開發人員指南

AWS Backup

AWS Backup: 開發人員指南

Table of Contents

什麼是 AWS Backup？

AWS Backup 這是一項全受管服務，可讓您輕鬆地跨服 AWS 務、雲端和內部部署集中及自動化資料保護。使用此服務，您可以在單一位置設定備份原則和監視資 AWS 源的活動。它可讓您自動化和合併先前執行的備份工作 service-by-service，並且不需要建立自訂指令碼和手動程序。只要在 AWS Backup 主控台按幾下，您就能將資料保護政策和排程自動化。

AWS Backup 不會管理您在 AWS 環境中進行之外的備份 AWS Backup。因此，如果您想要集中式的 end-to-end 解決方案來滿足商業和法規遵循要求，請 AWS Backup 立即開始使用。

支援的 AWS 資源和第三方應用

以下是您可以使用備份和還原的 AWS 資源和協力廠商應用程式 AWS Backup。

支援的資源	支援的資源類型
Amazon Elastic Compute Cloud (Amazon EC2)	Amazon EC2 執行個體 (不包括支援執行個體儲存體的 AMI)
Amazon Simple Storage Service (Amazon S3)	Amazon S3 資料
Amazon Elastic Block Store (Amazon EBS)	Amazon EBS 磁碟區
Amazon DynamoDB	Amazon DynamoDB 資料表
Amazon Relational Database Service (Amazon RDS)	Amazon RDS 資料庫執行個體 (包括所有資料庫引擎)；多可用區域叢集
Amazon Aurora	Aurora 叢集
Amazon Elastic File System (Amazon EFS)	Amazon EFS 檔案系統
FSx for Lustre	FSx for Lustre 檔案系統

支援的資源	支援的資源類型
FSx for Windows File Server	FSx for Windows File Serve 檔案系統
Amazon FSx NetApp	FSx for OnTAP 檔案系統
Amazon FSx for OpenZFS	FSx for OpenZFS 檔案系統
AWS Storage Gateway (磁碟區閘道)	AWS Storage Gateway 磁碟區
Amazon DocumentDB	Amazon DocumentDB 叢集
Amazon Neptune	Amazon Neptune 叢集
Amazon Redshift	Amazon Redshift 叢集
Amazon Timestream	Amazon Timestream 叢集
VMware 雲端™ 開啟 AWS	VMware 雲端™ 虛擬機器 AWS
VMware 雲端™ 開啟 AWS Outposts	VMware 雲端™ 虛擬機器 AWS Outposts
AWS CloudFormation	AWS CloudFormation 堆疊
SAP HANA 資料庫	Amazon EC2 執行個體上的 SAP HANA 資料庫

適用於所有支援資源的功能

AWS Backup 功能是根據資源和 AWS 區域. 下列各節和表格可協助您判斷功能可用性。

AWS Backup 為其支援的 AWS 服務以及支援的協力廠商應用程式提供下列功能。除非明確提及，否則不應假設支援任何功能或服務。

- 自動化備份排程與保留管理
- 集中式備份監控

- 增量備份，但 DynamoDB、Aurora、DocumentDB 和 Neptune 除外。
- AWS KMS整合式備份加密
- 跨帳戶管理 AWS Organizations
- 使用稽核管理員自動化備份 AWS Backup 稽核與報告
- 使用文件庫鎖定一次、多讀 (WORM) AWS Backup

各資源的功能可用性

要在特定地區 AWS Backup 與支持的 AWS 服務一起使用，該服務必須在該地區提供。若要判斷某個區域的服務可用性，請參閱《AWS 一般參考》中的服務端點。

AWS Backup 支持	跨區域備份	跨帳戶備份	AWS Backup Audit Manager	增量備份	持續備份與 point-in-time 還原 (PITR)	全面 AWS Backup 管理	生命週期至冷儲存	項目層級還原 ‡	還原測試
EC2	✓	✓	✓	✓					✓
S3	✓	✓	✓	✓	✓	✓		✓	✓
EBS	✓	✓	✓	✓					✓
RDS 單一執行個體	✓*	✓*	✓**	✓	✓				✓
RDS 叢集	✓*	✓*	✓**	✓					✓
Aurora	✓*	✓*	✓	✓+	✓				✓
EFS	✓	✓	✓	✓		✓	✓	✓	✓

AWS Backup 支持	跨區域備份	跨帳戶備份	AWS Backup Audit Manager	增量備份	持續備份與 point-in-time 還原 (PITR)	全面 AWS Backup 管理	生命週期至冷儲存	項目層級還原 ‡	還原測試
FSx for Lustre	✓	✓	✓	✓					✓
FSx for Windows File Server	✓	✓	✓	✓					✓
FSx for OnTAP			✓†	✓					✓
FSx for OpenZF	✓	✓	✓	✓					✓
Storage Gateway	✓	✓	✓	✓					
Documer B	✓*	✓*	✓						✓
Neptune	✓*	✓*	✓						✓
Amazon Redshift								✓	
Timestre m	✓	✓	✓	✓		✓	✓	✓	

AWS Backup 支持	跨區域備份	跨帳戶備份	AWS Backup Audit Manager	增量備份	持續備份與 point-in-time 還原 (PITR)	全面 AWS Backup 管理	生命週期至冷儲存	項目層級還原 ‡	還原測試
Windows VSS	✓	✓	✓	✓					
虛擬機器	✓	✓	✓	✓		✓	✓	✓	
CloudFormation 模板	✓	✓		✓'		✓	✓'		
DynamoDB (不含 AWS Backup 進階功能)			✓						✓
DynamoDB (含 AWS Backup 進階功能)	✓	✓	✓			✓	✓		✓
Amazon EC2 執行個體上的 SAP HANA 資料庫				✓	✓	✓	✓		

某些資源類型同時提供連續備份以及跨區域和跨帳戶複製功能。建立連續備份的跨區域或跨帳戶複本時，複製的復原點 (備份) 會變成快照 (定期) 備份。PITR (時間點還原) 不適用於這些複本。

* RDS、Aurora、DocumentDB 和 Neptune 不支援同時執行跨區域和跨帳戶備份的單一複製動作。您只能選擇其中一項。您也可以使用 AWS Lambda 指令碼偵聽第一個複本的完成，執行第二個複本，然後刪除第一個複本。RDS 多可用區域 (Multi-AZ) 資料庫執行個體可以複製，但 Multi-AZ 叢集目前不支援跨區域或跨帳戶複製。

+ AWS Backup 支援 Aurora 快照，以增量備份或完整備份計費。

** 如需提供 Backup Audit Manager 支援的區域，請參閱 RDS 多可用性區域備份。

†「 AWS Backup Audit Manager 程式」在所有控制項中支援此資源，跨帳戶副本與跨區域副本除外。

‡ 項目層級還原中的「項目」會根據支援的資源而有所不同。例如，檔案系統項目是檔案或目錄，而 S3 項目則是 S3 物件。VMware 項目是磁碟。如需詳細資訊，請參閱支援資源的還原備份一節。

'在CloudFormation 堆疊備份中，巢狀資源會保留其來源資源的功能。不過，堆疊中的資源不會保留時間點還原 (PITR) 功能 (例如 S3 和 RDS)。上面矩陣中的屬性僅適用於 CloudFormation 模板，而不適用於堆棧中的資源。

功能可用性 AWS 區域

AWS Backup 可在以下所有內容中使用 AWS 區域。 AWS Backup 除非下表另有說明，否則所有這些區域都可以使用功能。

AWS Backup 支持	跨區域備份	跨帳戶管理	跨帳戶備份	AWS Backup Audit Manager 和工作儀表板	還原測試
美國東部 (俄亥俄)	✓	✓	✓	✓	✓
美國東部 (維吉尼亞北部)	✓	✓	✓	✓	✓
美國西部 (加利佛尼亞北部)	✓	✓	✓	✓	✓

AWS Backup 支持	跨區域備份	跨帳戶管理	跨帳戶備份	AWS Backup Audit Manager 和工作儀表板	還原測試
美國西部 (奧勒岡)	✓	✓	✓	✓	✓
非洲 (開普敦)	✓		✓	✓	✓
亞太區域 (香港)	✓		✓	✓	✓
亞太區域 (海德拉巴)	✓		✓		✓
亞太區域 (雅加達)	✓		✓		✓
亞太區域 (墨爾本)	✓		✓		✓
亞太區域 (孟買)	✓	✓	✓	✓	✓
亞太區域 (大阪)	✓	✓	✓		✓
亞太區域 (首爾)	✓	✓	✓	✓	✓
亞太區域 (新加坡)	✓	✓	✓	✓	✓
亞太區域 (雪梨)	✓	✓	✓	✓	✓
亞太區域 (東京)	✓	✓	✓	✓	✓

AWS Backup 支持	跨區域備份	跨帳戶管理	跨帳戶備份	AWS Backup Audit Manager 和工作儀表板	還原測試
加拿大 (中部)	✓	✓	✓	✓	✓
中國 (北京)	✓				
中國 (寧夏)	✓				
歐洲 (法蘭克福)	✓	✓	✓	✓	✓
歐洲 (愛爾蘭)	✓	✓	✓	✓	✓
歐洲 (倫敦)	✓	✓	✓	✓	✓
歐洲 (米蘭)	✓		✓	✓	✓
Europe (Paris)	✓	✓	✓	✓	✓
歐洲 (西班牙)	✓		✓		✓
歐洲 (斯德哥爾摩)	✓	✓	✓	✓	✓
歐洲 (蘇黎世)	✓		✓		✓
以色列 (特拉維夫)	✓		✓		
Middle East (Bahrain)	✓		✓	✓	✓
中東 (阿拉伯聯合大公國)			✓		✓

AWS Backup 支持	跨區域備份	跨帳戶管理	跨帳戶備份	AWS Backup Audit Manager 和工作儀表板	還原測試
南美洲 (聖保羅)	✓	✓	✓	✓	✓
AWS GovCloud (美國東部)	✓	✓	✓	✓	
AWS GovCloud (美國西部)	✓	✓	✓	✓	

中國 (北京) 和中國 (寧夏) 支援從這兩個區域的其中一個到另一個的跨區域複製。不支援「從」這些區域到其他區域或這些區域內的跨區域複製。這些區域不支援跨帳戶複製。

目前 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 不提供「工作」控制面板。工作儀表板彙總僅適用於支援跨帳戶管理和 AWS Backup 稽核管理員的區域。

目前在中國 (北京)、中國 (寧夏)、(美國東部) 和 AWS GovCloud AWS GovCloud (美國西部) 區域不提供 Amazon EBS 冷儲存存檔層。

支援的服務 AWS 區域

AWS Backup 在所有受支援的區域中支援 Aurora、DynamoDB、具有 AWS Backup 進階功能、Amazon EBS、Amazon EC2、Amazon EFS、亞馬遜紅移和亞馬遜 RDS。

下列區域支援指定的服務：

區域和服務	Amazon FSx	EC2 執行個體上的 SAP HANA	Amazon Simple Storage Service (Amazon S3)	Storage Gateway	Amazon Timestream	VMware
美國東部 (維吉尼亞北部)	✓	✓	✓	✓	✓	✓
美國東部 (俄亥俄)	✓	✓	✓	✓	✓	✓
美國西部 (加利佛尼亞北部)	Windows；Lustre；ONTAP	✓	✓	✓	✓	✓
美國西部 (奧勒岡)	Windows；Lustre；ONTAP	✓	✓	✓	✓	✓
非洲 (開普敦)	Windows；Lustre；ONTAP	✓	✓ (無跨帳戶/跨區域複製)	✓	✓	✓
亞太區域 (香港)	✓	✓	✓ (無跨帳戶/跨區域複製)	✓	✓	✓
亞太區域 (海德拉巴)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)			
亞太區域 (雅加達)	Windows；Lustre；ONTAP		✓	✓		

區域和服務	Amazon FSx	EC2 執行個體上的 SAP HANA	Amazon Simple Storage Service (Amazon S3)	Storage Gateway	Amazon Timestream	VMware
亞太區域 (墨爾本)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)			
亞太區域 (孟買)	✓	✓	✓	✓	✓	✓
亞太區域 (大阪)	Windows；Lustre	✓	✓ (無跨帳戶/跨區域複製)			✓
亞太區域 (首爾)	✓	✓	✓	✓	✓	✓
亞太區域 (新加坡)	✓	✓	✓	✓	✓	✓
亞太區域 (雪梨)	✓	✓	✓	✓	✓	✓
亞太區域 (東京)	✓	✓	✓	✓	✓	✓
加拿大 (中部)	✓	✓	✓	✓	✓	✓
中國 (北京)	Windows；Lustre		✓ (無跨帳戶複製)	✓	✓	
中國 (寧夏)	Windows；Lustre		✓ (無跨帳戶複製)	✓	✓	

區域和服務	Amazon FSx	EC2 執行個體上的 SAP HANA	Amazon Simple Storage Service (Amazon S3)	Storage Gateway	Amazon Timestream	VMware
歐洲 (法蘭克福)	✓	✓	✓	✓	✓	✓
歐洲 (愛爾蘭)	✓	✓	✓	✓	✓	✓
歐洲 (倫敦)	✓	✓	✓	✓	✓	✓
歐洲 (米蘭)	Windows；Lustre；ONTAP	✓	✓ (無跨帳戶/跨區域複製)	✓	✓	✓
Europe (Paris)	Windows；Lustre；ONTAP	✓	✓	✓	✓	✓
歐洲 (西班牙)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)			
歐洲 (斯德哥爾摩)	✓	✓	✓	✓	✓	✓
歐洲 (蘇黎世)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)			
以色列 (特拉維夫)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)			

區域和服務	Amazon FSx	EC2 執行個體上的 SAP HANA	Amazon Simple Storage Service (Amazon S3)	Storage Gateway	Amazon Timestream	VMware
Middle East (Bahrain)	Windows；Lustre；ONTAP	✓	✓ (無跨帳戶/跨區域複製)	✓	✓	✓
中東 (阿拉伯聯合大公國)			✓ (無跨帳戶/跨區域複製)			
南美洲 (聖保羅)		✓	✓	✓	✓	✓
AWS GovCloud (美國西部)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)	✓	✓	✓
AWS GovCloud (美國東部)	Windows；Lustre；ONTAP		✓ (無跨帳戶/跨區域複製)	✓	✓	✓

在 Amazon FSx 下方的檢查表示該區域全部支援 FSx for Windows File Server 的 FSx、FSx for Lustre 的 FSx、用於 ONTAP 的 FSx 以及 OpenZF 的 FSx，否則會列出支援的組態。 AWS Backup

功能概觀

AWS Backup 提供許多功能和功能，包括：

集中式備份管理

AWS Backup 提供集中式備份主控台、一組備份 API，以及 AWS Command Line Interface (AWS CLI) 來管理應用程式所使用之 AWS 服務的備份。您可以使用 AWS Backup集中管理符合備份需求的備份原則。然後，您可以將它們套用至跨 AWS 服務的 AWS 資源，讓您能夠以一致且合規的方式備份應用程

式資料。 AWS Backup 集中式備份主控台提供備份和備份活動記錄的整合檢視，讓您更輕鬆地稽核備份並確保合規性。

以政策為基礎的備份

您可以使 AWS Backup用建立稱為備份計畫的備份原則。您可以使用這些備份計畫來定義備份需求，然後將其套用至您要在所使用 AWS 服務之間保護的 AWS 資源。您可以建立不同的備份計劃，而每個計劃皆符合特定的商業規範及合規要求。這有助於確保根據您的需求備份每個 AWS 資源。您能夠透過備份計劃，以可擴展的方式輕鬆地在整個組織和應用程式間強制實施備份策略。

如需備份計畫的所有組態選項，請參閱備份計畫選項和組態。

以標籤為基礎的備份政策

您可以使 AWS Backup 用多種方式將備份計劃套用至 AWS 資源，包括標記它們。標記可讓您更輕鬆地在所有應用程式中實作備份策略，並確保您的所有 AWS 資源都受到備份和保護。 AWS 標籤是組織和分類 AWS 資源的好方法。與 AWS 標籤整合可讓您快速將備份計畫套用至一組 AWS 資源，以便以一致且合規的方式進行備份。

如需將資源指派給備份計畫的所有方法，請參閱將資源指派至備份計畫。

生命週期管理政策

AWS Backup 透過將備份儲存在低成本的冷儲存層 (備份到冷存儲是完整備份)，使您能夠滿足合規要求，同時最大限度地降低備份存儲成本。您可以設定生命週期政策，讓系統依據定義的排程自動將備份從溫儲存層移轉至冷儲存層。

如需可轉移至不常用儲存的資源清單，請參閱各資源的功能可用性。如需在備份計畫中開啟不常用儲存的步驟，請參閱生命週期和儲存層。

跨區域備份

使用時 AWS Backup，您可以根據需要將備份複製到多個不同 AWS 區域 的備份，或自動作為排程備份計劃的一部分。如果您有業務持續性或合規性要求，需要將備份儲存在與生產資料最短距離的位置，則跨區域備份特別有用。如需詳細資訊，請參閱跨 AWS 區域建立備份複本。

跨帳戶管理和跨帳戶備份

您可以使用 AWS Backup 來管理AWS Organizations結構 AWS 帳戶 內所有內部的備份。藉由跨帳戶管理，您可以自動使用備份政策，對組織內的 AWS 帳戶 套用備份計畫。如此可大規模提高合規性和

資料保護，並降低營運開銷。它也有助於避免在個別帳戶間手動複製備份計畫。如需詳細資訊，請參閱管理多個 AWS 帳戶的 AWS Backup 資源。

您也可以將備份複製到 AWS Organizations 管理結構 AWS 帳戶 內的多個不同備份。如此一來，您就可以將備份「扇入」到單一儲存庫帳戶，然後「扇出」備份來獲得更高的復原能力。跨 AWS 帳戶建立備份複本。

您必須先在 AWS Organizations中設定現有的組織結構，然後才能使用跨帳戶管理和跨帳戶備份功能。組織單位 (OU) 是可以當做單一實體來管理的帳戶群組。 AWS Organizations 是可以分組為組織單位並作為單一實體進行管理的帳戶清單。

稽核管理員的 AWS Backup 稽核與報告

AWS Backup Audit Manager 可協助您簡化備份的資料控管與法規遵循管理 AWS。 AWS Backup Audit Manager 提供內建、可自訂的控制項，讓您能夠符合您的組織需求。您也可以使用這些控制項自動追蹤備份活動和資源。

AWS Backup Audit Manager 可協助您尋找尚未與您定義之控制項相容的特定活動和資源。此外，還會產生每日報告，以便您做為控制項隨著時間符合規範的證據。

若要將備份合規性納入整體符合性狀態，您可以自動將 AWS Backup Audit Manager 發現項目匯入到中 AWS Audit Manager。

增量備份

AWS Backup 有效地以增量方式儲存您的定期備份。 AWS 資源的第一次備份會備份資料的完整複本。對於每個後續的增量備份，只會備份對資 AWS 源的變更。增量備份可讓您的資料獲得經常備份的保護，同時又能將儲存成本降至最低 (備份至冷儲存是完整備份)。

如需支援增量備份的資源清單，請參閱各資源的功能可用性。

全面 AWS Backup 管理

某些資源類型支援完整 AWS Backup 管理。全面 AWS Backup 管理的好處包括：

- 獨立加密。 AWS Backup 使用 AWS Backup 保管庫的 KMS 金鑰自動加密備份，而不是使用與來源資源相同的加密金鑰。這增加了您的防禦層。如需詳細資訊，請參閱中備份的加密 AWS Backup。
- **awsbackup** Amazon Resource Name (ARN)。Backup ARN 的開頭為 `arn:aws:`*`source-resource`*，而不是 `arn:aws:backup`。這可讓您建立專門套用至備份 (而非來源資源) 的存取政策。如需詳細資訊，請參閱存取控制。

- 集中式備份計費和 Cost Explorer 成本分配標籤。費用 AWS Backup (包括儲存、資料傳輸、還原和提前刪除) 會顯示在 Amazon Web Services 帳單中的「Backup」下方，而不會顯示在每個支援的資源下方。您也可以使用 Cost Explorer 成本分配標籤來追蹤和最佳化備份成本。如需詳細資訊，請參閱計量、成本和帳單。

若要查看哪些資源類型適用於完全 AWS Backup 管理，請參閱各資源的功能可用性。

監控備份活動

AWS Backup 提供儀表板，可讓您輕鬆稽核跨 AWS 服務的備份和還原活動。只要在 AWS Backup 主控台按幾下，您就可以檢視最近備份工作的狀態。您也可以跨 AWS 服務還原工作，以確保您的 AWS 資源受到適當的保護。

AWS Backup 與 Amazon CloudWatch 和 Amazon 集成 EventBridge。 CloudWatch 可讓您追蹤指標並建立警示。 EventBridge 可讓您檢視和監視 AWS Backup 事件。如需詳細資訊，請參閱使用監視 AWS Backup 事件 EventBridge和使用監視 AWS Backup 指標 CloudWatch。

AWS Backup 與 AWS CloudTrail. CloudTrail 提供備份活動記錄的整合檢視，讓您快速輕鬆地稽核資源的備份方式。 AWS Backup 還與 Amazon Simple Notification Service (Amazon SNS) 整合，為您提供備份活動通知，例如備份成功或已啟動還原時。如需詳細資訊，請參閱使用 Amazon SNS 記錄 AWS Backup API 呼叫 CloudTrail和使用 Amazon SNS 追蹤 AWS Backup 事件。

保護備份文件庫中的資料

每個 AWS Backup 備份的內容都是不可變的，這意味著沒有人可以更改該內容。 AWS Backup 進一步保護備份儲存庫中的備份，以便將它們與來源執行個體安全地分開。例如，即使您刪除來源 Amazon EC2 執行個體和 Amazon EBS 磁碟區，您的文件庫仍會根據您選擇的生命週期政策保留 Amazon EC2 和 Amazon EBS 備份。

備份文件庫提供加密和以資源為基礎的存取政策，讓您能定義可存取備份的使用者。您能夠針對備份文件庫定義存取政策，進而定義可存取該文件庫中備份的使用者，以及其可執行的操作。這提供了一種簡單而安全的方式來控制跨 AWS 服務備份的存取。若要檢閱 AWS 和客戶管理的政策 AWS Backup，請參閱的受管政策 AWS Backup。

您可以使用文件 AWS Backup 庫鎖定來防止任何人（包括您）刪除備份或更改其保留期。 AWS Backup 文件庫鎖定可協助您強制執行 write-once-read-many(WORM) 模型，並為您的防禦深度增加另一層防禦。若要開始使用，請參閱AWS Backup Vault Lock。

合規義務的支援

AWS Backup 協助您履行全球法規遵循義務。 AWS Backup 在以下 AWS 合規計劃的範圍內：

- FedRAMP High
- GDPR
- SoC 1、2 和 3
- PCI
- HIPAA
- 以及更多

開始使用

要了解更多信息 AWS Backup，我們建議您從開始開始使用 AWS Backup。

AWS Backup：運作方式

AWS Backup 是一項全受管備份服務，可讓您輕鬆集中管理及自動化跨 AWS 服務的資料備份。您可以使 AWS Backup用建立稱為備份計畫的備份原則。您可以使用這些計劃來定義備份需求，例如備份資料的頻率，以及這些備份的保留時間。

AWS Backup 讓您只需標記 AWS 資源，即可將備份計劃套用至資源。 AWS Backup 然後根據您定義的備份計劃自動備份 AWS 資源。

下列各節說明 AWS Backup 運作方式、實作詳細資訊及安全性考量。

主題

如何使 AWS Backup 用支援的 AWS 服務

部分 AWS Backup支援的 AWS 服務提供自己的獨立備份功能。無論您是否使用 AWS Backup，這些功能都可供您使用。不過，其他 AWS 服務建立的備份無法透過中央控管使用 AWS Backup。

若 AWS Backup 要設定為集中管理所有支援服務的資料保護，您必須選擇使用管理該服務 AWS Backup、建立隨選備份或使用備份計劃排程備份，並將備份儲存在備份保存庫中。

主題

- 使用 Amazon RDS 及 Aurora
- 使用 AWS BackInt
- 使用 AWS Storage Gateway
- 使用 Amazon DocumentDB
- 使用 Amazon Neptune
- 使用 Amazon Timestream
- 使用 AWS Organizations
- 使用 AWS CloudFormation
- 與 AWS BackInt SAP 和 SAP HANA 一起工作 AWS Systems Manager
- AWS 服務如何備份自己的資源

選擇使用以下方式管理服務 AWS Backup

當新 AWS 服務可用時，您必須啟用 AWS Backup 才能使用這些服務。如果您嘗試使用來自未啟用服務的資源建立隨需備份或備份計劃，您會收到錯誤訊息，而且無法完成程序。

主 AWS Backup 控台有兩種方式可將資源類型納入備份計畫中：在備份計畫中明確指派資源類型或包含所有資源。請參閱下列要點，以了解這些選項如何與選擇加入服務搭配運作。

- 如果資源指派僅以標籤為基礎，則會套用選擇加入服務設定。
- 如果將資源類型明確指派給備份計畫 (例如 Amazon S3、Amazon EC2 或 Amazon RDS)，即使該特定服務未啟用選擇加入，該資源類型也會包含在備份中。
- 如果在資源指派中同時指定了資源類型和標籤，則備份計畫中指定的資源類型將優先於標籤條件。在此情況下，會忽略服務選擇加入設定。

> **Note**
>
> 服務選擇加入設定是區域特定。如果您變更正在使用的 AWS 區域 ，則必須重新設定與 AWS Backup搭配使用的服務。

若要設定搭配使用的服務 AWS Backup

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。

2. 在導覽窗格中，選擇設定。
3. 在 Service opt-in (選擇加入服務) 頁面上，選擇 Configure resources (設定資源)。
4. 使用切換開關可啟用或停用搭配使用的服務 AWS Backup。

> **Important**
>
> RDS、Aurora、Neptune 及 DocumentDB 共用相同的 Amazon Resource Name (ARN)。選擇管理這些資源類型之一，並在將其指定給備份計劃時 AWS Backup 選擇使用全部資源類型。無論如何，建議您選擇加入所有這些選項，以準確地呈現您的選擇加入狀態。

5. 選擇確認。

使用 Amazon S3 資料

AWS Backup 為 Amazon S3 備份提供全受管備份和還原功能。如需進一步了解，請參閱Amazon S3 備份。

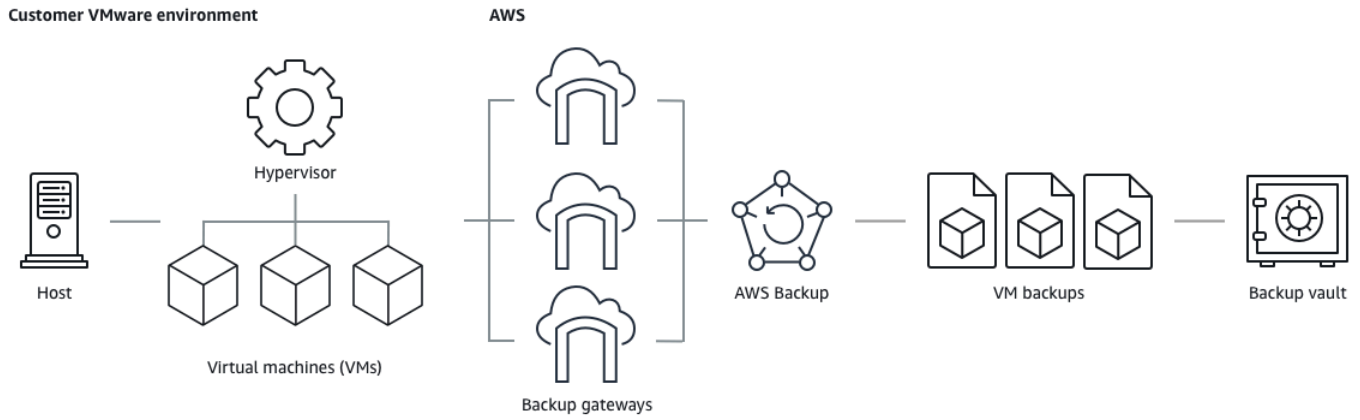
- 如何備份資源：開始使用 AWS Backup
- 如何使用以下方式恢復 Amazon S3 數據 AWS Backup：還原 S3 資料

如需 S3 資料的詳細資訊，請參閱 Amazon S3 文件。

使用 VMware 虛擬機器

AWS Backup 支援內部部署 VMware 虛擬機器 (VM) 以及 VMware Cloud™ (VMC) 中的虛擬機器上AWS的集中式自動化資料保護。您可以從內部部署和 VMC 虛擬機器備份到 AWS Backup. 然後，您可以從內部部署還原 AWS Backup 到內部部署或 VMC。

Backup 閘道是可下載的 AWS Backup 軟體，您可以部署到 VMware 虛擬機器以連線到這些虛擬機器 AWS Backup。閘道會連線至您的 VM 管理伺服器，以探索 VM、加密資料，並有效率地將資料傳輸至 AWS Backup。下圖說明備份閘道如何連線至您的 VM:



- 如何備份資源：虛擬機器備份
- 如何還原 VM 資源：還原虛擬機器

使用 Amazon DynamoDB

AWS Backup 支援備份和還原 Amazon DynamoDB 資料表。DynamoDB 是全受管 NoSQL 資料庫服務，能夠提供快速且可預期的效能，以及無縫的可擴展性。

自推出以來，一 AWS Backup 直支援 DynamoDB。自 2021 年 11 月起， AWS Backup 也推出了適用於 DynamoDB 備份的進階功能。這些進階功能包括跨 AWS 區域 帳戶複製備份、將備份分層到冷儲存，以及使用權限和成本管理的標籤。

2021 年 11 月之後上線的新 AWS Backup 客戶預設會啟用進階 DynamoDB 備份功能。

我們建議所有現有 AWS Backup 客戶啟用 DynamoDB 的進階功能。啟用進階功能後，暖備份儲存定價將不會出現變動，且您可以將備份分層至冷儲存，並使用成本分配標籤將成本最佳化，以節省成本。

如需進階功能的完整清單及啟用方式，請參閱 進階 DynamoDB 備份。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 DynamoDB 資源：還原 Amazon DynamoDB 資料表

如需 DynamoDB 的詳細資訊，請參閱《Amazon DynamoDB 開發人員指南》中的什麼是 Amazon DynamoDB？一節。

使用 Amazon FSx 檔案系統

AWS Backup 支援備份和還原 Amazon FSx 檔案系統。Amazon FSx 提供完全受管的第三方檔案系統，其中包含工作負載的原生相容性和功能集。 AWS Backup 使用 Amazon FSx 的內置備份功能。因此，從 AWS Backup 主控台擷取的備份，具有相同層級的檔案系統一致性和效能，並具有與透過 Amazon FSx 主控台進行備份相同的還原選項。

如果您使用 AWS Backup 來管理這些備份，您將獲得額外的功能，例如無限制的保留選項，以及每小時一次建立排程備份的能力。此外，即使刪除來源檔案系統， AWS Backup 仍會保留您的備份。這可防止意外或惡意刪除的情形發生。

如果您想要從中央備份主控台設定備份政策並監控備份任務，同時也可以擴展對其他 AWS 服務的支援，以保護 Amazon FSx 檔案系統。 AWS Backup

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Amazon FSx 資源：還原 FSX 檔案系統

如需 Amazon FSx 檔案系統的詳細資訊，請參閱 Amazon FSx 文件。

使用 Amazon EC2

使用時 AWS Backup，您可以排程或執行隨需備份任務，其中包括整個 EC2 執行個體和在 Amazon EC2 上執行的 Windows 應用程式，以及關聯的組態資料。這限制了您與儲存 (Amazon EBS) 磁碟區互動的需求。同樣地，您可以從單一還原點還原整個 Amazon EC2 執行個體。一項備份任務只能擁有單一資源。因此您可以擁有一項備份 EC2 執行個體的任務，該任務將備份根磁碟區、所有資料磁碟區和相關聯的執行個體組態。

AWS Backup 不會隨時重新啟動 EC2 執行個體。

備份 Amazon EC2 資源

備份 Amazon EC2 執行個體時， AWS Backup 會拍攝根 Amazon EBS 儲存磁碟區、啟動組態和所有關聯 EBS 磁碟區的快照。 AWS Backup 儲存 EC2 執行個體的特定組態參數，包括執行個體類型、安全群組、Amazon VPC、監控組態和標籤。備份資料會儲存為 Amazon EBS 磁碟區支援的 Amazon Machine Image (AMI)。

您也可以備份及還原已啟用 VSS 的 Microsoft Windows 應用程式。您可以在隨選備份或排程備份計畫中排程應用程式一致性備份、定義生命週期政策，以及執行一致的還原。如需詳細資訊，請參閱 建立 Windows VSS 備份。

AWS Backup 不會備份下列項目：

- 彈性推論加速器的組態 (如果連接到執行個體)。
- 啟動執行個體時使用的使用者資料。

> **Note**
>
> 對於所有執行個體類型，僅支援 Amazon EBS 支援的 EC2 執行個體。不支援暫時儲存執行個體 (也就是執行個體存放區後端的執行個體)。

當 AWS Backup 受管的 Amazon EC2 AMI (亞馬遜機器映像) 或 Amazon EBS 快照透過刪除， AWS Backup 且您已設定 Amazon EC2 資源回收筒時，映像或快照可能會根據 Amazon EC2 資源回收筒政策產生費用。Amazon EC2 資源回收筒中的快照和映像不再受管理，如果您從資源回收筒還原快照 AWS Backup 和映像，也不會受到 AWS Backup 政策管理。

AWS Backup 如果快照鎖定持續時間超過備份生命週期，則與已套用 Amazon EBS 快照鎖的 AWS Backup 受管 Amazon EBS AMI 相關聯的受管 Amazon EBS 快照和快照可能不會在復原點生命週期中刪除。這些復原點的狀態反而會是 `EXPIRED`。如果您選擇先移除 Amazon EBS 快照鎖定，則可以手動刪除這些復原點。

AWS Backup 可以加密與 Amazon EC2 備份相關聯的 EBS 快照。這類似於它加密 EBS 快照的方式。AWS Backup 建立 Amazon EC2 AMI 的快照時，會使用套用於基礎 EBS 磁碟區的相同加密，而原始執行個體的組態參數會保留在還原中繼資料中。

快照會從您所定義的磁碟區衍生其加密，並將相同的加密套用至對應的快照。複製 AMI 的 EBS 快照將一律加密。如果您在複製期間使用 KMS 金鑰，則會套用該金鑰。如果您不使用 KMS 金鑰，則會套用預設 KMS 金鑰。

- 如何備份資源：開始使用 AWS Backup
- 如何恢復 Amazon EC2 資源：還原 Amazon EC2 執行個體

如需 Amazon EC2 的詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的什麼是 Amazon EC2?一節。

使用 Amazon ECS

AWS Backup 支援 Amazon Elastic File System (Amazon EFS)。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Amazon EFS 資源：還原 Amazon EFS 檔案系統

如需 Amazon EFS 檔案系統的詳細資訊，請參閱《Amazon Elastic File System 使用者指南》中的什麼是 Amazon Elastic File System？一節。

使用 Amazon EBS

AWS Backup 支援 Amazon Elastic Block Store (Amazon EBS) 磁碟區。

AWS Backup 如果快照鎖定持續時間超過備份生命週期，則與已套用 Amazon EBS 快照鎖的 AWS Backup 受管 Amazon EBS AMI 相關聯的受管 Amazon EBS 快照和快照可能不會在復原點生命週期中刪除。這些復原點的狀態反而會是 `EXPIRED`。如果您選擇先移除 Amazon EBS 快照鎖定，則可以手動刪除這些復原點。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Amazon EBS 磁碟區：還原 Amazon EBS 磁碟區

如需 Amazon EBS 的詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的什麼是 Amazon Elastic Block Store (Amazon EBS) 一節。

如需詳細資訊，請參閱《Amazon EC2 Linux 執行個體使用者指南》中的建立 Amazon EBS 磁碟區。

使用 Amazon RDS 及 Aurora

AWS Backup 支援 Amazon RDS 資料庫引擎和 Aurora 叢集。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Amazon RDS 資源：還原 RDS 資料庫
- 如何還原 Aurora 叢集：還原 Amazon Aurora 叢集

如需 Amazon RDS 的詳細資訊，請參閱《Amazon RDS 使用者指南》中的 Amazon Relational Database Service 一節。

如需 Aurora 的詳細資訊，請參閱《Amazon Aurora 使用者指南》中的什麼是 Amazon Aurora？一節。

> **Note**
>
> 如果您從 Amazon RDS 主控台展開備份任務，這可能會與 Aurora 叢集備份任務產生衝突，導致 Backup job expired before completion 錯誤發生。如果發生這種情況，請在 AWS Backup中設定較長的備份期間。

> **Note**
>
> AWS Backup目前不支援適用於 SQL Server 的 RDS Custom 和適用於 Oracle 的 RDS Custom。

> **Note**
>
> AWS 只要 Aurora 已啟用自動備份，且 Aurora 自動備份的保留期超過 Aurora 快照的保留期限，就不會對儲存在備份保存庫中的 Aurora 快照收費。如果快照的資料庫遭到刪除 (可能出現意外刪除或在藍/綠部署期間刪除)，則將針對備份保存庫中的任何快照收取費用。
> 大型快照集和經常從刪除的資料庫進行備份，可能會導致大量的儲存費用。請造訪 AWS Backup 計算器估算潛在 AWS Backup 費用。

使用 AWS BackInt

AWS Backup 與 AWS Backint 合作，以支援在 Amazon EC2 執行個體上預覽 SAP HANA 資料庫備份和還原。

- 備份和還原 SAP HANA 資源的指示：SAP HANA Amazon EC2 執行個體備份和還原的公開預覽版
- 設定 AWS Backint Agent：SAP HANA 的AWS Backint Agent

使用 AWS Storage Gateway

AWS Backup 支援 Storage Gateway 磁碟區閘道。您也可以將 Amazon EBS 快照還原為 Storage Gateway 磁碟區。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Storage Gateway 資源：還原 Storage Gateway 磁碟區。

使用 Amazon DocumentDB

AWS Backup 支援 Amazon DocumentDB 叢集。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Storage Gateway 資源：還原 DocumentDB 叢集。

使用 Amazon Neptune

AWS Backup 支援 Amazon Neptune 叢集。

- 如何備份資源：開始使用 AWS Backup
- 如何還原 Amazon Neptune 叢集:還原 Neptune 叢集。

使用 Amazon Timestream

AWS Backup 支持 Amazon Timestream 表。

- 如何備份 Timestream 資料表。
- 如何還原 Timestream 資料表。

使用 AWS Organizations

AWS Backup 與之合作 AWS Organizations ，簡化跨帳戶監控和管理

- 在 Organizations 中建立管理帳戶。
- 開啟跨帳戶管理。
- 指定委派的管理員帳戶並委派政策。

使用 AWS CloudFormation

AWS Backup 支援 AWS CloudFormation 範本和應用程式堆疊

- AWS CloudFormation 堆疊備份

與 AWS BackInt SAP 和 SAP HANA 一起工作 AWS Systems Manager

AWS Backup AWS BackInt 與 SAP 專用的 SSM 搭配使用，以支援 SAP HANA 備份與還原功能。

- Amazon EC2 執行個體備份上的 SAP HANA 資料庫
- 開始使用 SAP AWS Systems Manager 的服務
- AWS 對於 SAP 哈納的 Backint Agent

AWS 服務如何備份自己的資源

您可以參考技術文件，瞭解特定 AWS 服務的備份與還原程序，尤其是在還原期間，您需要設定該 AWS 服務的新執行個體時。下列是文件清單:

- Amazon EC2 相關服務
- 搭 AWS Backup 配 Amazon EFS 使用
- DynamoDB 的隨需備份與還原
- Amazon EBS 快照
- 備份與還原 Amazon RDS 資料庫執行個體
  - 備份與還原 Aurora 資料庫叢集的概觀
- 與 FSx AWS Backup 搭配使用 FSx for Windows File Server
- AWS Backup 與 FSx 搭配使用以獲得光澤
- 備份您的磁碟區 AWS Storage Gateway
- 在 Amazon DocumentDB 中備份和還原
- 備份與還原 Amazon Neptune 叢集

計量、成本和帳單

AWS Backup 定價

目前的 AWS Backup 價格以AWS Backup 定價提供。

> **Important**
>
> 若要避免額外費用，請將保留政策的暖儲存期設定為至少一週。

例如，假設您每天進行備份，並將備份保留一天。此外，假設您受保護的資源太大，需要一整天的時間才能完成備份。 AWS Backup 實現一天的保留期，並在備份任務完成時從暖存儲中刪除備份。第二天， AWS Backup 無法創建增量備份，因為您在暖存儲中沒有備份。因為此保留期未遵循最佳實務，所以您將承擔每天建立完整備份的風險和費用。
請洽詢技術客戶經理或解決方案架構師，以取得使用案例的相關指引。

AWS Backup 帳單

當資源類型支援完整 AWS Backup 管理時， AWS Backup 活動的費用 (包括儲存、資料傳輸、還原和提前刪除) 會顯示在 Amazon Web Services 帳單的「Backup」區段中。如需支援完整 AWS Backup 管理的服務清單，請參閱各資源的功能可用性表格中的「完整 AWS Backup 管理」一節。

當資源類型不支援完整 AWS Backup 管理時，您的某些 AWS Backup 活動 (例如備份的儲存空間成本) 可能會由個別 AWS 服務收取費用。

複製任務失敗

只有在目的地保存庫中建立復原點後，才會向您收取費用。複製任務失敗且未建立復原點時，不會收取任何費用。

成本分配標籤

您可以使用成本分配標籤來追蹤和最佳化詳細層級的成 AWS Backup 本，並使用檢視和篩選這些標籤 AWS Cost Explorer (請注意，DynamoDB 目前不支援此功能)。

若要使用成本分配標籤，請參閱使用 AWS Backup針對 Amazon EFS 自動化備份和最佳化備份成本及使用成本分配標籤。

AWS Backup Audit Manager 定價

AWS Backup 「Audit Manager 程式」會根據控制項評估的數目，收取使用量費用。控制項評估是針對一個控制項的單一資源評估。 AWS Backup 帳單上會顯示控制評估費用。如需目前的控制項評估定價，請參閱 AWS Backup 定價。

若要使用 AWS Backup Audit Manager 控制項，您必須啟用 AWS Config 錄製才能追蹤備份活動。 AWS Config 記錄之每個組態料號的費用，而這些費用會顯示在您的 AWS Config 帳單上。如需目前組態項目記錄的定價，請參閱 AWS Config 定價。

Amazon Aurora 定價

在 Aurora 連續備份的設定保留期間內 (最多 35 天)，快照不會產生儲存費用。超過此期間保留的快照，會依完整備份來收取費用。

AWS Backup 部落格、影片、教學課程和其他資源

如需有關的詳細資訊 AWS Backup，請參閱下列內容：

- 使用 Backup 和還原內部部署 VMware 虛擬機器 AWS Backup。Olumuyiwa Koya 和 Ezekiel Oyerinde (2022 年 6 月) 著。
- 用 AWS Backup 於保護 Amazon Aurora 數據庫。Chris Hendon、Brandon Rubadou 和 Thomas Liddle (2022 年 5 月) 著。
- Protecting encrypted Amazon RDS instances with cross-account and cross-Region backups。Evan Peck 和 Sabith Venkitachalapathy (2022 年 5 月) 著。
- 使 AWS Backup 用和自動化並改善您的安全狀態 AWS PrivateLink。Bilal Alam (2022 年 4 月) 著。
- 獲取匯總的每日跨帳戶多區域 AWS Backup報告。Wali Akbari 和 Sabith Venkitachalapathy (2022 年 2 月) 著。
- 使用AWS Backup 和自動檢視備份發現項目 AWS Security Hub。Kanishk Mahajan (2022 年 1 月) 著。
- 保護備份的十大安全最佳做法 AWS Ibukun Oyewumi (2022 年 1 月) 著。
- AWS 使用 FSx for Lustre 行最佳化 SAS 網格 (並使用最佳化災難回復)。 AWS Backup Matt Saeger 和 Shea Lutton (2022 年 1 月) 著。
- 在 Amazon Neptune 中集中資料保護和合規與 AWS Backup. Brian O'Keefe (2021 年 11 月) 著。
- Manage backup and restore of Amazon DocumentDB (with MongoDB compatibility) with AWS Backup。Karthik Vijayraghavan (2021 年 11 月) 著。
- 使用稽核管理員簡化稽 AWS Backup 核您的資料保護原則。Jordan Bjorkman 和 Harshitha Putta (2021 年 11 月) 著。
- 使用文件 AWS Backup 庫鎖定增強備份的安全性狀態。Rolland Miller (2021 年 10 月) 著。
- 如何在 AWS Backup 還原工作中保留資源標籤。Ibukun Oyewumi、Amee Shah 和 Sabith Venkitachalapathy (2021 年 9 月) 著。
- 使用服務控制政策管理備份的存取 AWS Backup。Sabith Venkitachalapathy 和 Ibukun Oyewumi (2021 年 8 月) 著。

- 自動化跨 AWS 服務大規模的集中備份 AWS Backup。Ibukun Oyewumi 和 Sabith Venkitachalapathy (2021 年 7 月) 著。
- 博客：如何簡化 Microsoft SQL 服務器備份使用 AWS Backup 和 VSS。Siavash Irani and Sepehr Samiei (2021 年 7 月) 著。
- 使用自動化資料復原驗證 AWS Backup。Mahanth Jayadeva (2021 年 6 月) 著。
- 設定通知以監視 AWS Backup 工作。Virgil Ennes (2021 年 6 月) 著。
- Automating backups and optimizing backup costs for Amazon EFS using AWS Backup。Prachi Gupta 和 Rohit Verma (2021 年 6 月) 著。
- 管理 Amazon EFS 備份成本： AWS Backup 支援成本分配標籤。Aditya Maruvada (2021 年 5 月) 著。
- 使用跨帳戶和區域創建和共享加密備份 AWS Backup。Prachi Gupta (2021 年 5 月) 著。
- AWS Backup 現已通過 FedRAMP 高級認證，可滿足您的合規性和資料保護需求。Andy Grimes (2021 年 5 月) 著。
- ZS Associates 提高了備份效率。 AWS Backup Mitesh Naik、Hiranand Mulchandani 和 Sushant Jadhav (2021 年 5 月) 著。
- 教學課程：Amazon EBS Backup 和還原使用 AWS Backup. Fathima Kamal (2021 年 4 月) 著。
- 影片教學課程：Managing Cross-Region Copies of Backups。與大衛 DeLuca （ 2021 年 4 月 ）。
- 使用的 AWS 工具刪除多個 AWS Backup 復原點 PowerShell。Sherif Talaat (2021 年 4 月) 著。
- Amazon FSx 的跨區域和跨帳戶備份使用. AWS Backup Adam Hunter 和 Fathima Kamal (2021 年 4 月) 著。
- Amazon CloudWatch 事件和指標 AWS Backup. Rolland Miller (2021 年 3 月) 著。
- 教學課程：Amazon Relational Database Service (RDS) Backup 和還原使用 AWS Backup. Fathima Kamal (2021 年 3 月) 著。
- 用於 Amazon RDS 的 P oint-in-time 恢復和持續備份 AWS Backup。Kelly Griffin (2021 年 3 月) 著。
- AWS Backup 使用 AWS Service Catalog 自動化。與約翰·海斯默勒 (2021 年 1 月) 。
- Secure data recovery with cross-account backup and Cross-Region copy using AWS Backup。Cher Simon (2021 年 1 月) 著。
- AWS re：發明回顧：數據保護和合規性。 AWS Backup Nancy Wang (2020 年 12 月) 著。
- AWS Backup 為您的資源提供集中式 AWS 資料保護。Nancy Wang (2020 年 11 月) 著。
- Tech Talk: Data protection at scale with AWS Backup。Kareem Behairy (2020 年 9 月) 著。
- 集中式跨帳戶管理，跨區域複製使用. AWS Backup Cher Simon (2020 年 9 月) 著。

- 影片教學課程:在您 AWS Organizations 使用的時候大規模管理備份 AWS Backup。Ildar Sharafeev (2020 年 7 月) 著。
- 在您 AWS Organizations 使用中大規模管理備份 AWS Backup。Nancy Wang、Avi Drabkin、Ganesh Sundaresan 及 Vikas Shah (2020 年 6 月) 著。
- 使用恢復 Amazon EFS 檔案和資料夾 AWS Backup。Abrar Hussain 和 Gurudath Pai (2020 年 5 月) 著。
- Scheduling automated backups using Amazon EFS and AWS Backup。Rob Barnes (2019 年 12 月) 著。
- RE：發明錄音： AWS 重新：發明 2019 年：在英尺上深入潛水。 AWS Backup 機架空間。Nancy Wang 和 Jason Pavao (2019 年 12 月) 著。
- 保護您的資料 AWS Backup。Anthony Fiore (2019 年 7 月) 著。
- 行銷影片：Introducing AWS Backup。2019 年 1 月。
- 影片：Introduction to AWS Backup。通過 AWS 培訓和認證。

首次設定 AWS

初次使用 AWS Backup 之前，請先完成以下作業：

1. 註冊 AWS
2. 建立 IAM 使用者
3. 建立 IAM 角色

註冊 AWS

註冊 Amazon Web Services (AWS) 時，您的 AWS 帳戶 會自動註冊 AWS 的所有服務，包括 AWS Backup。您只需針對所使用的服務付費。

如需 AWS Backup 使用率的詳細資訊，請參閱《AWS Backup 定價》頁面。

如果您已擁有 AWS 帳戶，請跳至下一項任務。如果您還沒有 AWS 帳戶，請使用下列程序建立帳戶。

建立 AWS 帳戶

1. 開啟 https://portal.aws.amazon.com/billing/signup。
2. 請遵循線上指示進行。

   部分註冊程序需接收來電，並在電話鍵盤輸入驗證碼。

   註冊 AWS 帳戶 時，會建立 AWS 帳戶根使用者。根使用者有權存取該帳戶中的所有 AWS 服務和資源。作為安全最佳實務，將管理存取權指派給管理使用者，並且僅使用根使用者來執行需要根使用者存取權的任務。

因為您的下一個任務會需要 AWS 帳戶 編號，所以請記下此編號。

建立 IAM 使用者

AWS 中的服務 (例如 AWS Backup) 需要您在存取時提供憑證，使服務能夠判斷您是否擁有存取其資源的許可。AWS 建議您不要使用 AWS 帳戶 根使用者來提出要求。而是建立 IAM 使用者，然後授予該使用者完整的存取。我們稱這些使用者為管理員使用者。您不需要使用 AWS 帳戶 根使用者憑證，可以改用管理員使用者憑證來與 AWS 互動並執行任務，例如建立儲存貯體、建立使用者，以及授予許可。

如需詳細資訊，請參閱《AWS 一般參考》中的〈AWS 帳戶 根使用者憑證與 IAM 使用者憑證〉，以及《IAM 使用者指南》中的〈IAM 最佳實務〉。

如果您已註冊 AWS，但是尚未為自己建立 IAM 使用者，您可以使用 IAM 主控台加以建立。

若要建立管理員使用者，請選擇下列其中一個選項。

選擇一種管理管理員的方式	To	By	您也可以
在 IAM Identity Center (建議)	使用短期憑證存取 AWS。 這與安全性最佳實務一致。有關最佳實務的資訊，請參閱 IAM 使用者指南中的 IAM 安全最佳實務。	請遵循 AWS IAM Identity Center 使用者指南的入門中的說明。	請參閱 AWS Command Line Interface 使用者指南中的設定 AWS CLI 以使用 AWS IAM Identity Center 設定程式設計存取。
在 IAM 中 (不建議使用)	使用長期憑證存取 AWS。	請遵循 IAM 使用者指南中建立您的第一個 IAM 管理員使用者和使用者群組的說明。	請參閱 IAM 使用者指南中的管理 IAM 使用者的存取金鑰，設定程式設計存取。

若要以這個新的 IAM 使用者身分登入，請登出 AWS Management Console。接著，使用下列 URL，其中 your_aws_account_id 是去掉連字號的 AWS 帳戶 帳號 (例如，您的 AWS 帳戶 編號若是 1234-5678-9012，則 AWS 帳戶 ID 即為 123456789012)：

```
https://your_aws_account_id.signin.aws.amazon.com/console/
```

輸入您剛才建立的 IAM 使用者名稱和密碼。登入時瀏覽列會顯示 your_user_name@your_aws_account_id。

如果您不希望登入頁面的 URL 包含您的 AWS 帳戶 ID，可以建立一個帳戶別名。在 IAM 儀表板中，請按一下 建立帳戶別名，然後輸入別名，例如您的公司名稱。若要在建立帳戶別名後登入，請使用下列 URL：

```
https://your_account_alias.signin.aws.amazon.com/console/
```

若要確認您帳戶之 IAM 使用者的登入連結，請開啟 IAM 主控台，並在儀表板的 AWS 帳戶 別名 下加以確認。

建立 IAM 角色

您可使用 IAM 主控台來建立 IAM 角色，其可授與 AWS Backup 存取支援資源的許可。在您建立 IAM 角色 角色之後，您需要建立並將政策連接至該角色。

使用主控台建立 IAM 角色

1. 登入 AWS 管理主控台，並開啟 IAM 主控台。
2. 在 IAM 主控台的導覽窗格中，選擇 角色，然後選擇 建立角色。
3. 選擇 AWS 服務角色，然後針對 AWS Backup 選擇 選取。選擇 Next: Permissions (下一步：許可)。
4. 在 附加許可政策 頁面上，核取 `AWSBackupServiceRolePolicyForBackup` 和 `AWSBackupServiceRolePolicyForRestores` 兩者。這些 AWS 受管政策，可授與 AWS Backup 備份和還原所有支援 AWS 資源的許可。若要深入了解受管政策並檢視範例，請參閱《受管政策》。

   然後選擇 Next: Tags (下一步：標籤)。
5. 選擇 下一步：檢閱 。
6. 針對 Role Name (角色名稱)，輸入可描述此角色目的的名稱。角色名稱在您的 AWS 帳戶 內必須是獨一無二的。因為有各種實體可能會參考角色，所以您無法在建立角色之後編輯角色名稱。

   選擇建立角色。
7. 在 Roles (角色) 頁面上，選擇您建立的角色，開啟其詳細資訊頁面。

開始使用 AWS Backup

本教學課程向您展示使用 AWS Backup 特徵和功能的一般步驟。如同本技術文件的任何部分一樣，您應該遵循另一個視窗中的 AWS 管理主控台。

您也可以閱讀以下教學課程，了解如何 AWS Backup 搭配特定服務使用：

- Amazon Relational Database Service 服務 (Amazon RDS) Backup 和還原 AWS Backup
- 教學課程：使用 Amazon EBS Backup 和還原 AWS Backup

主題

必要條件

開始之前，請務必備妥下列項目：

- 一個 AWS 帳戶. 如需詳細資訊，請參閱 首次設定 AWS。
- 至少支援一個資源 AWS Backup。
- 您應該熟悉要備份的 AWS 服務和資源。請參閱支援的 AWS 資源和第三方應用程式清單。

  當新 AWS 服務可用時，啟用 AWS Backup 以使用這些服務。

  設定要搭配使用的 AWS 服務 AWS Backup

  1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。

2. 在導覽窗格中，選擇設定。
3. 在 Service opt-in (選擇加入服務) 頁面上，選擇 Configure resources (設定資源)。
4. 在 [設定資源] 頁面上，使用切換參數來啟用或停用搭配使用的服務 AWS Backup。設定服務時，請選擇 Confirm (確認)。請確定您選擇使用的 AWS 服務在您的 AWS 區域.

> **Note**
>
> 如果您在啟用 Amazon EFS 之後設定了自動備份 AWS Backup，即使您選擇退出或停用 Amazon EFS，自動備份也會繼續進行 AWS Backup。如需詳細資訊，請參閱 入門 4：建立 Amazon EFS 自動備份。若要停用自動備份，請使用 Amazon EFS 主控台或 API。

- 請確保您要備份的資源都位於相同的 AWS 區域內。

若要完成本教學課程，您可以使用 AWS 帳戶 root 使用者登入 AWS Management Console。不過，AWS Identity and Access Management (IAM) 建議您不要使用 AWS 帳戶 根使用者。反之，在帳戶中建立一個管理員，並使用這些登入資料來管理帳戶中的資源。如需詳細資訊，請參閱 首次設定 AWS。

主 AWS Backup 控台提供不同的選項來備份您的資源。您可以隨需建立備份、排程和設定資源的備份方式，或將資源設定為在建立時自動備份。

入門 1：選擇加入服務

主 AWS Backup 控台有兩種方式可將資源類型納入備份計畫中：在備份計畫中明確指派資源類型或包含所有資源。請參閱下列要點，以了解這些選項如何與選擇加入服務搭配運作。

- 如果資源指派僅以標籤為基礎，則會套用選擇加入服務設定。
- 如果將資源類型明確指派給備份計畫 (例如 Amazon S3、Amazon EC2 或 Amazon RDS)，即使該特定服務未啟用選擇加入，該資源類型也會包含在備份中。
- 如果在資源指派中同時指定了資源類型和標籤，則備份計畫中指定的資源類型將優先於標籤條件。在此情況下，會忽略服務選擇加入設定。

選擇加入選項適用於特定帳戶 AWS 區域，因此您可能必須使用同一帳戶選擇加入多個區域。

由於 AWS Backup 支援越來越多的 AWS 服務和第三方應用程式，因此您可能需要重新瀏覽此步驟，以選擇使用新支援的資源。

AWS Backup 不會管理或管理在環境以外的 AWS 環境中進行的備份 AWS Backup。

選擇加入以 AWS Backup 保護所有支援的資源類型

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側的導覽窗格中，選擇設定。
3. 在 選擇加入服務 下，選擇 設定資源。
4. 將所有切換向右移動，即可選擇加入所有 AWS Backup支援的資源。
5. 選擇確認。

後續步驟

若要使用建立隨選備份 AWS Backup，請繼續執行入門 2：建立隨需備份。

入門 2：建立隨需備份

在 AWS Backup 主控台上，[受保護的資源] 頁面會列出至 AWS Backup 少備份一次的資源。如果您是第一 AWS Backup 次使用，則此頁面上沒有列出任何資源，例如 Amazon EBS 磁碟區或 Amazon RDS 資料庫。如果備份計劃未至少執行一次排程備份任務，那麼即使資源已指派至備份計劃，結果仍然如上述。

在此第一步驟中，您建立您其中一個資源的隨需備份。接著，您會看到此資源列在 Protected resources (受保護的資源) 頁面。

建立隨需備份

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 使用導覽窗格選擇 受保護的資源，然後選擇 建立隨需備份。
3. 在 建立隨需備份 頁面上，選擇您要備份的資源類型；例如，選擇適用於 Amazon DynamoDB 資料表的 DynamoDB。
4. 選擇您要保護的資源名稱或 ID。請確保您選擇的資源是您想要的資源。

> **Note**
>
> Amazon FSx for Lustre 支援 Persistent 和 Persistent_2 部署類型。

5. 請確認已選取 Create backup now (立即建立備份)。如此將立即啟動備份，並且很快就能讓您在 Protected resources (受保護的資源) 頁面上查看您已儲存的資源。
6. 指定轉移至冷儲存值 (如果適用) 和過期值。

> **Note**
>
> - 若要查看可轉換為冷儲存的資源清單，請參閱 各資源的功能可用性 表格的「冷儲存生命週期」一節。所有其他資源類型都會儲存至暖儲存，並忽略轉換至冷庫運算式。Expire 值適用於所有資源類型。
> - 當備份到期並在生命週期政策中標記為要刪除時， AWS Backup 在接下來的 8 小時內隨機選擇的點刪除備份。此視窗有助於確保效能一致。

7. 選擇現有的備份文件庫。選擇 Create new backup vault (建立新的備份文件庫) 開啟新頁面來建立文件庫，完成後將返回 Create on-demand backup (建立隨需備份) 頁面。
8. 在 IAM role (IAM 角色) 中選擇 Default role (預設角色)。

> **Note**
>
> 如果您的帳戶中沒有 AWS Backup 預設角色，系統會以正確的權限為您建立角色。

9. 如果您要將一或多個標籤指派至您的隨需備份，請輸入 key (索引鍵) 和選用的 value (值)，然後選擇 Add tag (新增標籤)。

> **Note**
>
> - 對於 Amazon EC2 資源，除了新增至此備份的任何標籤之外，還 AWS Backup 會自動複製現有的群組和個別資源標籤。如需詳細資訊，請參閱 Copying tags onto backups。
> - 建立以標籤為基礎的備份計劃時，如果您選擇的角色不是 D efault 角色，請確定其具備備份所有已標記資源的必要權限。 AWS Backup 嘗試使用所選標籤處理所有資源。如果遇到沒有存取許可的資源，備份計劃就會失敗。

10. 選擇 Create on-demand backup (建立隨需備份)。您將會移到 Jobs (任務) 頁面，您會看到任務的清單。
11. 如果您的資源類型為 EC2，則會出現 進階備份設定 區段。如果您的 EC2 執行個體正在執行 Microsoft Windows，請選擇 Windows VSS。這可讓您取得應用程式一致性 Windows VSS 備份。

> **Note**
>
> AWS Backup 目前僅支援在 Amazon EC2 上執行的資源的應用程式一致性備份。並非所有執行個體類型或應用程式皆支援 Windows VSS 備份。如需詳細資訊，請參閱 建立 Windows VSS 備份。

12. 選擇您選擇要備份之資源的 Backup job ID (備份任務 ID)，以查看該任務的詳細資料。

後續步驟

若要自動化您的備份活動，請繼續執行 入門 3：建立排程備份。

入門 3：建立排程備份

在 AWS Backup 自學課程的這個步驟中，您會建立備份計畫、為其指定資源，然後建立備份儲存庫。

開始之前，請務必備妥必要的先決條件。如需詳細資訊，請參閱 開始使用 AWS Backup。

主題

步驟 1：基於現有備份計畫建立備份計畫

備份計畫是一種政策運算式，可定義備份 AWS 資源的時間和方式，例如 Amazon DynamoDB 資料表或 Amazon Elastic File System (Amazon EFS) 檔案系統。您可以將資源指派給備份計劃， AWS Backup 然後根據備份計劃自動備份並保留這些資源的備份。如需詳細資訊，請參閱 使用備份計畫管理備份。

有兩種方式可以建立新的備份計劃，一種是從頭開始建置，另一種則是根據現有的備份計劃來建置。此範例使用 AWS Backup 主控台修改現有備份計畫來建立備份計畫。

從現有的備份計劃建立備份計劃

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 從儀表板中，選擇 Manage Backup plans (管理備份計劃)。或者使用導覽窗格，選擇 備份計畫，然後選擇 建立備份計畫。
3. 選擇 從範本開始，再從清單中選擇計畫 (例如 `Daily-Monthly-1yr-Retention`)，然後在 備份計畫名稱 方塊中輸入名稱。

   > **Note**
   >
   > 如果您嘗試建立與現有計劃相同的備份計劃，您會收到 `AlreadyExistsException` 錯誤。

4. 在計畫摘要頁面上，選擇您想要的備份規則，然後選擇 編輯。
5. 檢閱，然後選擇規則所需要的值 (請參閱 備份計畫選項和組態 以了解規則選項)。
6. 針對備份保存庫，請選擇 預設 或選擇 建立新的備份保管庫，以建立新的保存庫。
7. (選擇性)- AWS 區域 從 [目的地] 區域的清單中選擇一個，將備份複製到不同的區域。若要新增更多區域，請選擇 新增複本。
8. 當您完成規則的編輯時，請選擇 儲存備份規則。

在 Summary (摘要) 頁面上，選擇 Assign resources (指派資源) 以為下一節做準備。

步驟 2：將資源指派至備份計畫

建立備份計畫之後，您必須將 AWS 資源指派給該備份計畫。如需指派資源的詳細資訊，請參閱 將資源指派至備份計畫。

如果您還沒有要指派給備份計劃的現有 AWS 資源，請建立一些新資源以用於此練習。使用受支援的 AWS 資源和第三方應用程式，建立一或兩項資源。

將資源指派至備份計劃

1. 上述步驟應該已將您帶至 指派資源 頁面。
2. 輸入資源指派名稱。
3. 針對 IAM 角色，請選擇 預設角色。如果您選擇其他角色，則該角色必須具有備份所有指派資源的許可。

4. 在 指派資源 區段中，選擇 包含所有資源類型。資源類型是 AWS Backup支援的 AWS 服務或協力廠商應用程式。此備份計劃現在將保護您選擇使用以保護的所有資源類型 AWS Backup
5. 請選擇 指定資源。

您會返回備份計畫 摘要 頁面。請選擇 建立備份計畫 以部署您的第一個備份計畫！

步驟 3：建立備份保存庫

您可以不使用 AWS Backup 主控台為您自動建立的預設備份文件庫，而是建立特定的備份文件庫，在相同的文件庫中儲存和整理備份群組。

如需備份文件庫的詳細資訊，請參閱備份文件庫。

建立備份文件庫

1. 在 AWS Backup 主控台的導覽窗格中，選擇「Backup 儲存庫」。

   > **Note**
   >
   > 如果左側看不到導覽窗格，您可以選擇 AWS Backup 主控台左上角的功能表圖示來開啟導覽窗格。

2. 選擇 Create backup vault (建立備份文件庫)。
3. 輸入備份文件庫的名稱。您可以為文件庫命名以反映所要儲存的內容，或是讓它更容易搜尋您所需要的備份。例如，您可以將它命名為 **`FinancialBackups`**。
4. 選取 AWS Key Management Service (AWS KMS) 鍵。您可以使用已建立的金鑰，或選取預設 AWS Backup KMS 金鑰。

   > **Note**
   >
   > 此處指定的 AWS KMS 金鑰僅適用於支援 AWS Backup 獨立加密的服務備份。若要查看支援 AWS Backup 獨立加密的資源類型清單，請參閱各資源的功能可用性表格的「完整 AWS Backup 管理」一節。

5. 或者，您可以新增標籤以協助您搜尋和識別您的備份文件庫。例如，您可以新增 **`BackupType:Financial`** 標籤。
6. 選擇 Create backup vault (建立備份文件庫)。
7. 在導覽窗格中選擇 Backup vaults (備份文件庫)，然後確認您的備份文件庫是否已經新增。

> **Note**
>
> 您現在可以在其中一個備份計劃中編輯備份規則來存放備份，這些備份是由您剛建立的備份文件庫中的規則所建立的。

後續步驟

若要額外備份 Amazon EFS 檔案系統，請繼續執行 入門 4：建立 Amazon EFS 自動備份。

入門 4：建立 Amazon EFS 自動備份

在使用 Amazon EFS 主控台建立 Amazon Elastic File System (Amazon EFS) 檔案系統時，預設會啟用自動備份功能。如果您想要自動備份現有的 Amazon EFS 檔案系統，可以使用 Amazon EFS 主控台、API 或 CLI 進行操作。

使用主控台自動備份現有的 Amazon EFS 檔案系統

1. 在 https://console.aws.amazon.com/efs 開啟 Amazon EFS 主控台。
2. 在 檔案系統 頁面上，選擇要開啟自動備份的檔案系統。
3. 在 一般 設定窗格中，選擇 編輯。
4. 若要開啟自動備份，請選擇 啟用自動備份。

預設備份計畫設定為 `daily backups, 35-day retention`。預設備份時段 (備份將會執行的時間範圍) 設定為在 UTC 上午 5 點 (國際標準時間) 開始，並會持續 8 小時。

> **Note**
>
> Amazon EFS 自動備份保留保存庫 `aws/efs/automatic-backup-vault` 僅供自動備份使用。如果您將其用作其他備份計畫的目的地，則會收到「許可不足」錯誤訊息。

AWS Backup 在您的帳戶中代表您建立服務連結角色。這項角色具有所需的許可來執行 Amazon EFS 備份。如需服務連結角色的詳細資訊，請參閱 使用 AWS Backup的服務連結角色。

如需有 step-by-step 關如何使用 Amazon EFS 主控台、API 或 CLI 開啟或關閉自動備份的指示，請參閱 Amazon Elastic File System 使用者指南中的自動備份。

後續步驟

若要檢視您已建立的備份，請繼續執行 入門 5：檢視備份任務和復原點。

入門 5：檢視備份任務和復原點

使用 AWS Backup，您可以檢視所使用 AWS 服務中備份和還原活動的狀態和其他詳細資料。

在 AWS Backup 儀表板上，您可以管理備份計劃、建立隨選備份、還原備份，以及檢視備份和還原工作的狀態。

主題

檢視備份任務的狀態

使用 AWS Backup 儀表板快速檢視備份和還原活動的狀態。

檢視備份任務狀態

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Dashboard (儀表板)。
3. 若要檢視備份任務的狀態，請選擇 Backup jobs details (備份任務詳細資訊)。您將會移到 Backup jobs (備份任務) 頁面以檢視包含備份任務和還原任務的資料表。
4. 您可以篩選依時間顯示的任務。例如，在過去 24 小時、上週或過去 30 天內建立的任務。您也可以選擇齒輪圖示以設定每頁顯示的任務數量。

檢視保存庫中的所有備份

依照這些步驟檢視在 AWS Backup中指定的文件庫建立的備份。

檢視文件庫中的所有備份

1. 在 AWS Backup 主控台的導覽窗格中，選擇「Backup 儲存庫」。

2. 選擇您在建立隨需或排程備份時使用的文件庫，並檢視在此文件庫中建立的所有備份。

> **Note**
>
> 每個備份都有其狀態，而該狀態通常為 已完成。如果由於某種原因 AWS Backup 無法根據其生命週期配置刪除備份，則會將此備份標記為「已過期」。系統會根據 已過期 備份所耗用的儲存體向您計費，且應將其刪除。

檢視受保護資源的詳細資訊

在 Protected resources (受保護的資源) 頁面上，您可以探索備份於 AWS Backup的資源的詳細資訊。

檢視受保護的資源

1. 在 AWS Backup 主控台的導覽窗格中，選擇 [受保護的資源]。
2. 檢視正在備份的 AWS 資源。在清單中選擇資源以探索您的資源備份。

後續步驟

若要還原已檢視的復原點，請繼續執行 入門 6：還原備份。

入門 6：還原備份

資源備份至少一次之後，即視為受保護且可以使用來還原資源 AWS Backup。依照以下步驟，使用 AWS Backup 主控台還原資源。

如需有關特定服務還原參數或使用或 AWS Backup API 還原 Backup 的 AWS CLI 詳細資訊，請參閱還原備份。

還原資源

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在瀏覽窗格中，選擇 Protected resources (受保護的資源) 和您要還原的資源 ID。
3. 復原點清單 (包括資源類型) 會以 Resource ID (資源 ID) 顯示。選擇資源以開啟 Resource details (資源詳細資訊) 頁面。

4. 若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
5. 指定還原參數。顯示的還原參數皆專屬於所選取的資源類型。

> **Note**
>
> 如果您只保留一個備份，則只能還原至在備份時的檔案系統狀態。您無法還原至先前的增量備份。

如需有關如何還原特定資源的指示，請參閱 Restoring a backup。

6. 針對 Restore role (還原角色)，選擇 Default role (預設角色)。

> **Note**
>
> 如果您的帳戶中沒有 AWS Backup 預設角色，系統會以正確的權限為您建立角色。

7. 選擇 Restore backup (還原備份)。

Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

> **Note**
>
> 當您執行還原以還原 Amazon EFS 執行個體中的特定項目時，您可以將這些項目還原到新的或現有的檔案系統。如果將項目還原到現有檔案系統，請從根目錄 AWS Backup 建立新的 Amazon EFS 目錄以包含這些項目。指定項目的完整階層會保留在復原目錄中。例如，如果目錄 A 包含子目錄 B、C 和 D，則會在復原 A、B、C 和 D 時 AWS Backup 保留階層結構。無論您是對現有的檔案系統或新檔案系統執行 Amazon EFS 部分還原，每次還原嘗試都會從根目錄建立一個新的復原目錄，以包含還原的檔案。如果您嘗試針對相同的路徑進行多次還原，則可能存在數個包含已還原項目的目錄。

還原 Amazon EFS 執行個體

如果您要還原 Amazon EFS 執行個體，可以執行 完整還原 以還原整個檔案系統。或者，您可以使用 項目層級還原 來還原特定檔案和目錄 (項目層級還原有其限制。如需詳細資訊，請參閱 Restoring an Amazon EFS file system)。如需還原其他資源類型的詳細資訊，請參閱還原備份。

> **Note**
>
> 若要還原 Amazon EFS 執行個體，您必須「允許」backup:startrestorejob。

如需還原備份的詳細資訊，請參閱 還原備份。

後續步驟

使用 AWS Backup Audit Manager，您可以稽核備份活動和資源。您也可以建立報告，以作為備份、還原和複製任務的證據。若要建立報告，請參閱 入門 7：建立稽核報告。

入門 7：建立稽核報告

在中入門 5：檢視備份任務和復原點，您在「 AWS Backup 儀表板」、「Backup 保管庫」和「受保護的資源」檢視中觀察到備份活動。但是，這些檢視是動態的，並且會根據您訪問這些項目的時間進行更新。這些檢視不一定是隨時間經過而持續遵循組織資料保護需求和控制項的最佳證據。

在此步驟中，您將使用 AWS Backup Audit Manager 建立隨選備份工作報告。

AWS Backup Audit Manager 每天隨需向您的 Amazon S3 儲存貯體提供 CSV、JSON 或兩種格式的各種稽核報告。您可以針對數個可自訂的控制項，稽核備份活動和資源的合規性。您可以接收有關備份、複製和還原任務的報告。備份任務報告是備份任務已執行的證據。

下列為備份計畫的範例。

```
{
  "reportItems": [
    {
      "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z",
      "accountId": "112233445566",
      "region": "us-west-2",
      "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC00000",
      "jobStatus": "COMPLETED",
      "resourceType": "EC2",
      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee77800000",
      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-
b489-4301-83ac-4b7dd7200000",
      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e6abcde",
      "creationDate": "2021-07-14T23:53:47.229Z",
```

```
      "completionDate": "2021-07-15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-030cafb98e5aabcde",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 8589934592,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/
AWSBackupDefaultServiceRole"
    }
  ]
}
```

若要建立備份報告 (包括隨需備份報告)，您必須先建立報告計畫來自動化報告，並將其傳送至 Amazon S3 儲存貯體。

報告計畫要求您擁有 Amazon S3 儲存貯體，以便接收報告。如需設定新 S3 儲存貯體的指示，請參閱《Amazon Simple Storage Service 使用者指南》中的步驟 1：建立您的第一個 S3 儲存貯體。

建立報告計畫。

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，請選擇 報告。
3. 選擇 建立報告計畫。
4. 在下拉式選單中選取 備份任務報告。
5. 對於 報告計畫名稱，輸入 **`TestBackupJobReport`**。
6. 對於 檔案格式，請同時選擇 CSV 和 JSON。
7. 對於 S3 儲存貯體名稱，請從下拉式清單中選取報告的目的地。
8. 選擇 建立報告計畫。

接下來，您必須允許 S3 儲存貯體接收來源的報告 AWS Backup。 AWS Backup Audit Manager 會自動為您產生 S3 存取政策。

檢視並套用此存取政策

1. 在左側導覽窗格中，請選擇 報告。
2. 在 報告計畫名稱 下，請選擇您的報告計畫名稱 (`TestBackupJobReport`)。
3. 選擇編輯。

4. 選擇 檢視 S3 儲存貯體的存取政策。
5. 選擇 複製許可。
6. 選擇 編輯儲存貯體政策 來編輯目的地 S3 儲存貯體的政策，以允許其接收備份任務報告。
7. 將許可複製或新增至目的地 S3 儲存貯體政策。

接下來，建立您的第一份備份任務報告。

建立隨需備份報告

1. 在左側導覽窗格中，請選擇 報告。
2. 在 報告計畫名稱 下，請選擇您的報告計畫名稱 (TestBackupJobReport)。
3. 選擇 建立隨需報告。

最後，檢視您的報告。

檢視您的報告

1. 在左側導覽窗格中，請選擇 報告。
2. 在 報告計畫名稱 下，請選擇您的報告計畫名稱 (TestBackupJobReport)。
3. 在 報告任務 區段中，選擇 S3 連結。進行此操作後，即可將您移往目的地 S3 儲存貯體。
4. 選擇 Download (下載)。
5. 請使用您用來處理 CSV 或 JSON 檔案的程式來開啟報告。

後續步驟

若要清理入門資源並避免不必要的費用，請繼續執行 入門 8：清理資源。

入門 8：清理資源

執行開始使用 AWS Backup中的所有任務之後，您可能會希望清除您已建立的任何項目，以避免產生任何不必要的費用。

主題

- 步驟 1：刪除還原的 AWS 資源
- 步驟 2：刪除備份計畫

步驟 1：刪除還原的 AWS 資源

若要刪除從復原點還原的 AWS 資源，例如 Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon DynamoDB 表格，請使用該服務的主控台。例如，若要刪除 Amazon Elastic File System (Amazon EFS) 檔案系統，請使用 Amazon EFS 主控台。

> **Note**
>
> 這項資訊所指的是已還原的資源，而非儲存在備份保存庫中的復原點。

步驟 2：刪除備份計畫

如果您不要建立排程備份，您應該刪除您的備份計畫。您必須先刪除對備份計畫指派的所有資源，才能刪除該備份計畫。

依照以下步驟刪除備份計劃：

刪除備份計劃

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Backup plans (備份計劃)。
3. 在 Backup plans (備份計劃) 頁面上，選擇您要刪除的備份計劃。您將會移至該備份的詳細資訊頁面。
4. 若要刪除您的計劃的資源指派，請選擇指派名稱旁的選項按鈕，然後選擇 Delete (刪除)。
5. 若要刪除備份計劃，請選擇該頁面右上角的 Delete (刪除)。
6. 在確認頁面上，輸入計劃名稱，然後選擇 Delete plan (刪除計劃)。

步驟 3：刪除復原點

接下來，您可以刪除備份文件庫中的備份復原點。

刪除復原點

1. 在 AWS Backup 主控台的導覽窗格中，選擇「Backup 儲存庫」。
2. 在 Backup vaults (備份文件庫) 頁面上，選擇您存放備份的備份文件庫。
3. 勾選復原點，然後選擇 刪除。
4. 如果您要刪除多個復原點，請依照下列步驟執行：

   a. 如果您的清單包含連續備份，請選擇要保留還是刪除連續備份資料。

   b. 若要刪除列出的所有復原點，請鍵入 **`delete`**，然後選擇 刪除復原點。

      在頁面頂端看到綠色的成功橫幅之前，請將瀏覽器標籤保持開啟。過早關閉此標籤將會結束刪除流程，而且可能會保留一些您想要刪除的復原點。如需詳細資訊，請參閱 Deleting backups。

步驟 4：刪除備份保存庫

您通常無法刪除預設備份保存庫。但是，如果某個區域中存在一或多個其他保存庫，則可以使用 AWS CLI刪除該區域中的預設備份保存庫。

刪除其中的所有備份 (復原點) 後，您就可以刪除其他非預設保存庫。若要執行此操作，請在空白保存庫中選取 刪除。

步驟 5：刪除報告計畫

您的報告計畫會每天自動傳送新的報告。若要停止這項任務，請刪除該報告計畫。

刪除報告計畫

1. 在 AWS Backup 主控台的導覽窗格中，選擇 [報表]。
2. 在 報告計畫名稱 下，請選擇報告計畫的名稱。
3. 選擇刪除。
4. 輸入報告計畫名稱，然後選擇 刪除報告計畫。

步驟 6：刪除報告

您可以遵循每個報告的 Deleting a single object 指示來刪除報告。如果您不再需要目的地 S3 儲存貯體，則在刪除儲存貯體中的所有物件後，您可以遵循 Deleting a bucket 的指示來刪除該儲存貯體。

使用備份計畫管理備份

在中 AWS Backup，備份計劃是一種政策表示式，用於定義備份 AWS 資源的時間和方式，例如 Amazon DynamoDB 表或 Amazon Elastic File System (Amazon EFS) 檔案系統。您可以將資源指派給備份計劃，並根據備份計劃 AWS Backup 自動備份和保留這些資源的備份。如果您擁有的工作負載有不同的備份需求，則可以建立多個備份計劃。依預設， AWS Backup會最佳化備份視窗。您可以在主控台或以程式設計方式自訂備份視窗。

AWS Backup 有效地以增量方式儲存您的定期備份。 AWS 資源的第一次備份會備份資料的完整複本。對於每個後續的增量備份，只會備份對資 AWS 源的變更。增量備份可讓您的資料獲得經常備份的保護，同時又能將儲存成本降至最低。

AWS Backup 還可以無縫管理您的備份鏈，讓您隨時還原。包括在備份計畫的生命週期自動刪除超過所定義保留期限的唯一完整備份後。

以下各節提供在中管理備份策略的基本概念 AWS Backup。

主題

建立備份計畫

您可以使用 AWS Backup 主控台、API、CLI、SDK 或 AWS CloudFormation 範本建立備份計劃。

主題

使用 AWS Backup 主控台建立備份計畫

請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup 從儀表板中，選擇 Manage Backup plans (管理備份計劃)。或者使用導覽窗格，選擇 備份計畫，然後選擇 建立備份計畫。

開始選項

新的備份計畫有三種選擇：

- 步驟 1：基於現有備份計畫建立備份計畫
- 建置新的計畫
- 使用 JSON 文件和 AWS Backup CLI 建立備份計畫

在此教學課程中，我們將選擇建置新的計劃。這個組態的每個部分都有一個連結，指向頁面上展開的區段，您可以瀏覽該區段以取得更多詳細資訊。

在 備份計畫名稱 方塊中輸入計畫名稱。如果您嘗試建立與現有計劃相同的備份計劃，您會收到 `AlreadyExistsException` 錯誤。

1. 您可以選擇性地將標籤新增至備份計畫。
2. 備份規則組態：您將在備份規則組態區段中，設定備份排程、時段和生命週期。
3. 排程：
    a. 在文字欄位中輸入備份規則名稱。
    b. 在備份保存庫下拉式功能表中，選擇預設或選擇建立新的備份保存庫，以建立新的保存庫。
    c. 在備份頻率下拉式功能表中，選擇您希望此計畫建立備份的頻率。
4. 備份時段：
    a. 系統當地時區中的開始時間預設為下午 1:00。
    b. 以下時間後開始預設為 8 小時。您可以變更此設定以指定備份的開始時段。
    c. 完成時間預設為 7 天。
5. 持續備份與 point-in-time 還原 (PITR)：您可以選取 [啟用連續備份以進行 point-in-time 復原 (PITR)]。若要確認這類備份支援哪些資源，請參閱各資源的功能可用性矩陣。
6. 生命週期

a. 不常用儲存：選取此方塊，可根據您在保留期間總計中指定的時間表，將合格的資源類型轉移至不常用儲存。要使用不常用儲存，保留期間總計必須為 90 天或更長的時間。

b. Amazon EBS 的不常用儲存是 Amazon EBS 快照存檔。轉移至封存儲存體的快照在主控台中會顯示為不常用儲存層。如果已啟用不常用儲存，而且備份頻率是每月或更低的頻率，您就具備備份計畫轉移 EBS 快照。

c. 保留期總計是您將資源存放在 AWS Backup的天數。這是常用儲存加上不常用儲存的總天數。

7. (選用) 如果您想要將備份副本存放在其他 AWS 區域中，請使用複製到目的地，以建立合格資源的跨區域副本。

8. (選用) 新增至復原點的標籤。

9. 根據規格完成所有區段的設定時，請選擇儲存備份規則。

使用 JSON 文件和 AWS Backup CLI 建立備份計畫

您也可以在 JSON 文件中定義備份計畫，然後使用 AWS Backup 主控台或 AWS CLI提供備份計畫。下列 JSON 文件包含一份每日於太平洋時間 1:00 建立備份的範例備份計畫 (當地時間會隨時區的日光節約、標準或夏令時間條件 (如適用) 而調整)。並會自動刪除保留期超過一年的備份。如需有關自訂的詳細資訊，請參閱 Amazon CloudWatch 事件使用者指南中的 Cron 運算式。如需有關時區的詳細資訊，請參閱 Amazon 定 Location Service API 參考中的TimeZone 頁面。

```
{
  "BackupPlan":{
    "BackupPlanName":"test-plan",
    "Rules":[
      {
        "RuleName":"test-rule",
        "TargetBackupVaultName":"test-vault",
        "ScheduleExpression":"cron(0 1 ? * * *)",
        "ScheduleExpressionTimezone": "America/Los_Angeles",
        "StartWindowMinutes":"480",
        "CompletionWindowMinutes":"10080",
        "Lifecycle":{
          "DeleteAfterDays":365
        }
      }
    ]
  }
```

```
}
```

您可以使用自己選擇的名稱儲存 JSON 文件。以下 CLI 命令會顯示 `create-backup-plan`，其 JSON名為 `test-backup-plan.json`：

```
aws backup create-backup-plan --cli-input-json file://PATH-TO-FILE/test-backup-plan.json
```

備份計畫選項和組態

在 AWS Backup 主控台中定義備份計畫時，請設定下列選項：

備份計畫名稱

您必須提供唯一的備份計劃名稱。

如果選擇的名稱與現有計畫名稱相同，您會收到錯誤訊息。

備份規則

備份計劃是由一個或多個備份規則組成的。將備份規則新增至備份計畫，或編輯備份計畫中的現有規則：

1. 在 AWS Backup 主控台的左側導覽窗格中，選擇 [Backup 方案]。
2. 在 備份計畫名稱 下，選擇備份計畫。
3. 在 備份規則 區塊下：
   - 如要新增備份規則，請選擇 新增備份規則。
   - 如要編輯現有的備份規則，請選取該規則，然後選擇 編輯。

> **Note**
>
> 如果您有具有多個規則的備份計劃，且兩個規則的時間範圍重疊，則會將備份 AWS Backup 最佳化，並為保留時間較長的規則進行備份。最佳化會考慮完整的開始時間，而非僅考慮每日備份的執行時間。

每個備份規則皆包含以下元素。

備份規則名稱

備份規則名稱區分大小寫。必須包含 1 到 50 個英數字元或連字號。

Backup frequency (備份頻率)

備份頻率決定 AWS Backup 建立快照備份的頻率。您可以使用主控台選擇的頻率包括每小時、每 12 小時、每日、每週或每月。您也可以建立 cron 運算式，以每小時的頻率建立快照備份。使用 AWS Backup CLI，您可以將快照備份排程為每小時的頻率。

選取每週時，您可以指定在星期幾執行備份。選取每月時，您可以選擇一個月中的某一天。

您也可以勾選啟用支援資源的連續備份核取方塊，以建立啟用 point-in-time 還原 (PITR) 的連續備份規則。與快照備份不同，連續備份可讓您執行 point-in-time 還原。若要深入瞭解連續備份，請參閱時間點復原。

備份時段

備份時段是由備份時段開始時間和時段持續時間 (小時) 所組成。備份任務會在這個時段內開始進行。主控台中的預設設定為：

- 系統時區當地時間的上午 1:00 (24 小時制為 1:00)
- 在 8 小時內開始
- 在 7 天內完成

  (完成時間參數不適用於 Amazon FSx 資源)

您可以使用 Cron 運算式來自訂備份頻率和備份時段的開始時間。若要查看 AWS cron 運算式的六個欄位，請參閱 Amazon CloudWatch 事件使用者指南中的 Cron 運算式。 AWS cron 表達式的兩個示例是`15 * ? * * *`（每小時在每小時 15 分鐘進行備份）和`0 12 * * ? *`（每天在 UTC 中午 12 點進行備份）。如需範例表格，請按一下前一個連結，然後向下捲動頁面。

AWS Backup 評估凌晨 12 點到 59 點之間的排程表達式。如果建立了「每 12 小時」的備份規則，但開始時間在 11:59 之後，則每天只會執行一次。

> **Note**
>
> 一般而言， AWS 資料庫服務無法在維護時段前 1 小時或期間啟動備份，而且 Amazon FSx 無法在維護時段或自動備份時段 4 小時前或期間啟動備份 (Amazon Aurora 不受此維護時段限制) 啟動備份。排程在這些時間內的快照備份會失敗。

當您為支援的服務選擇使用 AWS Backup 處理快照和連續備份時，就會發生例外狀況。 AWS Backup 會自動排程備份時段以免發生衝突。如需支援的服務清單以及如何使用 AWS Backup 連續備份的指示，請參閱時間點復原。

重疊的備份規則

備份計畫有時可能會包含多個重疊的規則。當不同規則的開始時段重疊時， AWS Backup 會在規則下保留備份，並保留較長的保留期。例如，假設備份計畫有兩條規則：

1. 每小時備份，啟動時段為 1 小時，保留 1 天。
2. 每 12 小時備份，啟動時段為 8 小時，保留 1 週。

24 小時後，第二條規則會建立兩個備份 (因為保留期較長)。第一條規則會建立八個備份 (因為第二條規則的 8 小時啟動時段會禁止執行更多的每小時備份)。具體而言：

在此啟動時段期間	此規則會建立 1 個備份
午夜至上午 8 點	12 小時
8 至 9	每小時
9 至 10	每小時
10 至 11	每小時
11 至中午	每小時
中午至下午 8 點	12 小時
8 至 9	每小時
9 至 10	每小時
10 至 11	每小時
11 至午夜	每小時

在啟動時段期間，備份任務狀態會保持在 CREATED 狀態，直到順利開始或啟動時段時間用完為止。如果在開始時段時間內 AWS Backup 收到允許重試工作的錯誤訊息，則 AWS Backup 會自動重試一次至少每 10 分鐘開始工作，直到備份成功開始 (工作狀態變更為RUNNING) 或工作狀態變更為 EXPIRED (預期會在開始時段時間結束時發生)。

生命週期和儲存層

會按照您指定的天數 (稱為備份生命週期) 存放備份。在備份生命週期結束前都可以還原備份。

這是在 AWS Backup 主控台備份規則組態的生命週期區段中設定的總保留期間。如果使用 AWS CLI，則使用參數設定DeleteAfterDays。快照的保留期為 1 天到 100 年 (如不輸入則無限期)，而連續備份的保留期則為 1 天到 35 天。

備份的維護會在儲存層中進行。如 AWS Backup 定價所述，每一層會產生不同的儲存和還原成本。每個備份的建立和存放會在常用儲存中進行。視您選擇存放備份的時間長度而定，您可能希望將備份轉移至名為不常用儲存的較低成本層。各資源的功能可用性 會顯示哪些資源具有此選用功能。

Console

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 建立或編輯備份計畫。
3. 在備份規則組態的生命週期區段中，勾選將備份從常用儲存移到不常用儲存此方塊。
4. (選用) 如果 Amazon EBS 是您備份的其中一個資源，而且備份頻率是每月或更低的頻率，您可以使用 EBS 快照存檔將其轉移至不常用儲存層。
5. 輸入您希望備份保留在暖存儲中的值（以天為單位）。 AWS Backup 建議至少 8 天。
6. 輸入保留期總計的值 (以天為單位)。保留期總計和常用儲存中時間之間的差異，在於備份在不常用儲存中保留的天數。

AWS CLI

1. 使用 create-backup-plan 或 update-backup-plan。
2.
3. 包括 EBS 資源的布林值參數 OptInToArchiveForSupportedResources。
4. 納入 MoveToColdStorageAfterdays 參數。
5. 使用 DeleteAfterDays 參數。此值必須為 90 (天) 加上您在 MoveToColdStorageAfterDays 中輸入的值。

不常用儲存目前可用於下列資源類型：

資源類型	不常用儲存中的增量或完整備份
AWS CloudFormation	增量
DynamoDB (含 進階功能)	完整；所有層均無增量備份
Amazon EBS (使用 EBS 快照存檔)	完整；轉移後，增量備份將變為「完整」。
Amazon EFS	增量
在 Amazon EC2 執行個體上執行的 SAP HANA 資料庫	增量
Amazon Timestream	增量
VMware 虛擬機器	增量

一旦您透過主控台或命令列啟用不常用儲存的轉移，不常用儲存 (或封存) 中的備份會發生下列情況：

- 轉換的備份除了在熱儲存的時間之外，還必須儲存在冷庫中至少 90 天。 AWS Backup 需要將保留時間設定為比「過後天過渡到冷」設定長 90 天。在備份轉移至冷儲存後，您就無法再變更「轉移至冷儲存前所需天數」設定。
- 某些服務支援增量備份。對於增量備份，您必須至少有一個完整備份。 AWS Backup 建議您將生命週期設定設定為在至少 8 天之後才將備份移至冷儲存。如果過早將完整備份轉換為冷儲存 (例如，在 1 天後轉換為冷儲存)， AWS Backup 將會建立另一個暖完整備份。
- 對於支援增量備份的資源類型，如果暖備份不再參考 AWS Backup 轉換的資料，請將資料從暖儲存轉換為冷儲存區。不常用儲存中保留之備份的資料，在僅供其他不常用備份參考的情況，會依不常用儲存層價格計費。其他備份則繼續依常用儲存層定價。

備份文件庫

備份文件庫是用來組織備份的容器。以備份規則建立的備份會整理在備份規則指定的備份文件庫中。您可以使用備份保存庫來設定 AWS Key Management Service (AWS KMS) 加密金鑰，該金鑰用於加密備份保存庫中的備份，以及控制對備份儲存庫中備份的存取。您也可以對備份文件庫新增標籤，以協助整理備份文件庫。如果您不想要使用預設的文件庫，可以建立自己的文件庫。如需建立備份儲存庫的 step-by-step 指示，請參閱步驟 3：建立備份保存庫。

複製到區域

您可以在備份計畫中選擇在另一個 AWS 區域建立備份副本。如需有關備份副本的詳細資訊，請參閱跨 AWS 區域建立備份副本。

當您定義備份副本時，您可以設定下列選項：

目的地區域

備份副本的目的地區域。

(進階設定) 備份文件庫

副本的目的地備份文件庫。

(進階設定) IAM 角色

建立副本時 AWS Backup 使用的 IAM 角色。角色也必須 AWS Backup 列為受信任的實體， AWS Backup 以便承擔該角色。如果您選擇 [預 AWS Backup 設]，但帳戶中沒有預設角色，則會以正確的權限為您建立角色。

(進階設定) 生命週期

指定何時將備份副本轉換為冷儲存，以及何時到期 (刪除) 副本。轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。在副本轉換至冷儲存後，您就無法變更此值。

Expire (到期) 指定在副本刪除建立後的天數。此值必須超過 Transition to cold storage (轉換至冷儲存) 值的 90 天。

新增至復原點的標籤

您在此列出的標籤會在備份建立時自動新增至備份。

新增至備份計畫的標籤

這些標籤與備份計劃本身相關聯，以協助您整理並追蹤您的備份計畫。

進階備份設定

為在 Amazon EC2 執行個體上執行的第三方應用程式，啟用應用程式一致備份。目前， AWS Backup 支援視窗 VSS 備份。 AWS Backup 從視窗 VSS 備份中排除特定的亞馬遜 EC2 執行個體類型。如需詳細資訊，請參閱 建立 Windows VSS 備份。

AWS CloudFormation 備份計劃的範本

我們提供兩個樣本 AWS CloudFormation 模板供您參考。第一種範本會建立簡單的備份計畫。第二種範本會在備份計畫中啟用 VSS 備份。

> **Note**
>
> 如果您要使用預設的服務角色，請將 *service-role* 換成 AWSBackupServiceRolePolicyForBackup。

```
Description: backup plan template to back up all resources daily at 5am UTC, and tag
 all recovery points with backup:daily.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
```

```
        BackupPlanRule:
          -
            RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
  DDBTableWithDailyBackupTag:
    Type: "AWS::DynamoDB::Table"
    Properties:
      TableName: "TestTable"
      AttributeDefinitions:
        - AttributeName: "Album"
          AttributeType: "S"
      KeySchema:
        - AttributeName: "Album"
          KeyType: "HASH"
      ProvisionedThroughput:
        ReadCapacityUnits: "5"
        WriteCapacityUnits: "5"
      Tags:
        - Key: "backup"
          Value: "daily"

  BackupRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - "arn:aws:iam::aws:policy/service-role/service-role"

  TagBasedBackupSelection:
    Type: "AWS::Backup::BackupSelection"
    Properties:
      BackupSelection:
        SelectionName: "TagBasedBackupSelection"
```

```
        IamRoleArn: !GetAtt BackupRole.Arn
        ListOfTags:
          - ConditionType: "STRINGEQUALS"
            ConditionKey: "backup"
            ConditionValue: "daily"
      BackupPlanId: !Ref BackupPlanWithDailyBackups
    DependsOn: BackupPlanWithDailyBackups
```

```
Description: backup plan template to enable Windows VSS and add backup rule to take
 backup of assigned resources daily at 5am UTC.

Resources:
  KMSKey:
    Type: AWS::KMS::Key
    Properties:
      Description: "Encryption key for daily"
      EnableKeyRotation: True
      Enabled: True
      KeyPolicy:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              "AWS": { "Fn::Sub": "arn:${AWS::Partition}:iam::${AWS::AccountId}:root" }
            Action:
              - kms:*
            Resource: "*"

  BackupVaultWithDailyBackups:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: "BackupVaultWithDailyBackups"
      EncryptionKeyArn: !GetAtt KMSKey.Arn

  BackupPlanWithDailyBackups:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: "BackupPlanWithDailyBackups"
        AdvancedBackupSettings:
          - ResourceType: EC2
            BackupOptions:
              WindowsVSS: enabled
```

```
        BackupPlanRule:
          -
            RuleName: "RuleForDailyBackups"
            TargetBackupVault: !Ref BackupVaultWithDailyBackups
            ScheduleExpression: "cron(0 5 ? * * *)"

    DependsOn: BackupVaultWithDailyBackups
```

將資源指派至備份計畫

資源指派 AWS Backup 會指定使用您的備份計畫來保護哪些資源。 AWS Backup 提供簡單的預設設定和精細的控制項，可將資源指派給備份計劃。每次執行備份計劃時，都會掃描符合資源指派準則的所有資源。 AWS 帳戶 此自動化層級可讓您只定義一次備份計劃和資源指派。 AWS Backup 摘要刪除尋找和備份符合您先前定義之資源工作分派的新資源的工作。

您可以指派任何已選擇管理的 AWS Backup支援資源類型。 AWS Backup 如需如何選擇加入更多 AWS Backup支援的資源類型的指示，請參閱入門 1：服務選擇加入。

主 AWS Backup 控台有兩種方式可將資源類型納入備份計畫中：在備份計畫中明確指派資源類型或包含所有資源。請參閱下列要點，以了解這些選項如何與選擇加入服務搭配運作。

- 如果資源指派僅以標籤為基礎，則會套用選擇加入服務設定。
- 如果將資源類型明確指派給備份計畫 (例如 Amazon S3、Amazon EC2 或 Amazon RDS)，即使該特定服務未啟用選擇加入，該資源類型也會包含在備份中。
- 如果在資源指派中同時指定了資源類型和標籤，則備份計畫中指定的資源類型將優先於標籤條件。在此情況下，會忽略選擇加入服務設定。

您的資源指派可以包含 (或排除) 資源類型 與 資源。

- 資源類型包含 AWS Backup支援 AWS 服務或協力廠商應用程式的每個執行個體或資源。例如，DynamoDB 資源類型會參考您所有的 DynamoDB 表。
- 資源是資源類型的單一執行個體，例如其中一份 DynamoDB 表。您可以使用資源的唯一資源 ID 來指定資源。

您可以使用標籤和條件運算子進一步完善資源指派。

主題

- 使用主控台指派資源
- 以程式設計方式指派資源
- 使用指定資源 AWS CloudFormation
- 資源指派的配額

使用主控台指派資源

瀏覽至 指派資源 頁面：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 選擇 備份計畫。
3. 選擇 建立備份計畫。
4. 在 選擇範本 下拉式清單中選取任一範本，然後選擇 建立計畫。
5. 輸入備份計畫名稱。
6. 選擇 建立計畫。
7. 選擇 指派資源。

若要開始指派資源，請在 一般 區段中：

1. 輸入資源指派名稱。
2. 選擇 預設角色 或 選擇 IAM 角色。

> **Note**
>
> 如果您選擇 IAM 角色，請確認其有權備份您要指派的所有資源。如果您的角色遇到無權備份的資源，您的備份計畫會失敗。

若要指派資源，請在 指派資源 區段中，選擇 定義資源選取 下的兩個選項之一：

- 包含所有資源類型。此選項可設定備份計劃，以保護指派給備份計劃的所有目前和 future AWS Backup支援的資源。使用此選項可快速輕鬆地保護您的資料資產。

  選擇此選項時，您也可以在下一步選擇 使用標籤縮小選取範圍。
- 包含特定的資源類型。選擇此選項時，您必須在後續步驟中 選取特定的資源類型：

1. 使用 選取資源類型 下拉式功能表，指派一或多個資源類型。

   > **Important**
   >
   > RDS、Aurora、Neptune 和 DocumentDB 共用相同的 Amazon Resource Name (ARN)。選擇以 AWS Backup 管理這些資源類型之一，即在將此類型指派給備份計畫時選擇加入全部資源類型。若要縮小選取範圍，請使用標籤和條件運算子。

   完成後，會 AWS Backup 顯示您選取的資源類型清單及其預設設定，以保護每個所選資源類型的所有資源。
2. 或者，您也可以從選取的資源類型中排除特定的資源：

   1. 使用 選擇資源 下拉式功能表，取消選取預設選項。
   2. 選取要指派給備份計畫的特定資源。
3. 或者，您也可以選擇 排除所選資源類型中的特定資源 ID。如果您想要在諸多資源中排除一或幾項資源，請使用此選項，因為這比上一個步驟的選取許多資源來得快。您必須先包含資源類型，才能排除資源類型中的資源。使用下列步驟排除資源 ID：

   1. 在 排除所選資源類型中的特定資源 ID 下，選擇您使用 選取資源類型 包含的一或多個資源類型。
   2. 針對每種資源類型，使用 選擇資源 下拉式功能表選取要排除的一或多項資源。

除了先前的選擇之外，您還可以使用選用的 使用標籤縮小選取範圍 功能進行更精細的選擇。此功能可讓您縮小目前的選取範圍，使用標籤包含資源的子集。

標籤是可以指派給特定資源的鍵值對，以利識別、組織與篩選資源。標籤會區分大小寫。如需詳細資訊，請參閱《AWS 一般參考》中的標記 AWS 資源。

當您使用兩個或以上的標籤縮小選取範圍時，效果如同 AND 條件。例如，如果您使用兩個標籤 `env: prod` 和 `role: application` 縮小選取範圍，僅會將同時具有兩個標籤的資源指派給備份計畫。

使用標籤縮小選取範圍：

1. 在 使用標籤縮小選取範圍 下，從下拉式清單中選擇 金鑰。
2. 從下拉式清單中選擇 值的條件。

   - 值 是指下一個輸入，即鍵值對的值。

- 條件 可以是 Equals、Contains、Begins with 或 Ends with，或與其相反的 Does not equal、Does not contain、Does not begin with 或 Does not end with。

3. 從下拉式清單中選擇 值。
4. 選擇 新增標籤 可使用其他標籤進一步縮小範圍。

以程式設計方式指派資源

您可以在 JSON 文件中定義資源指派。此範例資源指派會將所有 Amazon EC2 執行個體指派給備份計畫 *BACKUP-PLAN-ID*：

```
{
  "BackupPlanId":"BACKUP-PLAN-ID",
  "BackupSelection":{
    "SelectionName":"resources-list-selection",
    "IamRoleArn":"arn:aws:iam::ACCOUNT-ID:role/IAM-ROLE-ARN",
    "Resources":[
      "arn:aws:ec2:*:*:instance/*"
    ]
  }
}
```

假設此 JSON 儲存為 backup-selection.json，您可以使用下列 CLI 命令將這些資源指派給備份計畫：

```
aws backup create-backup-selection --cli-input-json file://PATH-TO-FILE/backup-selection.json
```

下表列出一些資源工作分派範例，以及使用 AWS Backup API、CLI 或 SDK 進行工作分派的對應 JSON 文件。為方便您閱讀此表格，範例省略了 "BackupPlanId"、"SelectionName" 和 "IamRoleArn" 欄位。萬用字元 * 代表零或多個非空白字元。

資源指派	JSON

選取我帳戶中的所有資源。	<pre>{
	  "BackupSelection":{
	    "Resources":[
	      "*"
	    ]</pre>

資源指派	JSON
	<pre> } }</pre>

選取我帳戶中的所有資源，但排除 EBS 磁碟區。	<pre>{
	  "BackupSelection":{
	    "Resources":[
	      "*"
	    ],
	    "NotResources":[
	      "arn:aws:ec2:*:*:volume/*"
	    ]
	  }
	}</pre>

選取我帳戶中所有標記為 "backup":"true" 的資源，但排除 EBS 磁碟區。	<pre>{
	  "BackupSelection":{
	    "Resources":[
	      "*"
	    ],
	    "NotResources":[
	      "arn:aws:ec2:*:*:volume/*"
	    ],
	    "Conditions":{
	      "StringEquals":[
	        {
	          "ConditionKey":"aws:Resourc
	eTag/backup",
	          "ConditionValue":"true"
	        }
	      ]
	    }
	  }
	}</pre>

資源指派	JSON

選取所有標記為 "backup":"true" 和 "stage":"prod" 的 EBS 磁碟區和 RDS 資料庫執行個體。	{
	  "BackupSelection":{
	    "Resources":[
	      "arn:aws:ec2:*:*:volume/*",
	      "arn:aws:rds:*:*:db:*"
	    ],
	    "Conditions":{
	      "StringEquals":[
	        {
	          "ConditionKey":"aws:ResourceTag/backup",
	          "ConditionValue":"true"
	        },
	        {
	          "ConditionKey":"aws:ResourceTag/stage",
	          "ConditionValue":"prod"
	        }
	      ]
	    }
	  }
	}
	
	Note
	布林算術與 IAM 政策的運算類似，使用布林運算 OR 合併的 "Resources" 項目以及使用布林運算 AND 合併的 "Conditions" 項目。
	
	Note
	"Resources" 運算式 "arn:aws:rds:*:*:db:*" 只選取 RDS 資料庫執行個體，因為沒有對應的

資源指派	JSON
	Aurora、Neptune 或 DocumentDB 資源。

選取所有標記為 "backup":"true" 但未標記為 "stage":"test" 的 EBS 磁碟區和 RDS 執行個體。	{
	"BackupSelection":{
	"Resources":[
	"arn:aws:ec2:*:*:volume/*",
	"arn:aws:rds:*:*:db:*"
	],
	"Conditions":{
	"StringEquals":[
	{
	"ConditionKey":"aws:ResourceTag/backup",
	"ConditionValue":"true"
	}
	],
	"StringNotEquals":[
	{
	"ConditionKey":"aws:ResourceTag/stage",
	"ConditionValue":"test"
	}
	]
	}
	}
	}

資源指派	JSON

選取所有以 "key1" 標記，以 "include" 開頭不以 "key2" 開頭，且值中包含單詞 "exclude" 的資源。	{
	  "BackupSelection":{
	    "Resources":[
	      "*"
	    ],
	    "Conditions":{
	      "StringLike":[
	        {
	          "ConditionKey":"aws:ResourceTag/key1",
	          "ConditionValue":"include*"
	        }
	      ],
	      "StringNotLike":[
	        {
	          "ConditionKey":"aws:ResourceTag/key2",
	          "ConditionValue":"*exclude*"
	        }
	      ]
	    }
	  }
	}
	
	萬用字元可以用在字串的開頭、結尾和中間。請注意上例中，include* 和 *exclude* 如何使用萬用字元 (*)。您也可以在字串中間使用萬用字元，如前例 arn:aws:rds:*:*:db:* 所示。

資源指派	JSON

選取所有以 "backup":"true" 標記的資源，但 FSx 檔案系統和 RDS、Aurora、Neptune 和 DocumentDB 資源除外。	{
	  "BackupSelection":{
	    "Resources":[
	      "*"
	    ],
	    "NotResources":[
	      "arn:aws:fsx:*",
	      "arn:aws:rds:*"
	    ],
	    "Conditions":{
	      "StringEquals":[
	        {
	          "ConditionKey":"aws:Resourc
	eTag/backup",
	          "ConditionValue":"true"
	        }
	      ]
	    }
	  }
	}
	
	NotResources 中的項目使用布林值 OR 合併。

資源指派	JSON

選取所有以標籤 "backup" 和任何值標記的資源	{
	  "BackupSelection":{
	  "Resources":[
	  "*"
	  ],
	  "Conditions":{
	  "StringLike":[
	  {
	  "ConditionKey":"aws:Resourc
	eTag/backup",
	  "ConditionValue":"*"
	  }
	  ]
	  }
	  }
	}

資源指派	JSON

選取所有 FSx 檔案系統、Aurora 叢集 "my-aurora-cluster" ，以及所有標記為 "backup":"true" 的資源，但標記為 "stage":"test" 的資源除外。	{
	  "BackupSelection":{
	    "Resources":[
	      "arn:aws:fsx:*",
	      "arn:aws:rds:*:*:cluster:my-aurora-cluster"
	    ],
	    "ListOfTags":[
	      {
	        "ConditionType":"StringEquals",
	        "ConditionKey":"backup",
	        "ConditionValue":"true"
	      }
	    ],
	    "Conditions":{
	      "StringNotEquals":[
	        {
	          "ConditionKey":"aws:ResourceTag/stage",
	          "ConditionValue":"test"
	        }
	      ]
	    }
	  }
	}

資源指派	JSON

選取所有以標籤 "backup":"true" 標記的資源，但以 "stage":"test" 標記的 EBS 磁碟區除外。	使用兩個 CLI 命令建立兩個選取範圍，以選取此資源群組。第一個選項套用到除 EBS 磁碟區以外的所有資源。第二個選項套用到 EBS 磁碟區。
	
	`{ "BackupSelection":{ "Resources":[ "*" ], "NotResources":[ "arn:aws:ec2:*:*:volume/*" ], "Conditions":{ "StringEquals":[ { "ConditionKey":"aws:ResourceTag/backup", "ConditionValue":"true" } ] } } }`
	
	`{ "BackupSelection":{ "Resources":[ "arn:aws:ec2:*:*:volume/*" ], "Conditions":{ "StringEquals":[ { "ConditionKey":"aws:ResourceTag/backup", "ConditionValue":"true" } ], "StringNotEquals":[ {`

資源指派	JSON

	<pre>"ConditionKey":"aws:ResourceTag/stage",
	"ConditionValue":"test"
	}
	]
	}
	}
	}</pre>

使用指定資源 AWS CloudFormation

此 end-to-end AWS CloudFormation 範本會建立資源工作分派、備份計劃和目的地備份儲存庫：

- 名為的備份儲存庫*CloudFormationTestBackupVault*。
- 名為的備份計劃*CloudFormationTestBackupPlan*。此計畫會執行兩條備份規則，這兩條規則每天都會在 UTC 時間中午 12 點執行備份，且備份保留期為 210 天。
- 名為的資源選取項*BackupSelectionName*。
- • 資源指派會備份下列資源：
  - 任何以鍵值對 backupplan:dsi-sandbox-daily 標記的資源。
  - 以值 prod 或開頭為 prod/ 的多個值標記的任何資源。
- 資源指派不會備份下列資源：
  - 任何 RDS、Aurora、Neptune 或 DocumentDB 叢集。
  - 以值 test 或開頭為 test/ 的多個值標記的任何資源。

```
Description: "Template that creates Backup Selection and its dependencies"
Parameters:
  BackupVaultName:
    Type: String
    Default: "CloudFormationTestBackupVault"
  BackupPlanName:
    Type: String
    Default: "CloudFormationTestBackupPlan"
  BackupSelectionName:
    Type: String
    Default: "CloudFormationTestBackupSelection"
```

```
  BackupPlanTagValue:
    Type: String
    Default: "test-value-1"
  RuleName1:
    Type: String
    Default: "TestRule1"
  RuleName2:
    Type: String
    Default: "TestRule2"
  ScheduleExpression:
    Type: String
    Default: "cron(0 12 * * ? *)"
  StartWindowMinutes:
    Type: Number
    Default: 60
  CompletionWindowMinutes:
    Type: Number
    Default: 120
  RecoveryPointTagValue:
    Type: String
    Default: "test-recovery-point-value"
  MoveToColdStorageAfterDays:
    Type: Number
    Default: 120
  DeleteAfterDays:
    Type: Number
    Default: 210
Resources:
  CloudFormationTestBackupVault:
    Type: "AWS::Backup::BackupVault"
    Properties:
      BackupVaultName: !Ref BackupVaultName
  BasicBackupPlan:
    Type: "AWS::Backup::BackupPlan"
    Properties:
      BackupPlan:
        BackupPlanName: !Ref BackupPlanName
        BackupPlanRule:
          - RuleName: !Ref RuleName1
            TargetBackupVault: !Ref BackupVaultName
            ScheduleExpression: !Ref ScheduleExpression
            StartWindowMinutes: !Ref StartWindowMinutes
            CompletionWindowMinutes: !Ref CompletionWindowMinutes
            RecoveryPointTags:
```

```
            test-recovery-point-key-1: !Ref RecoveryPointTagValue
          Lifecycle:
            MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
            DeleteAfterDays: !Ref DeleteAfterDays
        - RuleName: !Ref RuleName2
          TargetBackupVault: !Ref BackupVaultName
          ScheduleExpression: !Ref ScheduleExpression
          StartWindowMinutes: !Ref StartWindowMinutes
          CompletionWindowMinutes: !Ref CompletionWindowMinutes
          RecoveryPointTags:
            test-recovery-point-key-1: !Ref RecoveryPointTagValue
          Lifecycle:
            MoveToColdStorageAfterDays: !Ref MoveToColdStorageAfterDays
            DeleteAfterDays: !Ref DeleteAfterDays
      BackupPlanTags:
        test-key-1: !Ref BackupPlanTagValue
    DependsOn: CloudFormationTestBackupVault

  TestRole:
    Type: "AWS::IAM::Role"
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: "Allow"
            Principal:
              Service:
                - "backup.amazonaws.com"
            Action:
              - "sts:AssumeRole"
      ManagedPolicyArns:
        - !Sub "arn:${AWS::Partition}:iam::aws:policy/service-
role/AWSBackupServiceRolePolicyForBackup"
  BasicBackupSelection:
    Type: 'AWS::Backup::BackupSelection'
    Properties:
      BackupPlanId: !Ref BasicBackupPlan
      BackupSelection:
        SelectionName: !Ref BackupSelectionName
        IamRoleArn: !GetAtt TestRole.Arn
        ListOfTags:
          - ConditionType: STRINGEQUALS
            ConditionKey: backupplan
            ConditionValue: dsi-sandbox-daily
```

```
        NotResources:
          - 'arn:aws:rds:*:*:cluster:*'
        Conditions:
          StringEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod
          StringNotEquals:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test
          StringLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: prod/*
          StringNotLike:
            - ConditionKey: 'aws:ResourceTag/path'
              ConditionValue: test/*
```

資源指派的配額

下列配額適用於單一資源指派：

- 500 個不含萬用字元的 Amazon Resource Name (ARN)
- 30 個含萬用字元運算式的 ARN
- 30 個條件
- 每個資源指派有 30 個標籤 (每個標籤的資源不限數量)

刪除備份計畫

只有在刪除所有關聯的選取資源之後，才能刪除備份計劃。刪除備份計劃將會刪除該計劃的目前版本。目前版本和舊版本 (如果有) 仍會存在，但不會再列在主控台的 Backup plans (備份計畫) 之下。

> **Note**
>
> 刪除備份計劃時，不會刪除現有的備份。若要移除現有的備份，請使用 刪除備份 將其從備份文件庫中刪除。

使用 AWS Backup 主控台刪除備份計畫

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側的導覽窗格中，選擇 Backup plans (備份計劃)。
3. 在清單中選擇您的備份計劃。
4. 選取與該備份計劃關聯的任何資源指派。
5. 選擇刪除。

更新備份計畫

建立備份計畫後，即可開始編輯計畫，例如新增標籤，或者新增、編輯或刪除備份規則。您對備份計劃所做的任何變更，並不會影響備份計劃所建立的現有備份計畫。這些變更只適用於未來建立的備份。

例如，當您更新備份規則中的保留期，在您進行此更新之前的備份將維持相同的保留期。該備份規則建立的任何備份都將會反映更新後的保留期。

使用 AWS Backup 主控台編輯備份計畫

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Backup plans (備份計劃)。
3. 選擇一個備份規則，然後選擇 Edit (編輯)。
4. 在備份規則中，變更您希望的設定，然後選擇 Save (儲存)。

備份文件庫

> **Note**
>
> 從 2023 年 8 月 9 日開始，將 AWS Backup 提供使用邏輯氣隙保管庫的預覽。若要註冊此預覽版，請透過電子郵件傳送要求至 <aws-backup-vault-preview@amazon .com>。
> 我們可能會在預覽期間和之後變更或調整功能。當服務全面推出 (GA) 後，將無法再使用預覽期間提供的資料和組態。 AWS 建議您在預覽版中使用測試資料，不要使用生產資料。

在中 AWS Backup，備份保管庫是儲存和組織備份的容器。

建立備份儲存庫時，您必須指定 AWS Key Management Service (AWS KMS) 加密金鑰，以加密此儲存庫中的某些備份。其他備份的加密由其來源 AWS 服務管理。如需有關加密的詳細資訊，請參閱加密AWS中的備份中的圖表。

您的帳戶一定有一個預設的備份文件庫。如果您需要針對不同備份群組使用不同的加密金鑰或存取政策，您可建立多個備份文件庫。

本節會概述如何管理 AWS Backup中的備份文件庫。

主題

邏輯氣隙隔離保存庫 (預覽)

> **Note**
>
> 從 2023 年 8 月 9 日開始，將 AWS Backup 提供使用邏輯氣隙保管庫的預覽。若要註冊此預覽版，請透過電子郵件傳送要求至 <aws-backup-vault-preview@amazon .com>。
> 我們可能會在預覽期間和之後變更或調整功能。當服務全面推出 (GA) 後，將無法再使用預覽期間提供的資料和組態。 AWS 建議您在預覽版中使用測試資料，不要使用生產資料。

概觀

AWS Backup 正在預覽可將備份複本儲存在其他儲存庫中的次要類型的 Vault。邏輯氣隙隔離保存庫是一種特製的保存庫，不但在備份文件庫功能外提供了加強安全功能，還能夠共用其他帳戶和組織的保存庫存取權，以便在發生需要快速還原資源的事件時，能有更快、更靈活的復原時間 (RTO)。

邏輯上的空氣密封保存庫配備了額外的保護功能：這些文件庫中的每個文件庫都使用 AWS 自有的密鑰進行加密，並且每個文件庫都在合規模式下設置了文件庫鎖定。

您可以選擇跨組織和帳戶共用邏輯氣隙隔離保存庫，以便在需要時，可以從共用保存庫的帳戶還原儲存在其中的備份。

預覽期間，在邏輯氣隙隔離保存庫中儲存資料不另收取額外費用。即使在邏輯氣隙隔離保存庫中的所有備份副本都不收費，但標準備份文件庫和跨區域副本中的備份仍將按公告費率收費 (請參閱定價)。

使用案例

邏輯氣隙隔離保存庫是資料保護策略中的次要保存庫。當您希望擁有具有下列特性的備份文件庫時，此保存庫有助於加強組織的保留和復原能力：

- 在合規模式下使用保存庫鎖定自動設定
- 包含可與非備份建立帳戶外之其他帳戶共用並從中還原的備份
- 使用 AWS 擁有的密鑰進行加密

邏輯氣隙隔離保存庫支援的資源包括

- Amazon EC2
- Amazon EBS
- Amazon S3
- Amazon EFS
- Amazon RDS

邏輯氣隙隔離保存庫預覽僅在美國東部 (維吉尼亞北部) 區域提供。因為此功能目前僅適用於一個區域，所以預覽期間不支援跨區域副本。

與標準備份文件庫之比較和對比

備份儲存庫是中使用的主要和標準儲存庫類型 AWS Backup。備份建立後，每個備份都會儲存在備份文件庫中。您可以指派資源型政策管理儲存在保存庫中的備份，例如儲存在保存庫中的備份生命週期。

邏輯氣隙隔離保存庫是特製的保存庫，具有額外的安全性並可彈性共用，能加快復原時間 (RTO)。此保存庫會儲存最初建立並儲存在標準備份文件庫中的備份副本。

備份文件庫可以使用金鑰加密，這是限制特定使用者存取權的安全機制。這些金鑰可由客戶管理或 AWS 管理。此外，備份文件庫還可以利用保存庫鎖定加強保護；邏輯氣隙隔離保存庫在合規模式下即配備保存庫鎖定。

如果在建立初始資源時未手動變更金 AWS KMS 鑰或設定為客戶管理金鑰 (CMK)，則無法將備份複製到邏輯上無法將備份複製到邏輯上的空氣密封保存庫。

功能	備份文件庫	邏輯氣隙隔離保存庫 (預覽)
建立備份	備份建立時會儲存為復原點	備份建立時不會儲存在此保存庫
備份儲存體	可以儲存資源的初始備份和備份副本	可以儲存來自其他保存庫的備份副本
安全性	可選擇使用金鑰加密 (客戶管理或 AWS 管理) 可選擇是否使用保存庫鎖定功能來進行鎖定	使用 AWS 擁有的金鑰加密 在合規模式下一律使用保存庫鎖定功能進行鎖定
共用性	存取可以透過政策和 AWS Organizations 管理 不相容 AWS Resource Access Manager	可以選擇是否使用 AWS RAM 跨帳戶共用
還原	擁有保存庫的同一帳戶可以還原備份	如果保存庫與其他帳戶共用，則可由非備份擁有帳戶的其他帳戶還原備份

功能	備份文件庫	邏輯氣隙隔離保存庫 (預覽)
區域性	適用於所有 AWS Backup 營運地區	預覽期間於美國東部 (維吉尼亞北部) 區域提供
資源	可以存儲包含所有 AWS Backup 支持資源的備份	可以儲存包含 Amazon EC2、Amazon EBS、Amazon EFS、Amazon S3 或 Amazon RDS 資料的備份

從主控台建立邏輯氣隙隔離保存庫

> **Important**
>
> 保管庫建立之後，保管庫的名稱和類型，以及最長和最短保留期限即無法變更，而且保存庫鎖定也無法移除。
> 當服務變成「一般可用」時，預覽期間提供的資料和組態將不再可用。 AWS 建議在預覽中使用測試資料，而不是生產資料。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選取 保存庫。
3. 隨即顯示這兩種類型的保存庫。選取 建立新保存庫。
4. 輸入備份文件庫的名稱。您可以為文件庫命名以反映所要儲存的內容，或是讓它更容易搜尋您所需要的備份。例如，您可以將它命名為 `FinancialBackups`。
5. 選取 邏輯氣隙隔離保存庫 選項按鈕。
6. 設定 最短保留期限。

   此值 (天數、月數或年數) 是備份可保留在此保存庫中的最短時間。保留期限短於此值的備份無法複製到此保存庫。
7. 設定 最長保留期限。

   此值 (天數、月數或年數) 是備份可保留在此保存庫中的最長時間。保留期限長於此值的備份無法複製到此保存庫。
8. (選用) 新增有助於搜尋及識別邏輯氣隙隔離保存庫的標籤。例如，您可以新增 `BackupType:Financial` 標籤。

9. 選取 建立保存庫。
10. 檢閱設定。如果所有的設定都如預期顯示，請選取 建立邏輯氣隙隔離保存庫。
11. 主控台會帶您前往新保存庫的詳細資訊頁面。確認保存庫詳細資料是否一如預期。

在主控台中檢視邏輯氣隙隔離保存庫的詳細資訊

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中選取 保存庫。
3. 在保存庫描述下方會有兩份清單：此帳戶擁有的保存庫和與此帳戶共用的保存庫。選取檢視保存庫所需的索引標籤。
4. 在 保存庫名稱 下，按一下保存庫的名稱即可開啟詳細資訊頁面。您可以查看摘要、復原點、受保護的資源、帳號共用、存取政策和標籤詳細資訊。

在主控台中將標準備份文件庫複製到邏輯氣隙隔離保存庫

邏輯氣隙隔離保存庫只能是備份計畫的複製任務目的地目標，或隨選複製任務的目標。

您必須擁有以下項目，才能啟動複製任務

- 備份文件庫
- 邏輯氣隙隔離保存庫
- 包含 Amazon EC2、Amazon EBS、Amazon RDS、Amazon S3 或 Amazon EFS 資料的備份
- 建立副本所使用之角色的 `kms:CreateGrant` 許可。
- 將備份作為複製工作的一部分使用 AWS 託管密鑰加密到邏輯空氣密封保管庫

確認上述事項後，

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中選取 保存庫。
3. 在保存庫詳細資訊頁面中，會顯示該保存庫的所有復原點。勾選您想要複製的復原點。
4. 選取 動作，然後從下拉式功能表中選取 複製。
5. 在下個畫面中，輸入目的地詳細資訊。

    a. 區域必須設定為美國東部 (維吉尼亞北部)

b. 目的地備份文件庫下拉式功能表會顯示符合資格的目的地保存庫。選取類型為 `logically air-gapped vault` 的保存庫

6. 待所有詳細資訊依偏好設定好後，選取 複製。

在主控台的 任務 頁面上，您可以選取 複製 任務，查看目前的複製任務。

如需詳細資訊，請參閱複製備份、跨區域備份和跨帳戶備份。

從主控台共用邏輯氣隙隔離保存庫

> **Note**
>
> 只有具有特定 IAM 權限的帳戶才能共用及管理帳戶共用。

您可以使用與您指 AWS RAM 定的其他帳戶共用邏輯上的空隙保險箱。要使用共享 AWS RAM，請確保您具有以下內容：

- 可存取的兩個或多個帳戶 AWS Backup
- 打算共用保存庫的帳戶具有必要的 RAM 許可。權限 `ram:CreateResourceShare` 為此程序必要許可。政策 `AWSResourceAccessManagerFullAccess` 包含所有必要的 RAM 相關許可。
- 至少一個邏輯氣隙隔離保存庫

共用邏輯氣隙隔離保存庫，請

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中選取 保存庫。
3. 在保存庫描述下方會有兩份清單：此帳戶擁有的保存庫和與此帳戶共用的保存庫。選取檢視保存庫所需的清單。
4. 在 保存庫名稱 下，選取邏輯氣隙隔離保存庫的名稱即可開啟詳細資訊頁面。
5. 帳戶共用 窗格會顯示共用此保存庫的帳戶。
6. 若要開始與其他帳戶共用保存庫，或編輯已共用的帳戶，請選取 管理共用。

AWS RAM 主控台會在選取「管理共用」時開啟。如需使用 RAM 共用資源的步驟，請參閱在 AWS RAM 中建立資源共 AWS用。

確認擁有適當的許可。Backup 管理員 IAM 政策 [AWSBackupFullAccess] 和 Backup 操作員 IAM 政策 [AWSBackupOperatorAccess] 包含檢視共用帳戶所需的權限；但是，您用來共用的角色需要 Resource Access Manager 寫入權限才能從 RAM 共用帳戶，例如`ram:CreateResourceShare`。

獲邀接受共用邀請的帳戶需要 12 小時才能接受邀請。請參閱《AWS RAM 使用者指南》中的 < 接受與拒絕資源共用邀請 > 。

如已完成並接受共用步驟，則保存庫摘要頁面會顯示在 Account sharing = “已共用 - 請參閱下方的帳戶共用表” 下。

使用主控台還原邏輯氣隙隔離保存庫中的備份

您可以從擁有保存庫的帳戶或從共用保存庫的任一帳戶，還原儲存在邏輯氣隙隔離保存庫中的備份。

如需如何還原復原點的相關資訊，請參閱還原備份。

使用主控台刪除邏輯氣隙隔離保存庫

> **Important**
>
> 當服務變成「一般可用」時，預覽期間提供的資料和組態將不再可用。 AWS 建議在預覽中使用測試資料，而不是生產資料。

請參閱刪除備份文件庫以刪除保存庫。如果保存庫仍包含備份 (復原點) 即無法刪除。在啟動刪除作業之前，請確認保存庫中沒有任何備份。

透過 CLI I/API 執行邏輯氣隙隔離保存庫作業

您可以使用 AWS CLI 以程式設計方式執行邏輯空氣密封儲存庫的作業。每個 CLI 都是其起源所在的 AWS 服務所特有的。與共用相關的命令會在開頭加上 `aws ram`，而所有其他命令則應在前面加上 `aws backup`。

建立

您可以修改以下的範例 CLI 命令 `CreateLogicallyAirGappedBackupVault`，以建立邏輯氣隙隔離備份文件庫：

```
aws backup create-logically-air-gapped-backup-vault \
```

```
--region us-east-1 \
--logically-air-gapped-backup-vault-name sampleName \
--min-retention-days 1 \
--max-retention-days 7 \
--creator-request-id 123456789012-34567-8901 (optional)
```

View details (檢視詳細資訊)

您可以修改以下的範例 CLI 命令 `DescribeBackupVault`，以取得有關保存庫的詳細資訊：

```
aws backup describe-backup-vault \
--region us-east-1  \
--backup-vault-name testvaultname
```

Share (分享)

> **Note**
>
> 只有 IAM 許可足夠的帳戶才能共用及管理帳戶共用。

您可以透過協助使用者共用資源的服務 AWS Resource Access Manager (RAM)，共用邏輯氣隙隔離保存庫。

AWS RAM 使用 CLI 指令`create-resource-share`。只有許可足夠的管理員帳戶才能存取此命令。如需 CLI 執行步驟，請參閱在 AWS RAM中建立資源共用。

步驟 1 到 4 要以擁有邏輯氣隙隔離保存庫的帳戶執行。步驟 5 到 8 要以共用邏輯氣隙隔離保存庫的帳戶執行。

1. 登入擁有保存庫的帳戶，或者要求組織中有足夠認證可存取來源帳戶的使用者完成這些步驟。
   - 如過去已建立資源共用，現在希望在其中新增其他資源，請改用 CLI `associate-resource-share` 搭配新保存庫的 ARN。
2. 擷取具有足夠許可的角色認證，以透過 RAM 共用保存庫。將這些內容輸入 CLI。
   - 權限 `ram:CreateResourceShare` 為此程序必要許可。此原則AWSResourceAccessManagerFullAccess包含所有 RAM 相關權限。
3. 使用create-resource-share。

a. 包括邏輯氣隙隔離保存庫的 ARN。

b. 範例輸入：

```
aws ram create-resource-share \
--name MyLogicallyAirGappedVault \
--resource-arns arn:aws:backup:us-east-1:123456789012:backup-vault:test-vault-1
 \
--principals 123456789012 \
--region us-east-1
```

輸出範例：

```
{
   "resourceShare":{
      "resourceShareArn":"arn:aws:ram:us-east-1:123456789012:resource-
share/12345678-abcd-09876543",
      "name":"MyLogicallyAirGappedVault",
      "owningAccountId":"123456789012",
      "allowExternalPrincipals":true,
      "status":"ACTIVE",
      "creationTime":"2021-09-14T20:42:40.266000-07:00",
      "lastUpdatedTime":"2021-09-14T20:42:40.266000-07:00"
   }
}
```

4. 複製輸出內的資源共用 ARN (後續步驟的必要內容)。將 ARN 交給邀請接受共用的帳戶操作員。
5. 取得資源共用 ARN

a. 如果您未執行步驟 1 到 4，請 resourceShareArn 從任何人那裡取得。

b. 範例：arn:aws:ram:us-east-1:*123456789012*:resource-share/*12345678-abcd-09876543*

6. 在 CLI 中，擔任收件者帳戶的認證。
7. 使用 get-resource-share-invitations 取得資源共用邀請。如需詳細資訊，請參閱《AWS RAM 使用者指南》中的 < 接受與拒絕邀請 > 。
8. 接受目的地 (復原) 帳戶中的邀請。

- 使用 accept-resource-share-invitation (也可使用 reject-resource-share-invitation)。

清單

您可以修改 CLI 命令 ListBackupVaults，列出該帳戶擁有並顯示的所有保存庫：

```
aws backup list-backup-vaults \
--region us-east-1
```

若僅要列出邏輯氣隙隔離保存庫，請加入參數

```

--by-vault-type LOGICALLY_AIR_GAPPED_BACKUP_VAULT
```

若要列出與該帳戶共用的保存庫，請使用

```
aws backup list-backup-vaults \
--region us-east-1 \
--by-shared
```

Copy (複製)

邏輯氣隙隔離保存庫只能是備份複製任務的目標，不能是啟動備份任務的目標。使用 StartCopyJob 將備份文件庫的現有備份複製到邏輯氣隙隔離保存庫。

正在建立邏輯氣隙隔離保存庫複製任務所用的角色，必須有許可 kms:CreateGrant。

CLI 輸入範例：

```
aws backup start-copy-job \
--region us-east-1 \
--recovery-point-arn arn:aws:resourcetype:region::snapshot/snap-12345678901234567 \
--source-backup-vault-name sourcevaultname \
--destination-backup-vault-arn arn:aws:backup:us-east-1:123456789012:backup-
vault:destinationvaultname \
--iam-role-arn arn:aws:iam::123456789012:role/service-role/servicerole
```

還原

一旦您的帳戶共用了邏輯氣隙隔離保存庫的備份，您就可以使用 StartRestoreJob 還原該備份。CLI 輸入範例：

```
aws backup start-restore-job \
```

```
--recovery-point-arn arn:aws:backup:us-east-1:accountnumber:recovery-
point:RecoveryPointID \
--metadata {\"availabilityzone\":\"us-east-1d\"} \
--idempotency-token TokenNumber \
--resource-type ResourceType \
--iam-role arn:aws:iam::number:role/service-role/servicerole \
--region us-east-1
```

Delete

以下範例 CLI 命令 DeleteBackupVault 可用於刪除保存庫。保存庫只有在保存庫中沒有備份 (復原點) 時才能予以刪除。

```
aws backup delete-backup-vault
--region us-east-1
--backup-vault-name testvaultname
```

其他可用的程式化選項包括：

- CreateBackupPlan
- UpdateBackupPlan
- DescribeRecoveryPoint
- ListRecoveryPointByBackupVault
- ListProtectedResourcesByBackupVault

建立備份文件庫

您必須先建立至少一個保存庫，再建立備份計畫或開始備份任務。

當您第一次在中使用 AWS Backup 主控台時 AWS 區域，主控台會自動建立預設儲存庫。

但是，如果您 AWS Backup 透過 AWS CLI、 AWS SDK 或 AWS CloudFormation使用，則不會建立預設儲存庫。您必須建立自己專屬的保存庫。

每 AWS 區域個最多 AWS 帳戶 可建立 100 個備份儲存庫。

建立備份文件庫 (主控台)

如需 step-by-step 使用 AWS Backup 主控台建立備份儲存庫的指示，請參閱步驟 3：建立備份保存庫入門指南中的〈〉。

建立備份文件庫 (以程式設計方式)

下列 AWS Command Line Interface 指令會建立備份儲存庫：

```
aws backup create-backup-vault --backup-vault-name test-vault
```

您也可以為備份文件庫指定以下組態。

備份文件庫名稱

備份文件庫名稱有區分大小寫，必須包含 2 到 50 個英數字元、連字號或底線。

AWS KMS 加密金鑰

加 AWS KMS 密金鑰可保護您在此備份保存庫中的備份。 AWS Backup 預設會為您建立別名為 aws/backup 的 KMS 金鑰。您可以選擇該金鑰或選擇帳戶中的任何其他金鑰 (您可透過 CLI 使用跨帳戶 KMS 金鑰)。

您可以按照《AWS Key Management Service 開發人員指南》中的建立金鑰程序建立新的加密金鑰。

建立備份保存庫並設定 AWS KMS 加密金鑰後，您將無法再編輯該備份儲存庫的金鑰。

在 AWS Backup Vault 中指定的加密金鑰會套用至特定資源類型的備份。如需備份加密的詳細資訊，請參閱安全性一節中的 中備份的加密 AWS Backup。系統會採用加密來源資源所用的金鑰來備份其他所有資源類型的備份。

備份文件庫標籤

這些與備份文件庫相關聯的標籤能幫助您整理並追蹤備份文件庫。

設定備份文件庫的存取政策

使用 AWS Backup，您可以將原則指派給備份儲存庫及其包含的資源。指派政策可讓您執行多項任務，例如授予使用者存取權限以建立備份計劃和隨需備份，但限制他們在復原點建立後將其刪除的能力。

如需使用政策授予或限制資源存取許可的相關資訊，請參閱《IAM 使用者指南》中的< 身分型政策和資源型政策 >。您也可以使用標籤控制存取。

您可以使用下列範例原則做為指南，以限制在使用 AWS Backup Vault 時對資源的存取。

> **Note**
>
> 與其他以 IAM 為基礎的原則不同， AWS Backup 存取原則不支援金鑰中的萬用字元。`Action`

如需可用來識別不同資源類型復原點的 Amazon Resource Name (ARN) 清單，請參閱 AWS Backup 資源 ARN 中的資源特定復原點 ARN。

> **Note**
>
> 文件庫存取政策僅控制使用者對 AWS Backup API 的存取。有些備份類型，例如 Amazon Elastic Block Store (Amazon EBS) 和 Amazon Relational Database Service (Amazon RDS) 快照，也可以使用這些服務的 API 存取。您可以在 IAM 中建立不同的存取政策，控制對這些 API 的存取，以完全控制對備份類型的存取。
>
> 無論文件 AWS Backup 庫的存取策略為何，都 AWS Backup 會拒絕來自與所參考資源帳號不同之帳號的任何請求。

主題

拒絕對備份文件庫中某資源類型的存取

這項政策會拒絕對備份文件庫中所有 Amazon EBS 快照之指定 API 作業的存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
```

```
            "Action": [
                "backup:UpdateRecoveryPointLifecycle",
                "backup:DescribeRecoveryPoint",
                "backup:DeleteRecoveryPoint",
                "backup:GetRecoveryPointRestoreMetadata",
                "backup:StartRestoreJob"
            ],
            "Resource": ["arn:aws:ec2:Region::snapshot/*"]
        }
    ]
}
```

拒絕對備份文件庫的存取

這個政策可針對以備份文件庫為目標的指定 API 操作拒絕存取。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": {
                "AWS": "arn:aws:iam::Account ID:role/MyRole"
            },
            "Action": [
                "backup:DescribeBackupVault",
                "backup:DeleteBackupVault",
                "backup:PutBackupVaultAccessPolicy",
                "backup:DeleteBackupVaultAccessPolicy",
                "backup:GetBackupVaultAccessPolicy",
                "backup:StartBackupJob",
                "backup:GetBackupVaultNotifications",
                "backup:PutBackupVaultNotifications",
                "backup:DeleteBackupVaultNotifications",
                "backup:ListRecoveryPointsByBackupVault"
            ],
            "Resource": "arn:aws:backup:Region:Account ID:backup-vault:backup vault
 name"
        }
    ]
}
```

拒絕對刪除備份文件庫中復原點的存取

文件庫的存取權限及刪除當中所存放復原點的能力，都取決於您授予使用者的存取許可。

請遵循以下步驟在備份文件庫上建立以資源為基礎的存取政策，避免該備份文件庫中的任何備份遭到刪除。

在備份文件庫上建立以資源為基礎的存取政策

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側的導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 選擇清單中的備份文件庫。
4. 在 Access policy (存取政策) 區段中，貼上下列 JSON 範例。這個政策能防止任何不是委託人的使用者刪除目標備份文件庫中的復原點。將*### ID* 和 `aws:userId` (*role/MyRole*) 取代為您環境的值。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "aws:userId": [
                       "AAAAAAAAAAAAAAAAAAAAA:",
                       "BBBBBBBBBBBBBBBBBBBBB",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

若要允許使用其 ARN 列出 IAM 身分，請在下列範例中使用 aws:PrincipalArn 全域條件金鑰。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement ID",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "backup:DeleteRecoveryPoint",
            "Resource": "*",
            "Condition": {
                "ArnNotEquals": {
                    "aws:PrincipalArn": [
                       "arn:aws:iam::112233445566:role/mys3role",
                       "arn:aws:iam::112233445566:user/shaheer",
                       "112233445566"
                    ]
                }
            }
        }
    ]
}
```

如需取得 IAM 實體唯一 ID 的相關資訊，請參閱《IAM 使用者指南》中的 < 取得唯一識別符 > 。

如果您想將這個政策限制為特定資源類型，而不是 "Resource": "*"，則可明確包含要拒絕的復原點類型。例如，將 Amazon EBS 快照變更為以下資源類型。

```
"Resource": ["arn:aws:ec2:Region::snapshot/*"]
```

5. 選擇連接政策。

AWS Backup 文件庫鎖定

> **Note**
>
> AWS Backup 文件庫鎖定已經由科哈塞特關聯公司評估，可用於受 SEC 17a-4、CFTC 和 FINRA 法規規範的環境。如需文件 AWS Backup 庫鎖定如何與這些規則相關聯的詳細資訊，請參閱 Cohasset 關聯合規性評估。

AWS Backup 文件庫鎖定是備份文件庫的可選功能，可以幫助您提供額外的安全性和對備份保存庫的控制。當鎖定在合規模式下為作用中且寬限期已結束時，客戶、帳戶/資料擁有者或 AWS皆無法變更或刪除保存庫組態。每個保存庫都可以有一個保存庫鎖定。

AWS Backup 確保您的備份可供您使用，直到其保留期到期為止。如果有任何使用者 (包括 root 使用者) 嘗試刪除備份或變更鎖住的 Vault 中的生命週期性質， AWS Backup 將拒絕該作業。

- 在控管模式下鎖定的保存庫，可以讓具有足夠 IAM 許可的使用者移除鎖定。
- 冷靜期 (「寬限期」) 到期後，就無法刪除在合規模式下鎖定的保存庫。在寬限期內，您仍然可以移除保存庫鎖定並變更鎖定組態。

保存庫鎖定模式

建立保存庫鎖定時，有兩種模式可供選擇：治理模式或合規模式。治理模式目的在僅允許擁有足夠 IAM 許可的使用者管理保存庫。治理模式會協助組織達到治理要求，確保只有指定的人員可以變更備份文件庫。合規模式則能讓備份文件庫中的保存庫 (及擴充後的內容) 不會在資料保留期結束前遭到刪除或變更。保存庫一旦在合規模式下鎖定，即為不可變，意為鎖定無法移除。

具有適當 IAM 許可的使用者可以管理或刪除在控管模式下鎖定的保存庫。

任何使用者或 AWS皆無法變更或刪除在合規模式下鎖定的保存庫。在合規模式下鎖定之保存庫的寬限期，是您在其鎖定且變為不可變之前所設定。

保存庫鎖定的優點

AWS Backup 文件庫鎖定提供數個好處，包括：

- WORM (單寫多讀) 組態，適用於您在備份文件庫中儲存與建立的所有備份。
- 為備份文件庫中的備份 (復原點) 多加一層防禦，以免遭意外或惡意刪除。

- 強制執行保留期限，可防止有權限的使用者 (包括 AWS 帳戶 root 使用者) 提前刪除，並符合組織的資料保護政策和程序。

使用主控台鎖定備份文件庫

您可以使用「Backup」主控台將文件 AWS Backup 庫鎖定新增至保管庫。

在備份文件庫中新增保存庫鎖定：

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，尋找 備份文件庫。按一下 備份文件庫 下稱為 保存庫鎖定 的巢狀連結。
3. 在 保存庫鎖定運作方式 或 保存庫鎖定 下，按一下 + 建立保存庫鎖定。
4. 在 保存庫鎖定詳細資訊 窗格中，選擇您要套用鎖定的保存庫。
5. 在 保存庫鎖定模式 下，選擇您要鎖定保存庫的模式。如需有關選擇模式的詳細資訊，請參閱本頁前文中的保存庫鎖定模式。
6. 請在 保留期間 選擇最短和最長的保留期間 (保留期間為選用)。在保存庫中建立的新備份和複製任務，如不遵守設定的保留期間將會失敗，這些期間將不適用保存庫中已有的復原點。
7. 如果您選擇 合規模式，則會顯示名為 保存庫鎖定開始日期 的區段。如果您選擇 控管模式，則不會顯示該區段，並且可以跳過此步驟。

   在合規模式下，保存庫鎖定有一段冷靜，是從建立保存庫鎖定到保存庫及其鎖定成為不可變且不可變更為止。您選擇的這段期間 (稱為寬限期)，時長必須至少為 3 天 (72 小時)。

   > **Important**
   >
   > 寬限期到期後，保存庫及其鎖定即不可變。任何使用者或 AWS皆無法變更或刪除。

8. 當您對組態選項感到滿意後，請按一下 建立保存庫鎖定。
9. 為確認您希望在所選模式下建立此鎖定，請在文字方塊中輸入 `confirm`，然後勾選確認為預期組態的方塊。

當步驟順利完成後，主控台頂端就會出現「成功」橫幅。

以程式設計方式鎖定備份文件庫

若要設定文件 AWS Backup 庫鎖定，請使用 API PutBackupVaultLockConfiguration。要包括的參數將取決於您要使用的保存庫鎖定模式。如果您希望在控管模式下建立保存庫鎖定，請勿包含 ChangeableForDays。如果包含此參數，將會在合規模式下建立保存庫鎖定。

以下是建立合規模式保存庫鎖定的 CLI 範例：

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --changeable-for-days 3 \
        --min-retention-days 7 \
        --max-retention-days 30
```

以下是建立控管模式保存庫鎖定的 CLI 範例：

```
aws backup put-backup-vault-lock-configuration \
        --backup-vault-name my_vault_to_lock \
        --min-retention-days 7 \
        --max-retention-days 30
```

您可以設定四個選項。

1. **BackupVaultName**

   要鎖定的保存庫名稱。

2. **ChangeableForDays** (僅合規模式包含)

   此參數指示 AWS Backup 在符合性模式下建立資料保險箱鎖定。如果想要在控管模式下建立鎖定，請省略此參數。

   此值是以天數表示。必須是大於 3 且小於 36,500 的數字，否則會傳回錯誤。

   從建立此保存庫鎖定起到指定的到期日為止，您可以使用 DeleteBackupVaultLockConfiguration 移除保存庫的保存庫鎖定。或者，您可以在此期間使用 PutBackupVaultLockConfiguration 變更組態。

   在此參數決定的指定日期當天和之後，備份文件庫將為不可變，且無法變更或刪除。

3. **MaxRetentionDays** (選用)

   這是以天數表示的數值。這是保存庫保留復原點的最長保留期間。

您選擇的最長保留時間範圍應與組織的保留資料政策一致。如果組織指示了資料的保留期間，您可以將此值設定為該期間 (以天數為單位)。例如，財務或銀行資料可能需要保存 7 年 (約 2,557 天，隨閏年而增減)。

如果未指定，文件 AWS Backup 庫鎖定將不會強制執行最長保留期限。如已指定，則此保存庫中，生命週期保留期間超過最長保留期間的備份和複製任務將會失敗。在建立保存庫鎖定之前已儲存於保存庫的復原點不會受到影響。您可以指定的最長保留期間為 36500 天 (約 100 年)。

4. **`MinRetentionDays`**(選擇性；為必要項目 CloudFormation)

這是以天數表示的數值。這是保存庫保留復原點的最短保留期間。建議使用組織維護資料所需的時間長短設定此項設定。例如，如果法規或法律要求資料至少保留七年，則以天數設定的值約為 2,557，隨閏年而增減。

如果未指定，文件 AWS Backup 庫鎖定將不會強制執行最短保留期限。如已指定，則此保存庫中，生命週期保留期間不到最短保留期間的備份和複製任務將會失敗。在資料保險箱鎖定之前已儲存在資料保 AWS Backup 險箱中的復原點不會受到影響。您可以指定的最短保留期間為 1 天。

檢閱其文件庫鎖定組態的備份 AWS Backup 儲存庫

您可以隨時透過呼叫`DescribeBackupVault`或 `ListBackupVaults` API，檢閱 AWS Backup 文件庫上的文件庫鎖定詳細資料。

請呼叫 `DescribeBackupVault` 並檢查 `Locked` 屬性，確定是否已將保存庫鎖定套用至備份文件庫。如果`"Locked": true`與以下範例一樣，您已將文件 AWS Backup 庫鎖定套用至備份保管庫。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 1,
    "Locked": true,
    "MinRetentionDays": 7,
    "MaxRetentionDays": 30,
    "LockDate": "2021-09-30T10:12:38.089000-07:00"
}
```

上述輸出會確認下列選項：

1. Locked是一個布林值，表示您是否已將「 AWS Backup 資料保險箱鎖定」套用至此備份儲存庫。True表示「文件 AWS Backup 庫鎖定」會導致對儲存在資料保險箱中的復原點進行刪除或更新作業失敗 (無論您是否仍處於冷靜寬限期)。
2. LockDate 是冷靜寬限期結束的 UTC 日期與時間。在此時間之後，您即無法刪除或變更此保存庫的鎖定。使用任何可公開取得的時間轉換器將此字串轉換成您的當地時間。

如果是 "Locked":false，與以下範例一樣，即表示您尚未套用保存庫鎖定 (或已刪除之前的鎖定)。

```
{
    "BackupVaultName": "my_vault_to_lock",
    "BackupVaultArn": "arn:aws:backup:us-east-1:555500000000:backup-
vault:my_vault_to_lock",
    "EncryptionKeyArn": "arn:aws:kms:us-
east-1:555500000000:key/00000000-1111-2222-3333-000000000000",
    "CreationDate": "2021-09-24T12:25:43.030000-07:00",
    "CreatorRequestId": "ac6ce255-0456-4f84-bbc4-eec919f50709",
    "NumberOfRecoveryPoints": 3,
    "Locked": false
}
```

在寬限期內移除保存庫鎖定 (合規模式)

若要使用 AWS Backup 主控台在寬限期內刪除文件庫鎖定 (鎖定資料庫之後但在您之前的時間LockDate)，

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽的 我的帳戶 下，按一下 備份文件庫，再按一下 備份 Vault Lock。
3. 按一下您想要移除的保存庫鎖定，再按一下 管理保存庫鎖定。
4. 按一下 刪除保存庫鎖定。
5. 隨即會出現一個警告方塊，要求您確認是否刪除該保存庫鎖定。在文字方塊中輸入 confirm，然後按一下 確認。

順利完成所有步驟後，主控台畫面頂端就會顯示「成功」橫幅。

若要使用 CLI 命令在寬限期內刪除保存庫鎖定，請使用 DeleteBackupVaultLockConfiguration，如以下 CLI 範例所示：

```
aws backup delete-backup-vault-lock-configuration \
          --backup-vault-name my_vault_to_lock
```

AWS 帳戶 以鎖定的資料保險箱關閉

當您關閉包含備份保管庫的儲存庫， AWS 並 AWS Backup 暫停您的帳戶 90 天，且備份完整無損。AWS 帳戶 如果您在 90 天內未重新開啟帳戶，請 AWS 刪除備份保管庫的內容，即使已設定「文件 AWS Backup 庫鎖定」也一樣。

其他安全考慮事項

AWS Backup 文件庫鎖定為您的資料保護防禦增加了一層額外的安全性。保存庫鎖定可與下列其他安全功能合併：

- 加密復原點
- AWS Backup 儲存庫和復原點存取原則，可讓您授與或拒絕 Vault 層級的權限，
- AWS Backup 安全性最佳做法，包括其客戶管理政策庫，可讓您授與或拒絕受 AWS 支援服務的備份和還原權限，以及
- AWS Backup Audit Manager，可讓您根據您定義的控制項清單，自動執行備份的符合性檢查。

  您可以使用 AWS Backup Audit Manager 透過 使用 AWS Backup API 建立框架 來控制 備份受 AWS Backup 文件庫鎖定保護，以協助確保預期資源受到保存庫鎖定的保護。

> **Note**
>
> AWS Backup 文件庫鎖定與 S3 Glacier 彈性擷取文件庫鎖定功能不同，該功能僅與 Amazon S3 相容。

刪除備份文件庫。

> **Note**
>
> 您無法刪除兩個備份保存庫： AWS Backup 預設備份保存庫和 Amazon EFS 自動備份保管庫。

當您刪除備份文件庫時，請將備份計劃更新為指向新的備份文件庫。若備份計劃指向已刪除的備份文件庫，便會導致備份建立失敗。

為防止意外或惡意的大量刪除，您只能在刪除 (或備份計劃生命週期刪除) 備份文件庫中所有復原點之後，刪除 AWS Backup 中的備份文件庫。若要手動刪除所有復原點，請參閱清除資源中的該節內容。

使用 AWS Backup 主控台刪除備份保存庫

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 選擇您要刪除的備份文件庫。
4. 選擇並刪除與該備份文件庫相關聯的所有備份。
5. 選擇 刪除 (位於右上角) 刪除備份文件庫。

使用備份

備份 (亦稱為「復原點」) 表示某個特定時間的資源內容，例如 Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon DynamoDB 資料表。復原點是一個術語，通常指的是 AWS 服務中的不同備份，例如 Amazon EBS 快照和 DynamoDB 備份。復原點和備份這兩個詞可互換使用。

AWS Backup 將復原點儲存在備份儲存庫中，您可以根據業務需求進行組織。舉例來說，您可以儲存內含 2020 會計年度財務資訊的一組資源。當您需要復原資源時，可以使用主 AWS Backup 控台或 AWS Command Line Interface (AWS CLI) 尋找並復原所需的資源。

每個復原點都有唯一的 ID。唯一 ID 位於復原點的 Amazon Resource Name (ARN) 結尾。如需復原點 ARN 和唯一 ID 的範例，請參閱《資源和操作》中的表格。

> **Important**
>
> 若要避免額外費用，請將保留政策的暖儲存期設定為至少一週。如需詳細資訊，請參閱 計量、成本和帳單。

下列各節將提供 AWS Backup基本備份管理作業的概觀。

主題

- 建立備份
- 複製備份
- 刪除備份
- 編輯備份
- 還原備份
- 還原測試
- 檢視備份清單

建立備份

使用 AWS Backup，您可以使用備份計劃自動建立備份，也可以透過啟動隨選備份手動建立備份。

建立自動備份

透過備份計劃自動建立備份時，系統會使用該計劃中定義的生命週期設定來進行配置。系統會在備份計劃指定的備份文件庫中整理這些備份，系統會將備份計劃中所列的標籤指派給這些備份。如需備份計劃的詳細資訊，請參閱 使用備份計畫管理備份。

建立隨需備份

若選擇建立隨需備份，則可針對所建立的備份來配置這些設定。無論是自動或手動建立備份，都會啟動備份任務。若要了解如何建立隨需備份，請參閱《建立隨需備份》。

注意：隨需備份會建立備份任務；該備份任務將在一小時內 (或指定時間) 轉換為 Running 狀態。如果您希望在備份計畫中所定義排程時間以外的時間建立備份，您可以選擇隨需備份。例如，您可以隨時使用隨需備份來測試備份和功能。

隨選備份無法與 point-in-time 還原 (PITR) 搭配使用，因為隨選備份會將資源保留在進行備份時所處的狀態，而 PITR 則使用連續備份來記錄一段時間內的變更。

備份任務狀態

每個備份任務都具有唯一 ID。例如 D48D8717-0C9D-72DF-1F56-14E703BF2345。

您可以在 AWS Backup 主控台的 任務 頁面上檢視備份任務的狀態。備份任務狀態包括 等待處理中、執行中、已中止、已完成和失敗。

增量備份的運作方式

許多資源支援增量備份 AWS Backup。《各資源的功能可用性》表格的增量備份部分提供完整清單。

儘管在第一個備份之後的每個備份都是增量的（意味著它只會捕獲先前備份的更改），但使用此備份進行的所有備份都會 AWS Backup 保留必要的參考數據以進行完整還原。即使原始 (完整) 備份的生命週期已終止並遭到刪除也一樣。

例如，如果您的第 1 天 (完整) 備份由於 3 天生命週期政策而遭到刪除，您仍然可以使用第 2 天和第 3 天的備份執行完整還原。 AWS Backup 會保留第 1 天的必要參考資料，以便執行這項操作。

存取來源資源

AWS Backup 需要訪問您的源資源以備份它們。例如：

- 若要備份 Amazon EC2 執行個體，該執行個體可以處於 `running` 或 `stopped` 狀態，但不能處於 `terminated` 狀態。這是因為`running`或`stopped`執行個體可以與之通訊 AWS Backup，但`terminated`執行個體無法進行通訊。
- 若要備份虛擬機器，其 Hypervisor 必須具有狀態為 `ONLINE` 的 Backup 閘道。如需詳細資訊，請參閱《了解 Hypervisor 狀態》。
- 若要備份 Amazon RDS 資料庫、Amazon Aurora 或 Amazon DocumentDB 叢集，這些資源必須具有 `AVAILABLE` 狀態。
- 若要備份 Amazon Elastic File System (Amazon EFS)，其必須具有 `AVAILABLE` 狀態。
- 若要備份 Amazon FSx 檔案系統，其必須具有 `AVAILABLE` 狀態。如果狀態為 `UPDATING`，則備份請求會排入佇列，直到檔案系統變成 `AVAILABLE` 為止。

  FSx for ONTAP 不支援備份某些磁碟區類型，包括 DP (資料保護) 磁碟區、LS (負載共享) 磁碟區、完整磁碟區或檔案系統上已滿的磁碟區。如需詳細資訊，請參閱《FSx for ONTAP 使用備份》。

AWS Backup 無論來源資源的健康狀態為何，都會保留先前建立的備份與您的生命週期原則一致。

主題

- 建立隨需備份
- 持續備份與 point-in-time 還原 (PITR)
- Amazon S3 備份
- 虛擬機器備份
- 進階 DynamoDB 備份
- Amazon Timestream 備份
- Amazon EC2 執行個體上的 SAP HANA 資料庫備份
- Amazon Redshift 備份
- Amazon RDS 多可用區域備份
- AWS CloudFormation 堆疊備份
- 建立 Windows VSS 備份
- Amazon EBS 備份
- 將標籤複製到備份
- 停止備份任務

建立隨需備份

在 AWS Backup 主控台上，[受保護的資源] 頁面會列出至 AWS Backup 少備份一次的資源。如果您是第一 AWS Backup 次使用，則此頁面上沒有列出任何資源 (例如 Amazon EBS 磁碟區或 Amazon RDS 資料庫)。如果備份計劃未至少執行一次排程備份任務，那麼即使已將資源指派至備份計劃，結果仍然如上述。

注意：隨需備份會立即開始備份您的資源。如果您希望在備份計畫中所定義排程時間以外的時間建立備份，您可以選擇隨需備份。例如，您可以隨時使用隨需備份來測試備份和功能。

隨選備份無法與 point-in-time 還原 (PITR) 搭配使用，因為隨選備份會將資源保留在進行備份時所處的狀態，而 PITR 則使用連續備份來記錄一段時間內的變更。

建立隨需備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 從儀表板中選擇 Create on-demand backup (建立隨需備份)。您也可以在導覽窗格中選擇 Protected resources (受保護的資源)，然後選擇 Create on-demand backup (建立隨需備份)。
3. 在 建立隨需備份 頁面上，選擇您要備份的資源類型；例如，選擇表示 Amazon DynamoDB 資料表的 DynamoDB。
4. 選擇您要保護之資源的名稱或 ID，例如VideoMetadataTable。
5. 請確認已選取 Create backup now (立即建立備份)。如此將立即啟動備份，並且很快就能讓您在 Protected resources (受保護的資源) 頁面上查看您已儲存的資源。
6. 只有具備 轉換至冷儲存 功能的資源才能擁有輸入值；否則，此欄位會標示為 不適用，因為無法將該資源類型儲存至冷儲存。請參閱《各資源的功能可用性》表格中的生命週期至冷儲存一欄，以確定資源是否符合資格。

   如果您正在使用 Amazon EFS，請選擇當此備份轉換至冷儲存時想要指定的值。
7. 選擇 Expire (到期) 值。

   > **Note**
   >
   > 當備份到期並在生命週期政策中標記為刪除時， AWS Backup 會在接下來 8 小時內的隨機選擇時間點刪除備份。此時段有助於確保效能一致。
8. 選擇現有的 Backup vault (備份文件庫) 或新建一個。選擇 Create new Backup vault (建立新的備份文件庫) 開啟新頁面來建立文件庫，完成後將返回 Create on-demand backup (建立隨需備份) 頁面。

9. 在 IAM role (IAM 角色) 下，選擇 Default role (預設角色) 或您選擇的角色。

> **Note**
>
> 如果您的帳戶中沒有 AWS Backup 預設角色，系統會為您建立具有正確權限的角色。

10. 如果您要將一或多個標籤指派至您的隨需備份，請輸入 Key(索引鍵) 和選用的 Value(值)，然後選擇 Add tag (新增標籤)。

> **Note**
>
> 對於 Amazon EC2 資源，除了您在此步驟中新增的任何標籤之外，還 AWS Backup 會自動複製現有的群組和個別資源標籤。

11. 如果您要備份的資源正在執行 Amazon EC2 執行個體，請在 進階設定 區段中選擇 Windows VSS。這可讓您取得應用程式一致的 Windows 磁碟區陰影複製服務 (VSS) 備份。

> **Note**
>
> AWS Backup 採用 EC2 備份，「無重新啟動」作為默認行為。 AWS Backup 目前支援在 Amazon EC2 上執行的資源，並且不支援某些執行個體類型。如需詳細資訊，請參閱 建立 Windows VSS 備份。

12. 選擇 Create on-demand backup (建立隨需備份)。這會帶您前往 任務 頁面，您可以在此查看任務清單。
13. 為您選擇要備份的資源選擇 備份任務 ID。在任務詳細資訊頁面，停留在 Status (狀態) 上檢視您的任務狀態。

持續備份與 point-in-time 還原 (PITR)

對於某些資源，除了快照備份之外，還 AWS Backup 支援持續備份和 point-in-time 復原 (PITR)。

透過持續備份，您可以在 1 秒的精確度內將 AWS Backup支援的資源倒回您選擇的特定時間來還原支援的資源 (最多可追溯至 35 天)。連續備份的運作方式是先建立資源的完整備份，然後持續備份資源的交易日誌。PITR 還原的運作方式是存取您的完整備份，並在您指定要復原的時間重新顯示交易記錄檔。 AWS Backup

您也可以每小時進行一次快照備份。快照備份最多可儲存 100 年。快照可以是完整備份或增量備份的複本形式。

由於連續備份和快照備份提供不同的好處，因此建議您同時使用連續備份和快照備份規則來保護資源。

注意：隨需備份會立即開始備份您的資源。如果您希望在備份計畫中所定義排程時間以外的時間建立備份，您可以選擇隨需備份。例如，您可以隨時使用隨需備份來測試備份和功能。

隨選備份無法與 point-in-time 還原 (PITR) 搭配使用，因為隨選備份會將資源保留在進行備份時所處的狀態，而 PITR 則使用連續備份來記錄一段時間內的變更。

當您 AWS Backup 使用 AWS Backup 主控台或 API 建立備份計劃時，您可以選擇加入支援資源的持續備份。

使用主控台啟用連續備份

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 備份計畫，然後選擇 建立備份計畫。
3. 在 備份規則 下，選擇 新增備份規則。
4. 在 備份規則組態 區段中，選取 為支援的資源啟用連續備份。

時間點復原 (PITR) 支援的服務和應用程式

AWS Backup 支援下列服務和應用程式的持續備份與 point-in-time 復原：

主題

- Amazon S3
- RDS
- Aurora
- Amazon EC2 執行個體上的 SAP HANA

Amazon S3

若要開啟 S3 備份的 PITR，連續備份必須是備份計畫的一部分。

雖然來源儲存貯體的這個原始備份可能啟用了 PITR，但跨區域或跨帳戶目的地複本不會有 PITR，而且從這些複本中還原會還原至建立複本的時間 (這些複本會是快照複本)，而不是還原至指定的時間點。

RDS

Amazon RDS 稱其連續備份為「自動備份」。 AWS Backup 將 Amazon RDS 連續備份稱為「連續備份」。

如果您同時使 AWS Backup 用 Amazon RDS 快照和連續備份， AWS Backup 將智慧地排程備份時段以及 Amazon RDS 維護時段，以防止衝突。您不再需要手動將某個備份時段排程在另一個備份時段之前。

您無法控制 Amazon RDS 自動備份時段。這是因為 AWS Backup 會智慧地為您進行排程。

當您變更 PITR 保留期時，請立即 AWS Backup 致電`ModifyDBInstance`並套用該變更。如果您有其他組態更新擱置到下一個維護時段，變更 PITR 保留期也會立即套用這些組態更新。如需詳細資訊，請參閱《Amazon Relational Database Service API 參考》中的《`ModifyDBInstance`》。

您可以使用 AWS Backup 或 Amazon RDS 執行 point-in-time 恢復。如需 AWS Backup 主控台說明，請參閱《還原 Amazon RDS 資料庫》。如需 Amazon RDS 說明，請參閱《Amazon RDS 使用者指南》中的《將資料庫執行個體還原至指定的時間》。無論備份計畫是否有每天一次以外的快照備份頻率，RDS 都會每天建立一次快照。

增量式快照複製任務的處理速度比完整快照複製任務更快。將先前的快照複本保留到新的複製任務完成為止，可能會減少複製任務持續時間。如果您選擇從 RDS 資料庫執行個體複製快照，請務必注意，先刪除先前的複本會導致建立完整快照複本 (而非增量式)。如需如何將複製優化的詳細資訊，請參閱《Amazon RDS 使用者指南》中的《增量式快照複製》

Aurora

若要啟用 Aurora 資源的持續備份，請參閱本頁第一節中的步驟。

將 Aurora 叢集還原至某個時間點的程序是還原 Aurora 叢集快照的步驟變化。

當您執行時間點還原時，主控台會顯示 還原時間 區段。請參閱本頁使用備份底下的還原連續備份。

Amazon EC2 執行個體上的 SAP HANA

您可以建立可與 point-in-time 還原 (PITR) 搭配使用的連續備份 (請注意，隨選備份會保留資源的狀態，而 PITR 則使用連續備份來記錄一段時間內的變更)。

使用連續備份，您可以在 1 秒的精確度內倒回您選擇的特定時間來還原 EC2 執行個體上的 SAP HANA 資料庫 (最多可回到 35 天前)。連續備份的運作方式是先建立資源的完整備份，然後持續備份資源的交易日誌。PITR 還原的運作方式是存取您的完整備份，並在您指定要復原的時間重新顯示交易記錄檔。
AWS Backup

當您 AWS Backup 使用 AWS Backup 主控台或 API 建立備份計劃時，您可以選擇加入連續備份。

使用主控台啟用連續備份

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 備份計畫，然後選擇 建立備份計畫。
3. 在 備份規則 下，選擇 新增備份規則。
4. 在 備份規則組態 區段中，選取 為支援的資源啟用連續備份。

停用 SAP HANA 資料庫備份的 PITR (point-in-time 還原) 之後，記錄將繼續傳送到， AWS Backup 直到復原點到期為止 (狀態等於EXPIRED)。您可以在 SAP HANA 中變更為替代日誌備份位置，以停止將日誌傳輸至 AWS Backup。

狀態為的連續復原點STOPPED表示連續復原點已中斷；也就是說，從 SAP HANA 傳輸到顯 AWS Backup 示資料庫增量變更的記錄有間隙。在此時間範圍內發生的復原點都會具有 STOPPED. 狀態。

如需在連續備份 (復原點) 的還原任務期間可能遇到的問題，請參閱本指南的《SAP HANA 還原故障診斷》一節。

考量：

執行 point-in-time 復原時，請記住下列事項：

- 還原最近的活動 — Amazon RDS 活動最多允許還原至最近 5 分鐘的活動；Amazon S3 最多允許還原至最近 15 分鐘的活動。
- 建立 Amazon RDS 連續備份的副本 — 您無法建立 Amazon RDS 連續備份的副本，因 AWS Backup 為 Amazon RDS 不允許複製交易日誌。而是 AWS Backup 建立快照，並以備份計畫中指定的頻率複製快照。

如需使用 Amazon RDS 的一般資訊，請參閱《Amazon RDS 使用者指南》。

管理連續備份設定

將 AWS Backup 連續備份規則套用至 Amazon RDS 執行個體後，您無法在 Amazon RDS 中建立或修改該執行個體的連續備份設定。此限制的存在用意是為了防止衝突。

若要在 Amazon RDS 中檢視您的連續備份，請開啟 Amazon RDS 主控台，然後在左側選單中選擇 自動備份。

若要將該 Amazon RDS 執行個體的持續備份控制權轉換回 Amazon RDS，您可以使用 AWS Backup 主控台或 API。 AWS CLI

使用 AWS Backup 主控台將連續備份控制權轉移至 Amazon RDS

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Backup plans (備份計劃)。
3. 刪除具有連續備份保護該資源的所有 Amazon RDS 備份計畫。
4. 選擇 Backup vaults (備份文件庫)。從備份保存庫中刪除連續備份復原點。或者，等待其保留期間經過，導 AWS Backup 致自動刪除復原點。

完成這些步驟後， AWS Backup 會將資源的持續備份控制轉換回 Amazon RDS。

若要使用 AWS Backup API 或 CLI 將持續備份控制項轉換至 Amazon RDS

- 呼叫 `DisassociateRecoveryPoint` API 操作。

  如需進一步了解，請參閱DisassociateRecoveryPoint。

Amazon RDS 連續備份所需的 IAM 許可

- 若 AWS Backup 要用於設定 Amazon RDS 資料庫的連續備份，請確認 API 權限`rds:ModifyDBInstance`存在於備份計劃組態定義的 IAM 角色中。若要還原 Amazon RDS 連續備份，您必須將許可 `rds:RestoreDBInstanceToPointInTime` 新增至為還原任務提交的 IAM 角色。您可以使用 `AWS Backup default service role` 執行備份和還原。
- 要描述可用於 point-in-time 恢復的時間範圍，請 AWS Backup 撥打電話`rds:DescribeDBInstanceAutomatedBackupsAPI`。在 AWS Backup 主控台中，您必須在 AWS Identity and Access Management (IAM) 受管政策中擁有 `rds:DescribeDBInstanceAutomatedBackups` API 權限。您可以使用 `AWSBackupFullAccess` 或 `AWSBackupOperatorAccess` 受管政策。這兩個政策都有所有必要許可。如需詳細資訊，請參閱 受管政策。

使用連續備份

尋找連續備份

您可以使用 AWS Backup 主控台尋找持續備份。

使用 AWS Backup 主控台尋找持續備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 備份保存庫，然後在清單中選擇您的備份保存庫。
3. 在 備份 區段的 備份類型 欄中，排序找到連續復原點。您也可以依 復原點 ID 排序找到字首 continuous。

還原連續備份

使用 AWS Backup 主控台還原連續備份

- 在 PITR 還原程序期間， AWS Backup 主控台會顯示「還原時間」區段。在此區段中，執行下列其中一個動作：
  - 選擇還原至最近可還原的時間。
  - 選擇 指定日期和時間，輸入您自己保留期內的日期和時間。

使用 AWS Backup API 還原連續備份

1. 對於 Amazon S3，請參閱使用 AWS Backup API、CLI 或開發套件來還原 S3 復原點。
2. 對於 Amazon RDS，請參閱使用 AWS Backup API、CLI 或開發套件恢復 Amazon RDS 恢復點。

停止或刪除連續備份

您可以停止建立連續備份，也可以刪除特定備份 (point-in-time-recovery 或 PITR 點)。

如果您想要停止連續備份，您必須從備份計畫中刪除連續備份規則。如果您想要停止一或多個資源的連續備份，而不是所有資源的連續備份，請為您仍想要持續備份的資源建立具有連續備份規則的新備份計畫。如果您只是從備份保存庫中刪除連續備份復原點，則備份計畫仍會繼續執行連續備份規則，並建立新的復原點。

不過，即使在您刪除連續備份規則之後，仍 AWS Backup 會記住目前刪除之備份規則的保留期間。並會根據您指定的保留期，自動從備份保存庫中刪除您的連續備份復原點。

> **Warning**
>
> 刪除 Amazon RDS 的 point-in-time 復原點 (透過連續備份建立的備份) 時，會觸發資料庫重新開機，並停用二進位記錄。如需進一步詳細資訊，請參閱《Amazon RDS 使用者指南》中的《備份保留期》。

複製連續備份

如果連續備份規則同時指定跨帳戶或跨區域複製， AWS Backup 會建立連續備份的快照，並將該快照複製到目的地保存庫。若要進一步了解如何跨帳戶和區域複製復原點，請參閱《複製備份》。

連續備份會根據目的地帳戶和/或區域之備份計畫規則中設定的頻率來建立定期備份。

AWS Backup 不支援連續備份的隨選複本。

變更保留期

您可以用 AWS Backup 來增加或減少現有連續備份規則的保留期間。最短保留期為 1 天。最長保留期為 35 天。

如果您增加保留期，會立即生效。如果您縮短保留期， AWS Backup 將等到足夠的時間後再套用變更以防止資料遺失。例如，如果您將保留期從 35 天縮短為 20 天，則 AWS Backup 會繼續保留 35 天的連續備份，直到過去 15 天為止。此設計可保護您進行變更前過去 15 天的備份。

從備份計畫中移除唯一的連續備份規則

當您建立具有連續備份規則的備份計劃，然後移除該規則時， AWS Backup 會記住現在刪除之規則的保留期間。保留期過後，就會從您的備份保存庫中刪除連續備份。

在相同資源上重疊連續備份

一般而言，您應該確保每個資源只有一個連續備份規則。這是因為額外的連續備份是多餘的。但是，當您擴展備份資產時，多個備份計劃、規則和儲存庫可能會在單一資源上重疊。 AWS Backup 處理這些重疊的方式如下。

如果您使用連續備份規則將相同資源包含在多個備份計劃中，則只 AWS Backup 會為其評估的第一個備份計劃建立連續備份。並為所有其他備份計畫建立快照備份。

如果您在單一備份計畫中包含了多個連續備份規則：

- 如果您的規則指向相同的備份保存庫，則 AWS Backup 只會為保留期間最長的規則建立連續備份。並無視所有其他規則。

- 如果您的規則指向不同的備份儲存庫，則會將計劃 AWS Backup 拒絕為無效。

P oint-in-time 復原考量

請注意下列 point-in-time 復原的考量：

- 自動回復至快照 — 如果 AWS Backup 無法執行連續備份，則會嘗試改為執行「快照」備份。
- 不支援隨選連續備份 — AWS Backup 不支援隨選連續備份，因為隨選備份會記錄某個時間點，而連續備份記錄會在一段時間內變更。
- 不支援轉換至冷儲存 — 連續備份不支援轉換至冷儲存，因為轉換至冷儲存需要至少 90 天的轉換期，而連續備份的最長保留期為 35 天。

Amazon S3 備份

AWS Backup 支援將資料儲存在 S3 中的應用程式集中備份與還原，或與其他資料庫、儲存和運算 AWS 服務一起存放資料。許多功能適用於 S3 備份，包括 Backup Audit Manager。

您可以在中使用單一備份 AWS Backup 原則，集中自動建立應用程式資料的備份。 AWS Backup 自動將不同 AWS 服務和第三方應用程式的備份組織在一個集中的加密位置 (稱為備份保存庫)，以便您透過集中式體驗管理整個應用程式的備份。對於 S3，您可以建立連續備份並還原存放在 S3 中的應用程式資料，然後按一 point-in-time 下將備份還原到一個。

您可以使用 AWS Backup，建立下列 S3 儲存貯體的備份類型，包括物件資料、標籤、存取控制清單 (ACL) 和使用者定義的中繼資料：

- 連續備份可讓您還原至過去 35 天內的任何時間點。S3 儲存貯體的連續備份應該只在一個備份計畫中設定。

  如需支援的服務清單以及如何使用 AWS Backup 連續備份的指示，請參閱時間點復原。
- 定期備份使用資料的快照，讓您能夠保留資料一段指定的時間，最長可達 99 年。您可以按頻率排程定期備份，例如 1 小時、12 小時、1 天、1 週或 1 個月。 AWS Backup 在您在備份計劃中定義的備份時段期間定期進行備份。

  請參閱建立備份計畫，瞭解如何將備份計畫 AWS Backup 套用至資源。

S3 備份可使用跨帳戶和跨區域副本，但連續備份的副本沒有 point-in-time 還原功能。

S3 儲存貯體的連續備份和定期備份都必須位於相同的備份保存庫中。

對於這兩種備份類型，第一個備份都是完整備份，而後續備份則是在物件層級的增量備份。例如，如果 1 GB 物件有 1 KB 的變更，後續備份將在備份保存庫中建立新的 1 GB 物件。

> **Note**
>
> 您必須在 S3 儲存貯體上啟用 S3 版本控制，才能用 AWS Backup 於 Amazon S3。我們保留了這個先決條件，因為在 AWS 中，我們建議以 S3 版本控制作為資料保護的最佳實務。
> 建議您為 S3 版本設定生命週期到期期限。不設定生命週期到期時間可能會增加 S3 成本，因為 AWS Backup 備份和存放 S3 資料的所有未過期版本。若要進一步了解如何設定 S3 生命週期政策，請依照此頁面上的說明進行。

比較 S3 備份類型

S3 資源的備份策略可以僅涉及連續備份、僅涉及定期 (快照) 備份，也可以是兩者的組合。以下資訊可協助您選擇最適合您組織的策略：

僅限連續備份：

- 完成現有資料的第一個完整備份之後，系統會即時追蹤 S3 儲存貯體資料中出現的變更。
- 追蹤的變更可讓您在持續備份的保留期間內使用 PITR (point-in-time 還原)。若要執行還原任務，請選擇要還原的時間點。
- 每個連續備份的保留期最長為 35 天。

僅限定期 (快照) 備份 (排程或隨需)：

- AWS Backup 掃描整個 S3 儲存貯體、擷取每個物件的 ACL 和標籤 (如果適用且功能已開啟)，並針對先前快照中但在建立的快照中找不到的每個物件啟動 Head 請求。
- 備份是 point-in-time 一致的。
- 記錄的備份日期和時間是 AWS Backup 完成值區周遊的時間，而不是建立備份工作的時間。
- 儲存貯體的第一個備份是完整備份。每個後續備份都是增量備份，代表自上次快照以來的資料變更。
- 透過定期備份建立的快照最多可有 99 年的保留期。

連續備份結合定期/快照備份：

- 完成現有資料 (每個儲存貯體) 的第一個完整備份之後，系統會即時追蹤儲存貯體中出現的變更。
- 您可以從連續復 point-in-time 原點執行還原。

- 快照是 point-in-time 一致的。
- 快照會直接從連續復原點建立，不需要重新掃描儲存貯體，因此處理速度更快。
- 快照和連續復原點共用資料歷程；快照與連續復原點之間儲存的資料不會重複。

支援的 S3 儲存類別

AWS Backup 可讓您備份存放在下列 S3 儲存類別中的 S3 資料：

- S3 Standard
- S3 Standard - 不常存取 (IA)
- S3 單區域 – IA
- S3 Glacier Instant Retrieval
- S3 Intelligent-Tiering (S3 INT)

除了 Glacier Instant Retrieval 之外，不支援已封存的儲存類別 (包括 S3 INT - Glacier、Glacier Flexible Retrieval 和 Glacier Deep Archive)。

Amazon S3 AWS Backup 的注意事項

備份 S3 資源時，應考慮以下幾點：

- 焦點物件中繼資料支援： AWS Backup 支援下列中繼資料：標籤、存取控制清單 (ACL)、使用者定義的中繼資料、原始建立日期和版本 ID。您也可以還原所有備份的資料和中繼資料，但原始建立日期、版本 ID、儲存類別和電子標籤除外。
- S3 物件金鑰名稱可以由大多數 UTF-8 可編碼字串組成。允許使用以下 Unicode 字元：`#x9 | #xA | #xD | #x20 to #xD7FF | #xE000 to #xFFFD | #x10000 to #x10FFFF`。

  如果物件金鑰名稱包含了不在此清單中的字元，則可能會從備份中排除。如需詳細資訊，請參閱字元的 W3C 規格。
- 冷儲存轉換： AWS Backup的生命週期管理政策可讓您定義備份到期的時間表，但目前不支援 S3 備份的冷儲存轉換。
- 目前不支援備份具有在同一時間建立之多種版本相同物件的 S3 儲存貯體。
- 對於定期備份， AWS Backup 請盡最大努力追蹤物件中繼資料的所有變更。但是，如果您在 1 分鐘內多次更新標籤或 ACL，則 AWS Backup 可能不會擷取所有中繼狀態。

- AWS Backup 目前不支援 SSE-C 加密物件的備份。 AWS Backup 目前也不支援值區組態的備份，包括儲存貯體政策、設定、名稱或存取點。
- 如果您建立 S3 Intelligent-Tiering (INT) 物件的備份，則來源物件會移至比目前儲存層更昂貴的儲存層。
- AWS Backup 目前不支援 S3 的備份 AWS Outposts。

> **Important**
>
> 在記錄資料讀取事件的帳戶中，已啟用 CloudTrail 日誌的 S3 儲存貯體需要將其存取日誌儲存到不同的目標儲存貯體；如果 CloudTrail 日誌儲存在記錄的同一個儲存貯體中，則會形成無限迴圈。此迴圈可能會觸發意外和不必要的費用。
> 若要取得更多資訊，請參閱CloudTrail 使用指南中的資料事件。

S3 備份完成時間

下表顯示各種大小的範例儲存貯體，可協助指導您預估 S3 儲存貯體初始完整備份的完成時間。備份時間會因每個儲存貯體的大小、內容、組態和設定而有所不同。

儲存貯體大小	物件的數目	預估完成初始備份的時間
425 GB	1 億 3,500 萬	31 小時
800 TB	6 億 7,000 萬	38 小時
6 PB	50 億	100 小時
370 TB	75 億	180 小時

Amazon S3 備份和還原的許可和政策

若要備份、複製和還原 S3 資源，您的角色必須具有正確的政策。若要新增這些政策，請前往《AWS 受管政策》。將AWSBackupServiceRolePolicyForS3Backup和新增AWSBackupServiceRolePolicyForS3Restore至您要用來備份和還原 S3 儲存貯體的角色。

如果您沒有足夠的許可，請要求組織系統管理 (管理員) 帳戶的管理員，將政策新增至預期的角色。

如需詳細資訊，請參閱《IAM 使用者指南》中的受管政策和內嵌政策。

AWS Backup 對於 S3，依賴於通過 Amazon 接收 S3 事件 EventBridge。如果在 S3 儲存貯體通知設定中停用此設定，這些關閉設定的儲存貯體會停止連續備份。如需詳細資訊，請參閱使用 EventBridge。

S3 備份的最佳實務和成本優化

最佳實務

對於包含超過 3 億個物件的儲存貯體：

- 如果儲存貯體包含超過 3 億個物件，在儲存貯體的初始完整備份期間，備份速率最高可達每秒 17,000 個物件 (增量備份會有不同的速度)；如果儲存貯體包含少於 3 億個物件，則會以每秒近 1,000 個物件的速率進行備份。
- 建議使用連續備份。
- 如果規劃超過 35 天的備份生命週期，您也可以為儲存連續備份的同一個保存庫中的儲存貯體啟用快照備份。

成本最佳化

- S3 生命週期政策具有一項選用功能，稱為：刪除過期物件刪除標記。關閉此功能時，刪除標記 (有時好幾百萬個) 會在沒有清理計畫的情況下過期。備份沒有此功能的儲存貯體時，會有兩個影響時間和成本的問題：
  - 刪除標記會備份，就像物件一樣。備份時間和還原時間可能會受到影響，視物件與刪除標記的比例而定。
  - 每個備份的物件和標記都有最低費用。每個刪除標記要支付的費用就跟 128KiB 物件一樣。
- 對於每天至少一次或更頻繁地進行備份的帳戶，如果備份中的資料在備份之間的變化很小，則可以使用連續備份來實現成本效益。
- 不常變更的較大儲存貯體可受益於連續備份，由於不必對預先存在的物件 (自上次備份之後保持不變的物件) 執行整個儲存貯體的掃描以及針對每個物件提出多個請求，因此可降低成本。
- 與整體備份大小相比，包含超過 1 億個物件且刪除率較小的儲存貯體，可以透過同時包含保留期為 2 天的連續備份以及較長保留期的快照的備份計畫，從而實現成本效益。
- 當不需要儲存貯體掃描時，則適合開始進行定期 (快照) 備份。在同時包含連續備份和快照的儲存貯體中不需要掃描，因為在這些情況下，會從連續復原點建立快照。
- AWS KMS CloudTrail、和 Amazon CloudWatch 功能屬於備份策略的一部分，可能會導致 S3 儲存貯體資料儲存以外的額外成本。請參閱以下資訊，了解如何調整這些功能：
  - 《Amazon S3 使用者指南》中的《使用 Amazon S3 儲存貯體金鑰降低 SSE-KMS 的成本》。

- 您可以透過排除 AWS KMS 事件和停用 S3 資料事件來降低 CloudTrail 成本：
  - 排除 AWS KMS 事件：在CloudTrail 使用者指南中，在主控台中建立追蹤 (基本事件選取器) 可讓您選擇排除 AWS KMS 事件以從追蹤中篩選這些事件 (預設設定包括所有 KMS 事件)：
  - 記錄或排除 KMS 事件的選項只有在您在追蹤上記錄管理事件時才可用。如果您選擇不記錄管理事件，KMS 事件不會記錄，而且您無法變更 KMS 事件記錄設定。
  - AWS KMS 動作，例如`Encrypt`、`Decrypt`，`GenerateDataKey`通常會產生大量 (超過 99%) 的事件。這些動作現在會記錄為 Read (讀取) 事件。`Disable`、`Delete` 和 `ScheduleKey` 等少量、相關的 KMS 動作 (通常會佔 KMS 事件量的 0.5% 以下) 會記錄為寫入事件。
  - 若要排除、和等大量事件 `Encrypt` `Decrypt`，`GenerateDataKey`但仍記錄相關事件 (例如`Disable`、和`ScheduleKey`)`Delete`，請選擇記錄 Write 管理事件，然後清除 [排除 AWS KMS 事件] 的核取方塊。
  - 停用 S3 資料事件：根據預設，追蹤和事件資料存放區不會記錄資料事件。在初始備份之前停用 S3 資料事件可降低成本。
- 若要降低 CloudWatch 成本，您可以在更新追蹤以停用 CloudWatch 記錄檔設定時停止將 CloudTrail 事件傳送至 CloudWatch 記錄檔。

還原 S3 備份

您可以將使用備份的 S3 資料還原 AWS Backup 到 S3 標準儲存類別。您可以將 S3 資料還原至現有儲存貯體，包括原始儲存貯體。在還原期間，您也可以建立新的 S3 儲存貯體作為還原目標。您只能將 S3 備份還原到備份所 AWS 區域 在的位置。

您可以還原整個 S3 儲存貯體，或是儲存貯體內的資料夾或物件。 AWS Backup 會還原該物件的目前版本。

若要使用還原 S3 資料 AWS Backup，請參閱還原 S3 資料。

虛擬機器備份

AWS Backup 支援內部部署 VMware 虛擬機器 (VM) 的集中式自動化資料保護，以及 VMware 雲™ (VMC) 上的虛擬機器 AWS 和 VMware 雲™ (VMC) 上的虛擬機器。 AWS Outposts您可以從內部部署和 VMC 虛擬機器備份到 AWS Backup. 然後，您可以從 AWS Backup 還原至內部部署 VM、VMC 中的 VM 或 VMC on AWS Outposts。

AWS Backup 還為您提供全受管的 AWS原生 VM 備份管理功能，例如虛擬機器探索、備份排程、保留管理、低成本儲存層、跨區域和跨帳戶副本、文件 AWS Backup 庫鎖定和 AWS Backup Audit

Manager 支援、獨立於來源資料的加密，以及備份存取原則。如需功能的完整清單和詳細資訊，請參閱《各資源的功能可用性》表格。

您可以使 AWS Backup 用在 VMware 雲™ 上保護您的虛擬機器 AWS Outposts。 AWS Backup AWS 區域 將您的虛擬機器備份儲存在 VMware Cloud™ 所連線的 AWS Outposts 目標中。當您使用 VMware Cloud™ 時，您可以用 AWS Backup 來保護 AWS Backup 虛擬機器上的 VMware Cloud™，以滿足您 AWS Outposts 對應用程式資料的低延遲和本機資料處理需求。根據您的資料存放需求，您可 AWS Backup 以選擇將應用程式資料的備份儲存在您所連線 AWS Outposts 的父項 AWS 區域 中。

支援的 VM

AWS Backup 可以備份和還原下列虛擬機器：VMware ESXi 6.7、7.0 和 8.0 虛擬機器在內部部署和在 VMC 中執行的 NFS、VMFS 和 VSAN 資料存放區上執行。 AWS此外， AWS Backup 支援 SCSI 熱新增和網路區塊裝置安全通訊端層 (NBDSSL) 傳輸模式，可將來源虛擬機器的資料複製到 AWS 內部部署 VMware。若要保護 VMware 雲端上的虛擬機器 AWS，請 AWS Backup 支援熱新增模式。

AWS Backup 支援由 VMware 虛擬中心管理的虛擬機器，包括 vSphere 8。 AWS Backup 支援虛擬機器虛擬磁碟大小為 1 KiB 的倍數。

AWS Backup 不支援 RDM (原始磁碟對應) 磁碟或 NVMe 控制器及其磁碟。

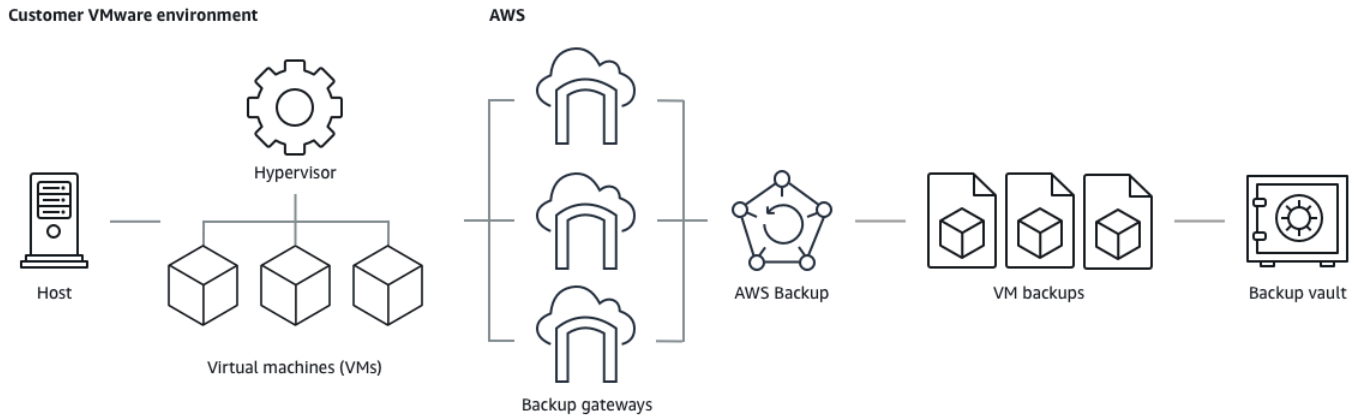
注意：不支援具有獨立持久性和獨立非持久性磁碟模式的 VM。

備份一致性

根據預設，AWS Backup會使用 VM 上的 VMware Tools 靜止設定擷取 VM 的應用程式一致備份。如果您的應用程式與 VMware Tools 相容，您的備份就是應用程式一致的。如果無法使用靜止功能，請 AWS Backup 擷取當機一致性備份。透過測試還原，即可驗證您的備份是否符合組織的需求。

Backup 閘道

Backup 閘道是可下載的 AWS Backup 軟體，您可部署至 VMware 基礎架構以連接 VMware 虛擬機器 AWS Backup。閘道會連線至您的 VM 管理伺服器，以探索 VM、加密資料，並有效率地將資料傳輸至 AWS Backup。下圖說明 Backup 閘道如何連線至 VM：



若要下載 Backup 閘道軟體，請遵循《使用閘道》的程序。

如需 VPC (虛擬私有雲) 端點的相關資訊，請參閱AWS Backup 和 AWS PrivateLink 連線。

Backup 閘道隨附自己的 API，會與 AWS Backup API 分開維護。若要檢視 Backup 閘道 API 動作清單，請參閱《Backup 閘道動作》。若要檢視 Backup 閘道 API 資料類型清單，請參閱《Backup 閘道資料類型》。

端點

目前使用公有端點並想切換至 VPC (虛擬私有雲端) 端點的現有使用者可以使用 AWS PrivateLink 建立具有 VPC 端點的新閘道，將現有 Hypervisor 與閘道建立關聯，然後刪除包含公有端點的閘道。

設定您的基礎設施以使用 Backup 閘道

Backup 閘道需要下列網路、防火牆和硬體組態，才能備份及還原您的虛擬機器。

網路組態

Backup 閘道需要允許特定連接埠才能進行操作。允許下列連接埠：

1. TCP 443 傳出
   - 來源：Backup 閘道
   - 目的地: AWS
   - 使用：允許 Backup 閘道與通訊 AWS。
2. TCP 80 傳入
   - 來源：您用來連接到 AWS Management Console

- 目的地：Backup 閘道
- 用途：供本機系統用於取得 Backup 閘道啟用金鑰。連接埠 80 僅在啟用 Backup 閘道期間使用。AWS Backup 不要求可公開存取連接埠 80。連接埠 80 所需的存取權限級別取決於您的網路設定。如果從啟動閘道 AWS Management Console，則連線到主控台的主機必須能夠存取閘道的連接埠 80。

3. UDP 53 傳出
   - 來源：Backup 閘道
   - 目的地：網域名稱服務 (DNS) 伺服器
   - 用途：允許 Backup 閘道與 DNS 通訊。
4. TCP 22 傳出
   - 來源：Backup 閘道
   - 目的地: AWS Support
   - 使用：允許 AWS Support 訪問您的網關以幫助您解決問題。您不需要開啟此連接埠就能正常操作閘道，但必須開啟才能進行故障診斷。
5. UDP 123 傳出
   - 來源：NTP 用戶端
   - 目的地：NTP 伺服器
   - 用途：供本機系統用於將虛擬機器時間與主機時間同步。
6. TCP 443 傳出
   - 來源：Backup 閘道
   - 目的地：VMware vCenter
   - 用途：允許 Backup 閘道與 VMware vCenter 通訊。
7. TCP 443 傳出
   - 來源：Backup 閘道
   - 目的地：ESXi 主機
   - 用途：允許 Backup 閘道與 ESXi 主機通訊。
8. TCP 902 傳出
   - 來源：Backup 閘道
   - 目的地：VMware ESXi 主機
   - 用途：用於透過 Backup 閘道進行資料傳輸。

防火牆組態

Backup 閘道需要存取下列服務端點才能與之通訊 Amazon Web Services。若您使用防火牆或路由器來篩選或限制網路流量，則必須設定防火牆和路由器，以允許這些服務端點可與 AWS進行傳出通訊。不支援在 Backup 閘道與服務點之間使用 HTTP 代理。

```
proxy-app.backup-gateway.region.amazonaws.com:443
dp-1.backup-gateway.region.amazonaws.com:443
anon-cp.backup-gateway.region.amazonaws.com:443
client-cp.backup-gateway.region.amazonaws.com:443
```

為 VMware 中的多個 NIC 設定閘道

您可以將多個虛擬網路介面連線 (NIC) 附加至閘道，然後分別導向內部流量 (閘道至 Hypervisor) 和外部流量 (閘道)，以便為內部和外部流量維護個別網路。 AWS

依預設，連線到 AWS Backup 閘道的虛擬機器具有一個網路介面卡 (eth0)。此網路包括虛擬機器管理程序、虛擬機器，以及與更廣泛的網際網路通訊的網路AWS Backup 閘道 (閘道)。

以下是具有多個虛擬網路介面的設定範例：

```
        eth0:
        - IP: 10.0.3.83
        - routes: 10.0.3.0/24

        eth1:
        - IP: 10.0.0.241
        - routes: 10.0.0.0/24
        - default gateway: 10.0.0.1
```

- 在此範例中是連線至 IP 為 10.0.3.123 的 Hypervisor，由於 Hypervisor IP 是 10.0.3.0/24 區塊的一部分，因此閘道會使用 eth0。
- 若要連線至 IP 為 10.0.0.234 的 Hypervisor，閘道會使用 eth1
- 若要連線至本機網路外部的 IP (例如 34.193.121.211)，閘道會回復至預設閘道 10.0.0.1，該閘道位於 10.0.0.0/24 區塊中，因此會通過 eth1

新增其他網路介面卡的第一個步驟會在 vSphere Client 中進行：

1. 在 VMware vSphere Client 中，以滑鼠右鍵按一下閘道虛擬機器以開啟內容選單，然後選擇 編輯設定。
2. 在 虛擬機器屬性 對話方塊的 虛擬硬體 索引標籤上，開啟 新增裝置 選單，然後選取 網路介面卡以新增網路介面卡。
3.
   a. 展開 新增網路 詳細資訊以設定新的介面卡。
   b. 確定已選取 在開機時連線。
   c. 針對 介面卡類型，請參閱《ESXi 和 vCenter Server 說明文件》中的網路介面卡類型。
4. 按一下 確定 以儲存新的網路介面卡設定。

設定其他 Adpater 的下一系列步驟會在 AWS Backup 閘道主控台中進行 (請注意，這與管理備份和其他服務的 AWS 管理主控台不同的介面)。

將新的 NIC 加入閘道 VM 之後，您需要

- 前往 `Command Prompt` 並開啟新的介面卡
- 為每個新的 NIC 設定靜態 IP
- 將偏好的 NIC 設定為預設值

若要執行這些動作：

1. 在 VMware vSphere Client 中，選取閘道虛擬機器，然後啟動 Web 主控台以存取 Backup 閘道本機主控台。
   - 如需存取本機主控台的詳細資訊，請參閱《使用 VMware ESXi 存取閘道本機主控台》
2. 結束命令提示字元並前往「網路組態」>「設定靜態 IP」，然後依照設定說明來更新路由表。
   a. 指派網路介面卡子網路內的靜態 IP。
   b. 設定網路遮罩。
   c. 輸入預設閘道的 IP 地址。這是連線至本機網路外部所有流量的網路閘道。
3. 選取 設定預設介面卡，將連線至雲端的介面卡指定為預設裝置。
4. 閘道的所有 IP 地址可顯示在本機主控台和 VMware vSphere 的 VM 摘要頁面上。

硬體要求

您必須能夠在 Backup 閘道的虛擬機器主機上指定下列基本資源：

- 4 個虛擬處理器
- 8 GiB 預留 RAM

VMware 許可

本節列出使用 Backup 閘道所需的最低 VMware 許可。Backup 閘道需要這些許可，才能探索、備份和還原虛擬機器。

若要使用 Backup 閘道，請建立具有下列許可的專用使用者。這些許可會根據 VMware 許可階層列出。

全球服務

- 停用方法
- 啟用方法
- 授權
- 日誌事件
- 管理自訂屬性
- 設定自訂屬性

vSphere 標記

- 指派或取消指派 vSphere 標籤

DataStore

- 配置空間
- 瀏覽資料儲存
- 設定資料儲存 (適用於 vSAN 資料儲存)
- 低層級檔案操作
- 更新虛擬機器檔案

主機

- 組態

- 進階設定
- 儲存分割區組態

資料夾

- 建立資料夾

網路

- 指派網路

dvPort 群組

- 建立
- Delete

資源

- 將虛擬機器指派給資源集區

虛擬機器

- 變更組態
  - 取得磁碟租用
  - 新增現有磁碟
  - 新增磁碟
  - 進階組態
  - 變更設定
  - 設定原始裝置
  - 修改裝置設定
  - 移除磁碟
  - 設定註釋
  - 切換磁碟變更追蹤
- 編輯庫存

  - 從現有項目建立
  - 建立新項目
  - 登錄
  - Remove (移除)
  - 取消註冊
- 互動
  - 關機
  - 開機
- 佈建中
  - 允許磁碟存取
  - 允許唯讀磁碟存取
  - 允許虛擬機器下載
- 快照管理
  - 建立快照
  - 移除快照
  - 還原至快照

使用閘道

若要使用 Backup 和還原虛擬機器 (VM) AWS Backup，您必須先安裝備份閘道。閘道是 OVF (開放虛擬化格式) 範本形式的軟體，可將 Amazon Web Services Backup 連接至您的 Hypervisor，讓它能夠自動偵測您的虛擬機器，並讓您備份和還原它們。

單一閘道一次最多可以執行 4 個備份或還原任務。若要一次執行 4 個以上的任務，請建立更多閘道，並將其與您的 Hypervisor 建立關聯。

建立閘道

若要建立閘道：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格的 外部資源 區段下，選擇 閘道。
3. 選擇 Create gateway (建立閘道)。
4. 在 設定閘道 區段中，依照下列說明下載並部署 OVF 範本。

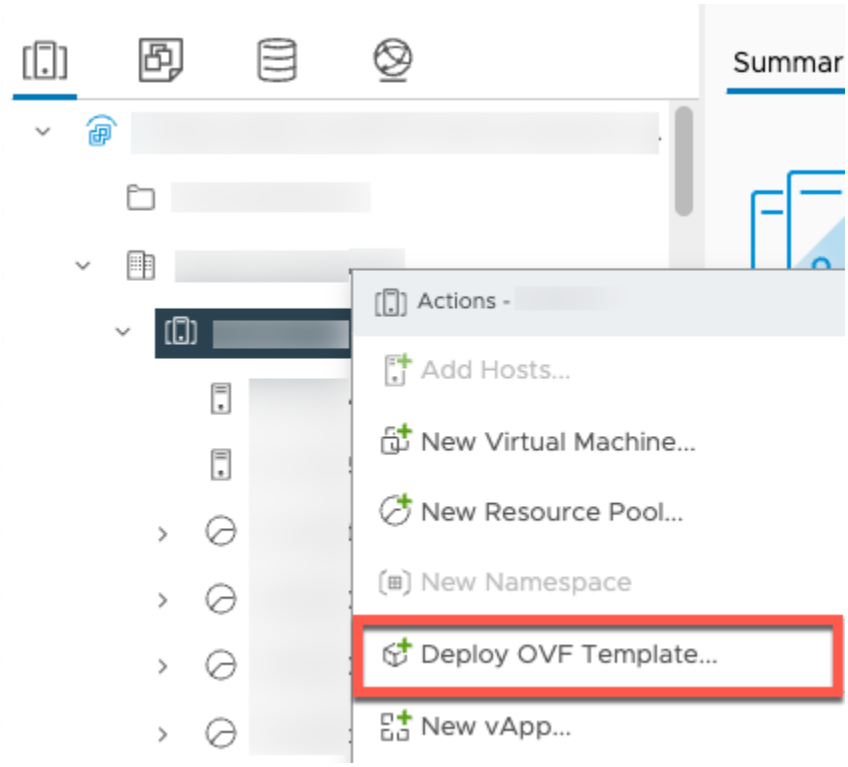
下載 VMware 軟體

連線至 Hypervisor

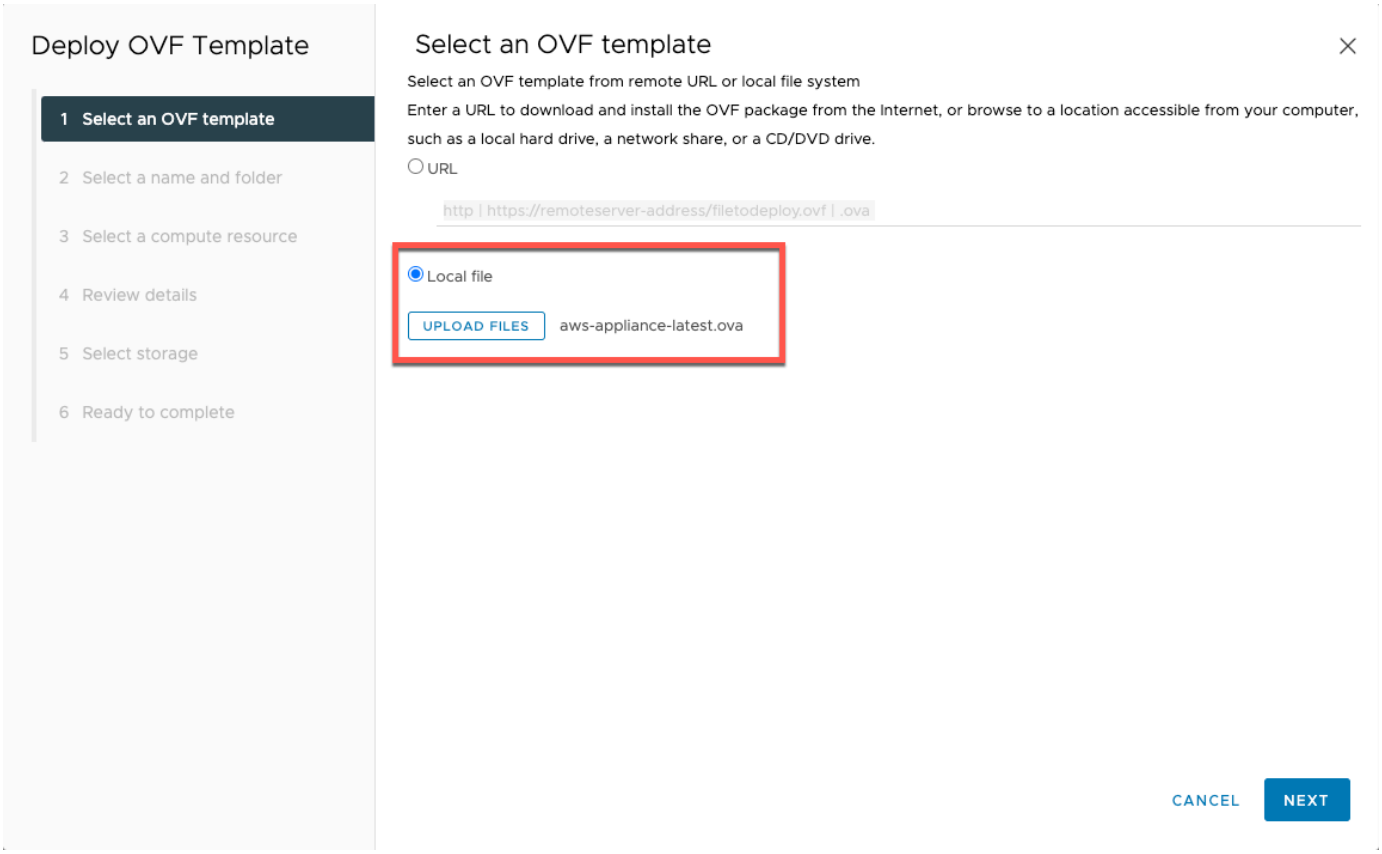
閘道會連線 AWS Backup 至您的 Hypervisor，因此您可以建立並儲存虛擬機器的備份。若要在 VMware ESXi 上設定閘道，請下載 OVF 範本。下載可能需要約 10 分鐘的時間。

完成後，請繼續執行下列步驟：

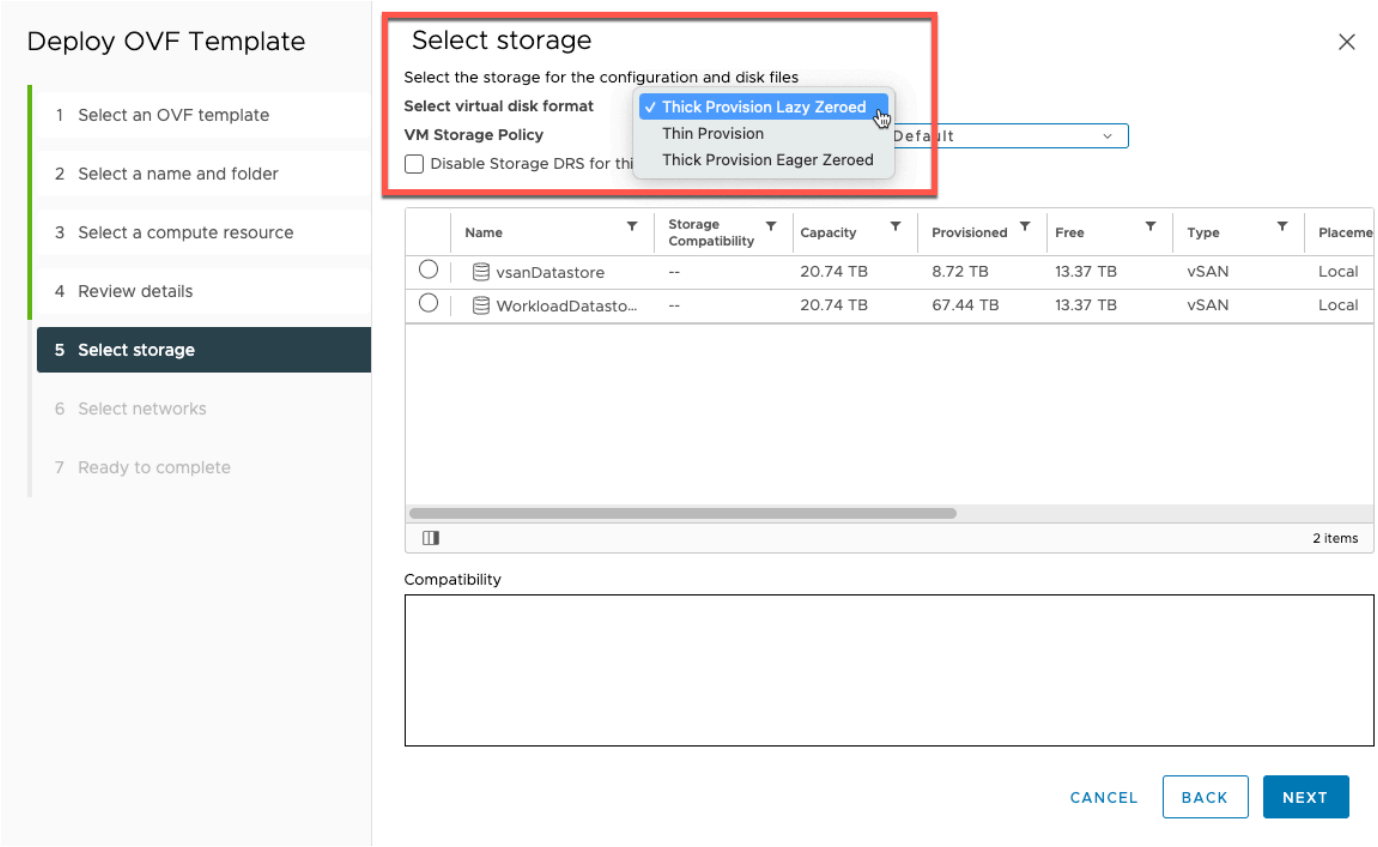
1. 使用 VMware vSphere 連線至您的虛擬機器 Hypervisor。
2. 以滑鼠右鍵按一下虛擬機器的父系物件，然後選取 部署 OVF 範本。



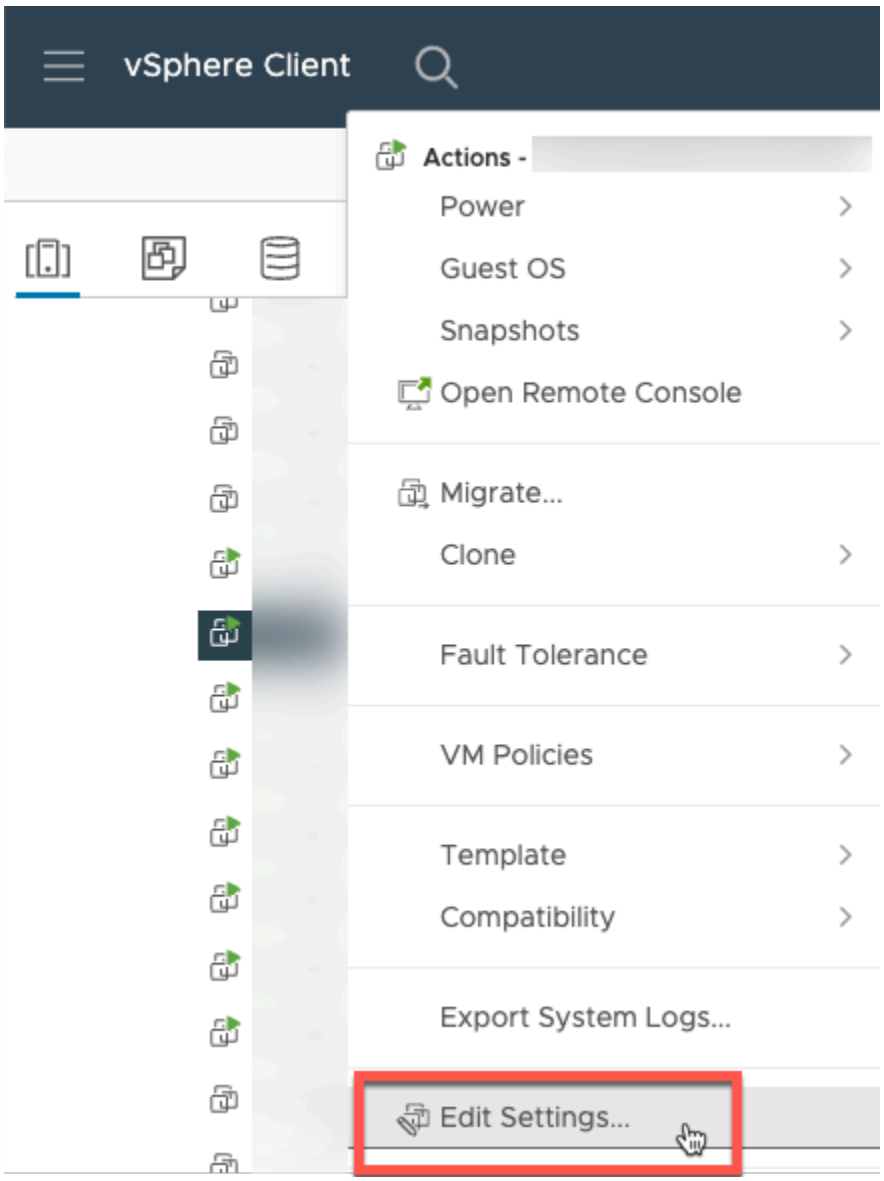
3. 選擇「本機檔案」，然後上傳您下載的 aws-appliance-latest.ova 檔案。



4. 依照部署精靈步驟進行部署。在 選取儲存 頁面上，選取虛擬磁碟格式 完整佈建全部初始化。

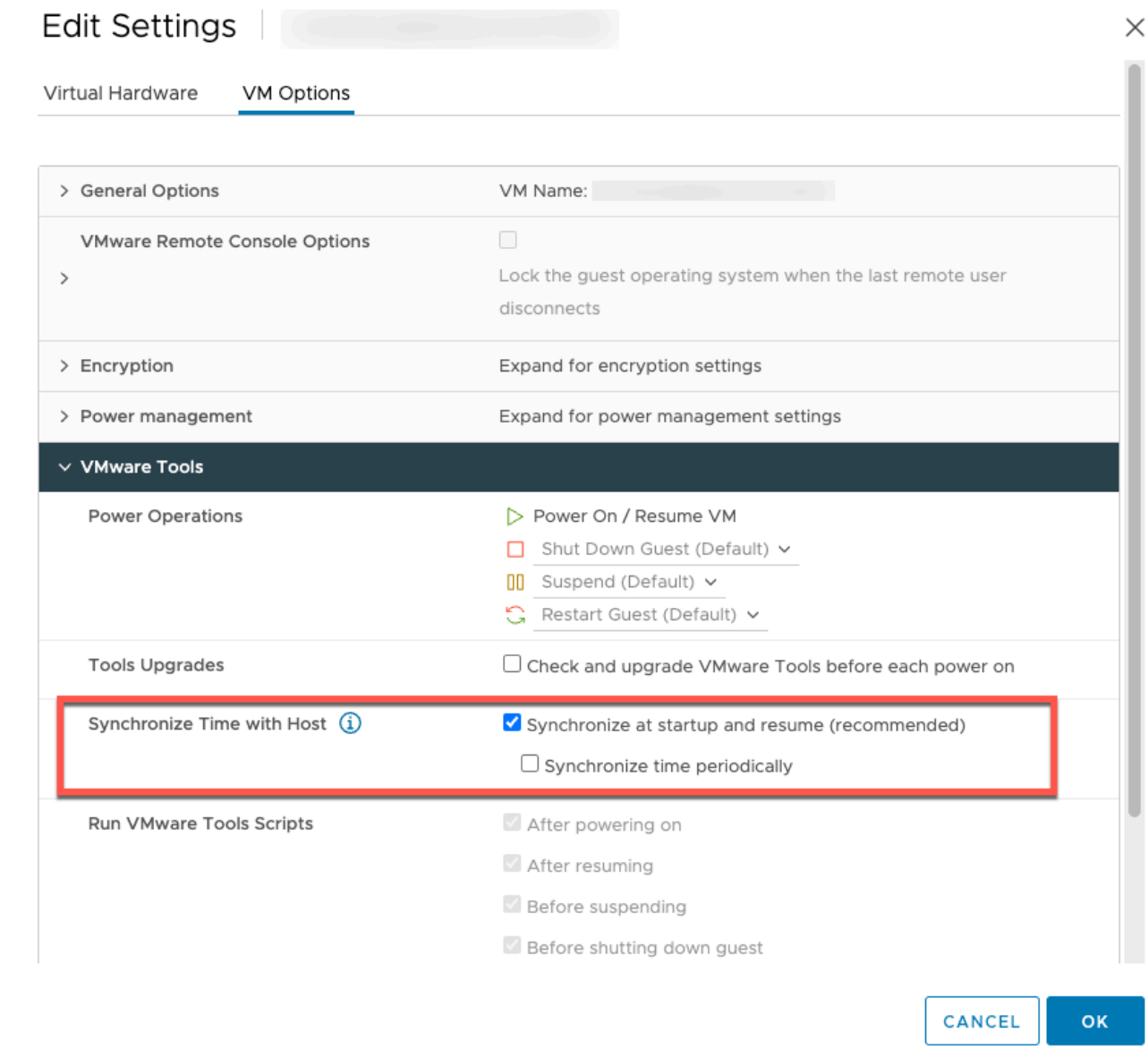


5. 部署 OVF 之後，請以滑鼠右鍵按一下閘道，然後選擇 編輯設定。

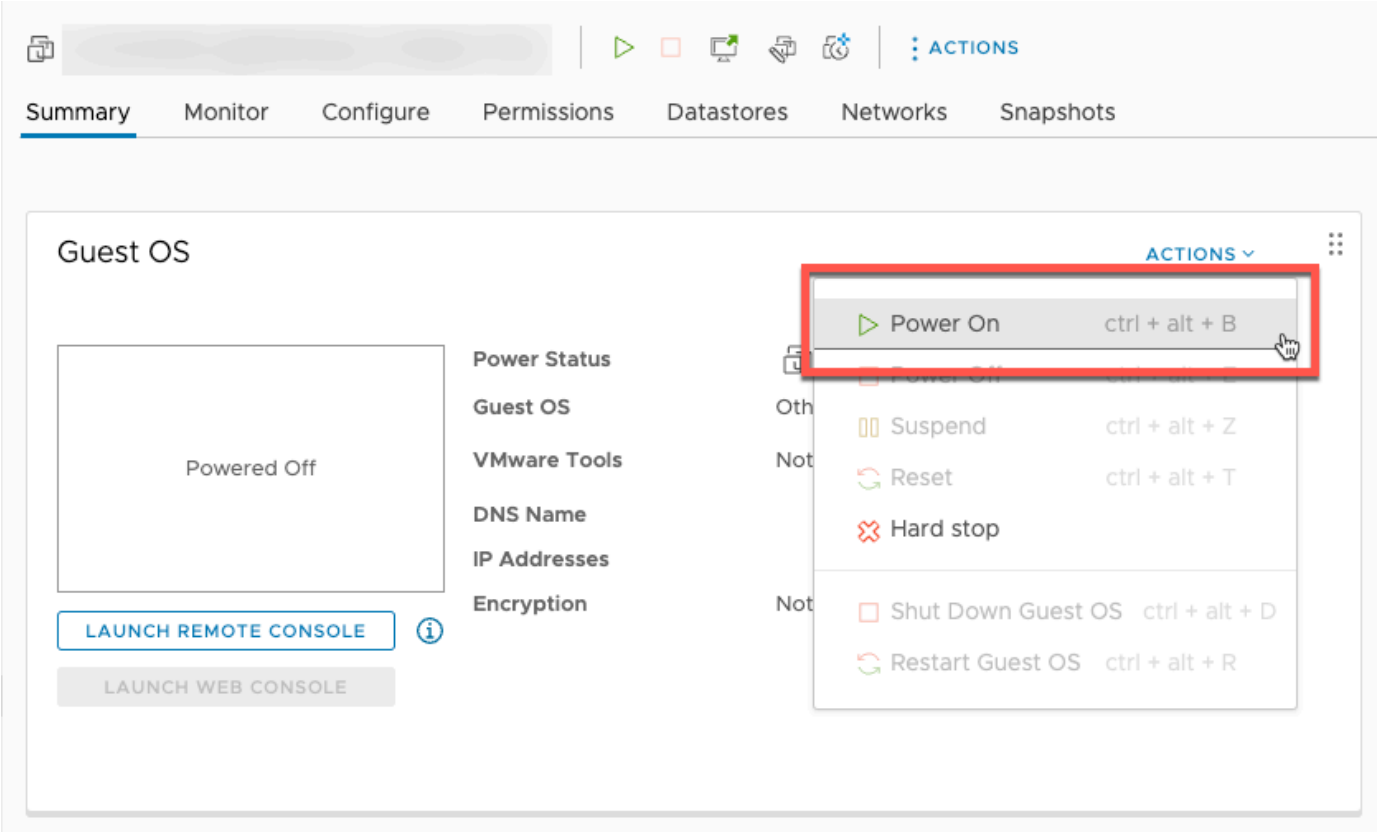


a. 在 VM 選項 下，前往 VM 工具。

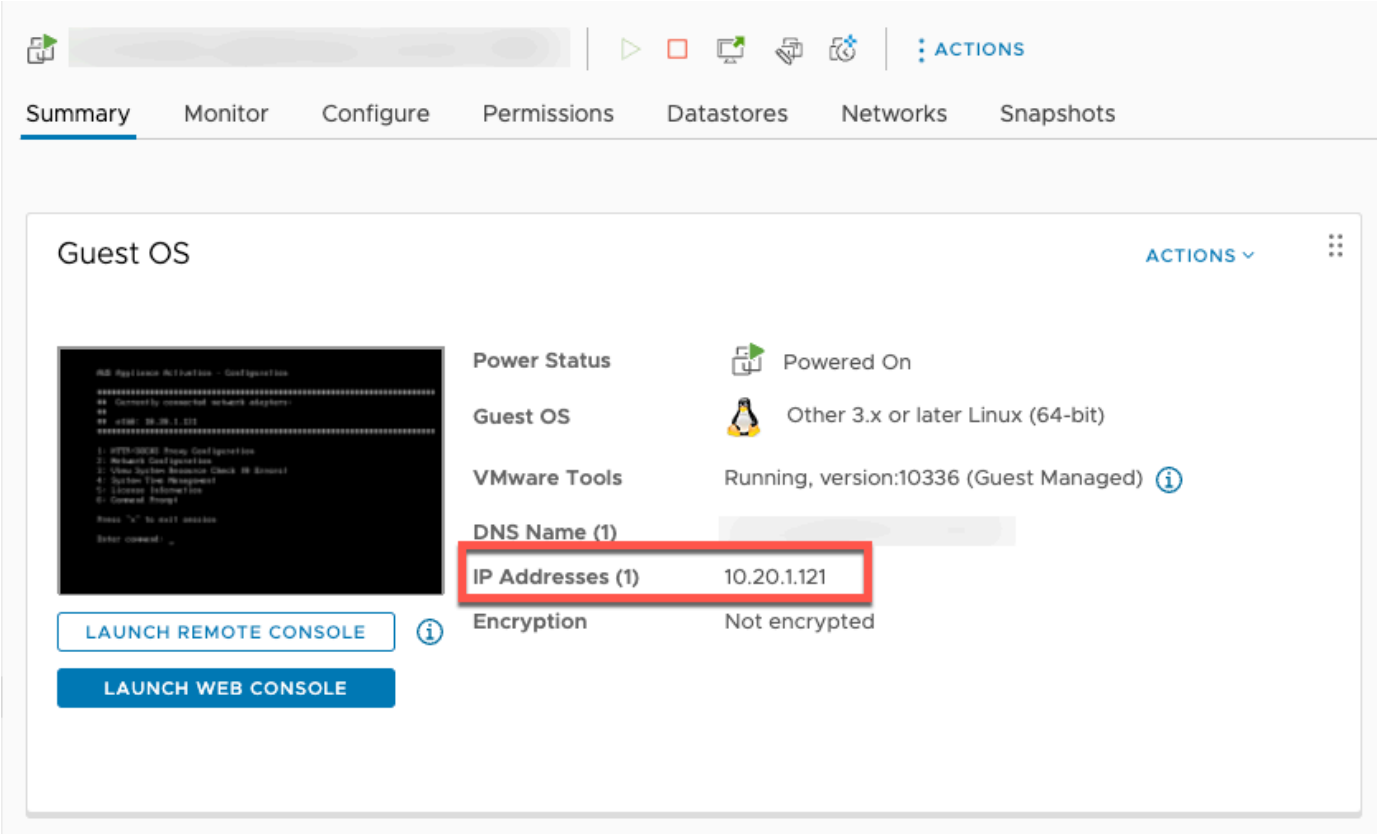
b. 確定已依序選取 主機同步時間、在啟動時同步並繼續。



6. 從 動作 選單中選取「開機」以啟動虛擬機器。



7. 從 VM 摘要複製 IP 地址，然後在下方輸入。



下載 VMware 軟體之後，請完成下列步驟：

1. 在 閘道連線 區段中，輸入閘道的 IP 地址。

   a. 若要尋找此 IP 地址，請前往 vSphere Client。

   b. 在 摘要 索引標籤下，選取您的閘道。

   c. 複製 IP 地址並將其粘貼到 AWS Backup 控制台文本欄中。

2. 在 閘道設定 區段中，

   a. 輸入 閘道名稱。

   b. 驗證「 AWS 區域」。

   c. 選擇端點是可公開存取，還是透過您的虛擬私有雲端 (VPC) 託管。

   d. 根據選擇的端點，輸入 VPC 端點 DNS 名稱。

      如需詳細資訊，請參閱《建立 VPC 端點》。。

3. [選擇性] 在 閘道標籤 區段中，您可以輸入金鑰和「選用」值來指派標籤。若要新增多個標籤，請按一下 新增其他標籤。

4. 若要完成程序，請按一下 建立閘道，這會帶您前往閘道詳細資訊頁面。

編輯或刪除閘道

若要編輯或刪除閘道：

1. 在左側導覽窗格的 外部資源 區段下，選擇 閘道。
2. 在 閘道 區段中，依 閘道名稱 選擇閘道。
3. 若要編輯閘道名稱，請選擇 編輯。
4. 若要刪除閘道，請選擇 刪除，然後選擇 刪除閘道。

   您無法重新啟用已刪除的閘道。如果您想要再次連線至 Hypervisor，請依照《建立閘道》中的程序進行。
5. 若要連線至 Hypervisor，請在 連網 Hypervisor 區段中，選擇 連線。

   每個閘道都會連線至單一 Hypervisor。不過，您可以將多個閘道連線至相同的 Hypervisor 來增加彼此之間的頻寬，以超出第一個閘道的頻寬。
6. 若要指派、編輯或管理標籤，請在 標籤 區段中，選擇 管理標籤。

Backup 閘道頻寬限流

> **Note**
>
> 此功能將在 2022 年 12 月 15 日之後部署的新閘道上提供。對於現有閘道，這項新功能將在 2023 年 1 月 30 日或之前透過自動軟體更新提供。若要手動將閘道更新為最新版本，請使用 AWS CLI 指令`UpdateGatewaySoftwareNow`。

您可以將閘道的上傳輸量限制 AWS Backup 為控制閘道使用的網路頻寬量。根據預設，啟用的閘道沒有速率限制。

您可以使用 AWS Backup 主控台或透過 AWS CLI (`PutBandwidthRateLimitSchedule`) 使用 API 來設定頻寬速率限制排程。使用頻寬速率限制排程時，您可以將限制設定為全天或全週自動變更。

頻寬速率限制的運作方式是平衡所有上傳資料的輸送量 (每秒進行平均)。雖然上傳可能會短暫超過任何指定微秒或毫秒的頻寬速率限制，但這通常不會導致更長時間出現大量尖峰。

您最多可以新增 20 個間隔。上傳速率的最大值為每秒 8,000,000 (百萬) MB (Mbps)。

使用主控台檢視和編輯閘道的頻寬速率限制排程。 AWS Backup

本節說明如何檢視和編輯閘道的頻寬速率限制排程。

檢視和編輯頻寬速率限制排程

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中，選擇 Gateways (閘道)。在「閘道」窗格中，閘道會依名稱顯示。按一下您要管理之閘道名稱旁的選項按鈕。
3. 選取選項按鈕之後，即可按一下 動作 下拉式選單。按一下 動作，然後按一下 編輯頻寬速率限制排程。目前排程會隨即顯示。根據預設，新的或未編輯的閘道沒有定義的頻寬速率限制。

   > **Note**
   >
   > 您也可以按一下閘道詳細資訊頁面中的 管理排程，導覽至「編輯頻寬」頁面。

4. (選擇性) 選擇 新增間隔，將新的可設定間隔加入排程。針對每個間隔，輸入下列資訊：

   a. 星期幾 — 選取要套用間隔的一或多個重複星期。選擇的星期會顯示在下拉式選單下方。您可以按一下該星期旁的 X 來移除星期。

   b. 開始時間 — 輸入頻寬間隔的開始時間，使用 HH: MM 24 小時格式。時間是以國際標準時間 (UTC) 表示。

      注意：您的 bandwidth-rate-limit 間隔從指定的分鐘開始開始。

   c. 結束時間 — 輸入頻寬間隔的結束時間，使用 HH: MM 24 小時格式。時間是以國際標準時間 (UTC) 表示。

      > **Important**
      >
      > 間 bandwidth-rate-limit 隔在指定的分鐘結束時結束。若要排定在小時結束時結束的間隔，請輸入 59。若要排程不間斷的連續間隔，在小時開始時轉換且間隔之間沒有中斷，請輸入 59 作為第一個間隔的結束分鐘。輸入 00 作為下一個間隔的開始分鐘。

   d. 上傳速率 — 輸入上傳速率限制，以每秒 MB 數 (Mbps) 為單位。最小值為每秒 102 MB (Mbps)。

5. (選擇性) 視需要重複上一個步驟，直到您的頻寬速率限制排程完成為止。如果您需要從排程中刪除間隔，請選擇 移除。

> **Important**
>
> 頻寬速率限制間隔不能重疊。間隔的開始時間必須在前一個間隔的結束時間之後，並在下一個間隔的開始時間之前；其結束時間必須在下一個間隔的開始時間之前。

6. 完成後，請按一下 儲存變更 按鈕。

使用 AWS CLI檢視和編輯閘道的頻寬速率限制排程

您可以使用 GetBandwidthRateLimitSchedule 動作來檢視指定閘道的頻寬限流排程。如果沒有設定排程，排程將會是一個空白的間隔清單。以下是使用擷 AWS CLI 取閘道頻寬排程的範例：

```
aws backup-gateway get-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/bgw-gw id"
```

若要編輯閘道的頻寬限流排程，您可以使用 PutBandwidthRateLimitSchedule 動作。請注意，您只能更新閘道的整個排程，不能修改、新增或移除個別間隔。呼叫此動作會覆寫閘道先前的頻寬限流排程。

```
aws backup-gateway put-bandwidth-rate-limit-schedule --gateway-arn "arn:aws:backup-gateway:region:account-id:gateway/gw-id" --bandwidth-rate-limit-intervals ...
```

使用 Hypervisor

完成之後建立閘道，您可以將它連接到 Hypervisor，以便 AWS Backup 與該 Hypervisor 管理的虛擬機器搭配使用。例如，適用於 VMware VM 的 Hypervisor 是 VMware vCenter Server。請確定您的 Hypervisor 已設定 AWS Backup的必要許可。

新增 Hypervisor

若要新增 Hypervisor：

1. 在左側導覽窗格的 外部資源 區段下，選擇 Hypervisors。
2. 選擇 新增 Hypervisor。
3. 在 Hypervisor 設定 區段中，輸入 Hypervisor 名稱。
4. 針對 vCenter Server 主機，使用下拉式選單選取 IP 地址 或 FQDN (完整網域名稱)。輸入對應的值。

5. 若 AWS Backup 要允許探索 Hypervisor 上的虛擬機器，請輸入 Hypervisor 的使用者名稱和密碼。
6. 加密您的密碼。您可以使用下拉式選單選取特定服務受管 KMS 金鑰或客戶自管 KMS 金鑰來指定此加密，或選擇 建立 KMS 金鑰。如果您未選取特定金鑰，則 AWS Backup 會使用服務擁有的金鑰來加密您的密碼。
7. 在 連線閘道 區段中，使用下拉式清單來指定要連線至 Hypervisor 的閘道。
8. 選擇 測試閘道連線 以確認您先前的輸入。
9. (選擇性) 在 Hypervisor 標籤 區段中，您可以選擇 新增標籤，將標籤指派給 Hypervisor。
10. 選用的 VMware 標籤對應：您最多可以新增 10 個目前在虛擬機器上使用的 VMware 標籤來產生標 AWS 籤。
11. 在日誌群組設定面板中，您可以選擇與 Amazon CloudWatch Logs 整合以維護虛擬機器管理程序的日誌 (標準CloudWatch 日誌定價將根據使用情況適用)。每個 Hypervisor 只能屬於一個日誌群組。

    a. 如果您尚未建立日誌群組，請選取 建立新的日誌群組 選項按鈕。您正在編輯的 Hypervisor 將與此日誌群組建立關聯。

    b. 如果您先前已為不同的 Hypervisor 建立日誌群組，則可以針對此 Hypervisor 使用該日誌群組。選取 使用現有的日誌群組。

    c. 如果您不想要 CloudWatch 記錄，請選取 [停用記錄]。
12. 選擇 新增 Hypervisor，這會帶您前往其詳細資訊頁面。

> **Tip**
>
> 您可以使用 Amazon CloudWatch Logs (請參閱上述步驟 11) 取得有關虛擬機器管理程序的資訊，包括錯誤監控、閘道和虛擬機器管理程序之間的網路連線，以及網路組態資訊。如需 CloudWatch 日誌群組的相關資訊，請參閱 Amazon CloudWatch 使用者指南中的使用日誌群組和日誌串流。

檢視由 Hypervisor 管理的虛擬機器

若要檢視 Hypervisor 上的虛擬機器：

1. 在左側導覽窗格的 外部資源 區段下，選擇 Hypervisors。
2. 在 Hypervisors 區段中，依其 Hypervisor 名稱 選擇 Hypervisor 以前往其詳細資訊頁面。

3. 在 Hypervisor 摘要 下的區段中，選擇 虛擬機器 索引標籤。
4. 在 連線的虛擬機器 區段中，會自動填入虛擬機器清單。

檢視連線至 Hypervisor 的閘道

若要檢視連線至 Hypervisor 的閘道：

1. 選擇 閘道 索引標籤。
2. 在 連線的閘道 區段中，會自動填入閘道清單。

將 Hypervisor 連線至其他閘道

您的備份和還原速度可能會受到閘道與 Hypervisor 之間連線的頻寬限制。您可以將一或多個額外的閘道連線至 Hypervisor 來提高速度。您可以在 連線的閘道 區段中執行這項操作，如下所示：

1. 選擇連線。
2. 使用下拉式選單選取其他閘道。或者，選擇 建立閘道 以建立新的閘道。
3. 選擇連線。

編輯 Hypervisor 組態

如果您未使用 測試閘道連線 功能，您可能會新增使用者名稱或密碼不正確的 Hypervisor。在此情況下，Hypervisor 的連線狀態一律為 `Pending`。或者，您也可以輪換使用者名稱或密碼來存取 Hypervisor。請使用下列程序來更新這項資訊：

若要編輯已新增的 Hypervisor：

1. 在左側導覽窗格的 外部資源 區段下，選擇 Hypervisors。
2. 在 Hypervisors 區段中，依其 Hypervisor 名稱 選擇 Hypervisor 以前往其詳細資訊頁面。
3. 選擇編輯。
4. 頂部面板的名稱為 Hypervisor 設定。
    a. 在 vCenter Server 主機 下，您也可以編輯 FQDN (完整網域名稱) 或 IP 地址。
    b. 選擇性地輸入 Hypervisor 的 使用者名稱 和 密碼。
5. 在日誌群組設定面板中，您可以選擇與 Amazon 整合 CloudWatch以維護 Hypervisor 的日誌 (標準定CloudWatch 價將根據使用情況適用)。每個 Hypervisor 只能屬於一個日誌群組。

a. 如果您尚未建立日誌群組，請選取 建立新的日誌群組 選項按鈕。您正在編輯的 Hypervisor 將與此日誌群組建立關聯。

b. 如果您先前已為不同的 Hypervisor 建立日誌群組，則可以針對此 Hypervisor 使用該日誌群組。選取 使用現有的日誌群組。

c. 如果您不想要 CloudWatch 記錄，請選取 [停用記錄]。

> **Tip**
>
> 您可以使用 Amazon CloudWatch Logs (請參閱上述步驟 5) 取得有關虛擬機器管理程序的資訊，包括錯誤監控、閘道和 Hypervisor 之間的網路連線，以及網路組態資訊。如需 CloudWatch 日誌群組的相關資訊，請參閱 Amazon CloudWatch 使用者指南中的使用日誌群組和日誌串流。

若要以程式設計方式更新虛擬化管理程序，請使用 CLI 命令更新虛擬機管理程序和 API 呼叫。UpdateHypervisor

刪除 Hypervisor 組態

如果您需要移除已新增的 Hypervisor，請移除 Hypervisor 組態並新增另一個 Hypervisor。此移除操作適用於連線至 Hypervisor 的組態，不會刪除 Hypervisor。

若要刪除連線至已新增 Hypervisor 的組態：

1. 在左側導覽窗格的 外部資源 區段下，選擇 Hypervisors。
2. 在 Hypervisors 區段中，依其 Hypervisor 名稱 選擇 Hypervisor 以前往其詳細資訊頁面。
3. 選擇 移除，然後選擇 移除 Hypervisor。
4. 選擇性：使用《新增 Hypervisor》的程序取代已移除的 Hypervisor 組態。

了解 Hypervisor 狀態

以下描述每個可能的 Hypevisor 狀態，以及修補步驟 (如果適用)。`ONLINE` 狀態是 Hypervisor 的正常狀態。Hypervisor 在備份和復原由 Hypervisor 管理的 VM 時，應該始終或大部分時間具有此狀態。

Hypervisor 狀態

Status	意義和修補
ONLINE	您已將 Hypervisor 新增至閘道 AWS Backup，並與其建立關聯，並且可以透過網路與該閘道連線，以執行由 Hypervisor 管理的虛擬機器的備份和復原。 您可以隨時對這些虛擬機器執行隨需和排程備份。
PENDING	您已新增虛擬化管理程序 AWS Backup ，但是： • 未與任何閘道建立關聯，或 • 與一或多個閘道建立關聯，但所有這些閘道都已遭到刪除或不在作用中。 若要將 Hypervisor 狀態從 PENDING 變更為 ONLINE，請建立閘道並將您的 Hypervisor 連線至該閘道。
OFFLINE	您已新增 Hypervisor AWS Backup 並將其與閘道相關聯，但閘道無法透過您的網路連線到 Hypervisor。 若要將 Hypervisor 狀態從 OFFLINE 變更為 ONLINE，請確認您的網路組態是否正確。 如果問題持續發生，請確認您 Hypervisor 的 IP 地址或完整網域名稱是否正確。如果不正確，請使用正確的資訊再次新增您的 Hypervisor，並測試閘道連線。
ERROR	您已將 Hypervisor 新增至閘道 AWS Backup 並將其與閘道相關聯，但閘道無法與 Hypervisor 進行通訊。

Status	意義和修補
	若要將 Hypervisor 狀態從 ERROR 變更為 ONLINE，請確認 Hypervisor 的使用者名稱和密碼是否正確。如果不正確，請編輯您的 Hypervisor 組態。

後續步驟

若要備份 Hypervisor 上的虛擬機器，請參閱《備份虛擬機器》。

備份虛擬機器

新增 Hypervisor 之後，Backup 閘道會自動列出您的虛擬機器。您可以在左側導覽窗格中選擇 Hypervisors 或 虛擬機器 來檢視虛擬機器。

- 選擇 Hypervisors 僅檢視由特定 Hypervisor 管理的虛擬機器。透過此檢視，您一次只能使用一個虛擬機器。
- 選擇虛擬機器以檢視您新增至您的所有 Hypervisor 中的所有虛擬機器。 AWS 帳戶透過此檢視，您可以使用多個 Hypervisor 中的部分或所有虛擬機器。

無論您選擇哪種檢視，若要在特定虛擬機器上執行備份操作，請選擇該虛擬機器的 VM 名稱以開啟其詳細資訊頁面。VM 詳細資訊頁面是下列程序的起點。

建立虛擬機器的隨需備份

隨需備份是您手動起始的一次性完整備份。您可以使用隨選備份來測試 AWS Backup的備份和還原功能。

若要建立虛擬機器的隨需備份：

1. 選擇 Create on-demand backup (建立隨需備份)。
2. 設定您的隨需備份。
3. 選擇 Create on-demand backup (建立隨需備份)。
4. 檢查您的備份任務何時具有 Completed 狀態。在左側導覽選單中，選擇 任務。
5. 選擇 備份任務 ID 以檢視備份任務資訊，例如 備份大小 以及 建立日期 到 完成日期 之間經過的時間。

增量 VM 備份

新版 VMware 包含一項稱為 已變更區塊追蹤 的功能，可追蹤虛擬機器的儲存區塊在一段時間內的變化。當您使 AWS Backup 用備份虛擬機器時，會 AWS Backup 嘗試使用 CBT 資料 (如果有的話)。AWS Backup 使用 CBT 資料來加速備份程序；如果沒有 CBT 資料，備份工作通常會變慢，而且會使用更多的 Hypervisor 資源。即使 CBT 資料無效或無法使用，備份仍然可以順利完成。例如，如果虛擬機器或 ESXi 主機發生硬關機，CBT 資料可能無效或可能無法使用。

在 CBT 資料無效或無法使用的情況下，備份狀態會是 `Successful` 並顯示訊息。在這些情況下，訊息會指出，在沒有 CBT 資料的情況下，會 AWS Backup 使用自己專屬的變更偵測機制來完成備份，而非 VMware 的 CBT 資料。後續備份將重新嘗試使用 CBT 資料，而且在大多數情況下，CBT 資料會順利變成有效且可供使用。如果問題持續存在，請參閱《VMware 故障診斷》以取得修正步驟。

若要讓 CBT 正常運作，必須滿足以下條件：

- 主機必須是 ESXi 4.0 或更新版本
- 擁有磁碟的 VM 必須具有硬體版本 7 或更新版本
- 必須為虛擬機器啟用 CBT (預設為啟用)

若要確認虛擬磁碟是否已啟用 CBT：

1. 開啟 vSphere Client，然後選取已關機的虛擬機器。
2. 以滑鼠右鍵按一下虛擬機器，然後導覽至 **編輯設定** > **選項** > **進階/一般** > **組態參數**。
3. 選項 `ctkEnabled` 必須為 `True`。

將資源指派給備份計畫來自動執行虛擬機器備份

備份計畫是使用者定義的資料保護政策，可自動化許多 AWS 服務與第三方應用程式間的資料保護。首先，您可以透過指定備份計畫的備份頻率、保留期、生命週期政策和許多其他選項來建立備份計畫。若要建立備份計畫，請參閱《入門教學課程》。

建立備份計劃後，您可以將 AWS Backup支援的資源 (包括虛擬機器) 指派給該備份計劃。 AWS Backup 提供多種指定資源的方法，包括指定帳戶中的所有資源 (包括或排除單一特定資源)，或新增具有特定標籤的資源。

除了現有的資源指派功能之外，對虛擬機器的 AWS Backup 支援還引入了數項新功能，可協助您快速將虛擬機器指派給備份計劃。從 **虛擬機器** 頁面，您可以將標籤指派給多個虛擬機器，或使用新的 **將資源指派給計畫** 功能。使用這些功能可指派 AWS Backup 閘道已探索到的虛擬機器。

如果您預期未來會探索和指派其他虛擬機器，並想要自動化資源指派步驟以包含這些未來的虛擬機器，請使用新的 建立群組指派 功能。

VMware 標籤

標籤是可用於管理、篩選和搜尋資源的鍵值對。

VMware 標籤是由類別和標籤名稱所組成。VMware 標籤可用於分組虛擬機器。標籤 (Tag) 名稱是指派給虛擬機器的標籤 (Label)。類別是標籤名稱的集合。

在 AWS 標籤中，您可以在 UTF-8 字母、數字、空格和特殊字元之間使用字元+ - = . _ : /。

如果您在虛擬機器上使用標籤，您最多可以在 AWS Backup 中新增 10 個比對標籤，以協助組織。您最多可以將 10 個 VMware 標籤對應至 AWS 標籤。在AWS Backup 主控台中，您可以在 [我的組織] > [虛擬機器] > [標籤] 或 [VMware AWS 標籤] 中找到。

VMware 標籤映射

如果您在虛擬機器上使用標籤，您最多可以在 AWS Backup 中新增 10 個比對標籤，以更清楚呈現和組織。這些映射會套用至 Hypervisor 上的任何虛擬機器。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在主控台中，前往 編輯 Hypervisor (依序按一下 外部資源、Hypervisor、Hypervisor 名稱和 管理映射)。
3. 最後一個窗格 (VMware 標籤對應) 包含四個文字方塊欄位，您可以在其中輸入現有的 VMware 標籤資訊至對應的標 AWS 籤。這四個欄位分別是 VMware 標籤類別、VMware 標籤名稱、AWS 標籤鍵和AWS 標籤值 (例如：類別 = 作業系統；標籤名稱 = 視窗； AWS 標籤鍵 = 作業系統視窗，AWS 標籤值 = 視窗)。
4. 輸入偏好的值之後，請按一下 新增映射。如果出現錯誤，您可以按一下 移除 刪除輸入的資訊。
5. 新增映射之後，請指定要用來將這些 AWS 標籤套用至 VMware 虛擬機器的 IAM 角色。

   政策 AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync 包含必要許可。您可以將此政策連接至目前使用的角色 (或讓管理員進行連接)，也可以為所使用的角色建立自訂政策。
6. 最後，按一下 新增 Hypervisor 或 儲存。

您應該修改 IAM 角色信任關係，以新增 backup-gateway.amazonaws.com 和 backup.amazonaws.com 服務。如果沒有此服務，在映射標籤時可能會發生錯誤。若要編輯現有角色的信任關係，

1. 登入 IAM 主控台。
2. 在主控台的導覽窗格中，選擇 角色。
3. 選擇您要修改的角色名稱，然後在詳細資訊頁面上選取 信任關係 索引標籤。
4. 在 政策文件 下，貼上以下內容：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "backup.amazonaws.com",
          "backup-gateway.amazonaws.com"
        ]
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

5. 選擇 Update Trust Policy (更新信任政策)。

如需詳細資訊，請參閱《AWS Directory Service 管理指南》中的《編輯現有角色的信任關係》。

檢視 VMware 標籤映射

在 AWS Backup 控制台中，依序按一下 外部資源、Hypervisor 和 Hypervisor 名稱連結，以檢視所選 Hypervisor 的屬性。在摘要窗格下有四個索引標籤，最後一個索引標籤是 VMware 標籤映射。請注意，如果您還沒有映射，則會顯示「沒有 VMware 標籤映射」 。

從這裡，您可以同步 Hypervisor 發現的虛擬機器的中繼資料，您可以將對應複製到您的 Hypervisor，也可以將對應至 VMware AWS 標籤的標記新增至備份計劃的備份選擇，或管理對應。

在主控台中，若要查看哪些標籤套用至選取的虛擬機器，請依序按一下 虛擬機器 和虛擬機器名稱，然後按一下 AWS 標籤 或 VMware 標籤。您可以檢視與此虛擬機器相關聯的標籤；此外，您還可以管理標籤。

使用 VMware 標籤映射將虛擬機器指派給計畫

若要使用映射標籤將虛擬機器指派給備份計畫，請執行下列動作：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在主控台中，前往 Hypervisor 詳細資訊頁面上的 VMware 標籤映射 (依序按一下 外部資源、Hypervisor 和 Hypervisor 名稱)。
3. 選取多個映射標籤旁的核取方塊，將這些標籤指派給同一個備份計畫。
4. 按一下 新增至資源指派。
5. 從下拉式清單中選擇現有的備份計畫。或者，您也可以選擇 建立備份計畫，建立新的備份計畫。
6. 按一下 確認。這會開啟 指派資源 頁面，其中包含已預先填入值的 使用標籤縮小選取範圍 欄位。

VMware 標籤使用 AWS CLI

AWS Backup 使用 API 呼叫PutHypervisorPropertyMappings將內部部署中的虛擬機器管理程序實體屬性對應至中的屬性。 AWS

在中 AWS CLI，使用下列作業put-hypervisor-property-mappings：

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:region:account:hypervisor/hypervisorId \
--vmware-to-aws-tag-mappings list of VMware to AWS tag mappings \
--iam-role-arn arn:aws:iam::account:role/roleName \
--region AWSRegion
--endpoint-url URL
```

請見此處範例：

```
aws backup-gateway put-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--vmware-to-aws-tag-mappings VmwareCategory=OS,VmwareTagName=Windows,AwsTagKey=OS-
Windows,AwsTagValue=Windows \
--iam-role-arn arn:aws:iam::123456789012:role/SyncRole \
--region us-east-1
```

您也可以使用 GetHypervisorPropertyMappings 來協助取得屬性映射資訊。在中 AWS CLI，使用作業get-hypervisor-property-mappings。以下是範例範本：

```
aws backup-gateway get-hypervisor-property-mappings --hypervisor-arn HypervisorARN
--region AWSRegion
```

請見此處範例：

```
aws backup-gateway get-hypervisor-property-mappings \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

在 AWS 使用 API、CLI 或 SDK 時同步虛擬機器探索到的虛擬機器的中繼資料

您可以同步虛擬機器的中繼資料。當您執行這項操作時，也會同步虛擬機器上屬於映射一部分的 VMware 標籤。此外，映射至虛擬機器上 VMware 標籤的 AWS 標籤也會套用至 AWS 虛擬機器資源。

AWS Backup 使用 API 呼叫StartVirtualMachinesMetadataSync來同步 Hypervisor 探索到之虛擬機器的中繼資料。若要使用 AWS CLI來同步 Hypervisor 探索到的虛擬機器中繼資料，請使用操作 `start-virtual-machines-metadata-sync`。

範例範本：

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

範例：

```
aws backup-gateway start-virtual-machines-metadata-sync \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

您也可以使用 GetHypervisor 來協助取得 Hypervisor 資訊 (例如主機、狀態、最新中繼資料同步狀態)，以及擷取上次成功的中繼資料同步時間。在中 AWS CLI，使用作業`get-hypervisor`。

範例範本：

```
aws backup-gateway get-hypervisor \
--hypervisor-arn Hypervisor ARN
--region AWSRegion
```

範例：

```
aws backup-gateway get-hypervisor \
--hypervisor-arn arn:aws:backup-gateway:us-east-1:123456789012:hypervisor/hype-12345 \
--region us-east-1
```

如需詳細資訊，請參閱 API 文件VmwareTag和 VmwareToAwsTagMapping.

此功能將在 2022 年 12 月 15 日之後部署的新閘道上提供。對於現有閘道，這項新功能將在 2023 年 1 月 30 日或之前透過自動軟體更新提供。若要手動將閘道更新為最新版本，請使用 AWS CLI 指令 UpdateGatewaySoftwareNow。

範例：

```
aws backup-gateway update-gateway-software-now \
--gateway-arn arn:aws:backup-gateway:us-east-1:123456789012:gateway/bgw-12345 \
--region us-east-1
```

使用標籤指派虛擬機器

您可以將目前探索的虛擬機器以及其他 AWS Backup 資源指派一個已指派給現有備份計劃的標籤，方法是為虛擬機器指派給這些虛擬機器。 AWS Backup您也可以建立新的備份計畫和新的以標籤為基礎的資源指派。備份計畫會在每次執行備份任務時檢查新指派的資源。

若要使用相同標籤標記多個虛擬機器：

1. 在左側導覽窗格中，選擇 虛擬機器。
2. 選取 VM 名稱 旁的核取方塊以選擇您所有的虛擬機器。或者，選取您要標記之 VM 名稱旁的核取方塊。
3. 選擇 Add tags (新增標籤)。
4. 輸入標籤鍵。
5. 建議：輸入標籤值。
6. 選擇確認。

使用「將資源指派給計畫」功能指派虛擬機器

您可以使用 [將資源指派給規劃] 功能，將目前探索 AWS Backup 到的虛擬機器指派給現有或新的備份計劃。

若要使用「將資源指派給計畫」功能指派虛擬機器：

1. 在左側導覽窗格中，選擇 虛擬機器。
2. 選取 VM 名稱 旁的核取方塊以選擇您所有的虛擬機器。或者，選取多個 VM 名稱旁的核取方塊以將其指派給同一個備份計畫。
3. 選擇 指派，然後選擇 將資源指派給計畫。

4. 輸入 資源指派名稱。
5. 選擇資源指派 IAM 角色以建立備份和管理復原點。如果您沒有要使用的特定 IAM 角色，建議您使用具有正確許可的預設角色。
6. 在 備份計畫 區段中，從下拉式清單中選擇現有的備份計畫。或者，選擇 建立備份計畫 以建立新的備份計畫。
7. 選擇 指派資源。
8. 選擇性：選擇 檢視備份計畫，確認將您的虛擬機器指派給備份計畫。然後，在 資源指派 區段中，選擇資源指派名稱。

使用「建立群組指派」功能指派虛擬機器

與前兩個虛擬機器的資源指派功能不同，「建立群組指派」功能不僅會指派目前探索到的虛擬機器 AWS Backup，還可以指派 future 在您定義的資料夾或 Hypervisor 中探索到的虛擬機器。

此外，您不需要選取任何核取方塊，就能使用 建立群組指派 功能。

若要使用「將資源指派給計畫」功能指派虛擬機器：

1. 在左側導覽窗格中，選擇 虛擬機器。
2. 選擇 指派，然後選擇 建立群組指派。
3. 輸入 資源指派名稱。
4. 選擇資源指派 IAM 角色以建立備份和管理復原點。如果您沒有要使用的特定 IAM 角色，建議您使用具有正確許可的預設角色。
5. 在 資源群組 區段中，選取 群組類型 下拉式選單。您的選項包括 資料夾 或 Hypervisor。

    a. 選擇 資料夾 以指派 Hypervisor 上資料夾中的所有虛擬機器。使用下拉式選單選取資料夾群組名稱，例如 `datacenter/vm`。您也可以選擇包含子資料夾。

    > **Note**
    >
    > 若要進行以資料夾為基礎的指派，請在探查程序期間，使用在探索程序期間找到虛擬機器的資料夾 AWS Backup 標記虛擬機器。如果您稍後將虛擬機器移至其他資料夾，則由於標 AWS 記最佳做 AWS Backup 法，因此無法為您更新標籤。此指派方法可能會導致繼續備份您從指派資料夾中移出的虛擬機器。

    b. 選擇 Hypervisor 以指派由 Hypervisor 管理的所有虛擬機器。使用下拉式選單選取 Hypervisor ID 群組名稱。

6. 在 備份計畫 區段中，從下拉式清單中選擇現有的備份計畫。或者，選擇 建立備份計畫 以建立新的備份計畫。
7. 選擇 建立群組指派。
8. 選擇性：選擇 檢視備份計畫，確認將您的虛擬機器指派給備份計畫。在 資源指派 區段中，選擇資源指派名稱。

後續步驟

若要還原虛擬機器，請參閱《還原虛擬機器》。

Backup 閘道的第三方來源元件相關資訊

在本節中，您可以找到我們賴以提供 Backup 閘道功能的第三方工具和授權相關資訊。

下列位置提供 Backup 閘道軟體隨附之特定第三方來源軟體元件的原始碼，以供下載：

- 對於部署在 VMware ESXi 上的閘道，請下載 sources.tgz。

本產品包含由 OpenSSL 專案開發的軟體，可用於 OpenSSL 工具組 (https://www.openssl.org/)。

此產品包含 VMware® vSphere 軟體開發套件所開發的軟體 (https://www.vmware.com)。

如需所有相依第三方工具的相關授權，請參閱《第三方授權》。

AWS 設備的開放原始碼元件

我們使用多項第三方工具和授權來提供 Backup 閘道的功能。

使用下列連結下載應用 AWS 裝置軟體隨附之特定開放原始碼軟體元件的原始碼：

- 對於部署在 VMware ESXi 上的閘道，請下載 sources.tar

本產品包含由 OpenSSL 專案開發的軟體，可用於 OpenSSL 工具組 (https://www.openssl.org/)。如需所有相依第三方工具的相關授權，請參閱《第三方授權》。

針對 VM 問題進行故障診斷

增量備份/CBT 問題和訊息

失敗訊息：**"The VMware Change Block Tracking (CBT) data was invalid during this backup, but the incremental backup was successfully completed with our proprietary change detection mechanism."**

如果此訊息持續出現，請依照 VMware 的指示重設 CBT。

訊息指出 CBT 未開啟或無法使用：「此虛擬機器無法使用 VMware 變更區塊追蹤 (CBT)，但已透過我們專屬的變更機制順利完成增量備份。」

確認已開啟 CBT。若要確認虛擬磁碟是否已啟用 CBT：

1. 開啟 vSphere Client，然後選取已關機的虛擬機器。
2. 以滑鼠右鍵按一下虛擬機器，然後導覽至 **編輯設定** > **選項** > **進階/一般** > **組態參數**。
3. 選項 `ctkEnabled` 必須為 `True`。

如果已開啟，請確定您使用的是 up-to-date VMware 功能。主機必須是 ESXi 4.0 或更新版本，而且擁有要追蹤之磁碟的虛擬機器必須是硬體版本 7 或更新版本。

如果 CBT 已開啟 (已啟用) 且軟體和硬體為最新狀態，請關閉虛擬機器，然後再重新開啟。確認已開啟 CBT。然後，再次執行備份。

進階 DynamoDB 備份

AWS Backup 支援其他進階功能，以滿足您的 Amazon DynamoDB 資料保護需求。在中啟用 AWS Backup進階功能之後 AWS 區域，您可以為您建立的 DynamoDB 表格備份的所有新功能解除鎖定下列功能：

- 節省成本和成本優化：
  - 將備份分層至冷儲存以降低儲存成本
  - 與 Cost Explorer 搭配使用的成本分配標記
- 業務持續性：
  - 跨區域複製
  - 跨帳戶複製
- 安全性：

- 將備份儲存在加密的 AWS Backup 保存庫中，以便使用 AWS Backup Vault Lock 、AWS Backup 政策和加密金鑰進行保護。
- 備份會從其來源 DynamoDB 資料表繼承標籤，以便您使用這些標籤來設定許可和服務控制政策 (SCP)。

在 2021 年 11 月 AWS Backup 之後上線的新客戶預設會啟用進階 DynamoDB 備份功能。具體而言，預設會為 2021 年 11 月 21 日之前尚未建立備份保存庫的客戶啟用進階 DynamoDB 備份功能。

我們建議所有現有 AWS Backup 客戶啟用 DynamoDB 的進階功能。啟用進階功能後，暖備份儲存定價將不會出現變動。您可以將備份分層至冷儲存，並使用成本分配標籤將成本優化，以節省成本。您也可以開始利用業務連續性和安全性功能。 AWS Backup

> **Note**
>
> 如果您使用自訂角色或原則而非預設服務角色，則必須在自訂角色中新增或使用下列權限原則 (或新增其對等權限)： AWS Backup
>
> - `AWSBackupServiceRolePolicyForBackup`，以執行進階 DynamoDB 備份。
> - `AWSBackupServiceRolePolicyForRestores`，以還原進階 DynamoDB 備份。
>
> 若要深入瞭解 AWS受管政策並檢視客戶管理政策的範例，請參閱。受管理的政策 AWS Backup

主題

使用主控台啟用進階 DynamoDB 備份

您可以使用 AWS Backup 或 DynamoDB 主控台為 DynamoDB 備份啟用 AWS Backup 進階功能。

若要從主控台啟用進階 DynamoDB 備份功能： AWS Backup

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽選單中，選擇 設定。
3. 在 支援的服務 區段下，確認 DynamoDB 為 已啟用。

   如果不是，請選擇 選擇加入 並啟用 DynamoDB 作為 AWS Backup 支援的服務。
4. 在 DynamoDB 備份的進階功能 區段下，選擇 啟用。
5. 選擇 Enable features (啟用功能)。

如需如何使用 DynamoDB 主控台啟用 AWS Backup 進階功能，請參閱 Amazon Dynam oDB 使用者指南中的啟用 AWS Backup 功能。

以程式設計方式啟用進階 DynamoDB 備份

您也可以使用 AWS Command Line Interface (CLI) 為 DynamoDB 備份啟用 AWS Backup 進階功能。當您將下列兩個值設定為 `true` 時，即可啟用進階 DynamoDB 備份：

若要以程式設計方式啟用 DynamoDB 備份的 AWS Backup 進階功能：

1. 檢查您是否已使用下列命令啟用 DynamoDB 的 AWS Backup 進階功能：

   ```
   $ aws backup describe-region-settings
   ```

   如果 `"ResourceTypeManagementPreference"` 和 `"ResourceTypeOptInPreference"` 下都是 `"DynamoDB":true`，則表示您已啟用進階 DynamoDB 備份。

   如果類似下列輸出，您至少有一個 `"DynamoDB":false` 執行個體尚未啟用進階 DynamoDB 備份，請繼續進行下一個步驟。

   ```
   {
     "ResourceTypeManagementPreference":{
       "DynamoDB":false,
       "EFS":true
     }
     "ResourceTypeOptInPreference":{
       "Aurora":true,
       "DocumentDB":false,
       "DynamoDB":false,
   ```

```
    "EBS":true,
    "EC2":true,
    "EFS":true,
    "FSx":true,
    "Neptune":false,
    "RDS":true,
    "Storage Gateway":true
  }
}
```

2. 使用下列 UpdateRegionSettings 操作，將 "ResourceTypeManagementPreference" 和 "ResourceTypeOptInPreference" 都設定為 "DynamoDB":true：

```
aws backup update-region-settings \
              --resource-type-opt-in-preference DynamoDB=true \
              --resource-type-management-preference DynamoDB=true
```

編輯進階 DynamoDB 備份

當您在啟用 AWS Backup 進階功能之後建立 DynamoDB 備份時，您可以使用 AWS Backup ：

- 跨區域複製備份
- 跨帳戶複製備份
- 變更將備份 AWS Backup 分層至冷儲存的時間
- 標記備份

若要在現有備份上使用這些進階功能，請參閱《編輯備份》。

如果您稍後停用 DynamoDB 的 AWS Backup 進階功能，您可以繼續對您在啟用進階功能期間建立的 DynamoDB 備份執行這些操作。

還原進階 DynamoDB 備份

您可以使用還原啟用 AWS Backup 進階功能的 DynamoDB 備份，方法與還原啟用進階功能之前所採用的 DynamoDB 備份相同。 AWS Backup 您可以使用 AWS Backup 或 DynamoDB 執行還原作業。

您可以使用下列選項指定如何加密新還原的資料表：

- 當您在與原始資料表相同的區域中進行還原時，您可以選擇性地為還原的資料表指定加密金鑰。如果您沒有指定加密金鑰，則 AWS Backup 會使用加密原始表格的相同金鑰，自動加密還原的資料表。

- 當您在與原始資料表不同的區域中進行還原時，您必須指定加密金鑰。

若要使用還原 AWS Backup，請參閱還原 Amazon DynamoDB 資料表。

若要使用 DynamoDB 進行還原，請參閱《Amazon DynamoDB 使用者指南》中的從備份中還原 DynamoDB 資料表。

刪除進階 DynamoDB 備份

您無法刪除使用 DynamoDB 中這些進階功能建立的備份。您必須使用 AWS Backup 來刪除備份，以維護整個 AWS 環境的全域一致性。

若要刪除 DynamoDB 備份，請參閱《刪除備份》。

啟用進階 DynamoDB 備份時的其他完整 AWS Backup 管理好處

當您啟用 DynamoDB 的 AWS Backup 進階功能時，您可以對 DynamoDB 備份進行完整管理。 AWS Backup這樣做會提供您以下額外好處：

加密

AWS Backup 使用目的地 AWS Backup 保管庫的 KMS 金鑰自動加密備份。之前是使用與來源 DynamoDB 資料表相同的加密方法進行加密。這會增加可用於保護資料的防禦層數。如需詳細資訊，請參閱中備份的加密 AWS Backup。

Amazon Resource Name (ARN)

每個備份 ARN 的服務命名空間都是 awsbackup。之前，服務命名空間為 dynamodb。換句話說，每個 ARN 的字首將從 arn:aws:dynamodb 變更為 arn:aws:backup。請參閱《服務授權參考》中的AWS Backup的 ARN。

有了這項變更，您或您的備份管理員就可以使用 awsbackup 服務命名空間建立備份的存取政策 (現在會套用至啟用進階功能之後建立的 DynamoDB 備份)。透過使用 awsbackup 服務命名空間，您也可以將政策套用至 AWS Backup所進行的其他備份。如需詳細資訊，請參閱存取控制。

帳單上的費用位置

Backup 費用（包括儲存、資料傳輸、還原和提前刪除）會顯示在 AWS 帳單中的「備份」下方。之前，費用會顯示在帳單中的 “DynamoDB” 下方。

這項變更可確保您可以使用 AWS Backup 帳單來集中監控備份成本。如需詳細資訊，請參閱計量、成本和帳單。

Amazon Timestream 備份

Amazon Timestream 是可擴展的時間序列資料庫，允許每天儲存和分析高達數兆個時間序列資料點。Timestream 已進行優化，依照您的政策將最新資料儲存在記憶體中，並將歷史資料儲存在成本優化儲存層中，進而節省成本和時間。

Timestream 資料庫具有資料表。這些資料表包含記錄，而且每個記錄都是時間序列中的單一資料點。時間序列是在一段時間間隔內記錄的一系列記錄，例如庫存價格、Amazon EC2 執行個體的記憶體使用量或溫度讀數。 AWS Backup 可以集中備份和還原時間流表。您可以將這些資料表備份複製到其他帳戶，以及同一組織 AWS 區域 內的其他多個帳戶。

Timestream 目前不提供原生備份和還原服務，因此使用 AWS Backup 建立 Timestream 表格的安全副本可以為您的資源增加額外的安全性和彈性層。

備份 Timestream 資料表

您可以透過 AWS Backup 主控台或使用 AWS CLI.

有兩種方式可使用 AWS Backup 主控台備份 Timestream 資料表：視需求或備份計畫的一部分進行備份。

建立隨需 Timestream 備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 使用導覽窗格選擇 受保護的資源，然後選擇 建立隨需備份。
3. 在 建立隨需備份 頁面上，選擇 Amazon Timestream。
4. 針對 資源類型 選擇 Timestream，然後選擇您要備份的資料表名稱。
5. 在「備份」視窗中，確認已選取 立即建立備份。這會立即起始備份，並且很快就能讓您在 受保護的資源 頁面上查看您的叢集。
6. 在 轉換至冷儲存 下拉式選單中，您可以設定轉換設定。
7. 在 保留期 中，您可以選擇保留備份的時間長度。
8. 選擇現有的備份保存庫或建立新的備份保存庫。選擇 Create new backup vault (建立新的備份文件庫) 開啟新頁面來建立文件庫，完成後將返回 Create on-demand backup (建立隨需備份) 頁面。
9. 在 [IAM 角色] 下，選擇 [預 AWS Backup 設角色] (如果您的帳戶中沒有預設角色，則會以正確的權限為您建立)。
10. 您也可以「選擇性地」將標籤新增至復原點。如果您要將一或多個標籤指派至您的隨需備份，請輸入 key (索引鍵) 和選用的 value (值)，然後選擇 Add tag (新增標籤)。

11. 選擇 Create on-demand backup (建立隨需備份)。您將會移到 Jobs (任務) 頁面，您會看到任務的清單。
12. 選擇叢集的 備份任務 ID，以查看該任務的詳細資訊。其中會顯示 `Completed`、`In Progress` 或 `Failed` 狀態。您可以按一下「重新整理」按鈕來更新顯示的狀態。

在備份計畫中建立排程 Timestream 備份

您的排程備份可以包含 Timestream 資料表 (如果這是受保護的資源)。若要選擇加入以保護 Amazon Timestream 資料表：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 使用導覽窗格選擇 受保護的資源。
3. 將 Amazon Timestream 切換為 開啟。
4. 請參閱將資源指派給主控台，以便在現有或新的計畫中包含 Timestream 資料表。

在 管理備份計畫 下，您可以選擇 建立備份計畫 並包含 Timestream 資料表，也可以選擇 更新現有的備份計畫 以包含 Timestream 資料表。新增 Timestream 資源類型時，您可以選擇新增所有 Timestream 資料表，或在 選取特定資源類型 下勾選要新增之資料表旁的方塊。

由 Timestream 資料表組成的第一個備份會是完整備份。後續備份會是增量備份。

建立或修改備份計畫之後，請導覽至左側導覽列中的「備份計畫」。您指定的備份計畫應該會在 資源指派 下顯示您的叢集。

以程式設計方式進行備份

您可以使用操作名稱 `start-backup-job`。包含以下參數：

```
aws backup start-backup-job \
--backup-vault-name backup-vault-name \
--resource-arn arn:aws:timestream:region:account:database/database-name/table/table-name \
--iam-role-arn arn:aws:iam::account:role/role-name \
--region AWS ## \
--endpoint-url URL
```

檢視 Timestream 資料表備份

若要在主控台中檢視和修改您的 Timestream 資料表備份：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 選擇 Backup vaults (備份文件庫)。然後，按一下包含 Timestream 資料表的備份保存庫名稱。
3. 備份保存庫會隨即顯示摘要和備份清單。

    a. 您可以按一下 復原點 ID 欄中的連結，或者

    b. 您可以勾選復原點 ID 左側的方塊，然後按一下 動作 刪除不再需要的復原點。

還原 Timestream 資料表

了解如何還原 Timestream 資料表

Amazon EC2 執行個體上的 SAP HANA 資料庫備份

> **Note**
>
> 如需何處提供 Amazon EC2 執行個體上 SAP HANA 之 AWS Backup 支援的資訊，請參閱《各 AWS 區域的功能可用性》。

AWS Backup 支援在 Amazon EC2 執行個體上備份和還原 SAP HANA 資料庫。

主題

- 概觀
- 必要條件
- AWS Backup 主控台中的 Backup 作業
- 檢視備份任務和復原點
- 使用 API 和 CLI 進行備份操作
- 故障診斷
- 詞彙表
- 版本備註

概觀

除了能夠建立備份和還原資料庫之外， AWS Backup 還與適用於 SAP 的 Amazon EC2 Systems Manager 整合，以便客戶識別和標記 SAP HANA 資料庫。

AWS Backup 與 AWS Backint Agent 整合，以執行 SAP HANA 備份和還原。如需詳細資訊，請參閱《AWS Backint》。

必要條件

您必須先完成幾個先決條件，才能執行備份和還原活動。請注意，您需要 SAP HANA 資料庫的管理存取權和許可，才能在 AWS 帳戶中建立新的 IAM 角色和政策，才能執行這些步驟。

請完成 Amazon EC2 Systems Manager 的這些先決條件。

1. 為執行 SAP HANA 資料庫的 Amazon EC2 執行個體設定必要許可
2. 在中註冊憑證 AWS Secrets Manager
3. 安裝管 AWS 理程式和 SAP AWS Systems Manager 代理程式
4. 驗證 SSM Agent
5. 驗證參數
6. 註冊 SAP HANA 資料庫

AWS Backup 主控台中的 Backup 作業

完成先決條件並設定適用於 SAP 的 SSM 之後，您就可以備份和還原 EC2 上的 SAP HANA 資料庫。

選擇加入以保護 SAP HANA 資源

為了 AWS Backup 保護您的 SAP HANA 資料庫，必須將 SAP HANA 切換為受保護的資源之一。若要選擇加入：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側的導覽窗格中，選擇設定。
3. 在 選擇加入服務 下，選取 設定資源。
4. 選擇加入 Amazon EC2 上的 SAP HANA。
5. 按一下 確認。

現在將會為 Amazon EC2 上的 SAP HANA 啟用「選擇加入服務」。

建立排程備份

您可以編輯現有的備份計畫並將 SAP HANA 資源新增至其中，也可以只為 SAP HANA 資源建立新的備份計畫。

如果您選擇建立新的備份計畫，您將有三個選項：

1. 選項 1：從範本開始

    1. 選擇備份計畫範本。
    2. 指定備份計畫名稱。
    3. 按一下 建立計畫。

2. 選項 2：建立新的計畫

    1. 指定備份計畫名稱。
    2. 選擇性地指定要新增至備份計畫的標籤。
    3. 指定備份規則組態。

        a. 指定備份規則名稱。

        b. 選取現有的保存庫或建立新的備份保存庫。這是備份的儲存位置。

        c. 指定備份頻率。

        d. 指定備份時段。

        請注意，目前不支援轉換至冷儲存。

        e. 指定保留期。

        目前不支援複製到目的地

        f. (選擇性) 指定要新增至復原點的標籤。

    4. 按一下 建立計畫。

3. 選項 3：使用 JSON 定義計畫

    1. 您可以透過修改現有備份計畫的 JSON 運算式或建立新的運算式，來指定用於備份計畫的 JSON。
    2. 指定備份計畫名稱。
    3. 按一下 驗證 JSON。

    成功建立備份計畫之後，您可以在下一個步驟中將資源指派給備份計畫。

無論您使用哪種計畫，都請務必指派資源。您可以選擇要指派的 SAP HANA 資料庫，包括系統和租戶資料庫。您也可以選擇排除特定資源 ID。

建立隨需備份

您可以建立完整的隨需備份，在建立後立即執行。請注意，Amazon EC2 執行個體上 SAP HANA 資料庫的隨需備份是完整備份；不支援增量備份。

現在建立您的隨需備份。一開始會備份您指定的資源。主控台會將您轉移至 備份任務 頁面，您可以在其中檢視任務進度。請記下畫面頂端藍色橫幅中的備份任務 ID，因為您將需要此 ID 才能輕鬆找到備份任務的狀態。備份完成後，其狀態會變成 Completed。備份最多可能需要數小時。

重新整理備份任務清單以查看狀態變更。您也可以搜尋並按一下 備份任務 ID 來檢視詳細的任務狀態。

SAP HANA 資料庫的連續備份

您可以建立可與 point-in-time 還原 (PITR) 搭配使用的連續備份 (請注意，隨選備份會保留資源的狀態，而 PITR 則使用連續備份來記錄一段時間內的變更)。

使用連續備份，您可以在 1 秒的精確度內倒回您選擇的特定時間來還原 EC2 執行個體上的 SAP HANA 資料庫 (最多可回到 35 天前)。連續備份的運作方式是先建立資源的完整備份，然後持續備份資源的交易日誌。PITR 還原的運作方式是存取您的完整備份，並在您指定要復原的時間重新顯示交易記錄檔。AWS Backup

當您 AWS Backup 使用 AWS Backup 主控台或 API 建立備份計劃時，您可以選擇加入連續備份。

使用主控台啟用連續備份

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 備份計畫，然後選擇 建立備份計畫。
3. 在 備份規則 下，選擇 新增備份規則。
4. 在 備份規則組態 區段中，選取 為支援的資源啟用連續備份。

停用 SAP HANA 資料庫備份的 PITR (point-in-time 還原) 之後，記錄將繼續傳送到， AWS Backup 直到復原點到期為止 (狀態等於EXPIRED)。您可以在 SAP HANA 中變更為替代日誌備份位置，以停止將日誌傳輸至 AWS Backup。

狀態為的連續復原點STOPPED表示連續復原點已中斷；也就是說，從 SAP HANA 傳輸到顯 AWS Backup 示資料庫增量變更的記錄有間隙。在此時間範圍內發生的復原點都會具有 STOPPED. 狀態。

如需在連續備份 (復原點) 的還原任務期間可能遇到的問題，請參閱本指南的《SAP HANA 還原故障診斷》一節。

檢視備份任務和復原點

檢視備份和還原任務的狀態：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Jobs (任務)。
3. 選擇備份任務、還原任務或複製任務，以查看您的任務清單。
4. 搜尋並按一下您的任務 ID 來檢視詳細的任務狀態。

檢視保存庫中的所有復原點：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 搜尋並按一下備份保存庫來檢視保存庫中的所有復原點。

檢視受保護資源的詳細資訊：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Protected resources (受保護的資源)。
3. 您也可以依資源類型進行篩選，以檢視該資源類型的所有備份。

使用 API 和 CLI 進行備份操作

Backup 主控台中的每個動作都有對應的 API 呼叫。

若要以程式設計方式設定 AWS Backup 和管理及其資源，請使用 API 呼叫`StartBackupJob`在 EC2 執行個體上備份 SAP HANA 資料庫。

使用 `start-backup-job` 作為 CLI 命令。

故障診斷

如果在嘗試進行備份操作時發生下列任何錯誤，請參閱相關的解決方法。

- 錯誤：`Encountered an issue with log backups, please check SAP HANA for details.`

解決方案：檢查 SAP HANA，確保記錄備份是 AWS Backup 從 SAP HANA 傳送至。

錯誤：`One or more log backup attempts failed for recovery point.`

解決方法：請檢查 SAP HANA 了解詳情。確保記錄檔備份是 AWS Backup 從 SAP HANA 傳送至。

錯誤：`Unable to determine the status of log backups for recovery point.`

解決方法：請檢查 SAP HANA 了解詳情。確保記錄檔備份是 AWS Backup 從 SAP HANA 傳送至。

錯誤：`Log backups for recovery point %s were interrupted due to a restore operation on the database.`

解決方法：等待還原任務完成。日誌備份應該會繼續進行。

錯誤：`b'* 447: backup could not be completed: [110507] Backint exited with exit code 1 instead of 0. console output: time=2022-08-12T11:03:18Z level=info msg=Starting execution. time=2022-08-12T11:03:18Z level=info msg=Configuration file not specified in argument, using default location time=2022-08-12T11:03:18Z level=info msg=Loading configuration file /opt/aws-backint-agent/aws-backint-agent-config.yaml time=2022-08-12T11:03:18Z level=error msg=Failed to read config file open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory time=2022-08-12T11:03:18Z level=error msg=Error reading config file open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory. time=2022-08-12T11:03:18Z level=fatal msg=Error occurred during configuration. open /opt/aws-backint-agent/aws-backint-agent-config.yaml: no such file or directory. , [110203] Not all data could be written: Expected 4096 but transferred 0 SQLSTATE: HY000\n'`

解決方案：很可能 BackInt 安裝未成功完成。重試在 SAP 應用程式伺服器上安裝 AWS Backint Agent 理程式和 Amazon EC2 系統管理器代理程式的程序。

- 錯誤：`Database cannot be backed up while it is stopped`。

  解決方法：確定要備份的資料庫處於作用中狀態。只有當資料庫在線上時，才能備份資料庫資料和日誌。

- 錯誤：`Getting backup metadata failed. Check the SSM document execution for more details.`

解決方法：確定要備份的資料庫處於作用中狀態。只有當資料庫在線上時，才能備份資料庫資料和日誌。

詞彙表

資料備份類型：SAP HANA 支援兩種類型的資料備份：完整和 INC (增量)。 AWS Backup 會優化每次備份操作期間使用的類型。

目錄備份：SAP HANA 會維護自己的清單檔案，稱為「目錄」。 AWS Backup 會與此目錄互動。每個新備份都會在目錄中建立一個項目。

連續日誌備份 (交易日誌)：SAP HANA 會追蹤自最近一次備份以來的所有交易，以便執行時間點復原 (PITR) 功能。

系統複製：一種還原任務，其中還原目標資料庫與建立復原點的來源資料庫不同。

破壞性還原：破壞性還原是一種還原任務類型，還原的資料庫會在此期間刪除或覆寫來源或現有資料庫。

完整：完整備份是完整資料庫的備份。

INC：增量備份是自上次備份以來對 SAP HANA 資料庫所做之所有變更的備份。

如需其他詳細資訊，請參閱《AWS 詞彙表》。

版本備註

目前不支援特定功能：

- 目前不支援跨區域和跨帳戶複製。
- 目前不支援 Backup Audit Manager 和報告。
- 目前不支援以下區域：亞太區域 (雅加達)、(美國西部)、 AWS GovCloud (美國東部)、中國 AWS GovCloud (北京)、中國 (寧夏)、歐洲 (西班牙)、歐洲 (蘇黎世)、亞太區域 (海德拉巴) 和亞太區域 (墨爾本)。

Amazon Redshift 備份

Amazon Redshift 是全受管、可擴展的雲端資料倉儲，利用快速、簡單且安全的分析讓您更快獲得洞察。您可 AWS Backup 以使用不可變的備份、個別的存取原則，以及集中式組織管理備份和還原工作來保護資料倉儲。

Amazon Redshift 資料倉儲是稱為節點的運算資源集合，這些資源被組織成一個稱為叢集的群組。AWS Backup 可以備份這些叢集。

如需 Amazon Redshift 的資訊，請參閱《Amazon Redshift 入門指南》、《Amazon Redshift 資料庫開發人員指南》和《Amazon Redshift 叢集管理指南》。

備份 Amazon Redshift 佈建叢集

您可以使用主控台或以程式設計方式使用 API 或 AWS Backup CLI 來保護您的 Amazon Redshift 叢集。這些叢集可以作為備份計畫的一部分按照定期排程進行備份，也可以視需要透過隨需備份進行備份。

您可以還原單一資料表 (也稱為項目層級還原) 或整個叢集。請注意，資料表不會自行備份，而是會在備份叢集時，作為叢集的一部分進行備份。

使用可 AWS Backup 讓您以集中的方式檢視資源；不過，如果 Amazon Redshift 是您唯一使用的資源，您可以繼續在 Amazon Redshift 中使用自動化快照排程器。請注意，如果您選擇透 AWS Backup 過管理這些設定，則無法繼續使用 Amazon Redshift 來管理手動快照設定。

您可 Amazon Redshift 主 AWS Backup 控台或使用 AWS CLI.

使用 AWS Backup 主控台備份 Amazon Redshift 叢集的方式有兩種：視需求或做為備份計劃的一部分。

建立隨需 Amazon Redshift 備份

如需詳細資訊，請參閱建立隨需備份類型頁面。

若要建立手動快照，請在建立包含 Amazon Redshift 資源的備份計畫時，保持不勾選連續備份核取方塊。

在備份計畫中建立排程 Amazon Redshift 備份

您的排程備份可以包含 Amazon Redshift 叢集 (如果這是受保護的資源)。若要選擇加入以保護 Amazon Redshift 資料表：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 使用導覽窗格選擇 受保護的資源。
3. 將 Amazon Redshift 切換為 開啟。

4. 請參閱將資源指派給主控台，以便在現有或新的計畫中包含 Amazon Redshift 叢集。

在 管理備份計畫 下，您可以選擇 建立備份計畫 並包含 Amazon Redshift 叢集，也可以選擇 更新現有的備份計畫 以包含 Amazon Redshift 叢集。新增 Amazon Redshift 資源類型時，您可以選擇新增所有 Amazon Redshift 叢集，或勾選叢集旁的方塊

以程式設計方式進行備份

您也可以在 JSON 文件中定義備份計畫，並使用 AWS Backup 主控台或提供備份計畫 AWS CLI。如需如何以程式設計方式建立備份計畫的詳細資訊，請參閱使用 JSON 文件和 AWS Backup CLI 建立備份計畫。

您可以使用 API 來執行下列操作：

- 啟動備份任務
- 描述備份任務
- 取得復原點中繼資料
- 依資源列出復原點
- 列出復原點的標籤

檢視 Amazon Redshift 叢集備份

若要在主控台中檢視和修改您的 Amazon Redshift 資料表備份：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 選擇 Backup vaults (備份文件庫)。然後，按一下包含 Amazon Redshift 叢集的備份保存庫名稱。
3. 備份保存庫會隨即顯示摘要和備份清單。您可以按一下 復原點 ID 欄中的連結。
4. 若要刪除一或多個復原點，請勾選您要刪除的方塊。在 動作 按鈕下，您可以選取 刪除。

還原 Amazon Redshift 叢集

如需詳細資訊，請參閱如何還原 Amazon Redshift 叢集。

Amazon RDS 多可用區域備份

AWS Backup 使用一個主要和兩個可讀取的備用資料庫執行個體，備份和支援 Amazon RDS (適用於 MySQL 版) 和 PostgreSQL 異地同步備份 (可用區域) 部署選項。

下列區域提供多可用區域備份：亞太區域 (雪梨) 區域、亞太區域 (東京) 區域、歐洲 (愛爾蘭) 區域、美國東部 (俄亥俄) 區域、美國西部 (奧勒岡) 區域、歐洲 (斯德哥爾摩) 區域、亞太區域 (新加坡) 區域、美國東部 (維吉尼亞北部) 區域和歐洲 (法蘭克福) 區域。

多可用區部署選項可將寫入交易優化。當您的工作負載需要額外的讀取容量、較低的寫入交易延遲、更容易從網路抖動 (這會影響寫入交易延遲的一致性) 中復原以及高可用性和持久性時，就很適合使用此選項。

若要建立多可用區域叢集，您可以選擇 MySQL 或 PostgreSQL 作為引擎類型。

在主 AWS Backup 控台中，有三個部署選項：

- 多可用區域資料庫叢集：建立包含一個主要資料庫執行個體和兩個可讀取待命資料庫執行個體的資料庫叢集，其中每個資料庫執行個體都位於不同的可用區域。提供高可用性、資料備援，並增加可供伺服器使用的工作負載容量。
- 多可用區域資料庫執行個體：在不同的可用區域中建立一個主要資料庫執行個體和一個待命資料庫執行個體。這會提供高可用性和資料備援，但待命資料庫執行個體不支援讀取工作負載的連線。
- 單一資料庫執行個體：建立不含待命資料庫執行個體的單一資料庫執行個體。

若要建立 Amazon RDS 的備份，請參閱《建立備份》以排程備份作為備份計畫的一部分，或建立隨需備份。

> **Note**
>
> 時間點復原 (PITR) 可支援執行個體，但不支援叢集。
> 不支援複製多可用區域資料庫叢集快照。

多可用區域叢集與 RDS 執行個體之間的差異

單一可用區域或兩個可用區域中的備份是 RDS 執行個體；具有三個或更多執行個體的部署和備份是叢集，類似於 Amazon Aurora、Amazon Neptune 和 Amazon DocumentDB 叢集。

ARN (Amazon Resource Name) 會根據使用的是執行個體或叢集而以不同的方式呈現：

RDS 執行個體 ARN：`arn:aws:rds:region: account:db:name`

RDS 多可用叢集：`arn:aws:rds:region:account :cluster:name`

如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的《多可用區域資料庫叢集部署》。

如需詳細資訊，請參閱《Amazon RDS 使用者指南》中的《建立多可用區域資料庫叢集快照》。

AWS CloudFormation 堆疊備份

CloudFormation 堆疊包含多個可設定狀態和無狀態的資源，您可以將其備份為單一單元。換句話說，您可以透過備份堆疊並還原其中的資源，來備份和還原包含多個資源的應用程式。堆疊中所有的資源都是由堆疊的 AWS CloudFormation 範本定義。

備份 CloudFormation 堆疊時，會針對 CloudFormation 範本和堆疊 AWS Backup 中所支援的每個額外資源建立復原點。這些復原點會在一個稱為複合的整體復原點中群組在一起。

您無法還原此複合復原點，但可以還原巢狀復原點。您可以使用主控台或 AWS CLI還原複合備份中的任何位置，從一個巢狀備份到所有巢狀備份。

CloudFormation 應用程式堆疊詞

- 複合復原點：用來將巢狀復原點以及其他中繼資料群組在一起的復原點。
- 巢狀復原點：資源的復原點，屬於 CloudFormation 堆疊的一部分，並備份為複合復原點的一部分。每個巢狀復原點都屬於一個複合復原點堆疊。
- 複合工作：堆疊的備份、複製或還原工作，可針對 CloudFormation堆疊中的個別資源觸發其他備份工作。
- 巢狀工作： AWS CloudFormation 堆疊中資源的備份、複製或還原工作。

CloudFormation 堆疊備份工作

建立備份的程序稱為備份任務。 CloudFormation 堆疊備份工作的狀態為。備份任務完成後，其狀態會變成 `Completed`。這表示已建立 AWS CloudFormation 復原點 (備份)。

CloudFormation 堆棧可以使用控制台備份或以編程方式備份。若要備份任何資源 (包括 CloudFormation 堆疊)，請參閱本AWS Backup 開發人員指南中的其他位置建立備份。

CloudFormation 可以使用 API 命令備份堆疊`StartBackupJob`。請注意，說明文件和主控台是以複合復原點和巢狀復原點指稱；API 語言在相同的內容關係中則使用「父系和子系復原點」術語。

CloudFormation 堆棧包含所有 AWS 資源由您的CloudFormation 模板指示。請注意，您的範本可能包含 AWS Backup目前不支援的資源。如果您的範本包含 AWS 支援的資源和不受支援的資源的組合，仍 AWS Backup 會將範本 Backup 到複合堆疊中，但是 Backup 只會建立備份支援服務的復原點。CloudFormation 範本中包含的所有資源類型都會包含在備份中，即使您尚未選擇使用特定服務 (在「主

控台設定」中將服務切換為「已啟用」)。您可以還原 AWS Backup 支援的巢狀「備份」(復原點)，但無法備份或還原巢狀「堆疊」。

AWS CloudFormation 復原點

復原點狀態

堆疊的備份任務完成後 (任務狀態為 Completed)，即已建立堆疊的備份。此備份也稱為複合復原點。複合復原點可能具有下列其中一種狀態：Completed、Failed 或 Partial。請注意，備份任務具有狀態，而復原點 (也稱為備份) 也會有個別的狀態。

完成的備份工作表示您的整個堆疊和中的資源都受到保護 AWS Backup。失敗狀態表示備份任務失敗；您應該在修正造成失敗的問題之後重新建立備份。

Partial 狀態表示堆疊中並非所有資源都已備份。如果 CloudFormation 範本包含目前不受支援的資源，則可能會發生這種情況 AWS Backup，或者如果一或多個屬於堆疊 (巢狀資源) 資源的備份工作具有以外的狀態，則可能會發生這種情況Completed。您可以手動建立隨需備份，重新執行產生 Completed 以外狀態的任何資源。如果您預期堆疊的狀態為 Completed，但卻標記為 Partial，請確認您的堆疊可能發生以上哪種情況。

複合復原點中的每個巢狀資源都有自己的個別復原點，每個復原點都有自己的狀態 (Completed 或 Failed)。您可以還原狀態為 Completed 的巢狀復原點。

管理復原點

您可以複製複合復原點 (備份)，以及複製、刪除、取消關聯或還原巢狀復原點，但無法刪除包含巢狀備份的複合復原點。刪除或取消關聯複合復原點中的巢狀復原點之後，您可以手動刪除複合復原點，或保留直到備份計畫生命週期將其刪除為止。

刪除復原點

您可以使用 AWS Backup 主控台或使用來刪除復原點 AWS CLI。

若要使用 AWS Backup 主控台刪除復原點，

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 按一下左側導覽列中的 受保護的資源。在文字方塊中輸入CloudFormation以只顯示CloudFormation堆疊。
3. 複合復原點會隨即顯示在「復原點」窗格中。您可以按一下每個復原點 ID 左側的加號 (+) 來展開每個複合復原點，以顯示複合中包含的所有巢狀復原點。您可以勾選任何復原點左側的方塊，將其包含在您選取要刪除的復原點中。

4. 按一下 刪除 按鈕。

當您使用主控台刪除一或多個複合復原點時，會快顯一個警告方塊。此警告方塊會要求您確認是否有意刪除複合復原點 (包括複合堆疊內的巢狀復原點)。

若要使用 API 刪除復原點，請使用 `DeleteRecoveryPoint` 命令。

搭配使用 API 時， AWS Command Line Interface 您必須先刪除所有巢狀復原點，然後才能刪除複合點。如果您傳送 API 請求以刪除其中仍包含巢狀復原點的複合堆疊備份 (復原點)，該請求會傳回錯誤。

取消巢狀復原點與複合復原點的關聯

您可以取消巢狀復原點與複合復原點的關聯 (例如，您想要保留巢狀復原點但刪除複合復原點)。兩個復原點都會保留下來，但不再相互關聯；也就是說，取消關聯之後，在複合復原點上進行的動作將不會再套用至巢狀復原點。

您可以使用主控台或呼叫 API `DisassociateRecoveryPointFromParent` 來取消復原點的關聯。[請注意，API 呼叫使用「父系」術語來表示複合復原點。]

複製復原點

您可以複製複合復原點；如果資源支援跨帳戶和跨區域複製，您也可以複製巢狀復原點。

若要使用 AWS Backup 主控台複製復原點：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 按一下左側導覽列中的 受保護的資源。在文字方塊中輸入`CloudFormation`以只顯示CloudFormation堆疊。
3. 複合復原點會隨即顯示在「復原點」窗格中。您可以按一下每個復原點 ID 左側的加號 (+) 來展開每個複合復原點，以顯示複合中包含的所有巢狀復原點。您可以按一下任何復原點左側的圓形選項按鈕進行複製。
4. 選取後，請按一下窗格右上角的 複製 按鈕。

當您複製複合復原點時，不支援複製功能的巢狀復原點不會出現在複製的堆疊中。複合復原點的狀態將會是 `Partial`。

常見問答集

1. 「在應用程式備份過程中會包含哪些內容？」

作為使用定義之應用 CloudFormation程式的每個備份的一部分，會備份範本、範本中每個參數的處理值，以及支援 AWS Backup 的巢狀資源。巢狀資源的備份方式與備份非 CloudFormation 堆疊一部分的個別資源相同。請注意，不會備份標記為 no-echo 的參數值。

2. 「我可以備份具有嵌套 AWS CloudFormation 堆棧的堆棧嗎？」

   是。包含嵌套 CloudFormation 堆棧的堆棧可以在備份中。

3. 「Partial 狀態是否表示我的備份建立失敗？」

   否。部分狀態表示某些復原點已備份，某些復原點則否。如果您預期 Completed 備份結果，可檢查下列三種情況：

   a. 您的 CloudFormation 堆棧是否包含當前不支持的資源 AWS Backup？ 如需支援的資源清單，請參閱開發人員指南中的支援 AWS 資源和第三方應用程式。

   b. 屬於堆疊內資源的一或多個備份任務失敗，必須重新執行任務。

   c. 已從複合復原點中刪除或取消關聯巢狀復原點。

4. 「如何排除 CloudFormation 堆疊備份中的資源？」

   備份 CloudFormation 堆疊時，您可以將資源排除在備份中。在主控台中，建立備份計畫和更新備份計畫過程中會有一個指派資源步驟。在此步驟中，有一個 資源選取 區段。如果您選擇「包含特定資源類型」並已包含 CloudFormation為要備份的資源，則可以從選取的資源類型中排除特定的資源 ID。您也可以使用標籤來排除堆疊內的資源。

   利用 CLI，您可以

   - NotResources在您的備份計劃中，從 CloudFormation 堆棧中排除特定資源。
   - 使用 StringNotLike 透過標籤排除項目。

5. 「巢狀資源支援哪些類型的備份？」

   巢狀資源的備份可以是完整備份或增量備份，具體取決於這些資源支援 AWS Backup 的備份類型。如需詳細資訊，請參閱《增量備份的運作方式》。但請注意，Amazon S3 和 Amazon RDS 巢狀資源不支援 PITR (point-in-time 還原)。

6. 「 CloudFormation 堆疊中的變更集是否已備份？」

   沒有 變更集不會做為 CloudFormation 堆疊備份的一部分進行備份。

7. 「 AWS CloudFormation 堆疊的狀態如何影響備份？」

   CloudFormation 堆疊的狀態可能會影響備份。您可以備份狀態包含 COMPLETE 的堆疊，例如 CREATE_COMPLETE、ROLLBACK_COMPLETE、UPDATE_COMPLETE、UPDATE_ROLLBACK_COMPLETE、I 或 IMPORT_ROLLBACK_COMPLETE 狀態。

   如果上傳新範本失敗且堆疊移至 ROLLBACK_COMPLETE 狀態，則會備份新範本，但巢狀資源的備份則會視資源是否已復原而定。

8. 「應用程式堆疊生命週期與其他復原點生命週期有何不同？」

   巢狀復原點生命週期取決於其所屬的備份計畫。複合復原點取決於所有巢狀復原點的最長生命週期。刪除或取消關聯複合復原點內的最後一個巢狀復原點時，也會刪除複合復原點。

9. 「如何將標籤 CloudFormation 複製到恢復點？」

   是。這些標籤會複製到各自的巢狀復原點。

10. 「刪除複合復原點和巢狀復原點 (備份) 是否有先後順序？」

    是。您必須先刪除某些備份，才能刪除其他備份。在刪除複合內的所有復原點之前，無法刪除包含巢狀復原點的複合備份。一旦複合復原點不再包含巢狀復原點，就可以手動將其刪除。否則，系統會根據備份計畫生命週期將其刪除。

還原堆疊內的應用程式

如需還原巢狀復原點的資訊，請參閱《如何還原應用程式堆疊備份》。

建立 Windows VSS 備份

您可以使 AWS Backup用備份和還原在 Amazon EC2 執行個體上執行的已啟用 VSS (磁碟區陰影複製服務) 的 Windows 應用程式。如果應用程式具有向 Windows VSS 註冊的 VSS 寫入器，則會 AWS Backup 建立與該應用程式保持一致的快照集。

您可以執行一致的還原，同時使用用來保護其他 AWS 資源的相同受管理備份服務。透過 EC2 上應用程式一致的 Windows 備份，您就可以獲得與傳統備份工具相同的一致性設定和應用程式感知。

> **Note**
>
> AWS Backup 目前僅支援在 Amazon EC2 上執行的資源的應用程式一致性備份，特別是備份案例，可透過將現有的執行個體替換為從備份建立的新執行個體來還原應用程式資料。並非所有執行個體類型或應用程式皆支援 Windows VSS 備份。

如需詳細資訊，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的《建立 VSS 應用程式一致的快照》。

若要備份和還原執行 Amazon EC2 之具備 VSS 功能的 Windows 資源，請依照下列步驟完成必要的先決條件任務。如需說明，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的《開始之前》。

1. 在中下載、安裝和設定 SSM 代理程式 AWS Systems Manager。此步驟為必要。如需說明，請參閱《AWS Systems Manager 使用者指南》中的《使用執行命令更新 SSM Agent》。
2. 在進行 Windows VSS (磁碟區陰影複製服務) 備份之前，請將 IAM 政策新增至 IAM 角色，並將該角色連接至 Amazon EC2 執行個體。如需說明，請參閱《Amazon EC2 Windows 執行個體使用者指南》中的《為具備 VSS 功能的快照建立 IAM 角色》。如需 IAM 政策範例，請參閱《受管理的政策 AWS Backup》。
3. 下載 VSS 元件並安裝至 Amazon EC2 執行個體上的 Windows
4. 在 AWS Backup以下位置啟用 VSS：

    1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
    2. 在儀表板上，選擇您要建立的備份類型：建立隨需備份 或 管理備份計畫。提供備份類型所需的資訊。
    3. 指派資源時，請選擇 EC2。目前僅 EC2 執行個體支援 Windows VSS 備份。
    4. 在 進階設定 區段中，選擇 Windows VSS。這可讓您取得應用程式一致的 Windows VSS 備份。
    5. 建立您的備份。

狀態為 `Completed` 的備份任務不保證 VSS 部分會成功，但會盡最大努力包含 VSS。繼續執行下列步驟，確定備份是應用程式一致、當機一致或失敗：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽列中的 我的帳戶 下，按一下 任務。
3. `Completed` 狀態表示應用程式一致 (VSS) 的成功任務。

`Completed with issues` 狀態表示 VSS 操作失敗，因此只有當機一致的備份成功。這種狀態也會快顯一則訊息 `"Windows VSS Backup Job Error encountered, trying for regular backup"`。

如果備份失敗，狀態將會是 `Failed`。

4. 若要檢視備份任務的其他詳細資訊，請按一下個別任務。例如，詳細資訊可能顯示 `Windows VSS Backup attempt failed because of timeout on VSS enabled snapshot creation`。

不支援的 Amazon EC2 執行個體

具備 VSS 功能的 Windows 備份不支援下列 Amazon EC2 執行個體類型，因為這是小型執行個體，可能無法成功進行備份。

- t3.nano
- t3.micro
- t3a.nano
- t3a.micro
- t2.nano
- t2.micro

Amazon EBS 備份

- 建立隨需備份
- 建立排程備份

Amazon EBS 資源的備份程序與備份其他資源類型所用的步驟類似。下列區段會說明資源特有的資訊。

適用於不常用儲存的 Amazon EBS 封存層

> **Note**
>
> 此功能目前不適用於中國 (北京)、中國 (寧夏)、(美國東部) 及 AWS GovCloud AWS GovCloud (美國西部) 地區。

EBS 是支援將備份轉移至不常用儲存的資源之一。如需詳細資訊，請參閱 建立備份計畫 中的 生命週期和儲存層。

Amazon EBS 多磁碟區、當機一致的備份

依預設， AWS Backup 會為連接到 Amazon Amazon EC2 執行個體的 Amazon EBS 磁碟區建立當機一致的備份。當機一致性表示連接至相同 Amazon EC2 執行個體的每個 Amazon EBS 磁碟區都會在同一時間建立快照。您不再需要停止執行個體或在多個 Amazon EBS 磁碟區之間進行協調，以確保應用程式狀態的當機一致性。

由於多磁碟區、當機一致的快照是預設 AWS Backup 功能，因此您無需執行任何其他動作即可使用此功能。您可以使用下列其中一個程序來備份 Amazon EBS 磁碟區：

Amazon EBS 快照鎖和 AWS Backup

AWS Backup 如果快照鎖定持續時間超過備份生命週期，則與已套用 Amazon EBS 快照鎖的 AWS Backup 受管 Amazon EBS AMI 相關聯的受管 Amazon EBS 快照和快照可能不會在復原點生命週期中刪除。這些復原點的狀態反而會是 `EXPIRED`。如果您選擇先移除 Amazon EBS 快照鎖定，則可以手動刪除這些復原點。

還原 Amazon EBS 資源

若要還原您的 Amazon EBS 磁碟區，請依照《還原 Amazon EBS 磁碟區》中的步驟進行。

將標籤複製到備份

一般而言，會 AWS Backup 將標籤從其保護的資源複製到復原點。如需如何在還原期間複製標籤的詳細資訊，請參閱《還原時複製標籤》。

例如，當您備份 Amazon EC2 磁碟區時，會 AWS Backup 將其群組和個別資源標籤複製到產生的快照，但具體情況如下：

- 如需在備份時儲存中繼資料標籤所需的資源特定許可清單，請參閱《將標籤指派給備份所需的許可》。
- 最初與資源關聯的標籤以及在備份期間指定的標籤會指定給儲存在備份儲存庫中的復原點，最多可達 50 個 (這是一項 AWS 限制)。在備份期間指派的標籤將有較高的優先順序，且系統會依字母順序來複製這兩組標籤。
- 除非先啟用 進階 DynamoDB 備份，否則 DynamoDB 不支援將標籤指派給備份。
- 連接至 Amazon EC2 執行個體的 Amazon EBS 磁碟區是巢狀資源。附加至 Amazon Amazon EC2 執行個體的 Amazon EBS 磁碟區上的標籤是巢狀標籤。 AWS Backup 盡最大努力嘗試複製巢狀標籤，但如果不成功，則會建立沒有這些標籤的備份，並報告 「狀態已完成」。
- Amazon EC2 備份建立映像復原點和一組快照時，會 AWS Backup 將標籤複製到產生的 AMI。 AWS Backup 也會盡最大努力，將與 Amazon EC2 執行個體關聯的磁碟區中的標籤複製到產生的快照。

如果您將備份複製到另一個備 AWS Backup 份 AWS 區域，請將原始備份的所有標籤複製到目的地 AWS 區域。

停止備份任務

您可以在中啟動備份工作 AWS Backup 後將其停止。當您執行此操作時，系統並不會建立備份，且備份任務記錄會以 aborted (已中止) 狀態進行保存。

使用 AWS Backup 主控台停止備份工作

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，選擇 Jobs (任務)。
3. 選擇要停止的備份任務。
4. 在備份任務詳細資訊窗格中，選擇 Stop (停止)。

複製備份

您可以將備份複製到多個備份 AWS 帳戶 或 AWS 區域 隨選，也可以自動複製為大多數資源類型的排程備份計劃的一部分。此功能尚不適用於 NetApp ONTAP 磁碟區的 Amazon FSx。

您也可以為大多數支援的資源自動化一系列跨帳戶和跨區域複製，但 Amazon RDS 和 Aurora 則除外。對於 Amazon RDS 和 Aurora 快照， AWS Backup 僅支援自動化跨帳戶或跨區域副本，因為這些服務如何建立加密金鑰 (不支援複製異地同步備份資料庫叢集快照)。

某些資源類型同時提供連續備份以及跨區域和跨帳戶複製功能。建立連續備份的跨區域或跨帳戶複本時，複製的復原點 (備份) 會變成快照 (定期) 備份。PITR (時間點還原) 不適用於這些複本。

除非您另有指定，否則複本會保留其來源組態，包括建立日期和到期日。來源和複本中的到期日會參考來源的建立日期，而不是複本的建立日期。

注意：來源組態會覆寫其複本的到期設定，即使複本已設定為永不過期也一樣；設定為永不過期的複本仍會保留其來源的到期日。

如果您希望新備份複本永不過期，請將來源備份設定為永不過期，或指定複本在建立後 100 年過期。

主題

- 跨越建立備份副本 AWS 區域
- 跨 AWS 帳戶建立備份複本

跨越建立備份副本 AWS 區域

使用時 AWS Backup，您可以根據需要將備份複製到多個 AWS 區域 備份，或自動將備份作為排程備份計劃的一部分。如果您有業務持續性或合規性要求，需要將備份儲存在與生產資料最短距離的位置，則跨區域複寫特別有用。如需教學課程影片，請參閱《管理備份的跨區域複本》。

當您第一次將備份複製到新備份時， AWS 區域 請完整 AWS Backup 複製備份。一般而言，如果服務支援增量備份，則該備份的後續副本 AWS 區域 將會是增量備份。 AWS Backup 將使用目的地保管庫的客戶管理密鑰重新加密您的副本。

一個例外是 Amazon EBS，其中指出：「在複製操作期間變更快照的加密狀態會導致完整 (非增量式) 複製」。

大部分支 AWS Backup援的資源都支援跨區域備份。如需詳細規格，請參閱《各資源的功能可用性》表格的該部分。

大部分 AWS 地區都支援跨區域備份。如需詳細規格，請參閱《功能可用性 AWS 區域》表格的該部分。

執行隨需跨區域備份

視需要複製現有備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 選擇 Backup vaults (備份文件庫)。
3. 選擇包含您要複製之復原點的保存庫。
4. 在 備份 區段中，選取要複製的復原點。
5. 使用 動作 下拉式按鈕選擇 複製。
6. 輸入下列值：

   複製到目的地

   選擇複製 AWS 區域 的目的地。您可以將每個副本的新副本規則新增至新的目的地。

   目的地備份保存庫

   選擇副本的目的地備份文件庫。

   轉換至冷儲存

   選擇何時將備份複本轉換至冷儲存。轉移至冷儲存的備份必須在其中存放至少 90 天之久。在副本轉換至冷儲存後，您就無法變更此值。

   若要查看可轉換至冷儲存的資源清單，請參閱《各資源的功能可用性》表格的「生命週期至冷儲存」部分。會忽略其他資源的冷儲存運算式。

   保留期間

   選擇建立後到刪除複本經過的指定天數。此值必須超過 Transition to cold storage (轉換至冷儲存) 值的 90 天。永遠 保留期會無限期保留您的複本。

   IAM 角色

   選擇建立副本時 AWS Backup 將使用的 IAM 角色。角色也必須 AWS Backup 列為受信任的實體， AWS Backup 以便承擔該角色。如果您選擇「預設」，但帳戶中沒有 AWS Backup 預設角色，系統會為您建立具有正確權限的角色。
7. 請選擇 Copy (複製)。

排程跨區域備份

您可以使用排程備份計畫跨 AWS 區域複製備份。

使用排程備份計畫複製備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在 我的帳戶 中，選擇 備份計畫，然後選擇 建立備份計畫。
3. 在 建立備份計畫 頁面上，選擇 建立新的計畫。
4. 針對 備份計畫名稱，輸入您的備份計畫名稱。
5. 在 備份規則組態 區段中，新增定義備份排程、備份時段和生命週期規則的備份規則。您可以在稍後新增更多備份規則。

   a. 針對 備份規則名稱，輸入您的規則名稱。

   b. 針對 備份保存庫，從清單中選擇一個保存庫。此備份的復原點將會儲存在此保存庫中。您可以建立新的備份保存庫。

   c. 針對 備份頻率，選擇您要進行備份的頻率。

   d. 對於支援 PITR 的服務，如果您需要此功能，請選擇啟用連續備份以進行 point-in-time 復原 (PITR)。如需支援 PITR 的服務清單，請參閱《各資源的功能可用性》表格的該部分。

   e. 針對 備份時段，選擇 使用備份時段預設值 - 建議。您可以自訂備份時段。

   f. 針對 複製到目的地，選擇您備份複本的目的地 AWS 區域 。您的備份將會複製到此區域。您可以將每個副本的新副本規則新增至新的目的地。然後輸入下列值：

      複製到其他帳戶的保存庫

      請勿切換此選項。若要深入瞭解跨帳戶複製，請參閱跨帳戶建立備份副本 AWS 帳戶

      目的地備份保存庫

      選擇要複製備份的目的地區域中 AWS Backup 的備份保管庫。

      如果您想要為跨區域複本建立新的備份保存庫，請選擇 建立新的備份保存庫。在精靈中輸入資訊。然後選擇 建立備份保存庫。

6. 選擇 建立計畫。

跨 AWS 帳戶建立備份複本

> **Note**
>
> AWS 帳戶 在中管理多個資源之前 AWS Backup，您的帳戶必須屬於 AWS Organizations 服務中的相同組織。

使用時 AWS Backup，您可以根據需要備份多個 AWS 帳戶 ，也可以自動備份為排程備份計劃的一部分。如果您基於營運或安全性考量，想要將備份安全地複製到組織 AWS 帳戶 中的一或多個備份，請使用跨帳戶備份。如果不小心刪除您的原始備份，您可以將備份從其目的地帳戶複製到其來源帳戶，然後啟動還原。您必須在 AWS Organizations 服務中有兩個屬於同一組織的帳戶，才能執行這項操作。如需詳細資訊，請參閱《Organizations 使用指南》中的《教學課程：建立和設定組織》。

在您的目的地帳戶中，您必須建立備份保存庫。然後，您可以指派客戶管理的金鑰來加密目標帳戶中的備份，以及以資源為基礎的存取政策， AWS Backup 以允許存取您要複製的資源。在來源帳戶中，如果您的資源使用客戶自管金鑰加密，您必須與目的地帳戶共用此客戶自管金鑰。然後，您可以建立備份計畫，並選擇屬於 AWS Organizations中組織單位的目的地帳戶。

大部分支 AWS Backup援的資源都支援跨帳戶備份。如需詳細規格，請參閱《各資源的功能可用性》表格的該部分。

大部分 AWS 地區都支援跨帳戶備份。如需詳細規格，請參閱《功能可用性 AWS 區域》表格的該部分。

設定跨帳戶備份

建立跨帳戶備份需要哪些項目？

- 來源帳戶

  來源帳戶是生產 AWS 資源和主要備份所在的帳戶。

  來源帳戶使用者會起始跨帳戶備份操作。來源帳戶使用者或角色必須具有適當的 API 許可才能起始操作。適當的權限可能是受 AWS 管理的策略`AWSBackupFullAccess`，它可以完全訪問 AWS Backup 操作，或者允許執行諸如此類操作的客戶管理策略`ec2:ModifySnapshotAttribute`。如需政策類型的詳細資訊，請參閱《AWS Backup 受管政策》。

- 目的地帳戶

目的地帳戶是您要保留備份複本的帳戶。您可以選擇多個目的地帳戶。目的地帳戶必須與 AWS Organizations中的來源帳戶位於同一組織。

您必須「允許」目的地備份保存庫的存取政策 `backup:CopyIntoBackupVault`。如果沒有此政策，嘗試複製到目的地帳戶會遭到拒絕。

- 中的管理帳戶 AWS Organizations

  管理帳戶是您組織中的主要帳戶 (由 AWS Organizations定義)，可用來管理各 AWS 帳戶間的跨帳戶備份。若要使用跨帳戶備份，您也必須啟用服務信任。啟用服務信任之後，您可以使用組織中的任何帳戶作為目的地帳戶。從目的地帳戶，您可以選擇要用於跨帳戶備份的保存庫。

- 在 AWS Backup 主控台中啟用跨帳戶備份

如需安全的資訊，請參閱《跨帳戶備份的安全考量》。

若要使用跨帳戶備份，您必須啟用跨帳戶備份功能。然後，您必須在目的地備份保存庫中「允許」存取政策 `backup:CopyIntoBackupVault`。

啟用跨帳戶備份

1. AWS 使用您的 AWS Organizations 管理帳戶認證登入。跨帳戶備份只能透過這些憑證啟用或停用。
2. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
3. 在 我的帳戶 中，選擇 設定。
4. 針對 跨帳戶備份，選擇 啟用。
5. 在 備份保存庫 中，選擇您的目的地保存庫。
6. 在 存取政策 區段中，「允許」`backup:CopyIntoBackupVault`。例如，選擇 新增許可，然後選擇 允許從組織存取備份保存庫。
7. 現在，您組織中的任何帳戶都可以與同一組織中的任何其他帳戶共用其備份保存庫的內容。如需詳細資訊，請參閱 與其他 AWS 帳戶共用備份保存庫。若要限制哪些帳戶可以接收其他帳戶備份保存庫的內容，請參閱《將您的帳戶設定為目的地帳戶》。

排程跨帳戶備份

您可以使用排程備份計畫跨 AWS 帳戶複製備份。

使用排程備份計畫複製備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在 我的帳戶 中，選擇 備份計畫，然後選擇 建立備份計畫。
3. 在 建立備份計畫 頁面上，選擇 建立新的計畫。
4. 針對 備份計畫名稱，輸入您的備份計畫名稱。
5. 在 備份規則組態 區段中，新增定義備份排程、備份時段和生命週期規則的備份規則。您可以在稍後新增更多備份規則。

   針對 規則名稱，輸入您的規則名稱。
6. 在 排程 區段的 頻率 下，選擇您要進行備份的頻率。
7. 針對 備份時段，選擇 使用備份時段預設值 (建議)。您可以自訂備份時段。
8. 針對 備份保存庫，從清單中選擇一個保存庫。此備份的復原點將會儲存在此保存庫中。您可以建立新的備份保存庫。
9. 在 產生複本 - 選用 區段中，輸入下列值：

   目的地區域

   選擇備份副本 AWS 區域 的目的地。您的備份將會複製到此區域。您可以將每個副本的新副本規則新增至新的目的地。

   複製到其他帳戶的保存庫

   切換以選擇此選項。選取時，該選項會變成藍色。外部保存庫 ARN 選項會隨即顯示。

   外部保存庫 ARN

   輸入目的地帳戶的 Amazon Resource Name (ARN)。ARN 是包含帳戶 ID 及其 AWS 區域的字串。 AWS Backup 會將備份複製到目標帳戶的保管庫。目的地區域 清單會自動更新為外部保存庫 ARN 中的區域。

   針對 允許存取備份保存庫，選擇 允許。然後在開啟的精靈中選擇 允許。

   AWS Backup 需要訪問外部帳戶的權限才能將備份複製到指定的值。此精靈會顯示以下提供此存取權限的範例政策。

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

```
      "Sid": "Allow account to copy into backup vault",
      "Effect": "Allow",
      "Action": "backup:CopyIntoBackupVault",
      "Resource": "*",
      "Principal": {
        "AWS": "arn:aws:iam::account-id:root"
      }
    }
  ]
}
```

轉換至冷儲存

選擇何時將備份副本轉換為冷儲存，以及何時到期 (刪除) 副本。轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。在副本轉換至冷儲存後，您就無法變更此值。

若要查看可轉換至冷儲存的資源清單，請參閱《各資源的功能可用性》表格的「生命週期至冷儲存」部分。會忽略其他資源的冷儲存運算式。

Expire (到期) 指定在副本刪除建立後的天數。此值必須超過 Transition to cold storage (轉換至冷儲存) 值的 90 天。

> **Note**
>
> 當備份到期並在生命週期政策中標記為要刪除時， AWS Backup 在接下來的 8 小時內隨機選擇的點刪除備份。此時段有助於確保效能一致。

10. 選擇 新增至復原點的標籤，將標籤新增至復原點。
11. 針對 進階備份設定，選擇 Windows VSS，為 EC2 上執行的選定第三方軟體啟用應用程式感知快照。
12. 選擇 建立計畫。

執行隨需跨帳戶備份

您可以 AWS 帳戶 根據需要將備份複製到其他備份。

視需要複製備份

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup

2. 針對 我的帳戶，選擇 備份保存庫 以查看您所有列出的備份保存庫。您可以依備份保存庫名稱或標籤進行篩選。
3. 選擇您要複製之備份的 復原點 ID。
4. 請選擇 Copy (複製)。
5. 展開 備份詳細資訊 以查看您要複製之復原點的相關資訊。
6. 在 複製組態 區段中，從 目的地區域 清單中選擇一個選項。
7. 選擇 複製到其他帳戶的保存庫。選取時，該選項會變成藍色。
8. 輸入目的地帳戶的 Amazon Resource Name (ARN)。ARN 是包含帳戶 ID 及其 AWS 區域的字串。 AWS Backup 會將備份複製到目標帳戶的保管庫。目的地區域 清單會自動更新為外部保存庫 ARN 中的區域。
9. 針對 允許存取備份保存庫，選擇 允許。然後在開啟的精靈中選擇 允許。

   若要建立副本， AWS Backup 需要存取來源帳戶的權限。此精靈會顯示提供此存取權限的範例政策。此政策如下所示。

   ```
   {
     "Version": "2012-10-17",
     "Statement": [
       {
         "Sid": "Allow account to copy into backup vault",
         "Effect": "Allow",
         "Action": "backup:CopyIntoBackupVault",
         "Resource": "*",
         "Principal": {
           "AWS": "arn:aws:iam::account-id:root"
         }
       }
     ]
   }
   ```

10. 針對 轉換至冷儲存，選擇何時將備份複本轉換至冷儲存，以及複本何時到期 (何時刪除複本)。轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。在副本轉換至冷儲存後，您就無法變更此值。

    若要查看可轉換至冷儲存的資源清單，請參閱《各資源的功能可用性》表格的「生命週期至冷儲存」部分。會忽略其他資源的冷儲存運算式。

    Expire (到期) 指定在副本刪除建立後的天數。此值必須超過 Transition to cold storage (轉換至冷儲存) 值的 90 天。

11. 針對 IAM 角色，指定具有許可能將備份用於複製的 IAM 角色 (例如預設角色)。複製動作是由目的地帳戶的服務連結角色執行。
12. 請選擇 Copy (複製)。視您要複製的資源大小而定，此程序可能需要數小時才能完成。複製任務完成時，您會在 任務 選單的 複製任務 索引標籤中看到該複本。

跨帳戶備份的金鑰注意事項

AWS 受管理金鑰不支援跨帳戶複製。 AWS 託管密鑰的密鑰策略是不可變的，這樣可以防止跨帳戶複製密鑰。如果您的資源使用 AWS 受管理金鑰加密，而您想要執行跨帳戶複製，您可以將加密金鑰變更為客戶管理的金鑰，因為這支援跨帳戶複製。或者，您可以按照使用跨帳戶和跨區域備份保護加密的 Amazon RDS 執行個體中的指示，繼續使用 AWS 受管金鑰。

將備份從一個還原 AWS 帳戶 到另一個

AWS Backup 不支援將資源從一個復原 AWS 帳戶 到另一個。不過，您可以將一個帳戶的備份複製到另一個帳戶，然後在該帳戶中還原備份。例如，您無法將帳戶 A 的備份還原至帳戶 B，但可以將帳戶 A 的備份複製到帳戶 B，然後在帳戶 B 中還原備份。

將一個帳戶的備份還原至另一個需要兩個步驟。

將一個帳戶的備份還原至另一個

1. 將備份從來源複製 AWS 帳戶 到您要還原的帳戶。如需說明，請參閱《設定跨帳戶備份》。
2. 使用適用於您資源的說明來還原備份。

與其他 AWS 帳戶共用備份保存庫

AWS Backup 可讓您與一或多個帳戶或您的整個組織共用備份保管庫 AWS Organizations。您可以與來源 AWS 帳戶、使用者或 IAM 角色共用目的地備份保存庫。

共用目的地備份保存庫

1. 選擇 AWS Backup，然後選擇 備份保存庫。
2. 選擇您要共用之備份保存庫的名稱。
3. 在 存取政策 窗格中，選擇 新增許可 下拉式清單。
4. 選擇 允許備份保存庫的帳戶層級存取權限。您也可以選擇允許組織層級或角色層級存取權限。
5. 輸入您要與此目的地保存庫共用之帳戶的 帳戶 ID。

6. 選擇 儲存政策。

您可以使用 IAM 政策來共用備份保存庫。

與 AWS 帳戶 或 IAM 角色共用目的地備份保存庫

下列政策會與帳戶號碼 4444555566666 以及帳戶號碼 111122223333 中的 IAM 角色 SomeRole 共用備份保存庫。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":[
          "arn:aws:iam::444455556666:root",
          "arn:aws:iam::111122223333:role/SomeRole"
        ]
      },
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*"
    }
  ]
}
```

在其中共用組織單位的目的地備份保管庫 AWS Organizations

下列政策會使用組織單位的 PrincipalOrgPaths 與其共用備份保存庫。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAnyValue:StringLike":{
          "aws:PrincipalOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
```

```
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

與中的組織共用目的地備份保管庫 AWS Organizations

下列政策會與 `PrincipalOrgID` 為 "o-a1b2c3d4e5" 的組織共用備份保存庫。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":"*",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "StringEquals":{
          "aws:PrincipalOrgID":[
            "o-a1b2c3d4e5"
          ]
        }
      }
    }
  ]
}
```

將您的帳戶設定為目的地帳戶

當您第一次使用 AWS Organizations 管理帳戶啟用跨帳戶備份時，成員帳戶的任何使用者都可以將其帳戶設定為目標帳戶。建議您在 AWS Organizations 中設定下列一或多個服務控制政策 (SCP)，以限制目的地帳戶。若要深入了解如何將服務控制原則附加至 AWS Organizations 節點，請參閱附加和卸離服務控制政策。

使用標籤限制目的地帳戶

當附加至 AWS Organizations 根、OU 或個人帳戶時，此原則會將目的地從根、OU 或帳戶限制複製到只有已標記`DestinationBackupVault`備份保存庫的帳戶。許可

"backup:CopyIntoBackupVault" 可控制備份保存庫的運作方式，以及在此情況下，哪些目的地備份保存庫有效。使用此政策，搭配套用至已核准目的地保存庫的對應標籤，即可控制跨帳戶複製的目的地，僅限於已核准的帳戶和備份保存庫。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyIntoBackupVault",
      "Resource":"*",
      "Condition":{
        "Null":{
          "aws:ResourceTag/DestinationBackupVault":"true"
        }
      }
    }
  ]
}
```

使用帳戶號碼和保存庫名稱限制目的地帳戶

當附加到 AWS Organizations 根帳戶、OU 或個別帳戶時，此策略會將源自該根、OU 或帳號的副本限制為只有兩個目標帳戶。許可 "backup:CopyFromBackupVault" 可控制備份保存庫中復原點的運作方式，以及在此情況下，該復原點可複製到的目的地。只有在一或多個目的地備份保存庫的名稱開頭為 cab- 時，來源保存庫才允許複製到第一個目的地帳戶 (112233445566)。只有在目的地是名為 fort-knox 的單一備份保存庫時，來源保存庫才允許複製到第二個目的地帳戶 (123456789012)。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"arn:aws:ec2:*:snapshot/*",
      "Condition":{
        "ForAllValues:ArnNotLike":{
          "backup:CopyTargets":[
            "arn:aws:backup:*:112233445566:backup-vault:cab-*",
            "arn:aws:backup:us-west-1:123456789012:backup-vault:fort-knox"
          ]
        }
```

```
      }
    }
  ]
}
```

使用中的組織單位限制目的地帳戶 AWS Organizations

當附加至包含來源帳戶的 AWS Organizations 根或 OU 時，或連結至來源帳戶時，下列策略會將目標帳戶限制在兩個指定 OU 內的這些帳戶。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Deny",
      "Action":"backup:CopyFromBackupVault",
      "Resource":"*",
      "Condition":{
        "ForAllValues:StringNotLike":{
          "backup:CopyTargetOrgPaths":[
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/",
            "o-a1b2c3d4e5/r-f6g7h8i9j0example/ou-def0-awsbbbbb/ou-jkl0-awsddddd/*"
          ]
        }
      }
    }
  ]
}
```

跨帳戶備份的安全考量

在 AWS Backup中執行跨帳戶備份時，請注意下列事項：

- 目的地保存庫不能是預設保存庫。這是因為預設保存庫使用了無法與其他帳戶共用的金鑰加密。
- 停用跨帳戶備份之後，跨帳戶備份最多仍可能執行 15 分鐘。這是由於最終一致性所致，即使在停用跨帳戶備份之後，也可能會導致某些跨帳戶任務正在啟動或完成。
- 如果目的地帳戶稍後離開組織，該帳戶將保留備份。為了避免潛在的資料外洩，請在連接至目的地帳戶的服務控制政策 (SCP) 中，對 `organizations:LeaveOrganization` 許可設定拒絕許可。如需 SCP 的詳細資訊，請參閱《Organizations 使用者指南》中的《從組織移除成員帳戶》。
- 如果您在跨帳戶複製期間刪除複製工作角色，則複製工作完成時， AWS Backup 無法從來源帳戶取消共用快照。在此情況下，備份任務會完成，但複製任務狀態會顯示為 無法取消共用快照。

刪除備份

建議您在 AWS Backup 建立備份計畫時設定生命週期，藉此自動刪除不再需要的備份。例如，如果您將備份計劃的生命週期設定為保留復原點一年，則 AWS Backup 會在 2022 年 1 月 1 日自動刪除其在 2021 年 1 月 1 日或之後數小時內建立的復原點。 (在復原點到期後 8 小時內AWS Backup 隨機刪除，以維持效能。) 若要進一步了解如何設定生命週期保留政策，請參閱《建立備份計畫》。

不過，您可能想要手動刪除一或多個復原點。例如：

- 您有 EXPIRED 復原點。這些復原點 AWS Backup 無法自動刪除，因為您刪除或修改了用於建立備份計劃的原始 IAM 政策。當 AWS Backup 試圖刪除它們時，它缺乏權限這樣做。

  如果 AWS 受管 Amazon EBS 或 Amazon EC2 復原點已套用 Amazon EBS 快照鎖，且 AWS Backup 無法完成通常會導致復原點刪除的生命週期程序，也可能會建立過期的復原點。請注意，您可以從 Amazon EC2 主控台和 API 或 Amazon EBS 主控台和 API 還原這些過期的復原點。

  > ⚠ Warning
  >
  > 您會繼續將已過期的復原點儲存在您的帳戶中。這可能會增加您的儲存成本。

  2021 年 8 月 6 日之後，目標復原點 AWS Backup 會在其備份保存庫中顯示為「已過期」。您可以將滑鼠移至紅色 已過期 狀態上方，這會快顯一則狀態訊息，說明無法刪除備份的原因。您也可以選擇 重新整理 來接收最新資訊。
- 您不想要備份計畫再依照您設定的方式運作。更新備份計畫會影響未來將建立的復原點，但不會影響已建立的復原點。若要進一步了解，請參閱《更新備份計畫》。
- 您需要在完成測試或教學課程之後進行清理。

手動刪除備份

手動刪除復原點

1. 在 AWS Backup 主控台的導覽窗格中，選擇「Backup 儲存庫」。
2. 在 Backup vaults (備份文件庫) 頁面上，選擇您存放備份的備份文件庫。
3. 依序選擇復原點、動作 下拉式清單和 刪除。
4. 1. 如果您的清單包含連續備份，請選擇下列其中一個選項。每個連續備份都有一個復原點。

- 永久刪除我的備份資料 或 刪除復原點。選取其中一個選項，即可停止未來的連續備份，同時刪除現有的連續備份資料。
- 保留我的連續備份資料 或 取消關聯復原點。選取其中一個選項，即可停止未來的連續備份，但會依照您保留期的定義，將現有的連續備份資料保留至到期為止。

2. 若要刪除列出的所有復原點，請按一下「刪除」，然後選擇 刪除復原點。
3. AWS Backup 開始送出要刪除的復原點，並顯示進度列。在提交過程中，請保持瀏覽器標籤開啟，切勿離開此頁面。
4. 在提交流程結束時，會在橫幅中 AWS Backup 顯示狀態。狀態可能是：
   - 已成功提交。您可以選擇 檢視進度 了解每個復原點的刪除狀態。
   - 無法提交。您可以選擇 檢視進度 了解每個復原點的刪除狀態，或選擇 再試一次 重新提交。
   - 某些復原點已成功提交，而其他復原點無法提交的混合結果。
5. 如果您選擇 檢視進度，則可以檢閱每個備份的 刪除狀態。如果刪除狀態為 失敗 或 已過期，您可以按一下該狀態來查看原因。您也可以選擇 重試失敗的刪除。

針對手動刪除進行故障診斷

在極少數情況下， AWS Backup 可能無法完成您的刪除要求。 AWS Backup 會使用服務連結角色執行AWSServiceRoleForBackup刪除作業。

如果刪除請求失敗，請確認您的 IAM 角色具有建立服務連結角色的許可。具體而言，請確認您的 IAM 角色具有 `iam:CreateServiceLinkedRole` 動作。如果沒有，請將此許可新增至用於建立備份的角色。新增此權限可執 AWS Backup 行手動刪除。

如果在確認 IAM 角色具有 `iam:CreateServiceLinkedRole` 動作之後，您的復原點仍卡在 `DELETING` 狀態，我們可能正在調查您的問題。請執行下列步驟來完成手動刪除：

1. 設定提醒，以在 2-3 天後回頭檢查。
2. 2-3 天後，請檢查是否有最近 `EXPIRED` 的刪除點為第一次手動刪除操作的結果。
3. 手動刪除這些 `EXPIRED` 復原點。

如需角色的詳細資訊，請參閱《使用服務連結角色》和《新增和移除 IAM 身分許可》。

編輯備份

使用建立備份之後 AWS Backup，您可以變更備份的生命週期或標籤。生命週期會定義備份會在何時轉移至冷儲存，以及會在何時過期。 AWS Backup 會根據您定義的生命週期來自動轉移備份以及使備份過期。

若要查看可轉換至冷儲存的資源清單，請參閱《各資源的功能可用性》表格的「生命週期至冷儲存」部分。會忽略其他資源的冷儲存運算式。

> **Note**
>
> 只有 Amazon 彈性檔案系統 (Amazon EFS) 檔案系統和進階 Amazon DynamoDB 的備份才支援使用 AWS Backup 主控台編輯備份標籤。
> 建立時為其他資源新增至復原點的標籤仍會顯示，但會變成灰色且無法編輯。即使這些標記無法在 AWS Backup 主控台中編輯，您也可以使用服務的主控台或 API 編輯這些其他服務備份的標籤。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。更新「轉移至冷儲存前所需天數」的設定時，該值必須至少為備份的有效期再加上一天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

下方範例將說明如何更新備份的生命週期。

編輯備份的生命週期

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 在 Backups (備份) 區段中，選擇備份。
4. 在備份詳細資訊頁面上，選擇 Edit (編輯)。
5. 配置生命週期設定，然後選擇 Save (儲存)。

還原備份

如何還原

如需各種 AWS Backup支援資源類型的主控台還原指示和說明文件連結，請參閱本頁底部的連結。

若要以程式設計方式還原備份，請使用 StartRestoreJob API 操作。

還原資源所需的組態值 (「還原中繼資料」) 會因要還原的資源而有所不同。若要取得用於建立備份的組態中繼資料，您可以呼叫 GetRecoveryPointRestoreMetadata。本頁底部的連結也提供還原中繼資料範例。

從冷儲存中還原所需的時間，通常比從暖儲存中還原所需的時間多 4 小時。

對於每個還原，都會建立一個具有唯一任務 ID (例如 1323657E-2AA4-1D94-2C48-5D7A423E7394) 的還原任務。

> **Note**
>
> AWS Backup 在還原時間內不提供任何服務等級協定 (SLA)。還原時間可能會根據系統負載和容量而有所不同，即使是包含相同資源的還原也是如此。

非破壞性還原

當您使 AWS Backup 用還原備份時，它會使用您要還原的備份建立新資源。如此可防止您現有的資源遭到還原活動的破壞。

還原測試

您可以對資源進行測試，以模擬還原體驗。這有助於判斷您是否符合組織的還原時間目標 (RTO)，並有助於為未來的還原需求做準備。

如需詳細資訊，請參閱還原測試。

在還原期間複製標籤

> **Note**
>
> Amazon DynamoDB、Amazon S3、Amazon EC2 執行個體上的 SAP HANA、虛擬機器和 Amazon Timestream 資源的還原目前未提供這項功能。

簡介

如果標籤在備份時屬於受保護的資源，您可以在還原資源時複製標籤。標籤 (Tag) 是包含鍵值對的標籤 (Label)，可協助您識別和搜尋資源。當您啟動還原任務時，可將屬於原始備份資源的標籤新增至要還原的資源。

當您選擇在還原任務期間包含標籤時，此步驟可取代在還原任務完成之後手動將標籤套用至資源的額外負荷與人力。請注意，這與將新標籤加入還原的資源不同。

當您在主控台流程中還原備份時，預設會複製您的來源標籤。在控制台中，如果您不想選擇將標籤複製到還原的資源，請取消勾選該方塊

在 API 操作 `StartRestoreJob` 中，參數 `CopySourceTagsToRestoredResource` 預設會設定為 `false`，這會將原始來源標籤從您要還原的資源中排除。如果您想要「包含」原始來源中的標籤，請將其設定為 `True`。

考量事項

- 資源最多可以有 50 個標籤，包括還原的資源。如需有關標記限制的詳細 AWS 資訊，請參閱標記您的資源。
- 確定還原用於複製標籤的角色具有正確的許可。還原的預設角色包含必要許可。自訂角色必須包含其他許可才能標記資源。
- 目前不支援包含還原標籤的下列資源：VMware 雲™ AWS、內部部署系統 AWS Outposts、Amazon EC2 執行個體上的 SAP HANA、時間流、動態支援、進階 DynamoDB 和 Amazon S3。™
- 針對連續備份，原始資源上最近備份的標籤會複製到還原的資源。
- 不會針對項目層級還原複製標籤。
- 在備份任務完成之後新增至備份，但在備份之前不存在於原始資源上的標籤，不會複製到還原的資源。只有在 2023 年 5 月 22 日之後建立的備份才有資格在還原時複製標籤。

與特定資源的標籤互動

- 當您還原 Amazon EFS 資源時，必須將其複製到新的檔案系統。還原至現有的檔案系統無法將標籤複製到其中。
- 根據預設，Amazon Redshift 叢集在還原任務期間一律會包含標籤。
- Amazon RDS
  - 如果已備份的 RDS 叢集仍處於作用中狀態，則會複製此叢集中的標籤。

- 如果原始叢集不再處於作用中狀態，則會改為複製叢集快照中的標籤。
- 無論 CopySourceTagsToRestoredResource 的布林值參數設定為 True 或 False，都會在還原期間複製備份時存在於資源上的標籤。不過，如果快照不包含標籤，則會使用上述布林值設定。

透過主控台複製標籤

1. 開啟 AWS Backup 主控台
2. 在導覽窗格中，選擇 受保護的資源，然後選取您要還原的 Amazon S3 資源 ID。
3. 在 資源詳細資訊 頁面上，您會看到所選資源 ID 的復原點清單。若要還原資源：
   a. 在 備份 窗格中，選擇資源的復原點 ID。
   b. 在窗格的右上角，選擇 還原 (或者，您可以前往備份保存庫，找到復原點，然後依序按一下 動作 和 還原)。
4. 在 還原備份 頁面上，找到名為「使用標籤還原」的面板。若要包含原始資源中的所有標籤，請保持勾選此方塊 (請注意，在控制台中，預設會勾選此方塊)。
5. 選取所有偏好的設定和角色之後，請按一下 還原備份。

以程式設計方式包含標籤

使用 API 操作 StartRestoreJob。確定下列布林值參數設定為 True：

```
CopySourceTagsToRestoredResource = true
```

如果布林值參數 CopySourceTagsToRestoredResource = True，則還原任務會將原始資源中的標籤複製到還原的資料。

> **Important**
>
> 如果不支援的資源 (VMware、現場部署系統、EC2 執行個體上的 SAP HANA AWS Outposts、時間流、DynamoDB、進階 DynamoDB 和 Amazon S3) 包含此參數，則還原任務將會失敗。

```
{
    "RecoveryPointArn": "arn:aws:ec2:us-east-1::image/ami-1234567890a1b234",
```

```
    "Metadata": {
        "InstanceInitiatedShutdownBehavior": "stop",
        "DisableApiTermination": "false",
        "EbsOptimized": "false",
        "InstanceType": "t1.micro",
        "SubnetId": "subnet-123ab456cd7efgh89",
        "SecurityGroupIds": "[\"sg-0a1bc2d345ef67890\"]",
        "Placement": "{\"GroupName\":null,\"Tenancy\":\"default\"}",
        "HibernationOptions": "{\"Configured\":false}",
        "IamInstanceProfileName": "UseBackedUpValue",
        "aws:backup:request-id": "1a2345b6-cd78-90e1-2345-67f890g1h2ij"
    },
    "IamRoleArn": "arn:aws:iam::123456789012:role/EC2Restore",
    "ResourceType": "EC2",
    "IdempotencyToken": "34ab5678-9012-3c4d-5678-efg9h01f23i4",
    "CopySourceTagsToRestoredResource": true
}
```

針對標籤還原問題進行故障診斷

錯誤：許可不足

解決方法：確定您的還原角色具有必要許可，以便在還原的資源上包含標籤。還原的預設AWS 受管理服務角色原AWSBackupServiceRolePolicyForRestores則包含此工作的必要權限。

如果您選擇使用自訂角色，請確定具有下列許可：

- `elasticfilesystem:TagResource`
- `storagegateway:AddTagsToResource`
- `rds:AddTagsToResource`
- `ec2:CreateTags`
- `cloudformation:TagResource`

如需詳細資訊，請參閱《API 許可》。

還原任務狀態

您可以在 AWS Backup 主控台的 任務 頁面上檢視還原任務的狀態。還原任務狀態包括 等待處理中、執行中、已完成、已中止 和 失敗。

主題

還原 S3 資料

您可以將使用備份的 S3 資料還原 AWS Backup 到 S3 標準儲存類別。您可以還原儲存貯體中的所有物件或特定物件。您可以將其還原至現有或新的儲存貯體。

如果您還原特定物件，您可以還原物件的目前版本。

雖然 S3 備份可跨區域複製，但還原任務只會在原始備份或複本所在的相同區域中進行。

Example

範例：在美國東部 (維吉尼亞北部) 區域建立的 S3 儲存貯體可複製到加拿大 (中部) 區域。您可以使用位於美國東部 (維吉尼亞北部) 區域的原始儲存貯體起始還原任務並還原至該區域，也可以使用位於加拿大 (中部) 區域的複本起始還原任務並還原至該區域。

使用主 AWS Backup 控台還原 Amazon S3 復原點

若要使用 AWS Backup 主控台還原 Amazon S3 資料：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選取您要還原的 Amazon S3 資源 ID。
3. 在 資源詳細資訊 頁面上，您會看到所選資源 ID 的復原點清單。若要還原資源：

   a. 在 備份 窗格中，選擇資源的復原點 ID。

   b. 在窗格右上角，選擇 Restore (還原)。

   (或者，您可以前往備份保存庫，找到復原點，然後依序按一下 動作 和 還原。)
4. 如果您要還原連續備份，請在 還原時間 窗格中，選取下列任一選項：

   a. 接受預設值，以還原至最近可還原的時間。

   b. 指定要還原的日期和時間。
5. 在 設定 窗格中，指定要還原整個儲存貯體還是執行項目層級還原。

   a. 如果選擇 項目層級還原，您可以指定每個項目的 S3 URI 來唯一識別物件，針對每個還原任務最多還原 5 個項目 (S3 物件)。

   (如需 S3 儲存貯體 URI 的詳細資訊，請參閱《Amazon Simple Storage Service 使用者指南》中的《存取儲存貯體的方法》。)

   b. 選擇 新增項目 以指定要還原的其他項目。
6. 選擇您的 還原目的地。您可以還原至來源儲存貯體、使用現有的儲存貯體或建立新的儲存貯體。

   > **Note**
   >
   > 您的還原目標值區必須已開啟版本控制。 AWS Backup 如果您選取的值區不符合此需求，便會通知您。

   a. 如果您選擇 [使用現有儲存貯體]，請從下拉式功能表中選取目標 S3 儲存貯體，以顯示目前 AWS 區域內所有現有的儲存貯體。

   b. 如果您選擇 建立新的儲存貯體，請輸入新的儲存貯體名稱。新的儲存貯體預設會啟用 S3 版本控制。預設會關閉 封鎖公開存取 (BPA) 設定。在 S3 中建立儲存貯體之後，您可以修改這些設定。

7. 您還有下列其他選項可選擇 還原的物件加密：使用原始加密金鑰 (預設)、Amazon S3 金鑰 (SSE-S3) 或 AWS Key Management Service 金鑰 (SSE-KMS)。

   a. 如果您選擇 使用原始加密金鑰 (預設)，但原始物件未加密，則還原的物件也不會加密。
   b. 如果您選擇 Amazon S3 金鑰 (SSE-S3)，則不需要指定任何其他選項。
   c. 如果您選擇金AWS Key Management Service 鑰 (SSE-KMS)，您可以進行下列選擇：AWS 受管金鑰 (aws/s3)、從您的金鑰中選擇或輸入金 AWS KMS 鑰 ARN。 AWS KMS

      i. 如果您選擇 AWS 受管金鑰 (aws/s3)，則不需要指定任何其他選項。
      ii. 如果您從 AWS KMS 按鍵中選擇，請從下拉式選單中選取一個按 AWS KMS 鍵。或者，選擇 建立金鑰。
      iii. 如果您輸入 AWS KMS 鍵 ARN，請在文本框中鍵入 ARN。或者，選擇 建立金鑰。

8. 在 Restore role (還原角色) 窗格中，選擇 AWS Backup 在此次還原中具有的 IAM 角色。
9. 選擇 Restore backup (還原備份)。Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

限制：

AWS Backup 建立所有 S3 版本的備份，但在任何時間點僅從版本堆疊還原最新版本。

考量：

必須在目的地儲存貯體中啟用存取控制清單 (ACL)，否則任務將會失敗。若要啟用 ACL，請依照《設定 ACL》頁面中的說明進行。

如果來源儲存貯體具有相同名稱或版本 ID 的物件，則會略過物件還原。

使用 AWS Backup API、CLI 或開發套件來還原 Amazon S3 復原點

請使用 `StartRestoreJob`。您可以在 Amazon S3 還原期間指定下列中繼資料：

```
// Mandatory metadata:
DestinationBucketName // The destination bucket for your restore.
ItemsToRestore // A list of up to five paths of individual objects to restore. Only
 required for item-level restore.
NewBucket // Boolean to indicate whether to create a new bucket.
Encrypted // Boolean to indicate whether to encrypt the restored data.
CreationToken // An idempotency token.
EncryptionType // The type of encryption to encrypt your restored objects. Options
 are original (same encryption as the original object), SSE-S3, or SSE-KMS).
```

```
RestoreTime // The restore time (only valid for continuous recovery points where it is
 required, in format 2021-11-27T03:30:27Z).

// Optional metadata:
KMSKey // Specifies the SSE-KMS key to use. Only needed if encryption is SSE-KMS.
aws:backup:request-id
```

復原點狀態

復原點會有一個狀態來表示其狀態。

PARTIAL狀態表示 AWS Backup 無法在備份視窗關閉之前建立復原點。若要使用 API 增加備份計劃時間，請參閱UpdateBackupPlan。您也可以使用主控台，透過選擇和編輯備份計畫來加長備份計畫時段。

EXPIRED狀態表示復原點已超過其保留期限，但 AWS Backup 缺少權限，或無法刪除它。若要手動刪除這些復原點，請參閱《入門》的《清理資源》一節中的《步驟 3：刪除復原點》。

STOPPED 狀態會出現在連續備份，其中使用者已採取某些動作，導致連續備份停用。這可能是因為移除權限、關閉版本控制、關閉傳送至 Amazon 的事件 EventBridge，或停用所設定的 EventBridge 規則所造成 AWS Backup。

若要解決 STOPPED 狀態，請確定已具備所有必要許可，並且已在 S3 儲存貯體上啟用版本控制。一旦符合這些條件，下次執行備份規則就會建立新的連續復原點。不需要刪除狀態為「已停止」的復原點。

還原虛擬機器

使用主 AWS Backup 控台還原虛擬機器復原點

您可以從 AWS Backup 主控台左側導覽窗格中的多個位置還原虛擬機器：

- 選擇 Hypervisors 可檢視連線至 AWS Backup之 Hypervisor 所管理虛擬機器的復原點。
- 選擇 虛擬機器 可檢視連線至 AWS Backup之所有 Hypervisor 中虛擬機器的復原點。
- 選擇「Backup 儲存庫」以檢視儲存在特定 AWS Backup 資料保險箱中的復原點。
- 選擇「受保護的資源」以檢視所有 AWS Backup 受保護資源的復原點。

如果您需要還原不再與 Backup 閘道連線的虛擬機器，請選擇 備份保存庫 或 受保護的資源 以找到您的復原點。

AWS Backup 虛擬機器的還原是非破壞性的。這表示在還原期間 AWS Backup 不會覆寫現有的虛擬機器。而是透過部署新的虛擬機器來進行還原。

還原的虛擬機器會以關機模式在您的基礎設施上啟動。

若要將虛擬機器還原至 VMware、VMware 雲端及 VMware 雲端 AWS，請執行下列動作 AWS Outposts：

1. 在 Hypervisors 或 虛擬機器 檢視中，選擇要還原的 VM 名稱。在 受保護的資源 檢視中，選擇要還原的虛擬機器 資源 ID。
2. 選擇要還原之 復原點 ID 旁的選項按鈕。
3. 選擇 Restore (還原)。
4. 選擇 還原類型。
    a. 完整還原 會還原所有虛擬機器的磁碟。
    b. 磁碟層級還原 會還原使用者定義的一或多個磁碟選項。使用下拉式選單來選取要還原的磁碟。
5. 選擇 還原位置。這些選項是 VMware, VMware 雲上 AWS, 和 VMware 雲上 AWS Outposts.
6. 如果您正在執行完整還原，請跳至下一個步驟。如果您正在執行磁碟層級還原，VM 磁碟 下會有一個下拉式選單。選擇要還原的一或多個可開機磁碟區。
7. 從下拉式選單中選取一個 Hypervisor 來管理還原的虛擬機器
8. 針對還原的虛擬機器，使用您組織的虛擬機器最佳實務來指定其：
    a. 名稱
    b. 路徑 (例如 `/datacenter/vm`)
    c. 運算資源名稱 (例如 VMHost 或叢集)

        如果主機是叢集的一部分，則無法還原至主機，只能還原至指定的叢集。
    d. 資料儲存
9. 針對 還原角色，選取 預設角色 (建議) 或使用下拉式選單選擇 IAM 角色。
10. 選擇 Restore backup (還原備份)。
11. 選擇性：檢查您的還原任務何時具有 `Completed` 狀態。在左側導覽選單中，選擇 任務。

若要將虛擬機器還原至 Amazon EBS：

1. 在 Hypervisors 或 虛擬機器 檢視中，選擇要還原的 VM 名稱。在 受保護的資源 檢視中，選擇要還原的虛擬機器 資源 ID。
2. 選擇要還原之 復原點 ID 旁的選項按鈕。
3. 選擇 Restore (還原)。
4. 選擇 還原類型。
   - 磁碟還原 會還原使用者定義的一個磁碟選項。使用下拉式選單來選取要還原的磁碟。
5. 針對 還原位置，選擇 Amazon EBS。
6. 在 VM 磁碟 下拉式選單下，選擇要還原的可開機磁碟區。
7. 在 EBS 磁碟區類型 下，選擇磁碟區類型。
8. 選擇您的可用區域。
9. 加密 (選用)。如果您選擇加密 EBS 磁碟區，請勾選此方塊。
10. 從下拉式選單中選取您的 KMS 金鑰。
11. 針對 還原角色，選取 預設角色 (建議) 或使用下拉式選單選擇 IAM 角色。
12. 選擇 Restore backup (還原備份)。
13. 選擇性：檢查您的還原任務何時具有 `Completed` 狀態。在左側導覽選單中，選擇 任務。
14. 選擇性：請造訪《如何在整個 Amazon EBS 磁碟區上建立 LVM 邏輯磁碟區》，進一步了解如何在還原的 Amazon EBS 磁碟區上掛載受管磁碟區和存取資料。

將虛擬機器還原至 Amazon EC2 執行個體

將虛擬機器還原 (或移轉) 至 EC2 需要授權。默認情況下， AWS 將包含許可證（收費）。如需詳細資訊，請參閱《Amazon EC2 VM Import/Export 使用者指南》中的《授權選項》。

每個虛擬機器磁碟的上限為 5 TB。

1. 在 Hypervisors 或 虛擬機器 檢視中，選擇要還原的 VM 名稱。在 受保護的資源 檢視中，選擇要還原的虛擬機器 資源 ID。
2. 選擇要還原之 復原點 ID 旁的選項按鈕。
3. 選擇 Restore (還原)。
4. 選擇 還原類型。

- 完整還原 會完整還原檔案系統，包括所有根層級的資料夾和檔案。

5. 針對 還原位置，選擇 Amazon EC2。
6. 在 執行個體類型 下拉式選單下，選擇新執行個體所需的運算和記憶體組合。

> **Note**
>
> 選擇具有符合或超過原始機器之運算和記憶體的執行個體；否則效能將受到影響。

7. 選取定義虛擬網路環境的 虛擬私有雲端 (VPC)。
8. 選取 子網路 群組。這是您虛擬私有雲端中的一系列 IP 地址，可用於將不同的 Amazon EC2 執行個體彼此隔離。
9. 指定確定執行個體流量的防火牆規則時所要使用的 安全群組。
10. 針對 還原角色，選取 預設角色 (建議) 或使用下拉式選單選擇 IAM 角色。
11. 選擇 Restore backup (還原備份)。

檢查您的還原任務何時具有 `Completed` 狀態。在左側導覽選單中，選擇 任務。

用 AWS CLI 於還原虛擬機器復原點

請使用 `StartRestoreJob`。

您可以為還原到 Amazon EC2 和 Amazon EBS 的虛擬機器指定下列中繼資料：

```
RestoreTo
InstanceType
VpcId
SubnetId
SecurityGroupIds
IamInstanceProfileName
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
Placement
CreditSpecification
RamdiskId
KernelId
UserData
EbsOptimized
```

```
LicenseSpecifications
KmsKeyId
AvailabilityZone
EbsVolumeType
IsEncrypted
ItemsToRestore
RequireIMDSv2
```

您可以為虛擬機器還原至 VMware、VMware 雲端和 AWS 前哨站上 AWS的 VMware 雲端指定下列中繼資料：

```
RestoreTo
HypervisorArn
VMName
VMPath
ComputeResourceName
VMDatastore
DisksToRestore
ItemsToRestore
```

此範例示範如何對 VMware 進行完整還原：

```
'{"RestoreTo":"VMware","HypervisorArn":"arn:aws:backup-gateway:us-
east-1:209870788375:hypervisor/hype-9B1AB1F1","VMName":"name","VMPath":"/Labster/
vm","ComputeResourceName":"Cluster","VMDatastore":"vsanDatastore","DisksToRestore":"[{\"DiskId
\":\"2000\",\"Label\":\"Hard disk 1\"}]","vmId":"vm-101"}'
```

若要還原至 Amazon EC2 執行個體，只需指定 `"RestoreTo":"EC2Instance"` 即可。系統將會預設所有其他屬性。

> **Note**
>
> 將虛擬機器還原 (或移轉) 至 EC2 需要授權。 AWS 預設會包含授權 (需支付費用)。如需詳細資訊，請參閱《Amazon EC2 VM Import/Export 使用者指南》中的《授權選項》。

還原 FSX 檔案系統

用於還原 Amazon FSx 檔案系統時可 AWS Backup 用的還原選項與使用原生 Amazon FSx 備份相同。您可以使用備份的復原點來建立新的檔案系統，並還原另一個檔案系統的 point-in-time 快照。

還原 Amazon FSx 檔案系統時，會 AWS Backup 建立新的檔案系統並將資料填入該檔案系統 (適用於 NetApp ONTAP 的 Amazon FSx 允許將磁碟區還原到現有檔案系統)。這類似於原生 Amazon FSx 備份和還原檔案系統的方式。將備份還原至新檔案系統所需的時間，會與建立新檔案系統所需的時間相同。從備份中還原的資料會延遲載入至檔案系統。因此，您可能會在過程中遇到稍高的延遲。

> **Note**
>
> 您無法還原至現有的 Amazon FSx 檔案系統，也無法還原個別檔案或資料夾。
> FSx for ONTAP 不支援備份某些磁碟區類型，包括 DP (資料保護) 磁碟區、LS (負載共享) 磁碟區、完整磁碟區或檔案系統上已滿的磁碟區。如需詳細資訊，請參閱《FSx for ONTAP 使用備份》。
> AWS Backup 包含 Amazon FSx 檔案系統復原點的儲存庫在外部可見。 AWS Backup您可以使用 Amazon FSx 還原復原點，但無法刪除復原點。

您可以從 AWS Backup 主控台查看內建 Amazon FSx 自動備份功能建立的備份。您也可以使用復原這些備份 AWS Backup。不過，您無法使 AWS Backup用刪除這些備份或變更 Amazon FSx 檔案系統的自動備份排程。

您可以還原 AWS Backup 使用 AWS Backup 主控台、API 或建立的備份 AWS CLI。本節說明如何使用 AWS Backup 主控台還原 Amazon FSx 檔案系統。

使用主 AWS Backup 控台還原 Amazon FSx 復原點

還原 FSx for Windows File Server 檔案系統

還原 FSx for Windows File Server 檔案系統

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 Amazon FSx 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。選擇資源的復原點 ID。
4. 在窗格的右上角，選擇 還原 以開啟 還原備份 頁面。
5. 在 檔案系統詳細資訊 區段中，您的備份 ID 會顯示在 備份 ID 下方，而檔案系統類型會顯示在 檔案系統類型 下方。您可以同時還原 FSx for Windows File Server 和 FSx for Lustre 檔案系統。
6. (選擇性) 輸入您的檔案系統名稱。
7. 針對 部署類型，接受預設值。您無法在還原期間變更檔案系統的部署類型。

8. 選擇要使用的 儲存類型。如果檔案系統的儲存容量低於 2,000 GiB，則無法使用 HDD 儲存類型。
9. 針對 輸送容量，選擇 建議的輸送容量 以使用建議的每秒 16 MB (Mbps) 速率，或選擇 指定輸送容量 並輸入新的速率。
10. 在 網路與安全 區段中，提供必要資訊。
11. 如果您正在還原 FSx for Windows File Server 檔案系統，請提供用於存取檔案系統的 Windows 身分驗證 資訊，您也可以建立新的身分驗證資訊。

    > **Note**
    >
    > 還原備份時，您無法變更檔案系統上的 Active Directory 類型。

    如需 Microsoft Active Directory 的詳細資訊，請參閱《Amazon FSx for Windows File Server 使用者指南》中的《在 FSx for Windows File Server 中使用 Active Directory》。
12. (選擇性) 在 備份與維護 區段中，提供資訊以設定您的備份偏好設定。
13. 在 還原角色 區段中，選擇 AWS Backup 代表您建立和管理備份時將使用的 IAM 角色。建議您選擇 預設角色。如果沒有預設角色，系統會為您建立一個具有正確許可的角色。您也可以提供自己的 IAM 角色。
14. 確認所有項目，然後選擇 還原備份。

還原 Amazon FSx for Lustre 檔案系統

AWS Backup 支援具有持續性儲存部署類型且未連結至 Amazon S3 等資料儲存庫的 Lustre 檔案系統的 Amazon FSx。

還原 Amazon FSx for Lustre 檔案系統

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 Amazon FSx 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。選擇資源的復原點 ID。
4. 在窗格的右上角，選擇 還原 以開啟 將備份還原至新的檔案系統 頁面。
5. 在 設定 區段中，您的備份 ID 會顯示在 備份 ID 下方，而檔案系統類型會顯示在 檔案系統類型 下方。檔案系統類型 應該是 Lustre。
6. (選擇性) 輸入您的檔案系統名稱。

7. 選擇部署類型。 AWS Backup 僅支援持續性部署類型。您無法在還原期間變更檔案系統的部署類型。

   持久性部署類型適用於長期儲存。如需 FSx for Lustre 部署選項的詳細資訊，請參閱《Amazon FSx for Lustre 使用者指南》中的《使用 Amazon FSx for Lustre 檔案系統可用的部署選項》。
8. 選擇您要使用的 每單位儲存輸送量。
9. 指定要使用的 儲存容量。輸入介於 32 GiB 到 64,436 GiB 之間的容量。
10. 在 網路與安全 區段中，提供必要資訊。
11. (選擇性) 在 備份與維護 區段中，提供資訊以設定您的備份偏好設定。
12. 在 還原角色 區段中，選擇 AWS Backup 代表您建立和管理備份時將使用的 IAM 角色。建議您選擇 預設角色。如果沒有預設角色，系統會為您建立一個具有正確許可的角色。您也可以提供 IAM 角色。
13. 確認所有項目，然後選擇 還原備份。

還原 ONTAP 磁碟 NetApp 區的 Amazon FSx

若要還原 NetApp ONTAP 磁碟區的 Amazon FSx：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 Amazon FSx 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。選擇資源的復原點 ID。
4. 在窗格的右上角，選擇 還原 以開啟 還原 頁面。

   第一個區段 檔案系統詳細資訊 會顯示復原點 ID、檔案系統 ID 和檔案系統類型。
5. 在 還原選項 下，有幾個選項。首先，從下拉式選單中選擇 檔案系統。
6. 接下來，從下拉式選單中選擇偏好的 儲存虛擬機器。
7. 輸入您的磁碟區名稱。
8. 指定 接合路徑，這是檔案系統內將掛載磁碟區的位置。
9. 指定您要建立的 磁碟區大小，以 MB 為單位。
10. (選擇性) 您可以勾選方塊來選擇 啟用儲存效率。這會允許重複資料刪除和壓縮。
11. 在 容量集區分層政策 下拉式選單中，選取分層偏好設定。
12. 在還原許可中，選擇 AWS Backup 將用於還原備份的 IAM 角色。

13. 確認所有項目，然後選擇 還原備份。

還原 Amazon FSx for OpenZFS 檔案系統

還原 FSx for OpenZFS 檔案系統

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 Amazon FSx 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。選擇資源的復原點 ID。
4. 在窗格的右上角，選擇 還原 以開啟 還原備份 頁面。

   在 檔案系統詳細資訊 區段中，您的備份 ID 會顯示在 備份 ID 下方，而檔案系統類型會顯示在 檔案系統類型 下方。檔案系統類型應該是 FSx for OpenZFS。
5. 在 還原選項 下，您可以選取 快速還原 或 標準還原。快速還原會使用來源檔案系統的預設設定。如果您正在進行快速還原，請跳至步驟 7。

   如果您選擇「標準還原」，請指定下列其他組態：

   a. 佈建的 SSD IOPS：您可以選擇 自動 選項按鈕，也可以選擇 使用者佈建 選項 (如果有的話)。

   b. 輸送容量：您可以選擇 建議的輸送容量 (64 MB/秒)，也可以選擇 指定輸送容量。

   c. (選擇性) VPC 安全群組：您可以指定要與檔案系統網路介面建立關聯的 VPC 安全群組。

   d. 加密金鑰：指定用來保護已還原檔案系統資料的 AWS Key Management Service 金鑰。

   e. (選擇性) 根磁碟區組態：預設會摺疊此組態。您可以按一下向下插入記號 (箭頭) 來展開。從備份建立檔案系統會建立新的檔案系統；磁碟區和快照會保留其來源組態。

   f. (選擇性) 備份與維護：若要設定排程備份，請按一下向下插入記號 (箭頭) 以展開區段。您可以選擇備份時段、小時和分鐘、保留期和每週維護時段。
6. (選擇性) 您可以輸入磁碟區名稱。
7. SSD 儲存容量 會顯示檔案系統的儲存容量。
8. 選擇可從中存取您檔案系統的 虛擬私有雲端 (VPC)。
9. 在 子網路 下拉式選單中，選擇您檔案系統網路介面所在的子網路。
10. 在 [還原角色] 區段中，選擇 AWS Backup 將用來代表您建立和管理備份的 IAM 角色。建議您選擇預設角色。如果沒有預設角色，系統會為您建立一個具有正確許可的角色。您也可以選擇 IAM 角色。

11. 確認所有項目，然後選擇 還原備份。

使用 AWS Backup API、CLI 或開發套件來還原 Amazon FSx 復原點

若要使用 API 或 CLI 還原 Amazon FSx，請使用 `StartRestoreJob`。您可以在任何 Amazon FSx 還原期間指定下列中繼資料：

```
FileSystemId
FileSystemType
StorageCapacity
StorageType
VpcId
KmsKeyId
SecurityGroupIds
SubnetIds
DeploymentType
WeeklyMaintenanceStartTime
DailyAutomaticBackupStartTime
AutomaticBackupRetentionDays
CopyTagsToBackups
WindowsConfiguration
LustreConfiguration
OntapConfiguration
OpenZFSConfiguration
aws:backup:request-id
```

FSx for Windows File Server 還原中繼資料

您可以在 FSx for Windows File Server 還原期間指定下列中繼資料：

- ThroughputCapacity
- PreferredSubnetId
- ActiveDirectoryId

FSx for Lustre 還原中繼資料

您可以在 FSx for Lustre 還原期間指定下列 `PerUnitStorageThroughput` 和 `DriveCacheType`。

FSx for ONTAP 還原中繼資料

您可以在 FSx for ONTAP 還原期間指定下列中繼資料：

- 要建立的磁碟區名稱 #name
- OntapConfiguration： # 點擊配置
- junctionPath
- sizeInMegabytes
- storageEfficiencyEnabled
- storageVirtualMachineId
- tieringPolicy

FSx for OpenZFS 還原中繼資料

您可以在 FSx for OpenZFS 還原期間指定下列中繼資料：

- ThroughputCapacity
- DesklopsConfiguration
- 如果指定 Iops if，您必須包含介於 0 到 160,000 之間的值，但不包含 Mode。

範例 CLI 還原命令：

```
aws backup start-restore-job --recovery-point-arn "arn:aws:fsx:us-west-2:1234:backup/
backup-1234" --iam-role-arn "arn:aws:iam::1234:role/Role" --resource-
type "FSx" --region us-west-2 --metadata 'SubnetIds="[\"subnet-1234\",
\"subnet-5678\"]",StorageType=HDD,SecurityGroupIds="[\"sg-bb5efdc4\",
\"sg-0faa52\"]",WindowsConfiguration="{\"DeploymentType\": \"MULTI_AZ_1\",
\"PreferredSubnetId\": \"subnet-1234\",\"ThroughputCapacity\": \"32\"}"'
```

範例還原中繼資料：

```
"restoreMetadata":  "{\"StorageType\":\"SSD\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:123456789012:key/123456a-123b-123c-defg-1h2i2345678\",\"StorageCapacity
\":\"1200\",\"VpcId\":\"vpc-0ab0979fa431ad326\",\"FileSystemType\":\"LUSTRE\",
\"LustreConfiguration\":\"{\\\"WeeklyMaintenanceStartTime\\\":\\\"4:10:30\\\",\\
\"DeploymentType\\\":\\\"PERSISTENT_1\\\",\\\"PerUnitStorageThroughput\\\":50,\\
\"CopyTagsToBackups\\\":true}\",\"FileSystemId\":\"fs-0ca11fb3d218a35c2\",\"SubnetIds
\":\"[\\\"subnet-0e66e94eb43235351\\\"]\"}"
```

還原 Amazon EBS 磁碟區

當您還原亞馬遜彈性區塊存放區 (Amazon EBS) 快照時， AWS Backup 會建立一個新的 Amazon EBS 磁碟區，您可以將其連接到 Amazon EC2 執行個體。

您可以選擇將快照還原為 EBS 磁碟區或 AWS Storage Gateway 磁碟區。

使用主 AWS Backup 控台還原 Amazon EBS 復原點

還原 Amazon EBS 磁碟區

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 EBS 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 指定資源的還原參數。您輸入的還原參數是您所選資源類型的特定參數。

   對於 [資源類型]，選擇還原此備份時要建立的 AWS 資源。
5. 如果您選擇 EBS volume (EBS 磁碟區)，請提供 Volume type (磁碟區類型)、Size(GiB) (大小 (GiB)) 的值，然後選擇 Availability zone (可用區域)。

   - 輸送量 之後有一個選用核取方塊 加密此磁碟區。如果 EBS 復原點已加密，此選項會保持作用中狀態。

     您可以指定 KMS 金鑰，也可以建立金 AWS KMS 鑰。

   如果您選擇 Storage Gateway 磁碟區，請選擇處於可連線狀態的閘道。同時選擇您的 iSCSI 目標名稱。

   - 針對 儲存的磁碟區 閘道，選擇 磁碟 ID。
   - 針對 快取的磁碟區 閘道，選擇至少與受保護的資源一樣大的容量。
6. 對於還原角色，請選擇 AWS Backup 將為此還原承擔的 IAM 角色。

   > **Note**
   >
   > 如果您的帳戶中沒有 AWS Backup 預設角色，系統會以正確的權限為您建立預設角色。您可以刪除此預設角色或使其無法使用。

7. 選擇 Restore backup (還原備份)。

   Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

還原封存的 EBS 快照會暫時將其從不常用儲存移至常用儲存，以建立新的 EBS 磁碟區。這類還原會產生一次性的擷取費用。在此還原期間，常用和不常用儲存的儲存成本都會計入費用。不常用儲存中的 EBS 磁碟區無法還原至備份閘道磁碟區。

您可以使用 AWS Backup 主控台或命令列，在不常用儲存中還原封存 EBS 快照。從不常用儲存還原最多可能需要 72 小時。如需詳細資訊，請參閱封存 Amazon EBS 快照。

Console

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 瀏覽至備份保存庫 > ### > 還原封存的 EBS 快照。
3. 在設定區段中，輸入 0 到 180 (含) 之間的值，以指定暫時還原封存快照的天數。
4. 輸入其他設定：磁碟區類型、大小、IOPS、可用區域、輸送量和加密。
5. 選擇還原角色。
6. 選取還原備份。在確認快顯視窗中，確認快照和還原類型。然後，選取還原快照。

AWS CLI

1. 使用 `start-restore-job`
2. 包含參數。
3.
4.
5.

使用 AWS Backup API、CLI 或開發套件來還原 Amazon EBS 復原點

若要使用 API 或 CLI 還原 Amazon EBS，請使用 `StartRestoreJob`。您可以在任何 Amazon EBS 還原期間指定下列中繼資料：

```
availabilityZone
```

```
volumeType
volumeSize
iops
throughput
temporaryRestoreDays
encrypted // if set to true, encryption will be enabled as volume is restored
kmsKeyId // if included, this key will be used to encrypt the restored volume instead
 of default KMS Key Id
aws:backup:request-id
```

範例：

```
"restoreMetadata": "{\"encrypted\":\"false\",\"volumeId\":\"vol-04cc95f3490b5ceea\",
\"availabilityZone\":null}"
```

還原 Amazon EFS 檔案系統

如果您要還原 Amazon Elastic File System (Amazon EFS) 執行個體，則可執行完整還原或項目層級還原。

完整還原

當您執行完整還原時，系統會還原整個檔案系統。

AWS Backup 不支援使用 Amazon EFS 進行破壞性還原。破壞性還原是指還原的檔案系統刪除或覆寫來源或現有檔案系統的情況。相反地， AWS Backup 會將您的檔案系統從根目錄還原至復原目錄。

項目層級還原

當您執行項目層級還原時，會還 AWS Backup 原特定的檔案或目錄。您必須指定與掛載點相關的相對路徑。例如，如果檔案系統是掛載到 `/user/home/myname/efs`，且檔案路徑為 `user/home/myname/efs/file1`，請輸入 **`/file1`**。路徑會區分大小寫。不支援萬用字元和 regex 字串。

當您使用主控台執行 EFS 還原時，最多可以選取 10 個項目。當您使用 CLI 進行還原時，則沒有項目限制；不過，可傳遞的還原中繼資料長度上限為 200 KB。

您可以將這些項目還原到新的或現有的檔案系統。無論如何， AWS Backup 都會從根目錄建立新的 Amazon EFS 目錄 (`aws-backup-restore_`*`datetime`*) 以包含這些項目。指定項目的完整階層會保留在復原目錄中。例如，如果目錄 A 包含子目錄 B、C 和 D，則 AWS Backup 會在復原 A、B、C 和 D 時保留階層結構。無論您是對現有檔案系統或新檔案系統執行 Amazon EFS 項目層級還原，每個還

原嘗試都會從根目錄建立一個新的復原目錄，以包含還原的檔案。如果您嘗試針對相同的路徑進行多次還原，則可能存在數個包含已還原項目的目錄。

> **Note**
>
> 如果您只保留一個每週備份，則只能還原至在備份時的檔案系統狀態。您無法還原至先前的增量備份。

使用主 AWS Backup 控台還原 Amazon EFS 復原點

還原 Amazon EFS 檔案系統

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 您的 EFS 備份保存庫會在建立時收到存取政策 Deny `backup:StartRestoreJob`。如果您是第一次還原備份保存庫，您必須依照下列方式變更存取政策。

   a. 選擇 Backup vaults (備份文件庫)。

   b. 選擇包含您要還原之復原點的備份保存庫。

   c. 向下捲動至保存庫的 存取政策

   d. 如果存在，請從 `Statement` 中刪除 `backup:StartRestoreJob`。您可以選擇 編輯，刪除 `backup:StartRestoreJob`，然後選擇 儲存政策 來執行這項操作。
3. 在導覽窗格中，選擇 受保護的資源 和您要還原的 EFS 檔案系統 ID。
4. 資源詳細資訊 頁面上會顯示所選檔案系統 ID 的復原點清單。若要還原檔案系統，請在 備份 窗格中，選擇檔案系統復原點 ID 旁的選項按鈕。在窗格右上角，選擇 Restore (還原)。
5. 指定您檔案系統的還原參數。您輸入的還原參數是您所選資源類型的特定參數。

   您可以執行還原 Full restore (完整還原)，將整個檔案系統的完整還原。或者，您可以使用 Item-level restore (項目層級還原) 來還原特定檔案和目錄。

   - 選擇 完整還原 選項，即可完整還原檔案系統，包括所有根層級的資料夾和檔案。
   - 選擇 Item-level restore (項目層級還原) 選項以還原特定檔案或目錄。您最多可以在 Amazon EFS 中選取並還原五個項目。

     若要還原特定檔案或目錄，您必須指定與掛載點相關的相對路徑。例如，如果檔案系統是掛載到 `/user/home/myname/efs`，且檔案路徑為 `user/home/myname/efs/file1`，請輸入 **`/file1`**。路徑區分大小寫，不能包含特殊字元、萬用字元和 regex 字串。

1. 在 Item path (項目路徑) 文字方塊中，輸入檔案或資料夾的路徑。
2. 選擇 Add item (新增項目) 以新增其他檔案或目錄。您最多可以在 EFS 檔案系統中選取並還原五個項目。

6. 對於 Restore location (還原位置)

   - 如果您要還原至來源檔案系統，請選擇 還原至來源檔案系統中的目錄。
   - 如果您要還原至不同的檔案系統，請選擇 還原至新的檔案系統。

7. 針對 檔案系統類型

   - (建議使用) 如果您要跨多個 AWS 可用區域還原檔案系統，請選擇 [地區]。
   - 如果您要將檔案系統還原至單一可用區域，請選擇 單區域。然後，在 可用區域 下拉式清單中，選擇您還原的目的地。

   如需詳細資訊，請參閱《Amazon EFS 使用者指南》中的《管理 Amazon EFS 儲存類別》。

8. 針對 效能

   - 如果您選擇執行區域性還原，請選擇 (建議) 一般用途 或 最大 I/O。
   - 如果您選擇執行單區域還原，則必須選擇 (建議) 一般用途。單區域還原不支援 最大 I/O。

9. 針對 啟用加密

   - 如果您要加密檔案系統，請選擇 Enable encryption (啟用加密)。使用 AWS Key Management Service (AWS KMS) 主控台建立 KMS 金鑰 ID 和別名後，它們就會出現在清單中。
   - 在 KMS 金鑰 文字方塊中，從清單中選擇您要使用的金鑰。

10. 對於還原角色，請選擇 AWS Backup 將為此還原承擔的 IAM 角色。

    > **Note**
    >
    > 如果您的帳戶中沒有 AWS Backup 預設角色，系統會以正確的權限為您建立預設角色。您可以刪除此預設角色或使其無法使用。

11. 選擇 Restore backup (還原備份)。

    Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

> **Note**
>
> 如果您只保留一個每週備份，則只能還原至在備份時的檔案系統狀態。您無法還原至先前的增量備份。

使用 AWS Backup API、CLI 或開發套件來還原 Amazon EFS 復原點

請使用 `StartRestoreJob`。還原 Amazon EFS 執行個體時，您可以還原整個檔案系統或是特定檔案或目錄。若要還原 Amazon EFS 資源，您需要下列資訊：

- `file-system-id`— 由備份的 Amazon EFS 檔案系統識別碼 AWS Backup。其會在 `GetRecoveryPointRestoreMetadata` 中傳回。
- `Encrypted` — 布林值，如果為 true，則表示檔案系統已經過加密。如果已指定 `KmsKeyId`，則請務必將 `Encrypted` 設為 `true`。
- `KmsKeyId`— 指定用來加密還原檔案系統的 AWS KMS 金鑰。
- `PerformanceMode` — 指定檔案系統的輸送量模式。
- `CreationToken` — 使用者提供的值，可確保請求的唯一性 (等冪性)。
- `newFileSystem` — 布林值，如果為 true，則表示復原點會還原至新的 Amazon EFS 檔案系統。
- `ItemsToRestore` — 最多五個字串的陣列，其中每個字串都是檔案路徑。使用 `ItemsToRestore` 來還原特定檔案或目錄，而不是整個檔案系統。此為選用參數。

您也可以包括 `aws:backup:request-id`。

如需 Amazon EFS 組態值的詳細資訊，請參閱create-file-system。

停用 Amazon EFS 中的自動備份

根據預設，Amazon EFS 會自動建立資料備份。這些備份在中表示為復原點 AWS Backup。嘗試移除復原點會導致錯誤訊息，指出權限不足以執行此動作。

最佳實務是保持啟用此自動備份。特別是在意外刪除資料的情況下，此備份可將檔案系統內容還原至上次建立復原點的日期。

在極少的情況下，若您希望關閉這些備份，則必須將存取政策從 `"Effect": "Deny"` 變更為 `"Effect": "Allow"`。如需開啟或關閉自動備份的詳細資訊，請參閱《Amazon EFS 使用者指南》。

還原 Amazon DynamoDB 資料表

使用主 AWS Backup 控台還原 DynamoDB 復原點

還原 DynamoDB 資料表

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 DynamoDB 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 Settings (設定) 中的 New table name (新表格名稱) 文字欄位中輸入新表格名稱。
5. 對於還原角色，請選擇 AWS Backup 將為此還原承擔的 IAM 角色。
6. 針對 加密設定：

   a. 如果您的備份是由 DynamoDB (其 ARN 開頭為`arn:aws:dyanmodb`) 管理，請使用擁有的金 AWS Backup 鑰加密還原的資料表。 AWS

      若要選擇不同的金鑰來加密還原的表格，您可以使用該 AWS Backup StartRestoreJob作業或從 DynamoDB 主控台執行還原。

   b. 如果您的備份支援完整 AWS Backup 管理 (ARN 開頭為`arn:aws:backup`)，您可以選擇下列任一加密選項來保護您還原的資料表：

      - (預設) DynamoDB 擁有的 KMS 金鑰 (加密無需支付額外費用)
      - DynamoDB 受管 KMS 金鑰 (需支付 KMS 費用)
      - 客戶自管 KMS 金鑰 (需支付 KMS 費用)

      「DynamoDB 擁有的」和「DynamoDB 受管」金鑰分別與「AWS擁有的」和「AWS受管」金鑰相同。如需釐清，請參閱《Amazon DynamoDB 開發人員指南》中的《靜態加密：如何運作》。

      如需完整 AWS Backup 管理的詳細資訊，請參閱進階 DynamoDB 備份。

> **Note**
>
> 下列指引僅適用於還原複製的備份，並想要使用您用於加密原始資料表的相同金鑰來加密還原資料表的情況。
> 還原跨區域備份時，若要使用您用來加密原始表格的相同金鑰來加密還原的資料表，您的金鑰必須是多區域金鑰。 AWS擁有和 AWS託管的密鑰不是多區域密鑰。若要進一步了解，請參閱《AWS Key Management Service 開發人員指南》中的《多區域金鑰》。
> 還原跨帳戶備份時，若要使用加密原始資料表時所用的相同金鑰來加密還原的資料表，您必須與目的地帳戶共用來源帳戶中的金鑰。 AWS帳戶之間無法共享擁有和 AWS託管的密鑰。若要進一步了解，請參閱《AWS Key Management Service 開發人員指南》中的《允許其他帳戶的使用者使用 KMS 金鑰》。

7. 選擇 Restore backup (還原備份)。

   Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

使用 AWS Backup API、CLI 或開發套件來還原 DynamoDB 復原點

請使用 `StartRestoreJob`。您可以在任何 DynamoDB 還原期間指定下列中繼資料。中繼資料不區分大小寫。

```
targetTableName
encryptionType
kmsMasterKeyArn
aws:backup:request-id
```

以下是 CLI 中 `StartRestoreJob` 操作的 `restoreMetadata` 引數範例：

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-east-1:123456789012:recovery-point:abcdef12-
g3hi-4567-8cjk-012345678901" \
--iam-role-arn "arn:aws:iam::123456789012:role/YourIamRole" \
--metadata
 'TargetTableName=TestRestoreTestTable,EncryptionType=KMS,KMSMasterKeyId=arn:aws:kms:us-
east-1:123456789012:key/abcdefg' \
--region us-east-1 \
--endpoint-url https://cell-1.gamma.us-east-1.controller.cryo.aws.a2z.com
```

上述範例會使用擁有的金鑰加密還原的 AWS資料表。使用 AWS擁有的金鑰指定加密的還原中繼資料部分為：`\"encryptionType\":\"Default\","kmsMasterKeyArn\":\"Not Applicable\"`。

若要使用 AWS-managed 金鑰加密還原的資料表，請指定下列還原中繼資料：`"encryptionType\":\"KMS\",\"keyArn\":\"Not Applicable\"`

若要使用客戶自管金鑰加密還原的資料表，請指定下列還原中繼資料：`"encryptionType\":\"KMS\",\"keyArn\":\"`*`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`*`\"`。

還原 RDS 資料庫

還原 Amazon RDS 資料庫需要指定多個還原選項。如需這些選項的詳細資訊，請參閱《Amazon RDS 使用者指南》中的《備份與還原 Amazon RDS 資料庫執行個體》。

使用主 AWS Backup 控台還原 Amazon RDS 復原點

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Amazon RDS 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 Instance specifications (執行個體規格) 窗格中，接受預設值或指定 DB engine (資料庫引擎)、License Model (授權模式)、DB instance class (資料庫執行個體類別)、Multi AZ (多個可用區) 和 Storage type (儲存類型) 設定的選項。例如，如果您想要待命資料庫執行個體，請指定 多可用區域。
5. 在 [設定] 窗格中，指定您在目前區域 AWS 帳戶 中擁有的所有資料庫執行個體和叢集的唯一名稱。資料庫執行個體識別符會區分大小寫，但全部以小寫形式儲存，如「`mydbinstance`」中所示。此為必要欄位。
6. 在 Network & Security (網路與安全) 窗格中，接受預設值或指定 Virtual Private Cloud (VPN) (虛擬私有雲端 (VPN))、Subnet group (子網路群組)、Public Accessibility (公用存取性) (通常為是) 和 Availability zone (可用區域) 設定的選項。
7. 在 Database options (資料庫選項) 窗格中，接受預設值或指定 Database port (資料庫連接埠)、DB parameter group (資料庫參數群組)、Option Group (選項群組)、Copy tags to snapshots (將標籤複製到快照) 和 IAM DB Authentication Enabled (啟用 IAM 資料庫身分驗證) 設定的選項。

8. 在 加密 窗格中，使用預設設定。如果快照的來源資料庫執行個體已加密，還原的資料庫執行個體也會加密。無法移除此加密。
9. 在「日誌匯出」窗格中，選擇要發佈到 Amazon CloudWatch 日誌的日誌類型。IAM role (IAM 角色) 已定義。
10. 在 Maintenance (維護) 窗格中，接受預設值或指定 Auto minor version upgrade (自動次要版本升級) 的選項。
11. 在 Restore role (還原角色) 窗格中，選擇 AWS Backup 在此次還原中具有的 IAM 角色。
12. 指定所有設定後，請選擇 Restore backup (還原備份)。

    Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

使用 AWS Backup API、CLI 或開發套件來還原 Amazon RDS 復原點

請使用 `StartRestoreJob`。如需有關已接受的中繼資料和值的資訊，請參閱《Amazon RDS API 參考》中的 `RestoreDBInstanceFromDBSnapshot`。此外， AWS Backup 接受下列僅供資訊使用的屬性。但是，包括這些屬性不會影響還原：

```
EngineVersion
KmsKeyId
Encrypted
vpcId
```

還原 Amazon Aurora 叢集

使用主 AWS Backup 控台還原 Aurora 復原點

AWS Backup 還原您的 Aurora 叢集；它不會建立 Amazon RDS 執行個體或將其連接到您的叢集。在下列步驟中，您將使用 CLI 建立 Amazon RDS 執行個體，並將其連接至還原的 Aurora 叢集。

還原 Aurora 叢集需要您指定多個還原選項。如需這些選項的資訊，請參閱《Amazon Aurora 使用者指南》中的《備份與還原 Aurora 資料庫叢集的概觀》。

還原 Amazon Aurora 叢集

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Aurora 資源 ID。

3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 Instance specifications (執行個體規格) 窗格 中，接受預設值或指定 DB engine (資料庫引擎)、DB engine version (資料庫引擎版本) 和 Capacity type (容量類型) 設定的選項。

   > **Note**
   >
   > 如果選取 Serverless (無伺服器) 容量類型，則會出現 Capacity settings (容量設定) 窗格。指定 Minimum Aurora capacity unit (最小 Aurora 容量單位) 和 Maximum Aurora capacity unit (最大 Aurora 容量單位) 設定的選項，或從 Additional scaling configuration (其他擴展組態) 區段中選擇不同的選項。

5. 在「設定」窗格中，為您 AWS 帳戶 在目前區域中擁有的所有資料庫叢集執行個體指定唯一的名稱。資料庫叢集識別符會區分大小寫，但全部以小寫形式儲存，如「`mydbclusterinstance`」中所示。此為必要欄位。
6. 在 網路與安全 窗格中，接受預設值，或指定 虛擬私有雲端 (VPC)、子網路群組 和 可用區域 設定的選項。
7. 在 Database options (資料庫選項) 窗格中，接受預設值或指定 Database port (資料庫連接埠)、DB cluster parameter group (資料庫叢集參數群組) 和 IAM DB Authentication Enabled (啟用 IAM 資料庫身分驗證) 設定的選項。
8. 在 Backup (備份) 窗格中，接受預設值，或指定 Copy tags to snapshots (將標籤複製到快照) 設定的選項。
9. 在 Backtrack (回溯) 窗格中，接受預設值，或指定 Enable Backtrack (啟用回溯) 或 Disable Backtrack (停用回溯) 設定的選項。
10. 在 Encryption (加密) 窗格中，接受預設值，或指定 Enable encryption (啟用加密) 或 Disable encryption (停用加密) 設定的選項。
11. 在「日誌匯出」窗格中，選擇要發佈到 Amazon CloudWatch 日誌的日誌類型。IAM role (IAM 角色) 已定義。
12. 在 Restore role (還原角色) 窗格中，選擇 AWS Backup 在此次還原中具有的 IAM 角色。
13. 指定所有設定之後，請選擇 Restore backup (還原備份)。

    Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。
14. 還原完成之後，請將還原的 Aurora 叢集連接至 Amazon RDS 執行個體。

    使用 AWS CLI：

- 若為 Linux、macOS 或 Unix：

```
aws rds create-db-instance --db-instance-identifier sample-instance \
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

- 針對 Windows：

```
aws rds create-db-instance --db-instance-identifier sample-instance ^
              --db-cluster-identifier sample-cluster --engine aurora-mysql --db-
instance-class db.r4.large
```

請參閱連續備份和 point-in-time 還原 (PITR)，以取得有關連續備份和還原至所選時間點的資訊。

使用 AWS Backup API、CLI 或 SDK 來還原 Aurora 復原點

請使用 StartRestoreJob。您可以在 Aurora 還原期間指定下列中繼資料：

```
List<String> availabilityZones;
Long backtrackWindow;
Boolean copyTagsToSnapshot;
String databaseName;
String dbClusterIdentifier;
String dbClusterParameterGroupName;
String dbSubnetGroupName;
List<String> enableCloudwatchLogsExports;
Boolean enableIAMDatabaseAuthentication;
String engine;
String engineMode;
String engineVersion;
String kmsKeyId;
Integer port;
String optionGroupName;
ScalingConfiguration scalingConfiguration;
List<String> vpcSecurityGroupIds;
```

範例：

```
"restoreMetadata":"{\"EngineVersion\":\"5.6.10a\",\"KmsKeyId\":\"arn:aws:kms:us-
east-1:234567890123:key/45678901-ab23-4567-8cd9-012d345e6f7\",\"EngineMode\":
```

\"serverless\",\"AvailabilityZones\":\"[\\\"us-east-1b\\\",\\\"us-east-1e\\\",\\
\"us-east-1c\\\"]\",\"Port\":\"3306\",\"DatabaseName\":\"\",\"DBSubnetGroupName\":
\"default-vpc-05a3b07cf6e193e1g\",\"VpcSecurityGroupIds\":\"[\\\"sg-012d52c68c6e88f00\
\\"]\",\"ScalingConfiguration\":\"{\\\"MinCapacity\\\":2,\\\"MaxCapacity\\\":64,
\\\"AutoPause\\\":true,\\\"SecondsUntilAutoPause\\\":300,\\\"TimeoutAction\\\":
\\\"RollbackCapacityChange\\\"}\",\"EnableIAMDatabaseAuthentication\":\"false\",
\"DBClusterParameterGroupName\":\"default.aurora5.6\",\"CopyTagsToSnapshot\":\"true\",
\"Engine\":\"aurora\",\"EnableCloudwatchLogsExports\":\"[]\"}"

還原 Amazon EC2 執行個體

使用主控台時，您可以透過 16 個選項執行還原。如果需要設定其他參數，您必須使用 CLI 或 SDK。

> **Note**
>
> AWS Backup 不會備份和還原啟動 Amazon EC2 執行個體時使用的使用者資料。

使用主 AWS Backup 控台還原 Amazon EC2 復原點

此為建議選項。

使用 AWS Backup 主控台還原 Amazon EC2 資源

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Amazon EC2 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 網路設定 窗格中，接受預設值，或指定 執行個體類型、虛擬私有雲端 (VPC)、子網路、安全群組 和 執行個體 IAM 角色設定的選項。
5. 在 [還原角色] 窗格中，接受 [預設角色] 或 [選擇 IAM 角色] 以指定 AWS Backup 將承擔此還原的 IAM 角色。
6. 在 進階設定 窗格中，接受預設值，或指定 關機行為、啟用終止保護、置放群組、T2/T3 無限制、租用 和 使用者資料 設定的選項。此區段可用來自訂關機和休眠行為、終止保護、置放群組、租用以及其他進階設定。
7. 指定所有設定之後，請選擇 Restore backup (還原備份)。

Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

主 AWS Backup 控台可讓您使用下列可自訂的參數和設定來還原 Amazon EC2 復原點：

- 執行個體類型
- Amazon VPC
- 子網路
- 安全群組
- IAM 角色
- 關機行為
- 停止休眠行為
- 終止保護
- T2/T3 無限制
- 配置群組名稱
- EBS 最佳化執行個體
- 租用
- RAM 磁碟 ID
- 核心 ID
- 使用者資料
- 終止時刪除

系統會預先填入這些參數來與原始備份比對。您可以在還原執行個體之前變更它們。 AWS Backup 識別具有可能無效或可能導致無效還原的值的參數。

使用恢復 Amazon EC2 AWS CLI

在命令行界面中，`start-restore-job`允許您使用多達 32 個參數進行還原（包括一些無法通過控制 AWS Backup 台自定義的參數）。

以下清單為您可以傳遞以還原 Amazon EC2 復原點的已接受中繼資料。

```
InstanceType
```

```
KeyName
VpcId
SubnetId
Architecture
EnaSupport
SecurityGroupIds
IamInstanceProfileName
CpuOptions
InstanceInitiatedShutdownBehavior
HibernationOptions
DisableApiTermination
CreditSpecification
Placement
RootDeviceType
RamdiskId
KernelId
UserData
Monitoring
NetworkInterfaces
ElasticGpuSpecification
CapacityReservationSpecification
InstanceMarketOptions
LicenseSpecifications
EbsOptimized
VirtualizationType
Platform
RequireIMDSv2
aws:backup:request-id
```

您也可以還原 Amazon EC2 執行個體，而不包含任何儲存的參數。您可以在 AWS Backup 主控台的受保護的資源 索引標籤上使用此選項。

> **Note**
>
> AWS Backup 將使用備份時使用的 SSH key pair 來自動執行還原。
> AWS Backup 不允許您修改實例配置文件。這是為了防止權限提升的可能性。如果您需要修改執行個體設定檔，請從 Amazon EC2 執行這項操作。

若要成功使用原始執行個體描述檔進行還原，您必須編輯還原政策。如果您在還原期間套用執行個體設定檔，則必須更新操作員角色，並將基礎執行個體設定檔角色的 `PassRole` 許可新增至 Amazon EC2。否則，Amazon EC2 無法授權執行個體啟動，並且會失敗。

在還原期間，適用所有 Amazon EC2 配額和組態限制。

還原 Storage Gateway 磁碟區

如果要還原 AWS Storage Gateway 磁碟區快照，可以選擇將快照還原為 Storage Gateway 磁碟區或 Amazon EBS 磁碟區。這是因為與這兩種服務 AWS Backup 整合，而且任何 Storage Gateway 快照都可以還原到 Storage Gateway 磁碟區或 Amazon EBS 磁碟區。

透過 AWS Backup 主控台還原 Storage Gateway

還原 Storage Gateway 磁碟區

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源，然後選擇您要還原的 Storage Gateway 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 指定資源的還原參數。您輸入的還原參數是您所選資源類型的特定參數。

   對於 [資源類型]，選擇還原此備份時要建立的 AWS 資源。
5. 如果您選擇 Storage Gateway 磁碟區，請選擇處於可連線狀態的閘道。同時選擇您的 iSCSI 目標名稱。

   1. 針對「儲存的磁碟區」閘道，選擇 磁碟 ID。
   2. 針對「快取的磁碟區」閘道，選擇至少與受保護的資源一樣大的容量。

   如果您選擇 EBS volume (EBS 磁碟區)，請提供 Volume type (磁碟區類型)、Size(GiB) (大小 (GiB)) 的值，然後選擇 Availability zone (可用區域)。
6. 對於還原角色，請選擇 AWS Backup 將為此還原承擔的 IAM 角色。

   > **Note**
   >
   > 如果您的帳戶中沒有 AWS Backup 預設角色，系統會以正確的權限為您建立預設角色。您可以刪除此預設角色或使其無法使用。
7. 選擇 Restore backup (還原備份)。

   Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

使用還原 Storage Gateway AWS CLI

在命令列介面中，`start-restore-job` 可讓您還原 Storage Gateway 磁碟區。

下列清單是接受的中繼資料。

```
gatewayArn // The Amazon Resource Name (ARN) of the gateway. Use the ListGateways
 operation to return a list of gateways for your account and AWS ##.
gatewayType // The type of created gateway. Valid value is BACKUP_VM
targetName
kmsKey
volumeSize
volumeSizeInBytes
diskId
```

還原 Amazon Timestream 資料表

當您還原 Amazon Timestream 資料表時，有幾個選項可供設定，包括新資料表名稱、目的地資料庫、您的儲存配置偏好設定 (記憶體和磁性儲存)，以及您用於完成還原任務的角色。您也可以選擇 Amazon S3 儲存貯體來儲存錯誤日誌。磁性儲存寫入是非同步的，因此您可能想要記錄錯誤。

Timestream 資料儲存有兩個層級：記憶體存放區和磁性存放區。記憶體存放區是必要項目，但您可以選擇在指定的記憶體時間結束之後，將還原的資料表傳輸至磁性存放區。記憶體存放區已針對高輸送量資料寫入和快速 point-in-time 查詢進行最佳化 磁性存放區已針對較低輸送量延遲抵達資料寫入、長期資料儲存和快速分析查詢優化。

當您還原 Timestream 資料表時，您可以確定資料表在每個儲存層中保留多久。使用控制台或 API，您可以設定兩者的儲存時間。請注意，儲存是線性且循序的。Timestream 會先將還原的資料表儲存在記憶體儲存中，然後在達到記憶體儲存時間時，自動將其轉換至磁性儲存。

> **Note**
>
> 磁性存放區保留期必須等於或大於原始保留期 (顯示在主控台的右上方)，否則資料將會遺失。

範例：您將記憶體存放區配置設定為保留資料一週，並將磁性存放區配置設定為保留相同資料一年。當記憶體存放區中的資料經過一週時，就會自動移至磁性存放區。然後會在磁性存放區中保留一年。該時間結束時，就會從 Timestream 和 AWS Backup中刪除。

使用主控台還原 Amazon Timestream 表格 AWS Backup

您可以在由 AWS Backup建立的 AWS Backup 主控台中還原「時間流」表格。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Amazon Timestream 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 指定您的新資料表組態設定，包括：
   a. 新資料表名稱，由 2 到 256 個字元 (字母、數字、連字號、句號和底線) 組成。
   b. 目的地資料庫，請從下拉式選單中選擇。
5. 儲存配置：設定還原的資料表最初在記憶體儲存中的時間，並設定還原的資料表接著在磁性儲存中的時間。記憶體儲存可設定為數小時、數天、數週或數月。磁性儲存可設定為數天、數週、數月或數年。
6. (選擇性) 啟用磁性儲存寫入：您可以選擇允許磁性儲存寫入。勾選此選項時，延遲抵達的資料 (時間戳記超出記憶體儲存保留期的資料) 將直接寫入至磁性存放區中。
7. (選擇性) Amazon S3 錯誤日誌位置：您可以指定儲存錯誤日誌的 S3 位置。瀏覽您的 S3 檔案，或複製並貼上 S3 檔案路徑。

   > **Note**
   >
   > 如果您選擇指定 S3 錯誤日誌位置，則用於此還原的角色必須具有寫入至 S3 儲存貯體的許可，或必須包含具有該許可的政策。

8. 選擇要傳遞以執行還原的 IAM 角色。您可以使用預設 IAM 角色或指定其他角色。
9. 按一下 還原備份。

您的還原任務會顯示在受保護的資源下方。您可以按一下「重新整理」按鈕或 CTRL-R 來查看還原任務的目前狀態。

使用 API、CLI 或 SDK 還原 Amazon Timestream 資料表

使用 `StartRestoreJob` 透過 API 還原 Timestream 資料表。

若要使用還原時間流 AWS CLI，請使用作業`start-restore-job.`並指定下列中繼資料：

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
aws:backup:request-id
```

以下是範例範本：

```
aws backup start-restore-job \
--recovery-point-arn "arn:aws:backup:us-west-2:accountnumber:recovery-point:1a2b3cde-
f405-6789-012g-3456hi789012_beta" \
--iam-role-arn "arn:aws:iam::accountnumber:role/rolename" \
--metadata
 'TableName=tablename,DatabaseName=databasename,MagneticStoreRetentionPeriodInDays=1,MemoryStor
\":true,\"MagneticStoreRejectedDataLocation\":{\"S3Configuration\":{\"BucketName\":
\"bucketname\",\"EncryptionOption\":\"SSE_S3\"}}}"' \
--region us-west-2 \
--endpoint-url url
```

您也可以使用 DescribeRestoreJob 來協助取得還原資訊。

在中 AWS CLI，使用作業describe-restore-job並使用下列中繼資料：

```
TableName: string;
DestinationDatabase: string;
MemoryStoreRetentionPeriodInHours: value: number unit: 'hours' | 'days' | 'weeks' |
 'months'
MagneticStoreRetentionPeriodInDays: value: number unit: 'days' | 'weeks' | 'months' |
 'years'
EnableMagneticStoreWrites?: boolean;
```

以下是範例範本：

```
aws backup describe-restore-job \
--restore-job-id restore job ID \
--region awsregion \
--endpoint-url url
```

還原 Amazon Redshift 叢集

您可以在 AWS Backup 主控台或透過 CLI 還原自動和手動快照。

當您還原 Amazon Redshift 叢集時，預設會將原始叢集設定輸入至主控台中。您可以為下列組態指定不同的設定。還原資料表時，您必須指定來源和目標資料庫。如需這些組態的詳細資訊，請參閱《Amazon Redshift 管理指南》中的《從快照還原叢集》。

- 單一資料表或叢集：您可以選擇還原整個叢集或單一資料表。如果您選擇還原單一資料表，則需要來源資料庫、來源結構描述和來源資料表名稱，以及目標叢集、結構描述和新資料表名稱。
- 節點類型：每個 Amazon Redshift 叢集都包含一個領導節點和至少一個運算節點。當您還原叢集時，需要指定符合您 CPU、RAM、儲存容量和磁碟機類型要求的節點類型。
- 節點數量：還原叢集時，您需要指定所需的節點數量。
- 組態摘要
- 叢集許可

使用主控台還原 Amazon Redshift 叢集或表格 AWS Backup

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 設定 和您要還原的 Amazon Redshift 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在復原點 窗格中，選擇資源復原點 ID 旁的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 還原選項

    a. 從快照還原叢集，或

    b. 將快照中的單一資料表還原至新叢集。如果您選擇此選項，則必須設定下列項目：

        i. 開啟或關閉「區分大小寫的名稱」。

        ii. 輸入來源資料表值，包括資料庫、結構描述和資料表。您可以在 Amazon Redshift 主控台中找到來源資料表資訊。

        iii. 輸入目標資料表值，包括資料庫、結構描述和新資料表名稱。
5. 指定您的新叢集組態設定。

    a. 針對叢集還原：選擇「叢集識別符」、「節點類型」和「節點數量」。

    b. 指定可用區域和維護時段。

    c. 您可以按一下 關聯 IAM 角色 來關聯其他角色。

6. 選擇性：其他組態：
   a. 預設會開啟 使用預設值。
   b. 使用下拉式選單選取「網路與安全」、「VPC 安全群組」、「叢集子網路群組」和「可用區域」的設定。
   c. 開啟或關閉 增強型 VPC 路由。
   d. 確定是否要讓叢集端點可公開存取。如果是，則 VPC 外部的執行個體和裝置可以透過叢集端點連線至您的資料庫。如果開啟此選項，請輸入彈性 IP 地址。
7. 選擇性：資料庫組態。您可以選擇輸入
   a. 資料庫連接埠 (透過在文字欄位中輸入)
   b. 參數群組
8. 維護：您可以選擇
   a. Maintenance window (維護時段)
   b. 維護追蹤 (包括目前、追蹤或預覽)。這可控制在維護時段內套用的叢集版本。
9. 自動快照已設定為預設值。
   a. 自動快照保留期。保留期必須為 0 到 35 天。選擇 0 表示不會建立自動快照。
   b. 手動快照保留期為 1 到 3653 天。
   c. 叢集重新放置有一個選用核取方塊。如果勾選此核取方塊，則允許將您的叢集重新放置在其他可用區域中。啟用重新放置之後，即可使用 VPC 端點。
10. 監控：還原叢集之後，您可以透過 CloudWatch 或透過 Amazon Redshift 設定監控。
11. 選擇要傳遞以執行還原的 IAM 角色。您可以使用預設角色，也可以指定其他角色。

您的還原任務會顯示在 任務 下方。您可以按一下「重新整理」按鈕或 CTRL-R 來查看還原任務的目前狀態。

使用 API、CLI 或 SDK 還原 Amazon Redshift 叢集

使用 `StartRestoreJob` 還原 Amazon Redshift 叢集。

若要使用還原 Amazon Redshift AWS CLI，請使用命令`start-restore-job`並指定下列中繼資料：

```
ClusterIdentifier // required string
AdditionalInfo // optional string
AllowVersionUpgrade // optional Boolean
```

```
AquaConfigurationStatus // optional string
AutomatedSnapshotRetentionPeriod // optional integer 0 to 35
AvailabilityZone // optional string
AvailabilityZoneRelocation // optional Boolean
ClusterParameterGroupName // optional string
ClusterSecurityGroups // optional array of strings
ClusterSubnetGroupName // optional strings
DefaultIamRoleArn // optional string
ElasticIp // optional string
Encrypted // Optional TRUE or FALSE
EnhancedVpcRouting // optional Boolean
HsmClientCertificateIdentifier // optional string
HsmConfigurationIdentifier // optional string
IamRoles // optional array of strings
KmsKeyId // optional string
MaintenanceTrackName // optional string

ManualSnapshotRetentionPeriod // optional integer

NodeType // optional string
NumberOfNodes // optional integer
OwnerAccount // optional string
Port // optional integer
PreferredMaintenanceWindow // optional string
PubliclyAccessible // optional Boolean
ReservedNodeId // optional string
SnapshotClusterIdentifier // optional string
SnapshotScheduleIdentifier // optional string
TargetReservedNodeOfferingId // optional string
VpcSecurityGroupIds // optional array of strings
RestoreType // CLUSTER_RESTORE  or TABLE_RESTORE
```

如需詳細資訊，請參閱《Amazon Redshift API 參考》中的 RestoreFromClusterSnapshot 和《AWS CLI 指南》中的 restore-from-cluster-snapshot。

以下是範例範本：

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:backup:region:account:snapshot:name
-\-iam-role-arn "arn:aws:iam:account:role/role-name" \
-\-metadata
-\-resource-type Redshift \
-\-region AWS ##
```

```
-\-endpoint-url URL
```

請見此處範例：

```
aws backup start-restore-job \
-\-recovery-point-arn "arn:aws:redshift:us-west-2:123456789012:snapshot:redshift-
cluster-1/awsbackup:job-c40dda3c-fdcc-b1ba-fa56-234d23209a40" \
-\-iam-role-arn "arn:aws:iam::974288443796:role/Backup-Redshift-Role" \
-\-metadata 'RestoreType=CLUSTER_RESTORE,ClusterIdentifier=redshift-cluster-
restore-78,Encrypted=true,KmsKeyId=45e261e4-075a-46c7-9261-dfb91e1c739c' \
-\-resource-type Redshift \
-\-region us-west-2 \
```

您也可以使用 DescribeRestoreJob 來協助取得還原資訊。

在中 AWS CLI，使用作業describe-restore-job並使用下列中繼資料：

```
Region
```

以下是範例範本：

```
aws backup describe-restore-job –restore-job-id restore job ID
-\-region AWS ##
```

請見此處範例：

```
aws backup describe-restore-job -\-restore-job-id BEA3B353-576C-22C0-9E99-09632F262620
 \
-\-region us-west-2 \
```

還原 Amazon EC2 執行個體上的 SAP HANA 資料庫

EC2 執行個體上的 SAP HANA 資料庫可以使用 AWS Backup 主控台、API 或使用來還原 AWS CLI。

主題

- 使用 AWS Backup 主控台在 Amazon EC2 執行個體資料庫上還原 SAP HANA
- StartRestoreJob 適用於 EC2 上的 API
- 適用於 EC2 上 SAP HANA 的 CLI

- 故障診斷

使用 AWS Backup 主控台在 Amazon EC2 執行個體資料庫上還原 SAP HANA

請注意，您無法對相同的資料庫同時進行備份任務和還原任務。進行 SAP HANA 資料庫還原任務時，嘗試備份相同的資料庫可能會導致錯誤：「資料庫在停止時無法備份」。

1. 使用先決條件中的認證存取 AWS Backup 主控台。
2. 在 目標還原位置 下拉式選單下，選擇一個資料庫，以使用您要用於還原的復原點覆寫 (請注意，託管還原目標資料庫的執行個體也必須具有先決條件中的許可)。

   > **Important**
   >
   > SAP HANA 資料庫還原是破壞性的。還原資料庫會覆寫位於指定目標還原位置的資料庫。

3. 只有在執行系統複製還原時才完成此步驟；否則，請跳至步驟 4。

   系統複製還原是一種還原任務，其中還原目標資料庫與產生復原點的來源資料庫不同。若要進行系統複製還原，請注意控制台上提供給您的 `aws ssm-sap put-resource-permission` 命令。必須複製此命令，並貼到已完成先決條件的機器上加以執行。執行命令時，請使用您設定註冊應用程式所需的許可先決條件中的角色憑證。

   ```
   // Example command
   aws ssm-sap put-resource-permission \
   --region us-east-1 \
   --action-type RESTORE \
   --source-resource-arn arn:aws:ssm-sap-east-1:112233445566:HANA/Foo/DB/HDB \
   --resource-arn arn:aws:ssm-sap:us-east-1:112233445566:HANA/Bar/DB/HDB
   ```

4. 選擇還原位置之後，即可看到目標資料庫的 資源 ID、應用程式名稱、資料庫類型 和 EC2 執行個體。
5. (選擇性) 您可以開啟 進階還原設定 來變更目錄還原選項。預設選項是從 AWS Backup中還原最新目錄。
6. 按一下 還原備份。
7. 目標位置將在還原期間遭到覆寫 (「破壞性還原」)，因此您必須在下一個快顯對話方塊中提供允許這項操作的確認。

   a. 若要繼續，您必須了解現有資料庫將遭到所要還原的資料庫覆寫。

b. 了解這點之後，您必須確認現有資料將遭到覆寫。若要確認這點並繼續進行，請在文字輸入欄位中輸入 overwrite。

8. 按一下 還原備份。

如果程序成功，主控台頂端會出現藍色橫幅。這表示還原任務正在進行中。系統會自動將您重新導向至「任務」頁面，其中您的還原任務會顯示在還原任務清單中。這個最近任務的狀態為 Pending。您也可以搜尋，然後按一下還原任務 ID，來查看每個還原任務的詳細資訊。您可以按一下「重新整理」按鈕來重新整理還原任務清單，以檢視還原任務狀態的變更。

StartRestoreJob 適用於 EC2 上的 API

此動作可復原 Amazon Resource Name (ARN) 所識別的已儲存資源。

請求語法

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json
{
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 請求參數：該請求不會使用任何 URI 參數。

請求內文：該請求接受 JSON 格式的以下資料。

IdempotencyToken客戶選擇的字串，可用來區分相同的呼叫。StartRestoreJob重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

中繼資料

一組中繼資料鍵值對。包含還原復原點所需的資訊，例如資源名稱。您可以在備份資源時，透過呼叫 GetRecoveryPointRestoreMetadata 取得有關資源的組態中繼資料。但是，除了

GetRecoveryPointRestoreMetadata 提供的值之外，還可能需要還原資源。例如，如果原始資源已存在，您可能需要提供新資源名稱。

您需要包含特定中繼資料，才能還原 Amazon EC2 執行個體上的 SAP HANA。請參閱 SAP Hana 特定項目的 StartRestoreJob 中繼資料。

若要擷取相關的中繼資料，您可以使用呼叫 GetRecoveryPointRestoreMetadata。

標準 SAP HANA 資料庫復原點的範例：

```
"RestoreMetadata": {
        "BackupSize": "1660948480",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "SYSTEM",
        "HanaBackupEndTime": "1674838362",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_SYSTEMDB_FULL",
        "HanaBackupStartTime": "1674838349",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/DATABASENAME",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9c"
    }
```

連續 SAP HANA 資料庫復原點的範例：

```
"RestoreMetadata": {
        "AvailableRestoreBases":
 "[1234567890123,9876543210987,1472583691472,7418529637418,1678942598761]",
        "BackupSize": "1711284224",
        "DatabaseName": "DATABASENAME",
        "DatabaseType": "TENANT",
        "EarliestRestorablePitrTimestamp": "1674764799789",
        "HanaBackupEndTime": "1668032687",
        "HanaBackupId": "1234567890123",
        "HanaBackupPrefix": "1234567890123_HDB_FULL",
        "HanaBackupStartTime": "1668032667",
        "HanaVersion": "2.00.040.00.1553674765",
        "IsCompressedBySap": "FALSE",
        "IsEncryptedBySap": "FALSE",
```

```
        "LatestRestorablePitrTimestamp": "1674850299789",
        "SourceDatabaseArn": "arn:aws:ssm-sap:region:accountID:HANA/applicationID/
DB/SystemDatabaseSid",
        "SystemDatabaseSid": "HDB",
        "aws:backup:request-id": "46bbtt4q-7unr-2897-m486-yn378k2mrw9d"
    }
```

適用於 EC2 上 SAP HANA 的 CLI

命令 `start-restore-job` 可復原 Amazon Resource Name (ARN) 所識別的已儲存資源。CLI 將遵循上述 API 指導方針。

概要：

```
start-restore-job
--recovery-point-arn value
--metadata value
--aws:backup:request-id value
[--idempotency-token value]
[--resource-type value]
[--cli-input-json value]
[--generate-cli-skeleton value]
[--debug]
[--endpoint-url value]
[--no-verify-ssl]
[--no-paginate]
[--output value]
[--query value]
[--profile value]
[--region value]
[--version value]
[--color value]
[--no-sign-request]
[--ca-bundle value]
[--cli-read-timeout value]
[--cli-connect-timeout value]
```

選項

`--recovery-point-arn` (字串) 是 Amazon Resource Name (ARN) 形式的字串，可唯一識別復原點；例如 `arn:aws:backup:region:123456789012:recovery-point:46bbtt4q-7unr-2897-m486-yn378k2mrw9d`

--metadata (映射)：一組中繼資料鍵值對。包含還原復原點所需的資訊，例如資源名稱。您可以在備份資源時，透過呼叫 GetRecoveryPointRestoreMetadata 取得有關資源的組態中繼資料。不過，除了 GetRecoveryPointRestoreMetadata 提供的值之外，還可能需要還原資源。您需要指定特定中繼資料，才能還原 Amazon EC2 執行個體上的 SAP HANA：

- aws:backup:request-id：這是用於等冪性的任何 UUID 字串。不會以任何方式改變您的還原體驗。
- aws:backup:TargetDatabaseArn：指定您要還原的目標資料庫。這是 Amazon EC2 上的 SAP HANA 資料庫 ARN。
- CatalogRestoreOption：指定您要還原目錄的來源位置。可以是 NO_CATALOG、LATEST_CATALOG_FROM_AWS_BACKUP、CATALOG_FROM_LOCAL_PATH 的其中之一
- LocalCatalogPath：如果 CatalogRestoreOption 中繼資料值為CATALOG_FROM_LOCAL_PATH，則指定 EC2 執行個體上本機目錄的路徑。這應該是 EC2 執行個體中的有效檔案路徑。
- RecoveryType：目前支援 FULL_DATA_BACKUP_RECOVERY、POINT_IN_TIME_RECOVERY 和 MOST_RECENT_TIME_RECOVERY 復原類型。

鍵 = (字串)；值 = (字串)。速記語法：

```
KeyName1=string,KeyName2=string
```

JSON 語法：

```
{"string": "string"
  ...}
```

--idempotency-token 是使用者所選擇的字串，可用來區分在其他方面相同的 StartRestoreJob 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

--resource-type 是一個字串，可啟動任務以還原下列其中一個資源的復原點：適用於 Amazon EC2 上 SAP HANA 的 SAP HANA on Amazon EC2。(選擇性) SAP HANA 資源可使用命令 aws ssm-sap tag-resource 進行標記

輸出：RestoreJobId 是一個字串，可唯一識別還原復原點的任務。

故障診斷

如果在嘗試進行備份操作時發生下列任何錯誤，請參閱相關的解決方法。

- 錯誤：連續備份日誌錯誤

  為了維護連續備份的復原點，SAP HANA 會為所有變更建立日誌。當日誌無法使用時，每個連續復原點的狀態都會是 STOPPED。可用來還原的最後一個可行復原點具有 AVAILABLE 狀態。如果在狀態為 STOPPED 的復原點與狀態為 AVAILABLE 的復原點時間間隔內遺失日誌資料，則無法保證這些時間還原成功。如果您輸入的日期和時間在此範圍內， AWS Backup 將嘗試備份，但會使用最接近的可還原時間。此錯誤會顯示訊息 “Encountered an issue with log backups. Please check SAP HANA for details."

  解決方法：在主控台中，會根據日誌顯示最近的可還原時間。您可以輸入比所顯示時間更近的時間。但是，如果記錄檔中無法使用此時間的資料， AWS Backup 將會使用最近的可還原時間。

- 錯誤：Internal error

  解決方法：從主控台建立支援案例，或 AWS Support 聯絡還原詳細資料，例如還原工作 ID。

- 錯誤：The provided role arn:aws:iam::*ACCOUNT_ID*:role/ServiceLinkedRole cannot be assumed by AWS Backup

  解決方法：確定呼叫還原時所扮演的角色具有建立服務連結角色的必要許可。

- 錯誤：User: arn:aws:sts::*ACCOUNT_ID*:assumed-role/ServiceLinkedRole/AWSBackup-ServiceLinkedRole is not authorized to perform: ssm-sap:GetOperation on resource: arn:aws:ssm-sap:us-east-1:*ACCOUNT_ID*:...

  解決方法：確定已正確輸入呼叫必要條件中所述的還原許可時所扮演的角色。

- 錯誤：b* 449: recovery strategy could not be determined: [111014] The backup with backup id '1660627536506' cannot be used for recovery SQLSTATE: HY000\n

  解決方法：確定已正確安裝 Backint Agent。檢查所有必要條件，特別是 SAP 應 AWS Systems Manager 用程式伺服器上的安裝 AWS BackInt 代理程式和 SAP，然後重新嘗試安裝 BackInt 代理程式。

- 錯誤：IllegalArgumentException: Restore job provided is not ready to return chunks, current restore job status is: CANCELLED

  解決方法：還原任務已由服務任務流程取消。請重試還原任務。

- 錯誤：RequestError: send request failed\ncaused by: read tcp 10.0.131.4:40482->35.84.99.47:443: read: connection timed out"

解決方法：執行個體上發生暫時性網路不穩定。請重試還原。如果此問題持續發生，請嘗試將 `ForceRetry: "true"` 新增至位於 `/hana/shared/aws-backint-agent/aws-backint-agent-config.yaml.` 的代理程式組態檔案

如需任何其他 AWS Backint Agent 相關問題，請參閱疑難排解 SAP HANA 的 AWS Backint 代理程式。

還原 DocumentDB 叢集

使用主 AWS Backup 控台還原 Amazon DocumentDB 復原點

還原 Amazon DocumentDB 叢集需要您指定多個還原選項。如需這些選項的資訊，請參閱《Amazon DocumentDB 開發人員指南》中的《從叢集快照還原》。

還原 Amazon DocumentDB 叢集

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Amazon DocumentDB 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 組態 窗格中，接受預設值，或指定 叢集識別符、引擎版本、執行個體類別 和 執行個體數量 的選項。

   - 注意：如果還原時預設 VPC 不存在，則必須在另一個 VPC 中指定子網路。
5. 在 網路與安全 窗格中，「無偏好設定」會隨即顯示。
6. 在 E ncryption-at-rest 窗格中，接受預設值或指定 [啟用加密] 或 [停用加密設定] 的選項。
7. 在 叢集選項 窗格中，輸入 連接埠，然後選擇 叢集參數群組。
8. 在 [Backup] 窗格中，選擇 [持續備份以進行 point-in-time 復原 (PITR)]、[排程快照備份] 或兩者。
9. 在「日誌匯出」窗格中，選擇要發佈到 Amazon CloudWatch 日誌的日誌類型。IAM role (IAM 角色) 已定義。
10. 在 維護 窗格中，指定維護時段，或選擇 無偏好設定。
11. 在 標籤 窗格中，您可以選擇 新增標籤。
12. 在 刪除保護 窗格中，您可以選擇 啟用刪除保護。
13. 指定所有設定之後，請選擇 Restore backup (還原備份)。

Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。

14. 還原完成之後，請將還原的 Amazon DocumentDB 叢集連接至 Amazon RDS 執行個體。

使用 AWS Backup API、CLI 或開發套件來還原 Amazon DocumentDB 復原點

請先還原叢集。請使用 StartRestoreJob。您可以在 Amazon DocumentDB 還原期間指定下列中繼資料：

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

然後使用 `create-db-instance` 將還原的 Amazon DocumentDB 叢集連接至 Amazon RDS 執行個體。

- 若為 Linux、macOS 或 Unix：

```
aws docdb create-db-instance --db-instance-identifier sample-instance /
                  --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

- 針對 Windows：

```
aws docdb create-db-instance --db-instance-identifier sample-instance ^
```

```
                --db-cluster-identifier sample-cluster --engine docdb --db-
instance-class db.r5.large
```

還原 Neptune 叢集

使用主 AWS Backup 控台還原 Amazon Neptune 復原點

還原 Amazon Neptune 資料庫需要您指定多個還原選項。如需這些選項的資訊，請參閱《Neptune 使用者指南》中的《從資料庫叢集快照還原》。

還原 Neptune 資料庫

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 受保護的資源 和您要還原的 Neptune 資源 ID。
3. Resource details (資源詳細資訊) 頁面上會顯示所選資源 ID 的復原點清單。若要還原資源，請在 Backups (備份) 窗格中，選擇資源復原點 ID 旁邊的選項按鈕。在窗格右上角，選擇 Restore (還原)。
4. 在 執行個體規格 窗格中，接受預設值，或指定 資料庫引擎 和 版本。
5. 在「設定」窗格中，為您 AWS 帳戶 在目前區域中擁有的所有資料庫叢集執行個體指定唯一的名稱。資料庫叢集識別符會區分大小寫，但全部以小寫形式儲存，如「mydbclusterinstance」中所示。此為必要欄位。
6. 在 資料庫選項 窗格中，接受預設值，或指定 資料庫連接埠 和 資料庫叢集參數群組 的選項。
7. 在 Encryption (加密) 窗格中，接受預設值，或指定 Enable encryption (啟用加密) 或 Disable encryption (停用加密) 設定的選項。
8. 在「日誌匯出」窗格中，選擇要發佈到 Amazon CloudWatch 日誌的日誌類型。IAM role (IAM 角色) 已定義。
9. 在 Restore role (還原角色) 窗格中，選擇 AWS Backup 在此次還原中具有的 IAM 角色。
10. 指定所有設定之後，請選擇 Restore backup (還原備份)。

    Restore jobs (還原任務) 窗格隨即出現。頁面頂端的訊息提供還原任務的相關資訊。
11. 還原完成之後，請將還原的 Neptune 叢集連接至 Amazon RDS 執行個體。

使用 AWS Backup API、CLI 或 SDK 來還原 Neptune 復原點

請先還原叢集。請使用 StartRestoreJob。您可以在 Amazon DocumentDB 還原期間指定下列中繼資料：

```
availabilityZones
backtrackWindow
copyTagsToSnapshot // Boolean
databaseName // string
dbClusterIdentifier // string
dbClusterParameterGroupName // string
dbSubnetGroupName // string
enableCloudwatchLogsExports // string
enableIAMDatabaseAuthentication // Boolean
engine // string
engineMode // string
engineVersion // string
kmsKeyId // string
port // integer
optionGroupName // string
ScalingConfiguration
pcSecurityGroupIds // string
```

然後使用 `create-db-instance` 將還原的 Neptune 叢集連接至 Amazon RDS 執行個體。

- 若為 Linux、macOS 或 Unix：

```
aws neptune create-db-instance --db-instance-identifier sample-instance \
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

- 針對 Windows：

```
aws neptune create-db-instance --db-instance-identifier sample-instance ^
                  --db-instance-class db.r5.large --engine neptune --engine-
version 1.0.5.0 --db-cluster-identifier sample-cluster --region us-east-1
```

如需詳細資訊，請參閱《Neptune 管理 API 參考》中的 RestoreDBClusterFromSnapshot 和《Neptune CLI 指南》中的 restore-db-cluster-from-snapshot。

還原 CloudFormation 堆疊備份

CloudFormation 複合備份是 CloudFormation 範本與所有相關聯巢狀復原點的組合。您可以還原任意數目的巢狀復原點，但無法還原複合復原點 (也就是最上層復原點)。

當您還原 CloudFormation 範本復原點時，您會建立具有變更集以代表備份的新堆疊。

CloudFormation 使用 AWS Backup 控制台恢復;

從 CloudFormation 控制台，你可以看到新的堆棧和更改集。若要進一步了解變更集，請參閱《AWS CloudFormation 使用者指南》中的《透過變更集更新堆疊》。

決定您要從 CloudFormation堆疊還原的巢狀復原點，然後使用 AWS Backup 主控台還原它們。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 前往 備份保存庫，選取包含所需復原點的備份保存庫，然後按一下 復原點。
3. 還原 AWS CloudFormation 範本復原點。
   a. 按一下包含您要還原之巢狀復原點的複合復原點，以顯示複合復原點的「詳細資訊」頁面。
   b. 巢狀復原點 下會顯示巢狀復原點。每個復原點都會有復原點 ID、狀態、資源 ID、資源類型、備份類型，以及建立復原點的時間。按一下 AWS CloudFormation 復原點旁邊的選項按鈕，然後按一下「還原」。確定您選取的復原點具有資源類型： AWS CloudFormation 和備份類型：備份。
4. CloudFormation 範本的還原工作完成後，您還原的 AWS CloudFormation 範本就會顯示在AWS CloudFormation 主控台的「堆疊」下方。
5. 在 堆疊名稱 下，您應該會找到狀態為 `REVIEW_IN_PROGRESS` 的還原範本。
6. 按一下堆疊的名稱以查看堆疊的詳細資訊。
7. 堆疊名稱下有索引標籤。按一下 變更集。
8. 執行變更集。
9. 在此程序之後，系統會在新堆疊中重新建立原始堆疊中的資源，並將具狀態的資源重新建立為空白資源。若要復原可設定狀態的資源，請返回 AWS Backup 主控台中的復原點清單，選取所需的復原點，然後啟動還原。

CloudFormation 使用恢復 AWS CLI

在指令行介面中，`start-restore-job`可讓您還原 CloudFormation堆疊。

下列清單是可用來還原資源的中繼 CloudFormation 資料。

```
// Mandatory metadata:
ChangeSetName // This is the name of the change set which will be created
StackName // This is the name of the stack that will be created by the new change set

// Optional metadata:
ChangeSetDescription // This is the description of the new change set
StackParameters // This is the JSON of the stack parameters required by the stack
aws:backup:request-id
```

還原測試

主題

概觀

還原測試是提供的一項功能 AWS Backup，可提供還原可行性的自動化和定期評估，以及監視還原工作持續時間的能力。

請先建立還原測試計畫，您會在其中提供計畫名稱、還原測試的頻率，以及目標開始時間。然後，您會指派要在計畫中包含的資源。然後，您可以選擇在測試中包含特定或隨機的恢復點。 AWS Backup 備份會以智慧方式推斷還原工作成功所需的中繼資料。

當計劃中的排定時間到達時，會根據您的計劃 AWS Backup 開始還原工作，並監視完成還原所花費的時間。

還原測試計畫完成執行之後，您可以使用結果來顯示組織或控管需求的合規性，例如還原測試案例的成功完成或還原任務完成時間。

或者，您可以使用 Amazon EventBridge (Amazon E CloudWatch vents) 將還原測試與測試套件整合，驗證還原的服務，並傳回驗證是成功還是失敗。

選擇性驗證完成或驗證視窗關閉後，會 AWS Backup 刪除還原測試相關的資源，並根據服務 SLA 刪除資源。

在測試程序結束時，您可以檢視測試的結果和完成時間。

還原測試與還原程序的比較

還原測試會以與隨需還原相同的方式執行還原任務，並使用與隨需還原相同的復原點 (備份)。您將看到`StartRestoreJob`通過恢復測試啟動的每個作業在 CloudTrail （如果選擇加入）的呼叫

不過，排程還原測試的作業與隨需還原作業之間有一些差異：

	還原測試	還原
帳戶	建議的最佳實務是指定用於還原測試的帳戶	您可以從帳號還原資源
AWS Backup Audit Manager	可以開啟控制項以確認還原測試是否符合指定的還原目標	
節奏	定期作為排程計畫的一部分。	隨需
區域性	適用於除以色列（特拉維夫）以外的所有商業地區 AWS Backup 不提供 AWS GovCloud （美國東部）、 AWS GovCloud （美國西部）、中國（北京）和中國（寧夏）。	適用於 AWS Backup 營運之所有商業區域

	還原測試	還原
資源	您可以指派給測試計畫的資源類型包括：Aurora、Amazon DocumentDB、Amazon DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、Amazon FSx (Lustre、ONTAP、OpenZFS, Windows)、Amazon Neptune、Amazon RDS 和 Amazon S3。	所有資源皆可還原。
結果	還原測試任務完成後，在驗證視窗完成後，會刪除還原的資源。	還原任務完成後，資源的還原版本仍會保留。
Tags (標籤)	對於在還原時支援標籤的資源類型，測試會在還原時套用標籤。	對於支援的資源，標籤是選用的。

還原測試管理

您可以在 AWS Backup 主控台中建立、檢視、更新或刪除還原測試計畫。

您可以使用 AWS CLI 以程式設計方式執行還原測試計畫的作業。每個 CLI 都是其起源所在的 AWS 服務所特有的。命令前面應加上 `aws backup`。

資料刪除

還原測試完成後，會 AWS Backup 開始刪除測試中涉及的資源。此刪除並非即時進行。每個資源都有基礎組態，用於判斷這些資源的使用方式。例如，如果 Amazon S3 儲存貯體是還原測試的一部分，則會將生命週期規則新增至儲存貯體。規則執行以及完全刪除儲存貯體及其物件最多可能需要數天的時間，但只有到生命週期規則啟動的那天 (預設為 1 天) 才會針對這些資源收取費用。刪除速度將因資源類型而異。

屬於還原測試計畫一部分的資源包含名為 `awsbackup-restore-test` 的標籤。如果用戶刪除此標籤，則 AWS Backup 無法在測試期結束時刪除該資源，用戶將不得不手動刪除它。

若要確認資源未如預期刪除的原因，您可以在主控台中搜尋失敗的任務，或使用命令列介面呼叫 API `DescribeRestoreJob` 請求以擷取刪除狀態訊息。

若要避免額外的備份費用，請確定備份計畫不包含還原測試所建立的資源。若要這麼做，請排除標記為 `awsbackup-restore-test` 或名稱開頭為 `awsbackup-restore-test` 的資源。

成本控制

每次還原測試都會產生費用。根據還原測試計畫中包含的資源而定，屬於計畫一部分的還原任務也可能會產生費用。如需詳細資訊，請參閱 AWS Backup 定價。

第一次設定還原測試計畫時，您可能會發現，納入最少數量的資源類型和受保護資源，對於熟悉功能、程序和所涉及的平均成本很有幫助。您可以在建立計畫後加以更新，以新增更多資源類型和受保護的資源。

建立還原測試計畫

還原測試計畫有兩個部分：計畫建立和指派資源。

使用主控台時，這些部分是有順序的。在第一部分中，您可以設定名稱、頻率和開始時間。在第二部分期間，您將資源指派給測試計畫。

使用 AWS CLI 和 API 時，首先使用 `create-restore-testing-plan`. 一旦您收到成功的回應且已建立計畫，請針對您要在計畫中包含的每個資源類型使用 `create-restore-testing-selection`。

Console

第 I 部分：使用主控台建立還原測試計畫

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽中，找到還原測試並加以選取。
3. 選擇建立還原測試計畫。
4. 一般

    a. 名稱：輸入新還原測試計畫的名稱。此名稱建立後就不可變更。此名稱必須包含英數字元和底線。

    b. 測試頻率：選擇還原測試的執行頻率。

    c. 開始時間：設定您希望測試開始的時間 (以小時和分鐘為單位)。您也可以設定希望還原測試計畫執行所用的當地時區。

d. 開始範圍：此值 (以小時為單位) 是指定還原測試開始的期間。 AWS Backup 盡最大努力在時間內開始所有指定的還原工作，並在此期間內隨機產生開始時間。

5. 復原點選擇：您可以在此設定來源保存庫、復原點範圍，以及您希望哪些復原點 (備份) 成為計畫一部份的選取條件。

   a. 來源保存庫：選擇要包括所有可用的保存庫還是僅包括特定的保存庫，以協助篩選可納入計畫的復原點。如果您選擇特定保存庫，請從下拉式功能表中選取您要包括的保存庫。

   b. 合格的復原點：指定要從中選取復原點的時間範圍。您可以選取 1 至 365 天、1 至 52 週、1 至 12 個月或 1 年。

   c. 選取條件：指定復原點的日期範圍後，您可以選擇是否要在計畫中包含最新還是隨機的復原點。您可能希望選擇隨機的復原點，以更頻繁的頻率來衡量復原點的一般運作狀態，以防需要還原到舊版本的情況。

   d. P oint-in-time 復原點：如果您的計劃包含具有持續備份和 point-in-time 復原點的資源，您可以核取此方塊，讓測試計劃將連續備份納入為合格復原點 (請參閱依資源類型具有此功能的資源提供功能)。

6. (選用) 為還原測試計畫新增的標籤：您可以選擇在還原測試計畫中新增最多 50 個標籤。每個標籤都必須個別新增。若要新增標籤，請選取新增標籤。

第 II 部分：使用主控台將資源指派給計畫

在本節中，您可以選擇已備份要包含在還原測試計畫中的資源。您將選擇資源指派的名稱、選擇用於還原測試的角色，並在清除之前設定保留期限。然後，您將選取資源類型、選取範圍，並選擇性地使用標籤縮小選擇範圍。

> **Tip**
>
> 若要重新瀏覽至要新增資源的還原測試計畫，您可以前往 AWS Backup 主控台、選取還原測試，然後尋找您偏好的測試計畫並加以選取。

1. 一般

   a. 資源指派名稱：使用英數字元與底線的字串 (不含空格)，輸入此資源指派的名稱。

   b. 還原 IAM 角色：此測試必須使用您指定的 Identity and Access Management (IAM) 角色。您可以選擇 AWS Backup 默認角色或其他角色。如果 AWS Backup 預設值在您完成此程

序時尚未存在，則 AWS Backup 會使用必要的權限自動為您建立預設值。您為還原測試選擇的 IAM 角色必須包含 AWSBackupServicePolicyForRestores 中找到的許可。

c. 清除前的保留期：在還原測試期間，會暫時還原備份資料。根據預設，此資料會在測試完成後遭到刪除。如果您希望在還原時執行驗證，則可以選擇延遲刪除此資料。

如果您計畫執行驗證，請選取保留特定小時數，並輸入 1 到 168 小時 (含) 之間的值。請注意，驗證可以透過程式設計的方式執行，但不能從 AWS Backup 主控台執行。

2. 受保護的資源：

a. 選取資源類型：選取要在資源測試計畫中包含的資源類型和這些類型的備份範圍。每個計畫都可以包含多種資源類型，但是必須將每種資源個別指派給計畫。

b. 資源選擇範圍：選擇類型之後，請選取是否要包含該類型的所有可用受保護資源，或者只包含特定受保護的資源。

c. (選用) 使用標籤調整資源選擇：如果備份具有標籤，則可以按標籤篩選以選取特定的受保護資源。輸入標籤索引鍵、要包含或不包含此索引鍵的條件，以及該索引鍵的值。然後，選取新增標籤按鈕。

透過檢查內含受保護資源的備份保存庫中最新復原點上的標籤，以評估受保護資源上的標籤。

3. 還原參數：某些資源需要指定參數來為還原任務做準備。在大多數情況下， AWS Backup 會根據儲存的備份推斷值。

在大多數情況下，建議您保留這些參數；但是，您可以從下拉式功能表中選擇不同的項目來變更這些值。變更值的最佳範例包括覆寫加密金鑰、無法推斷資料的 Amazon FSx 設定，以及建立子網路。

例如，如果 RDS 資料庫是您指派給還原測試計畫的其中一種資源，則可用區域、資料庫名稱、資料庫執行個體類別和 VPC 安全群組等參數都將顯示，並帶有您可以變更的推斷值 (如果適用)。

AWS CLI

CLI 命令 `CreateRestoreTestingPlan` 會用於制定還原測試計畫。

此測試計畫必須包含：

- `RestoreTestingPlan`，其中必須包含唯一的 `RestoreTestingPlanName`
- `ScheduleExpression` Cron 表達式

- RecoveryPointSelection

選擇可以有一或多個受保護的資源 ARN，或者可以有一或多個條件，但不能同時具有兩者。

您也可以包含：

- ScheduleExpressionTimezone
- Tags
- CreatorRequestId
- StartWindowHours

使用 CLI 命令 create-restore-testing-plan。

成功建立計畫後，您需要使用 create-restore-testing-selection 將資源指派至其中。

其中包括 RestoreTestingSelectionName、ProtectedResourceType 以及下列其中一項：

- ProtectedResourceArns

- ProtectedResourceConditions

每個受保護的資源類型可以有一個單一值。還原測試選擇可以包含 ProtectedResourceArns 和 ProtectedResourceConditions 的萬用字元值 (「*」)。或者，您可以在 ProtectedResourceArns 中包含最多 30 個特定受保護的資源 ARN。

更新還原測試計畫

您可以透過主控台或 AWS CLI更新還原測試計畫的部分內容以及其中的資源選擇。

Console

更新主控台中的還原測試計畫和選擇

在主控台中檢視還原測試計畫詳細資訊頁面時，您可以編輯 (更新) 計畫的許多設定。若要執行此作業，

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup

2. 在左側導覽中，找到還原測試並加以選取。
3. 選取編輯按鈕。
4. 調整頻率、開始時間以及測試開始時間 (測試將在所選開始時間之後於此時間內開始)。
5. 儲存您的變更。

AWS CLI

通過更新恢復測試計劃和選擇 AWS CLI

請求UpdateRestoreTestingPlan和UpdateRestoreTestingSelection可用於將部分更新發送到指定的計劃或選擇。名稱無法變更，但您可以更新其他參數。在每個請求中僅包含您希望變更的參數。

傳送更新要求之前，請使用GetRestoreTestingPlan和GetRestoreTestingSelection來判斷您是否RestoreTestingSelection包含特定的 ARN，或是否使用萬用字元和條件。

如果還原測試選擇已指定 ARN (而非萬用字元)，且您想要將其變更為具有條件的萬用字元，則更新請求必須同時包含 ARN 萬用字元和條件。選擇可以具有受保護的資源 ARN，也可以使用萬用字元搭配條件，但不能同時具有兩者。

- `get-restore-testing-plan`
- `get-restore-testing-selection`
- `update-restore-testing-plan`
- `update-restore-testing-selection`

檢視現有的還原測試計畫

Console

在主控台中檢視與現有還原測試計畫和指派資源的詳細資訊

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 從左側導覽中選取還原測試。此畫面會顯示還原測試計畫。依預設會依照上次執行期顯示這些計畫。
3. 從計畫中選取連結以查看其詳細資訊，包括計畫的摘要、名稱、頻率、開始時間和以下時間後開始值。

您也可以檢視此計畫中受保護的資源、此計畫中包含最近 30 天的還原測試任務，以及您可以建立屬於此測試計畫的任何標籤。

AWS CLI

使用命令列取得與現有還原測試計畫和測試選擇的詳細資訊

- list-restore-testing-plan
- list-restore-testing-selections
- get-restore-testing-plan
- get-restore-testing-selection

檢視還原測試任務

Console

在主控台中檢視現有的還原測試任務

還原任務頁面上包含還原測試任務。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 瀏覽至任務頁面。

   或者，您可以選取還原測試，然後選取還原測試計畫以查看其詳細資訊以及與計畫相關聯的任務。
3. 選取還原任務索引標籤。

   您可以在此頁面檢視狀態、還原時間、還原類型、資源 ID、資源類型、任務所屬的還原測試計畫、建立時間以及還原任務的復原點 ID。

   還原測試計畫中包含的任務具有還原類型測試。

還原測試任務有幾個狀態類別：

- 需要注意的狀態類型會加上底線；將游標暫留在狀態上可查看其他詳細資訊 (如果有的話)。
- 如果已在測試上啟動驗證測試 (在主控台中不可用)，則將顯示驗證狀態。
- 刪除狀態會記錄還原測試所產生之資料的狀態。三種可能的刪除狀態：成功、正在刪除和失敗。

如果還原測試任務刪除失敗，您將需要手動移除資源，因為還原測試流程無法自動完成資源。通常如果從資源中移除標籤 awsbackup-restore-test，則會觸發失敗的刪除。

AWS CLI

從命令列檢視現有的還原測試任務

- list-restore-jobs-by-protected-resource

刪除還原測試計畫

Console

在主控台中刪除還原測試計畫

1. 請前往 檢視現有的還原測試計畫 以查看您目前的還原測試計畫。
2. 在還原測試計畫詳細資訊頁面上，選取刪除以刪除計畫。
3. 選取 [刪除] 後，會出現快顯確認畫面，確認您是否要刪除計畫。在此畫面中，特定還原測試計畫的名稱將以粗體顯示。如要繼續，請輸入測試計畫的確切區分大小寫的名稱，包括任何底線、破折號和句號。

   如果無法選取刪除還原測試計畫選項，請重新輸入名稱，直到名稱與顯示的名稱相符為止。一旦完全相符，刪除還原測試計畫的選項將變為可選取的狀態。

AWS CLI

透過命令列刪除還原測試計畫

CLI 指令DeleteRestoreTestingSelection可用於刪除還原測試選取項。在請求中包含 RestoreTestingPlanName 和 RestoreTestingSelectionName。

刪除測試計畫之前，必須先刪除與測試計畫相關的所有測試選擇。刪除所有測試選項後，您可以使用 API 請求刪DeleteRestoreTestingPlan除還原測試計劃。您需要包括 RestoreTestingPlanName。

- delete-restore-testing-selection
- delete-restore-testing-plan

稽核還原測試

還原與 AWS Backup Audit Manager 的測試整合，以協助您評估還原的資源是否在目標還原時間內完成。

如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補中的資源的還原時間符合目標控制項。

考量事項

- 還原測試中不支援封存 (不常用) 儲存中的 Amazon EBS 復原點。包含這些復原點的測試將會失敗。為了修補，請確保還原測試計畫指定的是僅在常用儲存中包含恢復點 (備份) 的參數。例如，如果備份計畫中的生命週期在 30 天後將 Amazon EBS 磁碟區轉移至不常用儲存，則請將還原測試計畫設定為包含過去 29 天或更新的復原點。

> **Note**
>
> AWS Backup 在還原時間內不提供任何服務等級協定 (SLA)。還原時間可能會根據系統負載和容量而有所不同，即使是包含相同資源的還原也是如此。

還原測試配額和參數

- 100 個還原測試計畫
- 可以在每個還原測試計畫新增 50 個標籤
- 每個計畫 30 個選擇
- 每個選擇 30 個受保護資源的 ARN
- 每個選擇 30 個受保護資源的條件 (包括 `StringEquals` 和 `StringNotEquals` 內的條件)
- 每個選擇 30 個保存庫選擇器
- 最長選擇時段天數：365 天
- 開始時段時數：最短 1 小時；最長 168 小時 (7 天)
- 計畫名稱長度上限：50 個字元
- 選擇名稱長度上限：50 個字元

您可在 AWS Backup 配額 檢視有關限制的其他資訊。

還原測試推斷的中繼資料

還原復原點需要還原中繼資料。若要執行還原測試， AWS Backup 會自動推斷可能導致還原成功的中繼資料。該命令`get-restore-testing-inferred-metadata`可用於預覽 AWS Backup 將推斷的內容。命令會`get-restore-job-metadata`傳回由 AWS Backup推斷的一組中繼資料。請注意，對於某些資源類型 (Amazon FSx)， AWS Backup 無法推斷一組完整的中繼資料。

推斷的還原中繼資料是在還原測試程序期間決定的。您可以將參數 `RestoreMetadataOverrides` 包含在 `RestoreTestingSelection` 的主體中，來覆寫某些還原中繼資料索引鍵。請留意，索引鍵值不區分大小寫。

每個支援的資源都有推斷還原中繼資料索引鍵和值，以及可覆寫的還原中繼資料索引鍵。只有標記`###`的 `RestoreMetadataOverrides` 索引鍵值配對或巢狀索引鍵值對必須包含在其中；其他都是選用的值。

資源類型	推斷還原中繼資料索引鍵和值	可覆寫中繼資料

DynamoDB	`deletionProtection` ，其中值會設定為 `false`
	
	`targetTableName` ，其中值會設定為開頭為 `awsbackup-restore-test-` 的隨機值
		`encryptionType`
		
		`kmsMasterKeyArn`

Amazon EBS	`availabilityZone` ，其值會設定為隨機可用區域
	
	`encrypted` ，其值會設定為 `true`
		`availabilityZone`
		
		`kmsKeyId`

Amazon EC2	`disableApiTermination` 值會設定為 `false`
	
	`instanceType` 值會設定為要還原之復原點的 instanceType
		`instanceType`
		
		`requireImdsV2`
		
		`securityGroupIds`
		
		`subnetId`
		
		`vpcId`

資源類型	推斷還原中繼資料索引鍵和值	可覆寫中繼資料
	requiredImdsV2 值會設定為 true	
Amazon EFS	encrypted 值會設定為 true file-system-id 值會設定為要還原之復原點的檔案系統 ID kmsKeyId value 已設定為 alias/aws/elasticfilesystem newFileSystem 值會設定為 true performanceMode 值會設定為 generalPurpose	kmsKeyId
Amazon FSx for Lustre	lustreConfiguration 具有巢狀索引鍵。一個巢狀索引鍵是 automaticBackupRetentionDays ，其值會設為 0	kmsKeyId lustreConfiguration 具有巢狀索引鍵 logConfiguration securityGroupIds subnetIds ，######

資源類型	推斷還原中繼資料索引鍵和值	可覆寫中繼資料
Amazon FSx NetApp	name 會設定為開頭為 awsbackup_restore_test_ 的隨機值 ontapConfiguration 具有巢狀索引鍵，包括： • junctionPath ，其中 / name 是要還原的磁碟區名稱 • sizeInMegabytes ，其值會設定為要還原之復原點的大小 (MB) • snapshotPolicy ，其中值會設定為 none	ontapConfiguration 具有特定的可覆寫巢狀索引鍵，包括： • junctionPath • ontapVolumeType • securityStyle • sizeInMegabytes • storageEfficiencyEnabled • storageVirtualMachineId ，###### • tieringPolicy
Amazon FSx for OpenZFS	openZfzConfiguration ，其中有巢狀索引鍵，包括： • automaticBackupRetentionDays ，將值設定為 0 • deploymentType ，將值設定為要還原之復原點的部署類型 • throughputCapacity ，其值是以 deploymentType 為基礎。如果 deploymentType 是 SINGLE_AZ_1 ，則值會設為 64；如果 deploymentType 是 SINGLE_AZ_2 or MULTI_AZ_1 ，則值會設定為 160	kmsKeyId openZfsConfiguration 具有特定的可覆寫巢狀索引鍵，包括： • deploymentType • throughputCapacity • diskiopsConfiguration securityGroupIds subnetIds

資源類型	推斷還原中繼資料索引鍵和值	可覆寫中繼資料
Amazon FSx for Windows File Server	windowsConfiguration ，其中有巢狀索引鍵，包括： • automaticBackupRetentionDays ，將值設定為 0 • deploymentType ，將值設定為要還原之復原點的部署類型 • throughputCapacity ，將值設定為 8	kmsKeyId securityGroupIds subnetIds ###### windowsConfiguration ，包含特定的可覆寫巢狀索引鍵 • throughputCapacity • activeDirectoryId ###### • preferredSubnetId
Amazon RDS、Aurora、Amazon DocumentDB、Amazon Neptune 叢集	availabilityZones ，將值設定為最多三個隨機可用區域的清單 dbClusterIdentifier ，包含開頭為 awsbackup-restore-test 的隨機值 engine，將值設定為要還原之復原點的引擎	availabilityZones

資源類型	推斷還原中繼資料索引鍵和值	可覆寫中繼資料
Amazon RDS 執行個體	dbInstanceIdentifier ，包含開頭為 awsbackup-restore-test- 的隨機值 deletionProtection ，將值設定為 false multiAz，將值設定為 false publiclyAccessible ，將值設定為 false	availabilityZones
Amazon Simple Storage Service (Amazon S3)	destinationBucketName ，包含開頭為 awsbackup-restore-test- 的隨機值 encrypted ，將值設定為 true encryptionType ，將值設定為 SSE-S3 newBucket ，將值設定為 true	encryptionType kmsKey

檢視備份清單

您可以使用 AWS Backup 主控台或以程式設計方式檢視備份清單。

主題

- 在主控台中依受保護的資源列出備份
- 在主控台中依備份保存庫列出備份
- 以程式設計方式列出備份

在主控台中依受保護的資源列出備份

請遵循下列步驟以在 AWS Backup 主控台上檢視特定資源的備份清單。

1. 請登入 AWS Management Console，然後開啟 AWS Backup 主控台，網址為 https://console.aws.amazon.com/backup。
2. 在導覽窗格中，選擇 Protected resources (受保護的資源)。
3. 在清單中選擇受保護的資源，進而檢視其備份清單。只有已備份的資源才 AWS Backup 會列在「受保護的資源」下。

您可以檢視資源的備份。在此檢視畫面中，您也能選擇備份並予以還原。

在主控台中依備份保存庫列出備份

請遵循下列步驟以檢視備份文件庫中整理的備份清單。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在導覽窗格中，選擇 Backup vaults (備份文件庫)。
3. 在 Backups (備份) 區段中，您可以檢視這個備份文件庫歸整的所有備份清單。在此檢視中，您可以依任何欄標題 (包括狀態) 排序備份，也可以選取備份進行還原、編輯或刪除。

以程式設計方式列出備份

您可以使用 `ListRecoveryPoint` API 操作以程式設計方式列出備份：

- `ListRecoveryPointsByBackupVault`
- `ListRecoveryPointsByResource`

例如，以下 AWS Command Line Interface (AWS CLI) 命令列出了`EXPIRED`狀態的所有備份：

```
aws backup list-recovery-points-by-backup-vault \
  --backup-vault-name sample-vault \
  --query 'RecoveryPoints[?Status == `EXPIRED`]'
```

AWS Backup Audit Manager

您可以使用 AWS Backup Audit Manager 針對您定義的控制項來稽核 AWS Backup 策略的符合性。控制項是為稽核備份需求合規性所設計的程序，例如備份頻率或備份保留期間。

AWS Backup Audit Manager 可協助您回答以下問題：

- 「我備份了所有資源嗎？」
- 「我所有的備份都加密了嗎？」
- 「我每天都備份了嗎？」

您可以使用 AWS Backup Audit Manager 尋找尚未符合您定義之控制項的備份活動和資源。請注意，當控制項評估資源是否合規時，只會包含作用中的資源。例如，執行狀態下的 Amazon EC2 執行個體會受到評估。但停止狀態下的 EC2 執行個體則不會包含在合規評估中。

您也可以使用它來自動產生每日和隨需報告的稽核記錄，以滿足您的備份控管目的。

以下步驟提供如何使用 AWS Backup Audit Manager 的概觀。如需詳細的逐步解說，請選擇本頁結尾處的其中一個主題。

1. 建立包含一或多個控管控制範本的架構。上述問題是三個控管控制範本的範例。您可以自訂某些控管控制範本的參數。例如，您可以自訂最後一個控制項，詢問「我每週執行一次備份嗎？」 而不是每天。
2. 檢視您的架構，瞭解有多少資源符合 (或不符合) 您在該架構中定義的控制項規範。
3. 建立備份與合規狀態報告。將這些報告儲存為合規實務的證據，或找出尚不符合規範的個別備份活動和資源。

   AWS Backup Audit Manager 每 24 小時自動為您產生一份新報告，並將其發佈到 Amazon S3。您也可以產生隨需報告。

> **Note**
>
> 您必須先開啟資源追蹤，才能建立第一個與合規性相關的架構。這樣做可以 AWS Config 跟踪您的 AWS Backup 資源。如需如何管理資源追蹤的技術文件，請參閱AWS Config 開發人員指南中的 AWS Config 使用主控台進行設定。

開啟資源追蹤後需支付費用。如需有關 AWS Backup Audit Manager 資源追蹤定價和計費的詳細資訊，請參閱計量、成本和計費。

主題

- 使用稽核架構
- 使用稽核報告
- 使用 AWS Backup Audit Manager AWS CloudFormation
- 使用 AWS Backup Audit Manager AWS Audit Manager
- 控制與補救

使用稽核架構

架構是協助您評估備份實務的控制項集合。您可以使用預先建立的可自訂控制項定義政策，評估備份實務是否符合您的政策。您也可以設定每日自動報告，深入瞭解架構的合規性狀態。

每個框架都適用於單一帳戶和 AWS 區域. 每個區域每一帳戶最多可部署 10 個架構。您無法部署重複的架構 (包含相同控制項和參數的架構)。

架構有兩種不同類型：

- AWS Backup 架構 (建議)：使用 AWS Backup 架構部署所有可用的控制項，根據我們推薦的最佳實務監視備份活動、涵蓋範圍和資源。
- 您定義的自訂架構：使用自訂架構選擇一或多個特定控制項，並自訂控制項參數。

主題

- 選擇您的控制項
- 開啟資源追蹤
- 使用 AWS Backup 主控台建立架構
- 使用 AWS Backup API 建立框架
- 檢視架構合規狀態
- 尋找不合規的資源
- 更新稽核架構
- 刪除稽核架構

選擇您的控制項

下表列出 AWS Backup Audit Manager 控制項、其可自訂參數及其 AWS Config 記錄資源類型。每個控制項都需要有錄製資源類型 `AWS Config: resource compliance`，因為此類型會記錄您的合規狀態。

可用的控制項

控制項名稱	控制項描述	可自訂參數	AWS Config 記錄資源類型
備份資源受備份計畫保護	評估資源是否受到備份計畫保護。	無	`AWS Backup: backup selection`
備份計畫具有最低的頻率和最短的保留期	評估備份頻率是否至少為 [1 天] 且保留期至少為 [35 天]。	備份頻率、保留期間	`AWS Backup: backup plans`
保存庫可防止手動刪除復原點	評估備份保存庫是否不允許手動刪除復原點，但特定 AWS Identity and Access Management (IAM) 角色除外。所有 IAM 角色預設都不得手動刪除復原點。當您使用 AWS Backup 架構部署此控制項時，也沒有 IAM 角色例外狀況。	最多允許 5 個 IAM 角色可手動刪除復原點	`AWS Backup: backup vaults`
復原點已加密	評估復原點是否已加密。	無	`AWS Backup: recovery points`
針對復原點建立的最短保留期	評估復原點保留期間是否至少為 [35 天]。	復原點保留期間	`AWS Backup: recovery points`

控制項名稱	控制項描述	可自訂參數	AWS Config 記錄資源類型
已排程跨區域備份副本	評估資源是否設定為將自己的備份副本建立在其他 AWS 區域中。	AWS 區域	AWS Backup: backup selection
已排程跨帳戶備份副本	評估資源是否設定了跨帳戶備份副本。	AWS 帳號識別碼	AWS Backup: backup selection
備份受 AWS Backup 文件庫鎖定保護	評估資源是否設定為可在鎖定的備份文件庫中擁有備份。	最短保留天數、最長保留天數	AWS Backup: backup selection
已建立最後復原點	評估是否在指定的時段內建立復原點。	值以小時 [1 至 744] 或天數 [1 至 31] 為單位。	AWS Backup recovery points
資源的還原時間符合目標	評估還原測試任務是否在目標還原時間內完成	值 (以分鐘為單位)	無

如需這些控制項的詳細資訊，請參閱 控制與補救。

如需不支 AWS Backup援所有控制項的支援資源清單，請參閱各資源的功能可用性表格的 AWS Backup Audit Manager 一節。

> **Note**
>
> 如果您不想使用上述任何控制項，您仍然可以使用 AWS Backup Audit Manager 建立備份、複製和還原工作的每日報告。請參閱使用稽核報告。

開啟資源追蹤

您必須先開啟資源追蹤，才能建立第一個與合規性相關的架構。這樣做可以 AWS Config 跟踪您的 AWS Backup 資源。如需如何管理資源追蹤的技術文件，請參閱AWS Config 開發人員指南中的 AWS Config 使用主控台進行設定。

開啟資源追蹤後需支付費用。如需有關 AWS Backup Audit Manager 資源追蹤定價和計費的詳細資訊，請參閱計量、成本和計費。

主題

使用主控台開啟資源追蹤

使用主控台開啟資源追蹤：

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中，選擇 Audit Manager 下的 架構。
3. 選擇 管理資源追蹤 以開啟資源追蹤。
4. 選擇「前往 AWS Config 設定」。
5. 選擇 啟用或停用記錄。
6. 選擇 啟用 記錄下列所有資源類型，或選擇啟用記錄部分資源類型。請參閱 AWS Backup Audit Manager 控制項與修補，瞭解控制項需要的資源類型。

    - `AWS Backup: backup plans`
    - `AWS Backup: backup vaults`
    - `AWS Backup: recovery points`
    - `AWS Backup: backup selection`

> **Note**
>
> AWS Backup Audit Manager 需要`AWS Config: resource compliance`每個控制項。

7. 選擇關閉。
8. 等待顯示開啟資源追蹤的藍色橫幅，轉換成顯示已開啟資源追蹤的綠色橫幅。

您可以在 AWS Backup 主控台的兩個位置檢查是否已開啟資源追蹤，以及是否已開啟記錄的資源類型 (如果有)。在左側導覽窗格中，執行兩個動作之一：

- 選擇 架構，然後選擇 AWS Config 記錄器狀態 下的文字。
- 選擇 設定，然後選擇 AWS Config 記錄器狀態 下的文字。

使用 AWS Command Line Interface (AWS CLI) 開啟資源追蹤

如果您尚未登入 AWS Config，使用. AWS CLI

使用 AWS CLI開啟資源追蹤：

1. 輸入以下命令，確定是否已啟用 AWS Config 記錄器。

```
$ aws configservice describe-configuration-recorders
```

   a. 如果您的 `ConfigurationRecorders` 清單空白如下：

```
{
  "ConfigurationRecorders": []
}
```

   您的記錄器未啟用。請繼續步驟 2 建立您的記錄器。

   b. 如已啟用記錄所有資源，您的 `ConfigurationRecorders` 輸出結果會如下所示：

```
{
  "ConfigurationRecorders":[
    {
      "recordingGroup":{
        "allSupported":true,
        "resourceTypes":[

        ],
        "includeGlobalResourceTypes":true
      },
      "roleARN":"arn:aws:iam::[account]:role/[roleName]",
```

```
      "name":"default"
    }
  ]
}
```

因已啟用所有資源，所以您已開啟資源追蹤。您不需要完成此程序的其餘部分即可使用 AWS Backup Audit Manager。

c. 如果您的 ConfigurationRecorders 不是空的，但您尚未啟用記錄所有資源，請使用以下命令將備份資源新增到現有的記錄器中。接著跳至步驟 3。

```
$ aws configservice describe-configuration-recorders
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

2. 使用 AWS Backup Audit Manager 資源類型建立 AWS Config 記錄器

```
$ aws configservice put-configuration-recorder --configuration-recorder
 name=default, \
roleARN=roleARN=arn:aws:iam::accountId:role/aws-service-role/config.amazonaws.com/
AWSServiceRoleForConfig \
--recording-group
 resourceTypes="['AWS::Backup::BackupPlan','AWS::Backup::BackupSelection', \
'AWS::Backup::BackupVault','AWS::Backup::RecoveryPoint','AWS::Config::ResourceCompliance']"
```

3. 描述你的 AWS Config 錄音機。

```
$ aws configservice describe-configuration-recorders
```

將您的輸出與下列預期的輸出進行比較，以確認其具有 AWS Backup Audit Manager 資源類型。

```
{
  "ConfigurationRecorders":[
    {
      "name":"default",
      "roleARN":"arn:aws:iam::accountId:role/AWSServiceRoleForConfig",
      "recordingGroup":{
        "allSupported":false,
        "includeGlobalResourceTypes":false,
        "resourceTypes":[
          "AWS::Backup::BackupPlan",
          "AWS::Backup::BackupSelection",
          "AWS::Backup::BackupVault",
          "AWS::Backup::RecoveryPoint",
          "AWS::Config::ResourceCompliance"
        ]
      }
    }
  ]
}
```

4. 建立 Amazon S3 儲存貯體做為存放 AWS Config 組態檔案的目的地。

```
$ aws s3api create-bucket --bucket my-bucket –region us-east-1
```

5. 使用## *.json* 授予存取儲存貯體的 AWS Config 權限。請參閱下列範例 *policy.json*。

```
$ aws s3api put-bucket-policy --bucket MyBucket --policy file://policy.json
```

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"AWSConfigBucketPermissionsCheck",
      "Effect":"Allow",
      "Principal":{
```

```
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:GetBucketAcl",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketExistenceCheck",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:ListBucket",
      "Resource":"arn:aws:s3:::my-bucket"
    },
    {
      "Sid":"AWSConfigBucketDelivery",
      "Effect":"Allow",
      "Principal":{
        "Service":"config.amazonaws.com"
      },
      "Action":"s3:PutObject",
      "Resource":"arn:aws:s3:::my-bucket/*"
    }
  ]
}
```

6. 將您的儲存貯體設定為 AWS Config 交付管道

```
$ aws configservice put-delivery-channel --delivery-channel
 name=default,s3BucketName=my-bucket
```

7. 啟用 AWS Config 錄製

```
$ aws configservice start-configuration-recorder –configuration-recorder-
name default
```

8. 確認 DescribeFramework 輸出最後一行中的 "FrameworkStatus":"ACTIVE" 如下所示。

```
$ aws backup describe-framework --framework-name test --region us-east-1
```

```
{
  "FrameworkName":"test",
```

```
 "FrameworkArn":"arn:aws:backup:us-east-1:accountId:framework:test-
f0001b0a-0000-1111-ad3d-4444f5cc6666",
  "FrameworkDescription":"",
  "FrameworkControls":[
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK",
      "ControlInputParameters":[
        {
          "ParameterName":"requiredFrequencyUnit",
          "ParameterValue":"hours"
        },
        {
          "ParameterName":"requiredRetentionDays",
          "ParameterValue":"35"
        },
        {
          "ParameterName":"requiredFrequencyValue",
          "ParameterValue":"1"
        }
      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
```

```
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_ENCRYPTED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    },
    {
      "ControlName":"BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED",
      "ControlInputParameters":[

      ],
      "ControlScope":{

      }
    }
  ],
  "CreationTime":1633463605.233,
  "DeploymentStatus":"COMPLETED",
  "FrameworkStatus":"ACTIVE"
}
```

使用 AWS CloudFormation 範本開啟資源追蹤

如需開啟資源追蹤的 AWS CloudFormation 範本，請參閱搭配使用 AWS Backup Audit Manager AWS CloudFormation。

使用 AWS Backup 主控台建立架構

開啟資源追蹤後，請使用下列步驟建立架構。

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側的導覽窗格中，選擇 架構。
3. 選擇 建立架構。
4. 在 架構名稱 中，輸入唯一的名稱。此架構名稱的長度必須介於 1 到 256 個字元，以英文字母開頭，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。
5. (選用) 在 架構描述 中輸入描述內容。

6. 控制項 會顯示作用中的控制項。依預設，會列出符合資源資格的所有控制項。

   按一下 編輯控制項 可變更作用中的控制項。

   a. 第一個核取方塊會指出控制項是否已開啟。若要關閉控制項，請不要勾選此方塊。
   b. 在 選擇要評估的資源 下，您可以選取依類型、依標籤或依單一資源選擇資源。

   AWS Backup Audit Manager 控制項清單會描述每個控制項的自訂選項。
7. (選用) 選擇 新增標籤 以標記您的架構。您可以使用標籤來搜尋和篩選架構，或追蹤成本。
8. 選擇 建立架構。

AWS Backup Audit Manager 可能需要幾分鐘的時間來建立架構。

如果發生錯誤 `AlreadyExists`，即表示已有具相同控制項和參數的架構。若要成功建立新的架構，至少必須要有一個控制項或參數與現有的架構不同。

使用 AWS Backup API 建立框架

下表包含每個控制項的 CreateFramework 範例 API 請求，以及對應 DescribeFramework 請求的範例 API 回應。若要以程式設計方式使用 AWS Backup Audit Manager，您可以參考這些程式碼片段。

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
`Backup resources are protected by a backup plan`	`{"FrameworkName": "Control1", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes":`	`{"FrameworkName": "Control1", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control1-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [ {"ControlName": "BACKUP_RESOURCES_`

控制項	**CreateFramework** 請求	**DescribeFramework** 回應

	<pre>["RDS"] // Evaluate only RDS instances
	}
	}
	],
	"IdempotencyToken": "Control1",
	"FrameworkTags": {"key1": "foo"}
	}</pre>
		<pre>PROTECTED_BY_BACKUP_PLAN",
		"ControlInputParameters":[],
		"ControlScope": {"ComplianceResourceTypes": ["RDS"]
		}
		}
		],
		"CreationTime": 1516925490,
		"DeploymentStatus": "Active",
		"FrameworkStatus": "Completed",
		"IdempotencyToken": "Control1",
		"FrameworkTags": {"key1": "foo"}
		}</pre>

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Backup plan minimum frequency and minimum retention	{"FrameworkName": "Control2", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"} // Evaluate backup plans that tagged with "key1": "prod". } }],	{"FrameworkName": "Control2", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}, {"ParameterName": "requiredFrequencyUnit", "ParameterValue": "hours"}, {"ParameterName": "requiredFrequencyValue", "ParameterValue": "24"}], "ControlScope": { "Tags": {"key1": "prod"}

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
	"IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }	} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control2", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Vaults prevent manual deletion of recovery points	{"FrameworkName": "Control3", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:role/service-role/QuickSightAction"}], "ControlScope": {"ComplianceResourceIds":["default"],	{"FrameworkName": "Control3", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control2-de7655ae-1e31-45cb-96a0-4f43d8c1969d", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED", "ControlInputParameters": [{"ParameterName": "principalArnList", "ParameterValue": "arn:aws:iam::123456789012:role/application_abc/component_xyz/RDSAccess, arn:aws:iam::123456789012:role/aws-service-role/access-analyzer.amazonaws.com/AWSServiceRoleForAccessAnalyzer, arn:aws:iam::123456789012:r

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
	"Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }	ole/service-role/Q uickSightAction"}], "ControlScope": {"Complia nceResourceIds":[" default"], "Complian ceResourceTypes": ["AWS::Backup::Bac kupVault"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control3", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Minimum retention established for recovery point	{"FrameworkName": "Control4", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} // Default scope (no scope input) sets scope to all recovery points. }], "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control4", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-6e7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK", "ControlInputParameters": [{"ParameterName": "requiredRetentionDays", "ParameterValue": "35"}], "ControlScope": {} }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control4", "FrameworkTags": {"key1": "foo"}

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
		} }

Backup recovery points are encrypted	{"FrameworkName":
	"Control5",
	"FrameworkDescript
	ion": "This is a test
	framework",
	"FrameworkControls":
	[
	{"ControlName":
	"BACKUP_RECOVERY_P
	OINT_ENCRYPTED",
	"ControlInputParam
	eters":
	[],
	"ControlScope":
	{} // Default scope
	(no scope input) is all
	recovery points
	}
	],
	"IdempotencyToken":
	"Control5",
	"FrameworkTags":
	{"key1": "foo"}
	}
		{"FrameworkName":
		"Control5",
		"FrameworkArn":
		"arn:aws:backup:us
		-east-1:1234567890
		12:framework/Contr
		ol7-7e7655ae-1e31-
		45cb-96a0-4f43d8c1
		9642",
		"FrameworkDescript
		ion": "This is a test
		framework",
		"FrameworkControls
		":
		[
		{"ControlName":
		"BACKUP_RECOVERY_P
		OINT_ENCRYPTED",
		"ControlInputParam
		eters":
		[],
		"ControlScope": {}
		}
		],
		"CreationTime":
		1516925490,
		"DeploymentStatus":
		"Active",
		"FrameworkStatus":
		"Completed",
		"IdempotencyToken":
		"Control5",
		"FrameworkTags":
		{"key1": "foo"}
		}

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Cross-Region backup copy is scheduled	{"FrameworkName": "Control6", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control6", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control6-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control6", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Cross-account backup copy is scheduled	{"FrameworkName": "Control7", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control7", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control7-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control7", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Backups are protected by AWS Backup Vault Lock	{"FrameworkName": "Control8", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control8", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control8-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control8", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Last recovery point was created	{"FrameworkName": "Control9", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] // Evaluate only EC2 instances } }], "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }	{"FrameworkName": "Control9", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "BACKUP_LAST_RECOVERY_POINT_CREATED", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control9", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
Restore time for resources meet target	{"FrameworkName":"Control10", "FrameworkDescription":"This is a test framework", "FrameworkControls":[{ "ControlName":"RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[{ "ParameterName":"maxRestoreTime", "ParameterValue":"720" }], "ControlScope":{ "ComplianceResourceIds":[ ], "ComplianceResourceTypes":["DynamoDB" // Evaluates only DynamoDB databases] } }]"IdempotencyToken":"Control10", "FrameworkTags":{ "key1":"foo" }	{"FrameworkName": "Control10", "FrameworkArn": "arn:aws:backup:us-east-1:123456789012:framework/Control9-ce7655ae-1e31-45cb-96a0-4f43d8c19642", "FrameworkDescription": "This is a test framework", "FrameworkControls": [{"ControlName": "RESTORE_TIME_FOR_RESOURCES_MEET_TARGET", "ControlInputParameters":[], "ControlScope": {"ComplianceResourceTypes": ["EC2"] } }], "CreationTime": 1516925490, "DeploymentStatus": "Active", "FrameworkStatus": "Completed", "IdempotencyToken": "Control10", "FrameworkTags": {"key1": "foo"} }

控制項	**CreateFramework** 請求	**DescribeFramework** 回應
	}	

檢視架構合規狀態

稽核架構建立之後，就會顯示在您的架構表中。您可以選擇 AWS Backup 主控台左側導覽窗格中的 [架構] 來檢視此表格。若要檢視架構的稽核結果，請選擇其架構名稱。如此即可前往 架構詳細資訊 頁面，其包含兩個區段：摘要 和 控制項。

摘要 區段會從左到右列出下列狀態：

- 合規狀態 是稽核架構的整體合規狀態，由各個控制項的合規狀態決定。每個控制項的合規狀態都是由其評估之各項資源的合規狀態決定。

  只有當控制項評估範圍內的所有資源都通過這些評估時，架構合規狀態才會是 `Compliant`。如有一或多項資源無法通過控制項評估，則合規狀態會是 `Non-Compliant`。如需如何尋找不符合規範資源的相關資訊，請參閱尋找不符合規範的資源。如需如何使資源符合規範的相關資訊，請參閱 AWS Backup Audit Manager 控制項與修補的修補一節。
- 架構狀態 會指出您是否已開啟所有資源的資源追蹤。可能的狀態如下：
  - `Active`，當架構評估的所有資源皆開啟記錄時。
  - `Partially active`，當架構評估的資源中至少一項關閉記錄時。
  - `Inactive`，當架構評估的所有資源皆關閉記錄時。
  - `Unavailable`當 AWS Backup Audit Manager 目前無法驗證錄製檔狀態時。

  更正 **`Partially active`** 或 **`Inactive`** 狀態

  1. 在左側的導覽窗格中選擇 架構。
  2. 選擇 管理資源追蹤。
  3. 遵循快顯視窗中的指示，記錄之前未啟用記錄的資源類型。

  如需有關哪些資源類型需要根據架構所包含之控制項進行資源追蹤的詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補的資源元件。
- 部署狀態 是指架構的部署狀態。此狀態通常應該是 `Completed`，但也會是 `Create in progress`、`Update in progress`、`Delete in progress` 和 `Failed`。

  - Failed 狀態表示架構部署不正確。刪除架構，然後透過 AWS Backup 主控台或 AWS Backup API 重新建立架構。
- 合規控制項 會顯示通過所有評估的架構控制項計數。
- 不合規控制項 會顯示至少有一項評估未通過的架構控制項計數。

控制項 區段會顯示下列資訊：

- 控制項狀態 是指每個控制項的合規狀態。控制項狀態可以是：Compliant，表示所有資源都通過該評估；Non-compliant，表示至少有一項資源未通過該評估；或者 Insufficient data，表示控制項在評估範圍內找不到任何可評估的資源。
- 評估範圍 可能會根據您在建立稽核架構時自訂控制項的方式，將每個控制項限制為一或多個 資源類型、一個 資源 ID 或一對 標籤索引鍵 和 標籤值。如果所有欄位都是空白的 (以破折號 "-" 表示)，則控制項會評估所有適用的資源。

尋找不合規的資源

AWS Backup Audit Manager 可協助您透過兩種方式找出哪些資源不相容。

- 檢視架構合規狀態 時，請在 詳細資訊 區段中選擇控制項名稱。這樣做會將您帶到 AWS Config 主控台，您可以在其中檢視資Non-Compliant源清單。
- 使用包含架構的資源合規範本建立報告計畫之後，您可以 檢視報告，以識別所有控制項中的所有 Non-Compliant 資源。

  此外，您的 Resource compliance report 還會顯示 AWS Backup Audit Manager 上次評估每個控制項的時間。

更新稽核架構

您可以更新現有稽核架構的描述、控制項及參數。

更新現有的架構

1. 在 AWS Backup 主控台左側導覽窗格中，選擇 [架構]。
2. 選擇要編輯架構的架構名稱。
3. 選擇編輯。

刪除稽核架構

刪除現有的架構

1. 在 AWS Backup 主控台左側導覽窗格中，選擇 [架構]。
2. 選擇要刪除架構的架構名稱。
3. 選擇刪除。
4. 輸入架構的名稱，然後選擇 刪除架構。

使用稽核報告

AWS Backup Audit Manager 報告會自動產生您 AWS Backup 活動的證據，例如：

- 已完成的備份任務及完成時間
- 已備份的資源

報告有兩種類型。建立報告時，請選擇要建立的類型。

一種類型是任務報告，顯示過去 24 小時內完成的任務和所有作用中的任務。任務報告不會顯示 `completed with issues` 的狀態。若要尋找此狀態，您可以篩選具有一或多個狀態訊息的`Completed`工作。 AWS Backup 只有在訊息需要注意或採取行動時，才會包含狀態訊息`Completed`作為工作狀態的一部分。

第二種報告類型是合規報告。合規報告可以監視資源層級或生效的其他控制項。

AWS Backup Audit Manager 會將每日報告傳送到您的 Amazon S3 儲存貯體。如果是目前區域和目前帳戶的報告，您可以選擇接收 CSV 或 JSON 格式的報告。否則，只會提供 CSV 格式的報告。每日報告的時間可能會在數小時內波動，因為 AWS Backup Audit Manager 會執行隨機化以維持其效能。您也可以隨時執行隨需報告。

所有帳戶持有人都可以建立跨區域報告，管理和委派管理員帳戶持有人也可以建立跨帳戶報告。

每個報告計劃最多可以有 20 個 AWS 帳戶。

> **Note**
>
> 無法顯示特定備份之資料增量位元組的 RDS 等資源，其值 `backupSizeInBytes` 會顯示為 0。

若要允許 AWS Backup Audit Manager 建立每日或隨選報告，您必須先從報告範本建立報告計劃。

主題

選擇報告範本

報告範本會定義報告計畫在報表中包含的資訊。當您使用報告計劃自動化報告時， AWS Backup Audit Manager 會為您提供過去 24 小時的報告。 AWS Backup Audit Manager 會在 UTC 上午 1 點到 5 點之間建立這些報告。其提供以下報告範本。

備份報告範本

備份報告範本。這些範本會提供備份、還原或複製任務的每日更新。您可以使用這些報告監視作業狀態，以及找出任何可能需要採取進一步動作的故障。下表列出每個備份報告範本名稱及其範例輸出。

備份報告範本	JSON 格式的範例報告
BACKUP_JOB_REPORT	{ "reportItems": [{ "reportTimePeriod": "2021-07-14T00:00:00Z - 2021-07-15T00:00:00Z", "accountId": "112233445566", "region": "us-west-2", "backupJobId": "FCCB040A-9426-2A49-2EA9-5EAFFAC656AC", "jobStatus": "COMPLETED", "resourceType": "EC2",

備份報告範本	JSON 格式的範例報告


```
      "resourceArn": "arn:aws:ec2:us-
west-2:112233445566:instance/
i-0bc877aee7782ba75",
      "backupPlanArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-plan:349f2247-b48
9-4301-83ac-4b7dd724db9a",
      "backupRuleId": "ab88bbf8-
ff4e-4f1b-92e7-e13d3e65dcfb",
      "creationDate": "2021-07-
14T23:53:47.229Z",
      "completionDate": "2021-07-
15T00:16:07.282Z",
      "recoveryPointArn": "arn:aws:
ec2:us-west-2::image/ami-03
0cafb98e5a6dcdf",
      "jobRunTime": "00:22:20",
      "backupSizeInBytes": 858993459
2,
      "backupVaultName": "Default",
      "backupVaultArn": "arn:aws:
backup:us-west-2:1122334455
66:backup-vault:Default",
      "iamRoleArn": "arn:aws:
iam::112233445566:role/service-
role/AWSBackupDefaultServiceRole"
    }
  ]
}
```

備份報告範本	JSON 格式的範例報告

COPY_JOB_REPORT	{
	  "reportItems": [
	    {
	      "reportTimePeriod": "2021-07-14T15:48:31Z - 2021-07-15T15:48:31Z",
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "copyJobId": "E0AD48A9-0560-B668-3EF0-941FDC0AD6B1",
	      "jobStatus": "RUNNING",
	      "resourceType": "EC2",
	      "resourceArn": "arn:aws:ec2:us-west-2:112233445566:instance/i-0bc877aee7782ba75",
	      "backupPlanArn": "arn:aws:backup:us-west-2:112233445566:backup-plan:349f2247-b489-4301-83ac-4b7dd724db9a",
	      "backupRuleId": "ab88bbf8-ff4e-4f1b-92e7-e13d3e65dcfb",
	      "creationDate": "2021-07-15T15:42:04.771Z",
	      "backupSizeInBytes": 8589934592,
	      "sourceRecoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-007b3819f25697299",
	      "sourceBackupVaultArn": "arn:aws:backup:us-west-2:112233445566:backup-vault:Default",
	      "destinationRecoveryPointArn": "arn:aws:ec2:us-east-2::image/ami-0eba2199a0bcece3c",
	      "destinationBackupVaultArn": "arn:aws:backup:us-east-2:112233445566:backup-vault:Default",
	      "iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	    }

備份報告範本	JSON 格式的範例報告
	] }

RESTORE_JOB_REPORT	{
	"reportItems": [
	{
	"reportTimePeriod": "2021-07-14T15:53:30Z - 2021-07-15T15:53:30Z",
	"accountId": "112233445566",
	"region": "us-west-2",
	"restoreJobId": "4CACA67D-4E12-DC05-6C2B-0E97D01FA41E",
	"jobStatus": "RUNNING",
	"recoveryPointArn": "arn:aws:ec2:us-west-2::image/ami-00201ecb57a5271ae",
	"creationDate": "2021-07-15T15:52:49.797Z",
	"backupSizeInBytes": 8589934592,
	"percentDone": "0.00%",
	"iamRoleArn": "arn:aws:iam::112233445566:role/service-role/AWSBackupDefaultServiceRole"
	}
	]
	}

合規報告範本

合規報告範本會根據您在一或多個架構中定義的控制項，提供有關備份活動和資源合規性的每日報告。如果其中一個架構的合規狀態為 Non-compliant，請檢閱合規報告找出不合規的資源。

合規報告範本類型

- Control compliance report 會協助您根據架構中所定義之控制項追蹤控制項的合規狀態。

- Resource compliance report 會協助您根據架構中所定義之控制項追蹤資源的合規狀態。這些報告內含詳細的評估結果，包括找出不合規資源的資訊，用以識別與更正這些資源。

下表顯示合規報告的範例輸出。

合規報告範本	JSON 格式的範例報告
CONTROL_COMPLIANCE_REPORT	{ "reportItems": [{ "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_R ESOURCES_PROTECTED_BY_BACKUP_PLAN", "controlComplianceStatus": "NON_COMPLIANT", "lastEvaluationTime": "2021-08- 17T03:21:56.002Z", "numResourcesCompliant": 91, "numResourcesNonCompliant": 205, "controlFrequency": "Twelve_H ours", "controlScope": "", "controlParameters": "" }, { "accountId": "112233445566", "region": "me-south-1", "frameworkName": "TestFram ework7", "frameworkDescription": "A test framework", "controlName": "BACKUP_P LAN_MIN_FREQUENCY_AND_MIN_R ETENTION_CHECK", "controlComplianceStatus": "NON_COMPLIANT",

合規報告範本	JSON 格式的範例報告


```
      "lastEvaluationTime": "2021-08-
17T03:21:19.995Z",
      "numResourcesCompliant": 0,
      "numResourcesNonCompliant": 25,
      "controlScope": "{Complia
nceResourceTypes: [],}",
      "controlParameters": "{\"requi
redFrequencyValue\":\"1\",\
"requiredRetentionDays\":\"35\",
\"requiredFrequencyUnit\":\"hours
\"}"
    }
  ]
}
```

合規報告範本	JSON 格式的範例報告

RESOURCE_COMPLIANCE_REPORT	{
	  "reportItems": [
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-63c74e66",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.963Z"
	    },
	    {
	      "accountId": "112233445566",
	      "region": "us-west-2",
	      "frameworkName": "MyTestFr
	amework",
	      "frameworkDescription": "",
	      "controlName": "BACKUP_L
	AST_RECOVERY_POINT_CREATED",
	      "resourceName": "",
	      "resourceId": "AWS::EFS
	::FileSystem/fs-b3d7c218",
	      "resourceType": "AWS::EFS
	::FileSystem",
	      "resourceComplianceStatus":
	 "NON_COMPLIANT",
	      "lastEvaluationTime": "2021-07-
	07T18:55:40.961Z"
	    }
	  ]
	}

使用 AWS Backup 主控台建立報告計畫

報告有兩種類型。一種類型是任務報告，顯示過去 24 小時內完成的任務和所有作用中的任務。第二種報告類型是合規報告。合規報告可以監視資源層級或生效的其他控制項。建立報告時，請選擇要建立的報告類型。

注意：主控台顯示的內容會因帳戶類型而異。只有管理帳戶能看到多帳戶功能。

與備份計畫相似，您建立的報告計畫會自動建立報告並定義其目的地 Amazon S3 儲存貯體。報告計畫要求您必須擁有 S3 儲存貯體，以便接收報告。如需設定新 S3 儲存貯體的指示，請參閱《Amazon Simple Storage Service 使用者指南》中的< 步驟 1：建立您的第一個 S3 儲存貯體 >。

在 AWS Backup 主控台中建立報表計劃

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中，請選擇 報告。
3. 選擇 建立報告計畫。
4. 從下拉式清單中選擇其中一個報告範本。
5. 輸入唯一的報告計畫名稱。此名稱的長度必須介於 1 到 256 個字元，以英文字母開頭，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。
6. (選用) 輸入報告計畫描述。
7. 僅適用於一個帳戶的合規報告範本。選擇要報告的一或多個架構。一份報告計畫最多可新增 1,000 個架構。

    1. 使用下拉菜單選擇您的 AWS 地區。
    2. 使用下拉式功能表從該區域中選擇一個架構。
    3. 選擇 新增架構。
8. (選用) 若要在報告計畫中新增標籤，請選擇 將標籤新增至報告計畫。
9. 如果您使用的是管理帳戶，則可以指定要包含在此報告計畫中的帳戶。您可以選取 僅我的帳戶，這將只會產生您目前登入帳戶的報告。或者，您也可以選取 組織中的一或多個帳戶 (僅適用於管理帳戶)。
10. (如果只建立一個區域的合規報告，請略過此步驟)。您可以選取報告中要包含的區域。按一下下拉式功能表顯示您可使用的區域。選取 所有可用的區域 或您偏好的區域。

    - 當新區域併入 Backup Audit Manager 時，包含這些區域 核取方塊會在有新區域可用時，將新的區域包含在報告中。

11. 選擇報告的 檔案格式。所有報告均可以 CSV 格式匯出。此外，只有一個區域和單一區域的報告也可以 JSON 格式匯出。
12. 使用下拉式清單選擇您的 S3 儲存貯體名稱。
13. (選用) 輸入儲存貯體字首。

    AWS Backup 會將您目前的帳戶、目前的區域報告傳送給`s3://your-bucket-name/prefix/Backup/accountID/Region/year/month/day/report-name`。

    AWS Backup 將您的跨帳戶報告提供給 `s3://your-bucket-name/prefix/Backup/crossaccount/Region/year/month/day/report-name`

    AWS Backup 將您的跨區域報告提供給 `s3://your-bucket-name/prefix/Backup/accountID/crossregion/year/month/day/report-name`
14. 選擇 建立報告計畫。

接下來，您必須允許 S3 儲存貯體從中接收報告 AWS Backup。建立報告計劃後， AWS Backup Audit Manager 會自動產生 S3 儲存貯體存取政策供您套用。

如果您使用自訂 KMS 金鑰加密儲存貯體，請確定該金鑰是以使用者 AWS Backup 身分。許可 `s3:PutObject` 是完成此作業的必要項目。該策略AWSServiceRolePolicyForBackupReports具有此權限。

檢視此存取政策並套用至您的 S3 儲存貯體

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫名稱 下，選擇其名稱即可選取該報告計畫。
4. 選擇編輯。
5. 選擇 檢視 S3 儲存貯體的存取政策。您也可以在此程序結束時使用此政策。
6. 選擇 複製許可。
7. 選擇 編輯儲存貯體政策。
8. 將許可複製到 政策。

範例儲存貯體政策

```
{
```

```
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::11111111:role/aws-service-role/
reports.backup.amazonaws.com/AWSServiceRoleForBackupReports"
      },
      "Action":"s3:PutObject",
      "Resource":[
        "arn:aws:s3:::BucketName/*"
      ],
      "Condition":{
        "StringEquals":{
          "s3:x-amz-acl":"bucket-owner-full-control"
        }
      }
    }
  ]
}
```

使用 AWS Backup API 建立報表計劃

您也可以透過程式設計方式使用報告計畫。

報告有兩種類型。一種類型是任務報告，顯示過去 24 小時內完成的任務和所有作用中的任務。第二種報告類型是合規報告。合規報告可以監視資源層級或生效的其他控制項。建立報告時，請選擇要建立的報告類型。

單一帳戶、單一區域報表請使用下列語法呼叫 CreateReportPlan。

```
{
   "ReportPlanName": "string",
   "ReportPlanDescription": "string",
   "ReportSetting": {
        "ReportTemplate": enum, // Can be RESOURCE_COMPLIANCE_REPORT,
 CONTROL_COMPLIANCE_REPORT, BACKUP_JOB_REPORT, COPY_JOB_REPORT, or RESTORE_JOB_REPORT.
 Only include "ReportCoverageList" if your report is a COMPLIANCE_REPORT.
   "ReportDeliveryChannel": {
       "S3BucketName": "string",
       "S3KeyPrefix": "string",
       "Formats": [ enum ] // Optional. Can be either CSV, JSON, or both. Default is
 CSV if left blank.
```

```
    },
    "ReportPlanTags": {
        "string" : "string" // Optional.
    },
    "IdempotencyToken": "string"
}
```

當您使用唯一的報表計畫名稱呼叫 DescribeReportPlan 時， AWS Backup API 會以下列資訊回應。

```
{
    "ReportPlanArn": "string",
    "ReportPlanName": "string",
    "ReportPlanDescription": "string",
    "ReportSetting": {
        "ReportTemplate": enum,
    },
    "ReportDeliveryChannel": {
        "S3BucketName": "string",
        "S3KeyPrefix": "string",
        "Formats": [ enum ]
    },
    "DeploymentStatus": enum
    "CreationTime": timestamp,
    "LastAttemptExecutionTime": timestamp,
    "LastSuccessfulExecutionTime": timestamp
}
```

多帳戶、多區域報表請使用下列語法呼叫 CreateReportPlan。

```
{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ], *//Organization report only support CSV file*
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ]
```

```
      "OrganizationUnits": [ "string" ],
      "Regions": ["string"],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "ReportTemplate": "string"
   }
}
```

當您使用唯一的報表計畫名稱呼叫 DescribeReportPlan 時， AWS Backup API 會以下列多帳戶、多區域計畫資訊回應：

```
{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts":[ "string" ],
         "OrganizationUnits":[ "string" ],
         "Regions": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "ReportTemplate": "string"
      }
   }
}
```

建立隨需報告

您可以依照下列步驟建立隨選報告，在您方便時產生新報告。 AWS Backup Audit Manager 會將您的隨需報告交付到您在報告計劃中指定的 Amazon S3 儲存貯體。

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。

2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫名稱 下，選擇其名稱即可選取該報告計畫。
4. 選擇 建立隨需報告。

您可以為現有的報告計畫產生隨需報告。

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫 下，按一下報告計畫名稱旁的選項按鈕，即可選取報告計畫。
4. 按一下 動作，再按一下 建立隨需報告。

您可以對多份報告執行此作業，即使是正在產生報告時。

檢視稽核報告

您可以使用通常用來處理 CSV 或 JSON 檔案的程式來開啟、檢視和分析 AWS Backup 稽核管理員報告。請注意，多區域或多帳戶的報告僅以 CSV 格式提供。

檔案總大小超過 50 MB 的大型檔案會分割成多份報告。如果產生的檔案超過 50 MB， AWS Backup Audit Manager 會建立額外的 CSV 檔案，其餘部分為報告。

檢視報告

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫名稱 下，選擇其名稱即可選取該報告計畫。
4. 在 報告任務 下，按一下報告連結以檢視報告。
5. 如果報告的 報告狀態 有虛底線，請選擇它以取得報告的相關資訊。
6. 依 完成時間 選擇要檢視的報告。
7. 選擇 S3 連結。這會開啟目的地 S3 儲存貯體。
8. 在 名稱 下，選擇要檢視的報告名稱。
9. 若要將報告儲存到您的電腦，請選擇 下載。

更新報告計畫

您可以更新現有的報告計畫描述、交付目的地和格式。如果適用，您也可以在報告計畫中新增或移除架構。

更新現有的報告計畫

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫名稱 下，選擇其名稱即可選取該報告計畫。
4. 選擇編輯。
5. 您可以編輯報告計畫的詳細資訊，包括報告名稱和描述，以及報告包含的帳戶和區域。

刪除報告計畫

您可以刪除現有的報告計畫。刪除報告計畫時，該報告計畫已建立的所有報告都會保留在其目的地 Amazon S3 儲存貯體中。

刪除現有的報告計畫

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 在左側導覽窗格中，選擇 報告。
3. 在 報告計畫名稱 下，選擇其名稱即可選取該報告計畫。
4. 選擇刪除。
5. 輸入報告計畫名稱，然後選擇 刪除報告計畫。

使用 AWS Backup Audit Manager AWS CloudFormation

我們提供以下範例 AWS CloudFormation 範本供您參考：

主題

- 開啟資源追蹤
- 部署預設控制項
- 在控制項評估中豁免 IAM 角色
- 建立報告計畫

開啟資源追蹤

下列範本會依開啟資源追蹤所述，開啟資源追蹤。

```
AWSTemplateFormatVersion: 2010-09-09
Description: Enable AWS Config

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      - Label:
          default: Recorder Configuration
        Parameters:
          - AllSupported
          - IncludeGlobalResourceTypes
          - ResourceTypes
      - Label:
          default: Delivery Channel Configuration
        Parameters:
          - DeliveryChannelName
          - Frequency
      - Label:
          default: Delivery Notifications
        Parameters:
          - TopicArn
          - NotificationEmail
    ParameterLabels:
      AllSupported:
        default: Support all resource types
      IncludeGlobalResourceTypes:
        default: Include global resource types
      ResourceTypes:
        default: List of resource types if not all supported
      DeliveryChannelName:
        default: Configuration delivery channel name
      Frequency:
        default: Snapshot delivery frequency
      TopicArn:
        default: SNS topic name
      NotificationEmail:
        default: Notification Email (optional)

Parameters:
```

```
 AllSupported:
   Type: String
   Default: True
   Description: Indicates whether to record all supported resource types.
   AllowedValues:
     - True
     - False

 IncludeGlobalResourceTypes:
   Type: String
   Default: True
   Description: Indicates whether AWS Config records all supported global resource
types.
   AllowedValues:
     - True
     - False

 ResourceTypes:
   Type: List<String>
   Description: A list of valid AWS resource types to include in this recording group,
such as AWS::EC2::Instance or AWS::CloudTrail::Trail.
   Default: <All>

 DeliveryChannelName:
   Type: String
   Default: <Generated>
   Description: The name of the delivery channel.

 Frequency:
   Type: String
   Default: 24hours
   Description: The frequency with which AWS Config delivers configuration snapshots.
   AllowedValues:
     - 1hour
     - 3hours
     - 6hours
     - 12hours
     - 24hours

 TopicArn:
   Type: String
   Default: <New Topic>
   Description: The Amazon Resource Name (ARN) of the Amazon Simple Notification
Service (Amazon SNS) topic that AWS Config delivers notifications to.
```

```
  NotificationEmail:
    Type: String
    Default: <None>
    Description: Email address for AWS Config notifications (for new topics).

Conditions:
  IsAllSupported: !Equals
    - !Ref AllSupported
    - True
  IsGeneratedDeliveryChannelName: !Equals
    - !Ref DeliveryChannelName
    - <Generated>
  CreateTopic: !Equals
    - !Ref TopicArn
    - <New Topic>
  CreateSubscription: !And
    - !Condition CreateTopic
    - !Not
      - !Equals
        - !Ref NotificationEmail
        - <None>

Mappings:
  Settings:
    FrequencyMap:
      1hour   : One_Hour
      3hours  : Three_Hours
      6hours  : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours

Resources:

  ConfigBucket:
    DeletionPolicy: Retain
    Type: AWS::S3::Bucket
    Properties:
      BucketEncryption:
          ServerSideEncryptionConfiguration:
            - ServerSideEncryptionByDefault:
                SSEAlgorithm: AES256

  ConfigBucketPolicy:
```

```
    Type: AWS::S3::BucketPolicy
    Properties:
      Bucket: !Ref ConfigBucket
      PolicyDocument:
        Version: 2012-10-17
        Statement:
          - Sid: AWSConfigBucketPermissionsCheck
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:GetBucketAcl
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
          - Sid: AWSConfigBucketDelivery
            Effect: Allow
            Principal:
              Service:
                - config.amazonaws.com
            Action: s3:PutObject
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/AWSLogs/
${AWS::AccountId}/*"
          - Sid: AWSConfigBucketSecureTransport
            Action:
              - s3:*
            Effect: Deny
            Resource:
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}"
              - !Sub "arn:${AWS::Partition}:s3:::${ConfigBucket}/*"
            Principal: "*"
            Condition:
              Bool:
                aws:SecureTransport:
                  false

  ConfigTopic:
    Condition: CreateTopic
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Sub "config-topic-${AWS::AccountId}"
      DisplayName: AWS Config Notification Topic
      KmsMasterKeyId: "alias/aws/sns"
```

```
  ConfigTopicPolicy:
    Condition: CreateTopic
    Type: AWS::SNS::TopicPolicy
    Properties:
      Topics:
        - !Ref ConfigTopic
      PolicyDocument:
        Statement:
          - Sid: AWSConfigSNSPolicy
            Action:
              - sns:Publish
            Effect: Allow
            Resource: !Ref ConfigTopic
            Principal:
              Service:
                - config.amazonaws.com

  EmailNotification:
    Condition: CreateSubscription
    Type: AWS::SNS::Subscription
    Properties:
      Endpoint: !Ref NotificationEmail
      Protocol: email
      TopicArn: !Ref ConfigTopic

  ConfigRecorderServiceRole:
    Type: AWS::IAM::ServiceLinkedRole
    Properties:
      AWSServiceName: config.amazonaws.com
      Description: Service Role for AWS Config

  ConfigRecorder:
    Type: AWS::Config::ConfigurationRecorder
    DependsOn:
      - ConfigBucketPolicy
      - ConfigRecorderServiceRole
    Properties:
      RoleARN: !Sub arn:${AWS::Partition}:iam::${AWS::AccountId}:role/aws-service-role/
config.amazonaws.com/AWSServiceRoleForConfig
      RecordingGroup:
        AllSupported: !Ref AllSupported
        IncludeGlobalResourceTypes: !Ref IncludeGlobalResourceTypes
        ResourceTypes: !If
          - IsAllSupported
```

```
          - !Ref AWS::NoValue
          - !Ref ResourceTypes

  ConfigDeliveryChannel:
    Type: AWS::Config::DeliveryChannel
    DependsOn:
      - ConfigBucketPolicy
    Properties:
      Name: !If
        - IsGeneratedDeliveryChannelName
        - !Ref AWS::NoValue
        - !Ref DeliveryChannelName
      ConfigSnapshotDeliveryProperties:
        DeliveryFrequency: !FindInMap
          - Settings
          - FrequencyMap
          - !Ref Frequency
      S3BucketName: !Ref ConfigBucket
      SnsTopicARN: !If
        - CreateTopic
        - !Ref ConfigTopic
        - !Ref TopicArn
```

部署預設控制項

下列範本會依 AWS Backup Audit Manager 控制項與修補所述，使用預設控制項建立架構。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_PLAN
        - ControlName: BACKUP_RECOVERY_POINT_MINIMUM_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
        - ControlName: BACKUP_PLAN_MIN_FREQUENCY_AND_MIN_RETENTION_CHECK
          ControlInputParameters:
            - ParameterName: requiredRetentionDays
              ParameterValue: '35'
```

```
            - ParameterName: requiredFrequencyUnit
              ParameterValue: 'hours'
            - ParameterName: requiredFrequencyValue
              ParameterValue: '24'
          ControlScope:
            Tags:
              - Key: customizedKey
                Value: customizedValue
        - ControlName: BACKUP_RECOVERY_POINT_ENCRYPTED
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_REGION
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_CROSS_ACCOUNT
        - ControlName: BACKUP_RESOURCES_PROTECTED_BY_BACKUP_VAULT_LOCK
        - ControlName: BACKUP_LAST_RECOVERY_POINT_CREATED
        - ControlName: RESTORE_TIME_FOR_RESOURCES_MEET_TARGET
          ControlInputParameters:
            - ParameterName: maxRestoreTime
              ParameterValue: '720'

Outputs:
  FrameworkArn:
    Value: !GetAtt TestFramework.FrameworkArn
```

在控制項評估中豁免 IAM 角色

此控制項 BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED 可讓您豁免仍可手動刪除復原點的 IAM 角色，最多五個。下列範本會部署此控制項，並豁免兩個 IAM 角色。

```
AWSTemplateFormatVersion: '2010-09-09'
Resources:
  TestFramework:
    Type: AWS::Backup::Framework
    Properties:
      FrameworkControls:
        - ControlName: BACKUP_RECOVERY_POINT_MANUAL_DELETION_DISABLED
          ControlInputParameters:
            - ParameterName: "principalArnList"
              ParameterValue: !Sub
 "arn:aws:iam::${AWS::AccountId}:role/AccAdminRole,arn:aws:iam::${AWS::AccountId}:role/
ConfigRole"

Outputs:
  FrameworkArn:
```

```
    Value: !GetAtt TestFramework.FrameworkArn
```

建立報告計畫

下列範本會建立報告計畫。

```
Description: "Basic AWS::Backup::ReportPlan template"

Parameters:
  ReportPlanDescription:
    Type: String
    Default: "SomeReportPlanDescription"
  S3BucketName:
    Type: String
    Default: "some-s3-bucket-name"
  S3KeyPrefix:
    Type: String
    Default: "some-s3-key-prefix"
  ReportTemplate:
    Type: String
    Default: "BACKUP_JOB_REPORT"

Resources:
  TestReportPlan:
    Type: "AWS::Backup::ReportPlan"
    Properties:
      ReportPlanDescription: !Ref ReportPlanDescription
      ReportDeliveryChannel:
        Formats:
          - "CSV"
        S3BucketName: !Ref S3BucketName
        S3KeyPrefix: !Ref S3KeyPrefix
      ReportSetting:
        ReportTemplate: !Ref ReportTemplate
        Regions: ['us-west-2', 'eu-west-1', 'us-east-1']
        Accounts: ['123456789098']
        OrganizationUnits: ['ou-abcd-1234wxyz']
      ReportPlanTags:
        - Key: "a"
          Value: "1"
        - Key: "b"
          Value: "2"
```

```
Outputs:
  ReportPlanArn:
    Value: !GetAtt TestReportPlan.ReportPlanArn
```

使用 AWS Backup Audit Manager AWS Audit Manager

AWS Backup Audit Manager 控制項對映至中預先建立的標準控制項 AWS Audit Manager，可讓您將 AWS Backup Audit Manager 規範遵循發現項目匯入 AWS Audit Manager 報表。您可能想要這麼做，以協助分擔組織整體合規狀態任務的合規性主管、稽核經理或報告備份活動的其他同事。

您可以將 AWS Backup Audit Manager 控制項的合規性結果匯入 AWS Audit Manager 架構。若 AWS Audit Manager 要啟用自動從 AWS Backup Audit Manager 控制項收集資料，請使用《 AWS Audit Manager 使用AWS Audit Manager 者指南》中的〈自訂現有控制項〉的指示建立自訂控制項。當您遵循這些指示時，請注意 AWS Backup 控制項的資料來源為AWS Config。

如需 AWS Backup 控制項清單，請參閱選擇您的控制項。

控制與補救

此頁面列出 AWS Backup Audit Manager 的可用控制項。您可以選擇正確的資訊窗格查看控制項清單，並跳至特定的控制項。若要快速比較控制項，請參閱選擇您的控制項中的資料表。若要以程式設計方式定義控制項，請參閱使用 AWS Backup API 建立架構中的程式碼片段。

每個區域每個帳戶最多可以使用 50 個控制項。在兩個不同的架構中使用相同的控制項，在 50 個控制項的限制中會計為使用了兩個控制項。

本頁面會列出每個控制項，並包含下列資訊：

- 描述。方括號 ("[ ]") 中的值是預設參數值。
- 控制項評估的資源。
- 控制項的參數。
- 控制項的範圍，如下所示：
  - 您可以選擇一或多項 AWS Backup支援的服務，指定 依類型分類的資源。
  - 您可以使用單一標籤索引鍵和選用值來指定 標記的資源 範圍。
  - 您可以使用 單一資源 下拉式清單指定單一資源。
- 將適用資源納入合規性的修補步驟。

請注意，當控制項評估資源是否合規時，只會包含作用中的資源。例如，處於執行中狀態的 Amazon EC2 執行個體將由 已建立最後復原點 控制項進行評估。但停止狀態下的 EC2 執行個體則不會包含在合規評估中。

備份資源受備份計畫保護

描述：評估資源是否受備份計畫保護。

資源：`AWS Backup: backup selection`

參數：無

範圍：

- 標記的資源
- 依類型分類的資源 (預設值)
- 單一資源

修補：將資源指派給備份計畫。 AWS Backup 在您將資源指派給備份計畫後，會自動保護資源。如需詳細資訊，請參閱將資源指派到備份計畫。

備份計畫最低頻率和最低保留

描述：評估備份計畫是否包含至少一項備份規則，其備份頻率至少為 [1 天] 且保留期間至少為 [35 天]。

資源：`AWS Backup: backup plans`

參數：

- 所需的備份頻率按小時或天數計算。
- 所需的保留期間按天數、週數、月數或年數計算。我們建議您至少保留一週的熱儲存期限，以便在可能的情況下進行增量備份， AWS Backup 以免產生額外費用。

範圍：

- 標記的資源
- 單一資源

修補：更新備份計畫 以變更其備份頻率、保留期間或兩者皆變更。更新備份計畫會在您更新後，變更計畫建立的復原點保留期間。

保存庫可防止手動刪除復原點

描述：評估備份文件庫是否不允許手動刪除復原點，但特定 IAM 角色不在此限。

資源：`AWS Backup: backup vaults`

參數：最多允許五個 IAM 角色的 Amazon Resource Name (ARN) 手動刪除復原點。

範圍：

- 標記的資源
- 單一資源

修補：建立或修改備份文件庫的資源型存取政策。如需如何設定備份文件庫存取政策的範例政策和指示，請參閱拒絕存取：不允許刪除備份文件庫中的復原點。

復原點已加密

描述：評估復原點是否已加密。

資源：`AWS Backup: recovery points`

參數：無

範圍：

- 標記的資源

修補：設定復原點加密。根據資源類型的不同，您為 AWS Backup 復原點設定加密的方式會有所不同。

您可以為在使用中支援完整 AWS Backup 管理的資源類型配置加密 AWS Backup。如果資源類型不支援完整 AWS Backup 管理，您必須遵循該服務的指示來設定其備份加密，例如 Amazon 彈性運算雲端使用者指南中的 Amazon EBS 加密。若要查看支援完整 AWS Backup 管理的資源類型清單，請參閱各資源的功能可用性表格的「完整 AWS Backup 管理」一節。

為復原點建立的最短保留期

描述：評估復原點保留期間是否至少為 [35 天]。

資源：`AWS Backup: recovery points`

參數：所需的復原點保留期間按天數、週數、月數或年數計算。我們建議您至少保留一週的熱儲存期限，以便在可能的情況下進行增量備份， AWS Backup 以免產生額外費用。

範圍：

- 標記的資源

修補：變更復原點的保留期間。如需詳細資訊，請參閱編輯備份。

已排程跨區域備份副本

描述：評估資源是否設定為建立其備份到另一個 AWS 區域的複本。

資源：`AWS Backup: backup plans`

參數：

- 選取應該存在備份副本的位置 (選擇性) AWS 區域
- 區域

範圍：

- 標記的資源
- 依類型分類資源
- 單一資源

補救：更新備份計劃以變更應存 AWS 區域 在備份副本的位置。

已排程跨帳戶備份副本

描述：評估是否將資源設定為在其他帳戶下建立備份副本。供控制項評估的帳戶最多可新增 5 個。目的地帳戶必須與 AWS Organizations中的來源帳戶位於同一組織。

資源：`AWS Backup: backup plans`

參數：

- 選取應該存在備份副本的 AWS 帳號 ID (選擇性)
- 帳戶 ID

範圍：

- 標記的資源
- 依類型分類資源
- 單一資源

補救：更新備份計劃以變更或新增應存在副本的 AWS 帳號 ID。

備份受 AWS Backup 文件庫鎖定保護

描述：評估資源是否將不可變的備份儲存在鎖定的備份文件庫中。

資源：`AWS Backup: backup vaults`

參數：

- 輸入文件 AWS Backup 庫鎖定的最小和最長保留天數 (選擇性)
- 最短保留天數
- 最長保留天數

範圍：

- 標記的資源
- 依類型分類資源
- 單一資源

修補：鎖定備份文件庫 以設定其名稱、變更其最短保留天數、最長保留天數或兩者皆變更。也可以包含 `ChangeableForDays` 以在合規模式下鎖定保存庫。

已建立最後復原點

描述：此控制項會評估是否已在指定的時間範圍內建立復原點 (按天數或小時計算)。

如果資源已在指定的時間範圍內建立復原點，則控制項即符合規範。如果資源未在指定的天數或小時數內建立復原點，控制項即不符合規範。

此控制項每 24 小時自動執行一次。

資源：`AWS Backup: recovery points`

參數：

- 以整數輸入指定的時間範圍，以小時或天數為單位。
- `hours` 值可以從 1 到 744。
- `days` 值可以從 1 到 31。

範圍：

- 標記的資源
- 依類型分類資源
- 單一資源

修補：

- 更新備份計畫 以變更建立復原點的指定時間範圍。
- 此外，您可以建立隨需備份。

資源的還原時間符合目標

描述：評估受保護資源的還原是否在目標還原時間內完成。

此控制項會檢查特定資源的還原時間是否符合目標持續時間。如果資源類型的 `LatestRestoreExecutionTimeMinutes` 大於 `maxRestoreTime` (以分鐘為單位)，則該規則為「NON_COMPLIANT」。

此控制項每 24 小時自動執行一次。

參數：

- `maxRestoreTime` (以分鐘為單位)

範圍：

- 標記的資源
- 依類型分類資源
- 單一資源

> **Note**
>
> AWS Backup 在還原時間內不提供任何服務等級協定 (SLA)。還原時間可能會根據系統負載和容量而有所不同，即使是包含相同資源的還原也是如此。

跨多個管理 AWS Backup 資源 AWS 帳戶

> **Note**
>
> AWS 帳戶 在中管理多個資源之前 AWS Backup，您的帳戶必須屬於 AWS Organizations 服務中的相同組織。

您可以使用中的跨帳戶管理功能 AWS Backup 來管理和監控您設定的備份、還原和複製工作。 AWS 帳戶 AWS OrganizationsAWS Organizations是一項服務，可針對單一管理帳戶提供多個原 AWS 帳戶則式管理。它可讓您將實作備份政策的方式標準化，同時減少手動錯誤和人力。您可以集中檢視所有資源，輕鬆在所有帳戶中找出符合您感興趣條件的資源。

如果您進行設定 AWS Organizations，您可以設 AWS Backup 定在同一個位置監控所有帳戶中的活動。您也可以建立備份政策，並將其套用至屬於組織一部分的選取帳戶，並直接從 AWS Backup 主控台檢視彙總備份工作活動。這項功能讓備份管理員可從單一管理帳戶有效監控全企業數百個帳戶的備份任務狀態。AWS Organizations 配額適用之。

例如，您定義備份政策 A，該政策會每日備份特定資源，並將其保留 7 天。您選擇將備份政策 A 套用至整個組織。(這表示組織中的每個帳戶都會取得該備份政策，因此系統會建立一個對應的備份計畫顯示在該帳戶中。) 然後，您建立名為「財務」的組織單位，並決定其備份只保留 30 天。在此案例中，您定義一個覆寫生命週期值的備份政策 B，並將其連接至該「財務」組織單位。這表示「財務」組織單位下的所有帳戶都會取得新的有效備份計畫，該計畫會每日備份所有指定的資源，並將其保留 30 天。

在此範例中，備份政策 A 和備份政策 B 合併為單一備份政策，該政策會定義「財務」組織單位下所有帳戶的保護策略。組織中的所有其他帳戶仍然受到備份政策 A 保護。只有使用相同備份計畫名稱的備份政策才能合併。您也可以讓政策 A 和政策 B 共存在於該帳戶中，不進行任何合併。您只能在主控台的 JSON 檢視中使用進階合併運算子。如需合併政策的詳細資訊，請參閱《AWS Organizations 使用指南》的定義政策、政策語法和政策繼承。如需其他參考資料和使用案例，請參閱部落格在您的 AWS Organizations 使用中大規模管理備份，以 AWS Backup及影片教學課程在 AWS Organizations 使用中大規模管理備份 AWS Backup。

請參閱各 AWS 區域的功能可用性，了解跨帳戶管理功能的可用位置。

若要使用跨帳戶管理，您必須依照下列步驟執行：

1. 在中建立管理帳戶， AWS Organizations 並在管理帳戶下新增帳戶。

2. 啟用中的跨帳戶管理功能。 AWS Backup

3. 建立備份政策以套用至管理帳戶 AWS 帳戶 下的所有人。

> **Note**
>
> 至於由組織管理的備份計畫，管理帳戶中的資源選擇加入設定會覆寫成員帳戶中的設定，即使一或多個委派的管理員帳戶已設定也是如此。委派的管理員帳戶是具有增強功能的成員帳戶，但無法像管理帳戶一樣覆寫設定。

4. 管理所有的備份、還原和複製工作 AWS 帳戶。

主題

建立組織的管理帳戶

首先，您必須建立您的組織，並使用中的 AWS 成員帳戶進行設定 AWS Organizations。

在中建立管理帳戶 AWS Organizations 並新增帳戶

- 如需指示，請參閱《AWS Organizations 使用者指南》的教學課程：建立和設定組織。

啟用跨帳戶管理

在中使用跨帳戶管理之前 AWS Backup，您必須先啟用該功能（也就是選擇加入該功能）。啟用此功能後，您可以建立備份政策，讓您可以將同時管理多個帳戶的任務自動化。

啟用跨帳戶管理

1. 打開網 AWS Backup 主控台 址：https://console.aws.amazon.com/backup/。您必須使用管理帳戶憑證進行登入。
2. 在左側導覽窗格中，選擇 Settings (設定) 以開啟跨帳戶管理頁面。
3. 在 Backup policies (備份政策) 區段中，選擇 Enable (啟用)。

   這可讓您存取所有帳戶，並可讓您建立政策，以同時自動管理組織中的多個帳戶。
4. 在 Cross-account monitoring (跨帳戶監控) 區段中，選擇 Enable (啟用)。

   這可讓您從管理帳戶監控組織中所有帳戶的備份、複製和還原活動。

委派的管理員

委派管理為註冊成員帳戶中的指派使用者提供了一種方便的方式，以執行大部分的 AWS Backup 管理工作。您可以選擇將的 AWS Backup 管理委派給中的成員帳戶 AWS Organizations，從而擴展 AWS Backup 從管理帳戶外部和整個組織進行管理的能力。

管理帳戶預設是編輯和管理政策的帳戶。使用委派管理員功能，您可以將這些管理功能委派給您指定的成員帳戶。反之，除管理帳戶之外，這些帳戶也可以管理政策。

成功註冊可執行委派管理的成員帳戶，就是委派的管理員帳戶。請注意，被指定為委派管理員的是帳戶，非使用者。

啟用委派的管理員帳戶可讓您選擇管理備份政策、將可存取管理帳戶的使用者數量減至最少，並允許跨帳戶監控任務。

下表顯示管理帳戶的功能、委派為 Backup 系統管理員的帳戶，以及身為 AWS 組織內成員的帳戶。

> **Note**
>
> 委派的管理員帳戶是具有增強功能的成員帳戶，但無法像管理帳戶一樣覆寫其他成員帳戶的服務選擇加入設定。

PRIVILEGES	管理帳戶	委派管理員	成員帳戶
註冊/取消註冊委派管理員帳戶	是	否	否
管理跨帳戶的備份政策 AWS Organizations	是	是	否
監控跨帳戶任務	是	是	否

必要條件

在委派備份管理之前，您必須先將 AWS 組織中至少一個成員帳戶註冊為委派的系統管理員。您必須先設定下列項目，才能將帳戶註冊為委派管理員：

- AWS Organizations 除了您的預設管理帳戶之外，還必須啟用並設定至少一個成員帳戶。
- 在 AWS Backup 主控台中，請確定已開啟備份政策、跨帳戶監控和跨帳戶備份功能。這些位於 AWS Backup 主控台中的 [委派管理員] 窗格下方。
  - 跨帳戶監控可讓您從管理帳戶以及委派的管理員帳戶監控組織中所有帳戶的備份活動。
  - 選用：跨帳戶備份，允許組織中的帳戶將備份複製到其他帳戶 (用於支援備份的跨帳戶資源)。
  - 使用啟用服務存取 AWS Backup。

設定委派管理需要兩個步驟。第一個步驟是委派跨帳戶任務監控。第二個步驟是委派備份政策管理。

將成員帳戶註冊為委派管理員帳戶。

這是第一部分：使用 AWS Backup 控制台註冊委派的管理員帳戶以監視跨帳戶工作。若要委派 AWS Backup 策略，您將使用下一節中的 Organizations 主控台。

要使用 AWS Backup 控制台註冊成員帳戶：

1. 打開網 AWS Backup 主控台 址：https://console.aws.amazon.com/backup/。您必須使用管理帳戶憑證進行登入。
2. 在主控台左側導覽列中，選擇 我的帳戶 下的 設定。
3. 在 委派管理員 窗格中，按一下 註冊委派管理員 或 新增委派管理員。

4. 在 註冊委派管理員 頁面中，選取您要註冊的帳戶，然後選擇 註冊帳戶。

此指定帳戶現在會註冊為委派的管理員，具有管理權限，可監控組織內所有帳戶任務，並可檢視及編輯政策 (政策委派)。此成員帳戶不能註冊或取消註冊其他委派管理員帳戶。使用主控台最多可將 5 個帳戶註冊為委派管理員。

使用程式設計方式註冊成員帳戶：

使用 `register-delegated-administrator` CLI 命令。您可以在 CLI 請求中指定下列參數：

- `service-principal`
- `account-id`

以下是使用程式設計方式註冊成員帳戶的 CLI 請求範例：

```
aws organizations register-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

取消註冊成員帳戶

使用下列程序， AWS Backup 藉由取消註冊 AWS 組織中先前已指定為委派管理員的成員帳戶，以移除管理存取權。

使用主控台取消註冊成員帳戶

1. 打開網 AWS Backup 主控台 址：https://console.aws.amazon.com/backup/。您必須使用管理帳戶憑證進行登入。
2. 在主控台左側導覽列中，選擇 我的帳戶 下的 設定。
3. 在 委派管理員 區段，按一下 取消註冊帳戶。
4. 選擇您要取消註冊的帳戶。
5. 在 取消註冊帳戶 對話方塊中，檢閱安全性隱患，然後輸入 `confirm` 完成取消註冊。
6. 選擇 `Deregister account`。

使用程式設計方式取消註冊成員帳戶：

使用 CLI 命令 `deregister-delegated-administrator` 取消註冊委派的管理員帳戶。您可以在 CLI 請求中指定下列參數：

- `service-principal`
- `account-id`

以下是使用程式設計方式取消註冊成員帳戶的 CLI 請求範例：

```
aws organizations deregister-delegated-administrator \
--account-id 012345678912 \
--service-principal "backup.amazonaws.com"
```

透過委派 AWS Backup 政策 AWS Organizations

在 AWS Organizations 主控台內，您可以委派多個原則的管理，包括 Backup 政策。

您可以在登入 AWS Organizations 主控台的管理帳戶中，為組織建立、檢視或刪除資源型的委派政策。如需委派政策的步驟，請參閱《AWS Organizations 使用指南》的建立資源型委派政策。

建立備份政策

啟用跨帳戶管理後，請從您的管理帳戶建立跨帳戶備份政策。

建立備份政策

1. 在左側導覽窗格中，選擇 Backup policies (備份政策)。在 Backup policies (備份政策) 頁面上，選擇 Create backup policies (建立備份政策)。
2. 在 Details (詳細資訊) 區段中，輸入備份政策名稱並提供說明。
3. 在 Backup plans details (備份計畫詳細資訊) 區段中，選擇視覺化編輯器標籤，然後執行下列動作：

   a. 針對 Backup plan name (備份計畫名稱)，輸入名稱。

   b. 針對 Regions (區域)，選擇清單中的區域。
4. 在 Backup rule configuration (備份規則組態) 區段中，選擇 Add backup rule (新增備份規則)。

   a. 針對 Rule name (規則名稱)，輸入規則的名稱。規則名稱必須區分大小寫，而且只能包含英數字元或連字號。

b. 針對 Schedule (排程)，選擇 Frequency (頻率) 清單中的備份頻率，然後選擇其中一個 Backup window (備份時段) 選項。建議您選擇 使用備份時段預設值 (建議項目)。

5. 針對 Lifecycle (生命週期)，選擇您要的生命週期設定。
6. 針對 Backup vault name (備份文件庫名稱)，輸入名稱。這是儲存備份所建立復原點的備份文件庫。

   確保備份保管庫存在於您的所有帳戶中。 AWS Backup 不檢查這個。
7. (選擇性) 如果要將備份複製到另一個備份，請從清單中選擇目的地區域 AWS 區域，然後新增標記。無論跨區域複製設定為何，您都可以為所建立的復原點選擇標籤。您也可以新增更多規則。
8. 在 [資源指派] 區段中，提供 AWS Identity and Access Management (IAM) 角色的名稱。若要使用 AWS Backup 服務角色，請提供`service-role/AWSBackupDefaultServiceRole`。

   AWS Backup 在每個帳戶中擔任此角色，以取得執行備份和複製工作的權限，包括適用的加密金鑰權限。 AWS Backup 也會使用此角色執行生命週期刪除。

   > **Note**
   >
   > AWS Backup 不驗證角色是否存在，或者是否可以假定角色。
   > 對於跨帳戶管理建立的備份計劃， AWS Backup 將使用管理帳戶中的選擇加入設定，並覆寫特定帳戶的設定。
   > 您必須自行為要新增備份政策的每個帳戶，建立保存庫和 IAM 角色。
9. 視需要為備份計畫新增標籤。允許的標籤數目上限為 20。
10. 如果您要備份的資源正在 Amazon EC2 執行個體上執行 Microsoft Windows，請在 進階設定 區段選擇 Windows VSS。這可讓您取得應用程式一致的 Windows VSS 備份。

    > **Note**
    >
    > AWS Backup 目前僅支援在 Amazon EC2 上執行的資源的應用程式一致性備份。並非所有執行個體類型或應用程式皆支援 Windows VSS 備份。如需詳細資訊，請參閱 建立 Windows VSS 備份。

> **Note**
>
> AWS Organizations 如果透過 Organizations 織原則建立備份計劃，則原則允許最多指定 20 個標記。利用多項資源指派或通過 JSON 執行多個備份計畫，則可包含其他標籤。

11. 選擇 Add backup plan (新增備份計畫) 將其新增至政策，然後選擇 Create backup policy (建立備份政策)。

    建立備份政策並不會保護您的資源，除非您將其連接到帳戶。您可以選擇您的政策名稱，查看詳細資訊。

    以下是建立備份計劃的範例 AWS Organizations 原則。如果您啟用 Windows VSS 備份，即必須新增可讓您取得應用程式一致備份的許可，如政策的 `advanced_backup_settings` 區段所示。

```
{
  "plans": {
    "PiiBackupPlan": {
      "regions": {
        "@@append":[
          "us-east-1",
          "eu-north-1"
        ]
      },
      "rules": {
        "Hourly": {
          "schedule_expression": {
            "@@assign": "cron(0 0/1 ? * * *)"
          },
          "start_backup_window_minutes": {
            "@@assign": "60"
          },
          "complete_backup_window_minutes": {
            "@@assign": "604800"
          },
          "target_backup_vault_name": {
            "@@assign": "FortKnox"
          },
          "recovery_point_tags": {
            "owner": {
              "tag_key": {
```

```
                "@@assign": "Owner"
              },
              "tag_value": {
                "@@assign": "Backup"
              }
            }
          },
          "lifecycle": {
            "delete_after_days": {
              "@@assign": "365"
            },
            "move_to_cold_storage_after_days": {
              "@@assign": "180"
            }
          },
          "copy_actions": {
            "arn:aws:backup:eu-north-1:$account:backup-vault:myTargetBackupVault" :
 {
            "target_backup_vault_arn" : {
            "@@assign" : "arn:aws:backup:eu-north-1:$account:backup-
vault:myTargetBackupVault"  },
              "lifecycle": {
                "delete_after_days": {
                  "@@assign": "365"
                },
                "move_to_cold_storage_after_days": {
                  "@@assign": "180"
                }
              }
            }
          }
        },
        "selections": {
          "tags": {
            "SelectionDataType": {
              "iam_role_arn": {
                "@@assign": "arn:aws:iam::$account:role/MyIamRole"
              },
              "tag_key": {
                "@@assign": "dataType"
              },
              "tag_value": {
                "@@assign": [
```

```
                "PII",
                "RED"
              ]
            }
          }
        }
      },
      "backup_plan_tags": {
        "stage": {
          "tag_key": {
            "@@assign": "Stage"
          },
          "tag_value": {
            "@@assign": "Beta"
          }
        }
      }
    }
  }
}
```

12. 在 Targets (目標) 區段中，選擇要連接政策的組織單位或帳戶，然後選擇 Attach (連接)。您也可以將政策新增至個別組織單位或帳戶。

> **Note**
>
> 請務必驗證您的政策，並確認政策中包含了所有必要欄位。如果政策的某些部分無效，AWS Backup 會忽略這些部分，但政策的有效部分將會如預期般運作。目前， AWS Backup 不驗證 AWS Organizations 策略的正確性。
>
> 如果您將彼此互相衝突的兩項政策 (例如，具有不同的備份保留期間)，一項套用至管理帳戶，另一項套用至成員帳戶，則兩項政策的執行不會發生問題 (即每個帳戶都會獨立執行政策)。例如，如果管理帳戶政策每天備份一次 Amazon EBS 磁碟區，而本機政策每週備份一次 EBS 磁碟區，則兩項政策都可執行。
>
> 如果將要套用至帳戶的有效政策缺少了必要欄位 (可能因為合併不同政策所致)，則 AWS Backup 完全不會將政策套用至帳戶。如果某些設定無效，請對其 AWS Backup 進行調整。

無論從備份策略建立的備份計劃中，成員帳戶中的選擇加入設定為何，都 AWS Backup 會使用組織管理帳戶中指定的選擇加入設定。

若將政策連接至組織單位，加入此組織單位的每個帳戶都會自動取得此政策，而從組織單位移除的每個帳戶則會失去此政策。對應的備份計畫會自動從該帳戶中刪除。

監控多個 AWS 帳戶的活動

若要監控跨帳戶的備份、複製和還原任務，您必須啟用跨帳戶監控。這可讓您從組織管理帳戶監控所有帳戶的備份活動。當您選擇加入之後，您組織中所有在選擇加入之後建立的任務都會顯示出來。當您選擇退出時， AWS Backup 會將任務保留在彙總檢視中 30 天 (從達到終止狀態起)。系統不會顯示選擇退出後建立的任務，也不會顯示任何新建立的備份任務。如需選擇加入的說明，請參閱 啟用跨帳戶管理。

監控多個帳戶

1. 打開網 AWS Backup 主控台 址：https://console.aws.amazon.com/backup/。您必須使用管理帳戶憑證進行登入。
2. 在左側導覽窗格中，選擇 Settings (設定) 以開啟跨帳戶管理頁面。
3. 在 Cross-account monitoring (跨帳戶監控) 區段中，選擇 Enable (啟用)。

   這可讓您從管理帳戶監控組織中所有帳戶的備份和還原活動。
4. 在左側導覽窗格中，選擇 Cross-account monitoring (跨帳戶監控)。
5. 在 Cross-account monitoring (跨帳戶監控) 頁面上，選擇 Backup jobs (備份任務)、Restore jobs (還原任務) 或 Copy jobs (複製任務) 標籤，以查看在所有帳戶中建立的所有任務。您可以通過 AWS 帳戶 ID 查看每個作業，並且可以查看特定帳戶中的所有作業。
6. 在搜尋方塊中，您可以依 Account ID (帳戶 ID)、Status (狀態) 或 Job ID (任務 ID) 篩選任務。

   例如，您可以選擇 Backup jobs (備份任務) 標籤，並查看在您的所有帳戶中建立的所有備份任務。您可以依 Account ID (帳戶 ID) 篩選清單，並查看在該帳戶中建立的所有備份任務。

資源選擇加入規則

如果成員帳戶的備份計劃是由組織層級備份原則建立 (ID 開始時`orgs-`)，組 Organizations 管理帳戶的 AWS Backup 選擇加入設定將覆寫該成員帳戶中的選擇加入設定，但僅適用於該備份計劃。

如果成員帳戶也有使用者建立的本機層級備份計畫，則這些備份計畫會遵循成員帳戶中的選擇加入設定，不參考 Organizations 管理帳戶的選擇加入設定。

定義政策、政策語法和政策繼承

《 AWS Organizations 使用者指南》中將說明下列主題。

- 備份政策 – 請參閱備份政策。
- 政策語法 - 請參閱備份政策語法和範例。
- 管理政策類型的繼承 - 請參閱管理政策類型的繼承。

AWS Backup 與 AWS CloudFormation

一般情況

AWS CloudFormation 可讓您使用自己建立的範本，以安全、可重複的方式來佈建及管理 AWS 資源。您能夠利用 AWS CloudFormation 範本及 StackSets 來管理備份計畫、備份資源選項和備份保存庫。如需使用 AWS CloudFormation 的相關資訊，請參閱《AWS CloudFormation 使用者指南》中的 AWS CloudFormation 如何運作？一節。

在您建立 AWS CloudFormation 範本或 StackSet 前，應先考量下列事項：

- 請分別為備份計畫和備份保存庫建立範本。您只能刪除空白的備份保存庫。如果包含備份保存庫的堆疊內含復原點，則無法刪除該堆疊。
- 請先確認您具備可用的服務角色，再建立堆疊。當您第一次指派資源給備份計劃時，系統會為您建立 AWS Backup 預設服務角色。如果您尚未將資源指派給備份計畫，請在建立堆疊之前執行此操作。您也可以指定自己建立的自訂角色。如需角色的詳細資訊，請參閱IAM 服務角色。

使用 AWS CloudFormation 部署備份保存庫、備份計畫和資源指派

如需部署備份保存庫、備份計畫和資源指派的範例 AWS CloudFormation 範本，請參閱 使用指定資源 AWS CloudFormation。

使用 AWS CloudFormation 部署備份計畫

如需部署備份計畫的範例 AWS CloudFormation 範本，請參閱《AWS CloudFormation templates for backup plans》。

使用 AWS CloudFormation 部署 AWS Backup Audit Manager 架構和報告計畫

如需部署 AWS Backup Audit Manager 架構和報告計畫的範例 AWS CloudFormation 範本，請參閱《AWS CloudFormation templates for backup plans》。

使用 AWS CloudFormation 跨帳戶部署備份計畫

您可以在 AWS Organization 的多個帳戶內使用 AWS CloudFormation StackSets。範例範本可在《AWS CloudFormation 使用者指南》中找到。

《Automate centralized backup at scale across AWS services using AWS Backup》此書是一個很好的起點和參考。Ibukun Oyewumi 和 Sabith Venkitachalapathy (2021 年 7 月) 著。

深入了解 AWS CloudFormation

如需搭配使用 AWS CloudFormation 和 AWS Backup 的相關資訊，請參閱《AWS CloudFormation 使用者指南》中的 AWS Backup 資源類型參考一節。

如需在使用 AWS CloudFormation 時控制對 AWS 服務資源之存取的相關資訊，請參閱《AWS CloudFormation 使用者指南》中的使用 AWS Identity and Access Management 控制存取一節。

中的安全性 AWS Backup

雲安全 AWS 是最高的優先級。身為 AWS 客戶，您可以從資料中心和網路架構中獲益，該架構專為滿足對安全性最敏感的組織的需求而打造。

安全是 AWS 與您之間共同承擔的責任。共同責任模型 將此描述為雲端的安全和雲端內的安全：

- 雲端安全性 — AWS 負責保護中執行 AWS 服務的基礎架構 AWS 雲端。 AWS 還為您提供可以安全使用的服務。在 AWS 合規計畫中，第三方稽核員會定期測試並驗證我們的安全功效。若要深入瞭解適用於的規範遵循計劃 AWS Backup，請參閱合規方案的AWS 服務範圍。
- 雲端內部的安全 — 您對 AWS Backup 的責任包括但不限於以下各項。您也必須對其他因素負責，包括資料的敏感度、您組織的需求和適用的法律及法規。
  - 回應您收到的通訊 AWS。
  - 管理您和您的團隊使用的憑證。如需詳細資訊，請參閱中的身分識別與存取管理 AWS Backup。
  - 設定您的備份計畫和資源指派，以反映您組織的資料保護政策。如需詳細資訊，請參閱管理備份計畫。
  - 定期測試您找到某些復原點並將其還原的能力。如需詳細資訊，請參閱使用備份。
  - 將 AWS Backup 程序納入組織的災難復原和業務連續性書面程序中。如需起始點，請參閱 AWS Backup入門。
  - 確保您的員工熟悉並在緊急情況下 AWS Backup 與您的組織程序一起練習使用。如需詳細資訊，請參閱 AWS Well-Architected Framework。

本文件可協助您瞭解如何在使用時套用共同責任模型 AWS Backup。下列主題說明如何設定 AWS Backup 以符合安全性與合規性目標。您也會學到如何使用其他可協助您監控和保護 AWS Backup 資源的 AWS 服務。

主題

- AWS PrivateLink
- 韌性 AWS Backup

符合性驗證 AWS Backup

若要瞭解 AWS 服務 是否屬於特定規範遵循方案的範圍內，請參閱AWS 服務 遵循規範計劃方案中的，並選擇您感興趣的合規方案。如需一般資訊，請參閱AWS 規範計劃AWS。

您可以使用下載第三方稽核報告 AWS Artifact。如需詳細資訊，請參閱下載中的報告中的 AWS Artifact。

您在使用時的合規責任取決 AWS 服務 於資料的敏感性、公司的合規目標以及適用的法律和法規。AWS 提供下列資源以協助遵循法規：

- 安全性與合規性快速入門指南 — 這些部署指南討論架構考量，並提供部署以安全性和合規性 AWS 為重點的基準環境的步驟。
- 建構 HIPAA 安全性與合規性 Amazon Web Services— 本白皮書說明公司如何使用建立符合 HIPAA 資格的應 AWS 用程式。

> **Note**
>
> 並非所有人 AWS 服務 都符合 HIPAA 資格。如需詳細資訊，請參閱 HIPAA 資格服務參照。

- AWS 合規資源AWS — 此工作簿和指南集合可能適用於您的產業和所在地。
- AWS 客戶合規指南 — 透過合規的角度瞭解共同的責任模式。這份指南總結了在多個架構 (包括美國國家標準技術研究所 (NIST)、支付卡產業安全標準委員會 (PCI) 和國際標準化組織 (ISO)) 中，保 AWS 服務 護指引並對應至安全控制的最佳實務。
- 使用AWS Config 開發人員指南中的規則評估資源 — 此 AWS Config 服務會評估您的資源組態符合內部實務、產業準則和法規的程度。
- AWS Security Hub— 這 AWS 服務 提供了內部安全狀態的全面視圖 AWS。Security Hub 使用安全控制，可評估您的 AWS 資源並檢查您的法規遵循是否符合安全業界標準和最佳實務。如需支援的服務和控制清單，請參閱 Security Hub controls reference。
- AWS Audit Manager— 這 AWS 服務 有助於您持續稽核您的 AWS 使用情況，以簡化您管理風險的方式，以及遵守法規和業界標準的方式。

資料保護 AWS Backup

AWS Backup 符合 AWS 共同的責任模型，其中包括數據保護的法規和準則。 AWS 負責保護運行所有 AWS 服務的全球基礎設施。 AWS 保持對此基礎架構上託管的數據的控制，包括用於處理客戶內容和個人數據的安全配置控制。 AWS 客戶和合作 AWS 夥伴網路 (APN) 合作夥伴 (擔任資料控制者或資料處理者) 負責他們放入的任何個人資料 AWS 雲端。

基於資料保護目的，我們建議您使用 AWS Identity and Access Management (IAM) 保護 AWS 帳戶 登入資料並設定個別使用者帳戶。這有助於確保每個使用者都只獲得完成其任務所需的許可。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)。
- 使用安全通訊端層 (SSL)/傳輸層安全性 (TLS) 來與 AWS 資源通訊。
- 使用 AWS 加密解決方案，以及 AWS 服務中的所有預設安全性控制。

我們強烈建議您絕對不要將客戶帳戶號碼等敏感的識別資訊，放在自由格式的欄位中，例如Name (名稱) 欄位。這包括當您使用主控台、API AWS Backup 或 AWS SDK 使用 AWS 服務或其他服務時。AWS CLI您輸入 AWS Backup 或其他服務的任何資料都可能被選入診斷日誌中。當您提供外部伺服器的 URL 時，請勿在驗證您對該伺服器請求的 URL 中包含憑證資訊。

如需關於資料保護的詳細資訊，請參閱 AWS 安全部落格上的 AWS 共同責任模型和歐盟《一般資料保護規範》(GDPR) 部落格文章。

中備份的加密 AWS Backup

> **Note**
>
> AWS Backup Audit Manager 可協助您自動偵測未加密的備份。

您可以為在使用中支援完整 AWS Backup 管理的資源類型配置加密 AWS Backup。如果資源類型不支援完整 AWS Backup 管理，您必須遵循該服務的指示來設定其備份加密，例如 Amazon 彈性運算雲端使用者指南中的 Amazon EBS 加密。若要查看支援完整 AWS Backup 管理的資源類型清單，請參閱各資源的功能可用性表格的「完整 AWS Backup 管理」一節。

下表列出了每個支援的資源類型、如何設定備份的加密，以及是否支援備份獨立的加密。當 AWS Backup 獨立加密備份時，會使用業界標準的 AES-256 加密演算法。

資源類型	設定加密的方法	獨立 AWS Backup 加密
Amazon Simple Storage Service (Amazon S3)	Amazon S3 備份使用與備份保存庫關聯的 AWS KMS (AWS Key Management Service) 金鑰加密。 AWS KMS 金鑰可以是客戶管理的 CMK，也可以是與服務相關聯的 AWS受管 CMK。 AWS Backup AWS Backup 即使來源 Amazon S3 儲存貯體未加密，也會加密所有備份。	支援
虛擬機器	虛擬機器備份一律會加密。虛擬機器備份的 AWS KMS 加密金鑰在儲存虛擬機器備份所在的儲存 AWS Backup 庫中設定。	支援
啟用進階 DynamoDB 備份後的 Amazon DynamoDB	DynamoDB 備份一律會加密。DynamoDB 備份的 AWS KMS 加密金鑰是在儲存 DynamoDB 備份所在的 AWS Backup 儲存庫中設定。	支援
不啟用進階 DynamoDB 備份的 Amazon DynamoDB	DynamoDB 備份會自動加密 (使用和加密來源 DynamoDB 資料表時所用的同一個加密金鑰)。未加密 DynamoDB 資料表的快照也不會加密。 **Note** AWS Backup 若要建立加密 DynamoDB 表格的備份，您必須新增許可`kms:Decry`	不支援

資源類型	設定加密的方法	獨立 AWS Backup 加密
	pt 和kms:GenerateDataKey 用於備份的 IAM 角色。或者，您可以使用 AWS Backup 預設服務角色。	
Amazon Elastic File System (Amazon EFS)	Amazon EFS 備份一律會加密。Amazon EFS 備份的 AWS KMS 加密金鑰是在儲存 Amazon EFS 備份所在的儲存 AWS Backup 庫中設定。	支援
Amazon Elastic Block Store (Amazon EBS)	根據預設，Amazon EBS 備份會使用加密來源磁碟區時所用的金鑰加密，或者不會加密。在還原期間，您可以選擇指定 KMS 金鑰來覆寫預設加密方法。	不支援
Amazon Elastic Compute Cloud (Amazon EC2) AMI	以 Amazon EBS 快照為後端的 Amazon EC2 AMI 可以利用 Amazon EBS 加密。資料和根磁碟區的快照可以經過加密再連接至 AMI。未加密 AMI 的快照也不會加密。	不支援

資源類型	設定加密的方法	獨立 AWS Backup 加密
Amazon Relational Database Service (Amazon RDS)	Amazon RDS 快照會自動加密 (使用和加密來源 Amazon RDS 資料庫時所用的同一個加密金鑰)。未加密 Amazon RDS 資料庫的快照也不會加密。 **Note** AWS Backup 目前支援所有 Amazon RDS 資料庫引擎，包括 Amazon Aurora。	不支援
Amazon Aurora	Aurora 叢集快照會自動加密 (使用和加密來源 Amazon Aurora 叢集時所用的同一個加密金鑰)。未加密 Aurora 叢集的快照也不會加密。	不支援

資源類型	設定加密的方法	獨立 AWS Backup 加密
AWS Storage Gateway	Storage Gateway 快照會自動加密 (使用和加密來源 Storage Gateway 磁碟區時所用的同一個加密金鑰)。未加密 Storage Gateway 磁碟區的快照也不會加密。 **Note** 您不需要跨所有服務使用一個客戶自管金鑰來啟用 Storage Gateway。您只需要將 Storage Gateway 備份複製到已設定 KMS 金鑰的文件庫。這是因為 Storage Gateway 沒有服務特定的 AWS KMS 受管理金鑰。	不支援
Amazon FSx	Amazon FSx 檔案系統的加密功能會因基礎檔案系統而有所不同。若要進一步了解特定 Amazon FSx 檔案系統，請參閱適當的《FSx 使用者指南》。	不支援
Amazon DocumentDB	Amazon DocumentDB 叢集快照會自動加密 (使用和加密來源 Amazon DocumentDB 叢集時所用的同一個加密金鑰)。未加密 Amazon DocumentDB 叢集的快照也不會加密。	不支援

資源類型	設定加密的方法	獨立 AWS Backup 加密
Amazon Neptune	Neptune 叢集快照會自動加密 (使用和加密來源 Neptune 叢集時所用的同一個加密金鑰)。未加密 Neptune 叢集的快照也不會加密。	不支援
Amazon Timestream	Timestream 資料表快照備份一律會加密。Timestream 備份的 AWS KMS 加密金鑰，會在儲存 Timestream 備份的備份文件庫中設定。	支援
Amazon Redshift	Amazon Redshift 叢集會自動加密 (使用和加密來源 Amazon Redshift 叢集時所用的同一個加密金鑰)。未加密 Amazon Redshift 叢集的快照也不會加密。	不支援
AWS CloudFormation	CloudFormation 備份始終是加密的。 CloudFormation 備份的 CloudFormation 加密金鑰會在儲存 CloudFormation 備份的儲存 CloudFormation 庫中設定。	支援
Amazon EC2 執行個體上的 SAP HANA 資料庫	SAP HANA 資料庫備份一律會加密。SAP HANA 資料庫備份的 AWS KMS 加密金鑰會在儲存資料庫備份的儲存庫中設定。 AWS Backup	支援

備份複本的加密

當您使 AWS Backup 用跨帳戶或區域複製備份時，即使原始備份未加密，也 AWS Backup 會自動加密這些副本。 AWS Backup 使用目標保管庫的 KMS 金鑰加密您的副本。

> **Note**
>
> 注意：未加密 Aurora、Amazon DocumentDB 和 Neptune 叢集的快照也不會加密。

> **Note**
>
> AWS 跨帳戶副本不支援受管理金鑰。如需詳細資訊，請參閱跨帳戶備份。

虛擬機器 Hypervisor 憑證加密

由 Hypervisor 管理的虛擬機器使用 AWS Backup 閘道將內部部署系統連線到 AWS Backup。所有 Hypervisor 都必須擁有同樣強大且可靠的安全性。透過加密 Hypervisor，可透過 AWS 擁有的金鑰或客戶管理的金鑰來達成此安全性。

AWS 擁有和客戶管理的金鑰

AWS Backup 為 Hypervisor 認證提供加密，以使用AWS 擁有的加密金鑰來保護敏感的客戶登入資訊。您可以選擇改用客戶自管金鑰。

根據預設，用來在 Hypervisor 中加密認證的金鑰是AWS 擁有的金鑰。 AWS Backup 使用這些金鑰來自動加密虛擬機管理程序認證。您既不能檢視、管理或使用 AWS 擁有的金鑰，也不能稽核其使用。不過，您不需要採取任何動作或變更任何程式，即可保護加密您資料的金鑰。如需詳細資訊，請參閱 AWS KMS 開發人員指南中的 AWS 擁有金鑰。

或者，您也可以使用「客戶自管金鑰」來加密憑證。 AWS Backup 支援使用您建立、擁有和管理的對稱客戶自管金鑰來執行加密。由於您可以完全控管此加密，因此能執行以下任務：

- 建立和維護金鑰政策
- 建立和維護 IAM 政策和授予操作
- 啟用和停用金鑰政策
- 輪換金鑰密碼編譯資料
- 新增標籤
- 建立金鑰別名
- 安排金鑰供刪除

當您使用客戶管理的金鑰時，請 AWS Backup 驗證您的角色是否具有使用此金鑰進行解密的權限 (在執行備份或還原工作之前)。您必須將 `kms:Decrypt` 動作新增至用於啟動備份或還原任務的角色。

由於 `kms:Decrypt` 動作無法新增至預設備份角色，因此您必須使用預設備份角色以外的角色才能使用客戶自管金鑰。

如需詳細資訊，請參閱《AWS Key Management Service 開發人員指南》中的客戶自管金鑰。

使用客戶自管金鑰時需要授予

AWS KMS 需要授權才能使用您的客戶管理金鑰。當您匯入使用客戶管理金鑰加密的 Hypervisor 組態時，`CreateGrant`請將要求傳送至以 AWS KMS代表您 AWS Backup 建立授權。 AWS Backup 使用授權存取客戶帳戶中的 KMS 金鑰。

您可以隨時撤銷授權的存取權，或移除 AWS Backup對客戶管理金鑰的存取權。如果這樣做，所有與 Hypervisor 相關的閘道將無法再存取由客戶自管金鑰加密的 Hypervisor 使用者名稱和密碼，這會影響您的備份和還原任務。具體而言，您在此 Hypervisor 中的虛擬機器上執行的備份和還原任務將會失敗。

當您刪除 Hypervisor 時，Backup 閘道會使用 `RetireGrant` 操作來移除授予。

監控加密金鑰

將 AWS KMS 客戶受管金鑰與資 AWS Backup 源搭配使用時，可以使用AWS CloudTrail或 Amazon CloudWatch Logs 追蹤 AWS Backup 傳送至的請求 AWS KMS。

尋找具有下列`"eventName"`欄位的 AWS CloudTrail 事件，以監控所呼叫的 AWS KMS 作業， AWS Backup 以存取由客戶管理金鑰加密的資料：

- `"eventName": "CreateGrant"`
- `"eventName": "Decrypt"`
- `"eventName": "Encrypt"`
- `"eventName": "DescribeKey"`

身分識別與存取管理 AWS Backup

存取需 AWS Backup 要認證。這些憑證必須具備許可才能存取 AWS 資源，例如 Amazon DynamoDB 資料庫或 Amazon EFS 檔案系統。此外，無法使用來源服務 (例如 Amazon EFS) 刪除 AWS Backup 針對某些 AWS Backup支援服務建立的復原點。您可以使用刪除這些復原點 AWS Backup。

以下各節提供如何使用 AWS Identity and Access Management (IAM) 以及 AWS Backup 協助安全存取資源的詳細資訊。

> **Warning**
>
> AWS Backup 使用您在指派資源時選擇的 IAM 角色來管理復原點生命週期。如果您刪除或修改該角色，則 AWS Backup 無法管理復原點生命週期。發生這種情況時，其會嘗試使用服務連結角色來管理您的生命週期。在少數情況下，這可能也無法運作，導致在儲存體上留下 EXPIRED 復原點，而可能造成不必要的成本。若要刪除 EXPIRED 復原點，請使用刪除備份中的程序手動進行刪除。

主題

身分驗證

存取 AWS Backup 或備份的 AWS 服務需要 AWS 可用來驗證您的要求的認證。您可以存取 AWS 下列任何類型的身分識別：

- AWS 帳戶 root 使用者 — 當您註冊時 AWS，您會提供與您的 AWS 帳戶相關聯的電子郵件地址和密碼。這是您的「AWS 帳戶 根使用者」。其憑據提供對所有 AWS 資源的完整訪問權限。

> **Important**
>
> 基於安全理由，建議您只在建立管理員時使用根使用者，管理員是對您的 AWS 帳戶具有完整許可的「IAM 使用者」。然後，您可以使用此管理員使用者建立其他 IAM 使用者和角色，並授予有限許可。如需詳細資訊，請參閱IAM 使用者指南中的 IAM 最佳實務和建立您的第一個 IAM 管理員使用者和群組。

- IAM 使用者 – IAM 使用者是您 AWS 帳戶 中的一種身分，具有特定的自訂許可 (例如，建立備份文件庫以儲存備份的許可)。您可以使用 IAM 使用者名稱和密碼登入以保護 AWS 網頁 AWS Management Console，例如、AWS 討論區或中AWS Support 心。

  除了使用者名稱和密碼之外，您也可以為每個使用者產生存取金鑰。當您以程式設計方式存取 AWS 服務時，您可以使用這些金鑰，無論是透過數個 SDK 之一或使用 AWS Command Line Interface (AWS CLI)。此軟體開發套件和 AWS CLI 工具使用存取金鑰，以加密方式簽署您的請求。如果您不使用 AWS 工具，您必須自行簽署請求。如需有關驗證請求的詳細資訊，請參閱《AWS 一般參考》中的 Signature 第 4 版簽署程序。

- IAM 角色 – IAM 角色是您可以在帳戶中建立的另一種 IAM 身分，具有特定的許可。這類似 IAM 使用者，但不與特定的人關聯。IAM 角色可讓您取得可用來存取 AWS 服務和資源的臨時存取金鑰。使用暫時憑證的 IAM 角色在下列情況中非常有用：

  - 聯合使用者存取 — 您可以從 AWS Directory Service企業使用者目錄或 Web 身分提供者使用預先存在的使用者身分，而不是建立 IAM 使用者。這些稱為聯合身分使用者。透過身分提供者身分提供者來請求存取時， AWS 會指派角色給聯合身分使用者。如需有關聯合身分使用者的詳細資訊，請參閱 IAM 使用者指南中的聯合身分使用者和角色。
  - 跨帳戶管理 — 您可以在帳戶中使用 IAM 角色授予其他 AWS 帳戶 權限來管理帳戶的資源。如需範例，請參閱 IAM 使用者指南中的教學課程：跨 AWS 帳戶 使用 IAM 角色委派存取權。
  - AWS 服務存取 — 您可以在帳戶中使用 IAM 角色授予 AWS 服務許可以存取帳戶資源。如需詳細資訊，請參閱 IAM 使用者指南中的建立角色以將權限委派給 AWS 服務。
  - 在 Amazon 彈性運算雲端 (Amazon EC2) 上執行的應用程式 — 您可以使用 IAM 角色管理在 Amazon EC2 執行個體上執行之應用程式的臨時登入資料，以及提出 AWS API 請求。這是在 EC2 執行個體內儲存存取金鑰的較好方式。若要將 AWS 角色指派給 EC2 執行個體並提供給其所有應用程式，請建立連接至執行個體的執行個體設定檔。執行個體描述檔包含該角色，並且可讓 EC2 執行個體上執行的程式取得臨時憑證。如需詳細資訊，請參閱《IAM 使用者指南》中的使用 IAM 角色為在 Amazon EC2 執行個體上執行的應用程式授予許可。

存取控制

您可以擁有有效的認證來驗證您的請求，但除非您具有適當的權限，否則無法存取備份 Vault 等 AWS Backup 資源。您也無法備份 AWS 資源，例如亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區。

每個 AWS 資源都擁有 AWS 帳戶，建立或存取資源的權限由權限原則控制。帳戶管理員可以將許可政策附加到 AWS Identity and Access Management (IAM) 身分識別 (亦即使用者、群組和角色)。某些服務還支援將許可政策連接到資源。

> **Note**
>
> 帳戶管理員 (或管理員使用者) 是具有管理員許可的使用者。如需詳細資訊，請參《IAM 使用者指南》中的 IAM 最佳實務。

當您授予許可時，能夠決定取得許可的對象、這些對象取得許可的資源，以及可對上述資源進行的特定動作。

下列各節說明存取政策的運作方式，以及您可如何運用這些政策來保護備份。

主題

資源和操作

資源是存在於服務中的物件。 AWS Backup 資源包括備份計劃、備份儲存庫和備份。Backup 是指中存在的各種備份資源類型的一般術語 AWS。例如，Amazon EBS 快照、Amazon Relational Database Service (Amazon RDS) 快照和 Amazon DynamoDB 備份都是備份資源類型。

在中 AWS Backup，備份也稱為復原點。使用時 AWS Backup，您還可以使用您嘗試保護的其他 AWS 服務的資源，例如 Amazon EBS 磁碟區或 DynamoDB 表。這些資源具有與其相關聯的唯一 Amazon Resource Name (ARN)。ARN 可唯一識別 AWS 資源。如果需要在 AWS各處明確地指定資源 (例如在 IAM 政策或 API 呼叫中)，必須具有 ARN。

下表列出資源、子資源、ARN 格式和範例唯一 ID。

AWS Backup 資源 ARN

資源類型	ARN 格式	範例唯一 ID
備份計劃	arn:aws:backup: *region*:*account-id* :backup-plan:*	
備份文件庫	arn:aws:backup: *region*:*account-id* :backup-vault:*	
Amazon EBS 的復原點	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-05f426fd8kdjb4224
Amazon EC2 映像的復原點	arn:aws:ec2: *region*::image/ami-*	image/ami-1a2b3e4f5e6f7g890
Amazon RDS 的復原點	arn:aws:rds: *region*:*account-id* :snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Aurora 的復原點	arn:aws:rds: *region*:*account-id* :cluster-snapshot:awsbackup:*	awsbackup:job-be59cf2a-2343-4402-bd8b-226993d23453
Storage Gateway 的復原點	arn:aws:ec2: *region*::snapshot/*	snapshot/snap-0d40e49137e31d9e0
DynamoDB (不含進階 DynamoDB 備份) 的復原點	arn:aws:dynamodb: *region*:*account-id* :table/*/backup/*	table/MyDynamoDBTable/backup/01547087347000-c8b6kdk3

資源類型	ARN 格式	範例唯一 ID
DynamoDB (已啟用進階 DynamoDB 備份) 的復原點	arn:aws:backup: *region*:*account-id* :recovery-point:*	12a34a56-7bb8-901c-cd23-4567d8e9ef01
Amazon EFS 的復原點	arn:aws:backup: *region*:*account-id* :recovery-point:*	d99699e7-e183-477e-bfcd-ccb1c6e5455e
Amazon FSx 的復原點	arn:aws:fsx: *region*:*account-id* :backup/backup-*	backup/backup-1a20e49137e31d9e0
虛擬機器的復原點	arn:aws:backup: *region*:*account-id* :recovery-point:*	1801234a-5b6b-7dc8-8032-836f7ffc623b
Amazon S3 連續備份的復原點	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -5ec207d0
S3 定期備份的復原點	arn:aws:backup: *region*:*account-id* :recovery-point:*	*my-bucket* -20211231900000-5ec207d0

支援完整 AWS Backup 管理的資源都具有格式arn:aws:backup:*region*:*account-id:*:recovery-point:*的復原點，可讓您更輕鬆地套用權限原則來保護這些復原點。若要查看哪些資源支援完整 AWS Backup 管理，請參閱各資源的功能可用性表格的該部分。

AWS Backup 提供了一組操作來處理 AWS Backup 資源。如需可用操作的清單，請參閱 AWS Backup 動作。

資源擁有權

無論是誰建立資源，都 AWS 帳戶 擁有在帳戶中建立的資源。具體來說，資源擁有者是驗證資源建立請求的主體實體 (即 AWS 帳戶 根使用者、IAM 使用者或 IAM 角色) 的擁有者。 AWS 帳戶 下列範例說明其如何運作：

- 如果您使用的 AWS 帳戶 根使用者認證 AWS 帳戶 來建立備份保管庫，您 AWS 帳戶 就是該保存庫的擁有者。
- 如果您在您的中建立 IAM 使用者， AWS 帳戶 並授與建立備份保管庫的權限給該使用者，則該使用者可以建立備份保管庫。不過，您的 AWS 帳戶 (即該使用者所屬的帳戶) 會擁有備份文件庫的資源。
- 如果您在 AWS 帳戶 具有建立備份保管庫的許可中建立 IAM 角色，則任何可以擔任該角色的人都可以建立保管庫。您的 AWS 帳戶(角色所屬) 擁有備份 Vault 資源。

指定政策元素：動作、效果和主體

對於每個 AWS Backup 資源 (請參閱資源和操作)，服務會定義一組 API 作業 (請參閱動作)。若要授與這些 API 作業的權限，請 AWS Backup 定義一組您可以在政策中指定的動作。執行一項 API 操作可能需要多個動作的許可。

以下是最基本的政策元素：

- 資源 – 在政策中，您可以使用 Amazon Resource Name (ARN) 來識別要套用政策的資源。如需詳細資訊，請參閱 資源和操作。
- 動作：使用動作關鍵字識別您要允許或拒絕的資源操作。
- 效果 - 您可以指定使用者要求特定動作時會有什麼效果；可為允許或拒絕。如果您未明確授予存取 (允許) 資源，則隱含地拒絕存取。您也可以明確拒絕資源存取，這樣做可確保使用者無法存取資源，即使不同政策授予存取也是一樣。
- 委託人：在以身分為基礎的政策 (IAM 政策) 中，政策所連接的使用者就是隱含委託人。對於資源型政策，您可以指定想要收到許可的使用者、帳戶、服務或其他實體 (僅適用於資源型政策)。

如需進一步了解有關 IAM 政策語法和說明的詳細資訊，請參閱《IAM 使用者指南》中的 IAM JSON 政策參考。

如需顯示所有 AWS Backup API 動作的表格，請參閱API 許可：動作、資源和條件參考。

在政策中指定條件

當您授與許可時，您可以使用 IAM 政策語言指定政策生效時間的條件。例如，建議只在特定日期之後套用政策。如需使用政策語言指定條件的詳細資訊，請參閱IAM 使用者指南中的條件。

欲表示條件，您可以使用預先定義的條件金鑰。沒有 AWS Backup特定的條件金鑰。但是，您可以根據需要使用 AWS寬條件鍵。如需 AWS寬金鑰的完整清單，請參閱 IAM 使用者指南中的AWS 全域條件內容金鑰。

> **Note**
>
> AWS Backup 不支援其任何動作的存取原則中的標籤或內容索引鍵條件。

API 許可：動作、資源和條件參考

當您設定存取控制並撰寫可連接至 IAM 身分 (身分類型政策) 的許可政策時，可以參考下列清單。此單包括每個 AWS Backup API 作業、您可以授與執行動作權限的對應動作，以及您可以授與權限的 AWS 資源。您在政策的 `Action` 欄位中指定動作，然後在政策的 `Resource` 欄位中指定資源值。如果 `Resource` 欄位為空白，您可以使用萬用字元 (*) 來包含所有資源。

您可以在 AWS Backup 原則中使用 AWS寬條件金鑰來表示條件。如需完 AWS整金鑰清單，請參閱 IAM 使用者指南中的可用金鑰。

複製標籤許可

AWS Backup 執行備份或複製工作時，它會嘗試將標籤從您的來源資源 (複製的情況下為復原點) 複製到復原點。

> **Note**
>
> AWS Backup 在還原工作期間不會以原生方式複製標籤。如需將在還原工作期間複製標籤的事件導向架構，請參閱如何在還原工作中 AWS Backup 保留資源標籤。

在備份或複製工作期間，將您在備份計劃 (或複製計劃或隨選備份) 中指定的標籤與來源資源中的標籤 AWS Backup 彙總。但是，每個資源 AWS 強制執行 50 個標籤的限制， AWS Backup 不得超過。當備份或複製任務彙總計畫和來源資源中的標籤時，可能會探索總計超過 50 個標籤，而無法完成任務，導致任務失敗。這與 AWS全面的標記最佳做法一致。若要進一步了解，請參閱《AWS 一般參考指南》中的標籤限制。

- 將備份工作標籤與來源資源標籤彙總後，您的資源有 50 個以上的標籤。 AWS 每個資源最多支援 50 個標籤。如需詳細資訊，請參閱標籤限制。
- 您提供的 IAM 角色 AWS Backup 缺少讀取來源標記或設定目標標籤的權限。如需詳細資訊和 IAM 角色政策範例，請參閱受管政策。

您可以使用備份計畫，建立與來源資源標籤相衝突的標籤。當兩個標籤衝突時，會優先使用備份計畫中的標籤。如果您不想從來源資源複製標籤值，請使用此技巧。使用備份計畫指定相同的標籤金鑰，但不同或空白值。

將標籤指派給備份所需的許可

資源類型	所需的許可
Amazon EFS 檔案系統	`elasticfilesystem:DescribeTags`
Amazon FSx 檔案系統	`fsx:ListTagsForResource`
Amazon RDS 資料庫和 Amazon Aurora 叢集	`rds:AddTagsToResource` `rds:ListTagsForResource`
Storage Gateway 磁碟區	`storagegateway:ListTagsForResource`
Amazon EC2 執行個體和 Amazon EBS 磁碟區	`EC2:CreateTags` `EC2:DescribeTags`

除非先啟用 進階 DynamoDB 備份，否則 DynamoDB 不支援將標籤指派給備份。

Amazon EC2 備份建立映像復原點和一組快照時，會 AWS Backup 將標籤複製到產生的 AMI。 AWS Backup 也會將與 Amazon EC2 執行個體關聯的磁碟區中的標籤複製到產生的快照。

存取政策

許可政策描述誰可以存取哪些資源。連接到 IAM 身分的政策稱為身分類型政策 (IAM 政策)。附加至資源的策略稱為以資源為基礎的策略。 AWS Backup 支援以身分識別為基礎的原則和資源型政策。

> **Note**
>
> 本節討論在的內容中使用 IAM AWS Backup。它不提供 IAM 服務的詳細資訊。如需完整的 IAM 文件，請參閱 IAM 使用者指南中的什麼是 IAM？。如需 IAM 政策語法和說明的詳細資訊，請參閱 IAM 使用者指南中的 IAM JSON 政策參考。

身分類型政策 (IAM 政策)

以身分為基礎的政策是您可以連接到 IAM 身分 (例如使用者或角色) 的政策。例如，您可以定義允許使用者檢視和備份 AWS 資源，但防止他們還原備份的原則。

如需使用者、群組、角色和許可的詳細資訊，請參閱《IAM 使用者指南》中的身分 (使用者、群組和角色)。

如需如何使用 IAM 政策控管備份存取的資訊，請參閱受管理的政策 AWS Backup。

資源型政策

AWS Backup 支援備份儲存庫的以資源為基礎的存取原則。這可讓您定義存取政策，控管哪些使用者可以針對備份文件庫中所歸整的任何備份，進行何種存取。以資源為基礎的備份文件庫存取政策，提供了簡單的方法來控管對您備份的存取。

Backup 保管庫存取原則可控制使用者在使用 AWS Backup API 時的存取。某些備份類型 (例如 Amazon Elastic Block Store (Amazon EBS) 和 Amazon Relational Database Service (Amazon RDS) 快照) 也可以使用這些服務的 API 進行存取。您可以在 IAM 中建立不同的存取政策來控管對這些 API 的存取，以便完全控管對備份的存取。

若要了解如何建立備份文件庫的存取政策，請參閱 設定備份文件庫的存取政策。

IAM 服務角色

AWS Identity and Access Management (IAM) 角色與使用者類似，因為它是具有許可政策的 AWS 身分識別，可決定身分可以執行和不能在其中執行的動作 AWS。但是，角色的目的是讓需要它的任何人可代入，而不是單獨地與某個人員關聯。服務角色是服 AWS 務假定代表您執行動作的角色。做為代表您執行備份操作的服務， AWS Backup 需要獲得您傳遞的角色，以在代表您進行備份操作時擔任該角色。如需 IAM 角色的更多相關資訊，請參閱 IAM 使用者指南中的 IAM 角色。

您傳遞給的角色 AWS Backup 必須具有 IAM 政策，其許可 AWS Backup 才能執行與備份操作相關聯的動作，例如建立、還原或備份到期。每個 AWS Backup 支援的 AWS 服務都需要不同的權限。角色也必須 AWS Backup 列為受信任的實體， AWS Backup 以便承擔該角色。

將資源指派給備份計劃時，或執行隨選備份、複製或還原時，必須傳遞具有存取權的服務角色，才能在指定的資源上執行基礎作業。 AWS Backup 使用此角色建立、標記和刪除帳戶中的資源。

使用 AWS 角色控制對備份的存取

您可以使用角色，藉由定義狹義範圍的角色，和指定可以傳遞角色給 AWS Backup的人員，來控管對您備份的存取。例如，您可以建立一個角色，該角色僅授與備份 Amazon 關聯式資料庫服務 (Amazon

RDS) 資料庫的許可，並僅授與 Amazon RDS 資料庫擁有者將該角色傳遞給該角色的權限 AWS Backup。 AWS Backup 為每個支援的服務提供數個預先定義的受管理策略。您可以將這些受管政策連接至您建立的角色，如此可讓您更輕鬆地建立具有所 AWS Backup 需正確權限的服務特定角色。

如需有關的 AWS 受管理策略的詳細資訊 AWS Backup，請參閱受管理的政策 AWS Backup。

的預設服務角色 AWS Backup

第一次使用 AWS Backup 主控台時，您可以選擇為您 AWS Backup 建立預設服務角色。此角色具有對其支援的所有 AWS 服務執行備份作業所 AWS Backup 需的權限。若要選擇預設服務角色，請遵循入門中的任何選項。

> **Note**
>
> 當您使用 AWS Management Console時，系統會自動建立預設角色。您可以使用 AWS Command Line Interface （ AWS CLI ）創建默認角色，但必須手動完成。

如果您偏好使用自訂角色 (例如針對不同資源類型使用不同角色)，您也可以這麼做並將自訂角色傳遞給 AWS Backup。若要檢視為個別資源類型啟用備份和還原的角色範例，請參閱 < 客戶受管政策 > 表格。

透過 AWS Backup 管理建立和還原備份而不使用自訂角色而建立的預設服務角色。會呼叫預設服務角色AWSBackupDefaultServiceRole。

`AWSBackupDefaultServiceRole`包含兩個受管理的策略，AWSBackupServiceRolePolicyForBackup以及AWSBackupServiceRolePolicyForRestores。

`AWSBackupServiceRolePolicyForBackup`包括 IAM 政策，該政策授予 AWS Backup 權限以描述要備份的資源，無論其加密 AWS KMS 金鑰為何，都可以在備份中建立、刪除、描述或新增標籤。此 IAM 政策包含所有 AWS Backup 支援的資源類型的必要許可。

`AWSBackupServiceRolePolicyForRestores`包含 IAM 政策，授與建立、刪除或描述從備份建立的新資源 (不論其加密 AWS KMS 金鑰為何) 的 AWS Backup 權限。該政策還包含標記新建立資源的許可。此 IAM 政策針對 AWS Backup 支援的所有資源類型，包含了必要的許可。

若要還原 Amazon EC2 執行個體，您必須啟動新的執行個體。

在主控台中建立預設服務角色

您在 AWS Backup 主控台中執行的特定動作會建立 AWS Backup 預設服務角色。

若要**AWSBackupDefaultServiceRole**在您的 AWS 帳戶中建立 AWS Backup 預設服務角色：

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 若要為您的帳戶建立角色，請將資源指派給備份計畫，或建立隨需備份。
   a. 建立備份計畫，並將資源指派給備份。請參閱建立排程備份。
   b. 或者，建立隨需備份。請參閱建立隨需備份。
3. 依照下列步驟，確認您已在帳戶中建立 AWSBackupDefaultServiceRole：
   a. 請等待數分鐘。如需詳細資訊，請參閱《AWS Identity and Access Management 使用者指南》中的我所做的變更不一定都會立刻生效。
   b. 登入 AWS Management Console 並開啟身分與存取權管理主控台，網址為 https://console.aws.amazon.com/iam/。
   c. 在左側導覽選單中，選擇 角色。
   d. 在搜尋列中，輸入 AWSBackupDefaultServiceRole。如果此選取項存在，表示您已建立 AWS Backup 預設角色並完成此程序。
   e. 如果 AWSBackupDefaultServiceRole 仍未顯示，請將下列許可新增至您用來存取主控台的 IAM 使用者或 IAM 角色。

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource":"arn:aws:iam::*:role/service-role/AWSBackupDefaultServiceRole"
    },
    {
      "Effect":"Allow",
      "Action":[
        "iam:ListRoles"
      ],
      "Resource":"*"
    }
  ]
```

```
}
```

若是中國區域，請以 *aws-cn* 取代 *aws*。對於 AWS GovCloud (US) 區域，請將 *aws* 取代為 *aws-us-gov*.

f. 如果您無法將許可新增至 IAM 使用者或 IAM 角色，請要求管理員使用 AWSBackupDefaultServiceRole 以外的名稱手動建立角色，並將該角色連接到下列受管政策：

- AWSBackupServiceRolePolicyForBackup
- AWSBackupServiceRolePolicyForRestores

受管理的政策 AWS Backup

受管理的策略是獨立的以身分識別為基礎的策略，您可以將其附加到您的中的多個使用者、群組和角色。 AWS 帳戶將政策連接到主體實體時，便向實體授予了政策中定義的許可。

AWS 受管理的策略是由建立和管理 AWS。

客戶管理的政策為您提供精細的控制，以便在 AWS Backup中設置備份的訪問權限。例如，您可以使用這些政策為資料庫備份管理員提供 Amazon RDS 備份 (而非 Amazon EFS 備份) 的存取權限。

客戶受管政策

建立客戶管理政策的一個方式，是從複製現有 AWS 受管政策開始。如此從一開始您就可以確定政策是正確的，只需根據您的環境進行自訂即可。

下列原則會針對個別 AWS Backup支援的 AWS 服務和協力廠商應用程式指定備份與還原權限。您可以將它們自訂並附加至您建立的角色，以進一步限制對 AWS 資源的存取。

資源備份政策

下列原則會針對個別 AWS Backup支援的 AWS 服務和協力廠商應用程式指定備份權限。您可以將它們自訂並附加至您建立的角色，以進一步限制對 AWS 資源的存取。

Amazon S3

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"S3BucketBackupPermissions",
```

```
      "Action":[
        "s3:GetInventoryConfiguration",
        "s3:PutInventoryConfiguration",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketNotification",
        "s3:PutBucketNotification",
        "s3:GetBucketLocation",
        "s3:GetBucketTagging",
        "s3:GetBucketAcl"
      ],
      "Effect":"Allow",
      "Resource":[
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid":"S3ObjectBackupPermissions",
      "Action":[
        "s3:GetObjectAcl",
        "s3:GetObject",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion"
      ],
      "Effect":"Allow",
      "Resource":[
        "arn:aws:s3:::*/*"
      ]
    },
    {
      "Sid":"S3GlobalPermissions",
      "Action":[
        "s3:ListAllMyBuckets"
      ],
      "Effect":"Allow",
      "Resource":[
        "*"
      ]
    },
    {
      "Sid":"KMSBackupPermissions",
```

```
      "Action":[
        "kms:Decrypt",
        "kms:DescribeKey"
      ],
      "Effect":"Allow",
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "kms:ViaService":"s3.*.amazonaws.com"
        }
      }
    },
    {
      "Sid":"EventsPermissions",
      "Action":[
        "events:DescribeRule",
        "events:EnableRule",
        "events:PutRule",
        "events:DeleteRule",
        "events:PutTargets",
        "events:RemoveTargets",
        "events:ListTargetsByRule",
        "events:DisableRule"
      ],
      "Effect":"Allow",
      "Resource":"arn:aws:events:*:*:rule/AwsBackupManagedRule*"
    },
    {
      "Sid":"EventsMetricsGlobalPermissions",
      "Action":[
        "cloudwatch:GetMetricData",
        "events:ListRules"
      ],
      "Effect":"Allow",
      "Resource":"*"
    }
  ]
}
```

VM

```
{
      "Sid": "BackupGatewayBackupPermissions"
```

```
      "Effect": "Allow",
      "Action": [
        "backup-gateway:Backup",
        "backup-gateway:ListTagsForResource"
      ],
      "Resource": "arn:aws:backup-gateway:*:*:vm/*"
    }
```

Amazon EBS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":"ec2:CreateTags",
      "Resource":"arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot"
      ],
      "Resource":[
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots",
        "ec2:CopySnapshot",
        "ec2:DescribeTags"
      ],
      "Resource":"*"
    },
    {
      "Action":[
        "tag:GetResources"
      ],
```

```
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    }
  ]
}
```

Amazon EFS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Action":[
        "elasticfilesystem:Backup",
        "elasticfilesystem:DescribeTags"
      ],
      "Resource":"arn:aws:elasticfilesystem:*:*:file-system/*",
      "Effect":"Allow"
    },
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    }
  ]
```

```
}
```

Amazon RDS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:DescribeDBSnapshots",
        "rds:CreateDBSnapshot",
        "rds:CopyDBSnapshot",
        "rds:DescribeDBInstances",
        "rds:CreateDBClusterSnapshot",
    "rds:DescribeDBClusters",
    "rds:DescribeDBClusterSnapshots",
    "rds:CopyDBClusterSnapshot"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "rds:DeleteDBSnapshot",
        "rds:ModifyDBSnapshotAttribute"
      ],
      "Resource":[
        "arn:aws:rds:*:*:snapshot:awsbackup:*"
      ]
    },
    {
      "Effect": "Allow",
   "Action": [
    "rds:DeleteDBClusterSnapshot",
    "rds:ModifyDBClusterSnapshotAttribute"
   ],
   "Resource": [
    "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
   ]
    },
```

```
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Action":"kms:DescribeKey",
      "Effect":"Allow",
      "Resource":"*"
    }
  ]
}
```

Amazon Aurora

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "rds:CreateDBClusterSnapshot",
        "rds:DescribeDBClusters",
        "rds:DescribeDBClusterSnapshots",
        "rds:AddTagsToResource",
        "rds:ListTagsForResource",
        "rds:CopyDBClusterSnapshot"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
```

```
        "rds:DeleteDBClusterSnapshot"
      ],
      "Resource":[
        "arn:aws:rds:*:*:cluster-snapshot:awsbackup:*"
      ]
    },
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Action":"kms:DescribeKey",
      "Effect":"Allow",
      "Resource":"*"
    }
  ]
}
```

Storage Gateway

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "storagegateway:CreateSnapshot",
        "storagegateway:ListTagsForResource"
      ],
      "Resource":"arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
```

```
      "Effect":"Allow",
      "Action":[
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource":"arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeSnapshots"
      ],
      "Resource":"*"
    },
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    }
  ]
}
```

Amazon FSx

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Action": "fsx:DescribeBackups",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    },
    {
```

```
      "Action": "fsx:CreateBackup",
      "Effect": "Allow",
      "Resource": [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Action": "fsx:DescribeFileSystems",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Action": "fsx:ListTagsForResource",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Action": "fsx:DeleteBackup",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:ListTagsForResource",
        "fsx:ManageBackupPrincipalAssociations",
        "fsx:CopyBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:*:*:backup/*"
    }
  ]
}
```

Amazon EC2

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
```

```
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource":"arn:aws:ec2:*::snapshot/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateImage",
        "ec2:DeregisterImage"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CopyImage",
        "ec2:CopySnapshot"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateTags"
      ],
      "Resource":"arn:aws:ec2:*:*:image/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests"
      ],
      "Resource":"*"
    },
    {
```

```
      "Effect":"Allow",
      "Action":[
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
        "ec2:DescribeSnapshots"
      ],
      "Resource":[
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    }
  ]
}
```

Windows VSS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateTags",
        "ec2:DeleteSnapshot"
      ],
      "Resource":"arn:aws:ec2:*::snapshot/*"
    },
```

```
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateImage",
        "ec2:DeregisterImage"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CopyImage",
        "ec2:CopySnapshot"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateTags"
      ],
      "Resource":"arn:aws:ec2:*:*:image/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeSnapshots",
        "ec2:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceCreditSpecifications",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeElasticGpus",
        "ec2:DescribeSpotInstanceRequests"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeVolumes",
```

```
        "ec2:DescribeSnapshots"
      ],
      "Resource":[
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Action":[
        "tag:GetResources"
      ],
      "Resource":"*",
      "Effect":"Allow"
    },
    {
      "Effect":"Allow",
      "Action":[
        "backup:DescribeBackupVault",
        "backup:CopyIntoBackupVault"
      ],
      "Resource":"arn:aws:backup:*:*:backup-vault:*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ssm:CancelCommand",
        "ssm:GetCommandInvocation"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":"ssm:SendCommand",
      "Resource":[
        "arn:aws:ssm:*:*:document/AWSEC2-CreateVssSnapshot",
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}
```

資源還原政策

下列原則會針對個別 AWS Backup支援的 AWS 服務和協力廠商應用程式指定還原權限。您可以將它們自訂並附加至您建立的角色，以進一步限制對 AWS 資源的存取。

Amazon S3

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"S3BucketRestorePermissions",
      "Action":[
        "s3:CreateBucket",
        "s3:ListBucketVersions",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:PutBucketVersioning"
      ],
      "Effect":"Allow",
      "Resource":[
        "arn:aws:s3:::*"
      ]
    },
    {
      "Sid":"S3ObjectRestorePermissions",
      "Action":[
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:DeleteObject",
        "s3:PutObjectVersionAcl",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectTagging",
        "s3:PutObjectTagging",
        "s3:GetObjectAcl",
        "s3:PutObjectAcl",
        "s3:PutObject",
        "s3:ListMultipartUploadParts"
      ],
      "Effect":"Allow",
      "Resource":[
        "arn:aws:s3:::*/*"
      ]
```

```
    },
    {
      "Sid":"S3KMSPermissions",
      "Action":[
        "kms:Decrypt",
        "kms:DescribeKey",
        "kms:GenerateDataKey"
      ],
      "Effect":"Allow",
      "Resource":"*",
      "Condition":{
        "StringLike":{
          "kms:ViaService":"s3.*.amazonaws.com"
        }
      }
    }
  ]
}
```

VM

```
{
      "Sid": "GatewayRestorePermissions",
      "Effect": "Allow",
      "Action": [
        "backup-gateway:Restore"
      ],
      "Resource": "arn:aws:backup-gateway:*:*:hypervisor/*"
    }
```

Amazon EBS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource":[
        "arn:aws:ec2:*::snapshot/*",
```

```
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
    }
  ]
}
```

Amazon EFS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "elasticfilesystem:Restore",
        "elasticfilesystem:CreateFilesystem",
        "elasticfilesystem:DescribeFilesystems",
        "elasticfilesystem:DeleteFilesystem"
      ],
      "Resource":"arn:aws:elasticfilesystem:*:*:file-system/*"
    }
  ]
}
```

Amazon RDS

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "rds:DescribeDBInstances",
        "rds:DescribeDBSnapshots",
        "rds:ListTagsForResource",
```

```
        "rds:RestoreDBInstanceFromDBSnapshot",
        "rds:DeleteDBInstance",
        "rds:AddTagsToResource"
      ],
      "Resource":"*"
    }
  ]
}
```

Amazon Aurora

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "rds:DeleteDBCluster",
        "rds:DescribeDBClusters",
        "rds:RestoreDBClusterFromSnapshot",
        "rds:ListTagsForResource",
        "rds:AddTagsToResource"
      ],
      "Resource":"*"
    }
  ]
}
```

Storage Gateway

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "storagegateway:DeleteVolume",
        "storagegateway:DescribeCachediSCSIVolumes",
        "storagegateway:DescribeStorediSCSIVolumes"
      ],
      "Resource":"arn:aws:storagegateway:*:*:gateway/*/volume/*"
    },
    {
```

```
      "Effect":"Allow",
      "Action":[
        "storagegateway:DescribeGatewayInformation",
        "storagegateway:CreateStorediSCSIVolume",
        "storagegateway:CreateCachediSCSIVolume"
      ],
      "Resource":"arn:aws:storagegateway:*:*:gateway/*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "storagegateway:ListVolumes"
      ],
      "Resource":"arn:aws:storagegateway:*:*:*"
    }
  ]
}
```

Amazon FSx

```
{
  "Version": "2012-10-17",
  "Statement":
  [
    {
      "Action":
      [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Effect": "Allow",
      "Resource":
      [
        "arn:aws:fsx:*:*:file-system/*",
        "arn:aws:fsx:*:*:backup/*"
      ]
    },
    {
      "Action": "fsx:DescribeFileSystems",
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:file-system/*"
    },
    {
      "Action": "fsx:DescribeBackups",
```

```
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:backup/*"
    },
    {
      "Action":
      [
        "fsx:DeleteFileSystem",
        "fsx:UntagResource"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:fsx:*:*:file-system/*",
      "Condition":
      {
        "Null":
        {
          "aws:ResourceTag/aws:backup:source-resource": "false"
        }
      }
    },
    {
      "Action": "ds:DescribeDirectories",
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

Amazon EC2

```
{
  "Version":"2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":[
        "ec2:CreateVolume",
        "ec2:DeleteVolume"
      ],
      "Resource":[
        "arn:aws:ec2:*::snapshot/*",
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
```

```
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeSnapshots",
        "ec2:DescribeVolumes"
      ],
      "Resource":"*"
    },
    {
      "Effect":"Allow",
      "Action":[
        "ec2:DescribeImages",
        "ec2:DescribeInstances"
      ],
      "Resource":"*"
    },
    {
      "Action":[
        "ec2:RunInstances"
      ],
      "Effect":"Allow",
      "Resource":"*"
    },
    {
      "Action":[
        "ec2:TerminateInstances"
      ],
      "Effect":"Allow",
      "Resource":"arn:aws:ec2:*:*:instance/*"
    },
    {
      "Action":"iam:PassRole",
      "Resource":"arn:aws:iam::<account-id>:role/<role-name>",
      "Effect":"Allow"
    }
  ]
}
```

若要還原加密的備份，請執行下列其中一個動作

- 將您的角色新增至 AWS Key Management Service (AWS KMS) 金鑰原則的允許清單
- 將此政策連接到您的 IAM 角色以進行還原：

```
{
  "Action": [
     "kms:DescribeKey",
     "kms:Decrypt",
     "kms:Encrypt",
     "kms:GenerateDataKey",
     "kms:ReEncrypt*"
  ],
  "Effect": "Allow",
  "Resource": "*"
}
```

AWS 受管理政策

AWS 受管理的政策旨在為許多常見使用案例提供權限。 AWS 受管理的原則可讓您輕鬆地將適當的權限指派給使用者、群組和角色，而不是必須自行撰寫原則。

不過，您無法變更 AWS 受管理原則中定義的權限。 AWS 偶爾會更新受 AWS 管理策略中定義的權限。執行這項動作時，更新會影響政策連接到的所有委託人實體 (使用者、群組和角色)。

AWS Backup 針對常見使用案例提供數個 AWS 受管理的策略。這些政策可讓您更輕鬆地定義適當的許可，和控管對您備份的存取。受管政策有兩種。其中一種是設計用來指派給使用者，以控制這些使用者對 AWS Backup的存取。另一種受管政策是設計用來連接到您傳遞給 AWS Backup的角色。下表列出了 AWS Backup 提供的所有受管政策，並說明這些政策的定義。您可以在 IAM 主控台的 政策 區段中找到這些受管政策。

政策	受管政策名稱	描述
AWS Backup Backup 的服務連結角色原則	AWSBackupServiceLinkedRolePolicyforBackup	此原則會附加至名為的服務連結角色，AWSServiceRoleforBackup以 AWS Backup 允許代表您呼叫 AWS 服務以管理備份。 如需更多資訊，請參閱適用於 AWS Backup的服務連結角色許可。

政策	受管政策名稱	描述
AWS Backup 資料傳輸存取	AWSBackupDataTransferAccess	此原則提供 AWS Backup 儲存平面資料傳輸 API 的權限，允許 AWS Backint 代理程式透過 AWS Backup 儲存平面完成備份資料傳輸。使用者可以將此政策連接到使用 Backint Agent 執行 SAP HANA 的 Amazon EC2 執行個體所擔任的角色。
AWS Backup 還原存取權	AWSBackupRestoreAccessForSAPHANA	此政策提供在 Amazon EC2 上還原 SAP HANA 備份的 AWS Backup 許可。
AWS Backup 對於 Amazon S3 Backup 政策	AWSBackupServiceRolePolicyForS3Backup	此政策包含備份任何 S3 儲存貯體所需的許可。 AWS Backup 這包括存取值區中所有物件以及任何關聯 AWS KMS 金鑰的存取權。
AWS Backup 對於 Amazon S3 恢復政策	AWSBackupServiceRolePolicyForS3Restore	此政策包含將 S3 備份還原 AWS Backup 到儲存貯體所需的許可。這包括存儲桶的讀取和寫入許可，以及與 S3 操作有關的任何 AWS KMS 密鑰的使用。

政策	受管政策名稱	描述
Backup 稽核 IAM 政策	AWSBackupAuditAccess	此原則授予使用者建立控制項和架構的權限，以定義他們對 AWS Backup 資源和活動的期望，以及根據其定義的控制項和架構稽核 AWS Backup 資源和活動。此政策授予權限 AWS Config 和類似服務，以描述使用者期望執行稽核。 此政策也授予提供稽核報告給 Amazon S3 和類似服務的許可，並可讓使用者尋找和開啟其稽核報告。
AWS Backup 報告的服務角色原則	AWSServiceRolePolicyForBackupReports	AWS Backup 針對AWSServiceRoleForBackupReports 服務連結角色使用此原則。這個服務連結角色可讓 AWS Backup 您監控並報告您的備份設定、工作和資源與架構的合規性。
備份管理員 IAM 政策	AWSBackupFullAccess	備份管理員擁有完整的 AWS Backup 作業存取權，包括建立或編輯備份計畫、將 AWS 資源指定給備份計畫，以及還原備份。備份管理員會負責制定符合其組織業務與法規要求的備份計劃，以判定和強制執行備份合規。Backup 管理員也會確保其組織的 AWS 資源已指派給適當的計劃。

政策	受管政策名稱	描述
備份操作人員 IAM 政策	AWSBackupOperatorAccess	備份操作人員是使用者，負責確保所經手的資源能夠正確地備份。Backup 操作員具有將 AWS 資源指派給備份管理員建立的備份計劃的權限。他們也有權限建立其 AWS 資源的隨選備份，以及設定隨選備份的保留期限。備份操作人員不具有許可，來建立或編輯備份計劃，或是在排程備份建立後刪除這些備份。備份操作人員可以還原備份。您可以限制備份操作人員能夠指派給備份計劃或從備份還原的資源類型。您可以透過僅允許將某些服務角色傳遞給 AWS Backup 具有特定資源類型權限的服務角色來達到此目的。
Backup 管理員 AWS Organizations 原則	AWSBackupOrganizationAdminAccess	組織管理員擁有完整的 AWS Organizations 作業存取權，包括建立、編輯或刪除備份策略、將備份策略指定給帳號和組織單位，以及監視組織內的備份活動。組織管理員負責定義和指派符合組織業務和法規要求的備份政策，以保護組織中的帳戶。
備份的預設服務角色政策	AWSBackupServiceRolePolicyForBackup	提供代表您建立所有受支援資源類型備份的 AWS Backup 權限。

政策	受管政策名稱	描述
回復的預設服務角色政策	AWSBackupServiceRolePolicyForRestores	提供代表您還原所有受支援資源類型備份的 AWS Backup 權限。對於 EC2 執行個體還原，您還必須包含以下許可才能啟動 EC2 執行個體： `{ "Version": "2012-10-17", "Statement": [ { "Action": "iam:PassRole", "Resource": "arn:aws:iam:: account-id :role/role-name ", "Effect": "Allow" } ] }`

政策更新 AWS Backup

AWS 服務會維護和更新 AWS 受管理的策略。您無法變更 AWS 受管理原則中的權限。服務有時會將其他權限新增至受 AWS 管理的策略，以支援新功能。此類型的更新會影響已連接政策的所有身分識別 (使用者、群組和角色)。當新功能啟動或新作業可用時，服務最有可能更新 AWS 受管理的策略。服務不會從 AWS 受管理的政策移除權限，因此政策更新不會破壞您現有的權限。

此外，還 AWS 支援跨多個服務之工作職能的受管理原則。例如，ReadOnlyAccess AWS 受管理的策略提供對所有 AWS 服務和資源的唯讀存取權。當服務啟動新功能時，會為新作業和資源新 AWS 增唯讀權限。如需任務職能政策的清單和說明，請參閱 IAM 使用者指南中有關任務職能的AWS 受管政策。

檢視 AWS Backup 自此服務開始追蹤這些變更以來的 AWS 受管理策略更新詳細資料。如需有關此頁面變更的自動警示，請訂閱「 AWS Backup 文件歷史記錄」頁面上的 RSS 摘要。

變更	描述	日期
AWSBackupServiceRolePolicyForRestores-增加了許可以支持 AWS Backup 轉換到 Amazon 彈性區塊商店存檔存儲層	AWS Backup 添加了權限`ec2:DescribeSnapshotTierStatus` 和`ec2:RestoreSnapshotTier` . 使用者需要這些許可，才能選擇 AWS Backup 從存檔儲存還原與一起存放的 Amazon EBS 資源。 對於 EC2 執行個體還原，您還必須包含以下政策陳述式中所示的許可才能啟動 EC2 執行個體：	2023 年 11 月 27 日
AWSBackupServiceRolePolicyForBackups-增加了許可以支持 AWS Backup 轉換到 Amazon 彈性區塊商店存檔存儲層	AWS Backup 新增許可`ec2:DescribeSnapshotTierStatus` 並`ec2:ModifySnapshotTier` 支援額外的儲存選項，以便將備份的 Amazon EBS 資源轉換至存檔儲存層。 使用者需要這些許可，才能選擇將存放的 Amazon EBS 資源轉換為存檔儲存。 AWS Backup	2023 年 11 月 27 日
AWSBackupServiceLinkedRolePolicyForBackup-增	AWS Backup 新增許可`ec2:Descr`	

變更	描述	日期
加了許可以支持 AWS Backup 轉換到 Amazon 彈性區塊商店存檔存儲層 — 還新增了許可以支援 Amazon Aurora 的持續備份和 PITR (point-in-time 還原)。	`ibeSnapshotTierSta tus` 並`ec2:Modif ySnapshotTier` 支援額外的儲存選項，以便將備份的 Amazon EBS 資源轉換至存檔儲存層。 使用者需要這些許可，才能選擇將存放的 Amazon EBS 資源轉換為存檔儲存。 AWS Backup AWS Backup 添加了權限 `rds:Descr ibeDBClusterSnapsh ots` `rds:Resto reDBClusterToPoint InTime` ，這對於 Aurora 叢集的 PITR（point-in-time 還原）是必需的。	

變更	描述	日期
AWSServiceRoleForBackupRestoreTesting-增加了新的服務鏈接角色。	AWS Backup 已新增名為的新服務連結角色 AWSServiceRoleForBackupRestoreTesting，提供備份權限以進行還原測試。 這個新的服務連結角色提 AWS Backup 供執行還原測試所需的權限。這些許可包括要在還原測試中包含之下列服務的動作 `list, read, and write`：Aurora、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS 和 Amazon S3。 此政策的變更追蹤已開始。	2023 年 11 月 27 日
AWSBackupFullAccess— 新增傳遞角色權限以支援還原測試。	AWS Backup 已新增`restore-testing.backup.amazonaws.com` 至`IamPassRolePermissions` 和`IamCreateServiceLinkedRolePermissions` 。這項新增功能對 AWS Backup 於代表客戶進行還原測試是必要的。	2023 年 11 月 27 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 新增許可以支援 Amazon Aurora 的持續備份和 PITR (point-in-time 還原)。	AWS Backup 添加了權限 `rds:DescribeDBClusterSnapshots` `rds:RestoreDBClusterToPointInTime` ，這對於 Aurora 叢集的 PITR（point-in-time 還原）是必需的。	2023 年 9 月 6 日
AWSBackupFullAccess— 增加了新的許可，以支持持續備份和 PITR（point-in-time 恢復）Amazon Aurora。	AWS Backup 已新增權限`rds:DescribeDBClusterAutomatedBackups` ，這是 Aurora 叢集持續備份和 point-in-time 還原所需的權限。	2023 年 9 月 6 日
AWSBackupOperatorAccess— 增加了新的許可，以支持持續備份和 PITR（point-in-time 恢復）Amazon Aurora。	AWS Backup 已新增權限`rds:DescribeDBClusterAutomatedBackups` ，這是 Aurora 叢集持續備份和 point-in-time 還原所需的權限。	2023 年 9 月 6 日

變更	描述	日期
AWSBackupServiceRolePolicyForBackup— 新增許可以支援 Amazon Aurora 的持續備份和 PITR (point-in-time 還原)。	AWS Backup 添加了權限`rds:DescribeDBClusterAutomatedBackups` 。此權限對於 AWS Backup 支援 Aurora 叢集的持續備份和 point-in-time 還原是必要的。 AWS Backup 新增了許可，`rds:DeleteDBClusterAutomatedBackups` 允許 AWS Backup 生命週期在保留期結束時刪除和取消 Amazon Aurora 連續恢復點的關聯性。Aurora 復原點需要此許可，才能避免轉換為 EXIPIRED 狀態。 AWS Backup 新增允許 AWS Backup 與 Aurora 叢集互動的權`rds:ModifyDBCluster` 限。這項新增讓使用者能夠根據所需的組態啟用或停用連續備份。	2023 年 9 月 6 日
AWSBackupFullAccess— 已新增取得新儲存庫類型之資源共用關聯的權限。	AWS Backup 已加入動作，`ram:GetResourceShareAssociations` 以授與使用者取得新 Vault 類型之資源共用關聯的權限。 AWS Backup 需要此額外權限才能與之互動 AWS RAM。	2023 年 8 月 8 日

變更	描述	日期
AWSBackupOperatorAccess— 已新增取得新儲存庫類型之資源共用關聯的權限。	AWS Backup 已加入動作，ram:GetResourceShareAssociations 以授與使用者取得新 Vault 類型之資源共用關聯的權限。 AWS Backup 需要此額外權限才能與之互動 AWS RAM。	2023 年 8 月 8 日
AWSBackupServiceRolePolicyForS3Backup— 增加了支持 Amazon S3 備份的新許可	AWS Backup 添加了權限s3:PutInventoryConfiguration 。 AWS Backup 需要此權限才能使用存儲桶庫存來提高備份性能速度。	2023 年 8 月 1 日
AWSBackupServiceRolePolicyForRestores-添加了在還原工作期間向資源添加標籤的權限。	AWS Backup 已新增下列動作，以授與使用者新增標籤以還原資源的權限：storagegateway:AddTagsToResource elasticfilesystem:TagResource 、ec2:CreateAction ，僅ec2:CreateTags 適用於包含RunInstances 或CreateVolume fsx:TagResource 、和cloudformation:TagResource 。 這些新增的權限對於 AWS Backup 在還原程序期間將標籤新增至資源是必要的。	2023 年 5 月 22 日

變更	描述	日期
AWSBackupAuditAccess— 已取代資源選取	AWS Backup 將 API 中的資源選取取代為萬`config:DescribeComplianceByConfigRule` 用字元資源。 此擴充的資源選取可讓使用者更輕鬆地選取資源，而且錯誤更少。	2023 年 4 月 11 日
AWSBackupServiceRolePolicyForRestores— 新增許可以支援加密的 Amazon Elastic File System 還原。	AWS Backup 新增以下使用客戶受管金鑰還原 Amazon EFS 的權`kms:GenerateDataKeyWithoutPlaintext` 限： 需要此更新才能協助確保使用者具有還原 Amazon EFS 資源所需的許可。	2023 年 3 月 27 日
AWSServiceRolePolicyForBackupReports-更新的動作	AWS Backup 已更新`config:DescribeConfigRules` 和`config:DescribeConfigRuleEvaluationStatus` 動作，以允許 AWS Backup Audit Manager 存取 AWS Backup 稽核管理員管理 AWS Config 的規則。 AWS Backup 需要此更新才能與之互動 AWS Config。	2023 年 3 月 9 日

變更	描述	日期
AWSBackupServiceRolePolicyForS3Restore— 為涉及 AWS KMS 加密的還原添加新權限	AWS Backup 已新增下列權限：kms:Decrypt s3:PutBucketOwnershipControls 、和s3:GetBucketOwnershipControls 至策略AWSBackupServiceRolePolicyForS3Restore 。 需要這些許可，才能在原始備份中使用 KMS 加密時支援還原物件，以及在原始儲存貯體 (而非 ACL) 上已設定物件擁有權時還原物件。	2023 年 2 月 13 日

變更	描述	日期
AWSBackupFullAccess— 增加了新的權限以支持 VMware 備份操作	AWS Backup 已新增下列權限：backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine backup-gateway:PutHypervisorPropertyMappings 、backup-gateway:GetHypervisor 、backup-gateway:StartVirtualMachinesMetadataSync 、、backup-gateway:GetBandwidthRateLimitSchedule 、和backup-gateway:PutBandwidthRateLimitSchedule 。 這些權限對 AWS Backup 於使用虛擬機器的 VMware 標籤排程備份，以及支援以排程為基礎的頻寬節流是必要的。	2022 年 12 月 15 日

變更	描述	日期
AWSBackupOperatorAccess- 增加了新的權限以支持備份操作	AWS Backup 已新增下列權限：backup-gateway:GetHypervisorPropertyMappings backup-gateway:GetVirtualMachine 、backup-gateway:GetHypervisor 、和backup-gateway:GetBandwidthRateLimitSchedule 。 這些權限對 AWS Backup 於使用虛擬機器的 VMware 標籤排程備份，以及支援以排程為基礎的頻寬節流是必要的。	2022 年 12 月 15 日
AWS Backup GatewayServiceRolePolicyForVirtualMachineMetadataSync— 增加了具有權限的新策略，以支持與虛擬機器的 AWS Backup 閘道同步。	AWS Backup 引入此原則，並在其中包含下列權限：backup-gateway:ListTagsForResource backup-gateway:TagResource 、和backup-gateway:UntagResource 。 AWS Backup Gateway 必須具備這些權限，才能將內部部署網路中虛擬機器的中繼資料與 Backup 閘道同步。	2022 年 12 月 15 日

變更	描述	日期
AWSBackupServiceRolePolicyForBackup— 增加了許可 AWS Backup 以備份 Amazon Timestream 資源。	AWS Backup 已新增下列權限：`timestream:StartAwsBackupJob` `timestream:GetAwsBackupStatus` `timestream:ListTables` 、`timestream:ListDatabases` 、`timestream:ListTagsForResource` 、、`timestream:DescribeTable` 、`timestream:DescribeDatabase` 、和`timestream:DescribeEndpoints` 。 這些權限是支援時間流備份工作所必需的 AWS Backup 。	2022 年 12 月 13 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 增加了許可 AWS Backup 以恢復 Amazon Timestream 資源。	AWS Backup 已新增下列權限：timestream:StartAwsRestoreJob timestream:GetAwsRestoreStatus timestream:ListTables 、timestream:ListTagsForResource 、timestream:ListDatabases 、timestream:DescribeTable 、、timestream:DescribeDatabase 、s3:GetBucketAcl 、和timestream:DescribeEndpoints 。 這些權限對於支援時間流還原工作而言是必要的 AWS Backup 。	2022 年 12 月 13 日
AWSBackupFullAccess— 增加了許可，以 AWS Backup 允許支持 Amazon Timestream 資源。	AWS Backup 已新增下列權限：timestream:ListTables timestream:ListDatabases 、s3:ListAllMyBuckets 和timestream:DescribeEndpoints 。 這些權限對於支援時間流資源是必要的 AWS Backup 。	2022 年 12 月 13 日

變更	描述	日期
AWSBackupOperatorAccess— 增加了許可，以 AWS Backup 允許支持 Amazon Timestream 資源。	AWS Backup 已新增下列權限：`timestream:ListDatabases` `timestream:ListTables` 、`s3:ListAllMyBuckets` 、和`timestream:DescribeEndpoints` 。 這些權限對於支援時間流資源是必要的 AWS Backup 。	2022 年 12 月 13 日
AWSBackupServiceLinkedRolePolicyForBackup— 更新的受管策略權限 AWS Backup 允許有必要的訪問 Timestream 資源備份功能.	AWS Backup 已新增下列權限：`timestream:ListDatabases` `timestream:ListTables` `timestream:ListTagsForResource` 、`timestream:DescribeDatabase` 、`timestream:DescribeTable` 、、`timestream:GetAwsBackupStatus` 、`timestream:GetAwsRestoreStatus` 、和`timestream:DescribeEndpoints` 。 這些權限對於支援時間流資源是必要的 AWS Backup 。	2022 年 12 月 13 日

變更	描述	日期
AWSBackupFullAccess— 增加了許可，以 AWS Backup 允許支持 Amazon Redshift 資源。	AWS Backup 已新增下列權限：`redshift:DescribeClusters` `redshift:DescribeClusterSubnetGroups` `redshift:DescribeNodeConfigurationOptions` 、`redshift:DescribeOrderableClusterOptions` 、`redshift:DescribeClusterParameterGroups` 、、`redshift:DescribeClusterTracks` 、`redshift:DescribeSnapshotSchedules` 、和`ec2:DescribeAddresses` 。 這些許 AWS Backup 可是利用 Amazon Redshift 資源所必需的。	2022 年 11 月 27 日

變更	描述	日期
AWSBackupOperatorAccess— 增加了支持 Amazon Redshift 資源的許 AWS Backup 可。	AWS Backup 已新增下列權限：`redshift:DescribeClusters` `redshift:DescribeClusterSubnetGroups` 、`redshift:DescribeNodeConfigurationOptions` 、`redshift:DescribeOrderableClusterOptions` 、、`redshift:DescribeClusterParameterGroups`, 、`redshift:DescribeClusterTracks` 。 `redshift:DescribeSnapshotSchedules` ，和`ec2:DescribeAddresses` 。 這些許 AWS Backup 可是利用 Amazon Redshift 資源所必需的。	2022 年 11 月 27 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 增加了許可，以 AWS Backup 允許訪問 Amazon Redshift 資源。	AWS Backup 已新增下列權限：`redshift:RestoreFromClusterSnapshot` `redshift:RestoreTableFromClusterSnapshot` 、`redshift:DescribeClusters` 、和`redshift:DescribeTableRestoreStatus` 。 AWS Backup 需要這些許可才能支援 Amazon Redshift 還原任務。	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup— 增加了許可，以 AWS Backup 允許訪問 Amazon Redshift 資源。	AWS Backup 已新增下列權限：`redshift:CreateClusterSnapshot` `redshift:DescribeClusterSnapshots` `redshift:DescribeTags` 、`redshift:DeleteClusterSnapshot` 、、`redshift:DescribeClusters` 、和`redshift:CreateTags` 。 AWS Backup 需要這些許可才能支援 Amazon Redshift 備份任務。	2022 年 11 月 27 日

變更	描述	日期
AWSBackupFullAccess-增加了允許支持 AWS Backup AWS CloudFormation 資源的權限。	AWS Backup 添加了以下權限：`cloudformation:ListStacks` 。此權限對於支援 CloudFormation 資源而言是必要的 Backup。	2022 年 11 月 27 日
AWSBackupOperatorAccess-增加了允許支持 AWS Backup AWS CloudFormation 資源的權限。	AWS Backup 添加了以下權限：`cloudformation:ListStacks` 。此權限對於支援 CloudFormation 資源而言是必要的 Backup。	2022 年 11 月 27 日
AWSBackupServiceLinkedRolePolicyForBackup—增加了允許支持 AWS Backup AWS CloudFormation 資源的權限。	AWS Backup 已新增下列權限：`redshift:DescribeClusterSnapshots` `redshift:DescribeTags` 、`redshift:DeleteClusterSnapshot` 、和`redshift:DescribeClusters` 。 這些權限是支援 CloudFormation資源的 Backup 所必需的。	2022 年 11 月 27 日

變更	描述	日期
AWSBackupServiceRolePolicyForBackup— 增加了允許訪問 AWS Backup AWS CloudFormation 資源的權限。	AWS Backup 已新增下列權限：`cloudformation:GetTemplate cloudformation:DescribeStacks` 、和`cloudformation:ListStackResources` 。 這些權限對於支援 AWS CloudFormation 應用程式堆疊備份工作而言是必要的 AWS Backup 。	2022 年 11 月 16 日
AWSBackupServiceRolePolicyForRestores— 增加了允許訪問 AWS Backup AWS CloudFormation 資源的權限。	AWS Backup 添加了以下權限：`cloudformation:CreateChangeSet cloudformation:DescribeChangeSet` 這些權限對於支援 AWS CloudFormation 應用程式堆疊還原工作而言是必要的 AWS Backup 。	2022 年 11 月 16 日

變更	描述	日期
AWSBackupOrganizationAdminAccess— 針對委派管理員功能 AWS Backup 新增此原則的權限。	AWS Backup 將下列權限新增至此原則：`organizations:ListDelegatedAdministrator organizations:RegisterDelegatedAdministrator` 、和 `organizations:DeregisterDelegatedAdministrator` 需要這些許可，才能讓組織管理員使用「委派的管理員」功能。	2022 年 11 月 27 日
AWSBackupServiceRolePolicyForBackup— 增加了許可， AWS Backup 以允許在 Amazon EC2 實例上支持 SAP HANA。	AWS Backup 已新增下列權限：`ssm-sap:GetOperation ssm-sap:ListDatabases ssm-sap:BackupDatabase` 、`ssm-sap:UpdateHanaBackupSettings` 、、`ssm-sap:GetDatabase` 、和`ssm-sap:ListTagsForResource` 。 Backup 需要這些許可，才能支援 Amazon EC2 執行個體上的 SAP HANA。	2022 年 11 月 20 日

變更	描述	日期
AWSBackupFullAccess— 增加了許可，以允許在 Amazon EC2 實例上 AWS Backup 支持 SAP HANA。	AWS Backup 已新增下列權限：`ssm-sap:GetOperation` `ssm-sap:ListDatabases` 、`ssm-sap:GetDatabase` 、和`ssm-sap:ListTagsForResource` 。 Backup 需要這些許可，才能支援 Amazon EC2 執行個體上的 SAP HANA。	2022 年 11 月 20 日
AWSBackupOperatorAccess— 增加了許可，以允許在 Amazon EC2 實例上 AWS Backup 支持 SAP HANA。	AWS Backup 已新增下列權限：`ssm-sap:GetOperation` `ssm-sap:ListDatabases` 、`ssm-sap:GetDatabase` 、和`ssm-sap:ListTagsForResource` 。 Backup 需要這些許可，才能支援 Amazon EC2 執行個體上的 SAP HANA。	2022 年 11 月 20 日
AWSBackupServiceLinkedRolePolicyForBackup— 增加了允許在 Amazon EC2 實例上 AWS Backup 支持 SAP HANA 的許可。	AWS Backup 添加了以下權限：`ssm-sap:GetOperation` 。 Backup 需要此許可，才能支援 Amazon EC2 執行個體上的 SAP HANA。	2022 年 11 月 20 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 增加了許可 AWS Backup 以訪問 Amazon EC2 資源。	AWS Backup 添加了以下權限：`ec2:CreateTags` 。 此權限對於 AWS Backup 支援 EC2 執行個體的 Backup 閘道還原任務是必要的。	2022 年 11 月 20 日
AWSBackupDataTransferAccess— 新增許可，允許 AWS Backup 在亞馬遜 EC2 執行個體資源上支援 SAP HANA 的安全儲存資料傳輸。	AWS Backup 已新增下列權限：`backup-storage:StartObject backup-storage:PutChunk backup-storage:GetChunk 、backup-storage:ListChunks 、backup-storage:ListObjects 、、backup-storage:GetObjectMetadata 、和backup-storage:NotifyObjectComplete` 。 這些許可對於 AWS Backup 支援 SAP HANA 在 Amazon EC2 資源上進行安全的儲存資料傳輸是必要的。	2022 年 11 月 20 日

變更	描述	日期
AWSBackupRestoreAccessForSAPHANA— 為資料擁有者新增許可，可在 Amazon EC2 執行個體資源上執行 SAP HANA 的還原任務。	AWS Backup 已新增下列權限：backup:Get* backup:List* backup:Describe* 、backup:StartBackupJob 、backup:StartRestoreJob 、ssm-sap:GetOperation 、ssm-sap:ListDatabases 、ssm-sap:BackupDatabase 、ssm-sap:RestoreDatabase 、ssm-sap:UpdateHanaBackupSettings 、ssm-sap:GetDatabase 、和ssm-sap:ListTagsForResource 。 資源擁有者需要這些許可，才能執行 Amazon EC2 上 SAP HANA 資源的還原。	2022 年 11 月 20 日
AWSBackupServiceRolePolicyForS3Backup— 增加了支持 Amazon S3 備份的新許可	AWS Backup 添加了權限s3:GetBucketAcl 。 AWS Backup S3 的 AWS Backup 備份操作需要此權限。	2022 年 8 月 24 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 增加了對 Amazon RDS 恢復任務的訪問權限。	AWS Backup 已新增下列動作以授與建立資料庫執行處理的存取權：`rds:CreateDBInstance` AWS Backup 需要此權限才能支援 Amazon RDS 多重可用區域 (異地同步備份) 功能。	2022 年 7 月 20 日
AWSBackupServiceLinkedRolePolicyForBackup-增加了支持 Amazon S3 備份的權限	AWS Backup 添加了`s3:GetBucketTagging` 權限，以授予用戶選擇要使用資源通配符進行備份的存儲桶的權限。如果沒有此許可，使用者將無法使用資源萬用字元選取要備份的儲存貯體。 AWS Backup 需要該許可才能支援 Amazon S3 資料。	2022 年 5 月 6 日
AWSBackupServiceRolePolicyForBackup-增加了新的權限，以支持 FSx 進行 ONTAP 音量級別備份。	AWS Backup 在現有`fsx:CreateBackup` 和動`fsx:ListTagsForResource` 作範圍內新增磁碟區資源，並新增新動作`fsx:DescribeVolumes` 以支援 FSx 進行 ONTAP 磁碟區層級備份。 AWS Backup 需要此權限才能支援 FSx 的 ONTAP。	2022 年 4 月 27 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 新增權限以支援還原 ONTAP 磁碟區的 FSx。	AWS Backup 已新增下列動作，以授與使用者還原 ONTAP 磁碟區`fsx:DescribeVolumes` 、`fsx:CreateVolumeFromBackup` 、和 FSx 的權`fsx:DeleteVolume` 限。`fsx:UntagResource` AWS Backup 需要此權限才能支援 FSx 的 ONTAP。	2022 年 4 月 27 日
AWSBackupServiceRolePolicyForS3Backup— 增加了新的許可以支持 Amazon S3 備份	AWS Backup 已新增下列動作，以授與使用者在備份操作期間接收 Amazon S3 儲存貯體變更通知的權限：`s3:GetBucketNotification` 和`s3:PutBucketNotification` 。 AWS Backup 需要這些許可才能支援 Amazon S3 資料。	2022 年 2 月 25 日

變更	描述	日期
AWSBackupServiceRolePolicyForS3Backup— 增加了新的 AWS 受管政策以支持 Amazon S3 備份	在新的AWSBackupServiceRolePolicyForS3Backup AWS 受管政策中，新 AWS Backup 增下列動作以授與使用者備份其 Amazon S3 儲存貯體的許可：s3:GetInventoryConfiguration s3:PutInventoryConfiguration s3:ListBucketVersions s3:ListBucket 、、s3:GetBucketTagging 、s3:GetBucketVersioning 、s3:GetBucketNotification 、、s3:GetBucketLocation 、和s3:ListAllMyBuckets AWS Backup 新增下列動作以授與使用者備份其 Amazon S3 物件的權限：s3:GetObject s3GetObjectAcl s3:GetObjectVersionTagging 、s3:GetObjectVersionAcl 、s3:GetObjectTagging 、、和s3:GetObjectVersion 。 AWS Backup 已新增下列動作，以授與使用者備	2022 年 2 月 17 日

變更	描述	日期
	份其加密 Amazon S3 資料的權限：kms:Decrypt 和kms:DescribeKey 。 AWS Backup 新增以下動作以授予使用者使用 Amazon EventBridge 規則對其 Amazon S3 資料進行增量備份的許可：events:DescribeRule events:EnableRule events:PutRule events:DeleteRule events:PutTargets 、events:RemoveTargets 、events:ListTargetsByRule 、events:DisableRule 、cloudwatch:GetMetricData 、、和events:ListRules 。 AWS Backup 需要這些許可才能支援 Amazon S3 資料。	

變更	描述	日期
AWSBackupServiceRolePolicyForS3Restore-添加了新的 AWS 受管政策以支持 Amazon S3 恢復	在新的AWSBackupServiceRolePolicyForS3Restore AWS 受管政策中，新 AWS Backup 增下列動作以授與使用者還原 Amazon S3 儲存貯體的許可：s3:CreateBucket s3:ListBucketVersions s3:ListBucket 、s3:GetBucketVersioning 、s3:GetBucketLocation 、、和s3:PutBucketVersioning 。 AWS Backup 新增以下動作以授予使用者還原其 Amazon S3 儲存貯體的許可：s3:GetObject s3:GetObjectVersion s3:DeleteObject s3:PutObjectVersionAcl 、s3:GetObjectVersionAcl 、s3:GetObjectTagging 、s3:PutObjectTagging 、、s3:GetObjectAcl 、s3:PutObjectAcl 、s3:PutObject 、、和s3:ListMultipartUploadParts 。	2022 年 2 月 17 日

變更	描述	日期
	AWS Backup 已新增下列動作，以授與使用者加密其還原的 Amazon S3 資料的權限：`kms:Decrypt` `kms:DescribeKey` 、和`kms:GenerateDataKey` 。 AWS Backup 需要這些許可才能支援 Amazon S3 資料。	
AWSBackupServiceLinkedRolePolicyForBackup-增加了支持 Amazon S3 備份的權限	AWS Backup 已新增`s3:ListAllMyBuckets` 以授與使用者檢視其值區清單的權限，並選擇要指派給備份計劃的值區。 AWS Backup 需要該許可才能支援 Amazon S3 資料。	2022 年 2 月 14 日
AWSBackupServiceLinkedRolePolicyForBackup-增加了列出 AWS Backup 網關資源的權限	AWS Backup 已新增`backup-gateway:ListVirtualMachines` 以授與使用者檢視其虛擬機器清單的權限，並選擇要指派給備份計畫的虛擬機器。 AWS Backup 也新增`backup-gateway:ListTagsForResource` 以授與使用者列出其虛擬機器標籤的權限。 AWS Backup 需要這些權限才能支援 2021 年 11 月 30 日推出的虛擬機器。	2021 年 11 月 30 日

變更	描述	日期
AWSBackupServiceRolePolicyForBackup— 增加了備份虛擬機的權限	AWS Backup 添加backup-gateway:Backup 以授予用戶權限還原其虛擬機備份。 AWS Backup 還添加了授backup-gateway:ListTagsForResource 予用戶權限，以列出分配給其虛擬機器備份的標籤。 AWS Backup 需要此權限才能支援 2021 年 11 月 30 日推出的虛擬機器。	2021 年 11 月 30 日
AWSBackupServiceRolePolicyForRestores— 增加了恢復虛擬機的權限	AWS Backup 添加backup-gateway:Restore 以授予用戶權限還原其虛擬機備份。 AWS Backup 需要此權限才能支援 2021 年 11 月 30 日推出的虛擬機器。	2021 年 11 月 30 日

變更	描述	日期
AWSBackupFullAccess— 增加了使用虛擬機的權限	AWS Backup 已新增下列動作，以授與使用者使用 AWS Backup Gateway 備份、還原和管理其虛擬機器的權限：backup-gateway:AssociateGatewayToServer backup-gateway:CreateGateway backup-gateway:DeleteGateway backup-gateway:DeleteHypervisor backup-gateway:DisassociateGatewayFromServer backup-gateway:ImportHypervisorConfiguration 、backup-gateway:ListGateways 、、backup-gateway:ListHypervisors 、backup-gateway:ListTagsForResource 、backup-gateway:ListVirtualMachines 、backup-gateway:PutMaintenanceStartTime 、、backup-gateway:TagResource 、backup-gateway:TestHypervisorConfiguration 、backup-ga	2021 年 11 月 30 日

變更	描述	日期
	teway:UntagResource 、backup-gateway:UpdateGatewayInformation 、、和backup-gateway:UpdateHypervisor 。 AWS Backup 需要此許可才能支持 2021 年 11 月 30 日啟動的 AWS Backup 網關。	
AWSBackupOperatorAccess-增加了列出 AWS Backup 網關資源的權限	AWS Backup 已新增下列動作，以授與使用者備份其虛擬機器的權限：backup-gateway:ListGateways backup-gateway:ListHypervisors backup-gateway:ListTagsForResource 、、和backup-gateway:ListVirtualMachines 。 AWS Backup 需要此權限才能支援 2021 年 11 月 30 日推出的虛擬機器。	2021 年 11 月 30 日

變更	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup-添加了備份 Amazon DynamoDB 的權限	AWS Backup 已新增`dynamodb:ListTags0fResource` 以授與使用者權限，讓使用者列出其 DynamoDB 表格的標籤以使用 AWS Backup的進階 DynamoDB 備份功能進行備份。 AWS Backup 需要此權限才能使用 2021 年 11 月 23 日推出的進階 DynamoDB 備份功能。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForBackup— 添加了備份 Amazon DynamoDB 的許可	AWS Backup 已新增`dynamodb:StartAwsBackupJob` 以授與使用者使用進階備份功能備份其 DynamoDB 表格的權限。 AWS Backup 此外，還新`dynamodb:ListTags0fResource` 增了授與使用者將標籤從其來源 DynamoDB 表複製到其備份的權限。 AWS Backup 需要這些權限才能使用 2021 年 11 月 23 日推出的進階 DynamoDB 備份功能。	2021 年 11 月 23 日

變更	描述	日期
AWSBackupServiceLinkedRolePolicyForRestores— 增加了恢復 Amazon DynamoDB 的許可	AWS Backup 已新增`dynamodb:RestoreTableFromAwsBackup` 以授與使用者權限，還原使用進階 DynamoDB 進階備份功能備份 AWS Backup的 DynamoDB 表格。 AWS Backup 需要此權限才能還原使用 2021 年 11 月 23 日推出 AWS Backup的進階 DynamoDB 功能建立的備份。	2021 年 11 月 23 日
AWSBackupServiceRolePolicyForRestores— 增加了恢復 Amazon DynamoDB 的許可	AWS Backup 已新增`dynamodb:RestoreTableFromAwsBackup` 以授與使用者權限，還原使用進階 DynamoDB 進階備份功能備份 AWS Backup的 DynamoDB 表格。 AWS Backup 需要此權限才能還原使用 2021 年 11 月 23 日推出 AWS Backup的進階 DynamoDB 功能建立的備份。	2021 年 11 月 23 日

變更	描述	日期
AWSBackupOperatorAccess-刪除多餘的動作	AWS Backup 刪除了現有的操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因為它們是多餘的。 AWS Backup 並不需要backup:GetRecoveryPointRestoreMetadata 和backup:Get* 作為AWSBackupOperatorAccess AWS 受管策略的一部分。此外，也 AWS Backup 不需要rds:DescribeDBSnapshots 和rds:describeDBSnapshots 作為AWSBackupOperatorAccess AWS 受管理策略的一部分。	2021 年 11 月 23 日

變更	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup-添加了權限，以支持對備份計劃的細粒度資源分配	AWS Backup 新增了新動作elasticfilesystem:DescribeFileSystems 、dynamodb:ListTables 、storagegateway:ListVolumes 、ec2:DescribeVolumes 、ec2:DescribeInstances 、和 rds:DescribeDBInstances rds:DescribeDBClusters ，以fsx:DescribeFileSystems 便客戶在選取要指派給備份計劃的資源時，從 AWS Backup支援的資源清單中檢視和選擇。 AWS Backup 需要這些權限，才能為客戶提供額外、靈活的方式，將資源指派給備份計劃。	2021 年 11 月 10 日
AWSBackupAuditAccess-增加了新的政策	AWS Backup 已新增AWSBackupAuditAccess 以授與使用者使用 AWS Backup Audit Manager 的權限。這些許可包括設定合規架構及產生報告的能力。 AWS Backup AWS Backup 審計經理需要此許可，該 Audit Manager 於 2021 年 8 月 24 日推出。	2021 年 8 月 24 日

變更	描述	日期
AWSServiceRolePolicyForBackupReports-增加了新的政策	AWS Backup 已新增`AWSServiceRolePolicyForBackupReports` 以授與服務連結角色的權限，以自動監視備份設定、工作和資源，以符合使用者設定的架構。 AWS Backup AWS Backup 審計經理需要此許可，該 Audit Manager 於 2021 年 8 月 24 日推出。	2021 年 8 月 24 日
AWSBackupFullAccess-添加了創建服務鏈接角色的權限	AWS Backup 新增`iam:CreateServiceLinkedRole` 以建立服務連結角色 (盡最大努力)，以自動為您刪除過期的復原點。如果沒有此服務連結角色， AWS Backup 則無法在客戶刪除用於建立復原點的原始 IAM 角色後刪除過期的復原點。 AWS Backup 作為 `DeleteRecoveryPoint` API 操作的一部分需要此權限。	2021 年 7 月 5 日

變更	描述	日期
AWSBackupServiceLinkedRolePolicyForBackup—增加了支援刪除 DynamoDB 復原點的權限	AWS Backup 已新增新動作，dynamodb:DeleteBackup 以授與DeleteRecoveryPoint 權限，以根據您的備份計劃生命週期設定自動刪除過期 DynamoDB 復原點。 AWS Backup 需要此權限才能在 DeleteRecoveryPoint API 作業中刪除 DynamoDB 資料表。	2021 年 7 月 5 日
AWSBackupOperatorAccess-刪除多餘的動作	AWS Backup 刪除了現有的操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因為它們是多餘的。 AWS Backup 並不需要backup:GetRecoveryPointRestoreMetadata 和backup:Get* 作為AWSBackupOperatorAccess AWS 受管策略的一部分。此外，也 AWS Backup 不需要rds:DescribeDBSnapshots 和rds:describeDBSnapshots 作為AWSBackupOperatorAccess AWS 受管理策略的一部分。	2021 年 5 月 25 日

變更	描述	日期
AWSBackupOperatorPolicy-刪除多餘的動作	AWS Backup 刪除了現有的操作backup:GetRecoveryPointRestoreMetadata ，rds:DescribeDBSnapshots 因為它們是多餘的。 AWS Backup 並不需要backup:GetRecoveryPointRestoreMetadata 和backup:Get* 作為AWSBackupOperatorPolicy AWS 受管策略的一部分。此外，也 AWS Backup 不需要rds:DescribeDBSnapshots 和rds:describeDBSnapshots 作為AWSBackupOperatorPolicy AWS 受管理策略的一部分。	2021 年 5 月 25 日
AWSBackupServiceRolePolicyForRestores-增加了將標籤應用於 Amazon FSx 恢復的許可	AWS Backup 已新增新動作，fsx:TagResource 以授與StartRestoreJob 權限，以允許您在還原程序期間將標籤套用至 Amazon FSx 檔案系統。 AWS Backup 需要此權限才能將標籤套用至 Amazon FSx 檔案系統，做為 StartRestoreJob API 作業的一部分。	2021 年 5 月 24 日

變更	描述	日期
AWSBackupServiceRolePolicyForRestores— 增加了執行 Amazon EC2 恢復的許可	AWS Backup 添加了新操作`ec2:DescribeImages` 並授`ec2:DescribeInstances` 予`StartRestoreJob` 許可，以允許您從恢復點還原 Amazon EC2 實例。 AWS Backup 需要此權限才能從復原點還原 Amazon EC2 執行個體，做為 `StartRestoreJob` API 作業的一部分。	2021 年 5 月 24 日
AWSBackupServiceRolePolicyForBackup— 增加了執行 Amazon FSx 跨區域和跨帳戶副本的許可	AWS Backup 添加了新操作`fsx:CopyBackup` 以授予`StartCopyJob` 許可，以允許您跨區域和帳戶複製 Amazon FSx 恢復點。 AWS Backup 需要此權限才能跨區域和帳戶複製 Amazon FSx 復原點，做為 `StartCopyJob` API 作業的一部分。	2021 年 4 月 12 日
AWSBackupServiceLinkedRolePolicyForBackup-增加了權限執行 Amazon FSx 跨區域和跨帳戶副本	AWS Backup 添加了新操作`fsx:CopyBackup` 以授予`StartCopyJob` 許可，以允許您跨區域和帳戶複製 Amazon FSx 恢復點。 AWS Backup 需要此權限才能跨區域和帳戶複製 Amazon FSx 復原點，做為 `StartCopyJob` API 作業的一部分。	2021 年 4 月 12 日

變更	描述	日期
AWSBackupServiceRolePolicyForBackup— 新增權限以支援加密 DynamoDB 資料表備份	AWS Backup 更新其 AWS 受管理策略以符合下列要求： 若 AWS Backup 要建立加密 DynamoDB 表格的備份，您必須新增許可`kms:Decrypt` 和`kms:GenerateDataKey` 用於備份的 IAM 角色。	2021 年 3 月 10 日
AWSBackupFullAccess— 增加了許可以支持 Amazon RDS 連續備份和 point-in-time 恢復	AWS Backup 更新其 AWS 管理策略以符合以下要求： 若 AWS Backup 要用於設定 Amazon RDS 資料庫的連續 Backup，請確認 API 權限`rds:ModifyDBInstance` 存在於備份計劃組態定義的 IAM 角色中。 若要還原 Amazon RDS 連續備份，您必須將許可 `rds:RestoreDBInstanceToPointInTime` 新增至為還原任務提交的 IAM 角色。 在 AWS Backup 主控台中，若要描述可用於 point-in-time 復原的時間範圍，您必須在 IAM 管理的政策中包含 `rds:DescribeDBInstanceAutomatedBackups` API 權限。	2021 年 3 月 10 日
AWS Backup 開始追蹤變更	AWS Backup 開始追蹤其AWS管理政策的變更。	2021 年 3 月 10 日

使用 AWS Backup的服務連結角色

AWS Backup 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到 AWS Backup的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Backup 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

主題

使用角色以列出要備份、跨帳戶複製，以及自動備份 Amazon EFS 的資源

AWS Backup 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到 AWS Backup的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Backup 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Backup 更輕鬆地設定，因為您不必手動新增必要的權限。 AWS Backup 定義其服務連結角色的權限，除非另有定義，否則只 AWS Backup 能擔任其角色。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。這樣可以保護您的 AWS Backup 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (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。

服務連結角色權限 AWS Backup

AWS Backup 使用名為的服務連結角色 AWSServiceRoleForBackup— 提供列出可備份、跨帳戶複製備份以及自動備份 Amazon EFS 的資源的 AWS Backup 許可。

AWS Backup 此外，還會使用該角色刪除除 Amazon EC2 以外的所有資源類型的所有備份。

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

- `AWS Backup`

角色權限原則允許 AWS Backup 對指定的資源完成下列動作：

- 動作：`all resources AWS Backup supports` 上的 `list, read, write, and tag`

  有關特定權限，請參閱 AWS Identity and Access Management 控制台AWSBackupServiceLinkedRolePolicyForBackup中的策略。

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 AWS Backup建立服務連結角色

您不需要手動建立一個服務連結角色。當您列出要備份的資源、設定跨帳戶備份或在、或 AWS API 中執行 Amazon EFS 自動備份時 AWS CLI，會為您 AWS Backup 建立服務連結角色。 AWS Management Console

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

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。當您列出要備份的資源、設定跨帳戶備份，或執行 Amazon EFS 自動備份時， AWS Backup 會再次為您建立服務連結角色。

為 AWS Backup編輯服務連結角色

AWS Backup 不允許您編輯 AWSServiceRoleForBackup 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Backup刪除服務連結角色

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，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。首先，您必須刪除所有復原點。然後，您必須刪除所有備份保存庫。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS Backup 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘，然後再次嘗試操作。

若要刪除 AWSServiceRoleForBackup (控制台) 所使用的 AWS Backup 資源

1. 若要刪除所有復原點和備份保存庫 (預設保存庫除外)，請遵循刪除備份保存庫中的程序。
2. 若要刪除預設保存庫，請在 AWS CLI中使用下列指令：

```
aws backup delete-backup-vault --backup-vault-name Default --region us-east-1
```

若要刪除使用的 AWS Backup 資源 AWSServiceRoleForBackup (AWS CLI)

1. 若要刪除所有復原點，請使用delete-recovery-point。
2. 若要刪除所有備份保存庫，請使用 `delete-backup-vault`。

若要刪除使用的 AWS Backup 資源 AWSServiceRoleForBackup (API)

1. 若要刪除所有復原點，請使用 `DeleteRecoveryPoint`。
2. 若要刪除所有備份保存庫，請使用 `DeleteBackupVault`。

手動刪除服務連結角色

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

AWS Backup 服務連結角色的支援區域

AWS Backup 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Backup 支援的功能和區域。

使用 AWS Backup Audit Manager 的角色

AWS Backup 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到 AWS Backup的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Backup 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Backup 更輕鬆地設定，因為您不必手動新增必要的權限。 AWS Backup 定義其服務連結角色的權限，除非另有定義，否則只 AWS Backup 能擔任其角色。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。這樣可以保護您的 AWS Backup 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (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。

服務連結角色權限 AWS Backup

AWS Backup 使用名為的服務連結角色 AWSServiceRoleForBackupReports— 提 AWS Backup 供建立控制項、架構和報告的權限。

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

- `AWS Backup`

角色權限原則允許 AWS Backup 對指定的資源完成下列動作：

- 動作：`all resources AWS Backup supports` 上的 `list, read, and write`。

  如需特定權限的清單，請參閱 AWS Identity and Access Management 主控台AWSServiceRolePolicyForBackupReports中的原則。

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 AWS Backup建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中建立架構或報告計劃時 AWS CLI， AWS Backup 會為您建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

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。當您建立架構或報告計劃時， AWS Backup 會再次為您建立服務連結角色。

為 AWS Backup編輯服務連結角色

AWS Backup 不允許您編輯 AWSServiceRoleForBackupReports 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Backup刪除服務連結角色

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，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。您必須刪除所有架構和報告計劃。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS Backup 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘，然後再次嘗試操作。

若要刪除 AWSServiceRoleForBackupReports (控制台) 所使用的 AWS Backup 資源

1. 若要刪除所有架構，請參閱刪除架構。
2. 若要刪除所有報告計劃，請參閱刪除報告計劃。

若要刪除使用的 AWS Backup 資源 AWSServiceRoleForBackupReports (AWS CLI)

1. 若要刪除所有架構，請使用 delete-framework。
2. 若要刪除所有報表計劃，請使用delete-report-plan。

若要刪除使用的 AWS Backup 資源 AWSServiceRoleForBackupReports (API)

1. 要刪除所有框架，請使用 DeleteFramework.

2. 若要刪除所有報表計劃，請使用DeleteReportPlan。

手動刪除服務連結角色

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

AWS Backup 服務連結角色的支援區域

AWS Backup 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Backup 支援的功能和區域。

使用角色進行還原測試

AWS Backup 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到 AWS Backup的唯一 IAM 角色類型。服務連結角色由預先定義， AWS Backup 並包含服務代表您呼叫其他服 AWS 務所需的所有權限。

服務連結角色可讓您 AWS Backup 更輕鬆地設定，因為您不必手動新增必要的權限。 AWS Backup 定義其服務連結角色的權限，除非另有定義，否則只 AWS Backup 能擔任其角色。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。這樣可以保護您的 AWS Backup 資源，因為您無法不小心移除存取資源的權限。

如需關於支援服務連結角色的其他服務的資訊，請參閱可搭配 IAM 運作的AWS 服務，並尋找 Service-Linked Role (服務連結角色) 欄顯示為 Yes (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。

服務連結角色權限 AWS Backup

AWS Backup 使用名為的服務連結角色 AWSServiceRolePolicyForBackupRestoreTesting— 提供備份權限以進行還原測試。

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

- `AWS Backup`

角色權限原則允許 AWS Backup 對指定的資源完成下列動作：

- 動作：`all resources AWS Backup supports` 上的 `list, read, and write`。

如需特定權限的清單，請參閱 AWS Identity and Access Management 主控台AWSServiceRolePolicyForBackupRestoreTesting中的原則。

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 AWS Backup建立服務連結角色

您不需要手動建立一個服務連結角色。當您在 AWS Management Console、或 AWS API 中進行還原測試時 AWS CLI，會為您 AWS Backup 建立服務連結角色。

> **Important**
>
> 此服務連結角色可以顯示在您的帳戶，如果您於其他服務中完成一項動作時，可以使用支援此角色的功能。若要進一步了解，請參閱我的 IAM 帳戶中出現的新角色。

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。當您進行還原測試時，請再次為您 AWS Backup 建立服務連結角色。

為 AWS Backup編輯服務連結角色

AWS Backup 不允許您編輯 AWSServiceRolePolicyForBackupRestoreTesting 服務連結角色。因為有各種實體可能會參考服務連結角色，所以您無法在建立角色之後變更角色名稱。然而，您可使用 IAM 來編輯角色描述。如需詳細資訊，請參閱《IAM 使用者指南》中的編輯服務連結角色。

為 AWS Backup刪除服務連結角色

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，務必清除您的服務連結角色，之後才能以手動方式將其刪除。

清除服務連結角色

在您使用 IAM 刪除服務連結角色之前，您必須先刪除該角色所使用的任何資源。您必須刪除所有還原測試計畫。

> **Note**
>
> 當您嘗試刪除資源時，如果 AWS Backup 服務正在使用此角色，則刪除可能會失敗。若此情況發生，請等待數分鐘，然後再次嘗試操作。

若要刪除 AWSServiceRolePolicyForBackupRestoreTesting (控制台) 所使用的 AWS Backup 資源

- 若要刪除所有還原測試計畫，請參閱還原測試。

若要刪除使用的 AWS Backup 資源 AWSServiceRolePolicyForBackupRestoreTesting (AWS CLI)

- 若要刪除還原測試計畫，請使用 `delete-restore-testing-plan`。

若要刪除使用的 AWS Backup 資源 AWSServiceRolePolicyForBackupRestoreTesting (API)

- 若要刪除還原測試計畫，請使用 `DeleteRestoreTestingPlan`。

手動刪除服務連結角色

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

AWS Backup 服務連結角色的支援區域

AWS Backup 支援在所有提供服務的區域中使用服務連結角色。如需詳細資訊，請參閱 AWS Backup 支援的功能和區域。

預防跨服務混淆代理人

混淆代理人問題屬於安全性問題，其中沒有執行動作許可的實體可以強制具有更多許可的實體執行該動作。在 AWS 中，跨服務模擬可能會導致混淆代理人問題。在某個服務（呼叫服務）呼叫另一個服務（被呼叫服務）時，可能會發生跨服務模擬。可以操縱呼叫服務來使用其許可，以其不應有存取許可的方式對其他客戶的資源採取動作。為了預防這種情況，AWS 提供的工具可協助您保護所有服務的資料，而這些服務主體已獲得您帳戶中資源的存取權。

若要限制 AWS Backup 為資源提供另一項服務的許可，我們建議在資源政策中使用 `aws:SourceArn` 和 `aws:SourceAccount` 全域條件內容索引鍵。如果同時使用全域條件內容索引鍵，則在相同政策陳述式中使用 `aws:SourceAccount` 值和 `aws:SourceArn` 值中的帳戶時，必須使用相同的帳戶 ID。

使用 AWS Backup 代表您發佈 Amazon SNS 主題時，`aws:SourceArn` 的值必須是 AWS Backup 保存庫。

防範混淆代理人問題最有效的方法，是使用 `aws:SourceArn` 全域條件內容金鑰，以及資源的完整 ARN。如果不知道資源的完整 ARN，或者如果您指定了多個資源，請使用

aws:SourceArn 全域條件內容金鑰，同時使用萬用字元 (*) 表示 ARN 的未知部分。例如：arn:aws::*servicename*::*123456789012*:*。

基礎結構安全 AWS Backup

作為託管服務， AWS Backup 受到 AWS 全球網絡安全的保護。有關 AWS 安全服務以及如何 AWS 保護基礎架構的詳細資訊，請參閱AWS 雲端安全性。若要使用基礎架構安全性的最佳做法來設計您的 AWS 環境，請參閱安全性支柱架構良 AWS 好架構中的基礎架構保護。

您可以使用 AWS 已發佈的 API 呼叫透 AWS Backup 過網路存取。用戶端必須支援 Transport Layer Security (TLS) 1.2 或更新版本。用戶端還必須支援具備完全正向加密 (PFS) 功能的密碼套件，例如臨時 Diffie-Hellman (DHE) 或橢圓曲線臨時 Diffie-Hellman (ECDHE)。現代系統(如 Java 7 和更新版本)大多會支援這些模式。

此外，請求必須使用存取金鑰 ID 和與 IAM 主體相關聯的私密存取金鑰來簽署。或者，您可以透過 AWS Security Token Service (AWS STS) 來產生暫時安全憑證來簽署請求。

數據的完整性 AWS Backup

AWS Backup 資料完整性目標

AWS Backup 旨在在傳輸，存儲和處理您的數據過程中保持完整性。 AWS Backup 將儲存的資源資料視為與內容無關的重要資訊，因為無論您儲存的資料類型為何，我們都能為客戶提供相同的高度安全性。我們對客戶的安全保持警覺，並已實作複雜的技術和實體措施來防止未經授權的存取。您對於資料的分類方式、儲存資料的區域，以及控管、封存和保護資料防止洩露的方式，仍保有完整控制權。

AWS Backup 資料完整性實作

AWS Backup 與其他 AWS 和 Amazon 服務一起工作，以維護其存放和與其互動之資料的完整性。使用的工具可能會有所不同，可包括 (但不限於)：

- 根據其總和檢查碼持續進行物件驗證，以防止物件損毀
- 內部總和檢查碼，以確認傳輸中的資料和靜態資料的完整性
- 根據從主要存放區所建立備份中的資料計算而來的總和檢查碼
- 在磁碟損毀或偵測到裝置故障時，自動嘗試還原一般層級的物件儲存備援
- 跨多個實體位置的資料備援儲存

- 增強初始寫入期間跨多個可用區域的物件耐久性，並在裝置無法使用或偵測到位元衰減 (Bit Rot) 時進一步複寫
- 所有網路流量的總和檢查碼，以在儲存或擷取資料時偵測資料封包損毀

AWS Backup 使用進階功能、Amazon EFS、Amazon S3、Amazon Timestream，以及透過 Backup 閘道連接的 VMware 執行的虛擬機器，以原生方式為 Amazon DynamoDB 存放資料。 AWS Backup 促進與其他服務存儲的數據備份，包括 Amazon Aurora，Amazon DocumentDB，Amazon EBS，Amazon EC2，Windows 文件服務器的 Amazon FSx for Lustre，Amazon FSX，Amazon FSX 的 OpenZF，Amazon FSX 的 ONTAP，Amazon Neptune，亞馬遜 RDS 和 Amazon Redshift。NetApp

客觀確認並稽核 AWS Backup 資料完整性

直接存放的資料以 AWS Backup 及與其他 AWS Backup 互動 AWS 服務合作存放的資料，必須遵守 Amazon Simple Storage Service (Amazon S3) 的嚴格程序，以確保此資料完整性為基礎。此完整性會經過獨立的第三方稽核人員透過年度 SOC 稽核報告確認，該報告可透過 AWS Management Console中的 AWS Artifact 取得。

法務保存

法務保存是一種管理工具，可協助防止備份在保存下遭到刪除。如果有保存，則無法刪除保存下的備份，而且會變更備份狀態 (例如轉換為 `Deleted` 狀態) 的生命週期政策會延遲，直到移除法務保存為止。一個備份可以有多個法務保存。

法律保留可套用至一或多個由 AWS Backup 其生命週期允許建立的備份 (也稱為復原點)。一種稱為連續備份的備份類型，其生命週期上限為 35 天。法務保存不會延長連續備份生命週期。

建立法務保存時，可將特定的篩選條件納入考量，例如資源類型和資源 ID。此外，您可以定義要包含在法務保存中之備份的建立日期範圍。法務保存與備份具有多對多關係，這表示一個備份可以有多個法務保存，而一個法務保存可以包含多個備份。每個帳戶一次最多可有 50 個法務保存。

法務保存只會套用至放置的原始備份。跨區域或帳戶複製備份時 (如果資源支援此功能)，其法務保存不會隨著保留或移動。法務保存類似於其他資源，有一個相關聯的唯一 ARN (Amazon Resource Name)。只有由建立的復原點才 AWS Backup 能成為法律訴訟保留的一部分。

請注意，雖然 AWS Backup Vault Lock為文件庫提供額外的保護和不變性，但法務保存可提供額外的保護以防止個別備份 (復原點) 遭到刪除。法務保存不會過期，並會無限期保留備份中的資料。該保存會保持作用中，直到具有足夠 IAM 許可的使用者釋放保存為止。

建立法務保存

只有具有特定 IAM 許可的使用者才能新增和釋放法務保存。若要檢查您的許可或授予許可，請登入 AWS Identity and Access Management 主控台。

建立法務保存時，只會包含已建立的復原點。狀態為 EXPIRED 或 DELETING 的備份 (復原點) 不會包含在法務保存中。視完成時間而定，狀態為 CREATING 的復原點 (備份) 可能不會包含在法務保存中。

您可以使用 AWS Backup 主控台或以程式設計方式將法律保留新增至現有備份。

使用主控台建立法務保存

當您透過主控台建立法務保存時，您需要設定數個元素，包括其標題、其描述、其範圍，以及 (選擇性) 任何您想包含的標籤，以協助進行組織和篩選。

使用 AWS Backup 主控台建立法律訴訟保留

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 在主控台左側的儀表板中，找到 My Account。按一下 Legal holds。
3. 按一下 Add legal hold。
4. 這會顯示三個面板：Legal hold details、Legal hold scope 和 Legal hold tags。
   a. 在 Legal hold details 下方，於提供的文字方塊中輸入法務保存標題和描述。
   b. 在 Legal hold scope 面板中，選擇要如何選取資源以包含在保存中。當您建立保存時，您可以選擇要使用哪種方法來選取資源以包含在法務保存中。您可以選擇包含下列其中之一：
      - 特定資源類型和 ID；
      - 選取備份文件庫；
      - 包含帳戶中的所有資源類型或所有備份文件庫
   c. 指定法務保存的日期範圍。以 YYYY:MM:DD 格式輸入日期 (包含日期)。
   d. 或者，您可以為正在建立的保存新增標籤。標籤有助於分類保存，以供未來參考和組織。您總計最多可新增 50 個標籤。
5. 如果您對新法務保存的組態感到滿意，請按一下 Add new hold 按鈕。

使用 AWS CLI 建立法律訴訟保留

您可以指定下列中繼資料：

```
Title
```

```
Description
VaultArns
Resources
FromDate
ToDate
DateRange // Must contain FromDate and ToDate; dates cannot be in the past
LegalHoldTags // optional ; if included, can have up to 5 tags: "tag1", "tag2"
```

1. 複製下列 JSON 範本並將其輸入到 CLI 中。

```
{
    Title: "Your name for the legal hold"
    Description: "Your description of the legal hold"
    ResourceSelection: {
      VaultArns: string[], // only one of vaultArns or resourceIds is allowed;
 error will return if both are included
      Resources: string[]
    }
    ResourceFilters: {
      DateRange: {
          FromDate: DateTime;
          ToDate: DateTime;
        } // both required: future DateTime values will not be allowed
    }
    LegalHoldTags: { // optional,  up to 50 tags
      name: value,
    }
}
```

2. 檢閱此範例以供參考。

```
{
    "Title": "a legal hold",
    "Description": "some description",
    "ResourceSelection": {
      "VaultArns": [
        "arn:aws:backup:Region:Account ID:backup-vault:backup vault name"
      ]
    }
    "ResourceFilters": {
      "DateRange": {
          "FromDate": 1516925490.087,
          "ToDate": 1517525490.087
```

```
        }
    }
    "LegalHoldTags": {
      "tag1":"value1",
      "tag2": "value2",
    }
}
```

3. 檢閱回應，其中可能包含下列元素：

```
{
    "Title": "a legal hold",
    "Status": "CREATING",
    "Description": "some description",
    "LegalHoldArn": string,
    "ResourceSelection": {
      "VaultArns": [
        "arn:aws:backup:Region:Account ID:backup-vault:backup vault name"
      ]
    }
    "ResourceFilters": {
      "DateRange": {
          "FromDate": 1516925490.087,
          "ToDate": 1517525490.087
        }
    }
    "LegalHoldTags": {
      "tag1":"value1",
      "tag2": "value2",
    }
}
```

檢視法務保存

您可以在 AWS Backup 主控台或以程式設計方式查看法律訴訟保留詳細

在主控台中檢視法務保存

若要使用 Backup 主控台檢視帳戶中的所有法務保存，

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 使用儀表板的左側部分，在 My account 底下，按一下 Legal holds。

3. 法務保存表格會顯示現有保存的標題、狀態、描述、ID 和建立日期。按一下表格標題旁的插入記號 (向下箭頭)，依所選的欄篩選表格。

以程式設計方式檢視法務保存

若要以程式設計方式檢視所有法務保存，您可以使用下列 API 呼叫：

`GetLegalHold`：此動作會傳回指定法務保存的詳細資訊。詳細資訊是 JSON 格式的法務保存內文，以及中繼資料。

`ListRecoveryPointsByLegalHold`：此動作會傳回有關指定法務保存中所包含復原點的復原點 ARN (Amazon Resource Name)。您需要在請求中包含參數：`nextToken` 和 `maxResults`。

下列 JSON 範本可用於GetLegalHold。您可以將其複製並輸入到 CLI 中。

```
GET /legal-holds/{legalHoldId} HTTP/1.1

Request

empty body

Response

{
    Title: string,
    Status: LegalHoldStatus,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,

   ResourceSelection: {
        VaultArns: [ string ]
        Resources: [ string ]
   },
   ResourceFilters: {
        DateRange: {
          FromDate: number,
          ToDate: number
        }
```

```
    }
}
```

下列 JSON 範本可用於ListLegalHolds。您可以將其複製並輸入到 CLI 中。

```
GET /legal-holds/
  &maxResults=MaxResults
  &nextToken=NextToken


Request

empty body
url params:
  MaxResults: number  // optional,
  NextToken: string  // optional

status: Valid values: CREATING | ACTIVE | CANCELED | CANCELING
maxResults: 1-1000



Response

{
  NextToken: token,
  LegalHolds: [
    Title: string,
    Status: string,
    Description: string, // 280 chars max
    CancelDescription: string, // this is provided during cancel // 280 chars max
    LegalHoldId: string,
    LegalHoldArn: string,
    CreatedTime: number,
    CanceledTime: number,
  ]

}
```

有關返回信息的詳細信息，請參閱我們ListLegalHolds的 API 指南中的GetLegalHold和。

狀態	描述
CREATING	正在保留請求的復原點，且刪除這些復原點的請求可能會成功，因為該保存尚未完成建立。
ACTIVE	已建立法務保存，並保留此法務保存下列出的所有復原點。
CANCEL	正在移除法務保存，且刪除保存下的復原點請求可能會成功。
CANCELED	法務保存已完全釋放，不再具有任何效力。可刪除復原點。

釋放法務保存

法務保存會隨一或多個備份 (復原點) 保留，直到具有足夠 IAM 許可的使用者將其移除為止。移除法務保存也稱為取消、刪除或釋放法務保存。控制台使用「釋放」一詞，而 API 則使用命令 `cancelLegalHold`。移除法務保存會將其從所有連接的備份中排除。

使用 AWS Backup 主控台解除合法保留

若要使用主控台釋放保存，

1. 開啟主 AWS Backup 控台，網址為 https://console.aws.amazon.com/backup。
2. 輸入您要與釋放建立關聯的描述。
3. 檢閱詳細資訊，然後按一下 Release hold。
4. 當 Release hold 對話方塊出現時，請在文字方塊中輸入 `confirm` 以確認您有意釋放保存。
    - 勾選確認您要取消保存的方塊。

在 Legal holds 頁面上，您可以查看所有保存。如果釋放成功，該保存的狀態會顯示為 `Released`。

使用 API 和 AWS CLI 釋放法律訴訟保留

若要以程式設計方式移除保存，請使用 API 呼叫 `CancelLegalHold`。您可以指定下列中繼資料：

```
CancelDescription: String
```

```
DeleteAfterDays: number // Optional. Default equals 30 days. This specifies number (in
 days to keep legal hold record after cancellation. This applies to the actual legal
 hold record only. Recovery points are unlocked as soon as cancelation processes and
 are not subject to this date.
```

1. 複製下列 JSON 範本並將其輸入到 CLI 中。

```
POST /legal-holds/{legalHoldId}


Request

{
   CancelDescription: String
   DeleteAfterDays: number // optional
}


DeleteAfterDays: optional.
  Defaults to 180 days. how long to keep legal hold record after canceled.
  This applies to the actual legal hold record only.
  Recovery points are unlocked as soon as cancelation processes and are not subject
 to this date.

Response

Empty body

200 if successful
other standard codes
```

2. 檢閱回應，其中可能包含下列元素：

```
POST /legal-holds/abc1-4df0-989f-l9af HTTP/1.1


Request

{
   CancelDescription: "Canceling because case is closed 4/21"
}
```

如需詳細資訊，請參閱 CancelLegalHold。

AWS PrivateLink

AWS PrivateLink 可讓您透過建立介面 VPC 端點，在虛擬私有雲 (「VPC」) 和 AWS Backup 端點之間建立私有連線。介面端點採用這項技術 AWS PrivateLink，可讓您限制 VPC 和 AWS Backup Amazon 網路之間的所有網路流量，藉此私有存取 AWS Backup API。

AWS PrivateLink 可讓您在沒有網際網路閘道、NAT 裝置、VPN 連線或 AWS Direct Connect 連線的情況下私密存取 AWS Backup 作業。VPC 中的執行個體不需要公有 IP 位址即可與 AWS Backup API 端點通訊。您的執行個體也不需要公有 IP 位址即可使用任何可用的 AWS Backup API 和 Backup 閘道 API 作業。您的 VPC 和 AWS Backup 不會離開 Amazon 網絡之間的流量。

如需 VPC 端點的詳細資訊，請參閱《Amazon VPC 使用者指南》中的介面 VPC 端點 (AWS PrivateLink)。

Amazon VPC 端點的考量事項

在為端點設定界面 VPC AWS Backup 端點之前，請先參閱 Amazon VPC 使用者指南中的界面端點屬性和限制。

所有與管理 Amazon Backup 資源相關的 AWS Backup 操作都可以從您的 VPC 使用 AWS PrivateLink。

Backup 端點支援 VPC 端點政策。根據預設，允許透過端點對 Backup 操作進行完整存取。如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對服務的存取。

建立 AWS Backup VPC 端點

您可以建立 VPC 端點以 AWS Backup 使用 Amazon VPC 主控台或 AWS Command Line Interface (AWS CLI)。如需詳細資訊，請參閱 Amazon VPC 使用者指南中的建立介面端點。

建立 VPC 端點以 AWS Backup 使用服務名稱`com.amazonaws.region.backup`。

在中國 (北京) 區域和中國 (寧夏) 區域，服務名稱應為 `cn.com.amazonaws.region.backup`。

對於 Backup 閘道端點，請使用 `com.amazonaws.region.backup-gateway`。

為 Backup 閘道建立 VPC 端點時，必須在安全群組中允許下列 TCP 連接埠：

- TCP 443
- TCP 1026

- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

通訊協定	連線埠	Direction	來源	目的地	用量
TCP	443 (HTTPS)	傳出	Backup Gateway	AWS	用於從 Backup 閘道到 AWS 服務端點的通訊

使用 VPC 端點

例`backup.us-east-1.amazonaws.com`如，如果您為端點啟用私 AWS Backup 有 DNS，則可以使用 VPC 端點的 AWS 區域預設 DNS 名稱向其發出 API 要求。

但是，對於中國（北京）區域和中國（寧夏）區域 AWS 區域，應分別使用`backup.cn-north-1.amazonaws.com.cn`和`backup.cn-northwest-1.amazonaws.com.cn`向 VPC 端點提出 API 請求。

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的透過介面端點存取服務。

建立 VPC 端點政策

您可以將端點政策連接至控制 Amazon Backup API 存取權限的 VPC 端點。此政策指定：

- 可執行動作的委託人。
- 可執行的動作。
- 可供執行動作的資源。

> **Important**
>
> 將非預設政策套用至的介面 VPC 端點時 AWS Backup，某些失敗的 API 請求 (例如失敗者) 可能不會記錄到 AWS CloudTrail 或 Amazon。`RequestLimitExceeded` CloudWatch

如需詳細資訊，請參閱《Amazon VPC 使用者指南》中的使用 VPC 端點控制對服務的存取。

範例：用於動作的 VPC 端點原則 AWS Backup

以下是的端點策略範例 AWS Backup。連接到端點時，此策略會針對所有資源的所有原則授予所列 AWS Backup 動作的存取權。

```
{
  "Statement":[
    {
      "Action":"backup:*",
      "Effect":"Allow",
      "Principal":"*",
      "Resource":"*"
    }
  ]
}
```

範例：拒絕所有來自指定 AWS 帳戶之存取的 VPC 端點政策

下列 VPC 端點策略拒絕 AWS 帳戶123456789012所有使用端點存取資源的帳戶。此政策允許來自其他帳戶的所有動作。

```
{
  "Id":"Policy1645236617225",
  "Version":"2012-10-17",
  "Statement":[
    {
      "Sid":"Stmt1645236612384",
      "Action":"backup:*",
      "Effect":"Deny",
      "Resource":"*",
      "Principal":{
        "AWS":[
          "123456789012"
        ]
      }
    }
  ]
}
```

如需可用 API 回應的進一步詳細資訊，請參閱《API 指南》。

可用性 AWS Backup 目前支援下列 AWS 區域中的 VPC 端點：

- 美國東部 (俄亥俄) 區域
- 美國東部 (維吉尼亞北部) 區域
- 美國西部 (奧勒岡) 區域
- 美國西部 (加利佛尼亞北部) 區域
- 非洲 (開普敦) 區域
- 亞太區域 (香港) 區域
- 亞太 (孟買) 區域
- 亞太 (大阪) 區域
- 亞太 (首爾) 區域
- 亞太區域 (新加坡) 區域
- 亞太 (雪梨) 區域
- 亞太 (東京) 區域
- 加拿大 (中部) 區域
- 歐洲 (法蘭克福) 區域
- 歐洲 (愛爾蘭) 區域
- 歐洲 (倫敦) 區域
- 歐洲 (巴黎) 區域
- 歐洲 (斯德哥爾摩) 區域
- Europe (Milan) Region
- Middle East (Bahrain) Region
- 南美洲 (聖保羅) 區域
- 亞太區域 (雅加達)
- 亞太 (大阪) 區域
- 中國 (北京) 區域
- 中國 (寧夏) 區域
- AWS GovCloud (美國東部)
- AWS GovCloud (美國西部)

> **Note**
>
> AWS Backup VMware 不適用於中國區域 (中國 (北京) 區域和中國 (寧夏) 區域) 或亞太區域 (雅加達) 區域。

韌性 AWS Backup

AWS Backup 非常重視其彈性和資料安全性。

AWS Backup 存儲您的備份至少與您的資源的原始 AWS 服務會給你一樣多的彈性和耐久性，如果你在那裡備份它。

AWS Backup 旨在使用 AWS 全球基礎結構跨多個可用區域複寫備份，在任何給定年度保持 99.999999999% (11 個九) 的持久性，前提是您必須遵守最新的文件。 AWS Backup

AWS Backup 加密您的靜態備份計劃，並持續備份它們。您也可以使用 AWS Identity and Access Management (IAM) 登入資料和政策來限制對備份計劃的存取。如需詳細資訊，請參閱身分驗證、存取控制和 IAM 中的安全最佳實務。

AWS 全球基礎架構是圍繞 AWS 區域 和可用區域建立的。 AWS 區域 提供多個實體分離和隔離的可用區域，這些區域透過低延遲、高輸送量和高度備援的網路連線。 AWS Backup 跨可用區域儲存備份。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。如需詳細資訊，請參閱 AWS Backup 服務水準協議 (SLA)。

此外，還可 AWS Backup 讓您跨區域複製備份，以獲得更高的彈性。如需 AWS Backup 跨區域複製功能的詳細資訊，請參閱建立 Backup 副本。

如需 AWS 區域 和可用區域的詳細資訊，請參閱AWS 全域基礎結構。

AWS Backup 配額

使用時適用下列配額 AWS Backup。如果資源類型服務允許，則可以調整許多 AWS Backup 配額。若要請求配額調整，請向 AWS Support 描述您的使用案例。

AWS Backup 配額

資源	配額	備註
每個帳戶每一區域的備份保存庫數量	300	您可以請求調整。
每個備份文件庫的復原點數量	1,000,000	您可以請求調整。
每個帳戶每一區域的備份計畫數量	300	您可以請求調整。
每個備份計劃的版本數量	2,000	您可以請求調整。
每個備份計劃的資源指派數量	100	不可調整。
每個帳戶的作用中備份任務數量	無限制	
每個帳戶傳出至目的地區域的並行備份複本數量	100	您可以請求調整特定資源 (目前為虛擬機器、進階 DynamoDB、Timestream、Amazon EFS 和 Amazon EC2 執行個體上的 SAP HANA 資料庫)
達到限制 (上述項目) 後，帳戶內每個目的地備份保存庫的並行複本數量	5	不可調整。
可對相同目的地區域建立的相同資源並行跨帳戶複本數量	30	不可調整。

資源	配額	備註
每個資源的並行備份及複製任務數量	1	不可調整。這項配額可協助您維持工作負載的效能。
每個備份的中繼資料標籤數量	50	您無法請求調整。 AWS 在所有資源中強加此配額。請參閱《AWS General Reference》中的標籤命名限制和要求一節。
Hypervisor 數量	10	不可調整。
法務保存數量	每個帳戶 50 個	不可調整。
應用程式堆疊的巢狀備份層數量上限	10	不可調整。

AWS Backup Amazon Timestream 資源配額

資源	配額	備註
每個帳戶的並行 Timestream 備份任務數量	4	您可以請求調整。
每個帳戶的並行 Timestream 還原任務數量	1	您可以請求調整。

單一備份規則中的單一資源指派有其配額。您可以建立具有多項備份規則的備份計畫。

AWS Backup Audit Manager 配額

資源	配額	備註
每個帳戶每一區域的架構數量	10	您可以請求調整。
每個帳戶每一區域的控制數量	50	您可以請求調整。
每個帳戶的報告計畫數量	20	您可以請求調整。

資源	配額	備註
每個報告計畫的架構數量	1,000	不可調整。
報告計畫中的最大帳戶數量乘以區域	300	不可調整。

還原測試計畫配額

資源	配額	備註
還原測試計畫	100	不可調整。
每個計畫中的標籤數量	50	不可調整。
每個計畫的選擇	30	不可調整。
每個還原測試選擇的 ARN	30	不可調整。
每個選擇的條件	30	包含 `StringEquals` 和 `StringNotEquals` 中包含的項目。
每個還原測試選擇的保存庫選擇器	30	不可調整。
所選時段的最大值 (以天為單位)	365 天	
開始時段時數的界限	最短：1 小時；最長：168 小時	
還原測試計畫名稱的字元長度上限	50 個字元	英數字元和底線，沒有空格
還原測試選擇名稱的字元長度上限	50 個字元	英數字元和底線，沒有空格

AWS Backup gateway 配額

資源	配額	備註
每個閘道的備份或還原任務	4	您不能請求調整。相反地，請建立更多閘道，並將其連線至 hypervisor。

當您使用管理多個帳戶的備份時 AWS Organizations，可能會遇到 AWS Organizations 強制的配額。如需這些配額的資訊，請參閱《AWS Organizations 使用者指南》中的AWS Organizations配額一節。

您也可能會遇到由 AWS Backup支援的服務所設定的配額，包括：

- Amazon Elastic File System
- Amazon Elastic Block Store
- Amazon RDS
- Amazon Aurora
- Amazon EC2
- AWS Storage Gateway
- Amazon DynamoDB
- Amazon FSx for Lustre
- Amazon FSx for Windows File Server
- Amazon DocumentDB
- Amazon Neptune
- Amazon Simple Storage Service
- Amazon Timestream

監控

AWS Backup 與其他 AWS 工具搭配使用，讓您能夠監控其工作負載。這些工具包括下列項目：

- AWS Backup 控制台面板
  - 任務儀表板提供任務運作狀態監控功能，您可以在其中檢視指標，這些指標會依照原因、帳戶、區域和資源類型等篩選條件顯示任務的成功和失敗。
  - 工作儀表板可在支援 AWS Backup Audit Manager 的區域中使用。請參閱功能可用性 AWS 區域以了解那些區域。所有其他區域都能夠存取 CloudWatch 儀表板。
- Amazon CloudWatch 和 Amazon EventBridge 監控 AWS Backup 流程。
  - 您可以用 CloudWatch 來追蹤指標、建立警示和檢視儀表板。
  - 您可以使用 EventBridge 來檢視和監視 AWS Backup 事件。

  如需詳細資訊，請參閱使用監視 AWS Backup 事件 EventBridge和。
- AWS CloudTrail以監控 AWS Backup API 呼叫。您可以識別發出這些呼叫的時間、來源 IP、使用者和帳戶。如需詳細資訊，請參閱 使用記錄 AWS Backup API 呼叫 CloudTrail。
- Amazon 簡易通知服務 (Amazon SNS) 可訂閱 AWS Backup相關主題，例如備份、還原和複製事件。如需詳細資訊，請參閱 通知選項 AWS Backup。

AWS Backup 控制台面板

> **Note**
>
> 工作儀表板適用於所有支援「 AWS Backup Audit Manager」的區域。請參閱功能可用性 AWS 區域以了解那些區域。所有其他區域都能夠存取 CloudWatch 儀表板。

主題

- 備份儀表板概觀
- 檢視任務儀表板
- 有問題任務的原因
- 透過取得儀表板資料 AWS CLI

備份儀表板概觀

AWS Backup 在主控台中提供「工作」儀表板，以協助您監控備份、複製和還原工作的健全狀況。可以通過在命令行中檢索可視化顯示在控制台中的相同數據 AWS CLI。

任務儀表板可用於透過組織層級或成員帳戶監控，識別與備份、複製和還原任務相關的問題。有了這些資訊，您就可以識別和診斷事件與可能的問題，以協助確保活動的準確性。

任務儀表板可以顯示兩個時間範圍。依預設會顯示最近 14 天的資料，但您可以變更檢視以顯示最近 7 天的資料。如果您變更時間範圍，資料將會更新以反映新的時間間隔。

請留意，儀表板會顯示直到最近的 UTC 0:00 為止的資料；也就是說，不包括當天的資料。此儀表板會在世界協調時間約 1:30 – 2:30 期間進行每日更新。

檢視任務儀表板

若要檢視工作儀表板，請登入 AWS Backup 主控台並選取左側導覽列中的「工作」儀表板。

在任務儀表板頁面上，您可以從備份、複製或還原任務索引標籤中進行選取。

任務儀表板概觀顯示任務活動指定時間範圍內的彙總檢視，包括已完成、已完成但有問題、過期和失敗的任務。依預設會顯示最近 14 天的資料，但您可以變更檢視以顯示 7 天的資料。

> **Note**
>
> `Completed with issues` 是主控台中顯示的任務狀態，表示已完成的任務，並有狀態訊息。

任務運作狀態

折線圖會顯示一段時間內成功與失敗的任務率線。成功率線會顯示已完成與已完成但有問題任務的彙總。失敗率線會根據指定的時間範圍，顯示失敗和過期任務的總和。

未完成或非失敗狀態的任務 (狀態為「已建立」、「待定」、「執行中」、「已中止」、「中止中」或「部分」的任務) 不會包含在內；百分比總計可能不等於 100%。

一段時間的任務狀態

您可以使用長條圖產生自訂長條圖，其中顯示每個類別 (已完成、已完成但有問題、失敗和過期) 中按天數分配的任務數量。

使用下拉式功能表，選擇您要在圖表中查看的狀態、資源類型和 AWS 地區。如果您想進一步瀏覽選擇，請選取檢視任務以查看任務/跨帳戶監控頁面的預先篩選部分。

您可以將滑鼠暫留在橫條上，以顯示快顯視窗，其中顯示所選日期的詳細任務資料。

有問題的任務

有問題的任務是指狀態為「失敗」、「過期」或「已完成但有問題」的任務。每個圖表都會顯示對應的指標，其中包含帳戶、資源類型或包含最多有問題任務數量的最常見原因。

預設顯示畫面會依指定的指標以遞減順序排序儀表板小工具，從屬於該指標之有問題任務數量最多的指標開始。

只有透過組織擁有存取權的帳戶 (例如管理帳戶和委派的管理員帳戶) 中才會看到最常見的有問題帳戶顯示畫面。如果能夠看見此顯示畫面，您可以將游標暫留在帳戶上，以顯示屬於所選帳戶之有問題的任務數量。

您可以在圖形中選取橫條以開啟快顯視窗。您可以在此視窗中選取任務狀態，以開啟依所選狀態篩選的任務/跨帳戶監控資料表。

有問題任務的原因

最常見的問題原因小工具會顯示錯誤訊息所屬的訊息代碼類別。但是，該類別可能無法解釋任務所遇到的問題。展開下方的訊息代碼類別，查看與任務可能遇到之特定訊息或錯誤有關的更多詳細資訊。

「VSS_ERROR」

- 「Windows VSS 備份嘗試失敗，因為執行個體或 SSM 代理程式的狀態無效或權限不足。」
- 「Windows VSS 備份嘗試失敗，因為權限不足，無法執行此作業」
- 「Windows VSS 備份嘗試失敗，因為執行個體中未安裝 ec2-vss-agent.exe」
- 「Windows VSS 備份任務遇到錯誤，嘗試進行定期備份」
- 「Windows VSS 備份嘗試失敗，因為已啟用 VSS 的快照建立時逾時」
- 「Windows VSS 備份嘗試失敗，因為不支援的 Windows Server 版本。支援的版本是 Windows Server 2012 或更新版本。」
- 「Windows VSS 備份嘗試失敗，因為已啟用 VSS 的快照建立時逾時」

「LIMIT_EXCEEDED」

- 「超過訂閱用戶限制：您已達到同時備份數量上限 (即 300 個)。等到其他任務完成，然後再試一次。您也可以聯絡 AWS Support 要求提高配額。」
- 「超過單一磁碟區允許的進行中快照上限。」
- 「超過允許的作用中快照上限。」
- 「無法建立超過 20 個使用者快照」
- 「產生的標籤集不得擁有超過 50 個使用者標籤。」
- 「您已達到帳戶/資料庫支援的備份數量上限。如需更多資訊，請參閱 Timestream 開發人員指南中的配額。」
- 「您已達到此區域允許的公用和私人映像數量的 50,000 個配額。取消註冊未使用的映像，或要求提高 AMI 配額。」
- 「您的備份成功，但我們無法保留 NetworkInterfaces 元數據，因為它的大小超出了我們的內部限制。」
- 「REGEX#超出訂閱用戶限制」
- 「REGEX#指定超過 50 個標籤」
- 「REGEX#最多可以有」

"ACCESS_DENIED"

- 「未授權您執行此作業。」
- 「拒絕訪問嘗試呼叫 AWS Backup 服務」
- 「來自的圖像 AWS Marketplace 無法複製到另一個 AWS 帳戶。」
- 「會使用預設的備份服務託管金鑰加密目的地備份保存庫，因此複製任務失敗。無法複製此保存庫的內容。只能複製使用 AWS KMS 金鑰加密的 Backup 保存庫的內容。
- 使用加密的快照 AWS 受管金鑰 無法共享。指定另一個快照。
- 「使用 Amazon EBS 預設金鑰的加密快照無法共用
- 「複製任務失敗。來源和目的地帳戶都必須是相同組織的成員。」
- 「REGEX#存取遭拒」
- 「REGEX#未獲授權」
- 「正則表達式 #cannot 由 AWS Backup

- 「REGEX#沒有許可」
- 「REGEX#缺少許可」

「CONCURRENT_JOB」

- 「同一資源有正在執行的任務，因此備份任務失敗。」

「FEATURE_NOT_ENABLED」

- 「複製任務失敗。目前的組織未啟用跨帳戶複製功能。」

「JOB_EXPIRED」

- 「備份任務在完成前已過期。」

「INVALID_LIFECYCLE」

- 「複製任務失敗。任務中指定的保留不在為目標備份保存庫指定的範圍內。」
- 「REGEX#無法開始，因為其位於內部或太接近所設定的每週維護時段」
- 「REGEX#無法開始，因為其位於內部或太接近所設定的自動備份時段」

「INVALID_STATE」

- 「REGEX#執行個體不處於狀態」
- 「REGEX#不處於可用狀態」
- 「REGEX#不處於可用狀態」
- 「REGEX#無法擷取磁碟區的快照」

「KMS_KEY_ERROR」

- 「KMS 金鑰已停用或待刪除，或存取 KMS 金鑰遭拒」
- 「無法存取指定的金鑰 ID」
- 「AMI 快照複製失敗，並發生錯誤：無法存取指定的金鑰 ID。您必須擁有默認 CMK 的 DescribeKey 權限」
- 「REGEX#kms 金鑰」

「ACCESS_KEY_ERROR」

- 「 AWS 訪問密鑰 ID 需要服務的訂閱」

「HYPERVISOR_OFFLINE」

- 「此作業對指定的 Hypervisor 無效，因為其未上線」

「RESOURCE_NOT_FOUND」

- 「找不到指定的磁碟區。」
- 「找不到此虛擬機器。」
- 「指定的金鑰 ID 不存在」
- 「REGEX#不存在」
- 「REGEX#找不到資源」
- 「REGEX#找不到 cryopod」
- 「REGEX#找不到復原點」
- 「REGEX#找不到資源」
- 「REGEX#不再可用」
- 「REGEX#無效」

「RESOURCE_NOT_SUPPORTED」

- 「REGEX#不支援的資源類型」
- 「REGEX#不支援的資源類型」

「TAG_COPY_ERROR」

- 「由於內部失敗，我們無法將資源標籤複製到備份。」
- 「來源或目的地復原點無法使用，因此我們無法將資源標籤複製到備份」

「TOKEN_EXPIRED」

- 「字符已過期。請再試一次。」

「UNSUPPORTED_OPERATION」

- 「建立快照期間，虛擬機器管理程序不支援此CreateSnapshot 方法。已中止的備份任務」
- 「UnsupportedOperation ：Storage Gateway 備份副本需要使用者建立的備份儲存庫和目的地的 CMK。」
- 「REGEX#提供的資源類型不支援功能。」

「FATAL_ERROR」

- 「發生內部錯誤。」
- 「複製任務遇到嚴重錯誤。請聯繫 Sup AWS port 以獲得進一步的幫助。」
- 「複製任務遇到嚴重錯誤。」
- 「REGEX#備份任務遇到嚴重錯誤」

透過取得儀表板資料 AWS CLI

您可以使用命令列，以擷取主控台中出現的相同資料。請使用以下其中一個 CLI 命令：

- list-backup-job-summaries
- list-copy-job-summaries
- list-restore-job-summaries

以下為您可以在每個命令中包含的有效參數：

```
BackupJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

CopyJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
```

```
    ResourceType (string),
    MessageCategory (string),
AggregationPeriod: (string),
NextToken (string),
MaxResults (number)

RestoreJobSummaries (list)
    Region (string),
    Account (string),
    State (string),
    ResourceType (string),
AggregationPeriod: (string),
NextToken (string)
```

此範例顯示使用者輸入 `list-backup-job-summaries` 的範例請求，其中該請求會要求傳回過去 14 天內狀態為 `FAILED` 的所有可用帳戶：

```
GET /audit/backup-job-summaries/
    ?accountId=ANY
    &state=FAILED
    &aggregationPeriod=FOURTEEN_DAYS
```

若要取得狀態為 `completed with issues` 的任務計數，請將 `COMPLETED` 任務 (`MessageCategory` 為 `SUCCESS`) 的任務計數從 `COMPLETED` 總數減去。

使用監視 AWS Backup 事件 EventBridge

主題

使用監視事件 EventBridge

您可以使用 EventBridge 來監視 AWS Backup 事件。常見的使用案例是在備份工作失敗時接收警示。AWS Backup 每 5 分鐘以最大 EventBridge 的方式發出一次事件。

本文件頁面的目的是提供您用 EventBridge 來監視的參考資料 AWS Backup。如需如何使用追蹤 AWS Backup 事件 EventBridge，請參閱 Amazon 使用 EventBridge 者指南中的部落格設定要傳送至 EventBridge的 CloudWatch 事件 AWS Backup或建立 AWS 服務規則。

> **Note**
>
> 部分事件會報告 `status: COMPLETED`，而其他事件會報告 `state: COMPLETED`。這與 AWS Backup API 一致。

某些狀態特定於主 AWS Backup 控台：`Completed with issues`狀態是具有一或多個狀態訊息的`Completed`工作表示。若要監控 `Completed with issues` 事件，請監控具有狀態訊息的 `COMPLETED` 任務。

您可以在中追蹤下列 AWS Backup相關事件 EventBridge。

事件類型	狀態	事件詳細資訊
備份任務狀態變更	`ABORTED`, `EXPIRED`, `RUNNING`, `PENDING`	accountId、資源：、詳細資料 recoveryPointArn、位元組、backupJobId、 backupSize eIn位元組支援 backupVau ltName、完成日期 backupVau ltArn、、ARN、百分比完成、資 resource iAmRole Arn 範圍、resourceType expectedC ompletionDate、開始者、狀態、狀態訊息 創建者：，創建方式：backupPlanArn，創建方式：，創建者： backupPlanId backupPlanVersion backupRul eId
備份任務狀態變更	`COMPLETED` ，`FAILED`	accountId、資源：、詳細資料 recoveryPointArn、位元組、 backupJobId、backupSizeIn位元組支援 backupVaultName、完成日期 backupVaultArn、、ARN、百分比完成、重新計數、

事件類型	狀態	事件詳細資訊
		資 resource iAmRole Arn 範圍 expectedCompletion Date、resourceType、開始依據、狀態、狀態訊息 創建者：，創建方式：backupPlanArn，創建方式：，創建者： backupPlanId backupPlanVersion backupRuleId
備份任務狀態變更	CREATED	accountId、資源：、詳細資訊 recoveryPointArn、狀態 backupJobId、creationDate
複製任務狀態變更	COMPLETED ，FAILED, RUNNING	accountId、資源：、詳細資料 recoveryPointArn、 backupSizeIn位元組、完成日期、建立日期、Arn copyJobId、Arn、資 resource destinationBackupVault Arn 範圍、 destinationRecoveryPoint resourceType、狀態、 iAmRole狀態訊息 創建者：，創建方式：backupPlanArn，創建方式：，創建者： backupPlanId backupPlanVersion backupRuleId
複製任務狀態變更	CREATED	accountId、資源：、詳細資料 recoveryPointArn、狀態、creationDate、Arn 、 sourceBackupVault Arn destinationBackupVault

事件類型	狀態	事件詳細資訊
還原任務狀態變更	CREATED, COMPLETED , FAILED, PENDING, RUNNING, STOPPED	accountId、資源：、詳細資料 recoveryPointArn、狀態、creationDate、 restoreJobId
復原點狀態變更	COMPLETED , PARTIAL, EXPIRED	accountId, 資源:, 資源: recoveryPointArn, 詳細資料 backupVaultArn, backupSizeIn位元組,, calculatedLifeCycle: 刪除 backupVaultName,:, 完成日期, 建立日期 moveToColdStorageAt,, ARN, 未加密,, 生命週期 calculatedLifeCycle:, 生命週期: encryptionKeyArn, 資 resource iAmRole Arn 範圍, resourceType lastRestoreTime, 狀態 deleteAfterDays, 儲存體 moveToCold StorageAfterDays 創建者： ，創建方式： backupPlanArn，創建方式： ，創建者： backupPlanId backupPlanVersion backupRuleId
復原點狀態變更	FAILED, COMPLETED , RUNNING, ABORTED, PENDING	accountId、資源：、詳細資料 recoveryPointArn、backupSizeIn位元組、完成日期、creationDate、分鐘數 createdResourceArn、範圍、百 expectedCompletionTime分比完成、 iAmRole狀態、狀態訊息 restoreJobId

事件類型	狀態	事件詳細資訊
復原點狀態變更	MODIFIED, DELETED	accountId、資源:、資源: recoveryPointArn、詳細資料 backupVaultArn、生命週期、計算生命週期、狀態
備份保存庫狀態變更	CREATED, DELETED, MODIFIED	accountId、資源： backupVaultArn、詳細資料 backupVaultName、狀態
區域設定狀態變更	MODIFIED	accountId、詳細資訊、修改時間、狀態、 resourceTypeOptInPreference
備份計畫狀態變更	CREATED, DELETED, MODIFIED	accountId、資源：、詳細資料 backupPlanArn、versionId backupPlanId、creationDate、刪除日期

如果您想以程式設計方式使用這些事件，請使用下列範例 JSON 承載。

事件狀態	JSON 承載

備份任務：已失敗	{
	"version": "0",
	"id": "710b0398-d48e-f3c3-afca-cfeb2fdaa656",
	"detail-type": "Backup Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T20:15:26Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "34176239-e96d-4e1d-9fad-529dbb3c3556",

事件狀態	JSON 承載
	"backupVaultArn": "arn:aws:backup:us-west-2: 111223345566 :backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86_beta", "backupVaultName": "9ab3e749-82c6-4342-9320-5edbf4918b86_beta", "bytesTransferred": "0", "creationDate": "2020-07-29T20:13:07.392Z", "iamRoleArn": "arn:aws:iam:: 1112233445566 :role/MockRCBackupIntegTestRole", "resourceArn": "arn:aws:cryo-mock:us-west-2: 1112233445566 :resource:dummy-fs-1", "resourceType": "CryoTestClient", "state": "FAILED", "statusMessage": "\"Backup job failed because backup vault arn:aws:backup:us-west-2: 111223345566 :backup-vault:9ab3e749-82c6-4342-9320-5edbf4918b86_beta does not exist.\"", "startBy": "2020-07-30T04:13:07.392Z", "percentDone": 0, "retryCount": 3 } }

事件狀態	JSON 承載

備份任務：已完成	{
	"version": "0",
	"id": "dafac799-9b88-0134-26b7-fef4d54a134f",
	"detail-type": "Backup Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T21:41:17Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :recovery-point:f1d966fe-a3bd-410b-b292-99f442d13b56_beta"
	],
	"detail": {
	"backupJobId": "a827233a-d405-4a86-a440-759fa94f34dd",
	"backupSizeInBytes": "36048",
	"backupVaultArn": "arn:aws:backup:us-west-2: *111223344 5566* :backup-vault:9732c1b4-1091-472a-9d9f-52e0565ee39a_beta",
	"backupVaultName": "9732c1b4-1091-472a-9d9f-52e0565ee39a_beta",
	"bytesTransferred": "36048",
	"creationDate": "2020-07-15T21:40:31.207Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/MockRCBackupIntegTestRole",
	"resourceArn": "arn:aws:cryo-mock:us-west-2: *1112233445566* :resource:dummy-fs-1",
	"resourceType": "CryoTestClient",
	"state": "COMPLETED",
	"completionDate": "2020-07-15T21:41:05.921Z",
	"startBy": "2020-07-16T05:40:31.207Z",

事件狀態	JSON 承載

```
    "percentDone": 100,
    "retryCount": 3
  }
}
```

事件狀態	JSON 承載

備份任務：執行中	{
	"version": "0",
	"id": "44946c39-b519-3505-44e6-ba74afeb2e30",
	"detail-type": "Backup Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T21:39:13Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "B6EC38D2-CB3C-EF0A-F5A4-3CF324EF4945",
	"backupSizeInBytes": "3221225472",
	"backupVaultArn": "arn:aws:backup:us-west-2: *111223344 5566* :backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
	"backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
	"bytesTransferred": "0",
	"creationDate": "2020-07-15T21:38:31.152Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/FullBackupIntegTestRole",
	"resourceArn": "arn:aws:ec2:us-west-2: *1112233445566* :volume/vol-0b5ae24f2ee72d926",
	"resourceType": "EBS",
	"state": "RUNNING",
	"startBy": "2020-07-16T05:00:00Z",
	"expectedCompletionDate": "Jul 15, 2020 9:39:07 PM",
	"percentDone": 99,
	"createdBy": {
	"backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",

事件狀態	JSON 承載
	"backupPlanArn": "arn:aws:backup:us-west-2: 111223344 5566 :backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5_beta", "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5", "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5" } } }

事件狀態	JSON 承載

備份任務：已中止	{
	"version": "0",
	"id": "4c91ceb0-b798-da82-6818-c2
	9b3dce7543",
	"detail-type": "Backup Job State
	Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T21:33:16Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "58cdef95-7680-4c7
	4-80d5-1b64093999c8",
	"backupVaultArn": "arn:aws:
	backup:us-west-2: *111223344*
	5566 :backup-vault:f59bffcd-2538
	-4bbe-8343-1c60dae27c27_beta",
	"backupVaultName": "f59bffcd
	-2538-4bbe-8343-1c60dae27c27_beta",
	"bytesTransferred": "0",
	"creationDate": "2020-07-
	15T21:33:00.803Z",
	"iamRoleArn": "arn:aws:
	iam:: *1112233445566* :role/MockRCBackup
	IntegTestRole",
	"resourceArn": "arn:aws:cryo-mock
	:us-west-2: *1112233445566* :resource
	:dummy-fs-1",
	"resourceType": "CryoTestClient",
	"state": "ABORTED",
	"statusMessage": "\"Backup job was
	stopped by user.\"",
	"completionDate": "2020-07-
	15T21:33:01.621Z",
	"startBy": "2020-07-16T05:33:
	00.803Z",
	"percentDone": 0
	}
	}

事件狀態	JSON 承載

備份任務：已過期	{
	"version": "0",
	"id": "1d7bbc04-6120-1145-13b9-49
	b0af465328",
	"detail-type": "Backup Job State
	Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T13:04:57Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "01EE26DC-7107-4D8
	E-0C54-EAC27C662BA4",
	"backupVaultArn": "arn:aws:
	backup:us-west-2: *111223344
	5566* :backup-vault:aws/backup/Au
	tomatedBackupVaultDel2_beta",
	"backupVaultName": "aws/backup/
	AutomatedBackupVaultDel2_beta",
	"bytesTransferred": "0",
	"creationDate": "2020-07-
	29T05:10:20.077Z",
	"iamRoleArn": "arn:aws:
	iam:: *1112233445566* :role/MockRCBackup
	IntegTestRole",
	"resourceArn": "arn:aws:cryo-mock
	:us-west-2: *1112233445566* :resource
	.bbd99e4c-e974-489b-94f2-db
	9e8cc15dd5",
	"resourceType": "CryoTestClient",
	"state": "EXPIRED",
	"statusMessage": "\"Backup job
	failed because there was a running job
	for the same resource.\"",
	"completionDate": "2020-07-
	29T13:02:15.234Z",
	"startBy": "2020-07-29T13:00:
	00Z",
	"percentDone": 0,
	"createdBy": {

事件狀態	JSON 承載
	"backupPlanId": "aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b", "backupPlanArn": "arn:aws:backup:us-west-2: *111223345566* :backup-plan:aws/efs/414a5bd4-f880-47ad-95f3-f085108a4c3b_beta", "backupPlanVersion": "NjBjOTUzZjYtYzZiNi00NjhlLWIzMTEtNWRjOWY0YTNjN2Vj", "backupPlanRuleId": "3eb0017c-f262-4211-a802-302cebb11dc2" } } }

事件狀態	JSON 承載

備份任務：待定	{
	"version": "0",
	"id": "64dd1897-f863-31a3-9ee5-b05e306d81ff",
	"detail-type": "Backup Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T20:03:30Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "2cffdb68-d6ed-485f-9f9b-8b530749f1c2",
	"backupVaultArn": "arn:aws:backup:us-west-2: *111223344 5566* :backup-vault:ed1f2661-5587-48bf-8a98-fadb977bf975_beta",
	"backupVaultName": "ed1f2661-5587-48bf-8a98-fadb977bf975_beta",
	"bytesTransferred": "0",
	"creationDate": "2020-07-29T20:01:06.224Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/MockRCBackupIntegTestRole",
	"resourceArn": "arn:aws:cryo-mock:us-west-2: *1112233445566* :resource:testListProtectedResources-3",
	"resourceType": "CryoTestClient",
	"state": "PENDING",
	"statusMessage": "",
	"startBy": "2020-07-30T04:01:06.224Z",
	"percentDone": 0
	}
	}

事件狀態	JSON 承載

備份任務：已建立	{
	"version": "0",
	"id": "29af2bf2-eace-58ab-da3a-8c0bf738d692",
	"detail-type": "Backup Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-22T20:32:53Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"backupJobId": "7e8845b5-ca30-415f-a842-e0152bf4d0ca",
	"state": "CREATED",
	"creationDate": "2020-06-22T20:32:47.466Z"
	}
	}

事件狀態	JSON 承載

複製任務：失敗	{
	"version": "0",
	"id": "4660bc92-a44d-c939-4542-cda503f14855",
	"detail-type": "Copy Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T20:37:34Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::image/ami-00179b33a7a88cac5"
	],
	"detail": {
	"copyJobId": "47C8EF56-74D8-059D-1301-C5BE1D5C926E",
	"backupSizeInBytes": 22548578304,
	"creationDate": "2020-07-15T20:36:13.239Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/RoleForEc2BackupWithNoDescribeTagsPermissions",
	"resourceArn": "arn:aws:ec2:us-west-2: *1112233445566* :instance/i-0515aee7de03f58e1",
	"resourceType": "EC2",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2: *111223344 5566* :backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7_beta",
	"state": "FAILED",
	"statusMessage": "Access denied exception while trying to list tags",
	"completionDate": "2020-07-15T20:37:28.704Z",
	"destinationBackupVaultArn": "arn:aws:backup:us-west-2: *111223344 5566* :backup-vault:55aa945e-c46a-421b-aa27-f94b074e31b7_beta",

事件狀態	JSON 承載
	"destinationRecoveryPointArn": {} } }

事件狀態	JSON 承載

複製任務：執行中	{
	"version": "0",
	"id": "d17480ae-7042-edb2-0ff5-8b94822c58e4",
	"detail-type": "Copy Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T22:07:48Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
	],
	"detail": {
	"copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
	"backupSizeInBytes": 3221225472,
	"creationDate": "2020-07-15T22:06:27.234Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/OrganizationCanaryTestRole",
	"resourceArn": "arn:aws:ec2:us-west-2: *1112233445566* :volume/vol-050eba21ee4d3c001",
	"resourceType": "EBS",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2: *1112233445566* :backup-vault:846869de-4589-45c3-ab60-4fbbabcdd3ec_beta",
	"state": "RUNNING",
	"destinationBackupVaultArn": "arn:aws:backup:us-west-2: *1112233445566* :backup-vault:846869de-4589-45c3-ab60-4fbbabcdd3ec_beta",
	"destinationRecoveryPointArn": {},
	"createdBy": {
	"backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e",

事件狀態	JSON 承載
	"backupPlanArn": "arn:aws:backup:us-west-2: 111223344 5566 :backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e_beta", "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4", "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18" } } }

事件狀態	JSON 承載

複製任務：已完成	{
	"version": "0",
	"id": "47deb974-6473-aef1-56c2-52c3eaedfceb",
	"detail-type": "Copy Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T22:08:04Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::snapshot/snap-03886bc8d6ef3a1f9"
	],
	"detail": {
	"copyJobId": "0175DE71-5784-589F-D8AC-541ACCB4CAC8",
	"backupSizeInBytes": 3221225472,
	"creationDate": "2020-07-15T22:06:27.234Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/OrganizationCanaryTestRole",
	"resourceArn": "arn:aws:ec2:us-west-2: *1112233445566* :volume/vol-050eba21ee4d3c001",
	"resourceType": "EBS",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2: *1112233445566* :backup-vault:846869de-4589-45c3-ab60-4fbbabcdd3ec_beta",
	"state": "COMPLETED",
	"completionDate": "2020-07-15T22:07:58.111Z",
	"destinationBackupVaultArn": "arn:aws:backup:us-west-2: *1112233445566* :backup-vault:846869de-4589-45c3-ab60-4fbbabcdd3ec_beta",
	"destinationRecoveryPointArn": "arn:aws:ec2:us-west-2::snapshot/snap-0726fe70935586180",

事件狀態	JSON 承載
	"createdBy": { "backupPlanId": "b58e3621-1c53-4997-ad8a-afc3347a850e", "backupPlanArn": "arn:aws:backup:us-west-2: *111223345566* :backup-plan:b58e3621-1c53-4997-ad8a-afc3347a850e_beta", "backupPlanVersion": "Mjc4ZTRhMzUtMGE5Ni00NmQ5LWE1YmMtOWMwY2IwMTY4NWQ4", "backupPlanRuleId": "78e356d3-1a11-4f61-8585-af5d6b69bb18" } } }

事件狀態	JSON 承載

複製任務：已建立	{
	"version": "0",
	"id": "8398a4c4-8fe8-2b49-a4b9-fd4fdcd34a4e",
	"detail-type": "Copy Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-22T21:06:32Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::image/ami-0888b126e2170b98e"
	],
	"detail": {
	"creationDate": "2020-06-22T21:06:25.754Z",
	"state": "CREATED",
	"sourceBackupVaultArn": "arn:aws:backup:us-west-2: *111223345566* :backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17_beta",
	"destinationBackupVaultArn": "arn:aws:backup:us-west-2: *111223345566* :backup-vault:ef09da5a-21a6-461f-a98f-857e9e621a17_beta"
	}
	}

事件狀態	JSON 承載

還原任務：已失敗	{
	"version": "0",
	"id": "296805cc-6ad4-32f2-fb86-4e66c84abce7",
	"detail-type": "Restore Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T20:19:29Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::image/ami-06b9894dfb1f9cf48"
	],
	"detail": {
	"restoreJobId": "9B333A28-526B-01CD-4A77-9785A08922FD",
	"backupSizeInBytes": "22548578304",
	"creationDate": "2020-07-15T20:19:07.303Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/CanaryAWSBackupRole",
	"percentDone": 0,
	"resourceType": "EC2",
	"status": "FAILED",
	"statusMessage": "AWS Backup does not permit attaching a new instance profile to an EC2 instance. Please restore using the backed up instance profile."
	}
	}

事件狀態	JSON 承載

還原任務：執行中	{
	"version": "0",
	"id": "6137a1f0-33f3-99ee-a01a-3d8b96fe2ad6",
	"detail-type": "Restore Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T20:26:06Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:ec2:us-west-2::snapshot/snap-0fe679ca138cfad2c"
	],
	"detail": {
	"restoreJobId": "F143178C-A866-4782-3B19-BF776A1A790C",
	"backupSizeInBytes": "3221225472",
	"creationDate": "2020-07-29T20:26:00.098Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/OrganizationCanaryTestRole",
	"percentDone": 0,
	"resourceType": "EBS",
	"status": "RUNNING"
	}
	}

事件狀態	JSON 承載

還原任務：已完成	{
	"version": "0",
	"id": "8939bc73-dcf1-418c-9420-b9c5e097f0fb",
	"detail-type": "Restore Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T03:14:58Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:rds:us-west-2: *1112233445566* :snapshot:awsbackup:job-f2494617-4fe0-47e3-969e-a652d902b475"
	],
	"detail": {
	"restoreJobId": "EF332640-02A5-5978-693F-987970F09961",
	"backupSizeInBytes": "0",
	"creationDate": "2020-07-15T03:10:01.742Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/CanaryAWSBackupRole",
	"percentDone": 0,
	"resourceType": "RDS",
	"status": "COMPLETED",
	"createdResourceArn": "arn:aws:rds:us-west-2: *1112233445566* :db:cryo-instance7c3d1e78-987e-4450-92e1-3b6dbedb5384",
	"completionDate": "2020-07-15T03:14:53.128Z"
	}
	}

事件狀態	JSON 承載

還原任務：待定	{
	"version": "0",
	"id": "0586085f-3079-cd79-10b7-908d3c3a21ea",
	"detail-type": "Restore Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T20:08:26Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :recovery-point:42bb8260-92cd-46a2-ab8d-b29f4edb47b1_beta"
	],
	"detail": {
	"restoreJobId": "EB9CE5CB-2B92-8B66-FD16-9829F4DAAAD7",
	"backupSizeInBytes": "36048",
	"creationDate": "2020-07-29T20:08:21.083Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/MockRCBackupIntegTestRole",
	"percentDone": 0,
	"resourceType": "CryoTestClient",
	"status": "PENDING"
	}
	}

事件狀態	JSON 承載

還原任務：已建立	{
	"version": "0",
	"id": "af32977e-378f-2122-f985-fca4596f0709",
	"detail-type": "Restore Job State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-22T18:50:49Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :recovery-point:f6560d33-3660-494e-8d47-aaba939df32e_beta"
	],
	"detail": {
	"restoreJobId": "267EA62F-C125-EFE5-7099-9D98FC0E422A",
	"creationDate": "2020-06-22T18:50:46.407Z",
	"state": "CREATED"
	}
	}

事件狀態	JSON 承載

復原點：已完成	{
	"version": "0",
	"id": "ec6f75cc-989c-faaf-a642-dd0f1c95bff0",
	"detail-type": "Recovery Point Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-15T21:39:07Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:rds:us-west-2: *1112233445566* :cluster-snapshot:awsbackup:job-4ece7121-d60e-00c2-5c3b-49960142d03b"
	],
	"detail": {
	"backupVaultName": "e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
	"backupVaultArn": "arn:aws:backup:us-west-2:496821122410:backup-vault:e6625738-0655-4aa9-bd37-6ec1dd183b15_beta",
	"creationDate": "2020-07-15T21:38:31.152Z",
	"iamRoleArn": "arn:aws:iam:: *1112233445566* :role/FullBackupIntegTestRole",
	"resourceType": "Aurora",
	"resourceArn": "arn:aws:rds:us-west-2: *1112233445566* :cluster:cryo-aurora-14029f40-b0b6-4a61-9fd2-9886f2771add",
	"status": "COMPLETED",
	"isEncrypted": "false",
	"storageClass": "WARM",
	"completionDate": "2020-07-15T21:39:05.689Z",
	"createdBy": {
	"backupPlanId": "bde0f455-4e24-4668-aeaa-4932a97f5cc5",

事件狀態	JSON 承載
	"backupPlanArn": "arn:aws:backup:us-west-2:111223344 5566 :backup-plan:bde0f455-4e24-4668-aeaa-4932a97f5cc5_beta", "backupPlanVersion": "YTkzNmM0MmUtMWRhNS00Y2RkLThmZGUtNjA5NTc4NGM1YTc5", "backupPlanRuleId": "1f97bafa-14d6-4f39-94fd-94b51bd6d0d5" }, "lifecycle": { "deleteAfterDays": 100 }, "calculatedLifeCycle": { "deleteAt": "2020-10-23T21:38:31.152Z" } } }

事件狀態	JSON 承載

復原點：已刪除	{
	"version": "0",
	"id": "6089ee76-d856-0d7c-cee7-0a
	431cd43343",
	"detail-type": "Recovery Point
	Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-29T22:38:49Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-
	west-2:*1112233445566* :backup-v
	ault:157f892e-fe46-48da-9db
	e-4154f91f8acc_beta",
	"arn:aws:rds:us-west-2: *111223344
	5566* :snapshot:awsbackup:job-c1a
	6d40a-32d1-4d54-bd70-bced933ef107"
	],
	"detail": {
	"state": "DELETED",
	"lifecycle": {
	"deleteAfterDays": 300
	},
	"calculatedLifeCycle": {
	"deletedAt": "2021-05-25T22:29:
	02.452Z"
	}
	}
	}

事件狀態	JSON 承載

復原點：已修改	{
	"version": "0",
	"id": "14365bb1-adef-bc00-1ee3-8f
	ac188d7996",
	"detail-type": "Recovery Point
	Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-07-02T23:33:57Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-
	west-2:*1112233445566* :backup-v
	ault:helo12312_beta",
	"arn:aws:dynamodb:us-west-2
	: *1112233445566* :table/test/backup
	/01593730512469-033578ce"
	],
	"detail": {
	"calculatedLifeCycle": {
	"toColdStorageAfterDays": "Fri
	Dec 04 22:55:11 UTC 2020"
	},
	"state": "MODIFIED"
	}
	}

事件狀態	JSON 承載

備份保存庫：已建立	{
	"version": "0",
	"id": "d415609e-5f35-d9a2-76d1-613683e4e024",
	"detail-type": "Backup Vault State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T23:18:19Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :backup-vault:d8864642-155c-4283-a168-a04f40e12c97_beta"
	],
	"detail": {
	"backupVaultName": "d8864642-155c-4283-a168-a04f40e12c97",
	"state": "CREATED"
	}
	}

事件狀態	JSON 承載

備份保存庫：已修改	{
	"version": "0",
	"id": "*1a2b3cd4-5e6f-7g8h-9i0j-123456k7l890* ",
	"detail-type": "Backup Vault State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T23:18:19Z",
	"region": "*Region*",
	"resources": [
	"arn:aws:backup: *Region*:*111223344 5566* :backup-vault: *[nameOfTestBackup]* "
	],
	"detail": {
	"backupVaultName": " *[vaultName]* ",
	"state": "MODIFIED",
	'isLocked': 'true'
	}
	}

事件狀態	JSON 承載

備份保存庫：已刪除	{
	"version": "0",
	"id": "344bccc1-6d2e-da93-3adf-b3f82460294d",
	"detail-type": "Backup Vault State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-22T02:42:37Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :backup-vault:e8189629-1f8e-4ed2-af7d-b32415d04db1_beta"
	],
	"detail": {
	"backupVaultName": "e8189629-1f8e-4ed2-af7d-b32415d04db1",
	"state": "DELETED"
	}
	}

事件狀態	JSON 承載

備份計畫：已修改	{
	"version": "0",
	"id": "2895aefb-dd4a-0a23-6071-2652abd92c3f",
	"detail-type": "Backup Plan State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T23:18:25Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de_beta"
	],
	"detail": {
	"backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
	"versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
	"modifiedAt": "2020-06-24T23:18:19.168Z",
	"state": "MODIFIED"
	}
	}

事件狀態	JSON 承載

備份計畫：已刪除	{
	"version": "0",
	"id": "33fc5c1d-6db2-b3d9-1e70-1c9a2c23645c",
	"detail-type": "Backup Plan State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T23:18:25Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :backup-plan:83fcb8ee-2d93-42ac-b06f-591563f3f8de_beta"
	],
	"detail": {
	"backupPlanId": "83fcb8ee-2d93-42ac-b06f-591563f3f8de",
	"versionId": "NjIwNDFjMDEtNmZlNC00M2JmLTkzZDgtNzNkZjQyNzkxNDk0",
	"deletionDate": "2020-06-24T23:18:19.411Z",
	"state": "DELETED"
	}
	}

事件狀態	JSON 承載

備份計畫：已建立	{
	"version": "0",
	"id": "b64fb2d0-ae16-ff9a-faf6-0bdd0d4bfdef",
	"detail-type": "Backup Plan State Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T23:18:19Z",
	"region": "us-east-1",
	"resources": [
	"arn:aws:backup:us-west-2:*1112233445566* :backup-plan:2c103c5f-6d6e-4cac-9147-d3afa4c84f59_beta"
	],
	"detail": {
	"backupPlanId": "2c103c5f-6d6e-4cac-9147-d3afa4c84f59",
	"versionId": "N2Q4OTczMzEtZmY1My00N2UwLWE3ODUtMjViYWYyOTUzZWY4",
	"creationDate": "2020-06-24T23:18:15.318Z",
	"state": "CREATED"
	}
	}

事件狀態	JSON 承載

區域設定：已修改	{
	"version": "0",
	"id": "e7ed82ba-4955-4de5-10d6-db
	afcfb68b4f",
	"detail-type": "Region Setting State
	Change",
	"source": "aws.backup",
	"account": " *1112233445566* ",
	"time": "2020-06-24T22:55:03Z",
	"region": "us-east-1",
	"resources": [],
	"detail": {
	"modifiedAt": "2020-06-24T22:54:
	57.161Z",
	"ResourceTypeOptInPreference": {
	"Aurora": true
	},
	"state": "MODIFIED"
	}
	}

與 AWS Backup 通知 API 的差異

您也可以使用 AWS Backup 通知 API 透過亞馬遜簡單通知服務 (Amazon SNS) 追蹤 AWS Backup 事件。不過，會 EventBridge追蹤比通知 API 更多的變更，包括備份儲存庫的變更、複製工作狀態、區域設定，以及冷或暖復原點的數目。

AWS Backup Amazon 指標 CloudWatch

主題

- CloudWatch 儀表板
- 量度與 CloudWatch

CloudWatch 儀表板

> **Note**
>
> 主控台儀表板會因正在存取主控台的區域而異。請參閱功能可用性 AWS 區域以查看哪些區域可以存取「任務」儀表板。未列出的區域將能夠存取 CloudWatch 儀表板。

您的 AWS Backup 主控台包含儀表板，可查看已完成或失敗的備份、複製和還原工作的指標。在此儀表板中，您可以按時段檢視任務狀態，並根據所需的時間範圍進行自訂。

存取儀表板

1. 請在以下位置開啟 AWS Backup 主控台。 https://console.aws.amazon.com/backup
2. 請在左側導覽窗格中選擇儀表板。

檢視和了解儀表板

CloudWatch 儀表板會顯示數個小器具。每個小工具會依計數顯示任務指標。每個小工具都會顯示幾張折線圖。每行都對應一個受保護的資源 (如果未顯示預期的資源，請確保在 設定 中開啟該資源)。其不會顯示進行中的任務。

Y 軸 (垂直值) 會顯示計數。X 軸 (水平值) 會顯示時間點。如果選取任務狀態中沒有可供視覺化的資料點，則該值將設定為 0，並在 x 軸上顯示水平線。顯示資源的圖例仍然可見。

指標會顯示與目前登入相關的帳戶特定和區域特定資訊。若要查看其他帳戶或區域，您必須登入所選帳戶。

自訂儀表板

預設的顯示時間範圍為一週。在頂部選單上，有用於重新定義顯示時間範圍的選項。您可以從 1 小時、3 小時、12 小時、1 天、3 天和 1 週中進行選擇。此外，您可以選取 自訂 來指定不同的值。「自訂」會暫時將目前檢視變更為您的規格。

您可以將滑鼠移至小工具上方，其右上角會顯示 放大 按鈕。請按一下 放大，以全螢幕檢視開啟小工具。全螢幕中還有更多自訂圖形顯示的選項，例如變更時段 (每個資料點之間的時間間隔)。關閉全螢幕檢視後，將不會保留任何變更。

若要一次只檢視一種資源類型，請按一下您要在圖形圖例中檢視之資源類型的標籤文字。這將取消選取其他所有資源類型。若要還原此操作，請按一下圖例中的資源類型顏色方塊。若要返回所有資源類型的預設檢視，同時選擇所有標籤，請再按一下任意已選取資源類型的標籤文字。

按一下小工具右上角的三個垂直點會開啟下拉式選單，其中包含「重新整理」、「放大」、「在指標中檢視」和「在記錄中檢視」的選項。「在指標中檢視」會開啟主 CloudWatch 控台中 Widget 中使用的指標。您可以在此處對 Widget 進行任何變更，並將 Widget 新增至儀表板中的自訂 CloudWatch 儀表板。您在 CloudWatch 儀表板中所做的任何變更都不會反映在 AWS Backup 主控台的儀表板上。「檢視為記錄檔」會在 CloudWatch 主控台中開啟記錄檢視頁面。

要將顯示的小部件添加到您自己的自定義 CloudWatch 儀表板，請單擊儀表板右上角的「添加到儀表板」按鈕。這將打開 CloudWatch 控制台，您可以在其中選擇要添加所有六個小部件的自定義儀表板。

如需詳細資訊，請參閱使用 Amazon CloudWatch 指標。

量度與 CloudWatch

您可以使用 CloudWatch 來監視 AWS Backup 指標。命`AWS/Backup`名空間可讓您追蹤下列指標。AWS Backup CloudWatch 每 5 分鐘發出一次更新的指標。

本文件頁面的目的是提供您用 CloudWatch 來監視的參考資料 AWS Backup。要了解如何使用監控指標 CloudWatch，請參閱用戶指南中的 Amazon CloudWatch 事件和指標 AWS Backup或關注單一 AWS 服務中的CloudWatch 指標和警示的部落格。若要設定鬧鐘，請參閱使用CloudWatch 者指南中的使用 Amazon CloudWatch 鬧鐘。

類別	指標	範例維度	範例使用案例
任務	每個狀態的備份、還原和複製任務數目，包括 `CREATED`、`PENDING`、`RUNNING`、`FAILED` 和 `EXPIRED`。 不同任務類型具有不同的可用狀態。	資源類型、保存庫名稱。 複製任務的保存庫名稱與其目標保存庫相同。	監視一或多個特定備份保存庫中的失敗備份任務數量。如果在 1 小時內發生五個以上的失敗任務，請使用 Amazon SNS 傳送電子郵件或簡訊，或向工程團隊開立票證以進行調查。 報告條件：有非零值

類別	指標	範例維度	範例使用案例
復原點	每個狀態中的暖復原點和冷復原點數量：MODIFIED、COMPLETE、PARTIAL、EXPIREI	資源類型、保存庫名稱。	可追蹤 Amazon EBS 磁碟區刪除的復原點數量，並分別追蹤每個備份保存庫中的暖復原點和冷復原點數量。 報告條件：有非零值

> **Note**
>
> 的工作狀態僅適用於 AWS Backup 主控台；無法透過以下方式進行追蹤 CloudWatch。`Completed with issues`

下表列出可用的所有指標。

指標	描述
`NumberOfBackupJobsCreated`	建立的備份工作數 AWS Backup 目。
`NumberOfBackupJobsPending`	即將在 AWS Backup中執行的備份任務數量。
`NumberOfBackupJobsRunning`	目前在中執行的備份工作數目 AWS Backup。
`NumberOfBackupJobsAborted`	使用者取消的備份任務數量。
`NumberOfBackupJobsCompleted`	已完成的備份 AWS Backup 工作數目。
`NumberOfBackupJobsFailed`	狀態為 `Failed` 的備份任務數量。通常是在資料庫資源前 1 小時或 Amazon FSx 維護時段或自動備份時段或自動備份時段之前或 4 小時之前或期間排定備份任務，且未用 AWS Backup 於執行 point-in-time 還原的連續備份所致。如需支援的服務清單，以及如何使用 AWS Backup 連續

指標	描述
	備份或重新排程備份任務的指示，請參閱時間點復原。
NumberOfBackupJobsExpired	AWS Backup 嘗試根據備份保留生命週期刪除但無法刪除的備份工作數目。系統會針對過期備份所耗用的儲存體計費，而且您應手動刪除這些儲存體。
NumberOfCopyJobsCreated	AWS Backup 建立的跨帳戶與跨區域複製任務數量。
NumberOfCopyJobsRunning	目前在 AWS Backup中執行的跨帳戶與跨區域複製任務數量。
NumberOfCopyJobsCompleted	AWS Backup 已完成的跨帳戶與跨區域複製任務數量。
NumberOfCopyJobsFailed	AWS Backup 嘗試但無法完成的跨帳戶和跨區域副本工作數目。
NumberOfRestoreJobsPending	即將在 AWS Backup中執行的還原任務數量。
NumberOfRestoreJobsRunning	目前在中執行的還原工作數目 AWS Backup。
NumberOfRestoreJobsCompleted	已完成的還原 AWS Backup 工作數目。
NumberOfRestoreJobsFailed	AWS Backup 嘗試但無法完成的還原工作數目。
NumberOfRecoveryPointsCompleted	建立的復原點數 AWS Backup 目。
NumberOfRecoveryPointsPartial	AWS Backup 開始建立但無法完成的復原點數目。 AWS 稍後會重試處理程序，但由於稍後會發生重試，因此會保留部分復原點。
NumberOfRecoveryPointsExpired	AWS Backup 嘗試根據備份保留生命週期刪除但無法刪除的復原點數目。系統會針對過期備份所耗用的儲存體計費，而且您應手動刪除這些儲存體。

指標	描述
NumberOfRecoveryPointsDeleting	正在刪除的復原點 AWS Backup 數目。
NumberOfRecoveryPointsCold	AWS Backup 階層至冷藏庫的復原點數目。

除了表格中列出的維度之外，還有更多維度可供使用。若要檢視某個測量結果的所有維度，請在 CloudWatch 主控台「度量」區段的**AWS/Backup**命名空間中輸入該測量結果的名稱。

使用記錄 AWS Backup API 呼叫 CloudTrail

AWS Backup 與 (提供中的使用者 AWS CloudTrail、角色或服務所採取的動作記錄) 的 AWS 服務整合 AWS Backup。 CloudTrail 擷取 AWS Backup 作為事件的所有 API 呼叫。擷取的呼叫包括來自 AWS Backup 主控台的呼叫和 AWS Backup API 作業的程式碼呼叫。如果您建立追蹤，您可以啟用持續交付 CloudTrail 事件到 Amazon S3 儲存貯體，包括 AWS Backup. 如果您未設定追蹤，您仍然可以在 [事件歷程記錄] 中檢視 CloudTrail 主控台中最近的事件。使用收集的資訊 CloudTrail，您可以判斷提出的要求 AWS Backup、提出要求的 IP 位址、提出要求的人員、提出要求的時間，以及其他詳細資訊。若要進一步了解 CloudTrail，請參閱使AWS CloudTrail 用者指南。

主題

- AWS Backup 中的資訊 CloudTrail
- 瞭解 AWS Backup 記錄檔項目
- 記錄跨帳戶管理事件

> **Important**
>
> 在記錄資料讀取事件的帳戶中，已啟用 CloudTrail 日誌的 S3 儲存貯體需要將其存取日誌儲存到不同的目標儲存貯體；如果 CloudTrail 日誌儲存在記錄的同一個儲存貯體中，則會形成無限迴圈。此迴圈可能會觸發意外和不必要的費用。
> 若要取得更多資訊，請參閱CloudTrail 使用指南中的資料事件。

AWS Backup 中的資訊 CloudTrail

CloudTrail 在您創建帳戶 AWS 帳戶 時啟用。當活動發生在中時 AWS Backup，該活動會與事件歷史記錄中的其他 AWS 服務 CloudTrail 事件一起記錄在事件中。您可以在您的. 中檢視、搜尋和下載最近的活動 AWS 帳戶。 AWS Backup 在執行備份、還原、複製或通知時產生這些 CloudTrail 事件：

- `BackupDeleted`
- `BackupJobCompleted`
- `BackupJobStarted`
- `BackupSelectionDeletedDueToSLRDeletion`
- `BackupTransitionedToCold`
- `CopyJobCompleted`
- `CopyJobStarted`
- `ReportJobCompleted`
- `ReportJobStarted`
- `RestoreCompleted`
- `RestoreStarted`
- `PutBackupVaultNotifications`

這些事件不一定是通過使用 AWS Backup 公共 API 生成的。相反，它們是通過 AWS Backup 異步執行您的作業生成的。例如，您的 StartBackupJobAPI 呼叫可能會產生`BackupJobStarted`事件，但是從備份計畫排定的工作也可以產生`BackupJobStarted`事件。

如需詳細資訊，請參閱檢視具有事 CloudTrail 件記錄的事件。

對於您的事件的持續記錄 AWS 帳戶，包括事件 AWS Backup，請創建一個跟踪。追蹤可 CloudTrail 將日誌檔交付到 Amazon S3 儲存貯體。根據預設，當您在主控台建立線索時，線索會套用到所有 AWS 區域。追蹤記錄來自 AWS 分區中所有區域的事件，並將日誌檔傳送到您指定的 Amazon S3 儲存貯體。此外，您還可以設定其他 AWS 服務，以進一步分析 CloudTrail 記錄中收集的事件資料並採取行動。如需詳細資訊，請參閱下列內容：

- 建立追蹤的概觀
- CloudTrail 支援的服務與整合
- 設定的 Amazon SNS 通知 CloudTrail

- 從多個區域接收 CloudTrail 記錄檔並從多個帳戶接收 CloudTrail記錄檔

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

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

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

瞭解 AWS Backup 記錄檔項目

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

下列範例顯示示範`StartBackupJob`、`StartRestoreJob`和`DeleteRecoveryPoint`動作以及`BackupJobCompleted`事件的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": aceess-key,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:45:24Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartBackupJob",
    "awsRegion": "us-east-1",
```

```
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-00a422a05b9c6asd3",
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "startWindowMinutes": 60
    },
    "responseElements": {
        "backupJobId": "8a3c2a87-b23e-4d56-b045-fa9e88ede4e6",
        "creationDate": "Jan 10, 2019 1:45:24 PM"
    },
    "requestID": "98cf4d59-8c76-49f7-9201-790743931234",
    "eventID": "fe8146a5-7812-4a95-90ad-074498be1234",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": "access-key",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T13:49:50Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "StartRestoreJob",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
```

```
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-00a129455bdbc9d99",
        "metadata": {
            "volumeType": "gp2",
            "availabilityZone": "us-east-1b",
            "volumeSize": "100"
        },
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
        "idempotencyToken": "a9c8b4fb-d369-4a58-944b-942e442a8fe3",
        "resourceType": "EBS"
    },
    "responseElements": {
        "restoreJobId": "9808E090-8C76-CCB8-4CEA-407CF6AC4C43"
    },
    "requestID": "783ddddc-6d7e-4539-8fab-376aa9668543",
    "eventID": "ff35ddea-7577-4aec-a132-964b7e9dd423",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Root",
        "principalId": "123456789012",
        "arn": "arn:aws:iam::123456789012:root",
        "accountId": "account-id",
        "accessKeyId": "access-key",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-01-10T12:24:50Z"
            }
        }
    },
    "eventTime": "2019-01-10T14:52:42Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteRecoveryPoint",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.34.567.89",
    "userAgent": "aws-internal/3 aws-sdk-java/1.11.465
 Linux/4.9.124-0.1.ac.198.73.329.metal1.x86_64 OpenJDK_64-Bit_Server_VM/25.192-b12
 java/1.8.0_192",
    "requestParameters": {
        "backupVaultName": "Default",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-05f426fd9daab3433"
```

```
    },
    "responseElements": null,
    "requestID": "f1f1b33a-48da-436c-9a8f-7574f1ab5fd7",
    "eventID": "2dd70080-5aba-4a79-9a0f-92647c9f0846",
    "eventType": "AwsApiCall",
    "recipientAccountId": "account-id"
},
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "account-id",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2019-01-10T08:24:39Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "BackupJobCompleted",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "2e7e4fcf-0c52-467f-9fd0-f61c2fcf7d17",
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "completionDate": {
            "seconds": 1547108091,
            "nanos": 906000000
        },
        "state": "COMPLETED",
        "percentDone": 100,
        "backupJobId": "8A8E738B-A8C5-E058-8224-90FA323A3C0E",
        "backupVaultName": "BackupVault",
        "backupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-
vault:BackupVault",
        "recoveryPointArn": "arn:aws:ec2:us-east-1::snapshot/snap-07ce8c3141d361233",
        "resourceArn": "arn:aws:ec2:us-east-1:123456789012:volume/
vol-06692095a6a421233",
        "creationDate": {
            "seconds": 1547101638,
            "nanos": 272000000
        },
        "backupSizeInBytes": 8589934592,
        "iamRoleArn": "arn:aws:iam::123456789012:role/AWSBackup",
```

```
        "resourceType": "EBS"
    }
}
```

記錄跨帳戶管理事件

使用 AWS Backup，您可以管理AWS Organizations結構 AWS 帳戶 內所有內部的備份。 AWS Backup 當您建立、更新或刪除 AWS Organizations 備份政策 (將備份計劃套用至您的成員帳戶) 或有無效的組織備份計劃時，會產生這些 CloudTrail 事件：

- `CreateOrganizationalBackupPlan`
- `UpdateOrganizationalBackupPlan`
- `DeleteOrganizationalBackupPlan`
- `InvalidOrganizationalBackupPlan`

範例：跨帳戶管理的 AWS Backup 記錄檔項目

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

下列範例顯示示範`CreateOrganizationalBackupPlan`動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "account-id",
        "invokedBy": "backup.amazonaws.com"},
    "eventTime": "2020-06-02T00:34:00Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "CreateOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "f2642255-af77-4203-8c37-7ca19d898e84",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
```

```
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "backupRules": "[{\"id\":\"745fd0ea-7f57-3f35-8a0e-ed4b8c48a8e2\",
\"name\":\"hourly\",\"description\":null,\"cryopodArn\":\"arn:aws:backup:ca-
central-1:123456789012:backup-vault:CryoControllerCAMTestBackupVault\",
\"scheduleExpression\":\"cron(0 0/1 ? * * *)\",\"startWindow\":\"PT1H\",
\"completionWindow\":\"PT2H\",\"lifecycle\":{\"moveToColdStorageAfterDays\":null,
\"deleteAfterDays\":\"7\"},\"tags\":null,\"copyActions\":[]}]",
        "backupSelections": "[{\"name\":\"selectiondatatype\",\"arn\":
\"arn:aws:backup:ca-central-1:123456789012:selection:8b40c6d9-3641-3d49-926d-
a075ea715686\",\"role\":\"arn:aws:iam::123456789012:role/OrganizationmyRoleTestRole\",
\"resources\":[],\"notResources\":[],\"conditions\":[{\"type\":\"STRINGEQUALS\",\"key
\":\"dataType\",\"value\":\"PII\"},{\"type\":\"STRINGEQUALS\",\"key\":\"dataType\",
\"value\":\"RED\"}],\"creationDate\":\"2020-06-02T00:34:00.695Z\",\"creatorRequestId
\":null}]",
        "creationDate": {
            "seconds": 1591058040,
            "nanos": 695000000
        },
        "organizationId": "org-id",
        "accountId": "account-id"
    }
}
```

下列範例顯示示範DeleteOrganizationalBackupPlan動作的 CloudTrail 記錄項目。

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "accountId": "account-id",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2020-06-02T00:34:25Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "DeleteOrganizationalBackupPlan",
    "awsRegion": "ca-central-1",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
```

```
    "requestParameters": null,
    "responseElements": null,
    "eventID": "5ce66cd0-b90c-4957-8e00-96ea1077b4fa",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "recipientAccountId": "account-id",
    "serviceEventDetails": {
        "backupPlanId": "orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanVersionId": "ZTA1Y2ZjZDYtNmRjMy00ZTA1LWIyNTAtM2M1NzQ4OThmNzRj",
        "backupPlanArn": "arn:aws:backup:ca-central-1:123456789012:backup-
plan:orgs/544033d1-b19c-3f2a-9c20-40bcfa82ca68",
        "backupPlanName": "mybackupplan",
        "deletionDate": {
            "seconds": 1591058065,
            "nanos": 519000000
        },
        "organizationId": "org-id",
        "accountId": "account-id"
    }
}
```

下列範例顯示示範事件的 CloudTrail 記錄項目InvalidOrganizationBackupPlan，該項目會在 AWS Backup 收到來自 Organizations 的無效備份計劃時傳送。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "accountId": "123456789012",
        "invokedBy": "backup.amazonaws.com"
    },
    "eventTime": "2022-06-11T13:29:23Z",
    "eventSource": "backup.amazonaws.com",
    "eventName": "InvalidOrganizationBackupPlan",
    "awsRegion": "Region",
    "sourceIPAddress": "backup.amazonaws.com",
    "userAgent": "backup.amazonaws.com",
    "requestParameters": null,
    "responseElements": null,
    "eventID": "ab1de234-fg56-7890-h123-45ij678k9l01",
    "readOnly": false,
    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "recipientAccountId": "987654321098",
```

```
    "serviceEventDetails": {
        "effectivePolicyVersion": 7,
        "effectivePolicyId": "12345678-a9b0-123c-45d6-78e901f23456",
        "lastUpdatedTimestamp": "Jun 11, 2022 1:29:22 PM",
        "policyType": "BACKUP_POLICY",
        "effectiveBackupPlan": {
            "logicalName": "logical-name",
            "regions": [
                "Region"
            ],
            "rules": [
                {
                    "name": "test-orgs",
                    "targetBackupVaultName": "vault-name",
                    "ruleLifecycle": {
                        "deleteAfterDays": 100
                    },
                    "copyActions": [],
                    "enableContinuousBackup": true
                }
            ],
            "selections": {
                "tagSelections": [
                    {
                        "selectionName": "selection-name",
                        "iamRoleArn": "arn:aws:iam::$account:role/role",
                        "targetedTags": [
                            {
                                "tagKey": "key",
                                "tagValue": "value"
                            }
                        ]
                    }
                ]
            },
            "backupPlanTags": {
                "key": "value"
            }
        },
        "organizationId": "org-id",
        "accountId": "account-id"
    },
    "eventCategory": "Management"
```

```
}
```

通知選項 AWS Backup

有兩種方式可以接收有關的通知 AWS Backup：

- AWS 使用者通知可以傳送通知，包括 Amazon CloudWatch 警示 AWS Support，以及其他服務的通知。
- Amazon 簡單通知服務可以通知您 AWS Backup 事件。

AWS 用戶通知和 AWS Backup

AWS Backup 支援從「AWS 使用者通知」主控台管理備份通知。透過 AWS 使用者通知，您可以從「使用者通知」通知中心檢視備份、複製和還原任務的進度，以及備份政策、保存庫、復原點和設定的變更。

Amazon CloudWatch、Amazon EventBridge 警示和 AWS Support 案例更新是您可以從主控台管理的其他類型的通知。此外，您還可以設定數個傳送選項，包括電子郵件、 AWS Chatbot 通知和 AWS Console Mobile Application 推播通知。

Amazon SNS 和 AWS Backup 事件

AWS Backup 利用亞馬遜簡單通知服務 (Amazon SNS) 提供的強大通知。您可以將 Amazon SNS 設定為透過 Amazon SNS 主控台通知您 AWS Backup 事件。

常用案例

- 依照如何取得失敗工作的通知？中的步驟，設定失敗備份 AWS Backup 工作的通知。 來自 AWS 高級 Support。
- 在下列事件資料表範例中，檢閱已完成、已失敗和已過期備份任務的 Amazon SNS 通知 JSON 範例。

如需 Amazon SNS 一般項目的詳細資訊，請參閱《Amazon Simple Notification Service 開發人員指南》中的 Amazon SNS 入門。

> **Note**
>
> 雖然 Amazon SNS 服務允許跨帳戶通知，但目前 AWS Backup 不支援此功能。您必須指定自己的 AWS 帳號 ID 和主題的資源 ARN。

AWS Backup 通知 API

使用 Amazon SNS 主控台或 AWS Command Line Interface (AWS CLI) 建立主題後，您可以使用下列 AWS Backup API 操作來管理備份通知。

- DeleteBackupVaultNotifications — 刪除特定備份保存庫的事件通知。
- GetBackupVaultNotifications — 列出特定備份保存庫的所有事件通知。
- PutBackupVaultNotifications — 開啟特定主題與事件的通知。

AWS Backup 支持以下事件：

任務類型	事件
備份任務	`BACKUP_JOB_STARTED` | `BACKUP_JOB_COMPLETED`
複製任務	`COPY_JOB_STARTED` | `COPY_JOB_SUCCESSFUL` | `COPY_JOB_FAILED`
還原任務	`RESTORE_JOB_STARTED` | `RESTORE_JOB_COMPLETED`
復原點	`RECOVERY_POINT_MODIFIED`

AWS Backup 對於 S3 支持兩個額外的事件：

- 在備份任務期間，`S3_BACKUP_OBJECT_FAILED` 可通知您 AWS Backup 無法備份的任何 S3 物件。
- 在還原任務期間，`S3_RESTORE_OBJECT_FAILED` 可通知您 AWS Backup 無法還原的任何 S3 物件。

事件範例

事件	Amazon SNS 通知

備份任務已完成	{
	"Records": [{
	"EventSource": "aws:sns",
	"EventVersion": "1.0",
	"EventSubscriptionArn":
	"arn:aws:sns: ...-a3802aa1ed45 ",
	"Sns": {
	"Type": "Notification",
	"MessageId": "12345678-
	abcd-123a-def0-abcd1a234567",
	"TopicArn": "arn:aws:
	sns:us-west-1:123456789012:
	backup-2sqs-sns-topic",
	"Subject": "Notification
	from AWS Backup",
	"Message": "An AWS
	Backup job was completed successfu
	lly. Recovery point ARN: arn:aws:e
	c2:us-west-1:123456789012:volume/
	vol-012f345df6789012d. Resource
	ARN : arn:aws:ec2:us-west-1:12345
	6789012:volume/vol-012f345d
	f6789012e. BackupJob ID : 1b2345b2-
	f22c-4dab-5eb6-bbc7890ed123",
	"Timestamp": "2019-08-
	02T18:46:02.788Z",
	...
	"MessageAttributes": {
	"EventType": {"Type":"
	String","Value":"BACKUP_JOB"},
	"State": {"Type":"
	String","Value":"COMPLETED"},
	"AccountId": {"Type":"
	String","Value":"123456789012"},
	"Id": {"Type":"
	String","Value":"1b2345b2-f
	22c-4dab-5eb6-bbc7890ed123"},

事件	Amazon SNS 通知
	"StartTime": {"Type":"String","Value":"2019-09-02T13:48:52.226Z"} } } }] }

事件	Amazon SNS 通知

備份任務已失敗	{
	"Records": [{
	"EventSource": "aws:sns",
	"EventVersion": "1.0",
	"EventSubscriptionArn":
	"arn:aws:sns: ...-a3802aa1ed45 ",
	"Sns": {
	"Type": "Notification",
	"MessageId": "12345678-
	abcd-123a-def0-abcd1a234567",
	"TopicArn": "arn:aws:
	sns:us-west-1:123456789012:
	backup-2sqs-sns-topic",
	"Subject": "Notification
	from AWS Backup",
	"Message": "An AWS Backup
	job failed. Resource ARN : arn:aws:e
	c2:us-west-1:123456789012:volume/
	vol-012f345df6789012e. BackupJob
	ID : 1b2345b2-f22c-4dab-5eb6-bbc
	7890ed123",
	"Timestamp": "2019-08-
	02T18:46:02.788Z",
	...
	"MessageAttributes": {
	"EventType": {"Type":"
	String","Value":"BACKUP_JOB"},
	"State": {"Type":"
	String","Value":"FAILED"},
	"AccountId": {"Type":"
	String","Value":"123456789012"},
	"Id": {"Type":"
	String","Value":"1b2345b2-f
	22c-4dab-5eb6-bbc7890ed123"},
	"StartTime": {"Type":"
	String","Value":"2019-09-02
	T13:48:52.226Z"}
	}
	}
	}]

事件	Amazon SNS 通知
	<pre>}</pre>

事件	Amazon SNS 通知

備份任務無法在備份期間完成	{
	"Records": [{
	"EventSource": "aws:sns",
	"EventVersion": "1.0",
	"EventSubscriptionArn":
	"arn:aws:sns: ...-a3802aa1ed45 ",
	"Sns": {
	"Type": "Notification",
	"MessageId": "12345678-
	abcd-123a-def0-abcd1a234567",
	"TopicArn": "arn:aws:
	sns:us-west-1:123456789012:
	backup-2sqs-sns-topic",
	"Subject": "Notification
	from AWS Backup",
	"Message": "An AWS Backup
	job failed to complete in time.
	Resource ARN : arn:aws:ec2:us-
	west-1:123456789012:volume/vol
	-012f345df6789012e. BackupJob
	ID : 1b2345b2-f22c-4dab-5eb6-bbc
	7890ed123",
	"Timestamp": "2019-08-
	02T18:46:02.788Z",
	...
	"MessageAttributes" : {
	"EventType" : {"Type":"
	String","Value":"BACKUP_JOB"},
	"State" : {"Type":"
	String","Value":"EXPIRED"},
	"AccountId" : {"Type":"
	String","Value":"123456789012"},
	"Id" : {"Type":"
	String","Value":"1b2345b2-f
	22c-4dab-5eb6-bbc7890ed123"},
	"StartTime" : {"Type":"
	String","Value":"2019-09-02
	T13:48:52.226Z"}
	}
	}
	}]

事件	Amazon SNS 通知
	}

AWS Backup 通知指令範例

您可以使用 AWS CLI 命令來訂閱、列出和刪除 AWS Backup 事件的 Amazon SNS 通知。

開啟備份保存庫通知的範例

下列命令能訂閱特定備份保存庫的 Amazon SNS 主題，該保存庫可在還原任務開始或完成，或者復原點有所變動時通知您。

```
aws backup put-backup-vault-notifications
    --backup-vault-name myBackupVault
    --sns-topic-arn arn:aws:sns:region:account-id:myBackupTopic
    --backup-vault-events RESTORE_JOB_STARTED RESTORE_JOB_COMPLETED
 RECOVERY_POINT_MODIFIED
```

取得備份保存庫通知的範例

下列命令能列出目前訂閱特定備份保存庫 Amazon SNS 主題的所有事件。

```
aws backup get-backup-vault-notifications
           --backup-vault-name myVault
```

輸出範例如下所示：

```
{
    "SNSTopicArn": "arn:aws:sns:region:account-id:myBackupTopic",
    "BackupVaultEvents": [
        "RESTORE_JOB_STARTED",
        "RESTORE_JOB_COMPLETED",
        "RECOVERY_POINT_MODIFIED"
    ],
    "BackupVaultName": "myVault",
    "BackupVaultArn": "arn:aws:backup:region:account-id:backup-vault:myVault"
}
```

刪除備份保存庫通知的範例

下列命令能取消訂閱指定備份保存庫的 Amazon SNS 主題。

```
aws backup delete-backup-vault-notifications
          --backup-vault-name myVault
```

指定 AWS Backup 為服務主體

> **Note**
>
> 若 AWS Backup 要允許代表您發佈 SNS 主題，您必須指定 AWS Backup 為服務主體。

請在用來追蹤 AWS Backup 事件的 Amazon SNS 主題存取政策中加入下列 JSON。您必須指定該主題的資源 Amazon Resource Name (ARN)。

```
{
      "Sid": "My-statement-id",
      "Effect": "Allow",
      "Principal": {
        "Service": "backup.amazonaws.com"
      },
      "Action": "SNS:Publish",
      "Resource": "arn:aws:sns:region:account-id:myTopic"
}
```

如需有關在 Amazon SNS 存取政策中指定服務主體的詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的允許任何 AWS 資源發佈到主題。

> **Note**
>
> 如果您的主題已加密，您必須在原則中包含其他權限，才能發佈 AWS Backup 至該主題。如需有關啟用服務發佈到加密主題的詳細資訊，請參閱 Amazon 簡單通知服務開發人員指南中的啟用 AWS 服務的事件來源與加密主題之間的相容性。

疑難排 AWS Backup

使用時 AWS Backup，您可能會遇到問題。下列各節可幫助您排除一些可能發生的常見問題。

如需有關的一般問題 AWS Backup，請參閱AWS Backup 常見問題集。您也可以在 AWS Backup 論壇中搜尋解答和發表問題。

主題

疑難排解一般問題

當您備份和還原資源時，您不僅需要使用權限 AWS Backup，還必須具有存取要保護之資源的權限。擁有適當許可的最簡單方法，是在將資源指派給備份計畫時，選擇 預設角色。如需使用 AWS Identity and Access Management (IAM) 搭配使用存取控制的詳細資訊 AWS Backup，請參閱存取控制。

如果在備份和還原特定資源類型時發生問題，建議您查看該資源的備份和還原故障診斷主題。如需詳細資訊，請參閱「如何與支援的 AWS 服務 AWS Backup 搭配使用」下的連結。

如果 AWS Backup 無法建立或刪除資源，您可以使用檢視錯誤訊息或記錄檔 AWS CloudTrail 來深入瞭解問題。若要取得有關使用 CloudTrail與的更多資訊 AWS Backup，請參閱使用記錄 AWS Backup API 呼叫 CloudTrail。

建立資源問題的故障診斷

下列資訊可幫助您就建立備份的問題進行疑難排解。

- 一般而言，AWS 資料庫服務無法在維護時段或自動備份時段期間或前 1 小時內啟動備份。Amazon FSx 無法在維護時段或自動備份時段期間或前 4 小時內啟動備份 (Amazon Aurora 不受此維護時段限制)。排程在這些時段內的快照備份會失敗。一個例外狀況：當您 AWS Backup 針對支援的服務選擇同時使用快照和連續備份時，您不再需要擔心這些視窗，因為 AWS Backup 會為您排程這些視窗。如需支援的服務清單以及如何使用 AWS Backup 連續備份的指示，請參閱時間點復原。
- 建立資料表時將無法建立 DynamoDB 資料表備份。建立 DynamoDB 資料表一般需要好幾分鐘。

- 當檔案系統非常龐大時，備份 Amazon EFS 檔案系統最長需要 7 天。Amazon EFS 檔案系統一次只能佇列一個並行備份。當前一個備份仍在進行時，若有後續備份排入佇列，備份時段便會過期，且系統不會建立任何備份。
- Amazon EBS 每 AWS 區域 個帳戶的軟配額為 100,000 個備份，而當達到此配額時，其他備份會失敗。如果您達到此配額，則可刪除多餘的備份或請求提高配額。如需有關請求提高配額的詳細資訊，請參閱 AWS 服務配額。
- 建立 Amazon Relational Database Service (RDS) 備份時，請考量下列事項：
  - 如果您不使用 AWS Backup 同時管理 Amazon RDS 快照和具有 point-in-time 復原功能的連續備份，則如果在每日、使用者可設定的 30 分鐘備份時段內排定或按需進行，則備份將會失敗。如需自動化 Amazon RDS 備份的詳細資訊，請參閱《Amazon RDS 使用者指南》的使用備份。您可以使用管理 Amazon RDS 快照和具有 point-in-time 復原功能的連續備份 AWS Backup 來避免此限制。
  - 如果您從 Amazon RDS 主控台啟動備份任務，可能會與 Aurora 叢集的備份任務發生衝突，造成錯誤：`Backup job expired before completion.`；如果發生此情況，請在 AWS Backup 中設定較長的備份時段。
  - AWS Backup 建立複製工作時，目前未傳遞 TDE 選項群組。如果您打算使用此選項群組建立複製任務，即必須使用 Amazon RDS 主控台或 Amazon RDS API，而不是使用 AWS Backup 工具。如需詳細資訊，請參閱 《Amazon Relational Database Service 使用者指南》中的複製選項群組。
  - 錯誤：隨需備份完成，但排程備份失敗，並顯示錯誤訊息：「來源快照 KMS 金鑰不存在、未啟用或您無權存取」。隨需任務已完成，因為使用 API 呼叫 `CopyDBSnapshot`，不需要 KMS 存取權。

    補決方法：將 IAM 角色新增至您的 KMS 金鑰。只要在您的 KMS 金鑰政策中允許該角色即可。

    編輯政策步驟：

    1. 開啟 KMS 主控台。
    2. 在左側導覽列中，選取 客戶自管金鑰。
    3. 按一下您想要編輯的客戶自管金鑰。
    4. 在 金鑰政策 下，按一下 切換至政策檢視。
    5. 按一下 Edit (編輯)。
    6. 新增該角色。

刪除資源問題的故障診斷

AWS Backup 無法在受保護資源的主控台視窗中刪除由建立的復原點。您可以在 AWS Backup 主控台上刪除它們，方法是在儲存資料保險箱中選取它們，然後選擇「刪除」(Delete)。

您必須具備適當許可，才能刪除復原點或備份文件庫。如需使用 IAM 搭配使用存取控制的詳細資訊 AWS Backup，請參閱存取控制。

還原資源問題的故障診斷

使用 API 還原

若要以程式設計方式還原備份，請使用 StartRestoreJob API 作業。

若要取得建立備份所用的組態中繼資料，請呼叫 GetRecoveryPointRestoreMetadata。

如需詳細資訊，請參閱還原備份。

使用主控台還原

- 還原 Amazon S3 資料
- 還原虛擬機器
- 還原 Amazon FSx 檔案系統
- 還原 Amazon EBS 磁碟區
- 還原 Amazon EFS 檔案系統
- 還原 Amazon DynamoDB 資料表
- 還原 Amazon RDS 資料庫
- 還原 Aurora 叢集
- 還原 Amazon EC2 執行個體
- 還原 Storage Gateway 磁碟區
- 還原 Amazon DocumentDB 叢集
- 還原 Neptune 叢集

AWS Backup API

除了使用主控台，您可以使用 AWS Backup API 動作及資料類型，以程式設計方式設定和管理 AWS Backup 及其資源。本節說明 AWS Backup 動作和資料類型。其包含 AWS Backup 的 API 參考。

AWS Backup API

- AWS Backup 動作
- AWS Backup 資料類型

動作

AWS Backup 支援下列動作：

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework
- DeleteRecoveryPoint

- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection
- GetSupportedResourceTypes

- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob
- StartCopyJob

- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

AWS Backup gateway 支援下列動作：

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway
- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines

- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AWS Backup

AWS Backup 支援下列動作：

- CancelLegalHold
- CreateBackupPlan
- CreateBackupSelection
- CreateBackupVault
- CreateFramework
- CreateLegalHold
- CreateLogicallyAirGappedBackupVault
- CreateReportPlan
- CreateRestoreTestingPlan
- CreateRestoreTestingSelection
- DeleteBackupPlan
- DeleteBackupSelection
- DeleteBackupVault
- DeleteBackupVaultAccessPolicy
- DeleteBackupVaultLockConfiguration
- DeleteBackupVaultNotifications
- DeleteFramework

- DeleteRecoveryPoint
- DeleteReportPlan
- DeleteRestoreTestingPlan
- DeleteRestoreTestingSelection
- DescribeBackupJob
- DescribeBackupVault
- DescribeCopyJob
- DescribeFramework
- DescribeGlobalSettings
- DescribeProtectedResource
- DescribeRecoveryPoint
- DescribeRegionSettings
- DescribeReportJob
- DescribeReportPlan
- DescribeRestoreJob
- DisassociateRecoveryPoint
- DisassociateRecoveryPointFromParent
- ExportBackupPlanTemplate
- GetBackupPlan
- GetBackupPlanFromJSON
- GetBackupPlanFromTemplate
- GetBackupSelection
- GetBackupVaultAccessPolicy
- GetBackupVaultNotifications
- GetLegalHold
- GetRecoveryPointRestoreMetadata
- GetRestoreJobMetadata
- GetRestoreTestingInferredMetadata
- GetRestoreTestingPlan
- GetRestoreTestingSelection

- GetSupportedResourceTypes
- ListBackupJobs
- ListBackupJobSummaries
- ListBackupPlans
- ListBackupPlanTemplates
- ListBackupPlanVersions
- ListBackupSelections
- ListBackupVaults
- ListCopyJobs
- ListCopyJobSummaries
- ListFrameworks
- ListLegalHolds
- ListProtectedResources
- ListProtectedResourcesByBackupVault
- ListRecoveryPointsByBackupVault
- ListRecoveryPointsByLegalHold
- ListRecoveryPointsByResource
- ListReportJobs
- ListReportPlans
- ListRestoreJobs
- ListRestoreJobsByProtectedResource
- ListRestoreJobSummaries
- ListRestoreTestingPlans
- ListRestoreTestingSelections
- ListTags
- PutBackupVaultAccessPolicy
- PutBackupVaultLockConfiguration
- PutBackupVaultNotifications
- PutRestoreValidationResult
- StartBackupJob

- StartCopyJob
- StartReportJob
- StartRestoreJob
- StopBackupJob
- TagResource
- UntagResource
- UpdateBackupPlan
- UpdateFramework
- UpdateGlobalSettings
- UpdateRecoveryPointLifecycle
- UpdateRegionSettings
- UpdateReportPlan
- UpdateRestoreTestingPlan
- UpdateRestoreTestingSelection

CancelLegalHold

服務： AWS Backup

此動作會移除復原點上的指定法務保存。這個動作只能由擁有足夠許可的使用者執行。

請求語法

```
DELETE /legal-holds/legalHoldId?
cancelDescription=CancelDescription&retainRecordInDays=RetainRecordInDays HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

CancelDescription

字串，說明移除法務保存的原因。

必要：是

legalHoldId

移除復原點上指定法務保存所需的法務保存 ID。

必要：是

RetainRecordInDays

以天為單位的整數數量，指定此 API 操作後要刪除法務保存的天數。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 201
```

回應元素

如果動作成功，則服務會傳回具有空 HTTP 內文的 HTTP 201 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidResourceStateException

AWS Backup 已在此復原點上執行動作。在第一個動作完成之前，其無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateBackupPlan

服務： AWS Backup

使用備份計畫名稱和備份規則建立備份計畫。備份計畫是一份文件，其中包含 AWS Backup 用來排定建立資源復原點之任務的資訊。

如果呼叫 CreateBackupPlan 已經存在的計畫，您會收到 AlreadyExistsException 例外。

請求語法

```
PUT /backup/plans/ HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
```

```
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   },
   "BackupPlanTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

BackupPlan

指定備份計劃的本文。包括一個 BackupPlanName 和一或多組 Rules。

類型：BackupPlanInput 物件

必要：是

BackupPlanTags

為協助組織您的資源，您可以將自己的中繼資料指派給您建立的資源。每個標籤都是金鑰值對。指定的標籤會指派給使用此計畫建立的所有備份。

類型：字串到字串映射

必要：否

CreatorRequestId

可識別請求且允許重試失敗的請求，而不會有兩次執行操作的風險。如果請求包含符合現有備份計畫的 CreatorRequestId，則會傳回該計畫。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AdvancedBackupSettings

資源類型的 BackupOptions 設定清單。此選項僅適用於 Windows 磁碟區陰影複製服務 (VSS) 備份任務。

類型：AdvancedBackupSetting 物件陣列

BackupPlanArn

可唯一識別備份計畫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

類型：字串

BackupPlanId

唯一識別備份計畫。

類型：字串

CreationDate

建立備份計畫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。您無法對其進行編輯。

類型：字串

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateBackupSelection

服務： AWS Backup

建立 JSON 文件，可指定要指派給備份計畫的一組資源。如需範例，請參閱《Assigning resources programmatically》。

請求語法

```
PUT /backup/plans/backupPlanId/selections/ HTTP/1.1
Content-type: application/json

{
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
```

```
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreatorRequestId": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別與資源選取相關聯的備份計畫。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupSelection

指定請求的內文，將一組資源指派給備份計畫。

類型：BackupSelection 物件

必要：是

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "CreationDate": number,
   "SelectionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanId

唯一識別備份計畫。

類型：字串

CreationDate

建立備份選擇時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

SelectionId

可唯一識別請求本文，將一組資源指派給備份計畫。

類型：字串

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateBackupVault

服務： AWS Backup

建立用來存放備份的邏輯容器。CreateBackupVault 請求包含名稱、選用的一或多個資源標籤、加密金鑰以及請求 ID。

> **Note**
>
> 不得在備份文件庫名稱中包含敏感資料，例如護照號碼。

請求語法

```
PUT /backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由字母、數字和連字號組成。

模式：^[a-zA-Z0-9\-_]{2,50}$

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupVaultTags

您可以指派中繼資料，協助組織您建立的資源。每個標籤都是金鑰值對。

類型：字串到字串映射

必要：否

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

EncryptionKeyArn

用來保護備份的伺服器端加密金鑰，例如 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

建立備份保存庫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CreationDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateFramework

服務： AWS Backup

建立具有一或多個控制項的架構。架構是可用於評估備份實際做法的控制項集合。透過使用預先建立的可自訂控制項來定義政策，您即可評估備份實際做法是否符合您的政策，以及哪些資源尚未合規。

請求語法

```
POST /audit/frameworks HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkTags": {
      "string" : "string"
   },
   "IdempotencyToken": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

FrameworkControls

組成架構的控制項清單。清單中的每個控制項都具有名稱、輸入參數和範圍。

類型：FrameworkControl 物件陣列

必要：是

FrameworkDescription

架構的選用描述，最多包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`.*\S.*`

必要：否

FrameworkName

架構的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，以英文字母開頭，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必要：是

FrameworkTags

您可以指派的中繼資料，以協助組織您建立的架構。每個標籤都是金鑰值對。

類型：字串到字串映射

必要：否

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 CreateFrameworkInput 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "FrameworkArn": "string",
   "FrameworkName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

FrameworkArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

FrameworkName

架構的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，以英文字母開頭，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版

- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateLegalHold

服務： AWS Backup

此動作會對復原點 (備份) 建立法務保存。法務保存是在授權使用者取消法務保存之前，針對變更或刪除備份所進行的限制。如果復原點上有一或多個有效的法務保存，則刪除或取消關聯復原點的任何動作都會失敗，並顯示錯誤。

請求語法

```
POST /legal-holds/ HTTP/1.1
Content-type: application/json

{
   "Description": "string",
   "IdempotencyToken": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Tags": {
      "string" : "string"
   },
   "Title": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

Description

這是法務保存的字串描述。

類型：字串

必要：是

IdempotencyToken

這是使用者選擇的字符，可用於區分在其他方面相同的呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

RecoveryPointSelection

這指定了用於指派一組資源的條件，例如資源類型或備份保存庫。

類型：RecoveryPointSelection 物件

必要：否

Tags

要包含的選用標籤。標籤是可用於管理、篩選和搜尋資源的鍵值對。允許使用的字元包括 UTF-8 字母、數字、空格，以及下列字元：+ - = . _ : /。

類型：字串到字串映射

必要：否

Title

這是法務保存的字串標題。

類型：字串

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
```

```
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
   },
   "Status": "string",
   "Title": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationDate

建立法務保存時的時間 (以數字格式顯示)。

類型：Timestamp

Description

這是法務保存的傳回字串描述。

類型：字串

LegalHoldArn

這是所建立法務保存的 ARN (Amazon Resource Number)。

類型：字串

LegalHoldId

針對復原點上指定法務保存而傳回的法務保存 ID。

類型：字串

RecoveryPointSelection

這指定了用於指派一組資源的條件，例如資源類型或備份保存庫。

類型：RecoveryPointSelection 物件

Status

這會顯示建立法務保存後，所傳回法務保存的狀態。狀態可以是 ACTIVE、PENDING、CANCELED、CANCELING 或 FAILED。

類型：字串

有效值:CREATING | ACTIVE | CANCELING | CANCELED

Title

這是建立法務保存之後，所傳回法務保存的字串標題。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateLogicallyAirGappedBackupVault

服務： AWS Backup

這項請求會建立可複製備份的邏輯容器。

這項請求包括名稱、區域、保留天數上限、保留天數下限，並可選擇性地包含標籤和建立者請求 ID。

> **Note**
>
> 不得在備份文件庫名稱中包含敏感資料，例如護照號碼。

請求語法

```
PUT /logically-air-gapped-backup-vaults/backupVaultName HTTP/1.1
Content-type: application/json

{
   "BackupVaultTags": {
      "string" : "string"
   },
   "CreatorRequestId": "string",
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

這是正在建立之保存庫的名稱。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupVaultTags

這些是將包括在新建立保存庫中的標籤。

類型：字串到字串映射

必要：否

CreatorRequestId

這是建立請求的 ID。

此為選用參數。如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

MaxRetentionDays

這是指定保存庫保留其復原點最長保留期間的設定。若未指示此參數， AWS Backup 不會對保存庫中的復原點強制執行最長保留期間 (允許無限期儲存)。

若經指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或短於最長保留期間。若任務的保留期間超過該最長保留期間，則保存庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的保存庫。

類型：Long

必要：是

MinRetentionDays

這項設定可指定保存庫保留復原點的最短保留期間。若未指定此參數，則不會強制執行最短保留期間。

若經過指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或超過最短保留期間。若任務的保留期間未達最短保留期間，則保存庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的保存庫。

類型：Long

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "VaultState": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

這是要建立保存庫的 ARN (Amazon Resource Name)。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。邏輯氣隙隔離備份保存庫依名稱識別，這些名稱對用於建立保存庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

CreationDate

建立保存庫的日期和時間。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

VaultState

這是保存庫的目前狀態。

類型：字串

有效值:CREATING | AVAILABLE | FAILED

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

CreateReportPlan

服務： AWS Backup

建立報告計畫。報告計畫是一份文件，其中包含有關報告內容以及 AWS Backup 在何處交付報告的資訊。

如果呼叫 `CreateReportPlan` 已經存在的計畫，您會收到 `AlreadyExistsException` 例外。

請求語法

```
POST /audit/report-plans HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportPlanName": "string",
   "ReportPlanTags": {
      "string" : "string"
   },
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 CreateReportPlanInput 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

ReportDeliveryChannel

包含有關在何處和如何交付報告的架構，特別是 Amazon S3 儲存貯體名稱、S3 金鑰字首以及報告格式。

類型：ReportDeliveryChannel 物件

必要：是

ReportPlanDescription

報告計畫的選用描述，最多可包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：.*\S.*

必要：否

ReportPlanName

報告計畫的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，以英文字母開頭，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

ReportPlanTags

您可以指派中繼資料，協助組織您建立的報告計畫。每個標籤都是金鑰值對。

類型：字串到字串映射

必要：否

ReportSetting

識別報告的報告範本。使用報告範本建立的報告。報告範本包括：

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

如果報告範本為 RESOURCE_COMPLIANCE_REPORT 或 CONTROL_COMPLIANCE_REPORT，此 API 資源也可以依 AWS 區域 和架構描述報告涵蓋範圍。

類型：ReportSetting 物件

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

建立備份保存庫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

ReportPlanArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

ReportPlanName

報告計畫的唯一名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateRestoreTestingPlan

服務： AWS Backup

這是建立還原測試計畫之兩步驟中的第一步；一旦此請求成功，請使用請求 CreateRestoreTestingSelection 來完成程序。

您必須包含參數 RestoreTestingPlan。您可以選擇性地包括 CreatorRequestId 和標籤。

請求語法

```
PUT /restore-testing/plans HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "RestoreTestingPlanName": "string",
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   },
   "Tags": {
      "string" : "string"
   }
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

CreatorRequestId

此為可識別請求的不重複字串，且允許重試失敗的請求，而不會有兩次執行作業的風險。此為選用參數。如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

RestoreTestingPlan

還原測試計畫必須包含您建立的不重複 RestoreTestingPlanName 字串，並且必須包含 ScheduleExpression cron。您可以選擇性包含 StartWindowHours 整數和 CreatorRequestId 字串。

RestoreTestingPlanName 是不重複的字串，也是還原測試計畫的名稱。您無法在建立後變更此名稱，其必須只包含英數字元和底線。

類型：RestoreTestingPlanForCreate 物件

必要：是

Tags

要包含的選用標籤。標籤是可用於管理、篩選和搜尋資源的鍵值對。允許使用的字元包括 UTF-8 字母、數字、空格，以及下列字元：+ - = . _ : /。

類型：字串到字串映射

必要：否

回應語法

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

建立還原測試計畫的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

RestoreTestingPlanArn

唯一識別所建立還原測試計畫的 Amazon Resource Name (ARN)。

類型：字串

RestoreTestingPlanName

此不重複字串是還原測試計畫的名稱。

此名稱建立後就不可變更。此名稱僅包含英數字元和底線。長度上限為 50。

類型：字串

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

ConflictException

在完成上一個動作之前，AWS Backup 無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateRestoreTestingSelection

服務： AWS Backup

請求成功返回後，可以發送此 CreateRestoreTestingPlan 請求。這是建立資源測試計畫的第二部分，必須按順序完成。

其中包括 RestoreTestingSelectionName、ProtectedResourceType 以及下列其中一項：

- ProtectedResourceArns
- ProtectedResourceConditions

每個受保護的資源類型可以有一個單一值。

還原測試選擇可以包含 ProtectedResourceArns 和 ProtectedResourceConditions 的萬用字元值 (「*」)。或者，您可以在 ProtectedResourceArns 中包含最多 30 個特定受保護的資源 ARN。

無法同時依照受保護的資源類型和特定 ARN 進行選取。如果兩者都包含，則請求將失敗。

請求語法

```
PUT /restore-testing/plans/RestoreTestingPlanName/selections HTTP/1.1
Content-type: application/json

{
   "CreatorRequestId": "string",
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
```

```
        ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

輸入從相關 CreateRestoreTestingPlan 請求返回的還原測試計劃名稱。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

CreatorRequestId

此為可識別請求的選用不重複字串，且允許重試失敗的請求，而不會有兩次執行作業的風險。如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

RestoreTestingSelection

其中包括 RestoreTestingSelectionName、ProtectedResourceType 以及下列其中一項：

- ProtectedResourceArns
- ProtectedResourceConditions

每個受保護的資源類型可以有一個單一值。

還原測試選擇可以包含 ProtectedResourceArns 和 ProtectedResourceConditions 的萬用字元值 (「*」)。或者，您可以在 ProtectedResourceArns 中包含最多 30 個特定受保護的資源 ARN。

類型：RestoreTestingSelectionForCreate 物件

必要：是

回應語法

```
HTTP/1.1 201
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 201 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

這是成功建立資源測試選擇的時間。

類型：Timestamp

RestoreTestingPlanArn

這是與還原測試選擇相關聯的還原測試計畫 ARN。

類型：字串

RestoreTestingPlanName

不重複字串，也就是還原測試計畫的名稱。

此名稱建立後就不可變更。此名稱僅包含英數字元和底線。長度上限為 50。

類型：字串

RestoreTestingSelectionName

這是屬於相關還原測試計畫之還原測試選擇的不重複名稱。

類型：字串

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupPlan

服務： AWS Backup

刪除備份計劃。只有在刪除所有相關聯的選取資源之後，才能刪除備份計劃。刪除備份計劃將會刪除該備份計劃的目前版本。先前的版本 (若有) 將依然存在。

請求語法

```
DELETE /backup/plans/backupPlanId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "DeletionDate": number,
   "VersionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanArn

可唯一識別備份計畫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`。

類型：字串

BackupPlanId

唯一識別備份計畫。

類型：字串

DeletionDate

刪除備份計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`DeletionDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。版本 ID 不能編輯。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupSelection

服務： AWS Backup

刪除與備份計劃 (由 `SelectionId` 指定) 相關聯的資源選取項目。

請求語法

```
DELETE /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

selectionId

可唯一識別請求本文，將一組資源指派給備份計劃。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupVault

服務： AWS Backup

刪除以其名稱識別的備份保存庫。只有在保存庫為空時才能刪除。

請求語法

```
DELETE /backup-vaults/backupVaultName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupVaultAccessPolicy

服務： AWS Backup

刪除管理備份保存庫許可的政策文件。

請求語法

```
DELETE /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupVaultLockConfiguration

服務： AWS Backup

從備份 AWS Backup 資料保險箱名稱指定的備份儲存庫中刪除資料保險箱鎖住。

如果Vault Lock 組態不可變，則您無法使用 API 操作刪除 Vault Lock ，如果您嘗試這項動作，您將收到一個 `InvalidRequestException`。若要取得更多資訊，請參閱 AWS Backup 開發人員指南中的文件庫鎖定

請求語法

```
DELETE /backup-vaults/backupVaultName/vault-lock HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

要從中刪除文件庫鎖定的備份文件 AWS Backup 庫的名稱。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 V3 的 SDK

DeleteBackupVaultNotifications

服務： AWS Backup

刪除指定備份文件庫的事件通知。

請求語法

```
DELETE /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteFramework

服務： AWS Backup

刪除由架構名稱指定的架構。

請求語法

```
DELETE /audit/frameworks/frameworkName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

frameworkName

架構的唯一名稱。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteRecoveryPoint

服務： AWS Backup

可刪除復原點 ID 所指定的復原點。

如果復原點 ID 屬於連續備份，則呼叫此端點會刪除現有的持續備份，並停止未來的持續備份。

當 IAM 角色的許可不足以呼叫此 API 時，服務會傳回含有空白 HTTP 內文的 HTTP 200 回應，但不會刪除復原點。相反的，其會進入 EXPIRED 狀態。

一旦 IAM 角色執行 `iam:CreateServiceLinkedRole` 動作，就可以使用此 API 刪除 EXPIRED 復原點。若要深入了解如何新增此角色，請參閱疑難排解手動刪除。

如果刪除使用者或角色，或移除角色內的許可，則刪除將不會成功，並將進入 EXPIRED 狀態。

請求語法

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

InvalidResourceStateException

AWS Backup 已在此復原點上執行動作。在第一個動作完成之前，其無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteReportPlan

服務： AWS Backup

刪除由報告計劃名稱所指定的報告計劃。

請求語法

```
DELETE /audit/report-plans/reportPlanName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

reportPlanName

報告計畫的唯一名稱。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteRestoreTestingPlan

服務： AWS Backup

此請求會刪除指定的還原測試計畫。

只有先刪除所有關聯的還原測試選擇後，才能成功刪除。

請求語法

```
DELETE /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

要刪除的還原測試計畫的必要不重複名稱。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DeleteRestoreTestingSelection

服務： AWS Backup

輸入還原測試計畫名稱和還原測試選擇名稱。

必須刪除與還原測試計畫相關聯的所有測試選擇，然後才能刪除還原測試計畫。

請求語法

```
DELETE /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

還原測試計畫的必要不重複名稱，此還原測試計畫中包含您要刪除的還原測試選擇。

必要：是

RestoreTestingSelectionName

您要刪除之還原測試選擇的必要不重複名稱。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeBackupJob

服務： AWS Backup

傳回指定之 BackupJobId 的備份詳細資訊。

請求語法

```
GET /backup-jobs/backupJobId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupJobId

唯一識別備份 AWS Backup 資源的請求。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupJobId": "string",
   "BackupOptions": {
      "string" : "string"
   },
   "BackupSizeInBytes": number,
   "BackupType": "string",
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "BytesTransferred": number,
   "ChildJobsInState": {
      "string" : number
   },
```

```
   "CompletionDate": number,
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "ExpectedCompletionDate": number,
   "IamRoleArn": "string",
   "InitiationDate": number,
   "IsParent": boolean,
   "MessageCategory": "string",
   "NumberOfChildJobs": number,
   "ParentJobId": "string",
   "PercentDone": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "StartBy": number,
   "State": "string",
   "StatusMessage": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AccountId

傳回擁有備份任務的帳戶 ID。

類型：String

模式：^[0-9]{12}$

BackupJobId

唯一識別備份 AWS Backup 資源的請求。

類型：字串

BackupOptions

代表指定為備份計畫或隨需備份任務之一部分的選項。

類型：字串到字串映射

金鑰模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

BackupSizeInBytes

備份的大小，以位元組為單位。

類型：Long

BackupType

代表針對備份任務所選取的實際備份類型。例如，如果成功取得 Windows 磁碟區陰影複製服務 (VSS) 備份，BackupType 會傳回 "WindowsVSS"。如果 BackupType 為空，則備份類型為定期備份。

類型：字串

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:vault:aBackupVault。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：^[a-zA-Z0-9\-_]{2,50}$

BytesTransferred

查詢任務狀態時傳輸至備份文件庫的大小 (以位元組為單位)。

類型：Long

ChildJobsInState

這會傳回所包含之子 (巢狀) 複製任務的統計資訊。

類型：字串到長映射

有效金鑰：CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

CompletionDate

某任務建立備份任務的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CompletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CreatedBy

含有建立備份任務的相關識別資訊，包括用以建立備份任務之備份計畫的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

類型：RecoveryPointCreator 物件

CreationDate

建立備份任務時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

ExpectedCompletionDate

某任務備份資源預期完成的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。ExpectedCompletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN；例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

InitiationDate

這是備份任務的開始日期。

類型：Timestamp

IsParent

這會傳回備份任務為父項 (複合) 任務的布林值。

類型：布林值

MessageCategory

這是指定訊息類別的任務計數。

範例字串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 INVALIDPARAMETERS。檢視監視以取得接受的 MessageCategory 字串清單。

類型：字串

NumberOfChildJobs

這會傳回子 (巢狀) 備份任務的數目。

類型：Long

ParentJobId

這會傳回父項 (複合) 資源備份任務 ID。

類型：字串

PercentDone

包含查詢任務狀態時，任務的預估完成百分比。

類型：字串

RecoveryPointArn

可唯一識別復原點的 ARN；例如 arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

ResourceArn

可唯一識別已儲存資源的 ARN。ARN 的格式取決於資源類型。

類型：字串

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

ResourceType

要備份的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

StartBy

指定在備份任務取消之前必須開始的時間，以 Unix 格式和國際標準時間 (UTC) 顯示。該值是透過將開始時段加至排定時間來計算。因此，如果排定的時間為下午 6 點，而開始時段為 2 小時，則 StartBy 時間將是指定日期的下午 8 點。StartBy 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

State

備份任務目前的狀態。

類型：字串

有效值:`CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL`

StatusMessage

說明備份資源任務狀態的詳細訊息。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

DependencyFailureException

相依 AWS 服務或資源將錯誤傳回給 AWS Backup 服務，且動作無法完成。

HTTP 狀態碼：500

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 V3 的 SDK

DescribeBackupVault

服務： AWS Backup

傳回備份保存庫 (由其名稱所指定) 的相關中繼資料。

請求語法

```
GET /backup-vaults/backupVaultName?backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

這是指定的備份保存庫的帳戶 ID。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CreationDate": number,
   "CreatorRequestId": "string",
   "EncryptionKeyArn": "string",
   "LockDate": number,
   "Locked": boolean,
   "MaxRetentionDays": number,
```

```
    "MinRetentionDays": number,
    "NumberOfRecoveryPoints": number,
    "VaultType": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:vault:aBackupVault。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：字串

CreationDate

建立備份保存庫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

EncryptionKeyArn

用來保護備份的伺服器端加密金鑰，例如 arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

類型：字串

LockDate

無法變更或刪除 AWS Backup 資料庫鎖定組態的日期和時間。

如果在未指定鎖定日期的情況下，將「Vault Lock 」套用至保存庫，則可隨時變更任何「Vault Lock 」設定，或從保存庫中完全刪除「Vault Lock 」。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

Locked

表示文件 AWS Backup 庫鎖定目前是否正在保護備份資料保險箱的布林值。 `True`表示「資料庫鎖定」會導致對儲存在資料保險箱中的復原點進行刪除或更新作業失敗。

類型：布林值

MaxRetentionDays

「文件 AWS Backup 庫鎖定」設定，用於指定文件庫保留其復原點的最長保留期間。若未指定此參數，Vault Lock 不會對保存庫中的復原點強制執行最長保留期間 (允許無限期儲存)。

若經過指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或短於最長保留期間。若任務的保留期間超過該最長保留期間，則文件庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的文件庫。在執行Vault Lock 之前已儲存於保存庫的復原點不會受到影響。

類型：Long

MinRetentionDays

「文件 AWS Backup 庫鎖定」設定，用於指定文件庫保留其復原點的最短保留期。若未指定此參數，則Vault Lock 不會強制執行最短保留期間。

若經過指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或超過最短保留期間。若任務的保留期間未達最短保留期間，則保存庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的保存庫。在執行Vault Lock 之前已儲存於保存庫的復原點不會受到影響。

類型：Long

NumberOfRecoveryPoints

儲存在備份保存庫中的復原點數目。

類型：Long

VaultType

這是所描述的保存庫類型。

類型：字串

有效值:BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeCopyJob

服務： AWS Backup

傳回與建立資源複本相關聯的中繼資料。

請求語法

```
GET /copy-jobs/copyJobId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

copyJobId

可唯一識別複製作業。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJob": {
      "AccountId": "string",
      "BackupSizeInBytes": number,
      "ChildJobsInState": {
         "string" : number
      },
      "CompletionDate": number,
      "CompositeMemberIdentifier": "string",
      "CopyJobId": "string",
      "CreatedBy": {
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanVersion": "string",
         "BackupRuleId": "string"
```

```
      },
      "CreationDate": number,
      "DestinationBackupVaultArn": "string",
      "DestinationRecoveryPointArn": "string",
      "IamRoleArn": "string",
      "IsParent": boolean,
      "MessageCategory": "string",
      "NumberOfChildJobs": number,
      "ParentJobId": "string",
      "ResourceArn": "string",
      "ResourceName": "string",
      "ResourceType": "string",
      "SourceBackupVaultArn": "string",
      "SourceRecoveryPointArn": "string",
      "State": "string",
      "StatusMessage": "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CopyJob

包含複製作業的相關詳細資訊。

類型：CopyJob 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeFramework

服務： AWS Backup

傳回指定 FrameworkName 的架構詳細資訊。

請求語法

```
GET /audit/frameworks/frameworkName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

frameworkName

架構的唯一名稱。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "DeploymentStatus": "string",
   "FrameworkArn": "string",
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
```

```
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "FrameworkName": "string",
   "FrameworkStatus": "string",
   "IdempotencyToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

架構建立時的日期和時間，採用 ISO 8601 表示法。CreationTime 的值精確到毫秒。舉例來說，2020-07-10T15:00:00.000-08:00 代表 2020 年 7 月 10 日下午 3 點，比國際標準時間晚 8 小時。

類型：Timestamp

DeploymentStatus

架構的部署狀態。狀態如下：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

類型：字串

FrameworkArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

FrameworkControls

組成架構的控制項清單。清單中的每個控制項都具有名稱、輸入參數和範圍。

類型：FrameworkControl 物件陣列

FrameworkDescription

架構的選擇性說明。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`.*\S.*`

FrameworkName

架構的唯一名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

FrameworkStatus

架構包含一或多個控制項。每個控制項皆控管一項資源，例如備份計畫、備份選擇、備份保存庫或復原點。您也可以開啟或關閉每個資源的 AWS Config 記錄功能。狀態如下：

- 當架構控管的所有資源皆開啟記錄時為 ACTIVE。
- 當架構控管的資源中至少一項關閉記錄時為 PARTIALLY_ACTIVE。
- 當架構控管的所有資源皆關閉記錄時為 INACTIVE。
- UNAVAILABLE此 AWS Backup 時無法驗證錄製狀態。

類型：字串

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 DescribeFrameworkOutput 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeGlobalSettings

服務： AWS Backup

說明 AWS 帳戶是否已選擇加入跨帳戶備份。如果帳戶不是 Organizations 組織的成員，則會傳回錯誤。範例：`describe-global-settings --region us-west-2`

請求語法

```
GET /global-settings HTTP/1.1
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   },
   "LastUpdateTime": number
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GlobalSettings

`isCrossAccountBackupEnabled` 標記的狀態。

類型：字串到字串映射

LastUpdateTime

上次更新 `isCrossAccountBackupEnabled` 標記時的日期和時間。此更新以 Unix 格式和國際標準時間 (UTC) 顯示。`LastUpdateTime` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

DescribeProtectedResource

服務： AWS Backup

傳回已儲存資源的相關資訊，包括上次備份資源的時間、Amazon 資源名稱 (ARN)，以及已儲存資源的 AWS 服務類型。

請求語法

```
GET /resources/resourceArn HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

resourceArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "LastBackupTime": number,
   "LastBackupVaultArn": "string",
   "LastRecoveryPointArn": "string",
   "LatestRestoreExecutionTimeMinutes": number,
   "LatestRestoreJobCreationDate": number,
   "LatestRestoreRecoveryPointCreationDate": number,
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

LastBackupTime

上次備份資源時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastBackupTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

LastBackupVaultArn

這是備份保存庫的 ARN (Amazon Resource Name)，此備份保存庫中包含最新的備份復原點。

類型：字串

LastRecoveryPointArn

這是最近復原點的 Amazon Resource Name (ARN)。

類型：字串

LatestRestoreExecutionTimeMinutes

這是最近一次完成還原任務所需的時間 (以分鐘為單位)。

類型：Long

LatestRestoreJobCreationDate

這是最近一次還原任務的建立日期。

類型：Timestamp

LatestRestoreRecoveryPointCreationDate

這是最近一次復原點的建立日期。

類型：Timestamp

ResourceArn

可唯一識別資源的 ARN。ARN 的格式取決於資源類型。

類型：字串

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

ResourceType

儲存為復原點的 AWS 資源類型；例如，Amazon EBS 磁碟區或 Amazon RDS 資料庫。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeRecoveryPoint

服務： AWS Backup

傳回與復原點相關聯的中繼資料，包括 ID、狀態、加密和生命週期。

請求語法

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

這是指定的備份保存庫的帳戶 ID。

模式：`^[0-9]{12}$`

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupSizeInBytes": number,
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "CompletionDate": number,
   "CompositeMemberIdentifier": "string",
   "CreatedBy": {
      "BackupPlanArn": "string",
      "BackupPlanId": "string",
      "BackupPlanVersion": "string",
      "BackupRuleId": "string"
   },
   "CreationDate": number,
   "EncryptionKeyArn": "string",
   "IamRoleArn": "string",
   "IsEncrypted": boolean,
   "IsParent": boolean,
   "LastRestoreTime": number,
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "ParentRecoveryPointArn": "string",
   "RecoveryPointArn": "string",
   "ResourceArn": "string",
   "ResourceName": "string",
   "ResourceType": "string",
   "SourceBackupVaultArn": "string",
   "Status": "string",
   "StatusMessage": "string",
   "StorageClass": "string",
   "VaultType": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupSizeInBytes

備份的大小，以位元組為單位。

類型：Long

BackupVaultArn

可唯一識別備份文件庫的 ARN，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

CalculatedLifecycle

包含 `DeleteAt` 和 `MoveToColdStorageAt` 時間戳記的 `CalculatedLifecycle` 物件。

類型：CalculatedLifecycle 物件

CompletionDate

建立復原點任務的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CompletionDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CompositeMemberIdentifier

這是複合群組內的資源識別符，例如屬於複合 (父項) 堆疊的巢狀 (子) 復原點。ID 會從堆疊中的邏輯 ID 傳輸。

類型：字串

CreatedBy

含有建立復原點的相關識別資訊，包括用於建立復原點之備份計畫的 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

類型：RecoveryPointCreator 物件

CreationDate

建立復原點的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

EncryptionKeyArn

用來保護備份的伺服器端加密金鑰，例如 arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

類型：字串

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN，例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

IsEncrypted

如果指定的復原點已加密，則傳回的布林值為 TRUE；如果復原點未加密，則為 FALSE。

類型：布林值

IsParent

這會傳回復原點為父項 (複合) 任務的布林值。

類型：布林值

LastRestoreTime

最後還原復原點的日期和時間，以 Unix 格式和國際標準時間 (UTC) 格式顯示。LastRestoreTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

Lifecycle

生命週期定義受保護的資源何時轉換為冷存儲以及何時到期。 AWS Backup 根據您定義的生命週期，自動轉換備份並過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天。因此，「保留期」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。 AWS Backup 會忽略其他資源類型的這個表示式。

類型：Lifecycle 物件

ParentRecoveryPointArn

可唯一識別父項 (複合) 復原點的 ARN，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

RecoveryPointArn

可唯一識別復原點的 ARN；例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

ResourceArn

可唯一識別已儲存資源的 ARN。ARN 的格式取決於資源類型。

類型：字串

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

ResourceType

要另存為復原點的 AWS 資源類型；例如，Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon Relational Database Service (Amazon RDS) 資料庫。

類型：String

模式：^[a-zA-Z0-9\-_\.]{1,50}$

SourceBackupVaultArn

可唯一識別原始備份資源之來源保存庫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:vault:BackupVault。如果恢復恢復到相同的 AWS 帳戶或區域，則此值將是null。

類型：字串

Status

指定復原點狀態的狀態碼。

PARTIAL狀態表示 AWS Backup 無法在備份視窗關閉之前建立復原點。若要使用 API 增加備份計劃時間，請參閱UpdateBackupPlan。您也可以使用主控台，透過選擇和編輯備份計畫來加長備份計畫時段。

EXPIRED狀態表示復原點已超過其保留期限，但 AWS Backup 缺少權限，或無法刪除它。若要手動刪除這些復原點，請參閱《入門》的《清理資源》一節中的《步驟 3：刪除復原點》。

STOPPED 狀態會出現在連續備份，其中使用者已採取某些動作，導致連續備份停用。這可能是因為移除權限、關閉版本控制、關閉要傳送至的事件 EventBridge，或停用由設定的 EventBridge 規則所造成 AWS Backup。

若要解決 STOPPED 狀態，請確定已具備所有必要許可，並且已在 S3 儲存貯體上啟用版本控制。一旦符合這些條件，下次執行備份規則就會建立新的連續復原點。不需要刪除狀態為「已停止」的復原點。

至於 Amazon EC2 上的 SAP HANA，STOPPED會因為使用者動作、應用程式設定錯誤或備份失敗而發生。為確保未來的連續備份成功，請查看復原點狀態並檢查 SAP HANA 以取得詳細資訊。

類型：字串

有效值:COMPLETED | PARTIAL | DELETING | EXPIRED

StatusMessage

說明還原復原點狀態的狀態訊息。

類型：字串

StorageClass

指定復原點的儲存體方案。有效值為 WARM 或 COLD。

類型：字串

有效值:WARM | COLD | DELETED

VaultType

這是存放所述復原點所用的保存庫類型。

類型：字串

有效值:BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeRegionSettings

服務： AWS Backup

傳回「區域」的目前服務選擇加入設定。如果服務已啟用選擇加入服務，當資源包含在隨需備份或排程備份計畫中時，AWS Backup 會嘗試保護該服務在此「區域」中的資源。否則，AWS Backup 不會嘗試保護此「區域」中該服務的資源。

請求語法

```
GET /account-settings HTTP/1.1
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceTypeManagementPreference

不論 AWS Backup 是否完整管理資源類型的備份，皆會傳回。

如需完整 AWS Backup 管理的優勢，請參閱完整 AWS Backup 管理。

如需資源類型的清單，以及每種資源類型是否支援完整 AWS Backup 管理，請參閱各資源的功能可用性表格。

如果為 `"DynamoDB":false`，則您可以透過啟用 AWS Backup 的進階 DynamoDB 備份功能，以啟用 DynamoDB 備份的完整 AWS Backup 管理功能。

類型：字串到布林值映射

金鑰模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

ResourceTypeOptInPreference

傳回「區域」中所有服務的清單，以及選擇加入偏好設定。

類型：字串到布林值映射

金鑰模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版

- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

DescribeReportJob

服務： AWS Backup

傳回與建立報表 (由其 ReportJobId 指定) 相關聯的詳細資訊。

請求語法

```
GET /audit/report-jobs/reportJobId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

reportJobId

報告任務的識別碼。唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。無法編輯報告任務 ID。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJob": {
      "CompletionTime": number,
      "CreationTime": number,
      "ReportDestination": {
         "S3BucketName": "string",
         "S3Keys": [ "string" ]
      },
      "ReportJobId": "string",
      "ReportPlanArn": "string",
      "ReportTemplate": "string",
      "Status": "string",
      "StatusMessage": "string"
```

```
    }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ReportJob

報告任務的相關資訊清單，包括其完成和建立時間、報告目的地、唯一的報告任務 ID、Amazon Resource Name (ARN)、報告範本、狀態和狀態訊息。

類型：ReportJob 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeReportPlan

服務： AWS Backup

傳回和的所有報表計劃清 AWS 帳戶 單 AWS 區域。

請求語法

```
GET /audit/report-plans/reportPlanName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

reportPlanName

報告計畫的唯一名稱。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportPlan": {
      "CreationTime": number,
      "DeploymentStatus": "string",
      "LastAttemptedExecutionTime": number,
      "LastSuccessfulExecutionTime": number,
      "ReportDeliveryChannel": {
         "Formats": [ "string" ],
         "S3BucketName": "string",
         "S3KeyPrefix": "string"
```

```
      },
      "ReportPlanArn": "string",
      "ReportPlanDescription": "string",
      "ReportPlanName": "string",
      "ReportSetting": {
         "Accounts": [ "string" ],
         "FrameworkArns": [ "string" ],
         "NumberOfFrameworks": number,
         "OrganizationUnits": [ "string" ],
         "Regions": [ "string" ],
         "ReportTemplate": "string"
      }
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ReportPlan

傳回由名稱所指定報表計畫的詳細資訊。這些詳細資訊包括報告計畫的 Amazon Resource Name (ARN)、描述、設定、交付管道、部署狀態、建立時間，以及上一次嘗試並成功執行的時間。

類型：ReportPlan 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DescribeRestoreJob

服務： AWS Backup

傳回與任務 ID 所指定還原任務相關聯的中繼資料。

請求語法

```
GET /restore-jobs/restoreJobId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

restoreJobId

可唯一識別還原復原點的任務。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AccountId": "string",
   "BackupSizeInBytes": number,
   "CompletionDate": number,
   "CreatedBy": {
      "RestoreTestingPlanArn": "string"
   },
   "CreatedResourceArn": "string",
   "CreationDate": number,
   "DeletionStatus": "string",
   "DeletionStatusMessage": "string",
   "ExpectedCompletionTimeMinutes": number,
   "IamRoleArn": "string",
```

```
    "PercentDone": "string",
    "RecoveryPointArn": "string",
    "RecoveryPointCreationDate": number,
    "ResourceType": "string",
    "RestoreJobId": "string",
    "Status": "string",
    "StatusMessage": "string",
    "ValidationStatus": "string",
    "ValidationStatusMessage": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AccountId

傳回擁有還原任務的帳戶 ID。

類型：String

模式：`^[0-9]{12}$`

BackupSizeInBytes

所還原資源的大小，以位元組為單位。

類型：Long

CompletionDate

還原復原點任務的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CompletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CreatedBy

包含有關建立還原任務的識別資訊。

類型：RestoreJobCreator 物件

CreatedResourceArn

可唯一識別正在還原復原點之資源的 Amazon Resource Name (ARN)。ARN 的格式取決於備份資源的資源類型。

類型：字串

CreationDate

建立還原任務時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

DeletionStatus

此會記錄還原測試所產生的資料狀態。此狀態可能是 Deleting、Failed 或 Successful。

類型：字串

有效值:DELETING | FAILED | SUCCESSFUL

DeletionStatusMessage

此會說明還原任務刪除狀態。

類型：字串

ExpectedCompletionTimeMinutes

還原復原點之任務預計所需的時間 (分鐘)。

類型：Long

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN；例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

PercentDone

包含查詢任務狀態時，任務的預估完成百分比。

類型：字串

RecoveryPointArn

可唯一識別復原點的 ARN；例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

RecoveryPointCreationDate

這是指定還原任務所建立之復原點的建立日期。

類型：Timestamp

ResourceType

傳回與依資源類型列出之還原任務相關聯的中繼資料。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

RestoreJobId

可唯一識別還原復原點的任務。

類型：字串

Status

狀態碼，指定還原復原點所 AWS Backup 起始之工作的狀態。

類型：字串

有效值:`PENDING | RUNNING | COMPLETED | ABORTED | FAILED`

StatusMessage

顯示還原復原點任務狀態的訊息。

類型：字串

ValidationStatus

這是在指定的還原任務上執行驗證的狀態。

類型：字串

有效值:`FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING`

ValidationStatusMessage

此描述了在指定的還原任務上執行驗證的狀態。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

DependencyFailureException

相依 AWS 服務或資源將錯誤傳回給 AWS Backup 服務，且動作無法完成。

HTTP 狀態碼：500

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DisassociateRecoveryPoint

服務： AWS Backup

從中刪除指定的連續備份復原點， AWS Backup 並釋放對來源服務 (例如 Amazon RDS) 的持續備份的控制權。來源服務將繼續使用您在原始備份計畫中指定的生命週期，以建立和保留連續備份。

不支援快照備份復原點。

請求語法

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/disassociate
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

AWS Backup 儲存庫的唯一名稱。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

可唯一識別 AWS Backup 復原點的 Amazon 資源名稱 (ARN)。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

InvalidResourceStateException

AWS Backup 已在此復原點上執行動作。在第一個動作完成之前，其無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

DisassociateRecoveryPointFromParent

服務： AWS Backup

此動作針對特定子 (巢狀) 復原點，會移除指定復原點與其父項 (複合) 復原點之間的關係。

請求語法

```
DELETE /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/
parentAssociation HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

這是儲存子 (巢狀) 復原點的邏輯容器名稱。Backup 儲存庫的名稱是用來建立儲存庫的帳戶以及建立備份儲存庫的 AWS 區域所屬的唯一名稱來識別。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

這是可唯一識別子 (巢狀) 復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45.`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ExportBackupPlanTemplate

服務： AWS Backup

傳回由計劃 ID 指定為備份範本的備份計劃。

請求語法

```
GET /backup/plans/backupPlanId/toTemplate/ HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanTemplateJson

JSON 格式的備份計劃範本本文。

> **Note**
>
> 這是已簽署的 JSON 文件，無法在傳遞至 `GetBackupPlanFromJSON`. 之前修改

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetBackupPlan

服務： AWS Backup

傳回指定 BackupPlanId 的 BackupPlan 詳細資訊。詳細資料是 JSON 格式的備份計畫內文，並包括計畫中繼資料。

請求語法

```
GET /backup/plans/backupPlanId/?versionId=VersionId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。版本 ID 不能編輯。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlan": {
      "AdvancedBackupSettings": [
```

```
        {
           "BackupOptions": {
              "string" : "string"
           },
           "ResourceType": "string"
        }
     ],
     "BackupPlanName": "string",
     "Rules": [
        {
           "CompletionWindowMinutes": number,
           "CopyActions": [
              {
                 "DestinationBackupVaultArn": "string",
                 "Lifecycle": {
                    "DeleteAfterDays": number,
                    "MoveToColdStorageAfterDays": number,
                    "OptInToArchiveForSupportedResources": boolean
                 }
              }
           ],
           "EnableContinuousBackup": boolean,
           "Lifecycle": {
              "DeleteAfterDays": number,
              "MoveToColdStorageAfterDays": number,
              "OptInToArchiveForSupportedResources": boolean
           },
           "RecoveryPointTags": {
              "string" : "string"
           },
           "RuleId": "string",
           "RuleName": "string",
           "ScheduleExpression": "string",
           "ScheduleExpressionTimezone": "string",
           "StartWindowMinutes": number,
           "TargetBackupVaultName": "string"
        }
     ]
  },
  "BackupPlanArn": "string",
  "BackupPlanId": "string",
  "CreationDate": number,
  "CreatorRequestId": "string",
  "DeletionDate": number,
```

```
    "LastExecutionDate": number,
    "VersionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AdvancedBackupSettings

包含每種資源類型的 BackupOptions 清單。只有在為備份計畫設定進階選項時，才會填入清單。

類型：AdvancedBackupSetting 物件陣列

BackupPlan

指定備份計畫的內文。包括一個 BackupPlanName 和一或多組 Rules。

類型：BackupPlan 物件

BackupPlanArn

可唯一識別備份計畫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

類型：字串

BackupPlanId

唯一識別備份計畫。

類型：字串

CreationDate

建立備份計畫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。

類型：字串

DeletionDate

刪除備份計畫時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。DeletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

LastExecutionDate

上次使用此備份計畫執行備份資源任務的時候。日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastExecutionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。版本 ID 不能編輯。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetBackupPlanFromJSON

服務： AWS Backup

傳回指定備份計劃或錯誤的有效 JSON 文件。

請求語法

```
POST /backup/template/json/toPlan HTTP/1.1
Content-type: application/json

{
   "BackupPlanTemplateJson": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

BackupPlanTemplateJson

客戶提供的 JSON 格式備份計劃文件。

類型：字串

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
```

```
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlan

指定備份計劃的本文。包括一個 BackupPlanName 和一或多組 Rules。

類型：BackupPlan 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面

- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetBackupPlanFromTemplate

服務： AWS Backup

傳回由其 templateId 指定為備份計劃的範本。

請求語法

```
GET /backup/template/plans/templateId/toPlan HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

templateId

可唯一識別儲存的備份計劃範本。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanDocument": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
```

```
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
            },
            "RuleId": "string",
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanDocument

根據目標範本傳回備份計劃的主文，包括計劃的名稱、規則和備份保存庫。

類型：BackupPlan 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetBackupSelection

服務： AWS Backup

傳回所選取中繼資料和 JSON 格式的文件，此文件會指定與備份計劃相關聯的資源清單。

請求語法

```
GET /backup/plans/backupPlanId/selections/selectionId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

selectionId

可唯一識別請求本文，將一組資源指派給備份計劃。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanId": "string",
   "BackupSelection": {
      "Conditions": {
         "StringEquals": [
            {
               "ConditionKey": "string",
```

```
                "ConditionValue": "string"
            }
         ],
         "StringLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotEquals": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ],
         "StringNotLike": [
            {
               "ConditionKey": "string",
               "ConditionValue": "string"
            }
         ]
      },
      "IamRoleArn": "string",
      "ListOfTags": [
         {
            "ConditionKey": "string",
            "ConditionType": "string",
            "ConditionValue": "string"
         }
      ],
      "NotResources": [ "string" ],
      "Resources": [ "string" ],
      "SelectionName": "string"
   },
   "CreationDate": number,
   "CreatorRequestId": "string",
   "SelectionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanId

唯一識別備份計畫。

類型：字串

BackupSelection

指定請求的內文，將一組資源指派給備份計畫。

類型：BackupSelection 物件

CreationDate

建立備份選擇時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。

類型：字串

SelectionId

可唯一識別請求本文，將一組資源指派給備份計劃。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetBackupVaultAccessPolicy

服務： AWS Backup

傳回與具名備份保存庫相關聯的存取政策文件。

請求語法

```
GET /backup-vaults/backupVaultName/access-policy HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultName": "string",
   "Policy": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

Policy

JSON 格式的備份保存庫存取政策文件。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetBackupVaultNotifications

服務： AWS Backup

傳回指定備份文件庫的事件通知。

請求語法

```
GET /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "BackupVaultEvents": [ "string" ],
   "BackupVaultName": "string",
   "SNSTopicArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

BackupVaultEvents

事件陣列，指示將資源備份到備份文件庫的任務狀態。

類型：字串陣列

有效值:`BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED`

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對用於建立文件庫的帳戶和區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

SNSTopicArn

唯一識別 Amazon Simple Notification Service (Amazon SNS) 主題的 ARN，例如，`arn:aws:sns:us-west-2:111122223333:MyTopic`。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetLegalHold

服務： AWS Backup

此動作會傳回指定法務保存的詳細資訊。詳細資料是 JSON 格式的法務保存內文，並包括中繼資料。

請求語法

```
GET /legal-holds/legalHoldId/ HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

legalHoldId

這是使用 GetLegalHold 的必要 ID。此唯一 ID 與指定法務保存相關聯。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CancelDescription": "string",
   "CancellationDate": number,
   "CreationDate": number,
   "Description": "string",
   "LegalHoldArn": "string",
   "LegalHoldId": "string",
   "RecoveryPointSelection": {
      "DateRange": {
         "FromDate": number,
         "ToDate": number
      },
      "ResourceIdentifiers": [ "string" ],
      "VaultNames": [ "string" ]
```

```
    },
    "RetainRecordUntil": number,
    "Status": "string",
    "Title": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CancelDescription

字串，描述移除法務保存的原因。

類型：字串

CancellationDate

取消法務保存時的時間 (以數字顯示)。

類型：Timestamp

CreationDate

建立法務保存時的時間 (以數字格式顯示)。

類型：Timestamp

Description

這是法務保存的傳回字串描述。

類型：字串

LegalHoldArn

這是指定法務保存的傳回架構 ARN。可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

LegalHoldId

這是與指定法務保存相關聯的傳回 ID。

類型：字串

RecoveryPointSelection

這指定了用於指派一組資源的條件，例如資源類型或備份保存庫。

類型：RecoveryPointSelection 物件

RetainRecordUntil

這是法務保存記錄保留結束時的日期和時間。

類型：Timestamp

Status

這是法務保存的狀態。狀態可以是 ACTIVE、CREATING、CANCELED 和 CANCELING。

類型：字串

有效值:CREATING | ACTIVE | CANCELING | CANCELED

Title

這是法務保存的字串標題。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRecoveryPointRestoreMetadata

服務： AWS Backup

傳回一組用於建立備份的中繼資料鍵值對。

請求語法

```
GET /backup-vaults/backupVaultName/recovery-points/recoveryPointArn/restore-metadata?
backupVaultAccountId=BackupVaultAccountId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

這是指定的備份保存庫的帳戶 ID。

模式：`^[0-9]{12}$`

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultArn": "string",
   "RecoveryPointArn": "string",
   "ResourceType": "string",
   "RestoreMetadata": {
      "string" : "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份保存庫的 ARN，例如 arn:aws:backup:us-east-1:123456789012:vault:aBackupVault。

類型：字串

RecoveryPointArn

可唯一識別復原點的 ARN；例如 arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

ResourceType

這是與復原點相關聯的資源類型。

類型：String

模式：^[a-zA-Z0-9\-_\.]{1,50}$

RestoreMetadata

描述備份資源原始配置的中繼資料鍵值對集。這些值會根據正在還原的服務而有所不同。

類型：字串到字串映射

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRestoreJobMetadata

服務： AWS Backup

此請求會傳回指定還原任務的中繼資料。

請求語法

```
GET /restore-jobs/restoreJobId/metadata HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

restoreJobId

這是其中還原工作的唯一識別碼 AWS Backup。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "Metadata": {
      "string" : "string"
   },
   "RestoreJobId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Metadata

其中包含指定備份任務的中繼資料。

類型：字串到字串映射

RestoreJobId

這是其中還原工作的唯一識別碼 AWS Backup。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRestoreTestingInferredMetadata

服務： AWS Backup

此請求會傳回一組精簡的必要中繼資料，使用安全預設設定開始還原任務會需要這些資料。BackupVaultName 和 RecoveryPointArn 是必要的參數。BackupVaultAccountId 是選用的參數。

請求語法

```
GET /restore-testing/inferred-metadata?
BackupVaultAccountId=BackupVaultAccountId&BackupVaultName=BackupVaultName&RecoveryPointArn=Reco
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

這是指定的備份保存庫的帳戶 ID。

BackupVaultName

存放備份的邏輯容器的名稱。Backup 儲存庫的名稱是用來建立儲存庫的帳戶以及建立備份儲存庫的 AWS區域所屬的唯一名稱來識別。這些名稱由字母、數字和連字號組成。

必要：是

RecoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "InferredMetadata": {
      "string" : "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

InferredMetadata

這是從請求推斷之中繼資料的字串映射。

類型：字串到字串映射

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRestoreTestingPlan

服務： AWS Backup

傳回指定 RestoreTestingPlanName 的 RestoreTestingPlan 詳細資訊。詳細資訊是 JSON 格式的還原測試計畫內文，並包括計畫中繼資料。

請求語法

```
GET /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

還原測試計畫的必要不重複名稱。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingPlan": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "LastExecutionTime": number,
      "LastUpdateTime": number,
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
```

```
        "RestoreTestingPlanArn": "string",
        "RestoreTestingPlanName": "string",
        "ScheduleExpression": "string",
        "ScheduleExpressionTimezone": "string",
        "StartWindowHours": number
    }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

RestoreTestingPlan

指定還原測試計畫的內文。包括 RestoreTestingPlanName。

類型：RestoreTestingPlanForGet 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetRestoreTestingSelection

服務： AWS Backup

返回 RestoreTestingSelection，顯示還原測試計劃的資源和元素。

請求語法

```
GET /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

還原測試計畫的必要不重複名稱。

必要：是

RestoreTestingSelectionName

還原測試選擇的必要不重複名稱。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "RestoreTestingSelection": {
      "CreationTime": number,
      "CreatorRequestId": "string",
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
```

```
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "ProtectedResourceType": "string",
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "RestoreTestingPlanName": "string",
      "RestoreTestingSelectionName": "string",
      "ValidationWindowHours": number
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

RestoreTestingSelection

還原測試選擇的不重複名稱。

類型：RestoreTestingSelectionForGet 物件

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

GetSupportedResourceTypes

服務： AWS Backup

返回支持的 AWS 資源類型 AWS Backup。

請求語法

```
GET /supported-resource-types HTTP/1.1
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ResourceTypes": [ "string" ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceTypes

包含具有支援資 AWS 源類型的字串：

- Aurora 代表 Amazon Aurora
- DynamoDB 代表 Amazon DynamoDB
- EBS 代表 Amazon Elastic Block Store
- EC2 代表 Amazon Elastic Compute Cloud
- EFS 代表 Amazon Elastic File System

- FSX 代表 Amazon FSx
- RDS 代表 Amazon Relational Database Service
- Storage Gateway 代表 Storage Gateway
- DocDB 代表 Amazon DocumentDB (with MongoDB compatibility)
- Neptune 代表 Amazon Neptune

類型：字串陣列

模式：^[a-zA-Z0-9\-_\.]{1,50}$

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupJobs

服務： AWS Backup

傳回過去 30 天內已驗證帳戶的現有備份任務清單。如需更長的時間，請考慮使用這些監視工具。

請求語法

```
GET /backup-jobs/?
accountId=ByAccountId&backupVaultName=ByBackupVaultName&completeAfter=ByCompleteAfter&completeB
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByAccountId

列出任務的帳戶 ID。僅傳回與特定帳戶 ID 相關聯的備份任務。

如果從 AWS Organizations 管理帳戶使用，則傳遞會傳*回整個組織中的所有工作。

模式：`^[0-9]{12}$`

ByBackupVaultName

僅傳回將儲存在特定備份保存庫中的備份任務。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

ByCompleteAfter

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之後完成的備份任務。

ByCompleteBefore

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之前完成的備份任務。

ByCreatedAfter

僅傳回特定日期之後建立的備份任務。

ByCreatedBefore

僅傳回特定日期之前建立的備份任務。

ByMessageCategory

這是可選參數，可用來篩選出符合您輸入值的工作。 MessageCategory

範例字串可能包括 `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL` 和 `InvalidParameters`。

檢視監控

萬用字元 (`*`) 會傳回所有訊息類別的計數。

`AGGREGATE_ALL` 彙總所有訊息類別的任務計數，並傳回總和。

ByParentJobId

這是根據父系任務 ID 列出子 (巢狀) 任務的篩選器。

ByResourceArn

僅傳回符合特定資源 Amazon Resource Name (ARN) 的備份任務。

ByResourceType

僅傳回指定資源的備份任務：

- `Aurora` 代表 Amazon Aurora
- `CloudFormation`對於 AWS CloudFormation
- `DocumentDB` 代表 Amazon DocumentDB (with MongoDB compatibility)
- `DynamoDB` 代表 Amazon DynamoDB
- `EBS` 代表 Amazon Elastic Block Store
- `EC2` 代表 Amazon Elastic Compute Cloud
- `EFS` 代表 Amazon Elastic File System
- `FSx` 代表 Amazon FSx
- `Neptune` 代表 Amazon Neptune
- `Redshift` 代表 Amazon Redshift
- `RDS` 代表 Amazon Relational Database Service
- 適用於 SAP HANA 資料庫的 `SAP HANA on Amazon EC2`
- `Storage Gateway`對於 AWS Storage Gateway
- 適用於 Amazon S3 的 `S3`
- `Timestream` 代表 Amazon Timestream

- VirtualMachine 代表虛擬機器

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByState

僅傳回處於特定狀態的備份任務。

Completed with issues 是僅在 AWS Backup 主控台中找到的狀態。對於 API，此狀態是指狀態為 COMPLETED 且值不是 SUCCESS 之 MessageCategory 的任務；也就是說，狀態為已完成，但出現狀態訊息。

若要取得 Completed with issues 的任務計數，請執行兩個 GET 請求，並減去第二個較小的數字：

GET /backup-jobs/?state=COMPLETED

GET /backup-jobs/?messageCategory=SUCCESS&state=COMPLETED

有效值:CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
```

```
   "BackupJobs": [
      {
         "AccountId": "string",
         "BackupJobId": "string",
         "BackupOptions": {
            "string" : "string"
         },
         "BackupSizeInBytes": number,
         "BackupType": "string",
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "BytesTransferred": number,
         "CompletionDate": number,
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "ExpectedCompletionDate": number,
         "IamRoleArn": "string",
         "InitiationDate": number,
         "IsParent": boolean,
         "MessageCategory": "string",
         "ParentJobId": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "StartBy": number,
         "State": "string",
         "StatusMessage": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupJobs

結構陣列，其中包含以 JSON 格式傳回的備份任務相關中繼資料。

類型：BackupJob 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的項目，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP

- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupJobSummaries

服務： AWS Backup

這是最近 30 天內建立或執行的備份任務摘要請求。您可以包括 AccountID、狀態、、ResourceType、、 MessageCategory AggregationPeriod MaxResults、或參數 NextToken 來篩選結果。

此要求會傳回包含內含工作的「區域」、「帳戶」 ResourceType MessageCategory、「州/省」StartTime EndTime、、和「計數」的摘要。

請求語法

```
GET /audit/backup-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccountId

傳回指定帳戶的任務計數。

如果要求是從成員帳戶或不屬於 Organ AWS izations 的帳戶傳送，則會傳回要求者帳戶內的工作。

根、管理員和委派管理員帳戶可以使用 ANY 值，傳回組織中每個帳戶的任務計數。

AGGREGATE_ALL 彙總已驗證組織內所有帳戶的任務計數，然後傳回總和。

模式：^[0-9]{12}$

AggregationPeriod

這是設定傳回結果界限的期間。

可接受的值包含

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。

- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

有效值:ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

此參數會設定要傳回的項目數量上限。

值是整數。可接受值的範圍是從 1 到 500。

有效範圍：最小值為 1。最大值為 1000。

MessageCategory

此參數會傳回指定訊息類別的任務計數。

接受的字串範例包括 AccessDenied、Success 和 InvalidParameters。如需接受 MessageCategory 字串的清單，請參閱監視。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的任務計數，並傳回總和。

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

ResourceType

傳回指定資源類型的任務計數。使用請求 GetSupportedResourceTypes 取得支援資源類型的字串。

該值 ANY 會傳回所有資源類型的計數。

AGGREGATE_ALL 彙總所有資源類型的任務計數，並傳回總和。

要備份的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此參數會傳回具有指定狀態之任務的任務計數。

該值 ANY 會傳回所有狀態的計數。

AGGREGATE_ALL 彙總所有狀態的任務計數，並傳回總和。

Completed with issues 是僅在 AWS Backup 主控台中找到的狀態。對於 API，此狀態是指狀態為 COMPLETED 且值不是 SUCCESS 之 MessageCategory 的任務；也就是說，狀態為已完成，但出現狀態訊息。若要取得 Completed with issues 的任務計數，請執行兩個 GET 請求，並減去第二個較小的數字：

獲取/審計/？backup-job-summaries AggregationPeriod= 十四天和狀態 = 已完成

獲取/審計/？backup-job-summaries AggregationPeriod= 十四天 = MessageCategory 成功和狀態 = 已完成

有效值:CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "BackupJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AggregationPeriod

這是設定傳回結果界限的期間。

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。
- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

類型：字串

BackupJobSummaries

此要求會傳回包含內含工作的「區域」、「帳戶」 ResourceType MessageCategory、「州/省」 StartTime EndTime、、和「計數」的摘要。

類型：BackupJobSummary 物件陣列

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupPlans

服務： AWS Backup

傳回已驗證帳戶之所有使用中備份計畫的清單。此清單包含 Amazon Resource Names (ARNs)、計畫 ID、建立和刪除日期、版本 ID、計畫名稱和建立者請求 ID 等資訊。

請求語法

```
GET /backup/plans/?
includeDeleted=IncludeDeleted&maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

IncludeDeleted

預設值為 FALSE 的布林值，當設為 TRUE 時，會傳回已刪除的備份計畫。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlansList": [
      {
```

```
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlansList

一系列備份計畫清單項目，其中包含已儲存備份計畫的中繼資料。

類型：BackupPlansListMember 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupPlanTemplates

服務： AWS Backup

傳回已儲存備份計劃範本的中繼資料，包括範本 ID、名稱，以及建立和刪除日期。

請求語法

```
GET /backup/template/plans?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanTemplatesList": [
      {
         "BackupPlanTemplateId": "string",
         "BackupPlanTemplateName": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanTemplatesList

一系列範本清單項目，其中包含已儲存範本的中繼資料。

類型：BackupPlanTemplatesListMember 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupPlanVersions

服務： AWS Backup

傳回備份計畫的版本中繼資料，包括 Amazon Resource Name (ARN)、備份計畫 ID、建立和刪除日期、計畫名稱和版本 ID。

請求語法

```
GET /backup/plans/backupPlanId/versions/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupPlanVersionsList": [
```

```
      {
         "AdvancedBackupSettings": [
            {
               "BackupOptions": {
                  "string" : "string"
               },
               "ResourceType": "string"
            }
         ],
         "BackupPlanArn": "string",
         "BackupPlanId": "string",
         "BackupPlanName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "DeletionDate": number,
         "LastExecutionDate": number,
         "VersionId": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupPlanVersionsList

包含備份計畫中繼資料的一系列版本清單項目。

類型：BackupPlansListMember 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupSelections

服務： AWS Backup

傳回包含與目標備份計劃相關聯之資源中繼資料的陣列。

請求語法

```
GET /backup/plans/backupPlanId/selections/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupSelectionsList": [
```

```
      {
         "BackupPlanId": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "IamRoleArn": "string",
         "SelectionId": "string",
         "SelectionName": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupSelectionsList

備份選擇清單項目的陣列，其中包含清單中每個資源的中繼資料。

類型：BackupSelectionsListMember 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListBackupVaults

服務： AWS Backup

傳回復原點儲存體容器的清單及其相關資訊。

請求語法

```
GET /backup-vaults/?
maxResults=MaxResults&nextToken=NextToken&shared=ByShared&vaultType=ByVaultType
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByShared

此參數將依共用保存庫，對保存庫清單進行排序。

ByVaultType

此參數將依保存庫類型，對保存庫清單進行排序。

有效值:BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "BackupVaultList": [
      {
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CreationDate": number,
         "CreatorRequestId": "string",
         "EncryptionKeyArn": "string",
         "LockDate": number,
         "Locked": boolean,
         "MaxRetentionDays": number,
         "MinRetentionDays": number,
         "NumberOfRecoveryPoints": number
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultList

一系列包含保存庫中繼資料的備份保存庫清單成員，包括 Amazon Resource Name (ARN)、顯示名稱、建立日期、儲存的復原點數量，以及加密資訊 (如果儲存在備份保存庫中的資源已加密)。

類型：BackupVaultListMember 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的項目，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListCopyJobs

服務： AWS Backup

傳回複製任務的相關中繼資料。

請求語法

```
GET /copy-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByAccountId

要列出任務的帳戶 ID。僅傳回與指定帳戶 ID 相關聯的複製任務。

模式：`^[0-9]{12}$`

ByCompleteAfter

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之後完成的複製任務。

ByCompleteBefore

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之前完成的複製任務。

ByCreatedAfter

僅傳回特定日期之後建立的複製任務。

ByCreatedBefore

僅傳回特定日期之前建立的複製任務。

ByDestinationVaultArn

可唯一識別要複製之來源備份保存庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

ByMessageCategory

這是一 MessageCategory 個可選參數，可用於篩選出符合您輸入值的工作。

範例字串可能包括 `AccessDenied`、`SUCCESS`、`AGGREGATE_ALL` 和 `INVALIDPARAMETERS`。

檢視監控以取得接受的字串清單。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的任務計數，並傳回總和。

ByParentJobId

這是根據父系任務 ID 列出子 (巢狀) 任務的篩選器。

ByResourceArn

僅傳回符合特定資源 Amazon Resource Name (ARN) 的複製任務。

ByResourceType

僅傳回指定資源的備份任務：

- Aurora 代表 Amazon Aurora
- CloudFormation對於 AWS CloudFormation
- DocumentDB 代表 Amazon DocumentDB (with MongoDB compatibility)
- DynamoDB 代表 Amazon DynamoDB
- EBS 代表 Amazon Elastic Block Store
- EC2 代表 Amazon Elastic Compute Cloud
- EFS 代表 Amazon Elastic File System
- FSx 代表 Amazon FSx
- Neptune 代表 Amazon Neptune
- Redshift 代表 Amazon Redshift
- RDS 代表 Amazon Relational Database Service
- 適用於 SAP HANA 資料庫的 SAP HANA on Amazon EC2
- Storage Gateway對於 AWS Storage Gateway
- 適用於 Amazon S3 的 S3
- Timestream 代表 Amazon Timestream
- VirtualMachine 代表虛擬機器

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByState

僅傳回處於指定狀態的複製任務。

有效值:CREATED | RUNNING | COMPLETED | FAILED | PARTIAL

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求返回項目 MaxResults 數量，則 NextToken 允許您從下一個令牌指向的位置開始返回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "ChildJobsInState": {
            "string" : number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CopyJobId": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "DestinationBackupVaultArn": "string",
         "DestinationRecoveryPointArn": "string",
         "IamRoleArn": "string",
         "IsParent": boolean,
```

```
            "MessageCategory": "string",
            "NumberOfChildJobs": number,
            "ParentJobId": "string",
            "ResourceArn": "string",
            "ResourceName": "string",
            "ResourceType": "string",
            "SourceBackupVaultArn": "string",
            "SourceRecoveryPointArn": "string",
            "State": "string",
            "StatusMessage": "string"
        }
    ],
    "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CopyJobs

結構陣列，其中包含以 JSON 格式傳回的複製任務相關中繼資料。

類型：CopyJob 物件陣列

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求返回項目 MaxResults 數量，則 NextToken 允許您從下一個令牌指向的位置開始返回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListCopyJobSummaries

服務： AWS Backup

此請求會取得最近 30 天內建立或執行的複製任務清單。您可以包括 AccountID、狀態、、ResourceType、、 MessageCategory AggregationPeriod MaxResults、或參數 NextToken 來篩選結果。

此要求會傳回包含內含工作的「區域」、「帳戶」 RestourceType MessageCategory、「州/省」StartTime EndTime、、和「計數」的摘要。

請求語法

```
GET /audit/copy-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&MessageCategory=M
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccountId

傳回指定帳戶的任務計數。

如果要求是從成員帳戶或不屬於 Organ AWS izations 的帳戶傳送，則會傳回要求者帳戶內的工作。

根、管理員和委派管理員帳戶可以使用 ANY 值，傳回組織中每個帳戶的任務計數。

AGGREGATE_ALL 彙總已驗證組織內所有帳戶的任務計數，然後傳回總和。

模式：^[0-9]{12}$

AggregationPeriod

這是設定傳回結果界限的期間。

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。
- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

有效值:ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

此參數會設定要傳回的項目數量上限。

值是整數。可接受值的範圍是從 1 到 500。

有效範圍：最小值為 1。最大值為 1000。

MessageCategory

此參數會傳回指定訊息類別的任務計數。

接受的字串範例包括 AccessDenied、Success 和 InvalidParameters。如需接受 MessageCategory 字串的清單，請參閱監視。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的任務計數，並傳回總和。

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

ResourceType

傳回指定資源類型的任務計數。使用請求 GetSupportedResourceTypes 取得支援資源類型的字串。

該值 ANY 會傳回所有資源類型的計數。

AGGREGATE_ALL 彙總所有資源類型的任務計數，並傳回總和。

要備份的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此參數會傳回具有指定狀態之任務的任務計數。

該值 ANY 會傳回所有狀態的計數。

AGGREGATE_ALL 彙總所有狀態的任務計數，並傳回總和。

有效值:CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AggregationPeriod": "string",
   "CopyJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "MessageCategory": "string",
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AggregationPeriod

這是設定傳回結果界限的期間。

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。
- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

類型：字串

CopyJobSummaries

此傳回會顯示包含內含工作的「區域」、「帳戶」 ResourceType、「州」 MessageCategory StartTime、「 EndTime、」和「計數」的摘要。

類型：CopyJobSummary 物件陣列

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的資源，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK

- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListFrameworks

服務： AWS Backup

傳回和的所有架構清 AWS 帳戶 單 AWS 區域。

請求語法

```
GET /audit/frameworks?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

從 1 到 1000 的期望結果數量。選用。如果未指定，查詢將傳回 1 MB 的資料。

有效範圍：最小值為 1。最大值為 1000。

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "Frameworks": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "FrameworkArn": "string",
         "FrameworkDescription": "string",
         "FrameworkName": "string",
         "NumberOfControls": number
      }
   ],
```

```
    "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Frameworks

含有每個架構詳細資訊的架構清單，包括架構名稱、Amazon Resource Name (ARN)、描述、控制項數目、建立時間和部署狀態。

類型：Framework 物件陣列

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面

- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListLegalHolds

服務： AWS Backup

此動作會傳回與作用中和先前法務保存有關的中繼資料。

請求語法

```
GET /legal-holds/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

要傳回的資源清單項目最大數量。

有效範圍：最小值為 1。最大值為 1000。

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "LegalHolds": [
      {
         "CancellationDate": number,
         "CreationDate": number,
         "Description": "string",
         "LegalHoldArn": "string",
         "LegalHoldId": "string",
         "Status": "string",
         "Title": "string"
```

```
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

LegalHolds

這是傳回的法務保存陣列，包括作用中和先前的法務保存。

類型：LegalHold 物件陣列

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListProtectedResources

服務： AWS Backup

傳回成功備份的資源陣列 AWS Backup，包括儲存資源的時間、資源的 Amazon 資源名稱 (ARN) 和資源類型。

請求語法

```
GET /resources/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
```

```
            "ResourceType": "string"
        }
    ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

Results

成功備份的資源陣列， AWS Backup 包括資源的儲存時間、資源的 Amazon 資源名稱 (ARN) 和資源類型。

類型：ProtectedResource 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListProtectedResourcesByBackupVault

服務： AWS Backup

此請求會列出與每個備份保存庫對應的受保護資源。

請求語法

```
GET /backup-vaults/backupVaultName/resources/?
backupVaultAccountId=BackupVaultAccountId&maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

這是您依帳戶 ID 指定之保存庫內備份保存庫所保護的資源清單。

模式：^[0-9]{12}$

backupVaultName

這是您依名稱指定之保存庫內備份保存庫所保護的資源清單。

模式：^[a-zA-Z0-9\-_]{2,50}$

必要：是

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "Results": [
      {
         "LastBackupTime": number,
         "LastBackupVaultArn": "string",
         "LastRecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

Results

這些是為請求返回的結果 ListProtectedResourcesByBackupVault。

類型：ProtectedResource 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRecoveryPointsByBackupVault

服務： AWS Backup

傳回儲存在備份保存庫之復原點的詳細資訊。

請求語法

```
GET /backup-vaults/backupVaultName/recovery-points/?
backupPlanId=ByBackupPlanId&backupVaultAccountId=BackupVaultAccountId&createdAfter=ByCreatedAft
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

BackupVaultAccountId

此參數會依帳戶 ID 排序復原點清單。

模式：`^[0-9]{12}$`

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

> **Note**
>
> 當受支援的服務建立備份時，備份保存庫名稱可能無法使用。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

ByBackupPlanId

僅傳回符合指定備份計畫 ID 的復原點。

ByCreatedAfter

僅傳回在指定時間戳記之後建立的復原點。

ByCreatedBefore

僅傳回在指定時間戳記之前建立的復原點。

ByParentRecoveryPointArn

這只會傳回符合指定父系 (複合) 復原點 Amazon Resource Name (ARN) 的復原點。

ByResourceArn

僅傳回符合指定資源 Amazon Resource Name (ARN) 的復原點。

ByResourceType

僅傳回符合指定資源類型的復原點：

- `Aurora` 代表 Amazon Aurora
- `CloudFormation`對於 AWS CloudFormation
- `DocumentDB` 代表 Amazon DocumentDB (with MongoDB compatibility)
- `DynamoDB` 代表 Amazon DynamoDB
- `EBS` 代表 Amazon Elastic Block Store
- `EC2` 代表 Amazon Elastic Compute Cloud
- `EFS` 代表 Amazon Elastic File System
- `FSx` 代表 Amazon FSx
- `Neptune` 代表 Amazon Neptune
- `Redshift` 代表 Amazon Redshift
- `RDS` 代表 Amazon Relational Database Service
- 適用於 SAP HANA 資料庫的 `SAP HANA on Amazon EC2`
- `Storage Gateway`對於 AWS Storage Gateway
- 適用於 Amazon S3 的 `S3`
- `Timestream` 代表 Amazon Timestream
- `VirtualMachine` 代表虛擬機器

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeInBytes": number,
         "BackupVaultArn": "string",
         "BackupVaultName": "string",
         "CalculatedLifecycle": {
            "DeleteAt": number,
            "MoveToColdStorageAt": number
         },
         "CompletionDate": number,
         "CompositeMemberIdentifier": "string",
         "CreatedBy": {
            "BackupPlanArn": "string",
            "BackupPlanId": "string",
            "BackupPlanVersion": "string",
            "BackupRuleId": "string"
         },
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IamRoleArn": "string",
         "IsEncrypted": boolean,
         "IsParent": boolean,
         "LastRestoreTime": number,
         "Lifecycle": {
            "DeleteAfterDays": number,
```

```
            "MoveToColdStorageAfterDays": number,
            "OptInToArchiveForSupportedResources": boolean
         },
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceName": "string",
         "ResourceType": "string",
         "SourceBackupVaultArn": "string",
         "Status": "string",
         "StatusMessage": "string",
         "VaultType": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

RecoveryPoints

物件陣列，其中包含儲存在備份保存庫之復原點的詳細資訊。

類型：RecoveryPointByBackupVault 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRecoveryPointsByLegalHold

服務： AWS Backup

此動作會傳回指定法務保存的復原點 ARN (Amazon Resource Names)。

請求語法

```
GET /legal-holds/legalHoldId/recovery-points?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

legalHoldId

這是法務保存的 ID。

必要：是

MaxResults

這是要傳回之資源列表項目的最大數量。

有效範圍：最小值為 1。最大值為 1000。

NextToken

這是所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的資源，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
```

```
   "RecoveryPoints": [
      {
         "BackupVaultName": "string",
         "RecoveryPointArn": "string",
         "ResourceArn": "string",
         "ResourceType": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

此傳回是所傳回資源部分清單之後的下一個項目。

類型：字串

RecoveryPoints

這是 ListRecoveryPointsByLegalHold 傳回的復原點清單。

類型：RecoveryPointMember 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRecoveryPointsByResource

服務： AWS Backup

傳回資源 Amazon Resource Name (ARN) 所指定類型之所有復原點的詳細資訊。

> **Note**
>
> 對於 Amazon EFS 和 Amazon EC2，此動作僅列出由 AWS Backup建立的復原點。

請求語法

```
GET /resources/resourceArn/recovery-points/?maxResults=MaxResults&nextToken=NextToken
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

> **Note**
>
> Amazon RDS 需要至少為 20 的值。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的項目，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

resourceArn

可唯一識別資源的 ARN。ARN 的格式取決於資源類型。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RecoveryPoints": [
      {
         "BackupSizeBytes": number,
         "BackupVaultName": "string",
         "CreationDate": number,
         "EncryptionKeyArn": "string",
         "IsParent": boolean,
         "ParentRecoveryPointArn": "string",
         "RecoveryPointArn": "string",
         "ResourceName": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

RecoveryPoints

物件陣列，其中包含指定資源類型之復原點的詳細資訊。

> **Note**
>
> 只有 Amazon EFS 和 Amazon EC2 恢復點返回 BackupVaultName。

類型：RecoveryPointByResource 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListReportJobs

服務： AWS Backup

傳回報告任務的相關詳細資訊。

請求語法

```
GET /audit/report-jobs?
CreationAfter=ByCreationAfter&CreationBefore=ByCreationBefore&MaxResults=MaxResults&NextToken=N
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByCreationAfter

僅傳回以 Unix 格式和國際標準時間 (UTC) 指定之日期和時間之後建立的報告任務。例如，值 1516925490 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30 秒。

ByCreationBefore

僅傳回以 Unix 格式和國際標準時間 (UTC) 指定之日期和時間之前建立的報告任務。例如，值 1516925490 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30 秒。

ByReportPlanName

僅傳回具有指定報表計畫名稱的報表任務。

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

ByStatus

僅傳回處於指定狀態的報告任務。狀態如下：

`CREATED | RUNNING | COMPLETED | FAILED`

MaxResults

從 1 到 1000 的期望結果數量。選用。如果未指定，查詢將傳回 1 MB 的資料。

有效範圍：最小值為 1。最大值為 1000。

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportJobs": [
      {
         "CompletionTime": number,
         "CreationTime": number,
         "ReportDestination": {
            "S3BucketName": "string",
            "S3Keys": [ "string" ]
         },
         "ReportJobId": "string",
         "ReportPlanArn": "string",
         "ReportTemplate": "string",
         "Status": "string",
         "StatusMessage": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

類型：字串

ReportJobs

JSON 格式報告任務的詳細資訊。

類型：ReportJob 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 V3 的 SDK

ListReportPlans

服務： AWS Backup

傳回報告計畫的清單。如需單一報告計畫的詳細資訊，請使用 DescribeReportPlan。

請求語法

```
GET /audit/report-plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

從 1 到 1000 的期望結果數量。選用。如果未指定，查詢將傳回 1 MB 的資料。

有效範圍：最小值為 1。最大值為 1000。

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "ReportPlans": [
      {
         "CreationTime": number,
         "DeploymentStatus": "string",
         "LastAttemptedExecutionTime": number,
         "LastSuccessfulExecutionTime": number,
         "ReportDeliveryChannel": {
            "Formats": [ "string" ],
            "S3BucketName": "string",
```

```
            "S3KeyPrefix": "string"
         },
         "ReportPlanArn": "string",
         "ReportPlanDescription": "string",
         "ReportPlanName": "string",
         "ReportSetting": {
            "Accounts": [ "string" ],
            "FrameworkArns": [ "string" ],
            "NumberOfFrameworks": number,
            "OrganizationUnits": [ "string" ],
            "Regions": [ "string" ],
            "ReportTemplate": "string"
         }
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

從上一次呼叫此操作傳回的識別符，可用來傳回清單中的下一組項目。

類型：字串

ReportPlans

您的報告計畫清單，其中包含每個計畫的詳細資訊。此資訊包括 Amazon Resource Name (ARN)、報告計畫名稱、描述、設定、交付管道、部署狀態、建立時間，以及報告計畫上一次嘗試並成功執行的時間。

類型：ReportPlan 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRestoreJobs

服務： AWS Backup

傳回 AWS Backup 起始還原已儲存資源的工作清單，包括復原程序的詳細資訊。

請求語法

```
GET /restore-jobs/?
accountId=ByAccountId&completeAfter=ByCompleteAfter&completeBefore=ByCompleteBefore&createdAfte
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByAccountId

列出任務的帳戶 ID。僅傳回與指定帳戶 ID 相關聯的還原任務。

模式：`^[0-9]{12}$`

ByCompleteAfter

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之後完成的複製任務。

ByCompleteBefore

僅傳回以 Unix 格式和國際標準時間 (UTC) 所表示日期之前完成的複製任務。

ByCreatedAfter

僅傳回在指定日期之後建立的還原任務。

ByCreatedBefore

僅傳回在指定日期之前建立的還原任務。

ByResourceType

包含此參數以僅傳回指定資源的還原任務：

- `Aurora` 代表 Amazon Aurora
- `CloudFormation`對於 AWS CloudFormation
- `DocumentDB` 代表 Amazon DocumentDB (with MongoDB compatibility)
- `DynamoDB` 代表 Amazon DynamoDB
- `EBS` 代表 Amazon Elastic Block Store

- EC2 代表 Amazon Elastic Compute Cloud
- EFS 代表 Amazon Elastic File System
- FSx 代表 Amazon FSx
- Neptune 代表 Amazon Neptune
- Redshift 代表 Amazon Redshift
- RDS 代表 Amazon Relational Database Service
- 適用於 SAP HANA 資料庫的 SAP HANA on Amazon EC2
- Storage Gateway對於 AWS Storage Gateway
- 適用於 Amazon S3 的 S3
- Timestream 代表 Amazon Timestream
- VirtualMachine 代表虛擬機器

模式：^[a-zA-Z0-9\-_\.]{1,50}$

ByRestoreTestingPlanArn

此項僅傳回符合指定資源 Amazon Resource Name (ARN) 的還原測試任務。

ByStatus

僅傳回與指定任務狀態相關聯的還原任務。

有效值:PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

RestoreJobs

物件陣列，其中包含還原所儲存資源之任務的詳細資訊。

類型：RestoreJobsListMember 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRestoreJobsByProtectedResource

服務： AWS Backup

這將傳回包含指定受保護資源的還原任務。

您必須包含 ResourceArn。您可以選擇性地包含 NextToken、ByStatus、MaxResults、ByRecoveryPointCreationDateAfter 和 ByRecoveryPointCreationDateBefore。

請求語法

```
GET /resources/resourceArn/restore-jobs/?
maxResults=MaxResults&nextToken=NextToken&recoveryPointCreationDateAfter=ByRecoveryPointCreatio
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

ByRecoveryPointCreationDateAfter

僅傳回在指定日期之後建立的復原點還原任務。

ByRecoveryPointCreationDateBefore

僅傳回在指定日期之前建立的復原點還原任務。

ByStatus

僅傳回與指定任務狀態相關聯的還原任務。

有效值:PENDING | RUNNING | COMPLETED | ABORTED | FAILED

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目。

resourceArn

僅傳回符合指定資源 Amazon Resource Name (ARN) 的還原任務。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreJobs": [
      {
         "AccountId": "string",
         "BackupSizeInBytes": number,
         "CompletionDate": number,
         "CreatedBy": {
            "RestoreTestingPlanArn": "string"
         },
         "CreatedResourceArn": "string",
         "CreationDate": number,
         "DeletionStatus": "string",
         "DeletionStatusMessage": "string",
         "ExpectedCompletionTimeMinutes": number,
         "IamRoleArn": "string",
         "PercentDone": "string",
         "RecoveryPointArn": "string",
         "RecoveryPointCreationDate": number,
         "ResourceType": "string",
         "RestoreJobId": "string",
         "Status": "string",
         "StatusMessage": "string",
         "ValidationStatus": "string",
         "ValidationStatusMessage": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目

類型：字串

RestoreJobs

物件陣列，其中包含還原所儲存資源之任務的詳細資訊。>

類型：RestoreJobsListMember 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRestoreJobSummaries

服務： AWS Backup

此請求會取得最近 30 天內建立或執行的還原任務摘要。您可以包括 AccountID、狀態、、ResourceType AggregationPeriod MaxResults、或參數 NextToken 來篩選結果。

此要求會傳回包含內含工作的「區域」、「帳戶」 RestourceType MessageCategory、「州/省」StartTime EndTime、、和「計數」的摘要。

請求語法

```
GET /audit/restore-job-summaries?
AccountId=AccountId&AggregationPeriod=AggregationPeriod&MaxResults=MaxResults&NextToken=NextTok
 HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

AccountId

傳回指定帳戶的任務計數。

如果要求是從成員帳戶或不屬於 Organ AWS izations 的帳戶傳送，則會傳回要求者帳戶內的工作。

根、管理員和委派管理員帳戶可以使用 ANY 值，傳回組織中每個帳戶的任務計數。

AGGREGATE_ALL 彙總已驗證組織內所有帳戶的任務計數，然後傳回總和。

模式：^[0-9]{12}$

AggregationPeriod

這是設定傳回結果界限的期間。

可接受的值包含

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。
- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

有效值:ONE_DAY | SEVEN_DAYS | FOURTEEN_DAYS

MaxResults

此參數會設定要傳回的項目數量上限。

值是整數。可接受值的範圍是從 1 到 500。

有效範圍：最小值為 1。最大值為 1000。

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

ResourceType

傳回指定資源類型的任務計數。使用請求 GetSupportedResourceTypes 取得支援資源類型的字串。

該值 ANY 會傳回所有資源類型的計數。

AGGREGATE_ALL 彙總所有資源類型的任務計數，並傳回總和。

要備份的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

模式：^[a-zA-Z0-9\-_\.]{1,50}$

State

此參數會傳回具有指定狀態之任務的任務計數。

該值 ANY 會傳回所有狀態的計數。

AGGREGATE_ALL 彙總所有狀態的任務計數，並傳回總和。

有效值:CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "AggregationPeriod": "string",
   "NextToken": "string",
   "RestoreJobSummaries": [
      {
         "AccountId": "string",
         "Count": number,
         "EndTime": number,
         "Region": "string",
         "ResourceType": "string",
         "StartTime": number,
         "State": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AggregationPeriod

這是設定傳回結果界限的期間。

- ONE_DAY 為前 14 天的每日任務計數。
- SEVEN_DAYS 為前 7 天的彙總任務計數。
- FOURTEEN_DAYS 為前 14 天的彙總任務計數。

類型：字串

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 MaxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

RestoreJobSummaries

此傳回包含包含工作的「區域」、「帳戶」 ResourceType、「州/省」 MessageCategory StartTime EndTime、「」和「計數」的摘要。

類型：RestoreJobSummary 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRestoreTestingPlans

服務： AWS Backup

傳回還原測試計畫的清單。

請求語法

```
GET /restore-testing/plans?MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目。

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
   "RestoreTestingPlans": [
      {
         "CreationTime": number,
         "LastExecutionTime": number,
         "LastUpdateTime": number,
         "RestoreTestingPlanArn": "string",
         "RestoreTestingPlanName": "string",
         "ScheduleExpression": "string",
```

```
            "ScheduleExpressionTimezone": "string",
            "StartWindowHours": number
        }
    ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目。

類型：字串

RestoreTestingPlans

這是還原測試計畫的傳回清單。

類型：RestoreTestingPlanForList 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListRestoreTestingSelections

服務： AWS Backup

傳回還原測試選擇的清單。可以使用 MaxResults 和 RestoreTestingPlanName 進行篩選。

請求語法

```
GET /restore-testing/plans/RestoreTestingPlanName/selections?
MaxResults=MaxResults&NextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目。

RestoreTestingPlanName

依指定的還原測試計畫名稱傳回還原測試選擇。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "NextToken": "string",
```

```
   "RestoreTestingSelections": [
      {
         "CreationTime": number,
         "IamRoleArn": "string",
         "ProtectedResourceType": "string",
         "RestoreTestingPlanName": "string",
         "RestoreTestingSelectionName": "string",
         "ValidationWindowHours": number
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回清單中的更多項目。

類型：字串

RestoreTestingSelections

傳回與還原測試計畫相關聯的還原測試選擇。

類型：RestoreTestingSelectionForList 物件陣列

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

ListTags

服務： AWS Backup

傳回指派給目標復原點、備份計畫或備份保存庫的鍵值對清單。

ListTags 僅適用於支援備份完整 AWS Backup 管理的資源類型。這些資源類型會列在「依資源分類的功能可用性」表格的「完整 AWS Backup 管理」區段中。

請求語法

```
GET /tags/resourceArn/?maxResults=MaxResults&nextToken=NextToken HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

MaxResults

所要傳回的項目數量上限。

有效範圍：最小值為 1。最大值為 1000。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

resourceArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。ListTags 的有效目標為復原點、備份計劃和備份保存庫。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
Content-type: application/json
```

```
{
   "NextToken": "string",
   "Tags": {
      "string" : "string"
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

傳回項目之部分列表後的下一個項目。例如，如果請求傳回 MaxResults 個數量的項目，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

Tags

為協助組織您的資源，您可以將自己的中繼資料指派給您建立的資源。每個標籤都是金鑰值對。

類型：字串到字串映射

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutBackupVaultAccessPolicy

服務： AWS Backup

設定以資源為基礎的政策，用於管理目標備份保存庫的存取許可。需要備份保存庫名稱和 JSON 格式的存取政策文件。

請求語法

```
PUT /backup-vaults/backupVaultName/access-policy HTTP/1.1
Content-type: application/json

{
   "Policy": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Policy

JSON 格式的備份保存庫存取政策文件。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutBackupVaultLockConfiguration

服務： AWS Backup

將文件 AWS Backup 庫鎖定套用至備份儲存庫，以防止嘗試刪除儲存在備份保存庫中或建立的任何復原點。Vault Lock 也可防止嘗試更新生命週期政策，該政策控制目前儲存在備份保存庫中的任意復原點的保留期間。如果已指定，Vault Lock 會對以備份保存庫為目標的未來備份和複製任務，強制執行最短和最長保留期。

> **Note**
>
> AWS Backup 文件庫鎖定已由科哈塞特關聯公司評估，可用於受 SEC 17a-4、CFTC 和 FINRA 法規規範的環境。如需文件 AWS Backup 庫鎖定如何與這些規則相關聯的詳細資訊，請參閱 Cohasset 關聯合規性評估。

請求語法

```
PUT /backup-vaults/backupVaultName/vault-lock HTTP/1.1
Content-type: application/json

{
   "ChangeableForDays": number,
   "MaxRetentionDays": number,
   "MinRetentionDays": number
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

資 AWS Backup 料庫鎖定組態，指定其保護之備份儲存庫的名稱。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

ChangeableForDays

「AWS Backup 資料庫鎖定」組態，指定鎖定日期前的天數。例如，若於 UTC 時間 2022 年 1 月 1 日將 `ChangeableForDays` 設定為 30，則會將鎖定日期設定為 UTC 時間 2022 年 1 月 31 日晚上 8 點。

AWS Backup 在文件庫鎖定生效並變為不可變之前，強制執行 72 小時的冷靜期。因此，您必須將 `ChangeableForDays` 設定為 3 或以上。

在鎖定日期之前，您可使用 `DeleteBackupVaultLockConfiguration` 從文件庫中刪除 Vault Lock，或使用 `PutBackupVaultLockConfiguration` 變更 Vault Lock 組態。在鎖定日期當天和其後，Vault Lock 會轉為不可變狀態，且無法變更或刪除。

若未指定此參數，您可隨時使用 `DeleteBackupVaultLockConfiguration` 從文件庫中刪除 Vault Lock，或使用 `PutBackupVaultLockConfiguration` 變更 Vault Lock 組態。

類型：Long

必要：否

MaxRetentionDays

資料保 AWS Backup 險箱鎖定組態，用於指定資料保險箱保留其復原點的最長保留期間。例如，若組織的政策要求您在保留某些資料四年 (1460 天) 後將其銷毀，此設定會很實用。

若未包含此參數，Vault Lock 不會對文件庫中的復原點強制執行最長保留期間。若包含此參數時沒有值，Vault Lock 將不會強制執行最長保留期間。

若指定此參數，則文件庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或短於最長保留期間。若任務的保留期間超過該最長保留期間，則文件庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的文件庫。您可以指定的最長保留期間為 36500 天 (約 100 年)。在執行 Vault Lock 之前已儲存於文件庫的復原點不會受到影響。

類型：Long

必要：否

MinRetentionDays

資料保 AWS Backup 險箱鎖定組態，用於指定資料保險箱保留其復原點的最短保留期間。例如，若組織的政策要求您保留某些資料至少七年 (2555 天)，此設定會很實用。

若未指定此參數，Vault Lock 將不會強制執行最短保留期間。

若指定此參數，則文件庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或超過最短保留期間。若任務的保留期間未達最短保留期間，則文件庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的文件庫。您可以指定的最短保留期間為 1 天。在執行 Vault Lock 之前已儲存於文件庫的復原點不會受到影響。

類型：Long

必要：否

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutBackupVaultNotifications

服務： AWS Backup

開啟指定主題與事件的備份保存庫通知。

請求語法

```
PUT /backup-vaults/backupVaultName/notification-configuration HTTP/1.1
Content-type: application/json

{
   "BackupVaultEvents": [ "string" ],
   "SNSTopicArn": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupVaultEvents

事件陣列，指示將資源備份到備份文件庫的任務狀態。

如需常見使用案例和程式碼範例，請參閱使用 Amazon SNS 追蹤 AWS Backup 事件。

支援的事件如下：

- BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED
- COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED

- RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RECOVERY_POINT_MODIFIED
- S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

> **Note**
>
> 下列清單顯示為已取代事件 (供參考) 且不再使用的項目。這些項目不再受到支援，也不會傳回狀態或通知。請參閱上面的列表以了解當前支援的事件。

類型：字串陣列

有效值:BACKUP_JOB_STARTED | BACKUP_JOB_COMPLETED | BACKUP_JOB_SUCCESSFUL | BACKUP_JOB_FAILED | BACKUP_JOB_EXPIRED | RESTORE_JOB_STARTED | RESTORE_JOB_COMPLETED | RESTORE_JOB_SUCCESSFUL | RESTORE_JOB_FAILED | COPY_JOB_STARTED | COPY_JOB_SUCCESSFUL | COPY_JOB_FAILED | RECOVERY_POINT_MODIFIED | BACKUP_PLAN_CREATED | BACKUP_PLAN_MODIFIED | S3_BACKUP_OBJECT_FAILED | S3_RESTORE_OBJECT_FAILED

必要：是

SNSTopicArn

可指定備份保存庫事件主題的 Amazon Resource Name (ARN)，例如 `arn:aws:sns:us-west-2:111122223333:MyVaultTopic`。

類型：字串

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

PutRestoreValidationResult

服務： AWS Backup

此請求可讓您傳送獨立自行執行還原測試驗證結果。RestoreJobId 和 ValidationStatus 是必要項目。您也可以選擇性地輸入 ValidationStatusMessage。

請求語法

```
PUT /restore-jobs/restoreJobId/validations HTTP/1.1
Content-type: application/json

{
   "ValidationStatus": "string",
   "ValidationStatusMessage": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

restoreJobId

這是其中還原工作的唯一識別碼 AWS Backup。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

ValidationStatus

這是還原驗證的狀態。

類型：字串

有效值:FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

必要：是

ValidationStatusMessage

這是選用的訊息字串，您可以輸入此字串以描述還原測試驗證的驗證狀態。

類型：字串

必要：否

回應語法

```
HTTP/1.1 204
```

回應元素

如果動作成功，則服務會送回具有空 HTTP 主體的 HTTP 204 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

StartBackupJob

服務： AWS Backup

啟動指定資源的隨需備份工作。

請求語法

```
PUT /backup-jobs HTTP/1.1
Content-type: application/json

{
   "BackupOptions": {
      "string" : "string"
   },
   "BackupVaultName": "string",
   "CompleteWindowMinutes": number,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointTags": {
      "string" : "string"
   },
   "ResourceArn": "string",
   "StartWindowMinutes": number
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

BackupOptions

指定所選資源的備份選項。此選項僅適用於 Windows 磁碟區陰影複製服務 (VSS) 備份作業。

有效值：設定為 "WindowsVSS":"enabled" 即可啟用 WindowsVSS 備份選項，並建立 Windows VSS 備份。設定為 "WindowsVSS""disabled" 即可建立一般備份。WindowsVSS 選項預設為停用。

類型：字串到字串映射

金鑰模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

BackupVaultName

存放備份的邏輯容器名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：字串

模式：^[a-zA-Z0-9\-_]{2,50}$

必要：是

CompleteWindowMinutes

一個分鐘值，成功啟動的備份必須在此期間完成，否則 AWS Backup 將取消工作。此值是選用的。此值會從排程備份的時間開始倒數。其不會為 StartWindowMinutes 增加額外的時間，也不會因為備份比排程晚開始而增加時間。

就像 StartWindowMinutes，這項參數的最大值為 100 年 (52,560,000 分鐘)。

類型：Long

必要：否

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN；例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：是

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 StartBackupJob 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

Lifecycle

生命週期會定義受保護的資源會在何時轉移至冷儲存以及會在何時過期。AWS Backup 會根據您定義的生命週期來自動轉移備份和使之過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留期」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷儲存的資源類型會列在「依資源分類的功能可用性」表格的「冷儲存生命週期」部分。AWS Backup 會忽略其他資源類型的這項運算式。

這項參數的最大值為 100 年 (36,500 天)。

類型：Lifecycle 物件

必要：否

RecoveryPointTags

為協助組織您的資源，您可以將自己的中繼資料指派給您建立的資源。每個標籤都是金鑰值對。

類型：字串到字串映射

必要：否

ResourceArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：是

StartWindowMinutes

從排程備份到取消任務 (如未成功啟動) 的分鐘值。此為選用值，預設為 8 小時。若包含此值，則其必須至少為 60 分鐘以避免發生錯誤。

此參數的最大值為 100 年 (52,560,000 分鐘)。

在啟動時段期間，備份工作狀態會保持在 CREATED 狀態，直到順利開始或啟動時段時間用完為止。如果 AWS Backup 在啟動時段內收到允許重試工作的錯誤訊息，則 AWS Backup 會自動至少每 10 分鐘重試開始工作，直到備份順利開始 (工作狀態會變更為 RUNNING) 或工作狀態變更為 EXPIRED 為止 (預期會在啟動時段時間結束時發生)。

類型：Long

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupJobId": "string",
   "CreationDate": number,
   "IsParent": boolean,
   "RecoveryPointArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupJobId

可唯一識別要 AWS Backup 備份資源的請求。

類型：字串

CreationDate

建立備份作業時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

IsParent

此為傳回的布林值，表示這是父系 (複合) 備份作業。

類型：布林值

RecoveryPointArn

附註：只有 Amazon EFS 和進階 DynamoDB 資源才會傳回此欄位。

可唯一識別復原點的 ARN；例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

StartCopyJob

服務： AWS Backup

啟動任務以建立指定資源的一次性複本。

不支援連續備份。

請求語法

```
PUT /copy-jobs HTTP/1.1
Content-type: application/json

{
   "DestinationBackupVaultArn": "string",
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
   "RecoveryPointArn": "string",
   "SourceBackupVaultName": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

DestinationBackupVaultArn

可唯一識別要複製之目的地備份保存庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：是

IamRoleArn

指定用於複製目標復原點的 IAM 角色 ARN；例如 `arn:aws:iam::123456789012:role/S3Access`。

類型：字串

必要：是

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 `StartCopyJob` 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

Lifecycle

包含 `Transition` 物件的陣列，指定復原點轉換成冷儲存或刪除前的天數。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，在主控台上，「保留」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。 AWS Backup 會忽略其他資源類型的這個表示式。

類型：Lifecycle 物件

必要：否

RecoveryPointArn

可唯一識別要用於複製任務之復原點的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

必要：是

SourceBackupVaultName

存放備份的邏輯來源容器名稱。Backup 儲存庫的名稱是用來建立儲存庫的帳戶以及建立備份儲存庫的 AWS 區域所屬的唯一名稱來識別。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：^[a-zA-Z0-9\-_]{2,50}$

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CopyJobId": "string",
   "CreationDate": number,
   "IsParent": boolean
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CopyJobId

可唯一識別複製作業。

類型：字串

CreationDate

建立複製作業時的日期和時間，以 Unix 時間格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

IsParent

這是一項傳回的布林值，表示這是一個父系 (複合) 複製任務。

類型：布林值

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

StartReportJob

服務： AWS Backup

啟動指定報告計劃的隨需報告任務。

請求語法

```
POST /audit/report-jobs/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

reportPlanName

報告計畫的唯一名稱。

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 `StartReportJobInput` 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "ReportJobId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ReportJobId

報告任務的識別符。唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。無法編輯報告任務 ID。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

StartRestoreJob

服務： AWS Backup

復原 Amazon Resource Name (ARN) 所識別的已儲存資源。

請求語法

```
PUT /restore-jobs HTTP/1.1
Content-type: application/json

{
   "CopySourceTagsToRestoredResource": boolean,
   "IamRoleArn": "string",
   "IdempotencyToken": "string",
   "Metadata": {
      "string" : "string"
   },
   "RecoveryPointArn": "string",
   "ResourceType": "string"
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

CopySourceTagsToRestoredResource

這是選擇性的參數。如果此參數等於 `True`，則備份中包含的標籤將複製到還原的資源。

此參數只能套用至透過 AWS Backup 建立的備份。

類型：布林值

必要：否

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)，AWS Backup 可用此角色來建立目標資源；例如：`arn:aws:iam::123456789012:role/S3Access`。

類型：字串

必要：否

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 StartRestoreJob 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

Metadata

一組中繼資料鍵值對。包含還原復原點所需的資訊，例如資源名稱。

您可以在備份資源時，透過呼叫 GetRecoveryPointRestoreMetadata 取得有關資源的組態中繼資料。不過，除了 GetRecoveryPointRestoreMetadata 提供的值之外，還可能需要還原資源。例如，如果原始資源已存在，您可能需要提供新資源名稱。

您需要指定特定中繼資料以還原 Amazon Elastic File System (Amazon EFS) 執行個體：

- file-system-id：AWS Backup 備份的 Amazon EFS 檔案系統之 ID。其會在 GetRecoveryPointRestoreMetadata 中傳回。
- Encrypted：此屬性為布林值；如果該值為 true，表示檔案系統已經過加密。如果已指定 KmsKeyId，則請務必將 Encrypted 設為 true。
- KmsKeyId：可指定用來加密所還原檔案系統的 AWS KMS 金鑰。您可以從另一個 AWS 帳戶指定金鑰，前提是該金鑰已透過 AWS KMS 與您的帳戶正確共用。
- PerformanceMode：可指定檔案系統的輸送量模式。
- CreationToken：此屬性是使用者提供的值，可確保請求的唯一性 (等冪性)。
- newFileSystem：此屬性為布林值；如果該值為 true，表示復原點會還原至新的 Amazon EFS 檔案系統。
- ItemsToRestore:由一到五個字串組成的陣列，其中每個字串都是檔案路徑。使用 ItemsToRestore 即可還原特定檔案或目錄，而不是整個檔案系統。此為選用參數。例如："itemsToRestore":"[\"/my.test\"]"。

類型：字串到字串映射

必要：是

RecoveryPointArn

唯一識別復原點的 ARN；例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

必要：是

ResourceType

請開始作業以還原下列其中一個資源的復原點：

- Aurora 代表 Amazon Aurora
- DocumentDB 代表 Amazon DocumentDB (with MongoDB compatibility)
- 適用於 AWS CloudFormation 的 CloudFormation
- DynamoDB 代表 Amazon DynamoDB
- EBS 代表 Amazon Elastic Block Store
- EC2 代表 Amazon Elastic Compute Cloud
- EFS 代表 Amazon Elastic File System
- FSx 代表 Amazon FSx
- Neptune 代表 Amazon Neptune
- RDS 代表 Amazon Relational Database Service
- Redshift 代表 Amazon Redshift
- 適用於 AWS Storage Gateway 的 Storage Gateway
- 適用於 Amazon S3 的 S3
- Timestream 代表 Amazon Timestream
- VirtualMachine 代表虛擬機器

類型：字串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

回應語法

```
HTTP/1.1 200
```

```
Content-type: application/json

{
   "RestoreJobId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

RestoreJobId

唯一識別還原復原點的作業。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

StopBackupJob

服務： AWS Backup

嘗試取消任務，以建立資源的一次性備份。

下列服務不支援此動作：FSx for Windows File Server 的 Amazon FSx、Amazon FSx for Lustre 用於 NetApp ONTAP)、Amazon FSX (適用於 OpenZF)、Amazon FSX、Amazon 文件資料庫 (與 MongoDB 相容性)、亞馬遜 RDS、Amazon Aurora 和 Amazon Neptune。

請求語法

```
POST /backup-jobs/backupJobId HTTP/1.1
```

URI 請求參數

請求會使用下列 URI 參數。

backupJobId

唯一識別 AWS Backup 要備份資源的請求。

必要：是

請求主體

請求沒有請求主體。

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

TagResource

服務： AWS Backup

將一組鍵值對指派給復原點、備份計劃或以 Amazon Resource Name (ARN) 識別的備份保存庫。

請求語法

```
POST /tags/resourceArn HTTP/1.1
Content-type: application/json

{
   "Tags": {
      "string" : "string"
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

resourceArn

可唯一識別資源的 ARN。ARN 的格式取決於標籤資源類型。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Tags

用於協助組織資源的鍵值對。您可以將自己的中繼資料指派給所建立的資源。為了清楚起見，下列是指派標籤的結構：`[{"Key":"string","Value":"string"}]`。

類型：字串到字串映射

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UntagResource

服務： AWS Backup

從透過 Amazon Resource Name (ARN) 識別的復原點、備份計劃或備份保存庫移除一組鍵值對

請求語法

```
POST /untag/resourceArn HTTP/1.1
Content-type: application/json

{
   "TagKeyList": [ "string" ]
}
```

URI 請求參數

請求會使用下列 URI 參數。

resourceArn

可唯一識別資源的 ARN。ARN 的格式取決於標籤資源類型。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

TagKeyList

用於識別要從資源中移除哪些索引鍵值標籤的金鑰清單。

類型：字串陣列

必要：是

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK

- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateBackupPlan

服務： AWS Backup

更新由其 backupPlanId 與 JSON 格式的輸入文件所識別的現有備份計劃。新版本可由 VersionId 唯一識別。

請求語法

```
POST /backup/plans/backupPlanId HTTP/1.1
Content-type: application/json

{
   "BackupPlan": {
      "AdvancedBackupSettings": [
         {
            "BackupOptions": {
               "string" : "string"
            },
            "ResourceType": "string"
         }
      ],
      "BackupPlanName": "string",
      "Rules": [
         {
            "CompletionWindowMinutes": number,
            "CopyActions": [
               {
                  "DestinationBackupVaultArn": "string",
                  "Lifecycle": {
                     "DeleteAfterDays": number,
                     "MoveToColdStorageAfterDays": number,
                     "OptInToArchiveForSupportedResources": boolean
                  }
               }
            ],
            "EnableContinuousBackup": boolean,
            "Lifecycle": {
               "DeleteAfterDays": number,
               "MoveToColdStorageAfterDays": number,
               "OptInToArchiveForSupportedResources": boolean
            },
            "RecoveryPointTags": {
               "string" : "string"
```

```
            },
            "RuleName": "string",
            "ScheduleExpression": "string",
            "ScheduleExpressionTimezone": "string",
            "StartWindowMinutes": number,
            "TargetBackupVaultName": "string"
         }
      ]
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupPlanId

唯一識別備份計畫。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

BackupPlan

指定備份計畫的本文。包括一個 BackupPlanName 和一或多組 Rules。

類型：BackupPlanInput 物件

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "AdvancedBackupSettings": [
      {
```

```
         "BackupOptions": {
            "string" : "string"
         },
         "ResourceType": "string"
      }
   ],
   "BackupPlanArn": "string",
   "BackupPlanId": "string",
   "CreationDate": number,
   "VersionId": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

AdvancedBackupSettings

包含每種資源類型的 BackupOptions 清單。

類型：AdvancedBackupSetting 物件陣列

BackupPlanArn

可唯一識別備份計畫的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50。

類型：字串

BackupPlanId

唯一識別備份計畫。

類型：字串

CreationDate

建立備份計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。版本 ID 不能編輯。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateFramework

服務： AWS Backup

更新由其 FrameworkName 與 JSON 格式的輸入文件所識別的現有架構。

請求語法

```
PUT /audit/frameworks/frameworkName HTTP/1.1
Content-type: application/json

{
   "FrameworkControls": [
      {
         "ControlInputParameters": [
            {
               "ParameterName": "string",
               "ParameterValue": "string"
            }
         ],
         "ControlName": "string",
         "ControlScope": {
            "ComplianceResourceIds": [ "string" ],
            "ComplianceResourceTypes": [ "string" ],
            "Tags": {
               "string" : "string"
            }
         }
      }
   ],
   "FrameworkDescription": "string",
   "IdempotencyToken": "string"
}
```

URI 請求參數

請求會使用下列 URI 參數。

frameworkName

架構的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，且開頭要為英文字母，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

FrameworkControls

組成架構的控制項清單。清單中的每個控制項都具有名稱、輸入參數和範圍。

類型：FrameworkControl 物件陣列

必要：否

FrameworkDescription

架構的選用描述，最多包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：.*\S.*

必要：否

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 UpdateFrameworkInput 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
```

```
    "CreationTime": number,
    "FrameworkArn": "string",
    "FrameworkName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

架構建立時的日期和時間，採用 ISO 8601 表示法。CreationTime 的值精確到毫秒。舉例來說，2020-07-10T15:00:00.000-08:00 代表 2020 年 7 月 10 日下午 3 點，比國際標準時間晚 8 小時。

類型：Timestamp

FrameworkArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

FrameworkName

架構的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，且開頭要為英文字母，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

AlreadyExistsException

所需資源已存在。

HTTP 狀態碼：400

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

LimitExceededException

請求已超過限制；例如，請求中允許的最大項目數量。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++

- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateGlobalSettings

服務： AWS Backup

更新 AWS 帳戶是否選擇加入跨帳戶備份的資訊。如果帳戶不是「Organizations」管理帳戶，則傳回錯誤。使用 DescribeGlobalSettings API 判斷目前的設定。

請求語法

```
PUT /global-settings HTTP/1.1
Content-type: application/json

{
   "GlobalSettings": {
      "string" : "string"
   }
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

GlobalSettings

isCrossAccountBackupEnabled 和一個區域的值。範例：update-global-settings --global-settings isCrossAccountBackupEnabled=false --region us-west-2。

類型：字串到字串映射

必要：否

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UpdateRecoveryPointLifecycle

服務： AWS Backup

設定復原點的轉移生命週期。

生命週期定義受保護的資源何時轉換為冷存儲以及何時到期。 AWS Backup 根據您定義的生命週期，自動轉換備份並過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。AWS Backup 會忽略其他資源類型的這個表示式。

此操作不支援連續備份。

請求語法

```
POST /backup-vaults/backupVaultName/recovery-points/recoveryPointArn HTTP/1.1
Content-type: application/json

{
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

backupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

recoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

Lifecycle

生命週期定義受保護的資源何時轉換為冷存儲以及何時到期。 AWS Backup 根據您定義的生命週期，自動轉換備份並過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

類型：Lifecycle 物件

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "BackupVaultArn": "string",
   "CalculatedLifecycle": {
      "DeleteAt": number,
      "MoveToColdStorageAt": number
   },
   "Lifecycle": {
      "DeleteAfterDays": number,
      "MoveToColdStorageAfterDays": number,
      "OptInToArchiveForSupportedResources": boolean
   },
```

```
   "RecoveryPointArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BackupVaultArn

可唯一識別備份保存庫的 ARN，例如 arn:aws:backup:us-east-1:123456789012:vault:aBackupVault。

類型：字串

CalculatedLifecycle

包含 DeleteAt 和 MoveToColdStorageAt 時間戳記的 CalculatedLifecycle 物件。

類型：CalculatedLifecycle 物件

Lifecycle

生命週期定義受保護的資源何時轉換為冷存儲以及何時到期。 AWS Backup 根據您定義的生命週期，自動轉換備份並過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。 AWS Backup 會忽略其他資源類型的這個表示式。

類型：Lifecycle 物件

RecoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

InvalidRequestException

表示請求的輸入出現問題。例如，參數的類型錯誤。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateRegionSettings

服務： AWS Backup

更新「區域」的目前服務選擇加入設定。

使用 DescribeRegionSettings API 來判斷支援的資源類型。

請求語法

```
PUT /account-settings HTTP/1.1
Content-type: application/json

{
   "ResourceTypeManagementPreference": {
      "string" : boolean
   },
   "ResourceTypeOptInPreference": {
      "string" : boolean
   }
}
```

URI 請求參數

請求不會使用任何 URI 參數。

請求主體

請求接受採用 JSON 格式的下列資料。

ResourceTypeManagementPreference

啟用或停用資源類型備份的完整 AWS Backup 管理。若要啟用 DynamoDB 的完整 AWS Backup 管理及 AWS Backup 的進階 DynamoDB 備份功能，請遵循以程式設計方式啟用進階 Dynam oDB 備份的程序。

類型：字串到布林值映射

金鑰模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

ResourceTypeOptInPreference

更新服務清單及「區域」的選擇加入偏好設定。

如果資源指派僅以標籤為基礎，則會套用選擇加入服務設定。如果將資源類型明確指派給備份計畫 (例如 Amazon S3、Amazon EC2 或 Amazon RDS)，即使該特定服務未啟用選擇加入，該資源類型也會包含在備份中。如果在資源指派中同時指定了資源類型和標籤，則備份計畫中指定的資源類型將優先於標籤條件。在此情況下，會忽略選擇加入服務設定。

類型：字串到布林值映射

金鑰模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

回應語法

```
HTTP/1.1 200
```

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

InvalidParameterValueException

表示參數的值出現問題。例如，該值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UpdateReportPlan

服務： AWS Backup

使用 JSON 格式的輸入文件，更新由其 ReportPlanName 所識別的現有報表計劃。

請求語法

```
PUT /audit/report-plans/reportPlanName HTTP/1.1
Content-type: application/json

{
   "IdempotencyToken": "string",
   "ReportDeliveryChannel": {
      "Formats": [ "string" ],
      "S3BucketName": "string",
      "S3KeyPrefix": "string"
   },
   "ReportPlanDescription": "string",
   "ReportSetting": {
      "Accounts": [ "string" ],
      "FrameworkArns": [ "string" ],
      "NumberOfFrameworks": number,
      "OrganizationUnits": [ "string" ],
      "Regions": [ "string" ],
      "ReportTemplate": "string"
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

reportPlanName

報告計畫的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，且開頭要為英文字母，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

IdempotencyToken

客戶所選擇的字串，可用來區分在其他方面相同的 UpdateReportPlanInput 呼叫。重試具有相同等冪性字符的成功請求會導致出現成功消息，但未執行任何動作。

類型：字串

必要：否

ReportDeliveryChannel

包含有關在何處交付報告的架構，特別是 Amazon S3 儲存貯體名稱、S3 金鑰字首以及報告格式。

類型：ReportDeliveryChannel 物件

必要：否

ReportPlanDescription

報告計劃的選用描述，最多可包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：.*\S.*

必要：否

ReportSetting

識別報告的報告範本。使用報告範本建立的報告。報告範本包括：

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

如果報告模板是RESOURCE_COMPLIANCE_REPORT或CONTROL_COMPLIANCE_REPORT，則此 API 資源還通過 AWS 區域 和框架描述報告覆蓋範圍。

類型：ReportSetting 物件

必要：否

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "ReportPlanArn": "string",
   "ReportPlanName": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

建立報告計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

ReportPlanArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

ReportPlanName

報告計畫的唯一名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：[a-zA-Z][_a-zA-Z0-9]*

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK

- AWS 適用於紅寶石 V3 的 SDK

UpdateRestoreTestingPlan

服務： AWS Backup

此請求會將變更傳送至指定的還原測試計畫。RestoreTestingPlanName 建立後就無法更新。

RecoveryPointSelection 可能包含：

- Algorithm
- ExcludeVaults
- IncludeVaults
- RecoveryPointTypes
- SelectionWindowDays

請求語法

```
PUT /restore-testing/plans/RestoreTestingPlanName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingPlan": {
      "RecoveryPointSelection": {
         "Algorithm": "string",
         "ExcludeVaults": [ "string" ],
         "IncludeVaults": [ "string" ],
         "RecoveryPointTypes": [ "string" ],
         "SelectionWindowDays": number
      },
      "ScheduleExpression": "string",
      "ScheduleExpressionTimezone": "string",
      "StartWindowHours": number
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

這是您要更新的還原測試計畫名稱。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

RestoreTestingPlan

指定還原測試計畫的內文。

類型：RestoreTestingPlanForUpdate 物件

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "UpdateTime": number
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

這是資源測試計畫的建立時間。

類型：Timestamp

RestoreTestingPlanArn

還原測試計畫的不重複 ARN (Amazon Resource Name)。

類型：字串

RestoreTestingPlanName

此名稱建立後就不可變更。此名稱僅包含英數字元和底線。長度上限為 50。

類型：字串

UpdateTime

這是針對還原測試計畫完成更新的時間。

類型：Timestamp

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

UpdateRestoreTestingSelection

服務： AWS Backup

您可以使用此請求更新 RestoreTestingSelectionName 以外的大多數元素。

RestoreTestingSelection 可以使用受保護的資源 ARN 或條件，但不能同時使用兩者。也就是說，如果您選擇 ProtectedResourceArns，就無法順利使用參數 ProtectedResourceConditions 請求更新。

請求語法

```
PUT /restore-testing/plans/RestoreTestingPlanName/
selections/RestoreTestingSelectionName HTTP/1.1
Content-type: application/json

{
   "RestoreTestingSelection": {
      "IamRoleArn": "string",
      "ProtectedResourceArns": [ "string" ],
      "ProtectedResourceConditions": {
         "StringEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ],
         "StringNotEquals": [
            {
               "Key": "string",
               "Value": "string"
            }
         ]
      },
      "RestoreMetadataOverrides": {
         "string" : "string"
      },
      "ValidationWindowHours": number
   }
}
```

URI 請求參數

請求會使用下列 URI 參數。

RestoreTestingPlanName

需要還原測試計畫名稱，才能更新指定的測試計畫。

必要：是

RestoreTestingSelectionName

這是您要更新的還原測試選擇的必要還原測試選擇名稱。

必要：是

請求主體

請求接受採用 JSON 格式的下列資料。

RestoreTestingSelection

若要更新還原測試選擇，您可以使用受保護的資源 ARN 或條件，但不能同時使用兩者。也就是說，如果您選擇 ProtectedResourceArns，就無法順利使用參數 ProtectedResourceConditions 請求更新。

類型：RestoreTestingSelectionForUpdate 物件

必要：是

回應語法

```
HTTP/1.1 200
Content-type: application/json

{
   "CreationTime": number,
   "RestoreTestingPlanArn": "string",
   "RestoreTestingPlanName": "string",
   "RestoreTestingSelectionName": "string",
   "UpdateTime": number
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

CreationTime

這是資源測試選擇成功更新的時間。

類型：Timestamp

RestoreTestingPlanArn

不重複字串，也就是還原測試計畫的名稱。

類型：字串

RestoreTestingPlanName

這是與更新的還原測試選擇相關聯的還原測試計畫。

類型：字串

RestoreTestingSelectionName

這是傳回的還原測試選擇名稱。

類型：字串

UpdateTime

這是針對還原測試選擇完成更新的時間。

類型：Timestamp

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

AWS Backup 在完成上一個動作之前，無法執行您要求的動作。請稍後再試。

HTTP 狀態碼：400

InvalidParameterValueException

表示參數的值出現問題。例如，值超出範圍。

HTTP 狀態碼：400

MissingParameterValueException

表示缺少必要的參數。

HTTP 狀態碼：400

ResourceNotFoundException

動作所需的資源不存在。

HTTP 狀態碼：400

ServiceUnavailableException

由於伺服器發生臨時故障，請求失敗。

HTTP 狀態碼：500

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS 命令列介面
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於 JavaScript V3 的 SDK
- AWS SDK for PHP
- AWS 適用於 Python 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

AWS Backup gateway

AWS Backup gateway 支援下列動作：

- AssociateGatewayToServer
- CreateGateway
- DeleteGateway

- DeleteHypervisor
- DisassociateGatewayFromServer
- GetBandwidthRateLimitSchedule
- GetGateway
- GetHypervisor
- GetHypervisorPropertyMappings
- GetVirtualMachine
- ImportHypervisorConfiguration
- ListGateways
- ListHypervisors
- ListTagsForResource
- ListVirtualMachines
- PutBandwidthRateLimitSchedule
- PutHypervisorPropertyMappings
- PutMaintenanceStartTime
- StartVirtualMachinesMetadataSync
- TagResource
- TestHypervisorConfiguration
- UntagResource
- UpdateGatewayInformation
- UpdateGatewaySoftwareNow
- UpdateHypervisor

AssociateGatewayToServer

服務： AWS Backup gateway

將備份閘道與您的伺服器建立關聯。完成關聯程序後，您可以透過閘道備份和還原虛擬機器。

請求語法

```
{
   "GatewayArn": "string",
   "ServerArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 `ListGateways` 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

ServerArn

託管虛擬機器之伺服器的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

CreateGateway

服務： AWS Backup gateway

建立備份閘道。在建立閘道後，您可以使用 AssociateGatewayToServer 操作將其與伺服器建立關聯。

請求語法

```
{
   "ActivationKey": "string",
   "GatewayDisplayName": "string",
   "GatewayType": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ActivationKey

所建立閘道的啟用金鑰。

類型：字串

長度限制：長度下限為 1。長度上限為 50。

模式：^[0-9a-zA-Z\-]+$

必要：是

GatewayDisplayName

所建立閘道的顯示名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[a-zA-Z0-9-]*$

必要：是

GatewayType

所建立閘道的類型。

類型：字串

有效值:BACKUP_VM

必要：是

Tags

可將最多 50 個標籤指派給閘道的清單。每個標籤都是金鑰值對。

類型：Tag 物件陣列

必要：否

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

所建立閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

DeleteGateway

服務： AWS Backup gateway

刪除備份閘道。

請求語法

```
{
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

要刪除之閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

已刪除之閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面

- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

DeleteHypervisor

服務： AWS Backup gateway

刪除 hypervisor。

請求語法

```
{
   "HypervisorArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

要刪除之 hypervisor 的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "HypervisorArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

您刪除之 hypervisor 的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

因為您的許可不足，所以操作無法繼續。

HTTP 狀態碼：400

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

DisassociateGatewayFromServer

服務： AWS Backup gateway

將備份閘道與指定的伺服器取消關聯。取消關聯程序完成後，閘道將無法再存取伺服器上的虛擬機器。

請求語法

```
{
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

要取消關聯之閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

已取消關聯的閘道 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetBandwidthRateLimitSchedule

服務： AWS Backup gateway

擷取指定閘道的頻寬速率限制排程。根據預設，閘道沒有頻寬速率限制排程，這表示頻寬速率限制未生效。使用此項目即可取得閘道的頻寬速率限制排程。

請求語法

```
{
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 ListGateways 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

必要：是

回應語法

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
```

```
            "StartHourOfDay": number,
            "StartMinuteOfHour": number
        }
    ],
    "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

BandwidthRateLimitIntervals

陣列，其中包含閘道的頻寬速率限制排程間隔。未排程頻寬速率限制間隔時，陣列為空。

類型：BandwidthRateLimitInterval 物件陣列

陣列成員：項目數下限為 0。項目數上限為 20。

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 ListGateways 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetGateway

服務： AWS Backup gateway

可透過提供 ARN (Amazon Resource Name) 將此 API 傳回閘道。

請求語法

```
{
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "Gateway": {
      "GatewayArn": "string",
      "GatewayDisplayName": "string",
      "GatewayType": "string",
      "HypervisorId": "string",
      "LastSeenTime": number,
      "MaintenanceStartTime": {
         "DayOfMonth": number,
         "DayOfWeek": number,
```

```
            "HourOfDay": number,
            "MinuteOfHour": number
        },
        "NextUpdateAvailabilityTime": number,
        "VpcEndpoint": "string"
    }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Gateway

可透過提供 ARN (Amazon Resource Name) 將此 API 傳回閘道。

類型：GatewayDetails 物件

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetHypervisor

服務： AWS Backup gateway

此動作會要求閘道將連線之指定 Hypervisor 的相關資訊。Hypervisor 是一種硬體、軟體或韌體，可建立並管理虛擬機器，並將資源配置給虛擬機器。

請求語法

```
{
   "HypervisorArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "Hypervisor": {
      "Host": "string",
      "HypervisorArn": "string",
      "KmsKeyArn": "string",
      "LastSuccessfulMetadataSyncTime": number,
      "LatestMetadataSyncStatus": "string",
      "LatestMetadataSyncStatusMessage": "string",
      "LogGroupArn": "string",
```

```
        "Name": "string",
        "State": "string"
    }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Hypervisor

所要求 Hypervisor 的詳細資訊。

類型：HypervisorDetails 物件

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetHypervisorPropertyMappings

服務： AWS Backup gateway

此動作會擷取所指定 Hypervisor 的屬性對應。Hypervisor 屬性對應會顯示 Hypervisor 中可用實體屬性與 AWS 中可用屬性之間的關係。

請求語法

```
{
   "HypervisorArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
```

```
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

VmwareToAwsTagMappings

這是 VMware 標籤與 AWS 標籤的對應顯示。

類型：VmwareToAwsTagMapping 物件陣列

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

GetVirtualMachine

服務： AWS Backup gateway

可透過提供 ARN (Amazon Resource Name) 將此 API 傳回虛擬機器。

請求語法

```
{
   "ResourceArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ResourceArn

虛擬機器的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "VirtualMachine": {
      "HostName": "string",
      "HypervisorId": "string",
      "LastBackupDate": number,
      "Name": "string",
      "Path": "string",
      "ResourceArn": "string",
      "VmwareTags": [
         {
```

```
            "VmwareCategory": "string",
            "VmwareTagDescription": "string",
            "VmwareTagName": "string"
         }
      ]
   }
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

VirtualMachine

此物件包含 `VirtualMachine` 輸出所包含的 `GetVirtualMachine` 基本屬性

類型：VirtualMachineDetails 物件

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

ImportHypervisorConfiguration

服務： AWS Backup gateway

透過匯入 Hypervisor 的組態來連線至 Hypervisor。

請求語法

```
{
   "Host": "string",
   "KmsKeyArn": "string",
   "Name": "string",
   "Password": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ],
   "Username": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Host

Hypervisor 的伺服器主機。這可以是 IP 地址或完整網域名稱 (FQDN)。

類型：字串

長度限制：長度下限為 3。長度上限為 128。

模式：^.+$

必要：是

KmsKeyArn

Hypervisor 的 AWS Key Management Service。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必要：否

Name

Hypervisor 的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：是

Password

Hypervisor 的密碼。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[ -~]+$`

必要：否

Tags

要匯入的 Hypervisor 組態標籤。

類型：Tag 物件陣列

必要：否

Username

Hypervisor 的使用者名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必要：否

回應語法

```
{
   "HypervisorArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

取消關聯的 Hypervisor Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

因為您的許可不足，所以操作無法繼續。

HTTP 狀態碼：400

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

ListGateways

服務： AWS Backup gateway

列出 AWS 區域 內 AWS 帳戶 擁有的備份閘道。傳回的清單依閘道 Amazon Resource Name (ARN) 排序。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要列出的最大閘道數量。

類型：整數

有效範圍：最小值為 1。

必要：否

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 `MaxResults` 個數量的資源，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：`^.+$`

必要：否

回應語法

```
{
   "Gateways": [
      {
         "GatewayArn": "string",
         "GatewayDisplayName": "string",
         "GatewayType": "string",
         "HypervisorId": "string",
         "LastSeenTime": number
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Gateways

閘道的清單。

類型：Gateway 物件陣列

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 maxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：^.+$

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

ListHypervisors

服務： AWS Backup gateway

列出您的 hypervisor。

請求語法

```
{
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

MaxResults

要列出的 hypervisor 最大數量。

類型：整數

有效範圍：最小值為 1。

必要：否

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 `maxResults` 個數量的資源，則 `NextToken` 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：`^.+$`

必要：否

回應語法

```
{
```

```
   "Hypervisors": [
      {
         "Host": "string",
         "HypervisorArn": "string",
         "KmsKeyArn": "string",
         "Name": "string",
         "State": "string"
      }
   ],
   "NextToken": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

Hypervisors

您的 Hypervisor 物件清單，依其 Amazon Resource Name (ARN) 排序。

類型：Hypervisor 物件陣列

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 maxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：^.+$

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

ListTagsForResource

服務： AWS Backup gateway

列出套用至資源的標籤，標籤可透過其 Amazon Resource Name (ARN) 識別。

請求語法

```
{
   "ResourceArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ResourceArn

要列出之資源標籤的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "ResourceArn": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceArn

所列出資源標籤的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

Tags

資源標籤的清單。

類型：Tag 物件陣列

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

ListVirtualMachines

服務： AWS Backup gateway

列出您的虛擬機器。

請求語法

```
{
   "HypervisorArn": "string",
   "MaxResults": number,
   "NextToken": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

連線至虛擬機器之 hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

MaxResults

要列出的虛擬機器數量上限。

類型：整數

有效範圍：最小值為 1。

必要：否

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 maxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：^.+$

必要：否

回應語法

```
{
   "NextToken": "string",
   "VirtualMachines": [
      {
         "HostName": "string",
         "HypervisorId": "string",
         "LastBackupDate": number,
         "Name": "string",
         "Path": "string",
         "ResourceArn": "string"
      }
   ]
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

NextToken

所傳回資源部分清單之後的下一個項目。例如，如果請求傳回 maxResults 個數量的資源，則 NextToken 允許您從下一個字符指向的位置開始傳回列表中的更多項目。

類型：字串

長度限制：長度下限為 1。長度上限為 1000。

模式：^.+$

VirtualMachines

您的 VirtualMachine 物件清單，依 Amazon Resource Name (ARN) 排序。

類型：VirtualMachine 物件陣列

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版

- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

PutBandwidthRateLimitSchedule

服務： AWS Backup gateway

此動作會設定指定閘道的頻寬速率限制排程。根據預設，閘道沒有頻寬速率限制排程，這表示頻寬速率限制未生效。使用此項目即可啟動閘道的頻寬速率限制排程。

請求語法

```
{
   "BandwidthRateLimitIntervals": [
      {
         "AverageUploadRateLimitInBitsPerSec": number,
         "DaysOfWeek": [ number ],
         "EndHourOfDay": number,
         "EndMinuteOfHour": number,
         "StartHourOfDay": number,
         "StartMinuteOfHour": number
      }
   ],
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

BandwidthRateLimitIntervals

陣列，其中包含閘道的頻寬速率限制排程間隔。未排程頻寬速率限制間隔時，陣列為空。

類型：BandwidthRateLimitInterval 物件陣列

陣列成員：項目數下限為 0。項目數上限為 20。

必要：是

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 ListGateways 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 `ListGateways` 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

PutHypervisorPropertyMappings

服務： AWS Backup gateway

此動作會設定指定 hypervisor 的屬性對應。Hypervisor 屬性對應會顯示 Hypervisor 中可用之實體屬性與 AWS 中可用屬性之間的關係。

請求語法

```
{
   "HypervisorArn": "string",
   "IamRoleArn": "string",
   "VmwareToAwsTagMappings": [
      {
         "AwsTagKey": "string",
         "AwsTagValue": "string",
         "VmwareCategory": "string",
         "VmwareTagName": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 20。長度上限為 2048。

模式：`^arn:(aws|aws-cn|aws-us-gov):iam::([0-9]+):role/(\S+)$`

必要：是

VmwareToAwsTagMappings

此動作會請求 VMware 標籤與 AWS 標籤的對應。

類型：VmwareToAwsTagMapping 物件陣列

必要：是

回應語法

```
{
   "HypervisorArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

因為您的許可不足，所以操作無法繼續。

HTTP 狀態碼：400

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件

- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

PutMaintenanceStartTime

服務： AWS Backup gateway

設定閘道的維護開始時間。

請求語法

```
{
   "DayOfMonth": number,
   "DayOfWeek": number,
   "GatewayArn": "string",
   "HourOfDay": number,
   "MinuteOfHour": number
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

DayOfMonth

當月開始在閘道上進行維護的日期。

有效值範圍從 Sunday 到 Saturday。

類型：整數

有效範圍：最小值為 1。最大值為 31。

必要：否

DayOfWeek

當週開始在閘道上進行維護的日期。

類型：整數

有效範圍：最小值為 0。最大值為 6。

必要：否

GatewayArn

閘道的 Amazon Resource Name (ARN)，用來指定閘道的維護開始時間。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

HourOfDay

一天中開始在閘道上進行維護的時間 (小時)。

類型：整數

有效範圍：最小值為 0。最大值為 23。

必要：是

MinuteOfHour

開始在閘道上進行維護的時間 (分)。

類型：整數

有效範圍：最小值為 0。最大值為 59。

必要：是

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

閘道的 Amazon Resource Name (ARN)，您需要從中設定維護開始時間。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

StartVirtualMachinesMetadataSync

服務： AWS Backup gateway

此動作會傳送請求，以在指定的虛擬機器之間同步中繼資料。

請求語法

```
{
   "HypervisorArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "HypervisorArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

因為您的許可不足，所以操作無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

TagResource

服務： AWS Backup gateway

為資源新增標籤。

請求語法

```
{
   "ResourceARN": "string",
   "Tags": [
      {
         "Key": "string",
         "Value": "string"
      }
   ]
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ResourceARN

要新增標籤之資源的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

Tags

要指派給資源的標籤清單。

類型：Tag 物件陣列

必要：是

回應語法

```
{
   "ResourceARN": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceARN

已新增標籤之資源的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

TestHypervisorConfiguration

服務： AWS Backup gateway

測試您的 Hypervisor 組態，以驗證備份閘道是否可連線至 hypervisor 及其資源。

請求語法

```
{
   "GatewayArn": "string",
   "Host": "string",
   "Password": "string",
   "Username": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

用於測試的 hypervisor 閘道 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

Host

Hypervisor 的伺服器主機。這可以是 IP 地址或完整網域名稱 (FQDN)。

類型：字串

長度限制：長度下限為 3。長度上限為 128。

模式：`^.+$`

必要：是

Password

Hypervisor 的密碼。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[-~]+$

必要：否

Username

Hypervisor 的使用者名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必要：否

回應元素

如果動作成功，則服務會傳回具空 HTTP 內文的 HTTP 200 回應。

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UntagResource

服務： AWS Backup gateway

從資源移除標籤。

請求語法

```
{
   "ResourceARN": "string",
   "TagKeys": [ "string" ]
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

ResourceARN

要從中移除標籤之資源的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

TagKeys

指定要刪除哪些標籤的標籤金鑰清單。

類型：字串陣列

長度限制：長度下限為 1。長度上限為 128。

模式：`^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必要：是

回應語法

```
{
   "ResourceARN": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

ResourceARN

要從中移除標籤之資源的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UpdateGatewayInformation

服務： AWS Backup gateway

更新閘道的名稱。使用請求中的閘道 Amazon Resource Name (ARN) 來指定要更新的閘道。

請求語法

```
{
   "GatewayArn": "string",
   "GatewayDisplayName": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

要更新之閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

GatewayDisplayName

閘道的已更新顯示名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

回應語法

```
{
   "GatewayArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

已更新閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UpdateGatewaySoftwareNow

服務： AWS Backup gateway

更新閘道虛擬機器 (VM) 軟體。請求會立即觸發軟體更新。

> **Note**
>
> 當您提出此請求時，您會立即獲得 `200 OK` 成功回應。不過，更新可能需要一些時間才能完成。

請求語法

```
{
   "GatewayArn": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

GatewayArn

要更新之閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

回應語法

```
{
   "GatewayArn": "string"
```

```
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

GatewayArn

已更新閘道的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

錯誤

如需所有動作常見的錯誤資訊，請參閱《常見錯誤》。

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python
- 適用於 Ruby V3 的 AWS 開發套件

UpdateHypervisor

服務： AWS Backup gateway

更新 Hypervisor 中繼資料，包括其主機、使用者名稱和密碼。使用請求中的 Hypervisor Amazon Resource Name (ARN) 來指定要更新的 Hypervisor。

請求語法

```
{
   "Host": "string",
   "HypervisorArn": "string",
   "LogGroupArn": "string",
   "Name": "string",
   "Password": "string",
   "Username": "string"
}
```

請求參數

如需所有動作的一般參數相關資訊，請參閱《Common Parameters》。

請求接受採用 JSON 格式的下列資料。

Host

Hypervisor 的已更新主機。這可以是 IP 地址或完整網域名稱 (FQDN)。

類型：字串

長度限制：長度下限為 3。長度上限為 128。

模式：^.+$

必要：否

HypervisorArn

要更新的 Hypervisor Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：是

LogGroupArn

所請求日誌中閘道群組的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

模式：`^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:\*$`

必要：否

Name

Hypervisor 的已更新名稱

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

Password

Hypervisor 的已更新密碼。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[ -~]+$`

必要：否

Username

Hypervisor 的已更新使用者名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[-\.0-\[\]-~]*[!-\.0-\[\]-~][-\.0-\[\]-~]*$

必要：否

回應語法

```
{
   "HypervisorArn": "string"
}
```

回應元素

如果動作成功，則服務傳回 HTTP 200 回應。

服務會傳回下列 JSON 格式的資料。

HypervisorArn

所更新 Hypervisor 的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$

錯誤

如需所有動作常見錯誤的資訊，請參閱常見錯誤。

AccessDeniedException

因為您的許可不足，所以操作無法繼續。

HTTP 狀態碼：400

ConflictException

因為操作不受支援，所以無法繼續。

HTTP 狀態碼：400

InternalServerException

因為發生內部錯誤，所以操作未成功。請稍後再試。

HTTP 狀態碼：500

ResourceNotFoundException

找不到動作所需的資源。

HTTP 狀態碼：400

ThrottlingException

TPS 已受到限制，以防止有意或無意的大量請求。

HTTP 狀態碼：400

ValidationException

因為發生驗證錯誤，所以操作未成功。

HTTP 狀態碼：400

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- AWS 命令列介面
- 適用於 .NET 的 AWS 開發套件
- AWS SDK for C++
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 軟體開發套件第 2 版
- 適用於 JavaScript 的 AWS 開發套件第 3 版
- 適用於 PHP 的 AWS 開發套件第 3 版
- AWS SDK for Python

- 適用於 Ruby V3 的 AWS 開發套件

資料類型

AWS Backup 支援下列資料類型：

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope
- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue

- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate
- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AWS Backup gateway 支援下列資料類型：

- BandwidthRateLimitInterval
- Gateway

- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

AWS Backup

AWS Backup 支援下列資料類型：

- AdvancedBackupSetting
- BackupJob
- BackupJobSummary
- BackupPlan
- BackupPlanInput
- BackupPlansListMember
- BackupPlanTemplatesListMember
- BackupRule
- BackupRuleInput
- BackupSelection
- BackupSelectionsListMember
- BackupVaultListMember
- CalculatedLifecycle
- Condition
- ConditionParameter
- Conditions
- ControlInputParameter
- ControlScope

- CopyAction
- CopyJob
- CopyJobSummary
- DateRange
- Framework
- FrameworkControl
- KeyValue
- LegalHold
- Lifecycle
- ProtectedResource
- ProtectedResourceConditions
- RecoveryPointByBackupVault
- RecoveryPointByResource
- RecoveryPointCreator
- RecoveryPointMember
- RecoveryPointSelection
- ReportDeliveryChannel
- ReportDestination
- ReportJob
- ReportPlan
- ReportSetting
- RestoreJobCreator
- RestoreJobsListMember
- RestoreJobSummary
- RestoreTestingPlanForCreate
- RestoreTestingPlanForGet
- RestoreTestingPlanForList
- RestoreTestingPlanForUpdate
- RestoreTestingRecoveryPointSelection
- RestoreTestingSelectionForCreate

- RestoreTestingSelectionForGet
- RestoreTestingSelectionForList
- RestoreTestingSelectionForUpdate

AdvancedBackupSetting

服務： AWS Backup

每種資源類型的備份選項清單。

目錄

BackupOptions

指定所選資源的備份選項。此選項只在 Windows VSS 備份工作時才能使用。

有效值：

設定為 "WindowsVSS":"enabled" 即可啟用 WindowsVSS 備份選項，並建立 Windows VSS 備份。

設定為 "WindowsVSS":"disabled" 即可建立一般備份。WindowsVSS 選項預設會停用。

如果您指定了無效的選項，則會出現 InvalidParameterValueException 例外狀況。

如需 Windows VSS Backup 的詳細資訊，請參閱《建立啟用 VSS 的 Windows 備份》。

類型：字串到字串映射

金鑰模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

ResourceType

指定包含資源類型和備份選項的物件。唯一支援的資源類型，是具有 Windows 磁碟區陰影複製服務 (VSS) 的 Amazon EC2 執行個體。如需 CloudFormation 範例，請參閱《AWS Backup 使用者指南》中的〈啟用 Windows VSS 的範例 CloudFormation 範本〉一節。

有效值：EC2。

類型：字串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupJob

服務： AWS Backup

包含備份作業的相關詳細資訊。

目錄

AccountId

擁有備份作業的帳戶 ID。

類型：String

模式：^[0-9]{12}$

必要：否

BackupJobId

唯一識別備份 AWS Backup 資源的請求。

類型：字串

必要：否

BackupOptions

可指定所選資源的備份選項。此選項僅適用於 Windows 磁碟區陰影複製服務 (VSS) 備份作業。

有效值：設定為 "WindowsVSS":"enabled" 即可啟用 WindowsVSS 備份選項，並建立 Windows VSS 備份。設定為 "WindowsVSS":"disabled" 即可建立一般備份。如果您指定了無效的選項，則會出現 InvalidParameterValueException 的例外狀況。

類型：字串到字串映射

金鑰模式：^[a-zA-Z0-9\-_\.]{1,50}$

值模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

BackupSizeInBytes

備份的大小，以位元組為單位。

類型：Long

必要：否

BackupType

代表備份作業的備份類型。

類型：字串

必要：否

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：否

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：否

BytesTransferred

查詢作業狀態時傳輸至備份保存庫的大小 (以位元組為單位)。

類型：Long

必要：否

CompletionDate

建立備份作業的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CompletionDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreatedBy

含有建立備份作業的相關識別資訊，包括用於建立備份作業的備份計劃 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

類型：RecoveryPointCreator 物件

必要：否

CreationDate

建立備份作業的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

ExpectedCompletionDate

預期以 Unix 格式和國際標準時間 (UTC) 完成資源備份的日期和時間。ExpectedCompletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

IamRoleArn

指定用於建立目標復原點的 IAM 角色 ARN。預設角色以外的 IAM 角色，必須在角色名稱中包含 AWSBackup 或 AwsBackup。例如 arn:aws:iam::123456789012:role/AWSBackupRDSAccess。沒有這些字串的角色名稱，會缺乏執行備份作業的許可。

類型：字串

必要：否

InitiationDate

這是備份任務的開始日期。

類型：Timestamp

必要：否

IsParent

此為布林值，表示這是父系 (複合) 備份作業。

類型：布林值

必要：否

MessageCategory

此參數是指定訊息類別的任務計數。

範例字串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 INVALIDPARAMETERS。如需 MessageCategory 字串清單，請參閱監視。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的任務計數，並傳回總和。

類型：字串

必要：否

ParentJobId

這可唯一識別要 AWS Backup 備份資源的請求。傳回的值將是父系 (複合) 作業 ID。

類型：字串

必要：否

PercentDone

包含查詢作業狀態時，作業的預估完成百分比。

類型：字串

必要：否

RecoveryPointArn

可唯一識別復原點的 ARN；例如 arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

必要：否

ResourceArn

可唯一識別資源的 ARN。ARN 的格式取決於資源類型。

類型：字串

必要：否

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

必要：否

ResourceType

要備份的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。對於 Windows 磁碟區陰影複製服務 (VSS) 備份，唯一支援的資源類型為 Amazon EC2。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

StartBy

指定在備份作業取消之前必須開始的時間，以 Unix 格式和國際標準時間 (UTC) 顯示。該值是透過將開始時段加至排定時間來計算。因此，如果排定的時間為下午 6 點，而開始時段為 2 小時，則 `StartBy` 時間將是指定日期的下午 8 點。`StartBy` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

State

備份作業的目前狀態。

類型：字串

有效值:CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL

必要：否

StatusMessage

說明備份資源之作業狀態的詳細訊息。

類型：字串

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

BackupJobSummary

服務： AWS Backup

這是最近 30 天內建立或執行的工作摘要。

此傳回的摘要可能包含下列項目：
Region、Account，State、RestourceType、MessageCategory、StartTime、EndTime 和包含工作的計數。

目錄

AccountId

擁有摘要中工作的帳戶 ID。

類型：字串

模式：`^[0-9]{12}$`

必要：否

Count

作為工作摘要中工作數量的值。

類型：整數

必要：否

EndTime

工作結束時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

MessageCategory

此參數是指定訊息類別的工作計數。

範例字串包括 `AccessDenied`、`Success` 和 `InvalidParameters`。請參閱監控以取得 MessageCategory 字串清單。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的工作計數，並傳回總和。

類型：字串

必要：否

Region

工作摘要中的 AWS 區域。

類型：字串

必要：否

ResourceType

此值為所指定資源類型的工作計數。此請求 GetSupportedResourceTypes 會傳回所支援資源類型的字串。

類型：字串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

StartTime

工作開始時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

State

此值是具有指定狀態之工作的工作計數。

類型：字串

有效值:CREATED | PENDING | RUNNING | ABORTING | ABORTED | COMPLETED | FAILED | EXPIRED | PARTIAL | AGGREGATE_ALL | ANY

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

BackupPlan

服務： AWS Backup

包含選用的備份計劃顯示名稱和 `BackupRule` 物件陣列，各指定一項備份規則。備份計劃中的每個規則都是單獨的排程任務，可以備份不同的 AWS 資源選取項目。

目錄

BackupPlanName

備份計劃的顯示名稱。必須包含 1 到 50 個英數字元或 '-_'。字元。

類型：字串

必要：是

Rules

`BackupRule` 物件的陣列，每一個都會指定排程任務，用於備份選取的資源。

類型：BackupRule 物件陣列

必要：是

AdvancedBackupSettings

包含每種資源類型的 `BackupOptions` 清單。

類型：AdvancedBackupSetting 物件陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupPlanInput

服務： AWS Backup

包含選用的備份計劃顯示名稱和 `BackupRule` 物件陣列，各指定一項備份規則。備份計劃中的每個規則都是單獨的排程任務。

目錄

BackupPlanName

備份計劃的顯示名稱。必須包含 1 到 50 個英數字元或 '-_'。字元。

類型：字串

必要：是

Rules

`BackupRule` 物件的陣列，每一個都會指定排程任務，用於備份選取的資源。

類型：BackupRuleInput 物件陣列

必要：是

AdvancedBackupSettings

指定每個資源類型的 `BackupOptions` 清單。這些設定僅適用於 Windows 磁碟區陰影複製服務 (VSS) 備份作業。

類型：AdvancedBackupSetting 物件陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupPlansListMember

服務： AWS Backup

包含備份計劃的相關中繼資料。

目錄

AdvancedBackupSettings

包含資源類型的 `BackupOptions` 清單。

類型：AdvancedBackupSetting 物件陣列

必要：否

BackupPlanArn

可唯一識別備份計畫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`。

類型：字串

必要：否

BackupPlanId

唯一識別備份計畫。

類型：字串

必要：否

BackupPlanName

已儲存備份計劃的顯示名稱。

類型：字串

必要：否

CreationDate

建立資源備份計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CreationDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

DeletionDate

刪除備份計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。DeletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

LastExecutionDate

上次使用此規則執行備份資源任務的時候。日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastExecutionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

VersionId

唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。版本 ID 不能編輯。

類型：字串

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

BackupPlanTemplatesListMember

服務： AWS Backup

指定與備份計劃範本相關聯之中繼資料的物件。

目錄

BackupPlanTemplateId

可唯一識別儲存的備份計劃範本。

類型：字串

必要：否

BackupPlanTemplateName

備份計劃範本的選擇性顯示名稱。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupRule

服務： AWS Backup

可指定用於備份所選取資源的排程任務。

目錄

RuleName

備份規則的顯示名稱。必須包含 1 到 50 個英數字元或 '-_'。字元。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：是

TargetBackupVaultName

存放備份的邏輯容器名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：字串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

CompletionWindowMinutes

備份任務從成功啟動到必須由 AWS Backup 完成或取消的分鐘值。此值是選用的。

類型：Long

必要：否

CopyActions

`CopyAction` 物件的陣列，其包含複製操作的詳細資訊。

類型：CopyAction 物件陣列

必要：否

EnableContinuousBackup

指定 AWS Backup 是否建立連續備份。AWS Backup 建立能進行時間點還原 (PITR) 之連續備份的真正原因。False (或未指定) 會導致 AWS Backup 建立快照備份。

類型：布林值

必要：否

Lifecycle

生命週期會定義受保護的資源會在何時轉移至冷儲存以及會在何時過期。AWS Backup 會根據您定義的生命週期來自動轉移備份和使其過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷儲存的資源類型會列在「依資源分類的功能可用性」表格的「冷儲存生命週期」部分。AWS Backup 會忽略其他資源類型的這項運算式。

類型：Lifecycle 物件

必要：否

RecoveryPointTags

從備份還原時，指派給與此規則相關聯之資源的鍵值對字串陣列。

類型：字串到字串映射

必要：否

RuleId

可唯一識別用於排程所選取資源備份的規則。

類型：字串

必要：否

ScheduleExpression

指定 AWS Backup 何時啟動備份任務的 CRON 運算式 (UTC 格式)。如需 AWS cron 運算式的詳細資訊，請參閱《Amazon CloudWatch Events 使用者指南》中的〈排程規則表達式〉。AWS cron

運算式的兩個範例是 `15 * ? * * *` (每小時在整點 15 分執行一次備份) 和 `0 12 * * ? *` (每天在 UTC 中午 12 點執行一次備份)。如需範例表格，請按一下前一個連結，然後向下捲動頁面。

類型：字串

必要：否

ScheduleExpressionTimezone

這是設定排程運算式的時區。ScheduleExpressions 預設會使用 UTC 格式。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowMinutes

從排程備份到取消任務 (如未成功啟動) 的分鐘值。此值是選用的。若包含此值，則其必須至少為 60 分鐘以避免發生錯誤。

在啟動時段期間，備份工作狀態會保持在 `CREATED` 狀態，直到順利開始或啟動時段時間用完為止。如果 AWS Backup 在啟動時段內收到允許重試工作的錯誤訊息，則 AWS Backup 會至少每 10 分鐘自動重試開始工作，直到備份順利開始 (工作狀態會變更為 `RUNNING`) 或工作狀態變更為 `EXPIRED` 為止 (預期會在啟動時段時間結束時發生)。

類型：Long

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupRuleInput

服務： AWS Backup

可指定用於備份所選取資源的排程任務。

目錄

RuleName

備份規則的顯示名稱。必須包含 1 到 50 個英數字元或 '-_'。字元。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：是

TargetBackupVaultName

存放備份的邏輯容器名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：字串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：是

CompletionWindowMinutes

備份任務從成功啟動到必須由 AWS Backup 完成或取消的分鐘值。此值是選用的。

類型：Long

必要：否

CopyActions

`CopyAction` 物件的陣列，其包含複製操作的詳細資訊。

類型：CopyAction 物件陣列

必要：否

EnableContinuousBackup

指定 AWS Backup 是否建立連續備份。AWS Backup 建立能進行時間點還原 (PITR) 之連續備份的真正原因。False (或未指定) 會導致 AWS Backup 建立快照備份。

類型：布林值

必要：否

Lifecycle

生命週期會定義受保護的資源會在何時轉移至冷儲存以及會在何時過期。AWS Backup 會根據您定義的生命週期來自動轉移備份和使之過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留期」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷儲存的資源類型會列在「依資源分類的功能可用性」表格的「冷儲存生命週期」部分。AWS Backup 會忽略其他資源類型的這項運算式。

這項參數的最大值為 100 年 (36,500 天)。

類型：Lifecycle 物件

必要：否

RecoveryPointTags

為協助組織您的資源，您可以將自己的中繼資料指派給您建立的資源。每個標籤都是金鑰值對。

類型：字串到字串映射

必要：否

ScheduleExpression

指定 AWS Backup 何時啟動備份任務的 Cron 表達式 (UTC 格式)。

類型：字串

必要：否

ScheduleExpressionTimezone

這是設定排程運算式的時區。ScheduleExpressions 預設會以 UTC 格式表示。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowMinutes

從排程備份到取消任務 (如未成功啟動) 的分鐘值。此值是選用的。若包含此值，則其必須至少為 60 分鐘以避免發生錯誤。

此參數的最大值為 100 年 (52,560,000 分鐘)。

在啟動時段期間，備份工作狀態會保持在 CREATED 狀態，直到順利開始或啟動時段時間用完為止。如果 AWS Backup 在啟動時段內收到允許重試工作的錯誤訊息，則 AWS Backup 會自動至少每 10 分鐘重試開始工作，直到備份順利開始 (工作狀態會變更為 RUNNING) 或工作狀態變更為 EXPIRED 為止 (預期會在啟動時段時間結束時發生)。

類型：Long

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupSelection

服務： AWS Backup

用於將一組資源指派給備份計劃。

建議您指定所需的 Conditions、ListOfTags、NotResources 和/或 Resources。如果未指定這些資源，備份將嘗試選取所有受支援和已選擇加入的儲存資源，這些資源可能會產生非預期的成本影響。

目錄

IamRoleArn

備份目標資源時 AWS Backup 用來驗證的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：是

SelectionName

所選資源文件的顯示名稱。必須包含 1 到 50 個英數字元或 '-_'。字元。

類型：String

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：是

Conditions

您定義使用標籤將資源指派至備份計劃的條件清單。例如 "StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },。條件運算子名稱區分大小寫。

Conditions 與 ListOfTags 有以下差異：

- 當您指定多個條件時，僅會指派符合 ALL 條件的資源 (使用 AND 邏輯)。
- Conditions 支援 StringEquals、StringLike、StringNotEquals 和 StringNotLike。ListOfTags 僅支援 StringEquals。

類型：Conditions 物件

必要：否

ListOfTags

您定義使用標籤將資源指派至備份計劃的條件清單。例如 "StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },。條件運算子名稱區分大小寫。

ListOfTags 與 Conditions 有以下差異：

- 當您指定多個條件時，會指派符合 AT LEAST ONE 條件的所有資源 (使用 OR 邏輯)。
- ListOfTags 僅支援 StringEquals。Conditions 支援 StringEquals、StringLike、StringNotEquals 和 StringNotLike。

類型：Condition 物件陣列

必要：否

NotResources

要排除在備份計劃之外的 Amazon Resource Names (ARN) 清單。ARN 的數目上限為 500 個 (不含萬用字元)，或 30 個含萬用字元的 ARN。

若您需要從備份計劃中排除眾多資源，請考慮使用不同的資源選擇策略，例如僅指派一或數個資源類型，或使用標籤精簡您的資源選擇。

類型：字串陣列

必要：否

Resources

要指派給備份計劃的 Amazon Resource Name (ARN) 清單。ARN 的數目上限為 500 個 (不含萬用字元)，或 30 個含萬用字元的 ARN。

若您需要將眾多資源指派至備份計劃，請考慮使用不同的資源選擇策略，例如僅指派一個資源類型的所有資源，或使用標籤精簡您的資源選擇。

類型：字串陣列

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS 適用於 Java V2 的 SDK
- AWS 適用於紅寶石 V3 的 SDK

BackupSelectionsListMember

服務： AWS Backup

包含 BackupSelection 物件的相關中繼資料。

目錄

BackupPlanId

唯一識別備份計劃。

類型：字串

必要：否

CreationDate

建立備份計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

IamRoleArn

指定 IAM 角色 Amazon Resource Name (ARN) 以建立目標復原點，例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：否

SelectionId

唯一識別請求，將一組資源指派給備份計劃。

類型：字串

必要：否

SelectionName

所選資源文件的顯示名稱。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

BackupVaultListMember

服務： AWS Backup

包含備份保存庫的相關中繼資料。

目錄

BackupVaultArn

可唯一識別備份文件庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：否

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：否

CreationDate

建立資源備份時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CreationDate` 的值精確到毫秒。。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreatorRequestId

可識別請求的唯一字串，且允許重試失敗的請求，而不會有兩次執行操作的風險。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

EncryptionKeyArn

您可以指定從支援完整 AWS Backup 管理的服務加密備份的伺服器端加密金鑰，例如`arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。如果您要指定金鑰，則必須指定其 ARN，而不是其別名。如果您不指定金鑰，則根據預設， AWS Backup 會為您建立 KMS 金鑰。

若要瞭解哪些 AWS Backup 服務支援完整 AWS Backup 管理，以及如何 AWS Backup 處理來自尚未完整支援的服務備份的加密 AWS Backup，請參閱中的備份加密 AWS Backup

類型：字串

必要：否

LockDate

文件 AWS Backup 庫鎖定組態變為不可變的日期和時間，表示無法變更或刪除。

如果在未指定鎖定日期的情況下，將「Vault Lock 」套用至保存庫，則可隨時變更「Vault Lock 」設定，或從保存庫中完全刪除「Vault Lock 」。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

Locked

Boolean 值，指示文件 AWS Backup 庫鎖定是否套用至選取的備份儲存庫。如果為 `true`，則「Vault Lock 」會防止對所選保存庫的復原點進行刪除和更新操作。

類型：布林值

必要：否

MaxRetentionDays

「文件 AWS Backup 庫鎖定」設定，用於指定文件庫保留其復原點的最長保留期間。若未指定此參數，Vault Lock 不會對保存庫中的復原點強制執行最長保留期間 (允許無限期儲存)。

若經過指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或短於最長保留期間。若任務的保留期間超過該最長保留期間，則文件庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的文件庫。在執行Vault Lock 之前已儲存於保存庫的復原點不會受到影響。

類型：Long

必要：否

MinRetentionDays

「文件 AWS Backup 庫鎖定」設定，用於指定文件庫保留其復原點的最短保留期。若未指定此參數，則Vault Lock 不會強制執行最短保留期間。

若經過指定，則保存庫的所有備份或複製任務皆必須具有生命週期政策，其保留期間等於或超過最短保留期間。若任務的保留期間未達最短保留期間，則保存庫的備份或複製任務會失敗，您應修改生命週期設定或使用不同的保存庫。在執行Vault Lock 之前已儲存於保存庫的復原點不會受到影響。

類型：Long

必要：否

NumberOfRecoveryPoints

儲存在備份保存庫中的復原點數目。

類型：Long

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的开发
- AWS 適用於紅寶石 V3 的 SDK

CalculatedLifecycle

服務： AWS Backup

包含 `DeleteAt` 和 `MoveToColdStorageAt` 時間戳記，上述項目可用來指定復原點的生命週期。

生命週期會定義受保護的資源會在何時轉移至冷儲存以及會在何時過期。AWS Backup 會根據您定義的生命週期來自動轉移備份和使其過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留期」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷儲存的資源類型會列在「依資源分類的功能可用性」表格的「冷儲存生命週期」部分。AWS Backup 會忽略其他資源類型的這項運算式。

目錄

DeleteAt

時間戳記，指定何時刪除復原點。

類型：Timestamp

必要：否

MoveToColdStorageAt

指定何時將復原點轉移至冷儲存的時間戳記。

類型：Timestamp

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Condition

服務： AWS Backup

包含由條件類型 (例如 StringEquals)、金鑰和值這三者構成的陣列。用於透過標籤篩選資源，並將其指派給備份計劃。區分大小寫。

目錄

ConditionKey

鍵/值對中的索引鍵。例如，在標籤 Department: Accounting 中，Department 為索引鍵。

類型：字串

必要：是

ConditionType

可套用到鍵值對，用於將資源指派給備份計劃的操作。條件僅支援 StringEquals。如需更靈活的指派選項，包括 StringLike 並能夠從備份計劃中排除資源，請使用 BackupSelection 的.Conditions (字尾有 s)。

類型：字串

有效值: STRINGEQUALS

必要：是

ConditionValue

鍵/值對的值。例如，在標籤 Department: Accounting 中，Accounting 為值。

類型：字串

必要：是

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版

- 適用於 Ruby 的 AWS SDK 第 3 版

ConditionParameter

服務： AWS Backup

包含您定義以將標籤資源指派給備份計劃之標籤的資訊。

目錄

ConditionKey

鍵/值對中的索引鍵。例如，在標籤 `Department: Accounting` 中，`Department` 為索引鍵。

類型：字串

必要：否

ConditionValue

鍵/值對的值。例如，在標籤 `Department: Accounting` 中，`Accounting` 為值。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Conditions

服務： AWS Backup

包含使用其標籤在備份計劃中包含或排除哪些資源的相關資訊。條件區分大小寫。

目錄

StringEquals

僅針對您標記相同值的資源，篩選已標記資源的值。也稱為「完全相符」。

類型：ConditionParameter 物件陣列

必要：否

StringLike

在字串中的任何位置使用萬用字元 (*)，篩選已標記資源的值中相符的標籤值。例如，"prod*" 或 "*rod*" 與標籤值 "production" 相符。

類型：ConditionParameter 物件陣列

必要：否

StringNotEquals

僅針對您標記不具有相同值的資源，篩選已標記資源的值。也稱為「否定相符」。

類型：ConditionParameter 物件陣列

必要：否

StringNotLike

在字串中的任何位置使用萬用字元 (*)，篩選已標記資源的值中不相符的標籤值。

類型：ConditionParameter 物件陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK

- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ControlInputParameter

服務： AWS Backup

控制項參數的清單。一個控制項可以有零個、一個或多個參數。具有兩個參數的控制項範例為：「備份計劃頻率至少為 daily，且保留期間至少為 1 year」。第一個參數為 daily。第二個參數為 1 year。

目錄

ParameterName

參數的名稱，例如 BackupPlanFrequency。

類型：字串

必要：否

ParameterValue

參數的值，例如 hourly。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ControlScope

服務： AWS Backup

架構包含一或多個控制項。每個控制項都有自己的控制範圍。控制範圍可以包含一或多個資源類型、標籤索引鍵和值的組合，或一個資源類型和一個資源 ID 的組合。如果未指定範圍，會在組態中記錄群組的任何資源變更時，觸發規則評估。

> **Note**
>
> 若要設定包含所有特定資源的控制範圍，請將 `ControlScope` 留白，或在呼叫 `CreateFramework` 時不要傳遞。

目錄

ComplianceResourceIds

您希望控制範圍包含的唯一 AWS 資源的 ID。

類型：字串陣列

陣列成員：項目數下限為 1。項目數上限為 100。

必要：否

ComplianceResourceTypes

描述控制範圍是否包含一或多種類型的資源，例如 `EFS` 或 `RDS`。

類型：字串陣列

必要：否

Tags

標籤鍵值配對套用至您想要觸發規則評估的 AWS 資源。最多可提供一個索引鍵/值組。標籤值為選用，但不得為空字串。指派標籤的結構為：`[{"Key":"string","Value":"string"}]`。

類型：字串到字串映射

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的开发
- AWS 適用於紅寶石 V3 的 SDK

CopyAction

服務： AWS Backup

複製操作的詳細資訊。

目錄

DestinationBackupVaultArn

唯一識別複製備份之目的地備份文件庫的 Amazon Resource Name (ARN)。例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：是

Lifecycle

包含 `Transition` 物件的陣列，指定復原點轉換成冷儲存或刪除前的天數。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，在主控台上，「保留」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。 AWS Backup 會忽略其他資源類型的這個表示式。

類型：Lifecycle 物件

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於紅寶石 V3 的 SDK

CopyJob

服務： AWS Backup

包含複製作業的相關詳細資訊。

目錄

AccountId

擁有複製作業的帳戶 ID。

類型：String

模式：`^[0-9]{12}$`

必要：否

BackupSizeInBytes

複製作業的大小，以位元組為單位。

類型：Long

必要：否

ChildJobsInState

這會傳回所包含之子 (巢狀) 複製作業的統計資訊。

類型：字串到長映射

有效金鑰：`CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

必要：否

CompletionDate

複製作業的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CompletionDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CompositeMemberIdentifier

這是複合群組內資源的識別符，例如屬於複合 (父系) 堆疊的巢狀 (子) 復原點。ID 會從堆疊中的邏輯 ID 傳輸。

類型：字串

必要：否

CopyJobId

可唯一識別複製作業。

類型：字串

必要：否

CreatedBy

包含用於起始復原點備份的 AWS Backup 備份計劃和規則的相關資訊。

類型：RecoveryPointCreator 物件

必要：否

CreationDate

建立複製作業時的日期和時間，以 Unix 時間格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

DestinationBackupVaultArn

可唯一識別複本保存庫的 Amazon Resource Name (ARN)，例如，arn:aws:backup:us-east-1:123456789012:vault:aBackupVault。

類型：字串

必要：否

DestinationRecoveryPointArn

可唯一識別目的地復原點的 ARN，例如，arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45。

類型：字串

必要：否

IamRoleArn

指定用於複製目標復原點的 IAM 角色 ARN；例如，arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：否

IsParent

此為布林值，表示這是父系 (複合) 複製作業。

類型：布林值

必要：否

MessageCategory

此參數是指定訊息類別的任務計數。

範例字串可能包括 AccessDenied、SUCCESS、AGGREGATE_ALL 和 InvalidParameters。如需 MessageCategory 字串清單，請參閱監視。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的任務計數，並傳回總和

類型：字串

必要：否

NumberOfChildJobs

這是子 (巢狀) 複製作業的數量。

類型：Long

必要：否

ParentJobId

這可唯一識別要 AWS Backup 複製資源的請求。傳回的值將是父系 (複合) 作業 ID。

類型：字串

必要：否

ResourceArn

要複製的 AWS 資源；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

類型：字串

必要：否

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

必要：否

ResourceType

要複製的 AWS 資源類型；例如，亞馬遜彈性區塊存放區 (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

SourceBackupVaultArn

可唯一識別來源複本保存庫的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：否

SourceRecoveryPointArn

唯一識別來源復原點的 ARN；例如，`arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

必要：否

State

複製作業的目前狀態。

類型：字串

有效值:`CREATED | RUNNING | COMPLETED | FAILED | PARTIAL`

必要：否

StatusMessage

說明複製資源之作業狀態的詳細訊息。

類型：字串

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的開發
- AWS 適用於紅寶石 V3 的 SDK

CopyJobSummary

服務： AWS Backup

這是最近 30 天內建立或執行的複製工作摘要。

此傳回的摘要可能包含下列項目：
Region、Account，State、RestourceType、MessageCategory、StartTime、EndTime 和包含工作的計數。

目錄

AccountId

擁有摘要中工作的帳戶 ID。

類型：字串

模式：`^[0-9]{12}$`

必要：否

Count

作為工作摘要中工作數量的值。

類型：整數

必要：否

EndTime

工作結束時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

MessageCategory

此參數是指定訊息類別的工作計數。

範例字串包括 `AccessDenied`、`Success` 和 `InvalidParameters`。請參閱監控以取得 MessageCategory 字串清單。

該值 ANY 會傳回所有訊息類別的計數。

AGGREGATE_ALL 彙總所有訊息類別的工作計數，並傳回總和。

類型：字串

必要：否

Region

這是工作摘要中的 AWS 區域。

類型：字串

必要：否

ResourceType

此值為所指定資源類型的工作計數。此請求 GetSupportedResourceTypes 會傳回所支援資源類型的字串

類型：字串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

StartTime

工作開始時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

State

此值是具有指定狀態之工作的工作計數。

類型：字串

有效值:CREATED | RUNNING | ABORTING | ABORTED | COMPLETING | COMPLETED | FAILING | FAILED | PARTIAL | AGGREGATE_ALL | ANY

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

DateRange

服務： AWS Backup

這是包含「FromDate: DateTime」和「ToDate: DateTime」的資源篩選條件。兩個都是必要值。不允許使用未來的 DateTime 值。

日期和時間採用 Unix 格式和國際標準時間 (UTC) 格式，且精確到毫秒 (毫秒為選擇性)。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

目錄

FromDate

此值是開始日期 (括)。

日期和時間採用 Unix 格式和國際標準時間 (UTC) 格式，且精確到毫秒 (毫秒為選擇性)。

類型：Timestamp

必要：是

ToDate

此值是結束日期 (括)。

日期和時間採用 Unix 格式和國際標準時間 (UTC) 格式，且精確到毫秒 (毫秒為選擇性)。

類型：Timestamp

必要：是

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Framework

服務： AWS Backup

包含架構的詳細資訊。架構包含控制項，可評估並報告備份事件和資源。架構可產生每日合規性結果。

目錄

CreationTime

架構建立時的日期和時間，採用 ISO 8601 表示法。CreationTime 的值精確到毫秒。舉例來說，2020-07-10T15:00:00.000-08:00 代表 2020 年 7 月 10 日下午 3 點，比國際標準時間晚 8 小時。

類型：Timestamp

必要：否

DeploymentStatus

架構的部署狀態。狀態如下：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED | FAILED

類型：字串

必要：否

FrameworkArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：否

FrameworkDescription

架構的選用描述，最多包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：.*\S.*

必要：否

FrameworkName

架構的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，且開頭要為英文字母，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必要：否

NumberOfControls

架構所包含的控制項數量。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

FrameworkControl

服務： AWS Backup

包含所有框架控制項的詳細資訊。每個框架必須包含至少一個控制項。

目錄

ControlName

控制項的名稱。此名稱介於 1 至 256 個字元之間。

類型：字串

必要：是

ControlInputParameters

`ParameterName` 與 `ParameterValue` 配對的清單。

類型：ControlInputParameter 物件陣列

必要：否

ControlScope

控制項的範圍。控制項範圍定義控制項將評估的內容。控制項範圍的三個範例為：特定備份計劃、具有特定標籤的所有備份計劃或所有備份計劃。

如需更多詳細資訊，請參閱 `ControlScope`。

類型：ControlScope 物件

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

KeyValue

服務： AWS Backup

一對兩個相關的字串。允許的字元包括字母、空格和可以用 UTF-8 表示的數字，以及下列字元： + - = . _ : /

目錄

Key

標籤鍵 (字串)。索引鍵無法以 aws: 開頭。

長度限制：長度下限為 1。長度上限為 128。

模式：^(?![aA]{1}[wW]{1}[sS]{1}:)([\p{L}\p{Z}\p{N}_.:/=+\-@]+)$

類型：字串

必要：是

Value

此金鑰的值。

長度限制：長度上限為 256。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

類型：字串

必要：是

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

LegalHold

服務： AWS Backup

法務保存是一種管理工具，可協助防止備份在保存下遭到刪除。如果有保存，則無法刪除保存下的備份，而且會變更備份狀態 (例如轉換為冷儲存) 的生命週期政策會延遲，直到移除法務保存為止。一個備份可以有多個法務保存。法務保存可套用至一或多個備份 (也稱為復原點)。這些備份可以按資源類型和資源 ID 進行篩選。

目錄

CancellationDate

這是取消法務保存時的時間，以數字格式顯示。

類型：Timestamp

必要：否

CreationDate

這是建立法務保存時的時間，以數字格式顯示。

類型：Timestamp

必要：否

Description

這是法務保存的描述。

類型：字串

必要：否

LegalHoldArn

這是可唯一識別法務保存的 Amazon Resource Number (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

必要：否

LegalHoldId

一或多個復原點上的特定法務保存 ID。

類型：字串

必要：否

Status

這是法務保存的狀態。狀態可以是 ACTIVE、CREATING、CANCELED 和 CANCELING。

類型：字串

有效值: CREATING | ACTIVE | CANCELING | CANCELED

必要：否

Title

這是法務保存的標題。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Lifecycle

服務： AWS Backup

包含 `Transition` 物件的陣列，指定復原點轉換成冷儲存或刪除前的天數。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，在主控台上，「保留期」設定必須比「轉移至冷儲存前所需天數」設定長 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷儲存的資源類型會列在「依資源分類的功能可用性」表格的「冷儲存生命週期」部分。AWS Backup 會忽略其他資源類型的這項運算式。

目錄

DeleteAfterDays

指定復原點在建立後多少天予以刪除。必須超過 90 天以上，並加上 `MoveToColdStorageAfterDays`。

類型：Long

必要：否

MoveToColdStorageAfterDays

指定復原點在建立後，移至冷儲存的天數。

類型：Long

必要：否

OptInToArchiveForSupportedResources

選用布林值。如果此值為真，此設定會指示備份計畫根據生命週期設定，將支援的資源轉移至封存 (不常用) 儲存層。

類型：布林值

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

ProtectedResource

服務： AWS Backup

包含備份資源相關資訊的結構。

目錄

LastBackupTime

上次備份資源時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastBackupTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

LastBackupVaultArn

這是備份保存庫的 ARN (Amazon Resource Name)，此備份保存庫中包含最新的備份復原點。

類型：字串

必要：否

LastRecoveryPointArn

這是最近復原點的 Amazon Resource Name (ARN)。

類型：字串

必要：否

ResourceArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：否

ResourceName

這是屬於指定備份的資源非唯一名稱。

類型：字串

必要：否

ResourceType

AWS 資源的類型；例如 Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon Relational Database Service (Amazon RDS) 資料庫。對於 Windows 磁碟區陰影複製服務 (VSS) 備份，唯一支援的資源類型為 Amazon EC2。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

ProtectedResourceConditions

服務： AWS Backup

您使用標籤為還原測試計畫中的資源定義的條件清單。

例如："StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },。條件運算子名稱區分大小寫。

目錄

StringEquals

僅針對您標記相同值的資源，篩選已標記資源的值。也稱為「完全相符」。

類型：KeyValue 物件陣列

必要：否

StringNotEquals

僅針對您標記不具有相同值的資源，篩選已標記資源的值。也稱為「否定相符」。

類型：KeyValue 物件陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RecoveryPointByBackupVault

服務： AWS Backup

包含儲存在備份保存庫中之復原點的詳細資訊。

目錄

BackupSizeInBytes

備份的大小，以位元組為單位。

類型：Long

必要：否

BackupVaultArn

可唯一識別備份保存庫的 ARN，例如 `arn:aws:backup:us-east-1:123456789012:vault:aBackupVault`。

類型：字串

必要：否

BackupVaultName

存放備份的邏輯容器的名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：String

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：否

CalculatedLifecycle

包含 `DeleteAt` 和 `MoveToColdStorageAt` 時間戳記的 `CalculatedLifecycle` 物件。

類型：CalculatedLifecycle 物件

必要：否

CompletionDate

還原復原點之作業的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CompletionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CompositeMemberIdentifier

這是複合群組內資源的識別符，例如屬於複合 (父系) 堆疊的巢狀 (子) 復原點。ID 會從堆疊中的邏輯 ID 傳輸。

類型：字串

必要：否

CreatedBy

含有建立復原點的相關識別資訊，包括用於建立復原點的備份計劃 BackupPlanArn、BackupPlanId、BackupPlanVersion 和 BackupRuleId。

類型：RecoveryPointCreator 物件

必要：否

CreationDate

建立復原點時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

EncryptionKeyArn

用來保護備份的伺服器端加密金鑰，例如 arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab。

類型：字串

必要：否

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN；例如 `arn:aws:iam::123456789012:role/S3Access`。

類型：字串

必要：否

IsEncrypted

傳回的布林值，若指定的復原點已加密，則為 TRUE，若復原點未加密，則為 FALSE。

類型：布林值

必要：否

IsParent

此為布林值，表示這是父系 (複合) 復原點。

類型：布林值

必要：否

LastRestoreTime

最後還原復原點時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 格式顯示。`LastRestoreTime` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

Lifecycle

生命週期定義受保護資源何時轉換為冷存儲以及何時到期。 AWS Backup 根據您定義的生命週期，自動轉換備份並過期。

轉移至冷儲存的備份必須在冷儲存中存放至少 90 天之久。因此，「保留」設定必須比「轉移至冷儲存前所需天數」設定大上 90 天。「轉移至冷儲存前所需天數」設定在已有備份轉移至冷儲存後就無法再加以變更。

能夠轉換為冷庫的資源類型會列在「依資源分類的功能可用性」表格的「冷藏的生命週期」區段中。 AWS Backup 會忽略其他資源類型的這個表示式。

類型：Lifecycle 物件

必要：否

ParentRecoveryPointArn

這是父系 (複合) 復原點的 Amazon Resource Name (ARN)。

類型：字串

必要：否

RecoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

必要：否

ResourceArn

可唯一識別資源的 ARN。ARN 的格式取決於資源類型。

類型：字串

必要：否

ResourceName

這是屬於特定備份的資源非唯一名稱。

類型：字串

必要：否

ResourceType

儲存為復原點的 AWS 資源類型；例如，Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon Relational Database Service 服務 (Amazon RDS) 資料庫。對於 Windows 磁碟區陰影複製服務 (VSS) 備份，唯一支援的資源類型為 Amazon EC2。

類型：String

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

SourceBackupVaultArn

為復原點原始複製來源的備份保存庫。如果恢復點還原至相同的帳戶，則此值將為 null。

類型：字串

必要：否

Status

指定復原點狀態的狀態碼。

類型：字串

有效值:COMPLETED | PARTIAL | DELETING | EXPIRED

必要：否

StatusMessage

說明復原點刪除失敗原因的訊息。

類型：字串

必要：否

VaultType

這是存放所述復原點所用的保存庫類型。

類型：字串

有效值:BACKUP_VAULT | LOGICALLY_AIR_GAPPED_BACKUP_VAULT

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件

- AWS 適用於紅寶石 V3 的 SDK

RecoveryPointByResource

服務： AWS Backup

包含已儲存復原點的詳細資訊。

目錄

BackupSizeBytes

備份的大小，以位元組為單位。

類型：Long

必要：否

BackupVaultName

存放備份的邏輯容器名稱。備份文件庫依名稱識別，這些名稱對建立文件庫的帳戶和 AWS 區域來說是唯一的。這些名稱由小寫字母、數字和連字號組成。

類型：字串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：否

CreationDate

建立復原點時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

EncryptionKeyArn

用來保護備份的伺服器端加密金鑰，例如 `arn:aws:kms:us-west-2:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab`。

類型：字串

必要：否

IsParent

此為布林值，表示這是父系 (複合) 復原點。

類型：布林值

必要：否

ParentRecoveryPointArn

這是父系 (複合) 復原點的 Amazon Resource Name (ARN)。

類型：字串

必要：否

RecoveryPointArn

可唯一識別復原點的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

必要：否

ResourceName

這是屬於指定備份的資源非唯一名稱。

類型：字串

必要：否

Status

指定復原點狀態的狀態碼。

類型：字串

有效值: `COMPLETED | PARTIAL | DELETING | EXPIRED`

必要：否

StatusMessage

說明復原點刪除失敗原因的訊息。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

RecoveryPointCreator

服務： AWS Backup

包含 AWS Backup 用於起始復原點備份的備份計劃和規則相關資訊。

目錄

BackupPlanArn

可唯一識別備份計劃的 Amazon Resource Name (ARN)，例如 `arn:aws:backup:us-east-1:123456789012:plan:8F81F553-3A74-4A3F-B93D-B3360DC80C50`。

類型：字串

必要：否

BackupPlanId

唯一識別備份計劃。

類型：字串

必要：否

BackupPlanVersion

版本 ID 是唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。您無法對其進行編輯。

類型：字串

必要：否

BackupRuleId

可唯一識別用於排程所選取資源備份的規則。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

RecoveryPointMember

服務： AWS Backup

這是一個復原點，其為父系 (複合) 復原點的子 (巢狀) 復原點。這些復原點可以與其父系 (複合) 復原點取消關聯，在這種情況下，復原點將不再是成員。

目錄

BackupVaultName

這是備份保存庫 (儲存備份的邏輯容器) 的名稱。

類型：字串

模式：`^[a-zA-Z0-9\-\_]{2,50}$`

必要：否

RecoveryPointArn

這是父系 (複合) 復原點的 Amazon Resource Name (ARN)。

類型：字串

必要：否

ResourceArn

這是可唯一識別已儲存資源的 Amazon Resource Name (ARN)。

類型：字串

必要：否

ResourceType

這是儲存為復原點的 AWS 資源類型。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

RecoveryPointSelection

服務： AWS Backup

這指定了用於指派一組資源的條件，例如資源類型或備份保存庫。

目錄

DateRange

這是包含「FromDate: DateTime」和「ToDate: DateTime」的資源篩選條件。兩個都是必要值。不允許使用未來的 DateTime 值。

日期和時間採用 Unix 格式和國際標準時間 (UTC) 格式，且精確到毫秒 (毫秒為選擇性)。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：DateRange 物件

必要：否

ResourceIdentifiers

這些是資源選取項中包含的資源 (包括資源和保存庫的類型)。

類型：字串陣列

必要：否

VaultNames

這些保存庫的名稱，其中包含所選取的復原點。

類型：字串陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版

- 適用於 Ruby 的 AWS SDK 第 3 版

ReportDeliveryChannel

服務： AWS Backup

包含有關在何處交付報告的報告計劃資訊，特別是 Amazon S3 儲存貯體名稱、S3 金鑰字首以及報告格式。

目錄

S3BucketName

接收報告的 S3 儲存貯體唯一名稱。

類型：字串

必要：是

Formats

報告格式的清單：CSV、JSON 或兩者。如果未指定，則預設格式為 CSV。

類型：字串陣列

必要：否

S3KeyPrefix

AWS Backup Audit Manager 將您的報告交付給 Amazon S3 之位置的字首。字首在以下路徑的此部分：s3://your-bucket-name/prefix/Backup/us-west-2/year/month/day/report-name。如果未指定，則沒有字首。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ReportDestination

服務： AWS Backup

包含報告工作中有關報告目的地的資訊。

目錄

S3BucketName

接收報告的 S3 儲存貯體唯一名稱。

類型：字串

必要：否

S3Keys

可唯一識別 S3 儲存貯體中報告的物件金鑰。

類型：字串陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ReportJob

服務： AWS Backup

包含報告工作的相關詳細資訊。報告工作會根據報告計劃編譯報告，並將其發佈至 Amazon S3。

目錄

CompletionTime

完成報告工作時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CompletionTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreationTime

建立報告工作時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

ReportDestination

報告工作發佈報告所在目的地的 S3 儲存貯體名稱和 S3 金鑰。

類型：ReportDestination 物件

必要：否

ReportJobId

報告工作的識別符。唯一隨機產生的 Unicode、UTF-8 編碼字串，最長 1,024 個位元組。報告工作 ID 無法編輯。

類型：字串

必要：否

ReportPlanArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：否

ReportTemplate

識別報告的報告範本。使用報告範本建立的報告。報告範本包括：

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

類型：字串

必要：否

Status

報告工作的狀態。狀態如下：

`CREATED | RUNNING | COMPLETED | FAILED`

`COMPLETED` 表示該報告可在您指定的目的地進行檢閱。如果狀態為 `FAILED`，請檢閱 `StatusMessage` 以了解原因。

類型：字串

必要：否

StatusMessage

說明報告工作狀態的訊息。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK

- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ReportPlan

服務： AWS Backup

包含報告計劃的詳細資訊。

目錄

CreationTime

建立報告計劃時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

DeploymentStatus

報告計劃的部署狀態。狀態如下：

CREATE_IN_PROGRESS | UPDATE_IN_PROGRESS | DELETE_IN_PROGRESS | COMPLETED

類型：字串

必要：否

LastAttemptedExecutionTime

上次嘗試執行與此報表計劃相關聯之報表工作的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastAttemptedExecutionTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

LastSuccessfulExecutionTime

上次成功執行與此報表計劃相關聯之報表工作的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastSuccessfulExecutionTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

ReportDeliveryChannel

包含有關在何處和如何交付報告的資訊，特別是 Amazon S3 儲存貯體名稱、S3 金鑰字首以及報告格式。

類型：ReportDeliveryChannel 物件

必要：否

ReportPlanArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：否

ReportPlanDescription

報告計劃的選用描述，最多可包含 1,024 個字元。

類型：字串

長度限制：長度下限為 0。長度上限為 1024。

模式：`.*\S.*`

必要：否

ReportPlanName

報告計劃的唯一名稱。此名稱的長度必須介於 1 到 256 個字元，且開頭要為英文字母，由英文字母 (a-z、A-Z)、數字 (0-9) 和底線 (_) 組成。

類型：字串

長度限制：長度下限為 1。長度上限為 256。

模式：`[a-zA-Z][_a-zA-Z0-9]*`

必要：否

ReportSetting

識別報告的報告範本。使用報告範本建立的報告。報告範本包括：

RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT

如果報告範本為 RESOURCE_COMPLIANCE_REPORT 或 CONTROL_COMPLIANCE_REPORT，此 API 資源也可以依 AWS 區域 和架構描述報告涵蓋範圍。

類型：ReportSetting 物件

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

ReportSetting

服務： AWS Backup

包含報告設定的相關詳細資訊。

目錄

ReportTemplate

識別報告的報告範本。使用報告範本建立的報告。報告範本包括：

`RESOURCE_COMPLIANCE_REPORT | CONTROL_COMPLIANCE_REPORT | BACKUP_JOB_REPORT | COPY_JOB_REPORT | RESTORE_JOB_REPORT`

類型：字串

必要：是

Accounts

這些是要包含在報告中的帳戶。

類型：字串陣列

必要：否

FrameworkArns

報告涵蓋之架構的 Amazon Resource Name (ARN)。

類型：字串陣列

必要：否

NumberOfFrameworks

報告涵蓋的框架數量。

類型：整數

必要：否

OrganizationUnits

這些是要包含在報告中的組織單位。

類型：字串陣列

必要：否

Regions

這些是要包含在報告中的區域。

類型：字串陣列

必要：否

另請參閱

如需在其中一個特定語言 AWS SDK 中使用此 API 的詳細資訊，請參閱下列內容：

- AWS SDK for C++
- AWS SDK for Go
- AWS SDK for Java V2 的軟件
- AWS 適用於紅寶石 V3 的 SDK

RestoreJobCreator

服務： AWS Backup

包含 AWS Backup 用於啟動還原工作之還原測試計畫的相關資訊。

目錄

RestoreTestingPlanArn

可唯一識別還原測試計畫的 Amazon Resource Name (ARN)。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreJobsListMember

服務： AWS Backup

包含還原工作的相關中繼資料。

目錄

AccountId

擁有還原工作的帳戶 ID。

類型：字串

模式：`^[0-9]{12}$`

必要：否

BackupSizeInBytes

所還原資源的大小，以位元組為單位。

類型：Long

必要：否

CompletionDate

還原復原點之作業的完成日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。`CompletionDate` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

CreatedBy

包含有關建立還原工作的識別資訊。

類型：RestoreJobCreator 物件

必要：否

CreatedResourceArn

可唯一識別資源的 Amazon Resource Name (ARN)。ARN 的格式取決於資源類型。

類型：字串

必要：否

CreationDate

建立還原作業時的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

DeletionStatus

此會記錄還原測試所產生的資料狀態。此狀態可能是 Deleting、Failed 或 Successful。

類型：字串

有效值:DELETING | FAILED | SUCCESSFUL

必要：否

DeletionStatusMessage

此會說明還原工作刪除狀態。

類型：字串

必要：否

ExpectedCompletionTimeMinutes

還原復原點之工作預計所需的時間 (分鐘)。

類型：Long

必要：否

IamRoleArn

指定用來建立目標復原點的 IAM 角色 ARN；例如 arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：否

PercentDone

包含查詢作業狀態時，作業的預估完成百分比。

類型：字串

必要：否

RecoveryPointArn

可唯一識別復原點的 ARN；例如 `arn:aws:backup:us-east-1:123456789012:recovery-point:1EB3B5E7-9EB0-435A-A80B-108B488B0D45`。

類型：字串

必要：否

RecoveryPointCreationDate

復原點的建立日期。

類型：Timestamp

必要：否

ResourceType

所列出還原工作的資源類型。例如 Amazon Elastic Block Store (Amazon EBS) 磁碟區或 Amazon Relational Database Service (Amazon RDS) 資料庫。對於 Windows 磁碟區陰影複製服務 (VSS) 備份，唯一支援的資源類型為 Amazon EC2。

類型：字串

模式：`^[a-zA-Z0-9\-\_\.]{1,50}$`

必要：否

RestoreJobId

可唯一識別還原復原點的工作。

類型：字串

必要：否

Status

狀態碼，指定還原復原點之工作 (由 AWS Backup 所起始) 的狀態。

類型：字串

有效值:PENDING | RUNNING | COMPLETED | ABORTED | FAILED

必要：否

StatusMessage

說明還原復原點之工作狀態的詳細訊息。

類型：字串

必要：否

ValidationStatus

這是在指定的還原工作上執行驗證的狀態。

類型：字串

有效值:FAILED | SUCCESSFUL | TIMED_OUT | VALIDATING

必要：否

ValidationStatusMessage

此描述了在指定的還原工作上執行驗證的狀態。

類型：字串

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreJobSummary

服務： AWS Backup

這是最近 30 天內建立或執行的還原工作摘要。

此傳回的摘要可能包含下列項目：
Region、Account，State、ResourceType、MessageCategory、StartTime、EndTime 和包含工作的計數。

目錄

AccountId

擁有摘要中工作的帳戶 ID。

類型：字串

模式：`^[0-9]{12}$`

必要：否

Count

作為工作摘要中工作數量的值。

類型：整數

必要：否

EndTime

工作結束時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

Region

工作摘要中的 AWS 區域。

類型：字串

必要：否

ResourceType

此值為所指定資源類型的工作計數。此請求 GetSupportedResourceTypes 會傳回所支援資源類型的字串。

類型：字串

模式：^[a-zA-Z0-9\-_\.]{1,50}$

必要：否

StartTime

工作開始時間的時間值 (以數字格式表示)。

此值採用 Unix 格式、國際標準時間 (UTC)，且精確至毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

State

此值是具有指定狀態之工作的工作計數。

類型：字串

有效值:CREATED | PENDING | RUNNING | ABORTED | COMPLETED | FAILED | AGGREGATE_ALL | ANY

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingPlanForCreate

服務： AWS Backup

其中包含有關還原測試計畫的中繼資料。

目錄

RecoveryPointSelection

必要：演算法；必要：復原點類型；IncludeVaults (一或多個)。選用：SelectionWindowDays (如果未指定，則為「30」)；ExcludeVaults (選擇器清單)，如果未列出，則預設為空白清單。

類型：RestoreTestingRecoveryPointSelection 物件

必要：是

RestoreTestingPlanName

RestoreTestingPlanName 是唯一的字串，也就是還原測試計畫的名稱。您無法在建立後變更此名稱，其必須只包含英數字元和底線。

類型：字串

必要：是

ScheduleExpression

執行還原測試計畫時，指定時區中的 CRON 表達式。

類型：字串

必要：是

ScheduleExpressionTimezone

選用。這是設定排程運算式的時區。ScheduleExpressions 預設會以 UTC 格式表示。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowHours

預設為 24 小時。

在排程還原測試後到取消工作 (如未成功開始) 前的時數值。此值是選用的。如果包含此值，則此參數的最大值為 168 小時 (一週)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingPlanForGet

服務： AWS Backup

其中包含有關還原測試計畫的中繼資料。

目錄

CreationTime

建立還原測試計畫的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：是

RecoveryPointSelection

用於指派一組資源的指定條件，例如復原點類型或備份保存庫。

類型：RestoreTestingRecoveryPointSelection 物件

必要：是

RestoreTestingPlanArn

可唯一識別還原測試計畫的 Amazon Resource Name (ARN)。

類型：字串

必要：是

RestoreTestingPlanName

這是還原測試計畫的名稱。

類型：字串

必要：是

ScheduleExpression

執行還原測試計畫時，指定時區中的 CRON 表達式。

類型：字串

必要：是

CreatorRequestId

此可識別請求且允許重試失敗的請求，而不會有兩次執行操作的風險。如果請求包含符合現有備份計畫的 CreatorRequestId，則會傳回該計畫。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

LastExecutionTime

前次使用指定的還原測試計畫執行還原測試的時間。日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastExecutionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

LastUpdateTime

還原測試計畫的更新日期和時間。此更新以 Unix 格式和國際標準時間 (UTC) 顯示。LastUpdateTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

ScheduleExpressionTimezone

選用。這是設定排程運算式的時區。ScheduleExpressions 預設會以 UTC 格式表示。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowHours

預設為 24 小時。

在排程還原測試後到取消工作 (如未成功開始) 前的時數值。此值是選用的。如果包含此值，則此參數的最大值為 168 小時 (一週)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingPlanForList

服務： AWS Backup

其中包含有關還原測試計畫的中繼資料。

目錄

CreationTime

建立還原測試計畫的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：是

RestoreTestingPlanArn

可唯一識別還原測試計畫的 Amazon Resource Name (ARN)。

類型：字串

必要：是

RestoreTestingPlanName

這是還原測試計畫的名稱。

類型：字串

必要：是

ScheduleExpression

執行還原測試計畫時，指定時區中的 CRON 表達式。

類型：字串

必要：是

LastExecutionTime

前次使用指定的還原測試計畫執行還原測試的時間。日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。LastExecutionDate 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

LastUpdateTime

還原測試計畫的更新日期和時間。此更新以 Unix 格式和國際標準時間 (UTC) 顯示。`LastUpdateTime` 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：否

ScheduleExpressionTimezone

選用。這是設定排程運算式的時區。ScheduleExpressions 預設會以 UTC 格式表示。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowHours

預設為 24 小時。

在排程還原測試後到取消工作 (如未成功開始) 前的時數值。此值是選用的。如果包含此值，則此參數的最大值為 168 小時 (一週)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingPlanForUpdate

服務： AWS Backup

其中包含有關還原測試計畫的中繼資料。

目錄

RecoveryPointSelection

需要：`Algorithm`；`RecoveryPointTypes`；`IncludeVaults` (一或多個)。

選用：SelectionWindowDays (如果未指定，則為「30」)；`ExcludeVaults` (如果未列出，則預設為空白清單)。

類型：RestoreTestingRecoveryPointSelection 物件

必要：否

ScheduleExpression

執行還原測試計畫時，指定時區中的 CRON 表達式。

類型：字串

必要：否

ScheduleExpressionTimezone

選用。這是設定排程運算式的時區。ScheduleExpressions 預設會以 UTC 格式表示。您可以將此參數修改為指定的時區。

類型：字串

必要：否

StartWindowHours

預設為 24 小時。

在排程還原測試後到取消工作 (如未成功開始) 前的時數值。此值是選用的。如果包含此值，則此參數的最大值為 168 小時 (一週)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingRecoveryPointSelection

服務： AWS Backup

必要：演算法；必要：復原點類型；IncludeVaults (一或多個)。選用：SelectionWindowDays (如果未指定，則為「30」)；ExcludeVaults (選擇器清單)，如果未列出，則預設為空白清單。

目錄

Algorithm

可接受的值包括「LATEST_WITHIN_WINDOW」或「RANDOM_WITHIN_WINDOW」

類型：字串

有效值:`LATEST_WITHIN_WINDOW | RANDOM_WITHIN_WINDOW`

必要：否

ExcludeVaults

接受的值包括特定的 ARN 或選擇器清單。如果沒有列出，則預設為空白清單。

類型：字串陣列

必要：否

IncludeVaults

接受的值包括萬用字元 ["*"] 或依照特定的 ARN 或 ARN 萬用字元替換 ["arn:aws:backup:us-west-2:123456789012:backup-vault:asdf", ...] ["arn:aws:backup:*:*:backup-vault:asdf-*", ...]

類型：字串陣列

必要：否

RecoveryPointTypes

這些是復原點的類型。

類型：字串陣列

有效值:`CONTINUOUS | SNAPSHOT`

必要：否

SelectionWindowDays

接受的值是從 1 到 365 的整數。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingSelectionForCreate

服務： AWS Backup

其中包含有關特定還原測試選擇的中繼資料。

ProtectedResourceType 是必填欄位，例如 Amazon EBS 或 Amazon EC2。

其中包括 `RestoreTestingSelectionName`、`ProtectedResourceType` 以及下列其中一項：

- `ProtectedResourceArns`
- `ProtectedResourceConditions`

每個受保護的資源類型可以有一個單一值。

還原測試選擇可以包含 `ProtectedResourceArns` 和 `ProtectedResourceConditions` 的萬用字元值 (「*」)。或者，您可以在 `ProtectedResourceArns` 中包含最多 30 個特定受保護的資源 ARN。

`ProtectedResourceConditions` 範例包括作為 `StringEquals` 和 `StringNotEquals`。

目錄

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)，AWS Backup 可用此角色來建立目標資源；例如：`arn:aws:iam::123456789012:role/S3Access`。

類型：字串

必要：是

ProtectedResourceType

還原測試選擇中包含的 AWS 資源類型；例如，Amazon EBS 磁碟區或 Amazon RDS 資料庫。

接受的支援資源類型包含：

- `Aurora` 代表 Amazon Aurora
- `DocumentDB` 代表 Amazon DocumentDB (with MongoDB compatibility)
- `DynamoDB` 代表 Amazon DynamoDB
- `EBS` 代表 Amazon Elastic Block Store

- EC2 代表 Amazon Elastic Compute Cloud
- EFS 代表 Amazon Elastic File System
- FSx 代表 Amazon FSx
- Neptune 代表 Amazon Neptune
- RDS 代表 Amazon Relational Database Service
- 適用於 Amazon S3 的 S3

類型：字串

必要：是

RestoreTestingSelectionName

這是屬於相關還原測試計畫之還原測試選擇的不重複名稱。

類型：字串

必要：是

ProtectedResourceArns

可以按每個受保護資源特定的 ARN (例如 ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."])，也可以按萬用字元：ProtectedResourceArns: ["*"] 加以篩選，但不能同時使用兩者。

類型：字串陣列

必要：否

ProtectedResourceConditions

如果您已在 ProtectedResourceArns 中包含萬用字元，則可以包含資源條件，例如 ProtectedResourceConditions: { StringEquals: [{ key: "XXXX", value: "YYYY" }]。

類型：ProtectedResourceConditions 物件

必要：否

RestoreMetadataOverrides

您可以將參數 RestoreMetadataOverrides 包含在 RestoreTestingSelection 的主體中，來覆寫某些還原中繼資料索引鍵。索引鍵值不區分大小寫。

請參閱還原測試推斷中繼資料的完整清單。

類型：字串到字串映射

必要：否

ValidationWindowHours

這是可對資料執行驗證指令碼的時數 (1 到 168)。在驗證指令碼完成或指定保留期間結束時 (以先到者為準)，資料將遭到刪除。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingSelectionForGet

服務： AWS Backup

其中包含有關還原測試選擇的中繼資料。

目錄

CreationTime

建立還原測試選擇的日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：是

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)，AWS Backup 可用此角色來建立目標資源；例如：arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：是

ProtectedResourceType

資源測試選擇中包含的 AWS 資源類型；例如，Amazon EBS 磁碟區或 Amazon RDS 資料庫。

類型：字串

必要：是

RestoreTestingPlanName

RestoreTestingPlanName 是唯一的字串，也就是還原測試計畫的名稱。

類型：字串

必要：是

RestoreTestingSelectionName

這是屬於相關還原測試計畫之還原測試選擇的不重複名稱。

類型：字串

必要：是

CreatorRequestId

此可識別請求且允許重試失敗的請求，而不會有兩次執行操作的風險。如果請求包含符合現有備份計畫的 CreatorRequestId，則會傳回該計畫。此為選用參數。

如果使用，此參數必須包含 1 至 50 個英數字元或 '-_'。字元。

類型：字串

必要：否

ProtectedResourceArns

您可以包含 ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."] 之類的特定 ARN，或您可以包含萬用字元:ProtectedResourceArns: ["*"]，但不能同時包含兩者。

類型：字串陣列

必要：否

ProtectedResourceConditions

在資源測試選擇中，此參數會依特定條件 (例如 StringEquals 或 StringNotEquals) 進行篩選。

類型：ProtectedResourceConditions 物件

必要：否

RestoreMetadataOverrides

您可以將參數 RestoreMetadataOverrides 包含在 RestoreTestingSelection 的主體中，來覆寫某些還原中繼資料索引鍵。索引鍵值不區分大小寫。

請參閱還原測試推斷中繼資料的完整清單。

類型：字串到字串映射

必要：否

ValidationWindowHours

這是可對資料執行驗證指令碼的時數 (1 到 168)。在驗證指令碼完成或指定保留期間結束時 (以先到者為準)，資料將遭到刪除。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingSelectionForList

服務： AWS Backup

其中包含有關還原測試選擇的中繼資料。

目錄

CreationTime

此為還原測試選擇的建立日期和時間，以 Unix 格式和國際標準時間 (UTC) 顯示。CreationTime 的值精確到毫秒。例如，值 1516925490.087 代表 2018 年 1 月 26 日星期五上午 12 點 11 分 30.087 秒。

類型：Timestamp

必要：是

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)，AWS Backup 可用此角色來建立目標資源；例如：arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：是

ProtectedResourceType

還原測試選擇中包含的 AWS 資源類型；例如，Amazon EBS 磁碟區或 Amazon RDS 資料庫。

類型：字串

必要：是

RestoreTestingPlanName

不重複字串，也就是還原測試計畫的名稱。

此名稱建立後就不可變更。此名稱必須包含英數字元和底線。長度上限為 50。

類型：字串

必要：是

RestoreTestingSelectionName

還原測試選擇的不重複名稱。

類型：字串

必要：是

ValidationWindowHours

此值代表在還原測試之後資料的保留時間 (以小時為單位)，以便完成選用驗證。

接受的值是介於 0 到 168 之間的整數 (相當於七天的時數)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

RestoreTestingSelectionForUpdate

服務： AWS Backup

其中包含有關還原測試選擇的中繼資料。

目錄

IamRoleArn

IAM 角色的 Amazon Resource Name (ARN)，AWS Backup 可用此角色來建立目標資源；例如：arn:aws:iam::123456789012:role/S3Access。

類型：字串

必要：否

ProtectedResourceArns

您可以包含 ProtectedResourceArns: ["arn:aws:...", "arn:aws:..."] 之類的特定 ARN 清單，或您可以包含萬用字元：ProtectedResourceArns: ["*"]，但不能同時包含兩者。

類型：字串陣列

必要：否

ProtectedResourceConditions

您使用標籤為還原測試計畫中的資源定義的條件清單。

例如："StringEquals": { "Key": "aws:ResourceTag/CreatedByCryo", "Value": "true" },。條件運算子名稱區分大小寫。

類型：ProtectedResourceConditions 物件

必要：否

RestoreMetadataOverrides

您可以將參數 RestoreMetadataOverrides 包含在 RestoreTestingSelection 的主體中，來覆寫某些還原中繼資料索引鍵。索引鍵值不區分大小寫。

請參閱還原測試推斷中繼資料的完整清單。

類型：字串到字串映射

必要：否

ValidationWindowHours

此值代表在還原測試之後資料的保留時間 (以小時為單位)，以便完成選用驗證。

接受的值是介於 0 到 168 之間的整數 (相當於七天的時數)。

類型：整數

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS 開發套件
- 適用於 Go 的 AWS 開發套件
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS 開發套件第 3 版

AWS Backup gateway

AWS Backup gateway 支援下列資料類型：

- BandwidthRateLimitInterval
- Gateway
- GatewayDetails
- Hypervisor
- HypervisorDetails
- MaintenanceStartTime
- Tag
- VirtualMachine
- VirtualMachineDetails
- VmwareTag
- VmwareToAwsTagMapping

BandwidthRateLimitInterval

服務： AWS Backup gateway

說明閘道的頻寬速率限制間隔。頻寬速率限制排程由一或多個頻寬速率限制間隔組成。頻寬速率限制間隔定義了一週中一或多天內的一段時間，在此期間內，會指定頻寬速率限制以供上傳、下載或兩者使用。

目錄

DaysOfWeek

頻寬速率限制間隔的週內日期元件，以 0 到 6 的序數表示，其中 0 代表星期日，6 代表星期六。

類型：整數陣列

陣列成員：項目數下限為 1。項目數上限為 7。

有效範圍：最小值為 0。最大值為 6。

必要：是

EndHourOfDay

一天中結束帶寬速率限制間隔的時間 (小時)。

類型：整數

有效範圍：最小值為 0。最大值為 23。

必要：是

EndMinuteOfHour

結束頻寬速率限制間隔的時間 (分)。

> **Important**
> 頻寬速率限制間隔會在該分鐘結束時終止。若要在一小時結束時結束間隔，請使用 59 值。

類型：整數

有效範圍：最小值為 0。最大值為 59。

必要：是

StartHourOfDay

開始頻寬速率限制間隔的時間 (小時)。

類型：整數

有效範圍：最小值為 0。最大值為 23。

必要：是

StartMinuteOfHour

開始頻寬速率限制間隔的時間 (分)。間隔會始於該分鐘的開頭。若要整點時精確地開始一個間隔，請使用 0 值。

類型：整數

有效範圍：最小值為 0。最大值為 59。

必要：是

AverageUploadRateLimitInBitsPerSec

頻寬速率限制間隔的平均上傳速率限制元件，以每秒位元數為單位。如果未設定上傳速率限制，則回應中不會顯示此欄位。

> **Note**
>
> 對於 Backup Gateway，最小值為 `(Value)`。

類型：Long

有效範圍：最小值為 51200。最大值為 8000000000000。

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK

- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Gateway

服務： AWS Backup gateway

閘道是在客戶網路上執行的 AWS Backup 閘道設備，可為 AWS 雲端中的備份儲存提供流暢的連線。

目錄

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 `ListGateways` 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

GatewayDisplayName

閘道的顯示名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

GatewayType

閘道的類型。

類型：字串

有效值: `BACKUP_VM`

必要：否

HypervisorId

閘道的 hypervisor ID。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

必要：否

LastSeenTime

AWS Backup 閘道上次與閘道通訊的時間，以 Unix 格式和 UTC 時間顯示。

類型：Timestamp

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

GatewayDetails

服務： AWS Backup gateway

閘道的詳細資訊。

目錄

GatewayArn

閘道的 Amazon Resource Name (ARN)。使用 `ListGateways` 操作即可傳回您帳戶和 AWS 區域的閘道清單。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

GatewayDisplayName

閘道的顯示名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

GatewayType

閘道類型的類型。

類型：字串

有效值: `BACKUP_VM`

必要：否

HypervisorId

閘道的 hypervisor ID。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

必要：否

LastSeenTime

顯示 AWS Backup 閘道上次與雲端通訊的詳細資訊，以 Unix 格式和 UTC 時間顯示。

類型：Timestamp

必要：否

MaintenanceStartTime

傳回閘道的每週維護開始時間，包括星期幾和時間。請注意，該值是以閘道的時區表示。可以是每週或每月。

類型：MaintenanceStartTime 物件

必要：否

NextUpdateAvailabilityTime

顯示閘道下次更新可用時間的詳細資訊。

類型：Timestamp

必要：否

VpcEndpoint

虛擬私有雲端 (VPC) 端點的 DNS 名稱，閘道可用其連線至雲端以備份閘道。

類型：字串

長度限制：長度下限為 1。長度上限為 255。

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK

- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Hypervisor

服務： AWS Backup gateway

代表閘道將連線至之 hypervisor 的許可。

Hypervisor 是一種硬體、軟體或韌體，可建立並管理虛擬機器，並將資源配置給虛擬機器。

目錄

Host

Hypervisor 的伺服器主機。這可以是 IP 地址或完整網域名稱 (FQDN)。

類型：字串

長度限制：長度下限為 3。長度上限為 128。

模式：`^.+$`

必要：否

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

KmsKeyArn

AWS Key Management Service 用來加密 hypervisor 的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必要：否

Name

Hypervisor 的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

State

Hypervisor 的狀態。

類型：字串

有效值: `PENDING | ONLINE | OFFLINE | ERROR`

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

HypervisorDetails

服務： AWS Backup gateway

這些是所指定 hypervisor 的詳細資訊。Hypervisor 是一種硬體、軟體或韌體，可建立並管理虛擬機器，並將資源配置給虛擬機器。

目錄

Host

Hypervisor 的伺服器主機。這可以是 IP 地址或完整網域名稱 (FQDN)。

類型：字串

長度限制：長度下限為 3。長度上限為 128。

模式：`^.+$`

必要：否

HypervisorArn

Hypervisor的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

KmsKeyArn

用於加密 hypervisor的 AWS KMS Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^(^arn:(aws|aws-cn|aws-us-gov):kms:([a-zA-Z0-9-]+):([0-9]+):(key|alias)/(\S+)$)|(^alias/(\S+)$)$`

必要：否

LastSuccessfulMetadataSyncTime

這是最近一次成功同步中繼資料的時間。

類型：Timestamp

必要：否

LatestMetadataSyncStatus

這是所表示中繼資料同步的最新狀態。

類型：字串

有效值: CREATED | RUNNING | FAILED | PARTIALLY_FAILED | SUCCEEDED

必要：否

LatestMetadataSyncStatusMessage

這是所表示中繼資料同步的最新狀態。

類型：字串

必要：否

LogGroupArn

所請求日誌中閘道群組的 Amazon Resource Name (ARN)。

類型：字串

長度限制：長度下限為 0。長度上限為 2048。

模式：^$|^arn:(aws|aws-cn|aws-us-gov):logs:([a-zA-Z0-9-]+):([0-9]+):log-group:[a-zA-Z0-9_\-\/\.]+:*$

必要：否

Name

這是所指定 hypervisor 的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[a-zA-Z0-9-]*$

必要：否

State

這是所指定 hypervisor 的目前狀態。

可能的狀態為 PENDING、ONLINE、OFFLINE 或 ERROR。

類型：字串

有效值: PENDING | ONLINE | OFFLINE | ERROR

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

MaintenanceStartTime

服務： AWS Backup gateway

這是閘道的每週維護開始時間，包括星期幾和時間。請注意，該值是以閘道的時區表示。可以是每週或每月。

目錄

HourOfDay

維護開始時間的小時元件表示為 hh，其中 hh 是小時 (0 到 23)。一天中的時間以閘道的時區表示。

類型：整數

有效範圍：最小值為 0。最大值為 23。

必要：是

MinuteOfHour

維護開始時間的分鐘元件表示為 mm，其中 mm 是分鐘 (0 至 59)。小時的分鐘以閘道的時區表示。

類型：整數

有效範圍：最小值為 0。最大值為 59。

必要：是

DayOfMonth

維護開始時間的當月日期元件，以介於 1 至 28 的序號表示，其中 1 表示當月的第一天，28 表示當月的最後一天。

類型：整數

有效範圍：最小值為 1。最大值為 31。

必要：否

DayOfWeek

介於 0 到 6 之間的序數，代表星期幾，其中 0 代表星期日，6 代表星期六。星期幾以閘道的時區表示。

類型：整數

有效範圍：最小值為 0。最大值為 6。

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

Tag

服務： AWS Backup gateway

可用來管理、篩選和搜尋資源的鍵值對。允許使用的字元包括 UTF-8 字母、數字、空格，以及下列字元：+ - = . _ : /。

目錄

Key

標籤鍵值對的金鑰部分。索引鍵無法以 aws: 開頭。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$

必要：是

Value

標籤鍵值對的值部分。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：^[^\x00]*$

必要：是

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

VirtualMachine

服務： AWS Backup gateway

位於 hypervisor 上的虛擬機器。

目錄

HostName

虛擬機器的主機名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[a-zA-Z0-9-]*$

必要：否

HypervisorId

虛擬機器的 hypervisor ID。

類型：字串

必要：否

LastBackupDate

備份虛擬機器的最新日期，以 Unix 格式和 UTC 時間顯示。

類型：Timestamp

必要：否

Name

虛擬機器的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：^[a-zA-Z0-9-]*$

必要：否

Path

虛擬機器的路徑。

類型：字串

長度限制：長度下限為 1。長度上限為 4096。

模式：`^[^\x00]+$`

必要：否

ResourceArn

虛擬機器的 Amazon Resource Name (ARN)。例如 `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

VirtualMachineDetails

服務： AWS Backup gateway

您的 `VirtualMachine` 物件，依其 Amazon Resource Name (ARN) 排序。

目錄

HostName

虛擬機器的主機名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

HypervisorId

虛擬機器的 hypervisor ID。

類型：字串

必要：否

LastBackupDate

備份虛擬機器的最新日期，以 Unix 格式和 UTC 時間顯示。

類型：Timestamp

必要：否

Name

虛擬機器的名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 100。

模式：`^[a-zA-Z0-9-]*$`

必要：否

Path

虛擬機器的路徑。

類型：字串

長度限制：長度下限為 1。長度上限為 4096。

模式：`^[^\x00]+$`

必要：否

ResourceArn

虛擬機器的 Amazon Resource Name (ARN)。例如 `arn:aws:backup-gateway:us-west-1:0000000000000:vm/vm-0000ABCDEFGIJKL`。

類型：字串

長度限制：長度下限為 50。長度上限為 500。

模式：`^arn:(aws|aws-cn|aws-us-gov):backup-gateway(:[a-zA-Z-0-9]+){3}\/[a-zA-Z-0-9]+$`

必要：否

VmwareTags

這些是與指定虛擬機器相關聯的 VMware 標籤詳細資訊。

類型：VmwareTag 物件陣列

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

VmwareTag

服務： AWS Backup gateway

VMware 標籤是連接至特定虛擬機器的標籤。標籤為鍵值對，可用於管理、篩選和搜尋資源。

VMware 標籤的內容可以與 AWS 標籤進行比對。

目錄

VmwareCategory

這是 VMware 的類別。

類型：字串

長度限制：長度下限為 1。長度上限為 80。

必要：否

VmwareTagDescription

這是使用者定義的 VMware 標籤描述。

類型：字串

必要：否

VmwareTagName

這是 VMware 標籤的使用者定義名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 80。

必要：否

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK

- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

VmwareToAwsTagMapping

服務： AWS Backup gateway

這會顯示 VMware 標籤與對應 AWS 標籤的對應。

目錄

AwsTagKey

AWS 標籤鍵值對的金鑰部分。

類型：字串

長度限制：長度下限為 1。長度上限為 128。

模式：`^([\p{L}\p{Z}\p{N}_.:/=+\-@]*)$`

必要：是

AwsTagValue

AWS 標籤鍵值對的值部分。

類型：字串

長度限制：長度下限為 0。長度上限為 256。

模式：`^[^\x00]*$`

必要：是

VmwareCategory

這是 VMware 的類別。

類型：字串

長度限制：長度下限為 1。長度上限為 80。

必要：是

VmwareTagName

這是 VMware 標籤的使用者定義名稱。

類型：字串

長度限制：長度下限為 1。長度上限為 80。

必要：是

另請參閱

如需在語言特定的 AWS 開發套件之一中使用此 API 的詳細資訊，請參閱下列說明：

- 適用於 C++ 的 AWS SDK
- 適用於 Go 的 AWS SDK
- 適用於 Java 的 AWS 開發套件第 2 版
- 適用於 Ruby 的 AWS SDK 第 3 版

常見參數

以下清單內含所有動作用來簽署 Signature 第 4 版請求的參數以及查詢字串。任何專屬於特定動作的參數則列於該動作的主題中。如需有關 Signature 第 4 版的詳細資訊，請參閱《IAM 使用者指南》中的簽署 AWS API 請求。

Action

要執行的動作。

類型：字串

必要：是

Version

編寫請求所憑藉的 API 版本，以 YYYY-MM-DD 格式表示。

類型：字串

必要：是

X-Amz-Algorithm

建立請求簽章時所使用的雜湊演算法。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

有效值: AWS4-HMAC-SHA256

必要：有條件

X-Amz-Credential

憑證範圍值，此為一個字串，其中包含您的存取金鑰、日期、您的目標區域、您請求的服務，以及終止字串 (“aws4_request”)。值以下列格式表示：access_key/YYYYMMDD/region/service/aws4_request。

如需詳細資訊，請參閱《IAM 使用者指南》中的建立已簽署的 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-Date

用來建立簽署的日期。格式必須是 ISO 8601 基本格式 (YYYYMMDD'T'HHMMSS'Z')。例如，以下日期時間是有效的 X-Amz-Date 值：20120325T120000Z

條件： 對所有請求而言，X-Amz-Date 皆為選用，可用來覆寫用於簽署請求的日期。如果規定日期標頭採用 ISO 8601 基本格式，則不需要 X-Amz-Date。當使用 X-Amz-Date 時，其一律會覆寫日期標頭的值。如需詳細資訊，請參閱《IAM 使用者指南》中的 AWS API 請求簽章的元素。

類型：字串

必要：有條件

X-Amz-Security-Token

透過呼叫 AWS Security Token Service (AWS STS) 所取得的臨時安全字符。如需支援 AWS STS 的臨時安全憑證的服務清單，請參閱《IAM 使用者指南》中的可搭配 IAM 運作的 AWS 服務。

條件：如果您使用 AWS STS 的臨時安全憑證，則必須納入安全字符。

類型：字串

必要：有條件

X-Amz-Signature

指定從要簽署的字串和衍生的簽署金鑰中計算出的十六進位編碼簽章。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

X-Amz-SignedHeaders

指定納入作為標準請求一部分的所有 HTTP 標頭。如需有關指定已簽署的標頭之詳細資訊，請參閱《IAM 使用者指南》中的建立已簽署的 AWS API 請求。

條件：當您在查詢字串中而非 HTTP 授權標頭中納入驗證資訊時，應指定此參數。

類型：字串

必要：有條件

常見錯誤

本部分列出所有 AWS 服務 API 動作的常見錯誤。如需此服務之 API 動作的特定錯誤，請參閱該 API 動作的主題。

AccessDeniedException

您沒有足夠存取權可執行此動作。

HTTP 狀態碼：400

IncompleteSignature

請求簽署不符合 AWS 標準。

HTTP 狀態碼：400

InternalFailure

由於不明的錯誤、例外狀況或故障，處理請求失敗。

HTTP 狀態碼：500

InvalidAction

請求的動作或操作無效。確認已正確輸入動作。

HTTP 狀態碼：400

InvalidClientTokenId

提供的 X.509 憑證或 AWS 存取金鑰 ID 不存在於我們的記錄中。

HTTP 狀態碼：403

NotAuthorized

您沒有執行此動作的許可。

HTTP 狀態碼：400

OptInRequired

AWS 存取金鑰 ID 需要訂閱服務。

HTTP 狀態碼：403

RequestExpired

請求送達服務已超過戳印日期於請求上之後的 15 分鐘，或者已超過請求過期日期之後的 15 分鐘 (例如預先簽章的 URL)，或者請求上的日期戳印在未來將超過 15 分鐘。

HTTP 狀態碼：400

ServiceUnavailable

由於伺服器暫時故障，請求失敗。

HTTP 狀態碼：503

ThrottlingException

由於請求調節，因此請求遭到拒絕。

HTTP 狀態碼：400

ValidationError

輸入不符合 AWS 服務規定的限制。

HTTP 狀態碼：400

AWS 詞彙表

如需最新的 AWS 術語，請參閱《AWS 詞彙表 參考》中的 AWS 詞彙表。

的文件歷史記錄 AWS Backup

- API 版本：2023 年 12 月 6 日
- 最近的文件更新日期：2024 年 1 月 10 日

下表列出了自 2019 年 1 月至今服務 AWS Backup 推出以來的所有啟動。如需本文件的更新通知，您可以訂閱上文的 RSS 摘要。

變更	描述	日期
對於 ON FlexGroup TAP 磁碟區 FSx 的 Backup 與還原支援	AWS Backup 現在大部分支援 ONTAP FlexGroup 磁碟區的 FSx 備份和還原。 AWS 區域 如需詳細資訊，請參閱還原 Amazon FSx 檔案系統 .	2024 年 1 月 10 日
對 SAP HANA HA 備份與還原的支援	AWS Backup 現在在 Amazon EC2 備份和還原上提供支援 SAP HANA 高可用性資料庫。 如需詳細資訊，請參閱 Amazon EC2 備份上的 SAP HANA 和還原 SAP HANA 高可用性系統	2023 年 12 月 21 日
AWS Backup 還原測試的 Audit Manager 控制項	AWS Backup Audit Manager 現在提供控制項，讓資源符合目標的還原時間，以協助監視還原時間。此控制項會檢查資源的還原時間是否符合目標持續時間。 如需詳細資訊，請參閱 控制與補救 及 稽核還原測試。	2023 年 12 月 18 日

變更	描述	日期
支援 Amazon EBS 不常用儲存	AWS Backup 現在支援將 EBS 備份從暖儲存轉換為冷儲存。如需詳細資訊，請參閱 • 適用於不常用儲存的 Amazon EBS 封存層 • 生命週期和儲存層 • 建立備份計畫	2023 年 11 月 27 日
導入還原測試	AWS Backup 引入還原測試，帶來還原可行性的自動化和定期評估，以及監視還原工作持續時間的能力。 如需詳細資訊，請參閱還原測試。	2023 年 11 月 27 日

變更	描述	日期
已更新 AWS 受管政策	AWS Backup 添加了權限`ec2:DescribeSnapshotTierStatus` 和`ec2:ModifySnapshotTier` 受管理策略`AWSBackupServiceRolePolicyForBackups` 和`AWSBackupServiceLinkedRolePolicyForBackup` 。AWS Backup 還添加了權限`ec2:DescribeSnapshotTierStatus` 和`ec2:RestoreSnapshotTier` 託管策略`AWSBackupServiceRolePolicyForRestores` 。 使用者需要這些許可，才能選擇將存放的 Amazon EBS 資源轉換為存檔儲存，以及從存檔儲存層還原資源。 AWS Backup 如需詳細資訊，請參閱政策更新。	2023 年 11 月 27 日

變更	描述	日期
新增傳遞角色許可以支援還原測試。	AWS Backup 已新增`restore-testing.backup.amazonaws.com` 至`IamPassRolePermissions` 和`IamCreateServiceLinkedRolePermissions` 。這項新增功能對 AWS Backup 於代表客戶進行還原測試是必要的。	2023 年 11 月 27 日
已新增服務連結角色	AWS Backup 已新增名為的新服務連結角色 `AWSServiceRoleForBackupRestoreTesting` ，提供備份權限以進行還原測試。 這個新的服務連結角色提 AWS Backup 供執行還原測試所需的權限。這些許可包括要在還原測試中包含之下列服務的動作 `list, read, and write` ：Aurora、DocumentDB、DynamoDB、Amazon EBS、Amazon EC2、Amazon EFS、FSx for Lustre、FSx for Windows File Server、FSx for ONTAP、FSx for OpenZFS、Amazon Neptune、Amazon RDS 和 Amazon S3。	2023 年 11 月 27 日

變更	描述	日期
AWS Backup 主控台中的新工作指標儀表板	AWS Backup 主控台現在會顯示工作儀表板，透過全新的視覺化使用者介面，以及所 AWS Backup支援服務的彙總備份、複製和還原指標，簡化大規模備份健康狀態監控。 工作儀表板可在 AWS Backup Audit Manager 使用的所有區域中使用。 未列出的區域仍然可以存取CloudWatch 儀表板。 如需詳細資訊，請參閱 AWS Backup 主控台儀表板。	2023 年 11 月 15 日
支援巢狀堆疊備份	AWS Backup 擴大了對 AWS CloudFormation 資源備份的支持。您的 CloudFormation 應用程式堆疊中有巢狀堆疊的應用程式堆疊可以包含在備份中。 如需詳細資訊，請參閱 CloudFormation 堆疊備份。	2023 年 11 月 8 日
中國 (北京) 和中國 (寧夏) 支援 Amazon S3。	AWS Backup Amazon S3 的支援現已在中國 (北京) 和中國 (寧夏) 區域提供。 如需詳細資訊，請參閱各區域的功能可用性。	2023 年 10 月 26 日

變更	描述	日期
Support Amazon Aurora 持續備份和 P oint-in-time 還原	AWS Backup 現在支援 Aurora 資源的連續備份和 point-in-time 還原 (PITR)。 如需詳細資訊，請參閱持續備份和 P oint-in-time 復原。	2023 年 9 月 7 日
AWS CloudFormation 堆棧支持排除資源	AWS Backup 現在支援從 AWS CloudFormation 堆疊中排除所選資源的選項。 如需詳細資訊，請參閱 AWS CloudFormation 堆疊備份。	2023 年 9 月 6 日
備份計畫規則引入時區彈性	AWS Backup 計劃規則現在可以具有備份窗口的指定時區。 如需詳細資訊，請參閱管理備份計畫。	2023 年 8 月 28 日
AWS Backup 以色列 (特拉維夫) 地區現已推出	新的以色列（特拉維夫）地區現已提供許多 AWS Backup 功能。 請瀏覽各 AWS 區域的功能可用性，查看支援的資源。	2023 年 8 月 22 日
AWS Backup Audit Manager 員現在支援委派的管理員	AWS Backup Audit Manager 員報告產生現在可由委派的管理員帳戶存取。如需詳細資訊，請參閱 • 使 AWS Backup 用稽核 Audit Manager 備份並建立報告 • 使用稽核報告 • 委派的管理員	2023 年 8 月 16 日

變更	描述	日期
預覽邏輯氣隙隔離備份文件庫	AWS Backup 現在提供新型備份儲存庫的預覽，以協助補充資料保護作業。 如需詳細資訊，請參閱邏輯氣隙隔離保存庫 (預覽)。	2023 年 8 月 8 日
AWS Backup 增強 Amazon S3 備份	AWS Backup 提升 S3 儲存貯體備份的效能、大小和速度功能。 如需詳細資訊，請參閱 Amazon S3 備份。	2023 年 8 月 1 日
中國數個區域現可使用標記還原功能	現在於中國 (北京) 或中國 (寧夏) 區域建立還原任務時，可以複製屬於備份一部分的標籤。 如需詳細資訊，請參閱還原時複製標籤。	2023 年 7 月 17 日
AWS Backup 現在在其他區域支援 Amazon S3	AWS Backup Amazon S3 支援現已在歐洲 (西班牙)、歐洲 (蘇黎世)、亞太區域 (海德拉巴) 和亞太區域 (墨爾本) 區域提供。 如需詳細資訊，請參閱各區域的功能可用性。	2023 年 7 月 6 日

變更	描述	日期
跨帳戶複製擴展至其他區域	AWS Backup 現在支援以下地區大部分資源的跨帳戶備份副本：亞太區域 (雅加達)、中東 (巴林)、亞太區域 (香港)、非洲 (開普敦)、歐洲 (米蘭)、亞太區域 (大阪)、中東 (阿聯酋)、歐洲 (西班牙)、歐洲 (蘇黎世)、亞太區域 (海德拉巴) 和亞太區域 (墨爾本)。 如需詳細資訊，請參閱各區域的功能可用性	2023 年 7 月 5 日
Backup Audit Manager 可在 GovCloud 區域使用	AWS Backup 已將 AWS Backup Audit Manager 擴展至 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部)。 如需詳細資訊，請參閱各區域的功能可用性	2023 年 6 月 29 日
跨帳戶管理現已在區域提供 GovCloud	AWS Backup 現在支援 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 的資源跨帳戶管理。 如需詳細資訊，請參閱跨多個 AWS 帳戶管理 AWS Backup 資源。	2023 年 6 月 29 日

變更	描述	日期
支援在其他區域使用的 Amazon Aurora 跨區域副本	AWS Backup 現在支援 Aurora 叢集進出以下區域的跨區域備份副本：亞太區域 (雅加達)、中東 (巴林)、亞太區域 (香港)、非洲 (開普敦)、歐洲 (米蘭)、中東 (阿聯酋)、歐洲 (西班牙)、歐洲 (蘇黎世)、亞太區域 (海德拉巴) 和亞太區域 (墨爾本)。	2023 年 6 月 5 日
還原時複製標籤	現在建立還原任務時，可以複製屬於備份一部分的標籤。 如需詳細資訊，請參閱還原時複製標籤。	2023 年 5 月 22 日
AWS Backup 與 AWS 使用者通知整合	您現在可以選擇透過 AWS 使用者通知主控台接收與備份、複製和還原事件相關的通知。 如需詳細資訊，請參閱開始 AWS 使用使用者通知。	2023 年 5 月 10 日
四個新區域提供跨區域備份功能	AWS Backup 現在支援中東 (阿拉伯聯合大公國) 區域、歐洲 (西班牙) 區域、歐洲 (蘇黎世) 區域和亞太區域 (海德拉巴) 區域的跨區域備份。	2023 年 4 月 28 日
擴充的跨區域 AWS Backup 副本支援	您現在可於下列區域跨區域備份 Amazon EFS、VMware 和 DynamoDB 資源：亞太區域 (雅加達)、中東 (巴林)、亞太區域 (香港)、非洲 (開普敦) 和歐洲 (米蘭)。	2023 年 4 月 28 日

變更	描述	日期
南美洲 (聖保羅) 區域可備份和還原 Amazon S3	AWS Backup 南美洲 (聖保羅) 區域現已提供 Amazon S3 (Amazon 簡易儲存服務) 的支援。 如需詳細資訊，請參閱 Amazon S3 備份。	2023 年 4 月 20 日
AWS Backup 擴展至亞太區域 (墨爾本)	AWS Backup 亞太區域 (墨爾本) 區域現已推出。 如需詳細資訊，請參閱依 AWS 區域提供的功能。	2023 年 4 月 20 日
Amazon S3 的擴展區域支援	AWS Backup Amazon S3 (Amazon 簡易儲存服務) 的支援現已在 AWS GovCloud (美國東部) 和 AWS GovCloud (美國西部) 區域提供 如需詳細資訊，請參閱 Amazon S3 備份。	2023 年 4 月 19 日
在 Amazon EC2 執行個體上備份與還原 SAP HANA 資料庫	AWS Backup 現在提供備份和還原大部分區域 Amazon EC2 執行個體上執行的 SAP HANA 資料庫的功能。 如需詳細資訊，請參閱 Amazon EC2 執行個體上的 SAP HANA 資料庫備份。	2023 年 4 月 17 日

變更	描述	日期
AWS Backup 現已在歐洲 (西班牙)、歐洲 (蘇黎世) 和亞太區域 (海德拉巴) 區域推出	AWS Backup 支援服務已擴展至新地區，包括歐洲 (西班牙)、歐洲 (蘇黎世) 和亞太區域 (海德拉巴)。您可以在這些區域中備份和還原支援的資源。 如需詳細資訊，請參閱依 AWS 區域提供的功能。	2023 年 4 月 13 日
更新的 AWS 受管政策 `AWSBackupAuditAccess`	已更新 AWS 受管理策略AWSBackupAuditAccess。AWS Backup 將 API 中的資源選取取代為萬`config:DescribeComplianceByConfigRule` 用字元資源。 如需詳細資訊，請參閱 AWS Backup的政策更新。	2023 年 4 月 11 日
使用 Amazon 日誌的管理程序 CloudWatch	AWS Backup 閘道使用者現在可以將 Hypervisor 與 CloudWatch 記錄檔整合，以維護記錄檔。如需詳細資訊，請參閱編輯 Hypervisor 組態和 CloudWatch 記錄。	2023 年 3 月 29 日
Amazon S3 的擴展區域支援	AWS Backup 亞太區域 (雅加達) 和中東 (阿拉伯聯合大公國) 區域現已提供 Amazon S3 支援。	2023 年 3 月 22 日

變更	描述	日期
虛擬機器增量備份改善	發生 CBT (已變更區塊追蹤) 資料問題的 VMware VM (虛擬機器) 備份現在包含其他資訊，可協助修正及故障診斷。 如需詳細資訊，請參閱增量 VM 備份和虛擬機器故障診斷。	2023 年 3 月 15 日
AWS Backup 支援多個網路介面卡	AWS Backup 閘道現在支援設定多個網路介面卡 如需有關設定網路介面卡的詳細資訊，請參閱《AWS Backup 開發人員指南》中的在 VMware 中為多個 NIC 設定閘道。	2023 年 3 月 8 日
AWS Backup vSphere 援	AWS Backup 現在支援備份和還原在 VMware vSphere 8 上執行的虛擬機器。 如需支援的 VMware 選項詳細資訊，請參閱《AWS Backup 開發人員指南》中之支援的 VM。	2023 年 3 月 8 日
AWS Backup Audit Manager 支援 Amazon RDS 異地同步備份備份	Backup Audit Manager 現在提供 Amazon Relational Database Service 多可用區域備份的支援。 如需詳細資訊，請參閱如何使 AWS Backup 用稽核 Audit Manager 備份和建立報告。	2023 年 2 月 1 日

變更	描述	日期
AWS Backup 為 Amazon Timestream 表提供增量備份	AWS Backup 現在為時間流備份提供了擴展的備份功能。備份計畫現可採用增量備份，減少備份 Timestream 資源所需的時間並降低儲存成本。 如需詳細資訊，請參閱 Amazon Timestream 備份。	2023 年 1 月 23 日
AWS Backup 現已在杜拜推出	AWS Backup 已擴展到中東（阿聯酋）區域。您可在這個區域中備份與還原支援的資源。	2023 年 1 月 17 日
其他區域可執行跨區域複製作業	AWS Backup 現在，大部分資源都在亞太區域 (雅加達) 區域、中東 (巴林) 區域、亞太區域 (香港) 區域、非洲 (開普敦) 區域和歐洲 (米蘭) 區域提供跨區域備份服務。 如需詳細資訊，請參閱跨 AWS 區域建立備份副本。	2022 年 12 月 21 日

變更	描述	日期
備份閘道頻寬限制和限流	AWS Backup 閘道現在允許限制閘道的上傳輸量， AWS Backup 以控制閘道使用的網路頻寬量。 為了支援此功能， AWS Backup 已建立並更新受管理的政策，包括AWSBackupFullAccess 和AWSBackupOperatorAccess 。 如需詳細資訊，請參閱備份閘道頻寬限流。	2022 年 12 月 15 日
備份閘道 VMware 標籤支援	AWS Backup 閘道現在支援 VMware 標籤。使用者可以更靈活地建立 AWS 符合用於虛擬機器之標籤的標籤。 為了支援此功能， AWS Backup 已建立並更新受管理的策略AWSBackupGatewayServiceRolePolicyForVirtualMachineMetadataSync ，包括AWSBackupFullAccess 、和AWSBackupOperatorAccess 。 如需詳細資訊，請參閱 VMware 標籤。	2022 年 12 月 15 日
AWS Backup Amazon Timestream 的支持	AWS Backup 現在支援備份和還原 Amazon Timestream 表格。如需詳細資訊，請參閱 Amazon Timestream 備份。	2022 年 12 月 13 日

變更	描述	日期
AWS Backup 提供法律持有	AWS Backup 推出了一種新工具，以幫助通過合法保存來保護恢復點。如需詳細資訊，請參閱法務保存。	2022 年 11 月 27 日
AWS Backup Audit Manager 跨區域與跨帳戶報告	AWS Backup Audit Manager 為合規性和工作報告帶來額外的功能。使用者可以產生包含多個區域和多個帳戶的報告。 如需詳細資訊，請參閱使用稽核報告。	2022 年 11 月 27 日
AWS Backup 支持 Amazon Redshift	AWS Backup 現在提供備份 Amazon Redshift 叢集和恢復 Amazon Redshift 叢集和表格的支援。如需詳細資訊，請參閱 Amazon Redshift 備份。	2022 年 11 月 27 日
AWS Backup 提供備份 AWS CloudFormation 應用程式堆疊的支援	AWS Backup 透過備份堆疊 CloudFormation 並還原堆疊中的資源，提供備份和還原包含多個資源之應用程式的功能。 如需詳細資訊，請參閱應用程式堆疊備份。	2022 年 11 月 27 日
AWS Backup 提供委派的管理員帳戶和備份政策委派	AWS Backup 註冊的帳戶 AWS Organizations 可以將成員帳戶指定為委派管理員帳戶。 如需詳細資訊，請參閱使用管理多個帳戶 AWS Organizations。	2022 年 11 月 27 日

變更	描述	日期
在 Amazon EC2 執行個體上備份與還原 SAP HANA 的公開預覽	AWS Backup AWS Backint 提供功能的整合式公開預覽功能，以備份和還原 EC2 執行個體上的 SAP HANA 資料庫。 如需詳細資訊，請參閱我們的公開預覽 Amazon EC2 執行個體上的 SAP HANA。 為了支援此預覽， AWS Backup 已針對這些功能提供原則更新和新的AWS 受管理原則。	2022 年 11 月 20 日
將 VMware 還原到 Amazon EC2 執行個體	AWS Backup 除了能夠將機器還原到 EBS、VMware、VMware 雲和 VMware 雲上 AWS，現在還提供將虛擬機器還原到 Amazon EC2 執行個體的 AWS Outposts功能。 如需詳細資訊，請參閱如何使用 AWS Backup 主控台還原虛擬機器復原點的文件。	2022 年 11 月 9 日
擴充 AWS Backup 資料庫鎖定功能	AWS Backup 現在可以在治理模式下建立文件庫鎖定以獲得額外的 IAM 保護，或在合規模式下建立，以確保不變性。 在 AWS Backup Vault Lock 中進一步了解。	2022 年 10 月 4 日

變更	描述	日期
AWS Backup Audit Manager 現已在非洲（開普敦）地區和歐洲（米蘭）地區提供服務	AWS Backup Audit Manager 已擴展到非洲（開普敦）地區和歐洲（米蘭）地區。如需有關 Backup Audit Manager 的詳細資訊，請參閱稽核備份和使用 AWS Backup Audit Manager 建立報告。	2022 年 9 月 14 日
AWS Backup 將 Amazon CloudWatch 指標帶入 Backup 主控台儀表板	AWS Backup 增強其 Backup 主控台儀表板，以顯示用於備份和還原任務的整合式 Amazon CloudWatch 指標，以提供額外的監控功能和彈性	2022 年 9 月 8 日
支援還原期間的額外 Amazon EBS 加密彈性	AWS Backup 現在可在 Amazon EBS 快照還原期間提供額外的加密選項。	2022 年 9 月 1 日
AWS Backup 支援 Amazon S3 跨帳戶和跨區域備份複製	AWS Backup 現在為 Amazon S3 備份提供跨區域和跨帳戶備份複製功能。 如需詳細資訊，請參閱 Amazon S3 備份。	2022 年 7 月 28 日
AWS Backup Audit Manager 為 ONTAP 的 FSx 提供額外的控制支援	AWS Backup Audit Manager 現在提供額外的控制項，以支援 ONTAP 磁碟區的 FSx 監視和稽核，包括 Backup 資源受備份計畫保護，以及上次建立的復原點。 如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補。	2022 年 7 月 22 日

變更	描述	日期
AWS Backup 增加對備份和還原 Amazon RDS 異地同步 PostgreSQL 叢集的 MySQL 援	AWS Backup 已新增多重可用區域叢集備份與還原選項，其中包含一個主要和兩個可讀取的待命資料庫執行個體 若要進一步了解，請參閱 Amazon RDS Multi-AZ 備份。	2022 年 7 月 20 日
AWS Backup Audit Manager 為復原點建立新增控制	AWS Backup Audit Manager 提供新的稽核控制，以增加合規性支援。 `Last recovery point created` 是選用的額外控制項，以確保在指定的時間範圍內建立復原點。 若要進一步了解，請參閱上次建立的復原點控制項。	2022 年 6 月 29 日
新增 AWS Backup 閘道端點範例	AWS Backup 閘道提供了一個範例端點，以協助使用者連線至 VPN (虛擬私人網路)。如需詳細資訊，請參閱建立 AWS Backup VPC 端點。	2022 年 6 月 14 日
AWS Backup 現在提供適用於 VMware 的 Amazon VPC 端點	AWS Backup 現在支援適用於 VMware 的 Amazon VPC 端點，讓您能夠在 VMware 環境和 AWS 使用之間使 AWS PrivateLink用虛擬私有網路。 如需詳細資訊，請參閱建立閘道以及 AWS Backup 和 AWS PrivateLink。	2022 年 6 月 1 日

變更	描述	日期
AWS Backup Audit Manager 為 Amazon S3 提供額外的控制支援	Backup Audit Manager 現在為 S3 資源類型提供受備份計畫保護的備份資源合規控制項支援。 如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補。	2022 年 5 月 25 日
AWS Backup Audit Manager 為 Storage Gateway 提供額外的控制支援	Backup Audit Manager 現在為 Storage Gateway 資源類型提供受備份計畫保護的備份資源合規控制項支援。 如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補。	2022 年 5 月 25 日
支援 Amazon FSx for OpenZFS	AWS Backup 現在提供額外的資料保護管理功能，以備份及還原至 OpenZFS 檔案系統的 FSx。	2022 年 5 月 18 日
AWS Backup 針對 VMware 的 Audit Manager 支援	AWS Backup 現在可在 Backup Audit Manager 控制和修復中為虛擬機器提供支援。如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補。	2022 年 5 月 11 日
亞太區域 (大阪) 區域現支援 Amazon FSx	AWS Backup 現在提供 Amazon FSx 在亞太區域 (大阪) 區域之間和跨區域複本的備份服務。	2022 年 4 月 26 日

變更	描述	日期
支援 Amazon FSx for Lustre Persistent_2	AWS Backup 現在提供適用於 Lustre 的 Amazon FSx 的正式支援，相較於永久性 _1 檔案系統，支援每個儲存單位的輸送量更高層級。	2022 年 4 月 5 日
VMware 增強功能	AWS Backup 現在提供恢復到 Amazon EBS 磁碟區、磁碟層級還原，以及對於 AWS Outposts VMware 的支援。如需詳細資訊，請參閱還原虛擬機器。	2022 年 3 月 31 日
AWS Backup 亞太區域 (雅加達) 的可用性	AWS Backup 亞太區域 (雅加達) 區域的客戶現已開放使用。	2022 年 3 月 17 日
AWS Backup Audit Manager 的新控制項	AWS Backup Audit Manager 引進了三個新的稽核控制：跨區域複製、跨帳戶複製和 Backup 文件庫鎖定。如需詳細資訊，請參閱 AWS Backup Audit Manager 控制項與修補。	2022 年 3 月 17 日
Support AWS PrivateLink	使用 AWS PrivateLink for AWS Backup，您可以直接連線到 AWS Backup 使用 VPC 中的介面端點，而不是透過公用網際網路進行連線。介面端點可從內部部署或不同 AWS 區域的應用程式直接存取。如需更多資訊，請參閱AWS Backup 和 AWS PrivateLink。	2022 年 2 月 28 日

變更	描述	日期
支援 Amazon Simple Storage Service (Amazon S3)	除中國 (北京) 區域、中國 (寧夏) 區域、(美國西部) 和 AWS GovCloud AWS GovCloud (美國東部) 區域外，所有 Amazon S3 均可 AWS 區域 正式使用。AWS Backup 如需詳細資訊，請參閱使用 Amazon S3 資料。	2022 年 2 月 14 日
Support 中國區域的進階 DynamoDB 備份 AWS	中國 (北京) 區域和中國 (寧夏) 區域現可使用進階 DynamoDB 備份。如需詳細資訊，請參閱進階 DynamoDB 備份。	2022 年 1 月 18 日
Amazon S3 公開預覽支援	AWS Backup 提供 Amazon S3 備份的公開預覽。如需詳細資訊，請參閱 使用 Amazon S3 資料。	2021 年 11 月 30 日
支援 VMware 虛擬機器	您現在可以使 AWS Backup 用自動備份 VMware 虛擬機器。如需詳細資訊，請參閱 虛擬機器備份。	2021 年 11 月 30 日

變更	描述	日期
支援進階 DynamoDB 備份	您現在可以針對您建立的所有新 DynamoDB 表備份使用 AWS Backup 下列功能：冷儲存分層、成本配置標記、跨區域副本、跨帳戶複製、Indpendent 加密，以及從來源 DynamoDB 表複製標籤。如需詳細資訊，請參閱 Amazon DynamoDB 開發人員指南進階 DynamoDB 備份中的和與 Dynam oDB AWS Backup 搭配使用。	2021 年 11 月 23 日
Support 提升 AWS 中國地區的 AWS Backup 資源分配	AWS Backup 中國（北京）地區和中國（寧夏）地區現已提供資源分配增強功能。如需詳細資訊，請參閱將資源指派到備份計畫。	2021 年 11 月 16 日
啟動 AWS Backup 資源分配增強功能	Backup 資源指派增強功能為您提供額外、精細的控制項和全新的簡化程序，以部署備份計劃，以保護數十萬個資 AWS 源。使用此功能可在保護資料時利用 AWS Backup提高速度、彈性和精確度。如需詳細資訊，請參閱將資源指派到備份計畫。	2021 年 11 月 10 日
支援 Amazon Neptune	您現在可以使 AWS Backup 用備份 Amazon Neptune 叢集。如需進一步了解，請參閱什麼是 AWS Backup？	2021 年 11 月 5 日

變更	描述	日期
支援 Amazon DocumentDB	您現在可以使 AWS Backup 用備份 Amazon DocumentDB 集群。如需進一步了解，請參閱什麼是 AWS Backup？	2021 年 11 月 5 日
Support AWS 中國地區的 AWS Backup 文件庫鎖定	AWS Backup 文件庫鎖定現已在中國 (北京) 地區和中國 (寧夏) 區域推出。如需詳細資訊，請參閱 AWS Backup Vault Lock 。	2021 年 11 月 3 日
啟動文件 AWS Backup 庫鎖定	使用文件 AWS Backup 庫鎖定，您可以防止刪除儲存在 AWS Backup 備份保險箱中的備份。如需詳細資訊，請參閱 AWS Backup Vault Lock 。	2021 年 10 月 7 日
啟動 AWS Backup Audit Manager 規範遵循報告	使用合規性報告，您可以根據您在 AWS Backup Audit Manager 架構中定義的控制項，產生備份活動和資源合規性的每日報告。如需詳細資訊，請參閱合規報告範本。	2021 年 10 月 5 日
AWS CloudFormation AWS Backup Audit Manager 的支援	有了 AWS CloudFormation，您現在可以以安全、可重複的方式大規模部署 AWS Backup Audit Manager 架構、控制項和報告計劃。如需詳細資訊，請參閱使用稽核管理員 Backup AWS Backup 稽核和報告。	2021 年 10 月 4 日

變更	描述	日期
啟動 AWS Backup Audit Manager	使用 AWS Backup Audit Manager，您現在可以定義備份活動和資源的控制項，並識別不符合您控制項的活動和資源。您也可以使用 AWS Backup Audit Manager 產生每日和隨選報告，這些報告可作為一段時間內符合您定義的控制項的證明。如需詳細資訊，請參閱使用稽核管理員 Backup AWS Backup 稽核和報告。	2021 年 8 月 24 日
支援新的非同步復原點作業	AWS Backup 現在假設您修改或刪除原始 IAM 角色時，會採用服務連結角色來管理備份生命週期規則。如需詳細資訊，請參閱刪除備份。	2021 年 8 月 23 日
支援 Amazon EBS 的多磁碟區當機一致備份	現在，當您使用保護 Amazon EC2 執行個體時，依預設，會對連 AWS Backup 接 AWS Backup 到每個 Amazon Amazon EC2 執行個體的所有 Amazon EBS 磁碟區進行多磁碟區、當機一致性備份。如需詳細資訊，請參閱建立 Amazon EBS 的多磁碟區當機一致備份。	2021 年 6 月 14 日

變更	描述	日期
對 Amazon FSx 的 Support 額外 AWS 區域	您現在可以用 AWS Backup 來保護下列區域的 Amazon FSx 檔案系統： AWS GovCloud (US)、歐洲 (米蘭) 區域、非洲 (開普敦) 區域和中東 (巴林) 區域。如需詳細資訊，請參閱《AWS 一般參考》中的 AWS Backup 端點和配額。	2021 年 4 月 15 日
支援 Amazon FSx 跨區域和跨帳戶備份	您現在可以使 AWS Backup 用跨 AWS 區域 帳戶複製 Amazon FSx 備份。如需詳細資訊，請參閱建立備份副本。 如果您使用客戶管理政策，建議您新增許可 `fsx:CopyBackup` 以防止現有的備份任務失敗。如需該許可，請參閱客戶管理政策中，Amazon FSx 備份政策的最後一個陳述式。	2021 年 4 月 12 日
支援 Amazon EFS 備份的成本分配標籤	您現在可以使用成本分配標籤在詳細層級追蹤 Amazon EFS 備份的成本，並使用檢視和篩選這些標籤 AWS Cost Explorer。如需詳細資訊，請參閱使用成本分配標籤。	2021 年 4 月 7 日
FedRAMP 高級授權	AWS Backup 現已獲得授權，可支援 FedRAMP 高工作負載。如需詳細資訊，請參閱合規計畫的AWS 服務範圍。	2021 年 3 月 25 日

變更	描述	日期
新 AWS 區域	AWS Backup 亞太區域 (大阪) 區域現已推出。 AWS Backup 目前不支援此區域中的 Storage Gateway、Amazon FSx 和跨帳戶備份。如需詳細資訊，請參閱《AWS 一般參考》中的 AWS Backup 端點和配額。	2021 年 3 月 25 日
支援復原點批次作業	您現在可以使用主 AWS Backup 控台自動執行批次作業，以清除備份儲存庫中的復原點。如需詳細資訊，請參閱刪除備份。	2021 年 3 月 23 日
支援還原至 Amazon EFS One Zone 儲存類別	您現在可以將 Amazon EFS 備份還原到 Amazon EFS One Zone 儲存類別。如需詳細資訊，請參閱還原 Amazon EFS 檔案系統。	2021 年 3 月 12 日
Support Amazon 關聯式資料庫服務 point-in-time 還原和持續備份	除了協調快照備份之外，您現在 point-in-time 還可以使用 AWS Backup 自動化 Amazon RDS 連續備份和執行還原 (PITR)。如需詳細資訊，請參閱使用 point-in-time 復原還原到指定的時間。	2021 年 3 月 10 日
Support Amazon CloudWatch	您現在可以使用 CloudWatch 來監視 AWS Backup 指標。如需詳細資訊，請參閱使用 Amazon 和 Amazon 監控事件 CloudWatch 和指標 EventBridge。	2021 年 2 月 3 日

變更	描述	日期
Support Amazon EventBridge	您現在可以使用 EventBridge 來監視 AWS Backup 事件。如需詳細資訊，請參閱使用 Amazon 和 Amazon 監控事件 CloudWatch 和指標 EventBridge。	2021 年 2 月 3 日
支援跨帳戶備份	您現在可以 AWS Backup 使用跨多個備份資源 AWS 帳戶。如需詳細資訊，請參閱跨 AWS 帳戶建立備份副本。	2020 年 11 月 18 日
支援備份和還原 Amazon FSx 檔案系統	您現在可以使 AWS Backup 用備份 Amazon FSx 檔案系統。如需詳細資訊，請參閱使用 Amazon FSx 檔案系統。	2020 年 11 月 9 日
新 AWS 區域	AWS Backup 現已在非洲（開普敦）和歐洲（米蘭）上市 AWS 區域。如需詳細資訊，請參閱《AWS 一般參考》中的 AWS Backup 端點和配額。	2020 年 10 月 21 日
支援啟用 VSS 的 Windows 備份	您現在可以備份及還原在 Amazon EC2 執行個體上執行，啟用 VSS (磁碟區陰影複製服務) 的 Windows 應用程式。如需詳細資訊，請參閱建立 Windows VSS 備份。	2020 年 9 月 22 日
支援 Amazon EFS 的自動備份	您現在可以用 AWS Backup 來自動備份 Amazon EFS 檔案系統。如需詳細資訊，請參閱入門 4：建立 Amazon EFS 自動備份。	2020 年 7 月 16 日

變更	描述	日期
新 AWS 區域	AWS Backup 現在可在中使用 AWS GovCloud (US) Region。如需詳細資訊，請參閱《AWS 一般參考》中的AWS Backup 端點和配額。	2020 年 6 月 24 日
Support 管理多個備份 AWS 帳戶	您現在可以使用管理多 AWS 帳戶 個備份AWS Organizations。如需詳細資訊，請參閱跨帳戶管理的運作方式。	2020 年 6 月 24 日
對 Amazon Aurora 的 Support 已添加到 AWS Backup	您現在可以設定 AWS Backup 為備份 Amazon Aurora 的資源。如需詳細資訊，請參閱《Amazon Aurora 使用者指南》中的備份與還原 Aurora 資料庫叢集概觀。	2020 年 6 月 10 日
Support 設定要搭配使用的服務 AWS Backup	您現在可以設定 AWS Backup 為備份特定 AWS 服務的資源。如需詳細資訊，請參閱使用選擇加入管理服務 AWS Backup。	2020 年 5 月 20 日
支援備份 Amazon EC2 執行個體，並新增對跨區域備份的支援。	您現在可以備份整個 Amazon EC2 執行個體，也可以跨 AWS 區域複製資源。如需詳細資訊，請參閱跨 AWS 區域建立備份副本。	2020 年 1 月 13 日
新指南	AWS 啟動 AWS Backup 和AWS Backup 開發人員指南。	2019 年 1 月 15 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。