lambda 函數的 ARN

- 用於啟用 us-west-2 的 Lambda ARN：部署在 us-west-2 中的維護頁面 Lambda 函數的 ARN
- 要執行 Lambda 函數的區域：選擇在啟用區域中執行
- 逾時 （選用）
- 重試間隔 （選用）

如需此執行區塊所需 IAM 許可的資訊，請參閱 自訂動作 Lambda 執行區塊範例政策。

4. 選擇儲存步驟。

新增 Aurora 全域資料庫執行區塊

如需此執行區塊的詳細資訊，請參閱 Amazon Aurora 全域資料庫執行區塊。

1. 選擇新增步驟。
2. 選取 Aurora Global Database 執行區塊，然後選擇新增和編輯。此區塊會觸發 Aurora 全域資料庫切換 （不會遺失資料）。如需詳細資訊，請參閱《Aurora 使用者指南》中的使用 Aurora Global Database 的切換或容錯移轉。
3. 在右側面板中，設定 區塊：
   - 步驟名稱：輸入 Aurora 切換
   - 步驟描述 （選用）
   - Aurora 全域資料庫識別符：Aurora 叢集的名稱
   - 用於啟用 us-east-1 的叢集 ARN：us-east-1 中的 Aurora 叢集 ARN
   - 用於啟用 us-west-2 的叢集 ARN：us-west-2 中的 Aurora 叢集 ARN
   - 選取 Aurora 資料庫的選項：選擇切換
   - 逾時 （選用）

   如需此執行區塊所需 IAM 許可的資訊，請參閱 Aurora Global Database 執行區塊範例政策。
4. 選擇儲存步驟。

新增 ARC 路由控制執行區塊

如需此執行區塊的詳細資訊，請參閱 ARC 路由控制執行區塊。

1. 選擇新增步驟。

2. 選取 ARC 路由控制執行區塊，然後選擇新增和編輯。此區塊會執行 DNS 容錯移轉，將流量轉移到被動區域。
3. 在右側面板中，設定 區塊：
   - 步驟名稱：輸入切換 DNS
   - 步驟描述（選用）
   - 用於啟用 us-east-1 的路由控制：選擇新增路由控制
   - 逾時：輸入逾時值。
4. 選擇新增路由控制：
   - 路由控制 ARN：控制 us-east-1 之路由控制的 ARN
   - 路由控制狀態：選擇開啟
5. 再次選擇新增路由控制：
   - 路由控制 ARN：控制 us-west-2 之路由控制的 ARN
   - 路由控制狀態：選擇關閉
6. 選擇儲存。
7. 用於啟用 us-west-2 的路由控制：選擇新增路由控制
8. 選擇新增路由控制：
   - 路由控制 ARN：控制 us-west-2 之路由控制的 ARN
   - 路由控制狀態：選擇開啟
9. 再次選擇新增路由控制：
   - 路由控制 ARN：控制 us-east-1 之路由控制的 ARN
   - 路由控制狀態：選擇關閉
10. 選擇儲存。
11. 選擇儲存步驟。

    如需此執行區塊所需 IAM 許可的資訊，請參閱 ARC 路由控制執行區塊範例政策。
12. 選擇儲存。

步驟 3：執行計畫

1. 在區域切換計劃詳細資訊頁面的右上角，選擇執行。

2. 輸入執行詳細資訊：
   - 選取要啟用的區域。
   - 選取計劃執行模式。
   - （選用）檢視執行步驟。
   - 確認計劃執行。
3. 選擇 開始使用。
4. 您可以在計劃在執行詳細資訊頁面上執行時檢視詳細步驟。您可以查看計劃執行中的每個步驟，包括開始時間、結束時間、資源 ARN 和日誌訊息。

當受損的區域復原後，您可以再次執行計畫（變更您提供的參數）以啟用原始區域，將應用程式操作切換回原始主要區域。

教學課程：設定計畫執行報告自動產生

本教學課程會引導您設定區域切換計畫的計畫執行報告自動產生。報告提供計劃執行的完整 PDF 文件，用於合規目的。

在本教學課程中，您將完成下列步驟：

- 建立報告儲存的 Amazon S3 儲存貯體
- 在區域切換計劃上啟用報告自動產生
- 執行計劃並下載報告

先決條件

開始本教學課程之前，請確認您有下列項目：

- 已設定工作流程的現有區域切換計劃
- 建立 Amazon S3 儲存貯體的許可
- 您計劃的執行 IAM 角色已設定所需的許可。如需詳細資訊，請參閱自動計劃執行報告許可。

步驟 1：建立報告的 Amazon S3 儲存貯體

1. 在 開啟 Amazon S3 主控台https://console.aws.amazon.com/s3/。
2. 選擇建立儲存貯體。

3. 提供下列詳細資訊：
   - 儲存貯體名稱：輸入唯一名稱，例如 `my-region-switch-reports`
   - 封鎖公開存取設定：封鎖所有公開存取 （建議）
   - 儲存貯體版本控制：啟用版本控制 （選用但建議）
   - 預設加密：選取加密。如果使用 SSM-KMS，則 planExecutionRole 需要 s3 儲存貯體預設 CMK 的 kms:Encrypt 和 kms:GenerateDataKey 許可
4. 選擇建立儲存貯體。
5. 請注意要用於下一個步驟的儲存貯體名稱。

步驟 2：在您的計劃上啟用報告自動產生

1. 在 開啟區域切換主控台https://console.aws.amazon.com/route53recovery/regionswitch/home。
2. 選取您要為其設定報告的計劃。
3. 選擇導覽列中的動作，然後選取編輯計劃詳細資訊。
4. 在報告設定區段中，提供下列項目：
   - 選取啟用報告自動產生
   - Amazon S3 URI：選取或輸入您在步驟 1 中建立的儲存貯體 S3 URI
   - 擁有儲存貯體的帳戶 ID：輸入儲存貯體擁有者帳戶 ID
5. 選擇儲存。
6. 等待計劃評估完成。如果有任何組態問題，警告會顯示在計劃詳細資訊頁面上。

步驟 3：執行計畫並下載報告

1. 在計劃詳細資訊頁面上，選擇執行。
2. 照常完成計劃執行，選取要啟用的區域和執行模式。
3. 計畫執行完成後，導覽至執行詳細資訊頁面。
4. 在計劃執行報告區段中，監控報告產生狀態。報告產生通常會在執行完成後 30 分鐘內完成。
5. 當報告狀態顯示已完成時，請選擇下載計劃執行報告以下載 PDF。
6. 或者，導覽至 Amazon S3 儲存貯體以直接存取報告。報告會以下列命名模式儲存：
   `ExecutionReport-${planVersion.ownerAccountId}-${planName}-${execution.regionTo}-${event.executionId}-${dateStr}.pdf`

產生的報告包括：

- 具有服務概觀和報告建立日期的執行摘要
- 規劃執行時存在的組態詳細資訊
- 包含步驟、受影響資源和狀態的詳細執行時間表
- 規劃執行開始時出現的警告
- Amazon CloudWatch 警示狀態和相關警示的警示歷史記錄
- 對於父計畫、子計畫的組態和執行詳細資訊
- 術語和概念詞彙表

疑難排解

如果報告產生失敗，請檢查下列項目：

- 許可錯誤：確認執行角色具有正確的 IAM 許可。如需詳細資訊，請參閱自動計劃執行報告許可。檢查計劃評估警告是否有特定許可問題。
- Amazon S3 儲存貯體存取：確保 Amazon S3 儲存貯體存在，並且可從設定計劃的區域存取。確認儲存貯體政策不會封鎖來自執行角色的存取。
- 儲存貯體加密：如果使用客戶管理的 KMS 金鑰進行儲存貯體加密，請確保執行角色具有使用 KMS 金鑰的許可。

如需其他說明，請在執行詳細資訊頁面上檢視詳細的錯誤訊息，或聯絡 AWS Support。

教學課程：執行 RDS 復原後工作流程

本教學課程會引導您在成功 RDS 容錯移轉後執行復原後工作流程。此復原後執行會透過為 RDS 資料庫重新建立跨區域複寫來還原備援，確保您的 RDS 資料庫已準備好因應未來的區域事件。

在本教學課程中，您將完成下列步驟：

- 驗證復原後執行的先決條件
- 使用 RDS Create Cross-Region Replica 執行區塊建立復原後工作流程
- 執行復原後工作流程

先決條件

開始本教學課程之前，請確認您有下列項目：

- 具有啟用工作流程的區域切換作用中/被動計劃，其中包含 RDS 提升僅供讀取複本執行區塊
- 成功啟用執行，提升其他區域中的僅供讀取複本
- 兩個區域都正常運作且可存取
- 來自最近復原執行的執行 ID

步驟 1：建立復原後工作流程

1. 從區域切換主控台選擇計劃，選擇編輯工作流程、選取組態、勾選在計劃中包含復原後工作流程並儲存。
2. 在編輯工作流程頁面中，選取選取要新增步驟的工作流程下拉式清單，然後選擇復原後。
3. 選擇新增步驟。
4. 選取 Amazon RDS 建立跨區域複本執行區塊。
5. 在右側面板中，設定 區塊：

   - 步驟名稱：輸入「建立跨區域僅供讀取複本」
   - 步驟描述 （選用）
   - 主要區域的 RDS 資料庫執行個體 ARN：主要區域中資料庫的 ARN 應與提升僅供讀取複本步驟相同
   - 次要區域的 RDS 資料庫執行個體 ARN：次要 中提升資料庫的 ARN，應與提升僅供讀取複本步驟相同
   - 逾時 （選用）：輸入逾時值，例如 90 分鐘

   如需此執行區塊所需 IAM 許可的資訊，請參閱 Amazon RDS 執行區塊範例政策。
6. 選擇儲存步驟。
7. 選擇儲存工作流程。

步驟 2：執行復原後工作流程

1. 在區域切換計畫詳細資訊頁面的右上角，選擇執行復原後。
2. 輸入執行詳細資訊：

- 復原執行 ID：輸入最近復原執行的執行 ID。此欄位用於識別目前作用中的區域。
- 要在其中執行的區域：選取未接收任何應用程式流量的非作用中區域。這是將建立僅供讀取複本的區域。

3. 檢閱執行步驟並確認執行。
4. 選擇 Start Execution (開始執行)。
5. 在執行詳細資訊頁面上監控執行進度。RDS Create 跨區域複本執行區塊會重新命名舊的主要執行個體，並在先前受損的區域中建立新的僅供讀取複本。

在復原後執行成功完成之後，您的應用程式將會重新建立跨區域複寫，而您將為未來的區域事件做好準備。您可以檢查目標區域中的 RDS 主控台，以確認是否已建立新的僅供讀取複本。舊的主節點會重新命名並以 renamedByRegionSwitch 標記。

> **Important**
>
> 區域切換會驗證復原執行 ID 是否符合計劃的上次已知執行。如果執行 ID 無效或不是上次已知復原執行的 ID，則不會執行復原後執行。

區域切換 API 操作

下表列出可用於區域切換的 ARC 操作，以及相關文件的連結。

Action	使用 ARC 主控台	使用 ARC API	資料平面 API
核准或拒絕計劃執行步驟	請參閱 手動核准執行區塊	請參閱 ApprovePlanExecutionStep	是
取消計劃執行	請參閱 建立區域切換計畫	請參閱 CancelPlanExecution	是
建立計劃	請參閱 建立區域切換計畫	請參閱 CreatePlan	否
刪除計劃	請參閱 使用區域切換	請參閱 DeletePlan	否
取得計劃	請參閱 使用區域切換	請參閱 GetPlan	否

Action	使用 ARC 主控台	使用 ARC API	資料平面 API
取得計劃評估狀態	請參閱 計畫評估	請參閱 GetPlanEvaluationStatus	是
取得計劃執行	請參閱 區域切換儀表板	請參閱 GetPlanExecution	是
在 區域中取得計劃	請參閱 使用區域切換	請參閱 GetPlanInRegion	是
列出計畫執行事件	請參閱 執行區域切換計劃以復原應用程式	請參閱 ListPlanExecutionEvents	是
列出計畫執行	請參閱 執行區域切換計劃以復原應用程式	請參閱 ListPlanExecutions	是
列出計劃	請參閱 使用區域切換	請參閱 ListPlans	否
列出區域中的計劃	請參閱 使用區域切換	請參閱 ListPlansInRegion	是
列出計劃的 Route 53 運作狀態檢查	請參閱 Amazon Route 53 運作狀態檢查執行區塊	請參閱 ListRoute53HealthChecksForPlan	否
列出區域中計劃的 Route 53 運作狀態檢查	請參閱 Amazon Route 53 運作狀態檢查執行區塊	請參閱 ListRoute53HealthChecksForPlanInRegion	是
列出資源的標籤	請參閱 ARC 區域切換的標記；	請參閱 ListTagsForResource	否
開始計劃執行	請參閱 執行區域切換計劃以復原應用程式	請參閱 StartPlanExecution	是
標記資源	請參閱 建立區域切換計畫	請參閱 TagResource	否

Action	使用 ARC 主控台	使用 ARC API	資料平面 API
從資源移除標籤	請參閱 ARC 區域切換的標記；	請參閱 UntagResource	否
更新計劃	請參閱 建立區域切換計畫	請參閱 UpdatePlan	否
更新計劃執行	請參閱 建立區域切換計畫	請參閱 UpdatePlanExecution	是
更新計劃執行步驟	請參閱 建立區域切換計畫	請參閱 UpdatePlanExecutionStep	是

使用區域切換

本節提供使用區域切換計劃的step-by-step說明，您可以用來復原多區域應用程式。區域切換可讓您為主動/被動和主動/主動復原方法建立計劃。

若要為您的應用程式建立復原計劃，請執行下列動作：

1. 建立區域切換計畫。計劃是具有特定屬性 AWS 區域 的結構，例如您的應用程式執行所在的特定 。每個計劃都包含一或多個工作流程。

   或者，您可以建立數個計劃，並在整體復原計劃中巢狀化這些子計劃。
2. 為計劃建立工作流程。您必須先建立工作流程，才能執行計畫。
3. 在工作流程中，新增一個或多個各為執行區塊的步驟。

   例如，您可以新增步驟來擴展目的地區域中的 EC2 Auto Scaling 群組。
4. 將步驟新增至工作流程後，可能需要其他步驟，例如在 Amazon Route 53 中設定運作狀態檢查。每個執行區塊區段都包含您需要的組態資訊。如需詳細資訊，請參閱新增執行區塊。
5. 若要復原在受損 中執行的應用程式 AWS 區域，請執行 計畫。

   您可以在全域儀表板或區域儀表板中檢視資訊，以追蹤計劃執行的進度。

下列各節提供建立計劃和工作流程，以及在工作流程中新增執行區塊步驟的詳細資訊和步驟。

目錄

- 建立區域切換計畫
- 建立區域切換計畫工作流程
- 新增執行區塊
- 建立子計畫
- 建立區域切換計畫的觸發
- 執行區域切換計劃以復原應用程式

本節中的程序說明如何使用 來使用計劃、工作流程、執行區塊和觸發條件 AWS 管理主控台。若要改為使用區域切換 API 操作，請參閱 區域切換 API 操作。

建立區域切換計畫

您可以在區域切換中建立兩種不同類型的計劃：主動/主動計劃或主動/被動計劃。當您建立計劃時，請指定適用於您要管理容錯移轉方式的類型。

- 主動/被動方法會將兩個應用程式複本部署到兩個區域，其中流量只會路由到作用中區域。您可以執行區域切換計畫，在被動區域中啟用複本。
- 主動/主動方法會將兩個應用程式複本部署到兩個區域，而這兩個複本正在處理工作或接收流量。

建立區域切換計畫

1. 從區域切換主控台中，選擇使用主動/被動方法建立區域切換計劃。
2. 提供下列詳細資訊：
    - 計劃名稱 - 輸入計劃的描述性名稱。
    - 多區域方法 - 選取主動/被動或主動/主動。此方法表示兩個應用程式複本會部署到兩個區域，流量只會路由到作用中區域。您可以執行區域切換計畫，在被動區域中啟用複本。
        - 如果您已將兩個應用程式複本部署到兩個區域，且流量僅路由到作用中區域，請選擇作用中/被動。然後，您可以透過執行指定主動/被動的區域切換計畫，在被動區域中啟用複本。
        - 如果您已將兩個應用程式複本部署到兩個區域，且兩個複本正在處理工作或接收流量，請選擇作用中/作用中。
    - 主要和待命區域 - 為您的應用程式選取主要和待命區域。針對作用中/作用中部署，選取部署複本的區域。
    - 復原時間目標 (RTO) - 輸入所需的 RTO。區域切換會使用此項目來深入了解相較於您想要的 RTO，區域切換計畫執行需要多長時間才能完成。

- IAM 角色 - 提供區域切換的 IAM 角色，以用來執行計劃。如需許可的詳細資訊，請參閱「ARC 中區域切換的 Identity and Access Management」。
- Amazon CloudWatch 警示 - 提供您已使用 Amazon CloudWatch 建立的應用程式運作狀態警示，以指出每個區域中應用程式的運作狀態。區域切換使用這些應用程式運作狀態警示，以協助判斷切換區域以實作復原後的實際復原時間。

  將 CloudWatch 警示新增至區域切換計劃之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱應用程式運作狀態許可的 CloudWatch 警示。
- 自動產生報告 - 或者，為計劃執行啟用自動產生報告。啟用時，區域切換會在每個計劃執行完成後產生全面的 PDF 報告，並將其交付至您指定的 Amazon S3 儲存貯體。提供 Amazon S3 URI 和擁有儲存貯體的帳戶 ID。

  為計劃啟用自動產生報告之前，請確定您已備妥正確的 IAM 政策。如需報告產生和所需許可的詳細資訊，請參閱 自動計劃執行報告。
- 標籤 - 或者，將一或多個標籤新增至您的計劃。

建立區域切換計畫工作流程

建立區域切換計劃之後，您需要定義和建立工作流程，以指定應用程式的復原程序。對於每個計劃，您可以定義一或多個工作流程，以完成應用程式的復原。在每個工作流程中，您新增包含執行區塊的步驟，以定義您希望區域切換為應用程式復原執行的每個動作。

您建立的工作流程數量取決於您的應用程式部署案例，以及管理復原的偏好設定。例如：

- 如果您的區域切換計劃適用於作用中/作用中的應用程式部署，您也需要建立停用工作流程。這表示對於 或作用中/作用中部署，您至少有兩個工作流程：啟用工作流程和停用工作流程。
- 如果您的區域切換計劃用於主動/被動應用程式部署，則您有一個主要和次要區域。如果您選擇為每個區域建立個別的啟用工作流程，您將建立兩個工作流程：每個區域一個。

建立區域切換計畫工作流程

1. 在您建立的區域切換計畫中，選擇建置工作流程。
2. 選取下列其中一個工作流程選項：
   - 為所有區域建置相同的啟用工作流程 - 可讓您跨區域使用相同的啟用工作流程。
   - 為每個區域分別建立工作流程 - 為每個區域建立個別啟用工作流程。
3. 或者，提供每個工作流程的描述。

4. 定義復原應用程式所需的工作流程。在工作流程中，您可以新增執行區塊，以定義您希望區域切換為復原執行的步驟。每個執行區塊都會定義動作，例如應用程式流量重新路由或啟用區域中的資料庫復原，並支援另一個區域中的資源 AWS 帳戶。您可以選擇讓執行區塊平行或循序執行。如需可新增至工作流程之特定執行區塊的詳細資訊，請參閱 新增執行區塊。
5. 根據您選取的工作流程選項，執行下列動作：

   - 如果您選擇為所有區域建立相同的啟用工作流程，則需要一個啟用工作流程。
   - 如果您為每個區域分別選取建置工作流程，則需要兩個啟用工作流程。

   對於作用中/作用中計劃，您必須同時定義啟用工作流程和停用工作流程。

新增執行區塊

您可以將步驟新增至區域切換計畫中的工作流程，以執行個別步驟來完成應用程式的容錯移轉或切換。如需每種執行區塊的功能和行為詳細資訊，請參閱下列說明。

區域切換會在您建立計畫或更新計畫後立即執行計畫評估，然後在穩定狀態期間每 30 分鐘執行一次。區域切換會將計劃評估的相關資訊儲存在設定計劃的所有區域中。此處的每個執行區塊區段都包含區域切換執行計劃評估時評估項目的相關資訊。

區域切換包含執行區塊類型，有助於在復原過程中擴展運算資源。如果您在計劃中使用這些執行區塊，請注意區域切換不保證達到所需的運算容量。如果您有重要的應用程式且需要保證存取容量，建議您預留容量。您可以遵循一些策略，在次要區域中保留運算容量，同時限制成本。若要進一步了解，請參閱具有預留容量的指示燈：如何使用隨需容量預留最佳化 DR 成本。

區域切換支援下列執行區塊。

執行區塊	函式	不平穩的組態
ARC 區域切換計畫執行區塊	透過指定要執行的子計畫，在一個執行中協調多個應用程式的復原。	使用其不良組態啟動子計劃。
Amazon EC2 Auto Scaling 群組執行區塊	在計畫執行過程中擴展 Auto Scaling 群組中的 EC2 運算資源。	指定在您啟用的區域中應相符的運算容量百分比下限。
Amazon EKS 資源擴展執行區塊	在計畫執行過程中擴展 Amazon EKS 叢集 Pod。	N/A

執行區塊	函式	不平穩的組態
Amazon ECS 服務擴展執行區塊	在計畫執行過程中擴展 Amazon ECS 服務任務。	N/A
ARC 路由控制執行區塊	新增步驟以變更一或多個 ARC 路由控制的狀態，將應用程式流量重新導向至目標 AWS 區域。	N/A
Amazon Aurora 全域資料庫執行區塊	執行 Aurora 全域資料庫的復原工作流程。	執行 Aurora 全域資料庫容錯移轉（可能導致資料遺失）。
Amazon DocumentDB 全域叢集執行區塊	執行 Amazon DocumentDB 全域叢集的復原工作流程。	執行 Amazon DocumentDB 全域叢集容錯移轉（可能導致資料遺失）。
Amazon RDS 升級僅供讀取複本執行區塊	將 Amazon RDS 僅供讀取複本提升為獨立資料庫執行個體。	N/A
Amazon RDS 建立跨區域複本執行區塊	在復原後為 Amazon RDS 資料庫執行個體建立跨區域僅供讀取複本。	N/A
手動核准執行區塊	插入核准步驟，以要求核准或取消執行，然後再繼續。	N/A
自訂動作 Lambda 執行區塊	新增執行 Lambda 函數的自訂步驟，以啟用自訂動作。	略過 步驟。
Amazon Route 53 運作狀態檢查執行區塊	指定在容錯移轉期間將應用程式流量重新導向至的區域。	N/A

ARC 區域切換計畫執行區塊

區域切換計畫執行區塊可讓您透過參考其他子區域切換計畫，協調多個應用程式切換到您要啟用之區域的順序。使用此父/子關係，您可以建立複雜的協調復原程序，以跨基礎設施管理多個資源和相依性。

Configuration

當您使用區域切換計畫執行區塊時，請選取您想要在所建立計畫工作流程中執行的特定區域切換計畫。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱區域切換計畫執行區塊範例政策。

若要設定區域切換計畫執行區塊，請輸入下列值：

1. 步驟名稱：輸入名稱。
2. 步驟描述（選用）：輸入步驟的描述。
3. 區域切換計劃：選取要在目前計劃的工作流程中執行的計劃。

然後，選擇儲存步驟。

運作方式

使用區域切換計畫執行區塊，建立具有父/子關係的父工作流程。請注意，此執行區塊不支援其他層級的子計畫，並限制父子計畫的數量。子計畫必須支援父計畫支援的相同區域，且必須與父計畫具有相同的復原方法（即主動/主動或主動/被動）。

此區塊同時支援正常和不良的執行模式。不寬容的設定將使用其不寬容的組態啟動子計畫。如果區域切換區塊已正常執行，然後切換到不恢復的執行模式，則任何子計畫也會切換到不恢復的執行模式。

做為計畫評估的一部分而評估的內容

如果您跨帳戶共用計劃，且計劃不再與父計劃的帳戶共用，區域切換評估會傳回計劃無效的警告。

Amazon EC2 Auto Scaling 群組執行區塊

EC2 Auto Scaling 群組執行區塊可讓您在多區域復原程序中擴展 EC2 執行個體。您可以定義相對於您要離開的區域（來源和目的地）的容量百分比。

Configuration

當您設定 EC2 Auto Scaling 群組執行區塊時，您可以為與您的計劃相關聯的特定區域輸入 EC2 Auto Scaling ARNs。您應該在計劃執行期間要向上擴展的每個區域中輸入 EC2 Auto Scaling ARNs。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱EC2 Auto Scaling 執行區塊範例政策。

若要設定 EC2 Auto Scaling 群組執行區塊，請輸入下列值：

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 區域的 EC2 Auto Scaling 群組 ARN：輸入您計劃的每個區域中 EC2 Auto Scaling 群組的 ARN。
4. 符合啟用區域容量的百分比：輸入 Auto Scaling 群組中執行中執行個體數量的所需百分比，以符合啟用的區域。
5. 容量監控方法：選取下列其中一種方法來監控 EC2 Auto Scaling 群組的容量：
   - 24 小時內取樣的最大執行容量：選擇此選項可使用 EC2 Auto Scaling 群組組態中指定的所需容量值。此選項不會建立額外的成本，但可能比使用另一個選項 CloudWatch 指標更不準確。

     在區域切換 API 中，此選項對應於指定 `sampledMaxInLast24Hours`。

     如需詳細資訊，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的設定 Auto Scaling 群組的擴展限制。 Auto Scaling
   - 使用 CloudWatch 在 24 小時內取樣的最大執行容量：選擇此選項可使用 Amazon CloudWatch for EC2 Auto Scaling 中指定的指標。使用 選項可以更準確，但使用 CloudWatch 指標會產生額外的成本。

     在區域切換 API 中，此選項對應於指定 `autoscalingMaxInLast24Hours`。

     若要使用此選項，您必須先啟用 Auto Scaling 群組的群組指標。如需詳細資訊，請參閱《Amazon EC2 Auto Scaling 使用者指南》中的啟用 Auto Scaling 群組指標。 Auto Scaling
6. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

設定 EC2 Auto Scaling 執行區塊之後，區域切換會確認只有一個來源 Auto Scaling 群組和一個目的地 Auto Scaling 群組。如果有多個 Auto Scaling 群組，則執行區塊會在計劃評估期間失敗。目標容量定義為執行個體數量的狀態設為 `InService`。如需詳細資訊，請參閱 EC2 Auto Scaling 執行個體生命週期。

區域開關會根據您為相符百分比指定的值（當您設定 Auto Scaling 執行區塊時），計算目的地 Auto Scaling 群組的新所需容量。新的所需容量會與目的地 Auto Scaling 群組所需的容量進行比較。區域切換用於計算所需容量的公式如下：`ceil(percentToMatch * Source Auto Scaling group capacity)`，其中 ceil() 是四捨五入任何分數結果的函數。如果目的地 Auto Scaling 群組的目前所需容量大於或等於區域切換所計算之新 Auto Scaling 群組的所需容量，則執行區塊會繼續。請注意，區域切換不會縮減 Auto Scaling 群組容量。

當區域切換執行 Auto Scaling 區塊時，區域切換會嘗試擴展目標區域 Auto Scaling 群組容量，以符合所需的容量。然後，區域切換會等到目標區域的 Auto Scaling 群組中滿足請求的 Auto Scaling 群組容量，區域切換才會繼續進行計劃的下一個步驟。

> **Note**
>
> 執行此區塊會修改 Auto Scaling 群組的最小和所需容量設定，如果您透過infrastructure-as-code工具或其他自動化管理這些值，可能會導致組態偏離。確保您的組態管理程序考慮這些變更，以防止意外轉返。

如果您使用主動/主動方法，區域切換會使用其他設定的 區域做為來源。也就是說，如果某個區域正在停用，區域切換會使用另一個作用中區域做為來源，以符合要擴展的百分比。

此區塊同時支援正常和不良的執行模式。您可以指定目標區域中要比對的運算容量百分比下限，然後區域切換才能繼續計劃中的下一個步驟，以設定不良執行。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 EC2 Auto Scaling 群組執行區塊組態和許可執行數個關鍵檢查。區域切換評估會驗證兩個區域中都存在 Auto Scaling 群組，確保它們設定正確且可存取，並記下每個區域中執行中的執行個體數目。它也會確認目標區域的 Auto Scaling 群組中的最大容量足以處理所需容量的指定比例比對百分比。

區域切換也會驗證計劃的 IAM 角色是否具有 Auto Scaling 的正確許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。如果任何檢查失敗，區域開關會傳回警告訊息，您可以在 主控台中檢視。或者，您可以透過 EventBridge 或使用 API 操作來接收驗證警告。

Amazon EKS 資源擴展執行區塊

EKS 資源擴展執行區塊可讓您在多區域復原程序中擴展 EKS 資源。當您設定執行區塊時，您可以定義要擴展的容量百分比，相對於要停用區域中的容量。

設定 EKS 存取項目許可

在新增 EKS 資源擴展的步驟之前，您必須向區域交換器提供必要的許可，以對 EKS 叢集中的 Kubernetes 資源採取動作。若要提供區域切換的存取權，您必須使用下列區域切換存取政策，為區域切換用於計劃執行的 IAM 角色建立 EKS 存取項目： `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

區域切換 EKS 存取政策

以下資訊提供有關 EKS 存取政策的詳細資訊。

名稱: `AmazonARCRegionSwitchScalingPolicy`

政策 ARN： `arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy`

Kubernetes API 群組	Kubernetes 資源	Kubernetes 動詞 (許可)
*	*/scale	get、更新
*	*/狀態	get
自動擴展	horizontalpodautoscaler	get、修補

建立區域切換的 EKS 存取項目

下列範例說明如何建立所需的存取項目和存取政策關聯，讓區域切換可以為您的 Kubernetes 資源採取特定動作。在此範例中，許可適用於 IAM 角色 的 EKS 叢集 my-*cluster ###### my-namespace1*arn:aws:iam::555555555555:role/*my-role*。

當您設定這些許可時，請務必針對執行區塊中的兩個 EKS 叢集採取這些步驟。

先決條件

開始之前，請將叢集的身分驗證模式變更為 API_AND_CONFIG_MAP或 API。變更授權模式會新增存取項目的 API。如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的變更身分驗證模式以使用存取項目。

建立存取項目

第一步是使用類似下列的 AWS CLI 命令來建立存取項目：

```
aws eks create-access-entry --cluster-name my-cluster --principal-arn
        arn:aws:iam::555555555555:user/my-user --type STANDARD
```

如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的建立存取項目。

建立存取項目關聯

接著，使用類似以下的 AWS CLI 命令建立與區域切換存取政策的關聯：

```
aws eks associate-access-policy --cluster-name my-cluster --principal-arn
 arn:aws:iam::555555555555:role/my-role \
         --access-scope type=namespace,namespaces=my-namespace1 --policy-arn
         arn:aws:eks::aws:cluster-access-policy/AmazonARCRegionSwitchScalingPolicy
```

如需詳細資訊，請參閱《Amazon EKS 使用者指南》中的將存取政策與存取項目建立關聯。

請務必在另一個區域的執行區塊中對第二個 EKS 叢集重複這些步驟，以確保兩個叢集都可以由區域切換存取。

Configuration

> **Important**
>
> 在新增 EKS 資源擴展步驟之前，請先確定您已設定正確的許可。如需詳細資訊，請參閱設定 EKS 存取項目許可。此外，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Amazon EKS 資源擴展執行區塊範例政策。

請注意，區域切換目前支援下列 ReplicaSet 資源：app/v1、Deplation 和 app/v1。

針對執行區塊組態，輸入下列值。

1. 步驟名稱：輸入名稱。
2. 步驟描述（選用）：輸入步驟的描述。
3. 應用程式名稱：輸入 EKS 應用程式的名稱，例如 myApplication。
4. Kubernetes 資源類型：輸入應用程式的資源類型，例如部署。
5. 區域資源：針對每個區域，輸入 EKS 叢集的資訊，包括 EKS 叢集 ARN、資源命名空間等。
6. 符合啟用區域容量的百分比：輸入在來源區域中執行 Pod 在啟用區域中符合的所需百分比。
7. 容量監控方法：已選取容量監控的唯一選項，在 24 小時內取樣的最大執行容量。

   此容量監控方法使用 EKS 服務請求`ReplicaCount`的值。如需詳細資訊，請參閱《Amazon Elastic Kubernetes Service 使用者指南》中的了解 Amazon EKS 中的 ARC 區域轉移。
8. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

在計劃執行期間，區域切換會擷取您啟動之區域中目標資源過去 24 小時內取樣的複本數量上限。然後，它會使用以下公式計算目的地資源所需的複本計數： `ceil(percentToMatch * Source replica count)`

如果目的地就緒複本計數低於所需的值，區域開關會將目的地資源複本值擴展為所需的容量。它會等待複本準備就緒，並在必要時利用您的節點自動擴展器來增加節點容量。

如果選用`hpaName`欄位不是空的，區域切換會使用下列修補程式來修補 HorizontalPodAutoscaler，以防止執行期間或之後的任何自動縮減規模： `{"spec":{"behavior":{"scaleDown":{"selectPolicy":"Disabled"}}}}`

請務必設定任何偏離校正工具，例如 GitOps 工具，以忽略修補程式中資源的複本欄位，以及 HorizontalPodAutoscaler 欄位。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對設定的 EKS 執行區塊和許可執行數項檢查。區域切換會驗證計劃的 IAM 角色是否具有描述 EKS 叢集和列出相關存取項目政策的正確許可。區域切換也會驗證 IAM 角色是否與正確的存取項目政策相關聯，以便區域切換具有對 Kubernetes 資源採取行動所需的許可。最後，區域切換會確認設定的 EKS 叢集和 Kubernetes 資源是否存在。

此外，區域切換會檢查其是否已成功收集並存放必要的監控資料 (Kubernetes 複本計數），並擷取執行區域切換計畫所需的執行中 Pod 數量。

Amazon ECS 服務擴展執行區塊

ECS 服務擴展執行區塊可讓您在多區域復原程序中擴展目的地區域中的 ECS 服務。您可以定義容量百分比，相對於區域切換從 容錯移轉或停用的區域。

Configuration

若要設定 ECS 服務擴展執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Amazon ECS 服務擴展執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 區域資源：針對每個區域，輸入 ECS 叢集 ARN 和 ECS 服務 ARN。
4. 符合來源區域任務計數的百分比：輸入來源區域中要符合的所需執行中任務百分比。
5. 容量監控方法：選取下列其中一種方法來監控 Amazon ECS 的容量：
   - 24 小時內取樣的最大執行中容量：選擇此選項可在 Amazon ECS 服務中使用執行中的任務計數值。此選項不會建立額外的成本，但可能比使用另一個選項 CloudWatch 指標更不準確。

     在區域切換 API 中，此選項對應於指定 `sampledMaxInLast24Hours`。

     如需詳細資訊，請參閱《Amazon Elastic Container Service 開發人員指南》中的自動擴展 Amazon ECS 服務。
   - 透過容器洞察在 24 小時內取樣的最大執行容量：選擇此選項以使用 Amazon ECS Container Insights 指標。使用 選項可以更準確，但使用 Container Insights 會產生額外的成本。

     在區域切換 API 中，此選項對應於指定 `autoscalingMaxInLast24Hours`。

     若要使用此選項，您必須先啟用 Container Insights。如需詳細資訊，請參閱《Amazon CloudWatch 使用者指南》中的設定容器洞見。
6. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

在計劃中設定執行區塊後，區域切換會確認只有一個來源 ECS 服務和一個目的地服務。如果有多個服務，區域開關會傳回執行區塊的警告。區域切換會將此資料存放在您計劃設定的所有區域中。目標容量定義為 ECS 服務上設定的所需計數。

對於主動/被動方法，區域切換會計算目的地 （啟用） 區域中 ECS 服務的新所需容量。新的所需容量會與目的地 ECS 服務的所需容量進行比較。區域切換用於計算所需容量的公式如下：`ceil(percentToMatch * Source Auto Scaling group capacity)`，其中 ceil() 是四捨五入任何分數結果的函數。如果目的地 ECS 服務的目前所需計數高於 ECS 服務的計算新所需容量，則計劃執行會繼續進行。請注意，區域切換不會縮減 ECS 服務容量。

如果 ECS 服務已啟用 Application Autoscaling，區域切換會更新 Application Autoscaling 中的最小容量，也會更新 ECS 服務中所需的計數。

當區域切換執行 ECS 服務區塊時，區域切換會嘗試擴展目標區域 ECS 容量，以符合所需的容量。然後，區域切換會等到目標區域的 ECS 服務中滿足請求的 ECS 服務容量，區域切換才會繼續進行計劃的下一個步驟。如果您願意，您可以透過設定區域切換等待容量履行的逾時限制，將步驟設定為在履行完成之前完成。

如果您使用主動/主動方法，區域切換會使用其他設定的 區域做為來源。也就是說，如果某個區域正在停用，區域切換會使用另一個作用中區域做為來源，以符合要擴展的百分比。

做為計畫評估一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 ECS 服務執行區塊組態和許可執行數項檢查。區域切換會驗證來源和目標區域中是否存在 ECS 服務，並檢查以確保目標區域的 ECS 服務所設定的最大容量足以處理目標區域容量的指定百分比相符。區域切換也會驗證計劃的 IAM 角色是否具有 ECS 服務的正確許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

此外，區域切換會檢查 `ResourceMonitor` 是否已成功收集並儲存 ECS 服務的必要監控資料，並擷取執行中任務的計數。

如果任何檢查失敗，區域開關會傳回警告訊息，您可以在 主控台中檢視。或者，您可以透過 EventBridge 或使用 API 操作來接收驗證警告。

ARC 路由控制執行區塊

如果您已為應用程式設定 Amazon Application Recovery Controller (ARC) 路由控制，您可以新增 ARC 路由控制步驟來重新導向應用程式流量。此步驟可讓您變更一或多個 ARC 路由控制的狀態，將應用程

式流量重新導向至目的地 AWS 區域。ARC 路由控制會使用 Amazon Route 53 中的運作狀態檢查來重新導向流量，這些運作狀態檢查是以與路由控制相關聯的 DNS 記錄所設定。

> **Important**
>
> Amazon Application Recovery Controller (ARC) 路由控制僅適用於 AWS 商業分割區。

Configuration

若要設定路由控制執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱ARC 路由控制執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 所需的路由控制：針對您要啟用或停用的每個區域，輸入路由控制 ARN 和路由控制的初始狀態，開啟或關閉。
4. 逾時：輸入逾時值。

然後，選擇儲存步驟。

此執行區塊的預期模式是指定路由控制和初始狀態，以符合您在特定 中設定應用程式的方式 AWS 區域。例如，如果您的計劃可讓您為應用程式啟用區域 A 和區域 B，則您可能擁有區域 A 的路由控制，其中您將狀態設定為開啟，而將狀態設定為開啟的區域 B 的路由控制。

然後，當您執行計畫並指定您想要啟用區域 A 時，包含此執行區塊的工作流程會將指定的路由控制更新為開啟，這會將流量導向區域 A。

運作方式

透過設定 ARC 路由控制執行區塊，您可以將應用程式流量重新路由到目的地， AWS 區域或者，對於主動/主動方法，停止流量路由到您停用的區域。如果您的計劃包含多個工作流程，請確定您為所使用的所有路由控制執行區塊提供相同的 DNS 記錄輸入。

此區塊不支援不良執行模式。

做為計畫評估一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對路由控制執行區塊組態和許可執行數項檢查。區域切換會驗證指定的路由控制是否已正確設定並可存取。

區域切換也會驗證計劃的 IAM 角色具有存取和更新路由控制狀態所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於路由控制執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，擁有必要的存取權來管理和與 ARC 路由控制互動。

比較 ARC 路由控制和 Route 53 運作狀態檢查執行區塊

區域切換中的 Amazon Route 53 運作狀態檢查執行區塊為 DNS 型流量管理提供了成本較低的替代方案。不過，此執行區塊取決於 AWS 區域 您正在啟用的 ，因此 區域必須可用。這符合大多數客戶的需求，因為他們正在啟用運作狀態良好的區域。

ARC 路由控制提供高度可靠的 DNS 型流量管理，具有 100% 的可用性 SLA。透過路由控制，您的營運團隊可以使用安全防護機制在區域之間轉移流量。路由控制提供具有 100% SLA 的單一租戶解決方案。路由控制叢集分散在五個區域，可以容忍兩個區域離線。如果您有高度關鍵的應用程式，請考慮使用路由控制。

使用區域切換不需要路由控制。您可以使用區域切換來管理流量重新導向，方法是使用 Route 53 運作狀態檢查執行區塊，無需路由控制。

在下列情況中，路由控制會使用區域切換新增值：

- 您需要流量控制機制本身的 100% 可用性 SLA。
- 您的組織需要具有關鍵應用程式安全規則的手動操作控制。
- 您想要defense-in-depth，以便營運團隊可以視需要手動覆寫自動流量路由。

Route 53 運作狀態檢查執行區塊不依賴於控制平面。運作狀態檢查記錄變更使用資料平面，因此不需要啟用區域來處理組態更新。在下列情況中，Route 53 運作狀態檢查執行區塊已足夠：

- 您的應用程式可以取決於您正在啟用 AWS 區域 的 。
- 在復原工作流程中，自動流量重新導向符合您的需求。
- 成本最佳化是優先事項。Route 53 運作狀態檢查執行區塊的成本低於路由控制。

大多數客戶從 Route 53 運作狀態檢查執行區塊開始，做為預設流量路由機制，並僅為需要最高流量管理機制可靠性的最關鍵應用程式新增路由控制。

Amazon Aurora 全域資料庫執行區塊

Amazon Aurora 全域資料庫執行區塊可讓您執行全域資料庫的容錯移轉或切換復原工作流程。

- 容錯移轉 - 使用此方法從意外中斷的情況復原。使用此方法，您可以對 Aurora 全域資料庫中的其中一個次要資料庫叢集執行跨區域容錯移轉。此方法的復原點目標 (RPO) 通常是以秒為單位測量的非零值。資料遺失量取決於發生故障 AWS 區域 時跨 的 Aurora 全域資料庫複寫延遲。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的從意外中斷復原 Amazon Aurora 全域資料庫。
- 切換 – 此操作先前稱為受管計劃容錯移轉。將此方法用於受控案例，例如操作維護和其他計劃的操作程序，其中與其互動的所有 Aurora 叢集和其他服務都處於良好狀態。由於此功能會將次要資料庫叢集與主要資料庫叢集同步處理，再做出任何其他變更，因此 RPO 為 0 (不會遺失資料)。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的執行 Amazon Aurora 全域資料庫的切換。

Configuration

若要設定 Aurora Global Database 執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Aurora Global Database 執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. Aurora Global Database 叢集名稱：輸入全域資料庫的識別符。
4. 區域的叢集 ARN：輸入要在計劃中每個區域中使用的叢集 ARN。
5. 指定 Aurora 資料庫的選項：根據您想要的方式選擇切換或容錯移轉 （資料遺失 ）
6. Aurora Global Database 叢集名稱：
7. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

透過設定 Aurora Global Databases 執行區塊，您可以在應用程式復原過程中容錯移轉或切換全域資料庫。如果您使用主動/主動方法，區域切換會使用其他設定的 區域做為來源。也就是說，如果某個區域正在停用，區域切換會使用另一個作用中區域做為來源，以符合要擴展的百分比。

此區塊同時支援正常和不良的執行模式。不穩健的設定會執行 Aurora 全域資料庫容錯移轉，這可能會導致資料遺失。

如需 Aurora Global Database 災難復原的詳細資訊，包括容錯移轉和切換，請參閱《Amazon Aurora 使用者指南》中的在 Amazon Aurora 全域資料庫中使用切換或容錯移轉。

做為計畫評估一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Aurora 執行區塊組態和許可執行數項檢查。區域切換會驗證下列項目是否正確：

- 組態中指定的 Aurora 全域叢集存在。
- 來源和目的地區域都有 Aurora 資料庫叢集。
- 來源和目的地資料庫叢集處於允許全域資料庫切換的狀態。
- 來源和目的地叢集都有資料庫執行個體
- 切換動作的全域叢集引擎版本相容。這包括驗證叢集是否位於相同的主要、次要和修補程式版本，但 Aurora 文件中列出一些例外狀況。

區域切換也會驗證計劃的 IAM 角色具有 Aurora 容錯移轉和切換所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於 Aurora 執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，擁有必要的存取權來管理和與 Aurora 互動。

Amazon DocumentDB 全域叢集執行區塊

Amazon DocumentDB 全域叢集執行區塊可讓您執行全域叢集的容錯移轉或切換復原工作流程。

- 容錯移轉 - 使用此方法從意外中斷的情況復原。使用此方法，您可以對 Amazon DocumentDB 全域叢集中的其中一個次要叢集執行跨區域容錯移轉。此方法的復原點目標 (RPO) 通常是以秒為單位測量的非零值。資料遺失量取決於故障 AWS 區域 時跨 的 Amazon DocumentDB 全域叢集複寫延遲。

- 切換 – 將此方法用於受控案例，例如操作維護和其他計劃的操作程序，其中所有 Amazon DocumentDB 叢集都處於良好狀態。由於此功能會在進行任何其他變更之前，先同步次要叢集與主要叢集，因此 RPO 為 0（不會遺失資料）。

Configuration

若要設定 Amazon DocumentDB 全域叢集執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Amazon DocumentDB 全域叢集執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述（選用）：輸入步驟的描述。
3. Amazon DocumentDB 全域叢集識別符：輸入全域叢集的識別符。
4. 區域的叢集 ARN：輸入要在計劃中每個區域中使用的叢集 ARN。
5. 指定 Amazon DocumentDB 叢集的選項：選擇切換或容錯移轉（資料遺失）。
6. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

透過設定 Amazon DocumentDB 全域叢集執行區塊，您可以在應用程式復原過程中容錯移轉或切換全域叢集。如果您使用主動/主動方法，區域切換會使用其他設定的 區域做為來源。也就是說，如果某個區域正在停用，區域切換會使用另一個作用中區域做為來源，以符合要擴展的百分比。

此區塊同時支援正常和不良的執行模式。不穩健的設定會執行 Amazon DocumentDB 全域叢集容錯移轉，這可能會導致資料遺失。

在切換或容錯移轉操作期間，客戶用來寫入的 DNS 端點將會變更。客戶負責確保他們在操作完成後使用正確的端點。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Amazon DocumentDB 執行區塊組態和許可執行數項檢查。區域切換會驗證下列項目是否正確：

- 組態中指定的 Amazon DocumentDB 全域叢集存在。
- 來源和目的地區域都有 Amazon DocumentDB 叢集。
- 來源和目的地叢集處於可用狀態。
- 來源和目的地叢集中都有執行個體。
- 全域叢集引擎版本相容。

區域切換也會驗證計劃的 IAM 角色具有 Amazon DocumentDB 容錯移轉和切換所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於 Amazon DocumentDB 執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，擁有必要的存取權來管理和與 Amazon DocumentDB 互動。

Amazon RDS 升級僅供讀取複本執行區塊

Amazon RDS 升級僅供讀取複本執行區塊可讓您將 Amazon RDS 僅供讀取複本提升為獨立資料庫執行個體，做為多區域復原程序的一部分。這可讓您將該區域中的僅供讀取複本提升為新的主要資料庫，以容錯移轉至運作狀態良好的區域。

Configuration

若要設定 Amazon RDS Promote 僅供讀取複本執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Amazon RDS 執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 區域的 RDS 資料庫執行個體 ARN：輸入計劃中每個區域中僅供讀取複本的資料庫執行個體 ARN。
4. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

透過設定 Amazon RDS 提升僅供讀取複本執行區塊，您可以將僅供讀取複本提升為獨立資料庫執行個體，做為應用程式復原的一部分。當您執行計劃時，區域切換會提升您正在啟用的區域中的僅供讀取複本，以成為獨立的資料庫執行個體。

> **Note**
>
> 此區塊僅支援主動/被動計劃

在提升期間，您用來連線至資料庫的 DNS 端點將保持不變。不過，提升的執行個體將不再從原始主要資料庫複寫。您有責任確保其應用程式已設定為在操作完成後使用正確的端點。

提升後，提升的執行個體會從原始主要執行個體繼承下列備份設定：

- Backup retention period (備份保留期間)
- 偏好的備份時段

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Amazon RDS 執行區塊組態和許可執行數項檢查。區域切換會驗證下列項目是否正確：

- 組態中指定的 Amazon RDS 資料庫執行個體存在。
- 非主要區域中的資料庫執行個體是僅供讀取複本。
- 僅供讀取複本處於可用狀態。
- 資料庫執行個體已正確設定為跨區域複寫。

區域切換也會驗證計劃的 IAM 角色具有 Amazon RDS 僅供讀取複本提升所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於 Amazon RDS 執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，具有必要的存取權來管理和與 Amazon RDS 互動。

Amazon RDS 建立跨區域複本執行區塊

Amazon RDS Create 跨區域複本執行區塊可讓您在復原後程序中為 Amazon RDS 資料庫執行個體建立跨區域僅供讀取複本。此執行區塊通常會在提升僅供讀取複本以重新建立跨區域複寫之後使用，確保您的應用程式已準備好因應未來的區域事件。

Configuration

若要設定 Amazon RDS Create 跨區域複本執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Amazon RDS 執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述（選用）：輸入步驟的描述。
3. 區域的來源資料庫執行個體 ARN：輸入計劃中每個區域中來源資料庫的資料庫執行個體 ARN。執行區塊會使用啟動做為來源資料庫之區域的識別符，來建立跨區域僅供讀取複本。
4. 複本資料庫執行個體 ARN：輸入要用於新僅供讀取複本的執行個體 ARN。
5. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

透過設定 Amazon RDS Create 跨區域複本執行區塊，您可以在其他區域中建立僅供讀取複本，做為復原後程序的一部分。此執行區塊旨在成功容錯移轉後執行，以重新建立跨區域複寫。

此區塊只能新增至作用中/被動計劃。

在執行期間，舊的主要執行個體將重新命名並以 renamedByRegionSwitch 標記。然後，將使用從舊主要節點複製的下列設定建立新的僅供讀取複本執行個體：

- 執行個體識別碼
- 資料庫參數群組
- 資料庫子網路群組

- KMS 金鑰
- VPC security groups (VPC 安全群組)
- 選項群組
- 多可用區組態
- 網域身分驗證秘密 ARN

> **Important**
>
> 重新命名的主要執行個體會保持執行狀態並繼續產生費用。區域切換會將其標記為 renamedByRegionSwitch 以進行識別，但不會以其他方式修改或刪除。您負責管理重新命名的執行個體，包括決定是否讓執行個體持續執行、停止執行個體，或根據您的營運和成本需求將其刪除。

> **Note**
>
> 此執行區塊專為復原後工作流程而設計，需要來源區域正常運作且可存取。應該在成功容錯移轉後使用，以重新建立跨區域複寫。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Amazon RDS 執行區塊組態和許可執行數項檢查。區域切換會驗證下列項目是否正確：

- 組態中的資料庫執行個體 ARNs 有效且格式正確。
- 來源資料庫執行個體存在於其各自的 區域中。
- 來源資料庫執行個體處於可用狀態。

區域切換也會驗證計劃的 IAM 角色具有建立 Amazon RDS 僅供讀取複本所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於 Amazon RDS 執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，具有必要的存取權來管理和與 Amazon RDS 互動。

手動核准執行區塊

手動核准執行區塊可讓您插入與 IAM 角色相關聯的核准步驟。具有角色存取權的使用者可以核准或拒絕執行步驟、暫停步驟，直到授予核准，或可能阻止計畫進行。

為了確保在計劃執行期間需要手動核准，您可以在工作流程中的特定位置輸入手動核准步驟，然後設定 IAM 角色以指定誰可以核准該步驟。

Configuration

若要設定手動核准執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱手動核准執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. IAM 核准角色：為具有許可的 IAM 角色輸入 ARN，以手動核准繼續區域切換計劃的執行。IAM 角色必須位於計劃擁有者的帳戶內。
4. 逾時：輸入逾時值。

然後，選擇儲存步驟。

運作方式

透過設定手動核准執行區塊，您可以在應用程式復原期間要求核准。對於手動執行區塊，區域切換會執行下列動作：

- 當區域切換執行手動執行區塊時，它會暫停執行，並將計劃的執行狀態設定為待核准。
- 有權存取執行區塊中定義之角色的任何人都可以核准或拒絕執行該步驟。
- 如果他們核准步驟執行，區域切換會繼續執行計畫。如果他們拒絕，區域切換會取消計劃執行。

此區塊不支援不良執行模式。

作為計畫評估的一部分而評估的內容

區域切換不會完成手動核准執行區塊的任何評估。

自訂動作 Lambda 執行區塊

自訂動作 Lambda 執行區塊可讓您使用 Lambda 函數將自訂步驟新增至計劃。

Configuration

若要設定 Lambda 執行區塊，請輸入下列值。

> **Important**
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱自訂動作 Lambda 執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 啟用或停用區域時要叫用的 Lambda 函數 ARN：指定要在此步驟執行的 Lambda 函數 ARN。
4. 要執行 Lambda 函數的區域：在下拉式功能表中，選擇要執行 Lambda 函數的區域。
5. 逾時：輸入逾時值。
6. 重試間隔：輸入重試間隔，如果在此間隔內未成功，則重新執行 Lambda 函數。

然後，選擇儲存步驟。

運作方式

- 當您建立自訂動作 Lambda 執行區塊時，您需要為要執行的步驟指定兩個 Lambda 函數，每個計劃的區域各一個。
- 您可以設定您希望 Lambda 在哪個區域中執行，例如在啟用區域或停用區域中。不過，如果您在停用區域中執行 ，則需依賴該區域。我們不建議您對停用區域採取相依性。

此區塊同時支援正常和不良的執行模式。在不良執行模式中，區域切換會略過 Lambda 執行區塊步驟。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Lambda 執行區塊組態和許可執行多項檢查。區域切換會驗證下列項目是否正確：

- 組態中指定的 Lambda 函數存在。
- Lambda 函數的並行設定不會調節，包括驗證下列項目：
  - 並行未設定為 0。
  - 至少有一個並行執行可用，或者存在未預留的並行。

區域切換會執行 Lambda 函數的試轉，以驗證指定的參數和許可，而不執行實際的函數邏輯。當您執行試轉時，會產生標準 Lambda 成本。

區域切換也會驗證計劃的 IAM 角色是否具有 Lambda 執行所需的許可。如需區域切換執行區塊所需許可的詳細資訊，請參閱 ARC 中區域切換的身分型政策範例。

正確的 IAM 許可對於 Lambda 執行區塊的正常運作至關重要。如果任何這些驗證失敗，區域切換會傳回發生問題的警告，並提供特定錯誤訊息，協助您解決許可或組態問題。這可確保您的計劃在計劃執行期間執行此步驟時，具有必要的存取權來管理和與 Lambda 互動。

Amazon Route 53 運作狀態檢查執行區塊

Amazon Route 53 運作狀態檢查執行區塊可讓您指定在容錯移轉期間將應用程式流量重新導向至的區域。執行區塊會建立 Amazon Route 53 運作狀態檢查，然後連接到您帳戶中的 Route 53 DNS 記錄。當您執行區域切換計劃時，Route 53 運作狀態檢查狀態會更新，而流量會根據您的 DNS 組態重新導向。

> **Important**
>
> Route 53 託管區域必須與區域切換計劃位於相同的分割區中。

Configuration

若要設定 Route 53 運作狀態檢查執行區塊，請輸入下列值。

> **Important**
>
> 設定執行區塊之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱Route 53 運作狀態檢查執行區塊範例政策。

1. 步驟名稱：輸入名稱。
2. 步驟描述 （選用 ）：輸入步驟的描述。
3. 託管區域 ID：Route 53 中網域和 DNS 記錄的託管區域 ID。
4. 記錄名稱：輸入您使用的記錄的記錄名稱 （網域名稱 ），以及相關聯的運作狀態檢查，以重新導向應用程式的流量。區域切換會尋找記錄名稱的 Route 53 記錄集，並根據記錄集的值或設定識別符內的區域名稱，嘗試將每個記錄集映射至區域。
5. 記錄集識別符 （選用 ）：如果區域切換無法在建立計畫後，從步驟 4 中提供的記錄名稱自動將記錄集映射到區域，您可以選擇手動提供記錄集識別符。如果計劃評估傳回警告，指出需要更多資訊，請針對每個區域包含下列項目，以記錄集識別符更新您的計劃：
   - 記錄集識別符：為記錄集輸入設定識別符或值/路由流量到 。
   - 區域：輸入與具有記錄集識別符資訊的記錄集相關聯的區域。
6. 選擇儲存步驟。
7. 在 Route 53 中設定運作狀態檢查。

   區域切換會針對執行區塊中定義的託管區域中的每個記錄名稱，為每個區域提供運作狀態檢查 ID。請確定您在 Route 53 中為帳戶中的對應記錄集設定運作狀態檢查，以便區域切換可以在計劃執行期間正確重新導向應用程式的流量。在計劃詳細資訊頁面上的運作狀態檢查索引標籤中，您可以檢視所有執行區塊和區域的運作狀態檢查。

運作方式

您可以將運作狀態檢查步驟新增至區域切換工作流程，以便將流量重新導向至次要區域、用於作用中/被動組態，或用於作用中/作用中組態的已停用區域。如果您將多個工作流程新增至計劃，請為使用相同 DNS 記錄的所有運作狀態檢查執行區塊提供相同的組態值。

根據您在設定執行區塊時提供的資訊，區域切換會嘗試判斷計畫中每個區域的正確記錄集。一般而言，託管區域 ID 和記錄名稱有足夠的資訊來判斷記錄集和相關聯的區域。如果沒有，當區域切換在您建立計劃後執行其自動計劃評估時，會傳回警告，讓您知道需要更多資訊。

區域切換會為每個 Route 53 運作狀態檢查執行區塊提供運作狀態檢查。對於使用主動/被動復原方法的計劃，主要區域的運作狀態檢查會開始運作狀態良好，而待命區域的運作狀態檢查最初會設定為運作狀態不良。對於使用主動/主動復原方法的計劃，所有區域的運作狀態檢查都會以正常狀態開始。

若要讓區域切換成功為您的計劃執行此執行區塊，您必須將運作狀態檢查新增至您的 DNS 記錄。

對於作用中/作用中計劃，執行步驟的運作方式如下：

- 當區域執行停用工作流程時，運作狀態檢查會設定為運作狀態不佳，且流量不會再導向該區域。
- 當 區域的啟用工作流程執行時，運作狀態檢查會設定為正常運作，而流量會路由至 區域。

對於主動/被動計劃，執行步驟的運作方式如下：

- 當 區域的啟用工作流程執行時，該區域的運作狀態檢查會設為運作狀態良好，而流量會路由至 區域。同時，計劃中其他區域的運作狀態檢查會設定為運作狀態不佳，而流量會停止導向該區域。

作為計畫評估的一部分而評估的內容

當區域切換評估您的計劃時，區域切換會對 Route 53 運作狀態檢查執行區塊組態和許可執行多項檢查。區域切換會驗證運作狀態檢查是否連接到執行區塊組態中指定的 DNS 記錄。也就是說，區域切換會驗證特定 AWS 區域 的 DNS 記錄是否設定為使用該區域的運作狀態檢查。

比較 ARC 路由控制和 Route 53 運作狀態檢查執行區塊

區域切換中的 Amazon Route 53 運作狀態檢查執行區塊為 DNS 型流量管理提供了成本較低的替代方案。不過，此執行區塊取決於 AWS 區域 您正在啟用的 ，因此 區域必須可用。這符合大多數客戶的需求，因為他們正在啟用運作狀態良好的區域。

ARC 路由控制提供高度可靠的 DNS 型流量管理，具有 100% 的可用性 SLA。透過路由控制，您的營運團隊可以使用安全防護機制在區域之間轉移流量。路由控制提供具有 100% SLA 的單一租戶解決方案。路由控制叢集分散在五個區域，可以容忍兩個區域離線。如果您有高度關鍵的應用程式，請考慮使用路由控制。

使用區域切換不需要路由控制。您可以使用區域切換來管理流量重新導向，方法是使用 Route 53 運作狀態檢查執行區塊，無需路由控制。

在下列情況中，路由控制會使用區域切換新增值：

- 您需要流量控制機制本身的 100% 可用性 SLA。
- 您的組織需要具有關鍵應用程式安全規則的手動操作控制。

- 您想要defense-in-depth，以便營運團隊可以視需要手動覆寫自動流量路由。

Route 53 運作狀態檢查執行區塊不依賴於控制平面。運作狀態檢查記錄變更使用資料平面，因此不需要啟用區域來處理組態更新。在下列情況中，Route 53 運作狀態檢查執行區塊已足夠：

- 您的應用程式可以取決於您正在啟用 AWS 區域 的 。
- 在復原工作流程中，自動流量重新導向符合您的需求。
- 成本最佳化是優先事項。Route 53 運作狀態檢查執行區塊的成本低於路由控制。

大多數客戶從 Route 53 運作狀態檢查執行區塊開始，做為預設流量路由機制，並僅為需要最高流量管理機制可靠性的最關鍵應用程式新增路由控制。

建立子計畫

若要支援更複雜的復原案例，您可以使用區域切換計畫執行區塊新增子計畫，以建立子計畫。階層限制為兩個層級，但一個父計劃可以包含多個子計劃。

> **Important**
>
> 建立子計畫之前，請確定您已備妥正確的 IAM 政策。如需詳細資訊，請參閱區域切換計畫執行區塊範例政策。

為了相容性，子計畫必須支援父計畫支援的所有區域。此外，父系和子系計劃的復原方法，主動/主動或主動/被動，必須相同。

請記住，子計畫會以下列方式回應您對父計畫和父計畫案例所做的變更。

- 父系執行區塊會在所有子系計畫和其中的其他執行區塊完成時標示為已完成。
- 如果任何子計畫中的任何步驟失敗，則父計畫中的區域切換計畫執行區塊會失敗。
- 在區域切換步驟期間，在父系計畫中啟動的控制動作，例如暫停、正常或不良的切換，或取消，都會在子系計畫上自動嘗試，無論子系計畫目前的步驟為何。
- 略過操作有特殊行為：會略過父系計畫，但子系計畫仍會執行。
- 如果子計畫已在區域切換區塊中執行，為了判斷是否繼續執行，區域切換會評估子計畫與父計畫的相容性。如果子計劃的組態符合父計劃的需求，區域切換會將子計劃視為由父計劃啟動。
- 如果子計畫使用不相容的組態參數執行，父計畫步驟將會失敗，如下所示：

  - 子計畫正在不同的區域中操作
  - 當區域切換預期它執行啟用操作時，子計畫正在執行停用操作
- 如果子計畫在父計畫暫停期間成功完成，父計畫將在父計畫繼續時成功。

建立區域切換計畫的觸發

如果您想要在區域切換中自動復原應用程式，您可以為區域切換計畫建立一或多個觸發。觸發會根據您選擇的 CloudWatch 警示條件，自動開始執行區域切換計劃。

為區域切換計劃建立觸發

1. 建立計劃後，在計劃詳細資訊頁面上，選取觸發標籤。
2. 選擇管理觸發條件。
3. 選取您要自動執行的工作流程，然後選擇新增觸發。
4. 提供觸發的描述。
5. 選取 CloudWatch 警示，然後選取最多 10 個 CloudWatch 警示來建立觸發條件。

   當您選取多個條件時，必須先符合所有條件，計劃才會開始自動執行。

當 CloudWatch 警示轉換以符合觸發條件時，觸發會開始計劃執行。當觸發新增至計劃時，如果已符合條件，則計劃不會執行，以防止意外容錯移轉事件。

執行區域切換計劃以復原應用程式

若要在 AWS 區域 受損時復原應用程式，請在 Amazon Application Recovery Controller (ARC) 中執行區域切換計畫。

- 如果您的應用程式使用主動/主動方法部署，則您計劃中的工作流程會停用受損的區域，以便您的其他作用中區域適當擴展，並開始接收所有應用程式流量。
- 如果您的應用程式是使用主動/被動方法部署，則計劃中的工作流程會停用受損區域並啟用待命區域，方法是視需要在那裡擴展您的資源，並將應用程式流量重新導向至待命區域。

若要手動執行應用程式復原，請執行下列動作來執行區域切換計畫。

另一個選項是使用您指定啟動計畫執行的特定 Amazon CloudWatch 警示自動觸發執行。您可以在建立或更新計劃時指定計劃執行的觸發條件。如需詳細資訊，請參閱建立區域切換計畫的觸發。

執行區域切換計劃

1. 在 中 AWS 管理主控台，導覽至您要為應用程式啟用 AWS 區域 的 。
2. 在 Amazon Application Recovery Controller (ARC) 主控台上，選擇區域切換，然後選取您要執行的計劃。
3. 選擇執行計畫。
4. 如果您的計劃包含手動核准步驟，請在出現提示時核准每個步驟。

當計劃執行時，您可以在執行詳細資訊頁面上追蹤其進度，該頁面會在您選擇執行計劃時開啟。

您也可以在區域切換儀表板上檢視進行中應用程式復原的相關資訊。在區域切換主控台的左側導覽下，區域切換下，選擇下列其中一項：

- 全域儀表板
- 區域名稱中的執行

請注意，如果區域中存在損害，全域儀表板可能不會顯示您的所有計劃資料。因此，我們建議您在操作事件期間僅依賴區域執行儀表板。區域執行儀表板更具彈性，因為它使用本機區域切換資料平面。

當計劃執行完成時，您可以在計劃執行歷史記錄索引標籤的計劃詳細資訊頁面上，查看計劃執行的相關資訊，以及區域切換已執行的其他計劃。

區域切換儀表板

區域切換包含全域儀表板，您可以用來觀察整個組織和區域的區域切換計劃狀態。區域切換也有區域執行儀表板，只會顯示您目前登入 的區域中的計劃執行 AWS 管理主控台。

請注意，如果區域中存在損害，全域儀表板可能不會顯示您的所有計劃資料。因此，我們建議您在操作事件期間僅依賴區域執行儀表板。區域執行儀表板更具彈性，因為它使用本機區域切換資料平面。

開啟區域切換全域儀表板

1. 在 開啟 ARC 主控台https://console.aws.amazon.com/route53recovery/home#/dashboard。
2. 在區域切換下，選擇全域儀表板。

開啟區域切換區域儀表板

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

2. 在區域切換下，選擇區域儀表板。

區域切換中的跨帳戶支援

在區域切換中，您可以將其他帳戶的資源新增至您的計劃。您也可以與其他 帳戶共用區域切換計劃。如需詳細資訊，請參閱下列區段。

跨帳戶資源

區域切換允許資源託管在與包含區域切換計劃的帳戶分開的帳戶中。當區域切換執行計畫時，它會假設 executionRole。如果計劃使用來自與託管計劃之帳戶不同的 帳戶的資源，則區域切換會使用 executionRole 來擔任 crossAccountRole 來存取這些資源。

區域切換計畫中的每個資源有兩個選用欄位：crossAccountRole 和 externalId。

- crossAccountRole：此角色允許存取 帳戶中與託管區域切換計劃的帳戶不同的資源。角色只需要許可，即可對其帳戶中的資源採取動作，不需要許可，即可對託管區域切換計劃的帳戶中的資源採取動作。
- ExternalId：這是來自帳戶信任政策的 STS 外部 ID，其中包含需要 動作的資源。它是一個英數字串，是兩個帳戶之間的共用秘密。

共用區域切換計劃

區域切換與 AWS Resource Access Manager (AWS RAM) 整合，可讓您跨 共用計劃 AWS 帳戶。當您共用計劃時，您指定的帳戶可以檢視計劃詳細資訊、執行計劃，以及檢視計劃的執行，這可為不同團隊的復原功能提供更多控制和彈性。

若要開始使用區域切換中的跨帳戶共用，您可以在其中建立資源共用 AWS RAM。資源共享指定有權共享您帳戶所擁有計劃的參與者。參與者可以透過主控台、CLI 或 AWS SDKs 來檢視和執行共用計劃。

重要：您必須 AWS 帳戶 擁有要共用的計劃。您無法共用已與您共用的計劃。若要與您的組織或 中的組織單位共用計劃 AWS Organizations，您必須啟用與 Organizations 共用。

如需 的詳細資訊 AWS RAM，請參閱 支援跨 ARC 區域切換帳戶共用計劃。

支援跨 ARC 區域切換帳戶共用計劃

Amazon Application Recovery Controller (ARC) 與 整合 AWS Resource Access Manager 以啟用資源共用。 AWS RAM 是一種服務，可讓您與其他 AWS 帳戶 或透過 共用資源 AWS Organizations。

對於 ARC 區域切換，您可以共用區域切換計畫。（若要使用您計劃中另一個帳戶的資源，請使用 crossAccount 角色。 若要進一步了解，請參閱 跨帳戶資源。）

透過 AWS RAM，您可以透過建立資源共用來共用您擁有的資源。資源共用會指定要共用的資源，以及要共用的資源參與者。參與者可以包括：

- 中的特定擁有者組織 AWS 帳戶 內部或外部 AWS Organizations
- 中組織內部的組織單位 AWS Organizations
- 其在 中的整個組織 AWS Organizations

如需 的詳細資訊 AWS RAM，請參閱AWS RAM 《 使用者指南》。

透過使用 AWS Resource Access Manager 在 ARC 中跨帳戶共用計劃，您可以使用具有數個不同計劃的計劃 AWS 帳戶。當您選擇共用計劃時， AWS 帳戶 您指定的其他 可以執行計劃來執行應用程式復原。

AWS RAM 是一項服務，可 AWS 協助客戶安全地跨 共用資源 AWS 帳戶。透過 AWS RAM，您可以使用 IAM 角色和使用者 AWS Organizations，在 中的組織或組織單位 (OUs) 內共用資源。 AWS RAM 是共用計劃的集中控制方式。

當您共享計劃時，您可以減少組織所需的計劃總數。透過共享計劃，您可以分配在不同團隊之間執行計劃的總成本，以降低成本最大化 ARC 的優勢。跨帳戶共用計劃也可以簡化將多個應用程式加入 ARC 的程序，特別是如果您有大量應用程式分散在多個帳戶和營運團隊。

若要開始使用 ARC 中的跨帳戶共用，您可以建立資源共用 i n AWS RAM。資源共享指定有權共享您帳戶所擁有計劃的參與者。

本主題說明如何共用您擁有的參數，以及如何使用與您共用的參數。

目錄

- 共用計畫的先決條件
- 共用計劃
- 取消共用共用計劃
- 識別共享計劃
- 共用計劃的責任和許可
- 帳單成本
- 配額

共用計畫的先決條件

- 若要共用計畫，您必須在 中擁有該計畫 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計劃。
- 若要與組織或 中的組織單位共用計劃 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。

共用計劃

當您共用計畫時，您指定共用計畫的參與者可以檢視，如果您授予其他許可，請執行計畫。

若要共用計劃，您必須將其新增至資源共用。資源共用是可讓您在 AWS 帳戶之間共用資源的一種 AWS RAM 資源。資源共用會指定要共用的資源，以及與其共用的參與者。若要共用計劃，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享，您可以使用 AWS RAM 主控台，或搭配 AWS Command Line Interface AWS SDKs使用 AWS RAM API 操作。

如果您是 中組織的一部分， AWS Organizations 且已啟用組織內的共享，則組織中的參與者會自動獲得共享計劃的存取權。否則，參與者會收到加入資源共享的邀請，並在接受邀請後獲得共用計劃的存取權。

您可以使用 AWS RAM 主控台，或搭配 AWS CLI 或 SDK 使用 AWS RAM API 操作，來共用您擁有的計劃。 SDKs

使用 AWS RAM 主控台共享您擁有的計劃

請參閱AWS RAM 《 使用者指南》中的建立資源共享。

使用 共享您擁有的計劃 AWS CLI

使用 create-resource-share 命令。

授予共用計畫的許可

跨帳戶共用計劃需要使用下列其他許可，讓共用計劃的 IAM 委託人共用計劃 AWS RAM：

```
# read and execute plan permissions
"arc-region-switch:GetPlan",
"arc-region-switch:GetPlanInRegion",
"arc-region-switch:GetPlanExecution",
```

```
"arc-region-switch:ListPlanExecutionEvents",
"arc-region-switch:ListPlanExecutions",
"arc-region-switch:ListRoute53HealthChecks",
"arc-region-switch:GetPlanEvaluationStatus",
"arc-region-switch:StartPlanExecution",
"arc-region-switch:CancelPlanExecution",
"arc-region-switch:UpdatePlanExecution",
"arc-region-switch:UpdatePlanExecutionStep"
```

共用計劃的擁有者必須擁有下列許可。如果您在沒有這些許可 AWS RAM 的情況下嘗試透過 共用計劃，則會傳回錯誤。

```
"arc-region-switch:PutResourcePolicy" # Permission only apis
"arc-region-switch:DeleteResourcePolicy" # Permission only apis
"arc-region-switch:GetResourcePolicy" # Permission only apis
```

如需 IAM AWS Resource Access Manager 使用方式的詳細資訊，請參閱AWS RAM 《 使用者指南》中的 IAM AWS Resource Access Manager 使用方式。

取消共用共用計劃

當您取消共用計劃時，以下內容適用於參與者和擁有者：

- 參與者無法再檢視或執行未共用的計畫。

若要取消共用您擁有的共用計劃，請從資源共用中移除它。您可以使用 AWS RAM 主控台或搭配 或 AWS CLI SDKs 使用 AWS RAM API 操作來執行此操作。

使用 AWS RAM 主控台取消共用您擁有的共用計劃

請參閱《AWS RAM 使用者指南》中的更新資源共享。

使用 取消共用您擁有的共享計劃 AWS CLI

使用 disassociate-resource-share 命令。

識別共享計劃

擁有者和參與者可以透過在 中檢視資訊來識別共享計劃 AWS RAM。他們也可以使用 ARC 主控台和取得共用資源的相關資訊 AWS CLI。

一般而言，若要進一步了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 來檢視您與他人共用的所有資源 AWS RAM。如需詳細資訊，請參閱在 中檢視共用資源 AWS RAM。
- 身為參與者，您可以使用 檢視與您共用的所有資源 AWS RAM。如需詳細資訊，請參閱在 中檢視共用資源 AWS RAM。

身為擁有者，您可以透過在 中檢視資訊 AWS 管理主控台 ，或使用 AWS Command Line Interface 搭配 ARC API 操作來判斷您是共享計劃。

使用主控台識別是否共享您擁有的計劃

在 AWS 管理主控台的詳細資訊頁面上，查看計劃共用狀態。

身為參與者，當計劃與您共用時，您通常必須接受共用，才能存取計劃。

共用計劃的責任和許可

擁有者的許可

參與者可以檢視或執行計畫 （如果他們具有正確的許可）。

參與者的許可

當您與其他人共用您擁有的計劃時 AWS 帳戶，參與者可以檢視或執行計劃 （如果他們具有正確的許可）。

當您使用 共用計劃時， AWS RAM參與者預設具有唯讀許可。若要檢閱區域切換的唯讀許可清單，請參閱 唯讀許可。參與者需要額外許可才能執行區域切換計畫。需要執行計劃的參與者需要額外的許可。請注意，您無法將下列操作的許可授予 AWS RAM 參與者：

- `ApprovePlanExecutionStep`
- `UpdatePlan`

帳單成本

ARC 中計劃的擁有者需支付與計劃相關的費用。對於計劃擁有者或參與者，建立計劃中託管的資源無需額外費用。

如需詳細的定價資訊和範例，請參閱 Amazon Application Recovery Controller (ARC) 定價。

配額

在共用計劃中建立的所有資源都會計入計劃擁有者的配額。

如需區域切換計劃配額的清單，請參閱 區域切換的配額。

ARC 中區域切換的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目錄

- ARC 中的區域切換如何與 IAM 搭配使用
- ARC 中區域切換的身分型政策範例

ARC 中的區域切換如何與 IAM 搭配使用

在您使用 IAM 管理對 ARC 的存取之前，請先了解哪些 IAM 功能可與 ARC 搭配使用。

在您使用 IAM 在 Amazon Application Recovery Controller (ARC) 中管理區域切換的存取權之前，請先了解哪些 IAM 功能可與區域切換搭配使用。

您可以在 Amazon Application Recovery Controller (ARC) 中搭配區域切換使用的 IAM 功能

IAM 功能	區域切換支援
身分型政策	是
資源型政策	是
政策動作	是
政策資源	是
政策條件索引鍵	是
ACL	是
ABAC (政策中的標籤)	是

IAM 功能	區域切換支援
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 服務如何與大多數 IAM 功能搭配使用的高階整體檢視，請參閱《IAM 使用者指南》中的與 AWS IAM 搭配使用的 服務。

區域切換的身分型政策

支援身分型政策：是

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。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

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。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 ARC 身分型政策的範例，請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例。

區域切換內的資源型政策

支援資源型政策：是

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。

區域切換的政策動作

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。政策會使用動作來授予執行相關聯動作的許可。

適用於區域切換的 ARC 中的政策動作在動作之前使用下列字首：

```
arc-region-switch
```

若要在單一陳述式中指定多個動作，請用逗號分隔。例如，下列項目：

```
"Action": [
      "arc-region-switch:action1",
      "arc-region-switch: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-region-switch:Describe*"
```

若要檢視區域切換的 ARC 身分型政策範例，請參閱 ARC 中區域切換的身分型政策範例。

區域切換的政策資源

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。最佳實務是使用其 Amazon Resource Name (ARN) 來指定資源。若動作不支援資源層級許可，使用萬用字元 (*) 表示該陳述式適用於所有資源。

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

若要檢視區域切換的 ARC 身分型政策範例，請參閱 ARC 中區域切換的身分型政策範例。

區域切換的政策條件索引鍵

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 元素會根據定義的條件，指定陳述式的執行時機。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。若要查看所有 AWS 全域條件索引鍵，請參閱《IAM 使用者指南》中的AWS 全域條件內容索引鍵。

若要檢視區域切換的 ARC 身分型政策範例，請參閱 ARC 中區域切換的身分型政策範例。

區域切換中的存取控制清單 ACLs)

支援 ACL：是

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。

具有區域切換的屬性型存取控制 (ABAC)

支援 ABAC (政策中的標籤)：是

屬性型存取控制 (ABAC) 是一種授權策略，依據稱為標籤的屬性來定義許可。您可以將標籤連接至 IAM 實體 AWS 和資源，然後設計 ABAC 政策，以便在委託人的標籤符合資源上的標籤時允許操作。

如需根據標籤控制存取，請使用 aws:ResourceTag/*key-name*、aws:RequestTag/*key-name* 或 aws:TagKeys 條件索引鍵，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》中的使用 ABAC 授權定義許可。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)。

搭配區域切換使用臨時登入資料

支援臨時憑證：是

臨時登入資料提供 AWS 資源的短期存取權，當您使用聯合或切換角色時會自動建立。 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 使用者指南》中的 IAM 中的臨時安全憑證與可與 IAM 搭配運作的AWS 服務。

區域切換的跨服務主體許可

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，您會被視為委託人。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。

區域切換的服務角色

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。如需詳細資訊，請參閱《IAM 使用者指南》中的建立角色以委派許可給 AWS 服務。

區域切換的服務連結角色

支援服務連結角色：否

服務連結角色是連結至 的一種服務角色 AWS 服務。服務可以擔任代表您執行動作的角色。服務連結角色會出現在您的 中 AWS 帳戶 ，並由服務擁有。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。在資料表中尋找服務，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。

ARC 中區域切換的身分型政策範例

根據預設，使用者和角色沒有建立或修改 ARC 資源的許可。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。

如需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 (主控台)。

如需 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 ARNs 格式，請參閱《服務授權參考》中的 Amazon Application Recovery Controller (ARC) 的動作、資源和條件索引鍵。

主題

- 政策最佳實務
- 規劃執行角色信任政策
- 完整存取許可
- 唯讀許可
- 執行區塊許可
- 應用程式運作狀態許可的 CloudWatch 警示
- 自動計劃執行報告許可
- 跨帳戶資源許可

- 完成計劃執行角色許可

政策最佳實務

身分型政策會判斷您帳戶中的某個人員是否可以建立、存取或刪除 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 受管政策並邁向最低權限許可 – 若要開始將許可授予您的使用者和工作負載，請使用將許可授予許多常見使用案例的 AWS 受管政策。它們可在您的 中使用 AWS 帳戶。我們建議您定義特定於使用案例 AWS 的客戶受管政策，以進一步減少許可。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。
- 套用最低權限許可 – 設定 IAM 政策的許可時，請僅授予執行任務所需的許可。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。如果透過特定 例如 使用服務動作 AWS 服務，您也可以使用條件來授予其存取權 CloudFormation。如需詳細資訊，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，可協助您撰寫安全且實用的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM Access Analyzer 驗證政策。
- 需要多重要素驗證 (MFA) – 如果您的案例需要 IAM 使用者或 中的根使用者 AWS 帳戶，請開啟 MFA 以提高安全性。如需在呼叫 API 操作時請求 MFA，請將 MFA 條件新增至您的政策。如需詳細資訊，請參閱《IAM 使用者指南》中的透過 MFA 的安全 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。

規劃執行角色信任政策

這是計劃執行角色所需的信任政策，因此 ARC 可以執行區域切換計劃。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
```

```
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "arc-region-switch.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

完整存取許可

下列 IAM 政策會授予所有區域交換器 APIs的完整存取權：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "arc-region-switch.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:CreatePlan",
        "arc-region-switch:UpdatePlan",
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:DeletePlan",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:ApprovePlanExecutionStep",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
```

```
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource",
        "arc-region-switch:TagResource",
        "arc-region-switch:UntagResource",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:UpdatePlanExecutionStep"
      ],
      "Resource": "*"
    }
  ]
}
```

唯讀許可

下列 IAM 政策會授予區域切換的唯讀存取許可：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlan",
        "arc-region-switch:ListPlans",
        "arc-region-switch:GetPlanInRegion",
        "arc-region-switch:ListPlansInRegion",
        "arc-region-switch:GetPlanEvaluationStatus",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListRoute53HealthChecks",
        "arc-region-switch:ListRoute53HealthChecksInRegion",
        "arc-region-switch:ListPlanExecutions",
        "arc-region-switch:ListPlanExecutionEvents",
        "arc-region-switch:ListTagsForResource"
      ],
      "Resource": "*"
```

```
    }
  ]
}
```

執行區塊許可

下列各節提供範例 IAM 政策，為您新增至區域切換計畫的特定執行區塊提供所需的許可。

目錄

- EC2 Auto Scaling 執行區塊範例政策
- Amazon EKS 資源擴展執行區塊範例政策
- Amazon ECS 服務擴展執行區塊範例政策
- ARC 路由控制執行區塊範例政策
- Aurora Global Database 執行區塊範例政策
- Amazon DocumentDB 全域叢集執行區塊範例政策
- Amazon RDS 執行區塊範例政策
- 手動核准執行區塊範例政策
- 自訂動作 Lambda 執行區塊範例政策
- Route 53 運作狀態檢查執行區塊範例政策
- 區域切換計畫執行區塊範例政策

EC2 Auto Scaling 執行區塊範例政策

如果您將執行區塊新增至 EC2 Auto Scaling 群組的區域切換計劃，可連接下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:UpdateAutoScalingGroup"
      ],
      "Resource": [
        "arn:aws:autoscaling:us-
east-1:123456789012:autoScalingGroup:123d456e-123e-1111-abcd-
EXAMPLE22222:autoScalingGroupName/app-asg-primary",
        "arn:aws:autoscaling:us-
west-2:123456789012:autoScalingGroup:1234a321-123e-1234-aabb-
EXAMPLE33333:autoScalingGroupName/app-asg-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon EKS 資源擴展執行區塊範例政策

如果您將執行區塊新增至 Amazon EKS 資源擴展的區域切換計劃，可連接以下範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "eks:DescribeCluster"
      ],
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:cluster/app-eks-primary",
        "arn:aws:eks:us-west-2:123456789012:cluster/app-eks-secondary"
```

```
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "eks:ListAssociatedAccessPolicies"
      ],
      "Resource": [
        "arn:aws:eks:us-east-1:123456789012:access-entry/app-eks-primary/*",
        "arn:aws:eks:us-west-2:123456789012:access-entry/app-eks-secondary/*"
      ]
    }
  ]
}
```

注意：除了此 IAM 政策之外，還需要使用 存取政策將計劃執行角色新增至 Amazon EKS 叢集的`AmazonArcRegionSwitchScalingPolicy`存取項目。如需詳細資訊，請參閱[設定 EKS 存取項目許可](#)。

Amazon ECS 服務擴展執行區塊範例政策

如果您將執行區塊新增至 Amazon ECS 服務擴展的區域切換計劃，可連接以下範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeServices",
        "ecs:UpdateService"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:service/app-cluster-primary/app-
service",
        "arn:aws:ecs:us-west-2:123456789012:service/app-cluster-secondary/app-
service"
      ]
    },
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ecs:DescribeClusters"
      ],
      "Resource": [
        "arn:aws:ecs:us-east-1:123456789012:cluster/app-cluster-primary",
        "arn:aws:ecs:us-west-2:123456789012:cluster/app-cluster-secondary"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:ListServices"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "application-autoscaling:DescribeScalableTargets",
        "application-autoscaling:RegisterScalableTarget"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:GetMetricStatistics"
      ],
      "Resource": "*"
    }
  ]
}
```

ARC 路由控制執行區塊範例政策

注意：Amazon ARC 路由控制執行區塊要求套用至計劃執行角色的任何服務控制政策 (SCPs) 都允許存取這些服務的下列區域：

- route53-recovery-control-config: us-west-2
- route53-recovery-cluster: us-west-2, us-east-1, eu-west-1, ap-southeast-2, ap-northeast-1

如果您將執行區塊新增至 ARC 路由控制的區域切換計劃，則要附加下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53-recovery-control-config:DescribeControlPanel",
        "route53-recovery-control-config:DescribeCluster"
      ],
      "Resource": [
        "arn:aws:route53-recovery-control::123456789012:controlpanel/
abcd1234abcd1234abcd1234abcd1234",
        "arn:aws:route53-recovery-
control::123456789012:cluster/4b325d3b-0e28-4dcf-ba4a-EXAMPLE11111"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "route53-recovery-cluster:GetRoutingControlState",
        "route53-recovery-cluster:UpdateRoutingControlStates"
      ],
      "Resource": [
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/abcdef1234567890",
        "arn:aws:route53-recovery-
control::123456789012:controlpanel/1234567890abcdef1234567890abcdef/
routingcontrol/1234567890abcdef"
      ]
    }
  ]
}
```

您可以使用 CLI 擷取路由控制面板 ID 和叢集 ID。如需詳細資訊，請參閱設定路由控制元件。

Aurora Global Database 執行區塊範例政策

如果您將執行區塊新增至 Aurora 資料庫的區域切換計畫，可連接下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": [
        "arn:aws:rds::123456789012:global-cluster:app-global-db",
       "arn:aws:rds:us-east-1:123456789012:cluster:app-db-primary",
        "arn:aws:rds:us-west-2:123456789012:cluster:app-db-secondary"
      ]
    }
  ]
}
```

Amazon DocumentDB 全域叢集執行區塊範例政策

如果您將執行區塊新增至 Amazon DocumentDB 全域叢集的區域切換計劃，可連接下列範例政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
```

```
        "rds:DescribeGlobalClusters",
        "rds:DescribeDBClusters",
        "rds:FailoverGlobalCluster",
        "rds:SwitchoverGlobalCluster"
      ],
      "Resource": "*"
    }
  ]
}
```

Amazon RDS 執行區塊範例政策

如果您將執行區塊新增至 Amazon RDS 僅供讀取複本提升或跨區域複本建立的區域切換計劃，要連接下列範例政策。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "rds:PromoteReadReplica",
        "rds:CreateDBInstanceReadReplica",
        "rds:ModifyDBInstance"
      ],
      "Resource": "*"
    }
  ]
}
```

手動核准執行區塊範例政策

如果您將執行區塊新增至區域切換計畫以進行手動核准，可連接下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:ApprovePlanExecutionStep"
      ],
      "Resource": "arn:aws:arc-region-switch::123456789012:plan/sample-
plan:0123abc"
    }
  ]
}
```

自訂動作 Lambda 執行區塊範例政策

如果您將執行區塊新增至 Lambda 函數的區域切換計劃，可連接下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "lambda:GetFunction",
        "lambda:InvokeFunction"
      ],
      "Resource": [
        "arn:aws:lambda:us-east-1:123456789012:function:app-recovery-primary",
        "arn:aws:lambda:us-west-2:123456789012:function:app-recovery-secondary"
      ]
    }
  ]
}
```

Route 53 運作狀態檢查執行區塊範例政策

如果您將執行區塊新增至 Route 53 運作狀態檢查的區域切換計劃，可連接下列範例政策。

JSON

```
{
```

```
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "route53:ListResourceRecordSets"
      ],
      "Resource": [
        "arn:aws:route53:::hostedzone/Z1234567890ABCDEFGHIJ"
      ]
    }
  ]
}
```

區域切換計畫執行區塊範例政策

如果您將執行區塊新增至區域切換計劃以執行子計劃，可連接下列範例政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:StartPlanExecution",
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:CancelPlanExecution",
        "arc-region-switch:UpdatePlanExecution",
        "arc-region-switch:ListPlanExecutions"
      ],
      "Resource": [
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch::123456789012:plan/child-plan-2/fghij2"
      ]
    }
  ]
}
```

應用程式運作狀態許可的 CloudWatch 警示

以下是連接 以存取應用程式運作狀態 CloudWatch 警示的範例政策，用於協助判斷實際的復原時間。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarmHistory",
        "cloudwatch:DescribeAlarms"
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary",
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ]
    }
  ]
}
```

自動計劃執行報告許可

如果您為區域切換計劃設定自動產生報告，可連接以下範例政策。此政策包含將報告寫入 Amazon S3、存取 CloudWatch 警示資料，以及擷取父系計劃子計劃資訊的許可。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::your-bucket-name/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DescribeAlarms",
        "cloudwatch:DescribeAlarmHistory"
```

```
      ],
      "Resource": [
        "arn:aws:cloudwatch:us-east-1:123456789012:alarm:app-health-primary"
        "arn:aws:cloudwatch:us-west-2:123456789012:alarm:app-health-secondary"
      ],
    },
    {
      "Effect": "Allow",
      "Action": [
        "arc-region-switch:GetPlanExecution",
        "arc-region-switch:ListPlanExecutionEvents"
      ],
      "Resource": [
        "arn:aws:arc-region-switch:us-east-1:123456789012:plan/child-plan-1/abcde1",
        "arn:aws:arc-region-switch:us-west-2:123456789012:plan/child-plan-2/fghij2"
      ],
    }
  ]
}
```

注意：如果您為 Amazon S3 儲存貯體加密設定客戶受管 AWS KMS 金鑰，您還必須為金鑰新增 `kms:GenerateDataKey`和 `kms:Encrypt`許可。

跨帳戶資源許可

如果資源位於不同的帳戶中，您將需要跨帳戶角色。以下是跨帳戶角色的範例信任政策。

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:role/RegionSwitchExecutionRole"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
```

```
    }
  ]
}
```

以下是計劃執行角色擔任此跨帳戶角色的許可：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::987654321098:role/RegionSwitchCrossAccountRole",
      "Condition": {
        "StringEquals": {
          "sts:ExternalId": "UniqueExternalId123"
        }
      }
    }
  ]
}
```

完成計劃執行角色許可

建立包含所有執行區塊許可的完整政策需要相當大的政策。實際上，您應該只包含您在特定計劃中使用的執行區塊的許可。

以下是範例政策，您可以用作計劃執行角色政策的起點。請務必新增您在計劃中包含的特定執行區塊所需的其他政策。僅包含您在計劃中使用的特定執行區塊所需的許可，以遵循最低權限原則

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Effect": "Allow",
            "Action": "iam:SimulatePrincipalPolicy",
            "Resource": "arn:aws:iam::123456789012:role/
RegionSwitchExecutionRole"
        },
        {
            "Effect": "Allow",
            "Action": [
                "arc-region-switch:GetPlan",
                "arc-region-switch:GetPlanExecution",
                "arc-region-switch:ListPlanExecutions"
            ],
            "Resource": "*"
        }
    ]
}
```

在 ARC 中記錄和監控區域切換

您可以使用 Amazon CloudWatch AWS CloudTrail和 Amazon EventBridge 在 Amazon Application Recovery Controller (ARC) 中監控區域切換，以取得提醒、分析模式，並協助疑難排解問題。

主題

- 使用 記錄區域切換 API 呼叫 AWS CloudTrail
- 在 ARC 中使用區域切換搭配 Amazon EventBridge

使用 記錄區域切換 API 呼叫 AWS CloudTrail

Amazon Application Recovery Controller (ARC) 區域切換已與 服務整合 AWS CloudTrail，該服務提供使用者、角色或 ARC 中 AWS 服務所採取動作的記錄。CloudTrail 會將 ARC 的所有 API 呼叫擷取為事件。擷取的呼叫包括來自 ARC 主控台的呼叫，以及對 ARC API 操作的程式碼呼叫。

如果您建立線索，您可以將 CloudTrail 事件持續交付至 Amazon S3 儲存貯體，包括 ARC 的事件。即使您未設定追蹤，依然可以透過 CloudTrail 主控台中的事件歷史記錄檢視最新事件。

您可以使用 CloudTrail 所收集的資訊，判斷向 ARC 提出的請求、提出請求的 IP 地址、提出請求的人員、提出請求的時間，以及其他詳細資訊。

若要進一步了解 CloudTrail，請參閱「AWS CloudTrail 使用者指南」。

CloudTrail 中的 ARC 資訊

建立帳戶 AWS 帳戶 時，您的 上會啟用 CloudTrail。當活動在 ARC 中發生時，該活動會與事件歷史記錄中的其他服務 AWS 事件一起記錄在 CloudTrail 事件中。您可以在 中檢視、搜尋和下載最近的事件 AWS 帳戶。如需詳細資訊，請參閱使用 CloudTrail 事件歷史記錄。

若要持續記錄 中的事件 AWS 帳戶，包括 ARC 的事件，請建立追蹤。線索能讓 CloudTrail 將日誌檔案交付至 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。線索會記錄 AWS 分割區中所有區域的事件，並將日誌檔案交付至您指定的 Amazon S3 儲存貯體。此外，您可以設定其他 AWS 服務，以進一步分析和處理 CloudTrail 日誌中所收集的事件資料。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務和整合
- 設定 CloudTrail 的 Amazon SNS 通知
- 接收多個區域的 CloudTrail 日誌檔案及接收多個帳戶的 CloudTrail 日誌檔案

CloudTrail 會記錄所有 ARC 動作，並記錄在 TBD API REFERENCE LINK 中。例如，對 TBD、TBD 和 TBD 動作發出的呼叫會在 CloudTrail 記錄檔案中產生專案。

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：

- 是否使用根或 AWS Identity and Access Management (IAM) 使用者登入資料提出請求。
- 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 userIdentity 元素。

檢視事件歷史記錄中的區域切換事件

CloudTrail 可讓您使用 Event history (事件歷史記錄) 檢視最近的事件。區域切換 API 請求的大多數事件都位於您使用區域切換計劃的區域中，例如，您在其中建立計劃或執行計劃。不過，您在 ARC 主控台中執行的某些區域切換動作是使用控制計畫 API 操作，而不是資料平面操作。對於控制平面操作，您可以檢視美國東部（維吉尼亞北部）的事件。若要了解哪些 API 呼叫是控制平面操作，請參閱 區域切換 API 操作。

了解 ARC 日誌檔案項目

追蹤是一種組態，能讓事件以日誌檔案的形式交付到您指定的 Amazon S3 儲存貯體。CloudTrail 日誌檔案包含一或多個日誌專案。一個事件為任何來源提出的單一請求，並包含請求動作、請求的日期和時間、請求參數等資訊。CloudTrail 日誌檔並非依公有 API 呼叫的堆疊追蹤排序，因此不會以任何特定順序出現。

下列範例顯示 CloudTrail 日誌項目，示範區域切換`StartPlanExecution`的動作。


```
{
    "eventVersion": "1.11",
    "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"
            },
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2025-07-06T17:38:05Z"
            }
        }
    },
    "eventTime": "2025-07-06T18:08:03Z",
    "eventSource": "arc-region-switch.amazonaws.com",
    "eventName": "StartPlanExecution",
    "awsRegion": "us-east-1",
    "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": {
        "planArn": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "targetRegion": "us-east-1",
        "action": "activate"    }
```

```
    "responseElements": {
        "executionId": "us-east-1/ddddddddEXAMPLE",
        "plan": "arn:aws:arc-region-switch::555555555555:plan/
CloudTrailIntegTestPlan:bbbbb",
        "planVersion": "1",
        "activateRegion": "us-east-1"    },
    "requestID": "fd42dcf7-6446-41e9-b408-d096example",
    "eventID": "4b5c42df-1174-46c8-be99-d67aexample",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management",
      "tlsDetails": {
        "tlsVersion": "TLSv1.3",
        "cipherSuite": "TLS_AES_128_GCM_SHA256",
        "clientProvidedHostHeader": "us-east-1.arc.amazon.aws"
}
```


在 ARC 中使用區域切換搭配 Amazon EventBridge

使用 Amazon EventBridge，您可以設定事件驅動規則，以監控 Amazon Application Recovery Controller (ARC) 中的區域切換資源，然後啟動使用其他服務的目標動作 AWS 。例如，您可以在區域切換計劃完成執行時發出 Amazon SNS 主題訊號，以設定傳送電子郵件通知的規則。

您可以在 Amazon EventBridge 中建立規則，以處理下列 ARC 區域切換事件：

- 區域切換計畫執行。事件指定區域切換計劃已執行 （ 執行 ）。
- 區域切換計畫評估。事件指定區域切換計畫評估已完成。

若要擷取您感興趣的特定 ARC 事件，請定義 EventBridge 可用來偵測事件的事件特定模式。事件模式的結構與其相符的事件相同。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。在正常操作情況下，它們會以近乎即時的方式從 ARC 交付至 EventBridge。不過，可能會發生可能延遲或阻止交付事件的情況。

如需 EventBridge 規則如何使用事件模式的詳細資訊，請參閱 EventBridge 中的事件和事件模式。

使用 EventBridge 監控區域切換資源

使用 EventBridge，您可以建立規則，定義 ARC 為區域切換資源發出事件時要採取的動作。

若要在 EventBridge 主控台中輸入或複製事件模式並貼上，請在主控台中選取 以輸入我自己的選項。為了協助您判斷可能對您有用的事件模式，本主題包含範例區域切換模式。

建立資源事件的規則

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 若要 AWS 區域 在 中建立規則，請選擇您建立要監控事件之計劃的區域。
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，請保留預設值 。
6. 選擇下一步。
7. 對於建置事件模式步驟，對於事件來源，請保留預設值 AWS 事件。
8. 在範例事件下，選擇輸入我自己的。
9. 針對範例事件，輸入或複製並貼上事件模式。如需範例，請參閱下一節。

範例區域切換模式

事件模式的結構與其相符的事件相同。該模式引用您欲比對的欄位，並提供您正在尋找的數值。

您可以將本節的事件模式複製並貼到 EventBridge 中，以建立可用來監控 ARC 動作和資源的規則。

下列事件模式提供您可能會在 EventBridge 中用於 ARC 中區域切換功能的範例。

- 從區域切換中選取 PlanExecution 的所有事件。

```
{
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region switch Plan Execution" ]
}
```

- 從區域切換選取所有事件以進行 PlanEvaluation。

```
    {
    "source": [ "aws.arc-region-switch" ],
    "detail-type": [ "ARC Region Switch Plan Evaluation" ]
    }
```

以下是區域切換計劃執行的範例 ARC 事件：

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "ExecutionStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
   }
}
```

以下是區域切換計劃步驟層級執行的範例 ARC 事件：

```
{
   "version": "0",
   "id": "1111111-bbbb-aaaa-cccc-dddddEXAMPLE", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/aaaaaExample"], #
 planArn
   "detail": {
    "version": "0.0.1",
    "eventType": "StepStarted",
    "executionId": "bbbbbbEXAMPLE",
    "executionAction": "activating/deactivating {region}",
    "idempotencyKey": "1111111-2222-3333-4444-5555555555", # As there is a possibility
 of dual logging
    "stepDetails" : {
     "stepName": "Routing control step",
     "resource": ["arn:aws:route53-recovery-control::111122223333:controlpanel/
abcdefghiEXAMPLE/routingcontrol/jklmnopqrsEXAMPLE"]
```

```
    }
   }
}
```

以下是區域切換計畫評估警告的範例 ARC 事件。

對於區域切換計畫評估，會在傳回警告時發出事件。如果未清除警告，則只會每 24 小時發出一次警告的事件。清除事件時，不會針對該警告發出其他事件。

```
{
   "version": "0",
   "id": "05d4d2d5-9c76-bfea-72d2-d4614802adb4", # Random uuid
   "detail-type": "ARC Region Switch Plan Execution",
   "source": "aws.arc-region-switch",
   "account": "111122223333",
   "time": "2023-11-16T23:38:14Z",
   "region": "us-east-1",
   "resources": ["arn:aws:arc-region-switch::111122223333:plan/a2b89be4821bfd1d"],
   "detail": {
     "version": "0.0.1",
     "idempotencyKey": "1111111-2222-3333-4444-5555555555",
     "metadata": {
        "evaluationTime" : "timestamp",
        "warning" : "There is a plan evaluation warning for arn:aws:arc-region-
switch::111122223333:plan/a2b89be4821bfd1d. Navigate to the Region switch console to
 resolve."
     }
   }
}
```

指定要用作目標的 CloudWatch 日誌群組

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 EventBridge 可用目標的清單，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 日誌群組新增為目標的需求，並提供在建立規則時新增日誌群組的程序。

若要將 CloudWatch 日誌群組新增為目標，您可以執行下列其中一項操作：

- 建立新的日誌群組
- 選擇現有的日誌群組

如果您在建立規則時使用主控台指定新的日誌群組，EventBridge 會自動為您建立日誌群組。請確定您用作 EventBridge 規則目標的日誌群組以 開頭/aws/events。如果您想要選擇現有的日誌群組，請注意，只有開頭為 的日誌群組才會在下拉式功能表中/aws/events顯示為選項。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 操作建立或使用 CloudWatch 日誌群組做為目標，請確定您正確設定許可。如果您使用主控台將日誌群組新增至 EventBridge 規則，則日誌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 來指定日誌群組，則必須更新日誌群組的資源型政策。下列範例政策說明您必須在日誌群組的資源型政策中定義的許可：

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Action": [
        "logs:CreateLogStream",
        "logs:PutLogEvents"
      ],
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "events.amazonaws.com",
          "delivery.logs.amazonaws.com"
        ]
      },
      "Resource": "arn:aws:logs:us-east-1:222222222222:log-group:/aws/events/
*:*",
      "Sid": "TrustEventsToStoreLogEvent"
    }
  ]
}
```

您無法使用 主控台為日誌群組設定資源型政策。若要將必要的許可新增至以資源為基礎的政策，請使用 CloudWatch PutResourcePolicy API 操作。然後，您可以使用 describe-resource-policies CLI 命令來檢查政策是否正確套用。

為資源事件建立規則並指定 CloudWatch 日誌群組目標

1. 前往 https://console.aws.amazon.com/events/ 開啟 Amazon EventBridge 主控台。
2. 選擇您要 AWS 區域 在其中建立規則的 。
3. 選擇建立規則，然後輸入該規則的任何相關資訊，例如事件模式或排程詳細資訊。

   如需建立 EventBridge 整備規則的詳細資訊，請參閱使用 EventBridge 監控整備檢查資源。
4. 在選取目標頁面上，選擇 CloudWatch 做為您的目標。
5. 從下拉式選單中選擇 CloudWatch 日誌群組。

區域切換的配額

Amazon Application Recovery Controller (ARC) 中的區域切換受下列配額約束。

實體	配額
每個帳戶的計劃數量	10 您可以請求提高配額。
每個計劃的執行區塊數量	100
每個計劃的區域切換計劃執行區塊數量	25
每個步驟的平行執行區塊數量	20
每個觸發條件的 CloudWatch 警示數量	10

使用 AWS SDKs的應用程式復原控制器程式碼範例

下列程式碼範例示範如何使用 Application Recovery Controller 搭配 AWS 軟體開發套件 (SDK)。

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 將此服務與 AWS SDK 搭配使用。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 SDKs的應用程式復原控制器基本範例
  - 使用 AWS SDKs的應用程式復原控制器的動作
    - GetRoutingControlState 搭配 AWS SDK 使用
    - UpdateRoutingControlState 搭配 AWS SDK 使用

使用 AWS SDKs的應用程式復原控制器基本範例

下列程式碼範例示範如何搭配使用 Amazon Route 53 應用程式復原控制器的基本功能與 AWS SDK。

範例

- 使用 AWS SDKs的應用程式復原控制器的動作
  - GetRoutingControlState 搭配 AWS SDK 使用
  - UpdateRoutingControlState 搭配 AWS SDK 使用

使用 AWS SDKs的應用程式復原控制器的動作

下列程式碼範例示範如何使用 AWS SDKs執行個別應用程式復原控制器動作。每個範例均包含 GitHub 的連結，您可以在連結中找到設定和執行程式碼的相關說明。

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》。

範例

- GetRoutingControlState 搭配 AWS SDK 使用

- UpdateRoutingControlState 搭配 AWS SDK 使用

GetRoutingControlState 搭配 AWS SDK 使用

下列程式碼範例示範如何使用 GetRoutingControlState。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
    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》中的 GetRoutingControlState。

Python

適用於 Python 的 SDK (Boto3)

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
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 詳細資訊，請參閱《AWS SDK for Python (Boto3) API 參考》中的 GetRoutingControlState。

SAP ABAP

適用於 SAP ABAP 的開發套件

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
```

```
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.

    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.

          " Create session for this region
          lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

          " Create client with the specific endpoint
          lo_client = create_recovery_client(
            iv_endpoint = lv_url
            iv_region   = lv_region
            io_session  = lo_session ).

          " Try to get the routing control state
          oo_result = lo_client->getroutingcontrolstate(
            iv_routingcontrolarn = iv_routing_control_arn ).

          " If successful, return the result
          RETURN.

        CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
```

```
          " This endpoint is temporarily unavailable, try the next one
          lo_exception = lo_endpoint_ex.
          CONTINUE.

        CATCH /aws1/cx_r5vaccessdeniedex
              /aws1/cx_r5vinternalserverex
              /aws1/cx_r5vresourcenotfoundex
              /aws1/cx_r5vthrottlingex
              /aws1/cx_r5vvalidationex
              /aws1/cx_rt_generic INTO lo_exception.
          " For other errors, re-raise immediately
          RAISE EXCEPTION lo_exception.
      ENDTRY.
    ENDLOOP.

    " If we get here, all endpoints failed - re-raise the last exception
    IF lo_exception IS BOUND.
      RAISE EXCEPTION lo_exception.
    ENDIF.
```

- 如需 API 詳細資訊，請參閱《適用於 AWS SAP ABAP 的 SDK API 參考》中的 GetRoutingControlState。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 將此服務與 AWS SDK 搭配使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

`UpdateRoutingControlState` 搭配 AWS SDK 使用

下列程式碼範例示範如何使用 `UpdateRoutingControlState`。

Java

適用於 Java 2.x 的 SDK

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
    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》中的 UpdateRoutingControlState。

Python

適用於 Python 的 SDK (Boto3)

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
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 詳細資訊，請參閱《AWS SDK for Python (Boto3) API 參考》中的 UpdateRoutingControlState。

SAP ABAP

適用於 SAP ABAP 的開發套件

> **Note**
>
> GitHub 上提供更多範例。尋找完整範例，並了解如何在 AWS 程式碼範例儲存庫中設定和執行。

```
    CONSTANTS cv_pfl TYPE /aws1/rt_profile_id VALUE 'ZCODE_DEMO'.
    DATA lo_exception TYPE REF TO /aws1/cx_rt_generic.
    DATA lo_session TYPE REF TO /aws1/cl_rt_session_base.
    DATA lo_client TYPE REF TO /aws1/if_r5v.
    DATA lt_endpoints TYPE TABLE OF string.
    DATA lv_endpoint TYPE string.
    DATA lv_region TYPE /aws1/rt_region_id.
```

```
    " Parse the comma-separated cluster endpoints
    " Expected format: "https://endpoint1.com|us-west-2,https://endpoint2.com|us-
east-1"
    SPLIT iv_cluster_endpoints AT ',' INTO TABLE lt_endpoints.

    " As a best practice, shuffle cluster endpoints to distribute load
    " For more information, see https://docs.aws.amazon.com/r53recovery/latest/
dg/route53-arc-best-practices.html#route53-arc-best-practices.regional
    " For simplicity, we'll try them in order (shuffling can be added if needed)

    " Try each endpoint in order
    LOOP AT lt_endpoints INTO lv_endpoint.
      TRY.
          " Parse endpoint and region from the format "url|region"
          DATA(lv_pos) = find( val = lv_endpoint sub = '|' ).
          IF lv_pos > 0.
            DATA(lv_url) = substring( val = lv_endpoint len = lv_pos ).
            lv_region = substring( val = lv_endpoint off = lv_pos + 1 ).
          ELSE.
            " If no region specified, use default
            lv_url = lv_endpoint.
            lv_region = 'us-east-1'.
          ENDIF.

          " Create session for this region
          lo_session = /aws1/cl_rt_session_aws=>create( cv_pfl ).

          " Create client with the specific endpoint
          lo_client = create_recovery_client(
            iv_endpoint = lv_url
            iv_region   = lv_region
            io_session  = lo_session ).

          " Try to update the routing control state
          oo_result = lo_client->updateroutingcontrolstate(
            iv_routingcontrolarn     = iv_routing_control_arn
            iv_routingcontrolstate   = iv_routing_control_state
            it_safetyrulestooverride = it_safety_rules_override ).

          " If successful, return the result
          RETURN.

        CATCH /aws1/cx_r5vendpttmpyunavailex INTO DATA(lo_endpoint_ex).
```

```
        " This endpoint is temporarily unavailable, try the next one
        lo_exception = lo_endpoint_ex.
        CONTINUE.

      CATCH /aws1/cx_r5vaccessdeniedex
            /aws1/cx_r5vconflictexception
            /aws1/cx_r5vinternalserverex
            /aws1/cx_r5vresourcenotfoundex
            /aws1/cx_r5vthrottlingex
            /aws1/cx_r5vvalidationex
            /aws1/cx_rt_generic INTO lo_exception.
        " For other errors, re-raise immediately
        RAISE EXCEPTION lo_exception.
    ENDTRY.
  ENDLOOP.

  " If we get here, all endpoints failed - re-raise the last exception
  IF lo_exception IS BOUND.
    RAISE EXCEPTION lo_exception.
  ENDIF.
```

- 如需 API 詳細資訊，請參閱《適用於 AWS SAP ABAP 的 SDK API 參考》中的 UpdateRoutingControlState。

如需 AWS SDK 開發人員指南和程式碼範例的完整清單，請參閱 將此服務與 AWS SDK 搭配使用。此主題也包含有關入門的資訊和舊版 SDK 的詳細資訊。

Amazon Application Recovery Controller 的安全性

的雲端安全性 AWS 是最高優先順序。身為 AWS 客戶，您可以受益於資料中心和網路架構，這些架構是為了滿足最安全敏感組織的需求而建置。

安全性是 AWS 與您之間的共同責任。共同責任模式將其描述為雲端的安全性，和雲端中的安全性：

- 雲端的安全性 – AWS 負責保護在 中執行 AWS 服務的基礎設施 AWS 雲端。 AWS 也為您提供可安全使用的服務。在AWS 合規計畫中，第三方稽核人員會定期測試和驗證我們安全的有效性。若要了解適用於 Amazon Application Recovery Controller 的合規計劃，請參閱AWS 合規計劃的 服務範圍。
- 雲端的安全性 – 您的責任取決於您使用 AWS 的服務。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。

本文件可協助您了解如何在使用 ARC 時套用共同責任模型。下列主題說明如何設定 ARC 以符合您的安全與合規目標。您也會了解如何使用其他 AWS 服務來協助您監控和保護 ARC 資源。

主題

- Amazon Application Recovery Controller 中的資料保護
- Amazon Application Recovery Controller (ARC) 的 Identity and Access Management
- 在 ARC 中記錄和監控
- Amazon Application Recovery Controller 的合規驗證
- Amazon Application Recovery Controller 中的彈性
- Amazon Application Recovery Controller 中的基礎設施安全性

Amazon Application Recovery Controller 中的資料保護

AWS 共同責任模型適用於 Amazon Application Recovery Controller 中的資料保護。如此模型所述，AWS 負責保護執行所有 的全域基礎設施 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 共同責任模型和 GDPR 部落格文章。

基於資料保護目的，我們建議您保護 AWS 帳戶 登入資料，並使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 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。如需有關使用 CloudTrail 追蹤擷取 AWS 活動的資訊，請參閱AWS CloudTrail 《 使用者指南》中的使用 CloudTrail 追蹤。
- 使用 AWS 加密解決方案，以及其中的所有預設安全控制 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。
- 如果您在 AWS 透過命令列界面或 API 存取 時需要 FIPS 140-3 驗證的密碼編譯模組，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) 140-3。

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 ARC 或使用 AWS 服務 主控台、API AWS CLI或其他 時 AWS SDKs 。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

Amazon Application Recovery Controller 儲存的客戶組態資訊會靜態加密。

傳輸中加密

Amazon Application Recovery Controller 的客戶請求和回應會在傳輸期間使用 TLS 加密。

Amazon Application Recovery Controller (ARC) 的 Identity and Access Management

AWS Identity and Access Management (IAM) 是 AWS 服務 ，可協助管理員安全地控制對 AWS 資源的存取。IAM 管理員可控制誰可以進行身分驗證 （ 登入 ） 和授權 （ 具有許可 ） 來使用 ARC 資源。IAM 是您可以免費使用 AWS 服務 的 。

目標對象

使用方式 AWS Identity and Access Management (IAM) 會根據您的角色而有所不同：

- 服務使用者 — 若無法存取某些功能，請向管理員申請所需許可 (請參閱 對 Amazon Application Recovery Controller (ARC) 身分和存取進行故障診斷)
- 服務管理員 — 負責設定使用者存取權並提交相關許可請求 (請參閱 Amazon Application Recovery Controller (ARC) 功能如何與 IAM 搭配使用)
- IAM 管理員 — 撰寫政策以管理存取控制 (請參閱 Amazon Application Recovery Controller (ARC) 中的身分型政策範例)

使用身分驗證

身分驗證是您 AWS 使用身分憑證登入 的方式。您必須以 AWS 帳戶根使用者、IAM 使用者或擔任 IAM 角色身分進行身分驗證。

您可以使用身分來源的登入資料，例如 AWS IAM Identity Center (IAM Identity Center)、單一登入身分驗證或 Google/Facebook 登入資料，以聯合身分的形式登入。如需有關登入的詳細資訊，請參閱《AWS 登入 使用者指南》中的如何登入您的 AWS 帳戶。

對於程式設計存取， AWS 提供 SDK 和 CLI 以密碼編譯方式簽署請求。如需詳細資訊，請參閱《IAM 使用者指南》中的 API 請求的AWS 第 4 版簽署程序。

AWS 帳戶 根使用者

當您建立 時 AWS 帳戶，您會從一個名為 AWS 帳戶 theroot 使用者的登入身分開始，該身分可完整存取所有 AWS 服務 和 資源。強烈建議不要使用根使用者來執行日常任務。有關需要根使用者憑證的任務，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

最佳實務是要求人類使用者使用聯合身分提供者，以 AWS 服務 使用臨時憑證存取 。

聯合身分是來自您的企業目錄、Web 身分提供者的使用者，或使用來自身分來源的 AWS 服務 憑證存取 Directory Service 的使用者。聯合身分會擔任角色，而該角色會提供臨時憑證。

若需集中化管理存取權限，建議使用 AWS IAM Identity Center。如需詳細資訊，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https://docs.aws.amazon.com/IAM/latest/UserGuide/id_users.html是一種身分具備單人或應用程式的特定許可權。建議以臨時憑證取代具備長期憑證的 IAM 使用者。如需詳細資訊，請參閱《IAM 使用者指南》中的要求人類使用者使用聯合身分提供者來 AWS 使用臨時憑證存取 。

IAM 群組會指定 IAM 使用者集合，使管理大量使用者的許可權更加輕鬆。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 使用者的使用案例。

IAM 角色

IAM 角色https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html的身分具有特定許可權，其可以提供臨時憑證。您可以透過從使用者切換到 IAM 角色（主控台）或呼叫 AWS CLI 或 AWS API 操作來擔任角色。如需詳細資訊，請參閱《IAM 使用者指南》中的擔任角色的方法。

IAM 角色適用於聯合身分使用者存取、臨時 IAM 使用者許可、跨帳戶存取權與跨服務存取，以及在 Amazon EC2 執行的應用程式。如需詳細資訊，請參閱《IAM 使用者指南》中的 IAM 中的快帳戶資源存取。

使用政策管理存取權

您可以透過建立政策並將其連接到身分或資源 AWS 來控制 AWS 中的存取。政策定義與身分或資源相關聯的許可。當委託人提出請求時 AWS ， 會評估這些政策。大多數政策會以 JSON 文件 AWS 的形式存放在 中。如需進一步了解 JSON 政策文件，請參閱《IAM 使用者指南》中的 JSON 政策概觀。

管理員會使用政策，透過定義哪些主體可在哪些條件下對哪些資源執行動作，以指定可存取的範圍。

預設情況下，使用者和角色沒有許可。IAM 管理員會建立 IAM 政策並將其新增至角色，供使用者後續擔任。IAM 政策定義動作的許可，無論採用何種方式執行。

身分型政策

身分型政策是附加至身分 (使用者、使用者群組或角色) 的 JSON 許可政策文件。這類政策控制身分可對哪些資源執行哪些動作，以及適用的條件。如需了解如何建立身分型政策，請參閱《IAM 使用者指南》中的透過客戶管理政策定義自訂 IAM 許可。

身分型政策可分為內嵌政策 (直接內嵌於單一身分) 與受管政策 (可附加至多個身分的獨立政策)。如需了解如何在受管政策及內嵌政策之間做選擇，請參閱《IAM 使用者指南》中的在受管政策與內嵌政策之間選擇。

資源型政策

資源型政策是附加到資源的 JSON 政策文件。範例包括 IAM 角色信任政策與 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。您必須在資源型政策中指定主體。

資源型政策是位於該服務中的內嵌政策。您無法在資源型政策中使用來自 IAM 的 AWS 受管政策。

其他政策類型

AWS 支援其他政策類型，可設定更多常見政策類型授予的最大許可：

- 許可界限 — 設定身分型政策可授與 IAM 實體的最大許可。如需詳細資訊，請參閱《 IAM 使用者指南》中的 IAM 實體許可界限。
- 服務控制政策 (SCP) — 為 AWS Organizations中的組織或組織單位指定最大許可。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的服務控制政策。
- 資源控制政策 (RCP) — 設定您帳戶中資源可用許可的上限。如需詳細資訊，請參閱《AWS Organizations 使用者指南》中的資源控制政策 (RCP)。
- 工作階段政策 — 在以程式設計方式為角色或聯合身分使用者建立臨時工作階段時，以參數形式傳遞的進階政策。如需詳細資訊，請參《IAM 使用者指南》中的工作階段政策。

多種政策類型

當多種類型的政策適用於請求時，產生的許可會更複雜而無法理解。若要了解如何 AWS 在涉及多個政策類型時決定是否允許請求，請參閱《IAM 使用者指南》中的政策評估邏輯。

Amazon Application Recovery Controller (ARC) 功能如何與 IAM 搭配使用

如需每個 Amazon Application Recovery Controller (ARC) 功能如何與 IAM 搭配使用的詳細資訊，請參閱下列主題：

- 區域轉移的 IAM
- 區域自動轉移的 IAM
- 用於路由控制的 IAM
- 準備度檢查的 IAM
- 區域切換的 IAM

Amazon Application Recovery Controller (ARC) 中的身分型政策範例

若要查看 Amazon Application Recovery Controller (ARC) 中每個功能的身分型政策範例，請參閱各功能 AWS Identity and Access Management 章節中的下列主題：

- ARC 中區域自動轉移的身分型政策範例
- ARC 中區域轉移的身分型政策範例

- ARC 中路由控制的身分型政策範例
- ARC 中整備檢查的身分型政策範例

AWS Amazon Application Recovery Controller (ARC) 的 受管政策

如需 ARC 功能的 AWS 受管政策與受管政策的相關資訊，包括服務連結角色的受管政策，請參閱下列主題：

- 區域自動轉移的受管政策
- 路由控制的受管政策
- 準備度檢查的受管政策

Amazon Application Recovery Controller (ARC) 的 AWS 受管政策更新

檢視自此服務開始追蹤 ARC 功能之 AWS 受管政策更新以來的詳細資訊。如需此頁面變更的自動提醒，請訂閱 ARC 文件歷史記錄頁面上的 RSS 摘要。

變更	描述	Date
AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy – 新政策	Amazon Application Recovery Controller (ARC) 發佈了新的受管政策，授予區域切換計畫執行和評估的許可。 此政策提供區域切換計畫資訊的唯讀存取權、執行狀態和 Amazon CloudWatch 監控資料。它還包含模擬 IAM 主體政策以進行計劃評估的許可。	2025 年 11 月 3 日
AWSZonalAutoshiftPracticeRunSLRPolicy 受管政策 – 更新的政策	新增`AutoshiftPracticeCheckPermissions` 具有許可 `autoscaling:DescribeAutoScalingGroups` 、`elasticloadbalancing:DescribeTargetHealth` 、 和 `ec2:Descr`	2025 年 6 月 30 日

變更	描述	Date
	ibeInstances 的政策陳述式elasticloadbalancing:DescribeTargetHealth ，以支援平衡容量檢查。 如需詳細資訊，請參閱 區域自動轉移和實務執行的運作方式。	
AWSServiceRoleForPercPracticePolicy – 新政策	ARC 為自動轉移和練習執行新增了新的服務連結角色。 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 Health 儀板表 事件，以進行練習執行，並開始練習執行。 若要進一步了解新的服務連結角色，請參閱 AWSServiceRoleForZonalAutoshiftPracticeRun 的服務連結角色許可。	2023 年 11 月 30 日
AmazonRoute53RecoveryControlConfigReadOnlyAccess – 更新的政策	新增 的許可GetResourcePolicy ，以支援傳回有關共用 AWS Resource Access Manager 資源之資源政策的詳細資訊。	2023 年 10 月 18 日

變更	描述	Date

Route53RecoveryReadinessServiceRolePolicy – 已更新政策	ARC 新增了查詢 Amazon EC2 執行個體相關資訊的新許可。
	
	ARC 使用以下許可來支援輪詢 Amazon EC2 執行個體、執行整備檢查並判斷執行個體的整備狀態。
	
	`ec2:DescribeVpnGateways`
	
	`ec2:DescribeCustomerGateways`
		2023 年 2 月 17 日

Route53RecoveryReadinessServiceRolePolicy – 已更新政策	ARC 新增了查詢 Lambda 函數相關資訊的新許可。 ARC 使用以下許可來查詢 Lambda 函數的相關資訊，以執行整備檢查並判斷函數的整備狀態。 `lambda:ListProvisionedConcurrencyConfigs`	2022 年 8 月 31 日
AmazonRoute53RecoveryControlConfigFullAccess – 已更新政策	從政策中移除 Amazon Route 53 許可，並新增列出選用許可的備註。	2022 年 5 月 26 日
AmazonRoute53RecoveryControlConfigFullAccess – 已更新政策	將缺少必要的 Amazon Route 53 許可新增至政策。	2022 年 4 月 15 日

變更	描述	Date
AmazonRoute53RecoveryClusterReadOnlyAccess – 更新的政策	ARC 新增了新的許可 `route53-recovery-cluster:ListRoutingControls` ，以允許列出具有高可用性ARNs。	2022 年 3 月 15 日
AmazonRoute53RecoveryControlConfigReadOnlyAccess – 更新的政策	ARC 新增了新的許可 `route53-recovery-control-config:ListTagsForResources` ，以允許列出資源的標籤。	2021 年 12 月 20 日
Route53RecoveryReadinessServiceRolePolicy – 已更新政策	ARC 新增了查詢 Amazon API Gateway 相關資訊的新許可。 ARC 使用 許可 `apigateway:GET` 來查詢 API Gateway 的相關資訊，以執行整備檢查並判斷整備狀態。	2021 年 10 月 28 日
AmazonRoute53RecoveryReadinessReadOnlyAccess – 新增新許可	ARC 將兩個新許可新增至 AmazonRoute53RecoveryReadinessReadOnlyAccess： ARC 使用 `route53-recovery-readiness:GetArchitectureRecommendations` 和 `route53-recovery-readiness:GetCellReadinessSummary` 允許唯讀存取這些動作，以處理復原準備。	2021 年 10 月 15 日

變更	描述	Date

Route53RecoveryReadinessServiceRolePolicy – 已更新政策	ARC 新增了查詢 Lambda 函數相關資訊的新許可。
	
	ARC 使用以下許可來查詢 Lambda 函數的相關資訊，以執行整備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	Date
Route53RecoveryReadinessServiceRolePolicy – 新增了新的受管政策	ARC 新增了下列新的受管政策： AmazonRoute53RecoveryReadinessFullAccess AmazonRoute53RecoveryReadinessReadOnlyAccess AmazonRoute53RecoveryClusterFullAccess AmazonRoute53RecoveryClusterReadOnlyAccess AmazonRoute53RecoveryControlConfigFullAccess AmazonRoute53RecoveryControlConfigReadOnlyAccess	2021 年 8 月 18 日
ARC 已開始追蹤變更	ARC 開始追蹤其 AWS 受管政策的變更。	2021 年 7 月 27 日

對 Amazon Application Recovery Controller (ARC) 身分和存取進行故障診斷

使用以下資訊來協助您診斷和修正使用 Amazon Application Recovery Controller (ARC) 和 IAM 時可能遇到的常見問題。

主題

- 我無權在 ARC 中執行動作
- 我未獲得執行 iam:PassRole 的授權
- 我想要允許 以外的人員 AWS 帳戶 存取我的 ARC 資源

我無權在 ARC 中執行動作

如果 AWS 管理主控台 告訴您無權執行 動作，則必須聯絡管理員尋求協助。您的管理員是為您提供登入資料的人員。

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。

我未獲得執行 iam:PassRole 的授權

如果您收到錯誤，告知您無權執行iam:PassRole動作，您的政策必須更新，以允許您將角色傳遞給 ARC。

有些 AWS 服務 可讓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 marymajor 使用者嘗試使用主控台在 ARC 中執行動作時，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 沒有將角色傳遞給服務的許可。

```
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。

我想要允許 以外的人員 AWS 帳戶 存取我的 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：

- 若要了解 ARC 是否支援這些功能，請參閱 Amazon Application Recovery Controller (ARC) 功能如何與 IAM 搭配使用。
- 若要了解如何 AWS 帳戶 在您擁有的 資源之間提供存取權，請參閱《IAM 使用者指南》中的在您擁有 AWS 帳戶 的另一個 中為 IAM 使用者提供存取權。
- 若要了解如何將資源的存取權提供給第三方 AWS 帳戶，請參閱《IAM 使用者指南》中的將存取權提供給第三方 AWS 帳戶 擁有。
- 如需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)。
- 如需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 中的跨帳戶資源存取。

使用介面端點 () 存取 Amazon Application Recovery Controller (ARC AWS PrivateLink) 區域轉移

您可以使用 在 VPC 和 Amazon Application Recovery Controller (ARC) 區域轉移之間 AWS PrivateLink 建立私有連線。您可以像在 VPC 中一樣存取 ARC 區域轉移，無需使用網際網路閘道、NAT 裝置、VPN 連接或 Direct Connect 連線。VPC 中的執行個體不需要公有 IP 地址即可存取 ARC 區域轉移。

您可以建立由 AWS PrivateLink提供支援的介面端點來建立此私有連線。我們會在您為介面端點啟用的每個子網中建立端點網路介面。這些是申請者管理的網路界面，可做為目的地為 ARC 區域轉移之流量的進入點。

如需詳細資訊，請參閱《 AWS PrivateLink 指南》中的AWS 服務 透過 存取 AWS PrivateLink 。

ARC 區域轉移的考量事項

在您設定 ARC 區域轉移的界面端點之前，請檢閱《 AWS PrivateLink 指南》中的考量事項。

ARC 區域轉移支援透過界面端點呼叫其所有 API 動作。

建立 ARC 區域轉移的界面端點

您可以使用 Amazon VPC 主控台或 AWS Command Line Interface () 建立 ARC 區域轉移的介面端點 AWS CLI。如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「建立介面端點」。

使用下列服務名稱建立 ARC 區域轉移的介面端點：

```
com.amazonaws.region.arc-zonal-shift
```

如果您為介面端點啟用私有 DNS，您可以使用其預設的區域 DNS 名稱向 ARC 區域轉移提出 API 請求。例如 `arc-zonal-shift.us-east-1.amazonaws.com`。

為您的介面端點建立端點政策

端點政策為 IAM 資源，您可將其連接至介面端點。預設端點政策允許透過界面端點完整存取 ARC 區域轉移。若要控制允許從 VPC 進行 ARC 區域轉移的存取權，請將自訂端點政策連接至介面端點。

端點政策會指定以下資訊：

- 可執行動作 (AWS 帳戶、IAM 使用者和 IAM 角色) 的主體。
- 可執行的動作。
- 可供執行動作的資源。

如需詳細資訊，請參閱《AWS PrivateLink 指南》中的「使用端點政策控制對服務的存取」。

範例：ARC 區域轉移動作的 VPC 端點政策

以下是自訂端點政策的範例。當您將此政策連接到介面端點時，它會授予所有資源上所有委託人的所列 ARC 區域轉移動作的存取權。

```
{
   "Statement": [
      {
         "Principal": "*",
         "Effect": "Allow",
         "Action": [
            "arc-zonal-shift:ListManagedResources",
            "arc-zonal-shift:StartZonalShift",
            "arc-zonal-shift:CancelZonalShift"
         ],
         "Resource":"*"
      }
   ]
}
```

`Resource` 也可以列為 `arn:aws:elasticloadbalancing:us-east-1:111122223333:loadbalancer/app/Testing/1111111ecd42dc05`。

在 ARC 中記錄和監控

監控是維護 ARC 和您的 AWS 解決方案可用性和效能的重要部分。您應該從 AWS 解決方案的所有部分收集監控資料，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 ARC 資源和活動，以及回應潛在事件，例如 AWS CloudTrail 和 Amazon CloudWatch。

如需有關監控 ARC 中每個功能的資訊，請參閱下列主題：

- 區域轉移的記錄和監控
- 區域自動轉移的記錄和監控
- 記錄和監控路由控制
- 區域切換的記錄和監控
- 記錄和監控準備度檢查

Amazon Application Recovery Controller 的合規驗證

在多個合規計畫中，第三方稽核人員會評估 Amazon Application Recovery Controller 的安全性和 AWS 合規性。這些包括 SOC、PCI、HIPAA 等。

若要了解 是否 AWS 服務 在特定合規計劃範圍內，請參閱AWS 服務 合規計劃範圍內然後選擇您感興趣的合規計劃。如需一般資訊，請參閱AWS 合規計劃。

您可以使用 下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱在 中下載報告 AWS Artifact。

您使用 時的合規責任 AWS 服務 取決於資料的機密性、您公司的合規目標，以及適用的法律和法規。如需使用 時合規責任的詳細資訊 AWS 服務，請參閱 AWS 安全文件。

Amazon Application Recovery Controller 中的彈性

AWS 全球基礎設施是以 AWS 區域 和 可用區域為基礎建置。 AWS 區域 提供多個實體分隔和隔離的可用區域，這些可用區域與低延遲、高輸送量和高度備援聯網連接。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 全球基礎設施。

除了 AWS 全球基礎設施之外，ARC 還提供數種功能，以協助支援您的資料彈性和備份需求。

Amazon Application Recovery Controller 中的基礎設施安全性

作為受管服務， 受到 AWS 全球網路安全的保護。如需 AWS 安全服務以及 如何 AWS 保護基礎設施的相關資訊，請參閱AWS 雲端安全。若要使用基礎設施安全最佳實務來設計您的 AWS 環境，請參閱安全支柱 AWS Well-Architected Framework 中的基礎設施保護。

您可以使用 AWS 發佈的 API 呼叫，透過網路存取 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。

Amazon Application Recovery Controller (ARC) 開發人員指南的文件歷史記錄

下列項目說明對 Amazon Application Recovery Controller (ARC) 文件所做的重要變更。

- 版本：最新版本
- 文件最近更新時間：2026 年 3 月 31 日

變更	描述	Date
準備度檢查可用性變更	自 2026 年 4 月 30 日起，Amazon Application Recovery Controller (ARC) 中的整備檢查功能將不再開放給新客戶使用。現有客戶可以繼續正常使用該服務。 如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 整備檢查可用性變更。	2026 年 3 月 31 日
區域切換計劃執行的新受管政策	Amazon Application Recovery Controller (ARC) 發佈了新的受管政策 `AmazonApplicationRecoveryControllerRegionSwitchPlanExecutionPolicy` ，授予區域切換計畫執行和評估的許可。 如需詳細資訊，請參閱 AWS 受管政策的 Amazon Application Recovery Controller (ARC) 更新。	2025 年 11 月 3 日

變更	描述	Date
您現在可以在 VPC 和 Amazon Application Recovery Controller (ARC) 區域轉移 AWS PrivateLink 之間使用 。	您可以使用 AWS PrivateLink 在 VPC 和 Amazon Application Recovery Controller (ARC) 區域轉移之間建立私有連線。 如需詳細資訊，請參閱使用介面端點 () 存取 Amazon Application Recovery Controller (ARC AWS PrivateLink) 區域轉移。	2025 年 8 月 11 日
新的區域切換服務	區域切換可讓客戶協調在另一個區域之外操作多區域應用程式所需的特定步驟，支援跨帳戶 AWS 區域。 如需詳細資訊，請參閱 ARC 中的區域切換。	2025 年 8 月 1 日
練習執行的增強功能	您現在可以在 ARC 中開始隨需練習執行。此外，實務執行現在包括檢查區域中其他AZs的足夠容量。 如需詳細資訊，請參閱其運作方式。	2025 年 6 月 30 日

變更	描述	Date
更新受管政策	透過新增`Autoshift PracticeCheckPermissions` 具有許可 `autoscaling:DescribeAutoScalingGroups` 、`ec2:DescribeInstances` 、 和 的政策陳述式`elasticloadbalancing:DescribeTargetHealth` 來更新`AWSZonalAutoshiftPracticeRunSLRPolicy` 受管政策`elasticloadbalancing:DescribeTargetHealth` ，以支援平衡容量檢查。 如需詳細資訊，請參閱 AWSZonalAutoshiftPracticeRunSLRPolicy 受管政策。	2025 年 6 月 30 日
區域自動轉移例外類型的更新	您現在可以根據資源與區域自動轉移互動。 如需詳細資訊，請參閱其運作方式。	2025 年 4 月 21 日
使用 測試 ARC 區域自動轉移 AWS FIS	您可以使用 AWS FIS 來測試 ARC 區域自動轉移如何在 AZ 電源中斷期間自動復原您的應用程式 如需詳細資訊，請參閱使用 測試區域自動轉移 AWS FIS。	2025 年 3 月 26 日

變更	描述	Date
ARC 現在支援 IPv6 端點進行路由控制和區域轉移。	ARC 現在支援 IPv6 端點進行路由控制和區域轉移。 如需詳細資訊，請參閱設定路由控制元件。	2024 年 11 月 21 日
Amazon EC2 Auto Scaling 群組的區域轉移功能	ARC 現在支援 Amazon EC2 Auto Scaling 群組的區域轉移。 如需詳細資訊，請參閱支援 Amazon EC2 Auto Scaling 群組。	2024 年 11 月 18 日
Amazon EKS 的區域轉移功能	您可以為 Amazon EKS 叢集啟動區域轉移，也可以透過啟用區域自動轉移 AWS 來允許 為您執行。藉助此區域轉移，可將叢集中的東向西網路流量更新為只考慮正常運作 AZ 中工作節點上執行之 Pod 的網路端點。 如需詳細資訊，請參閱支援 Amazon Elastic Kubernetes Service。	2024 年 10 月 22 日
Network Load Balancer 的區域轉移功能	ARC 現在支援啟用跨區域或停用跨區域組態的 Network Load Balancer 區域轉移。 如需詳細資訊，請參閱支援 Network Load Balancer。	2024 年 10 月 11 日

變更	描述	Date
Autoshift 觀察器通知	透過自動轉移觀察器通知，您可以設定區域自動轉移，在每當 AWS 開始自動轉移時透過 Amazon EventBridge 通知您，以將流量移離可能受損的可用區域。您不需要使用區域自動轉移設定任何特定資源，即可啟用這些個別的通知。 如需詳細資訊，請參閱搭配 Amazon EventBridge 使用區域自動轉移。	2024 年 7 月 12 日
每個功能的文件重組	重組開發人員指南內容，以孤立成子開發指南。也就是說，現在有不同的區段包含 ARC 中每個功能的完整資訊：區域轉移和區域自動轉移用於多可用區域復原，以及路由控制和多區域復原準備度檢查。 如需詳細資訊，請參閱什麼是 Amazon Application Recovery Controller (ARC)。	2024 年 4 月 30 日
新增區域自動轉移功能	在 ARC 中新增新功能，您授權 AWS 代表您從可用區域轉移應用程式的資源流量，以協助縮短事件期間的復原時間。 如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 中的區域自動轉移。	2023 年 11 月 30 日

變更	描述	Date
新增服務連結角色	為區域自動轉移實務執行新增新的服務連結角色 AWSServiceRoleForZonalAutoshiftPracticeRun。 如需詳細資訊，請參閱 AWSServiceRoleForZonalAutoshiftPracticeRun 的服務連結角色許可。	2023 年 11 月 30 日
新增叢集的跨帳戶支援	使用 新增 ARC 中叢集的跨帳戶支援 AWS Resource Access Manager，讓您可以輕鬆且安全地使用一個叢集來託管數個不同 AWS 帳戶所擁有的控制面板和路由控制。 如需詳細資訊，請參閱支援 ARC 中叢集的跨帳戶。	2023 年 10 月 18 日
更新受管政策	更新 `AmazonRoute53RecoveryControlConfigReadOnly` 受管政策以新增 的許可`GetResourcePolicy` ，以支援傳回有關共用 AWS Resource Access Manager 資源之資源政策的詳細資訊。 如需詳細資訊，請參閱 AWS 受管政策。	2023 年 9 月 19 日

變更	描述	Date
已更新服務連結角色	將新的許可 `ec2:DescribeVpnGateways` 和 `ec2:DescribeCustomerGateways` 新增至 ARC 的服務連結角色，以支援輪詢 Amazon EC2 執行個體。 如需詳細資訊，請參閱使用 ARC 的服務連結角色。	2023 年 2 月 17 日
區域轉移的 GA 版本	支援 ARC 區域轉移的 GA 版本，其中包括在 ARC 中註冊區域轉移的受管資源的屬性型存取控制 (ABAC)。 如需詳細資訊，請參閱使用 ARC 的屬性型存取控制 (ABAC)。	2023 年 1 月 10 日
新增了新的多可用區域轉移	新增描述多可用區域應用程式 ARC、區域轉移中新服務的內容。您可以開始區域轉移，將負載平衡器資源的流量暫時移離可用區域。 如需詳細資訊，請參閱 ARC 中的區域轉移。	2022 年 11 月 28 日
已更新服務連結角色	已將新的許可 新增至 ARC 的服務連結角色`lambda:ListProvisionedConcurrencyConfigs` ，以查詢 Lambda 函數的相關資訊。 如需詳細資訊，請參閱使用 ARC 的服務連結角色。	2022 年 8 月 31 日

變更	描述	Date
已更新受管政策	已更新 AmazonRoute53RecoveryControlConfigFullAccess 受管政策以移除 Amazon Route 53 許可，並將其列為選用。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策。	2022 年 5 月 26 日
已更新受管政策	已更新 AmazonRoute53RecoveryControlConfigFullAccess 受管政策，以包含必要的 Amazon Route 53 許可。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策。	2022 年 4 月 15 日
新增新清單路由控制 API 的 CLI 範例	新增了範例 CLI 命令和新清單路由控制 API 操作的最佳實務建議，包含在非常可靠的 ARC 資料平面 API 中。 如需詳細資訊，請參閱列出和更新路由控制和狀態。	2022 年 3 月 31 日

變更	描述	Date
新增覆寫安全規則的支援	新增覆寫安全規則的支援，這可讓您繞過使用您設定的安全規則強制執行的路由控制保護措施。可能需要安全規則覆寫，例如，在容錯移轉期間，在「中斷玻璃」案例中進行災難復原。 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
新增其他標記支援	新增在 ARC 中標記其他資源的支援，包括叢集、控制面板、路由控制和安全規則。 如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 中的標記。	2021 年 12 月 20 日
已更新受管政策	已更新 `AmazonRoute53RecoveryControlConfigReadOnly` 受管政策，以新增列出資源標籤的許可。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策	2021 年 12 月 20 日

變更	描述	Date
新增使用 EventBridge 即時警示的支援	新增對 EventBridge 的支援，這表示您現在可以新增規則以取得警示，並對 ARC 整備檢查狀態變更採取動作，例如，狀態從 READY 變更為 NOT READY。 如需詳細資訊，請參閱搭配 Amazon EventBridge 使用 ARC。	2021 年 12 月 20 日
新增路由控制狀態程式碼範例	新增程式碼範例，說明當您使用 API 操作來取得或更新路由控制狀態時，會依序嘗試叢集端點。 如需詳細資訊，請參閱 Amazon Application Recovery Controller (ARC) 的 API 範例。	2021 年 11 月 16 日
已將新許可新增至唯讀政策	已將兩個新許可新增至政策 `AmazonRoute53RecoveryReadinessReadOnlyAccess` ：`route53-recovery-readiness:GetArchitectureRecommendations` 和 `route53-recovery-readiness:GetCellReadinessSummary` 。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策。	2021 年 11 月 9 日

變更	描述	Date
新增對 Amazon API Gateway 資源類型的支援	新增了新的資源類型 Amazon API Gateway，並更新了 ARC 服務連結角色許可，以便 ARC 可以使用準備程度檢查稽核 API Gateway。 如需詳細資訊，請參閱就緒規則和支援的資源類型，以及使用 ARC 的服務連結角色。	2021 年 10 月 28 日
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 ARC 服務連結角色許可，以便 ARC 可以使用整備檢查稽核 Lambda 函數。 如需詳細資訊，請參閱就緒規則和支援的資源類型，以及使用 ARC 的服務連結角色。	2021 年 10 月 8 日
新增 CloudFormation 和 Terraform 範本的連結	新增可下載 CloudFormation 和 Hashicorp Terraform 範本的連結，協助您快速開始使用 ARC。如需詳細資訊，請參閱使用新應用程式的復原準備。	2021 年 9 月 13 日

變更	描述	Date
新增了新的 受管政策	新增下列 ARC AWS 受管政策：AmazonRoute53RecoveryReadinessFullAccess 、AmazonRoute53RecoveryReadinessReadOnlyAccess 、AmazonRoute53RecoveryClusterFullAccess 、AmazonRoute53RecoveryControlConfigFullAccess 、AmazonRoute53RecoveryClusterReadOnlyAccess 和 AmazonRoute53RecoveryControlConfigReadOnlyAccess 。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策。	2021 年 8 月 18 日
開始追蹤 Amazon Application Recovery Controller (ARC) 的 AWS 受管政策	受管政策的更新將從初始發行日期開始追蹤。 如需詳細資訊，請參閱 AWS Amazon Application Recovery Controller (ARC) 的 受管政策。	2021 年 7 月 27 日

變更	描述	Date
Amazon Application Recovery Controller (ARC) 的初始版本	ARC 透過集中協調 AWS 區域內或跨多個區域的容錯移轉來改善應用程式的可用性。ARC 提供整備檢查，以確保您的應用程式已擴展處理容錯移轉流量，並設定為繞過故障進行路由。它還提供非常可靠的路由控制，以便您可以透過重新路由流量來復原應用程式，例如跨可用區域或區域。如需詳細資訊，請參閱什麼是 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。